

Scanning Networks

Module 03

Unmask the Invisible Hacker.



How Tech Companies Prepare for Cyber Attacks



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>

Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Module Objectives

CEH
Certified Ethical Hacker

- 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

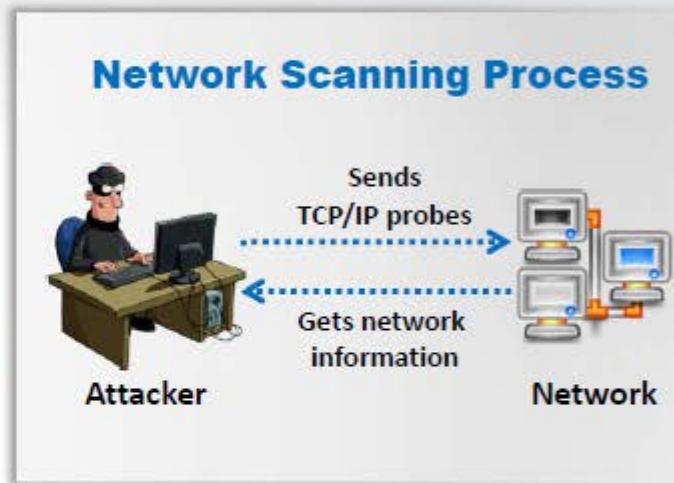
CEH
Certified Ethical Hacker

01

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

02



Objectives of Network Scanning

To discover live hosts, IP address, and open ports of live hosts

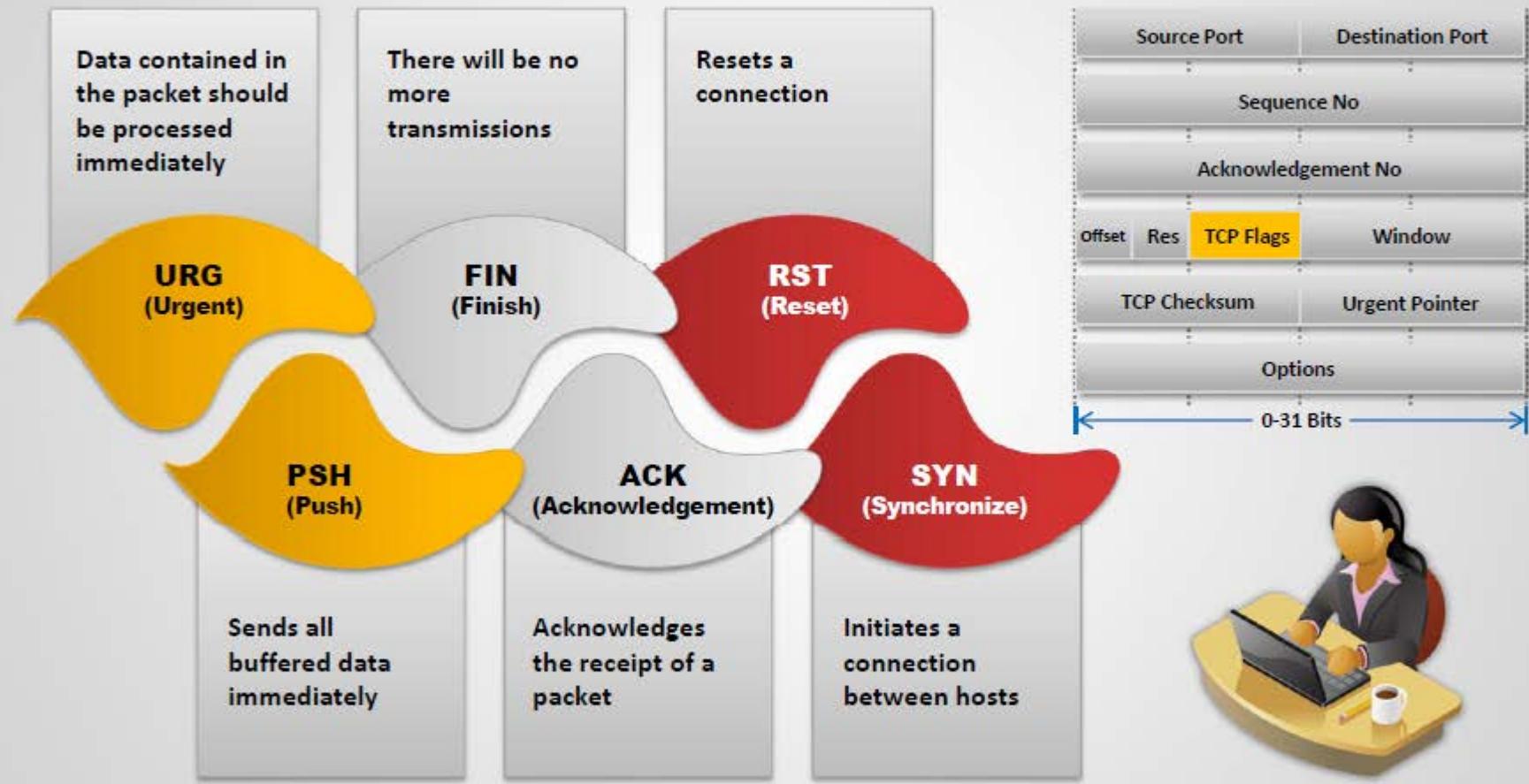
To discover operating systems and system architecture

To discover services running on hosts

To discover vulnerabilities in live hosts

TCP Communication Flags

CEH
Certified Ethical Hacker



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

TCP/IP Communication

CEH
Certified Ethical Hacker

TCP Session Establishment
(Three-way Handshake)



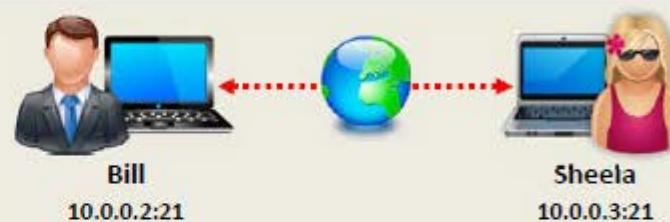
I would like to talk with you
Sheela on port 21, Are you open?
SYN, SEQ# 10

Ok, let's talk Bill,
I am open on port 21

SYN + ACK, ACK#11, SEQ#142

Ok, thanks Sheela
ACK, ACK#143, SEQ# 11

TCP Session Termination



I am done with the data transfer
FIN, SEQ# 50

Ok, I received your
termination request

ACK, ACK#51, SEQ#170

I have received all the data sent
FIN, SEQ#171

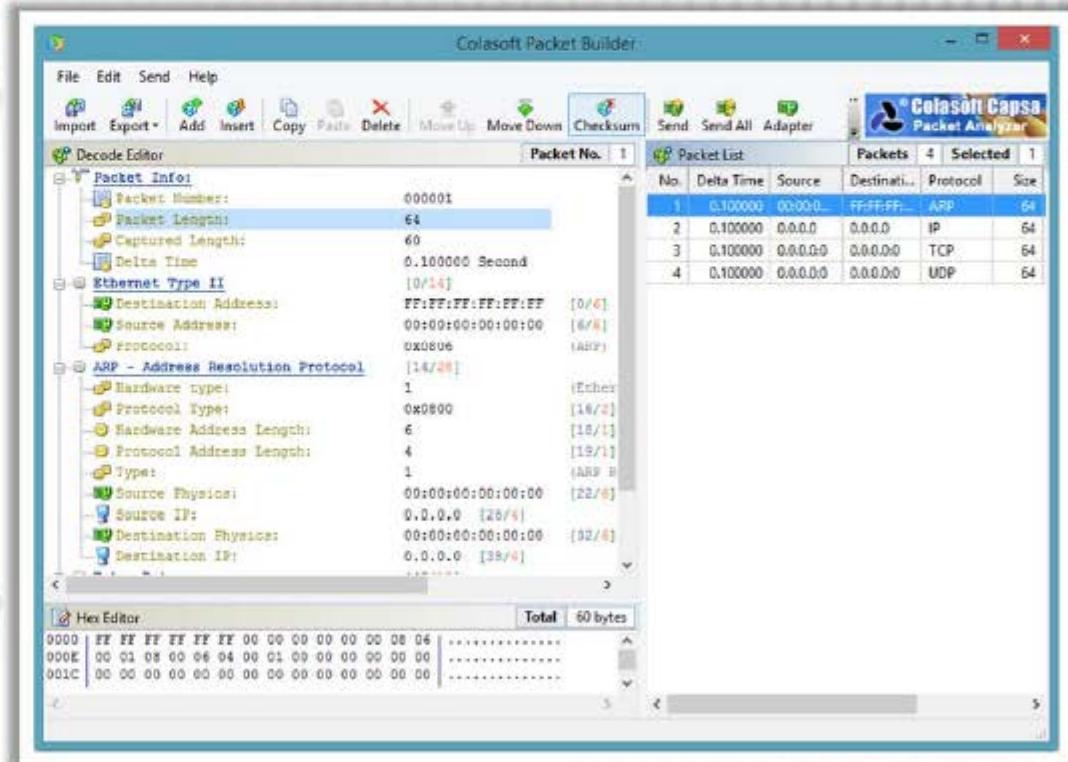
Ok, thanks Sheela
ACK, ACK#172, SEQ# 51

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

CEH
Certified Ethical Hacker

Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

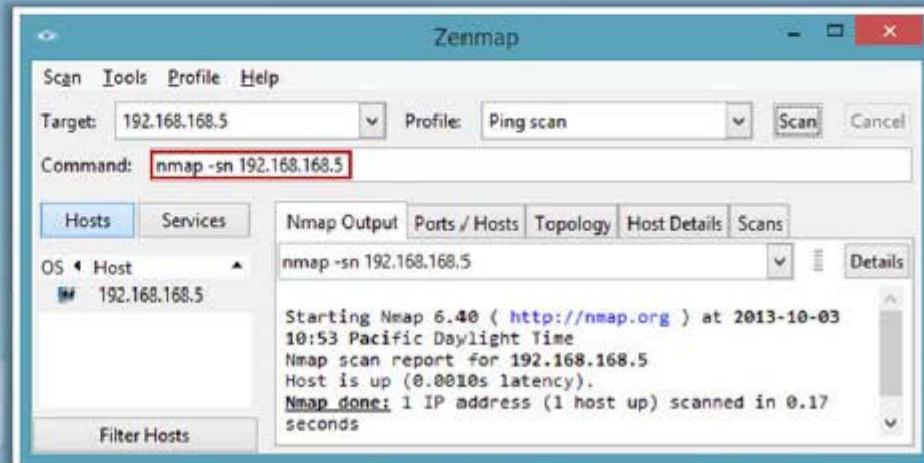
Checking for Live Systems - ICMP Scanning



- 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

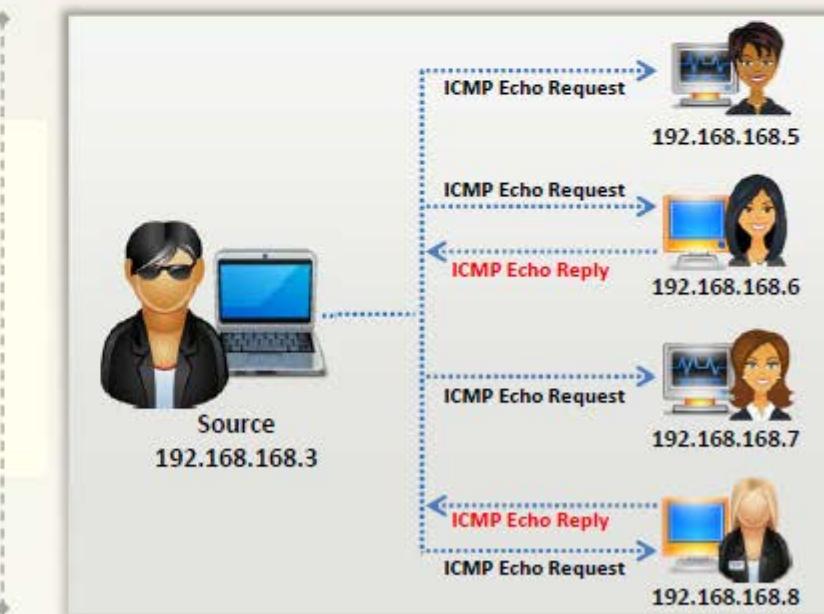
CEH
Certified Ethical Hacker



- 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.

IP Range - Angry IP Scanner

Scan Go to Commands Favorites Tools Help

IP Range: 192.168.168.70 to 192.168.168.130

Hostname: admin

IP Ping Hostname Ports [0+]

192.168.168.70	4 ms	[n/a]	[n/s]
192.168.168.71	5 ms	[n/a]	[n/s]
192.168.168.72	[n/a]	[n/s]	
192.168.168.73	[n/a]	[n/s]	
192.168.168.74	[n/a]	[n/s]	
192.168.168.75	3 ms	[n/a]	
192.168.168.76	[n/a]	[n/s]	
192.168.168.77	3 ms	[n/a]	
192.168.168.78	[n/a]	[n/s]	
192.168.168.79	[n/a]	[n/s]	
192.168.168.80	[n/a]	[n/s]	
192.168.168.81	[n/a]	[n/s]	
192.168.168.82	[n/a]	[n/s]	
192.168.168.83	[n/a]	[n/s]	
192.168.168.84	[n/a]	[n/s]	
192.168.168.85	[n/a]	[n/s]	
192.168.168.86	[n/a]	[n/s]	

Scan Statistics

Scanning completed

Total time: 25.8 sec

Average time per host: 0.6 sec

IP Range

192.168.168.70 - 192.168.168.130

Hosts scanned: 61

Hosts alive: 9

Close

Ready Display All Threads: 0

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**.

Ping Sweep

File Edit Skins Help

Starting IP Address: 192.168.168.10

Ending IP Address: 192.168.168.32

Scan For: All IPs

Scan

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	
192.168.168.32	2 ms	

Scan Completed Scan DNS 90

SolarWinds Engineer's Toolset

<http://www.solarwinds.com>

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>



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)



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

CEH
Certified Ethical Hacker

Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability

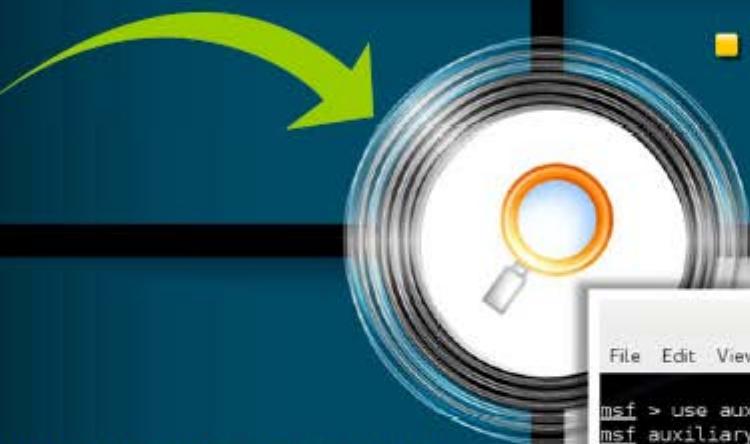


Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

SSDP Scanning



- 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

■ 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

```
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
KALI LINUX
[*] 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

C|EH
Certified Ethical Hacker

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

Zenmap window showing the results of a basic port scan. The target is set to `-p 1-65535 -A -v -p 1-65535 -A -v 192.168.168.5`. The output shows the host 192.168.168.5 is up and has several ports open, including 80/tcp (HTTP) and 443/tcp (HTTPS).

```
nmap -p 1-65535 -T4 -A -v -p 1-65535 -A -v 192.168.168.5
Starting Nmap 6.40 ( http://nmap.org ) at 2013-10-03
12:56 Pacific Daylight Time
NSE: Loaded 110 scripts for scanning.
NSE: Script Pre-scanning.
Initiating Ping Scan at 12:56
Scanning 192.168.168.5 [4 ports]
Completed Ping Scan at 12:56; 0.03s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 12:56
Completed Parallel DNS resolution of 1 host at 12:56; 0.22s elapsed
Initiating SYN Stealth Scan at 12:56
Scanning 192.168.168.5 [65535 ports]
Discovered open port 993/tcp on 192.168.168.5
Discovered open port 8800/tcp on 192.168.168.5
Discovered open port 8888/tcp on 192.168.168.5
Discovered open port 587/tcp on 192.168.168.5
Discovered open port 355/tcp on 192.168.168.5
Discovered open port 80/tcp on 192.168.168.5
Discovered open port 25/tcp on 192.168.168.5
Discovered open port 110/tcp on 192.168.168.5
Discovered open port 143/tcp on 192.168.168.5
Discovered open port 445/tcp on 192.168.168.5
Discovered open port 995/tcp on 192.168.168.5
Discovered open port 139/tcp on 192.168.168.5
Discovered open port 443/tcp on 192.168.168.5
Discovered open port 8081/tcp on 192.168.168.5
SYN Stealth Scan Timing: About 2.27% done; ETC: 13:20
(8:23:42 remaining)
```

Zenmap window showing the results of a detailed port scan. The target is set to `-p 1-65535 -T4 -A -v -p 1-65535 -A -v 192.168.168.5`. The output provides more detailed information for each open port, including service names and versions. For example, port 80/tcp is identified as HTTP and port 445/tcp is identified as Microsoft Windows RPC.

```
nmap -p 1-65535 -T4 -A -v -p 1-65535 -A -v 192.168.168.5
NOT SHOWN: 65534 PORTS
PORT      STATE SERVICE          VERSION
25/tcp    open  smtp?
[..._smtp-commands: Couldn't establish connection on port 25]
80/tcp    open  http?
81/tcp    open  hosts2-ms?
82/tcp    open  xfer?
110/tcp   open  pop3?
119/tcp   open  nntp?
135/tcp   open  msrpc?           Microsoft Windows RPC
139/tcp   open  netbios-ssn?
143/tcp   open  imap?
[..._imap-capabilities:
[..._ERROR Failed to connect to server
443/tcp  open  skype?           Skype
[..._http-title: Site doesn't have a title.
445/tcp  open  netbios-san?
465/tcp  open  smtp?
[..._smtp-commands: Couldn't establish connection on port 465]
563/tcp  open  snesir?
587/tcp  open  submission?
[..._smtp-commands: Couldn't establish connection on port 587]
512/tcp  open  vmauthd?         VMware Authentication
Daemon 1.0 (Uses VNC, SOAP)
993/tcp  open  imaps?
```

<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>

```
root@kali:~# hping3 -I 192.168.0.105
HPING 192.168.0.105 (eth0 192.168.0.105): icmp mode set, 28 headers + 0 data bytes
es
len=28 ip=192.168.0.105 ttl=128 id=448 icmp_seq=0 rtt=0.4 ms
len=28 ip=192.168.0.105 ttl=120 id=449 icmp_seq=1 rtt=0.4 ms
len=28 ip=192.168.0.105 ttl=128 id=450 icmp_seq=2 rtt=0.3 ms
len=28 ip=192.168.0.105 ttl=128 id=451 icmp_seq=3 rtt=0.5 ms
len=28 ip=192.168.0.105 ttl=128 id=452 icmp_seq=4 rtt=0.3 ms
len=28 ip=192.168.0.105 ttl=128 id=453 icmp_seq=5 rtt=0.9 ms
len=28 ip=192.168.0.105 ttl=128 id=454 icmp_seq=6 rtt=0.3 ms
len=28 ip=192.168.0.105 ttl=128 id=456 icmp_seq=7 rtt=0.4 ms
len=28 ip=192.168.0.105 ttl=128 id=458 icmp_seq=8 rtt=0.5 ms
len=28 ip=192.168.0.105 ttl=128 id=460 icmp_seq=9 rtt=0.3 ms
len=28 ip=192.168.0.105 ttl=128 id=461 icmp_seq=10 rtt=0.3 ms
```

ICMP Scanning

```
root@kali:~# hping3 -A 192.168.0.105 -p 80
HPING 192.168.0.105 (eth0 192.168.0.105): A set, 140 headers + 0 data bytes
len=40 ip=192.168.0.105 ttl=128 DF id=598 sport=80 flags=R seq=0 win=0 rtt=0.5 ms
len=40 ip=192.168.0.105 ttl=128 DF id=601 sport=80 flags=R seq=1 win=0 rtt=0.4 ms
len=40 ip=192.168.0.105 ttl=128 DF id=603 sport=80 flags=R seq=2 win=0 rtt=0.4 ms
len=40 ip=192.168.0.105 ttl=128 DF id=606 sport=80 flags=R seq=3 win=0 rtt=0.5 ms
len=40 ip=192.168.0.105 ttl=128 DF id=608 sport=80 flags=R seq=4 win=0 rtt=0.5 ms
len=40 ip=192.168.0.105 ttl=128 DF id=610 sport=80 flags=R seq=5 win=0 rtt=0.4 ms
len=40 ip=192.168.0.105 ttl=128 DF id=612 sport=80 flags=R seq=6 win=0 rtt=0.4 ms
len=40 ip=192.168.0.105 ttl=128 DF id=615 sport=80 flags=R seq=7 win=0 rtt=0.4 ms
len=40 ip=192.168.0.105 ttl=128 DF id=617 sport=80 flags=R seq=8 win=0 rtt=0.3 ms
```

ACK Scanning on port 80

Hping Commands



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

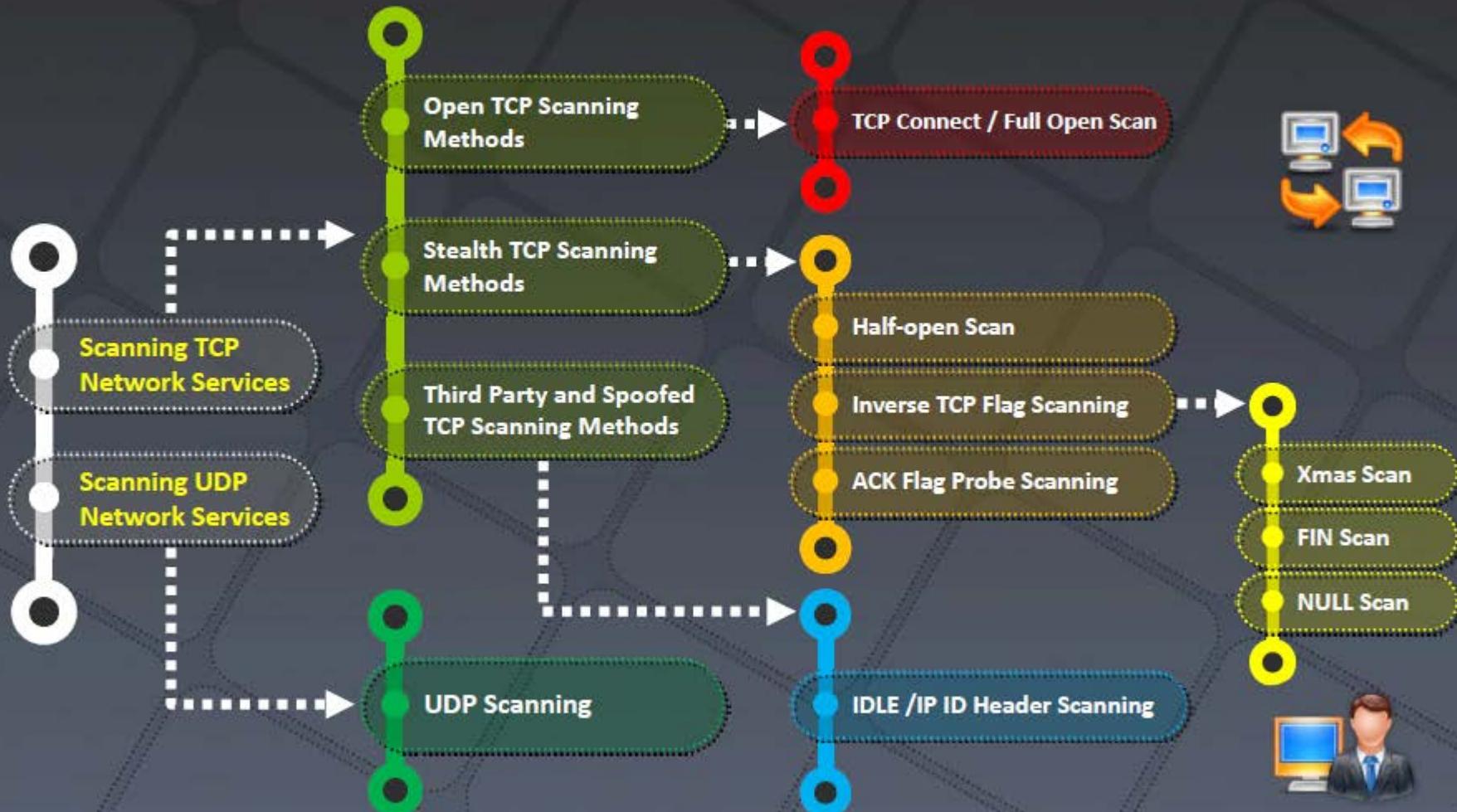
```
hping3 -S 72.14.207.99 -p 80 --  
tcp-timestamp
```



SYN flooding a victim

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

Scanning Techniques



TCP Connect / Full Open Scan

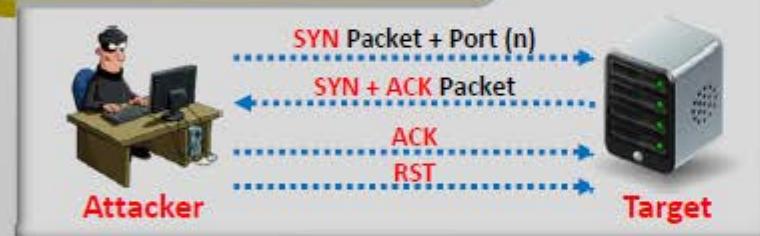
CEH
Certified Ethical Hacker

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

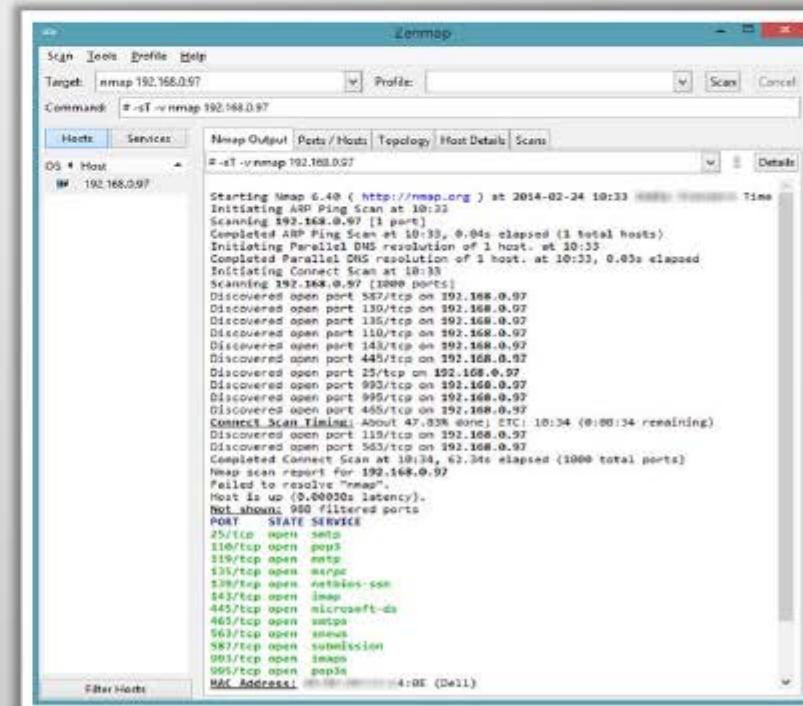
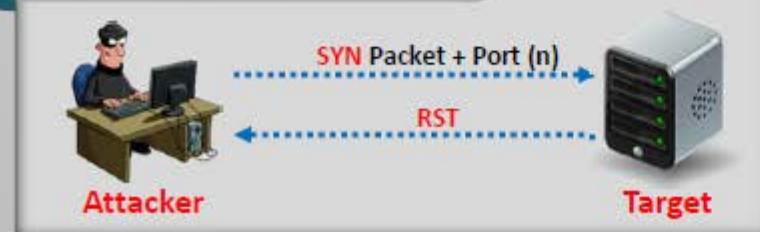
> 02 TCP Connect scan **establishes a full connection** and tears it down by sending a **RST packet**

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

Scan result when a port is open



Scan result when a port is closed



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

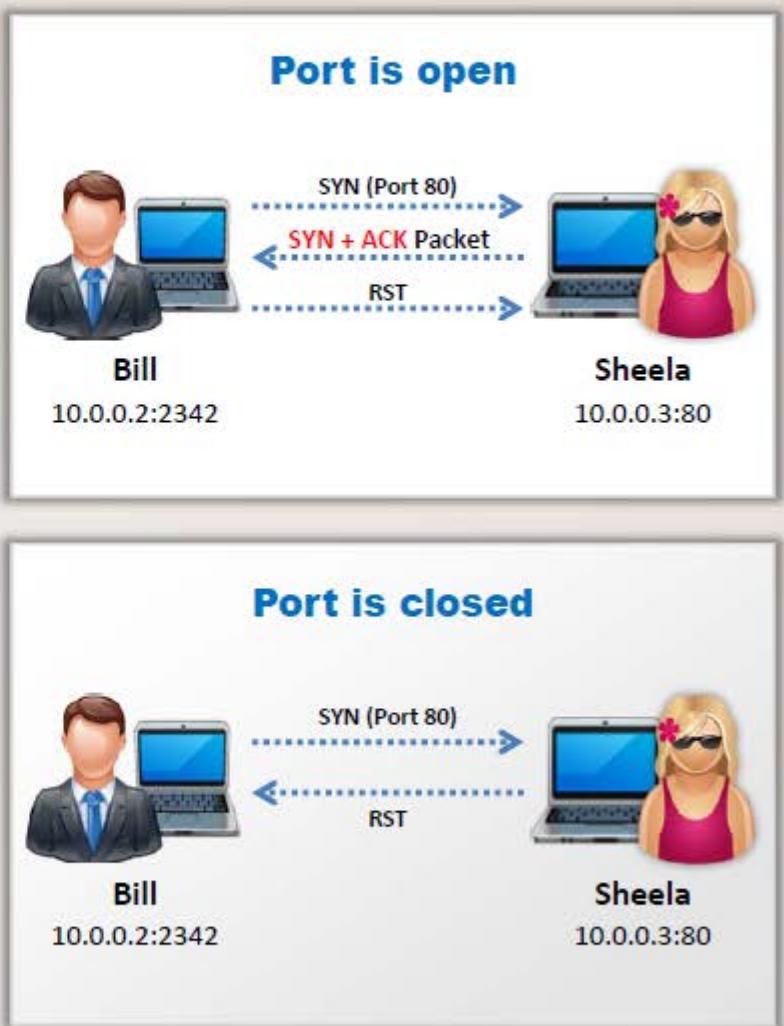
02

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)



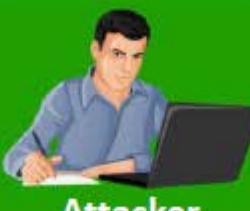
No Response



Target Host

03

Port is closed



Probe Packet (FIN/URG/PSH/NULL)

RST/ACK



Target Host

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

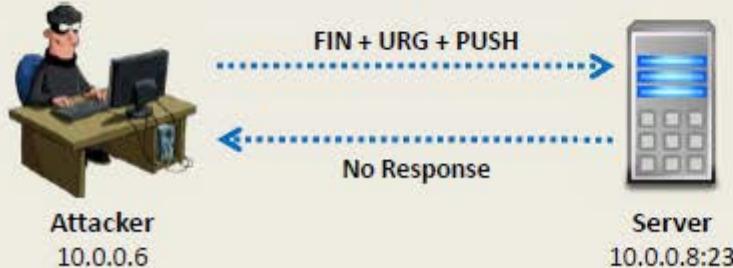
It will not work against any current version of **Microsoft Windows**

The screenshot shows the Zenmap interface with the command `# -sX -v nmap 192.168.0.97` entered. The output window displays the results of the XMAS scan:

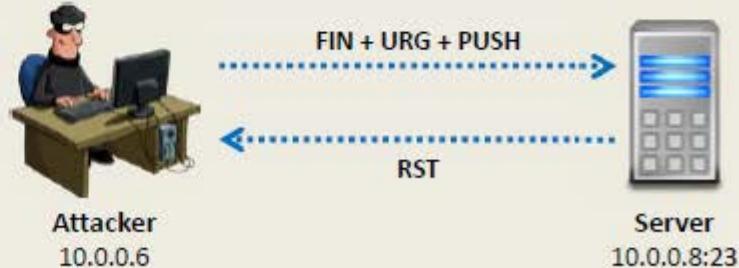
```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 10:45 UTC
Initiating ARP Ping Scan at 10:45
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 10:45, 0 ms elapsed (1 target up)
Initiating Parallel DNS resolution of 1 host at 10:45
Completed Parallel DNS resolution of 1 host at 10:45, 0.04s elapsed
Initiating XMAS Scan at 10:45
Scanning 192.168.0.97 [1000 ports]
Completed XMAS Scan at 10:45, 21.39s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Failed to resolve "nmap".
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.0.97 are open|filtered
MAC Address: 00:0C:29:4E:0F (Dell)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.94 seconds
Raw packets sent: 1801 (88.82kB) | Rcvd: 1 (28B)
```

Port is open



Port is closed

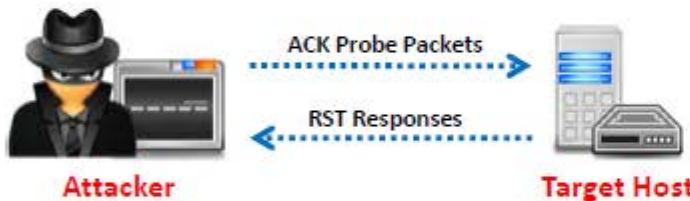


ACK Flag Probe Scanning

- 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
```

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

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**



Stateful Firewall is Present



No Firewall



The screenshot shows the Zenmap interface with the command `# -sA -v nmap 192.168.0.96` entered. The output window displays the results of the scan:

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 11:04
Time:Initiating ARP Ping Scan at 11:04
Scanning 192.168.0.96 [1 port]
Completed ARP Ping Scan at 11:04, 0.01s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:04
Completed Parallel DNS resolution of 1 host. at 11:04, 0.04s
elapsed
Initiating ACK Scan at 11:04
Scanning 192.168.0.96 [1000 ports]
Completed ACK Scan at 11:05, 21.40s elapsed (1000 total ports)
Nmap scan report for 192.168.0.96
Failed to resolve "nmap".
Host is up (0.00s latency).
All 1000 scanned ports on 192.168.0.96 are filtered
MAC Address: 00:0C:29:2D:05 (Dell)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 23.93 seconds
Raw packets sent: 2001 (80.02KB) | Rcvd: 1 (288)
```

IDLE/IPID Header Scan

CEH
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

```
C:\>nmap -Pn -sI www.juggyboy.com www.certifiedhacker.com
Starting Nmap ( http://nmap.org )
Idlescan using zombie www.juggyboy.com (192.130.18.124:80); Class: Incremental
Nmap scan report for 198.182.30.110
(The 40321 ports scanned but not shown below are in state: closed)
Port      State       Service
21/tcp    open        ftp
25/tcp    open        smtp
80/tcp    open        http
Nmap done: 1 IP address (1 host up) scanned in 1931.23 seconds
```

IDLE Scan: Step 1

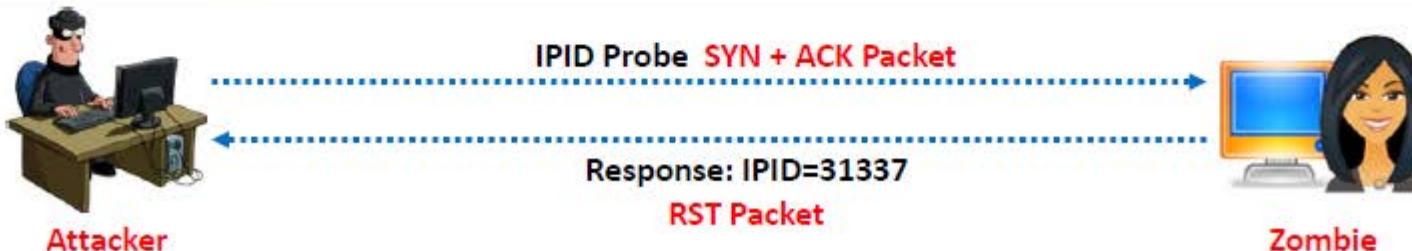
Send SYN + ACK packet to the zombie machine to **probe its IPID number**



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**

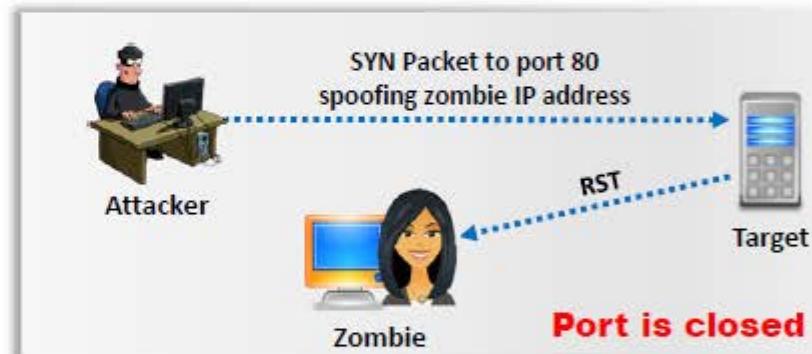
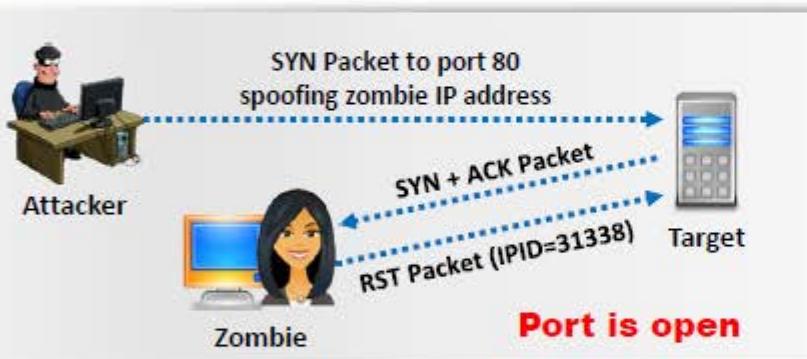


IDLE Scan: Step 2 and 3

CEH
Certified Ethical Hacker

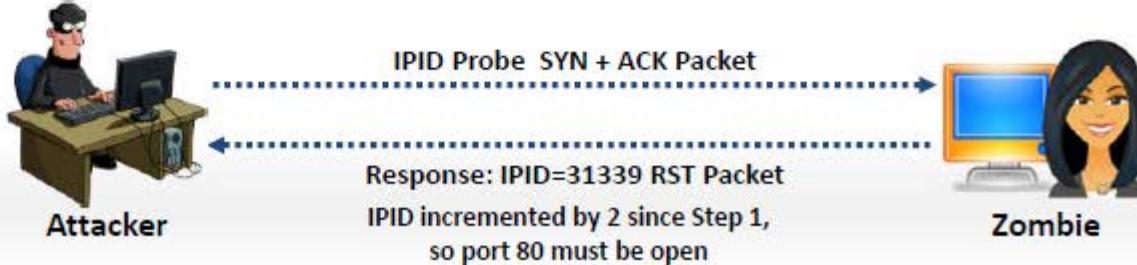
Step 2

- 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

CEH
Certified Ethical Hacker



Attacker

Are you **open** on UDP Port 29?



No response if port is **Open**



Server

If Port is Closed, an **ICMP Port unreachable** message is received

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

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 11:14
Initiating ARP Ping Scan at 11:14
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 11:14, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 11:14
Completed Parallel DNS resolution of 1 host. at 11:14, 0.01s elapsed
Initiating UDP Scan at 11:14
Scanning 192.168.0.97 [1000 ports]
Discovered open port 137/udp on 192.168.0.97
Completed UDP Scan at 11:14, 8.79s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Host is up (0.0011s latency).
Not shown: 999 open|filtered ports
PORT      STATE SERVICE
137/udp  open  netbios-ns
MAC Address: 00:0C:29:4E:0E (Dell)

Read data files from: C:\Program Files (x86)\Nmap
Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
Raw packets sent: 2001 (57.562KB) | Rcvd: 5 (386B)
```

ICMP Echo Scanning/List Scan

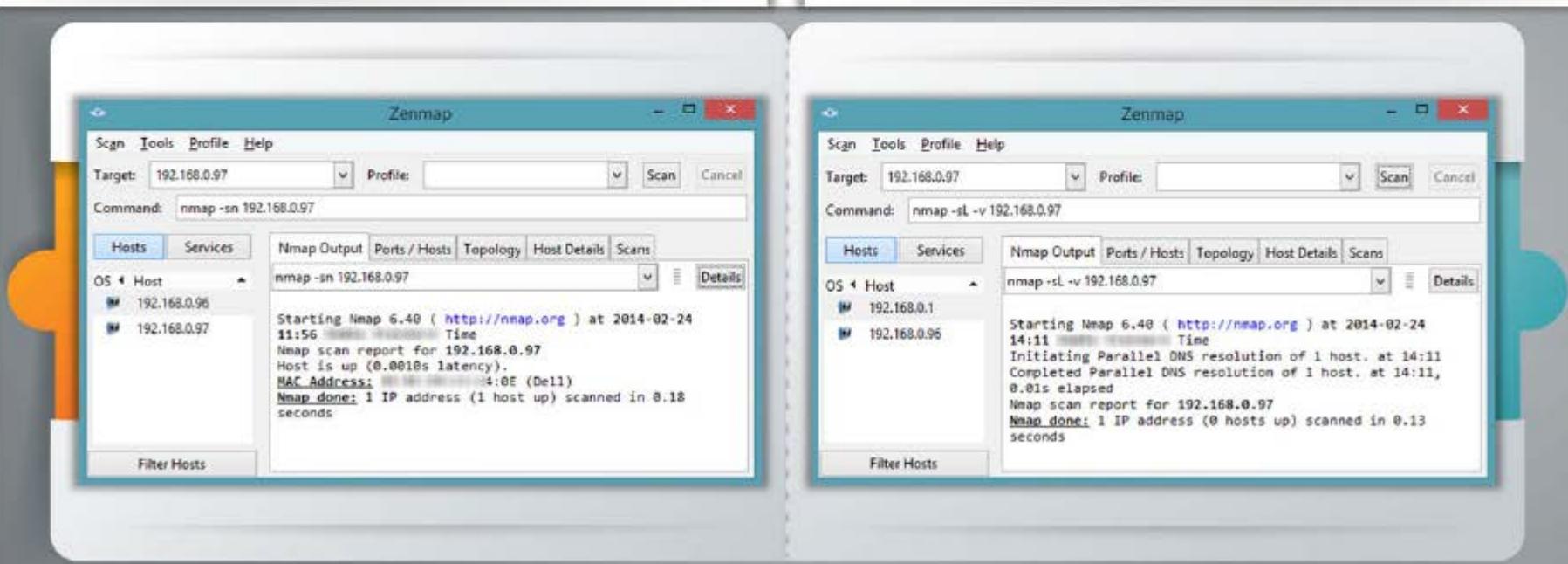
CEH
Certified Ethical Hacker

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

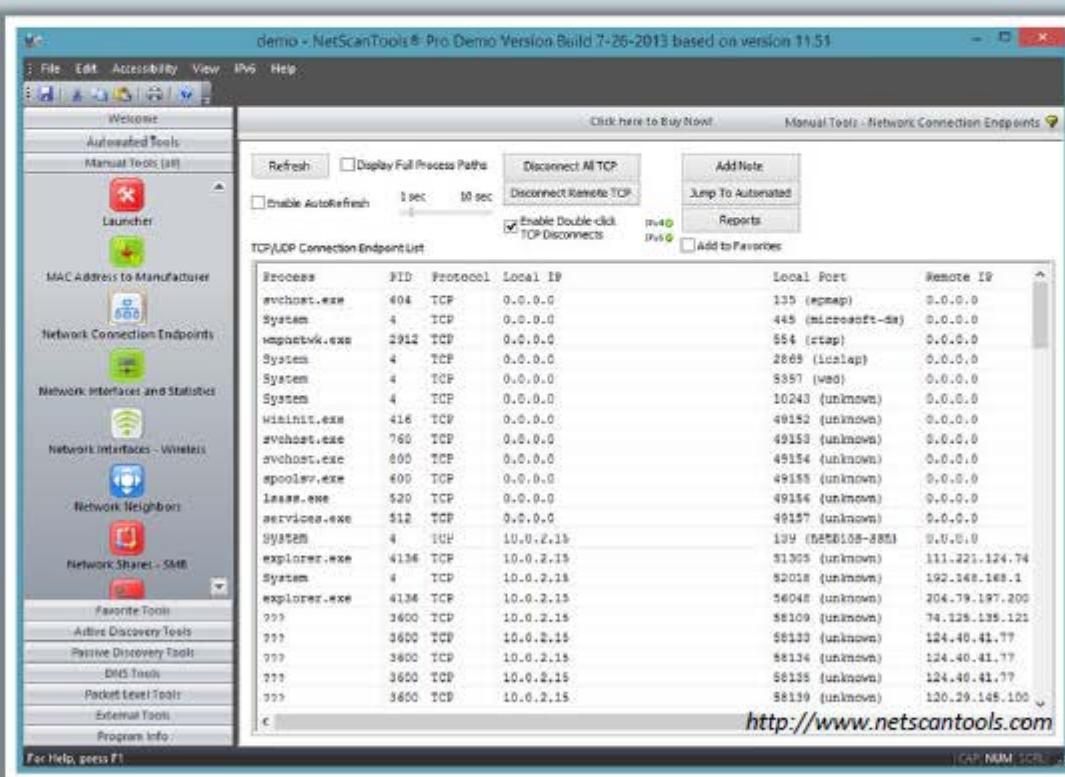
- This type of scan simply generates and prints a list of IPs/Names without actually pinging them
- A reverse DNS resolution is carried out to identify the host names



Scanning Tool: NetScan Tools Pro

C|EH
Certified Ethical Hacker

- 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

CEH
Certified Ethical Hacker



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>



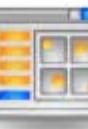
Global Network Inventory Scanner
<http://www.magnetosoft.com>



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



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

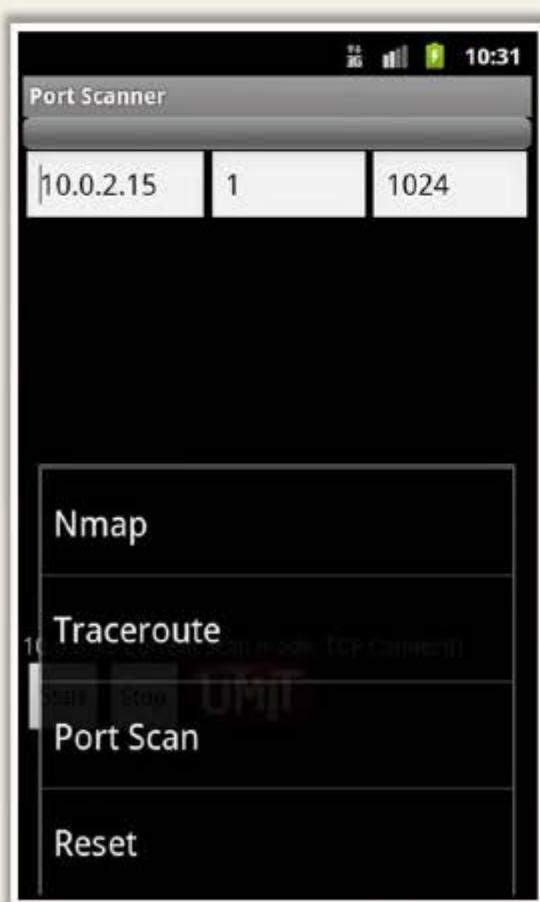


CurrPorts
<http://www.nirsoft.net>

Scanning Tools for Mobile

C|EH
Certified Ethical Hacker

Umit Network Scanner



<http://www.umitproject.org>

Fing



<http://www.overlooksoft.com>

IP Network Scanner



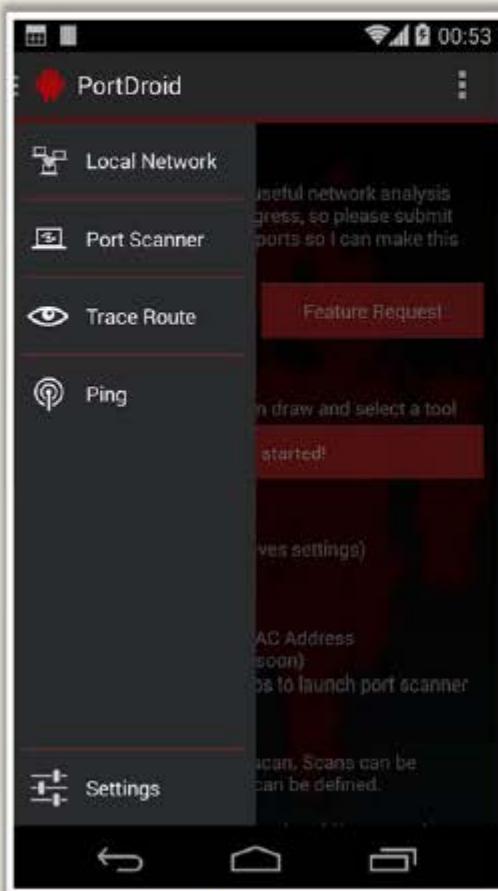
<http://10base-t.com>

Scanning Tools for Mobile

(Cont'd)



PortDroid Network Analysis



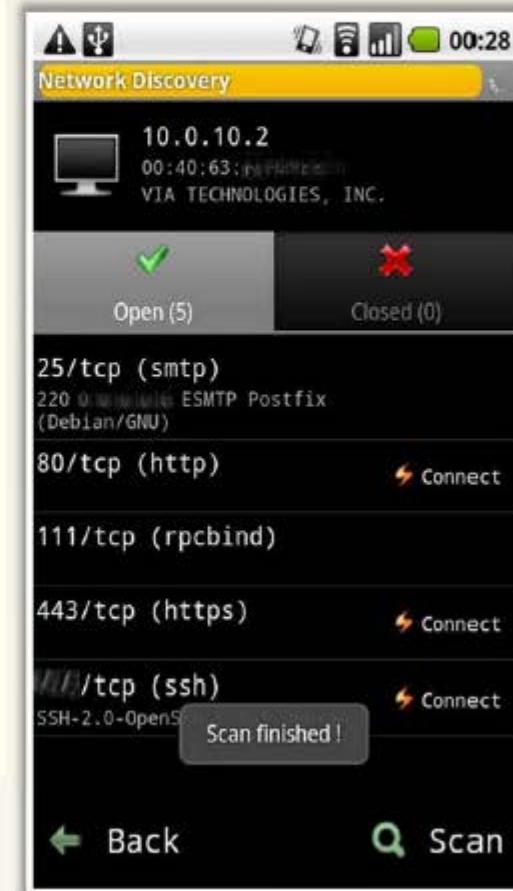
<http://www.stealthcopter.com>

Pamn IP Scanner



<http://pips.wjholden.com>

Network Discovery



<http://rorist.github.io>

Port Scanning Countermeasures



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

CEH
Certified Ethical Hacker

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

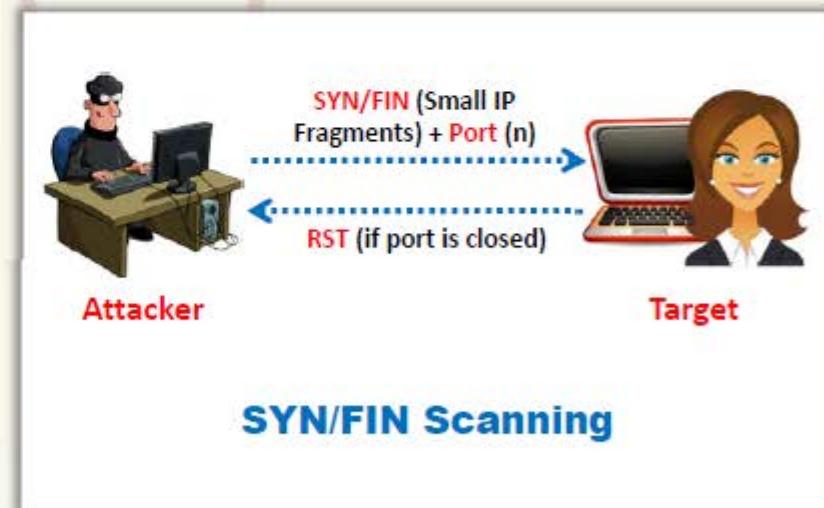


It is not a new scanning method but a **modification** of the earlier methods



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

```
Command Prompt
C:\>nmap -sS -T4 -A -f -v 192.168.168.5
Starting Nmap 6.40 ( http://nmap.org ) at
2014-02-10 11:03 EDT
Initiating SYN Stealth Scan at 11:03
Scanning 192.168.168.5 [1000 ports]
Discovered open port 139/tcp on 192.168.168.5
Discovered open port 445/tcp on 192.168.168.5
Discovered open port 135/tcp on 192.168.168.5
Discovered open port 912/tcp on 192.168.168.5
Completed SYN Stealth Scan at 11:03, 4.75s
elapsed (1000 total ports)
```



CEH Scanning Methodology

CEH
Certified Ethical Hacker

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

CEH
Certified Ethical Hacker

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

CEH
Certified Ethical Hacker

ID Serve

- ① ID Serve is used to identify the **make, model**, and **version** of any web site's server software
- ② It is also used to **identify non-HTTP** (non-web) **Internet servers** such as FTP, SMTP, POP, NEWS, etc.



<http://www.grc.com>

Netcraft

- ③ 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

The screenshot shows the 'Site report for www.certifiedhacker.com' from Netcraft. It includes sections for 'Background' (Site title: Certified Hacker, Site ID: 79842, Data first seen: December 2003), 'Network' (Site: http://www.certifiedhacker.com, Domain: certifiedhacker.com, Organization: certifiedhacker.com, Top Level Domain: .com, Netblock owner: TM VAOS DC Hosting, IP address: 203.75.54.101, etc.), 'Last Reboot' (1 day ago), and 'Hosting History' (a table showing multiple entries for TM VAOS DC Hosting, IP address 203.75.54.101, with columns: Netblock owner, IP address, OS, Web server, Last seen). A red box highlights the 'Background' section.

<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
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: 2165
Content-Type: text/html
Content-Location: http://10.49.39.26/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

```
Telnet www.certifiedhacker.com
```

```
HTTP/1.1 403 Forbidden
Content-Length: 218
Content-Type: text/html
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
Date: Fri, 04 Oct 2013 04:29:51 GMT
Connection: close

<html><head><title>Error</title></head><body><head><title>Directory Listing Denied</title></head><body><h1>Directory Listing Denied</h1>This Virtual Directory does 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 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



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

CEH
Certified Ethical Hacker

Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



Prepare Proxies

Draw Network Diagrams

Scanning Pen Testing

Vulnerability Scanning

CEH
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



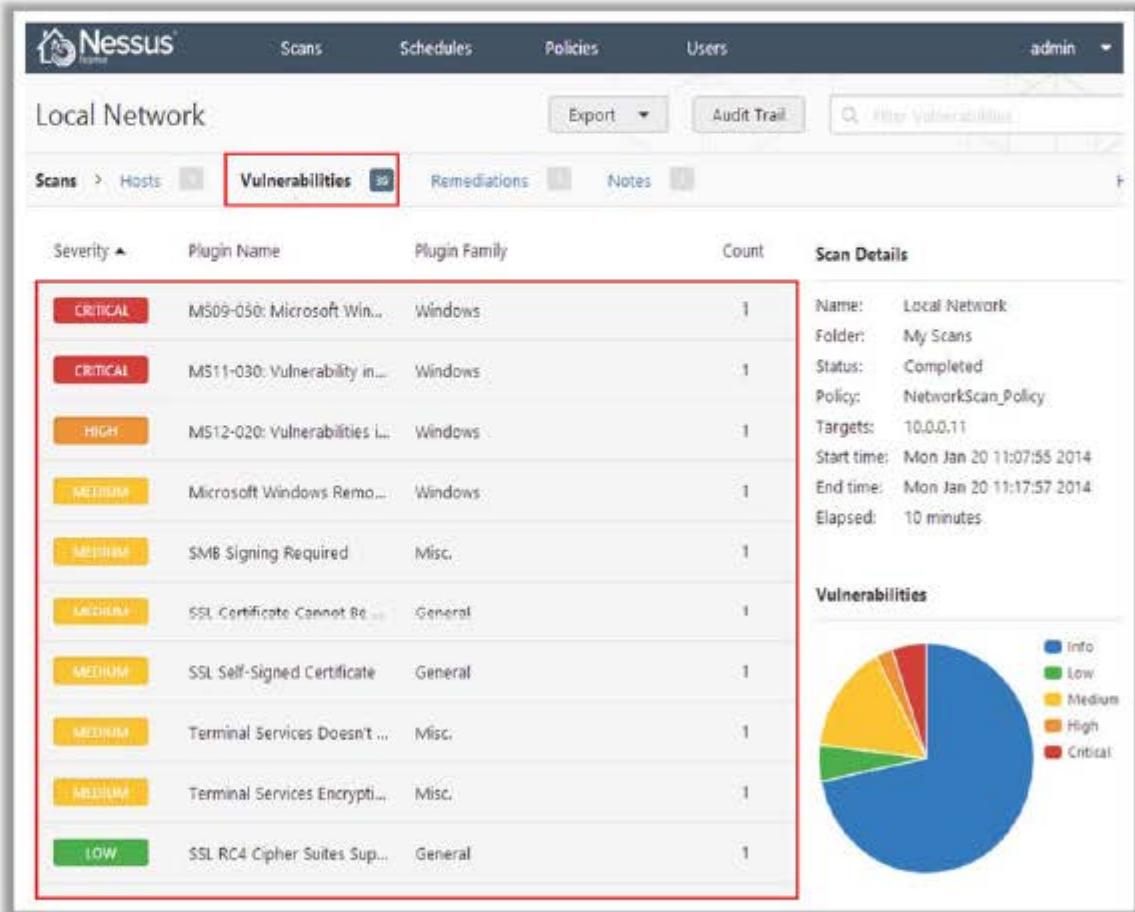
Vulnerability Scanning Tool: Nessus



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

CEH
Certified Ethical Hacker

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

Welcome Vanessa
Thanks for choosing Qualys FreeScan. Using FreeScan you can quickly and easily verify the security of your business.

Take the tour | [Vanessa Foley](#) | [It's scans remaining](#)

Scan in Progress
<http://www.mwtest.info/malware-demos-named/malwtest.html>
In progress
In progress
In progress

OWASP Scan [View report](#)
Summary: 116 pages impacted 1117 threats found.
Threat summary: 264 vulnerabilities found.
Patch report summary: No patches available.

SCAP Scan [View report](#)
SCAP summary: 43 of 227 Rules Not Compliant
10.10.30.32

Scan on 02/14/2013 [View report](#)
Summary: 203 vulnerabilities found.
10.10.26.238

SCAP scan on 02/14/2013 [View report](#)
SCAP summary: 43 of 227 Rules are failing (18.04%) Not Compliant
10.10.30.32

OWASP scan Report on 02/14/2013 [View report](#)
Summary: 116 pages impacted 1117 threats found.
http://10.10.26.238

A blue callout box is overlaid on the "Vulnerability Audit" section of the dashboard.

Welcome Vanessa
Thanks for choosing Qualys FreeScan. Using FreeScan you can quickly and easily verify the security of your business.

Quick Tour | Take the tour | [Vanessa Foley](#) | [It's scans remaining](#)

More Results

OWASP Report **Patch Report** **Threat Report** [Print Report](#)

Vulnerability Scan External host vulnerability report

24 Vulnerabilities detected 7 High Risk
Medium Risk Low Risk Info gathered

Malware Detection
Identify if malware is hosted on your website and served to your clients.

February 15, 2013 at 11:44 [http://www.mwtest.info/m.../www.mwtest.info](#) [Rescan URL](#)

All Scan Results 1 - 25 of 25

A Malicious Process Launch Was Detected

CID: 294612 CVE Base: 5.0 CVSS Temporal: 4.2 Port: - Category: Malware
CVE ID: Found at: http://www.mwtest.info/malware-demos-named/malwtest/0042MD-NH
Threat: Upon visiting the Web page, a process launch was detected by the malware detection service. External process launches should never occur in normal Web browsing activity. This is an indication of malicious behavior. The process launched is noted in the Results section.
Impact: n/a
Solution: n/a
Results: Upon visiting the Web page, a process launch was detected by the malware detection service. External process launches should never occur in normal Web browsing activity. This is an indication of malicious behavior.

<http://www.qualys.com>

Network Vulnerability Scanners

CEH
Certified Ethical Hacker



Retina CS
<http://www.beyondtrust.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>



SAINT
<http://www.saintcorporation.com>



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

Vulnerability Scanning Tools for Mobile



Retina CS for Mobile



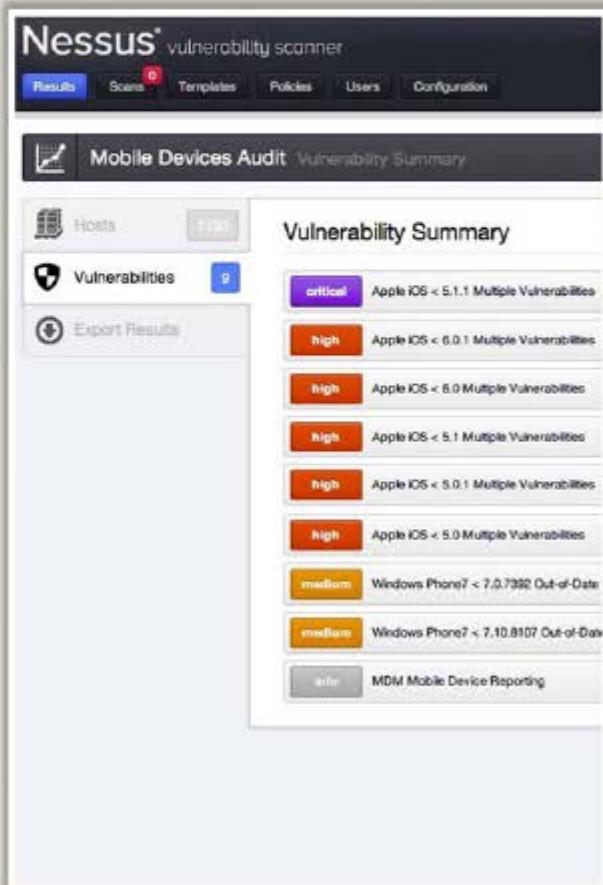
<http://www.beyondtrust.com>

SecurityMetrics MobileScan



<https://www.securitymetrics.com>

Nessus Vulnerability Scanner

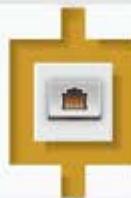


<http://www.tenable.com>

CEH Scanning Methodology

CEH
Certified Ethical Hacker

Check for Live Systems



Check for Open Ports



Scanning Beyond IDS

Banner Grabbing



Scan for Vulnerability

Draw Network Diagrams



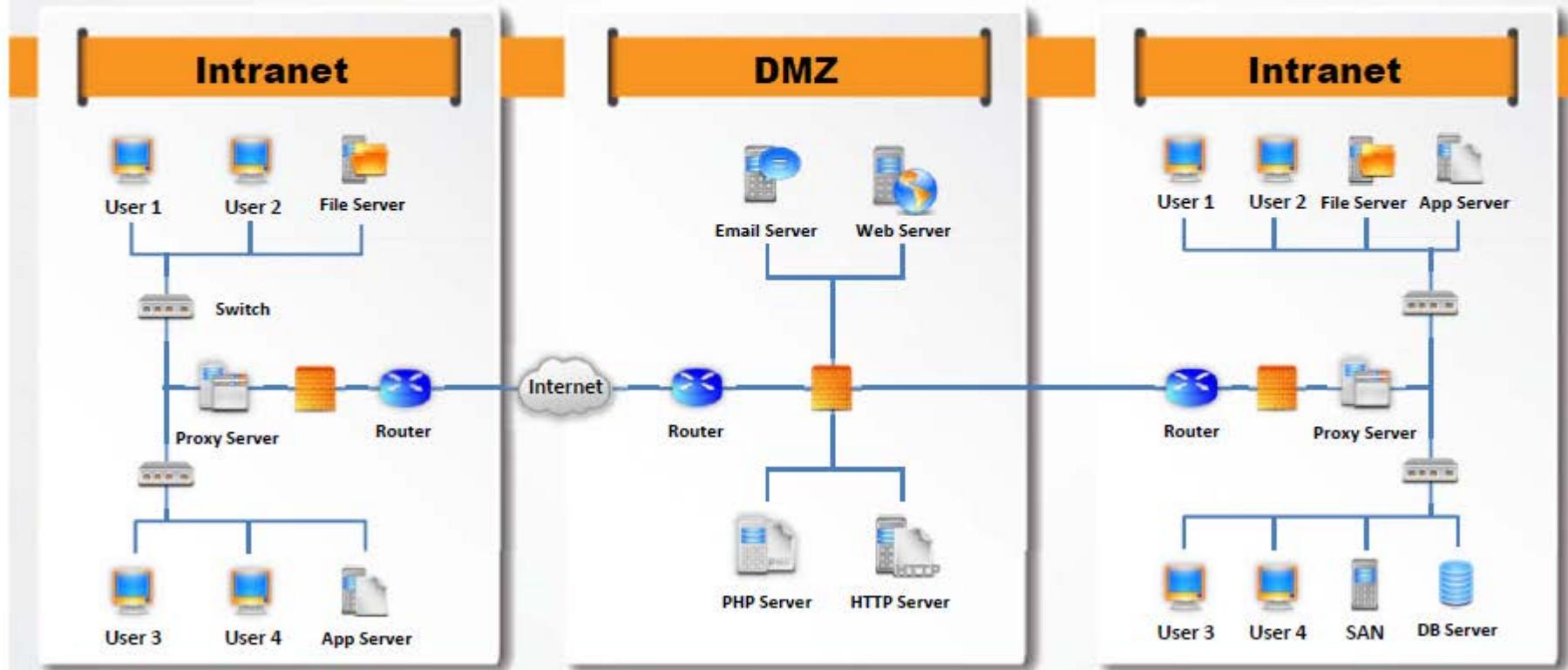
Prepare Proxies

Scanning Pen Testing

Drawing Network Diagrams

CEH
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

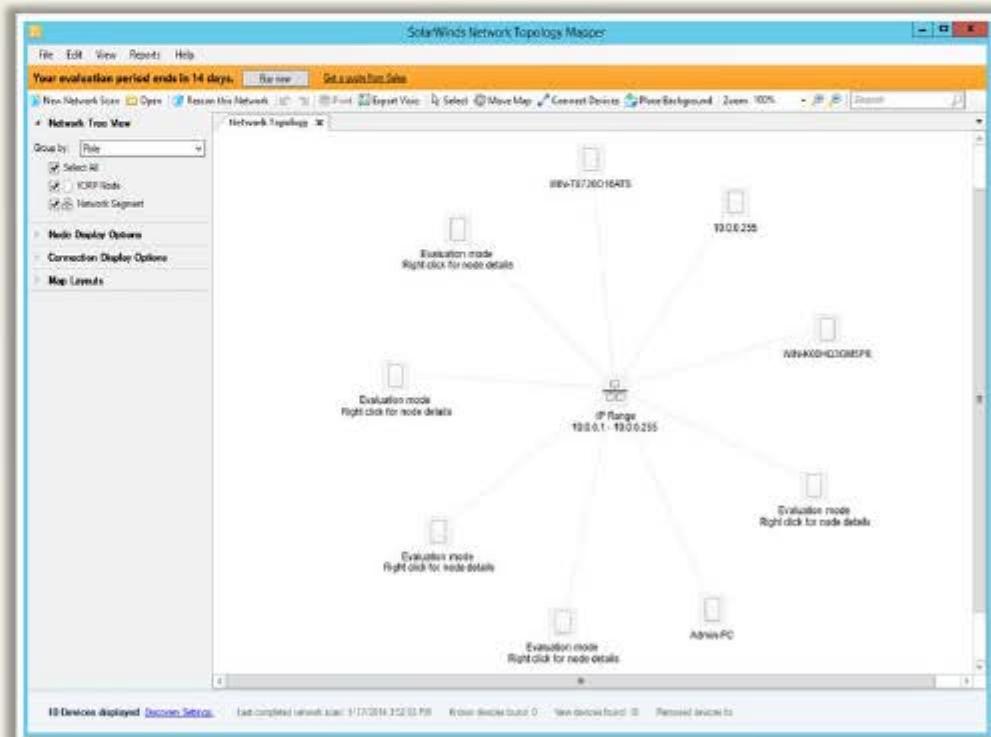
Export network diagrams to Visio

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

100

OpManager

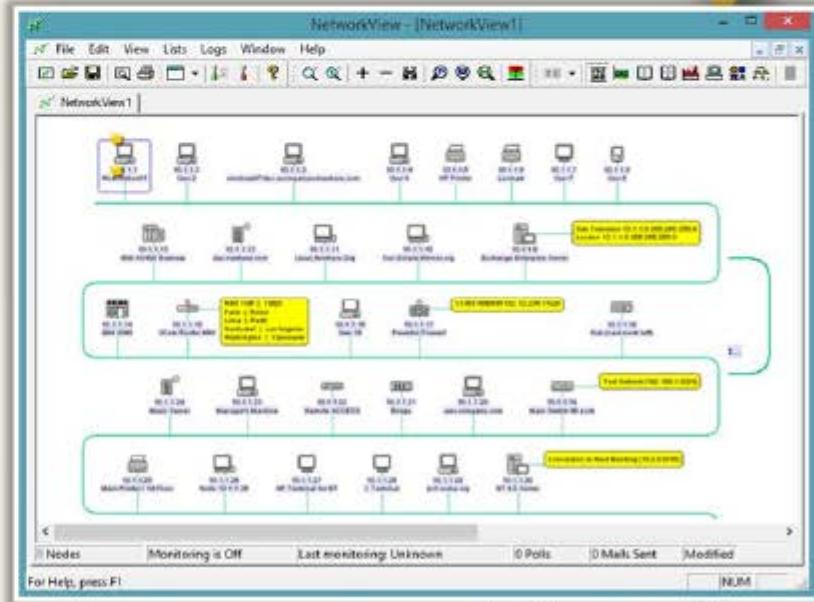
OpManager is a network monitoring software that offers advanced **fault and performance management** functionality across critical **IT resources** such as routers, WAN links, switches, firewalls, VoIP call paths, physical servers, etc.



<http://www.mariageengine.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

CEH
Certified Ethical Hacker



The Dude
<http://www.mikrotik.com>



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



Friendly Pinger
<http://www.kilievich.com>



Ipsonar
<http://www.lumeta.com>



WhatsConnected
<http://www.whatsupgold.com>



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



InterMapper
<http://www.intermapper.com>



NetMapper
<http://www.opnet.com>



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

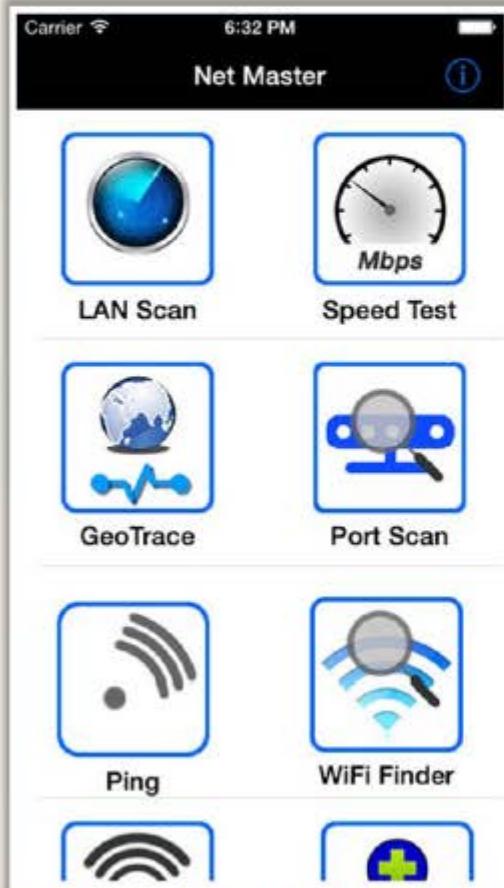


Spiceworks-Network Mapper
<http://www.spiceworks.com>

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

CEH
Certified Ethical Hacker

Check for Live Systems



Check for Open Ports

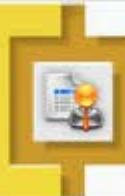


Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



Draw Network Diagrams

Prepare Proxies

Scanning Pen Testing

Proxy Servers

CEH
Certified Ethical Hacker

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



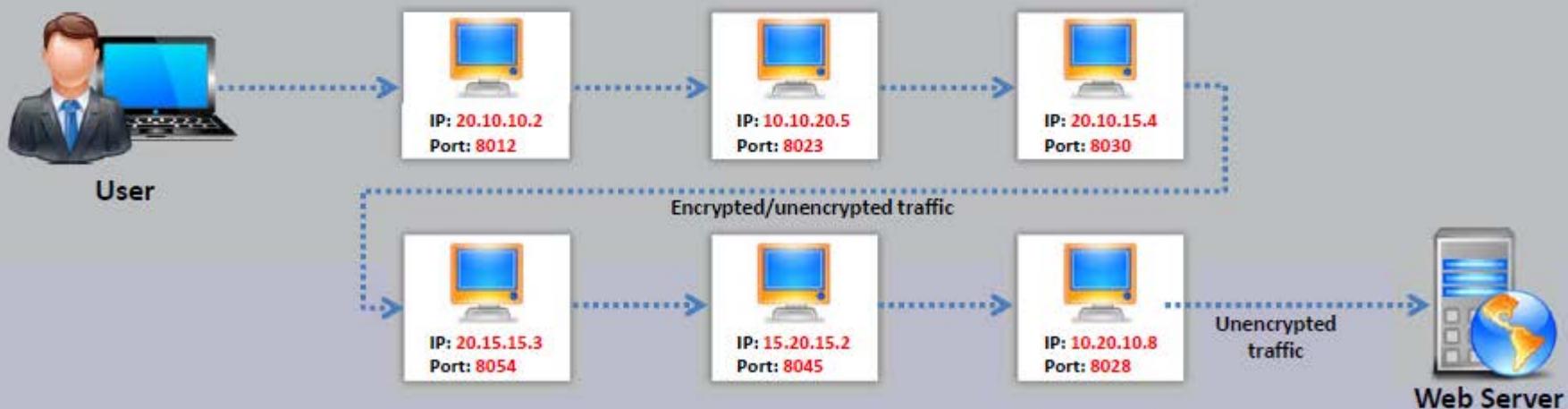
To **interrupt all the requests** sent by a user and transmit them to a third destination, hence victims will only be able to identify the proxy server address



Attackers chain **multiple proxy servers** to avoid detection

Proxy Chaining

- 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

CEH
Certified Ethical Hacker

Proxy Switcher Unregistered (Active Proxy: 217.33.193.179:3128 - UNITED KINGDOM)

File Edit Actions View Help

Proxy Scanner

- New (1026)
- High Anonymous (0)
- SSL (0)
- Elite (0)
- Dead (5886)
 - Permanently (0)
 - Basic Anonymity (646)
 - Private (18)
 - Dangerous (1546)
 - My Proxy Servers (0)
 - ProxySwitcher (0)

Server	State	Response	Country
213.122.178.99:8080	Alive	10062ms	UNITED KINGDOM
94.136.35.125:4444	Alive	12426ms	UNITED KINGDOM
162.13.113.63:3128	(Alive-SSL)	13203ms	UNITED KINGDOM
217.33.193.179:3128	(Alive-SSL)	13211ms	UNITED KINGDOM
94.136.35.124:4444	Alive	13463ms	UNITED KINGDOM
88.150.200.9:3128	(Alive-SSL)	16730ms	UNITED KINGDOM
196.41.38.18:8080	(Alive-SSL)	13988ms	UNITED REPUBLIC OF TANZA
41.59.17.36:8080	(Alive-SSL)	18461ms	UNITED REPUBLIC OF TANZA
41.223.231.43:3128	Alive	16187ms	UNITED REPUBLIC OF TANZA
1541-175.members.linode...	Alive	12505ms	UNITED STATES
173.230.150.121:3128	(Alive-SSL)	13941ms	UNITED STATES
166.78.179.35:5555	Alive	13448ms	UNITED STATES
97.73.31.100:87	Alive	18333ms	UNITED STATES
75.148.172.41:9999	Alive	16245ms	UNITED STATES
2.54.204.12.206:8080	(Alive-SSL)	11914ms	UNITED STATES

Disabled Keep Alive Auto Switch

Your tcplip.sys driver seems to be not limiting half-open connection count. It's a good thing.
You are using the most recent version.

Basic Anonymity 0/32

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

The screenshot shows the Proxy Workbench interface. The title bar reads "Proxy Workbench". The menu bar includes "File", "View", "Tools", and "Help". The toolbar contains icons for monitoring, tools, and status. The main window displays "Monitoring: WIN-QEBBMOPE8PE [192.168.0.54]". On the left, a tree view shows "All Activity" with items like "SMTP - Outgoing e-mail (25)", "POP3 - Incoming e-mail (110)", "HTTP Proxy - Web (8080)", "HTTPS Proxy - Secure Web (443)", "FTP - File Transfer Protocol (21)", and "Pass Through - For Testing Apps (10001)". The central pane shows "Details for All Activity" with a table of connections. The bottom pane shows "Real time data for All Activity" with a hex dump of network traffic. Status bars at the bottom show "Memory: 36 KBytes", "Sockets: 4", and "Events: 00".

<http://proxyworkbench.com>

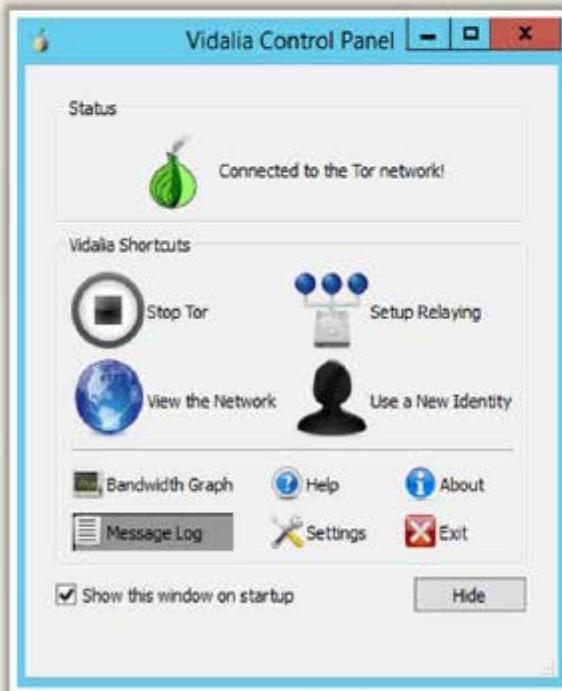
Copyright © by EC-Council. All Rights Reserved. Reproduction is Strictly Prohibited.

Proxy Tools: TOR and CyberGhost

C|EH
Certified Ethical Hacker

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>



Burp Suite

<http://www.portswigger.net>



Proxifier

<https://www.proxifier.com>



Proxy Tool Windows App

<http://webproxylist.com>



Charles

<http://www.charlesproxy.com>



Fiddler

<http://www.telerik.com>



Proxy

<http://www.analogx.com>



Protoport Proxy Chain

<http://www.protoport.com>



ProxyCap

<http://www.proxycap.com>



CCProxy

<http://www.youngzsoft.net>

Proxy Tools for Mobile

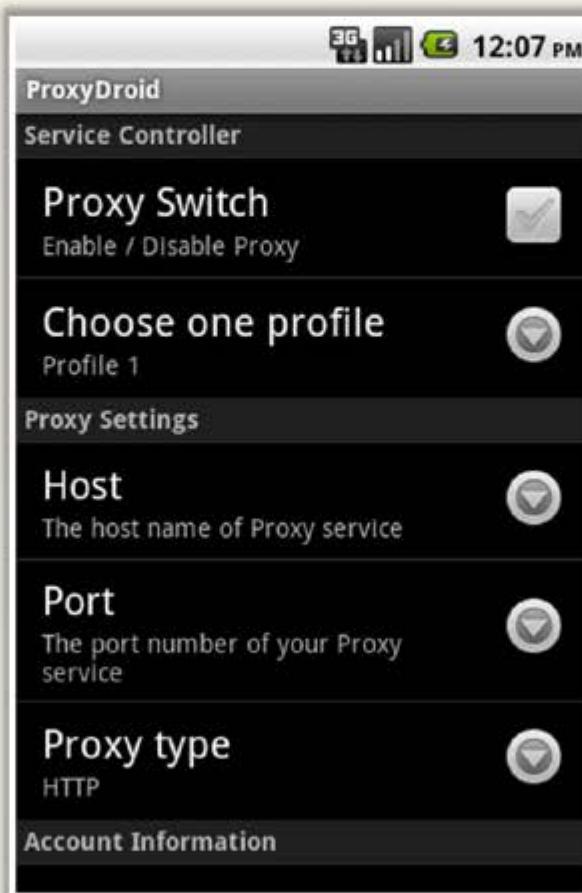
CEH
Certified Ethical Hacker

Proxy Browser for Android



<https://play.google.com>

ProxyDroid



<https://github.com>

NetShade



<http://www.raynersw.com>

Free Proxy Servers

The screenshot shows a Google search results page with the query "Free Proxy Servers". The results include links to various proxy lists and checkers, such as "Free Proxy List - Public Proxy Servers (IP PORT) - Hide My Ass!", "Free Proxy Servers - Protect Your Online Privacy with Our Proxy List", and "List of Free Proxy Servers - Page 1 of 11 - Proxy 4 Free". A large orange ribbon graphic highlights the search bar and the first result. To the right of the search results, a callout box contains the text: "A search in Google lists thousands of free proxy servers".

Google search results for "Free Proxy Servers":

- [Free Proxy List - Public Proxy Servers \(IP PORT\) - Hide My Ass!](https://www.google.com/search?q=Free+Proxy+Servers&source=lnms&sa=X&ei=wBkMU7G6NaaZiAeR14CoBA&ved=0CAgQ_AUoAA&biv)
https://hidemyass.com/proxy-list/ ▾
50+ items - Free proxy list index; the largest real-time database of public ...
Last update: IP address Country
4 minutes 19. 19. 25. 313636. 36. 4143435055. 92. 114. 114 ... flag KENYA.
11 minutes 180.303088180.11. 11. 17. 17. 20. 20. 2328. 28 ... flag Thailand.
- [Free Proxy Servers - Protect Your Online Privacy with Our Proxy List](https://www.google.com/search?q=Free+Proxy+Servers&source=lnms&sa=X&ei=wBkMU7G6NaaZiAeR14CoBA&ved=0CAgQ_AUoAA&biv)
www.proxy4free.com/ ▾
Proxy 4 Free is a free proxy list and proxy checker providing you with the best free proxy servers for over 10 years. Our sophisticated checking system measures ...
Proxy List - Country - Rating - Domain
- [List of Free Proxy Servers - Page 1 of 11 - Proxy 4 Free](https://www.google.com/search?q=Free+Proxy+Servers&source=lnms&sa=X&ei=wBkMU7G6NaaZiAeR14CoBA&ved=0CAgQ_AUoAA&biv)
www.proxy4free.com/list/webproxy1.html ▾
The best list of working and continuously checked proxy servers - page 1 of 11.
- [Top Free Anonymous Web Proxy Servers - Wireless / Networking](https://www.google.com/search?q=Free+Proxy+Servers&source=lnms&sa=X&ei=wBkMU7G6NaaZiAeR14CoBA&ved=0CAgQ_AUoAA&biv)
compnetworking.about.com/.../proxyserversandlists/... ▾ About.com ▾
by Bradley Mitchell
These sites support Web-based, free anonymous proxy servers. An anonymous Web proxy is an alternative to configuring HTTP or SOCKS proxies in the Web ...

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

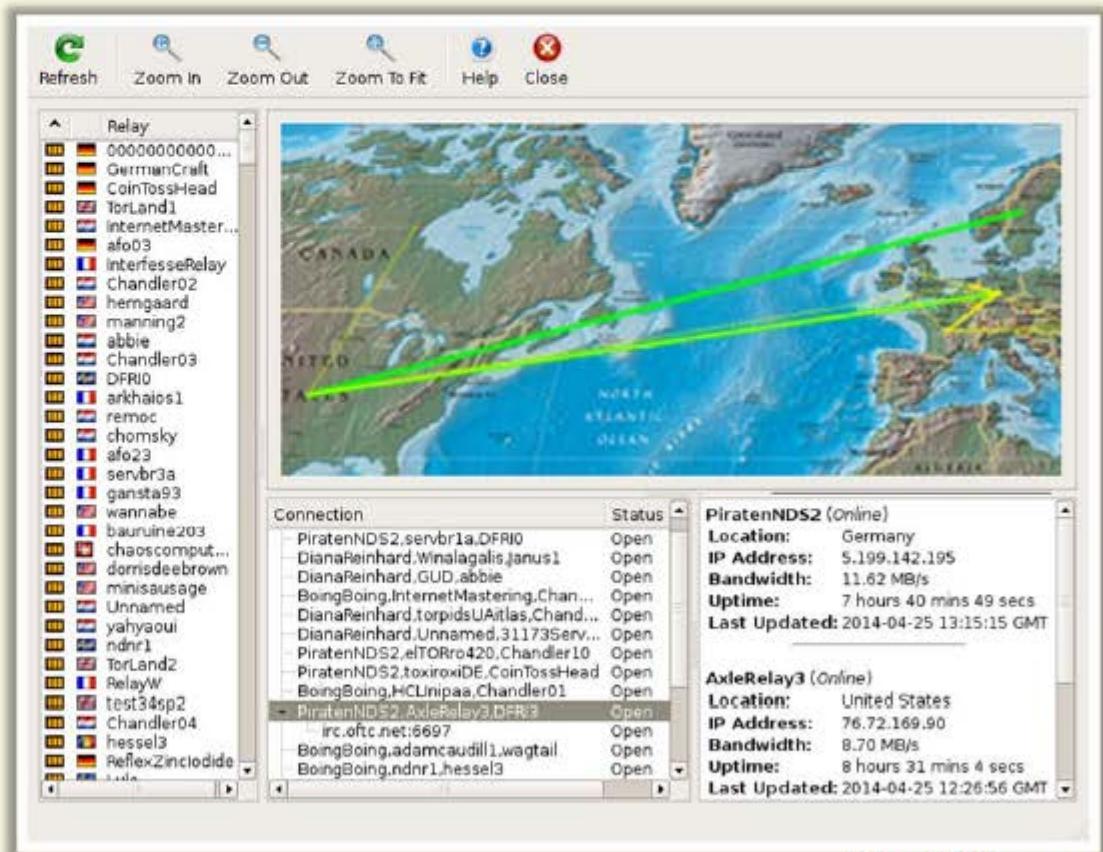
Censorship Circumvention Tool:Tails



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:

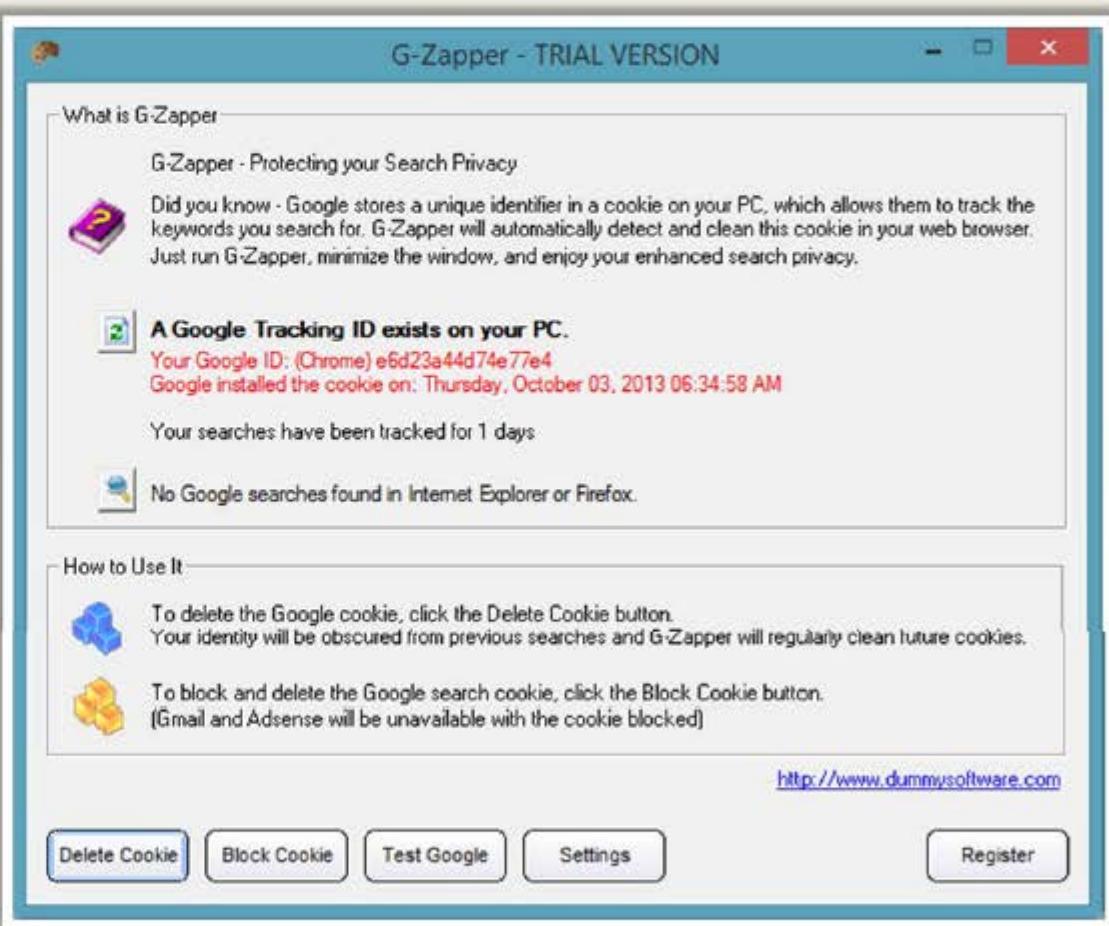
- Use the **Internet anonymously and circumvent censorship**
- Leave **no trace** on the computer
- Use **state-of-the-art cryptographic tools** to encrypt files, emails and instant messaging



<https://tails.boum.org>

G-Zapper

- 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



Proxy
<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

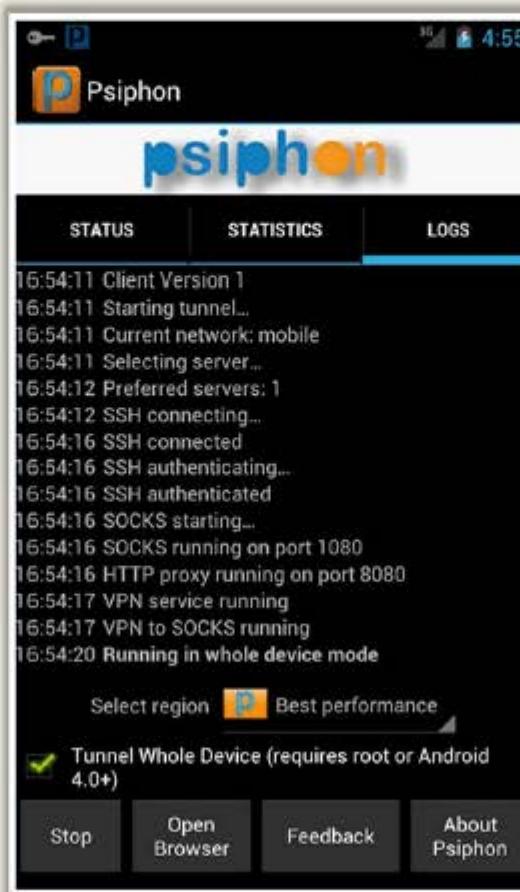
C|EH
Certified Ethical Hacker

Orbot



<https://guardianproject.info>

Psiphon



<https://s3.amazonaws.com>

OpenDoor



<https://itunes.apple.com>

Spoofing IP Address

CEH
Certified Ethical Hacker

- 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**



IP Spoofing Detection Techniques: Direct TTL Probes

CEH
Certified Ethical Hacker

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

CEH
Certified Ethical Hacker

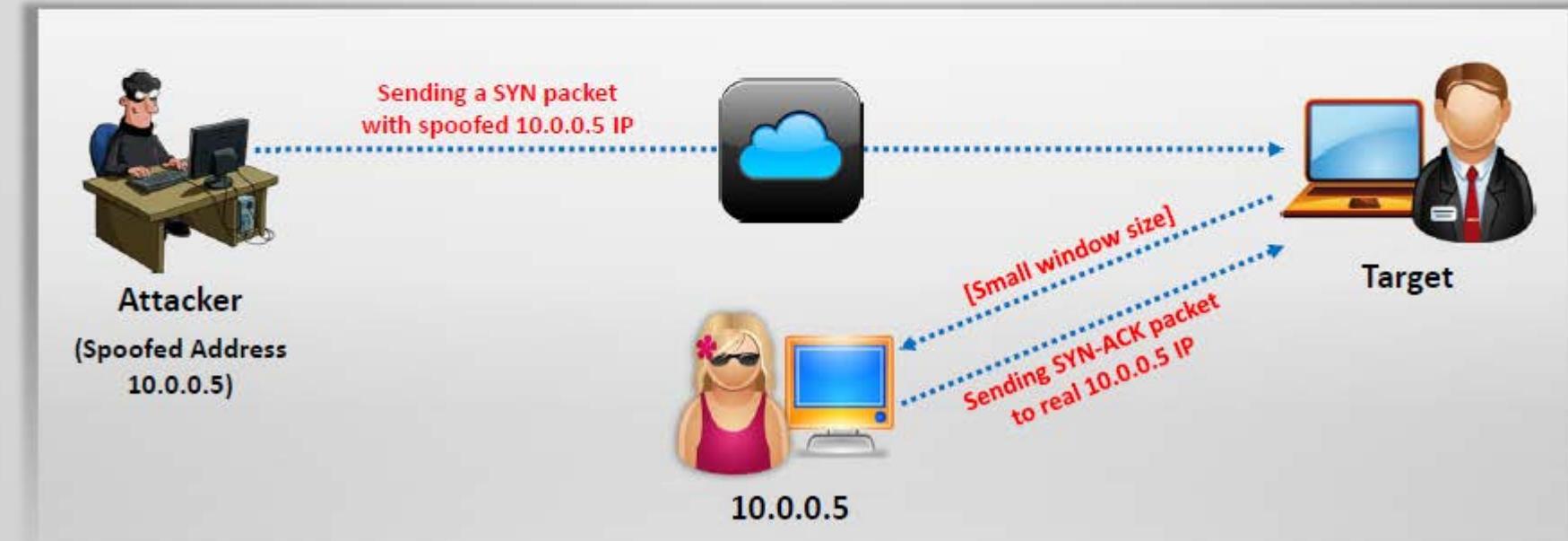
- 01** Send probe to host of suspect spoofed traffic that triggers reply and **compare IP ID** with suspect traffic
- 02** If IP IDs are **not in the near value** of packet being checked, suspect traffic is spoofed
- 03** This technique is successful even if the attacker is in the **same subnet**



IP Spoofing Detection Techniques: TCP Flow Control Method

CEH
Certified Ethical Hacker

- 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



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

Use multiple firewalls providing multi-layered depth of protection

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

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

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

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

CEH Scanning Methodology

CEH
Certified Ethical Hacker

Check for Live Systems



Check for Open Ports



Scanning Beyond IDS



Banner Grabbing

Scan for Vulnerability



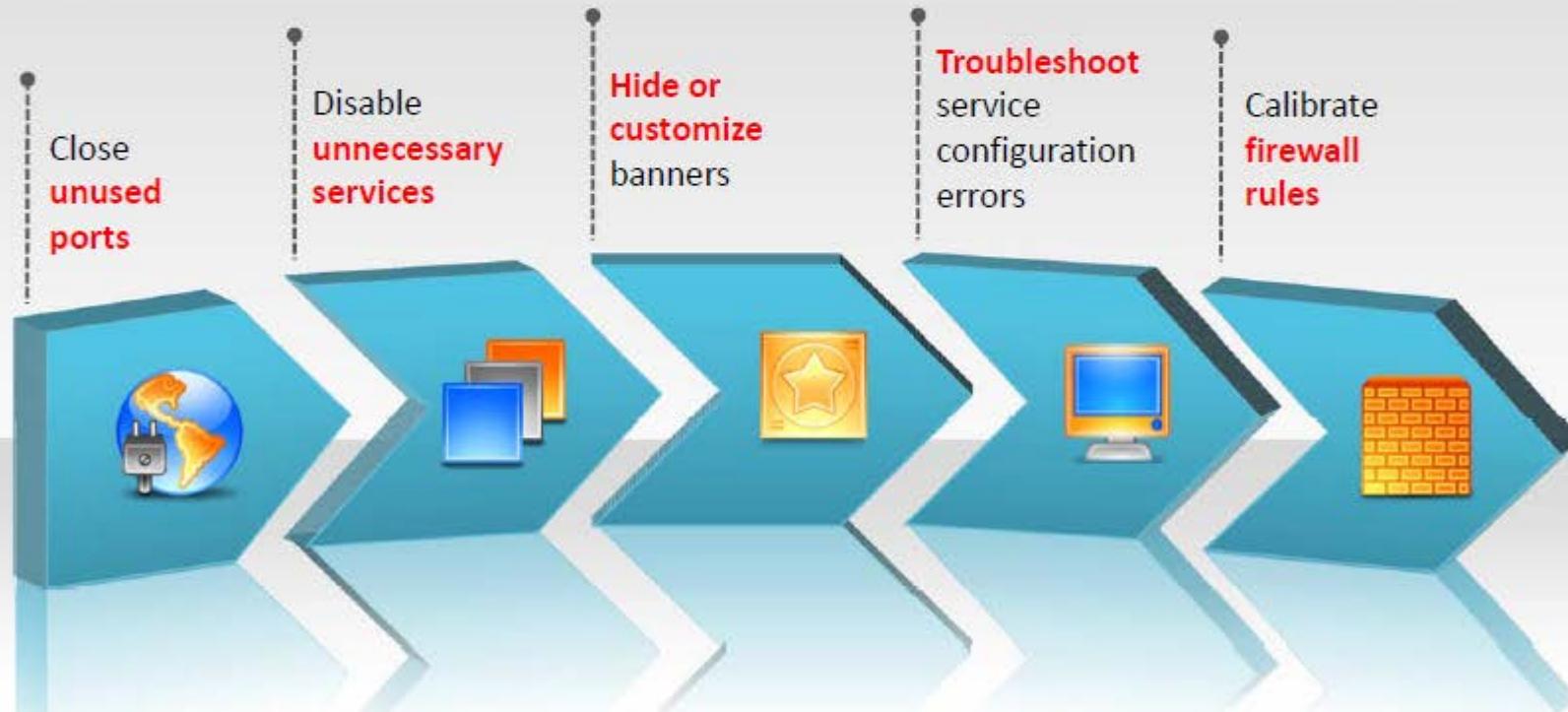
Prepare Proxies

Draw Network Diagrams

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)

CEH
Certified Ethical Hacker

Draw network diagrams

Use tools such as Network Topology Mapper, 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 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