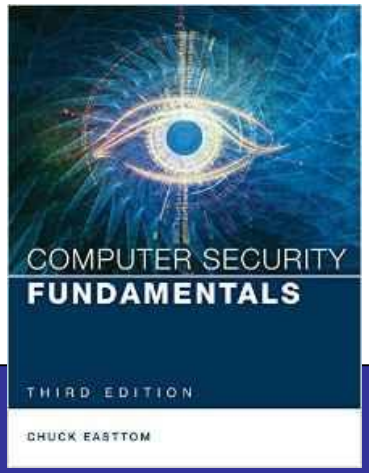
Computer Security Fundamentals

by Chuck Easttom



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.

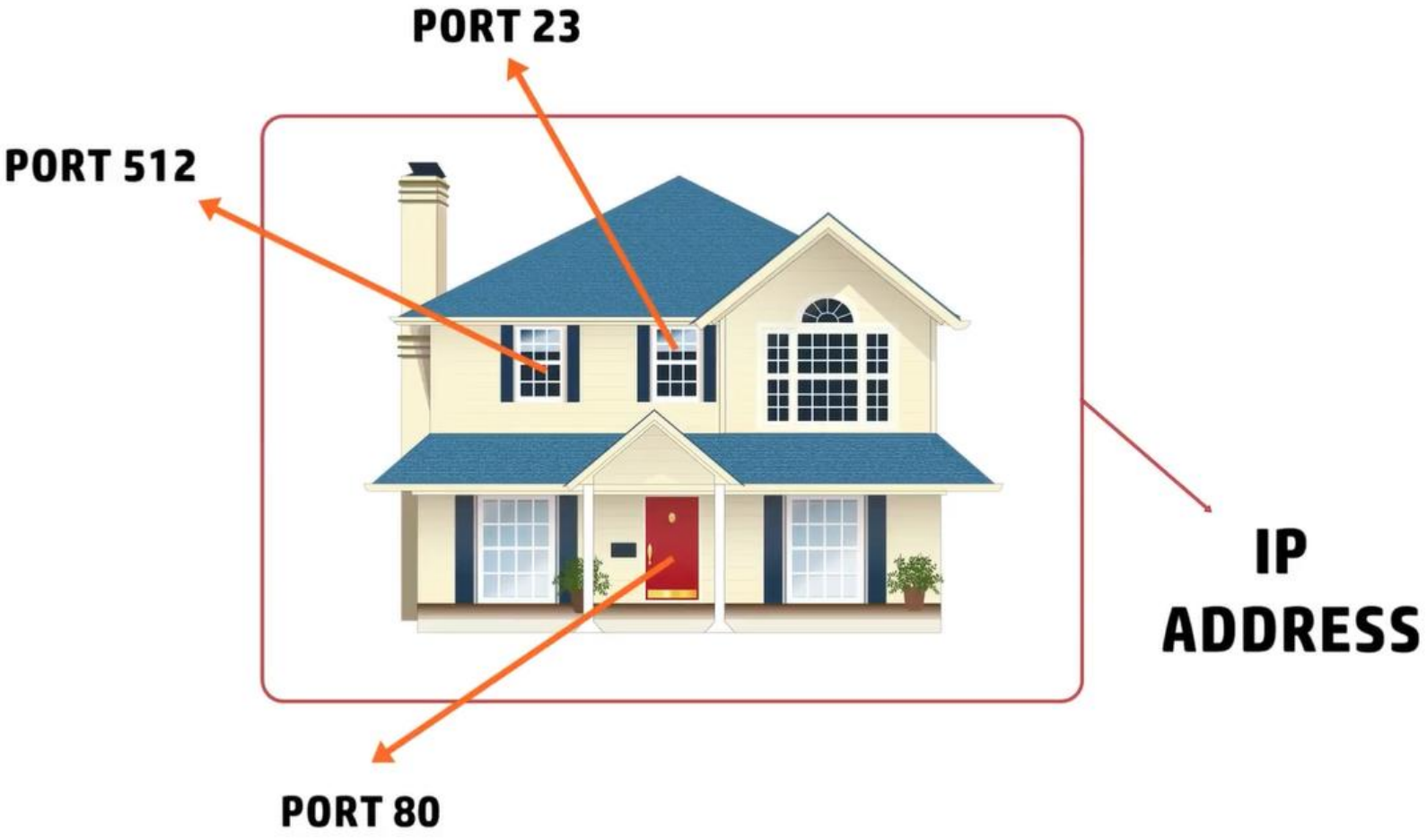
Basics of Security

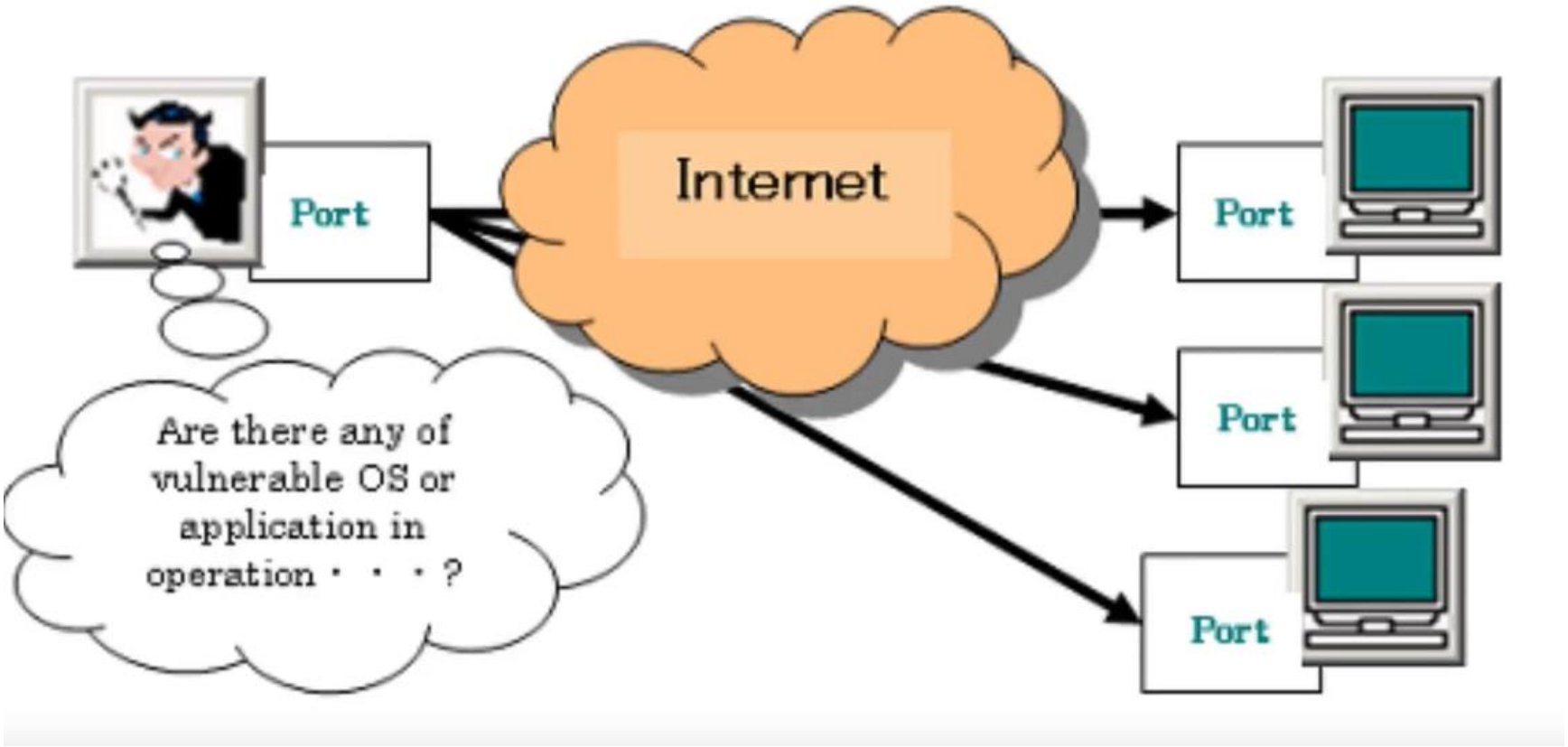
- **Patch:** A modification to a program to improve its security, performance, or other feature.

  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


PORT 23
PORT 512
IP
ADDRESS
PORT 80

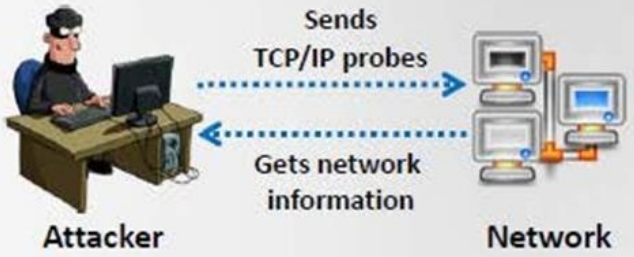

Port
Internet
Port
Port
Port
Are there any of vulnerable OS or application in operation · · · ?

Overview of Network Scanning

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

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

Network Scanning Process



Objectives of Network Scanning

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

TCP Communication Flags

Data contained in the packet should be processed immediately

URG (Urgent)

There will be no more transmissions

FIN (Finish)

Resets a connection

RST (Reset)

PSH (Push)

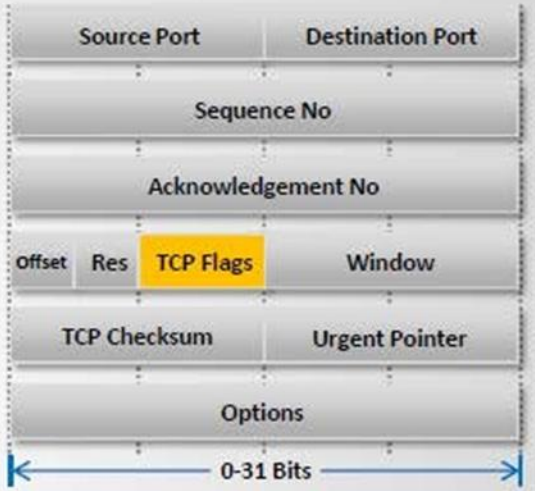
Sends all buffered data immediately

ACK (Acknowledgement)

Acknowledges the receipt of a packet

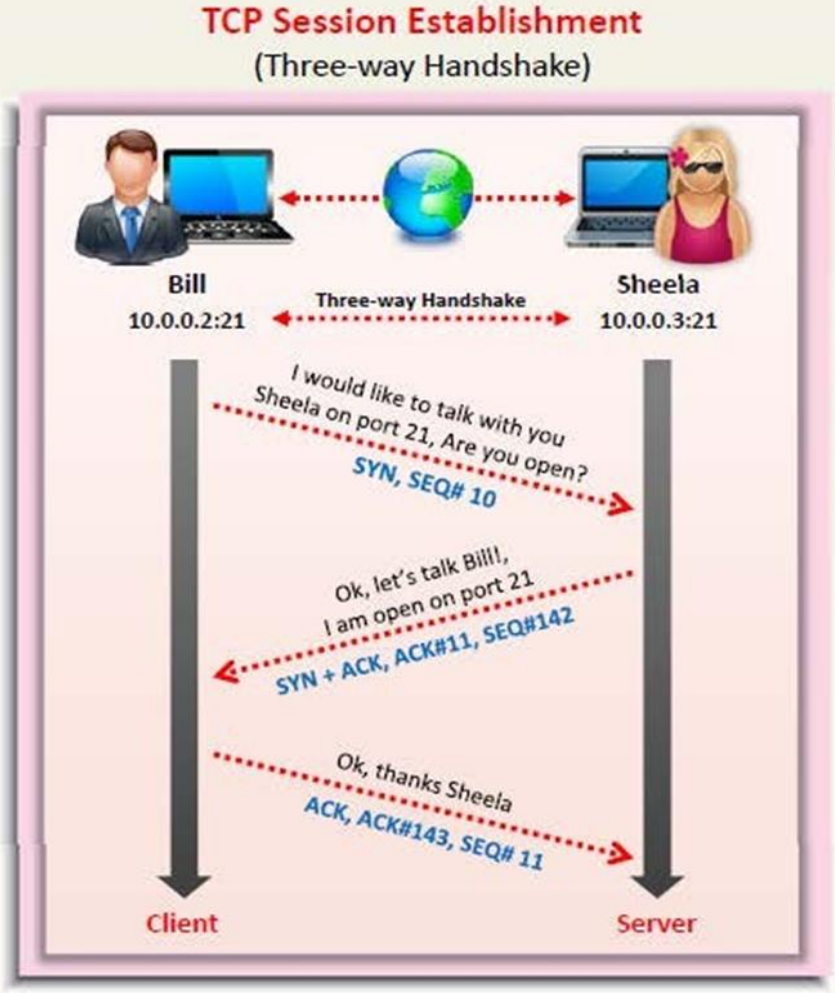
SYN (Synchronize)

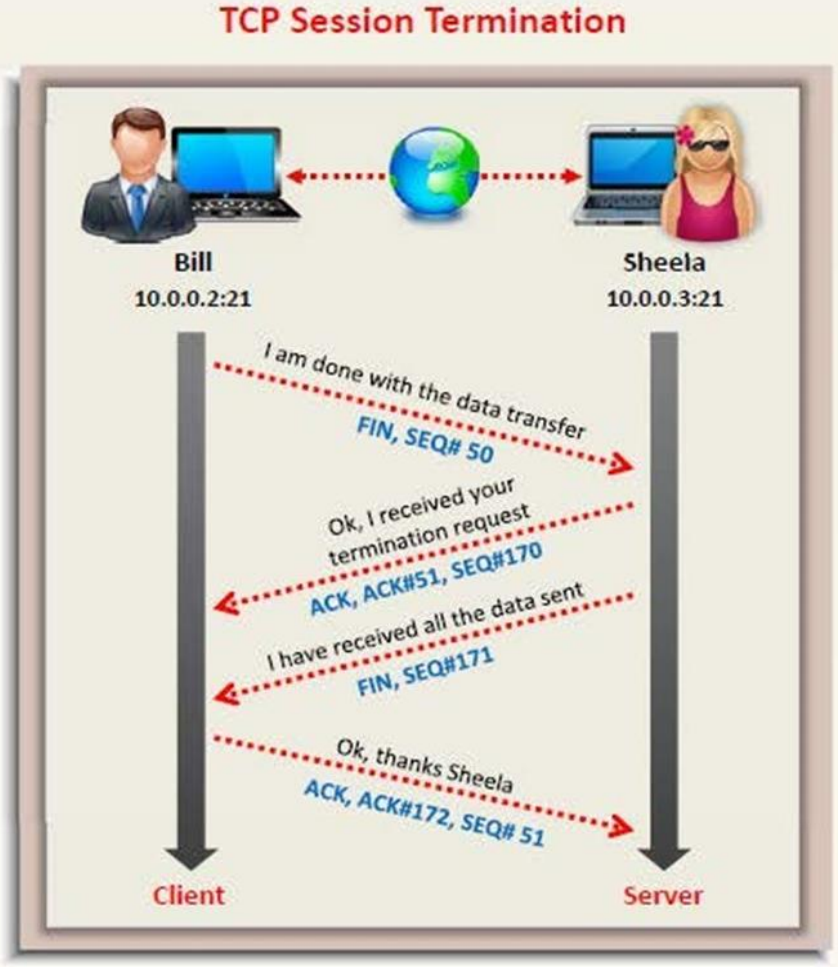
Initiates a connection between hosts



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

TCP/IP Communication

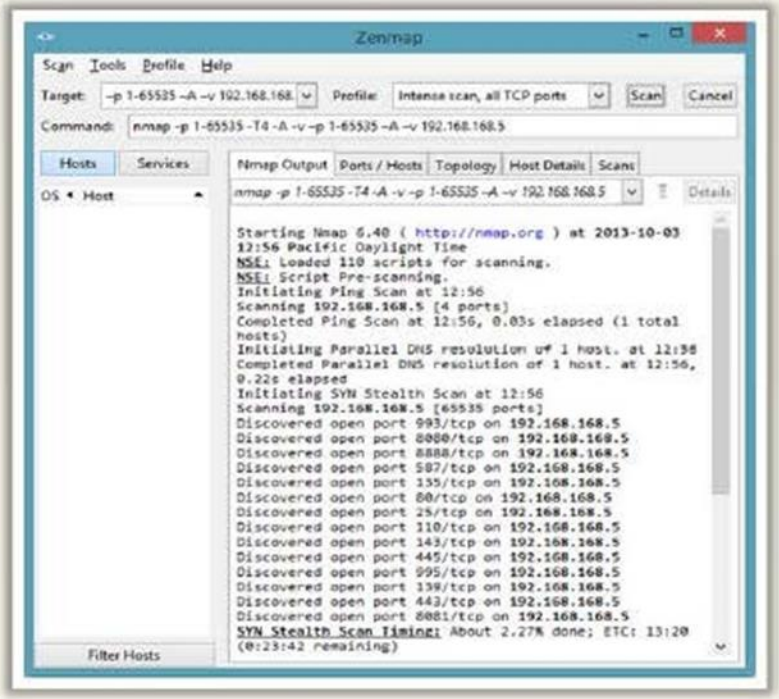


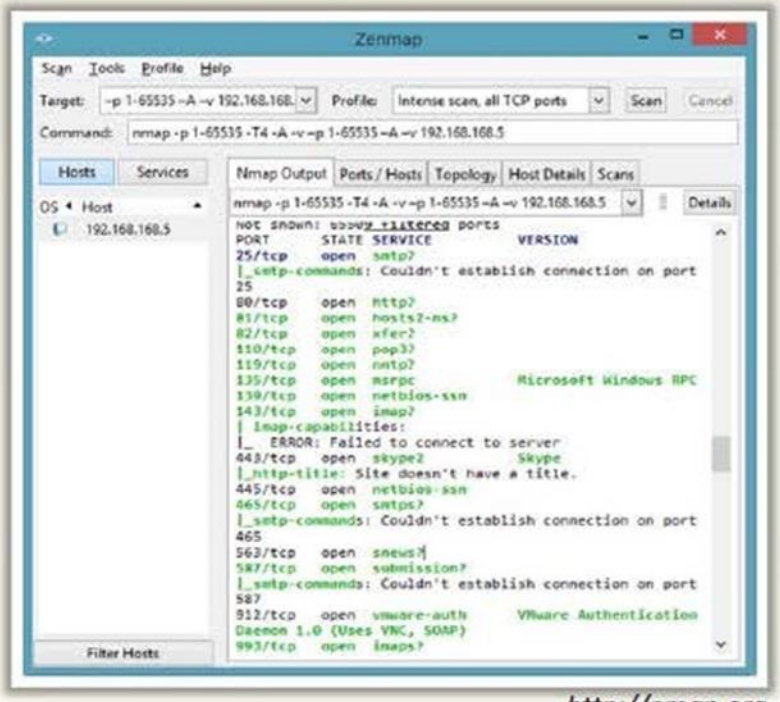


Scanning Tool: Nmap

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

02 Attacker uses Nmap to extract information such as live hosts on the network, services (application name and version), type of packet filters/firewalls, operating systems and OS versions



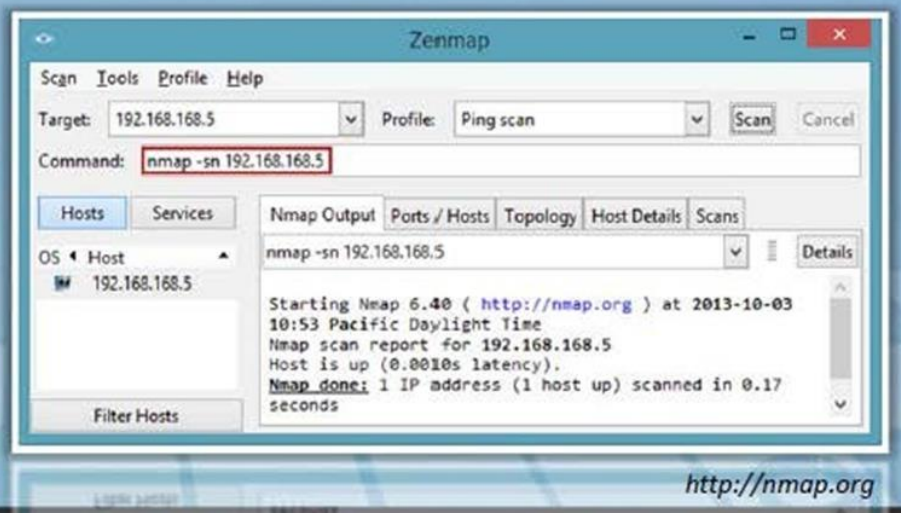


http://nmap.org

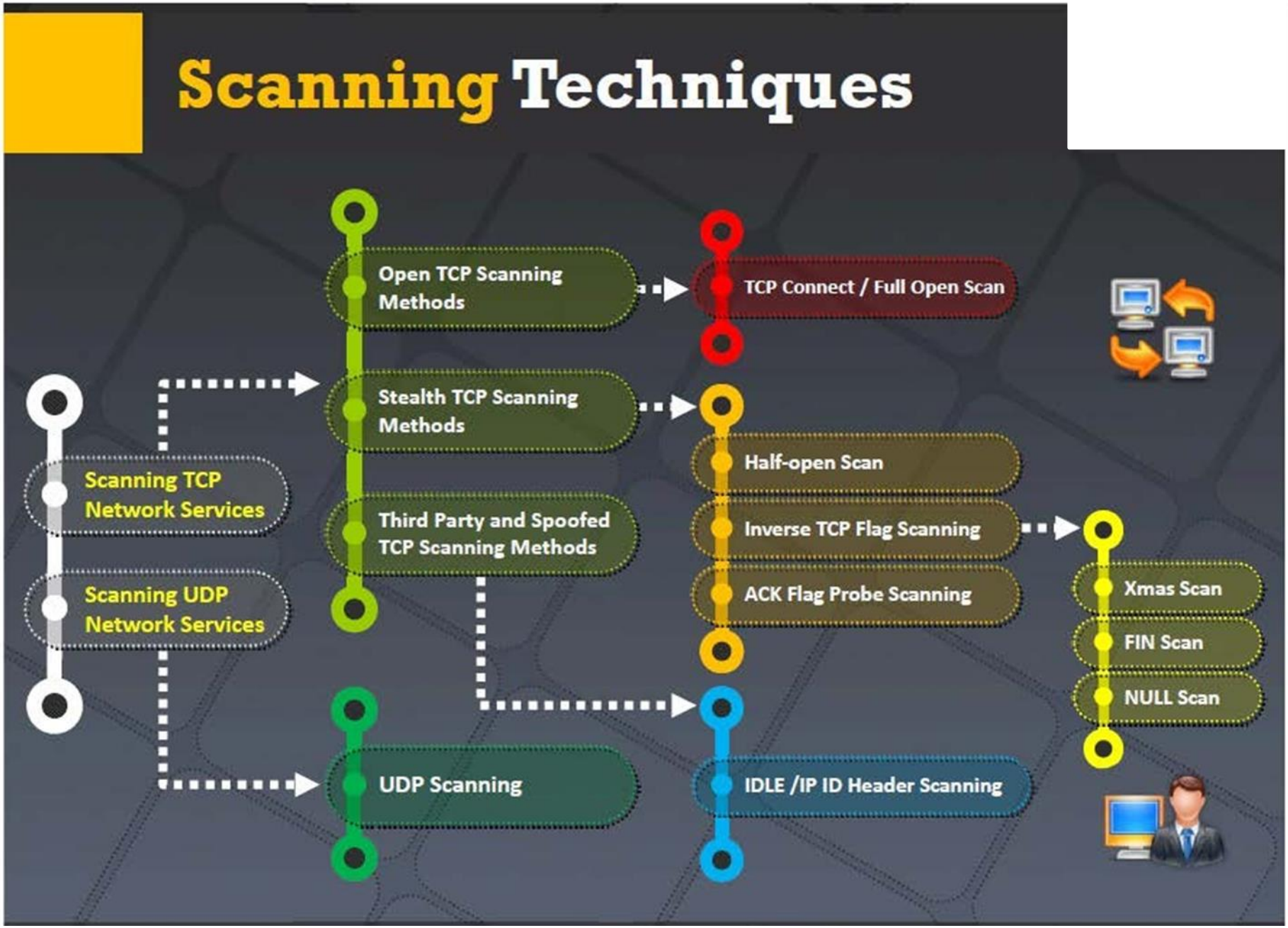
Checking for Live Systems - ICMP Scanning

- 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:



Scanning Techniques

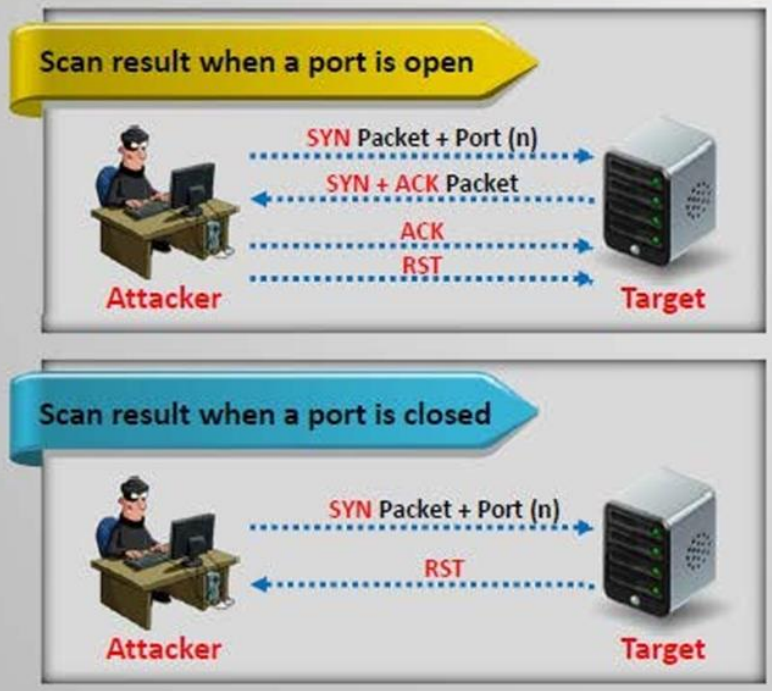


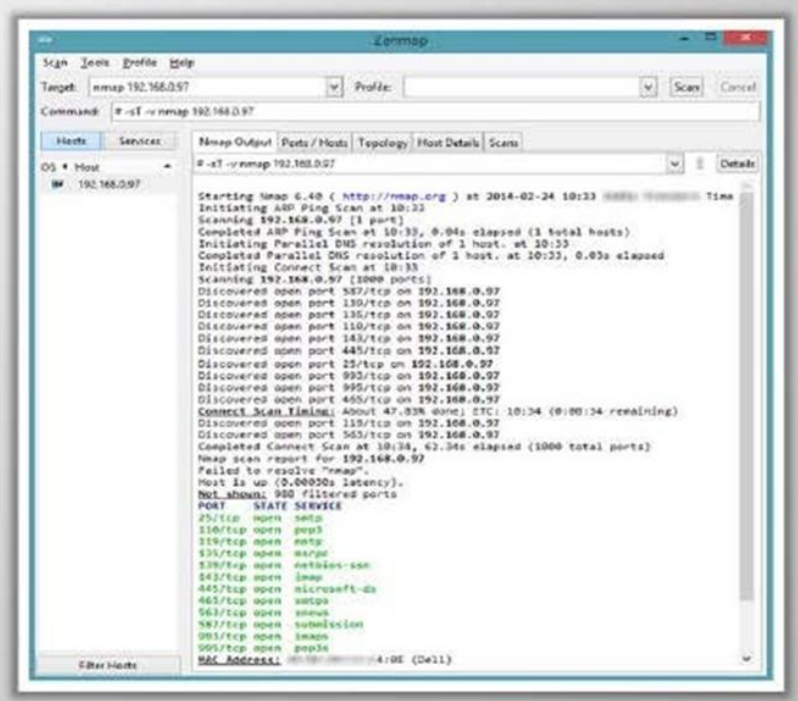
TCP Connect / Full Open Scan

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

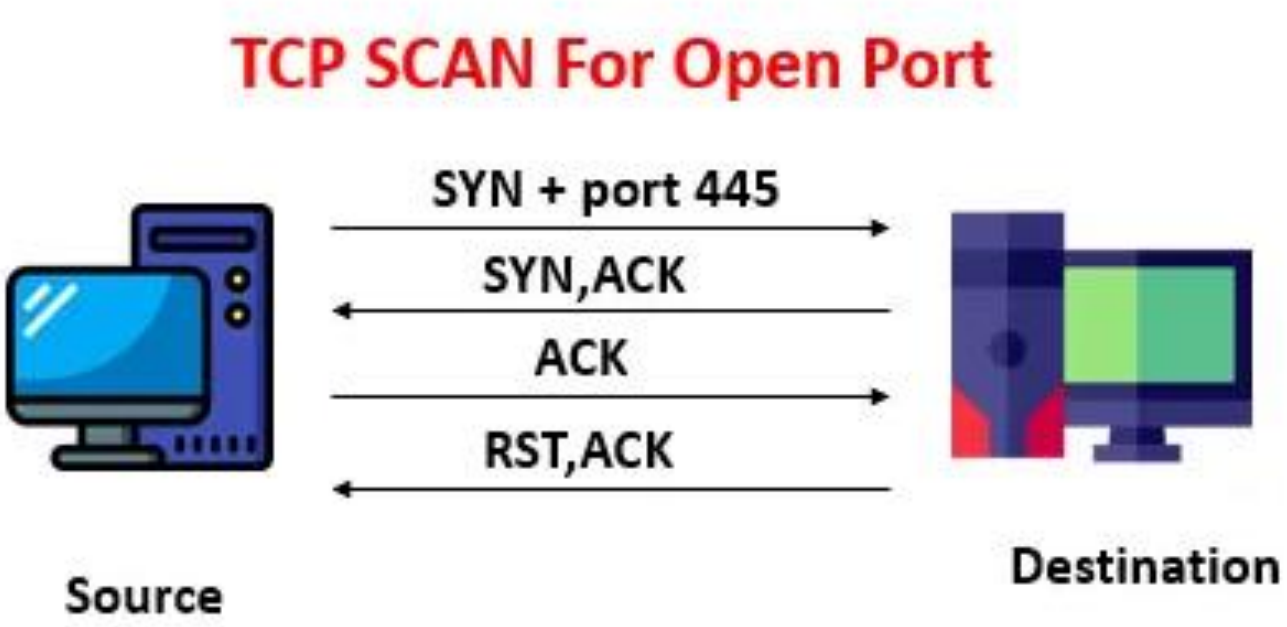
02 TCP Connect scan **establishes a full connection** and tears it down by sending a **RST packet**

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

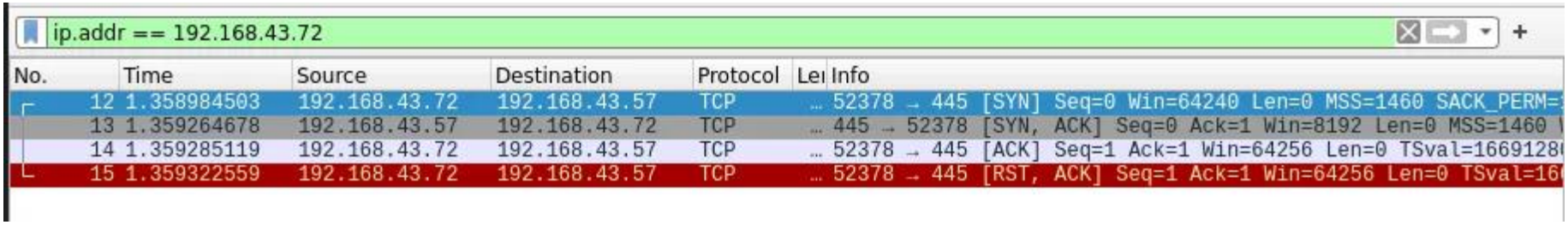


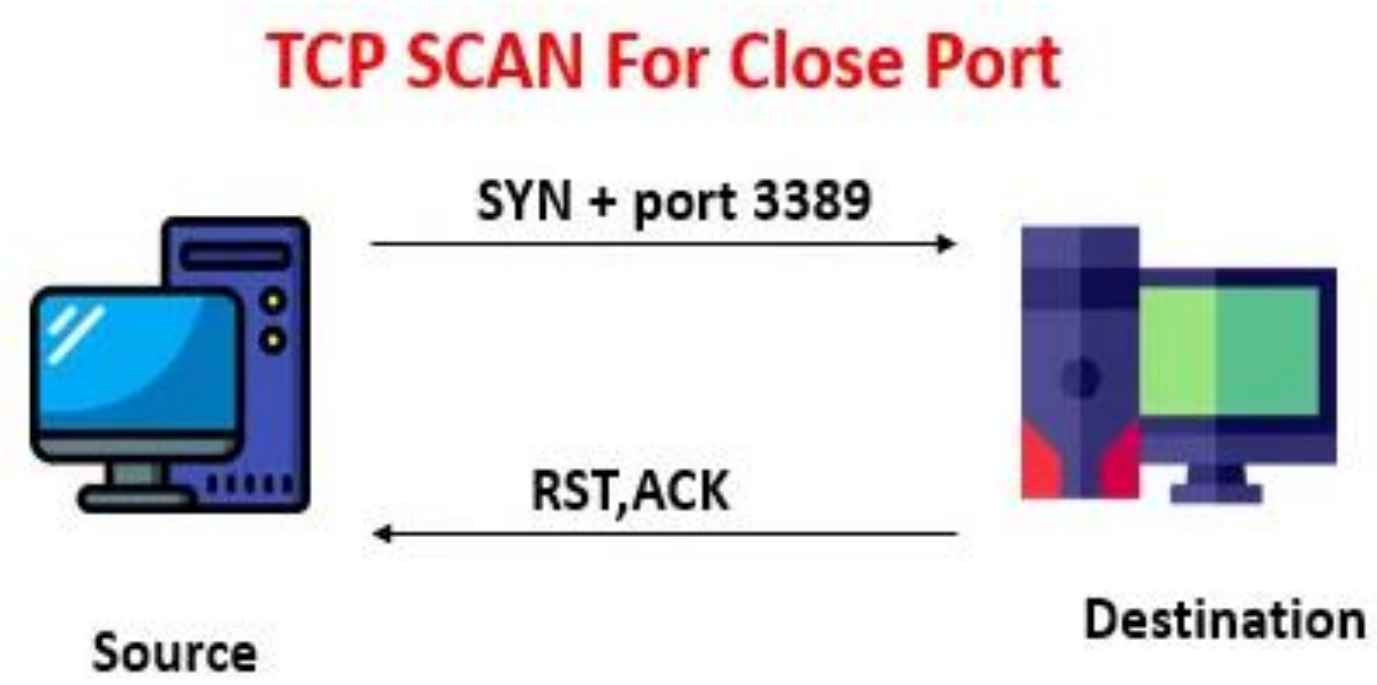


- TCP scan will scan for TCP port like port 22, 21, 23, 445 etc and ensure for listening port (open) through 3-way handshake connection between the source and destination port. If the port is open then source made request with **SYN** packet, a response destination sent **SYN, ACK** packet and then source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


TCP SCAN For Open Port
SYN + port 445
SYN,ACK
ACK
RST,ACK
Source
Destination

```
┌──(root💀kali)-[/home/sam]
└─# 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
```




TCP SCAN For Close Port
SYN + port 3389
RST,ACK
Source
Destination

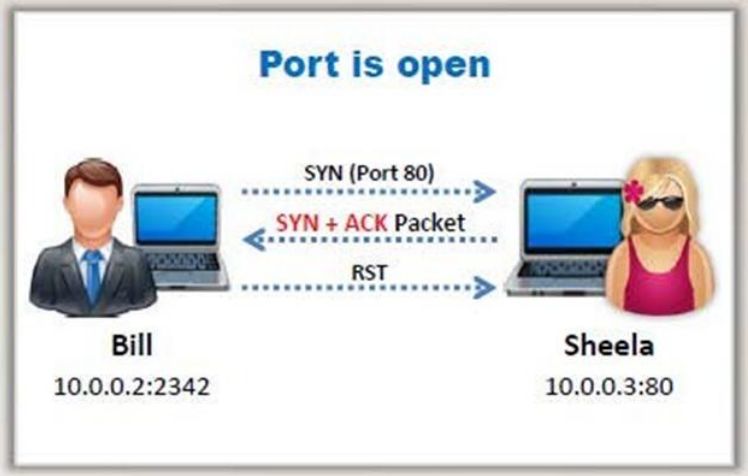
```
┌──(root💀kali)-[/home/sam]
└─# nmap -sT -p 3389 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:42 IST
Nmap scan report for 192.168.43.251
Host is up (0.00021s latency).

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
```

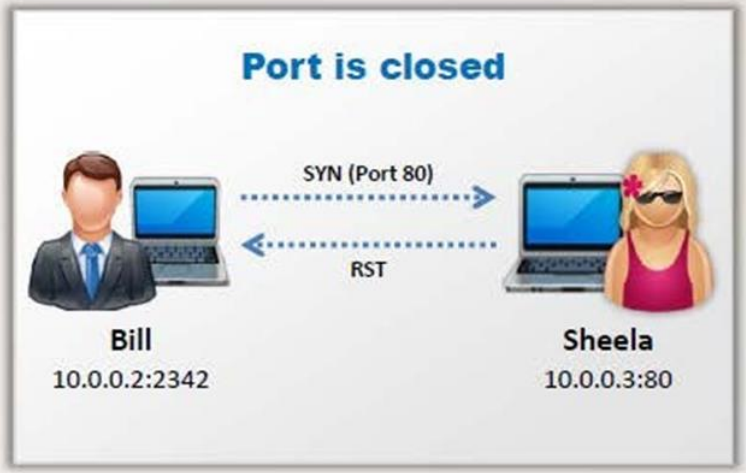
Stealth Scan (Half-open Scan)

- 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

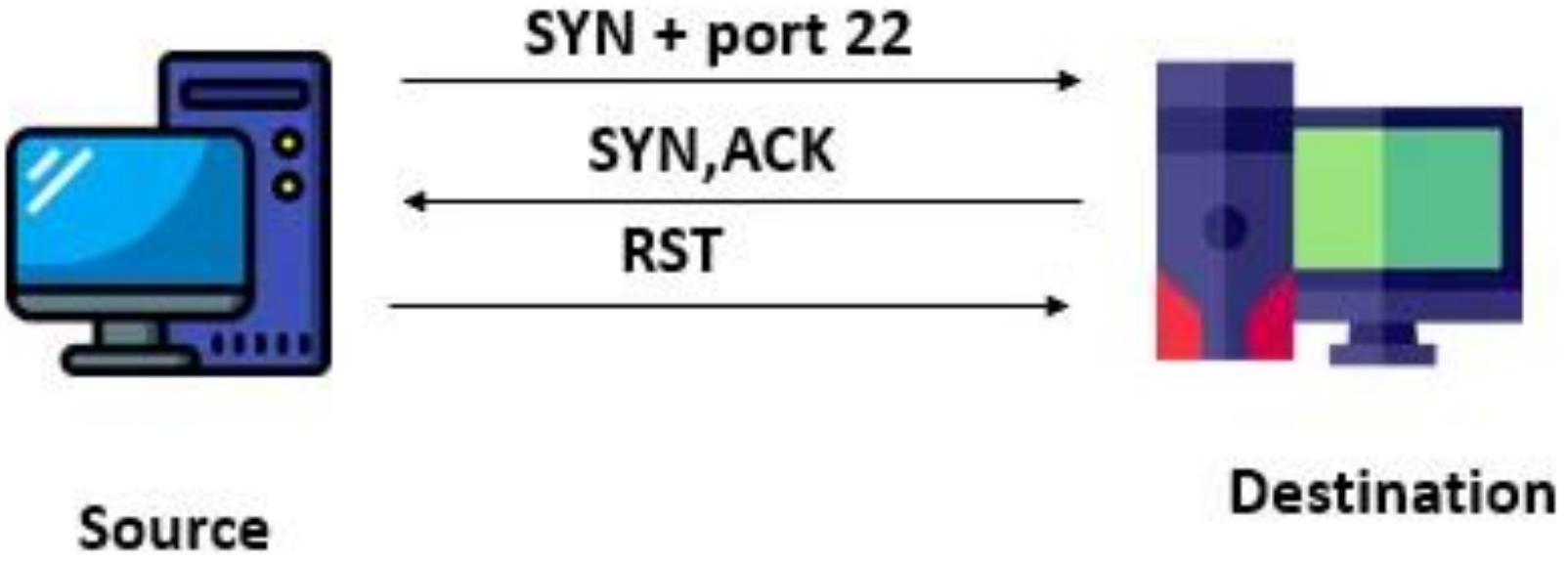
The client sends a single **SYN** packet to the server on the appropriate port	01
If the port is open then the server responds with a **SYN/ACK** packet	02
If the server responds with an **RST** packet, then the remote port is in the "closed" state	03
The client sends the **RST** packet to close the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



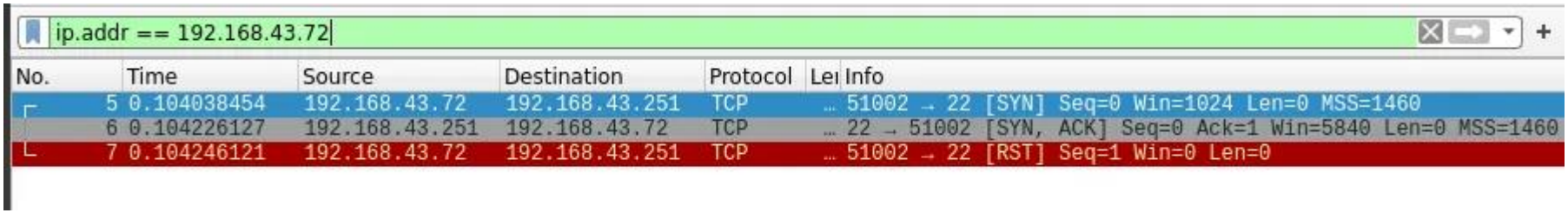


- SYN scan is the default and most popular scan option for good reasons. It can be performed quickly, scanning thousands of ports per second on a fast network not hampered by restrictive firewalls. It is also relatively typical and stealthy since it never completes TCP connections.

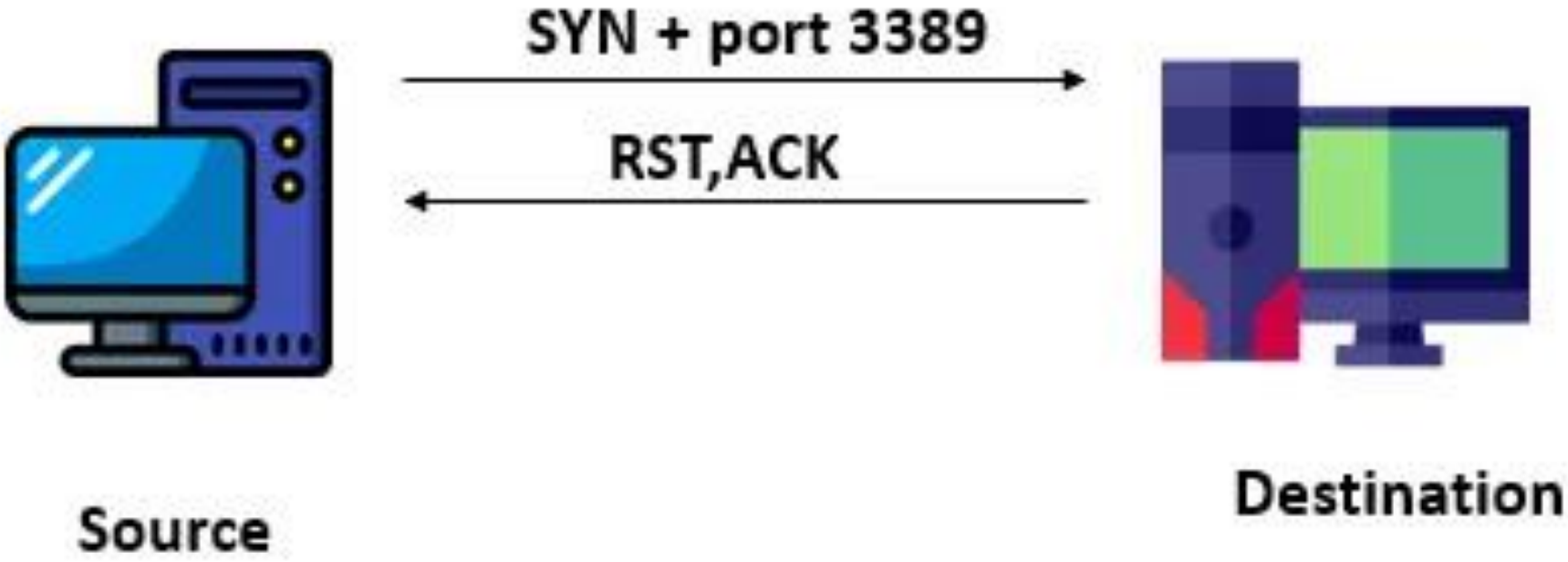
Stealth SCAN For Open Port



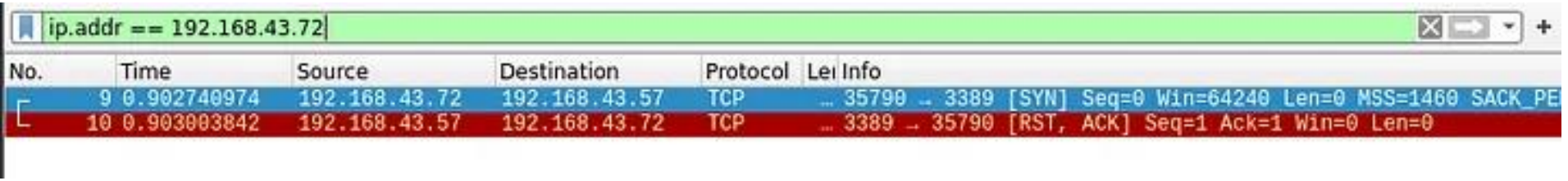
```
┌──(root💀kali)-[/home/sam]
└─# nmap -sS -p 22 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 10:50 IST
Nmap scan report for 192.168.43.251
Host is up (0.00027s latency).

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
```



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
```

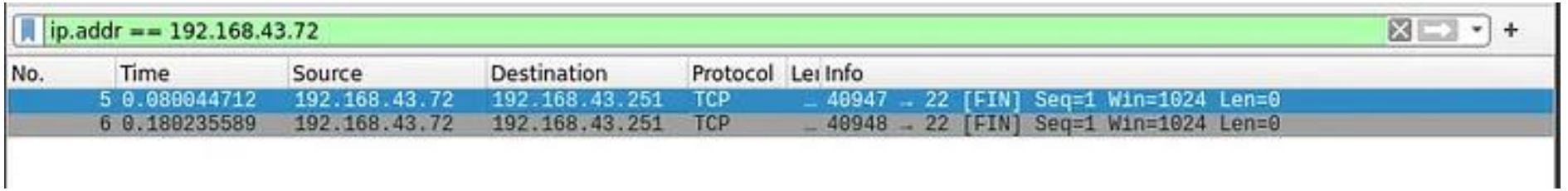


Fin Scan

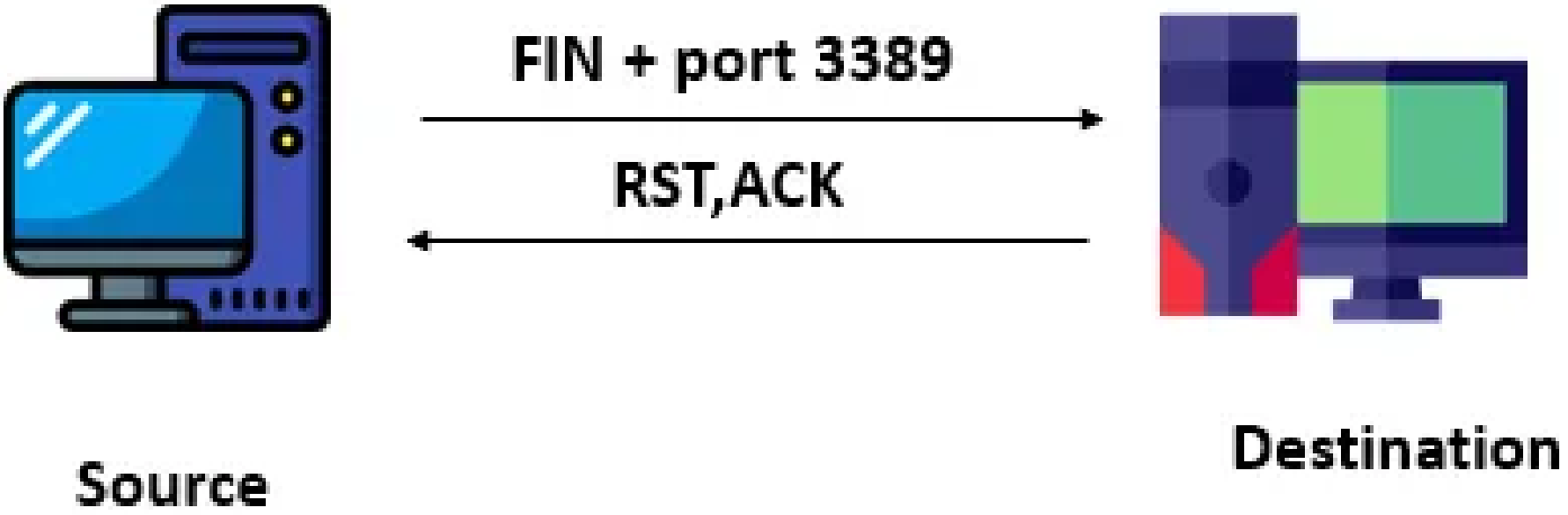
- A FIN packet is used to terminate the TCP connection between the source and destination port typically after the data transfer is complete. In the place of an SYN packet, Nmap starts a FIN scan by using a FIN packet. If the port is open then no response will come from destination port when FIN packet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

FIN SCAN For Open Port

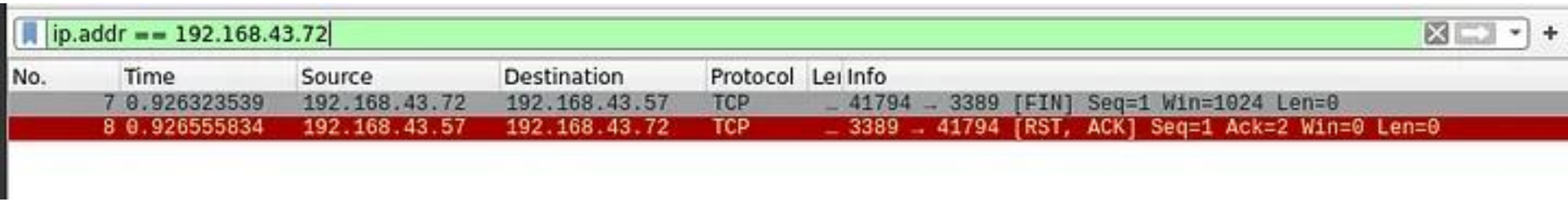
```
┌──(root💀kali)-[/home/sam]
└─# nmap -sF -p 22 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 10:55 IST
Nmap scan report for 192.168.43.251
Host is up (0.00020s latency).

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
```



FIN SCAN For Close Port



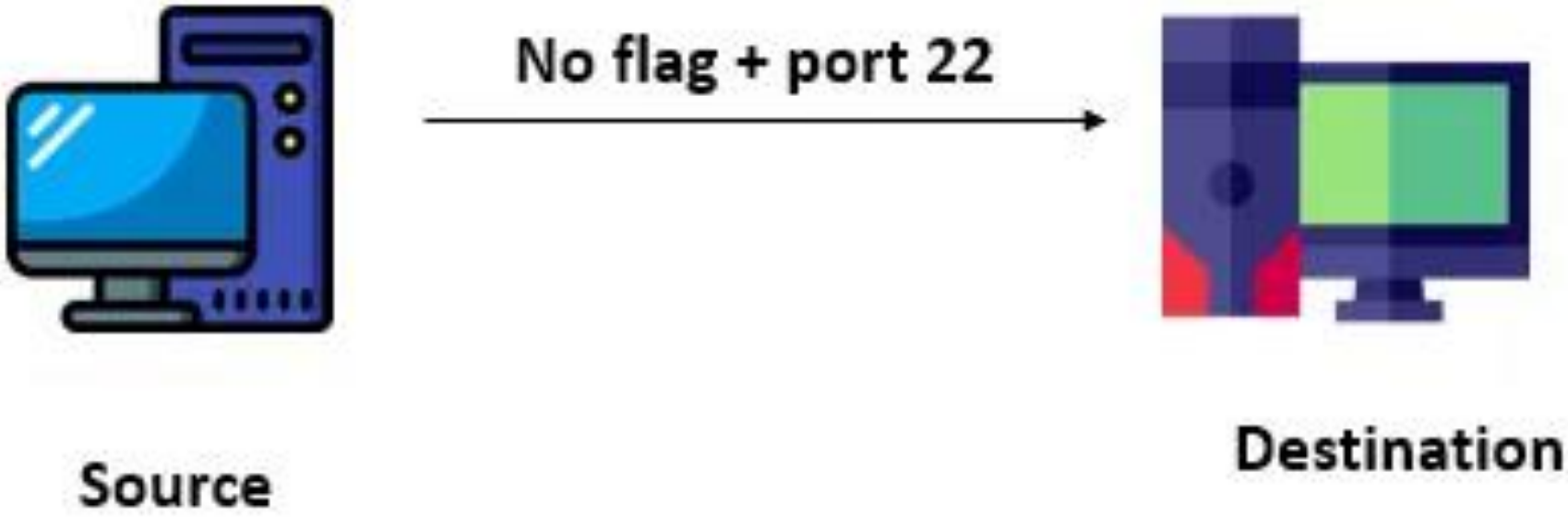
```
┌──(root💀kali)-[/home/sam]
└─# nmap -sF -p 3389 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:46 IST
Nmap scan report for 192.168.43.251
Host is up (0.00022s latency).

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
```



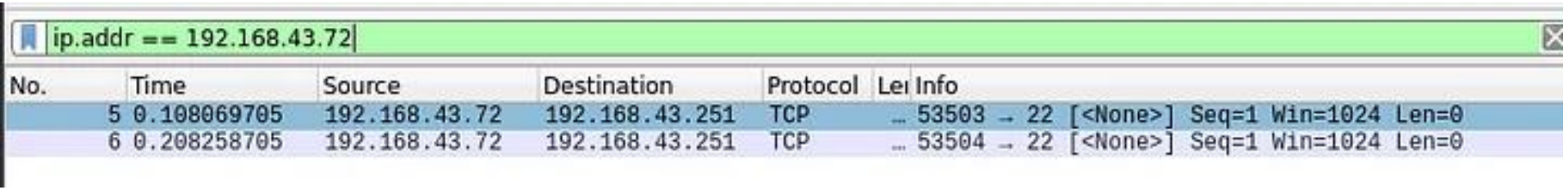
Null Scan

- 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.

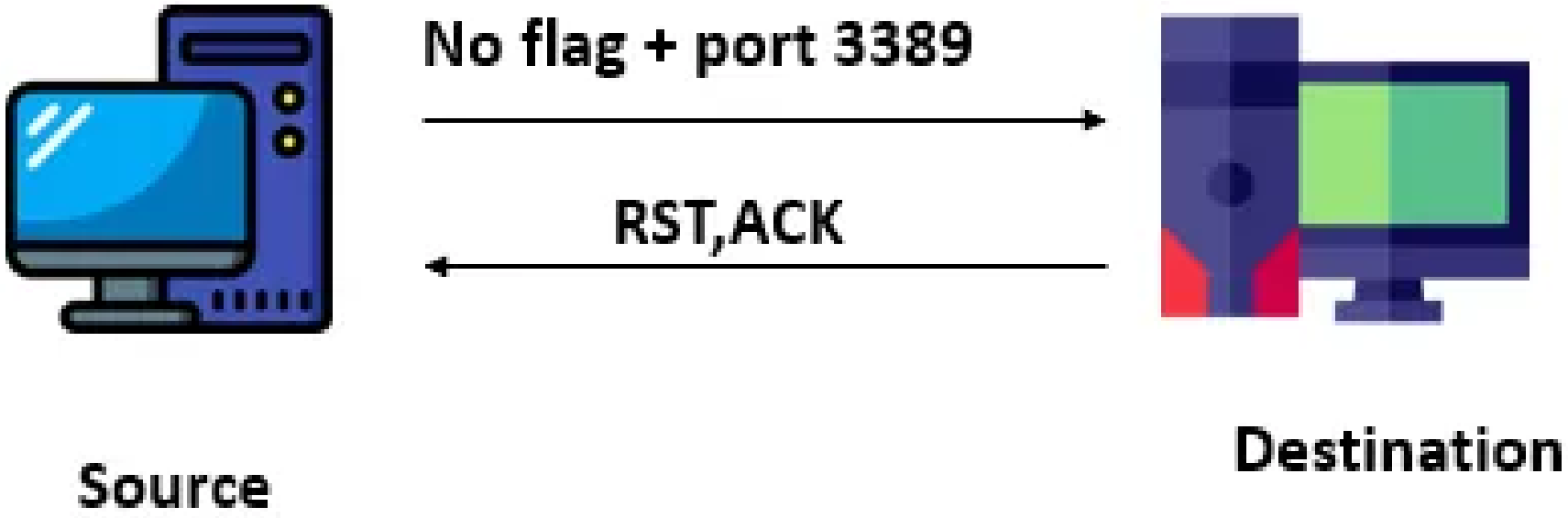
NULL SCAN For Open Port



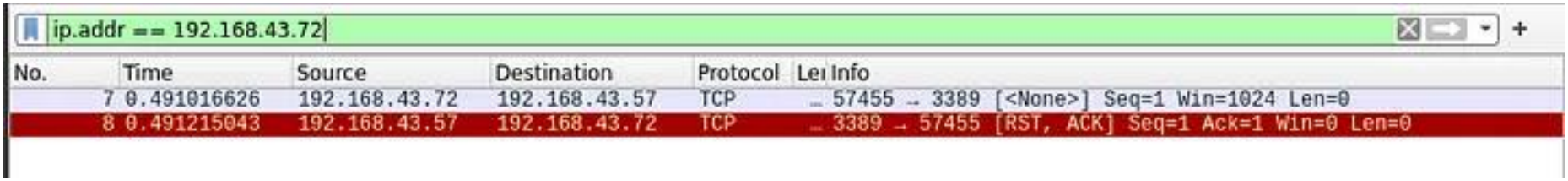
```
┌──(root💀kali)-[/home/sam]
└─# nmap -sN -p 22 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 10:58 IST
Nmap scan report for 192.168.43.251
Host is up (0.00028s latency).

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
```



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
```



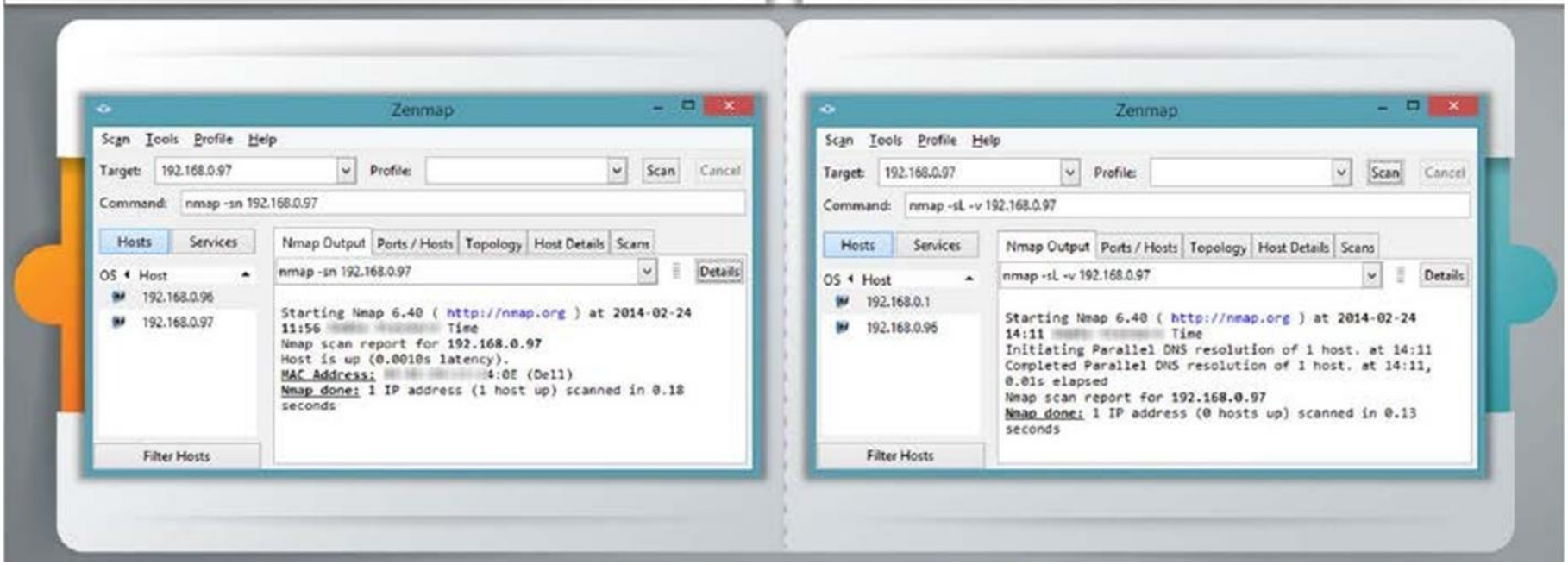
ICMP Echo Scanning/List Scan

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



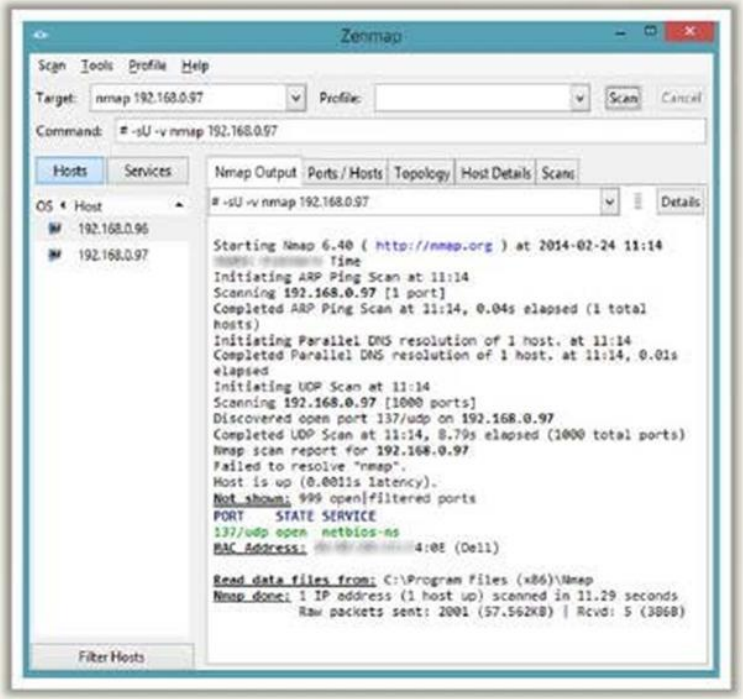
UDP Scanning

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

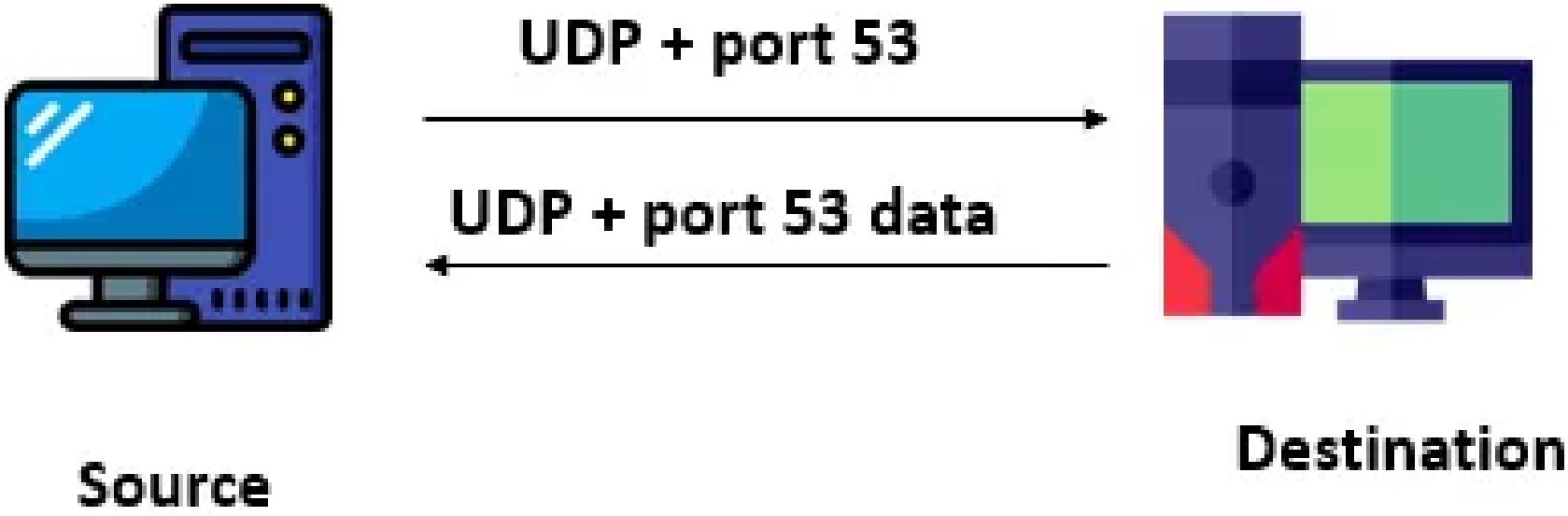
- If a UDP packet is sent to closed port, the system responds with ICMP port unreachable message
- Spywares, Trojan horses, and other malicious applications use UDP ports



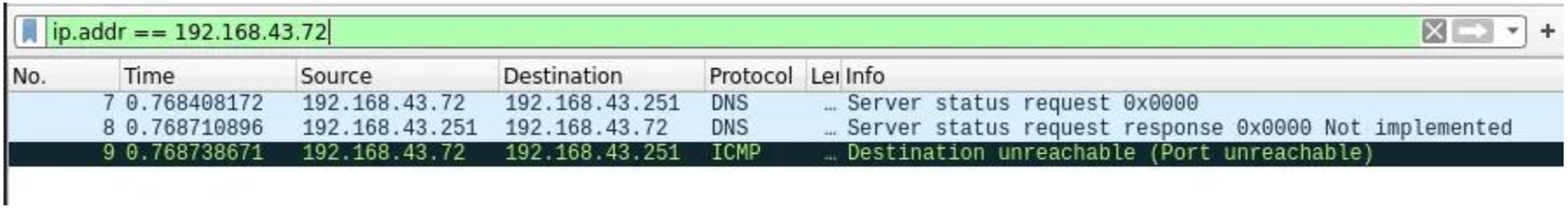
UDP Scan

- 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

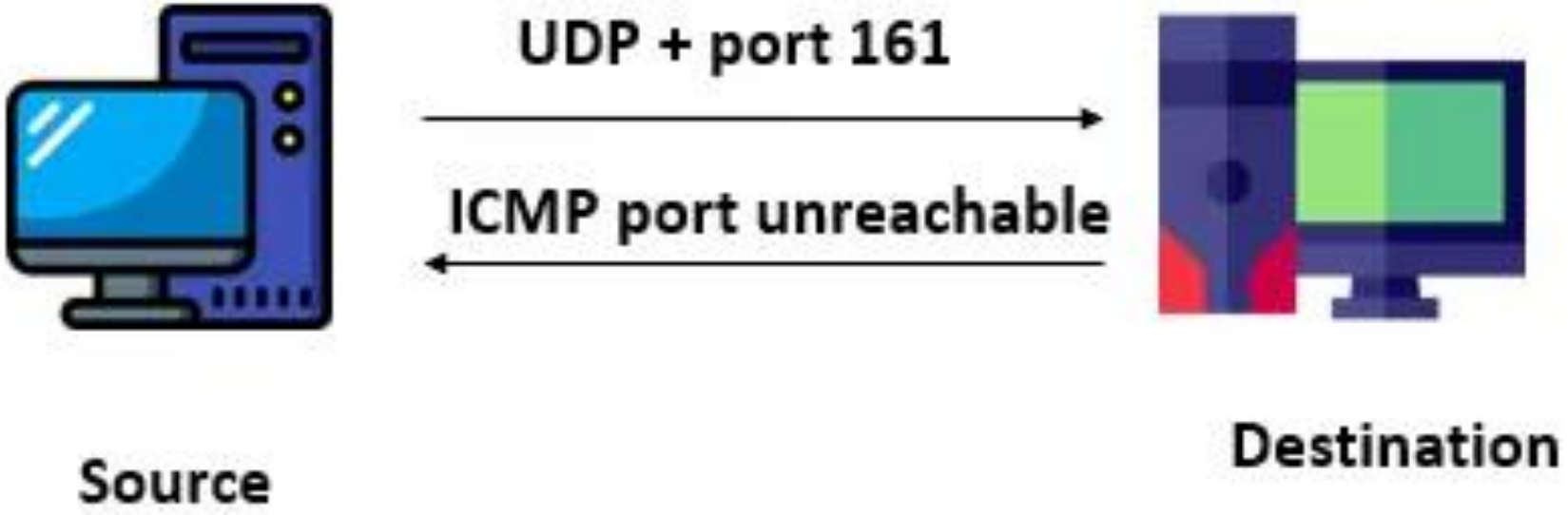
UDP SCAN For Open Port



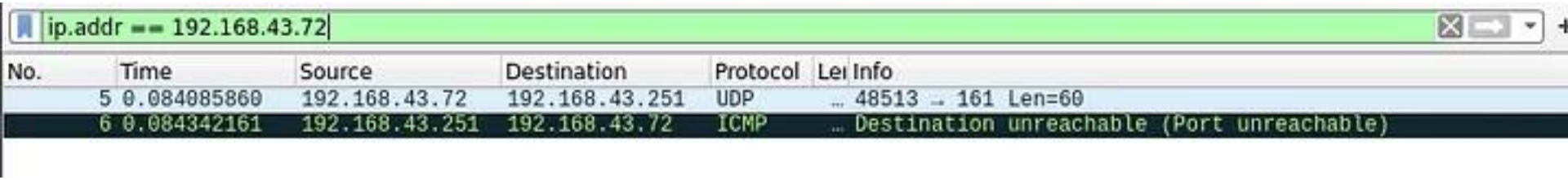
```
┌──(root💀kali)-[/home/sam]
└─# nmap -sU -p 53 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:31 IST
Nmap scan report for 192.168.43.251
Host is up (0.00025s latency).

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
```



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
```

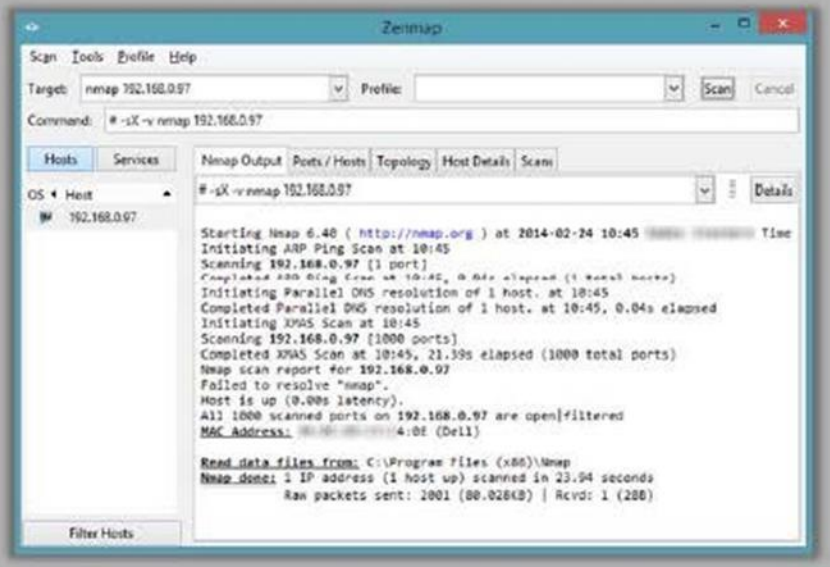


Xmas Scan

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

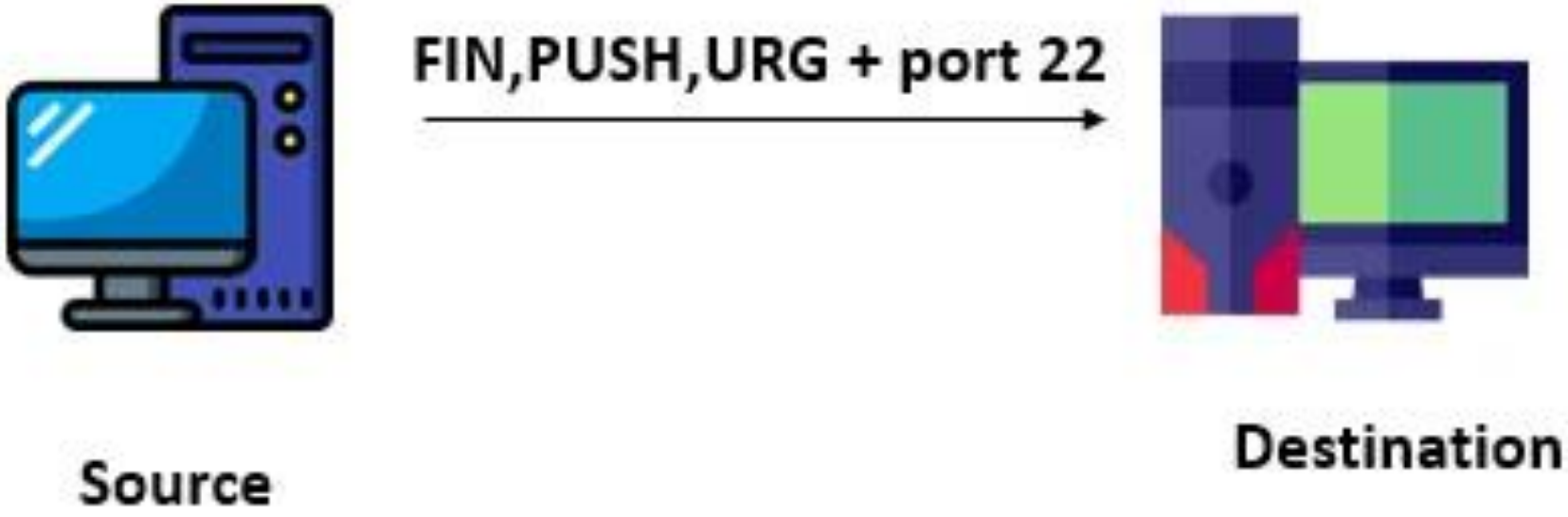
FIN scan works only with OSes with **RFC 793-based** TCP/IP implementation

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

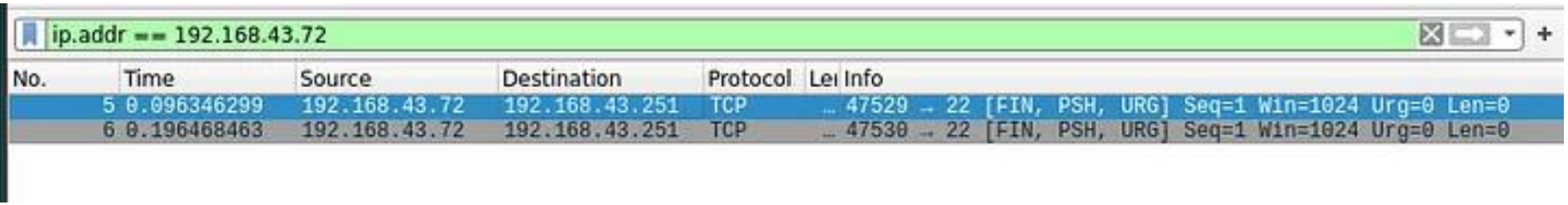


- These scans are designed to manipulate the PSH, URG and FIN flags of the TCP header, Sets the FIN, PSH, and URG flags, lighting the packet up like a Christmas tree. When source sent FIN, PUSH, and URG packet to a specific port and if the port is open then destination will discard the packets and will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

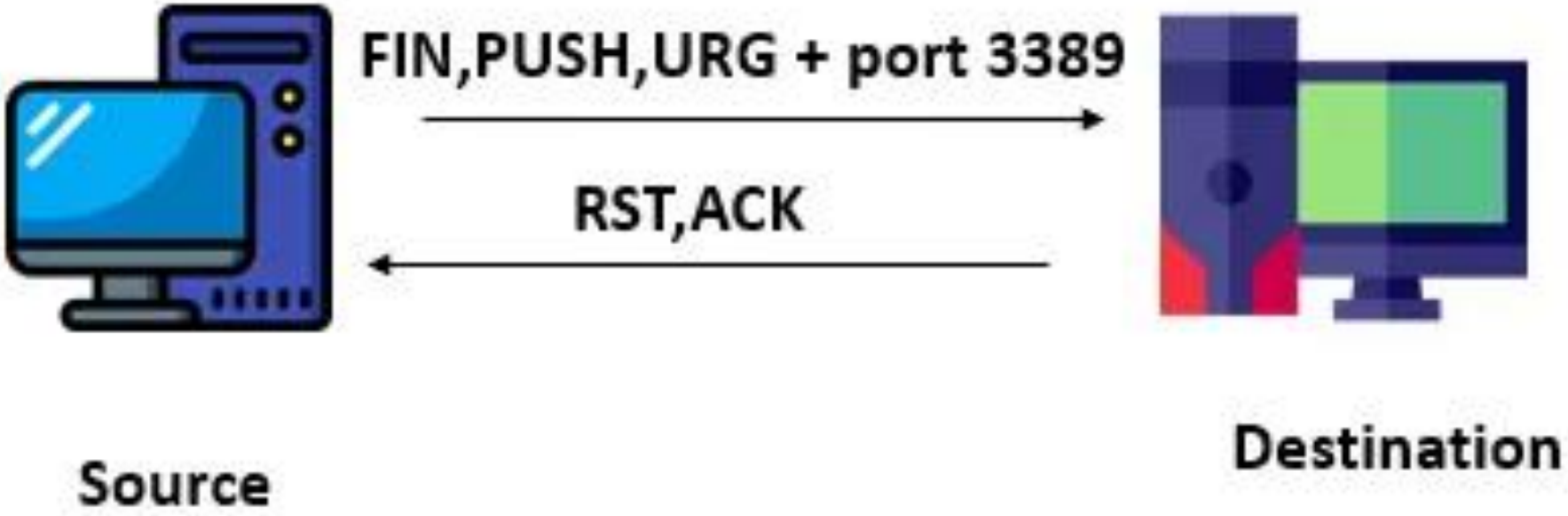
XMAS SCAN For Open Port



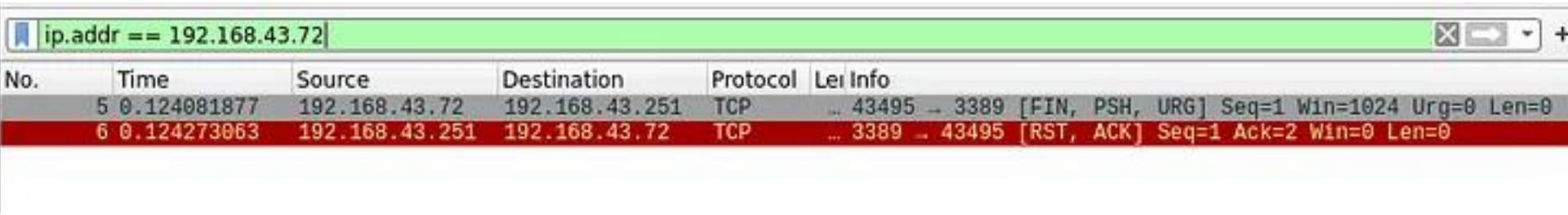
```
┌──(root💀kali)-[/home/sam]
└─# nmap -sX -p 22 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:36 IST
Nmap scan report for 192.168.43.251
Host is up (0.00018s latency).

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
```



XMAS SCAN For Close Port

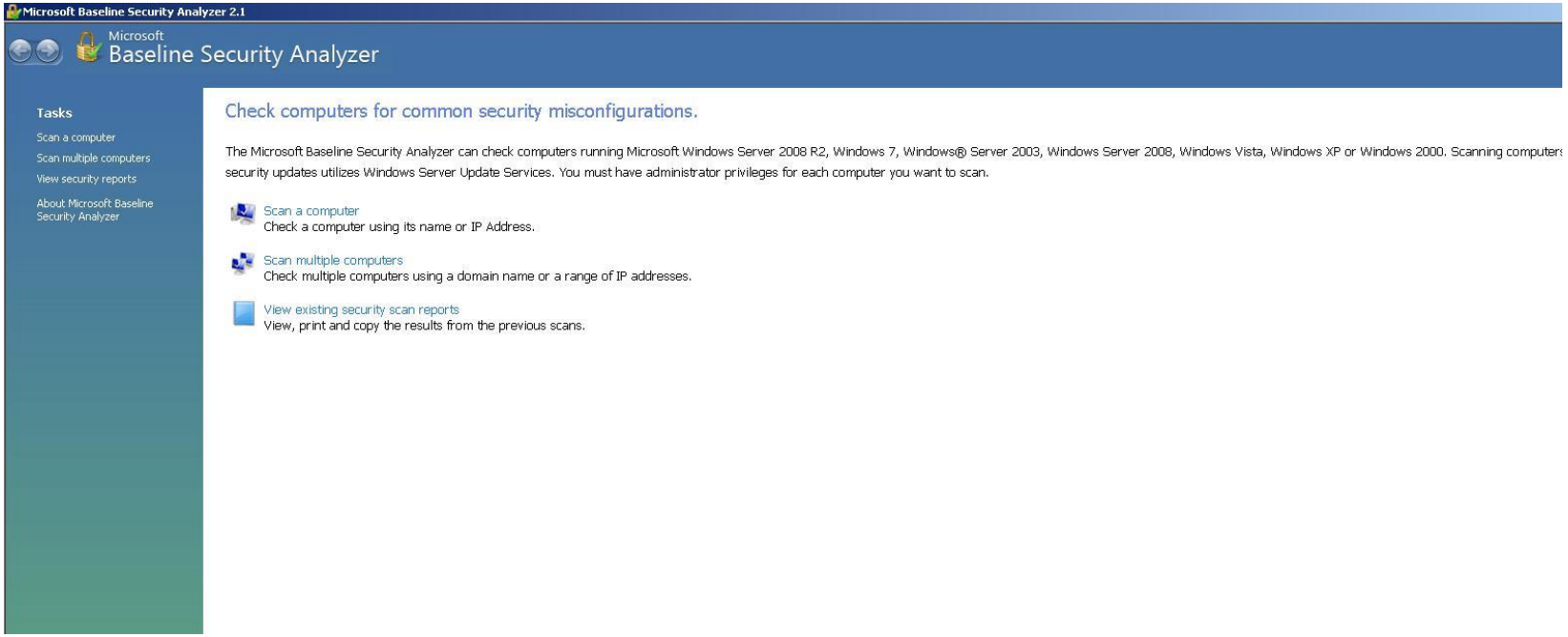


```
┌──(root💀kali)-[/home/sam]
└─# nmap -sX -p 3389 192.168.43.251
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-10 12:37 IST
Nmap scan report for 192.168.43.251
Host is up (0.00019s latency).

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
```

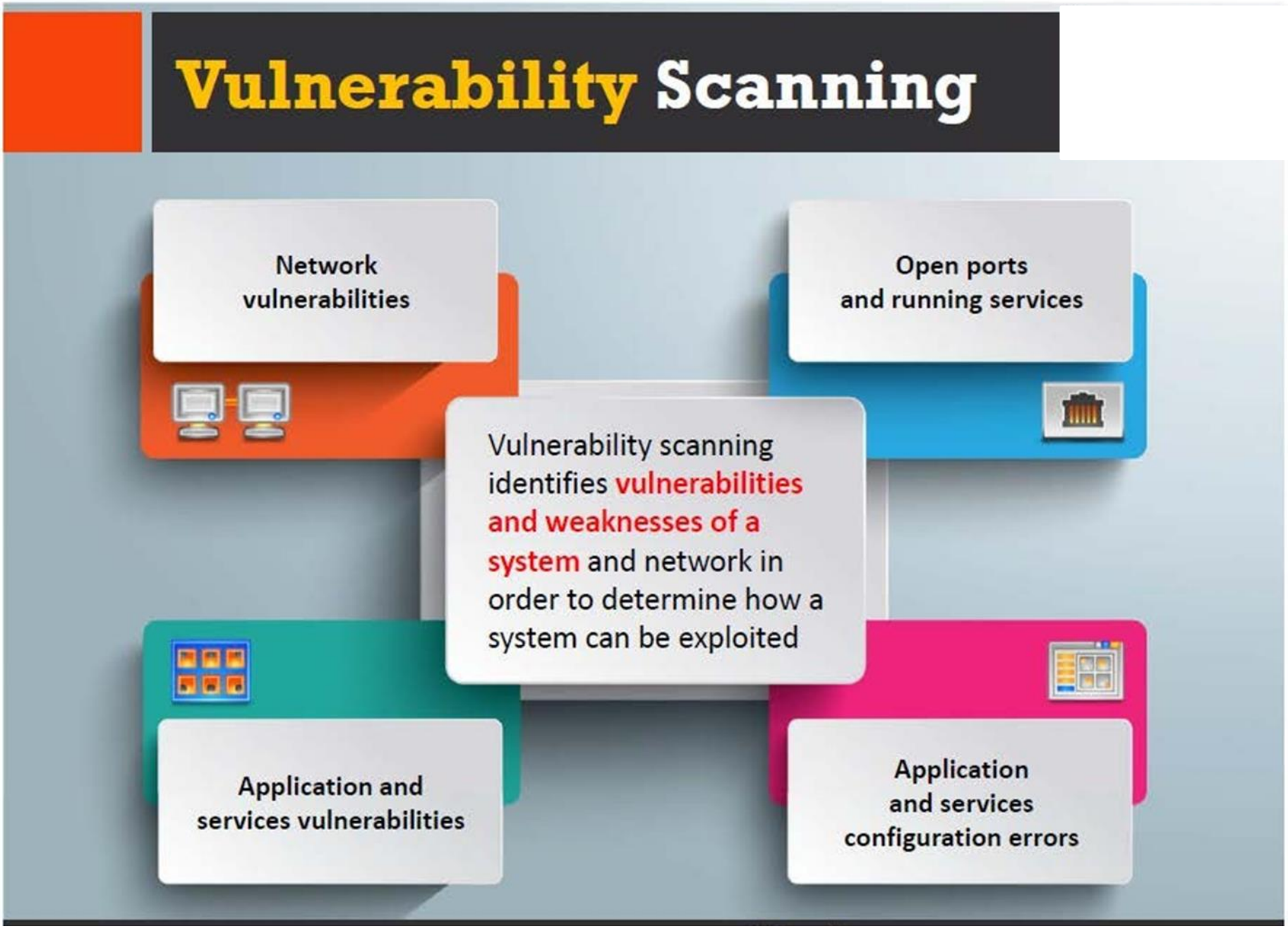


MBSA

- Microsoft Baseline Security Analyzer



Vulnerability Scanning

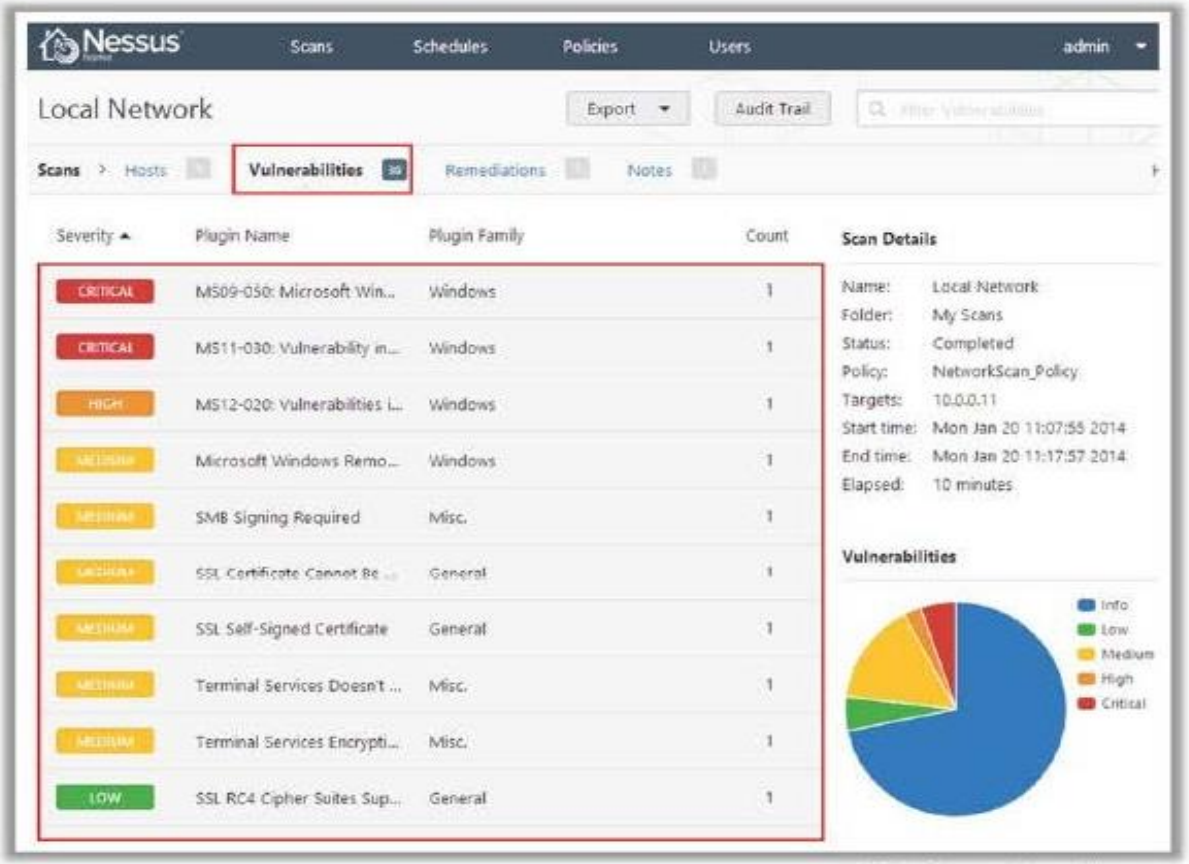


Vulnerability Scanning Tool: Nessus

Nessus is the vulnerability and configuration assessment product

Features

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



http://www.tenable.com

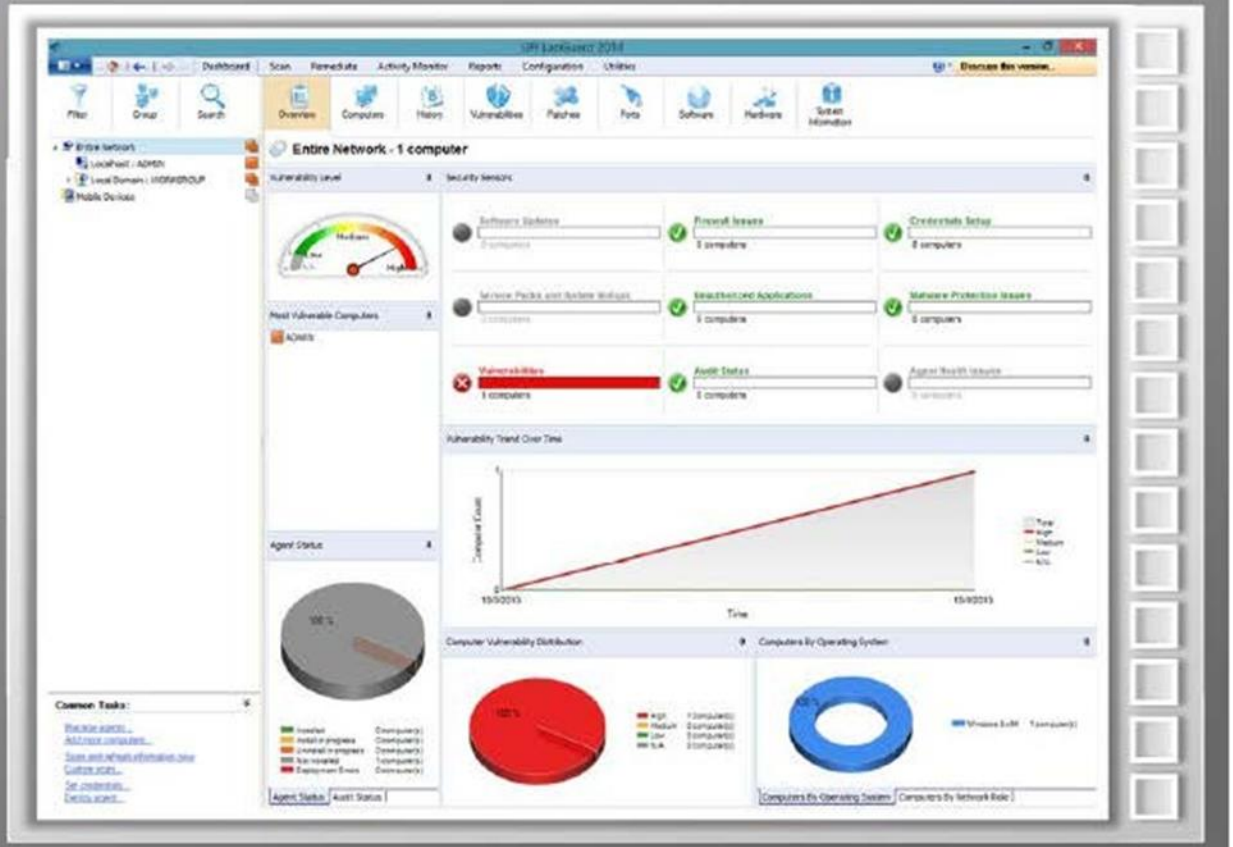
Vulnerability Scanning Tool: GFI LanGuard

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

Features

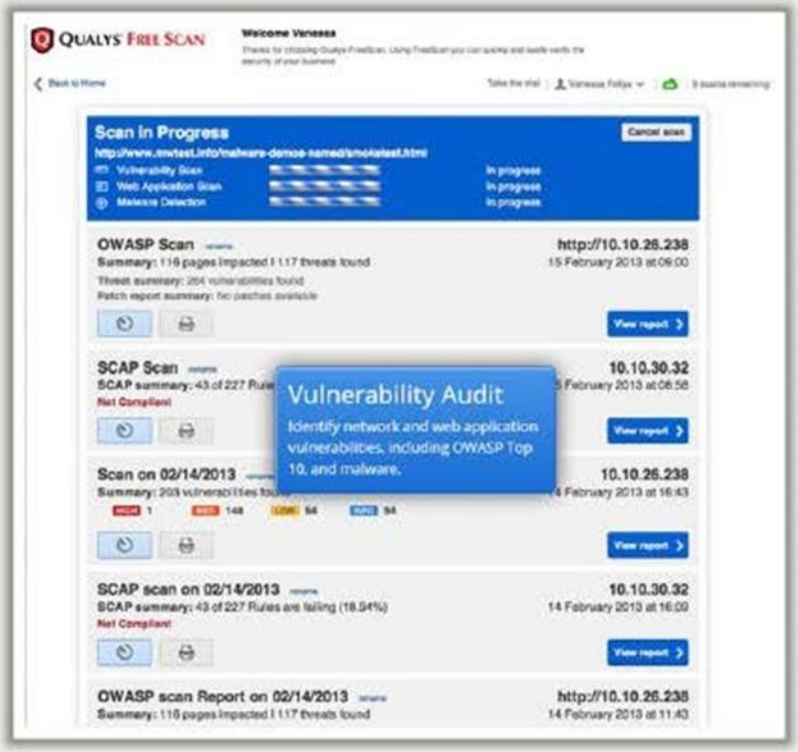
- Selectively creates **custom vulnerability checks**
- Identifies **security vulnerabilities** and takes remedial action
- Creates different types of **scans and vulnerability tests**
- Helps ensure third-party security applications offer **optimum protection**
- Performs **network device vulnerability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

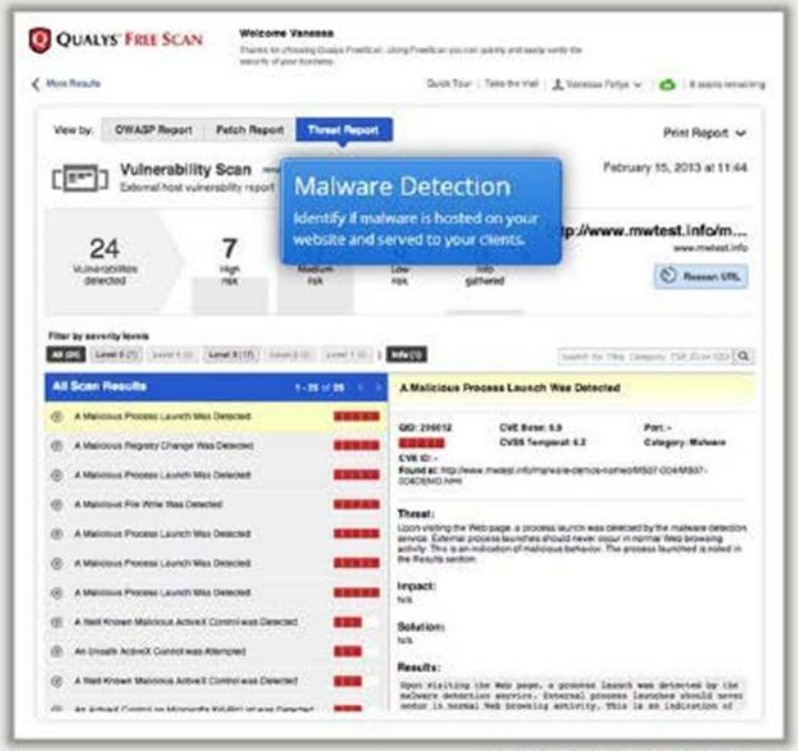
http://www.gfi.com



Vulnerability Scanning Tool: Qualys FreeScan

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





http://www.qualys.com

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

Network Vulnerability Scanners

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

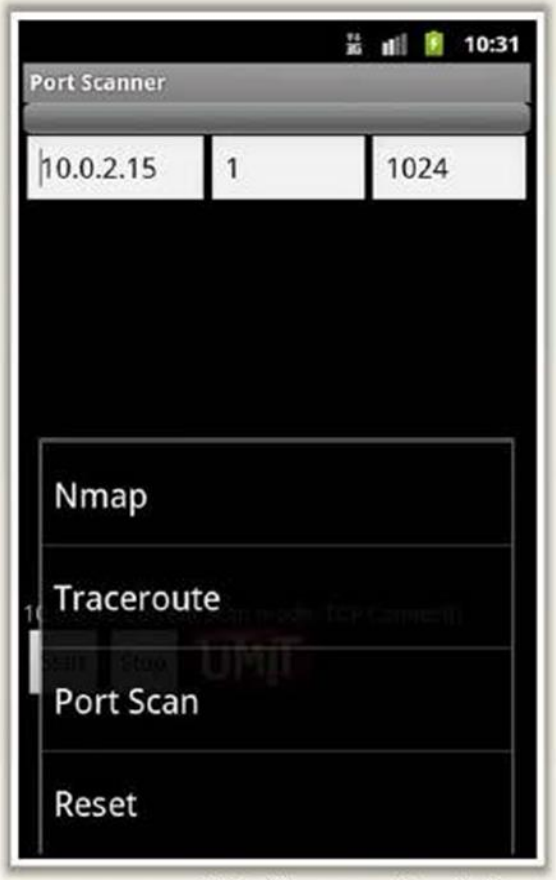
Nexpose
http://www.rapid7.com

SAINT
http://www.saintcorporation.com

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

Scanning Tools for Mobile

Umit Network Scanner



http://www.umitproject.org

Fing

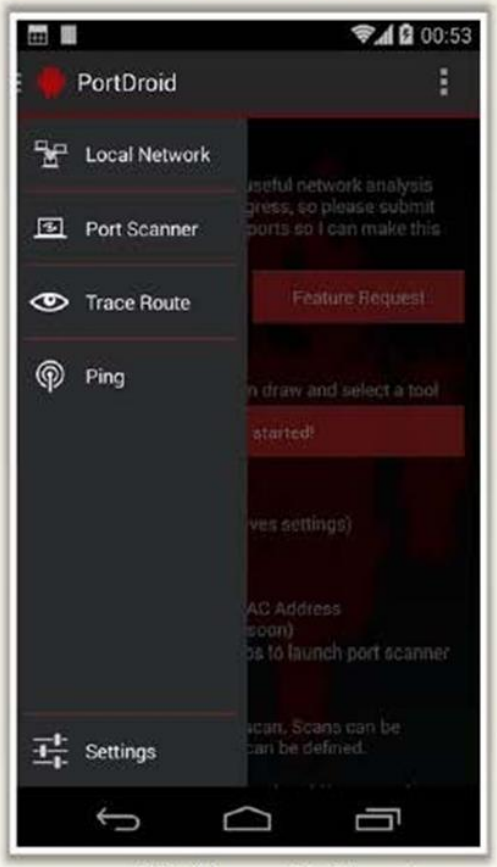
http://www.overlooksoft.com

IP Network Scanner

http://10base-t.com

Scanning Tools for Mobile (Cont'd)

PortDroid Network Analysis



http://www.stealthcopter.com

Pamn IP Scanner

http://pips.wjholden.com

Network Discovery

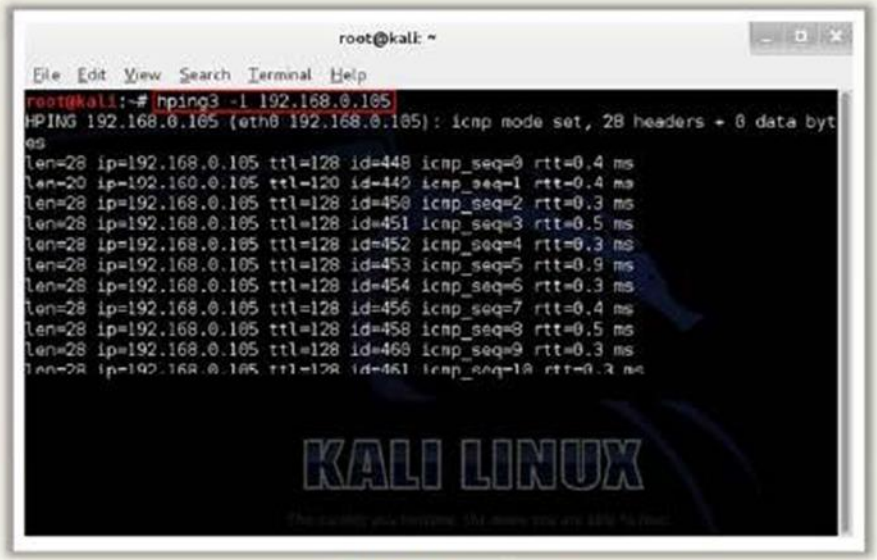
http://rorist.github.io

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



ICMP Scanning

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

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

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.