Scanning Networks

Module 03

Unmask the Invisible Hacker.

How Tech Companies Prepare for Cyber Attacks

C|EH Certified Ethical Hacker

98% of small and mid-size companies are increasing resources devoted to cyber security

50% are increasing their spend, and investing in active response, not infrastructure

52% are storing their info privately, not in the public cloud

78% say their data and IP are threatened

76% say cyber attacks threaten serious business interruption

46% say media attention has increased awareness of the issue

54% of non-security companies have or plan to add a cybersecurity component to their product

Most Common Cybersecurity Resource Investments

According to the survey of U.S. technology and healthcare executives nationwide by Silicon Valley Bank *http://dr.svb.com*

Module Objectives

- Overview of Network Scanning
- Understanding different techniques to check for Live Systems
- Understanding different techniques to check for Open Ports
- Understanding various Scanning Techniques
- Understanding various IDS Evasion Techniques

- Understanding Banner Grabbing
- Overview of Vulnerability Scanning
- Drawing Network Diagrams
- Using Proxies and Anonymizers for Attack
- Understanding IP Spoofing and various Detection Techniques
- Overview of Scanning Pen Testing

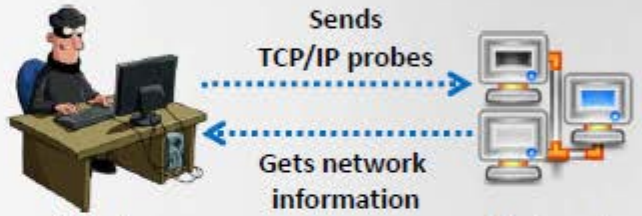


Overview of Network Scanning

01 Network scanning refers to a set of procedures for identifying hosts, ports, and services in a network

02 Network scanning is one of the components of intelligence gathering an attacker uses to create a profile of the target organization

Network Scanning Process



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

TCP Communication Flags

C|EH Certified Ethical Hacker

URG (Urgent)
Data contained in the packet should be processed immediately

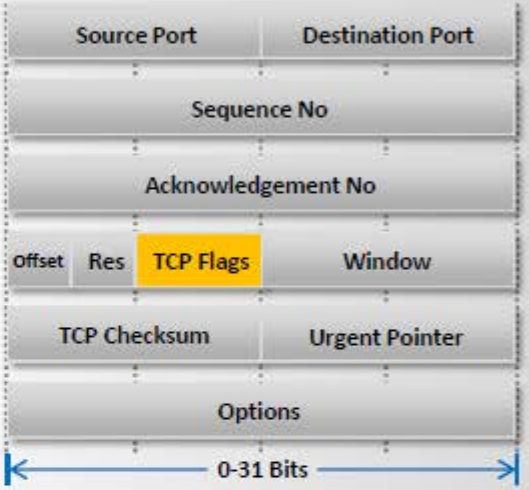
FIN (Finish)
There will be no more transmissions

RST (Reset)
Resets a connection

PSH (Push)
Sends all buffered data immediately

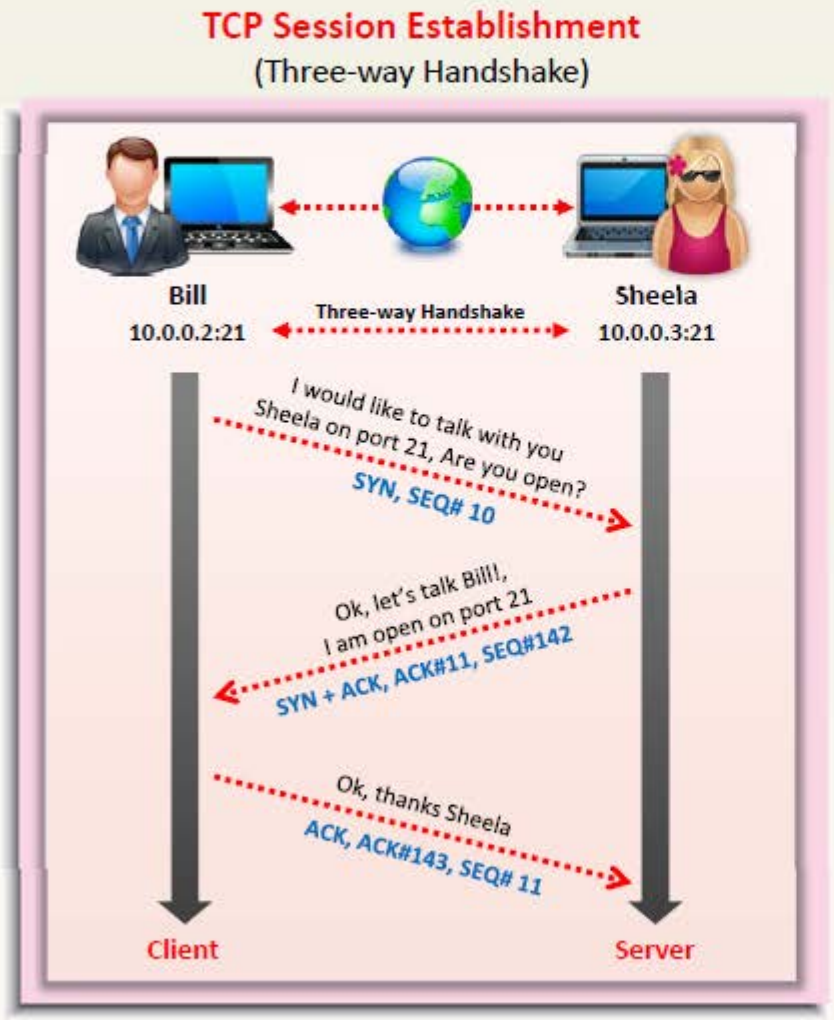
ACK (Acknowledgement)
Acknowledges the receipt of a packet

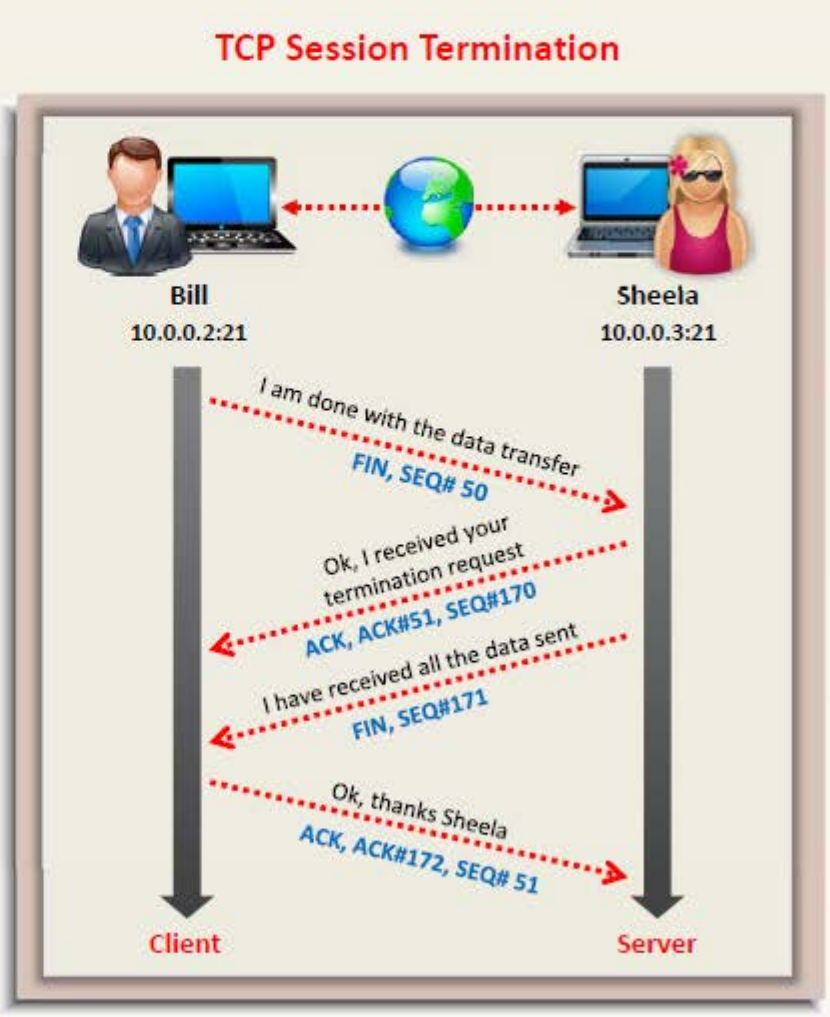
SYN (Synchronize)
Initiates a connection between hosts



Standard TCP communications are controlled by flags in the TCP packet header

TCP/IP Communication

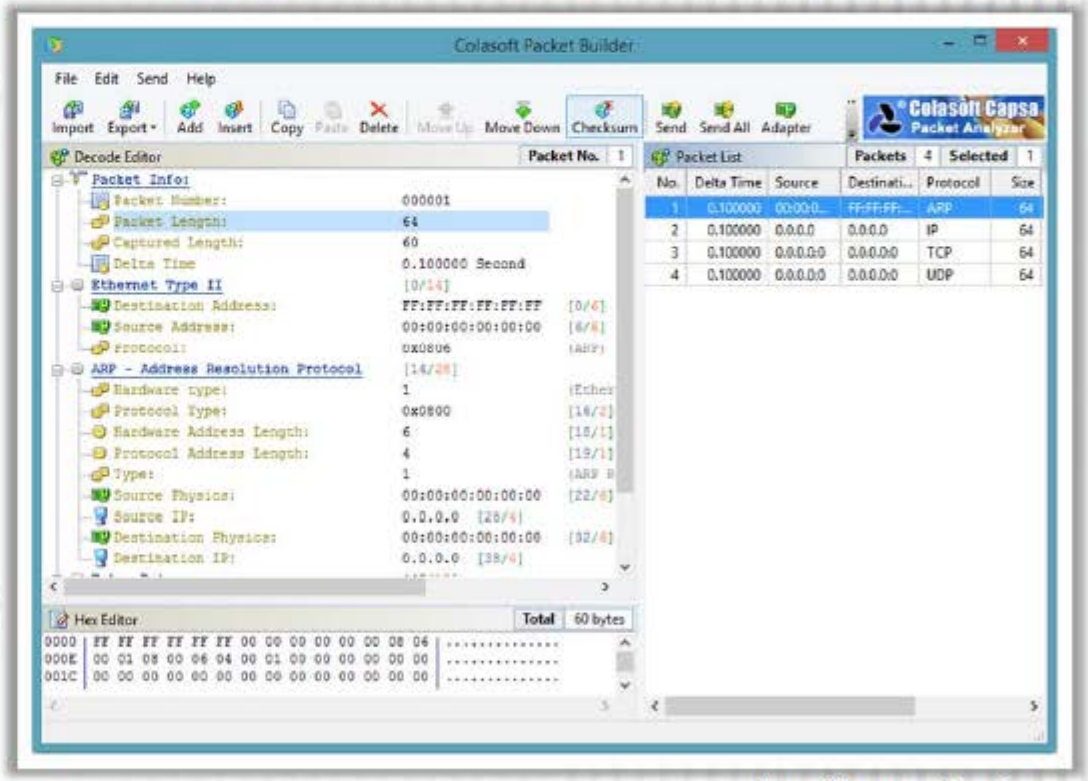




Creating Custom Packet Using TCP Flags

Colasoft Packet Builder enables creating custom network packets to audit networks for various attacks

Attackers can also use it to create fragmented packets to bypass firewalls and IDS systems in a network



http://www.colasoft.com

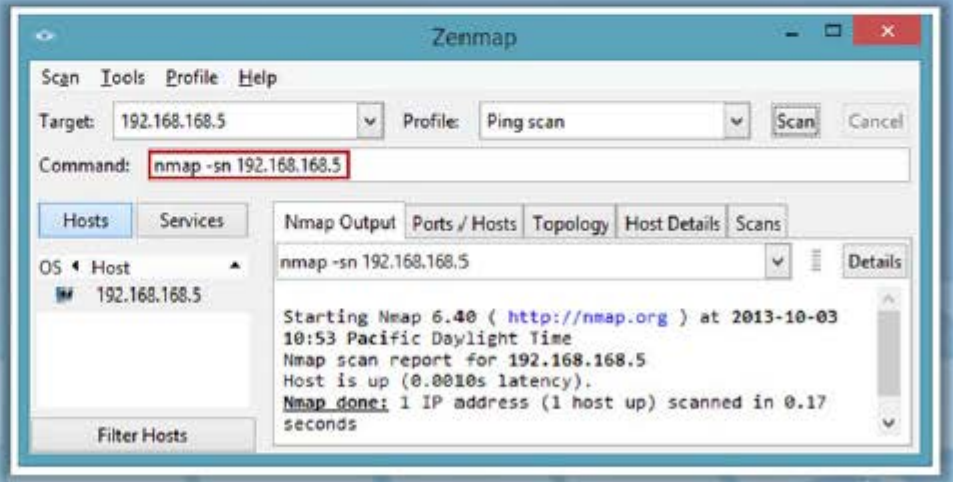
CEH Scanning Methodology

- 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:

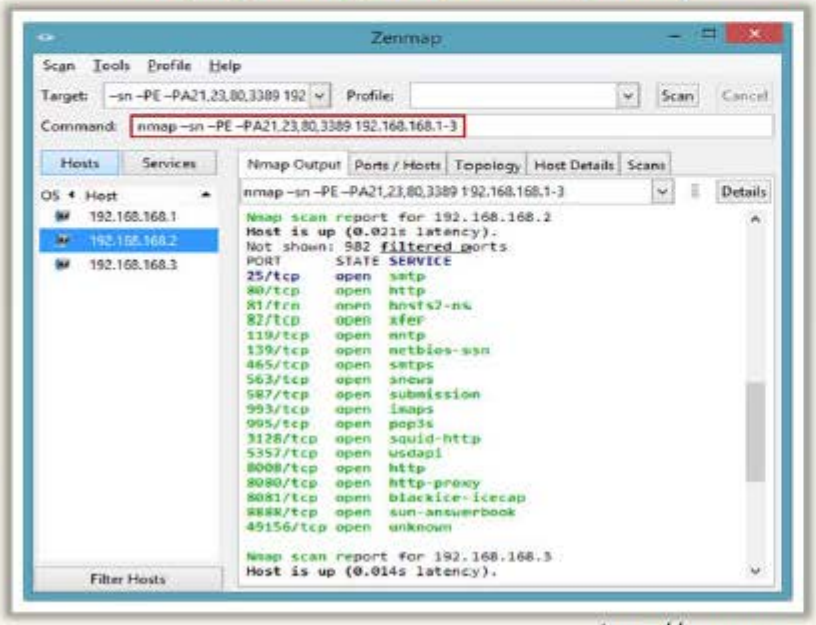


http://nmap.org

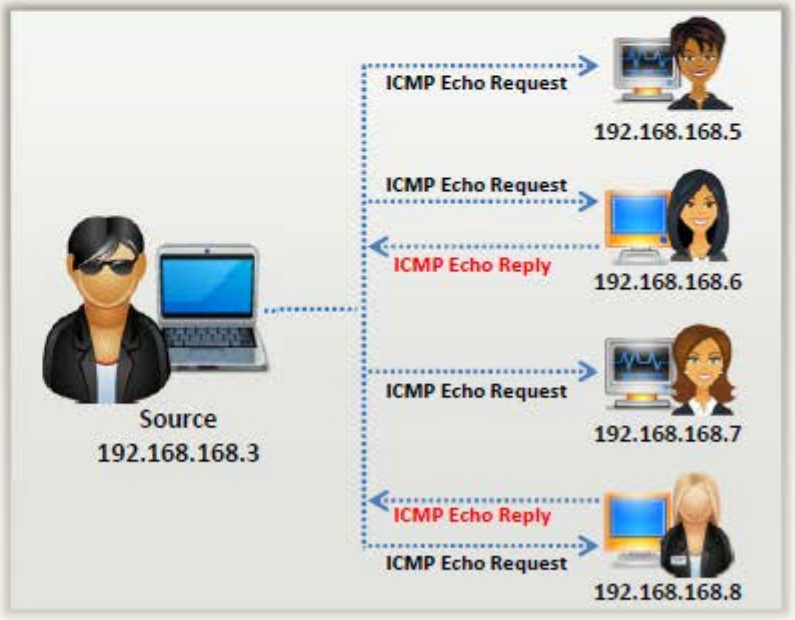
Ping Sweep

- 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

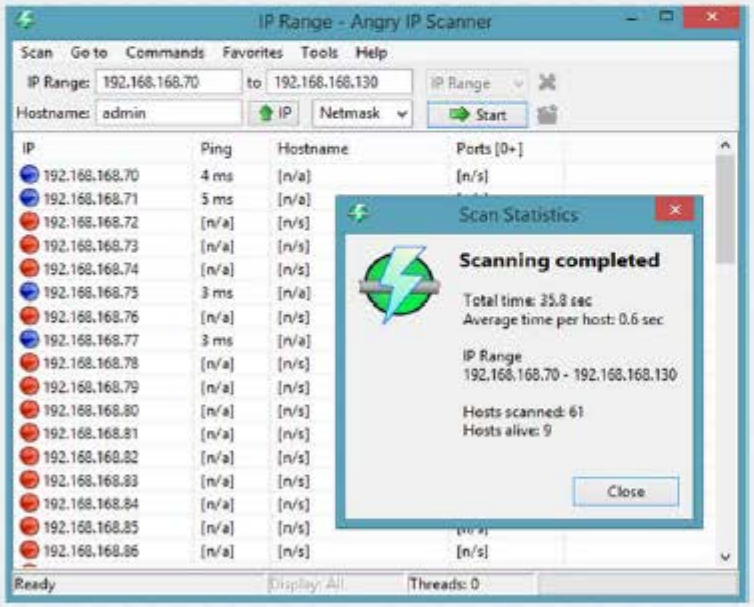


http://nmap.org



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.



Angry IP Scanner

http://www.angryip.org

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**.

SolarWinds Engineer's Toolset

http://www.solarwinds.com

Ping Sweep Tools (Cont'd)

C|EH Certified Ethical Hacker

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

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

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

OpUtils
http://www.manageengine.com

PingInfoView
http://www.nirsoft.net

Advanced IP Scanner
http://www.radmin.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

Ping Sweep Tools (Cont'd)

C|EH Certified Ethical Hacker

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

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

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

OpUtils
http://www.manageengine.com

PingInfoView
http://www.nirsoft.net

Advanced IP Scanner
http://www.radmin.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

CEH 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

SSDP Scanning

- The Simple Service Discovery Protocol (SSDP) is a network protocol that **works in conjunction with UPnP to detect plug and play devices** available in a network

- Vulnerabilities in UPnP may allow attackers to launch **Buffer overflow** or **DoS attacks**
- Attacker may use **UPnP SSDP M-SEARCH** information discovery tool to check if the machine is vulnerable to uPnP exploits or not

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

msf > use auxiliary/scanner/upnp/ssdp_msearch
msf auxiliary(ssdp_msearch) > set RHOSTS 192.168.0.17
RHOSTS => 192.168.0.17
msf auxiliary(ssdp_msearch) > show options

Module options (auxiliary/scanner/upnp/ssdp_msearch):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   BATCHSIZE        256              yes       The number of hosts to probe in each set
   CHOST                             no        The local client address
   REPORT_LOCATION  false            yes       This determines whether to report the UPnP e
   RHOSTS           192.168.0.17     yes       The target address range or CIDR identifier
   RPORT            1900             yes       The target port
   THREADS          1                yes       The number of concurrent threads

msf auxiliary(ssdp_msearch) > exploit

[*] Sending UPnP SSDP probes to 192.168.0.17->192.168.0.17 (1 hosts)
[*] No SSDP endpoints found.
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf auxiliary(ssdp_msearch) >
```

Scanning in IPv6 Networks

C|EH Certified Ethical Hacker

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 some scanning tools do not support ping sweeps on IPv6 networks

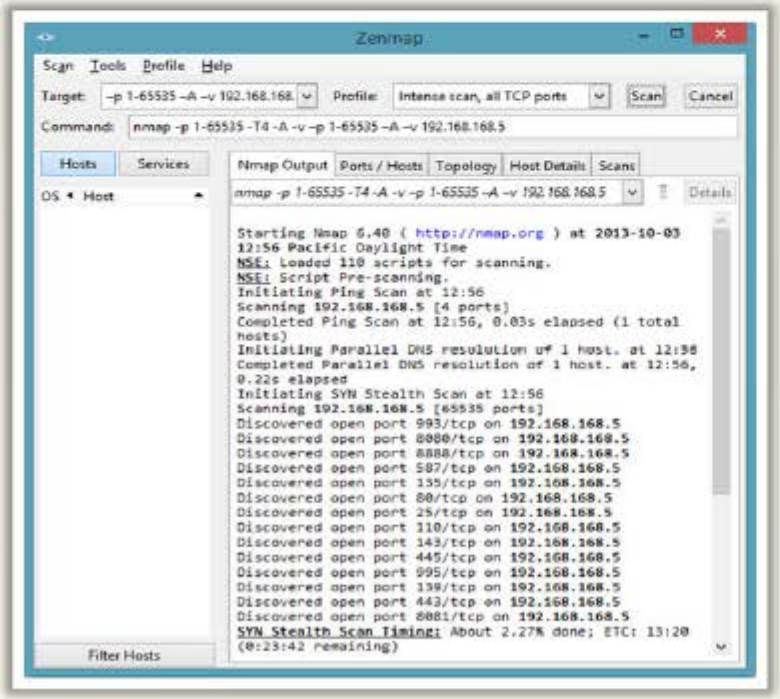
Attackers need to harvest IPv6 addresses from network traffic, recorded logs or Received from: and other header lines in archived email or Usenet news messages

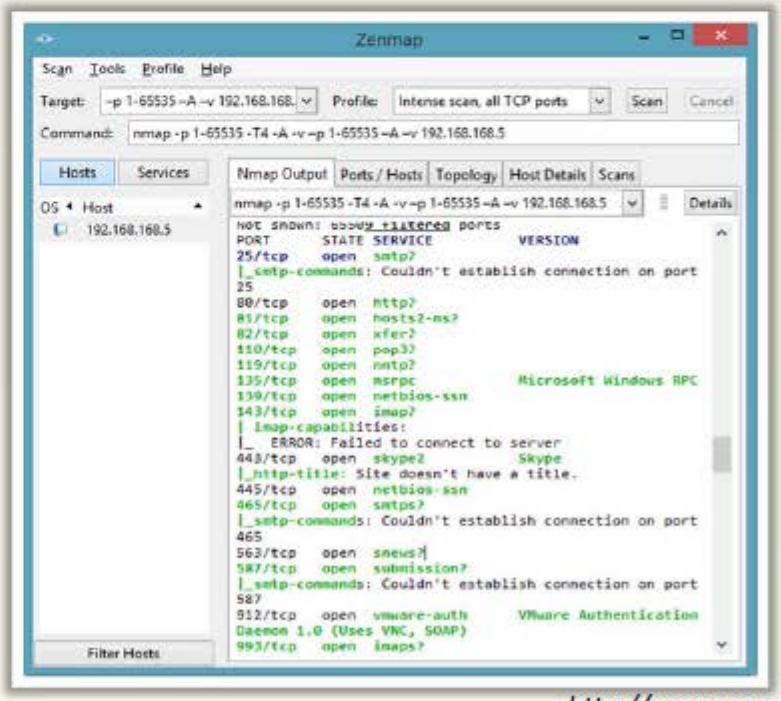
Scanning IPv6 network, however, offers a large number of hosts in a subnet if an attacker can compromise one host in the subnet; attacker can probe the "all hosts" link local multicast address

Scanning Tool: Nmap

01 Network administrators can use Nmap for network inventory, managing service upgrade schedules, and monitoring host or service uptime

02 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





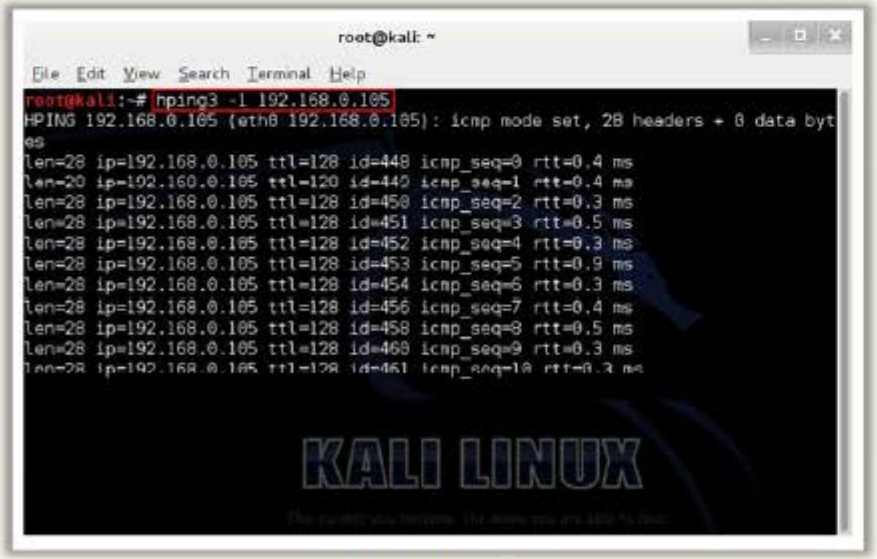
http://nmap.org

Hping2 / Hping3

1. Command line **network scanning** and **packet crafting** tool for the TCP/IP protocol

2. It can be used for **network security auditing**, **firewall testing**, manual path MTU discovery, advanced traceroute, remote OS fingerprinting, remote uptime guessing, TCP/IP stacks auditing, etc.

http://www.hping.org



ICMP Scanning

ACK Scanning on port 80

Hping Commands

C|EH Certified Ethical Hacker

ICMP Ping

```
hping3 -1 10.0.0.25
```

SYN scan on port 50-60

```
hping3 -8 50-60 -S 10.0.0.25 -V
```

ACK scan on port 80

```
hping3 -A 10.0.0.25 -p 80
```

FIN, PUSH and URG scan on port 80

```
hping3 -F -P -U 10.0.0.25 -p 80
```

UDP scan on port 80

```
hping3 -2 10.0.0.25 -p 80
```

Scan entire subnet for live host

```
hping3 -1 10.0.1.x --rand-dest
-I eth0
```

Collecting Initial Sequence Number

```
hping3 192.168.1.103 -Q -p 139 -s
```

Intercept all traffic containing HTTP signature

```
hping3 -9 HTTP -I eth0
```

Firewalls and Time Stamps

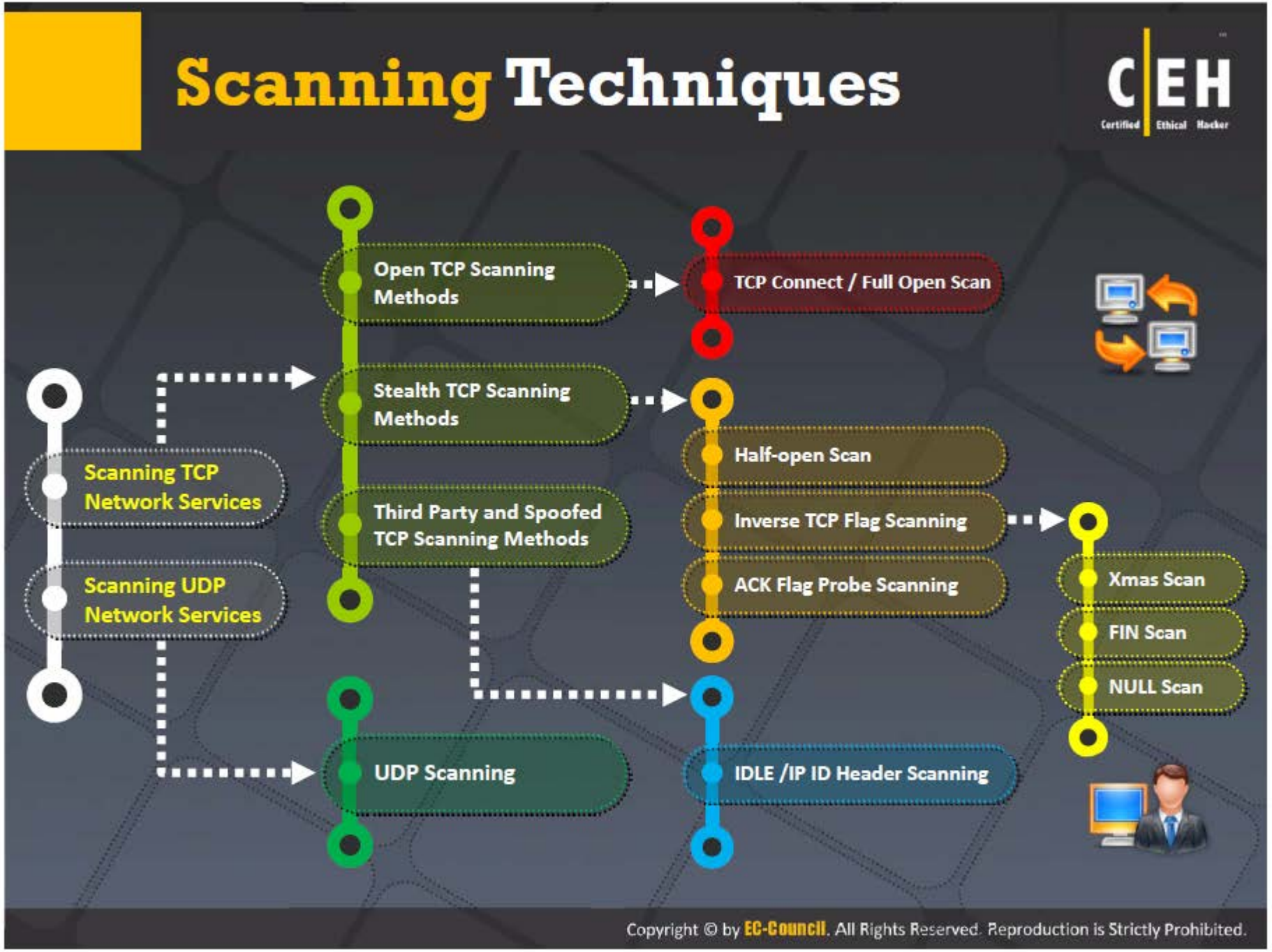
```
hping3 -S 72.14.207.99 -p 80 --
tcp-timestamp
```

SYN flooding a victim

```
hping3 -S 192.168.1.1 -a
192.168.1.254 -p 22 --flood
```

Scanning Techniques

C|EH Certified Ethical Hacker



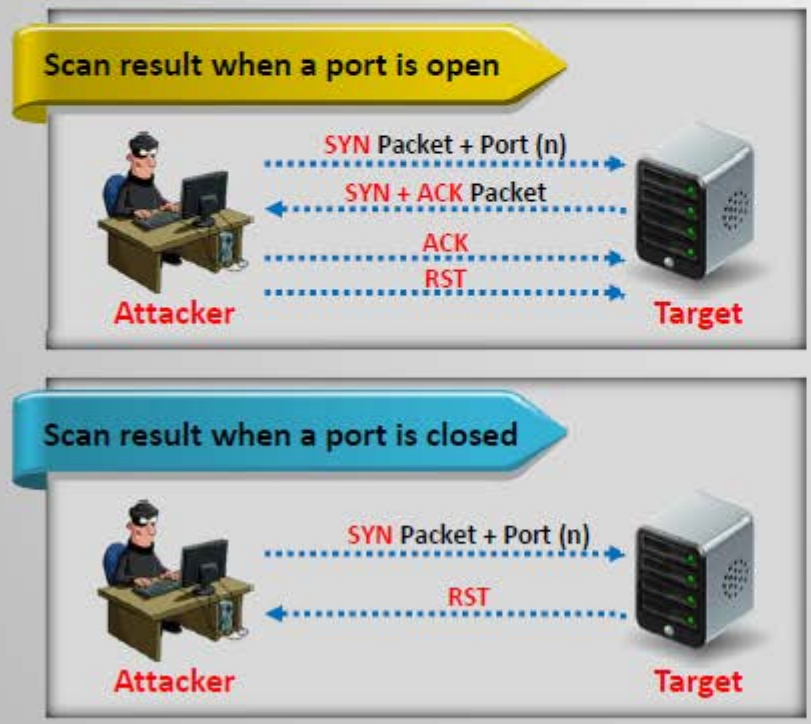
TCP Connect / Full Open Scan

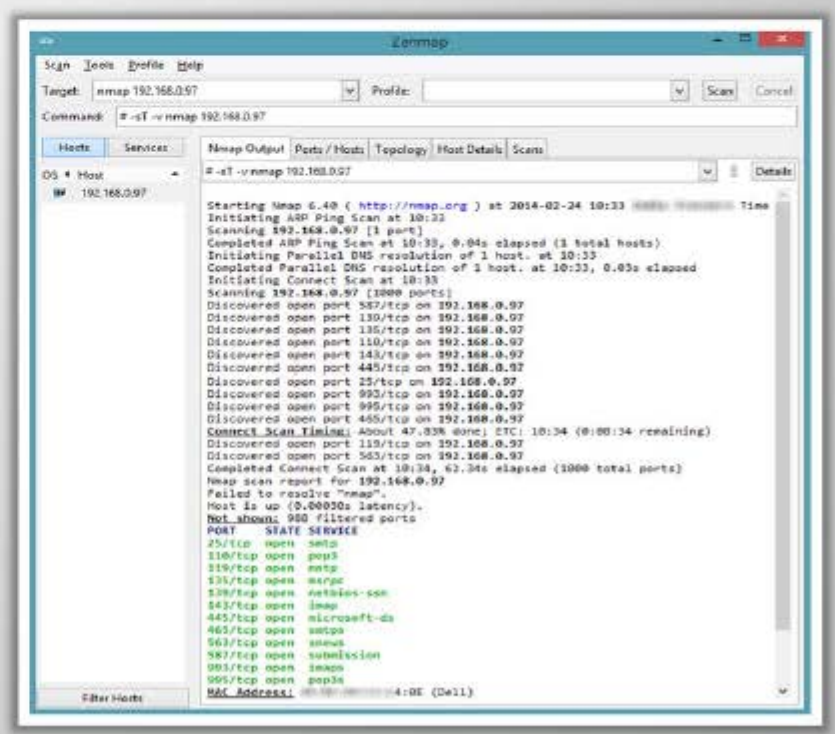
C|EH Certified Ethical Hacker

01 TCP Connect scan detects when a port is open by completing the **three-way handshake**

02 TCP Connect scan **establishes a full connection** and tears it down by sending a **RST packet**

03 It does not require **super user privileges**



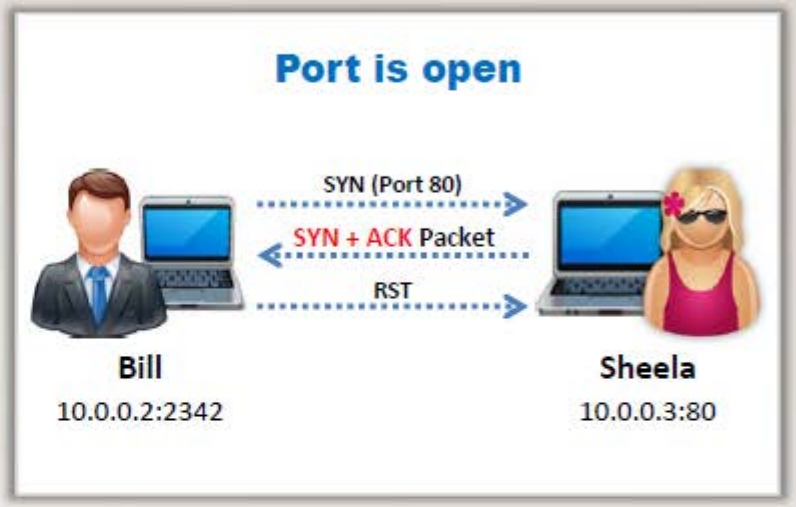


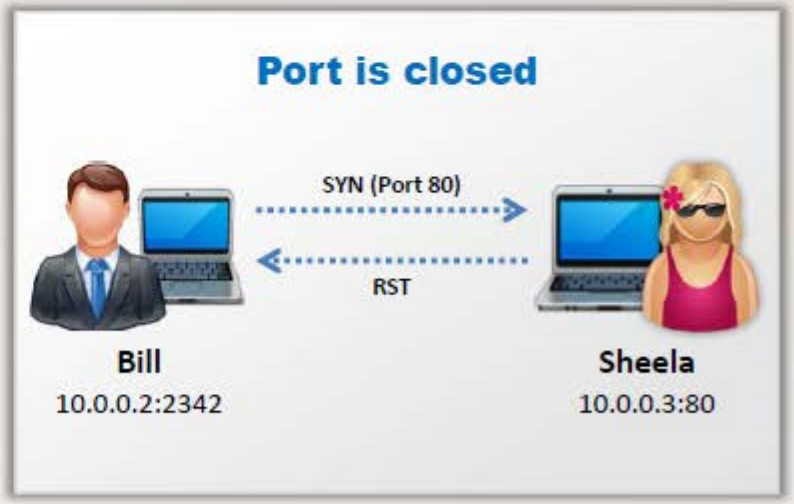
Stealth Scan (Half-open Scan)

- Stealth scan involves resetting the TCP connection between client and server abruptly before completion of **three-way handshake signals** making the connection half open
- Attackers use stealth scanning techniques to **bypass firewall rules**, **logging mechanism**, and hide themselves as usual network traffic

Stealth Scan Process

The client sends a single **SYN** packet to the server on the appropriate port	01
If the port is open then the server responds with a **SYN/ACK** packet	02
If the server responds with an **RST** packet, then the remote port is in the "closed" state	03
The client sends the **RST** packet to close the initiation before a connection can ever be established	04





Inverse TCP Flag Scanning

C|EH Certified Ethical Hacker

01 Attackers send TCP probe packets with a TCP flag (FIN, URG, PSH) set or with no flags, no response means port is open and RST means the port is closed

02 Port is open

Probe Packet (FIN/URG/PSH/NULL)

No Response

03 Port is closed

Probe Packet (FIN/URG/PSH/NULL)

RST/ACK

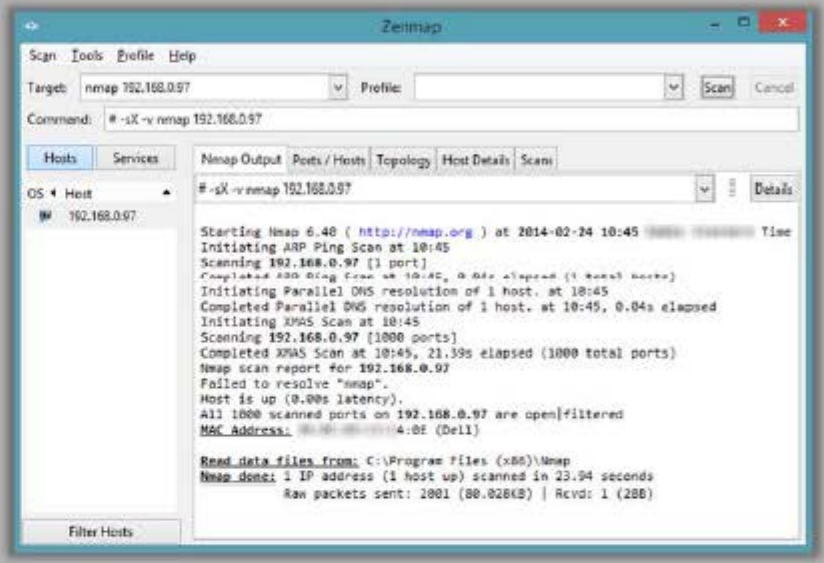
Note: Inverse TCP flag scanning is known as FIN, URG, PSH scanning based on the flag set in the probe packet. It is known as null scanning if there is no flag set

Xmas Scan

In Xmas scan, attackers send a TCP frame to a remote device with **FIN**, **URG**, and **PUSH** flags set

FIN scan works only with OSes with **RFC 793-based** TCP/IP implementation

It will not work against any current version of **Microsoft Windows**



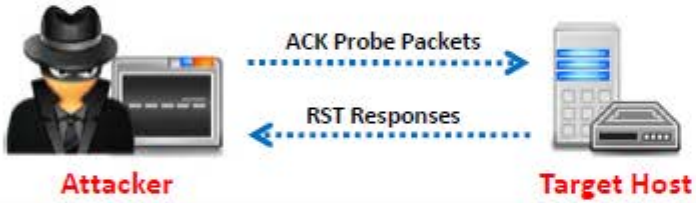
Port is open

Port is closed

ACK Flag Probe Scanning

- Attackers send **TCP probe packets with ACK flag** set to a remote device and then **analyzes the header information** (TTL and WINDOW field) of received RST packets to find whether the **port is open or closed**

TTL based ACK flag probe scanning




```
1: host 10.2.2.11 port 20: F:RST -> ttl: 80 win: 0
2: host 10.2.2.11 port 21: F:RST -> ttl: 80 win: 0
3: host 10.2.2.11 port 22: F:RST -> ttl: 50 win: 0
4: host 10.2.2.11 port 23: F:RST -> ttl: 80 win: 0
```

If the **TTL value of RST packet** on particular port is less than the boundary value of **64**, then that **port is open**

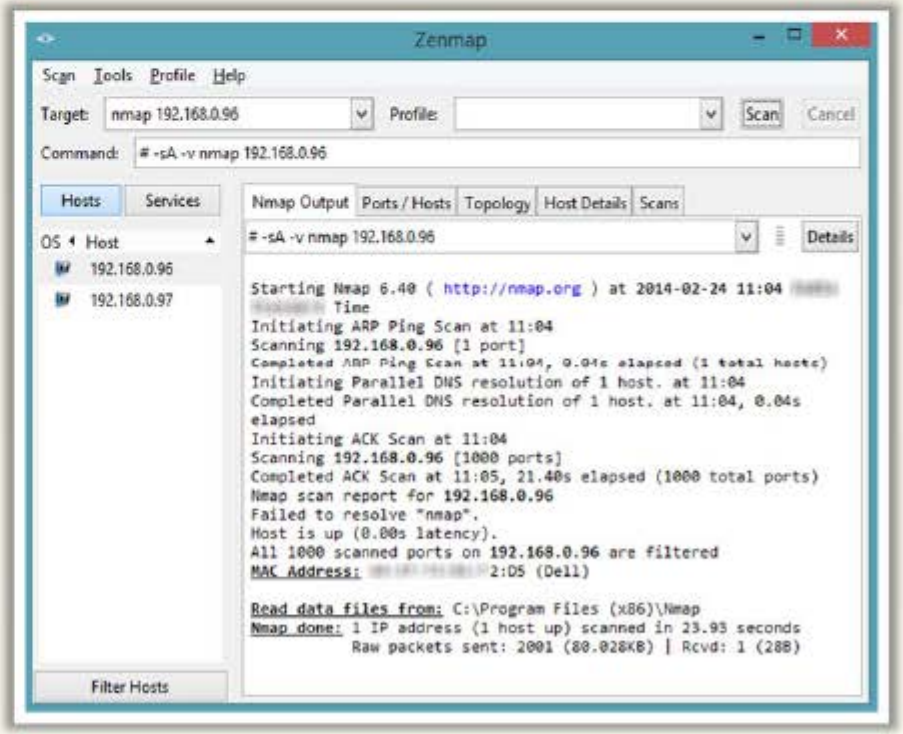
WINDOW based ACK flag probe scanning


```
1: host 10.2.2.12 port 20: F:RST -> ttl: 64 win: 0
2: host 10.2.2.12 port 21: F:RST -> ttl: 64 win: 0
3: host 10.2.2.12 port 22: F:RST -> ttl: 64 win: 512
4: host 10.2.2.12 port 23: F:RST -> ttl: 64 win: 0
```

If the **WINDOW value of RST packet** on particular port has **non zero value**, then that **port is open**

ACK Flag Probe Scanning (Cont'd)

- ACK flag probe scanning can also be used to **check the filtering system of target**
- Attackers send an **ACK probe packet** with random sequence number, no response means **port is filtered** (stateful firewall is present) and RST response means the **port is not filtered**



IDLE/IPID Header Scan

C|EH Certified Ethical Hacker

01 Most network servers listen on TCP ports, such as **web servers on port 80** and **mail servers on port 25**. Port is considered "open" if an application is listening on the port

02 One way to determine whether a port is open is to **send a "SYN"** (session establishment) packet to the port

03 The target machine will send back a **"SYN|ACK"** (session request acknowledgment) packet if the port is open, and an **"RST" (Reset) packet** if the port is closed

04 A machine that receives an **unsolicited SYN|ACK packet** will respond with an RST. An unsolicited RST will be ignored

05 Every IP packet on the Internet has a **"fragment identification" number** (IPID)

06 OS increments the IPID for each packet sent, thus probing an IPID gives an attacker the **number of packets sent** since last probe

IDLE Scan: Step 1

C|EH Certified Ethical Hacker

Send SYN + ACK packet to the zombie machine to probe its IPID number

Every IP packet on the Internet has a fragment identification number (IPID), which increases every time a host sends IP packet

Zombie not expecting a SYN + ACK packet will send RST packet, disclosing the IPID

Analyze the RST packet from zombie machine to extract IPID

Attacker

IPID Probe SYN + ACK Packet

Response: IPID=31337

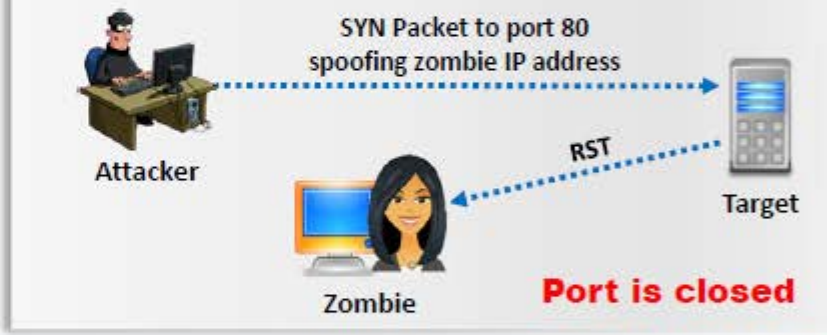
RST Packet

Zombie

IDLE Scan: Step 2 and 3

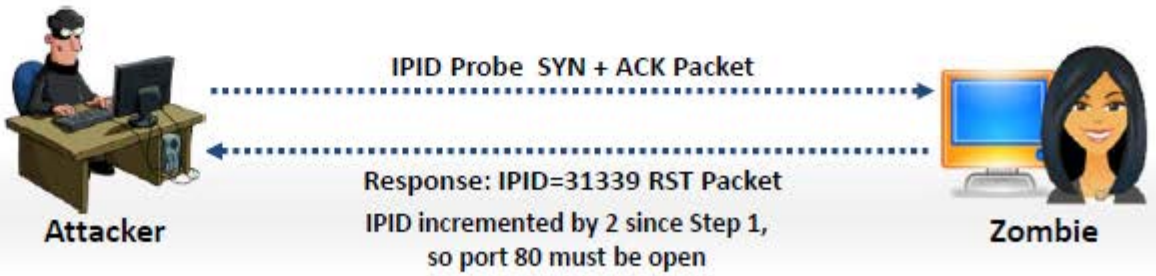
Step 2

- Send SYN packet to the **target machine (port 80)** spoofing the IP address of the "zombie"
- If the port is open, the target will send **SYN+ACK Packet** to the zombie and in response zombie sends RST to the target
- If the port is closed, the target will send **RST to the "zombie"** but zombie will not send anything back



Step 3

- Probe "zombie" IPID again



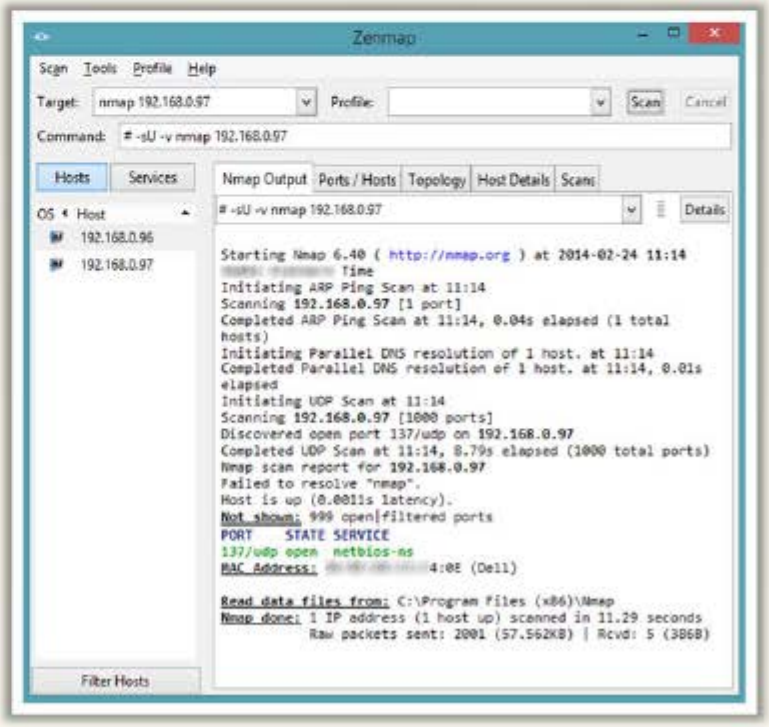
UDP Scanning

UDP Port Open

- There is no three-way TCP handshake for UDP scan
- The system does not respond with a message when the port is open

UDP Port Closed

- If a UDP packet is sent to closed port, the system responds with ICMP port unreachable message
- Spywares, Trojan horses, and other malicious applications use UDP ports



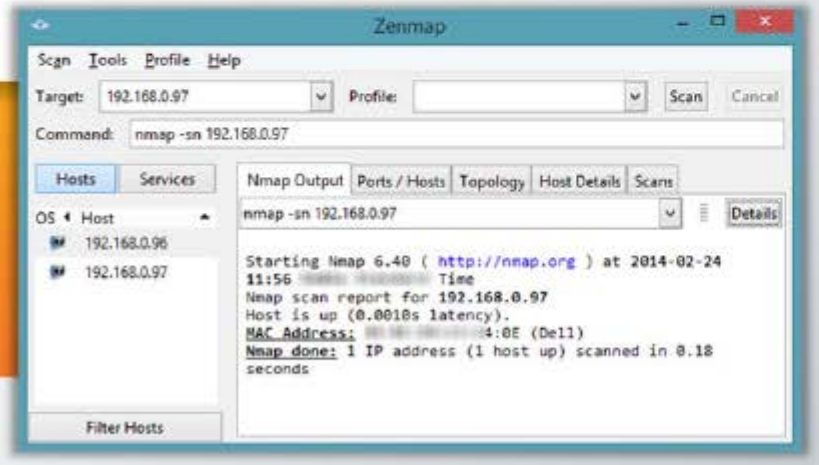
ICMP Echo Scanning/List Scan

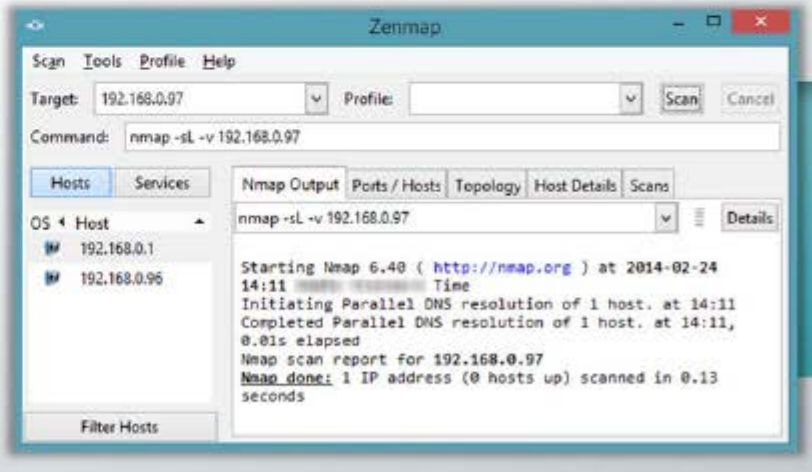
ICMP Echo Scanning

- This is not really port scanning, since **ICMP** does not have a port abstraction
- But it is sometimes useful to determine which hosts in a network are up by **pinging** them all
- `nmap -P cert.org/24 152.148.0.0/16`

List Scan

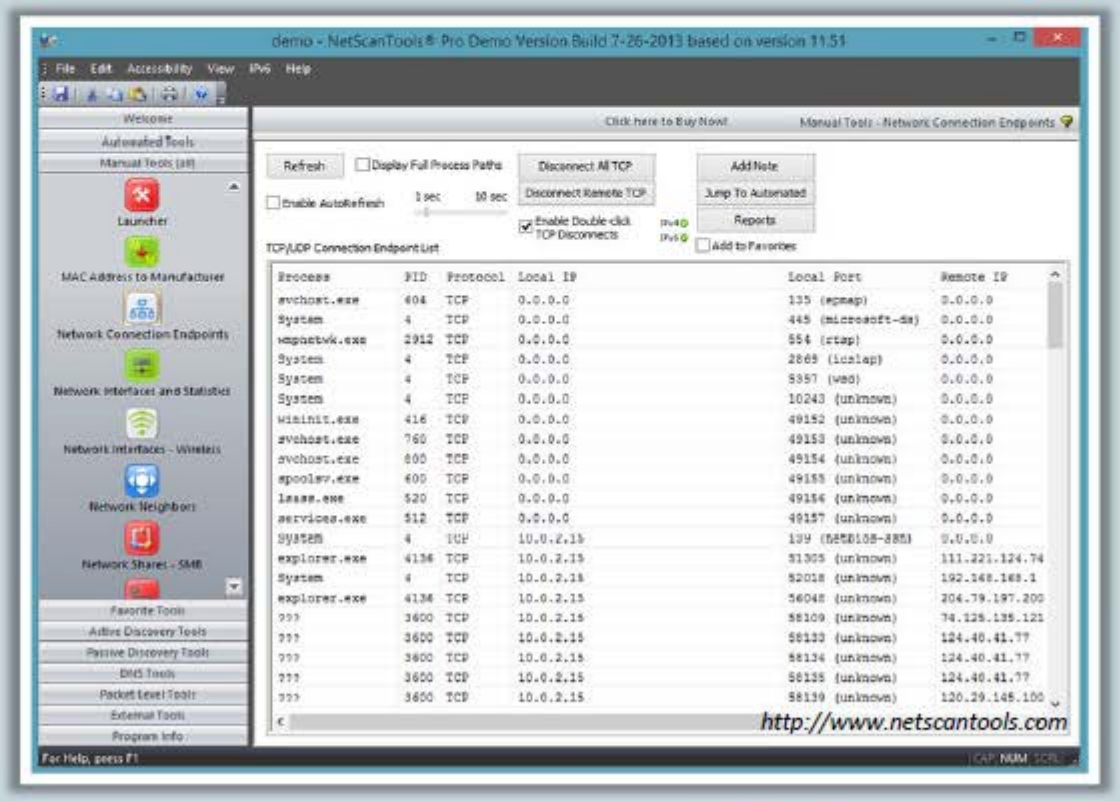
- This type of scan simply generates and prints a **list of IPs/Names** without actually pinging them
- A **reverse DNS resolution** is carried out to identify the host names





Scanning Tool: NetScan Tools Pro

- Network Tools Pro assists in **troubleshooting**, **diagnosing**, **monitoring** and **discovering** devices on the network
- It lists **IPv4/IPv6** addresses, hostnames, **domain names**, email addresses, and URLs automatically or with manual tools



Scanning Tools

SuperScan
http://www.mcafee.com

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

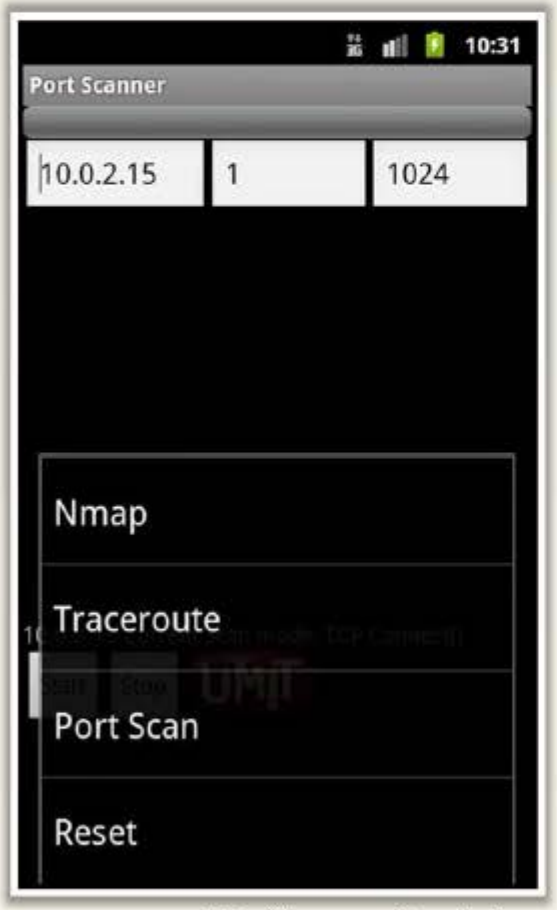
Advanced Port Scanner
http://www.radmin.com

CurrPorts
http://www.nirsoft.net

Scanning Tools for Mobile

C|EH Certified Ethical Hacker

Umit Network Scanner



http://www.umitproject.org

Fing

http://www.overlooksoft.com

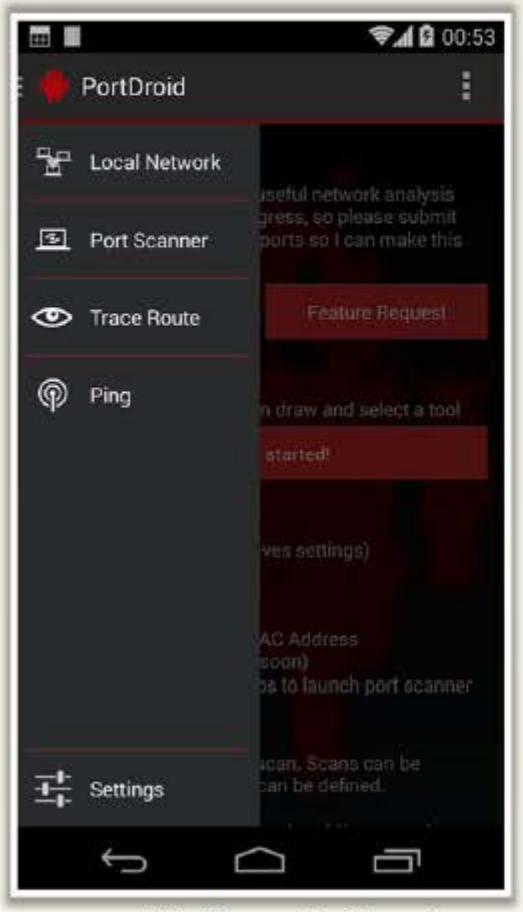
IP Network Scanner

http://10base-t.com

Scanning Tools for Mobile (Cont'd)

C|EH Certified Ethical Hacker

PortDroid Network Analysis



http://www.stealthcopter.com

Pamn IP Scanner

http://pips.wjholden.com

Network Discovery

http://rorist.github.io

Port Scanning Countermeasures

C|EH Certified Ethical Hacker

01 Configure **firewall** and **IDS rules** to detect and block probes

02 Run the **port scanning tools** against hosts on the network to determine whether the firewall properly **detects the port scanning activity**

03 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

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

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

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

07 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**

08 Ensure that the **anti scanning** and **anti spoofing** rules are configured

CEH 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

IDS Evasion Techniques

C|EH Certified Ethical Hacker

01 Use fragmented IP packets

Spoof your IP address when launching attacks and sniff responses from server

02

03 Use source routing (if possible)

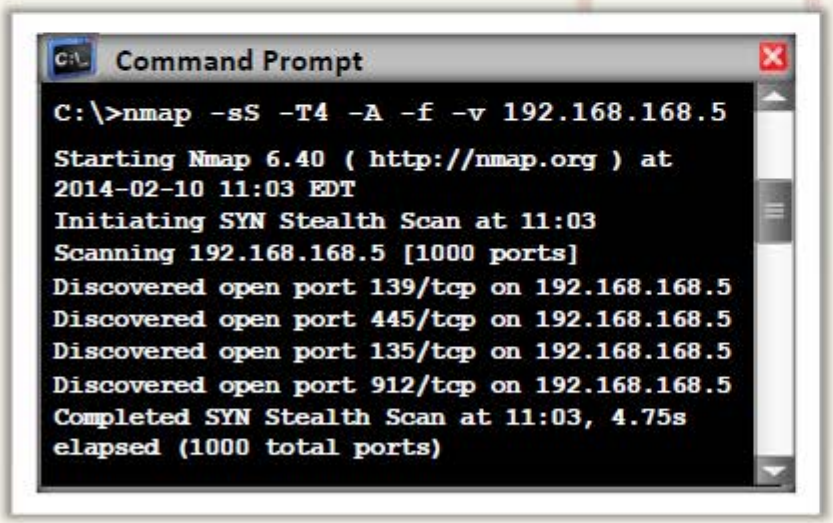
Connect to proxy servers or compromised trojaned machines to launch attacks

04

SYN/FIN Scanning Using IP Fragments

It is not a new scanning method but a **modification** of the earlier methods

The **TCP header** is split into several packets so that the packet filters are not able to detect what the packets intend to do



CEH 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

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

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**

Active Banner Grabbing

- **Specially crafted packets** are sent to remote OS and the responses are 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

Banner Grabbing Tools

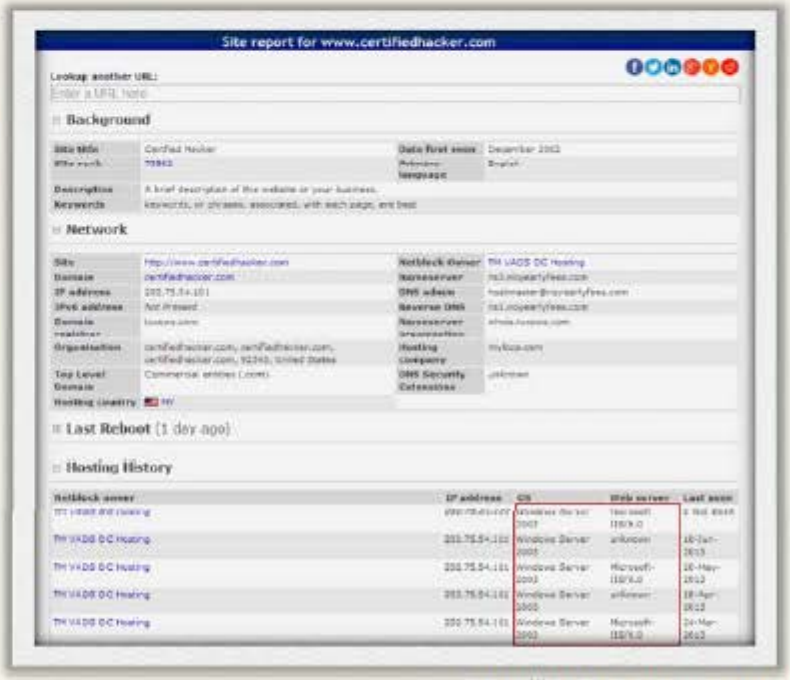
ID Serve

- 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.

http://www.grc.com

Netcraft

- 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



http://toolbar.netcraft.com

Banner Grabbing Tools (Cont'd)

Netcat

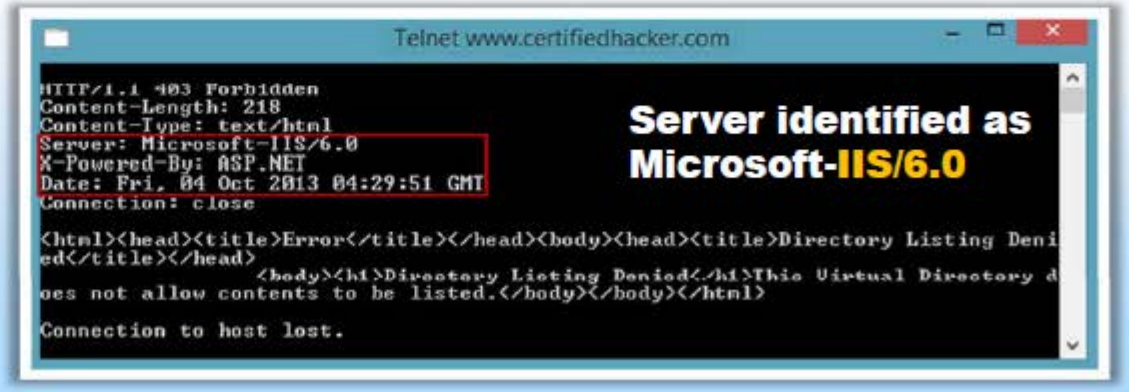
This utility **reads and writes data across network connections**, using the TCP/IP protocol

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

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



Banner Grabbing Countermeasures: Disabling or Changing Banner

Display **false banners** to misguide attackers

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

Use **ServerMask** (http://www.port80software.com) tools to disable or change banner information

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

Banner Grabbing Countermeasures: Hiding File Extensions from Web Pages

C|EH Certified Ethical Hacker

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

02 Hide file extensions to mask the web technology

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

04 Apache users can use mod_negotiation directives

05 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

CEH 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

Vulnerability Scanning

C|EH Certified Ethical Hacker

Network vulnerabilities

Open ports and running services

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

Application and services vulnerabilities

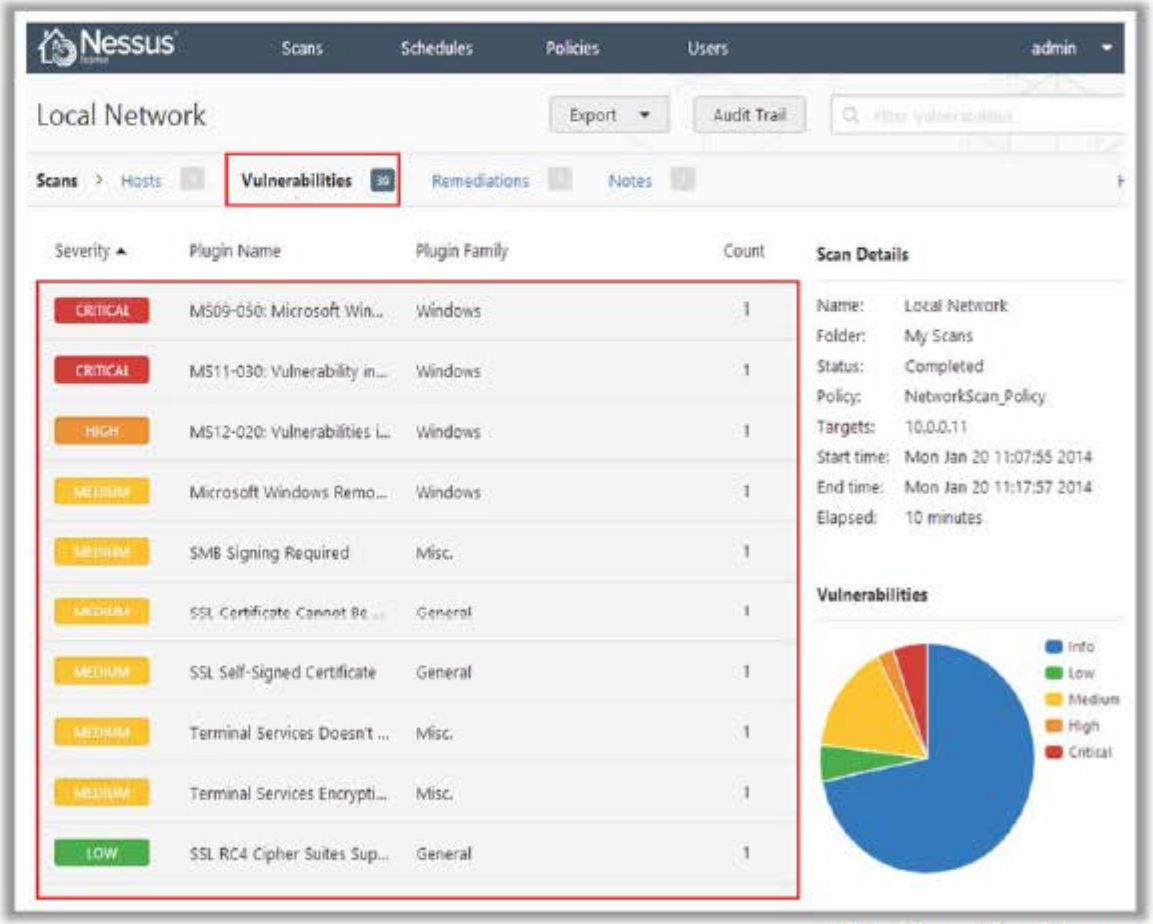
Application and services configuration errors

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

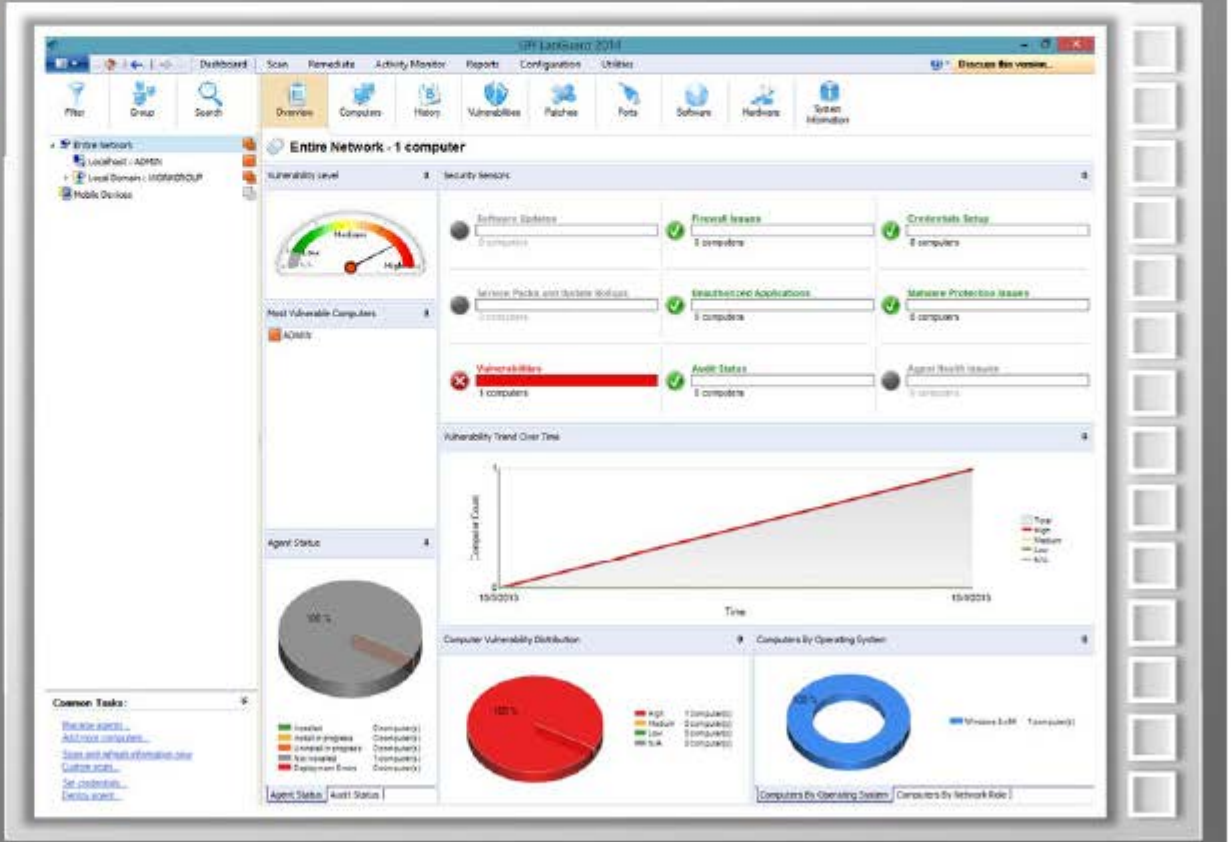
Vulnerability Scanning Tool: GFI LanGuard

GFI LanGuard assists in **asset inventory**, change management, **risk analysis**, and proving compliance

Features

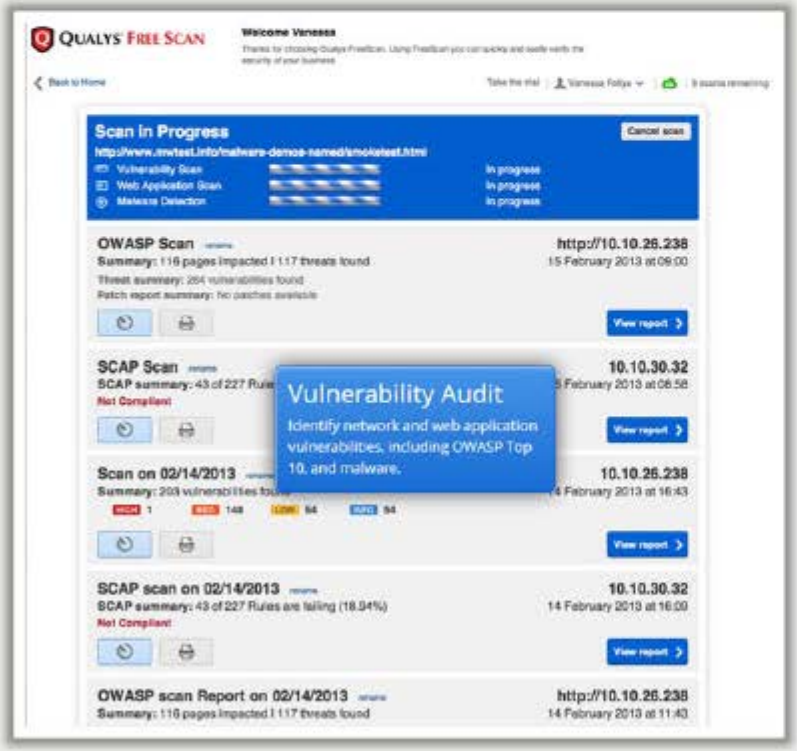
- Selectively creates **custom vulnerability checks**
- Identifies **security vulnerabilities** and takes remedial action
- Creates different types of **scans and vulnerability tests**
- Helps ensure third-party security applications offer **optimum protection**
- Performs **network device vulnerability checks**

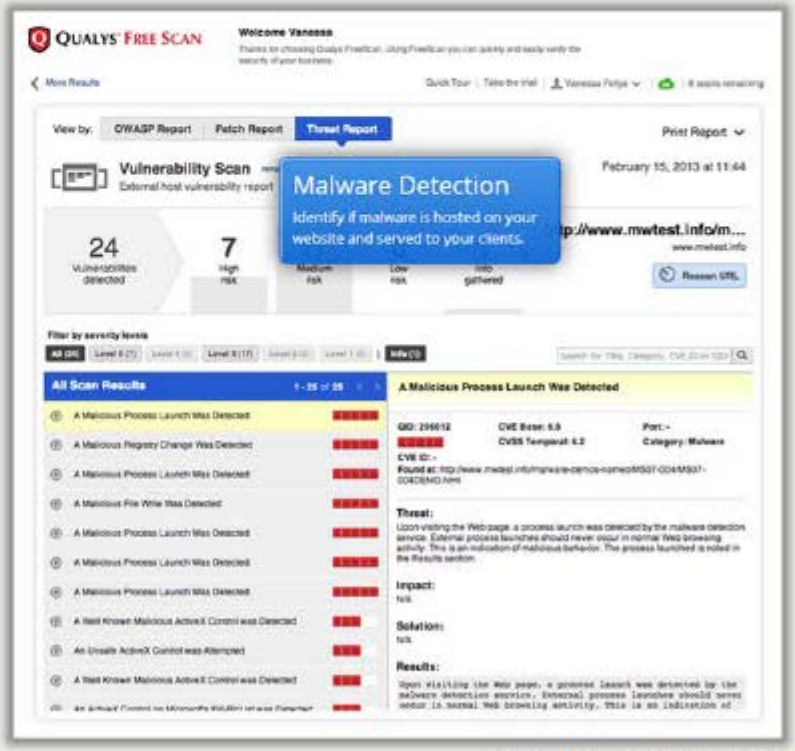
http://www.gfi.com



Vulnerability Scanning Tool: Qualys FreeScan

- **Scans computers and apps** on the Internet or in your network
- Tests websites and apps for **OWASP Top Risks and malware**





http://www.qualys.com

Network Vulnerability Scanners

C|EH Certified Ethical Hacker

Retina CS
http://www.beyondtrust.com

OpenVAS
http://www.openvas.org

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

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

MBSA
http://www.microsoft.com

Nexpose
http://www.rapid7.com

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

SAINT
http://www.saintcorporation.com

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

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

Vulnerability Scanning Tools for Mobile

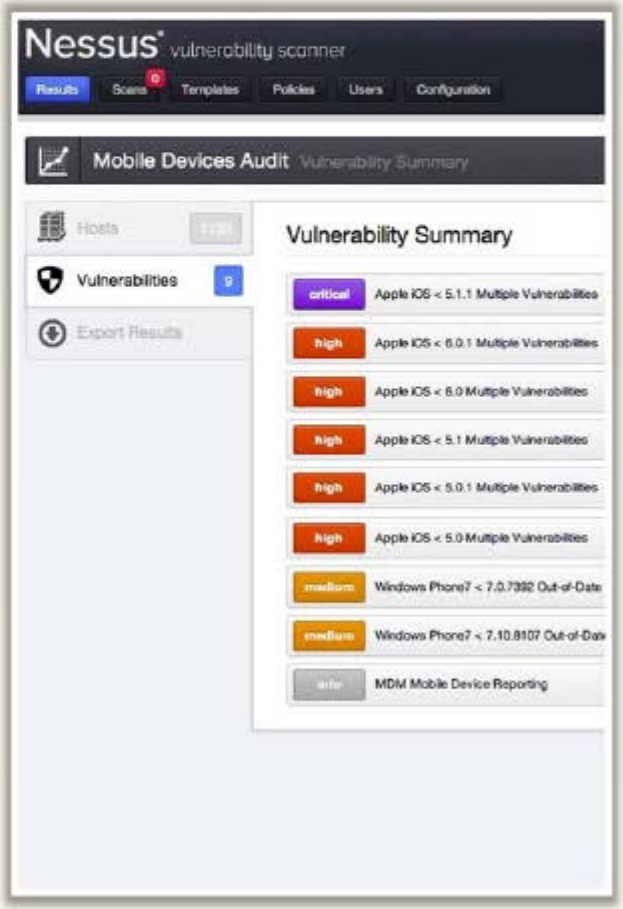
Retina CS for Mobile

http://www.beyondtrust.com

SecurityMetrics MobileScan

https://www.securitymetrics.com

Nessus Vulnerability Scanner



http://www.tenable.com

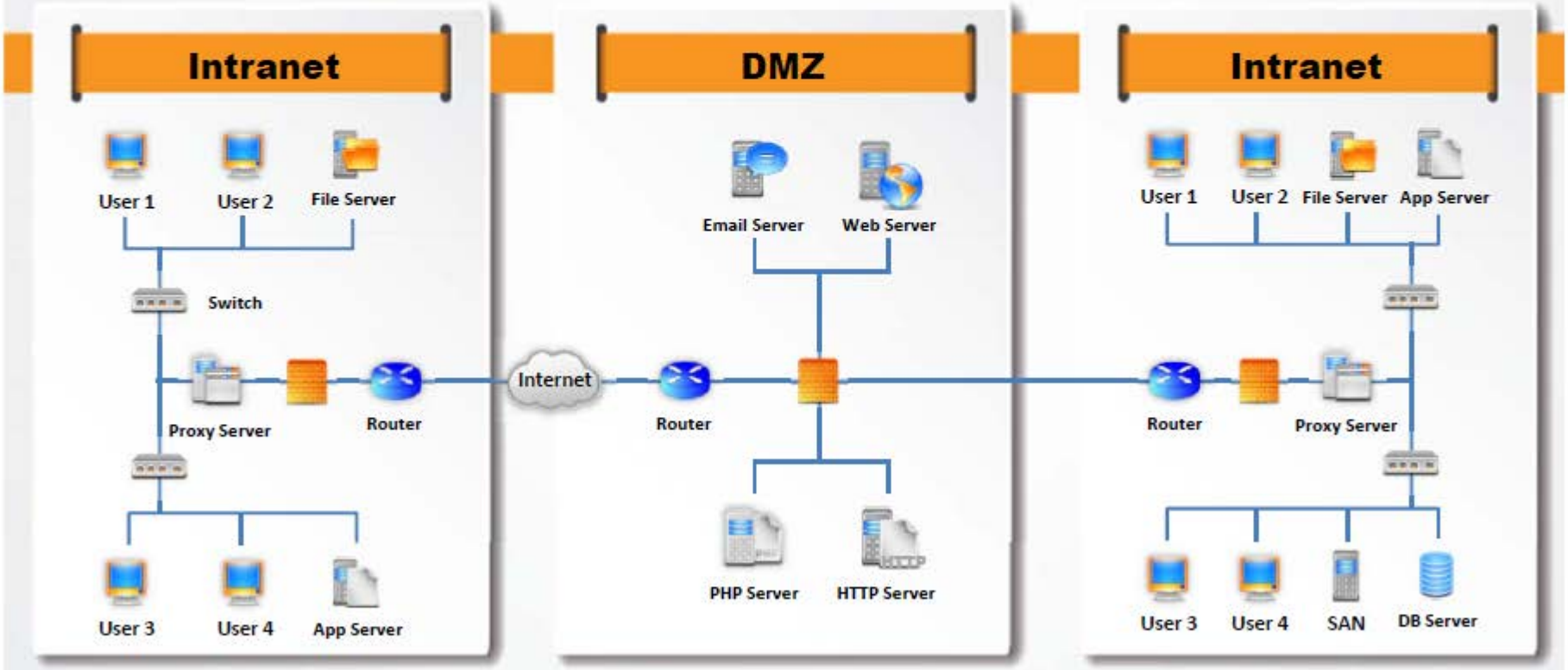
CEH Scanning Methodology

- 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

C|EH Certified Ethical Hacker

- 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

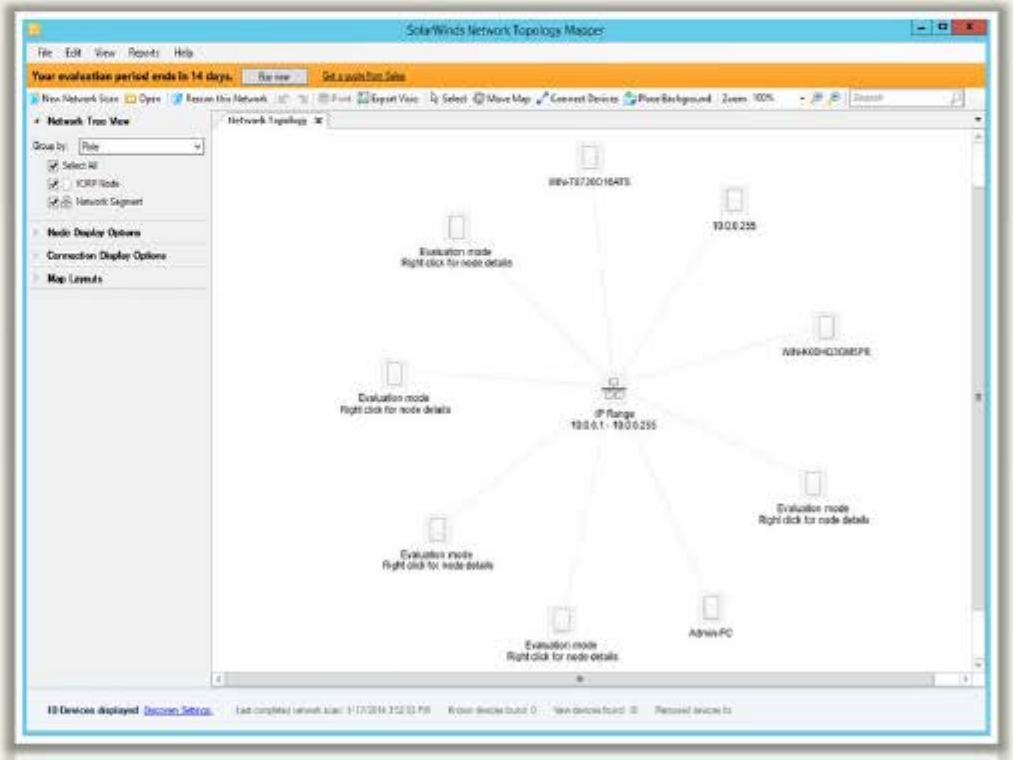


Network Discovery Tool: Network Topology Mapper

Features

- Network topology discovery and mapping
- Export network diagrams to Visio
- Network mapping for regulatory compliance
- Multi-level network discovery
- Auto-detect changes to network topology

Network Topology Mapper **discovers a network** and **produces a comprehensive network diagram**



http://www.solarwinds.com

Network Discovery Tools: OpManager and NetworkView

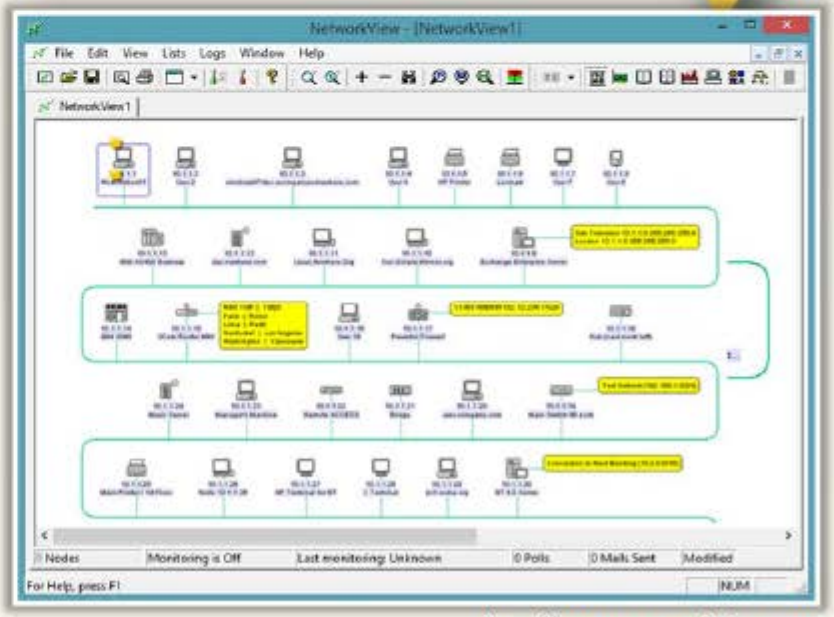
OpManager

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, etc.

http://www.manageengine.com

NetworkView

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



http://www.networkview.com

Network Discovery and Mapping Tools

The Dude
http://www.mikrotik.com

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

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

InterMapper
http://www.intermapper.com

Friendly Pinger
http://www.kilievich.com

NetMapper
http://www.opnet.com

Ipsonar
http://www.lumeta.com

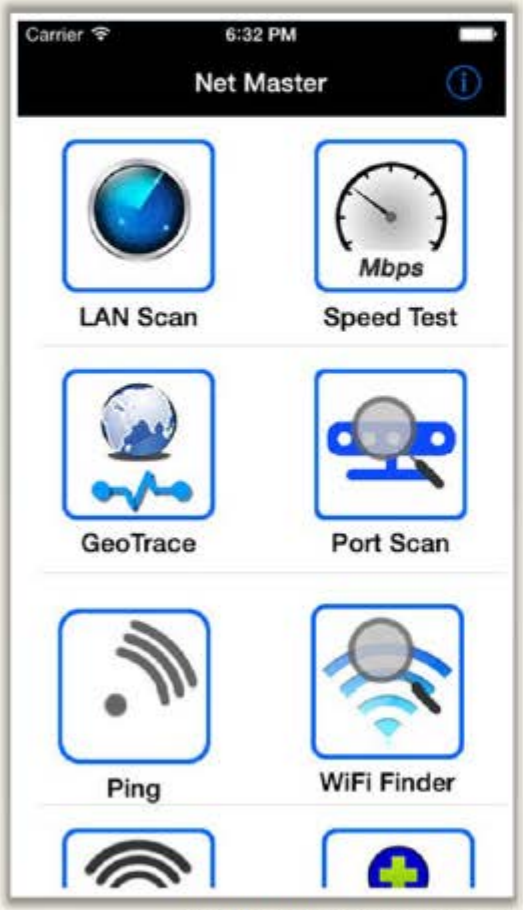
NetBrain Enterprise Suite
http://www.netbraintech.com

WhatsConnected
http://www.whatsupgold.com

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

Network Discovery Tools for Mobile

Net Master



http://www.nutecapps.com

Scany

http://happymagenta.com

Network "Swiss-Army-Knife"

http://foobang.weebly.com

CEH 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 server is an application that can **serve as an intermediary** for connecting with other computers

Why Attackers Use Proxy Servers?

- To hide the **source IP address** so that they can hack without any legal corollary
- To **mask the actual source** of the attack by impersonating a fake source address of the proxy
- To **remotely access intranets** and other **website resources** that are normally off limits
- To **interrupt all the requests** sent by a user and transmit them to a third destination, hence victims will only be able to identify the proxy server address
- Attackers chain **multiple proxy servers** to avoid detection

Proxy Chaining

C|EH Certified Ethical Hacker

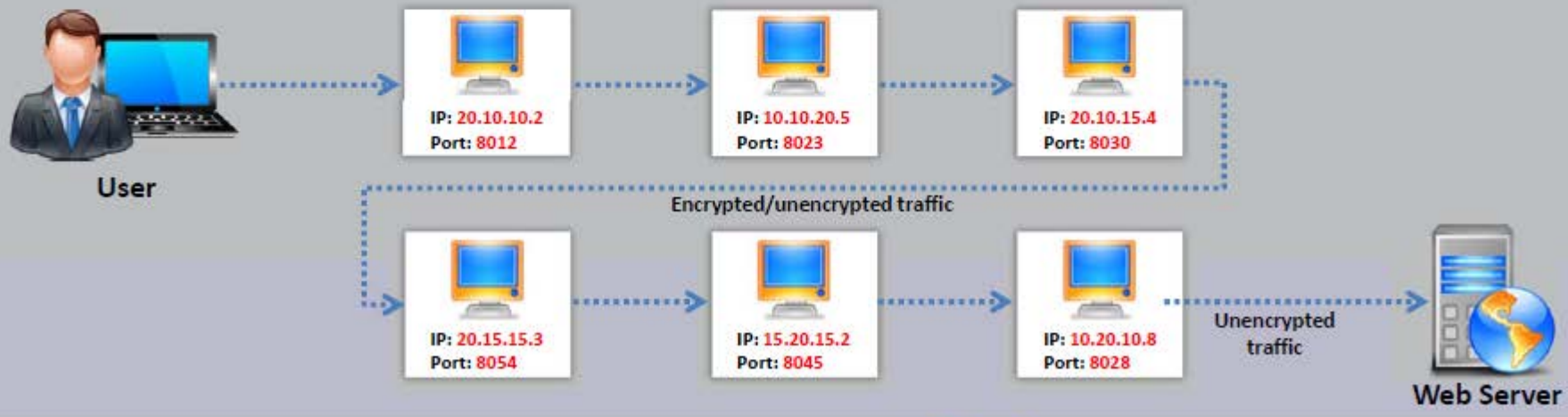
01 User requests a resource from the destination

02 Proxy client at the user's system connects to a proxy server and passes the request to proxy server

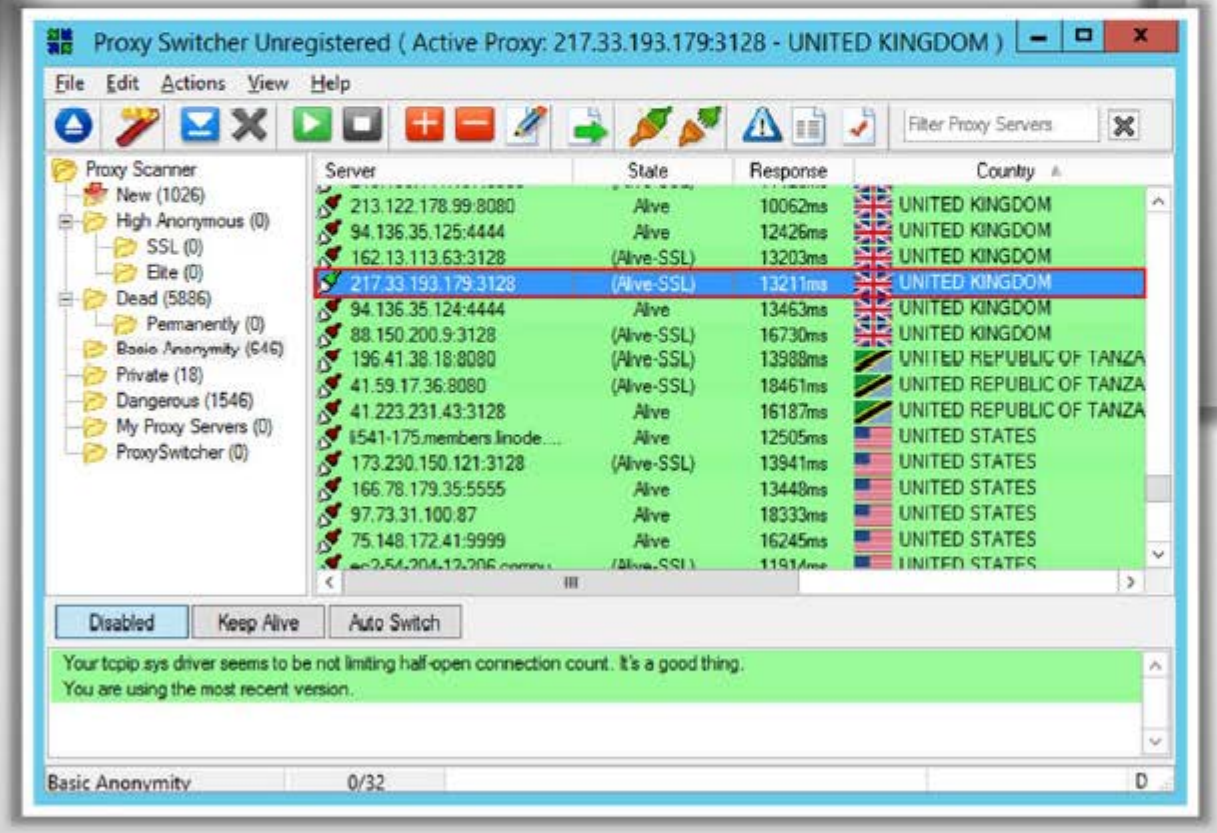
03 The proxy server strips the user's identification information and passes the request to next proxy server

04 This process is repeated by all the proxy servers in the chain

05 At the end unencrypted request is passed to the web server



Proxy Tool: Proxy Switcher

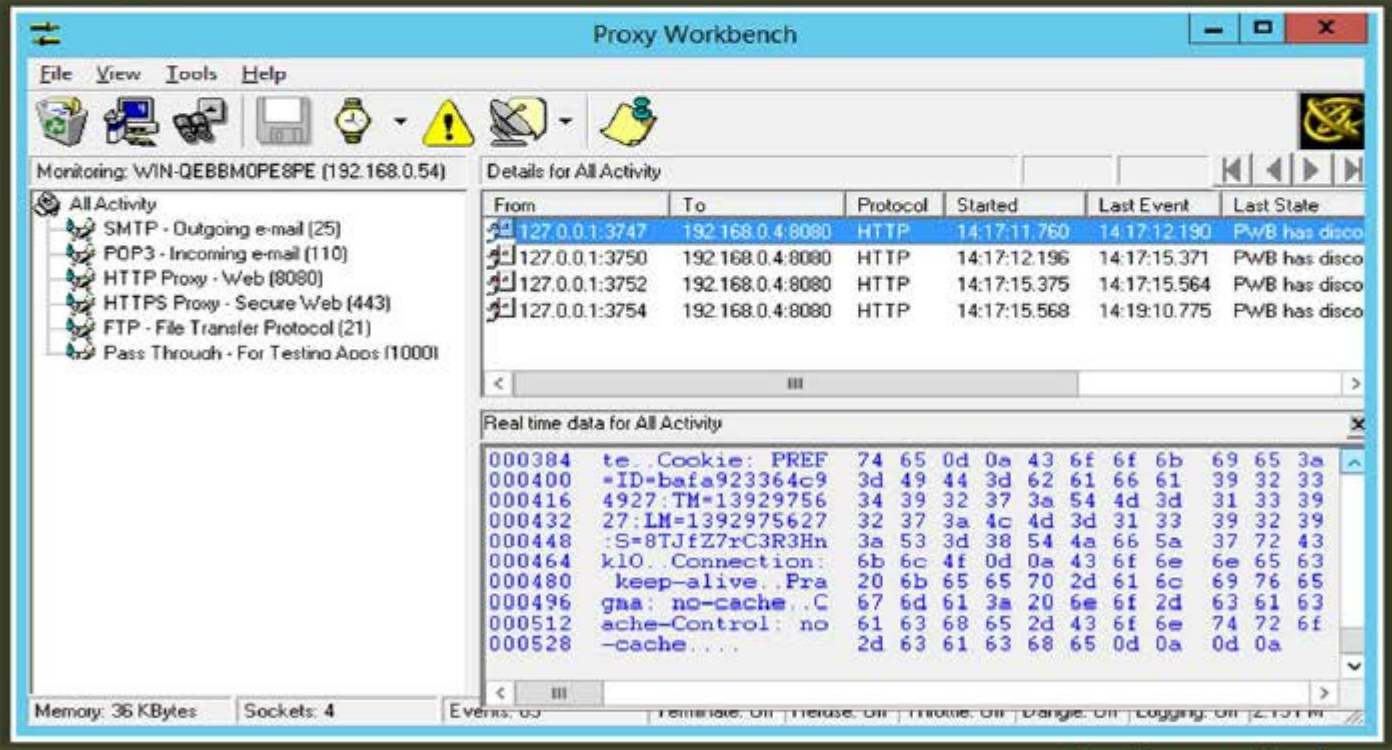


Proxy Switcher **hides your IP address** from the websites you visit

http://www.proxyswitcher.com

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 Tools: TOR and CyberGhost

Tor allows you to protect your **privacy** and defend yourself against **network surveillance** and **traffic analysis**

- **CyberGhost** allows you to protect your **online privacy**, **surf anonymously**, and access **blocked** or **censored** content
- It hides your IP and replaces it with one of your choice, allowing you to surf anonymously

https://www.torproject.org

http://www.cyberghostvpn.com

Proxy Tools

SocksChain
http://ufasoft.com

Fiddler
http://www.telerik.com

Burp Suite
http://www.portswigger.net

Proxy
http://www.analogx.com

Proxifier
https://www.proxifier.com

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

Proxy Tool Windows App
http://webproxylist.com

ProxyCap
http://www.proxycap.com

Charles
http://www.charlesproxy.com

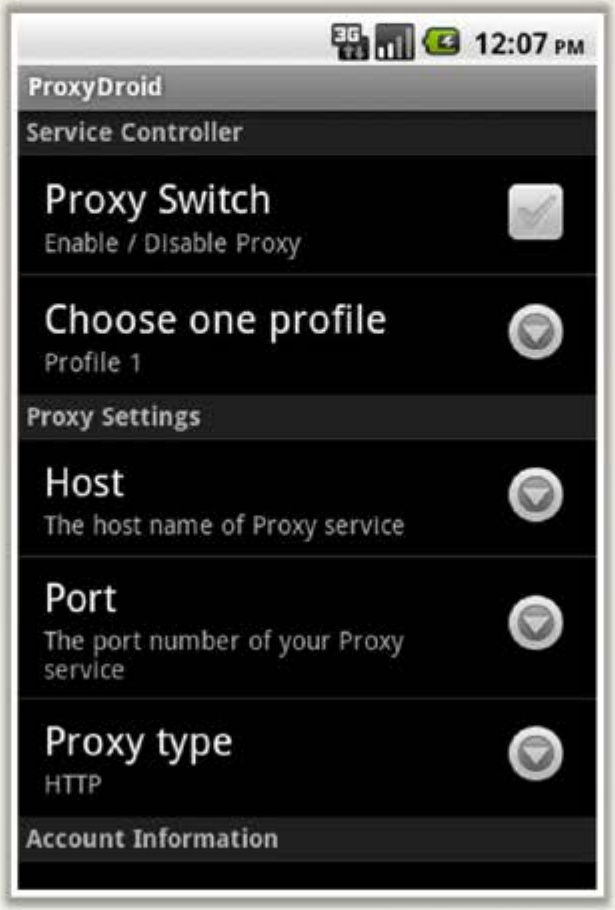
CCProxy
http://www.youngzsoft.net

Proxy Tools for Mobile

Proxy Browser for Android

https://play.google.com

ProxyDroid

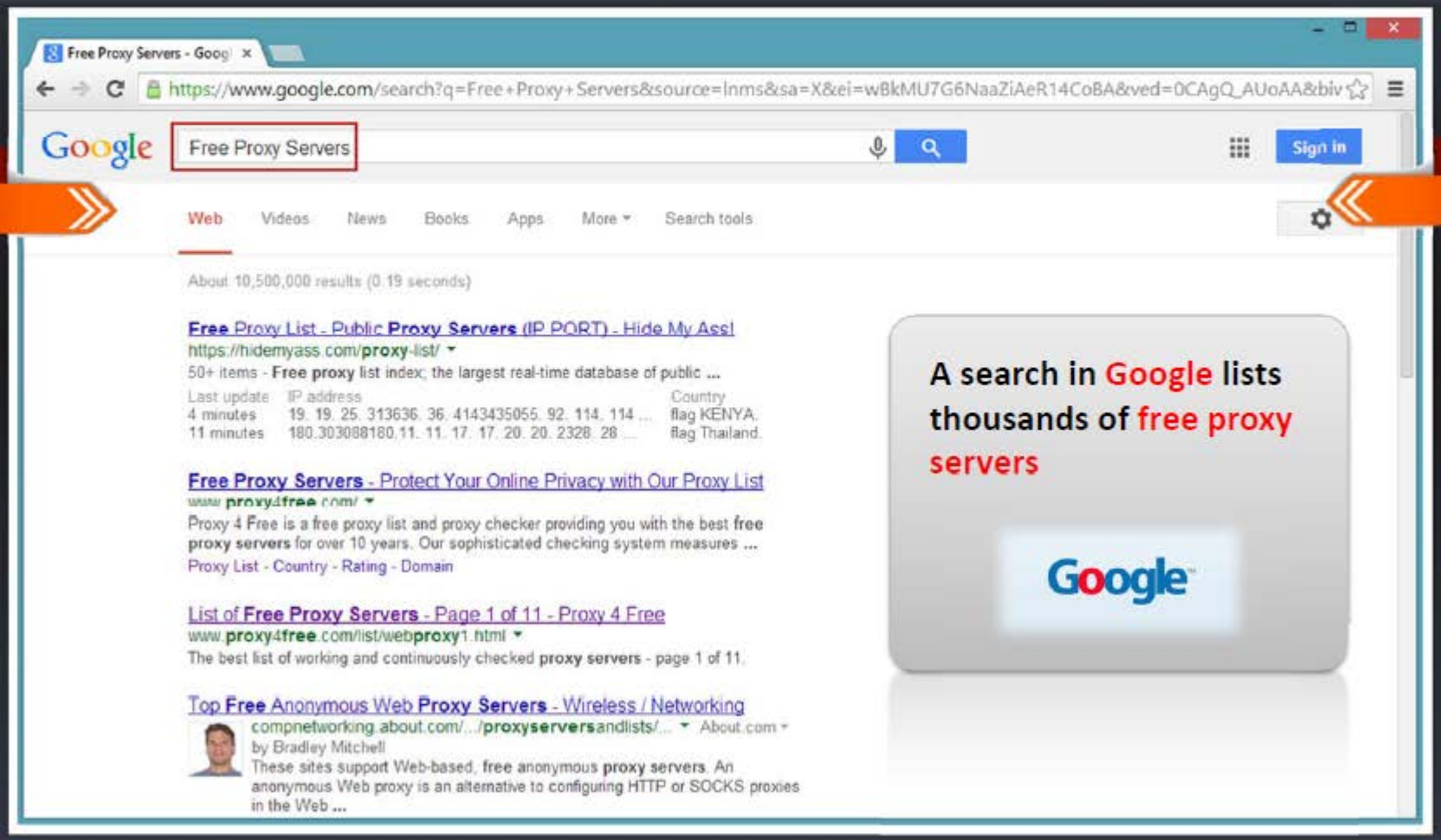


https://github.com

NetShade

http://www.raynersw.com

Free Proxy Servers



Introduction to Anonymizers

C|EH Certified Ethical Hacker

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

Anonymizers allow you to bypass Internet censors

Why use Anonymizer?

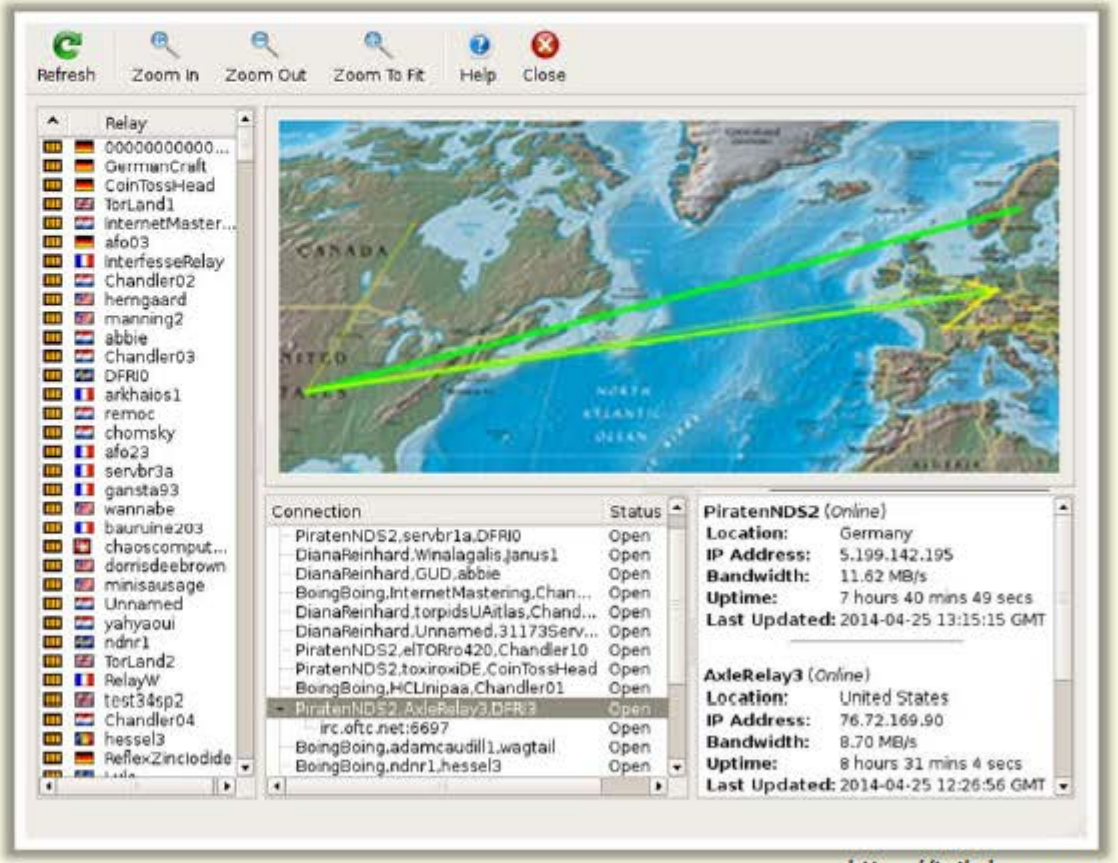
- Privacy and anonymity
- Protects from online attacks
- Access restricted content
- Bypass IDS and Firewall rules

Censorship Circumvention Tool: Tails

Tails is a **live operating system**, that user can start on any computer from a DVD, USB stick, or SD card

It aims at preserving privacy and anonymity and helps you to:

- Use the **Internet anonymously and circumvent censorship**
- **Leave no trace** on the computer
- Use **state-of-the-art cryptographic tools** to encrypt files, emails and instant messaging

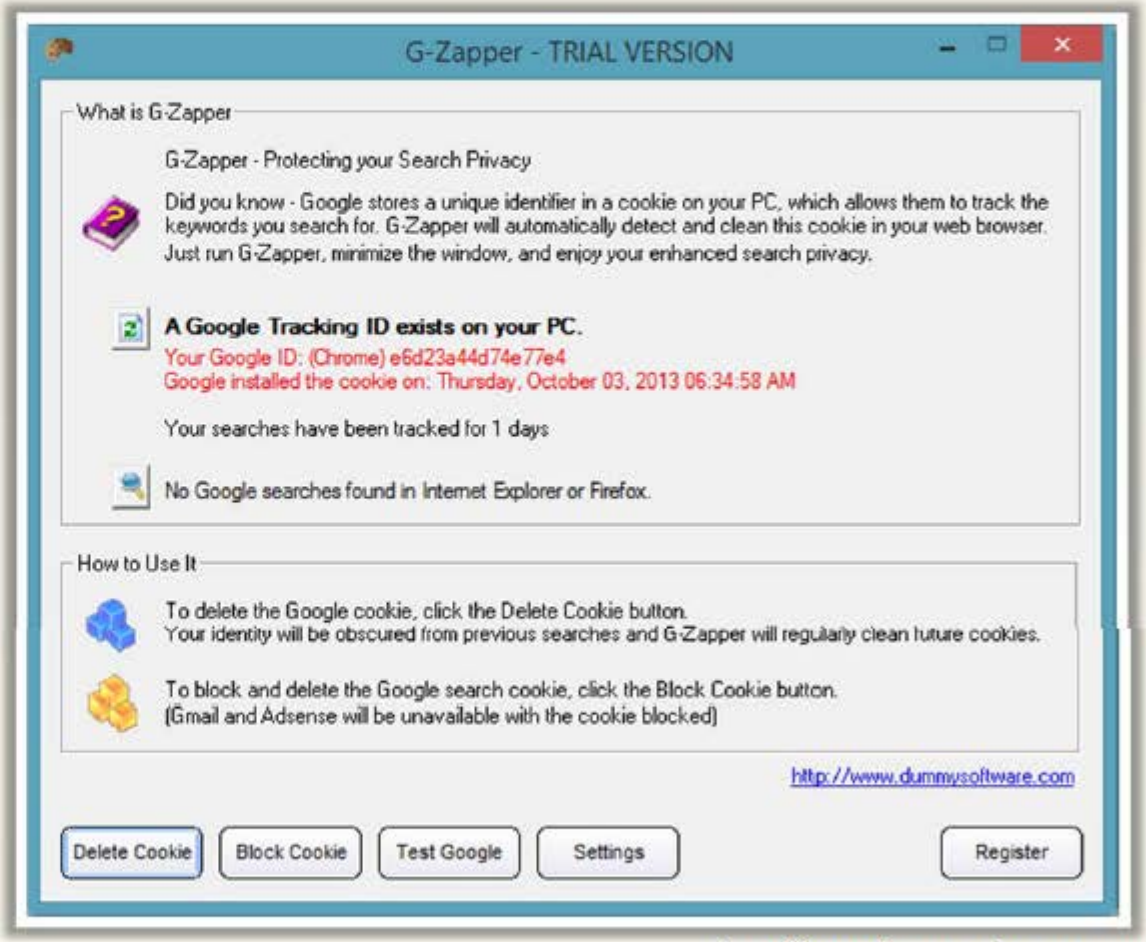


https://tails.boum.org

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



http://www.dummysoftware.com

Anonymizers

Proxify
http://proxify.com

Psiphon
http://psiphon.ca

Anonymous Web Surfing Tool
http://www.anonymous-surfing.com

Hide Your IP Address
http://www.hideyouripaddress.net

Anonymizer Universal
http://www.anonymizer.com

Guardster
http://www.guardster.com

Spotflux
http://www.spotflux.com

Ultrasurf
https://ultrasurf.us

Head Proxy
http://www.headproxy.com

Hope Proxy
http://www.hopeproxy.com

Anonymizers for Mobile

C|EH Certified Ethical Hacker

Orbot

https://guardianproject.info

Psiphon

https://s3.amazonaws.com

OpenDoor

https://itunes.apple.com

Spoofing IP Address

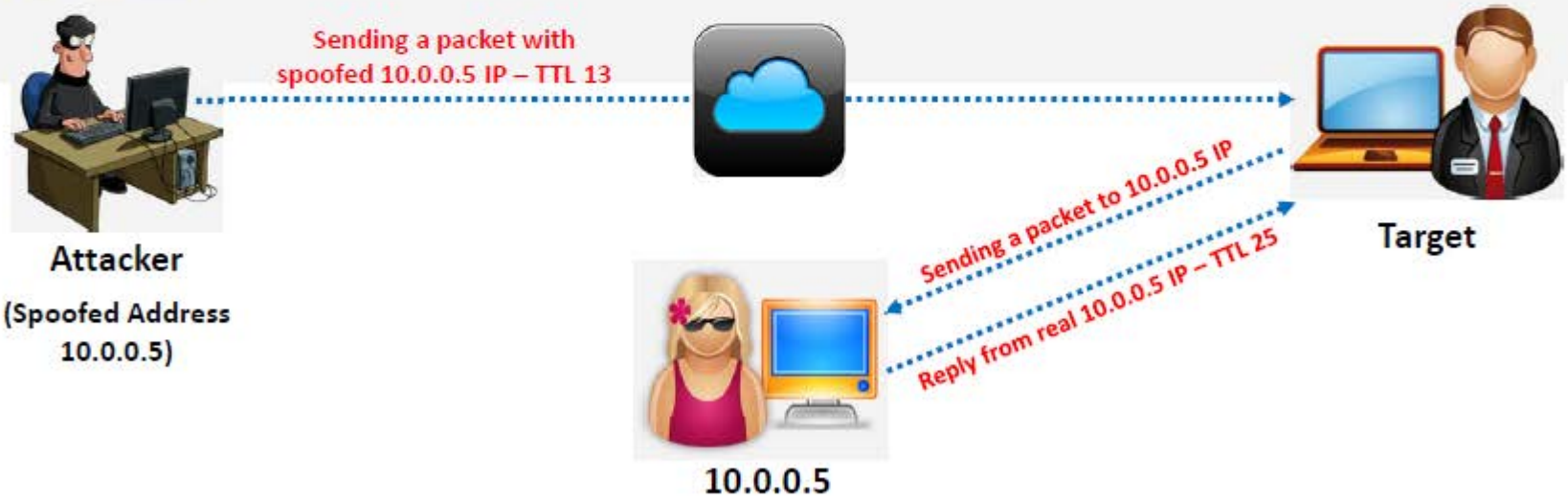
- IP spoofing refers to **changing source IP addresses** so that the attack **appears to be come from someone else**
- When the victim replies to the address, it goes back to the **spoofed address** and not to the **attacker's real address**

You will not be able to complete the three-way handshake and open a successful TCP connection with spoofed IP addresses

IP Spoofing Detection Techniques: Direct TTL Probes

01 Send packet to host of suspect spoofed packet that triggers reply and compare TTL with suspect packet; if the **TTL in the reply is not the same** as the packet being checked, it is a spoofed packet

02 This technique is successful when attacker is in a **different subnet** from victim



Note: Normal traffic from one host can vary TTLs depending on traffic patterns

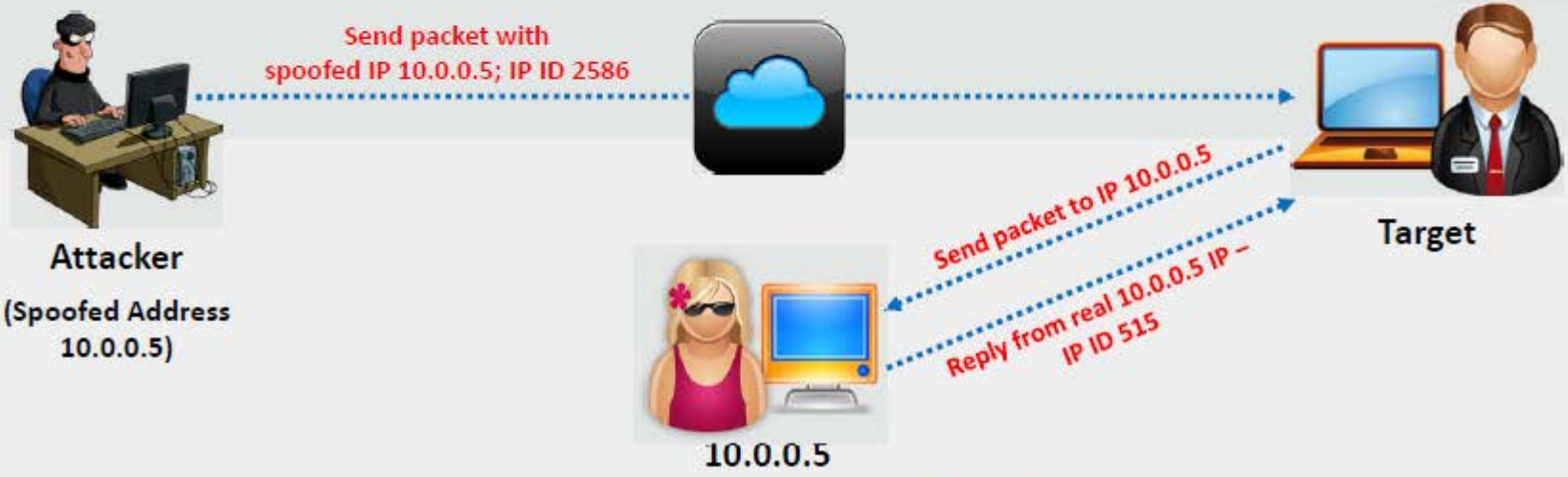
IP Spoofing Detection Techniques: IP Identification Number

C|EH Certified Ethical Hacker

01 Send probe to host of suspect spoofed traffic that triggers reply and **compare IP ID** with suspect traffic

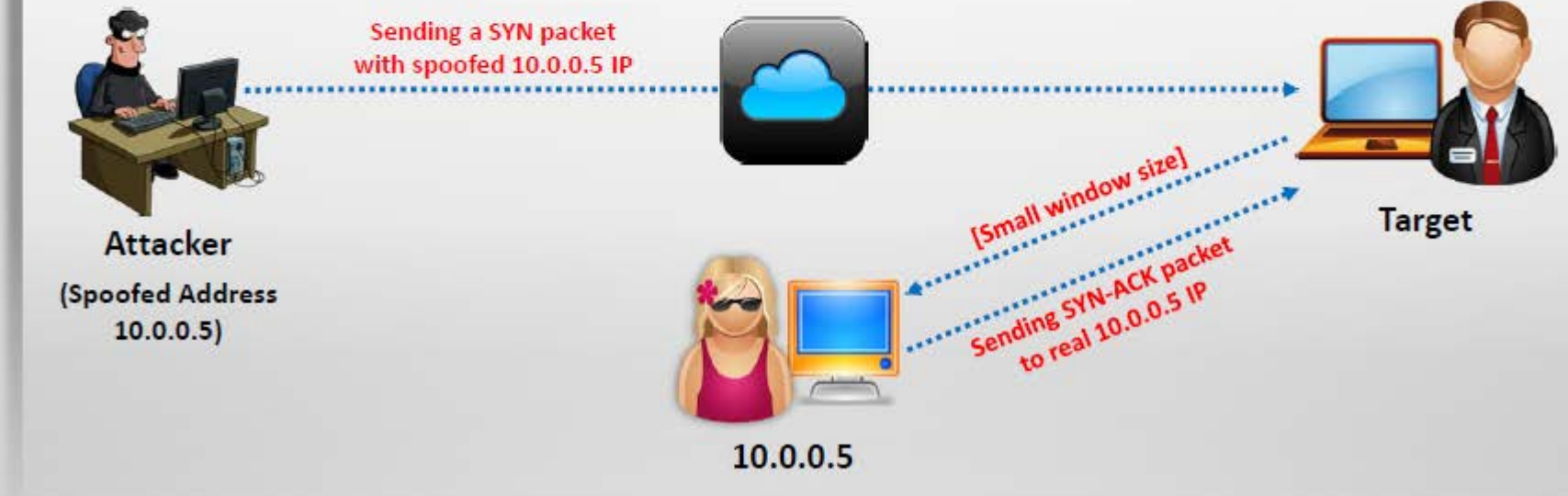
02 If IP IDs are **not in the near value** of packet being checked, suspect traffic is spoofed

03 This technique is successful even if the attacker is in the **same subnet**



IP Spoofing Detection Techniques: TCP Flow Control Method

- Attackers sending spoofed TCP packets, will not receive the **target's SYN-ACK packets**
- Attackers cannot therefore be responsive to change in the congestion window size
- When received traffic continues after a window size is exhausted, most probably the **packets are spoofed**



IP Spoofing Countermeasures

C|EH Certified Ethical Hacker

Encrypt all network traffic using cryptographic network protocols such as IPsec, TLS, SSH, and HTTPS

Use random initial sequence number to prevent IP spoofing attacks based on sequence number spoofing

Use multiple firewalls providing multi-layered depth of protection

Ingress Filtering: Use routers and firewalls at your network perimeter to filter incoming packets that appear to come from an internal IP address

Do not rely on **IP-based authentication**

Egress Filtering: Filter all outgoing packets with an invalid local IP address as source address

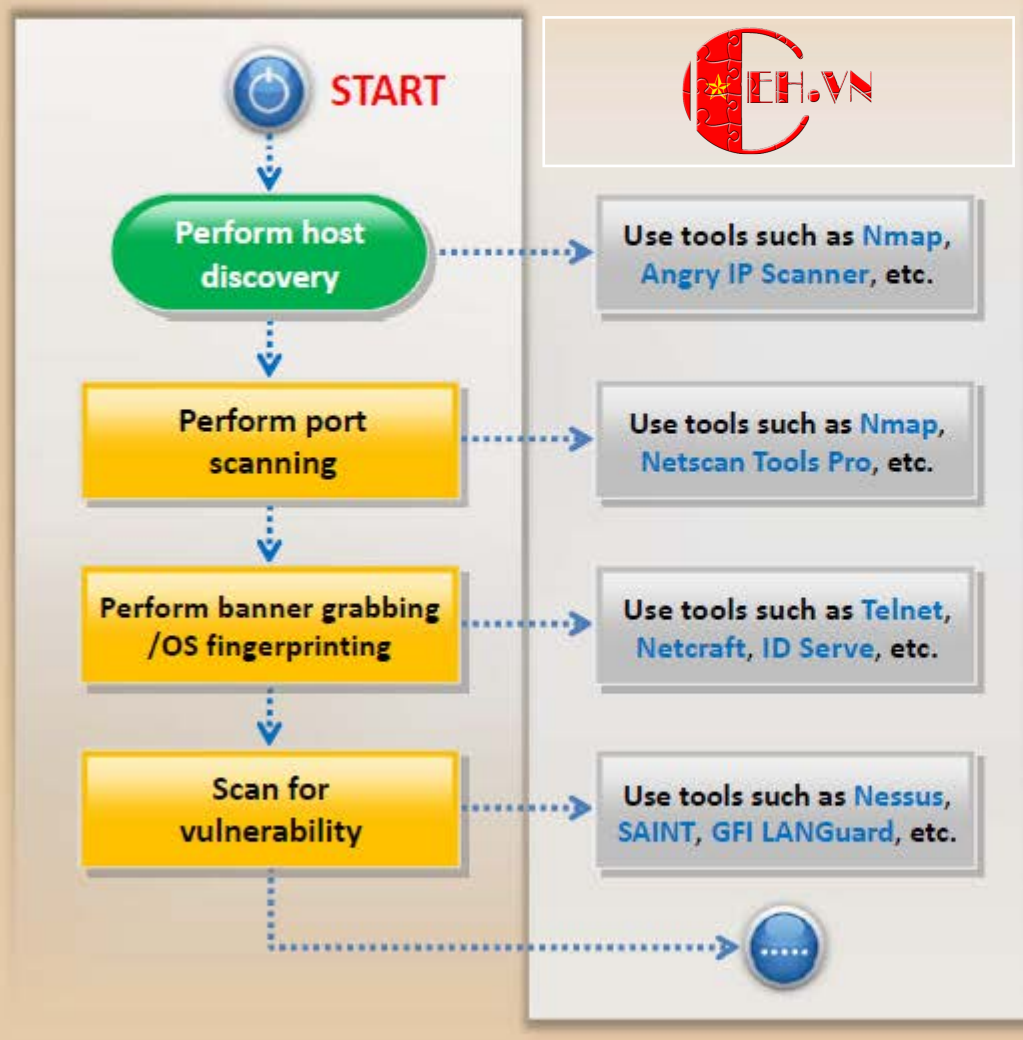
CEH Scanning Methodology

- 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

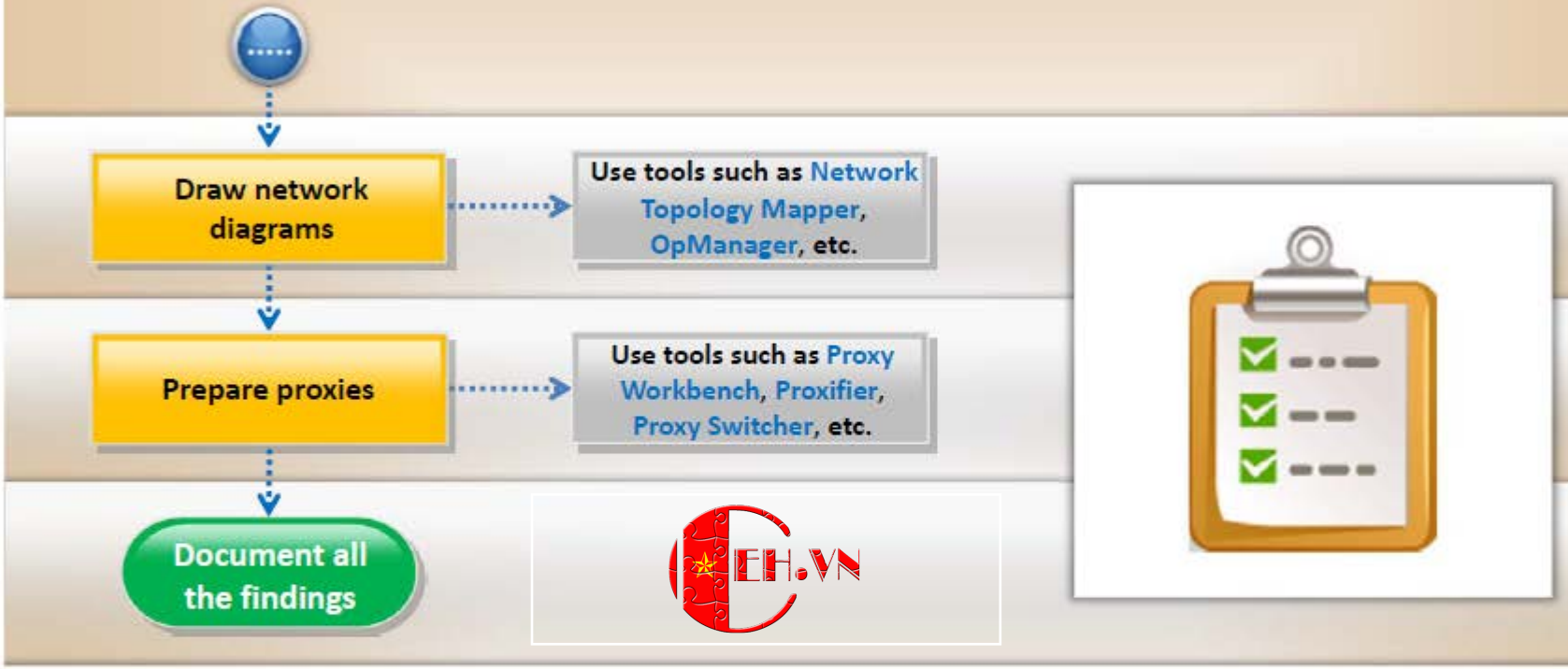
- Pen testing a network for scanning vulnerabilities determines the network's **security posture** by identifying **live systems**, discovering **open ports**, associating **services** and grabbing **system banners** to simulate a network hacking attempt
- The penetration testing report will help **system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

Scanning Pen Testing (Cont'd)



- 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, SuperScan, 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, SAINT, Core Impact Professional, Retina CS Management, MBSA, etc.

Scanning Pen Testing (Cont'd)



- Draw network diagrams of the vulnerable hosts using tools such as Network Topology Mapper, 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
- A proxy server is an application 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