Penetration Testing
Implementation Plan

Azhar Ghafoor

Fall-2024

Department of Cyber Security,
FCAI, Air University, Islamabad

Assessing IDS Security Implementation

Assessing IDS Security Implementation

To protect the networks, organizations use various network security measures such as firewalls, intrusion detection system (IDS), intrusion prevention system (IPS), and so on.

In this section, we will discuss the penetration steps for assessing the IDS. This section also discusses about the threats associated with IDS and how a well-planned penetration testing helps in protecting it.

Why IDS Penetration Testing?

- To check if IDS properly enforces an **organization's IDS policy**
- To check if the **IDS** enforces organization's network security policies
- To check if the IDS is good enough to **prevent external attacks**
- To check the effectiveness of the **network's security perimeter**
- To check the **amount of network information accessible** to an intruder
- To check the IDS for **potential breaches of security** that can be exploited
- To verify whether the **security policy is correctly enforced** by a sequence of IDS rules

Common Techniques Used to Evade IDS Systems

I. Try the **pattern matching approach** to identify potential attacks within the exploit code

II. Use the **Unicode Evasion method**, which allows for viewing files on the IIS server

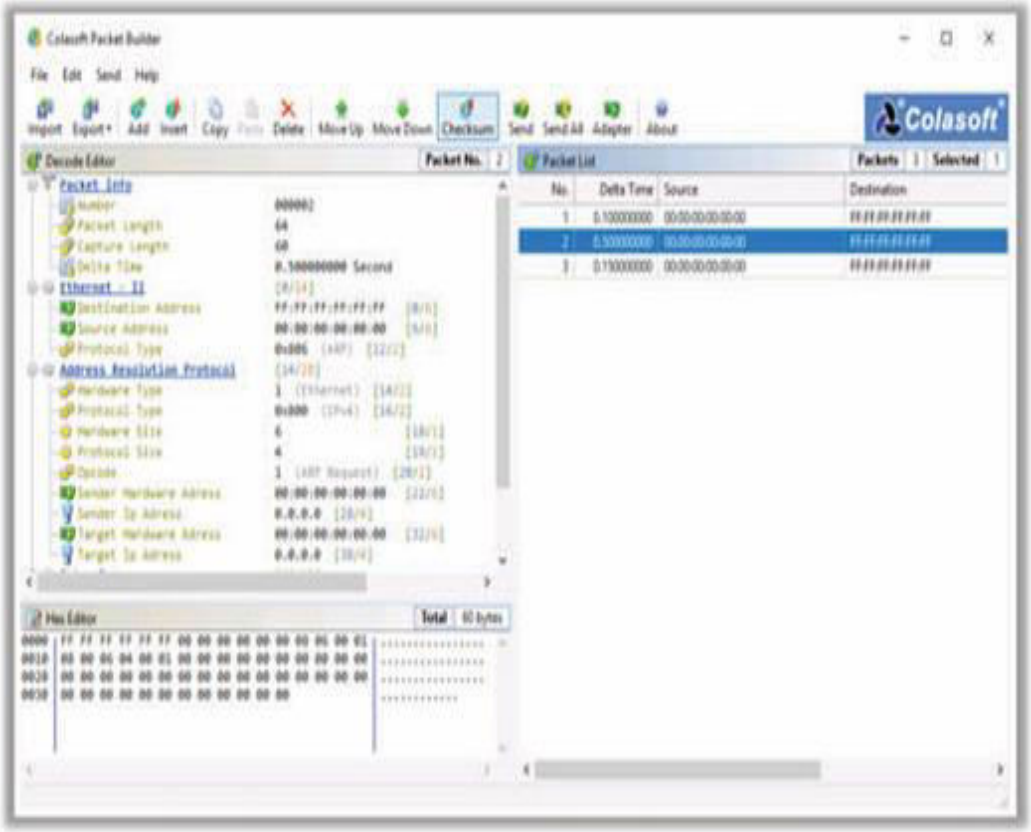
III. Search for the **central log server's IP address** and crash the system using a DoS attack

IV. Send specially **crafted packets** in order to trigger alerts and breed a large number of false reports

V. **Flood the network** with noise traffic to exhaust its resources examining risk-free traffic

Test for Resource Exhaustion

- Every IDS system has **memory**, **CPU**, and **bandwidth** limitations and is prone to resource exhaustion attacks
- IDS performance might degrade or fail if these resources are **exhausted**
- Use tools, such as **Colasoft Packet Builder**, **Network Traffic Generator and Monitor**, etc. to generate the traffic
- Test by sending large amounts of **traffic** to the IDS



Source: https://www.colasoft.com

Intrusion Detection Systems (IDS) Testing

1. Sending an ARP Flood

- Flood the network by sending ARP packets
- Use tools such as NetScanTools Pro to generate the ARP packets
- See the IDS response and how it reacts to this attack

Other ARP Packet Generator Tools

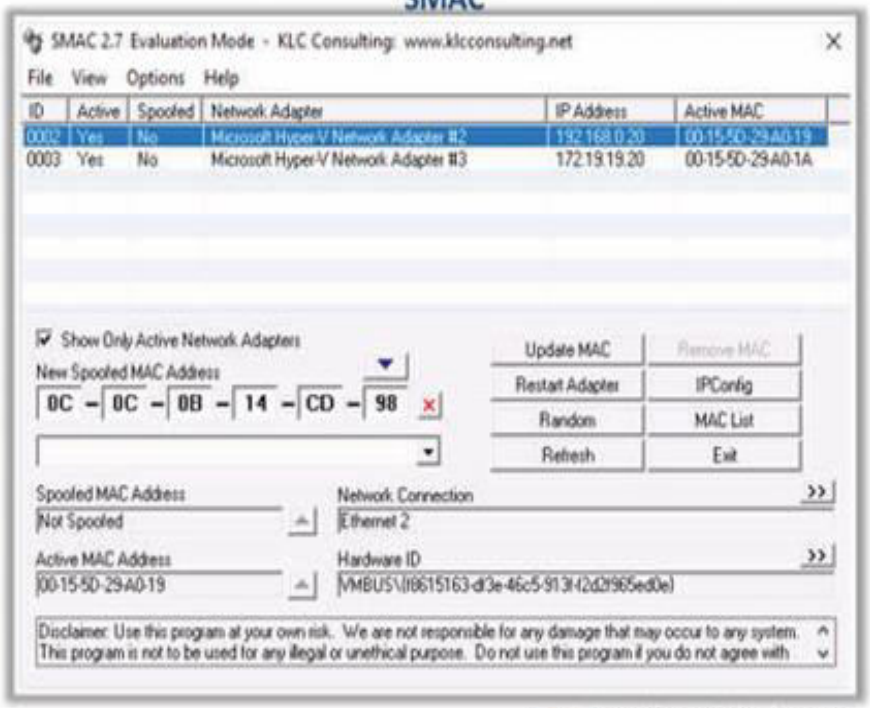
- Arping (http://www.habets.pp.se)
- arp-scan (https://github.com)

Source: https://www.netscantools.com

2. MAC Spoofing

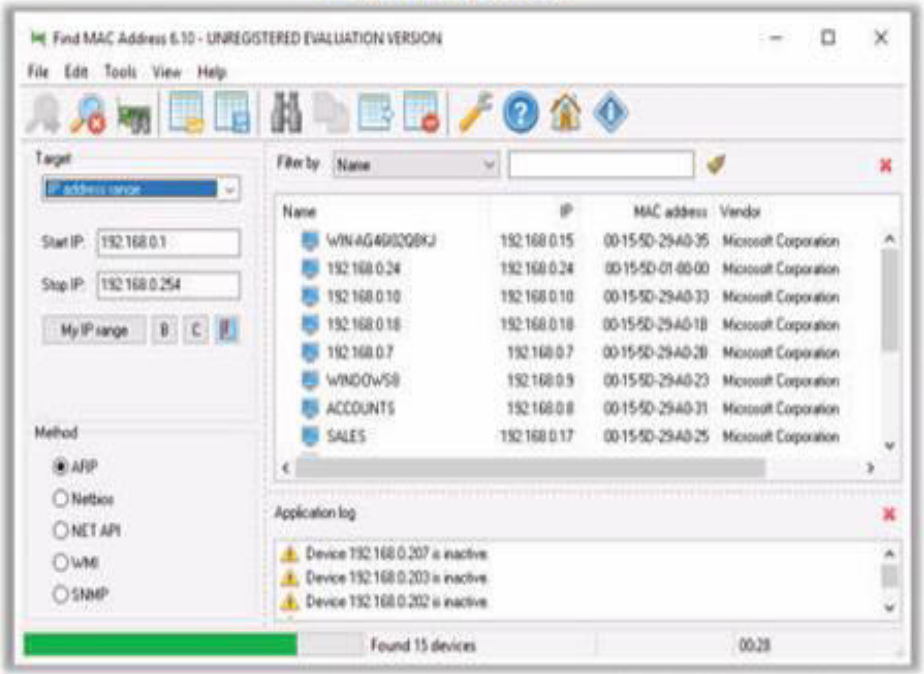
- Traffic can be disrupted on a network if two **Ethernet adapters** have exactly the same hardware (or **MAC** – Media Access Control) addresses
- Use tools such as **SMAC**, macof, etc. to generate spoofed MAC addresses
- Test the IDS by sending spoofed **MAC addresses**

SMAC



Source: http://www.klcconsulting.net

Find MAC Address

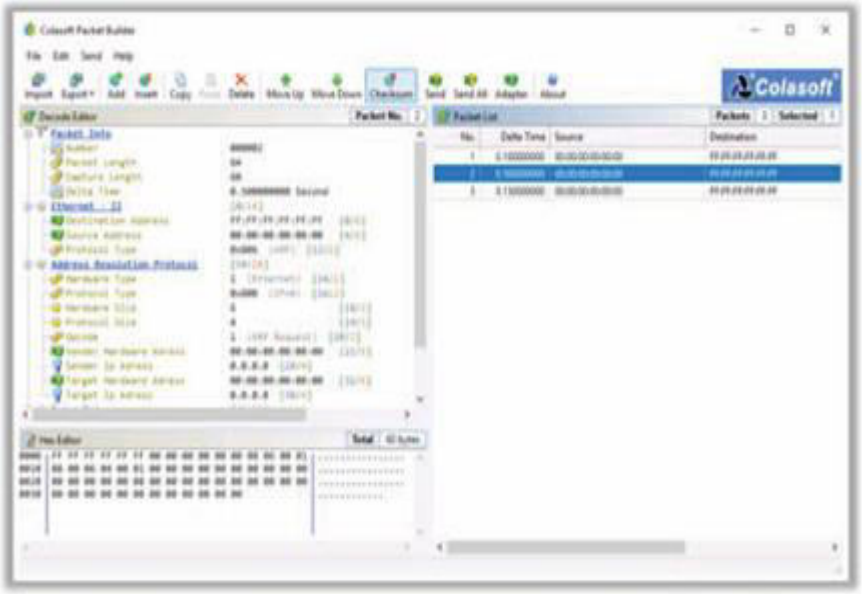


Source: https://lizardsystems.com

3. IP Spoofing

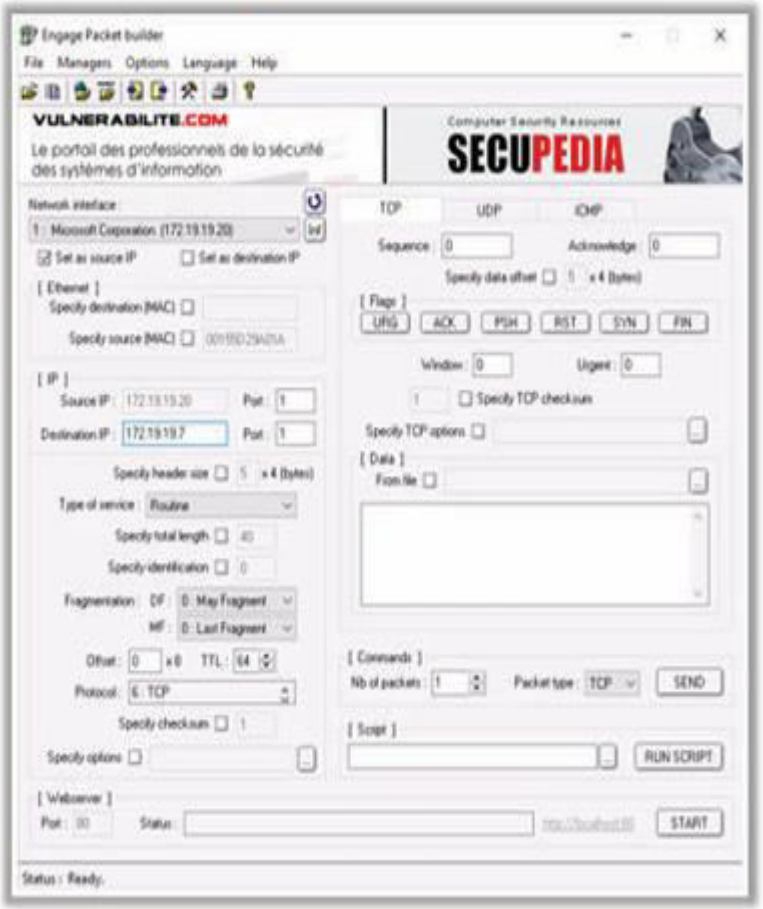
- Spoof the **IP address** to flood the IDS
- Check for the responses received by the **target system**

Colasoft Packet Builder



Source: https://www.colasoft.com

Engage Packet Builder



Source: http://www.engagesecurity.com

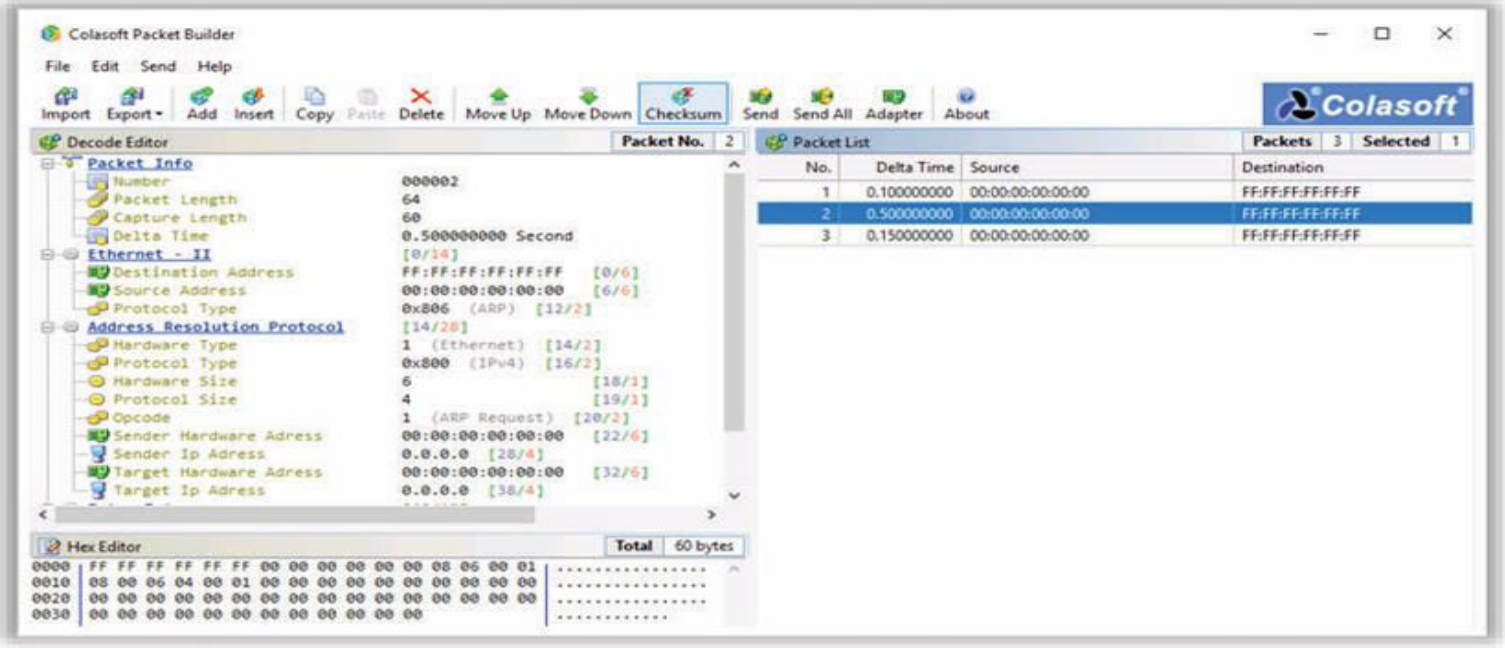
3. IP Spoofing (Cont'd)

IP spoofing in a network means generating the IP packets with a fake source IP address for performing various attacks. You can flood the IDS with IP address spoofed packets and analyze the responses received by the target system.

- **Colasoft Packet Builder**

  Source: *https://www.colasoft.com*

  Colasoft Packet Builder enables creating custom network packets. You can use Colasoft Packet Builder to generate IP packets and perform flood attack on the IDS.



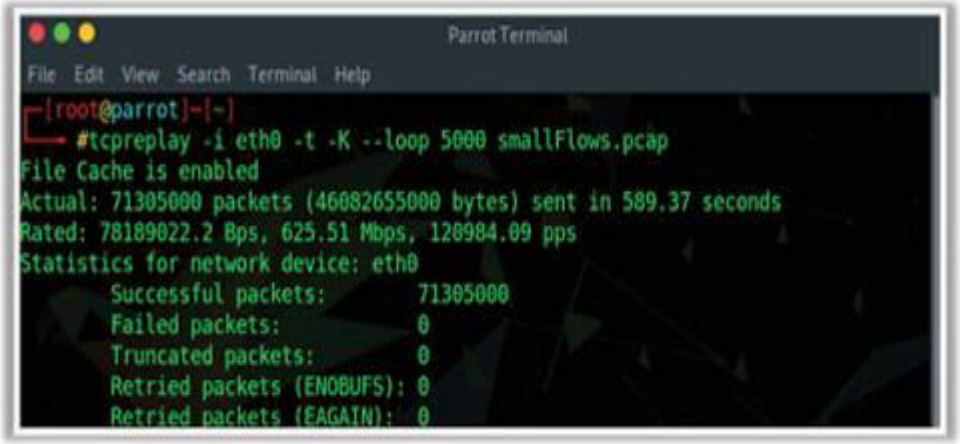
4. Sending SYN Floods

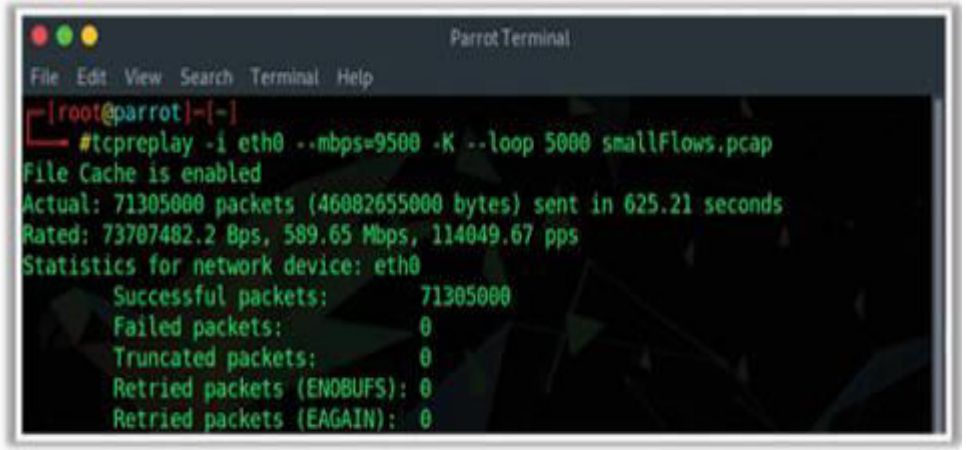
1. Many TCP implementations are vulnerable to a **resource-exhaustion attack** known as SYN flooding, in which excessive requests are made to create sessions, causing memory utilization to occur

2. If these SYN packets are spoofed from addresses that do not exist, **no response packet containing SYN/ACK** will be received, and the pending connection queue will expand

5. Editing and Replaying Captured Network Traffic

- Capture the traffic running on a target computer network by using **packet sniffing tools,** such as Wireshark
- Use **Tcpreplay tool** for editing and replaying captured network traffic
- **Replay** the traffic back onto the network



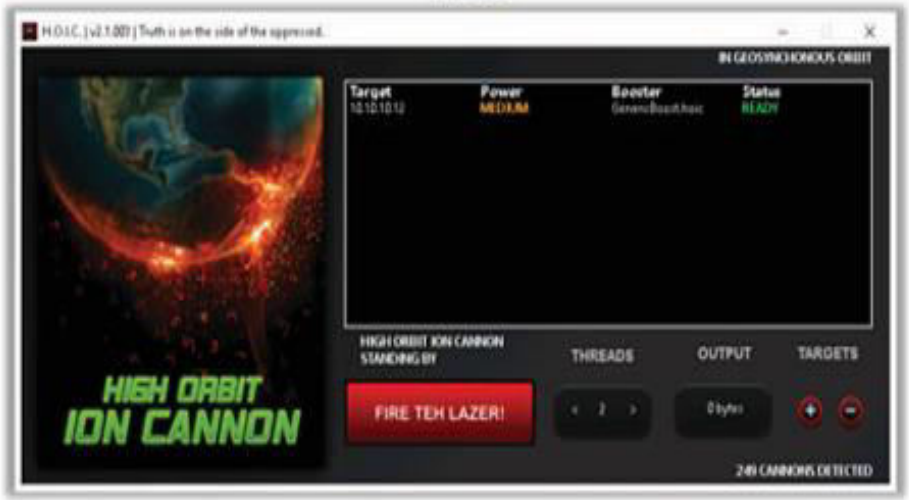


Source: http://tcpreplay.appneta.com

6. Denial-of-Service (DoS) Attack

- Many IDSes today employ central logging servers that are used exclusively to store IDS alert logs
- Perform a Denial-of-Service (DoS) attack on the central log server to slow down or crash the central logging system
- Search for the central log server's IP address
- Use DoS Attack tools such as HOIC, DDOSIM, DoS HTTP, Tor's Hammer, etc. to perform the DoS attack

HOIC



Source: https://sourceforge.net

7. Anonymous Website Surfing Sites and a Proxy Server

- Search over the Internet for anonymous website surfing sites which provide options to **encrypt the URLs** of the websites
- These websites will **hide the actual IP address** and will show another IP address, which could prevent the website from being blocked by the IDS, thus allowing access to the target system
- Search the Internet for a proxy server, configure it in your system, and try to bypass the IDS

Anonymous Web-Surfing Sites

1 http://anonymouse.org	6 http://proxify.com
2 http://www.anonymizer.com	7 http://www.spysurfing.com
3 http://www.webproxyserver.net	8 http://zendproxy.com
4 http://kproxy.com	9 http://anype.com

8. Sending Inconsistent Packets

In the IP header, the maximum packet length is **65,635 byes**; Internet Header Length (IHL) is a **4-bit field**, and the header contains a **16-bit (total length) field**

The TCP header has an **Offset field** that specifies the length of header and data, whereas the **UDP header** has a UDP Length field that determines the total size of the UDP packet

Use packet **crafting tools** to send specially crafted **TCP/IP** or **UDP/IP** packets with different TCP/UDP and IP header sizes to the IDS

Packets with **inconsistent** information may bypass the sanity check at the **IDS**

9. IP Packet Fragmentation

1. IP packets must follow standard Maximum Transmission Unit (**MTU**) size while traveling across the network
2. If the packet size exceeds, it splits into **multiple fragments** (called fragmentation) and then is reassembled later
3. Send malicious packets to the IDS at **regular interval of time** (greater than the IDS fragmentation reassembly timeout) to attack the target system
4. See the **example** in the next slide

Case Study:

Fragment Reassembly Timeout Difference:

- The **Intrusion Detection System (IDS)** has a reassembly timeout of **10 seconds**.
- The **target system** (victim) has a reassembly timeout of **20 seconds**.

Attacker's Strategy:

- The attacker sends data to the target in **fragments**, like breaking a message into pieces.
- The attacker waits **15 seconds** before sending the next fragment.

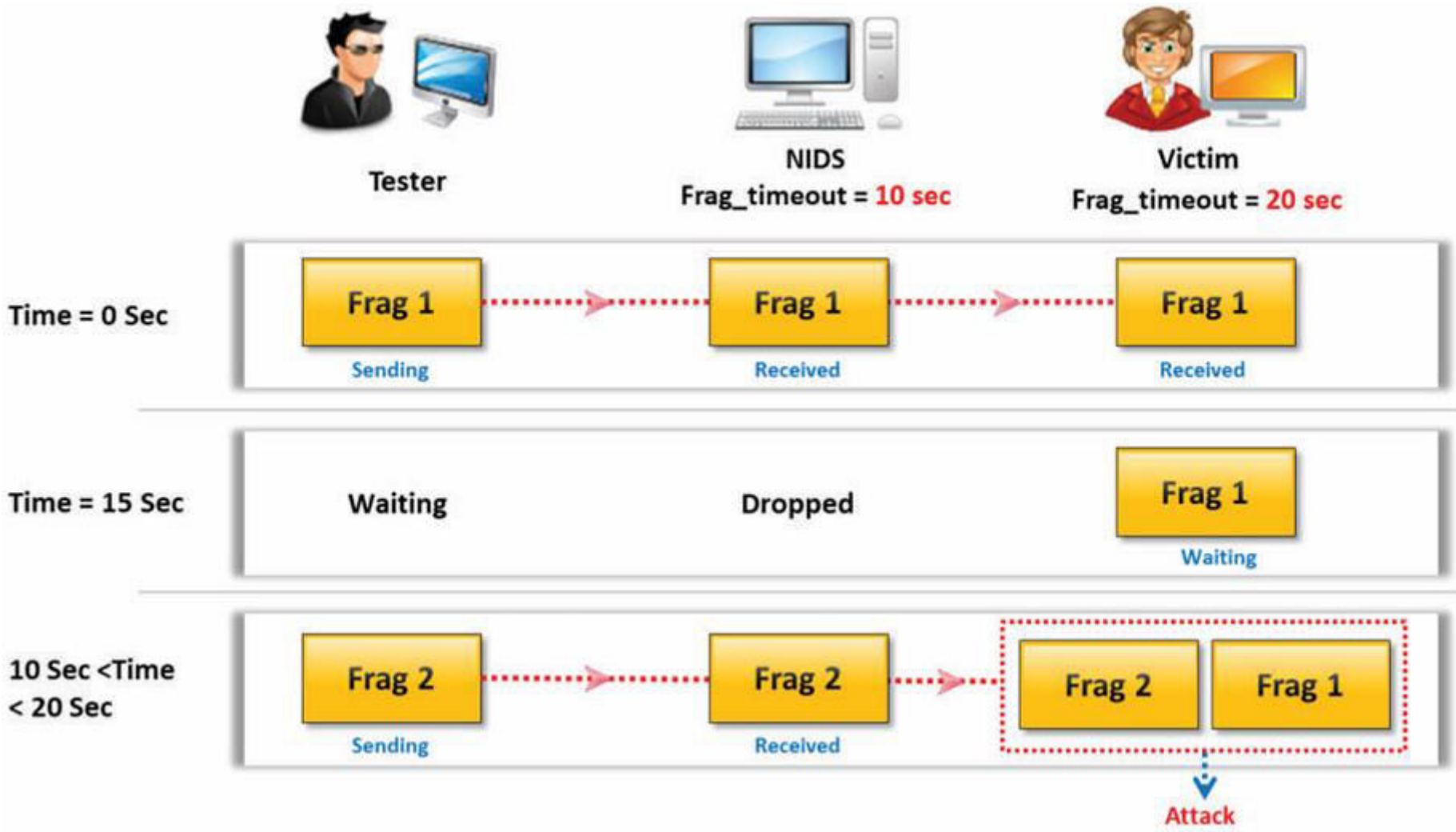
How It Works:

- The **IDS** will wait only **10 seconds** to reassemble the data, but after **10 seconds**, it gives up and **discards the fragment**, thinking it is incomplete and no longer relevant.
- Meanwhile, the **target system** waits **20 seconds**, which means it still waits for the remaining fragments.

Effect:

- The **IDS** discards the fragments and doesn’t raise any alerts.
- The **target system** reassembles the fragments correctly after **15 seconds**, meaning the full attack payload gets through undetected by the IDS.

Solution


Tester
NIDS
Frag_timeout = 10 sec
Victim
Frag_timeout = 20 sec
Time = 0 Sec
Frag 1
Sending
Frag 1
Received
Frag 1
Received
Time = 15 Sec
Waiting
Dropped
Frag 1
Waiting
10 Sec <Time
< 20 Sec
Frag 2
Sending
Frag 2
Received
Frag 2
Frag 1
Attack

Evading Intrusion Detection Systems (IDS)

1. Obfuscating or Encoding the Attack Payload

- Obfuscation is the process of creating **obfuscated code** that is difficult for the IDS to understand

- Evade the IDS by obfuscating or **encoding the attack payload** in a way that the target system understands but the IDS does not

- Encode the **attack patterns** in unicode to bypass IDS filters, but be understood by an IIS web server

- Try to manipulate the **path referenced** in the signature to fool the IDS

2. False-Positive Generation

I	Within the IDS, check the packets that are generating the alerts, and whether it has activated a large number of false reports
II	Examine the large amount of alert data that is generated and logged by the IDS
III	To verify the log data, it is very difficult to differentiate between false positives and legitimate attacks
IV	With knowledge of the specific IDS, a tester can generate false positives

3. TTL Evasion

In the TTL evasion technique, an IDS **rejects the packets** that an end system accepts

The tester tries to send request packets, which are **mistakenly rejected** by the IDS to remove parts of the stream from the IDS's view

A **malicious host** uses a combination of TTL to fool the IDS and retransmits the fragments to the target host

4. UDP Checksum

- The UDP checksum is only optionally computed if this **16-bit field** is exactly 0; it signifies that the UDP checksum was not computed on **transmission** and should not be checked upon **reception**
- Any packets that have the **UDP checksum** turned off are questionable and may be **subtle evasion** attempts
- Send UDP packets with a **wrong checksum** to the IDS, and see the IDS response and how it reacts to this packet

5. TCP Retransmissions

- TCP retransmits packets to introduce a level of **reliability** to the unreliable **IP transport mechanism**

- If an IDS sees a **retransmitted** packet (with correct checksums) that has different contents than the **original packet**, it can assume either a buggy **TCP/IP** implementation or a malicious attack

6. Covert Channels

A covert channel can be defined as a **hidden communication** mechanism

When a system has been **compromised** by other means, some hackers will use these covert channels in an attempt to hide their activities

Detect the covert channel's deliberate attempt to make information leaks possible, when bypassing the **security policy** or causing a compromised system to obey an external system

7. Reverse Traversal

- Break apart a signature, such as:

  `"/cgi-bin/some.cgi"`
  by using reverse traversal directory tricks:
  `GET /cgi-bin/blahblah/../some.cgi HTTP/1.0`

- Equates to "`/cgi-bin/some.cgi`" once the directory traversal has been accounted for

- Most IDSs can detect this technique

The ideal way for breaking any signature is using reverse traversal directory. This method differs from the URL encoding technique. The raw IDS gives the information that the request contains "`/../.`" You can break apart a signature, such as "`/cgi-bin/some.cgi`" by using reverse traversal directory tricks such as "`GET /cgi-bin/blahblah/../some.cgi HTTP/1.0`." This equates to "`/cgi-bin/some.cgi`" once the directory traversal has been accounted for. Most IDSs can detect this technique.

8. HTTP Mis formatting

Some IDS systems that implement minimal signatures depend on the trailing space for matching

For example, matching "/phf" could lead to many false positives, but "/phf " (notice the trailing space) helps to ensure that the final requested page is closer to the actual "phf" and not just starting with the letters "phf"

9. NULL Method Processing

I

Many C string libraries use the NULL character to denote the end of the string

II

Some IDSs still use these libraries, so the occurrence of using NULLs to denote the end of strings is still quite common

III

We can use this to our advantage with the following type of request:

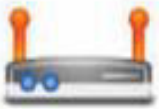
```
GET%00 /cgi-bin/some.cgi HTTP/1.0
```

Assessing Security of Routers

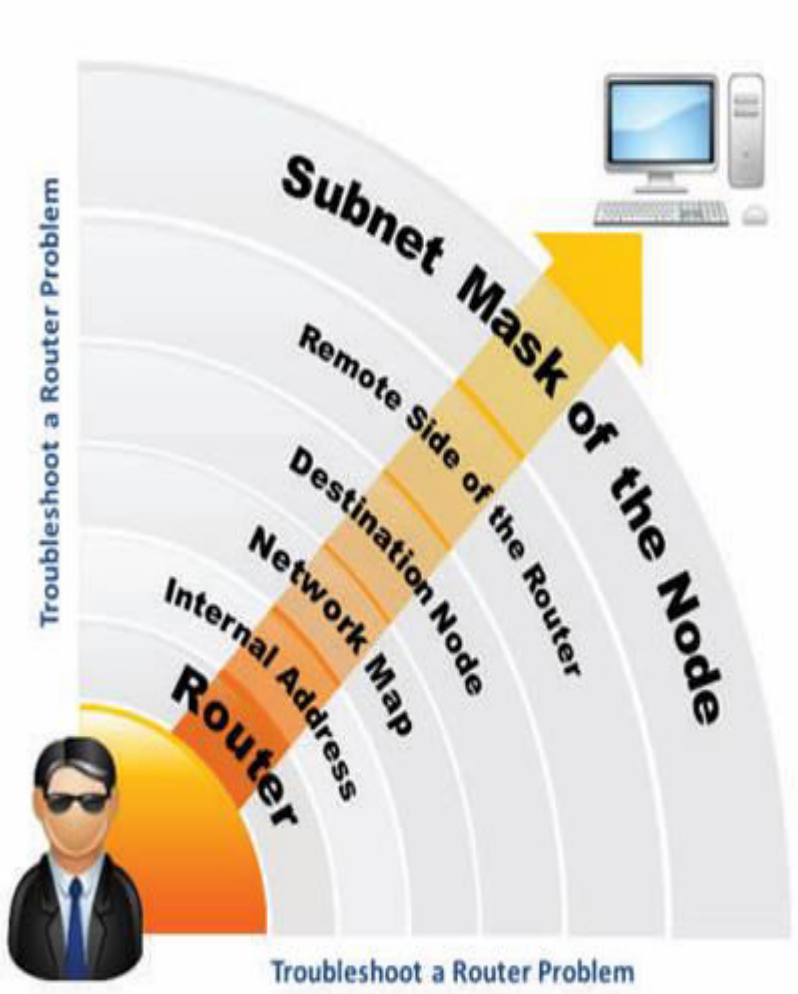
Need for Router Testing

Router testing is needed to provide a single point of reference for **router security** assessment and countermeasures for **identified weaknesses**

You will need to assess **end-to-end** router **security** with target knowledge and/or without target knowledge



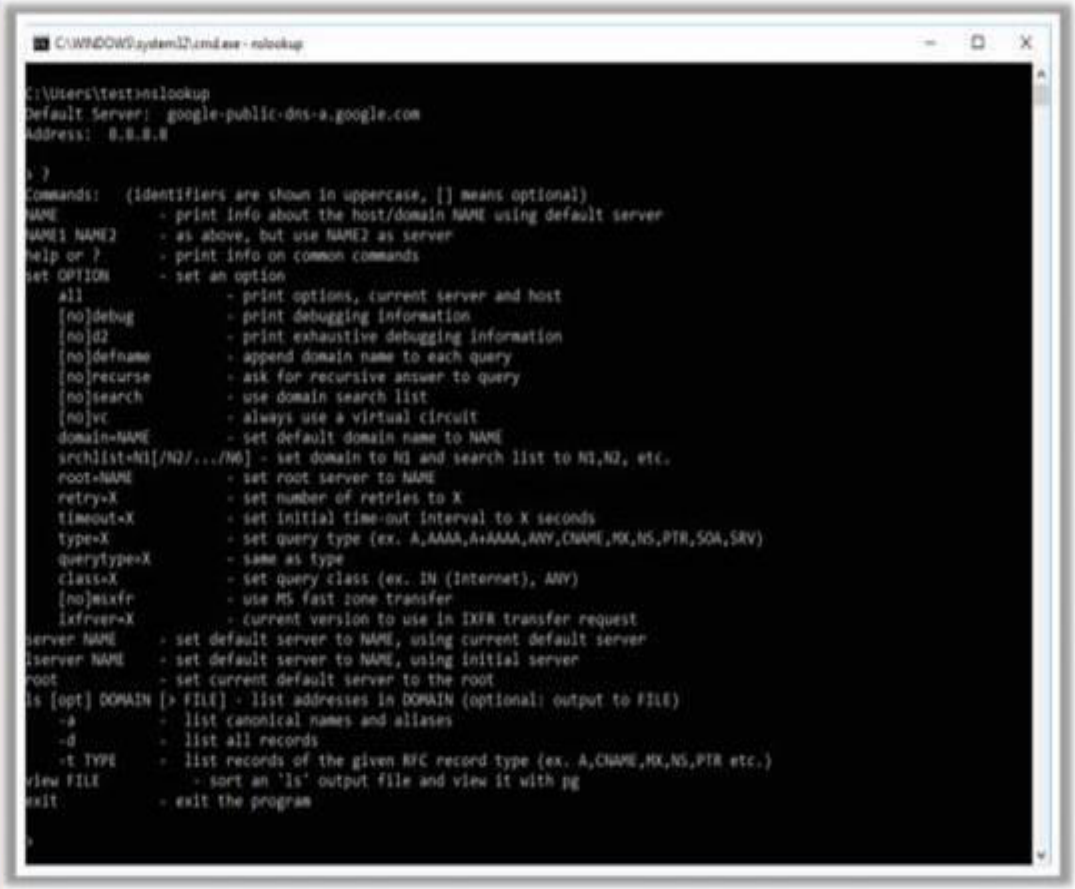
Router Testing Issues



- Test for **misconfigurations** of routers
- Test for **router product-specific** vulnerabilities (example: IOS vulnerabilities in Cisco routers)
- A compromised routing device compromises all **network traffic**
- Without directly compromising a **routing device**, it can be used to compromise the **entire network**
- Routing devices are used to **direct network traffic**, and any one router can be used to **manipulate** network traffic

Identify the Router Hostname

- Identifying router hostnames lets you know which **router you are working on**
- If the router is registered with DNS, a reverse query on the **router's IP address** will give the DNS name of the router
- This DNS name might be the same as the hostname
- **Tools:**
  - DIG
  - Nslookup



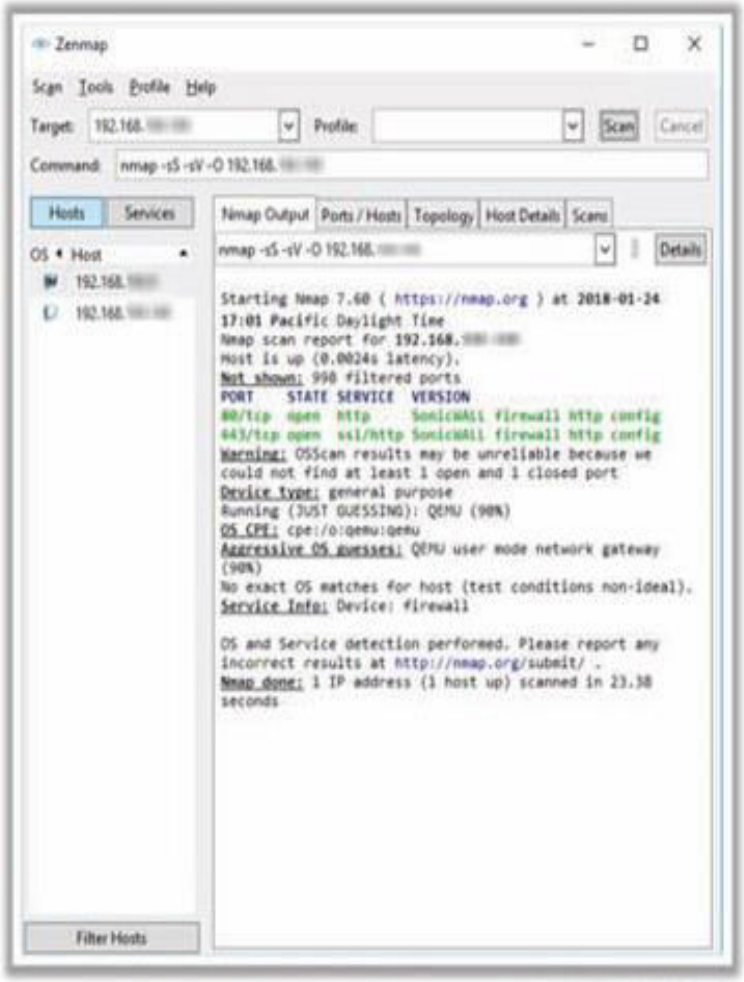
Port Scan the Router

- **Port scanning** the router pings computers, scans for listening TCP ports, and displays default services and resources that are shared on the network
- Scan for the **router's default services**

Port	Service	Protocol
23	Telnet	TCP
80	HTTP	TCP
161	SNMP	UDP

Identify the Router OS and its Version

- If you know the router's **operating system** and its **version**, identify the vulnerabilities in the device:
  - **Example**: Cisco router model 2500 and IOS version 11.2
- Tool: **Nmap**
  - # nmap –sS –sV –O <router ip address>



Source: https://nmap.org

Identify Protocols Running

- Identify the router protocols running on the router

- Example:
  - CDP (Cisco Discovery Protocol)
  - RIP (Routing Information Protocol)
  - RIPv/v2 (Routing Information Protocol Version 2)
  - IGMP (Internet Group Management Protocol)
  - OSPF (Open Shortest Path First)

Recover Router Passwords from Config File

01

Locate the **router password** from the config file; passwords could be plain-text or encrypted using Vigenere/MD5 algorithms

02

Use a **router password recovery tool,** such as Router Password Kracker and RouterPassView to decrypt the encrypted router password

Source: https://securityxploded.com

Router Running Modes

Routers are configured for many **different modes**

Common modes are **"user mode"** and **"privileged mode"**

In **user mode**, the router displays the hostname followed by '>'

Example of **user mode** access:

- TargetRouter >
- Collect the password hash and decrypt it; Cain & Abel can be used to decrypt it

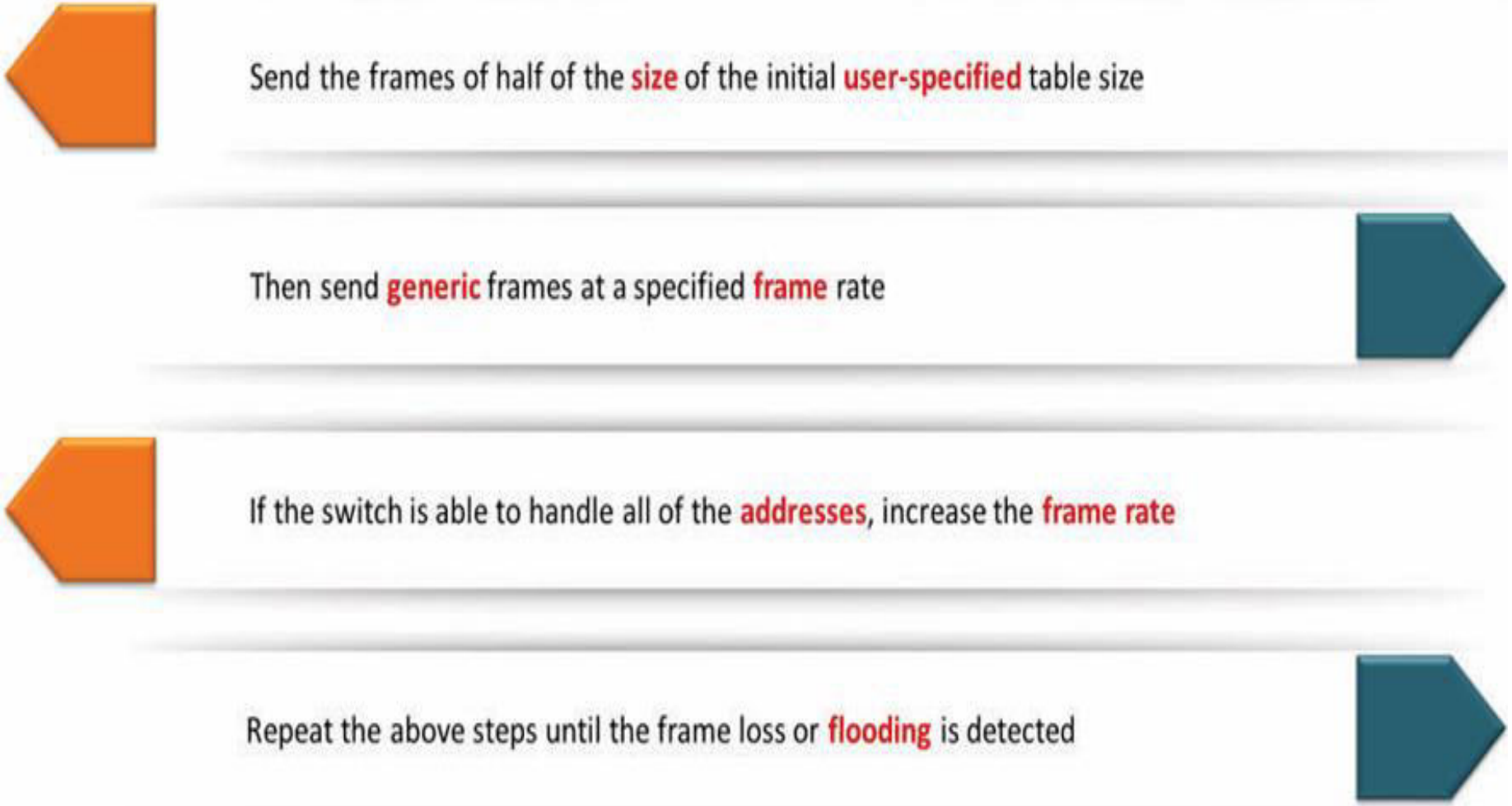
Assessing Security of Switches

Security Misconfigurations In Cisco Switch Configuration

- Get the switch configuration document and compare it with standard security configuration baseline
- Some of the common switch security misconfiguration checks for CISCO and other manufacturers:
  - Default vulnerable configurations
  - Unused ports
  - DHCP snooping
  - Port security
  - Correct timestamp

```
S1# show port-security interface fastethernet 0/18
Port Security              : Enabled
Port Status                : Secure-up
Violation Mode             : Shutdown
Aging Time                 : 0 mins
Aging Type                 : Absolute
SecureStatic Address Aging : Disabled
Maximum MAC Addresses      : 1
Total MAC Addresses        : 1
Configured MAC Addresses   : 0
Sticky MAC Addresses       : 0
Last Source Address:Vlan   : 0025.83e6.4b01:1
Security Violation Count   : 0
```

Address Cache Size



Data Integrity and Error Checking

Check the switch's ability to **forward frames** under certain traffic rates without corrupting the payload

Frames are transmitted with a **predefined data pattern**

Verify whether the switch forwards the frames properly

Calculate the number of **sequence errors** and the number of **data errors**

Back-to-Back Frame Capacity

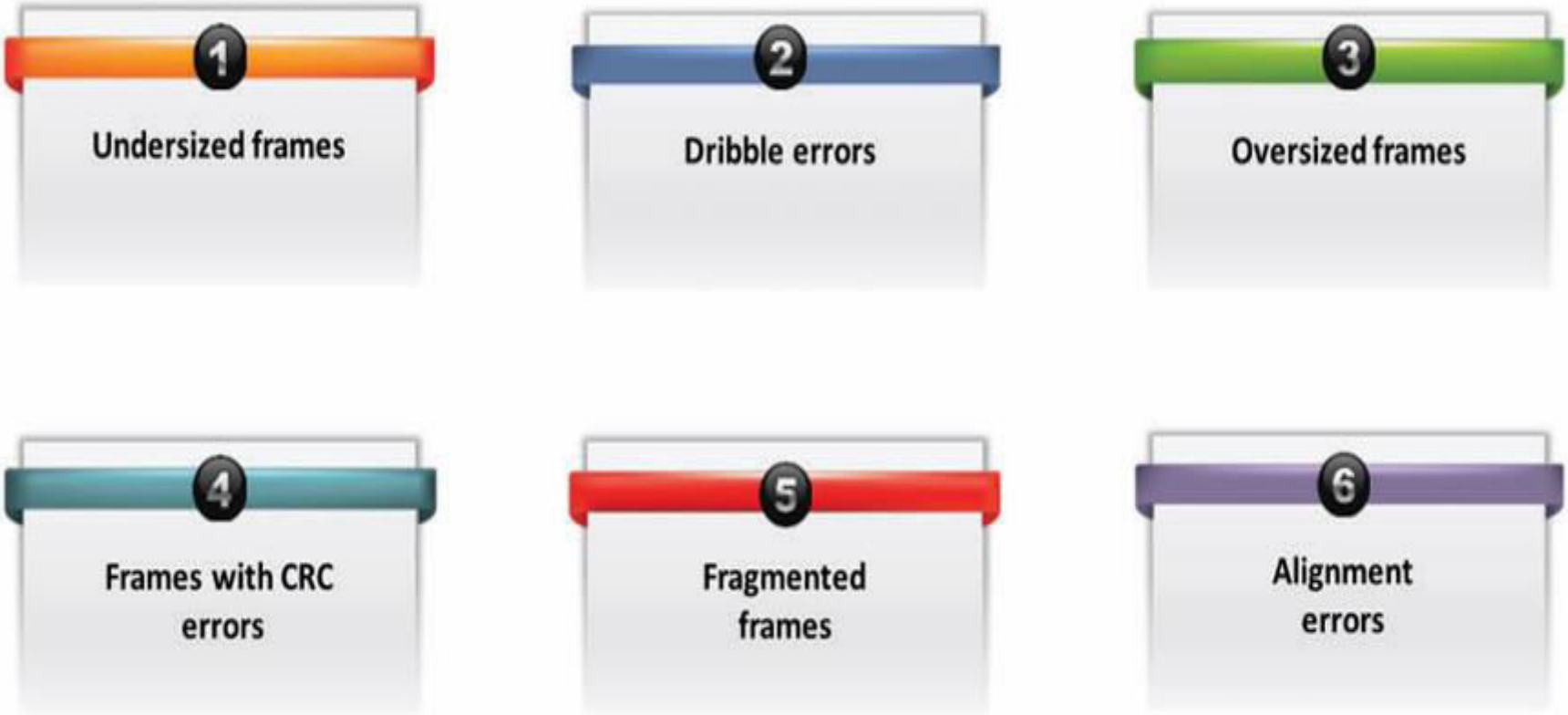
- The back-to-back value is the number of frames in the **longest burst** that the switch will handle without the loss of any frames
- Send a burst of frames with **minimum inter-frame gaps** to the switch and count the number of frames forwarded by the switch
- If the count of **transmitted frames** is equal to the number of frames forwarded, the length of the burst is increased, and the test is **rerun**
- If the number of **forwarded frames** is less than the number transmitted, the length of the burst is reduced, and the test is rerun
- The trial length must be **2 seconds** and should be repeated 50 times with the average of the recorded values being reported

Latency Test

- Send a stream of frames through the switch at the determined rate to a specific destination for a duration of 120 seconds
- Provide an identifying tag in one frame after 60 seconds
- Record the time at which this frame is fully transmitted (timestamp A)
- Record the time at which the tagged frame was received by a receiver (timestamp B)
- The latency is timestamp B minus timestamp A
- Repeat the test 20 times with the reported value being the average of the recorded values

Test for Frame Error Filtering

- Check if the switch correctly **filters illegal frames**, such as



Test for Frame Error Filtering (Cont'd)

A switch should filter out malicious and unauthorized frames to ensure safety. Check if the switch correctly filters illegal frames, such as:

- **Undersized frames**

  Frames that are less than 64 bytes and are being propagated must be filtered by switch. These frames should not be forwarded.

- **Dribble bit errors**

  Frames with dribbling bits must be corrected and forwarded by the switch. Frames that do not end in an octet boundary but have a valid check sequence must be accepted and corrected by the switch before forwarding.

- **Oversized frames**

  Switch must filter the frames that are oversized or larger than 1518 bytes.

- **Frames with CRC errors**

  Switch must filter the frames with error in check sequence validation. These frames should not be forwarded.

- **Alignment errors**

  Combination of both CRC error and dribble bit error is called alignment error. Frames with CRC errors and frames that do not end in an octet boundary are not to be transmitted by the switch.

Document the Result

- Note down the flaws found in perimeter devices
- Firewall rules though which evasion has been possible
- IDS rules though which evasion has been possible
- Configuration mistakes found in router and switches

Q&A

Thankyou