Sniffing

Jayson Waigwa - Security Analyst

Strathmore UNIVERSITY

Outline

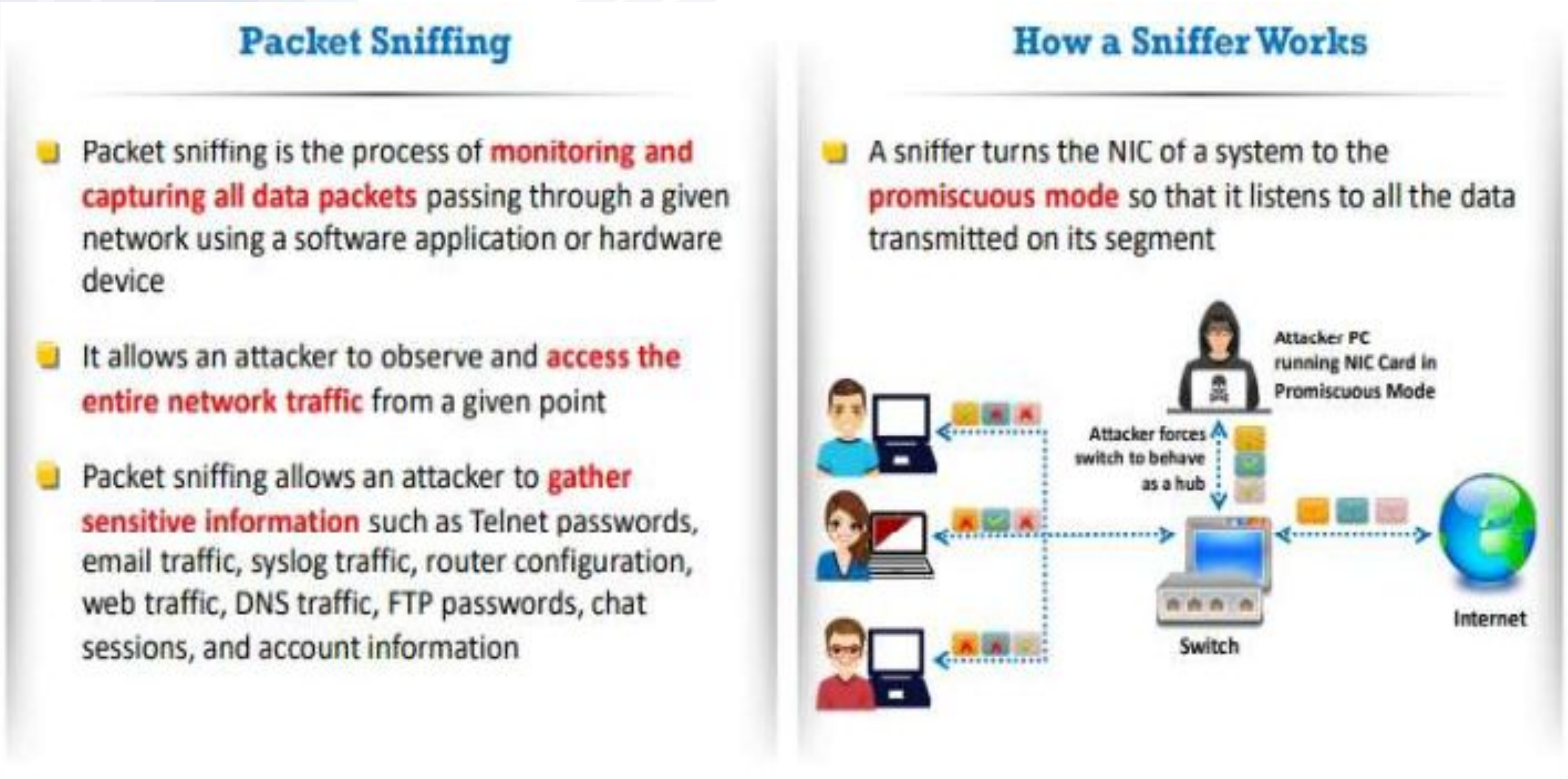
Strathmore UNIVERSITY

SESSION	CONTENT
1	Concepts of Sniffing
2	Sniffing Techniques
3	Defending against sniffing
4	Sniffing Tools
5	Sniffing Countermeasures

Introduction

- Sniffing is the process of monitoring and capturing all data packets passing through a given network.

Network Sniffing



Packet Sniffing

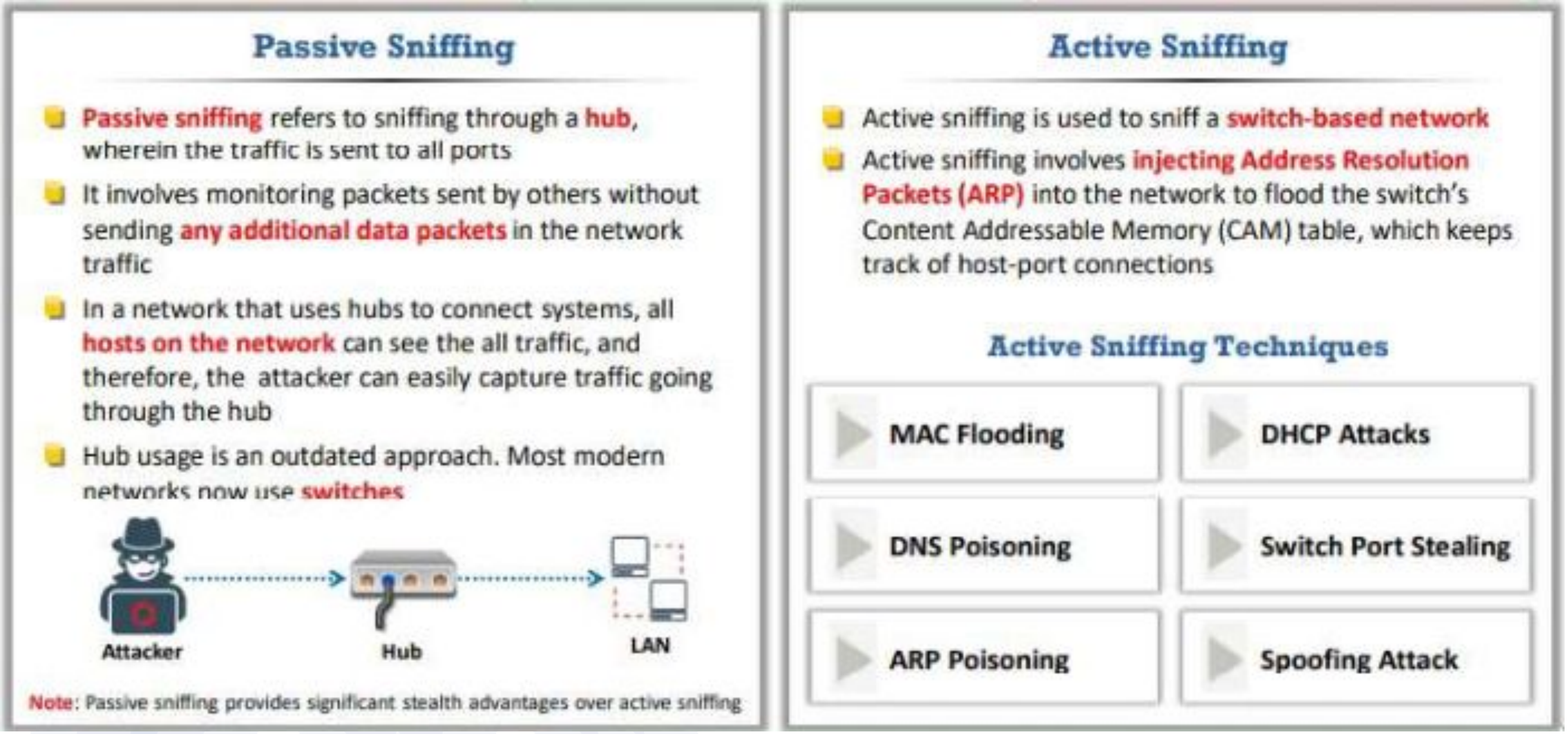
- Packet sniffing is the process of **monitoring and capturing all data packets** passing through a given network using a software application or hardware device
- It allows an attacker to observe and **access the entire network traffic** from a given point
- Packet sniffing allows an attacker to **gather sensitive information** such as Telnet passwords, email traffic, syslog traffic, router configuration, web traffic, DNS traffic, FTP passwords, chat sessions, and account information

How a Sniffer Works

- A sniffer turns the NIC of a system to the **promiscuous mode** so that it listens to all the data transmitted on its segment

Attacker PC running NIC Card in Promiscuous Mode
Attacker forces switch to behave as a hub
Switch
Internet

Types of Sniffing



Passive Sniffing

- **Passive sniffing** refers to sniffing through a **hub**, wherein the traffic is sent to all ports
- It involves monitoring packets sent by others without sending **any additional data packets** in the network traffic
- In a network that uses hubs to connect systems, all **hosts on the network** can see the all traffic, and therefore, the attacker can easily capture traffic going through the hub
- Hub usage is an outdated approach. Most modern networks now use **switches**

Note: Passive sniffing provides significant stealth advantages over active sniffing

Active Sniffing

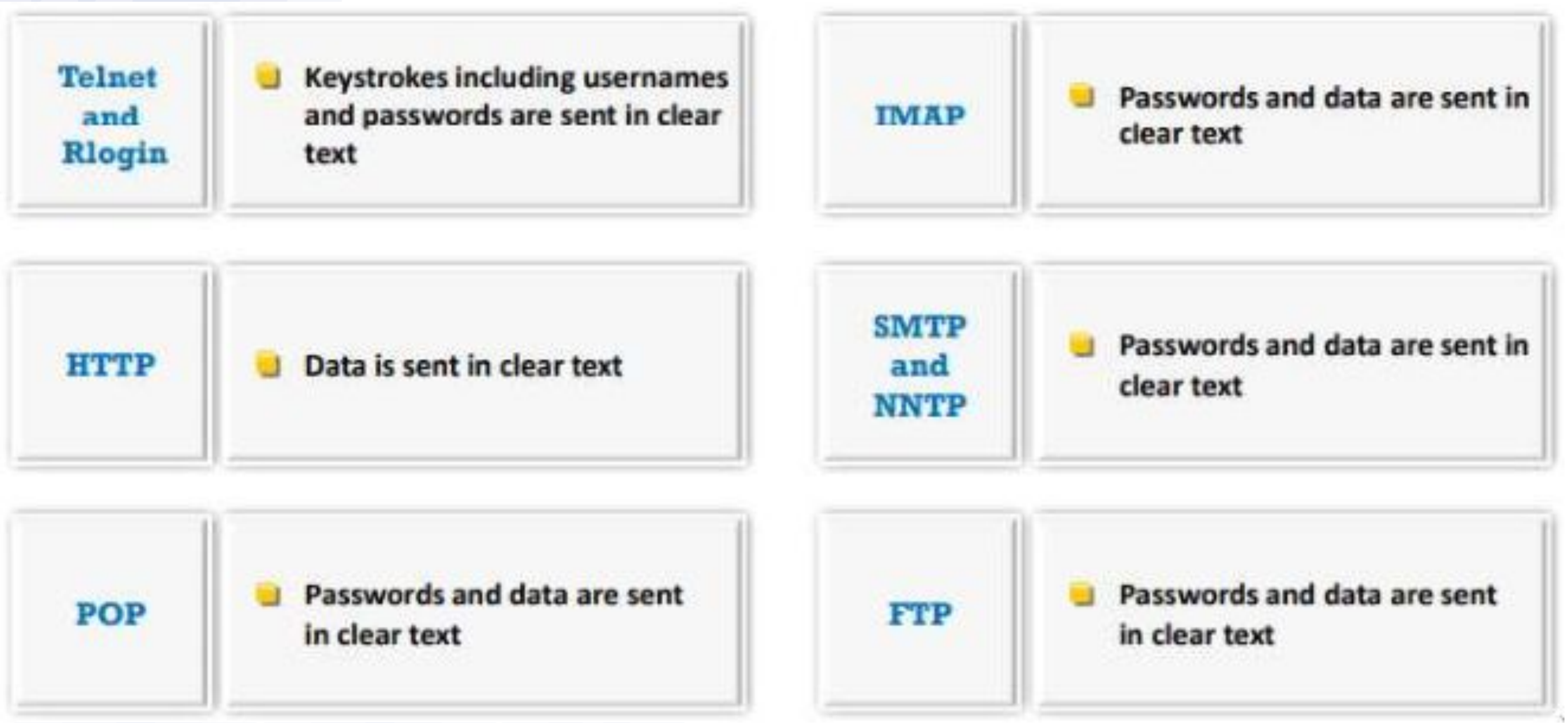
- Active sniffing is used to sniff a **switch-based network**
- Active sniffing involves **injecting Address Resolution Packets (ARP)** into the network to flood the switch's Content Addressable Memory (CAM) table, which keeps track of host-port connections

Active Sniffing Techniques

- MAC Flooding
- DHCP Attacks
- DNS Poisoning
- Switch Port Stealing
- ARP Poisoning
- Spoofing Attack

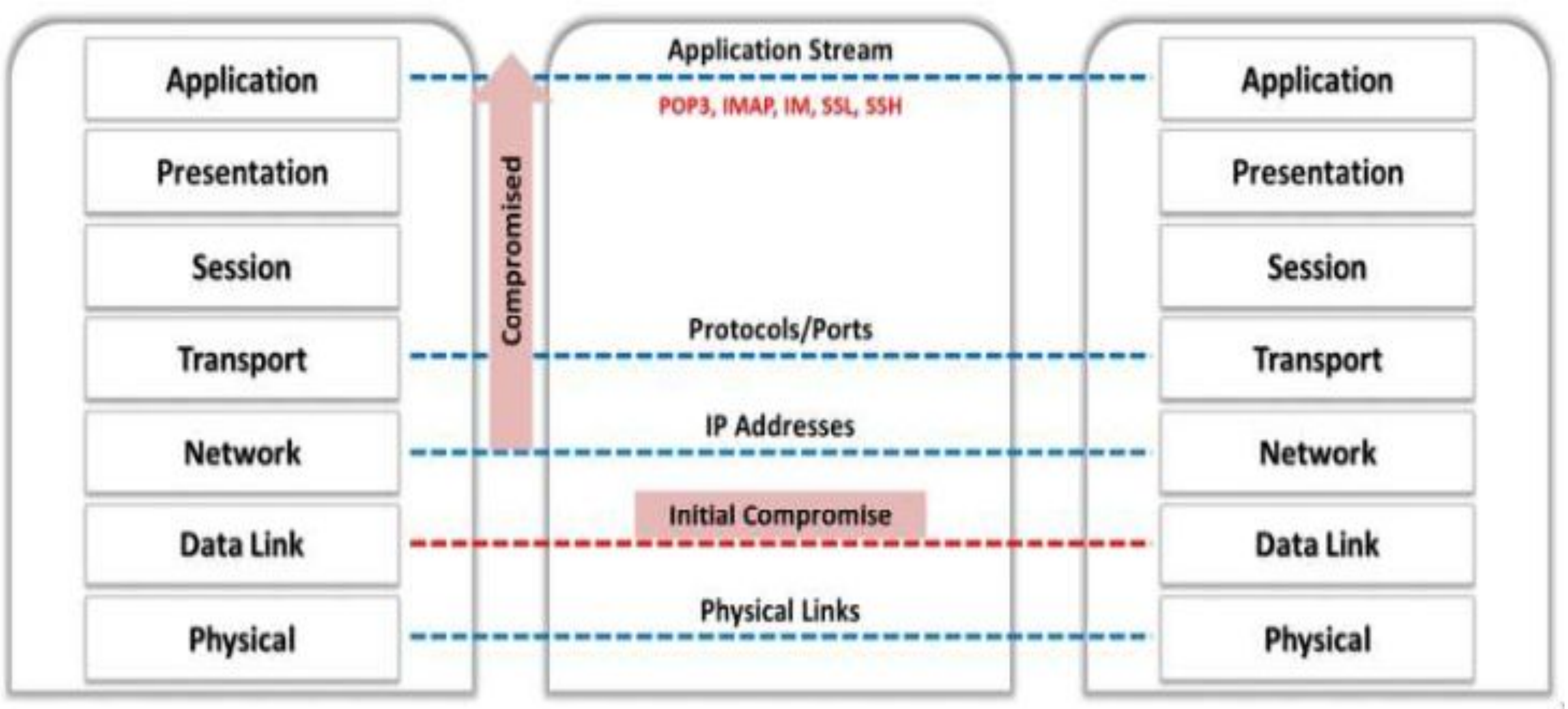
- **ARP Spoofing** - Stateless, a machine can send ARP reply even without requesting, it can also accept replies.
- **MAC Flooding** - happens when the attacker tries to send numerable invalid MAC addresses to the MAC table. It floods the source table with the invalid MAC addresses.

Protocols Vulnerable to sniffing

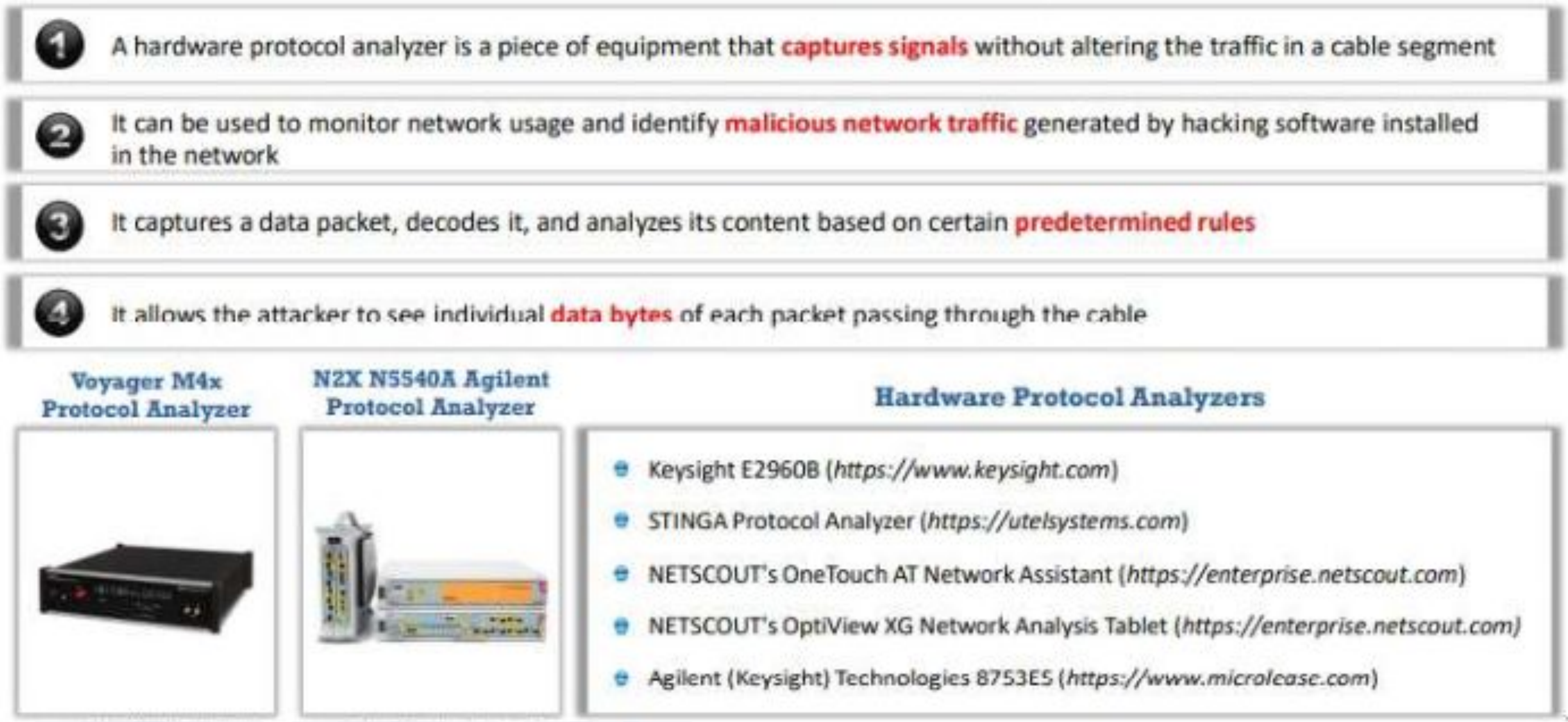


Telnet and Rlogin	Keystrokes including usernames and passwords are sent in clear text	IMAP	Passwords and data are sent in clear text
HTTP	Data is sent in clear text	SMTP and NNTP	Passwords and data are sent in clear text
POP	Passwords and data are sent in clear text	FTP	Passwords and data are sent in clear text

Sniffing in the OSI Model



Hardware protocol Analyzers



1 A hardware protocol analyzer is a piece of equipment that **captures signals** without altering the traffic in a cable segment

2 It can be used to monitor network usage and identify **malicious network traffic** generated by hacking software installed in the network

3 It captures a data packet, decodes it, and analyzes its content based on certain **predetermined rules**

4 It allows the attacker to see individual **data bytes** of each packet passing through the cable

Voyager M4x Protocol Analyzer

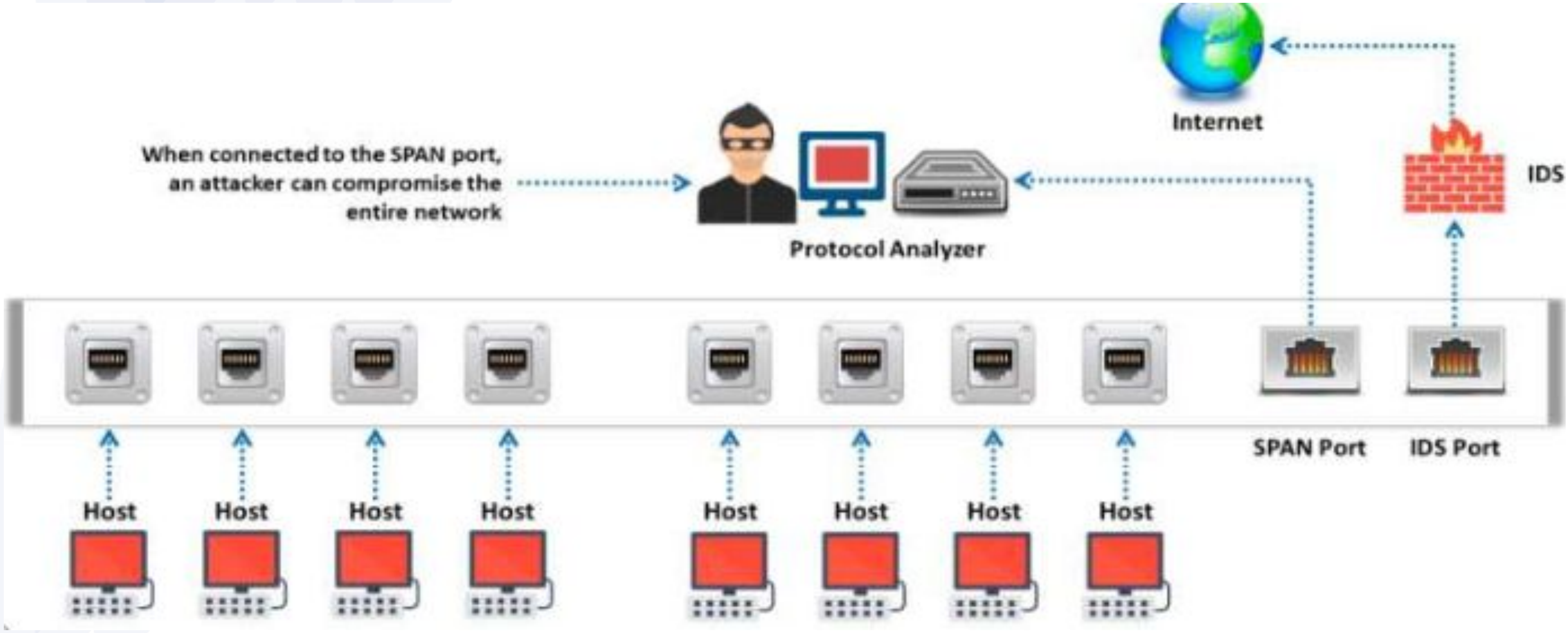
N2X N5540A Agilent Protocol Analyzer

Hardware Protocol Analyzers

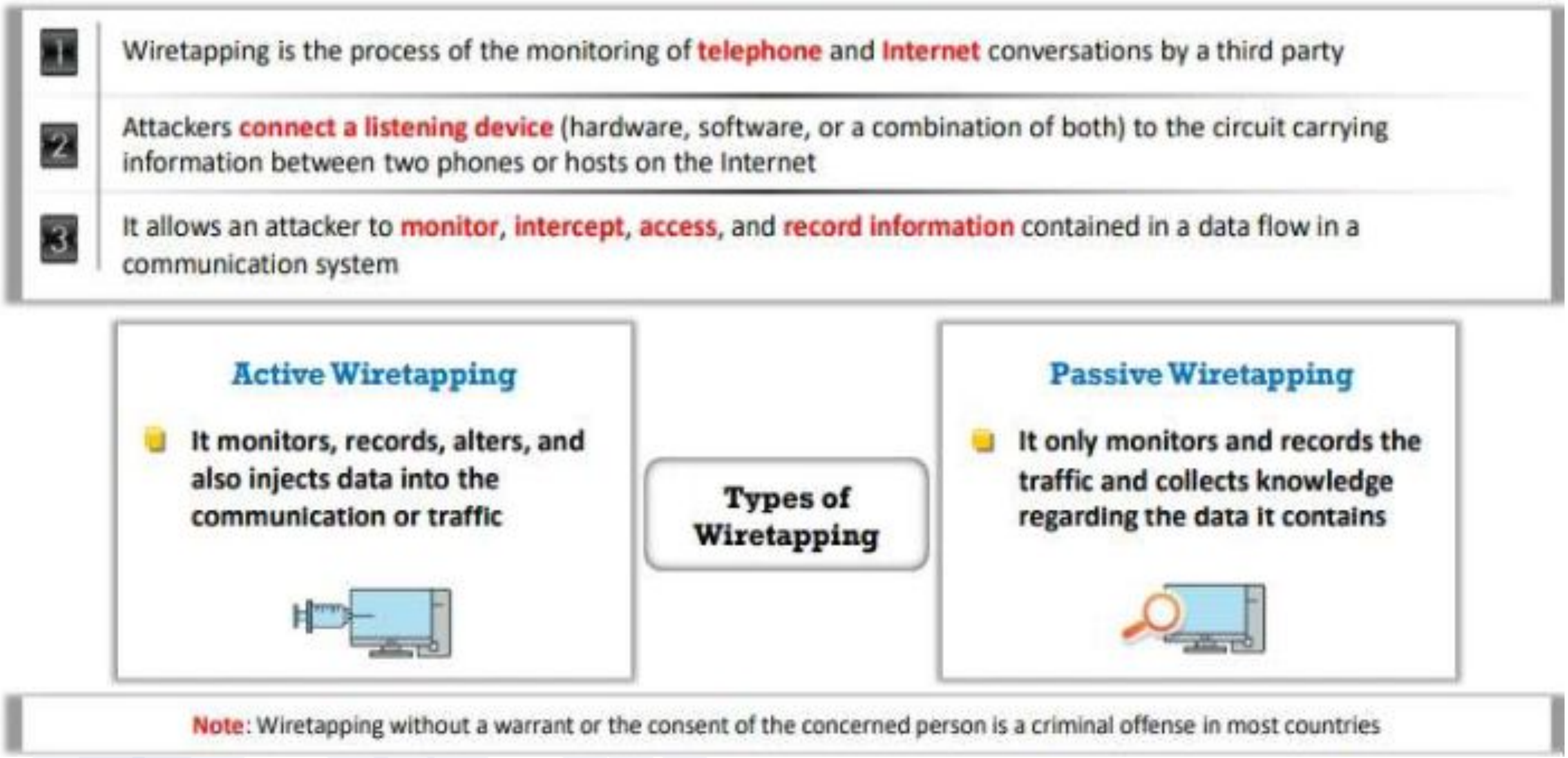
- Keysight E2960B (*https://www.keysight.com*)
- STINGA Protocol Analyzer (*https://utelsystems.com*)
- NETSCOUT's OneTouch AT Network Assistant (*https://enterprise.netscout.com*)
- NETSCOUT's OptiView XG Network Analysis Tablet (*https://enterprise.netscout.com*)
- Agilent (Keysight) Technologies 8753ES (*https://www.microlease.com*)

SPAN Port

- Switched Port Analyzer is a CISCO feature that monitors network traffic on one or more ports on the switch.


Internet
When connected to the SPAN port, an attacker can compromise the entire network
Protocol Analyzer
IDS
SPAN Port
IDS Port
Host
Host
Host
Host
Host
Host
Host
Host

Wiretapping



1 Wiretapping is the process of the monitoring of **telephone** and **Internet** conversations by a third party

2 Attackers **connect a listening device** (hardware, software, or a combination of both) to the circuit carrying information between two phones or hosts on the Internet

3 It allows an attacker to **monitor**, **intercept**, **access**, and **record information** contained in a data flow in a communication system

Types of Wiretapping

Active Wiretapping

- It monitors, records, alters, and also injects data into the communication or traffic

Passive Wiretapping

- It only monitors and records the traffic and collects knowledge regarding the data it contains

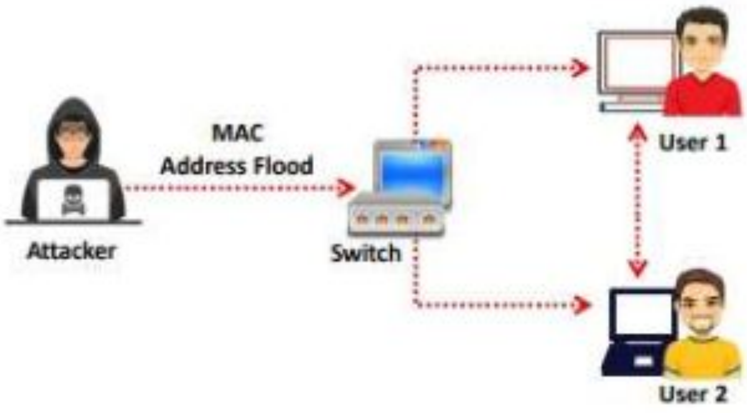
Note: Wiretapping without a warrant or the consent of the concerned person is a criminal offense in most countries

What is Lawful Interception?

Sniffing Techniques

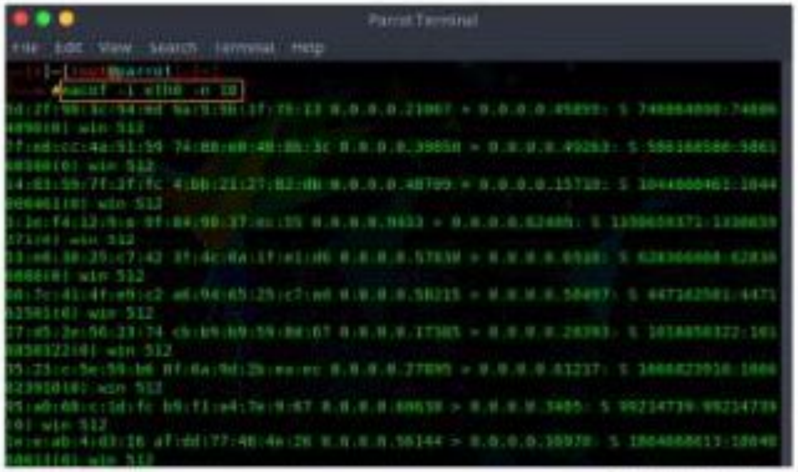
- MAC Attacks
  - Uses MAC flooding technique to force the switch to act as a hub.

- MAC flooding involves the **flooding of the CAM table** with fake MAC address and IP pairs until it is full
- The switch then **acts as a hub** by broadcasting packets to all machines on the network, and therefore, the attackers can sniff the traffic easily



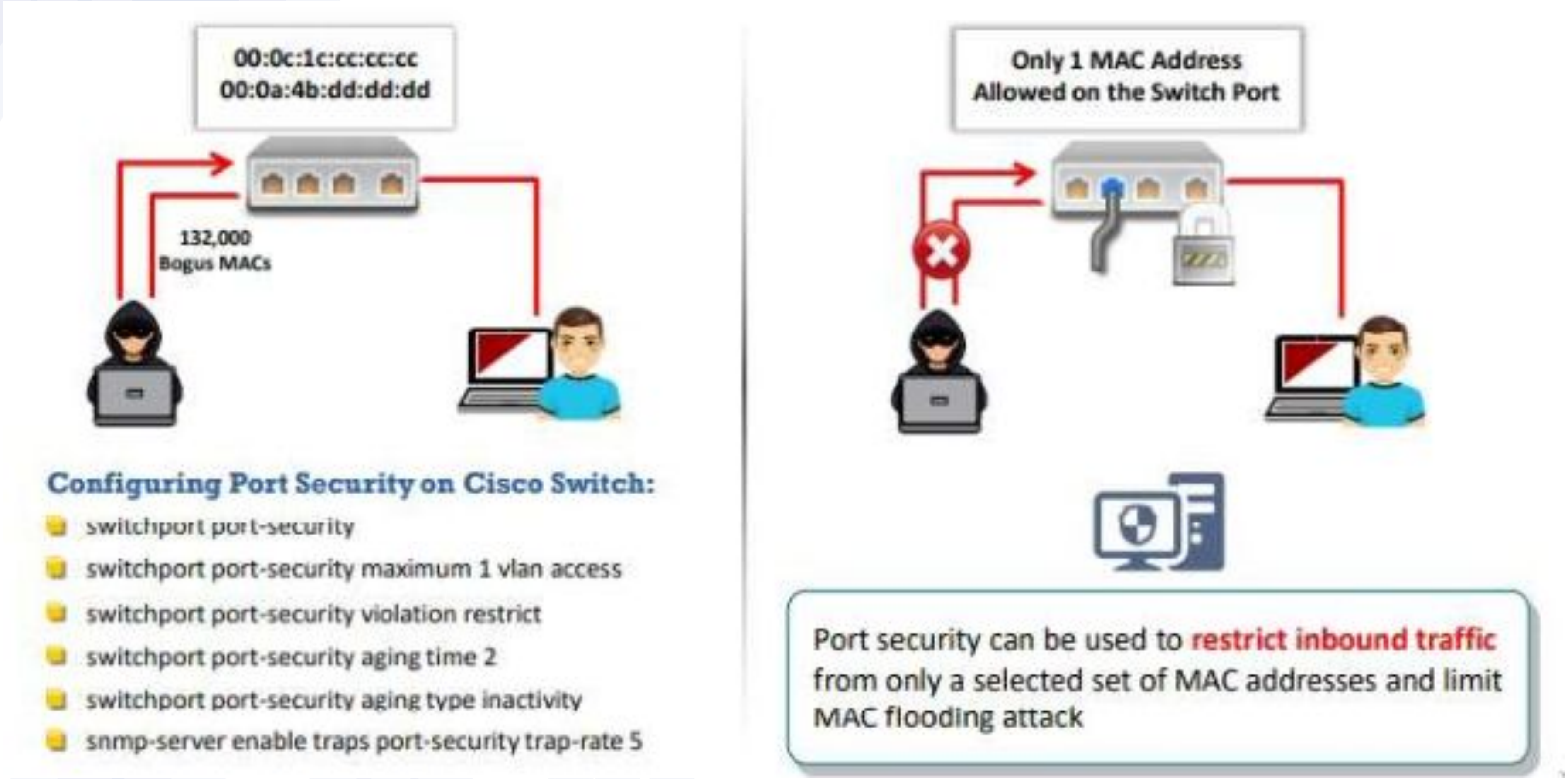
Mac Flooding Switches with macof

- **macof** is a Unix/Linux tool that is a part of the dsniff collection
- macof sends random **source MAC** and **IP addresses**
- This tool **floods the switch's CAM tables** (131,000 per min) by sending bogus MAC entries



```
[illegible]@parrot
macof -i eth0 -n 10
[illegible]
```

Defending against MAC Attacks

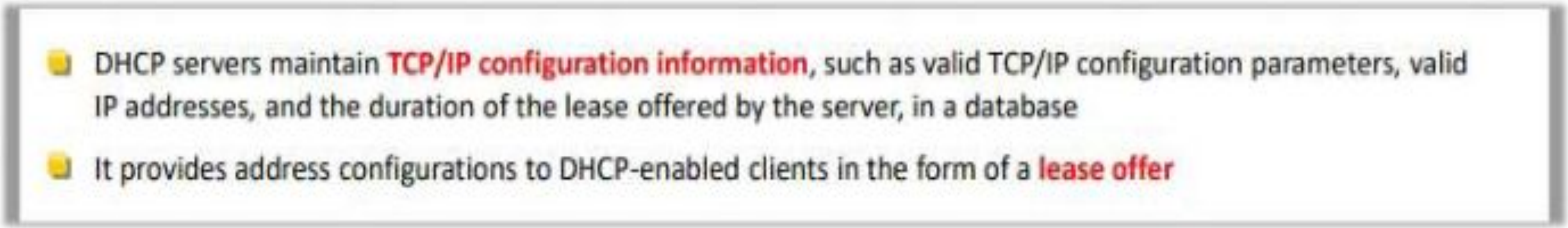


Configuring Port Security on Cisco Switch:

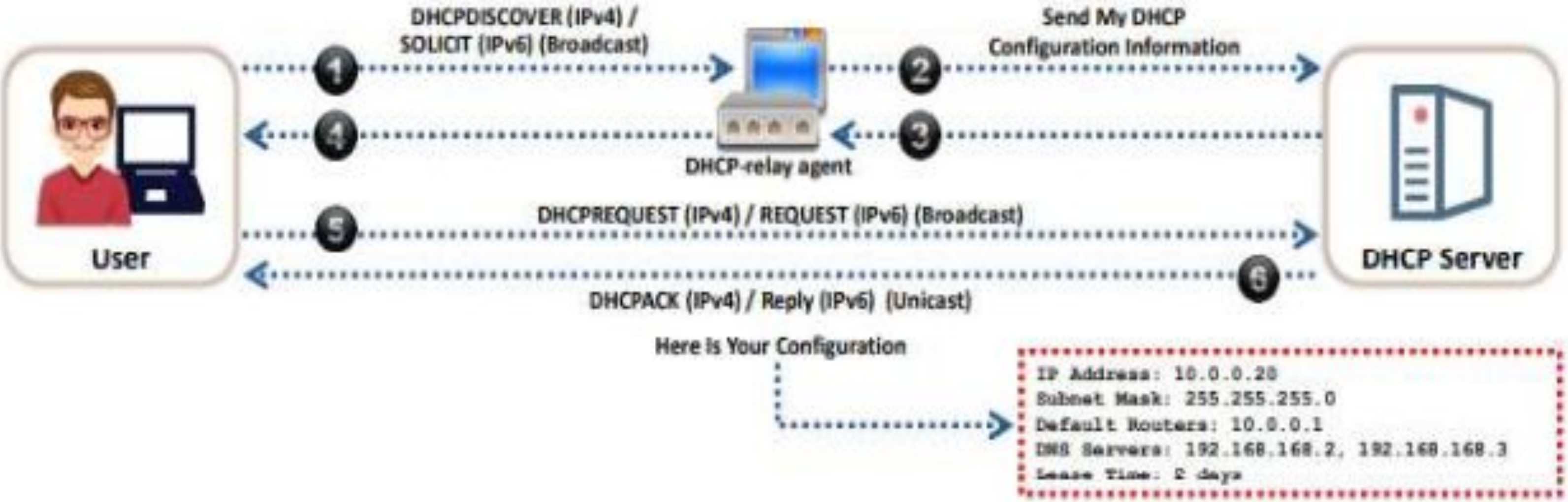
- switchport port-security
- switchport port-security maximum 1 vlan access
- switchport port-security violation restrict
- switchport port-security aging time 2
- switchport port-security aging type inactivity
- snmp-server enable traps port-security trap-rate 5

Port security can be used to **restrict inbound traffic** from only a selected set of MAC addresses and limit MAC flooding attack

DHCP Attacks



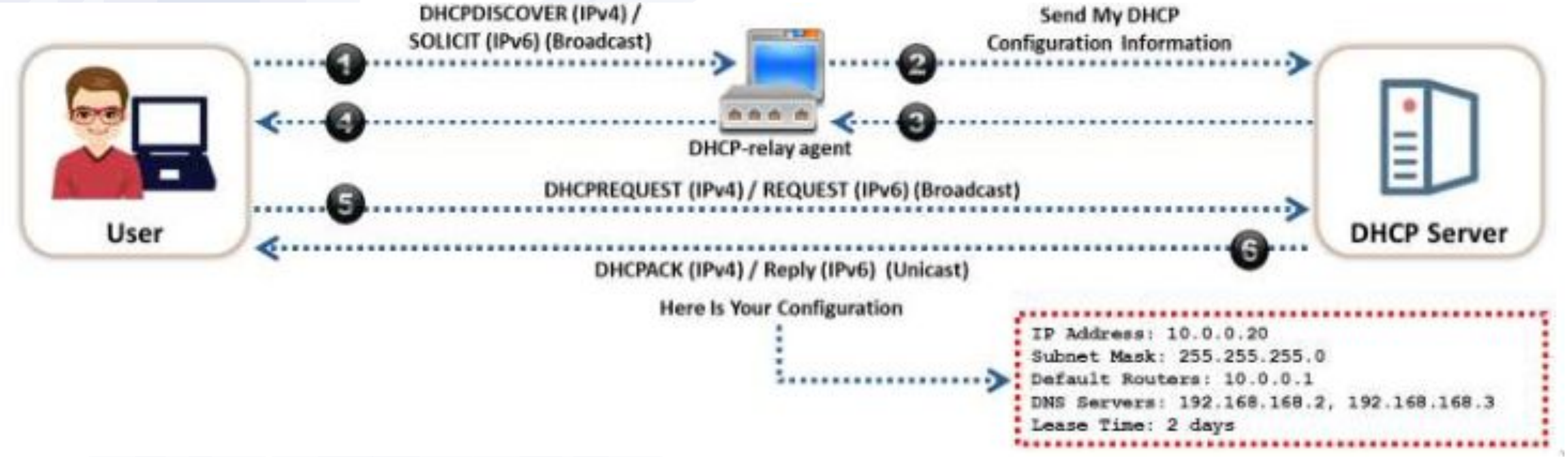
- DHCP servers maintain **TCP/IP configuration information**, such as valid TCP/IP configuration parameters, valid IP addresses, and the duration of the lease offered by the server, in a database
- It provides address configurations to DHCP-enabled clients in the form of a **lease offer**



DHCPDISCOVER (IPv4) / SOLICIT (IPv6) (Broadcast)
Send My DHCP Configuration Information
1
2
3
4
DHCP-relay agent
User
DHCP Server
5
DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)
6
DHCPACK (IPv4) / Reply (IPv6) (Unicast)
Here Is Your Configuration

```
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2, 192.168.168.3
Lease Time: 2 days
```

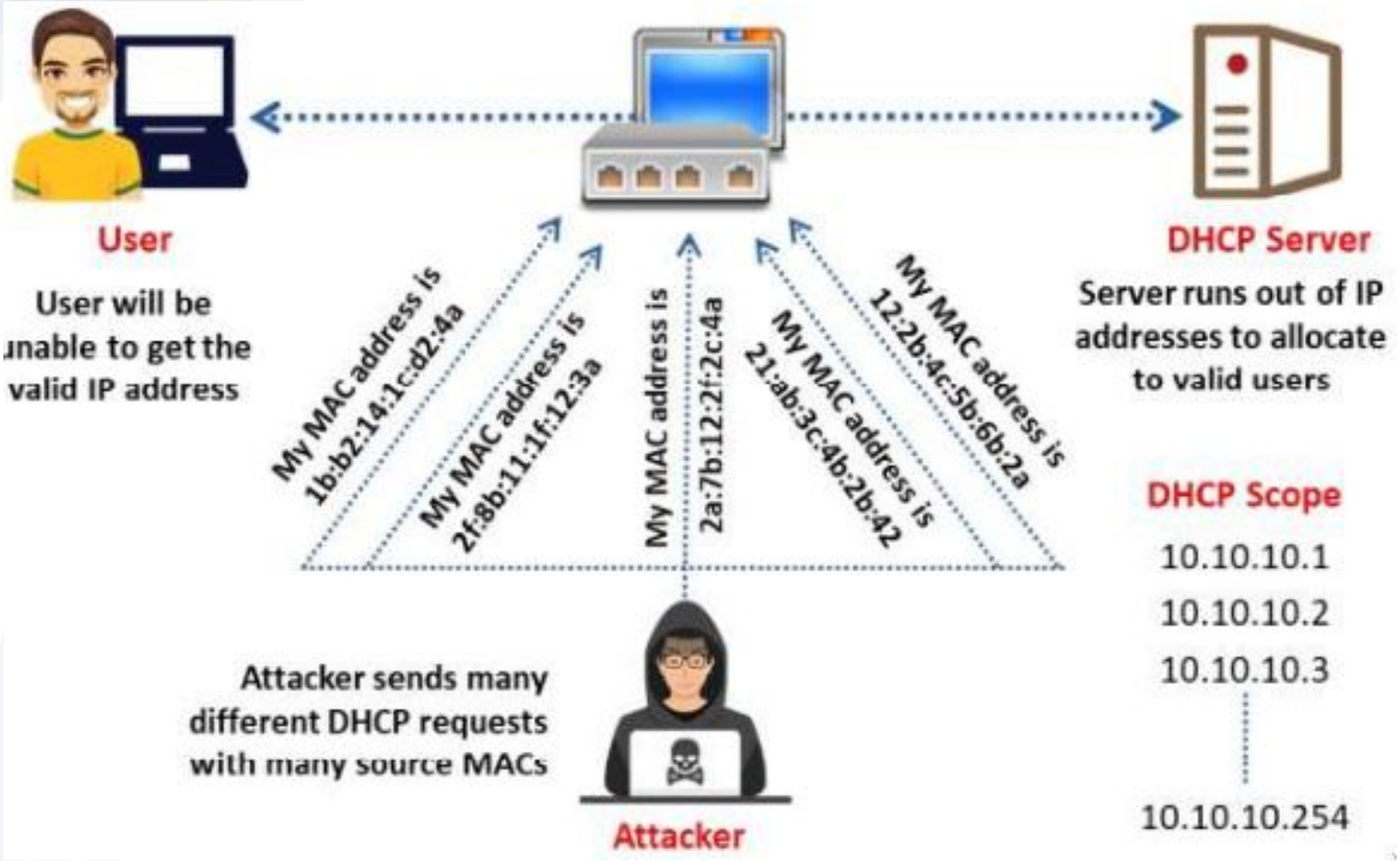
How a DHCP Server Works



DHCPDISCOVER (IPv4) /
SOLICIT (IPv6) (Broadcast)
Send My DHCP
Configuration Information
1
2
3
4
DHCP-relay agent
User
DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)
5
DHCP Server
6
DHCPACK (IPv4) / Reply (IPv6) (Unicast)
Here Is Your Configuration

```
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2, 192.168.168.3
Lease Time: 2 days
```

DHCP Starvation Attack



User
DHCP Server
Attacker
My MAC address is 1b:b2:14:1c:d2:4a
My MAC address is 2f:8b:11:1f:12:3a
My MAC address is 2a:7b:12:2f:2c:4a
My MAC address is 21:ab:3c:4b:2b:42
My MAC address is 12:2b:4c:5b:6b:2a
DHCP Scope
10.10.10.1
10.10.10.2
10.10.10.3
10.10.10.254

User will be unable to get the valid IP address

Server runs out of IP addresses to allocate to valid users

Attacker sends many different DHCP requests with many source MACs

DHCP Starvation tools

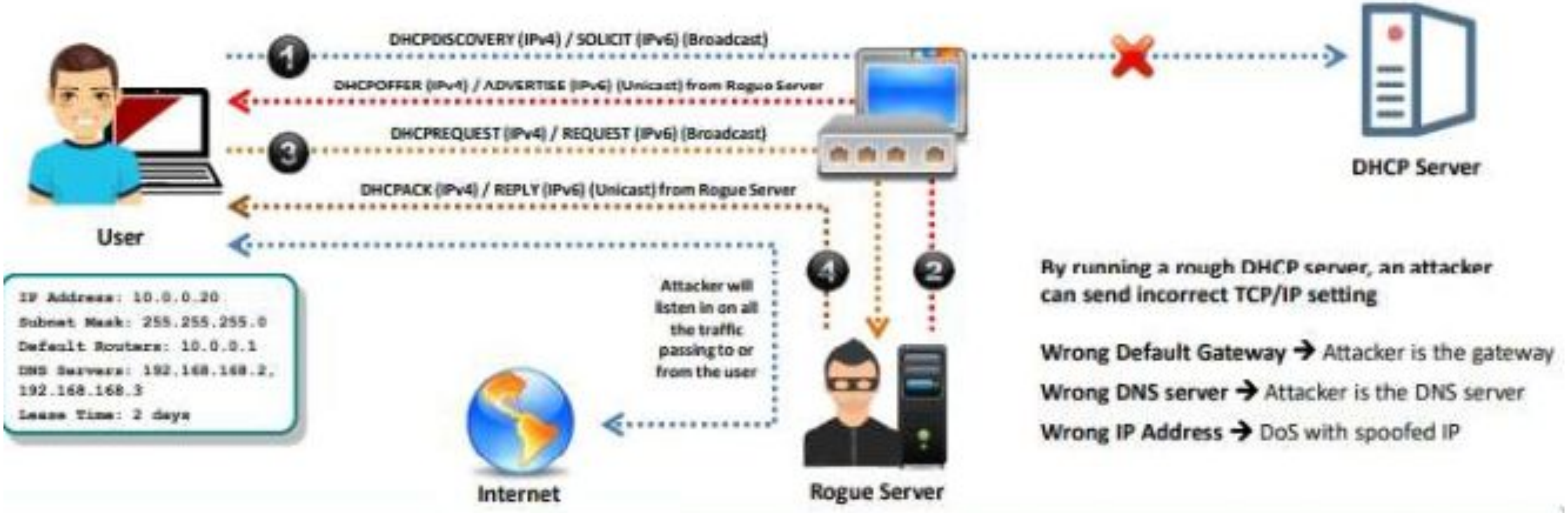
- Yersinia
- Hyenae
- dhcpstarv
- Gobbler
- DHCPig

Rogue DHCP Server Attack

Strathmore UNIVERSITY

1 The attacker sets up a **rogue DHCP server** on the network and responds to DHCP requests with bogus IP addresses resulting in compromised network access

2 This attack works in conjunction with the DHCP starvation attack; the attacker sends a **TCP/IP setting** to the user after knocking him/her out from the genuine DHCP server


DHCPDISCOVERY (IPv4) / SOLICIT (IPv6) (Broadcast)
1
DHCPOFFER (IPv4) / ADVERTISE (IPv6) (Unicast) from Rogue Server
DHCPREQUEST (IPv4) / REQUEST (IPv6) (Broadcast)
3
DHCPACK (IPv4) / REPLY (IPv6) (Unicast) from Rogue Server
DHCP Server
User
4
2
Attacker will listen in on all the traffic passing to or from the user
Internet
Rogue Server

```
IP Address: 10.0.0.20
Subnet Mask: 255.255.255.0
Default Routers: 10.0.0.1
DNS Servers: 192.168.168.2,
192.168.168.3
Lease Time: 2 days
```

By running a rough DHCP server, an attacker can send incorrect TCP/IP setting

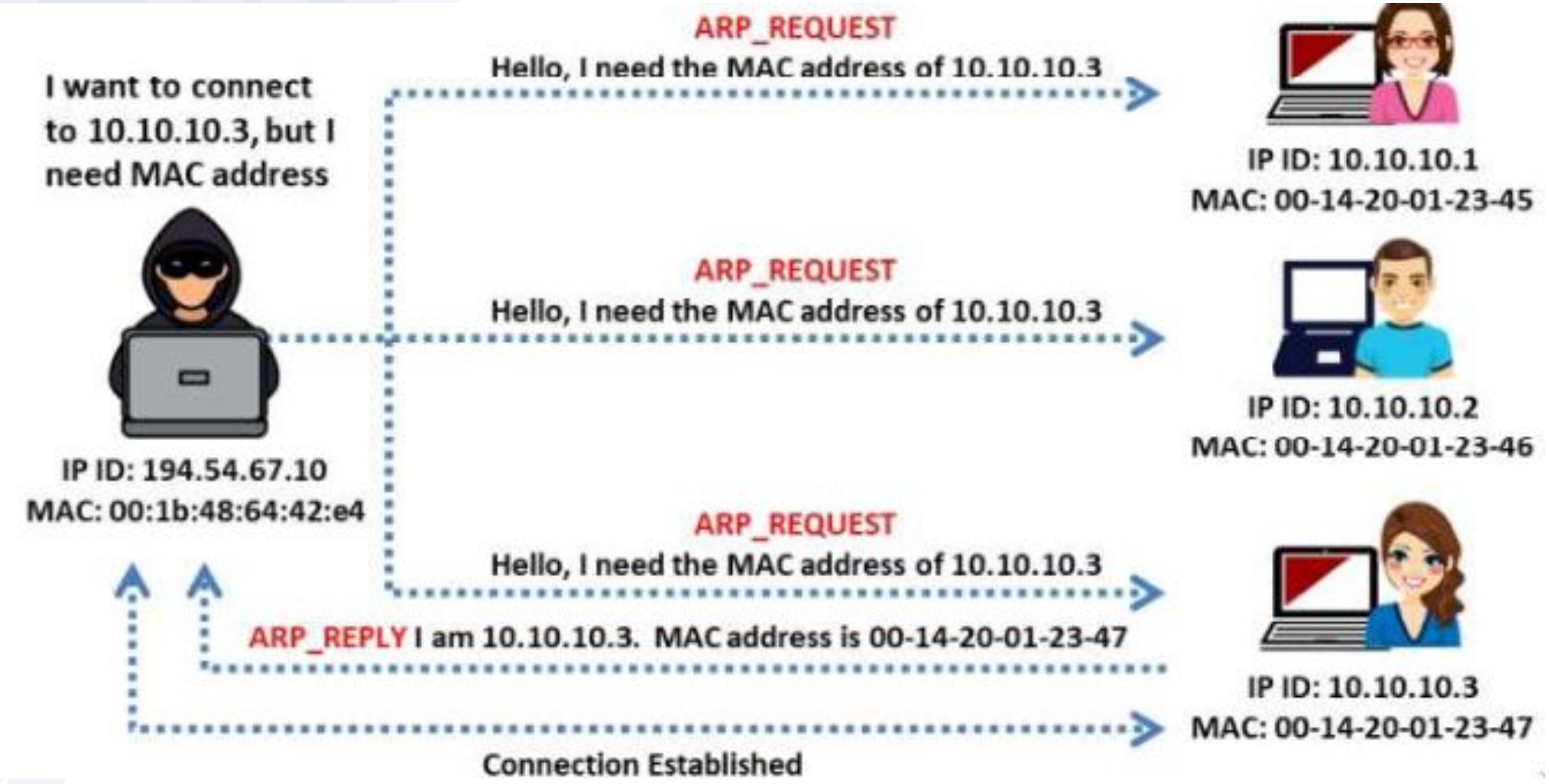
Wrong Default Gateway → Attacker is the gateway

Wrong DNS server → Attacker is the DNS server

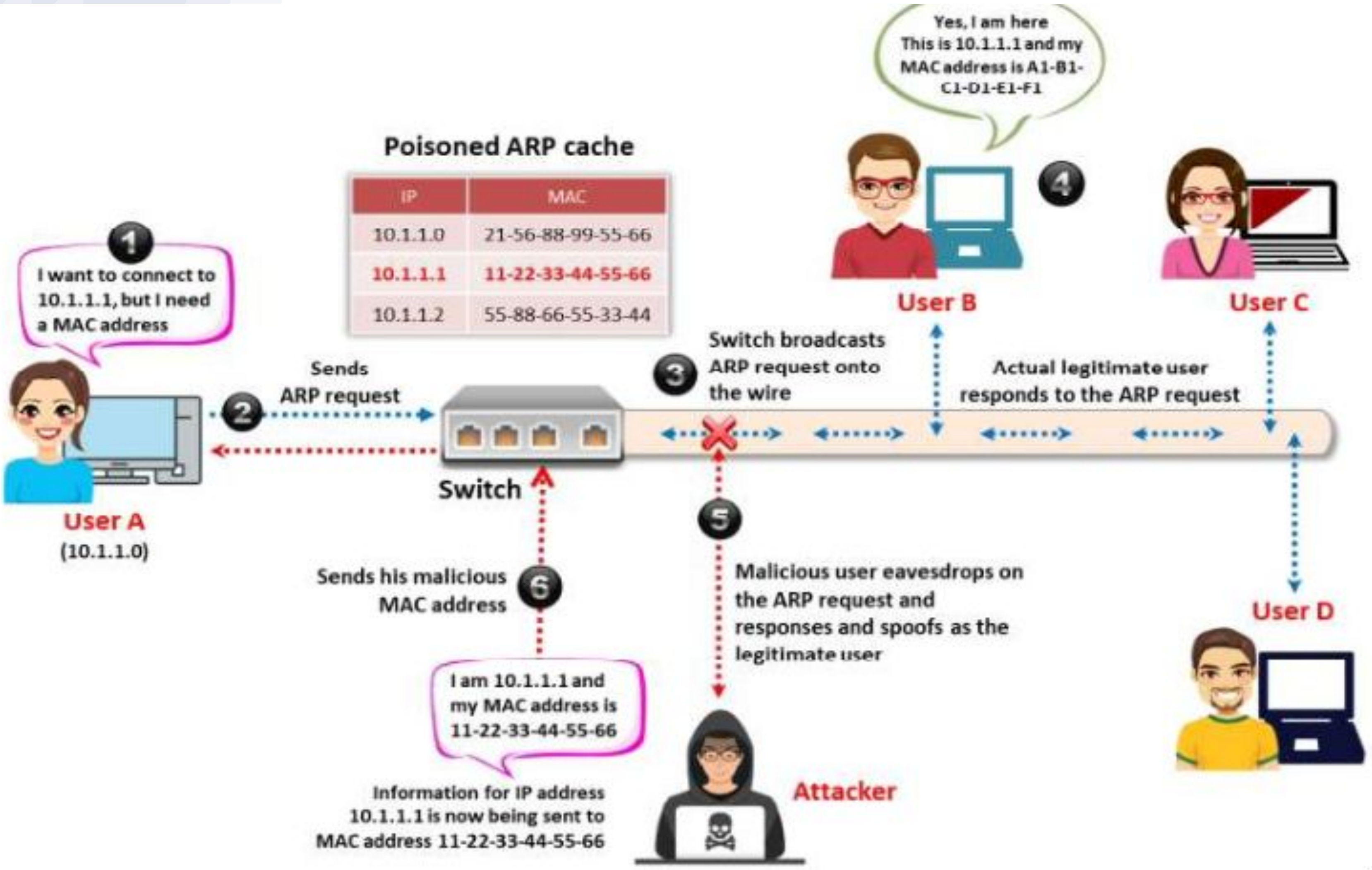
Wrong IP Address → DoS with spoofed IP

Address Resolution Protocol

Resolves IP Address to MAC address of the interface to send data.


I want to connect to 10.10.10.3, but I need MAC address
IP ID: 194.54.67.10
MAC: 00:1b:48:64:42:e4
ARP_REQUEST
Hello, I need the MAC address of 10.10.10.3
IP ID: 10.10.10.1
MAC: 00-14-20-01-23-45
ARP_REQUEST
Hello, I need the MAC address of 10.10.10.3
IP ID: 10.10.10.2
MAC: 00-14-20-01-23-46
ARP_REQUEST
Hello, I need the MAC address of 10.10.10.3
ARP_REPLY I am 10.10.10.3. MAC address is 00-14-20-01-23-47
IP ID: 10.10.10.3
MAC: 00-14-20-01-23-47
Connection Established

ARP Spoofing Attack



Poisoned ARP cache

IP	MAC
10.1.1.0	21-56-88-99-55-66
10.1.1.1	11-22-33-44-55-66
10.1.1.2	55-88-66-55-33-44

1 I want to connect to 10.1.1.1, but I need a MAC address

2 Sends ARP request

3 Switch broadcasts ARP request onto the wire

4 Yes, I am here This is 10.1.1.1 and my MAC address is A1-B1-C1-D1-E1-F1

Actual legitimate user responds to the ARP request

5 Malicious user eavesdrops on the ARP request and responses and spoofs as the legitimate user

6 Sends his malicious MAC address

I am 10.1.1.1 and my MAC address is 11-22-33-44-55-66

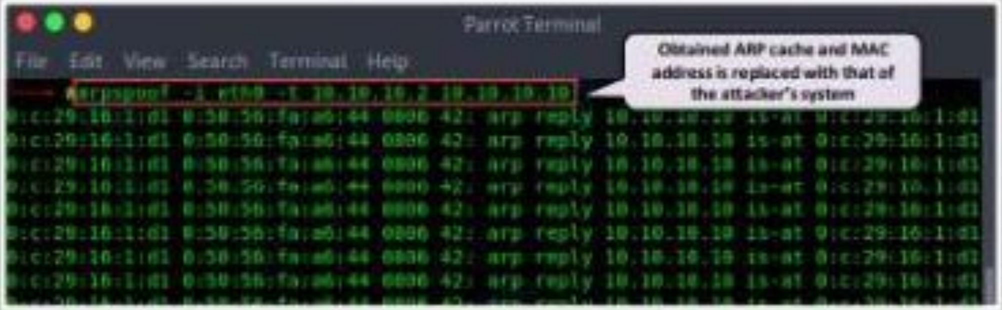
Information for IP address 10.1.1.1 is now being sent to MAC address 11-22-33-44-55-66

What are the Threats of ARP poisoning?

ARP Poisoning Tools

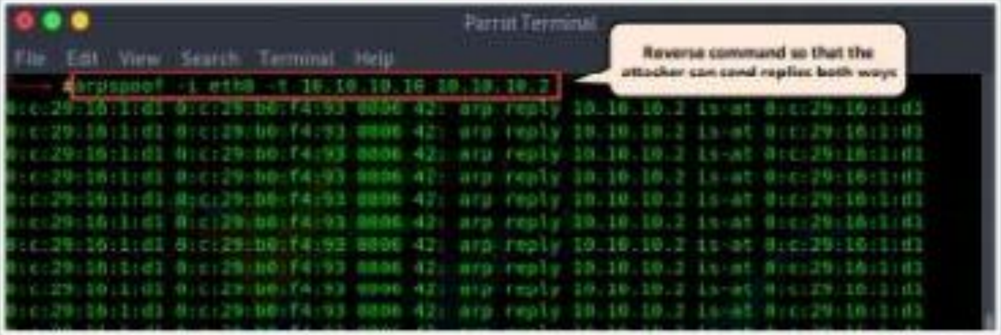
arpspoof

arpspoof **redirects packets** from a target host (or all hosts) on the LAN intended for another host on the LAN by forging ARP replies



```
arpspoof -i eth0 -t 10.10.10.2 10.10.10.10
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:50:56:fa:a6:44 0806 42: arp reply 10.10.10.10 is-at 0:c:29:16:1:d1
```

Obtained ARP cache and MAC address is replaced with that of the attacker's system



```
arpspoof -i eth0 -t 10.10.10.10 10.10.10.2
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
0:c:29:16:1:d1 0:c:29:b0:f4:93 0806 42: arp reply 10.10.10.2 is-at 0:c:29:16:1:d1
```

Reverse command so that the attacker can send replies both ways

BetterCAP
https://www.bettercap.org

Ettercap
http://www.ettercap-project.org

dsniff
https://www.monkey.org

MITMf
https://github.com

Arpoison
https://sourceforge.net

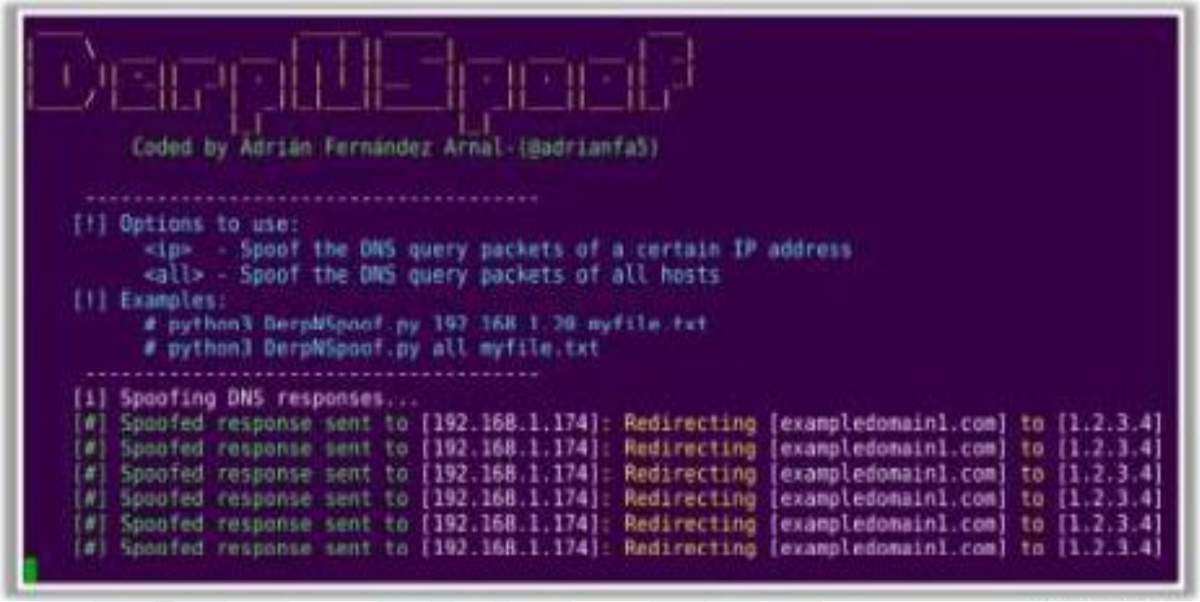
Other Techniques

- IRDP Spoofing - Can be used to launch MITM attack and DoS Attack
- VLAN Hopping - Can be used to steal sensitive information.
- STP Attack - Attacker sets up a less priority switch in the network making it the root bridge.
- DNS Poisoning

DNS Poisoning Tools

DerpNSpoof

DerpNSpoof is a DNS poisoning tool that assists in spoofing the **DNS query packet** of a certain IP address or a group of hosts in the network



```
      Coded by Adrián Fernández Arnal-(@adrianfa5)

  -------------------------------------
 [!] Options to use:
       <ip>  - Spoof the DNS query packets of a certain IP address
       <all> - Spoof the DNS query packets of all hosts
 [!] Examples:
       # python3 DerpNSpoof.py 192.168.1.20 myfile.txt
       # python3 DerpNSpoof.py all myfile.txt
  -------------------------------------
 [i] Spoofing DNS responses...
 [#] Spoofed response sent to [192.168.1.174]: Redirecting [exampledomain1.com] to [1.2.3.4]
 [#] Spoofed response sent to [192.168.1.174]: Redirecting [exampledomain1.com] to [1.2.3.4]
 [#] Spoofed response sent to [192.168.1.174]: Redirecting [exampledomain1.com] to [1.2.3.4]
 [#] Spoofed response sent to [192.168.1.174]: Redirecting [exampledomain1.com] to [1.2.3.4]
 [#] Spoofed response sent to [192.168.1.174]: Redirecting [exampledomain1.com] to [1.2.3.4]
 [#] Spoofed response sent to [192.168.1.174]: Redirecting [exampledomain1.com] to [1.2.3.4]
```

DNS Spoof
https://github.com

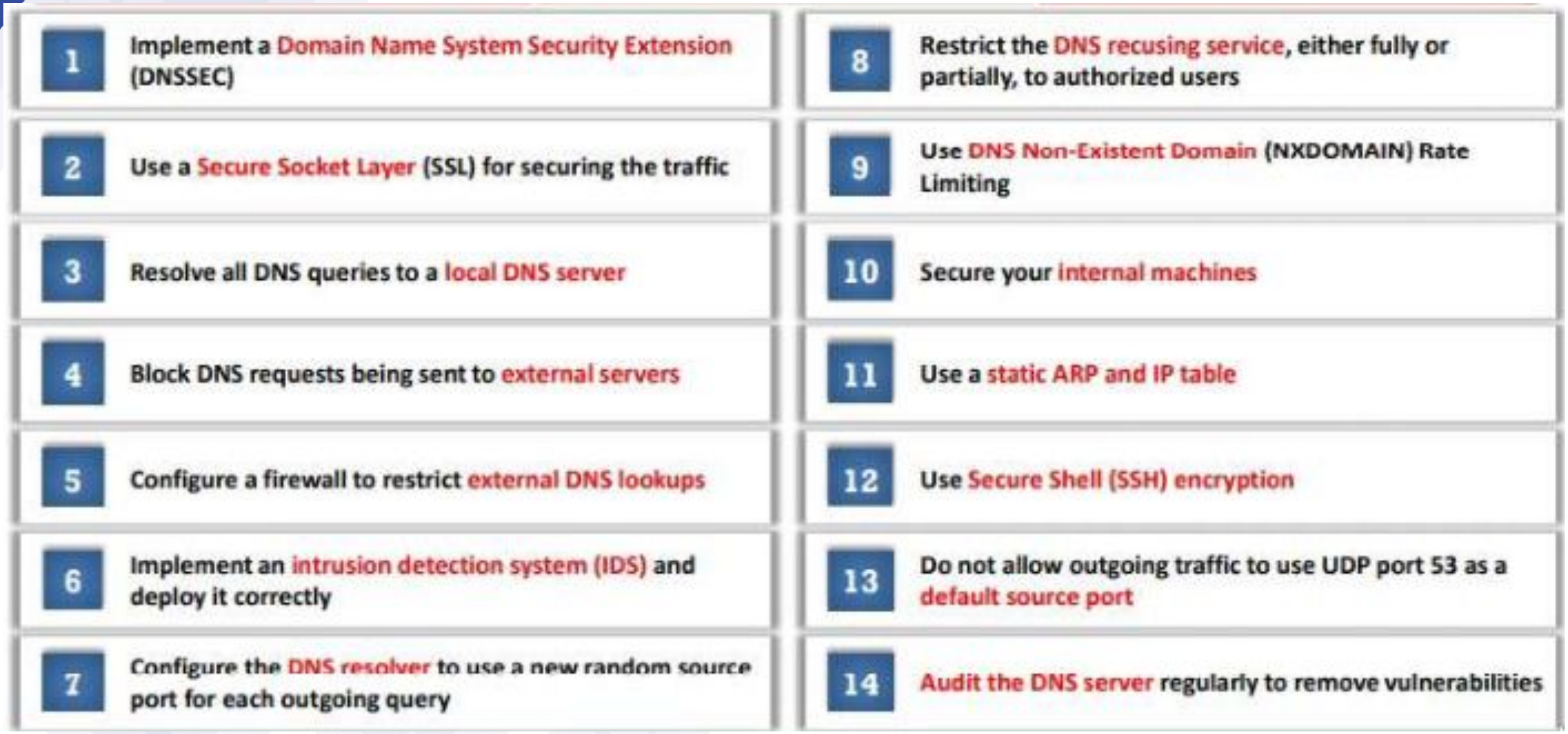
DNS-poison
https://github.com

Ettercap
http://www.ettercap-project.org

Evilgrade
https://github.com

TORNADO
https://github.com

Defending against DNS poisoning



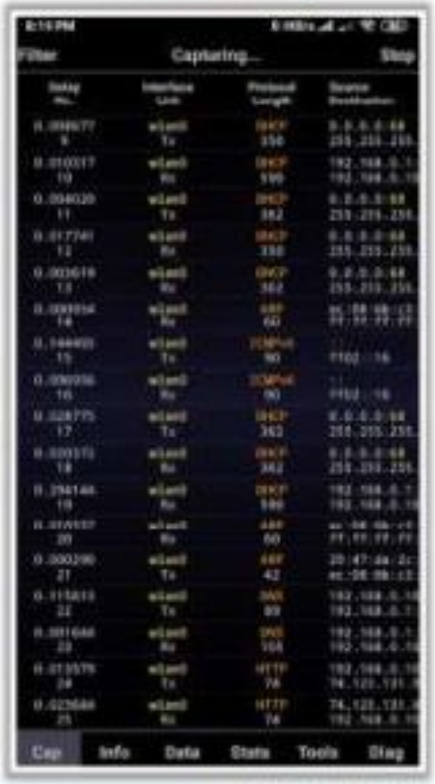
1. Implement a Domain Name System Security Extension (DNSSEC)
2. Use a Secure Socket Layer (SSL) for securing the traffic
3. Resolve all DNS queries to a local DNS server
4. Block DNS requests being sent to external servers
5. Configure a firewall to restrict external DNS lookups
6. Implement an intrusion detection system (IDS) and deploy it correctly
7. Configure the DNS resolver to use a new random source port for each outgoing query
8. Restrict the DNS recusing service, either fully or partially, to authorized users
9. Use DNS Non-Existent Domain (NXDOMAIN) Rate Limiting
10. Secure your internal machines
11. Use a static ARP and IP table
12. Use Secure Shell (SSH) encryption
13. Do not allow outgoing traffic to use UDP port 53 as a default source port
14. Audit the DNS server regularly to remove vulnerabilities

Sniffing Tools

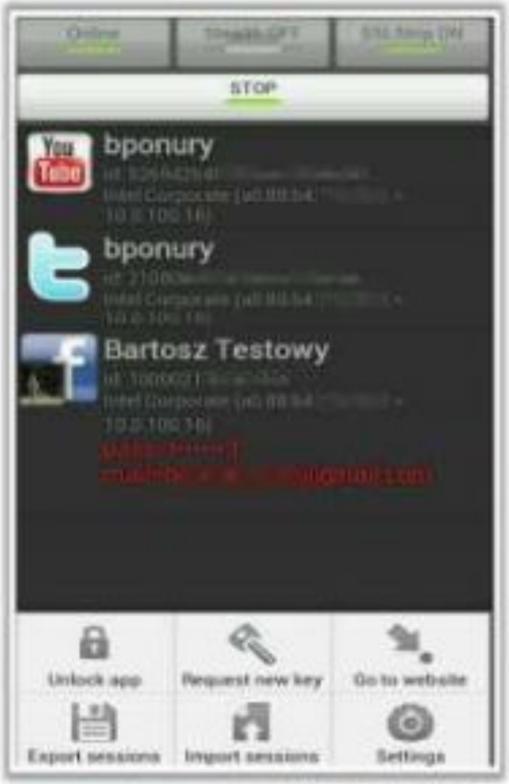
- Wireshark - Cheatsheet
- Omnipeek
- SteelCentral Packet analyzer
- Solarwinds deep packet inspection and analysis

Sniffing tools for Mobile

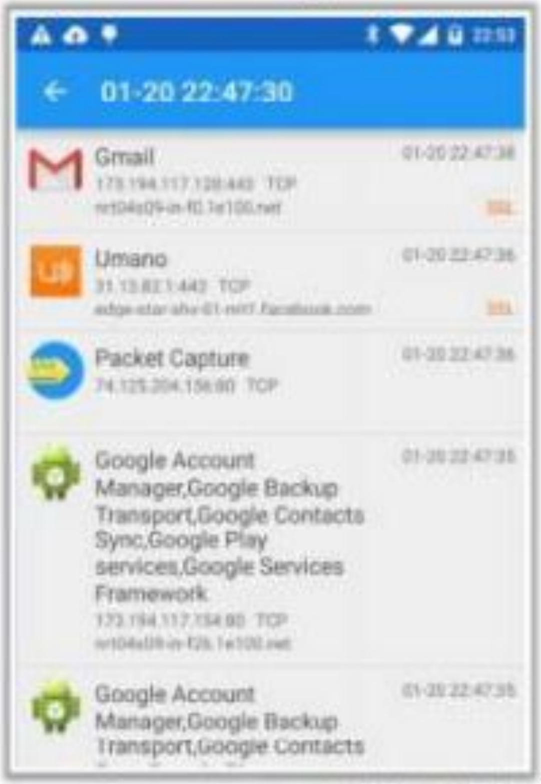
Sniffer Wicap



FaceNiff



Packet Capture



01-20 22:47:30

Gmail 01-20 22:47:38
TCP

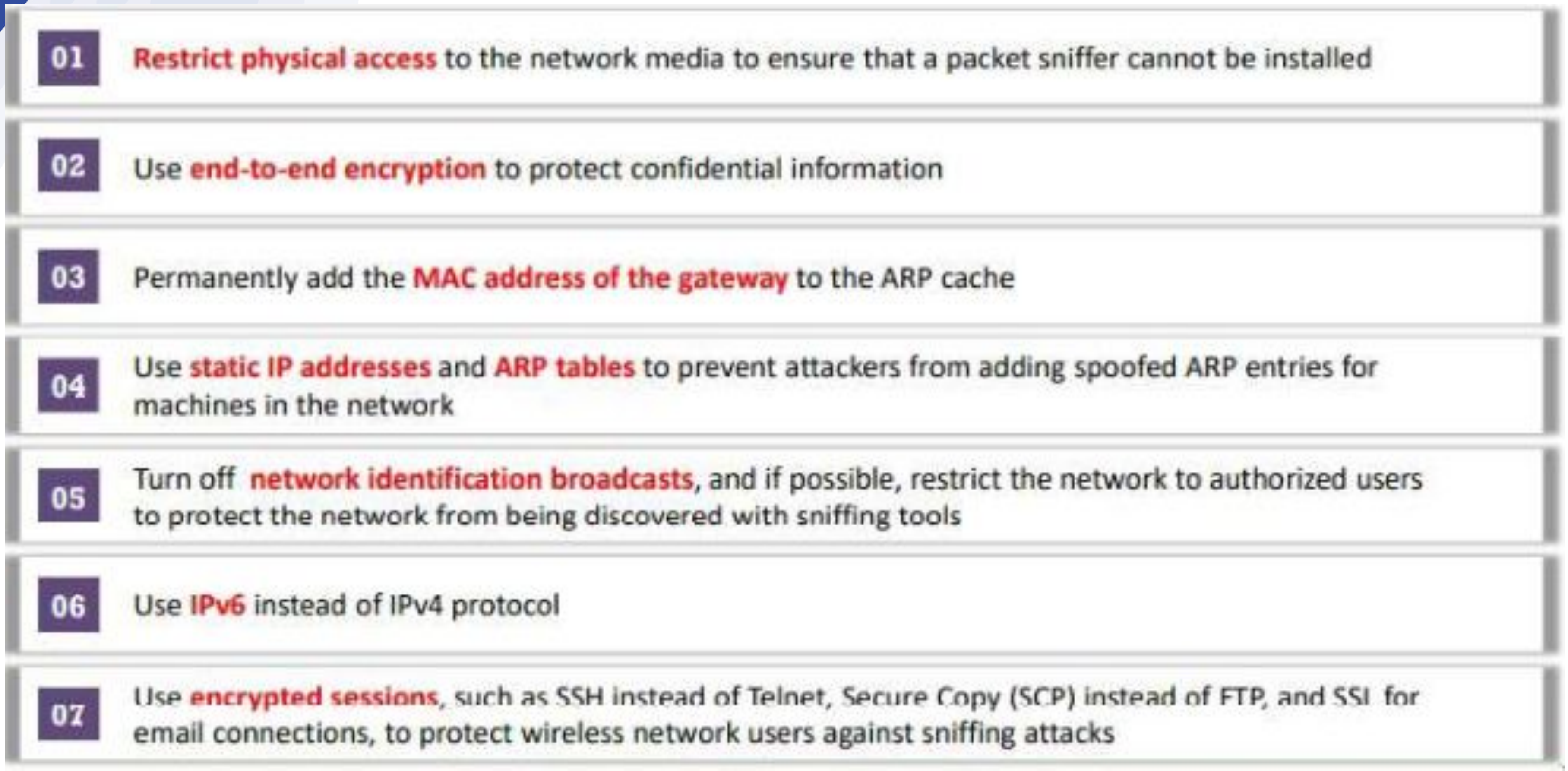
Umano 01-20 22:47:36
TCP

Packet Capture 01-20 22:47:36
TCP

Google Account Manager,Google Backup Transport,Google Contacts Sync,Google Play services,Google Services Framework 01-20 22:47:35
TCP

Google Account Manager,Google Backup Transport,Google Contacts 01-20 22:47:35

Countermeasure



01 **Restrict physical access** to the network media to ensure that a packet sniffer cannot be installed

02 Use **end-to-end encryption** to protect confidential information

03 Permanently add the **MAC address of the gateway** to the ARP cache

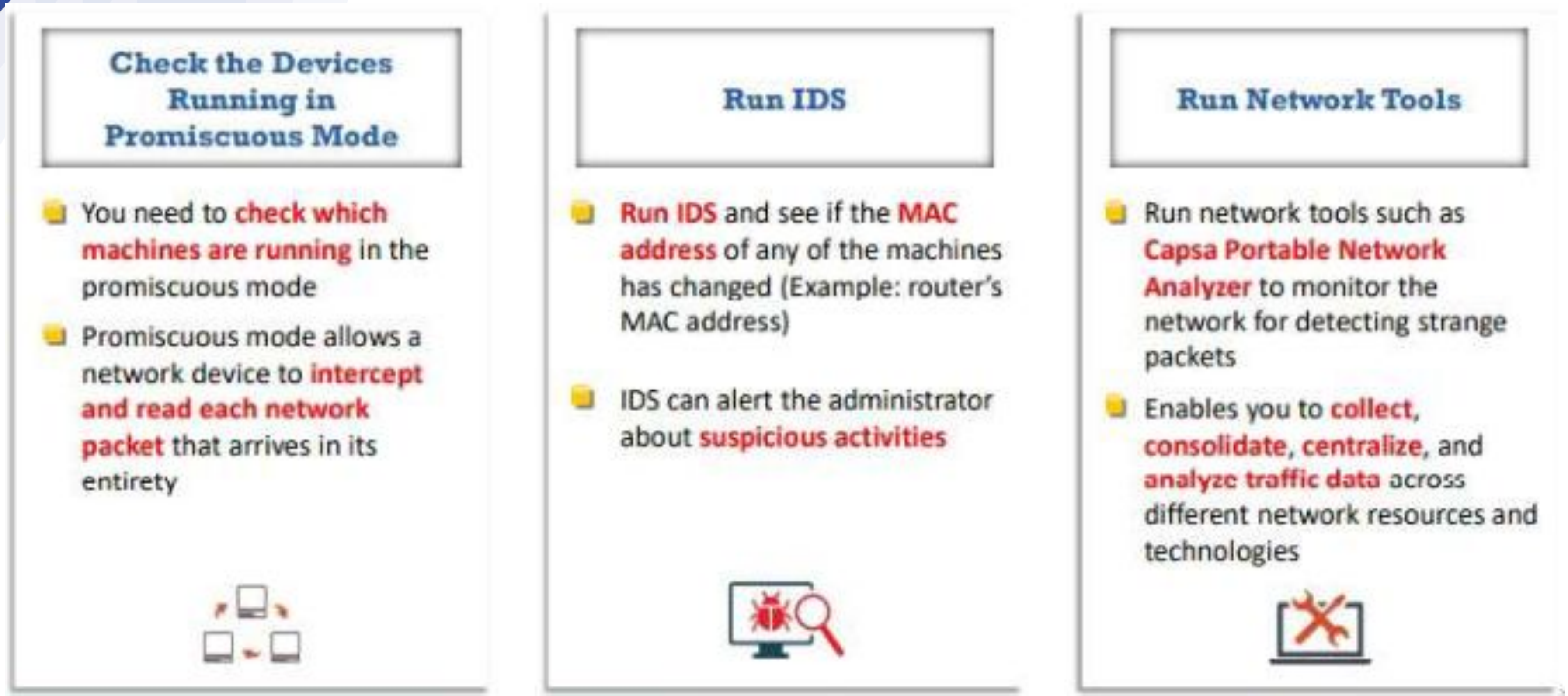
04 Use **static IP addresses** and **ARP tables** to prevent attackers from adding spoofed ARP entries for machines in the network

05 Turn off **network identification broadcasts**, and if possible, restrict the network to authorized users to protect the network from being discovered with sniffing tools

06 Use **IPv6** instead of IPv4 protocol

07 Use **encrypted sessions**, such as SSH instead of Telnet, Secure Copy (SCP) instead of FTP, and SSL for email connections, to protect wireless network users against sniffing attacks

Detecting Sniffing



Check the Devices Running in Promiscuous Mode

- You need to check which machines are running in the promiscuous mode
- Promiscuous mode allows a network device to intercept and read each network packet that arrives in its entirety

Run IDS

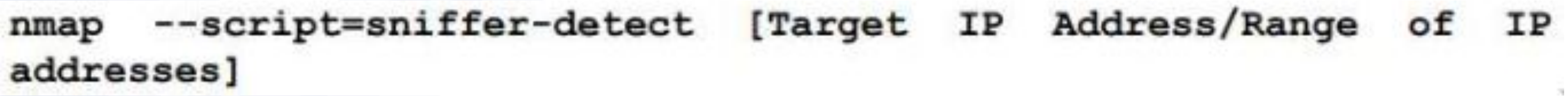
- Run IDS and see if the MAC address of any of the machines has changed (Example: router's MAC address)
- IDS can alert the administrator about suspicious activities

Run Network Tools

- Run network tools such as Capsa Portable Network Analyzer to monitor the network for detecting strange packets
- Enables you to collect, consolidate, centralize, and analyze traffic data across different network resources and technologies

Promiscuous Detection Tools

- Nmap



```
nmap --script=sniffer-detect [Target IP Address/Range of IP
addresses]
```

- Netscantools

Strathmore UNIVERSITY

Thank you!

Any Questions?