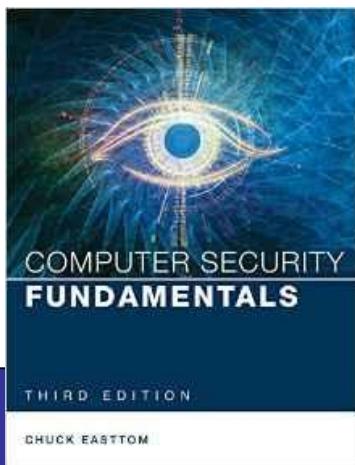


Computer Security Fundamentals

by Chuck Easttom



Chapter 11 Network Scanning and Vulnerability Scanning

Chapter 11 Objectives

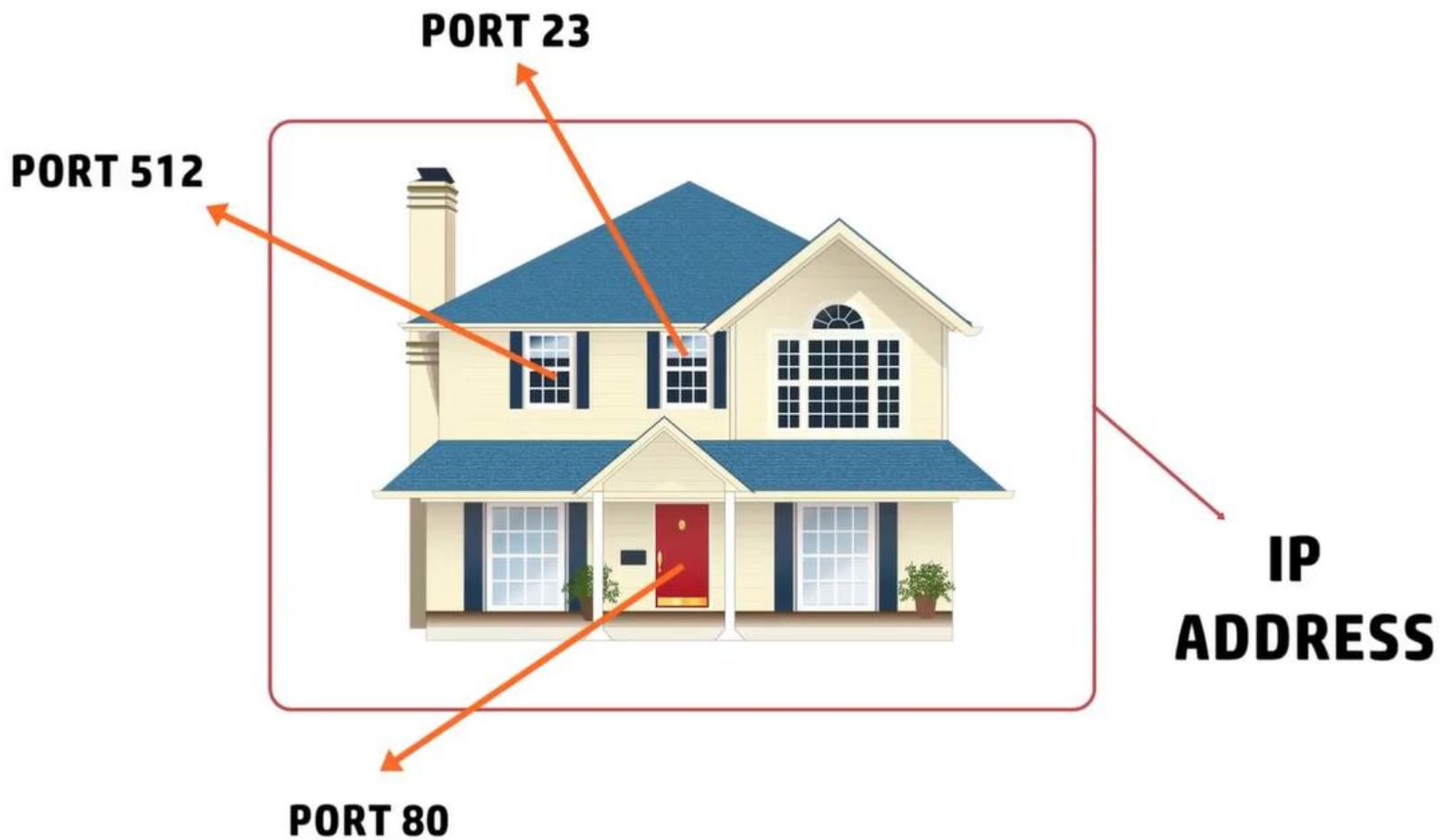
- Understand how to secure a system
- Probe a system for vulnerabilities
- Use Vulnerability vulnerability scanning tools
- Evaluate potential security consultants

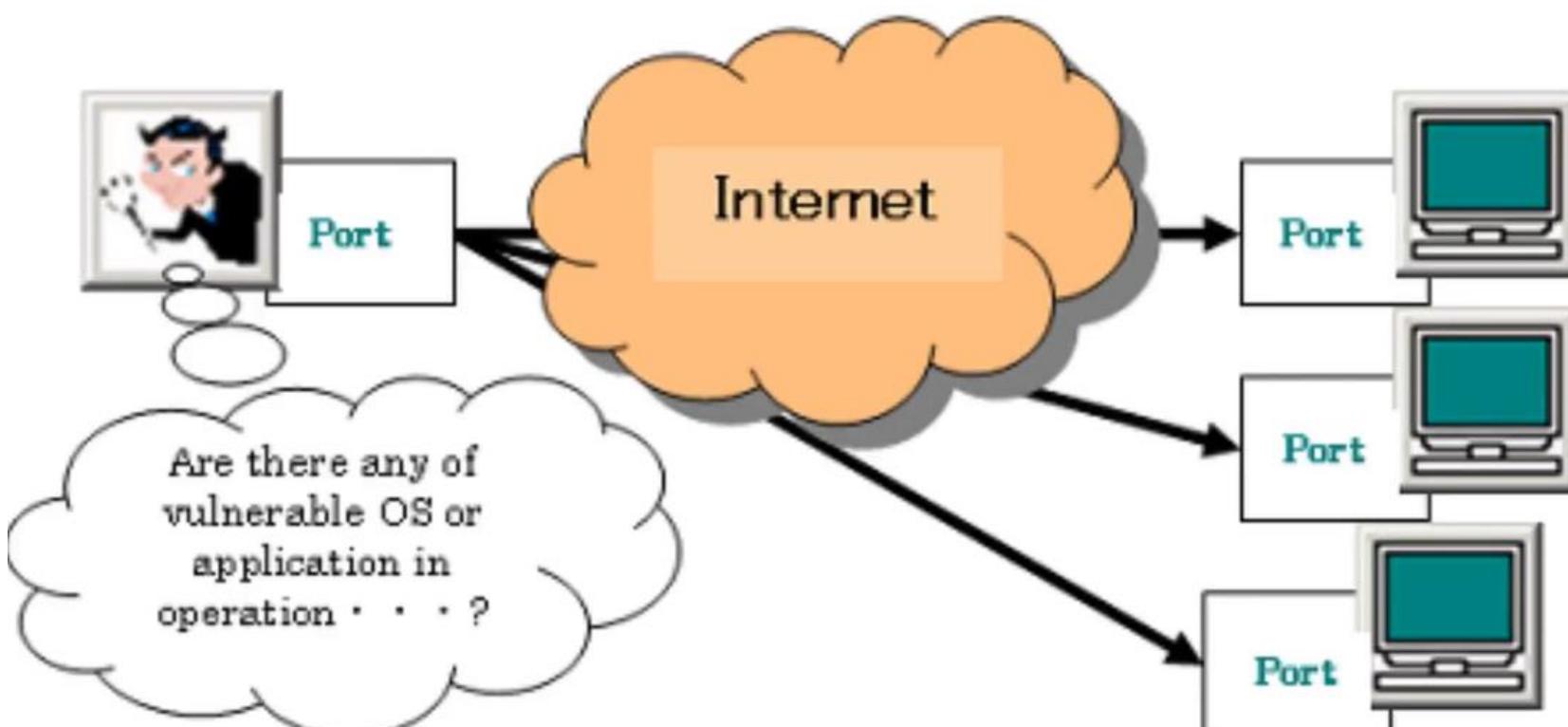
Introduction

- Secure the system.

Basics of Security

- **Patch:** A modification to a program to improve its security, performance, or other feature.
 - Critical, Recommended, and optional
 - Updated, read me, compatible
- **Ports:** virtual places within an operating system where network connections start and end.
- **Protect:** software, firewalls, IDS, IPS, virus scanner, update regularly
- **Policies:** software installation, attachments,, code word, data access, backup password, disaster recovery plan, employee termination
- **Probe:** A small utility program that is used to investigate, or test, the status of a system, network or website. Relative to computer security in a network, a probe is an attempt to gain access to a computer and its files through a known or probable weak point in the computer system
- **Physical:** Old backup tapes should be destroyed before disposal, access to routers and hubs, fire-resistant room





Overview of Network Scanning

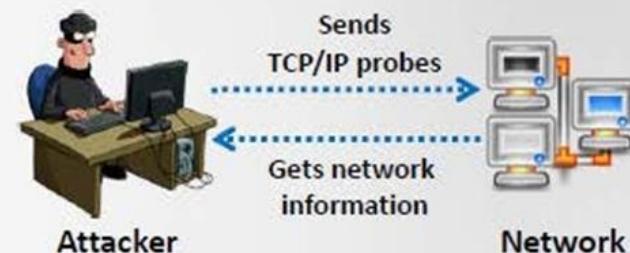
01

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

Network Scanning Process



Objectives of Network Scanning

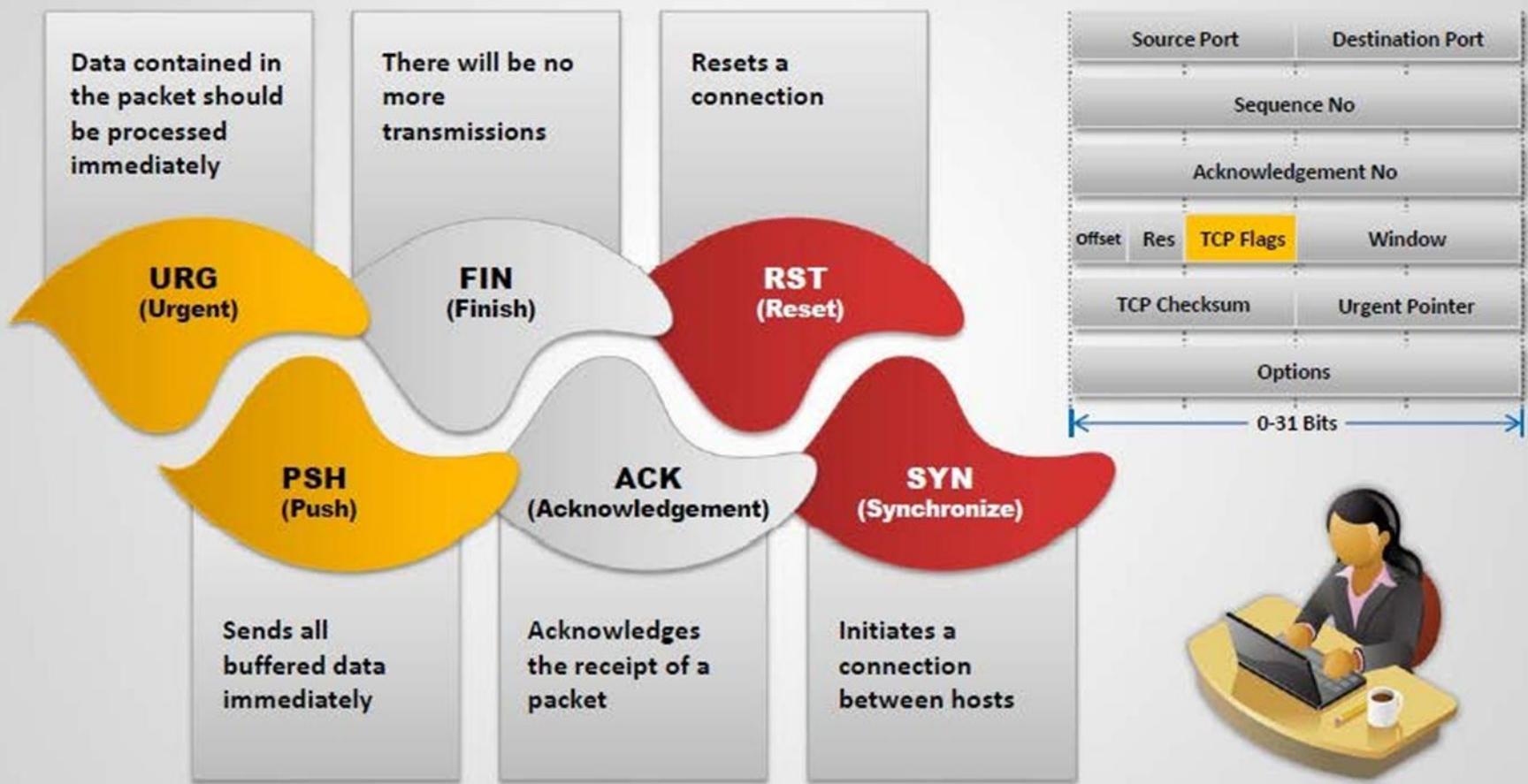
To discover live hosts, IP address, and open ports of live hosts

To discover operating systems and system architecture

To discover services running on hosts

To discover vulnerabilities in live hosts

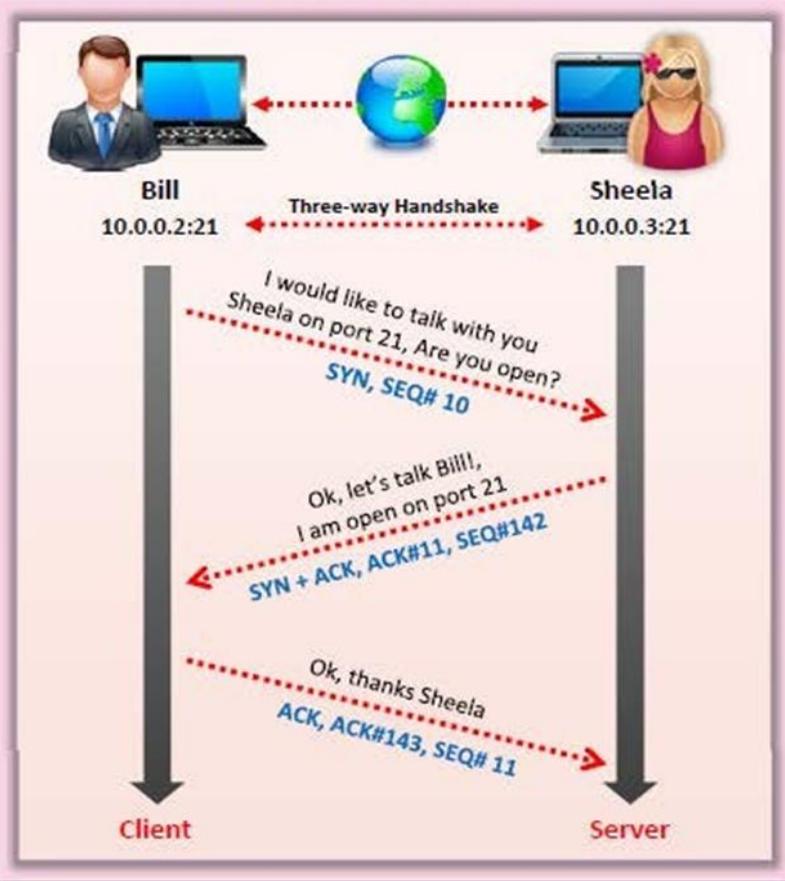
TCP Communication Flags



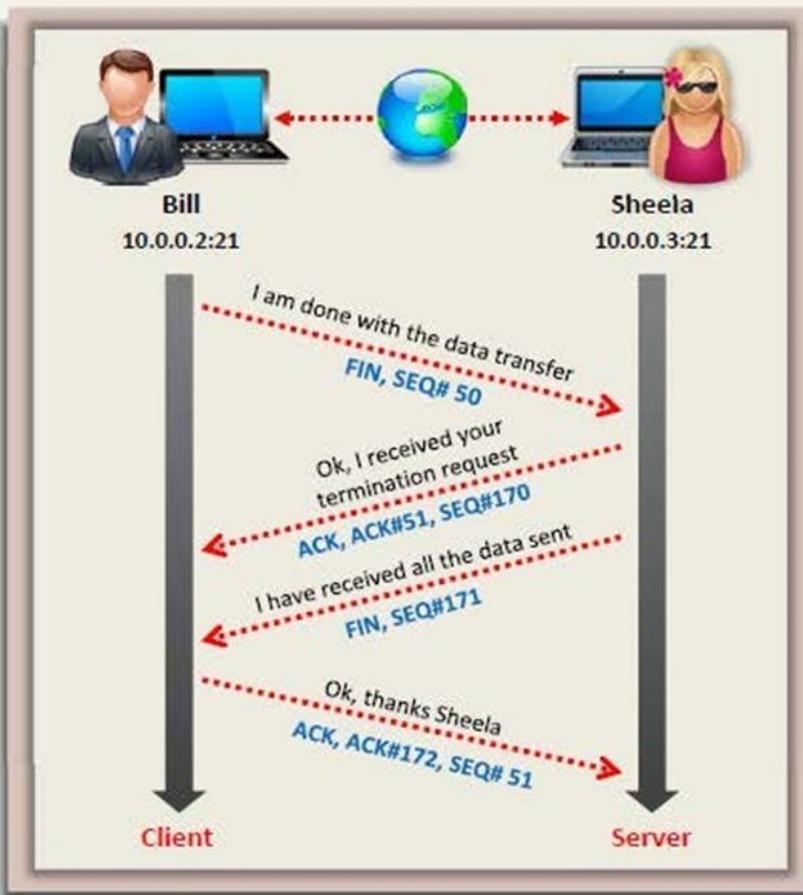
Standard TCP communications are controlled by flags in the TCP packet header

TCP/IP Communication

TCP Session Establishment
(Three-way Handshake)



TCP Session Termination



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

The image displays two side-by-side screenshots of the Zenmap graphical user interface. Both windows show the same scan command: `nmap -p 1-65535 -T4 -A -v -p 1-65535 -A -v 192.168.168.5`. The left window shows the initial scan progress, while the right window shows the completed scan output.

Left Window (Scan Progress):

```
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 8000/tcp on 192.168.168.5
Discovered open port 8888/tcp on 192.168.168.5
Discovered open port 507/tcp on 192.168.168.5
Discovered open port 135/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 138/tcp on 192.168.168.5
Discovered open port 443/tcp on 192.168.168.5
Discovered open port 8881/tcp on 192.168.168.5
SYN Stealth Scan Timing: About 2.27s done; ETC: 13:20
(0:23:42 remaining)
```

Right Window (Scan Output):

```
not shown: bbrvvv-timedout 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-ns?
82/tcp    open  xfer?
110/tcp   open  pop3?
115/tcp   open  nntt?
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  skype2           Skype
|_http-title: Site doesn't have a title.
445/tcp   open  netbios-ssn
465/tcp   open  smtp?
|_smtp-commands: Couldn't establish connection on port
465
563/tcp   open  snews?
587/tcp   open  submission?
|_smtp-commands: Couldn't establish connection on port
587
912/tcp   open  vnc-auth        VMware Authentication Daemon 1.0 (Uses VNC, SOAP)
993/tcp   open  imaps?
```

<http://nmap.org>

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**

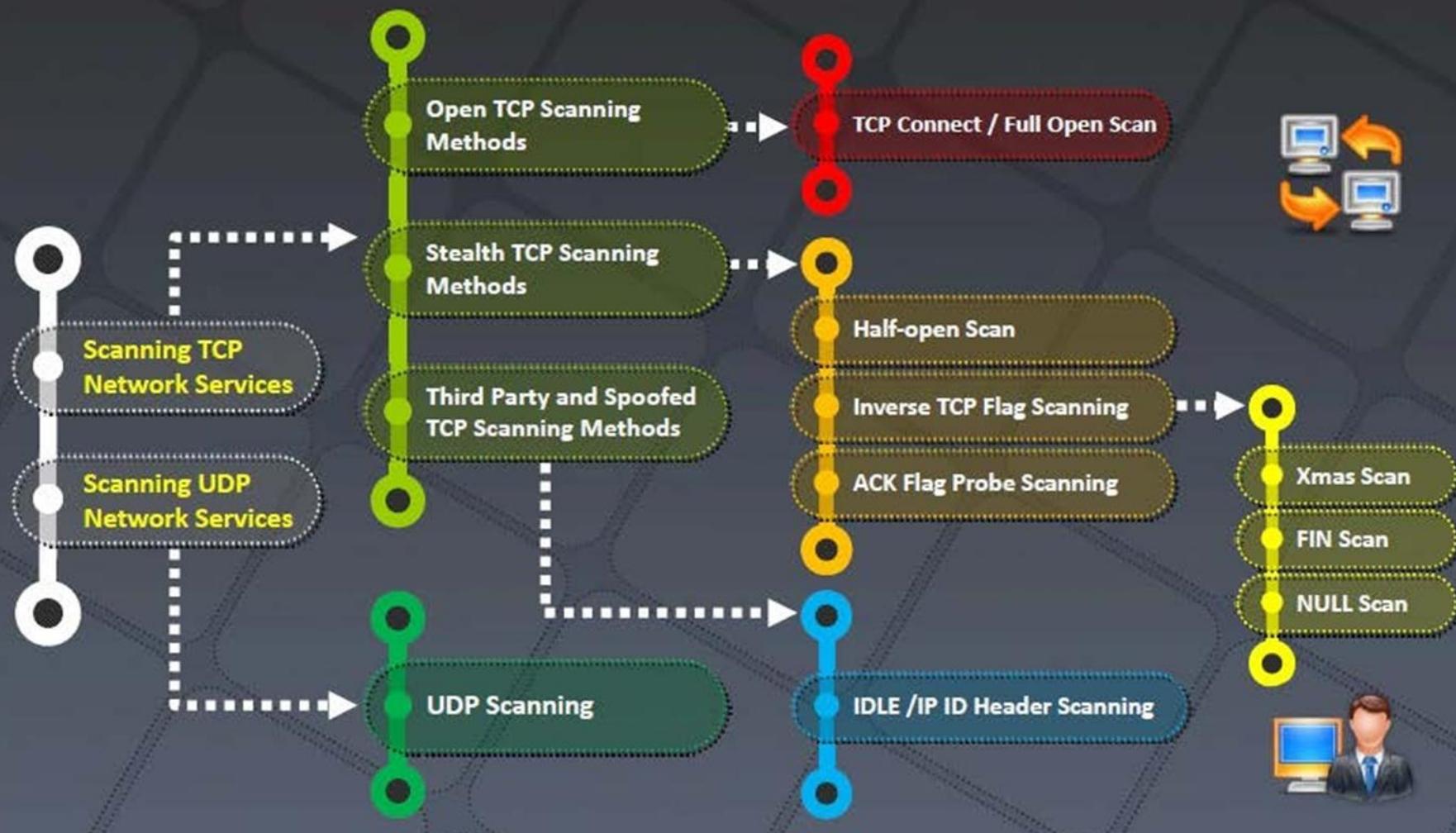


The ping scan output using Nmap:

The screenshot shows the Zenmap graphical user interface for Nmap. The "Scan" tab is selected, with the target set to "192.168.168.5" and the profile set to "Ping scan". The command entered is "nmap -sn 192.168.168.5". The "Nmap Output" tab displays the results of the scan:
Starting Nmap 6.40 (http://nmap.org) at 2013-10-03
10:53 Pacific Daylight Time
Nmap scan report for 192.168.168.5
Host is up (0.0010s latency).
Nmap done: 1 IP address (1 host up) scanned in 0.17 seconds

<http://nmap.org>

Scanning Techniques



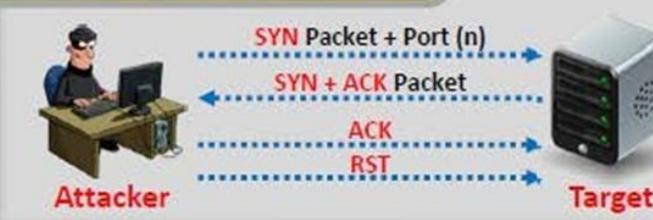
TCP Connect / Full Open Scan

> 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

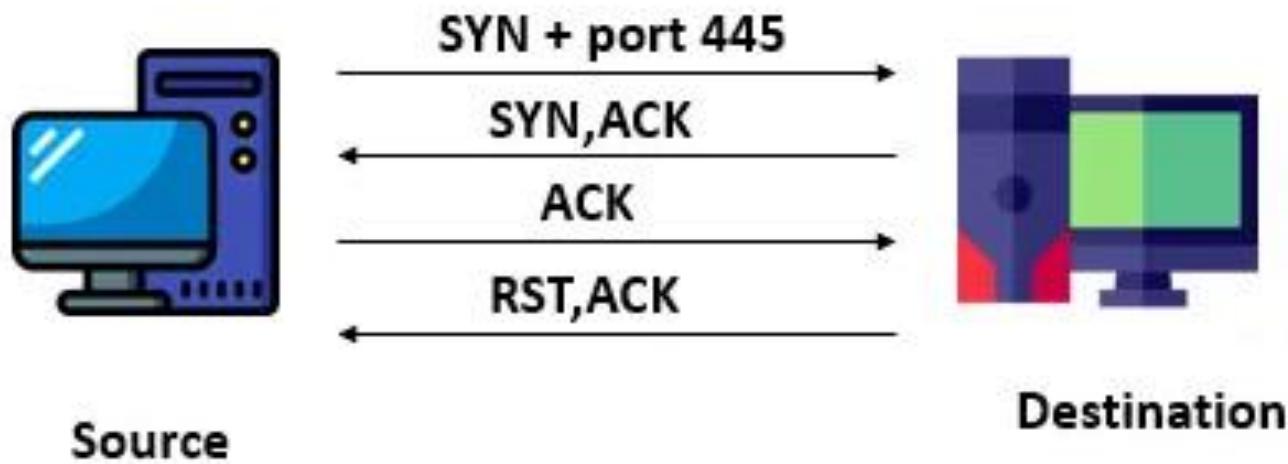


A screenshot of the Zenmap interface. The target is set to nmap 192.168.0.97. The command is # -sT -v nmap 192.168.0.97. The output window shows the results of the scan:

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 10:33 (EDT)
Initiating ARP Ping Scan at 10:33
Scanning 192.168.0.97 [1 port]
Completed ARP Ping Scan at 10:33, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host at 10:33
Completed Parallel DNS resolution of 1 host at 10:33, 0.03s elapsed
Initiating Connect Scan at 10:33
Scanning 192.168.0.97 [1000 ports]
Discovered open port 587/tcp on 192.168.0.97
Discovered open port 130/tcp on 192.168.0.97
Discovered open port 130/tcp on 192.168.0.97
Discovered open port 110/tcp on 192.168.0.97
Discovered open port 110/tcp on 192.168.0.97
Discovered open port 445/tcp on 192.168.0.97
Discovered open port 25/tcp on 192.168.0.97
Discovered open port 993/tcp on 192.168.0.97
Discovered open port 995/tcp on 192.168.0.97
Discovered open port 460/tcp on 192.168.0.97
Connect Scan Timing: About 47.3% done. ETC: 10:34 (0:00:34 remaining)
Discovered open port 21/tcp on 192.168.0.97
Discovered open port 21/tcp on 192.168.0.97
Completed Connect Scan at 10:34, 62.34s elapsed (1000 total ports)
Nmap scan report for 192.168.0.97
Failed to resolve "nmap".
Host is up (0.0003s latency).
Not shown: 980 filtered ports
PORT      STATE SERVICE
25/tcp    open  smtp
130/tcp   open  pop3
130/tcp   open  smtp
587/tcp   open  https
445/tcp   open  microsoft-ds
460/tcp   open  https
563/tcp   open  snews
587/tcp   open  submission
993/tcp   open  imaps
995/tcp   open  pop3s
MAC Address: 00:0C:29 (Dell)
```

- TCP scan will scan for TCP port like port 22, 21, 23, 445 etc and ensure for listening port (open) through 3-way handshake connection between the source and destination port. If the port is open then source made request with **SYN** packet, a response destination sent **SYN, ACK** packet and then source sent **ACK** packets, at last source again sent **RST, ACK** packets.

TCP SCAN For Open Port



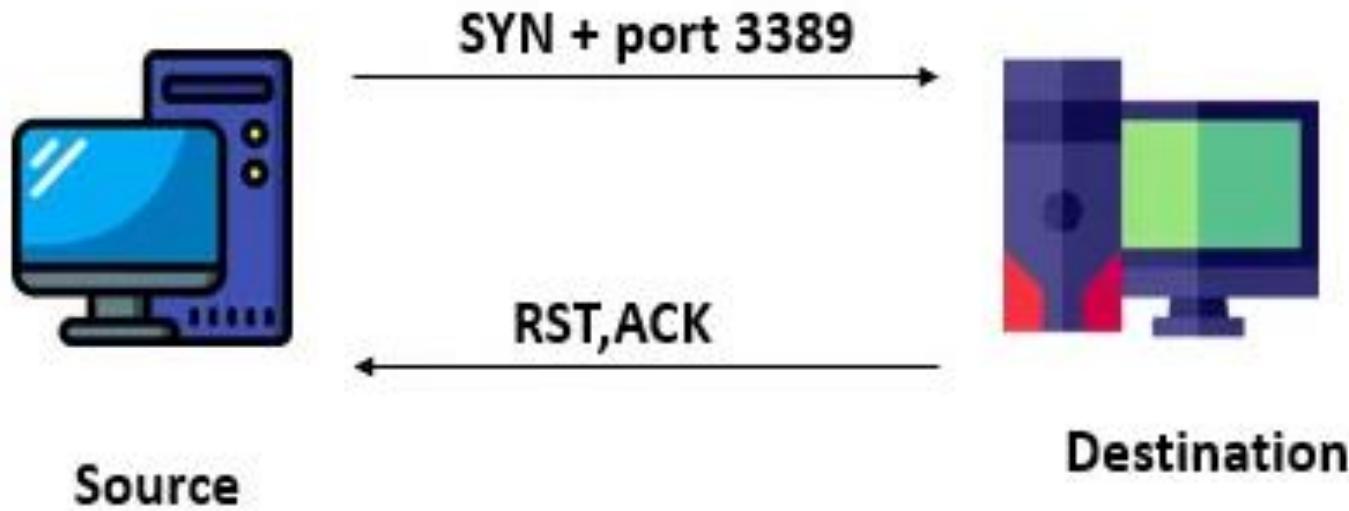
```
[root@kali ~]# nmap -sT -p 445 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:41 IST
Nmap scan report for 192.168.43.251
Host is up (0.00046s latency).

PORT      STATE SERVICE
445/tcp    open  microsoft-ds
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.16 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
12	1.358984503	192.168.43.72	192.168.43.57	TCP	... 52378 → 445	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=0
13	1.359264678	192.168.43.57	192.168.43.72	TCP	... 445 → 52378	[SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
14	1.359285119	192.168.43.72	192.168.43.57	TCP	... 52378 → 445	[ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=16691280
15	1.359322559	192.168.43.72	192.168.43.57	TCP	... 52378 → 445	[RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=16691280

TCP SCAN For Close Port



```
[root@kali ~]# nmap -sT -p 3389 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:42 IST
Nmap scan report for 192.168.43.251
Host is up (0.00021s latency).

PORT      STATE    SERVICE
3389/tcp  closed   ms-wbt-server
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.14 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
9	1.370541629	192.168.43.72	192.168.43.57	TCP	... 35780 → 3389	[SYN] Seq=0 Win=64
10	1.370780489	192.168.43.57	192.168.43.72	TCP	... 3389 → 35780	[RST, ACK] Seq=1

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

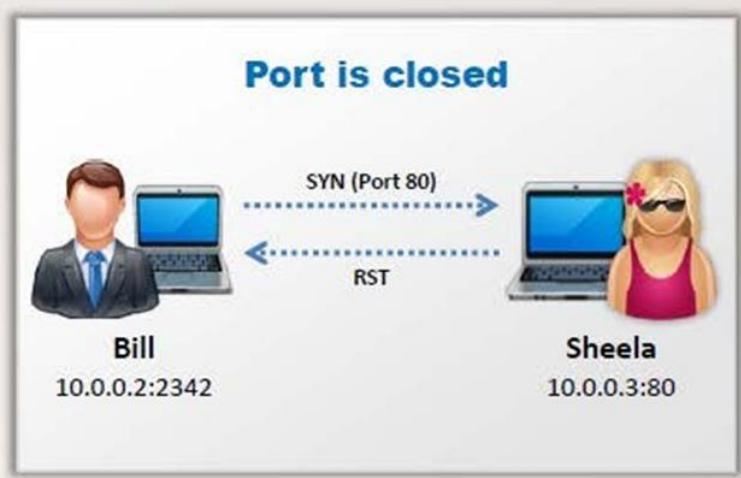
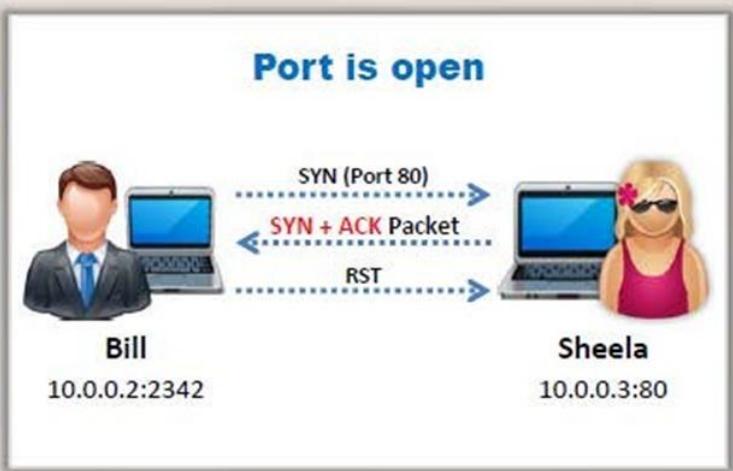
02

If the server responds with an **RST** packet, then the remote port is in the "closed" state

03

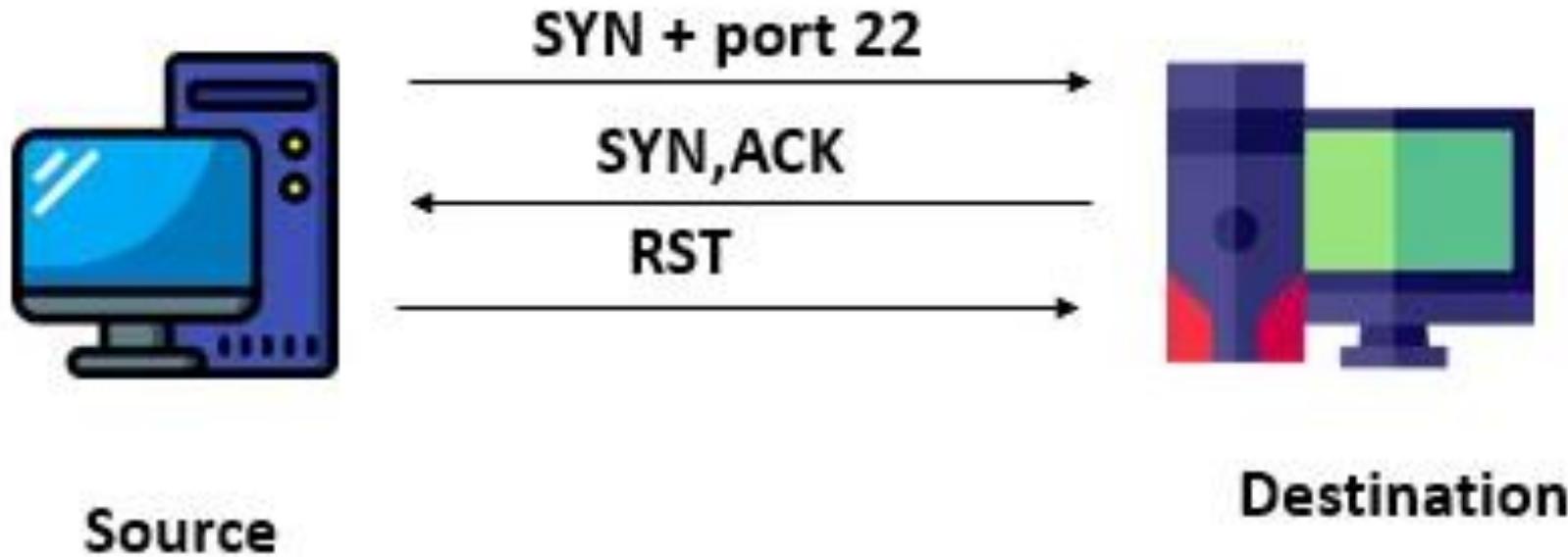
The client sends the **RST** packet to close the initiation before a connection can ever be established

04



- SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively typical and stealthy since it never completes TCP connections.

Stealth SCAN For Open Port



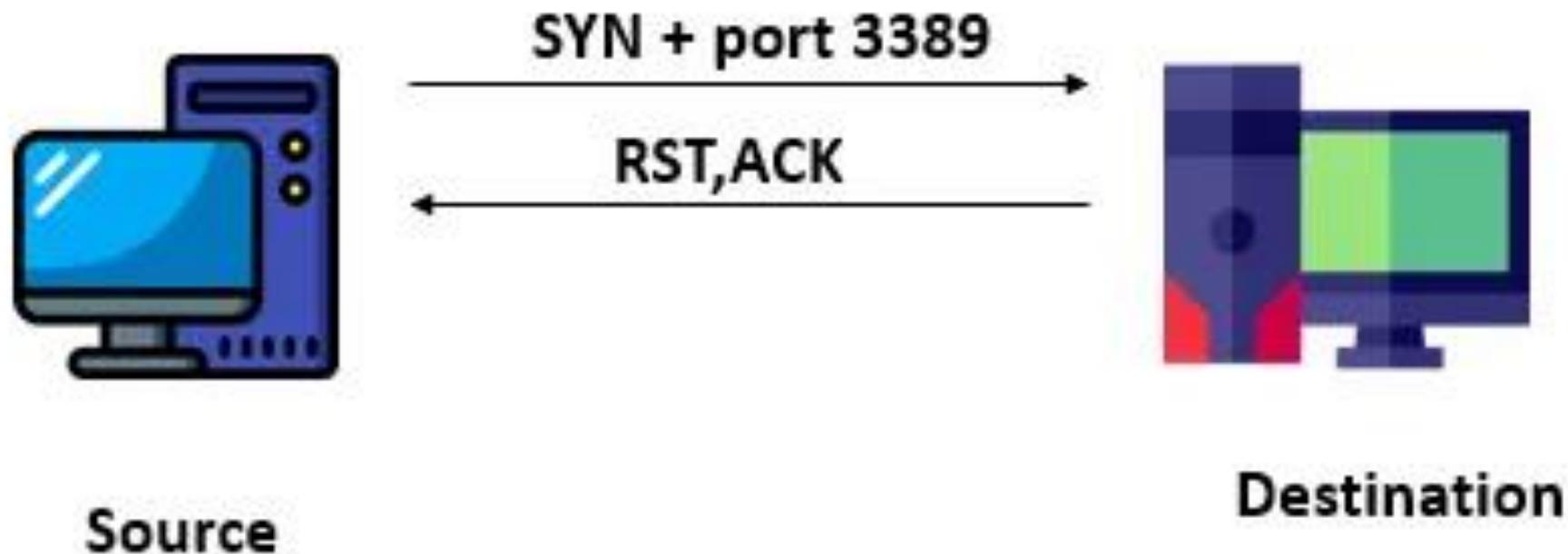
```
(root💀 kali)-[~/home/sam]
# nmap -sS -p 22 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 10:50 IST
Nmap scan report for 192.168.43.251
Host is up (0.00027s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.25 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
5	0.104038454	192.168.43.72	192.168.43.251	TCP	... 51002 → 22 [SYN]	Seq=0 Win=1024 Len=0 MSS=1460
6	0.104226127	192.168.43.251	192.168.43.72	TCP	... 22 → 51002 [SYN, ACK]	Seq=0 Ack=1 Win=5840 Len=0 MSS=1460
7	0.104246121	192.168.43.72	192.168.43.251	TCP	... 51002 → 22 [RST]	Seq=1 Win=0 Len=0

Stealth SCAN For Close Port



```
[root💀 kali)-[~/home/sam]
# nmap -sS -p 3389 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:44 IST
Nmap scan report for 192.168.43.251
Host is up (0.00023s latency).

PORT      STATE    SERVICE
3389/tcp  closed   ms-wbt-server
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
[9 0.902740974	192.168.43.72	192.168.43.57	TCP	... 35790 → 3389	[SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PEE
]	10 0.903003842	192.168.43.57	192.168.43.72	TCP	... 3389 → 35790	[RST, ACK] Seq=1 Ack=1 Win=0 Len=0

Fin Scan

- A FIN packet is used to terminate the TCP connection between the source and destination port typically after the data transfer is complete. In the place of an SYN packet, Nmap starts a FIN scan by using a FIN packet. If the port is open then no response will come from destination port when FIN packet is sent through source port.

FIN SCAN For Open Port



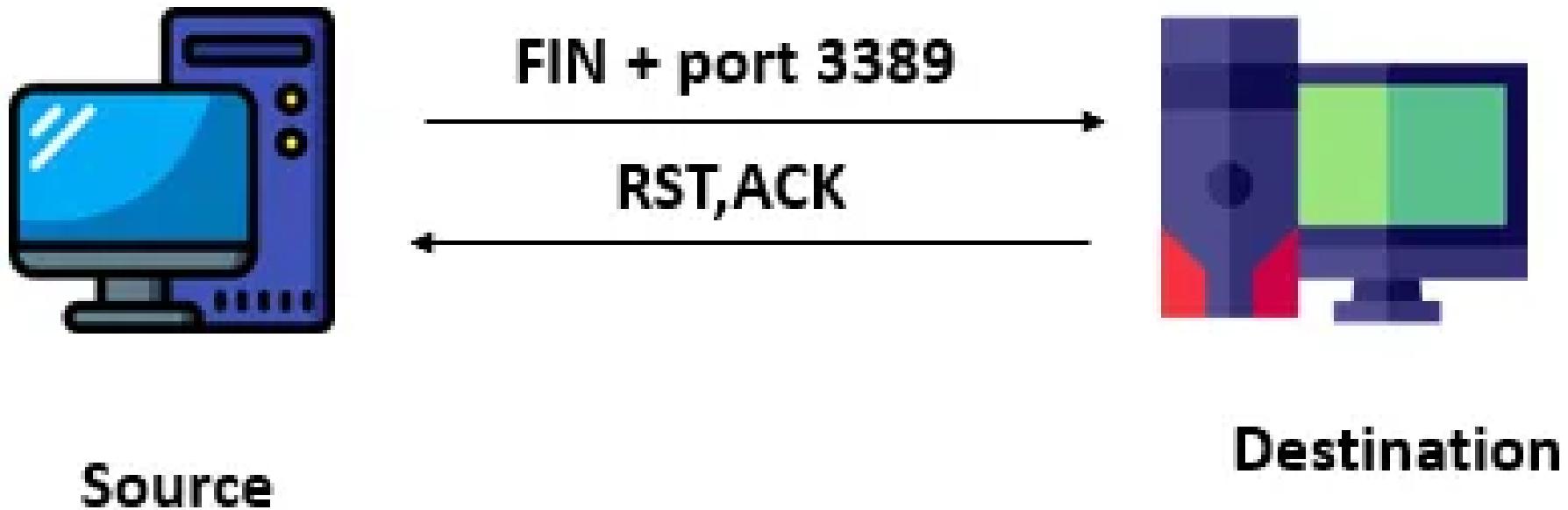
```
[root@kali ~]# nmap -sF -p 22 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 10:55 IST
Nmap scan report for 192.168.43.251
Host is up (0.00020s latency).

PORT      STATE            SERVICE
22/tcp     open|filtered  ssh
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
5	0.080044712	192.168.43.72	192.168.43.251	TCP	22	[FIN] Seq=1 Win=1024 Len=0
6	0.180235589	192.168.43.72	192.168.43.251	TCP	22	[FIN] Seq=1 Win=1024 Len=0

FIN SCAN For Close Port



```
[root💀 kali㉿home/sam]# nmap -sF -p 3389 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:46 IST
Nmap scan report for 192.168.43.251
Host is up (0.00022s latency).

PORT      STATE SERVICE
3389/tcp  closed ms-wbt-server
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.24 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
7	0.926323539	192.168.43.72	192.168.43.57	TCP	0	41794 → 3389 [FIN] Seq=1 Win=1024 Len=0
8	0.926555834	192.168.43.57	192.168.43.72	TCP	0	3389 → 41794 [RST, ACK] Seq=1 Ack=2 Win=0 Len=0

Null Scan

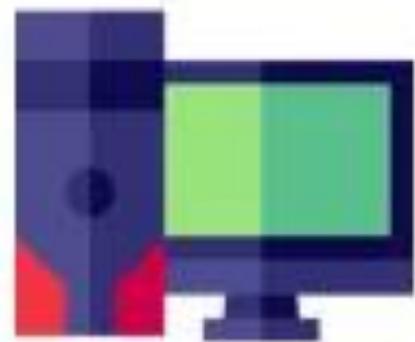
- A Null Scan is a series of TCP packets which hold a sequence number of “zeros” (0000000) and since there are none flags set, the destination will not know how to reply the request. It will discard the packet and no reply will be sent, which indicate that the port is open.

NULL SCAN For Open Port



Source

No flag + port 22



Destination

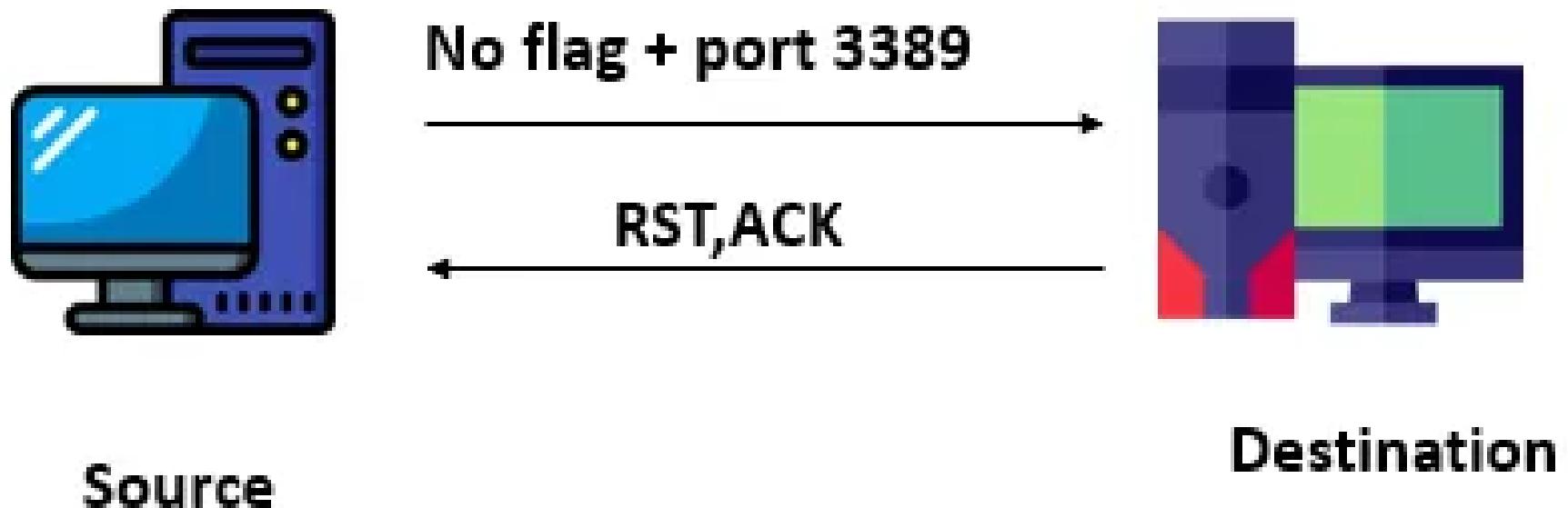
```
[root@kali ~]# nmap -sN -p 22 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 10:58 IST
Nmap scan report for 192.168.43.251
Host is up (0.00028s latency).

PORT      STATE            SERVICE
22/tcp     open|filtered  ssh
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.43 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
5	0.108069705	192.168.43.72	192.168.43.251	TCP	... 53503 → 22 [<None>]	Seq=1 Win=1024 Len=0
6	0.208258705	192.168.43.72	192.168.43.251	TCP	... 53504 → 22 [<None>]	Seq=1 Win=1024 Len=0

NULL SCAN For Close Port



```
(root💀 kali)-[~/home/sam]
# nmap -sN -p 3389 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:48 IST
Nmap scan report for 192.168.43.251
Host is up (0.00021s latency).

PORT      STATE SERVICE
3389/tcp  closed ms-wbt-server
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Lif	Info
7	0.491016626	192.168.43.72	192.168.43.57	TCP	—	57455 → 3389 [<None>] Seq=1 Win=1024 Len=0
8	0.491215043	192.168.43.57	192.168.43.72	TCP	—	3389 → 57455 [RST, ACK] Seq=1 Ack=1 Win=0 Len=0

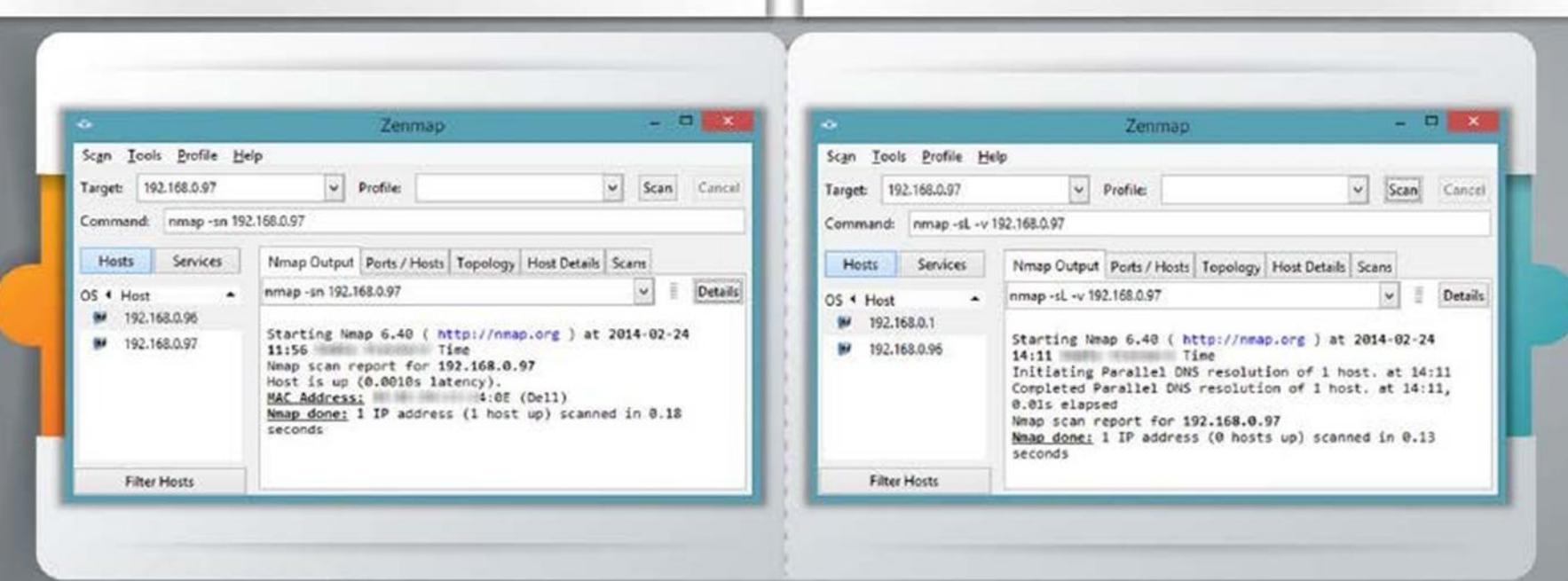
ICMP Echo Scanning/List Scan

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



UDP Scanning



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

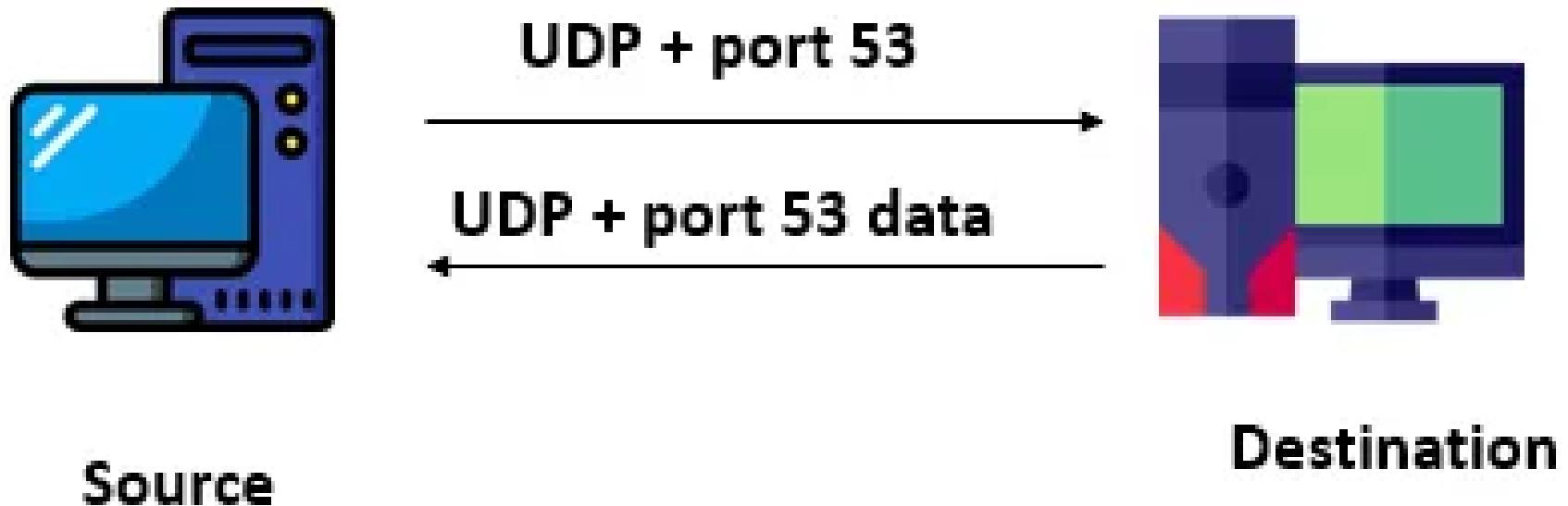
- If a UDP packet is sent to closed port, the system responds with **ICMP port unreachable message**
- Spywares, Trojan horses**, and other malicious applications use UDP ports

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 11:14
[INFO] Platform: Win7SP1; OS CPE: cpe:/o:microsoft:windows_7::sp1
[INFO] Hostscript results:
[INFO] OS detection results:
[INFO] Nmap done: 1 IP address (1 host up) scanned in 11.29 seconds
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 (306B)
```

UDP Scan

- UDP scan works by sending a UDP packet to every destination port; it is a connectionless protocol. For some common ports such as 53 and 161, a protocol-specific payload is sent to increase the response rate, a service will respond with a UDP packet, proving that it is open. If no response is received after retransmissions, the port is classified as open|filtered. This means that the port could be open, or perhaps packet filters are blocking the communication

UDP SCAN For Open Port



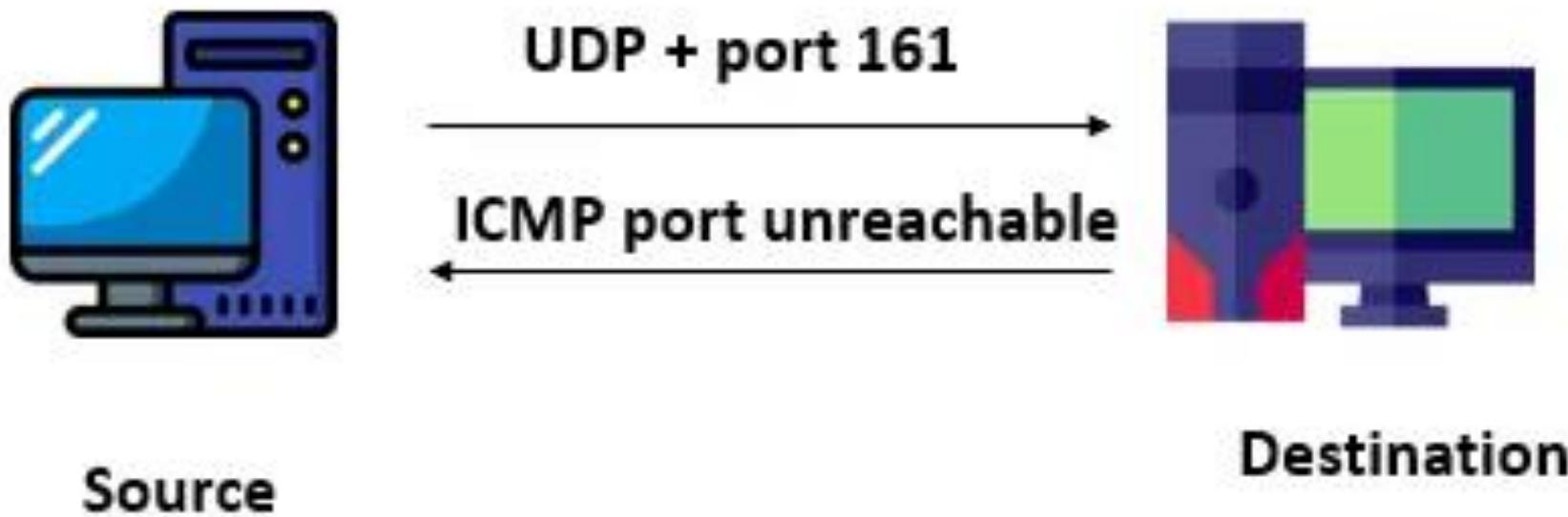
```
[root@kali ~]# nmap -sU -p 53 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:31 IST
Nmap scan report for 192.168.43.251
Host is up (0.00025s latency).

PORT      STATE SERVICE
53/udp    open  domain
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.23 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Lei	Info
7	0.768408172	192.168.43.72	192.168.43.251	DNS	...	Server status request 0x0000
8	0.768710896	192.168.43.251	192.168.43.72	DNS	...	Server status request response 0x0000 Not implemented
9	0.768738671	192.168.43.72	192.168.43.251	ICMP	...	Destination unreachable (Port unreachable)

UDP SCAN For Close Port



```
(root💀 kali)-[~/home/sam]
# nmap -sU -p 161 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:34 IST
Nmap scan report for 192.168.43.251
Host is up (0.00026s latency).

PORT      STATE SERVICE
161/udp    closed  snmp

MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.22 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
5	0.084085860	192.168.43.72	192.168.43.251	UDP	... 48513 → 161 Len=60	
6	0.084342161	192.168.43.251	192.168.43.72	ICMP	... Destination unreachable (Port unreachable)	

Xmas Scan

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

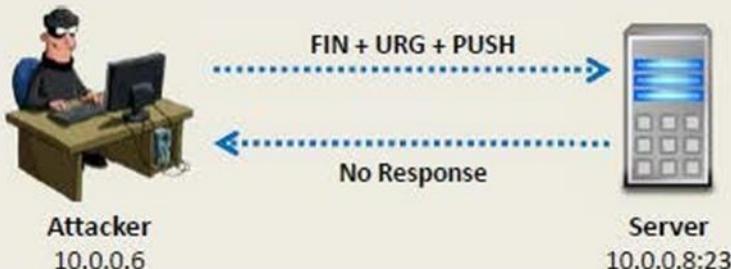
FIN scan works only with OSes with **RFC 793-based** TCP/IP implementation

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

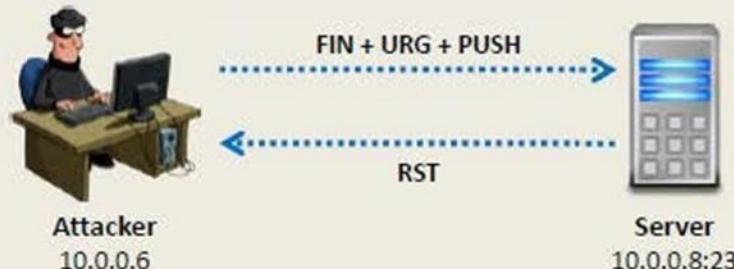
The screenshot shows the Zenmap interface with the target set to "nmap 192.168.0.97". The command entered is "# -sX -v nmap 192.168.0.97". The output window displays the results of the XMAS scan, including the start time, scanning process, and final report. The report indicates that port 192.168.0.97 is up and all scanned ports (1000) are open|filtered.

```
Starting Nmap 6.40 ( http://nmap.org ) at 2014-02-24 10:45
Initiating ARP Ping Scan at 10:45
Scanning 192.168.0.97 [1 port]
Completed 192.168.0.97 [1 port] (1 hosts up) (0 hosts down)
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 (0.000 latency).
All 1000 scanned ports on 192.168.0.97 are open|filtered
MAC Address: [REDACTED] (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: 2001 (80.026KB) | Rcvd: 1 (288)
```

Port is open



Port is closed

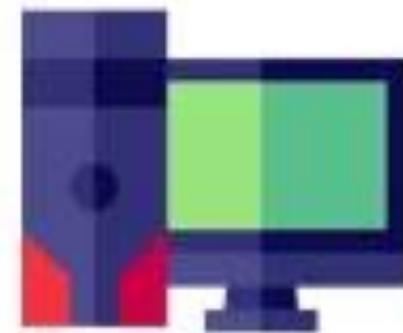


- These scans are designed to manipulate the PSH, URG and FIN flags of the TCP header, Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. When source sent FIN, PUSH, and URG packet to a specific port and if the port is open then destination will discard the packets and will not send any reply to the source.

XMAS SCAN For Open Port



FIN,PUSH,URG + port 22



Source

Destination

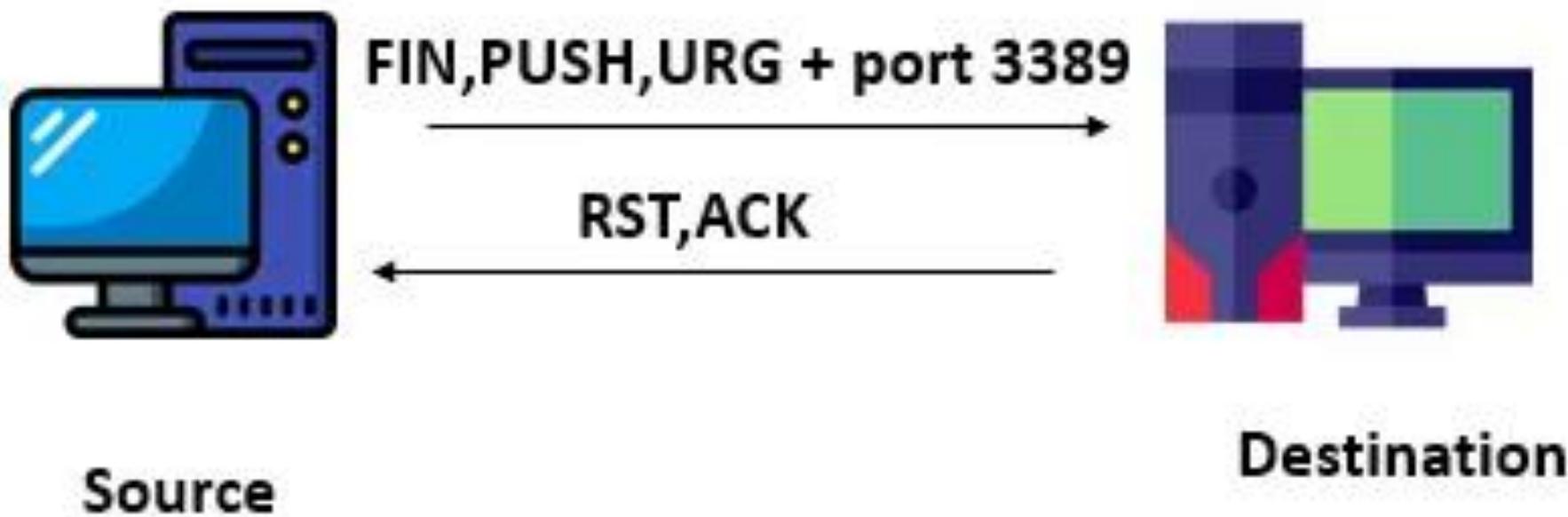
```
[root💀 kali)-[~/home/sam]
# nmap -sX -p 22 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:36 IST
Nmap scan report for 192.168.43.251
Host is up (0.00018s latency).

PORT      STATE            SERVICE
22/tcp    open|filtered  ssh
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.42 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
5	0.096346299	192.168.43.72	192.168.43.251	TCP	... 47529 → 22	[FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
6	0.196468463	192.168.43.72	192.168.43.251	TCP	... 47530 → 22	[FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0

XMAS SCAN For Close Port



```
(root💀kali㉿kali:[/home/sam]
# nmap -sX -p 3389 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:37 IST
Nmap scan report for 192.168.43.251
Host is up (0.00019s latency).

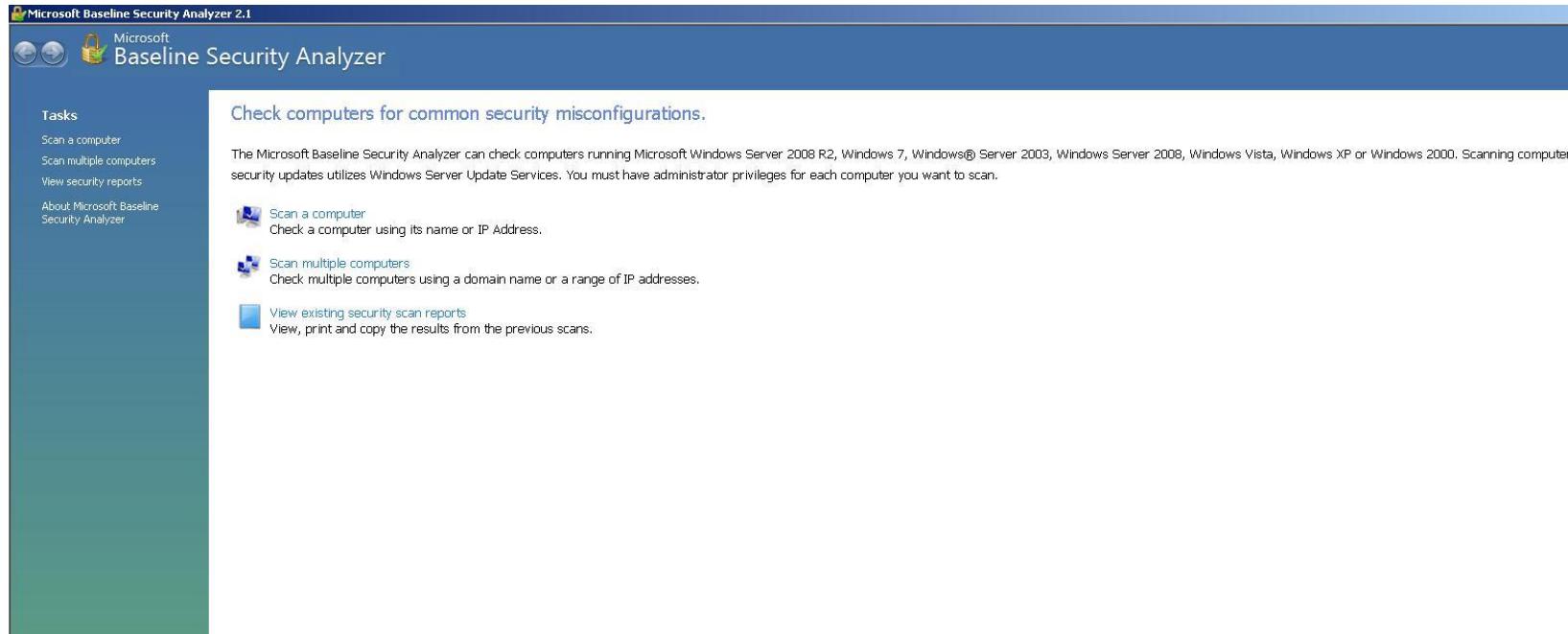
PORT      STATE    SERVICE
3389/tcp  closed   ms-wbt-server
MAC Address: 08:00:27:FF:32:FB (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.19 seconds
```

ip.addr == 192.168.43.72						
No.	Time	Source	Destination	Protocol	Len	Info
5	0.124081877	192.168.43.72	192.168.43.251	TCP	... 43495 → 3389	[FIN, PSH, URG] Seq=1 Win=1024 Urg=0 Len=0
6	0.124273063	192.168.43.251	192.168.43.72	TCP	... 3389 → 43495	[RST, ACK] Seq=1 Ack=2 Win=0 Len=0

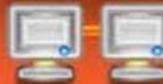
MBSA

■ Microsoft Baseline Security Analyzer



Vulnerability Scanning

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

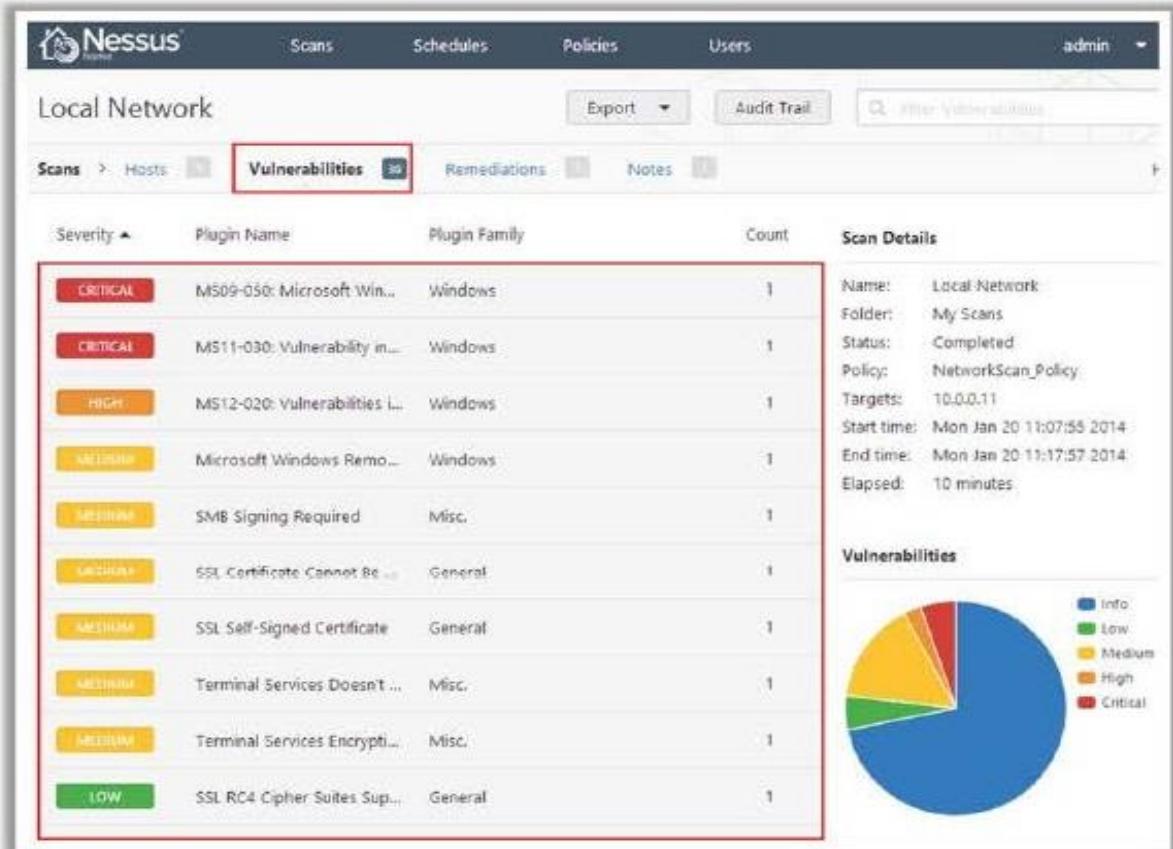


Vulnerability Scanning Tool: Nessus

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



Scan in Progress		Cancel scan	
http://www.rnatest.info/malware-demos-named/smoketest.htm			
	Vulnerability Scan		In progress
	Web Application Scan		In progress
	Malware Detection		In progress
 OWASP Scan		http://10.10.26.238	
Summary: 116 pages impacted 117 threats found		15 February 2013 at 09:00	
Threat summary: 264 vulnerabilities found			
Patch export summary: No patches available			
		View report >	
 SCAP Scan		10.10.30.32	
SCAP summary: 43 of 227 Rules		5 February 2013 at 06:58	
Not Compliant			
		View report >	
 Scan on 02/14/2013		10.10.26.238	
Summary: 203 vulnerabilities found		4 February 2013 at 16:43	
		View report >	
 SCAP scan on 02/14/2013		10.10.30.32	
SCAP summary: 43 of 227 Rules are failing (18.94%)		14 February 2013 at 16:00	
Not Compliant			
		View report >	
 OWASP scan Report on 02/14/2013		http://10.10.26.238	
Summary: 116 pages impacted 117 threats found		14 February 2013 at 11:40	

Welcome Vanessa

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

[More Results](#) [Quick Tour](#) [Take the Trial](#) [Log In](#) [Vanessa Polyk](#) [Help](#) [It scans incoming](#)

View by: [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**

February 15, 2013 at 11:44

Malware Detection

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

<http://www.mwtest.info/m...> [www.mwtest.info](#)

[Reason URLs](#)

Filter by severity levels

All (24) Level 1 (7) Level 2 (15) Level 3 (0) Level 4 (0) Level 5 (0) **Info (2)** [Search for this category](#) [Filter](#) [CSV](#)

All Scan Results 1 - 24 of 29 ▾

A. Malicious Process Launch Was Detected

QID: 296612 CVSS Base: 5.8 CVSS Temporal: 6.2 Port: - Category: Malware

CVE ID: - Found At: <http://www.mwtest.info/malware-detection?name=MZ37-MZ37-SOACREMO.html>

These:
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

<http://www.qualys.com>

Vulnerability Scanning Tools for Mobile

Retina CS for Mobile



SecurityMetrics MobileScan



Nessus Vulnerability Scanner



<http://www.beyondtrust.com>

<https://www.securitymetrics.com>

<http://www.tenable.com>

Network Vulnerability Scanners



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



OpenVAS
<http://www.openvas.org>



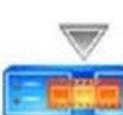
Core Impact Professional
<http://www.coresecurity.com>



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>



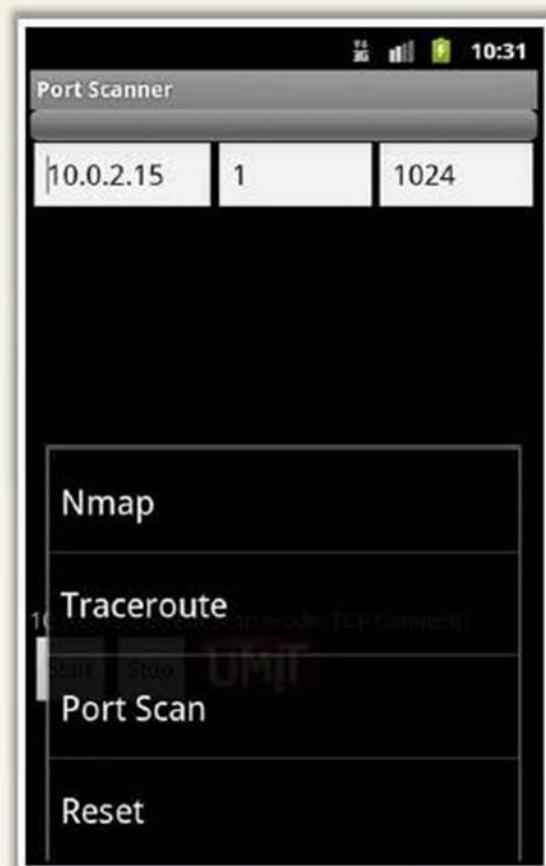
Nsauditor Network Security Auditor
<http://www.nsauditor.com>



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

Scanning Tools for Mobile

Umit Network Scanner



<http://www.umitproject.org>

Fing



<http://www.overlooksoft.com>

IP Network Scanner

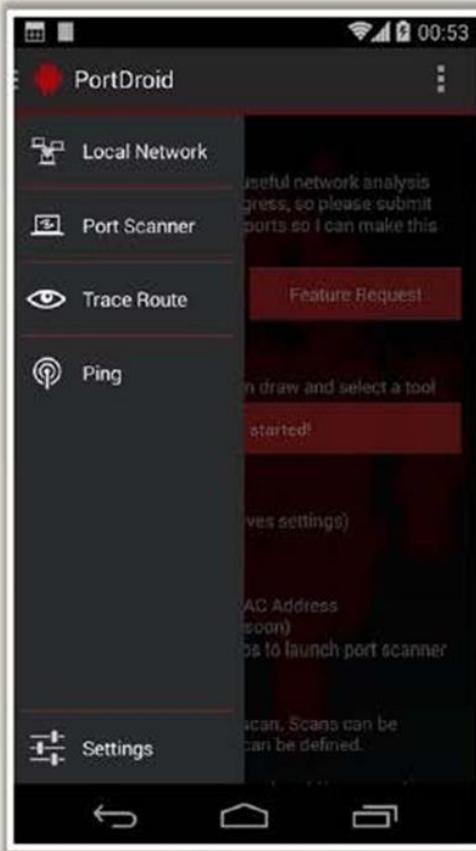


<http://10base-t.com>

Scanning Tools for Mobile

(Cont'd)

PortDroid Network Analysis



Pamn IP Scanner



Network Discovery



<http://www.stealthcopter.com>

<http://pips.wjholden.com>

<http://rorist.github.io>

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>

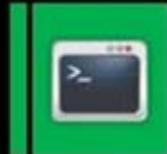
```
root@kali:~# hping3 -l 192.168.0.105
HPING 192.168.0.105 (eth0 192.168.0.105): icmp mode set, 28 headers + 0 data bytes
es
len=28 ip=192.168.0.105 ttl=128 id=448 icmp_seq=0 rtt=0.4 ms
len=20 ip=192.168.0.105 ttl=120 id=440 icmp_seq=1 rtt=0.4 ms
len=28 ip=192.168.0.105 ttl=128 id=450 icmp_seq=2 rtt=0.3 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, 128 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=605 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
```



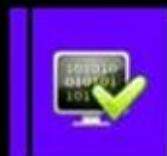
Collecting Initial Sequence Number

```
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
```

Port Scanning Countermeasures

01

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

05

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

02

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

06

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

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

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**

04

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

08

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

Summary

■ Information

- The more information you have about the vulnerabilities and weaknesses of your system, the better prepared you are to defend it.
- The more information the hacker has about your system's vulnerabilities and weaknesses, the sooner it will be violated.
- The tools in this chapter are for the network and security administrator and are to be used for legal, not illegal, purposes.