Scanning Networks

Module 03

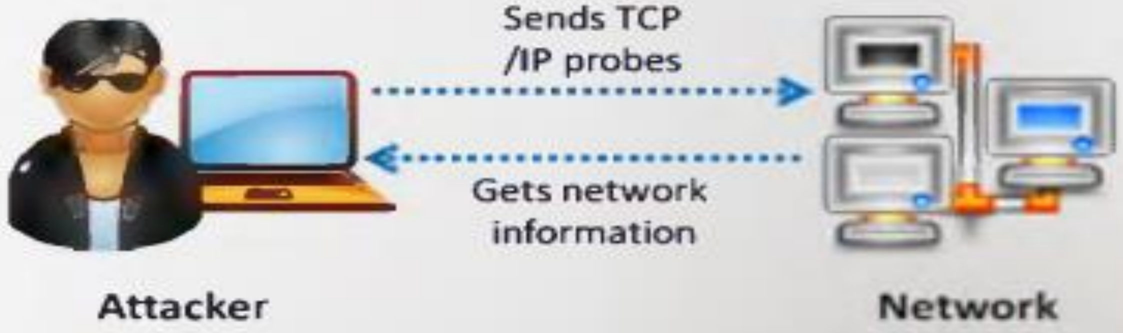
Module Objectives

- Overview of Network Scanning
- CEH Scanning Methodology
- Checking for Live Systems
- Scanning Techniques
- IDS Evasion Techniques
- Banner Grabbing
- Vulnerability Scanning
- Drawing Network Diagrams

- Use of Proxies for Attack
- Proxy Chaining
- HTTP Tunneling Techniques
- SSH Tunneling
- Anonymizers
- IP Spoofing Detection Techniques
- Scanning Countermeasures
- Scanning Pen Testing

Overview of Network Scanning

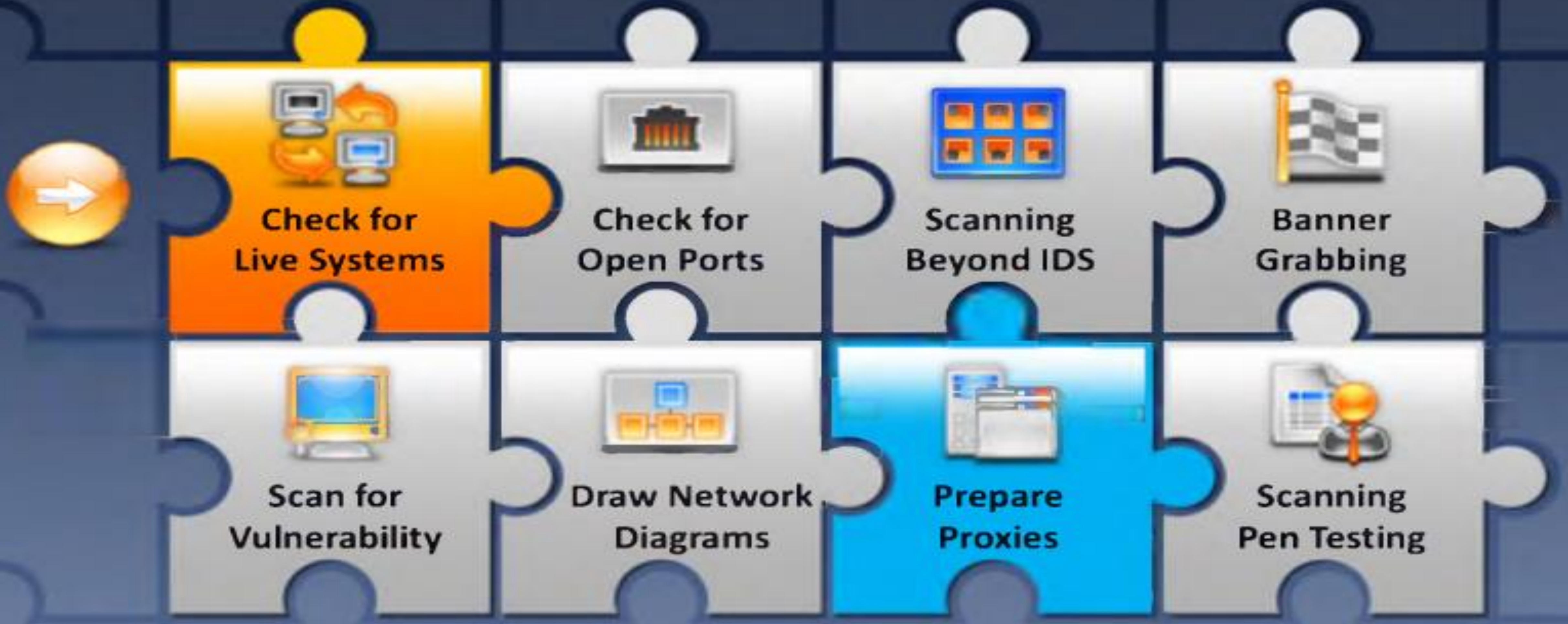
- Network scanning refers to a set of procedures for **identifying hosts, ports,** and **services in a network**
- Network scanning is one of the **components of intelligence gathering** an attacker uses to create a profile of the target organization



Objectives of Network Scanning

- To discover live hosts, IP address, and open ports of live hosts
- To discover operating systems and system architecture
- To discover services running on hosts
- To discover vulnerabilities in live hosts

Scanning Methodology



Check for Live Systems

Check for Open Ports

Scanning Beyond IDS

Banner Grabbing

Scan for Vulnerability

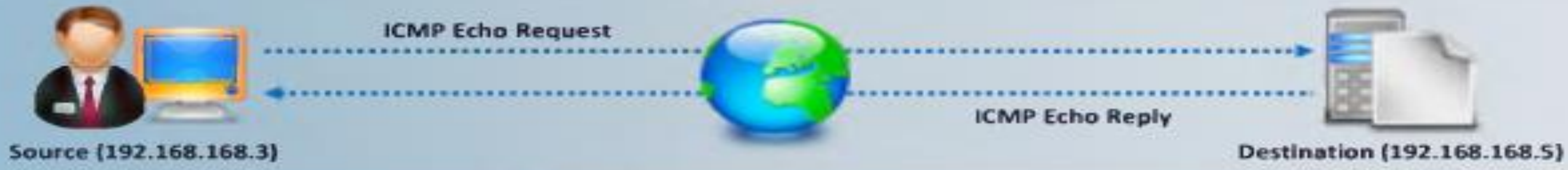
Draw Network Diagrams

Prepare Proxies

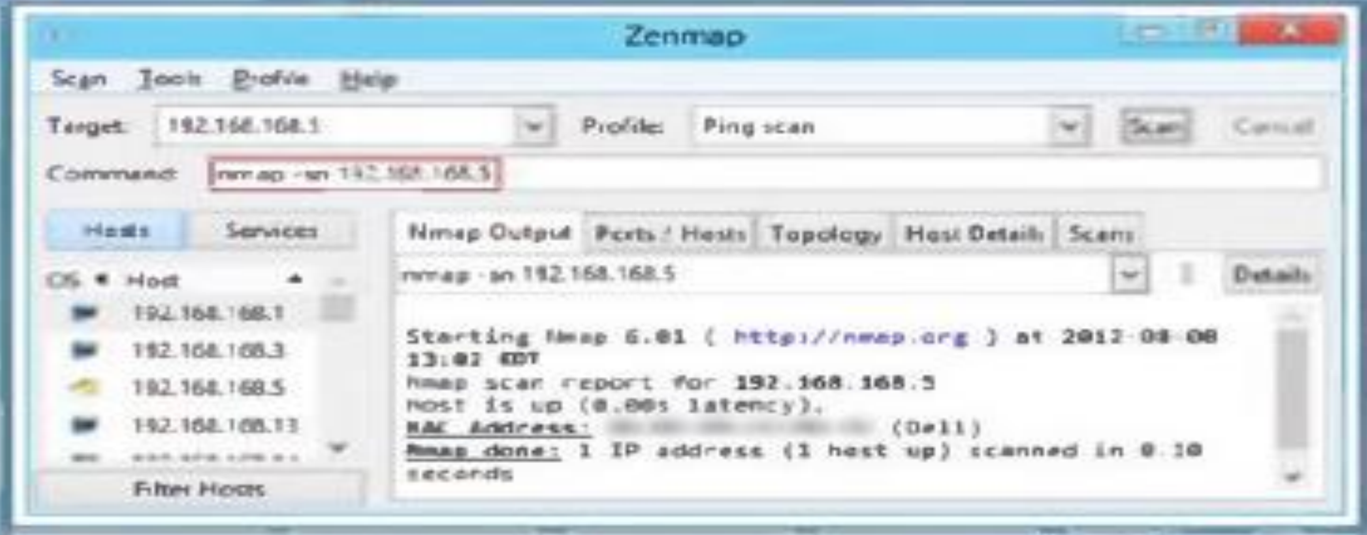
Scanning Pen Testing

Checking for Live Systems - ICMP Scanning

- Ping scan involves sending **ICMP ECHO requests** to a host. If the host is live, it will return an ICMP ECHO reply
- This scan is useful for **locating active devices** or determining if **ICMP is passing through a firewall**



The ping scan output using Nmap:



Target: 192.168.168.1

Profile: Ping scan

Command: nmap -sn 192.168.168.5

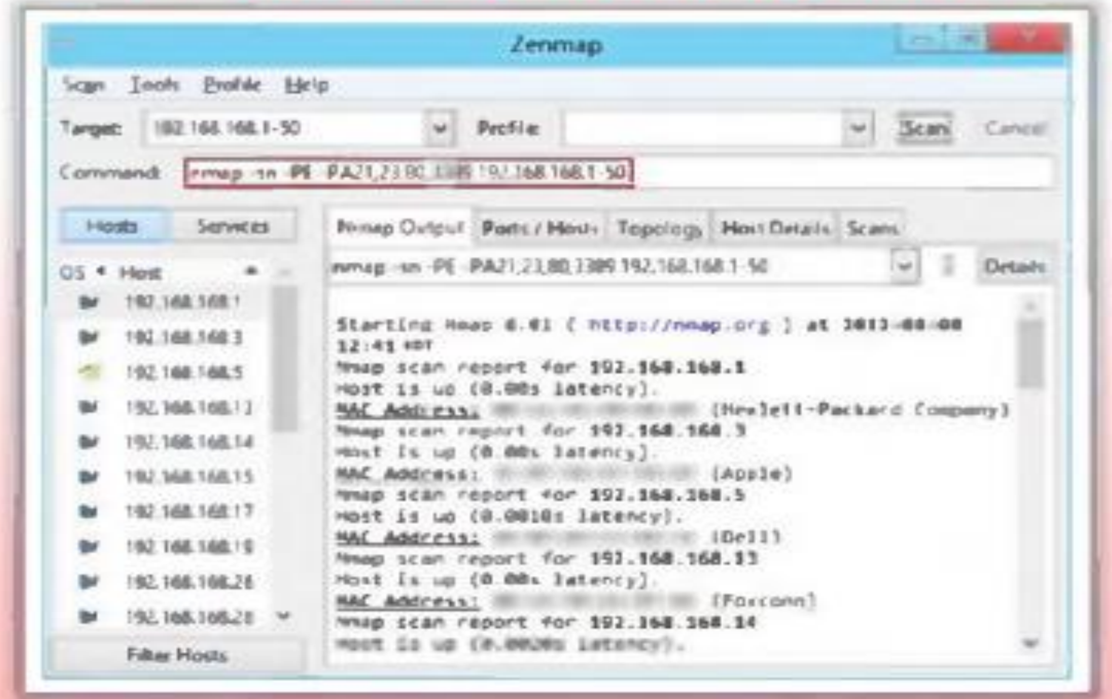
```
nmap -sn 192.168.168.5

Starting Nmap 6.01 ( http://nmap.org ) at 2012-08-08
13:02 EDT
Nmap scan report for 192.168.168.5
Host is up (0.00s latency).
MAC Address: [redacted] (Dell)
Nmap done: 1 IP address (1 host up) scanned in 0.10
seconds
```

http://nmap.org

Ping Sweep

- Ping sweep is used to determine the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts. If a host is live, it will return an ICMP ECHO reply
- Attackers calculate subnet masks using Subnet Mask Calculators to identify the number of hosts present in the subnet
- Attackers then use ping sweep to create an inventory of live systems in the subnet

The ping sweep output using Nmap



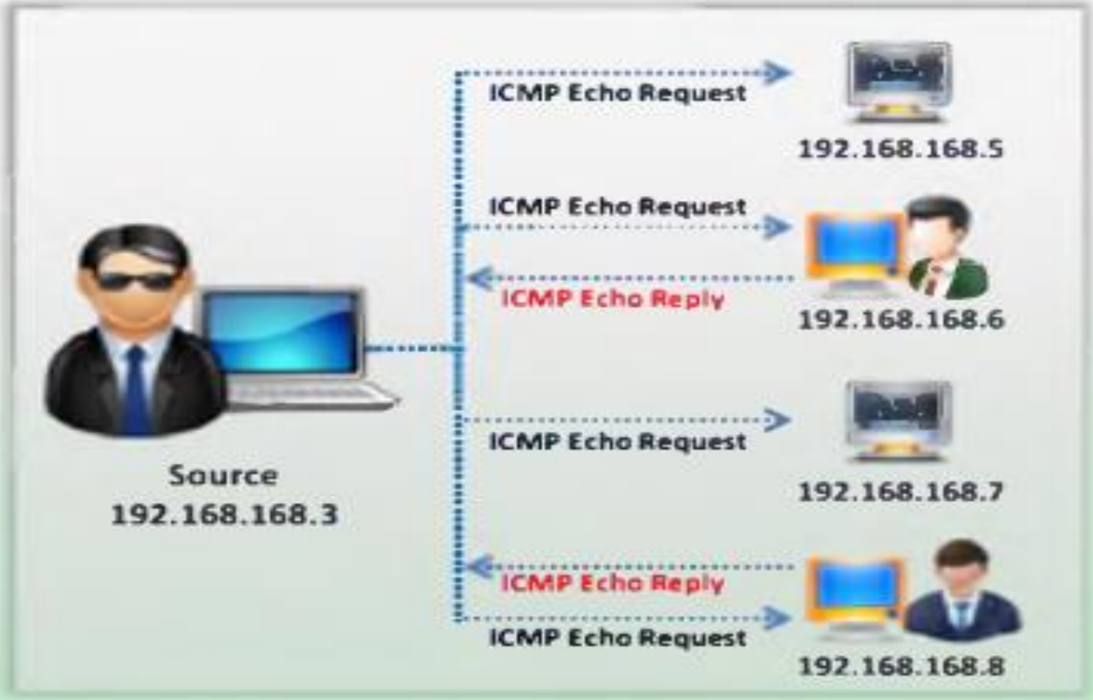
Target: 192.168.168.1-50

Command: nmap -sn -PE -PA21,23,80,3389 192.168.168.1-50

OS	Host
	192.168.168.1
	192.168.168.3
	192.168.168.5
	192.168.168.13
	192.168.168.14
	192.168.168.15
	192.168.168.17
	192.168.168.19
	192.168.168.26
	192.168.168.28

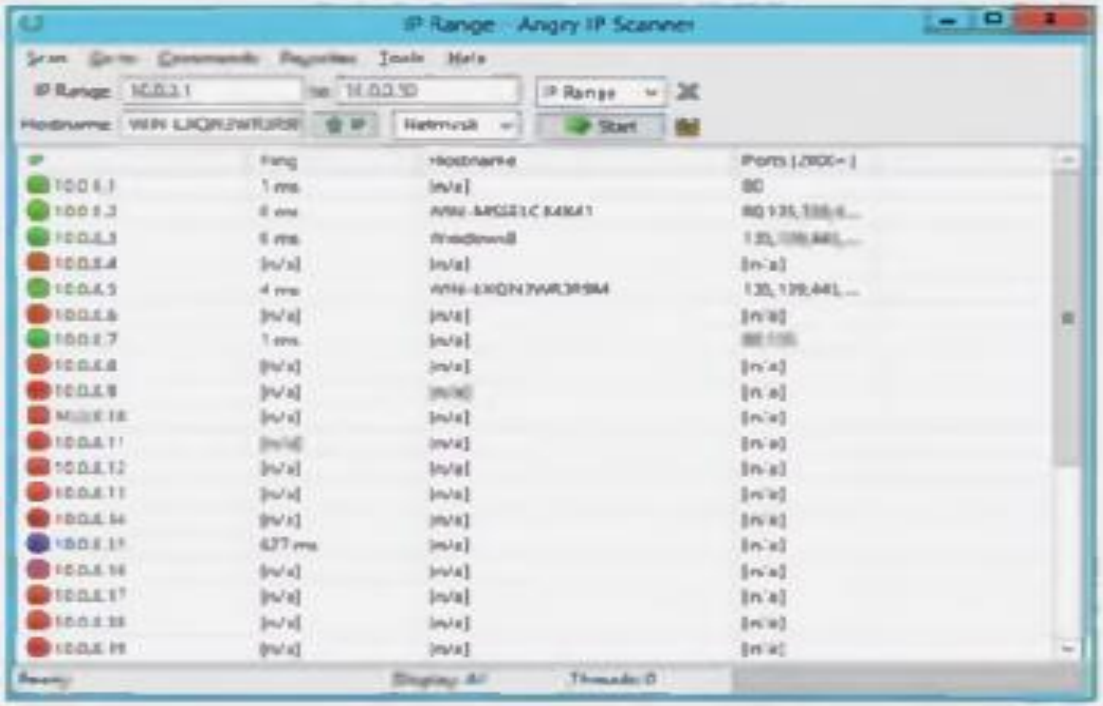
```
nmap -sn -PE -PA21,23,80,3389 192.168.168.1-50

Starting Nmap 6.01 ( http://nmap.org ) at 2013-08-08
12:41 EDT
Nmap scan report for 192.168.168.1
Host is up (0.00s latency).
MAC Address: [redacted] (Hewlett-Packard Company)
Nmap scan report for 192.168.168.3
Host is up (0.00s latency).
MAC Address: [redacted] (Apple)
Nmap scan report for 192.168.168.5
Host is up (0.0010s latency).
MAC Address: [redacted] (Dell)
Nmap scan report for 192.168.168.13
Host is up (0.00s latency).
MAC Address: [redacted] (Foxconn)
Nmap scan report for 192.168.168.14
Host is up (0.00020s latency).
```

http://nmap.org



Ping Sweep Tools

Angry IP Scanner pings each IP address to check if it's alive, then optionally resolves its hostname, determines the MAC address, scans ports, etc.



IP Range: 10.0.0.1 to: 10.0.0.50 IP Range

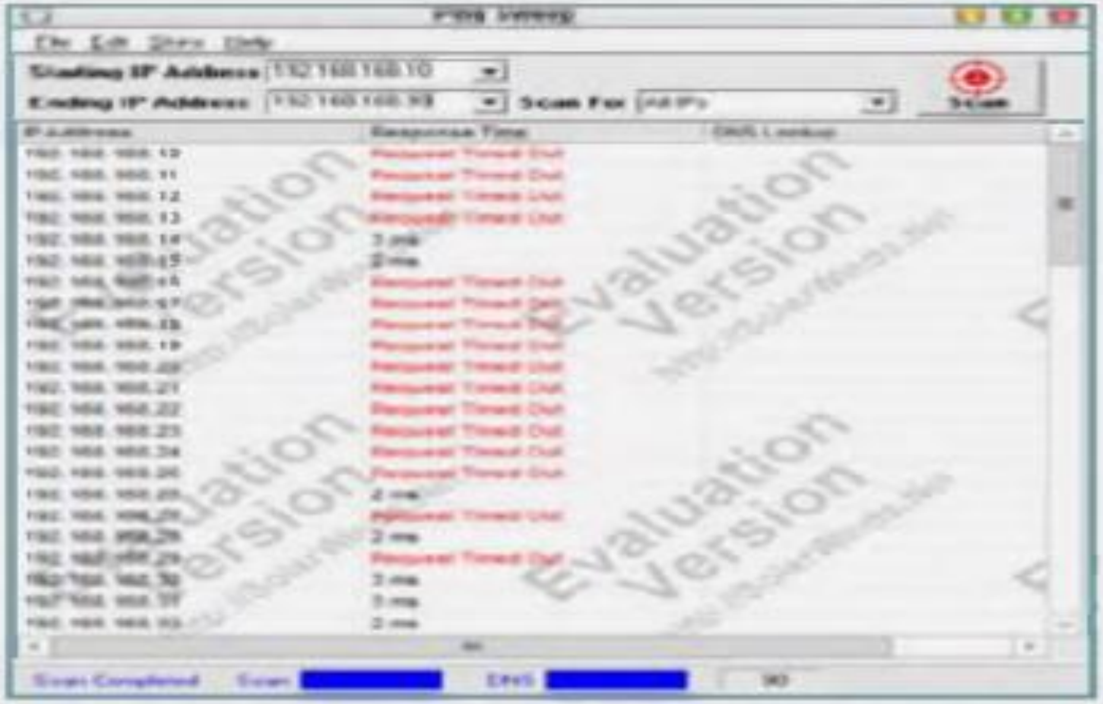
Hostname: WIN-LXQN7WR3R9M Netmask

IP	Ping	Hostname	Ports [2800+]
10.0.0.1	1 ms	[n/a]	80
10.0.0.2	[illegible] ms	WIN-MG22LC44K41	80,135,139,4...
10.0.0.3	6 ms	Windows8	135,139,445,...
10.0.0.4	[n/a]	[n/a]	[n/a]
10.0.0.5	4 ms	WIN-LXQN7WR3R9M	135,139,445,...
10.0.0.6	[n/a]	[n/a]	[n/a]
10.0.0.7	1 ms	[n/a]	80,135
10.0.0.8	[n/a]	[n/a]	[n/a]
10.0.0.9	[n/a]	[n/a]	[n/a]
10.0.0.10	[n/a]	[n/a]	[n/a]
10.0.0.11	[n/a]	[n/a]	[n/a]
10.0.0.12	[n/a]	[n/a]	[n/a]
10.0.0.13	[n/a]	[n/a]	[n/a]
10.0.0.14	[n/a]	[n/a]	[n/a]
10.0.0.15	477 ms	[n/a]	[n/a]
10.0.0.16	[n/a]	[n/a]	[n/a]
10.0.0.17	[n/a]	[n/a]	[n/a]
10.0.0.18	[n/a]	[n/a]	[n/a]
10.0.0.19	[n/a]	[n/a]	[n/a]

Ready Display: All Threads: 0

Angry IP Scanner

SolarWinds Engineer Toolset's Ping Sweep enables scanning a range of IP addresses to identify which IP addresses are in use and which ones are currently free. It also performs reverse DNS lookup.



Starting IP Address 192.168.168.10

Ending IP Address 192.168.168.93 Scan For All IPs

IP Address	Response Time	DNS Lookup
192.168.168.10	Request Timed Out	
192.168.168.11	Request Timed Out	
192.168.168.12	Request Timed Out	
192.168.168.13	Request Timed Out	
192.168.168.14	3 ms	
192.168.168.15	2 ms	
192.168.168.16	Request Timed Out	
192.168.168.17	Request Timed Out	
192.168.168.18	Request Timed Out	
192.168.168.19	Request Timed Out	
192.168.168.20	Request Timed Out	
192.168.168.21	Request Timed Out	
192.168.168.22	Request Timed Out	
192.168.168.23	Request Timed Out	
192.168.168.24	Request Timed Out	
192.168.168.25	Request Timed Out	
192.168.168.26	2 ms	
192.168.168.27	Request Timed Out	
192.168.168.28	2 ms	
192.168.168.29	Request Timed Out	
192.168.168.30	3 ms	
192.168.168.31	3 ms	
192.168.168.32	2 ms	

Scan Completed Scan DNS 90

SolarWinds Engineer's Toolset

Ping Sweep Tools (Cont'd)

Colasoft Ping Tool
http://www.colasoft.com

Visual Ping Tester - Standard
http://www.pingtester.net

Ping Scanner Pro
http://www.digilextechnologies.com

Ultra Ping Pro
http://ultraping.webs.com

PingInfoView
http://www.nirsoft.net

PacketTrap MSP
http://www.packettrap.com

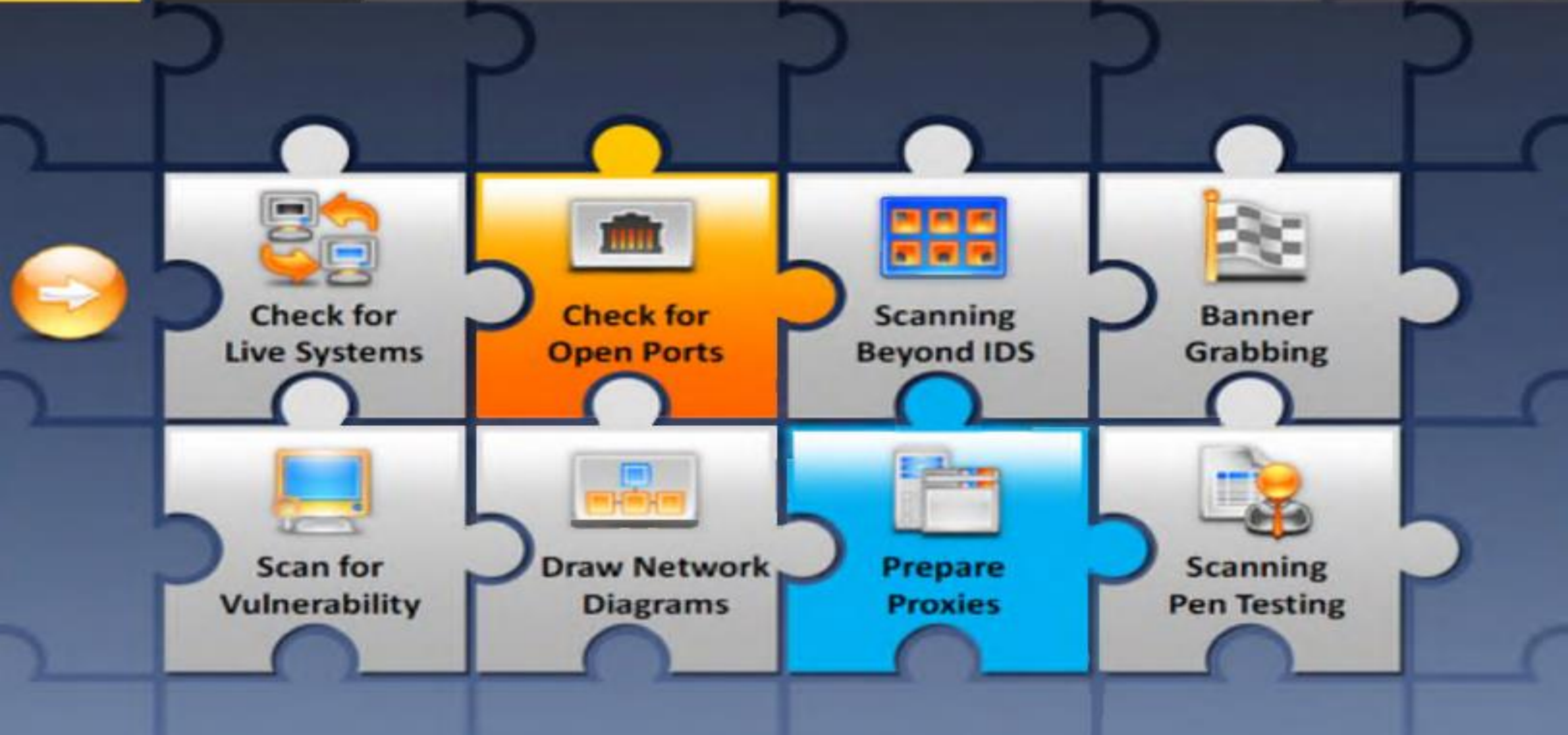
Ping Sweep
http://www.whatsupgold.com

Network Ping
http://www.greenline-soft.com

Ping Monitor
http://www.niliand.com

Pinkie
http://www.ipuptime.net

Scanning Methodology



Check for Live Systems

Check for Open Ports

Scanning Beyond IDS

Banner Grabbing

Scan for Vulnerability

Draw Network Diagrams

Prepare Proxies

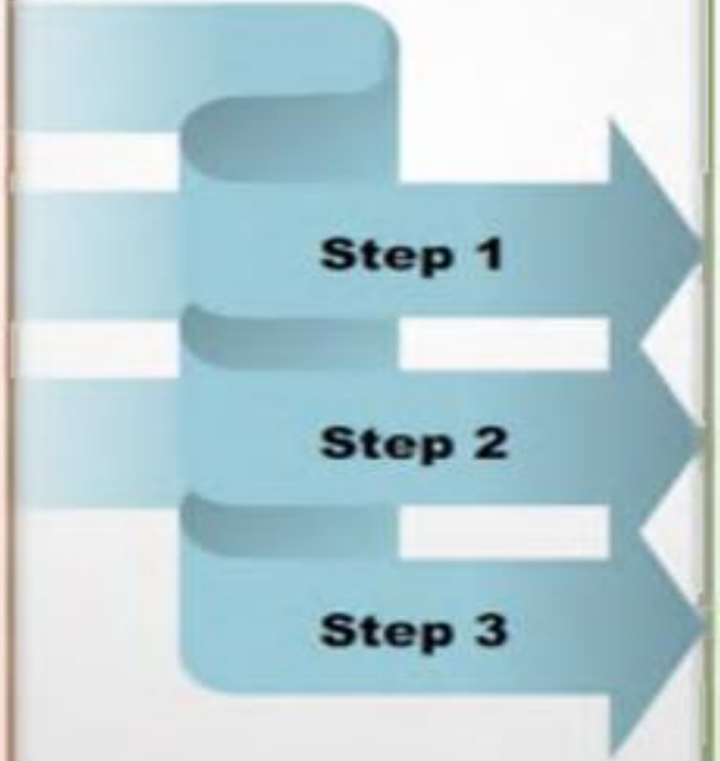
Scanning Pen Testing

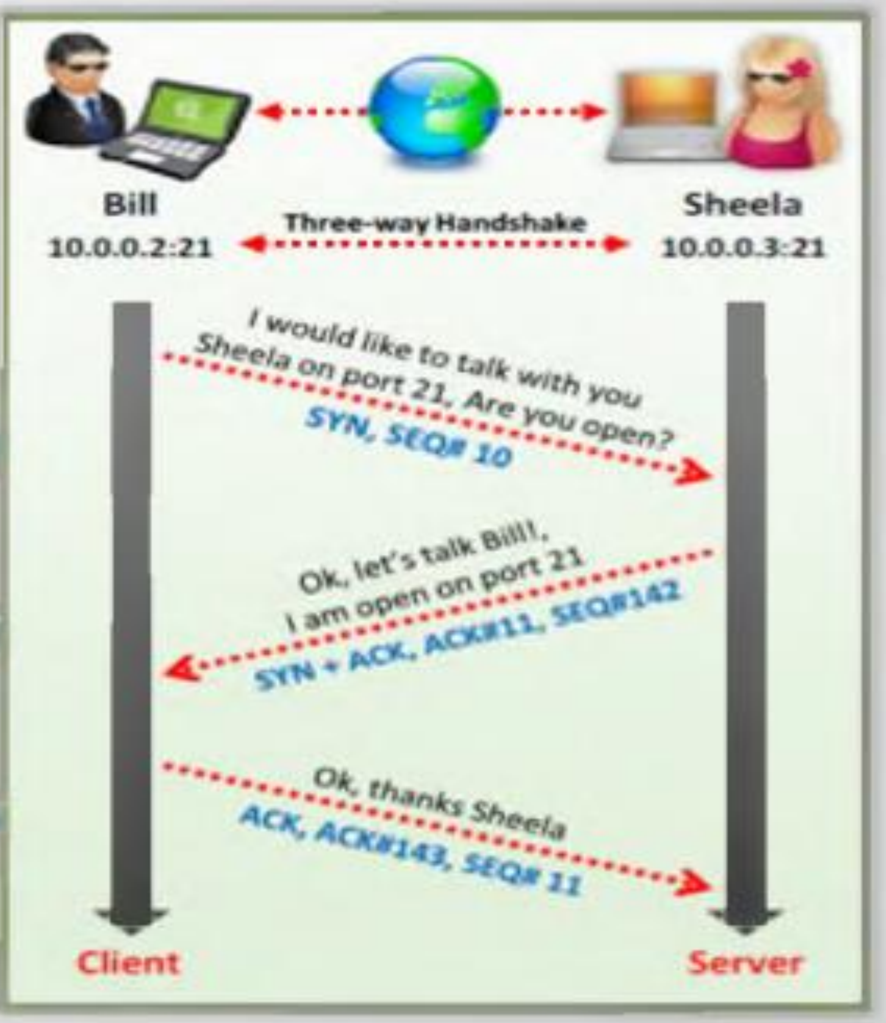
Three-Way Handshake

TCP uses a **three-way handshake** to establish a connection between server and client

Three-way Handshake Process

1. The Computer A (10.0.0.2) initiates a connection to the server (10.0.0.3) via a packet with only the **SYN** flag set
2. The server replies with a packet with both the **SYN** and the **ACK** flag set
3. For the final step, the client responds back to the server with a single **ACK** packet
4. If these three steps are completed without complication, then a TCP connection is established between the client and the server





Scanning IPv6 Network

- IPv6 increases the IP address size from **32 bits** to **128 bits,** to support more levels of addressing hierarchy

- Traditional network scanning techniques will be **computationally less feasible** due to larger search space (64 bits of host address space or 2^{64} addresses) provided by IPv6 in a subnet

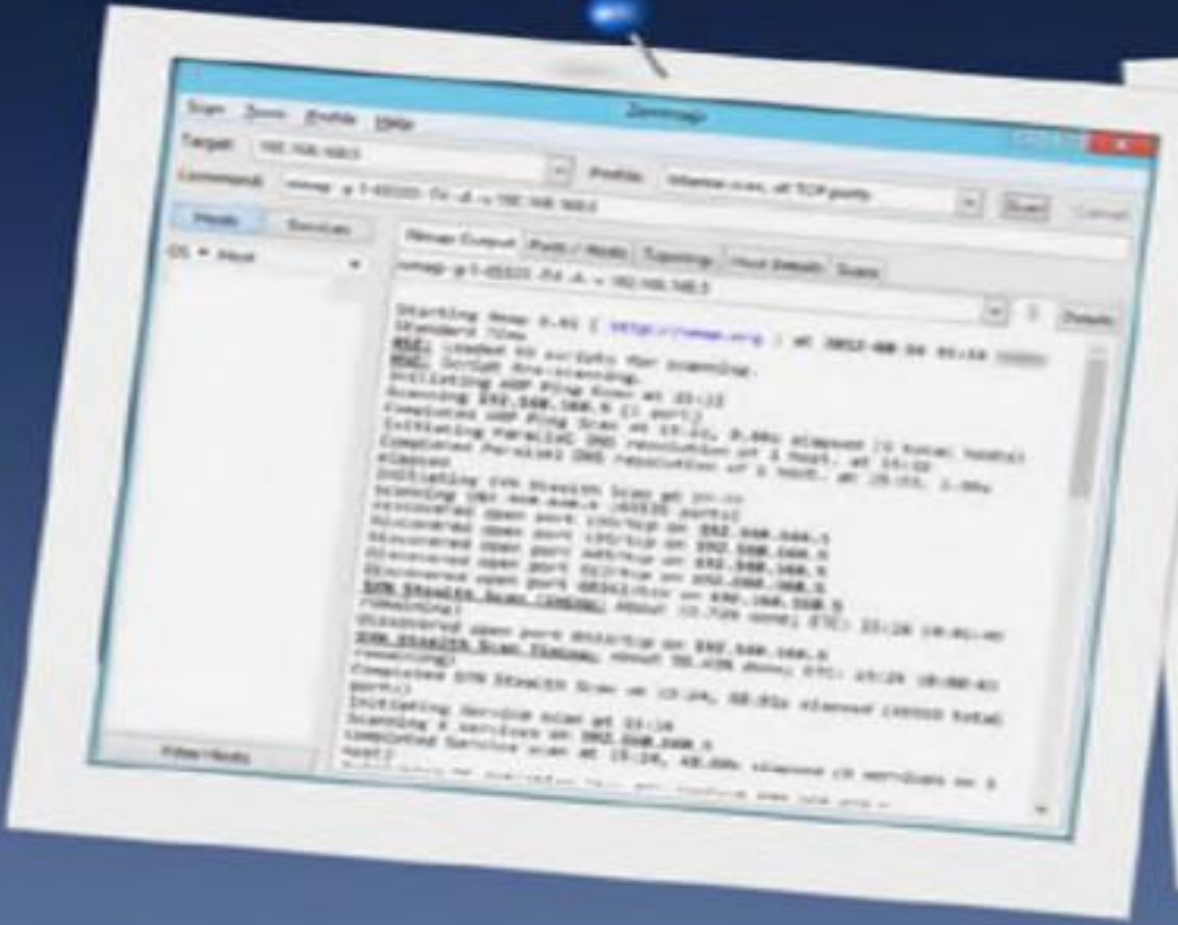
- Scanning in IPv6 network is more difficult and complex than the IPv4 and also major scanning tools such as **Nmap** do not support ping sweeps on **IPv6 networks**

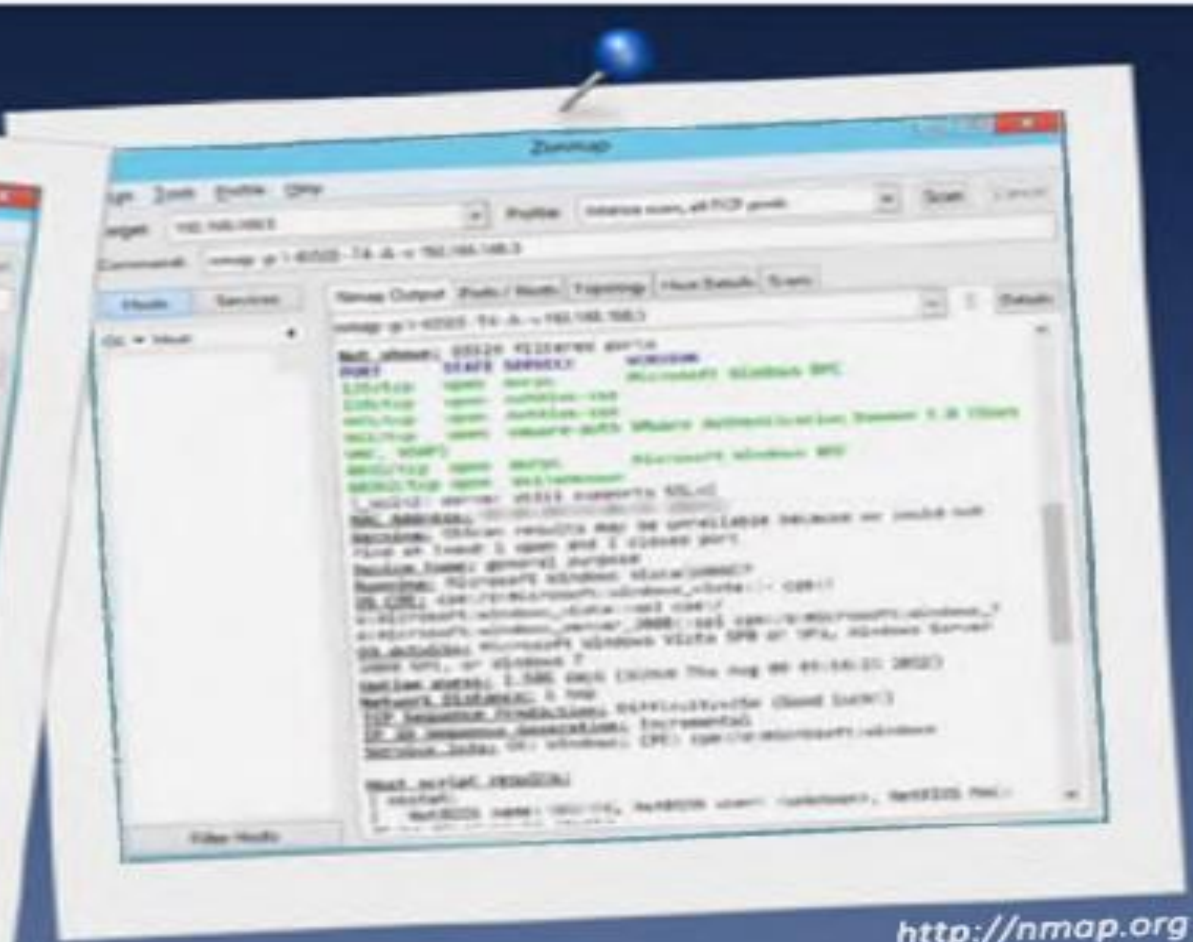
- Attackers need to harvest IPv6 addresses from **network traffic, recorded logs** or **Received from:** and other header lines in archived email or Usenet news messages

- Scanning IPv6 network, however, offers a large number of hosts in a subnet if an attacker can compromise one host in the subnet; attacker can probe the **"all hosts" link local multicast address**

Scanning Tool: Nmap

- Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime
- Attacker uses Nmap to extract information such as live hosts on the network, services (application name and version), type of packet filters/firewalls, operating systems and OS versions





http://nmap.org

Scanning Tools

PRTG Network Monitor
http://www.paessler.com

Net Tools
http://mabsoft.com

IP Tools
http://www.ks-soft.net

MegaPing
http://www.magnetosoft.com

Network Inventory Explorer
http://www.10-strike.com

Global Network Inventory Scanner
http://www.magnetosoft.com

SoftPerfect Network Scanner
http://www.softperfect.com

Advanced Port Scanner
http://www.radmin.com

Netifera
http://netifera.com

Free Port Scanner
http://www.nsauditor.com

Port Scanning Countermeasures

Configure firewall and IDS rules to detect and block probes

Use custom rule set to lock down the network and block unwanted ports at the firewall

Hide sensitive information from public view

Filter all ICMP messages (i.e. inbound ICMP message types and outbound ICMP type 3 unreachable messages) at the firewalls and routers

Ensure that mechanism used for routing and filtering at the routers and firewalls respectively cannot be bypassed using particular source ports or source-routing methods

Perform TCP and UDP scanning along with ICMP probes against your organization's IP address space to check the network configuration and its available ports

Ensure that the router, IDS, and firewall firmware are updated to their latest releases

Ensure that the anti scanning and anti spoofing rules are configured

Banner Grabbing

- Banner grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system. There are two types of banner grabbing: active and passive.

Active Banner Grabbing

- Specially crafted packets are sent to remote OS and the response is noted
- The responses are then compared with a database to determine the OS
- Response from different OSes varies due to differences in TCP/IP stack implementation

Passive Banner Grabbing

- Banner grabbing from error messages:

  Error messages provide information such as type of server, type of OS, and SSL tool used by the target remote system
- Sniffing the network traffic:

  Capturing and analyzing packets from the target enables an attacker to determine OS used by the remote system
- Banner grabbing from page extensions:

  Looking for an extension in the URL may assist in determining the application version

  Example: .aspx => IIS server and Windows platform

Why Banner Grabbing?

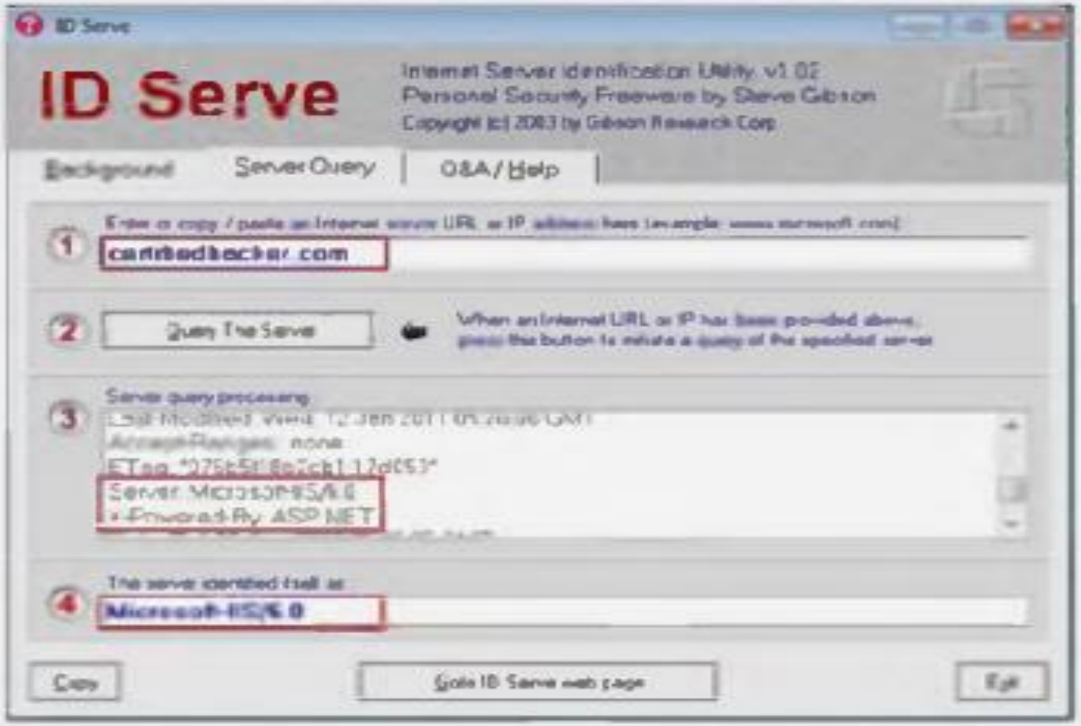
Identifying the OS used on the target host allows an attacker to figure out the vulnerabilities the system posses and the exploits that might work on a system to further carry out additional attacks

Banner Grabbing Tools

- ID Serve is used to identify the make, model, and version of any web site's server software
- It is also used to identify non-HTTP (non-web) Internet servers such as FTP, SMTP, POP, NEWS, etc.

- Netcraft reports a site's operating system, web server, and netblock owner together with, if available, a graphical view of the time since last reboot for each of the computers serving the site

ID Serve



Internet Server Identification Utility, v1.02
Personal Security Freeware by Steve Gibson
Copyright (c) 2003 by Gibson Research Corp.

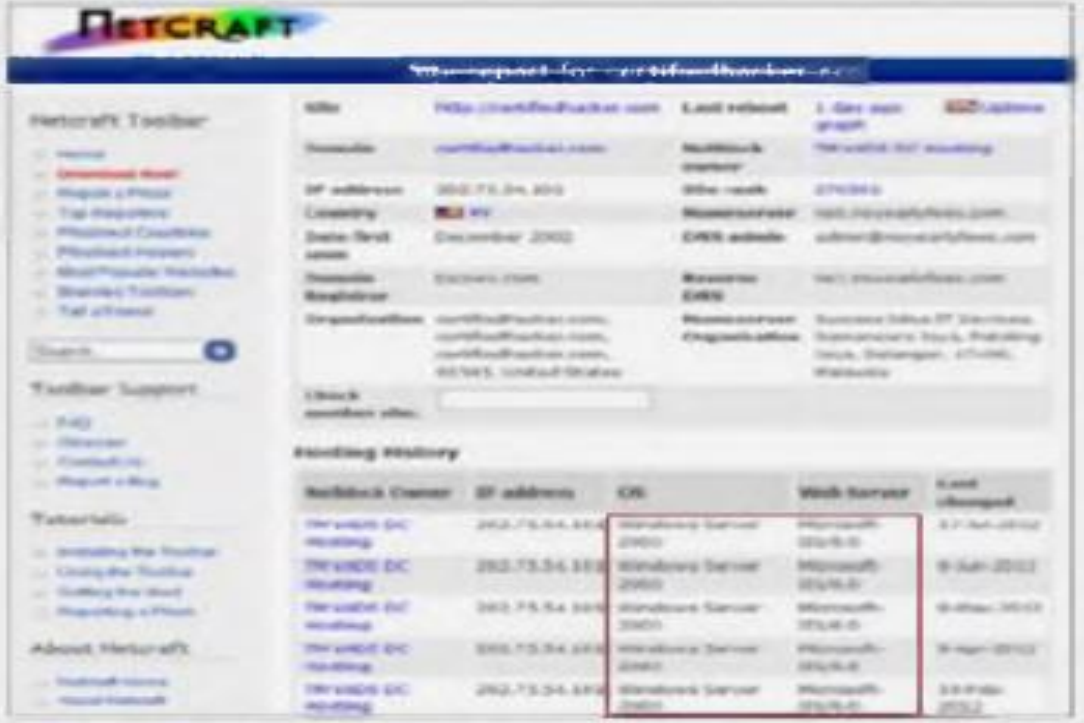
1. Enter or copy / paste an Internet server URL or IP address here (example: www.microsoft.com): certifiedhacker.com
2. When an Internet URL or IP has been provided above, press this button to initiate a query of the specified server
3. Server query processing:

```
Last-Modified: Wed, 12 Jan 2011 05:26:56 GMT
Accept-Ranges: none
ETag: "0756518e0c1:17d053"
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
```

4. The server identified itself as: Microsoft-IIS/6.0

http://www.grc.com

Netcraft



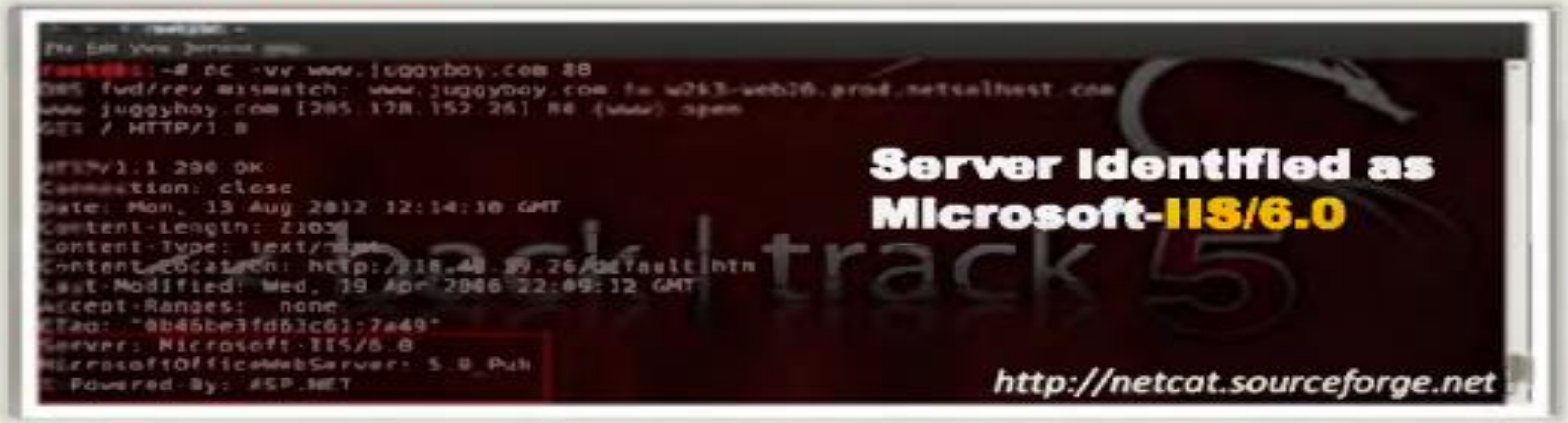
http://toolbar.netcraft.com

Banner Grabbing Tools (Cont'd)

Netcat

This utility **reads and writes data across network connections,** using the TCP/IP protocol

1. `# nc –vv www.juggyboy.com 80` - press[Enter]
2. `GET / HTTP/1.0` - Press [Enter] twice



```
root@bt:~# nc -vv www.juggyboy.com 80
DNS fwd/rev mismatch: www.juggyboy.com != w2k3-web26.prod.netsolhost.com
www.juggyboy.com [205.178.152.26] 80 (www) open
GET / HTTP/1.0

HTTP/1.1 200 OK
Connection: close
Date: Mon, 13 Aug 2012 12:14:10 GMT
Content-Length: 2103
Content-Type: text/html
Content-Location: http://218.40.39.26/Default.htm
Last-Modified: Wed, 19 Apr 2006 22:09:12 GMT
Accept-Ranges: none
ETag: "0b46be3fd63c61:7a49"
Server: Microsoft-IIS/6.0
MicrosoftOfficeWebServer: 5.0_Pub
X-Powered-By: ASP.NET
```

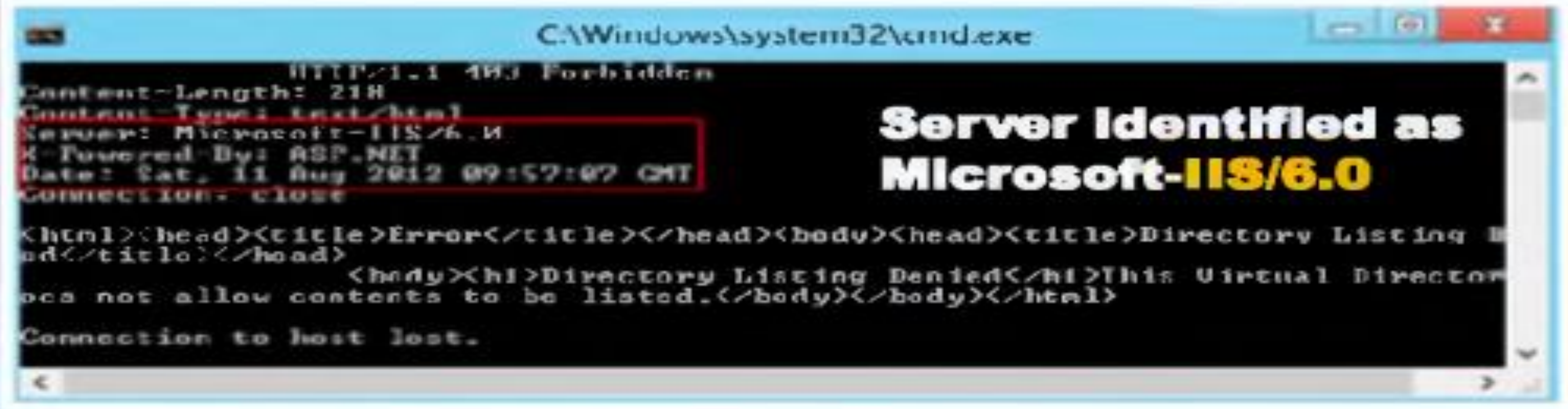
Server Identified as Microsoft-IIS/6.0

http://netcat.sourceforge.net

Telnet

This technique probes **HTTP servers** to determine the **Server field** in the HTTP response header

1. `telnet www.certifiedhacker.com 80` - press[Enter]
2. `GET / HTTP/1.0` - Press [Enter] twice



```
           HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Sat, 11 Aug 2012 09:57:07 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing D
ed</title></head>
               <body><h1>Directory Listing Denied</h1>This Virtual Director
oes not allow contents to be listed.</body></body></html>

Connection to host lost.
```

Server Identified as Microsoft-IIS/6.0

Banner Grabbing Countermeasures: Disabling or Changing Banner

Display **false banners** to misguide the attackers

Turn off unnecessary services on the network host to limit the information disclosure

IIS users can use these tools to disable or change banner information

- **IIS Lockdown Tool** (http://microsoft.com)
- **ServerMask** (http://www.port80software.com)

Apache 2.x with `mod_headers` module - use a directive in `httpd.conf` file to change banner information **Header set Server "New Server Name“**

Alternatively, change the `ServerSignature` line to `ServerSignature Off` in `httpd.conf` file

Hiding File Extensions from Web Pages

File extensions reveal information about the **underlying server technology** that an attacker can utilize to launch attacks

Hide file extensions to **mask the web technology**

Change **application mappings** such as .asp with .htm or .foo, etc. to disguise the identity of the servers

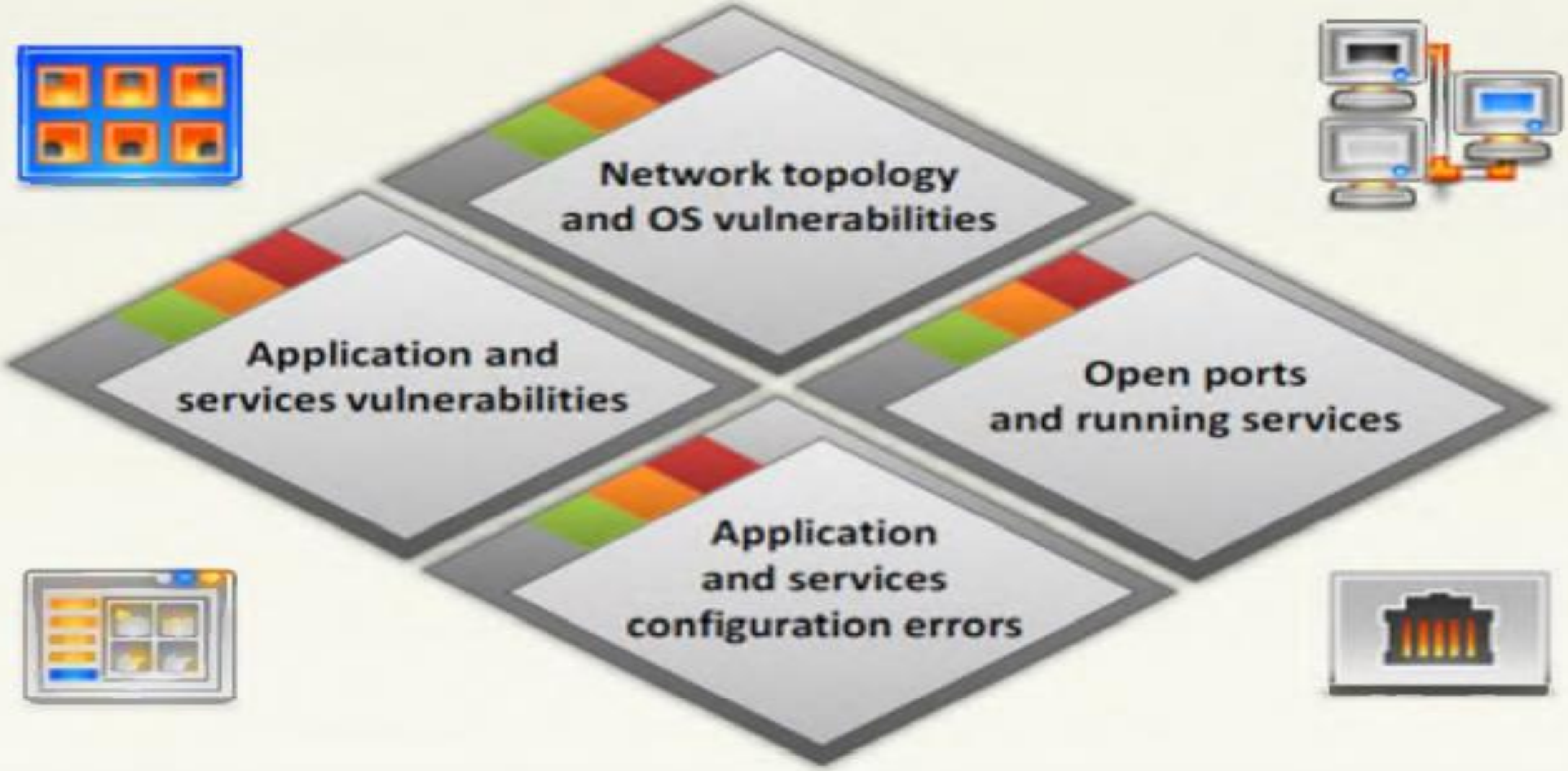
Apache users can use **mod_negotiation** directives

IIS users use tools such as **PageXchanger** to manage the file extensions

✓ **It is even better if the file extensions are not at all used**

Vulnerability Scanning

Vulnerability scanning identifies **vulnerabilities and weaknesses of a system** and network in order to determine how a system can be exploited



Network topology and OS vulnerabilities

Application and services vulnerabilities

Open ports and running services

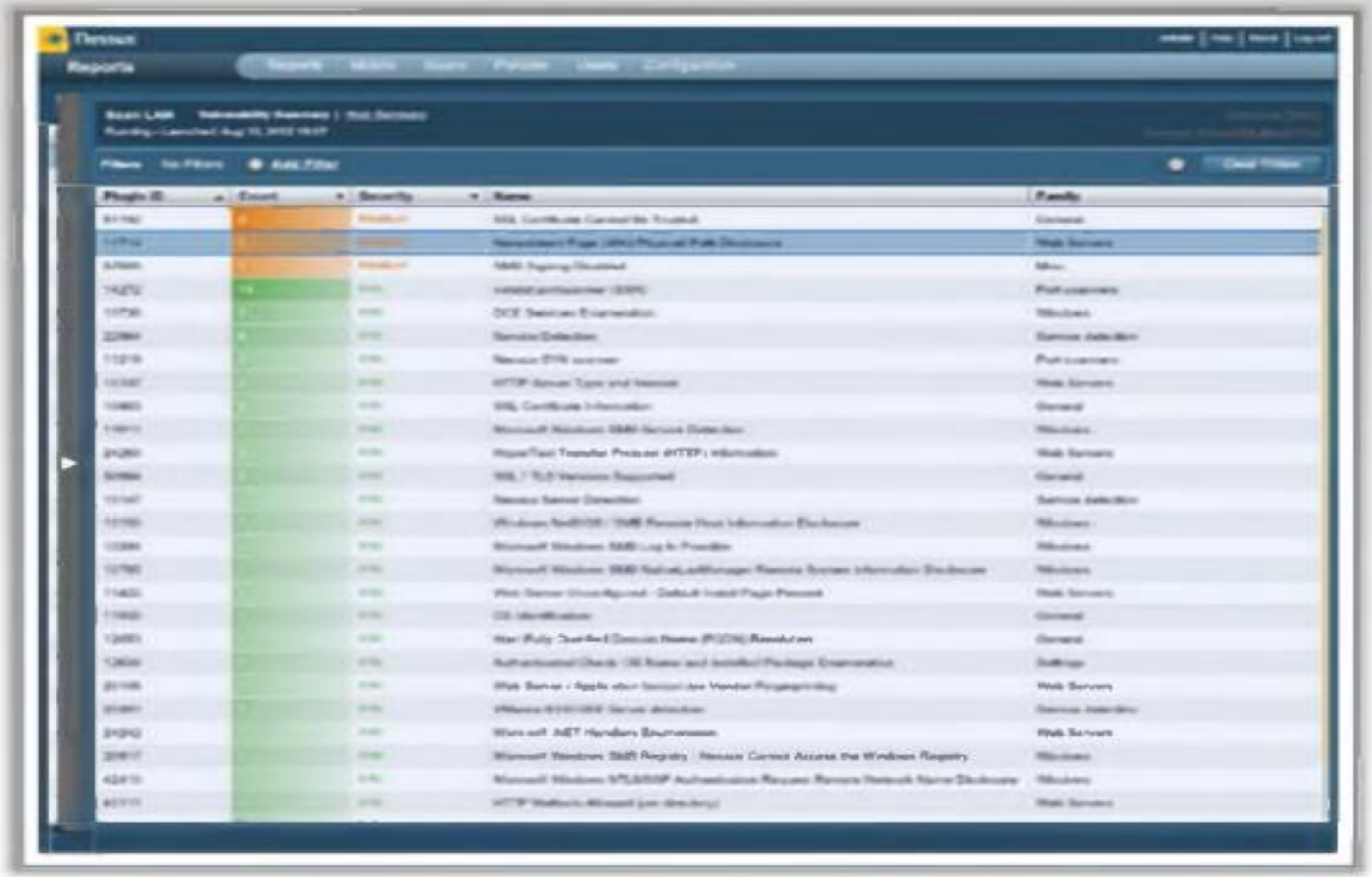
Application and services configuration errors

Vulnerability Scanning Tool: Nessus

Nessus is the vulnerability and configuration assessment product

Features

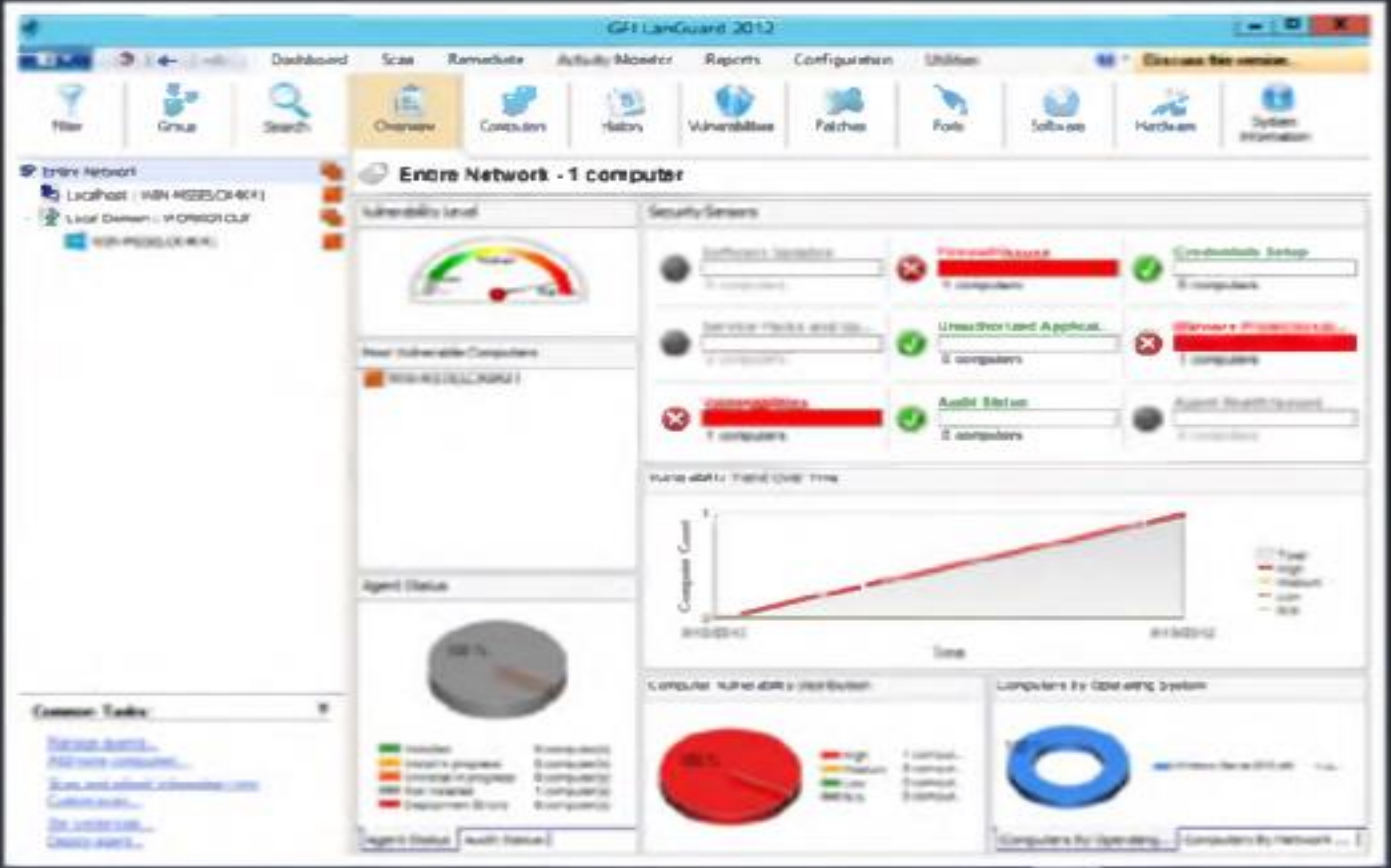
- Agentless auditing
- Compliance checks
- Content audits
- Customized reporting
- High-speed vulnerability discovery
- In-depth assessments
- Mobile device audits
- Patch management integration
- Scan policy design and execution



http://www.tenable.com

Vulnerability Scanning Tool: GFI LanGuard

- GFI LanGuard assists in **asset inventory**, change management, **risk analysis**, and proving compliance
- Features:
  - Selectively creates **custom vulnerability checks**
  - Identifies **security vulnerabilities** and takes remedial action
  - Creates different types of **scans and vulnerability tests**
  - Helps ensure third-party security applications offer **optimum protection**
  - Performs **network device vulnerability checks**



Network Vulnerability Scanners

Retina CS
http://go.eeye.com

Core Impact Professional
http://www.coresecurity.com

MBSA
http://www.microsoft.com

Shadow Security Scanner
http://www.safety-lab.com

Nsauditor Network Security Auditor
http://www.nsauditor.com

OpenVAS
http://www.openvas.org

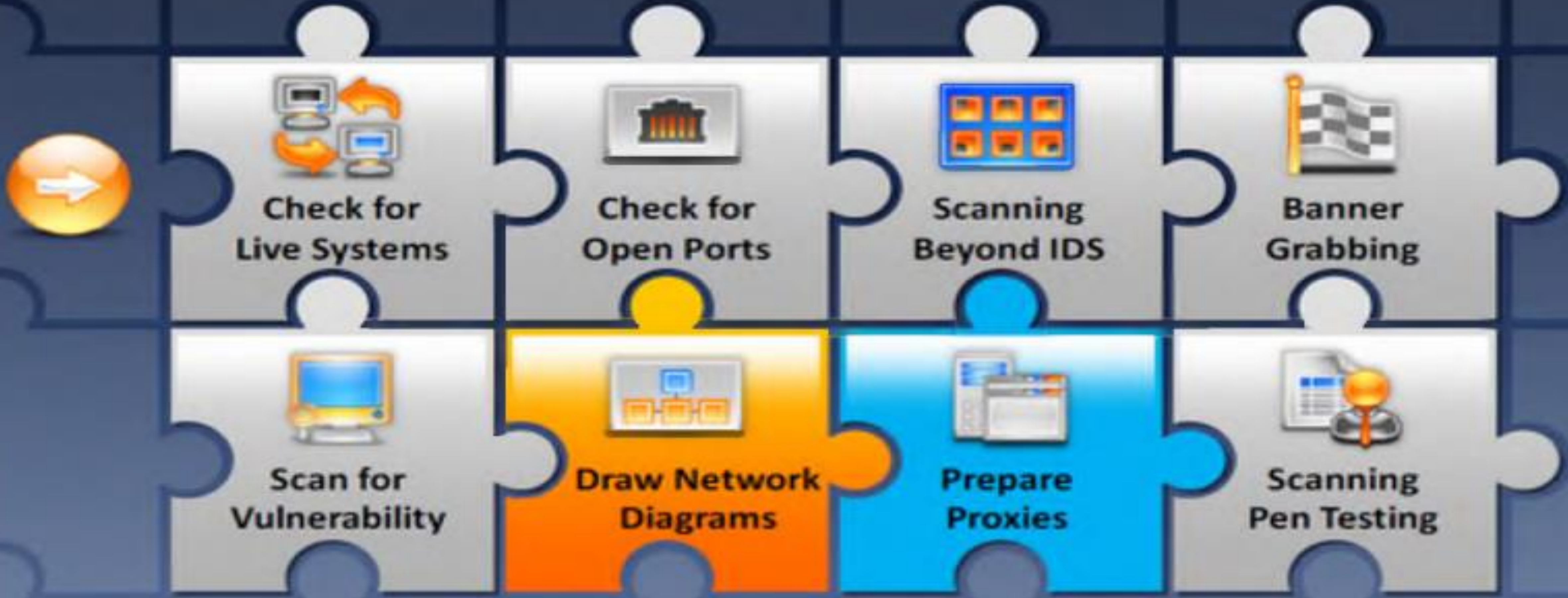
Security Manager Plus
http://www.manageengine.com

Nexpose
http://www.rapid7.com

QualysGuard
http://www.qualys.com

Security Auditor's Research Assistant (SARA)
http://www-arc.com

Scanning Methodology



Check for Live Systems

Check for Open Ports

Scanning Beyond IDS

Banner Grabbing

Scan for Vulnerability

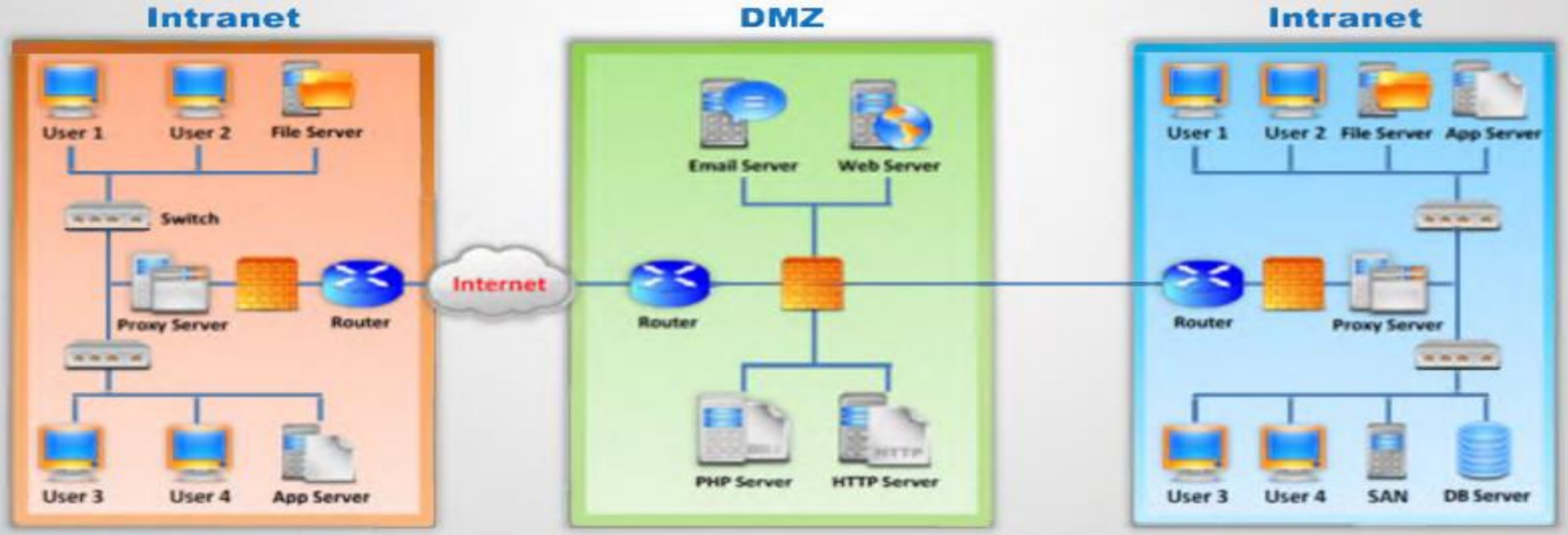
Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

Drawing Network Diagrams

- Drawing target's network diagram gives valuable information about the **network and its architecture** to an attacker
- Network diagram shows **logical or physical path** to a potential target

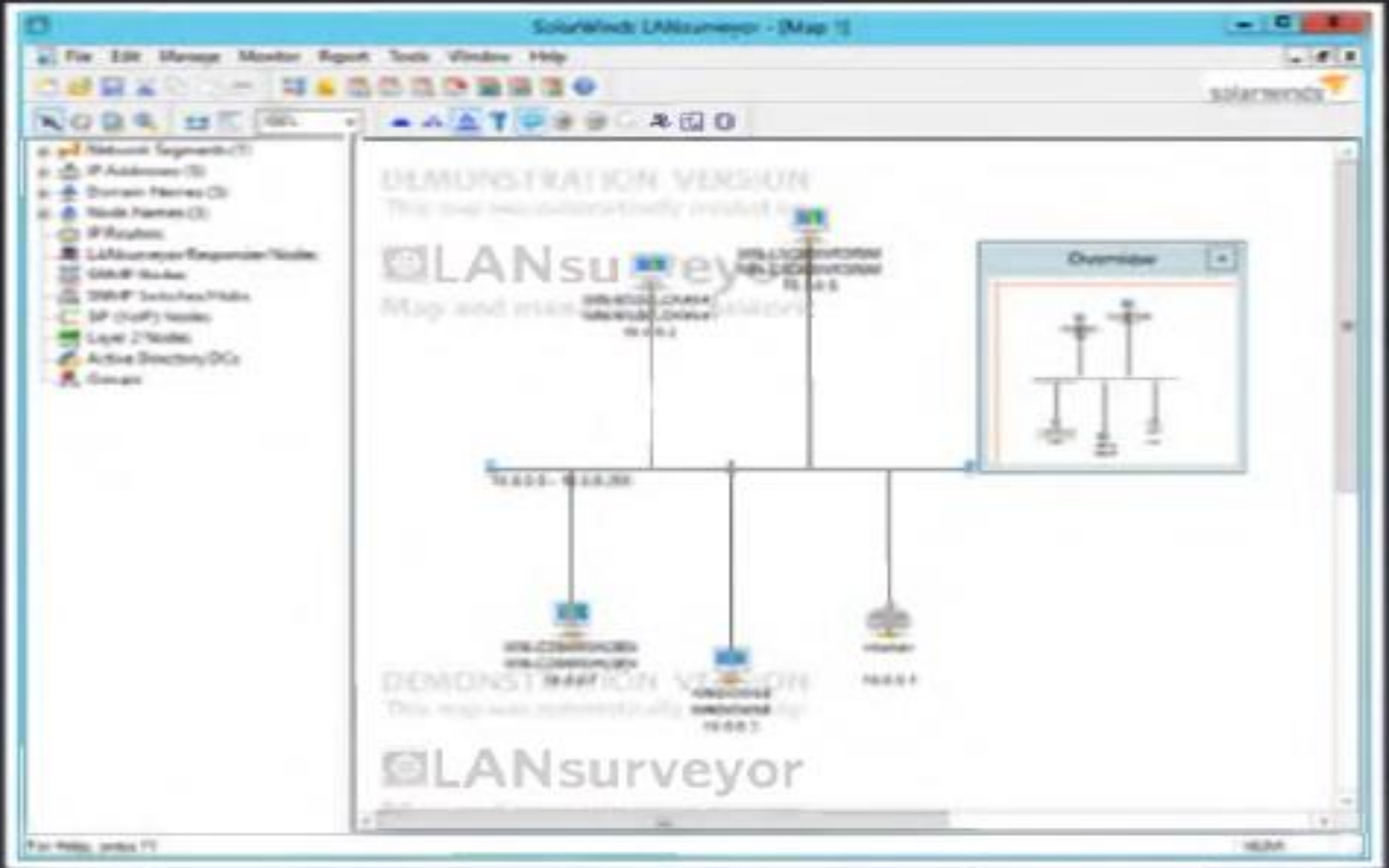


Network Discovery Tool: **LANsurveyor**

LANsurveyor **discovers a network** and **produces a comprehensive network diagram** that integrates OSI Layer 2 and Layer 3 topology data

Features

- Auto-generate Network Maps
- Export Network Maps to Visio
- Auto-detect Changes
- Inventory Management
- Network Regulatory Compliance
- Network Topology Database
- Multi-level Network Discovery

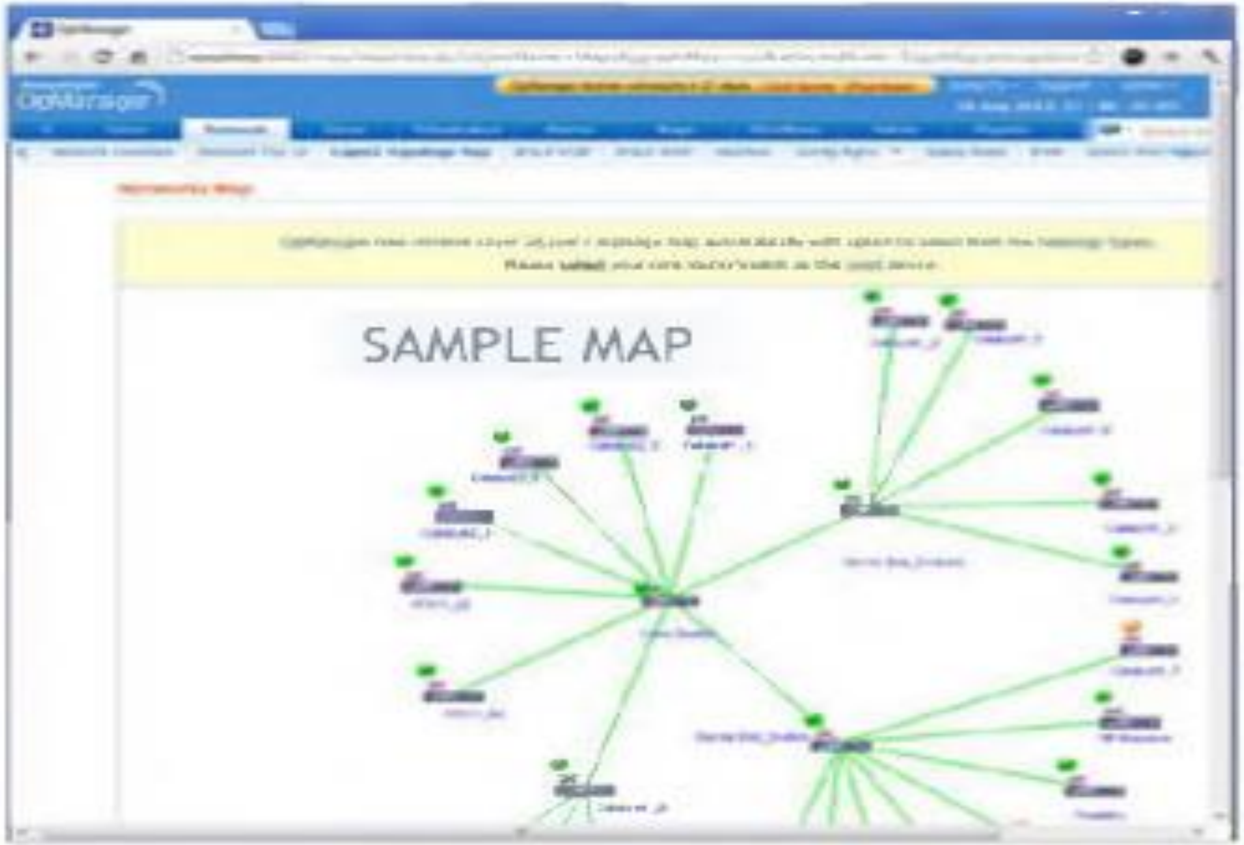


Network Discovery Tool: OpManager

OpManager is a network monitoring software that offers advanced **fault and performance management** functionality across critical **IT resources** such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, virtual servers, domain controllers, and other IT infrastructure devices

Features

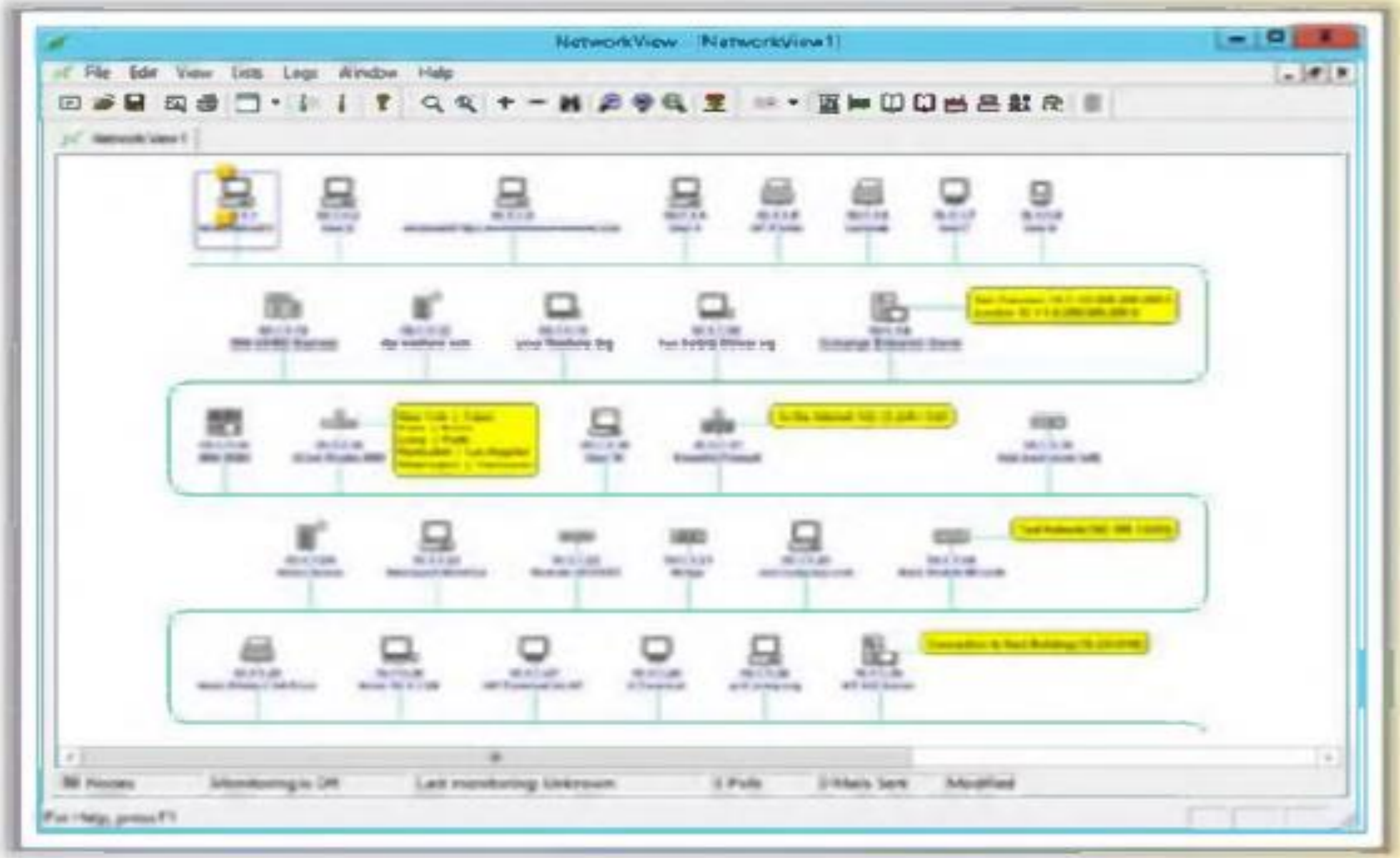
- Availability and Uptime Monitoring
- Network Traffic Analysis
- IP Address Management
- Switch Port Mapper
- Network Performance Reporting
- Network Configuration Management
- Exchange Server Monitoring
- Active Directory Monitoring
- Hyper-V Monitoring
- SQL Server Monitoring



http://www.manageengine.com

Network Discovery Tool: NetworkView

- NetworkView is a **network discovery and management** tool for Windows
- **Discover TCP/IP nodes and routes** using DNS, SNMP, ports, NetBIOS, and WMI

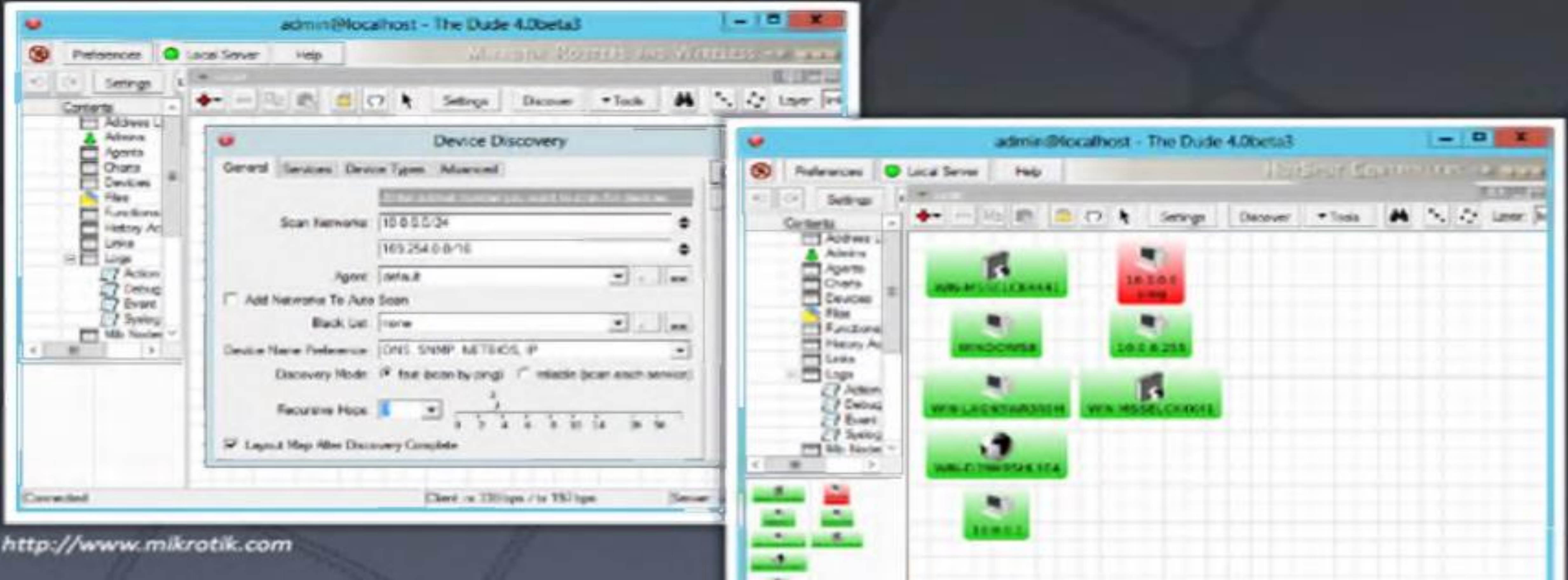


88 Nodes | Monitoring is Off | Last monitoring: Unknown | 0 Polls | 0 Mails Sent | Modified

For Help, press F1

Network Discovery Tool: The Dude

- The Dude sniffer scans all devices **within the specified subnets** and draws a detailed layout map



Device Discovery

General | Services | Device Types | Advanced

Scan Networks: 10.0.0.0/24
169.254.0.0/16
Agent: default
□ Add Networks To Auto Scan
Black List: none
Device Name Preference: DNS, SNMP, NETBIOS, IP
Discovery Mode: ● fast (scan by ping) ○ reliable (scan each service)
Recursive Hops: 1
☑ Layout Map After Discovery Complete

http://www.mikrotik.com

Network Discovery and Mapping Tools

LANState
http://www.10-strike.com

FriendlyPinger
http://www.kilievich.com

Ipsonar
http://www.lumeta.com

CartoReso
http://cartoreso.campus.ecp.fr

Switch Center Enterprise
http://www.lan-secure.com

HP Network Node Manager i Software
http://www8.hp.com

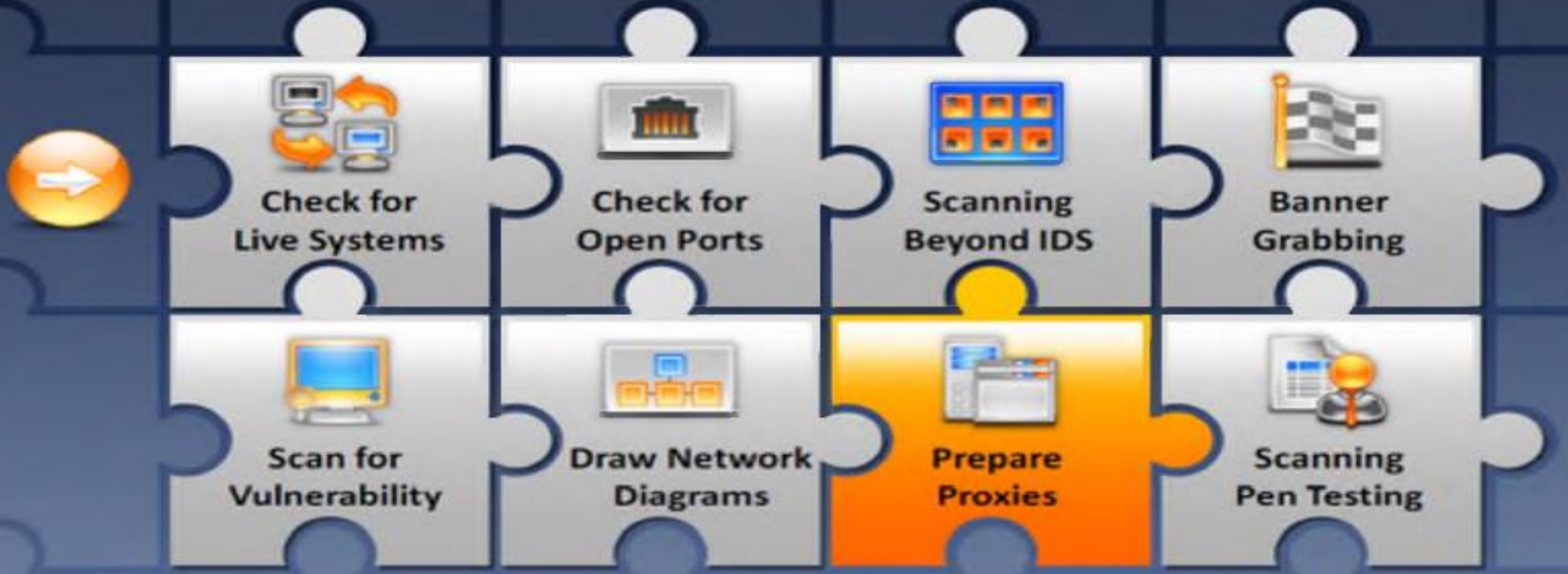
NetMapper
http://www.opnet.com

NetBrain Enterprise Suite
http://www.netbraintech.com

Spiceworks-Network Mapper
http://www.spiceworks.com

NetCrunch
http://www.adremsoft.com

Scanning Methodology



Check for Live Systems

Check for Open Ports

Scanning Beyond IDS

Banner Grabbing

Scan for Vulnerability

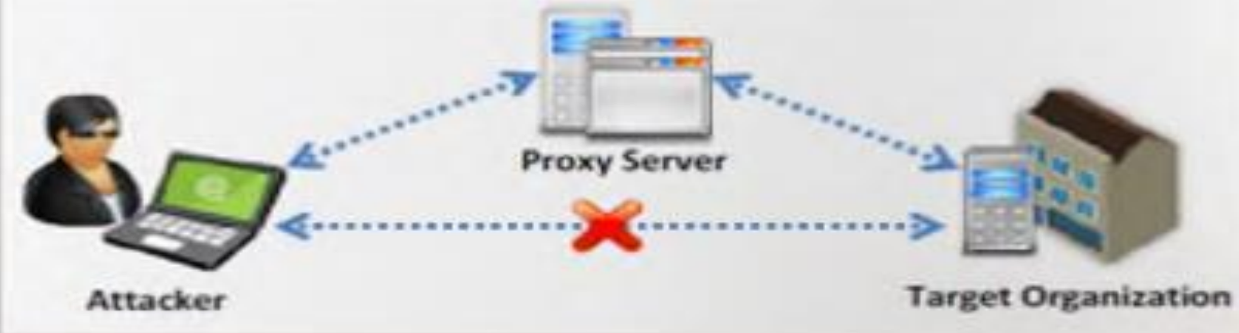
Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

Proxy Servers

A proxy is a network computer that can **serve as an intermediary** for connecting with other computers



As a firewall, a **proxy protects the local network** from outside access

As an IP addresses multiplexer, a proxy **allows the connection** of a number of computers to the Internet while having only one IP address

Specialized proxy servers can **filter out unwanted content**

Proxy servers can be used (to some extent) to **anonymize web surfing**

Why Attackers Use Proxy Servers?

1. To hide the source IP address so that an attacker can hack without any legal corollary

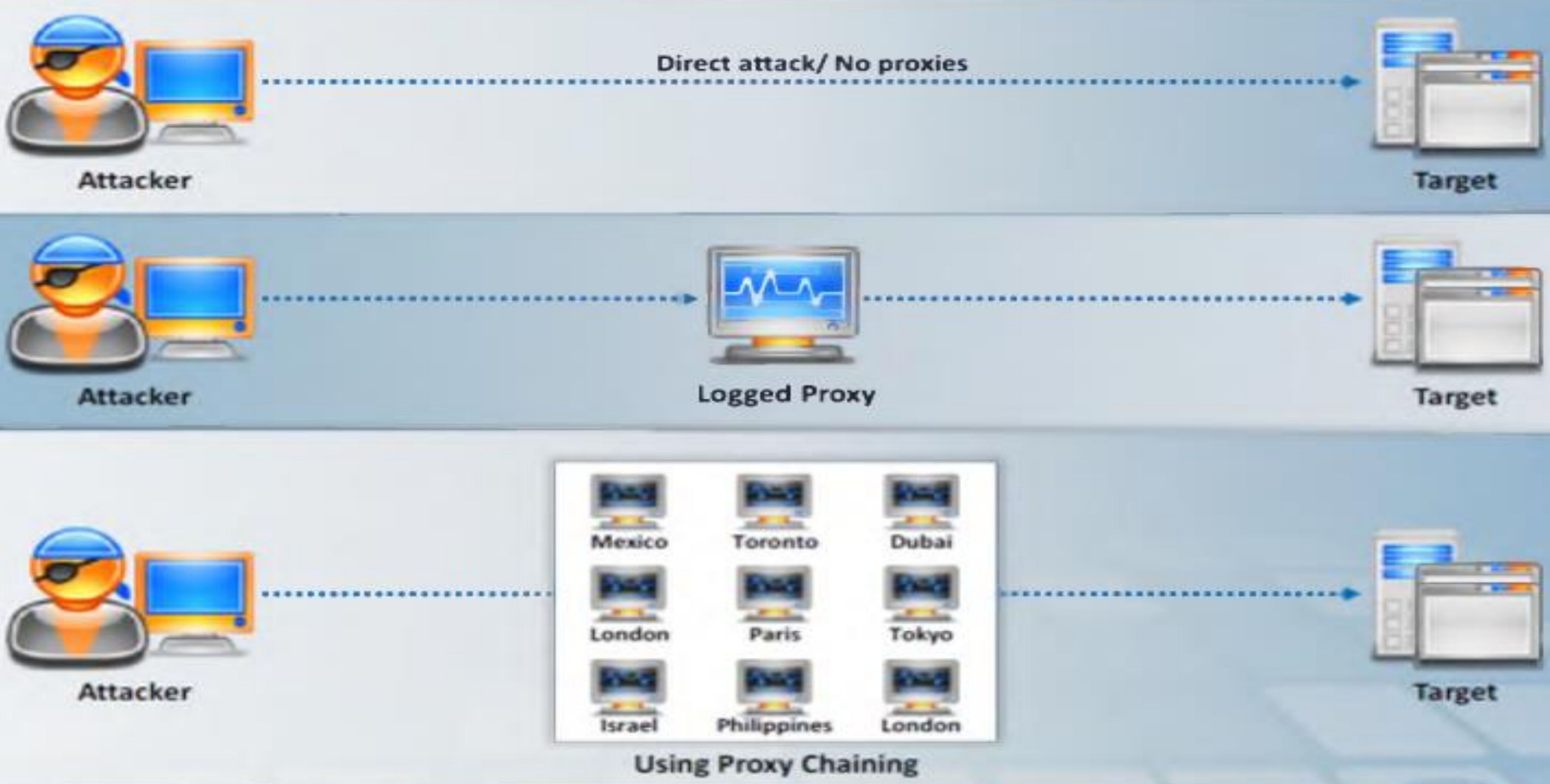
2. To mask the actual source of the attack by impersonating a fake source address of the proxy

3. To remotely access intranets and other website resources that are normally off limits

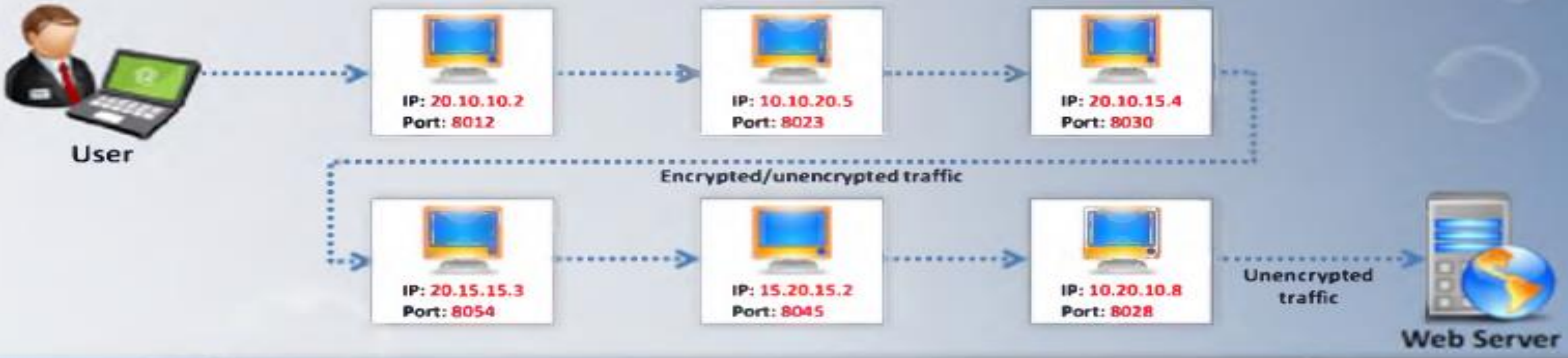
4. To interrupt all the requests sent by an attacker and transmit them to a third destination, hence victims will only be able to identify the proxy server address

5. Attackers chain multiple proxy servers to avoid detection

Use of Proxies for Attack



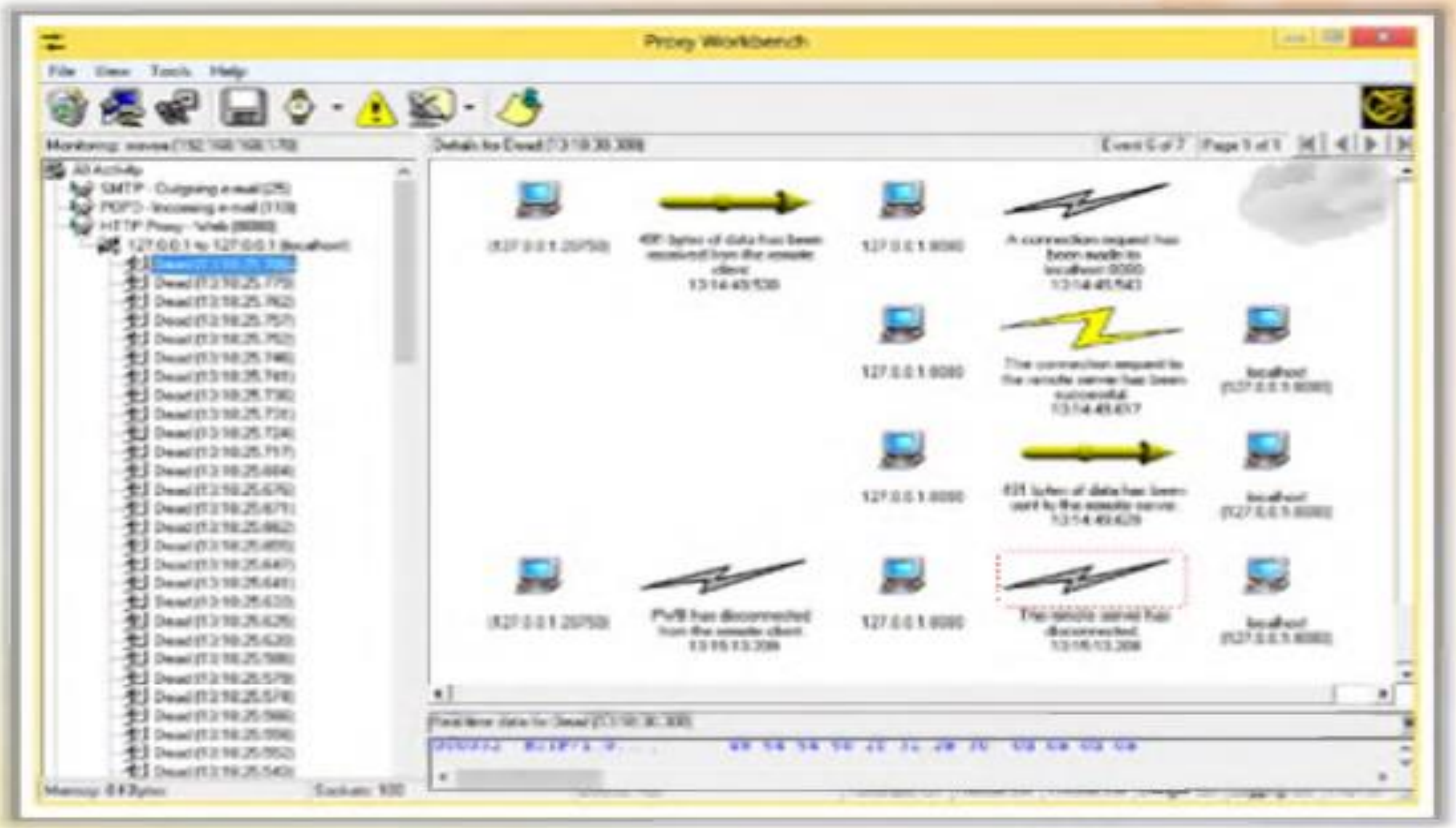
Proxy Chaining



1. User requests a resource from the destination
2. Proxy client at the user's system connects to a proxy server and passes the request to proxy server
3. The proxy server strips the user's identification information and passes the request to next proxy server
4. This process is repeated by all the proxy servers in the chain
5. At the end unencrypted request is passed to the web server

Proxy Tool: Proxy Workbench

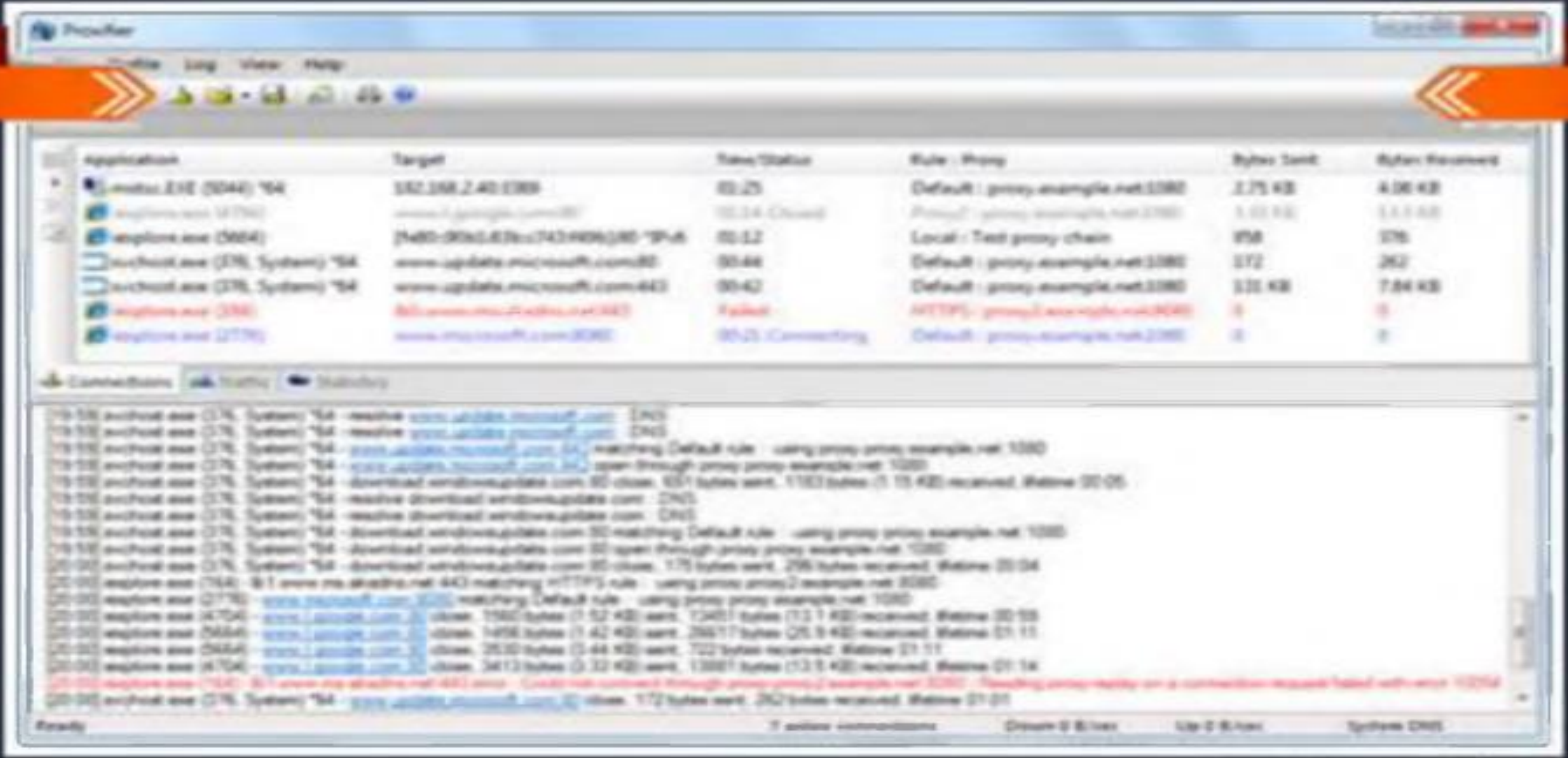
Proxy Workbench is a proxy server that **displays data passing through it in real time**, allows you to drill into particular TCP/IP connections, view their history, save the data to a file, and view the socket connection diagram



http://proxyworkbench.com

Proxy Tool: Proxifier

Proxifier is a program that allows network applications that do not support working through proxy servers to operate through an HTTPS or SOCKS proxy or a chain of proxy servers

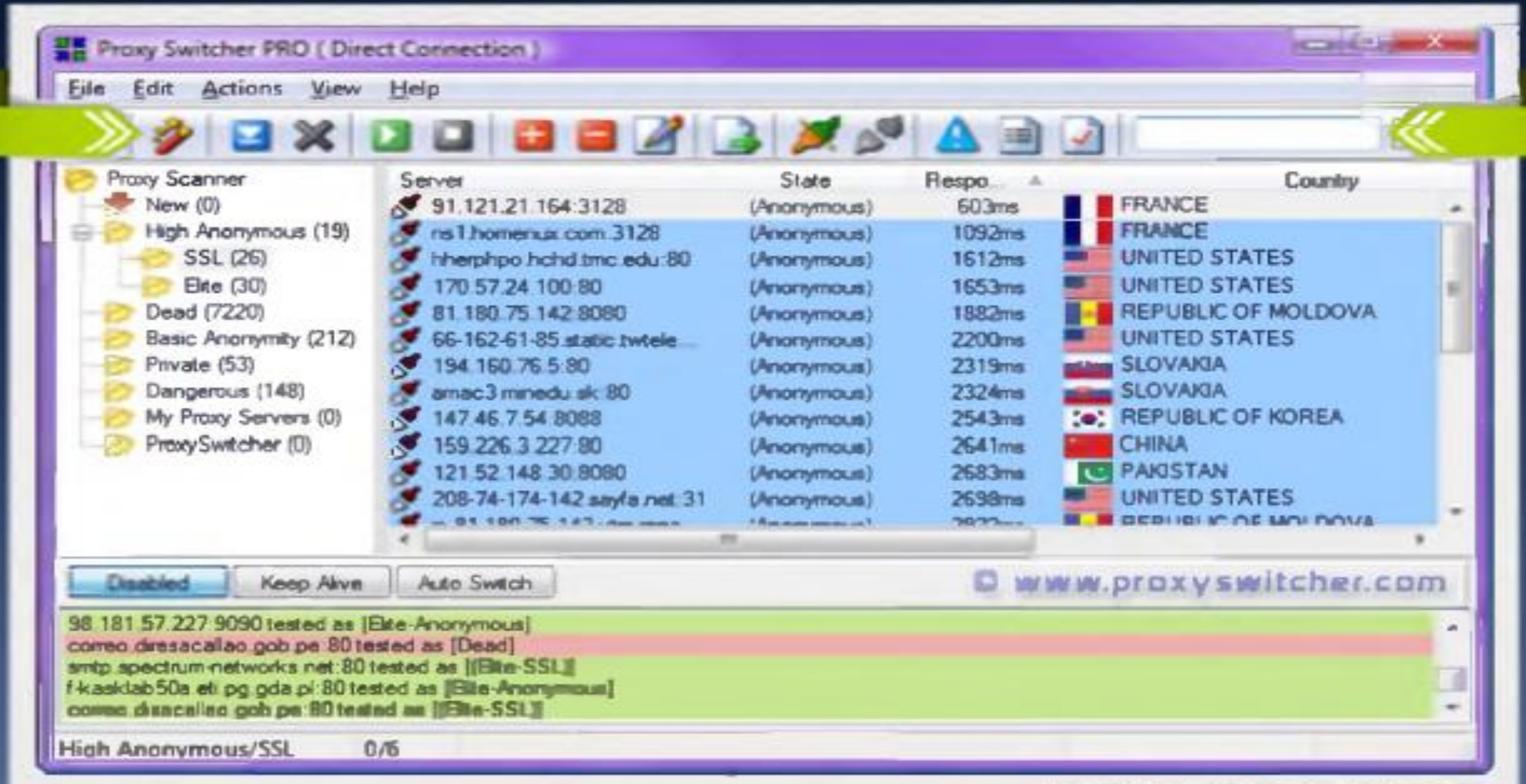


Application	Target	Time/Status	Rule : Proxy	Bytes Sent	Bytes Received
mstsc.EXE (5044) *64	192.168.2.40:3389	01:25	Default : proxy.example.net:1080	2.75 KB	4.08 KB
iexplore.exe (4704)	www.l.google.com:80	01:14 Closed	Proxy2 : proxy.example.net:1080	[illegible]	[illegible]
iexplore.exe (5664)	[fe80::9061:83fc:c743:f406]:80 *IPv6	01:12	Local : Test proxy chain	858	376
svchost.exe (376, System) *64	www.update.microsoft.com:80	00:44	Default : proxy.example.net:1080	172	262
svchost.exe (376, System) *64	www.update.microsoft.com:443	00:42	Default : proxy.example.net:1080	131 KB	7.84 KB
iexplore.exe (164)	[illegible]	Failed	HTTPS : proxy2.example.net:8080	0	0
iexplore.exe (2776)	www.microsoft.com:8080	00:21 Connecting	Default : proxy.example.net:1080	0	0

```
[19:59] svchost.exe (376, System) *64 - resolve www.update.microsoft.com : DNS
[19:59] svchost.exe (376, System) *64 - resolve www.update.microsoft.com : DNS
[19:59] svchost.exe (376, System) *64 - www.update.microsoft.com:443 matching Default rule : using proxy proxy.example.net:1080
[19:59] svchost.exe (376, System) *64 - www.update.microsoft.com:443 open through proxy proxy.example.net:1080
[19:59] svchost.exe (376, System) *64 - download.windowsupdate.com:80 close, 931 bytes sent, 1183 bytes (1.15 KB) received, lifetime 00:05
[19:59] svchost.exe (376, System) *64 - resolve download.windowsupdate.com : DNS
[19:59] svchost.exe (376, System) *64 - resolve download.windowsupdate.com : DNS
[19:59] svchost.exe (376, System) *64 - download.windowsupdate.com:80 matching Default rule : using proxy proxy.example.net:1080
[19:59] svchost.exe (376, System) *64 - download.windowsupdate.com:80 open through proxy proxy.example.net:1080
[20:00] svchost.exe (376, System) *64 - download.windowsupdate.com:80 close, 175 bytes sent, 298 bytes received, lifetime 00:04
[20:00] iexplore.exe (164) - [illegible] matching HTTPS rule : using proxy proxy2.example.net:8080
[20:00] iexplore.exe (2776) - www.microsoft.com:8080 matching Default rule : using proxy proxy.example.net:1080
[20:00] iexplore.exe (4704) - www.l.google.com:80 close, 1560 bytes (1.52 KB) sent, [illegible] bytes received, lifetime 00:59
[20:00] iexplore.exe (5664) - www.l.google.com:80 close, 1456 bytes (1.42 KB) sent, [illegible] bytes received, lifetime 01:11
[20:00] iexplore.exe (5664) - www.l.google.com:80 close, 3530 bytes (3.44 KB) sent, 722 bytes received, lifetime 01:11
[20:00] iexplore.exe (4704) - www.l.google.com:80 close, 3413 bytes (3.33 KB) sent, [illegible] bytes received, lifetime 01:14
[20:00] iexplore.exe (164) - [illegible] error : Could not connect through proxy proxy2.example.net:8080 - [illegible]
[20:00] svchost.exe (376, System) *64 - www.update.microsoft.com:80 close, 172 bytes sent, 262 bytes received, lifetime 01:01
```

Proxy Tool: **Proxy Switcher**

Proxy Switcher **hides your IP address** from the websites you visit



Server	State	Respo...	Country
91.121.21.164:3128	(Anonymous)	603ms	FRANCE
ns1.homenux.com:3128	(Anonymous)	1092ms	FRANCE
hherphpo.hchd.tmc.edu:80	(Anonymous)	1612ms	UNITED STATES
170.57.24.100:80	(Anonymous)	1653ms	UNITED STATES
81.180.75.142:8080	(Anonymous)	1882ms	REPUBLIC OF MOLDOVA
66-162-61-85.static.twtele...	(Anonymous)	2200ms	UNITED STATES
194.160.76.5:80	(Anonymous)	2319ms	SLOVAKIA
amac3.minedu.sk:80	(Anonymous)	2324ms	SLOVAKIA
147.46.7.54:8088	(Anonymous)	2543ms	REPUBLIC OF KOREA
159.226.3.227:80	(Anonymous)	2641ms	CHINA
121.52.148.30:8080	(Anonymous)	2683ms	PAKISTAN
208-74-174-142.sayfa.net:31	(Anonymous)	2698ms	UNITED STATES

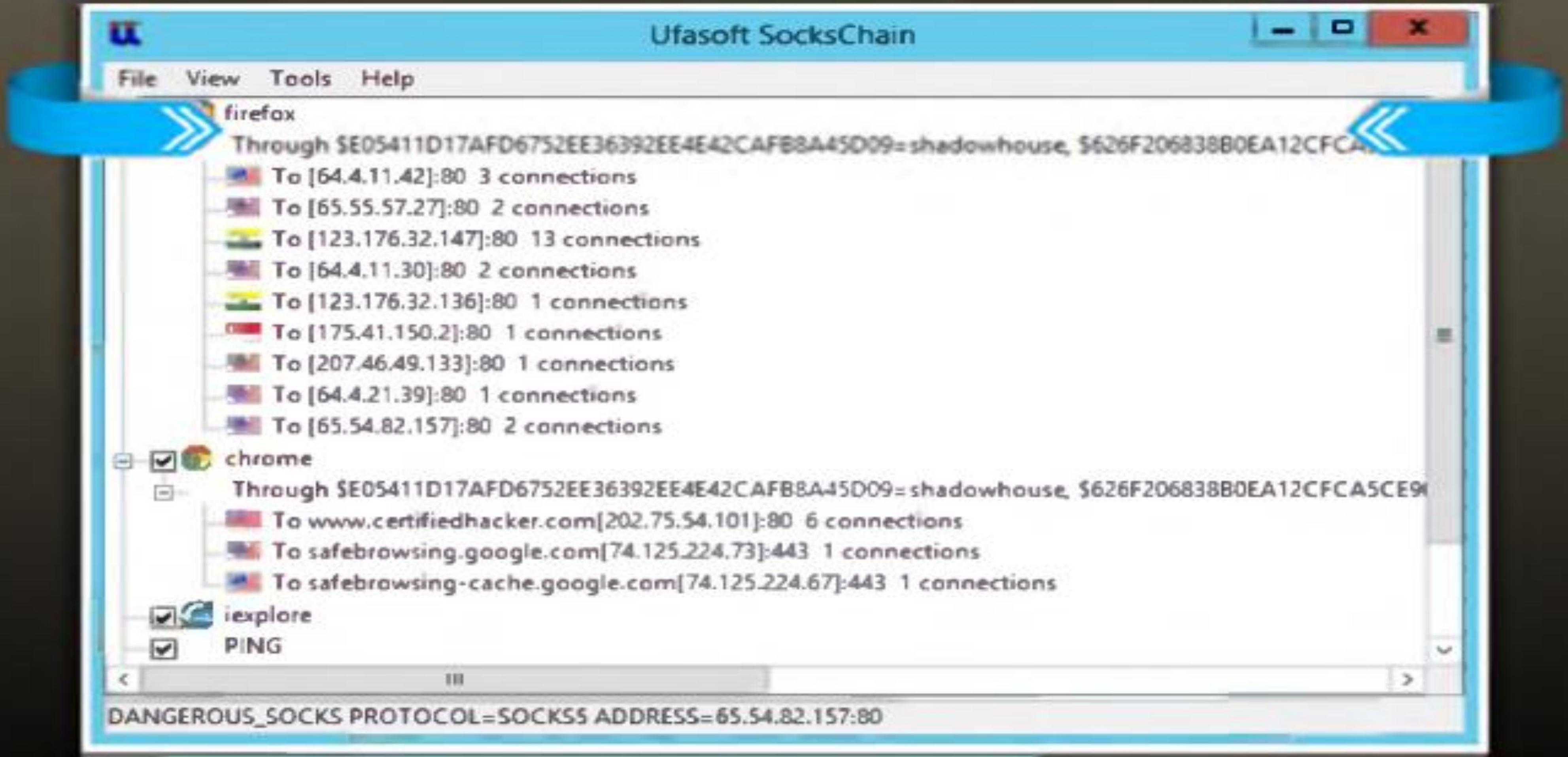
```
98.181.57.227:9090 tested as [Elite-Anonymous]
correo.diresacallao.gob.pe:80 tested as [Dead]
smtp.spectrum-networks.net:80 tested as [(Elite-SSL)]
f-kasklab50a.eti.pg.gda.pl:80 tested as [Elite-Anonymous]
correo.diresacallao.gob.pe:80 tested as [(Elite-SSL)]
```

High Anonymous/SSL 0/6

http://www.proxyswitcher.com

Proxy Tool: SocksChain

- SocksChain **transmits the TCP/IP applications** through a chain of proxy servers



```
firefox
  Through $E05411D17AFD6752EE36392EE4E42CAFB8A45D09=shadowhouse, $626F206838B0EA12CFCA
    To [64.4.11.42]:80  3 connections
    To [65.55.57.27]:80  2 connections
    To [123.176.32.147]:80  13 connections
    To [64.4.11.30]:80  2 connections
    To [123.176.32.136]:80  1 connections
    To [175.41.150.2]:80  1 connections
    To [207.46.49.133]:80  1 connections
    To [64.4.21.39]:80  1 connections
    To [65.54.82.157]:80  2 connections
☑ chrome
  Through $E05411D17AFD6752EE36392EE4E42CAFB8A45D09=shadowhouse, $626F206838B0EA12CFCA5CE9
    To www.certifiedhacker.com[202.75.54.101]:80  6 connections
    To safebrowsing.google.com[74.125.224.73]:443  1 connections
    To safebrowsing-cache.google.com[74.125.224.67]:443  1 connections
☑ iexplore
☑ PING
DANGEROUS_SOCKS PROTOCOL=SOCKS5 ADDRESS=65.54.82.157:80
```

Proxy Tool: TOR (The Onion Routing)

Anonymity

Provides anonymous communication over Internet

Privacy

Ensures the privacy of both sender and recipient of a message

Security

Provides multiple layers of security to a message

Encryption

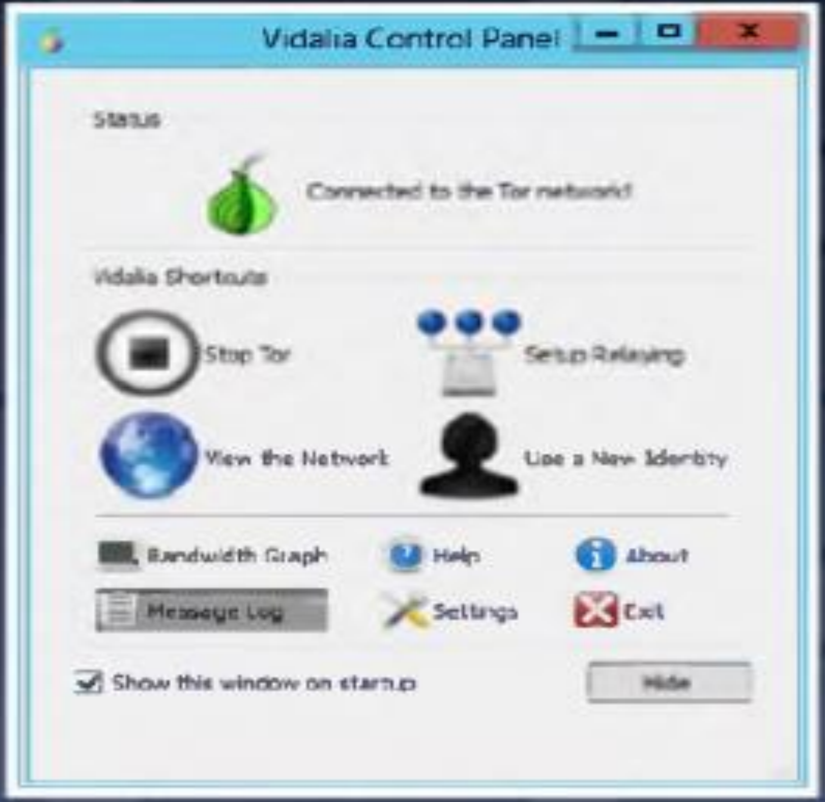
Encrypts and decrypts all data packets using public key encryption

Proxy Chain

Uses cooperating proxy routers throughout the network

Tor Proxy

The initiating onion router, called a "Tor client" determines the path of transmission



Vidalia Control Panel

Status

Connected to the Tor network!

☑ Show this window on startup

https://www.torproject.org

Proxy Tools

Burp Suite
http://www.portswigger.net

Proxy Commander
http://www.dlao.com

Proxy Tool Windows App
http://webproxylist.com

Gproxy
http://gpass1.com

Fiddler
http://www.fiddler2.com

Proxy
http://www.analogx.com

Protoport Proxy Chain
http://www.protoport.com

Proxy+
http://www.proxyplus.cz

FastProxySwitch
http://affinity-tools.com

ProxyFinder
http://www.proxy-tool.com

Proxy Tools
(Cont'd)

ProxyFinder Enterprise
http://www.proxy-tool.com

ezProxy
http://www.oclc.org

JAP Anonymity and Privacy
http://anon.inf.tu-dresden.de/index_en.html

CC Proxy Server
http://www.youngzsoft.net

FoxyProxy Standard
https://addons.mozilla.org

Socks Proxy Scanner
http://www.mylanviewer.com

Charles
http://www.charlesproxy.com

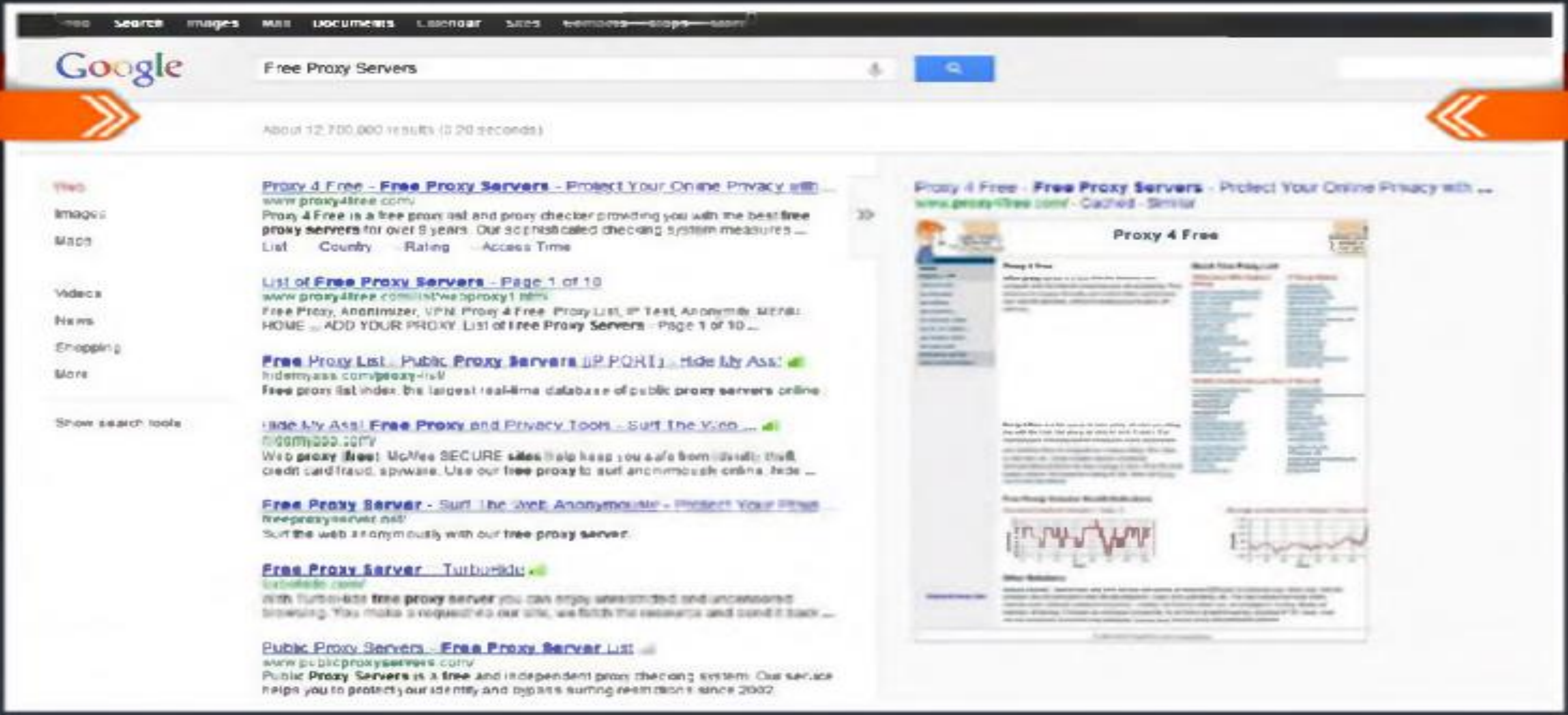
UltraSurf
http://www.ultrasurf.us

WideCap
http://widecap.ru

ProxyCap
http://www.proxycap.com

Free Proxy Servers

A search in Google lists thousands of free proxy servers



About 12,700,000 results (0.20 seconds)

[Proxy 4 Free - **Free Proxy Servers** - Protect Your Online Privacy with ...]
www.proxy4free.com/
Proxy 4 Free is a free proxy list and proxy checker providing you with the best **free proxy servers** for over 8 years. Our sophisticated checking system measures ...
List Country Rating Access Time

[List of **Free Proxy Servers** - Page 1 of 10]
www.proxy4free.com/list/webproxy1.html
Free Proxy, Anonimizer, VPN. Proxy 4 Free. Proxy List, IP Test, Anonymity. MENU: HOME ... ADD YOUR PROXY. List of **free Proxy Servers** - Page 1 of 10 ...

[**Free** Proxy List - Public **Proxy Servers** (IP PORT) - Hide My Ass!]
hidemyass.com/proxy-list/
Free proxy list index, the largest real-time database of public **proxy servers** online.

[Hide My Ass! **Free Proxy** and Privacy Tools - Surf The Web ...]
hidemyass.com/
Web **proxy free**! McAfee SECURE **sites** help keep you safe from identity theft, credit card fraud, spyware. Use our **free proxy** to surf anonymously online, hide ...

[**Free Proxy Server** - Surf The Web Anonymously - Protect Your Priva...]
freeproxyserver.net/
Surf the web anonymously with our **free proxy server**.

[**Free Proxy Server** - TurboHide]
turbohide.com/
With TurboHide **free proxy server** you can enjoy unrestricted and uncensored browsing. You make a request to our site, we fetch the resource and send it back ...

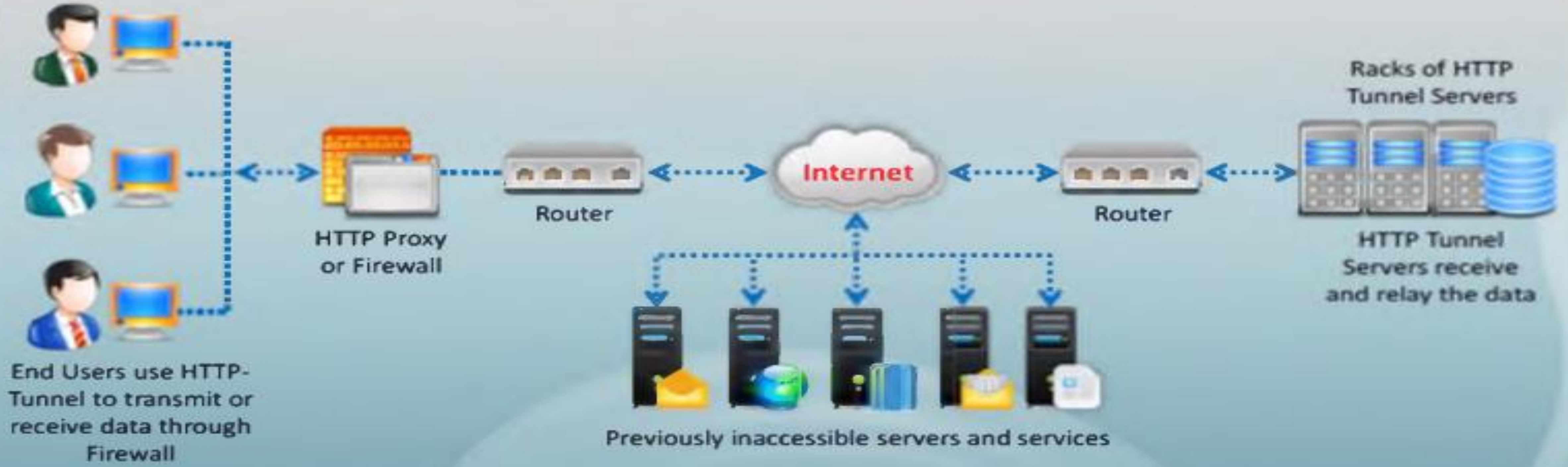
[Public Proxy Servers - **Free Proxy Server** List]
www.publicproxyservers.com/
Public **Proxy Servers** is a **free** and independent proxy checking system. Our service helps you to protect your identity and bypass surfing restrictions since 2002.

[Proxy 4 Free - **Free Proxy Servers** - Protect Your Online Privacy with ...]
www.proxy4free.com/ - Cached - Similar

Proxy 4 Free

HTTP Tunneling Techniques

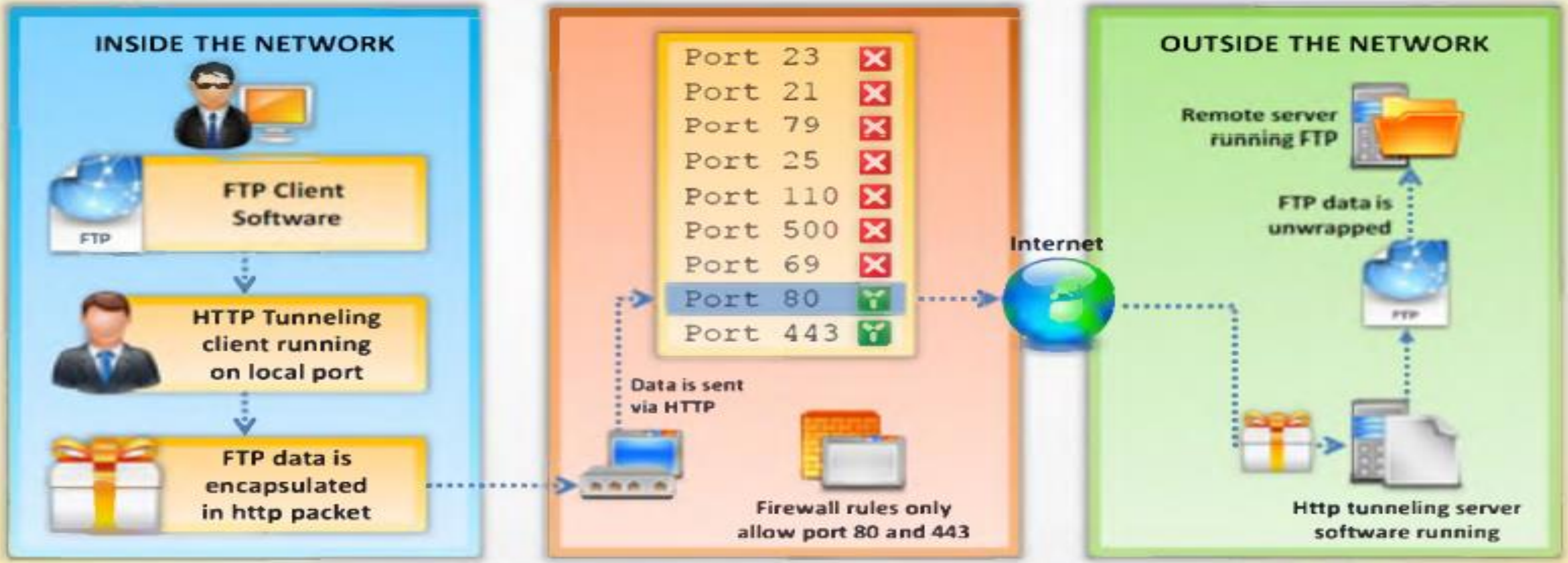
- HTTP Tunneling technology allows users to **perform various Internet tasks** despite the restrictions imposed by firewalls
- **Encapsulates data** inside **HTTP traffic** (port 80)



End Users use HTTP-Tunnel to transmit or receive data through Firewall
HTTP Proxy or Firewall
Router
Internet
Router
Racks of HTTP Tunnel Servers
HTTP Tunnel Servers receive and relay the data
Previously inaccessible servers and services

Why do I Need HTTP Tunneling

- Organizations firewall all ports except **80** and **443**, and you may want to use FTP
- HTTP tunneling will enable use of **FTP via HTTP protocol**



INSIDE THE NETWORK

FTP Client Software

HTTP Tunneling client running on local port

FTP data is encapsulated in http packet

Port 23	☒
Port 21	☒
Port 79	☒
Port 25	☒
Port 110	☒
Port 500	☒
Port 69	☒
Port 80	✓
Port 443	✓

Data is sent via HTTP

Firewall rules only allow port 80 and 443

Internet

OUTSIDE THE NETWORK

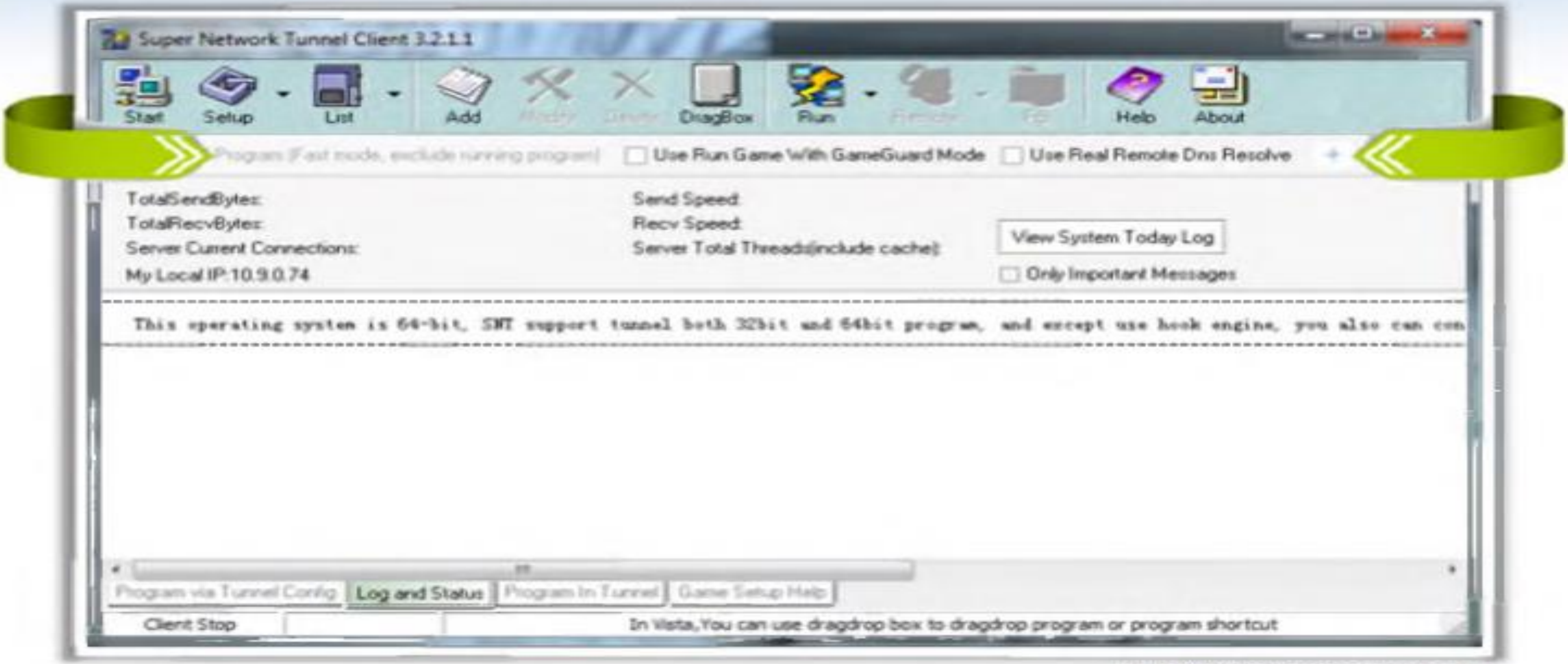
Remote server running FTP

FTP data is unwrapped

Http tunneling server software running

HTTP Tunneling Tool: Super Network Tunnel

- A **two-way http tunnel** software connecting two computers
- Works like **VPN tunneling** but uses HTTP protocol to establish a connection



Program (Fast mode, exclude running program) □ Use Run Game With GameGuard Mode □ Use Real Remote Dns Resolve

TotalSendBytes:
TotalRecvBytes:
Server Current Connections:
My Local IP:10.9.0.74

Send Speed:
Recv Speed:
Server Total Threads(include cache):

□ Only Important Messages

```
This operating system is 64-bit, SNT support tunnel both 32bit and 64bit program, and except use hook engine, you also can con
```

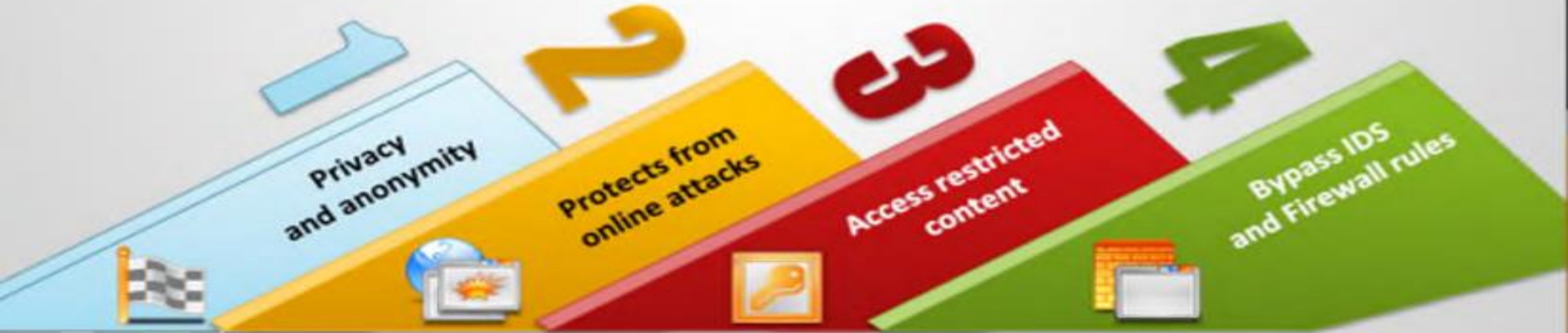
Client Stop | In Vista,You can use dragdrop box to dragdrop program or program shortcut

http://www.networktunnel.net

Anonymizers

- An anonymizer **removes all the identifying information** from the user's computer while the user surfs the Internet
- Anonymizers make **activity on the Internet untraceable**
- Anonymizer tools allow you to **bypass Internet censored websites**

Why use Anonymizer?



1
Privacy and anonymity
2
Protects from online attacks
3
Access restricted content
4
Bypass IDS and Firewall rules

Case: Bloggers Write Text Backwards to **Bypass Web Filters** in China

Bloggers and journalists in China are using a novel approach to **bypass Internet filters** in their country – they write backwards or from right to left

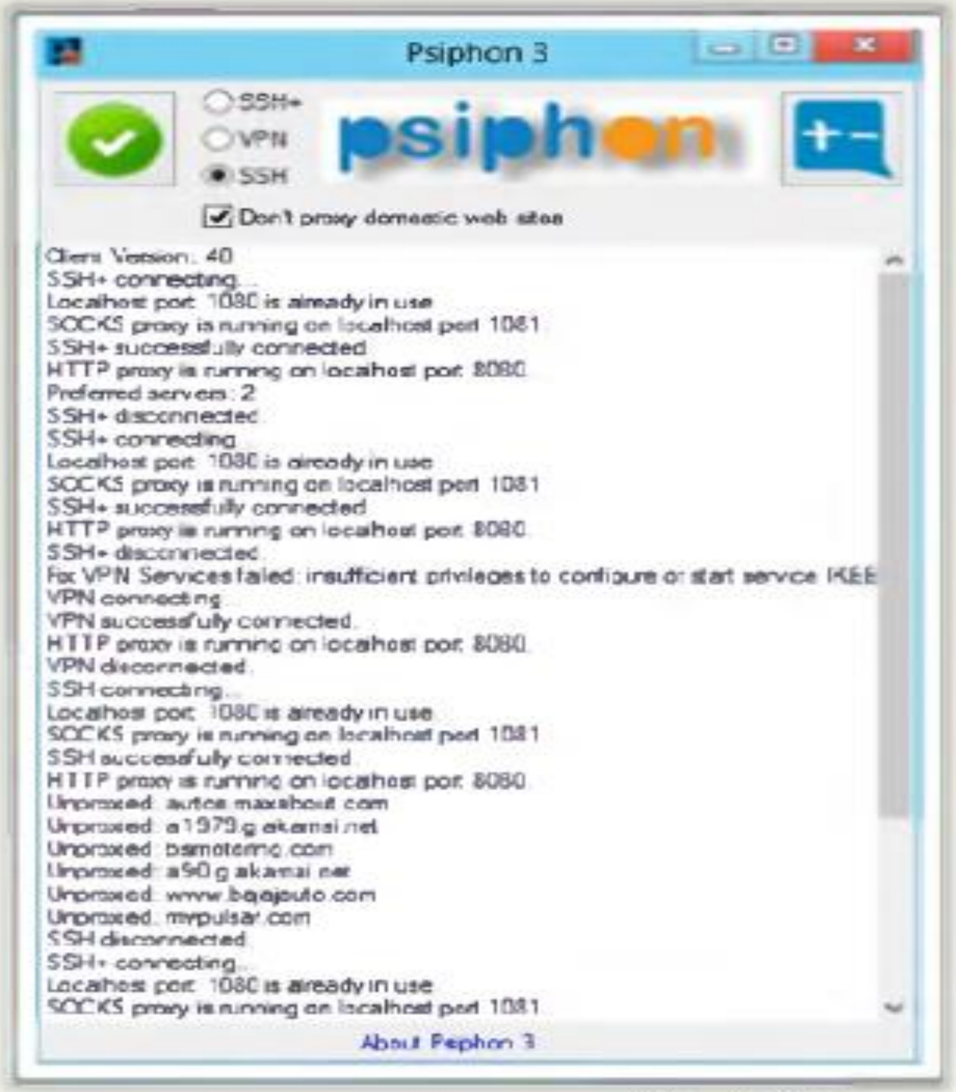
"IF IT BOTHERS YOU THAT THE CHINA GOVERNMENT DOES IT, IT SHOULD BOTHER YOU WHEN YOUR CABLE COMPANY DOES IT."

The content therefore remains readable by human beings but defeats the **web filtering software**

China is implementing '**packet filtering**' to detect TCP packets containing controversial keywords such as Tibet, Democracy, Tiananmen, etc.

Censorship Circumvention Tool: Psiphon

- Psiphon is a censorship circumvention system that allows users to bypass firewalls and access blocked sites in countries where the Internet is censored
- It uses a secure, encrypted HTTP tunnel connection to receive requests from psiphonite to psiphonode which in turn transports the results back to the requested psophonite
- It acts as a web proxy for authenticated psiphonites, even works on mobile devices
- It bypass the content-filtering systems of countries like China, North Korea, Iran, Saudi Arabia, Egypt and others



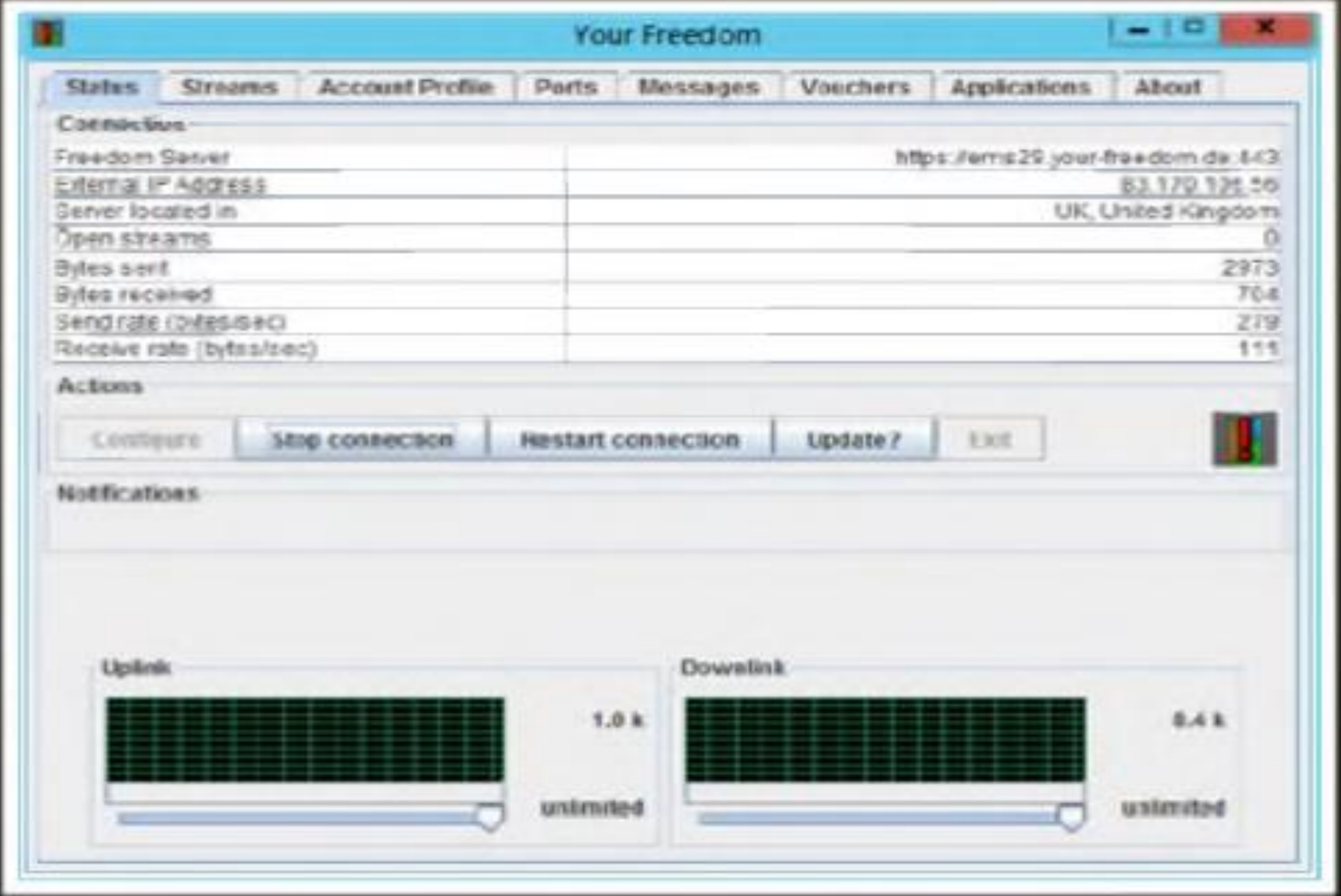
☑ Don't proxy domestic web sites

```
Client Version: 40
SSH+ connecting...
Localhost port 1080 is already in use
SOCKS proxy is running on localhost port 1081
SSH+ successfully connected
HTTP proxy is running on localhost port 8080
Preferred servers: 2
SSH+ disconnected
SSH+ connecting
Localhost port 1080 is already in use
SOCKS proxy is running on localhost port 1081
SSH+ successfully connected
HTTP proxy is running on localhost port 8080
SSH+ disconnected
Fix VPN Services failed: insufficient privileges to configure or start service IKEE
VPN connecting
VPN successfully connected.
HTTP proxy is running on localhost port 8080
VPN disconnected
SSH connecting...
Localhost port 1080 is already in use
SOCKS proxy is running on localhost port 1081
SSH successfully connected
HTTP proxy is running on localhost port 8080
Unproxied: autos.maxabout.com
Unproxied: a1979.g.akamai.net
Unproxied: bsmotoring.com
Unproxied: a90.g.akamai.net
Unproxied: www.bajajauto.com
Unproxied: mypulsar.com
SSH disconnected
SSH+ connecting...
Localhost port 1080 is already in use
SOCKS proxy is running on localhost port 1081
```

http://psiphan.ca

Censorship Circumvention Tool: Your-Freedom

- Freedom services makes accessible what is inaccessible to you, and it hides your network address from those who do not need to know
- It turns your own PC into an uncensored, anonymous web proxy and an uncensored, anonymous SOCKS proxy that your applications can use



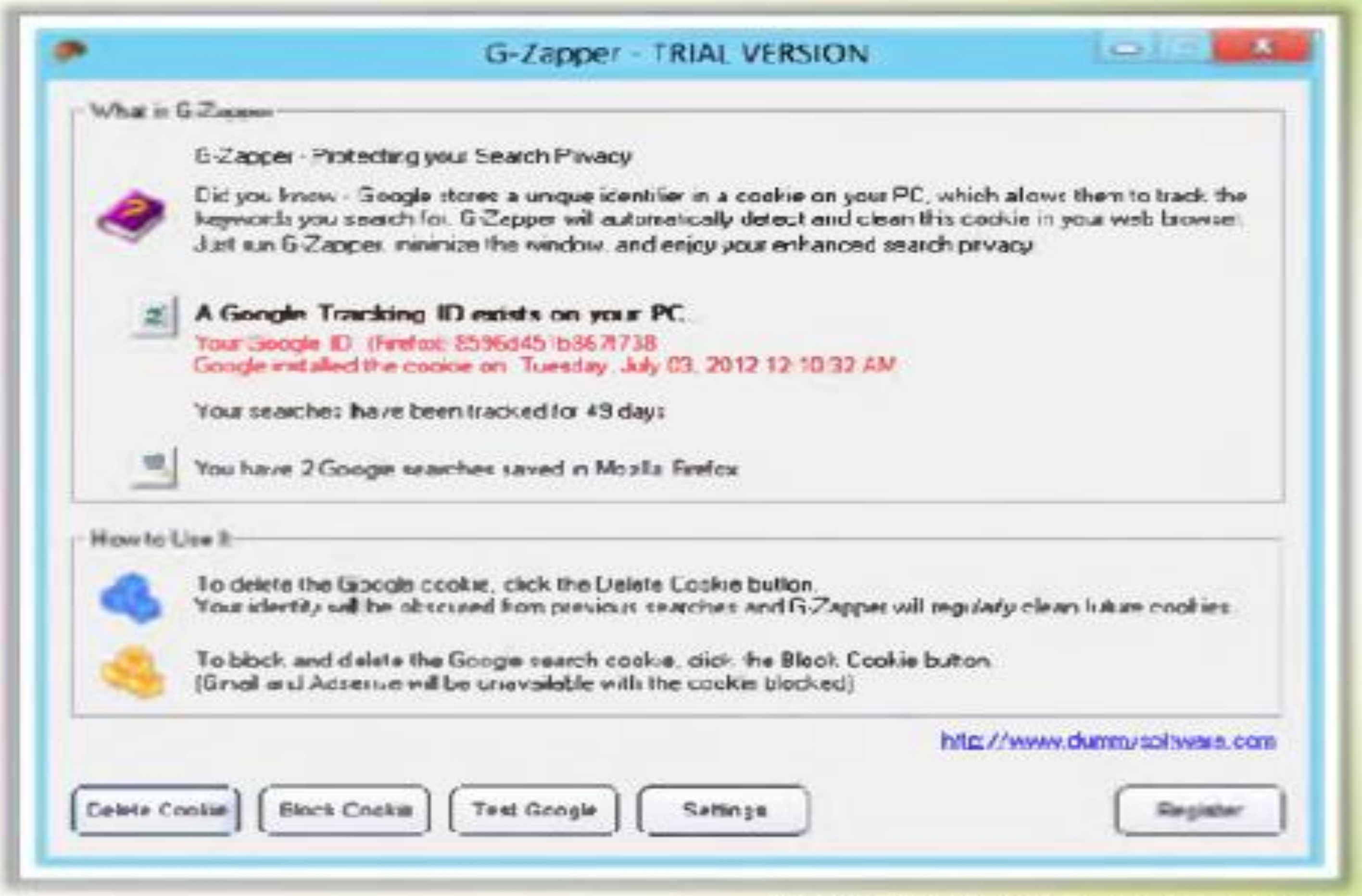
Connection

Freedom Server	https://ems29.your-freedom.de:443
External IP Address	83.170.124.56
Server located in	UK, United Kingdom
Open streams	0
Bytes sent	2973
Bytes received	704
Send rate (bytes/sec)	279
Receive rate (bytes/sec)	111

G-Zapper

G-Zapper

- Google sets a cookie on user's system with a unique identifier that enables them to track user's web activities such as:
  - Search Keywords and habits
  - Search results
  - Websites visited
- Information from Google cookies can be used as evidence in a court of law



G-Zapper - Protecting your Search Privacy

Did you know - Google stores a unique identifier in a cookie on your PC, which allows them to track the keywords you search for. G-Zapper will automatically detect and clean this cookie in your web browser. Just run G-Zapper, minimize the window, and enjoy your enhanced search privacy

A Google Tracking ID exists on your PC.

Your Google ID: (Firefox) 8596d451b8678738
Google installed the cookie on: Tuesday, July 03, 2012 12:10:32 AM

Your searches have been tracked for 49 days

You have 2 Google searches saved in Mozilla Firefox

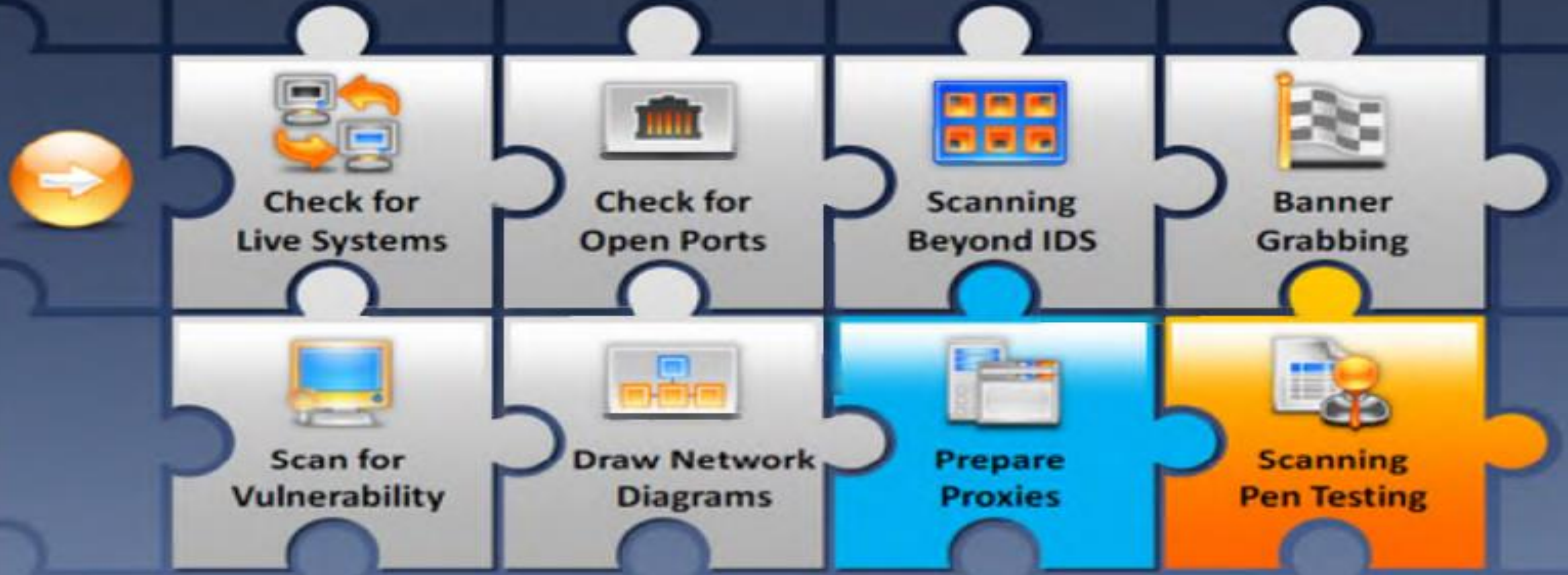
To delete the Google cookie, click the Delete Cookie button.
Your identity will be obscured from previous searches and G-Zapper will regularly clean future cookies

To block and delete the Google search cookie, click the Block Cookie button
(Gmail and Adsense will be unavailable with the cookie blocked)

http://www.dummysoftware.com

http://www.dummysoftware.com

Scanning Methodology



Check for Live Systems

Check for Open Ports

Scanning Beyond IDS

Banner Grabbing

Scan for Vulnerability

Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

Scanning Pen Testing

- Pen testing a network for scanning vulnerabilities determines the network's security posture by identifying live systems, discovering open ports, associating services and grabbing system banners to simulate a network hacking attempt
- The penetration testing report will help system administrators to:

Close unused ports

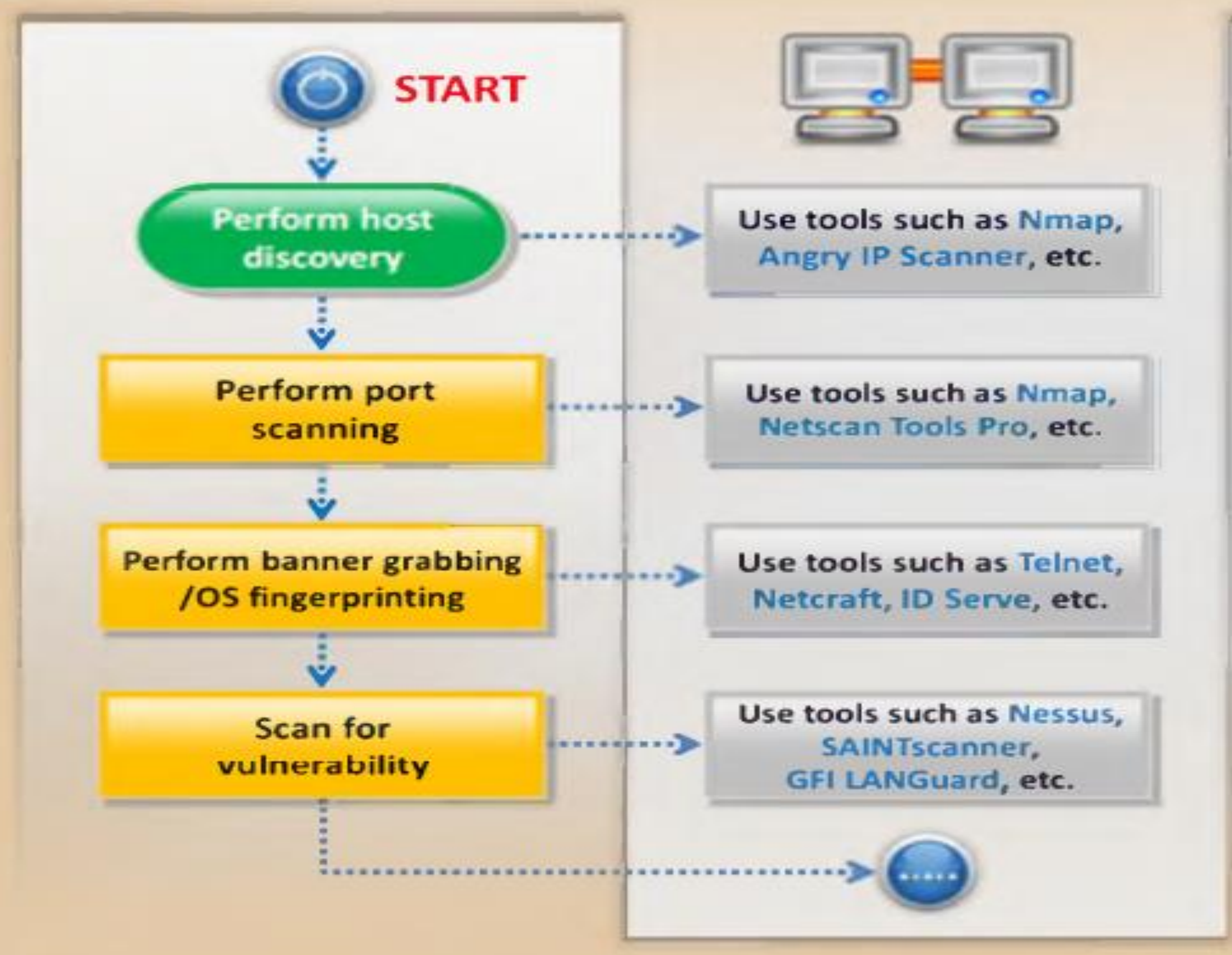
Calibrate firewall rules

Disable unnecessary services

Troubleshoot service configuration errors

Hide or customize banners

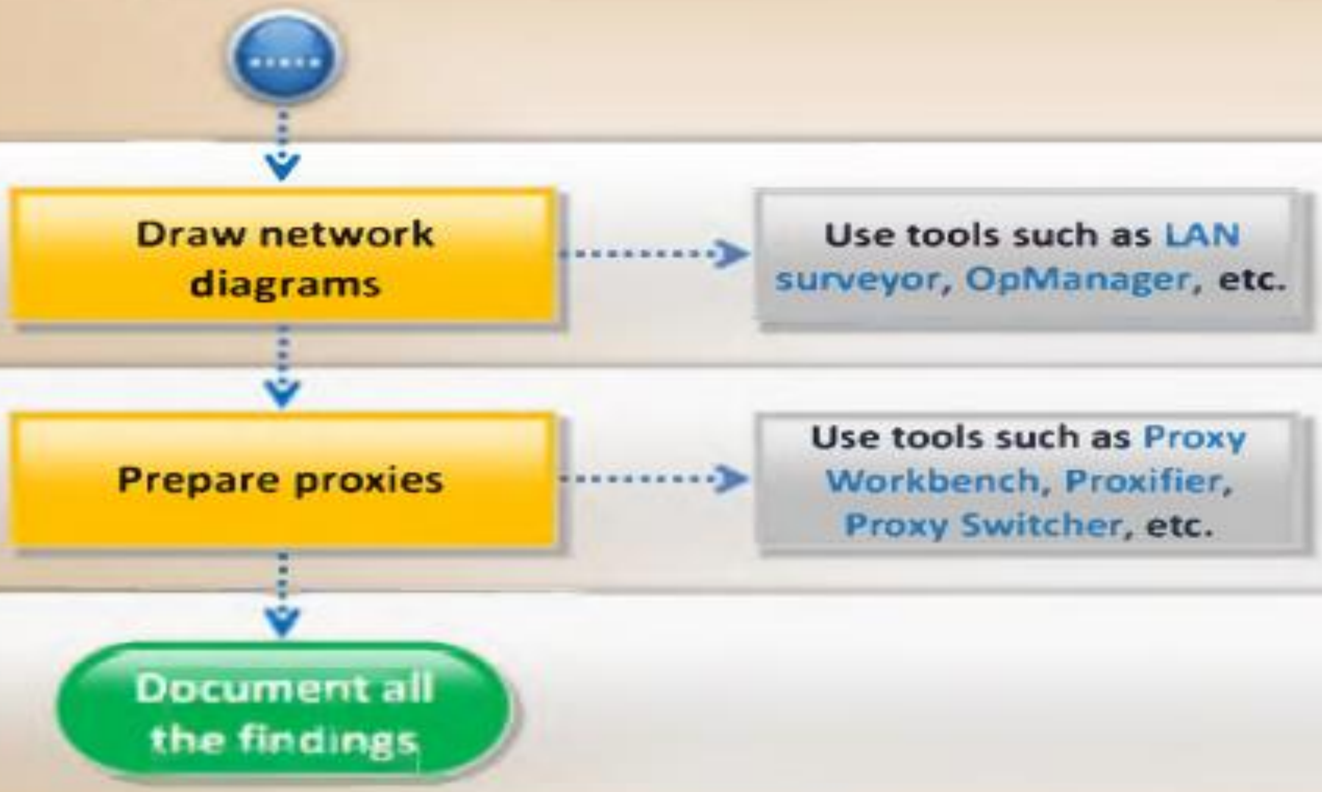
Scanning Pen Testing
(Cont'd)



START
Perform host discovery
Use tools such as Nmap, Angry IP Scanner, etc.
Perform port scanning
Use tools such as Nmap, Netscan Tools Pro, etc.
Perform banner grabbing /OS fingerprinting
Use tools such as Telnet, Netcraft, ID Serve, etc.
Scan for vulnerability
Use tools such as Nessus, SAINTscanner, GFI LANGuard, etc.
.....

- Check for the live hosts using tools such as **Nmap, Angry IP Scanner, SolarWinds Engineer's toolset, Colasoft Ping Tool**, etc.
- Check for open ports using tools such as **Nmap, Netscan Tools Pro, PRTG Network Monitor, Net Tools**, etc.
- Perform banner grabbing/OS fingerprinting using tools such as **Telnet, Netcraft, ID Serve**, etc.
- Scan for vulnerabilities using tools such as **Nessus, GFI LANGuard, SAINTscanner, Core Impact Professional, Retina CS Management, MBSA**, etc.

Scanning Pen Testing (Cont'd)



Draw network diagrams

Use tools such as LAN surveyor, OpManager, etc.

Prepare proxies

Use tools such as Proxy Workbench, Proxifier, Proxy Switcher, etc.

Document all the findings

- Draw network diagrams of the vulnerable hosts using tools such as LAN surveyor, OpManager, NetworkView, The Dude, FriendlyPinger, etc.
- Prepare proxies using tools such as Proxy Workbench, Proxifier, Proxy Switcher, SocksChain, TOR, etc.
- Document all the findings

Module Summary

- ❑ The objective of scanning is to discover live systems, active/running ports, the operating systems, and the services running on the network
- ❑ Attacker determines the live hosts from a range of IP addresses by sending ICMP ECHO requests to multiple hosts
- ❑ Attackers use various scanning techniques to bypass firewall rules and logging mechanism, and hide themselves as usual network traffic
- ❑ Banner grabbing or OS fingerprinting is the method to determine the operating system running on a remote target system
- ❑ Drawing target's network diagram gives valuable information about the network and its architecture to an attacker
- ❑ HTTP Tunneling technology allows users to perform various Internet tasks despite the restrictions imposed by firewalls
- ❑ Proxy is a network computer that can serve as an intermediary for connecting with other computers
- ❑ A chain of proxies can be created to evade a traceback to the attacker