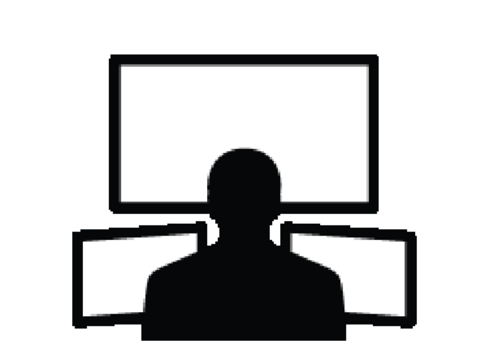
UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Prednáška 5
Network monitoring and vulnerabilities



Riešenie bezpečnostných incidentov
(CyberOps Associate v1.02)

Mgr. Jana Uramová, PhD.
Katedra informačných sietí
Fakulta riadenia a informatiky, ŽU

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.

Ktorý výsledok pokrýva táto prednáška

Výsledky vzdelávania

CISCO CERTIFIED
CyberOps
Associate

Študent po absolvovaní predmetu získa vedomosti a zručnosti potrebné na úspešné zvládnutie úloh, povinností a zodpovedností bezpečnostného analytika v operačnom centre bezpečnosti.
Študent po absolvovaní predmetu bude vedieť:

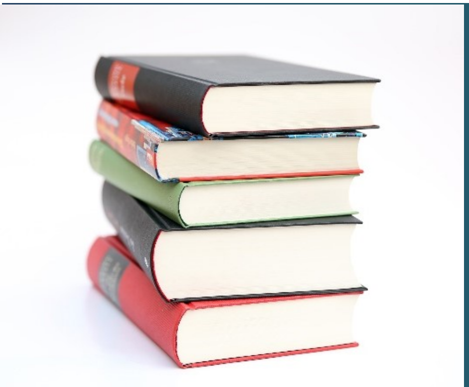
- Vysvetliť rolu analytika v rámci kybernetickej bezpečnosti
- Vysvetliť prostriedky operačného systému Windows
  a Linux a charakteristiky pre podporu analýzy v rámci kybernetickej bezpečnosti
- Analyzovať operácie v rámci sieťových protokolov a služieb
- Vysvetliť operácie sieťovej infraštruktúry
- Klasifikovať rôzne typy sieťových útokov
- Použiť sieťové monitorovacie nástroje na identifikáciu útokov proti sieťovým protokolom a službám
- Použiť rôzne metódy na prevenciu škodlivého prístupu do počítačových sietí, k používateľom a k dátam
- Vysvetliť vplyvy kryptografie v rámci monitorovania bezpečnostných sietí
- Vysvetliť, ako skúmať zraniteľnosti a útoky koncových zariadení
- Identifikovať hlásenia v rámci sieťovej bezpečnosti
- Analyzovať sieťovú prevádzku na overenie potencionálneho zneužitia siete
- Aplikovať reakčné modely na incident, a získať prostriedky na manažovanie sieťových bezpečnostných incidentov

- Prerekvizity:
  - Princípy IKS, Počítačové siete 1, Úvod do OS

Preliminary version of topics for lectures

Planning

week	CyberOps Modules in lectures	Exam from:
1	Chapter 1 The Danger Chapter 2 Fighters in the War Against Cybercrime Chapter 3: The Windows Operating System	none
2	Chapter 4: Linux Overview Chapter 5 Network Protocols Chapter 6 Ethernet and Internet Protocol (IP) Chapter 7 Connectivity Verification Chapter 8 Address Resolution Protocol Chapter 10 Network Services Chapter 11 Network Communication Devices	1-2
3	Chapter 9 The Transport Layer (+nmap) Chapter 12 Network Security Infrastructure	3-4
4	Chapter 13 Attackers and Their Tools Chapter 14 Common Threats and Attacks	5-10
5	Chapter 15 Network Monitoring and Tools *(SIEM, SOAR)* Chapter 16 Attacking the Foundation *(L2, L3 protocols vulnerabilities and attacks)* Chapter 17 Attacking What We Do *(L7 vulnerabilities and attacks)*	11-12
6	Chapter 18 Understanding Defense *(security management)* Chapter 19 Access Control *(AAA)* Chapter 20 Threat Intelligence *(commercials, CVE database)*	13-17
7	Chapter 21 Cryptography Chapter 22 Endpoint Protection	18-20
8	Chapter 23 Endpoint Vulnerability Assessment Chapter 24 Technologies and Protocols	none
9	Chapter 25 Network Security Data Chapter 26 Evaualting Alerts (in Security Onion)	21-23
10	Chapter 27 Working with Network Security Data (Security Onion and ELK)	24-25
11	Chapter 28 Digital Forensics and Incident Analysis and Response	none
12	Expert talk (invited lecture)	26-28



Obsah dnešnej prednášky

Čo prejdeme spolu na prednáške:

- **Chapter 15 Network Monitoring and Tools**
  (SPAN, RSPAN, Wireshark, tshark, tcpdump, Netflow, SIEM, SOAR, ELK a analýza útokov pomocou ELK)

Čo ostane na domáce preštudovanie
(veľa slajdov, ale mnoho pre nás už známych vecí z PS1, PS2, čítanie pôjde rýchlo)

- **Chapter 16 Attacking the Foundation**
  (L2, L3 protocols vulnerabilities and attacks)
- **Chapter 17 Attacking What We Do**
  (L7 vulnerabilities and attacks)
  - *Nevynechajte útoky na HTTP, HTTPs, SQL injection – bude na ďalšom cvičení*

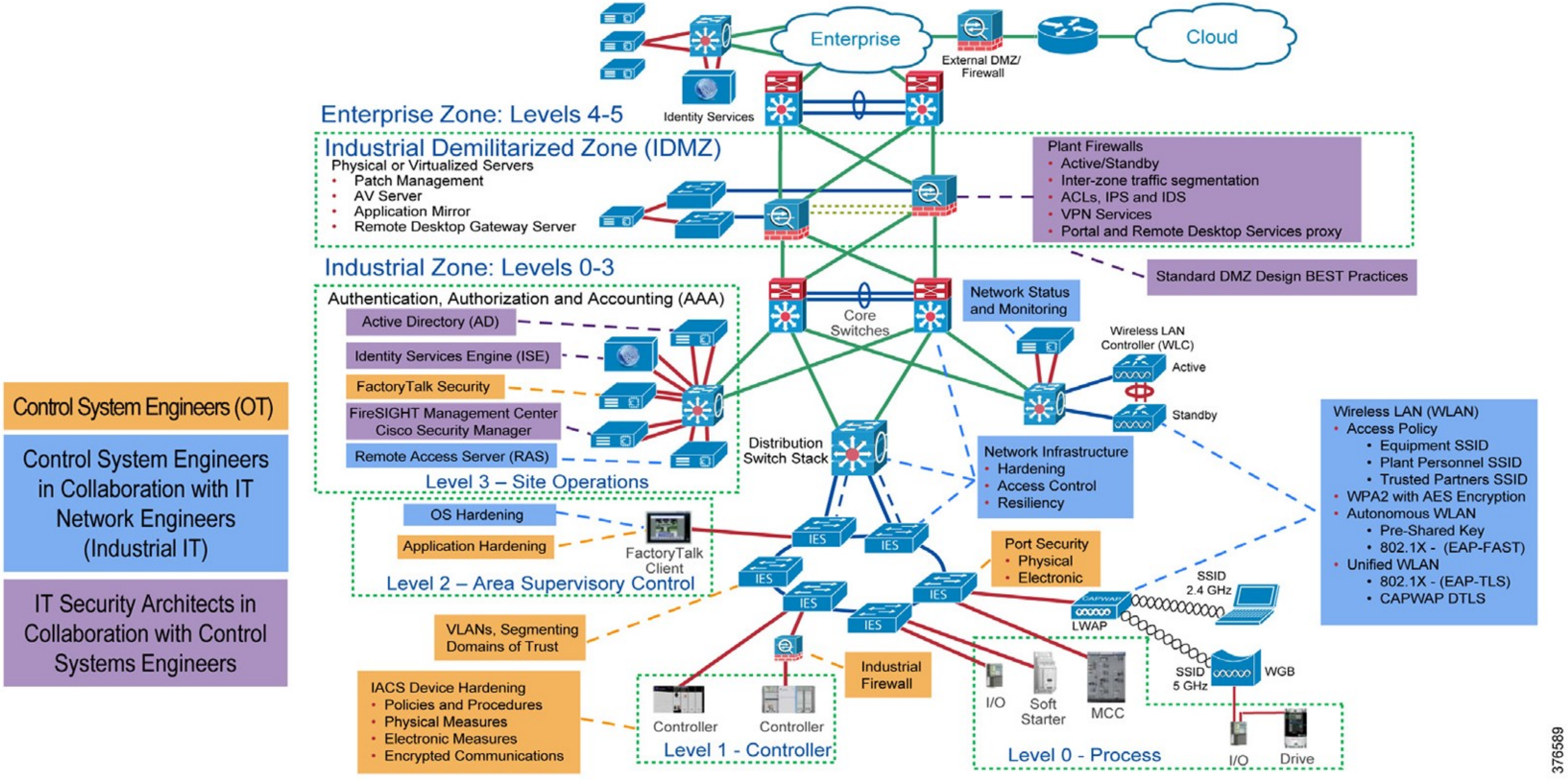
Module 15:
Network Monitoring and Tools

Module Objective: Explain how networks are attacked

Topic Title	Topic Objective
Introduction to Network Monitoring	Explain the importance of network monitoring.
Introduction to Network Monitoring Tools	Explain how network monitoring is conducted.

15.1 Introduction to Network Monitoring

Network Security Architectures (obrázok z prednášky 3)



Physical or Virtualized Servers
- Patch Management
- AV Server
- Application Mirror
- Remote Desktop Gateway Server

Plant Firewalls
- Active/Standby
- Inter-zone traffic segmentation
- ACLs, IPS and IDS
- VPN Services
- Portal and Remote Desktop Services proxy

Standard DMZ Design BEST Practices

Authentication, Authorization and Accounting (AAA)

Active Directory (AD)

Identity Services Engine (ISE)

FactoryTalk Security

FireSIGHT Management Center
Cisco Security Manager

Remote Access Server (RAS)

Network Status and Monitoring

Network Infrastructure
- Hardening
- Access Control
- Resiliency

Wireless LAN (WLAN)
- Access Policy
  - Equipment SSID
  - Plant Personnel SSID
  - Trusted Partners SSID
- WPA2 with AES Encryption
- Autonomous WLAN
  - Pre-Shared Key
  - 802.1X - (EAP-FAST)
- Unified WLAN
  - 802.1X - (EAP-TLS)
  - CAPWAP DTLS

Port Security
- Physical
- Electronic

OS Hardening

Application Hardening

VLANs, Segmenting Domains of Trust

Industrial Firewall

IACS Device Hardening
- Policies and Procedures
- Physical Measures
- Electronic Measures
- Encrypted Communications

Control System Engineers (OT)

Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)

IT Security Architects in Collaboration with Control Systems Engineers

- GOAL: mitigate threats
- HOW: secure and protect network
- WHICH tools: FW, IDS, IPS, ESS (pre-configured rules)
- SOC analyst: review all alerts

Securely Traversing IACS Data across the Industrial Demilitarized Zone Design and Implementation Guide, March 2022

Network Monitoring and Tools

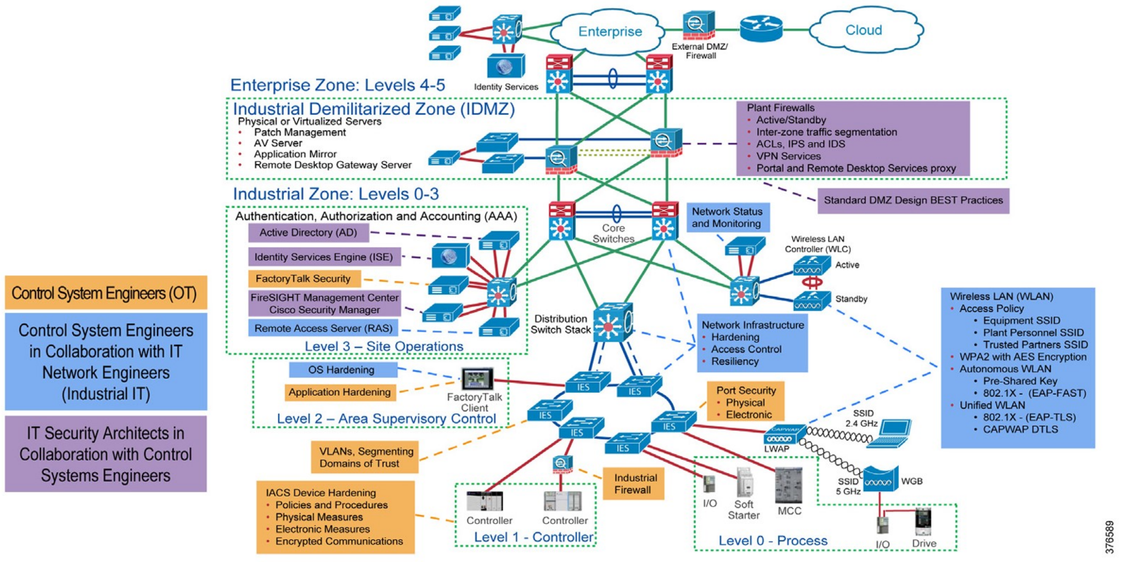
Network Security Topology

- To mitigate threats, all networks must be **secured** and **protected**.
- Network requires a security infrastructure consisting of firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and endpoint security software to protect.
- These methods and technologies are used to introduce automated monitoring, creating security alerts, or automatically blocking offensive devices.
- For large networks, an extra layer of protection is added.
- Devices such as firewalls and IPS operate based on pre-configured rules and monitor traffic and compare it against the configured rules. If there is a match, the traffic is handled according to the rule.
- An important part of the cybersecurity analyst is to review all alerts generated by network devices and determine the validity of the alerts.

Network Monitoring Methods

- The day-to-day operations of a network consists of
  - traffic flow
  - bandwidth usage
  - resource access

  to identify **normal network behavior**


Enterprise
External DMZ/ Firewall
Cloud
Identity Services
Enterprise Zone: Levels 4-5
Industrial Demilitarized Zone (IDMZ)
Physical or Virtualized Servers
• Patch Management
• AV Server
• Application Mirror
• Remote Desktop Gateway Server
Plant Firewalls
• Active/Standby
• Inter-zone traffic segmentation
• ACLs, IPS and IDS
• VPN Services
• Portal and Remote Desktop Services proxy
Standard DMZ Design BEST Practices
Industrial Zone: Levels 0-3
Authentication, Authorization and Accounting (AAA)
Active Directory (AD)
Identity Services Engine (ISE)
FactoryTalk Security
FireSIGHT Management Center
Cisco Security Manager
Remote Access Server (RAS)
Level 3 – Site Operations
Core Switches
Network Status and Monitoring
Wireless LAN Controller (WLC)
Active
Standby
Distribution Switch Stack
Network Infrastructure
• Hardening
• Access Control
• Resiliency
Wireless LAN (WLAN)
• Access Policy
• Equipment SSID
• Plant Personnel SSID
• Trusted Partners SSID
• WPA2 with AES Encryption
• Autonomous WLAN
• Pre-Shared Key
• 802.1X - (EAP-FAST)
• Unified WLAN
• 802.1X - (EAP-TLS)
• CAPWAP DTLS
Control System Engineers (OT)
Control System Engineers in Collaboration with IT Network Engineers (Industrial IT)
IT Security Architects in Collaboration with Control Systems Engineers
OS Hardening
Application Hardening
FactoryTalk Client
Level 2 – Area Supervisory Control
IES
Port Security
• Physical
• Electronic
SSID 2.4 GHz
LWAP
VLANs, Segmenting Domains of Trust
Industrial Firewall
SSID 5 GHz
WGB
IACS Device Hardening
• Policies and Procedures
• Physical Measures
• Electronic Measures
• Encrypted Communications
Controller
Controller
Level 1 - Controller
I/O
Soft Starter
MCC
Level 0 - Process
I/O
Drive
376589

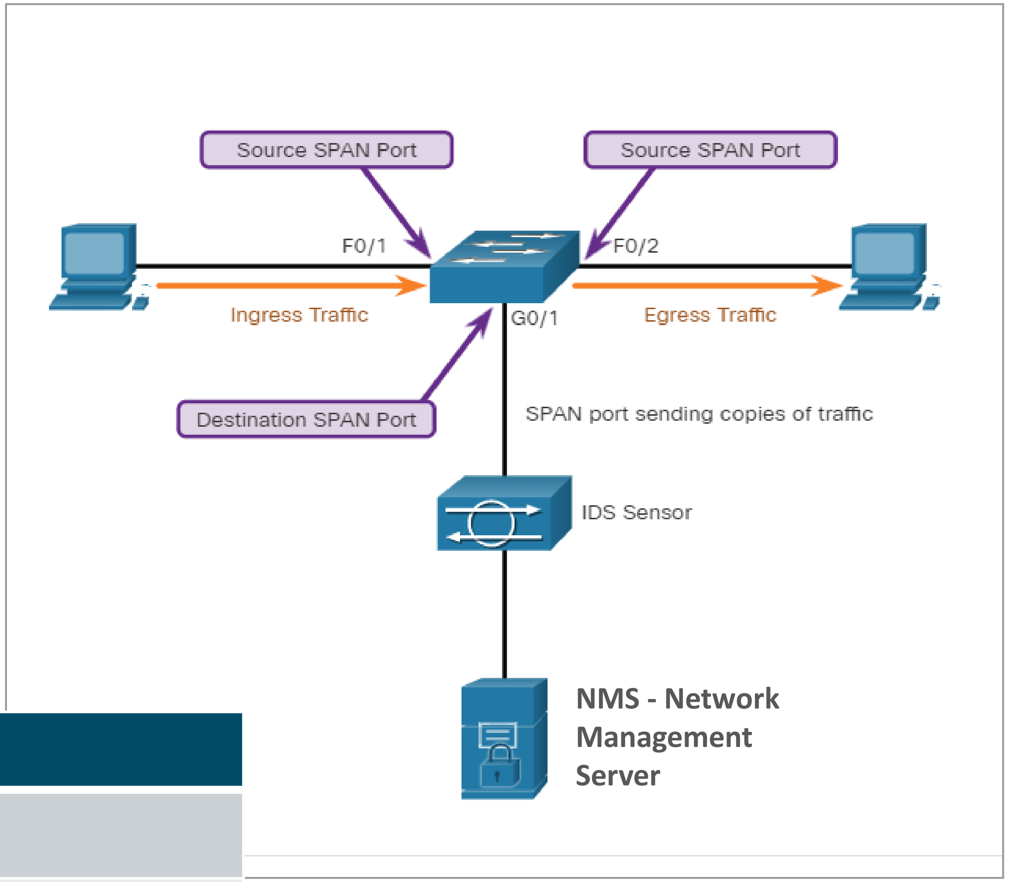
- HOW:
  - implement network monitoring
- WHICH (tools):
  - capture
    - traffic and send it to NMS devices
      - TAPs (Test Access Points)
      - Port mirror (SPAN)
    - packet flow info
      - Netflow
    - SNMP traps and info
    - logs
  - Analyze
    - Packet sniffer
      - Wireshark / Tshark
      - Tcpdump
    - IDS
    - SIEM

Network Monitoring and Tools

Traffic Mirroring and SPAN

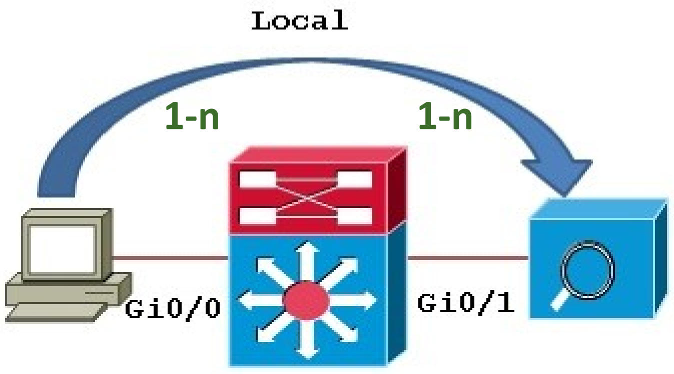
- Capturing data for network monitoring requires all traffic to be captured.
- Special techniques such as port mirroring must be employed to bypass network segmentation imposed by network switches.
- Port mirroring enables the switch to copy frames that are received on one or more ports to a Switch Port Analyzer (SPAN) port that is connected to an analysis device.
- The table identifies and describes the SPAN terms.

SPAN Term	Description
Ingress traffic	Traffic that enters the switch
Egress traffic	Traffic that leaves the switch.
Source (SPAN) port	Source ports are monitored as traffic entering them is replicated (mirrored) to the destination ports.
Destination (SPAN) port	A port that mirrors source ports. Destination SPAN ports often connect to analysis devices such as a packet analyzer or an IDS.

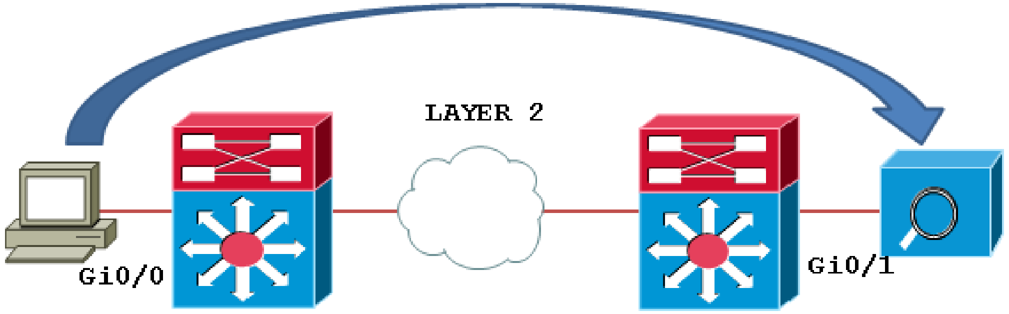


Traffic Mirroring and SPAN (Contd.)

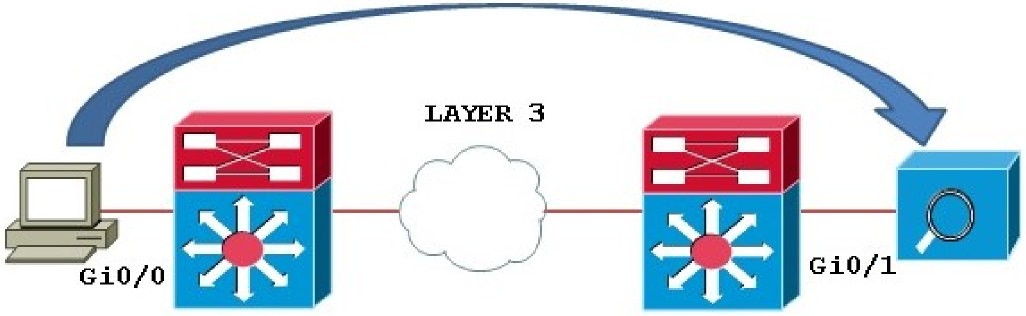
- **SPAN session** = association between source ports and a dest. port
- Single **Local SPAN** session:
  - Source:
    - **one or multiple ports can be monitored, or:**
    - **source VLAN** can be specified in which all ports in the source VLAN become sources of SPAN traffic.
  - Destination
    - In few Cisco switches, session traffic can be copied **to more than one destination port**.
- Variations:
  - **Remote SPAN (RSPAN)** enables a network administrator to use the flexibility of VLANs to monitor traffic on remote switches.
  - **encapsulated Remote SPAN (ERSPAN)**, brings generic routing encapsulation (GRE) for all captured traffic and allows it to be extended across Layer 3 domains
    - we need to have an **RSPAN VLAN**, those VLANs have **special properties** and can't be assigned to any access ports



Local SPAN

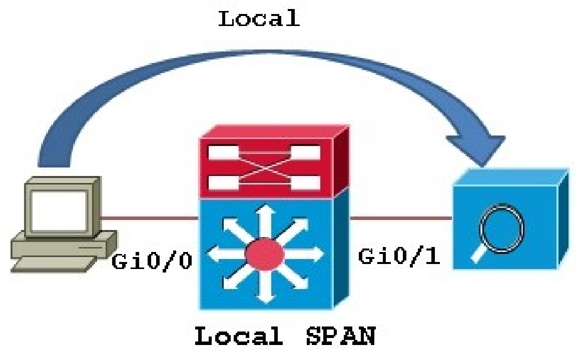


Remote SPAN



ERSPAN

SPAN configuration



- **Local SPAN**

```
Switch1(config)# monitor session 1 source interface Gi0/0
Switch1(config)# monitor session 1 destination interface Gi0/1
```

- **Remote SPAN**

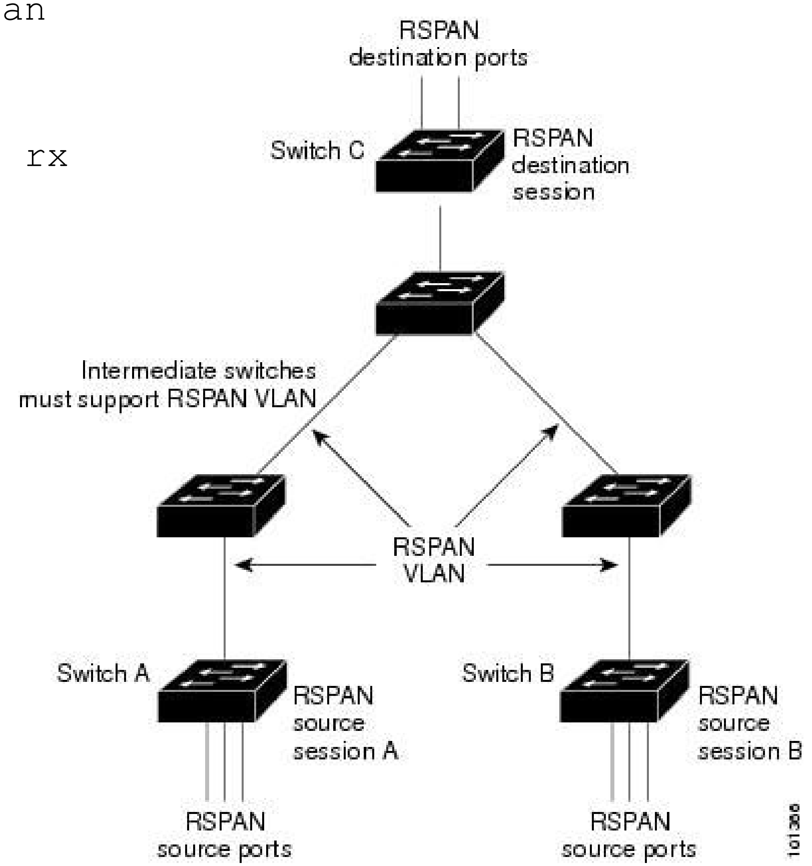
```
SwitchA(config)# vlan 200       ... SwitchC(config)# vlan 200
SwitchA(config-vlan)# remote-span ..SwitchC(config-vlan)# remote-span
```

Source switch:

```
SwitchA(config)# monitor session 1 source interface fastEthernet0/2 rx
SwitchA(config)# monitor session 1 destination remote vlan 200
```

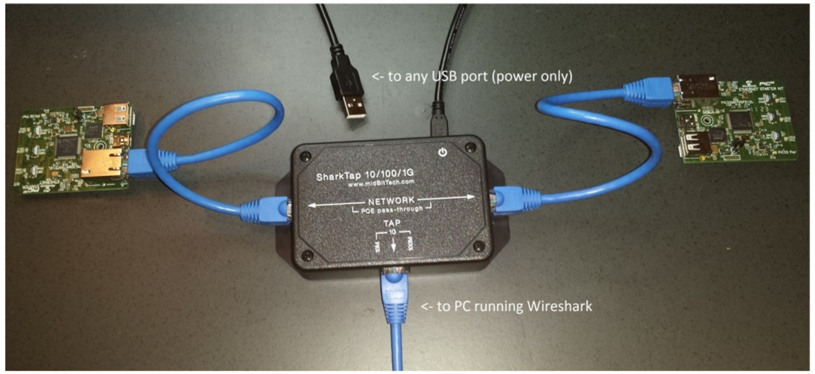
Destination switch (na ktorom je NMS)

```
SwitchC(config)# monitor session 1 source remote vlan 200
SwitchC(config)# monitor session 1 destination interface fa0/3
```

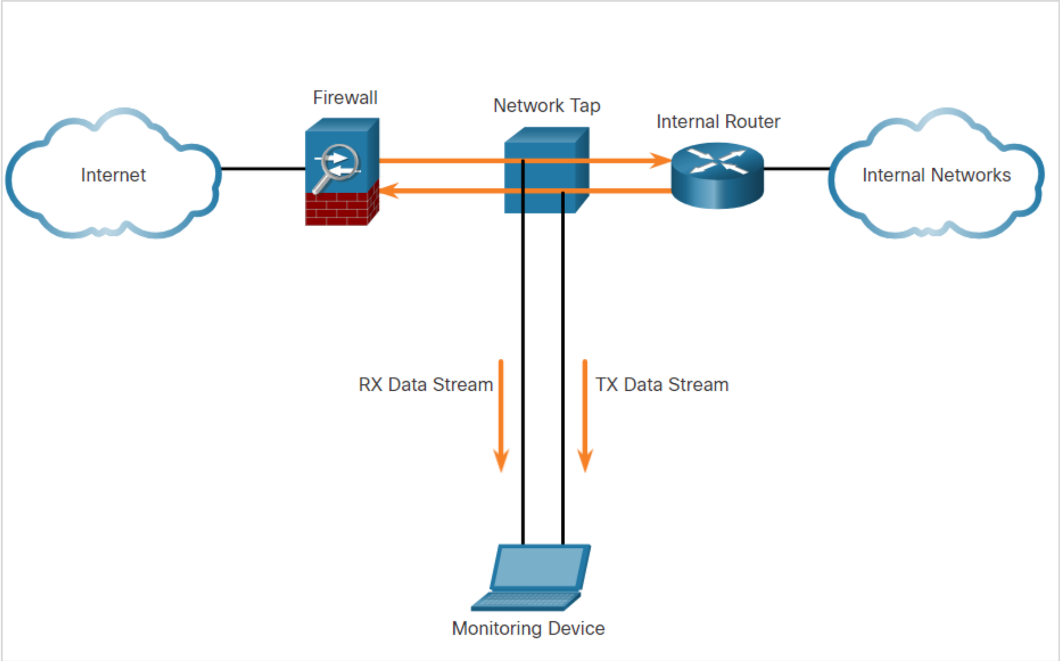


Network Monitoring and Tools

Network Taps



- A network tap is a **passive splitting device** implemented inline between a device of interest and the network.
- A tap forwards all traffic, **including physical layer errors**, to an analysis device while allowing the traffic to reach its intended destination.
- Here, the tap simultaneously sends both the transmit (**TX**) data stream from the internal router and the receive (**RX**) data stream to the internal router on separate, dedicated channels.
- This ensures that all data arrives at the monitoring device **in real time**.
- Taps are **fail-safe**, which means that the traffic between the firewall and internal router is not affected.



Implementing a TAP in a Sample Network

15.2 Introduction to Network Monitoring Tools

Introduction to Network Monitoring and Tools

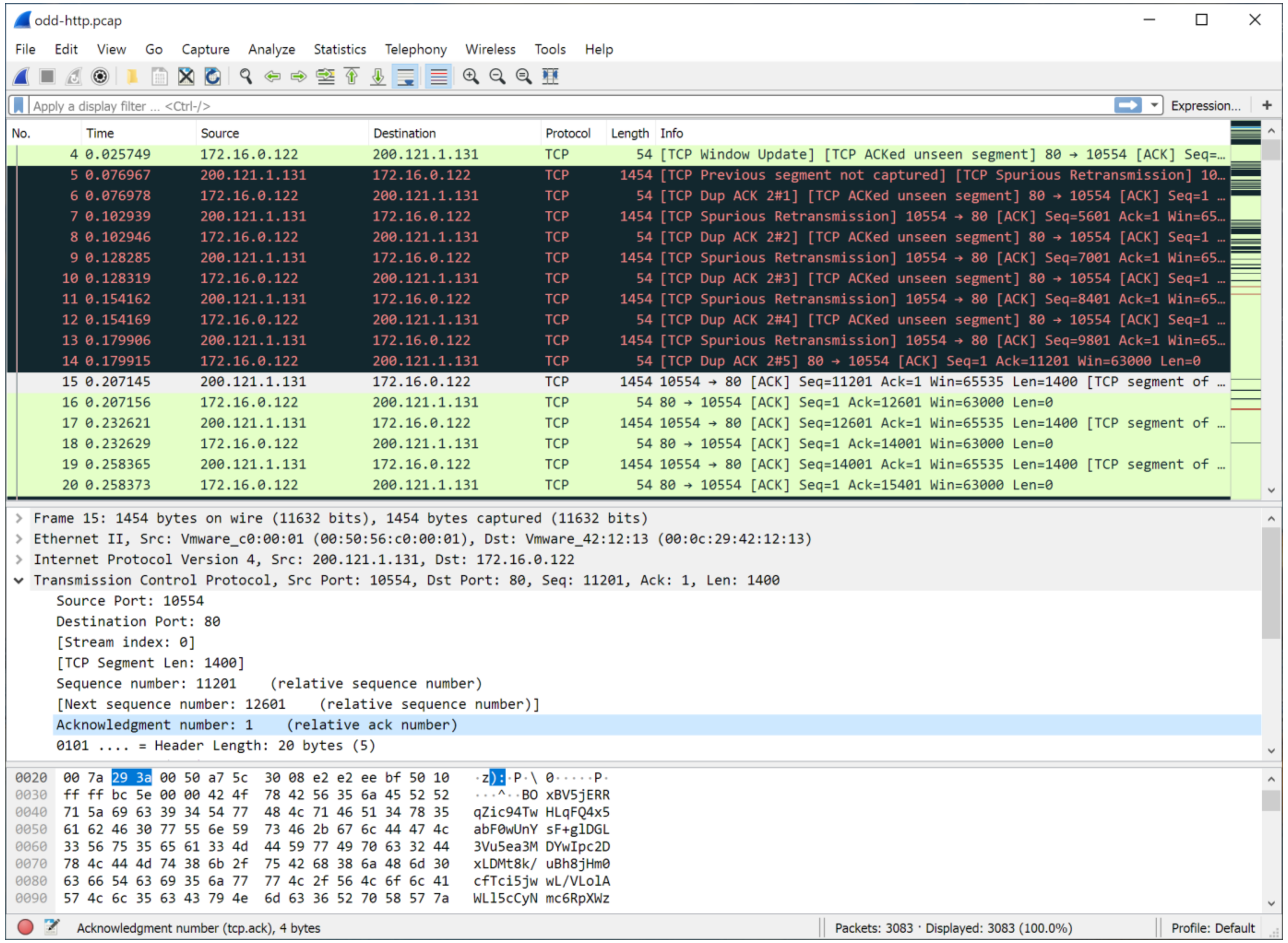
Network Security Monitoring Tools

- Common tools that are used for network security monitoring include:
  - Network protocol analyzers such as Wireshark/Tshark and Tcpdump
  - NetFlow
  - Security Information and Event Management Systems (SIEM)
- It is common for security analysts to rely on log files and Simple Network Management Protocol (SNMP) for network behavior discovery.

- HOW
  - To implement network monitoring
- WHICH (tools):
  - **To capture**
    - traffic and send it to NMS devices
      - With TAPs (Test Access Points)
      - With Port mirror (SPAN)
    - packet flow info
      - Netflow
  - **To Analyze**
    - With Packet sniffer
      - Wireshark / Tshark
      - Tcpdump
    - With IDS
    - With SIEM

Network Protocol Analyzers

- Network protocol analyzers (or ‘packet sniffer’ applications) are programs used to capture traffic.
- Protocol analyzers display what is happening on the network through
  - a graphical user interface
  - or CLI
- Network protocol analyzers are not only used for security analysis but also used for network troubleshooting, software and protocol development, and education.
- As shown in the figure, Wireshark is used in Windows, Linux, and Mac OS environments. It is a very useful tool for learning network protocol communications.



```
No.  Time       Source          Destination     Protocol  Length Info
   4 0.025749   172.16.0.122    200.121.1.131   TCP         54 [TCP Window Update] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=…
   5 0.076967   200.121.1.131   172.16.0.122    TCP       1454 [TCP Previous segment not captured] [TCP Spurious Retransmission] 10…
   6 0.076978   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#1] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
   7 0.102939   200.121.1.131   172.16.0.122    TCP       1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=5601 Ack=1 Win=65…
   8 0.102946   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#2] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
   9 0.128285   200.121.1.131   172.16.0.122    TCP       1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=7001 Ack=1 Win=65…
  10 0.128319   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#3] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
  11 0.154162   200.121.1.131   172.16.0.122    TCP       1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=8401 Ack=1 Win=65…
  12 0.154169   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#4] [TCP ACKed unseen segment] 80 → 10554 [ACK] Seq=1 …
  13 0.179906   200.121.1.131   172.16.0.122    TCP       1454 [TCP Spurious Retransmission] 10554 → 80 [ACK] Seq=9801 Ack=1 Win=65…
  14 0.179915   172.16.0.122    200.121.1.131   TCP         54 [TCP Dup ACK 2#5] 80 → 10554 [ACK] Seq=1 Ack=11201 Win=63000 Len=0
  15 0.207145   200.121.1.131   172.16.0.122    TCP       1454 10554 → 80 [ACK] Seq=11201 Ack=1 Win=65535 Len=1400 [TCP segment of …
  16 0.207156   172.16.0.122    200.121.1.131   TCP         54 80 → 10554 [ACK] Seq=1 Ack=12601 Win=63000 Len=0
  17 0.232621   200.121.1.131   172.16.0.122    TCP       1454 10554 → 80 [ACK] Seq=12601 Ack=1 Win=65535 Len=1400 [TCP segment of …
  18 0.232629   172.16.0.122    200.121.1.131   TCP         54 80 → 10554 [ACK] Seq=1 Ack=14001 Win=63000 Len=0
  19 0.258365   200.121.1.131   172.16.0.122    TCP       1454 10554 → 80 [ACK] Seq=14001 Ack=1 Win=65535 Len=1400 [TCP segment of …
  20 0.258373   172.16.0.122    200.121.1.131   TCP         54 80 → 10554 [ACK] Seq=1 Ack=15401 Win=63000 Len=0
```

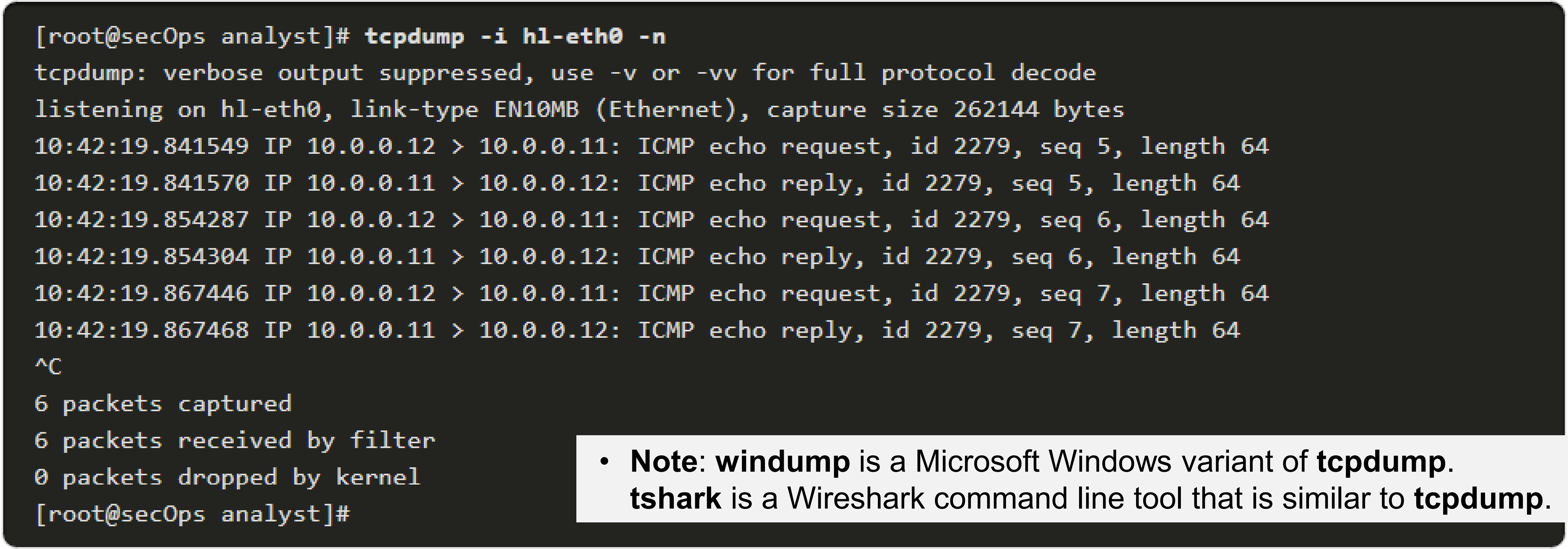
```
> Frame 15: 1454 bytes on wire (11632 bits), 1454 bytes captured (11632 bits)
> Ethernet II, Src: Vmware_c0:00:01 (00:50:56:c0:00:01), Dst: Vmware_42:12:13 (00:0c:29:42:12:13)
> Internet Protocol Version 4, Src: 200.121.1.131, Dst: 172.16.0.122
v Transmission Control Protocol, Src Port: 10554, Dst Port: 80, Seq: 11201, Ack: 1, Len: 1400
    Source Port: 10554
    Destination Port: 80
    [Stream index: 0]
    [TCP Segment Len: 1400]
    Sequence number: 11201    (relative sequence number)
    [Next sequence number: 12601    (relative sequence number)]
    Acknowledgment number: 1    (relative ack number)
    0101 .... = Header Length: 20 bytes (5)
```

```
0020  00 7a 29 3a 00 50 a7 5c  30 08 e2 e2 ee bf 50 10   ·z):·P·\ 0·····P·
0030  ff ff bc 5e 00 00 42 4f  78 42 56 35 6a 45 52 52   ···^··BO xBV5jERR
0040  71 5a 69 63 39 34 54 77  48 4c 71 46 51 34 78 35   qZic94Tw HLqFQ4x5
0050  61 62 46 30 77 55 6e 59  73 46 2b 67 6c 44 47 4c   abF0wUnY sF+glDGL
0060  33 56 75 35 65 61 33 4d  44 59 77 49 70 63 32 44   3Vu5ea3M DYwIpc2D
0070  78 4c 44 4d 74 38 6b 2f  75 42 68 38 6a 48 6d 30   xLDMt8k/ uBh8jHm0
0080  63 66 54 63 69 35 6a 77  77 4c 2f 56 4c 6f 6c 41   cfTci5jw wL/VLolA
0090  57 4c 6c 35 63 43 79 4e  6d 63 36 52 70 58 57 7a   WLl5cCyN mc6RpXWz
```

Acknowledgment number (tcp.ack), 4 bytes | Packets: 3083 · Displayed: 3083 (100.0%) | Profile: Default

Network Protocol Analyzers (Contd.)

- Frames captured by Wireshark are saved in a PCAP file that contains information regarding the frame, interface, packet length, time stamps, and all binary files sent across the network.
- Wireshark can open files containing captured traffic from other software such as the **tcpdump** utility.
- The example in the command output displays a sample **tcpdump** capture of **ping** packets.



```
[root@secOps analyst]# tcpdump -i hl-eth0 -n
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on hl-eth0, link-type EN10MB (Ethernet), capture size 262144 bytes
10:42:19.841549 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 5, length 64
10:42:19.841570 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 5, length 64
10:42:19.854287 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 6, length 64
10:42:19.854304 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 6, length 64
10:42:19.867446 IP 10.0.0.12 > 10.0.0.11: ICMP echo request, id 2279, seq 7, length 64
10:42:19.867468 IP 10.0.0.11 > 10.0.0.12: ICMP echo reply, id 2279, seq 7, length 64
^C
6 packets captured
6 packets received by filter
0 packets dropped by kernel
[root@secOps analyst]#
```

- **Note**: **windump** is a Microsoft Windows variant of **tcpdump**. **tshark** is a Wireshark command line tool that is similar to **tcpdump**.

tcpdump

- Version: 4.99.1
  Last Release: June 9, 2021
- **Van Jacobson**, Craig Leres and Steven McCanne, all of the Lawrence Berkeley National Laboratory, University of California, Berkeley, CA

What does tcpdump do?

- **prints out a description** of the contents of packets on a network interface
  - that match the boolean *expression*
  - **-w** flag, which causes it to save the packet data to a file for later analysis
  - **-r** flag, which causes it to read from a saved packet file rather than to read packets from a network interface

INTERNET HALL of FAME

one of the primary contributors to the TCP/IP protocol stack

Jacobson's algorithm to handle congestion

Van Jacobson TCP/IP Header Compression

- **continue capturing packets until** it is interrupted by
  - SIGINT signal (control-C) or
  - SIGTERM signal (**kill**(1) command)
  - if run with the **-c** flag, it will capture packets until specified number of packets have been processed (or interupt)
- When *tcpdump* finishes capturing packets, it will **report counts of**:
  - packets *'captured'*,
  - packets *'received by filter'*,
  - packets *'dropped by kernel'*, (lack of buffer space)
- Requirements – special rights:
  - Linux: You must be root or *tcpdump* must be installed setuid to root

tcpdump

- **tcpdump** [**-AdDeflLnNOpqRStuUvxX**]
  [**-c** *count*]
  [**-C** *file_size*]
  [**-W** *filecount*] (in conjuctions with -C)
  [**-F** *file_as_input_for expression*]
  [**-i** *interface_listen_on*]
  [**-m** *module_SMI_MIB*]
  [**-M** *secret_MD5*] (diggest with TCP segments)
  [**-w** *file_name*]
  [**-r** *file*]
  [**-s** *snapshotLength*] (default 262144 B)
  [**-T** *type*] (ptp, quic, radius, snmp, tftp, ..)
  [**-E** *spi@ipaddr algo:secret,...*]

  secret for decrypting IPsec ESP packets that are addressed to *addr* and contain Security Parameter Index value *spi*. This combination may be repeated with comma or newline separation

  [**-y** *datalinktype*] (see –L in the table)

  wifi... fake Eth headers, or 802.11 headers

  [**-Z** *user*]

  Drops privileges (if root) and changes user ID to user and the group ID to the primary group of user. This behavior can also be enabled by default at compile time.

  [*expression*] (next slide...)

-A	Print each packet (minus its link level header) in ASCII. Handy for capturing web pages.
-d	Dump the compiled packet-matching code in a human readable form to standard output and stop.
-D	Print the list of the network interfaces available on the system and on which *tcpdump* can capture packets
-e	Print the link-level header on each dump line.
-f	Print `foreign' IPv4 addresses numerically rather than symbolically
-l	Make stdout line buffered. Useful if you want to see the data while capturing
-L	List the known data link types for the interface and exit.
-n	Don't convert addresses and port numbers, etc. to names
-N	Don't print domain name qualification of host names.

Tcpdump – filter boolean expressions

- **selects** which packets will be dumped
  - if **no *expression*** is given, **all** packets on the net will be dumped
  - **otherwise**, only packets for which *expression* is `**true**' will be dumped
- consists of one or more *primitives*
  - *id* (name or number) preceded by one or more qualifiers:
    - *type*
      - **host** foo, net 128.3, port 20, portrange 6000-6008
    - *dir (*transfer direction*)*
      - src foo, dst net 128.3, **src or dst** port ftp-data
    - *Proto*
      - ether, fddi, tr, wlan, ip, ip6, arp, rarp, dec net, tcp and udp
      - ether src foo, arp net 128.3, tcp port 21, `udp portrange 7000-7009

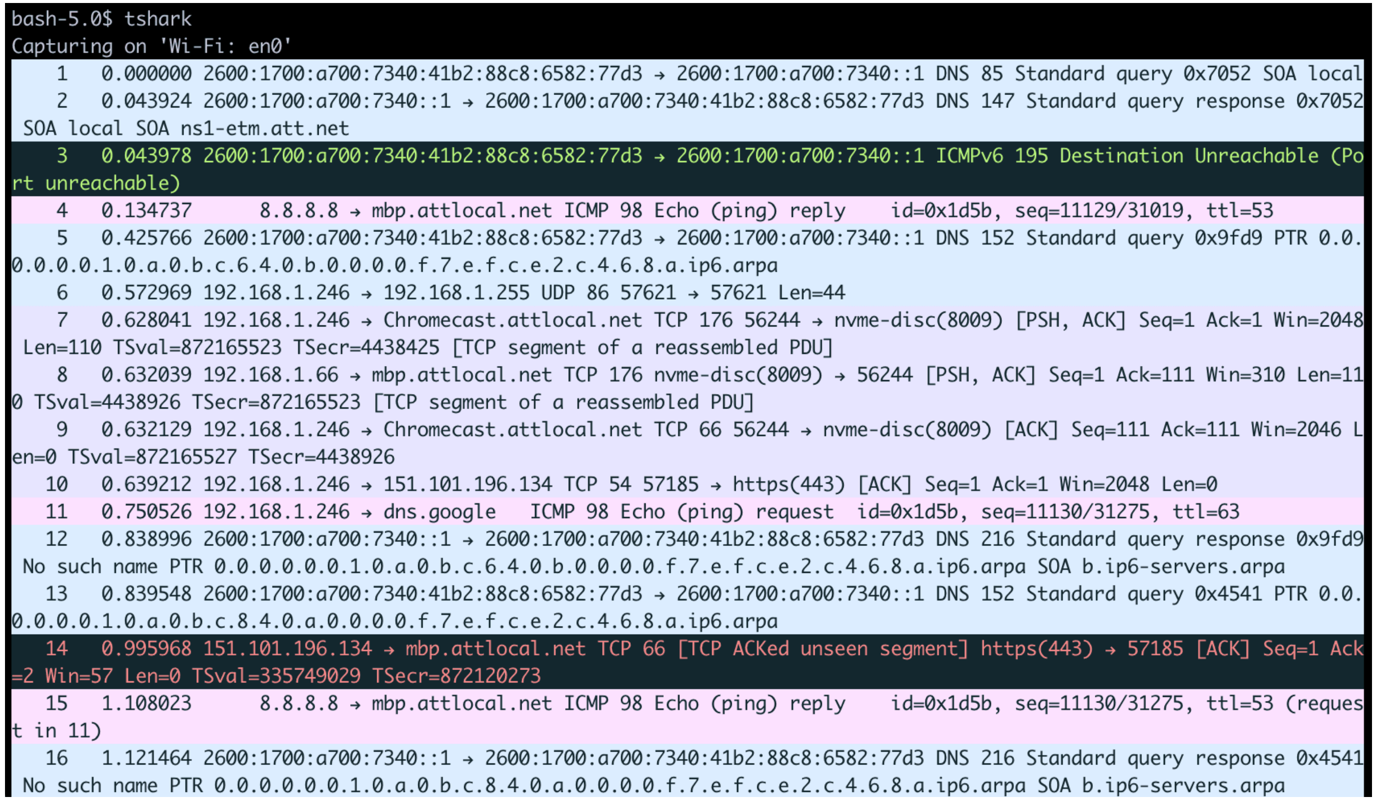
- **Special primitives**
  - gateway, broadcast, less, greater and arithmetic expressions
  - and, or, not

https://www.tcpdump.org/manpages/tcpdump.1.html
https://www.tcpdump.org/manpages/pcap-filter.7.html

Terminal wire**SHARK**

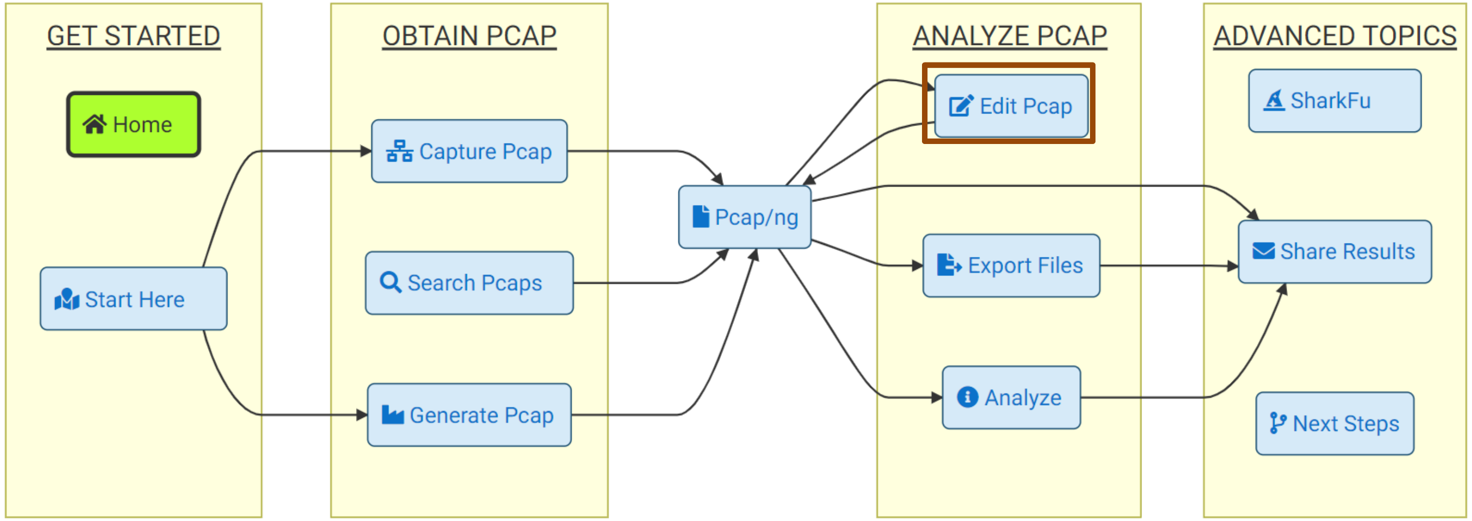
Tshark

- tshark is the CLI component of Wireshark
- has most, but not all,
  of the features of Wireshark
- but far better for scripting



```
bash-5.0$ tshark
Capturing on 'Wi-Fi: en0'
    1   0.000000 2600:1700:a700:7340:41b2:88c8:6582:77d3 → 2600:1700:a700:7340::1 DNS 85 Standard query 0x7052 SOA local
    2   0.043924 2600:1700:a700:7340::1 → 2600:1700:a700:7340:41b2:88c8:6582:77d3 DNS 147 Standard query response 0x7052
 SOA local SOA ns1-etm.att.net
    3   0.043978 2600:1700:a700:7340:41b2:88c8:6582:77d3 → 2600:1700:a700:7340::1 ICMPv6 195 Destination Unreachable (Po
rt unreachable)
    4   0.134737      8.8.8.8 → mbp.attlocal.net ICMP 98 Echo (ping) reply    id=0x1d5b, seq=11129/31019, ttl=53
    5   0.425766 2600:1700:a700:7340:41b2:88c8:6582:77d3 → 2600:1700:a700:7340::1 DNS 152 Standard query 0x9fd9 PTR 0.0.
0.0.0.0.1.0.a.0.b.c.6.4.0.b.0.0.0.0.f.7.e.f.c.e.2.c.4.6.8.a.ip6.arpa
    6   0.572969 192.168.1.246 → 192.168.1.255 UDP 86 57621 → 57621 Len=44
    7   0.628041 192.168.1.246 → Chromecast.attlocal.net TCP 176 56244 → nvme-disc(8009) [PSH, ACK] Seq=1 Ack=1 Win=2048
 Len=110 TSval=872165523 TSecr=4438425 [TCP segment of a reassembled PDU]
    8   0.632039 192.168.1.66 → mbp.attlocal.net TCP 176 nvme-disc(8009) → 56244 [PSH, ACK] Seq=1 Ack=111 Win=310 Len=11
0 TSval=4438926 TSecr=872165523 [TCP segment of a reassembled PDU]
    9   0.632129 192.168.1.246 → Chromecast.attlocal.net TCP 66 56244 → nvme-disc(8009) [ACK] Seq=111 Ack=111 Win=2046 L
en=0 TSval=872165527 TSecr=4438926
   10   0.639212 192.168.1.246 → 151.101.196.134 TCP 54 57185 → https(443) [ACK] Seq=1 Ack=1 Win=2048 Len=0
   11   0.750526 192.168.1.246 → dns.google   ICMP 98 Echo (ping) request  id=0x1d5b, seq=11130/31275, ttl=63
   12   0.838996 2600:1700:a700:7340::1 → 2600:1700:a700:7340:41b2:88c8:6582:77d3 DNS 216 Standard query response 0x9fd9
 No such name PTR 0.0.0.0.0.0.1.0.a.0.b.c.6.4.0.b.0.0.0.0.f.7.e.f.c.e.2.c.4.6.8.a.ip6.arpa SOA b.ip6-servers.arpa
   13   0.839548 2600:1700:a700:7340:41b2:88c8:6582:77d3 → 2600:1700:a700:7340::1 DNS 152 Standard query 0x4541 PTR 0.0.
0.0.0.0.1.0.a.0.b.c.8.4.0.a.0.0.0.0.f.7.e.f.c.e.2.c.4.6.8.a.ip6.arpa
   14   0.995968 151.101.196.134 → mbp.attlocal.net TCP 66 [TCP ACKed unseen segment] https(443) → 57185 [ACK] Seq=1 Ack
=2 Win=57 Len=0 TSval=335749029 TSecr=872120273
   15   1.108023      8.8.8.8 → mbp.attlocal.net ICMP 98 Echo (ping) reply    id=0x1d5b, seq=11130/31275, ttl=53 (reques
t in 11)
   16   1.121464 2600:1700:a700:7340::1 → 2600:1700:a700:7340:41b2:88c8:6582:77d3 DNS 216 Standard query response 0x4541
 No such name PTR 0.0.0.0.0.0.1.0.a.0.b.c.8.4.0.a.0.0.0.0.f.7.e.f.c.e.2.c.4.6.8.a.ip6.arpa SOA b.ip6-servers.arpa
```

Capture Lifecycle with Tshark



Edit pcaps

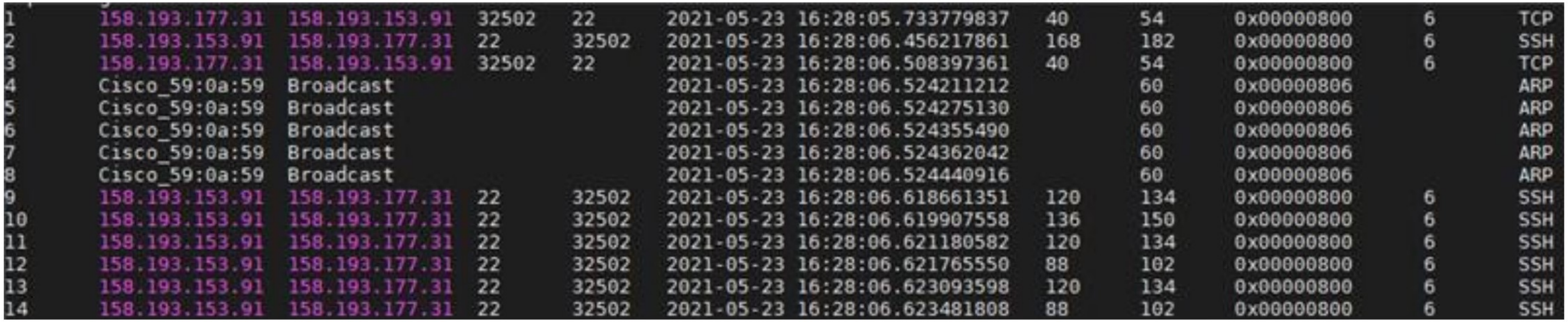
- Editing Hex
  - *Put a hex on your hex*
- reordercap
  - *I am still making order out of chaos by reinvention. — John le Carre*
- editcap
  - *Edit packet captures after they have been taken*
- mergecap
  - *Merge captures together*
- text2pcap
  - *Convert hexdumps to packet captures*
- Sanitizing Hex
  - *Put a hex on your hex*

ip.proto je ale len pre IPv4, takze pre IPv6 je to treba riešiť extra stĺpcami
ipv6.nxt / Next Header v IPv6
ipv6.plen / payload length

tshark

- Príklad pre zistenie týchto info z prevádzky:

*No. | IPsrc | IPdst | SrcPort | DstPort | Time | ip.Length | Length | eth.type | **ip.proto** | Protocol |*



```
1    158.193.177.31  158.193.153.91  32502  22     2021-05-23 16:28:05.733779837  40   54   0x00000800  6  TCP
2    158.193.153.91  158.193.177.31  22     32502  2021-05-23 16:28:06.456217861  168  182  0x00000800  6  SSH
3    158.193.177.31  158.193.153.91  32502  22     2021-05-23 16:28:06.508397361  40   54   0x00000800  6  TCP
4    Cisco_59:0a:59  Broadcast                     2021-05-23 16:28:06.524211212       60   0x00000806     ARP
5    Cisco_59:0a:59  Broadcast                     2021-05-23 16:28:06.524275130       60   0x00000806     ARP
6    Cisco_59:0a:59  Broadcast                     2021-05-23 16:28:06.524355490       60   0x00000806     ARP
7    Cisco_59:0a:59  Broadcast                     2021-05-23 16:28:06.524362042       60   0x00000806     ARP
8    Cisco_59:0a:59  Broadcast                     2021-05-23 16:28:06.524440916       60   0x00000806     ARP
9    158.193.153.91  158.193.177.31  22     32502  2021-05-23 16:28:06.618661351  120  134  0x00000800  6  SSH
10   158.193.153.91  158.193.177.31  22     32502  2021-05-23 16:28:06.619907558  136  150  0x00000800  6  SSH
11   158.193.153.91  158.193.177.31  22     32502  2021-05-23 16:28:06.621180582  120  134  0x00000800  6  SSH
12   158.193.153.91  158.193.177.31  22     32502  2021-05-23 16:28:06.621765550  88   102  0x00000800  6  SSH
13   158.193.153.91  158.193.177.31  22     32502  2021-05-23 16:28:06.623093598  120  134  0x00000800  6  SSH
14   158.193.153.91  158.193.177.31  22     32502  2021-05-23 16:28:06.623481808  88   102  0x00000800  6  SSH
```

sudo tshark -i 2 -i 3 -o nameres.mac_name:FALSE -o gui.column.format:"No.,%m,Source,%s,Destination,%d,SrcPort,%uS,DstPort,%uD,Time,%Yt,Length,%L,Protocol,%p" -T fields -e _ws.col.No. -e _ws.col.Source -e _ws.col.Destination -e _ws.col.SrcPort -e _ws.col.DstPort -e _ws.col.Time -e ip.len -e _ws.col.Length -e eth.type -e ip.proto -e ipv6.nxt -e ipv6.plen -e _ws.col.Protocol -e ip.geoip.country_iso -t ad -b filesize:10000000 -b files:40 -w /pcap.pcapng > tshark3.csv

No. | IPsrc | IPdst | SrcPort | DstPort | Time | ip.Length | Length | eth.type | ip.proto | ipv6.nxt |ipv6.plen | Protocol | SrcCountry,DstContry

tshark

- Nastavenie **interfaces** na zachytávanie (ich zoznam možno získať príkazom tshark -D):
  - -i 2 -i 3
- **Vypnutie prekladania MAC** adries:
  - -o nameres.mac_name:FALSE
- Atribúty začínajúce na _ws.col. sú **stĺpce**, ktoré tshark preberá z WS
  - ich **formát** je možne zmeniť v nastaveniach WS na localhoste, alebo je možne použiť ad hoc override v príkaze:
    - -o gui.column.format:"No.,%m,Source,%s,Destination,%d,SrcPort,%uS,DstPort,%uD,Time,%Yt,Length,%L,Protocol,%p"
- Nastavenie **formátu času**, bez tohto sa zobrazí len čas od začiatku capture:
  - -t ad
- Nastavenia **ring buffera** (zapisovanie do n pcapng suborov dookola):
  - Nastavenie maximálnej veľkosti pcapng súboru (10000000 by malo byt približne 10 GB, ale reálne sa veľkosť súborov pohybuje okolo 2 GB):
    - -b filesize:10000000
  - Nastavenia poctu súborov ring buffera (Čim väčšia prevádzka, tým väčšie číslo tu musí byť - https://wireshark-users.wireshark.narkive.com/WGRBS9Bk/tshark-crash-with-capture-ring-buffer-b-and-decoding-packets-s):
    - -b files:40

No. | IPsrc | IPdst | SrcPort | DstPort | Time | ip.Length | Length | eth.type | ip.proto | ipv6.nxt |ipv6.plen | Protocol | SrcCountry,DstContry

tshark

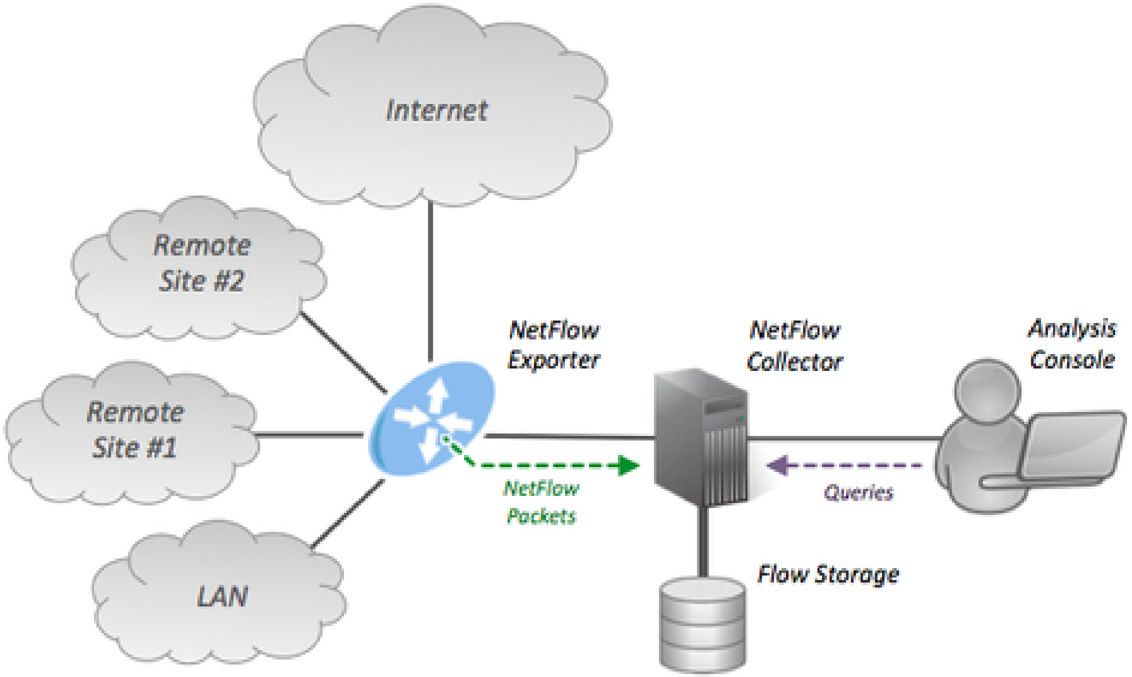
- Nastavenie **výstupného pcapng** súboru (vzhľadom na použitie ring buffera je braný ako maska pre názov jednotlivých súborov, napr. /pcap_00160_20210601211638.pcapng):
  - -w /pcap.pcapng
- **Ring buffer** tu sluzi na 2 veci:
  - Bez neho by po par hodinách zabral celu RAM a spadol by (s ring bufferom uvoľní väčšinu RAMky keď prechádza na zapisovanie do ďalšieho súboru)
  - Bez neho by tshark zapisoval do jedného pcapng súboru v /tmp/ a po par hodinách by zabral celý disk
  - Do .pcapng súboru zapisuje vždy, aj keď výstupný súbor nie je špecifikovaný cez -w
  - Ring buffer ma jednu nevýhodu, pri prepnutí na zapisovanie do ďalšieho súboru sa resetne Tshark session
    - takže počítadlá, vrátane poradia paketov sa vynulujú.
- **Zapisovanie výstupu** z terminálu do **súboru** (pre rewrite: >, pre append: >>):
  - > tshark3.csv
- **GeoIP**
  - V súbore /usr/share/wireshark/maxmind_db_paths sa nachádza cesta ku adresáru GeoIP databázy, ktorý používa tshark na zobrazenie krajiny
  - Treba stiahnuť GeoIP databázu z maxmind a nalinkovať cestu k nej.
  - -e ip.geoip.country_iso (pre source a dest krajinu)

No. | IPsrc | IPdst | SrcPort | DstPort | Time | ip.Length | Length | eth.type | ip.proto | ipv6.nxt |ipv6.plen | Protocol | SrcCountry,DstContry

- ip.proto je ale len pre IPv4, takze pre IPv6 je to treba riešiť extra stĺpcami
  - ipv6.nxt / Next Header v IPv6
  - ipv6.plen / payload length
- Ako doplniť GeoIP databázu - SrcCountry,DstContry
  - -e ip.geoip.country_iso

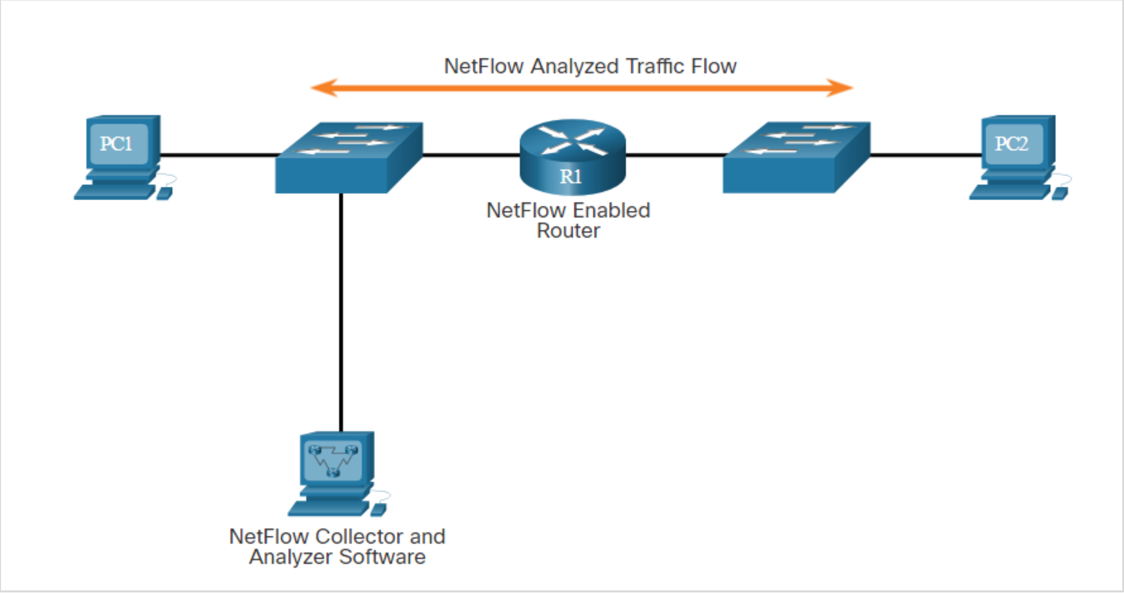
NetFlow

- NetFlow is a Cisco IOS technology that provides 24x7 statistics on packets that flow through a Cisco router or multilayer switch.
- NetFlow is the standard for collecting IP operational data in IP networks.
- NetFlow can be used for network and security monitoring, network planning, and traffic analysis. It provides a complete audit trail of basic information about every IP flow forwarded on a device.
- Although NetFlow stores flow information in a local cache on the device, it should always be configured to forward data to a NetFlow collector which stores the NetFlow data.



NetFlow (Contd.)

- NetFlow can monitor application connection by tracking byte and packet counts for that individual application flow.
- It pushes the statistics over to an external server called a NetFlow collector.
- Cisco Stealthwatch collects NetFlow statistics to perform advanced functions including:
  - **Flow stitching -** It groups individual entries into flows.
  - **Flow deduplication** - It filters duplicate incoming entries from multiple NetFlow clients.
  - **NAT stitching** - It simplifies flows with NAT entries.

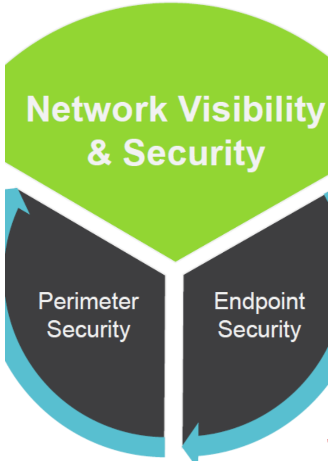

NetFlow Analyzed Traffic Flow
PC1
R1
NetFlow Enabled Router
PC2
NetFlow Collector and Analyzer Software

PC1 connected to PC2 using HTTPS

Security Services

NetFlow

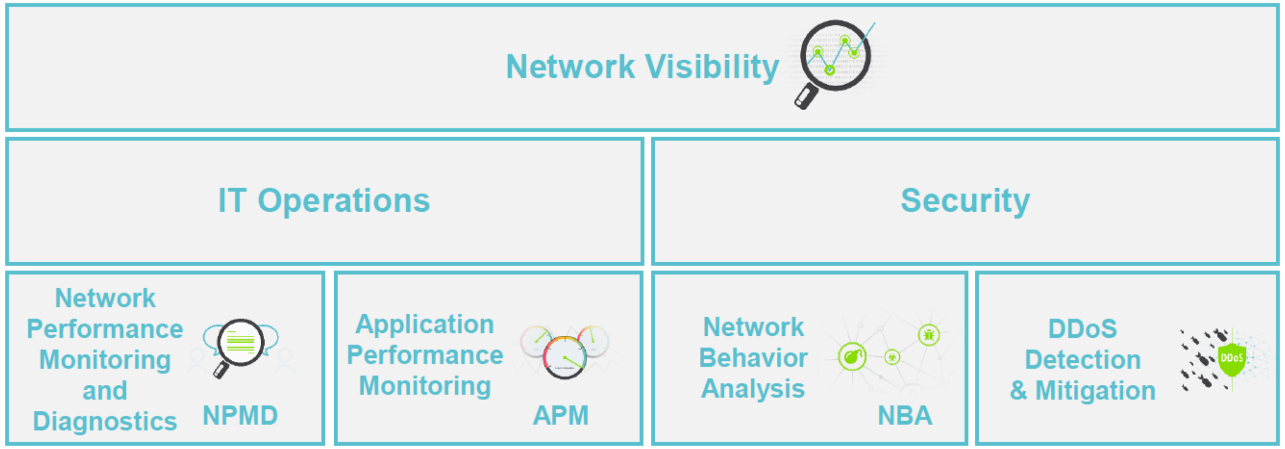
- NetFlow is a feature that was **introduced** on **Cisco routers** around **1996** that provides the ability to collect IP network traffic as it enters or exits an interface.
- NetFlow provides data to enable:
  - network and security monitoring,
    - NPMD Network Performance Monitoring & Diagnostics
    - Network visibility & security
      - Perimeter Security
      - Endpoint Security
  - network planning
  - traffic analysis to include identification of network bottlenecks
  - IP accounting for billing purposes.



Network Visibility & Security

Perimeter Security

Endpoint Security



Network Visibility

IT Operations

Security

Network Performance Monitoring and Diagnostics NPMD

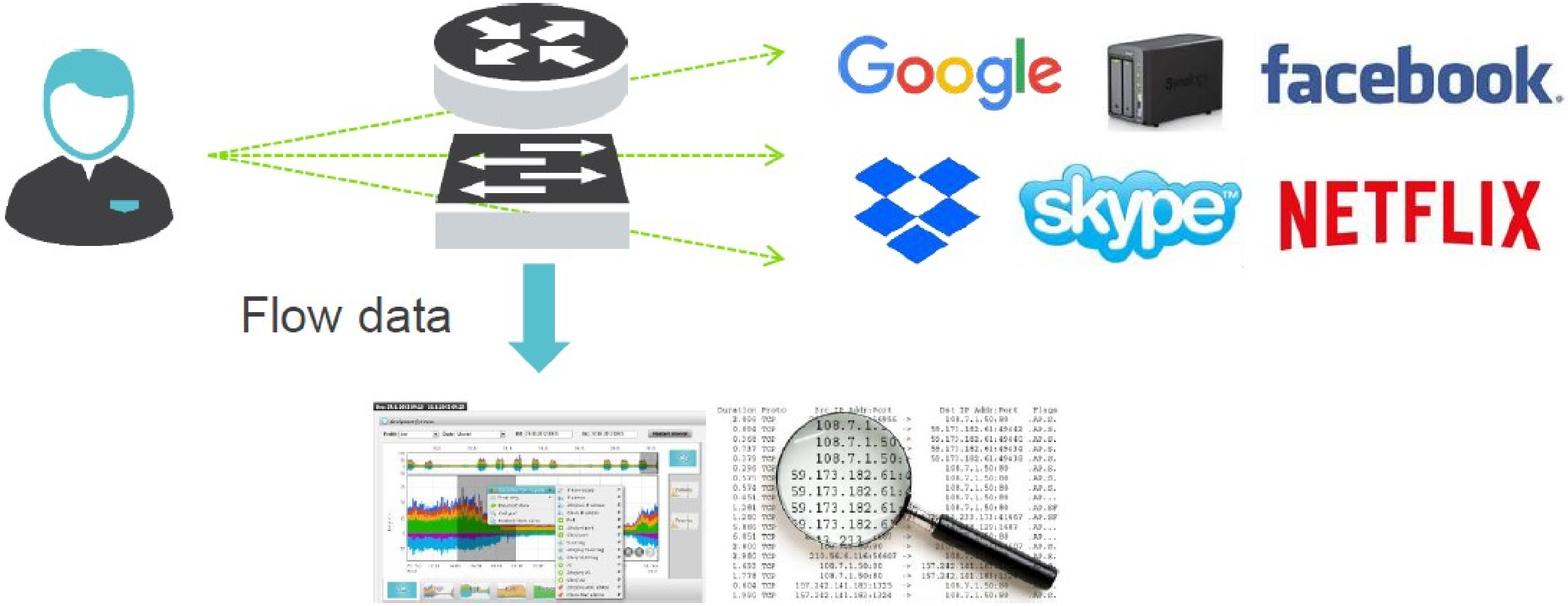
Application Performance Monitoring APM

Network Behavior Analysis NBA

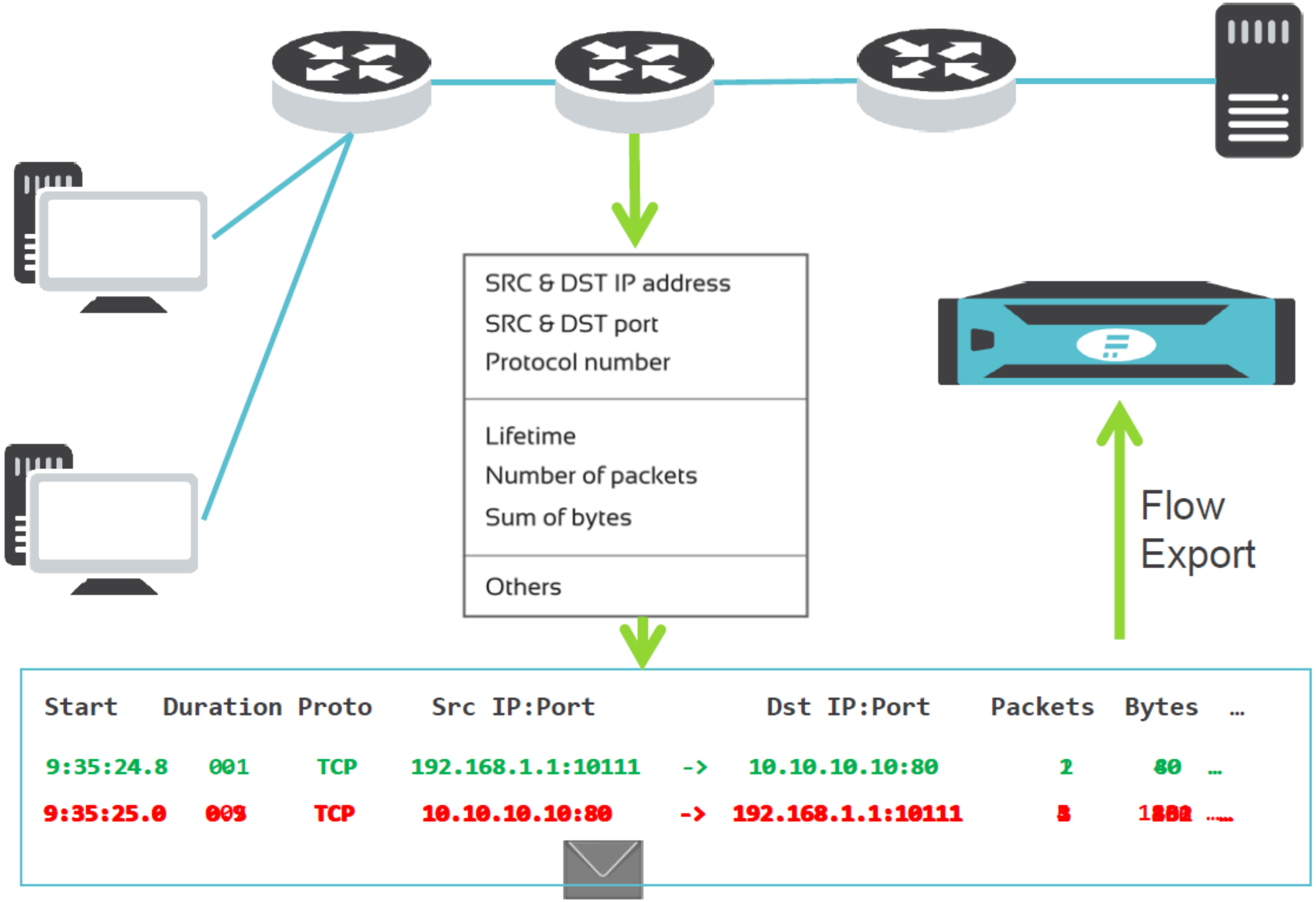
DDoS Detection & Mitigation

What is Flow Data?

- Modern method for network monitoring –flow measurement
- Cisco standard NetFlow v5/v9, IETF standard IPFIX
- Focused on L3/L4 information and volumetric parameters
- Real network traffic to flow statistics reduction ratio 500:1



Flow Monitoring Principle



SRC & DST IP address
SRC & DST port
Protocol number

Lifetime
Number of packets
Sum of bytes

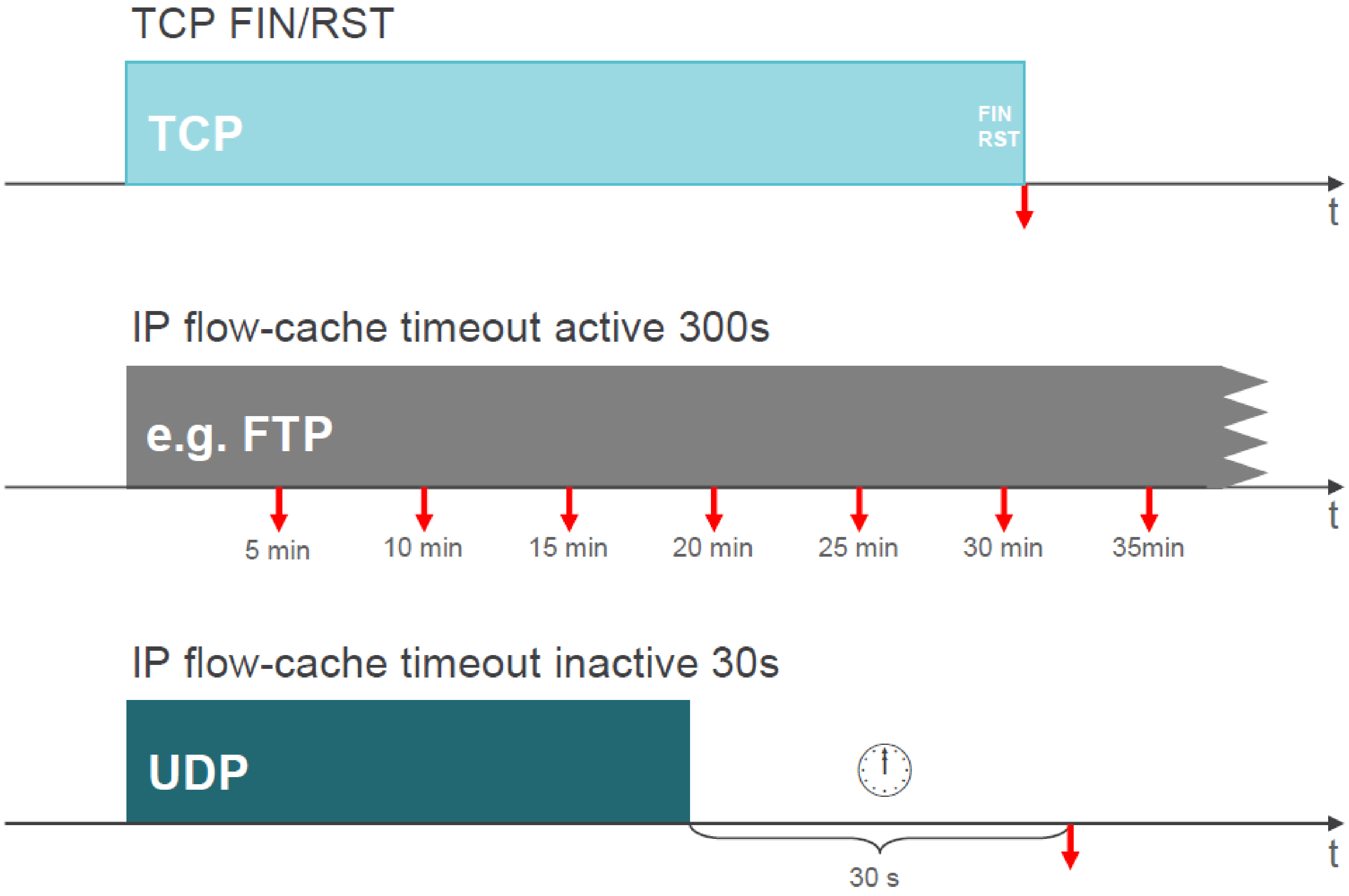
Others

```
Start     Duration  Proto    Src IP:Port                Dst IP:Port          Packets   Bytes   …

9:35:24.8   001      TCP    192.168.1.1:10111   ->   10.10.10.10:80              2        80   …
9:35:25.0   005      TCP     10.10.10.10:80     ->  192.168.1.1:10111            5      1800   ……
```

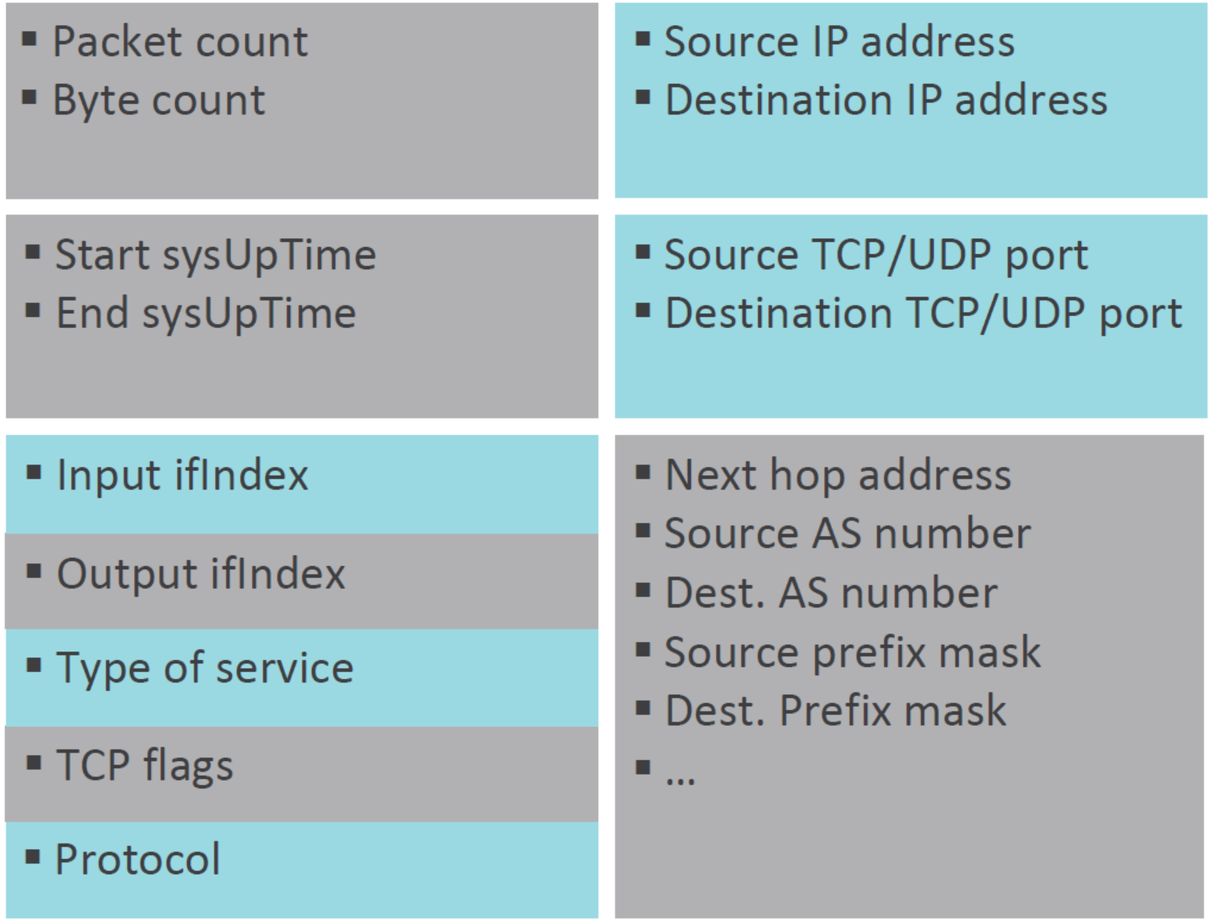
Flow Export Principle

- Flow aging
  - ak smerovač (flow exporter) vidí novú sieťovú prevádzku pre už existujúci/prenášajúci sa flow, tak resetne znova timer
- Flow export
  - TCP
    - FIN/RST
    - alebo aj skôr: flow-cache timeout
  - UDP
    - flow-cache timeout - neakivita



Flow Key vs. Non-Key Fields

Flow Key vs. Non-Key Field



- Packet count
- Byte count

- Source IP address
- Destination IP address

- Start sysUpTime
- End sysUpTime

- Source TCP/UDP port
- Destination TCP/UDP port

- Input ifIndex
- Output ifIndex
- Type of service
- TCP flags
- Protocol

- Next hop address
- Source AS number
- Dest. AS number
- Source prefix mask
- Dest. Prefix mask
- …

Flow Standards

Cisco standard	**NetFlow v5**	fixed format only basic items available no IPv6, MAC, VLANs, …
	NetFlow v9 (Flexible NetFlow)	flexible format using templates mandatory for current needs provides IPv6, VLANs, MAC, …
Independent IETF standard	**IPFIX (“NetFlow v10”)**	the future of flow monitoring more flexibility than NetFlow v9
Huawei	**NetStream**	same as original Cisco standard NetFlow v9
Juniper	**jFlow**	similar to NetFlow v9 issues in timestamps limited usability

Flow Standards

Related standards	**Cisco – NEL, NSEL**	uses NetFlow protocol to export firewall or NAT events and logs, similar format but different interpretation and use-cases
	sFlow	works on packet sampling basis not a real flow data, limited usability impossible to use for security purposes

- **Trends**
  - New monitored items (L7 application information)
    - NBAR2 (L7 application detection), HTTP, …
  - Number of flow-enabled devices is growing
    - Firewalls, UTMs, virtualization, SMB network equipment, …

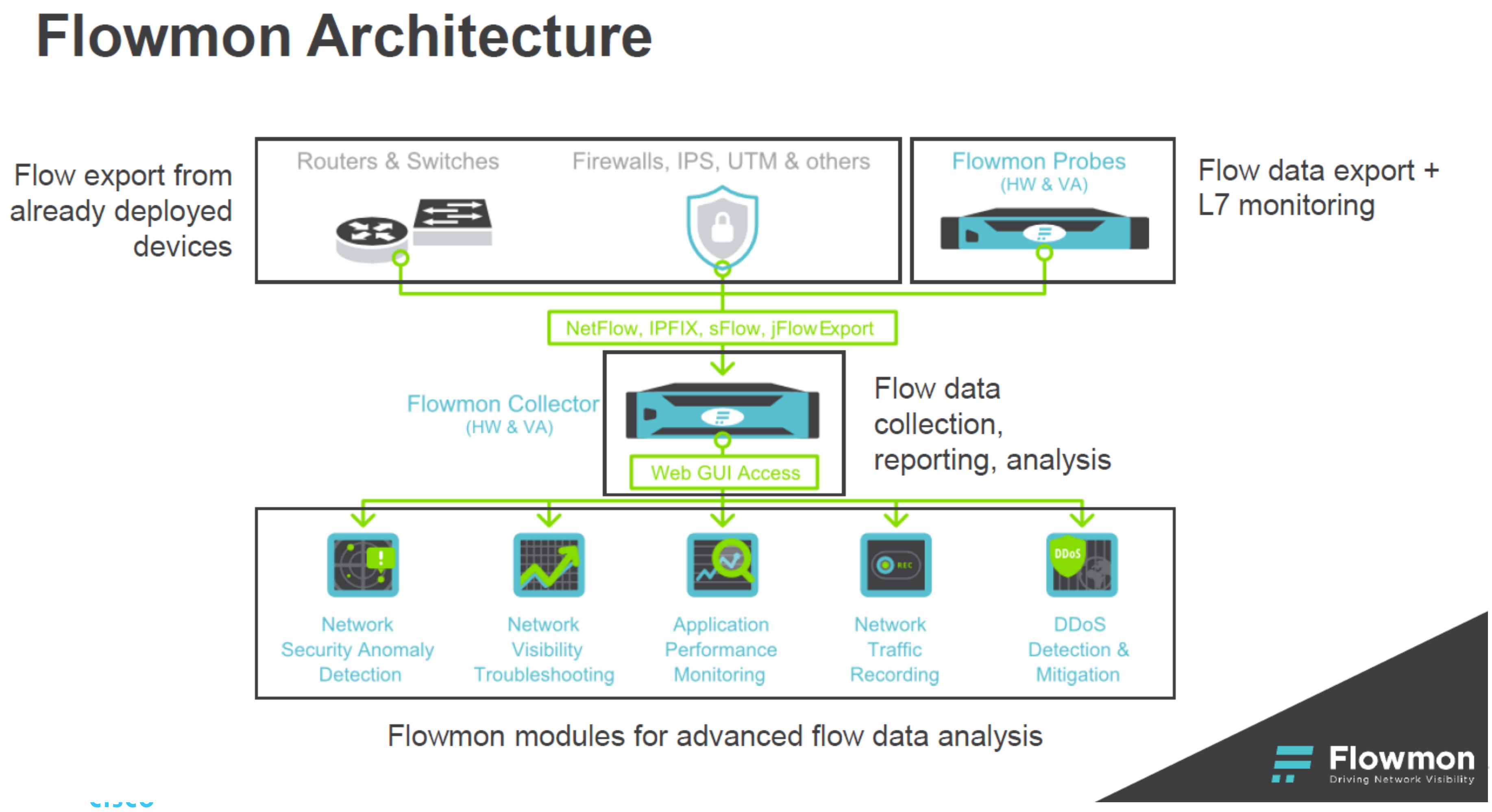
Netflow versions

Version	Comment
v1	First implementation, now obsolete, and restricted to IPv4 (without IP mask and AS Numbers).
v2	Cisco internal version, never released.
v3	Cisco internal version, never released.
v4	Cisco internal version, never released.
v5	Most common version, available (as of 2009) on many routers from different brands, but restricted to IPv4 flows.
v6	No longer supported by Cisco. Encapsulation information (?).
v7	Like version 5 with a source router field. Used (only?) on Cisco Catalyst switches.
v8	Several aggregation form, but only for information that is already present in version 5 records
v9	Template Based, available (as of 2009) on some recent routers. Mostly used to report flows like IPv6, MPLS, or even plain IPv4 with BGP nexthop.
v10	Used for identifying IPFIX. Although IPFIX is heavily based on NetFlow, v10 does not have anything to do with NetFlow.

Netflow support by vendors

Vendor and type	Models	NetFlow Version
Cisco IOS-XR routers	CRS, ASR9000 old 12000	v5, v8, v9
Cisco IOS routers	10000, 7200, old 7500	v5, v8, v9
Cisco Catalyst switches	7600, 6500, 4500	v5, v8, v9
Cisco Nexus switches	5600, 7000, 7700	v5, v9
Juniper legacy routers	M-series, T-series, MX-series with DPC	v5, v8
Juniper legacy routers	M-series, T-series, MX-series with DPC	v5, v8, v9
Juniper routers	MX-series with MPC-3D, FPC5 for T4000	v5, IPFIX
Nokia routers	7750SR	v5, v8, v9, v10 IPFIX
Huawei routers	NE5000E NE40E/X NE80E	v5, v9
Enterasys Switches	S-Serie[9] and N-Serie[10]	v5, v9
Flowmon Probes	Flowmon Probe 1000, 2000, 4000, 6000, 10000, 20000, 40000, 80000, 100000	v5, v9, IPFIX
Nortel Switches	Ethernet Routing Switch 5500 Series (ERS5510, 5520 and 5530) and 8600 (Chassis-based)	v5, v9, IPFIX
PC and Servers	Linux FreeBSD NetBSD OpenBSD	v5, v9, IPFIX
VMware servers	vSphere 5.x[16]	v5, IPFIX (>5.1)[17]
Mikrotik RouterOS	RouterOS 3.x, 4.x, 5.x, 6.x [18]	v1, v5, v9, IPFIX (>6.36RC3)

Ukážka jedného nástroja založeného na NetFlow dátach



Flowmon Architecture

Flow export from already deployed devices

Routers & Switches

Firewalls, IPS, UTM & others

Flowmon Probes (HW & VA)

Flow data export + L7 monitoring

NetFlow, IPFIX, sFlow, jFlow Export

Flowmon Collector (HW & VA)

Web GUI Access

Flow data collection, reporting, analysis

Network Security Anomaly Detection

Network Visibility Troubleshooting

Application Performance Monitoring

Network Traffic Recording

DDoS Detection & Mitigation

Flowmon modules for advanced flow data analysis

Success story

- Skupina vedcov združenia CESNET v ČR 2002 - začala aktivity v oblasti programovateľného hardvéru s názvom Liberouter project.
- Počas účasti na vývojovom projekte pre GEANT2 (európska akademická sieť), tím Liberouter vyvinul prototyp sieťovej monitorovacej sondy s názvom FlowMon.
- V 2012 – umiestnili sa v Gartner Magic Quadrant v NPMD.
- 2020 - Spoločnosť Flowmon Networks získala spoločnosť Kemp Technologies

SIEM and SOAR

SIEM

- Security Information Event Management (SIEM) is a technology used in enterprise organizations to provide **real time reporting** and **long-term analysis** of security events.
- SIEM systems include the following essential functions:
  - **Forensic analysis** – The ability to search logs and event records from sources and provide complete information for forensic analysis.
  - **Correlation** – Examines logs and events from different systems or applications, speeding detection of and reaction to security threats.
  - **Aggregation** - Reduces the volume of event data by **consolidating duplicate event records**.
  - **Reporting** - Presents the correlated and aggregated event data in real-time monitoring and long-term summaries.

SIEM and SOAR (Contd.)

- SIEM provides details on the source of suspicious activity:
  - User information such as username, authentication status, location.
  - Device information such as manufacturer, model, OS version, MAC address, network connection method, and location.
  - Posture information such as compliance of the device with the security policy and updated antivirus files and OS patches.

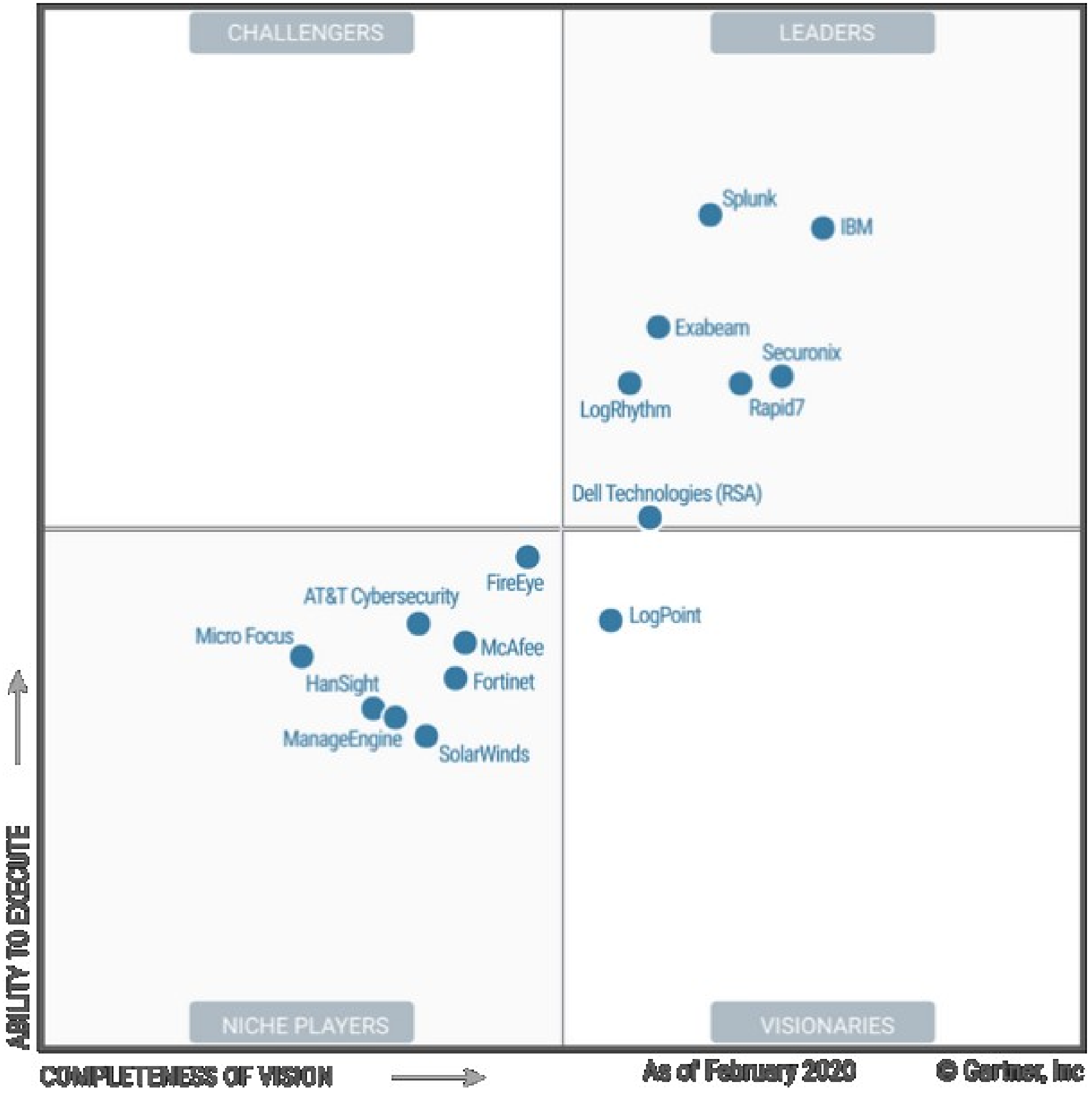
SOAR

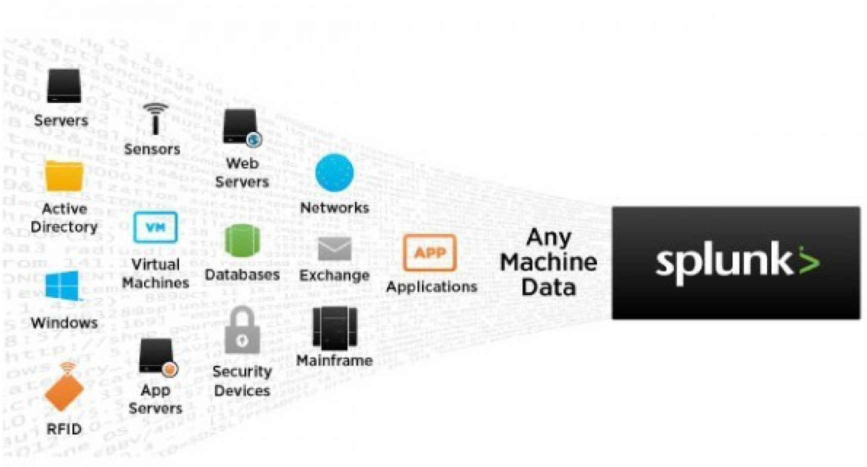
- Security Orchestration, Automation, and Response (SOAR) enhances SIEM.
- SOAR helps security teams investigate security incidents and add enhanced data gathering and a number of functionalities that aid in security incident response.

SIEM and SOAR (Contd.)

- SOAR solutions:
  - Provides case management tools that allow cybersecurity personnel to research and investigate incidents, frequently by integrating threat intelligence into the network security platform.
  - Use artificial intelligence to detect incidents that aid in incident analysis and response.
  - Automate complex incident response procedures and investigations, which are potentially labor intensive tasks performed by Security Operations Center (SOC) staff by executing run books.
  - Offers dashboards and reports to document incident response to improve SOC key performance indicators and can enhance network security for organizations.
- SOAR helps analysts respond to the threat.

SIEM magic quadrant





QRadar

SIEM Systems

- An open source product called Security Onion includes the ELK suite for SIEM functionality.
- ELK is an acronym for three products from Elastic:
  - **Elasticsearch** - Document oriented full text search engine.
  - **Logstash** - Pipeline processing system that connects ‘inputs’ to ‘outputs’ with optional ‘filters’ in between.
  - **Kibana** - Browser based analytics and search dashboard for Elasticsearch.
- **Note**: SolarWinds Security Event Manager and Splunk Enterprise Security are two popular proprietary SIEM systems used by SOCs.

Elastic Stack

- Elastic je názov spoločnosti, ktorá stojí za produktom Elastic Stack - obsahuje nástroje:
  - Elasticsearch
  - Kibana
  - Logstash
- Pomáhajú používateľom zabezpečene spracovávať dáta
  - z ľubovoľného zdroja
  - v ľubovoľnom formáte

  následne v nich
  - vyhľadávať
  - analyzovať
  - zobrazovať v reálnom čase
- „free and open" s možnosťou kúpy platených licencií zahrňujúcich doplnkové funkcionality
  - strojové učenie
  - zabezpečenie a reportovanie
- Umožňuje nasadenie v cloude alebo on-premise

Elasticsearch

- bezplatný distribuovaný vyhľadávací a analytický nástroj
- pre všetky typy údajov vrátane
  - Textových
  - Číselných
  - Geopriestorových
  - Štruktúrovaných
  - aj neštruktúrovaných
- ES je postavený na Apache Lucene
- * 2010
- Je známy pre svoje
  - jednoduché REST API
  - distribuovanú povahu
  - Rýchlosť
  - škálovateľnosť

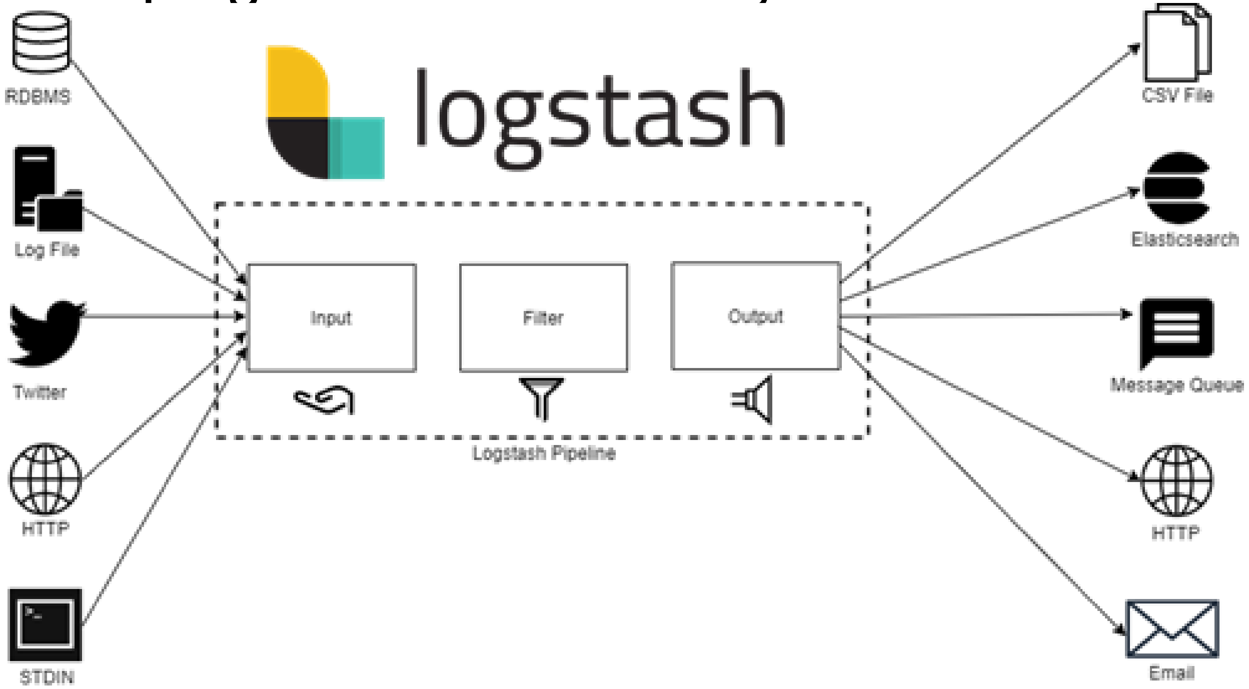
Elasticsearch (cont.)

- Prijíma dáta z rôznych zdrojov vrátane
  - Logov
  - systémových metrík
  - webových aplikácií
- Originálne (raw) prijímané dáta sa
  - Parsujú, normalizujú a rozširujú pred tým
  - ako sú indexované v databáze
  - Až následne sa dá spustiť komplexné dopyty (queries) nad týmito dátami a pomocou agregácií načítať komplexné súhrny dát.
- Index je zbierka dokumentov, ktoré navzájom súvisia
- ES ukladá dáta ako JSON dokumenty
- Každý dokument koreluje množinu kľúčov (názvy polí alebo vlastností) s ich zodpovedajúcimi hodnotami (reťazce, čísla, boolovské hodnoty, dátumy, polia hodnôt, geolokačné údaje alebo iné typy údajov)

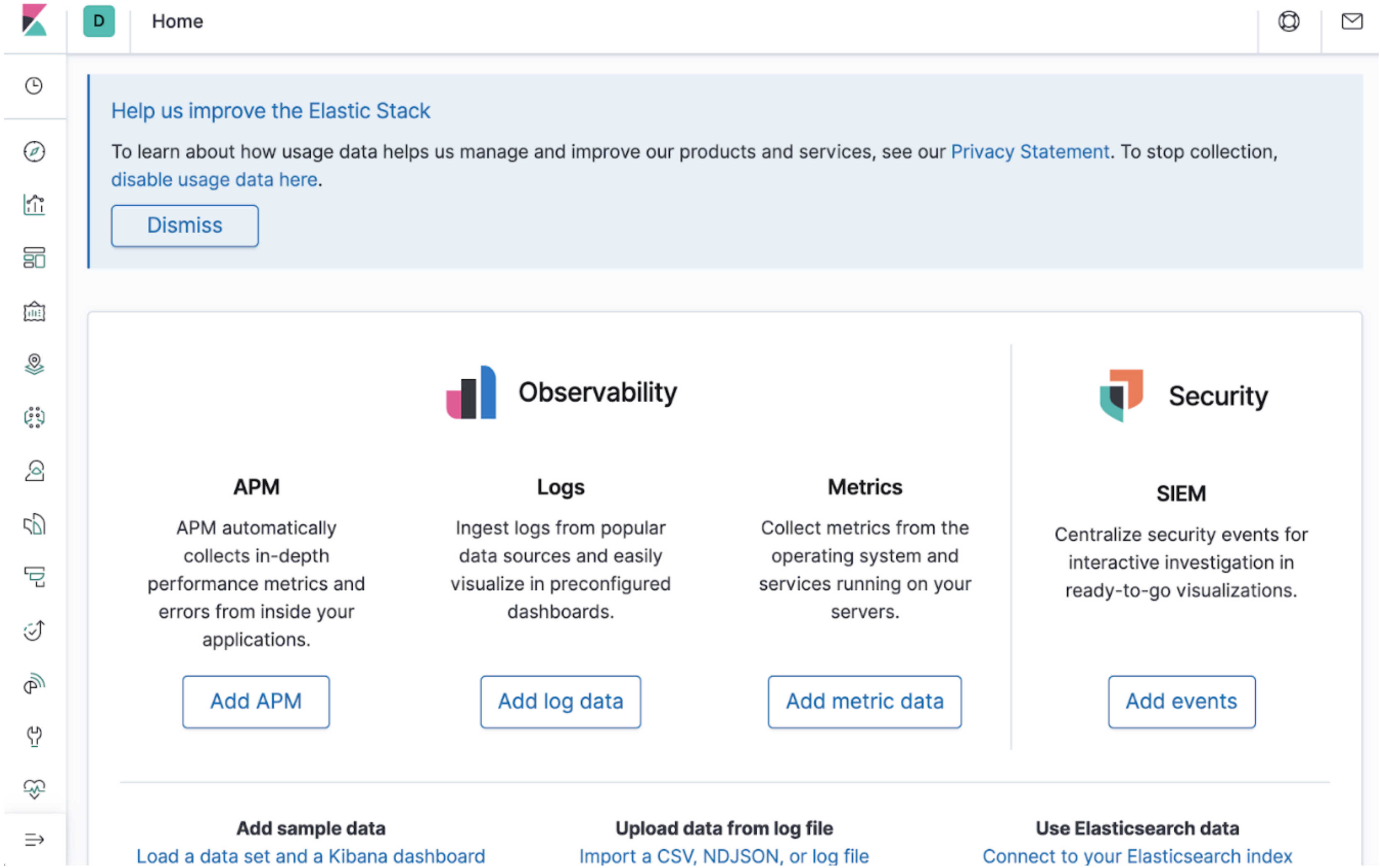
- ES používa dátovú štruktúru nazývanú inverzný index (inverted index), ktorá je navrhnutá tak, aby umožňovala veľmi rýchle fulltextové vyhľadávanie
  - Inverzný index obsahuje zoznam všetkých jedinečných slov, ktoré sa vyskytujú v ľubovoľných dokumentoch
  - a identifikuje všetky dokumenty, v ktorých sa každé slovo vyskytuje
  - počas procesu indexovania ES ukladá dokumenty a vytvára inverzný index, vďaka ktorému je možné v dokumentoch vyhľadávať takmer v reálnom čase
  - indexovanie sa iniciuje pomocou indexovacieho API rozhrania, prostredníctvom ktorého je možné pridať alebo aktualizovať JSON dokument v konkrétnom indexe
- Index Lifecycle Management (ILM)
  - Cez neho je možné nakonfigurovať politiky pre automatické manažovanie indexov podľa požiadaviek na výkon a veľkosť úložiska

Logstash

- Dokáže dynamicky zbierať údaje z rôznych zdrojov a normalizovať ich do cieľov podľa výberu používateľa
- Pôvodne podporoval hlavne zber logov, v súčasnosti dokáže akýkoľvek typ udalosti rozšíriť
- 200 pluginov a možnosť vytvoriť si vlastné



Webové rozhranie Kibany



Help us improve the Elastic Stack

To learn about how usage data helps us manage and improve our products and services, see our Privacy Statement. To stop collection, disable usage data here.

Observability

Security

APM

APM automatically collects in-depth performance metrics and errors from inside your applications.

Logs

Ingest logs from popular data sources and easily visualize in preconfigured dashboards.

Metrics

Collect metrics from the operating system and services running on your servers.

SIEM

Centralize security events for interactive investigation in ready-to-go visualizations.

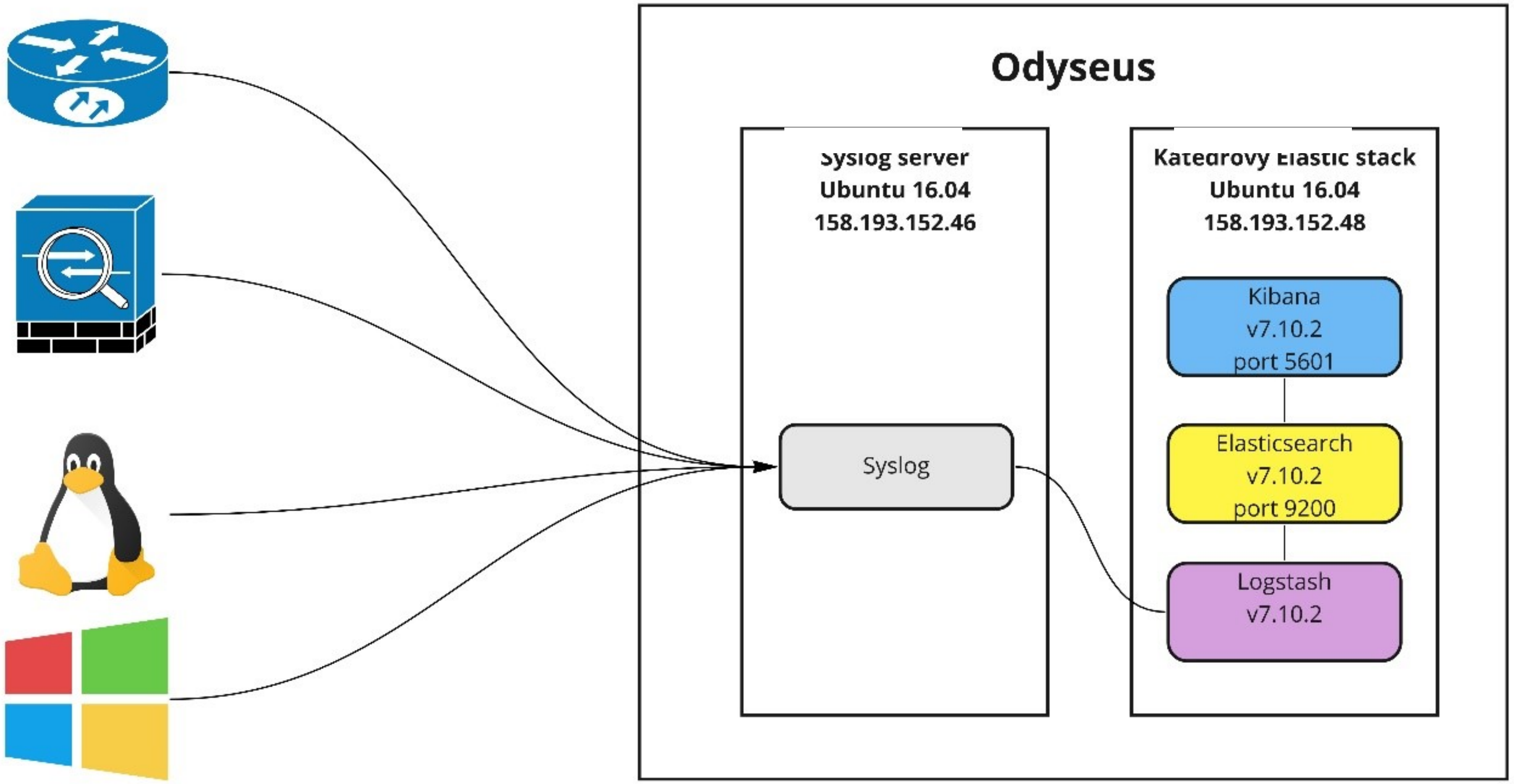
Add sample data
Load a data set and a Kibana dashboard

Upload data from log file
Import a CSV, NDJSON, or log file

Use Elasticsearch data
Connect to your Elasticsearch index

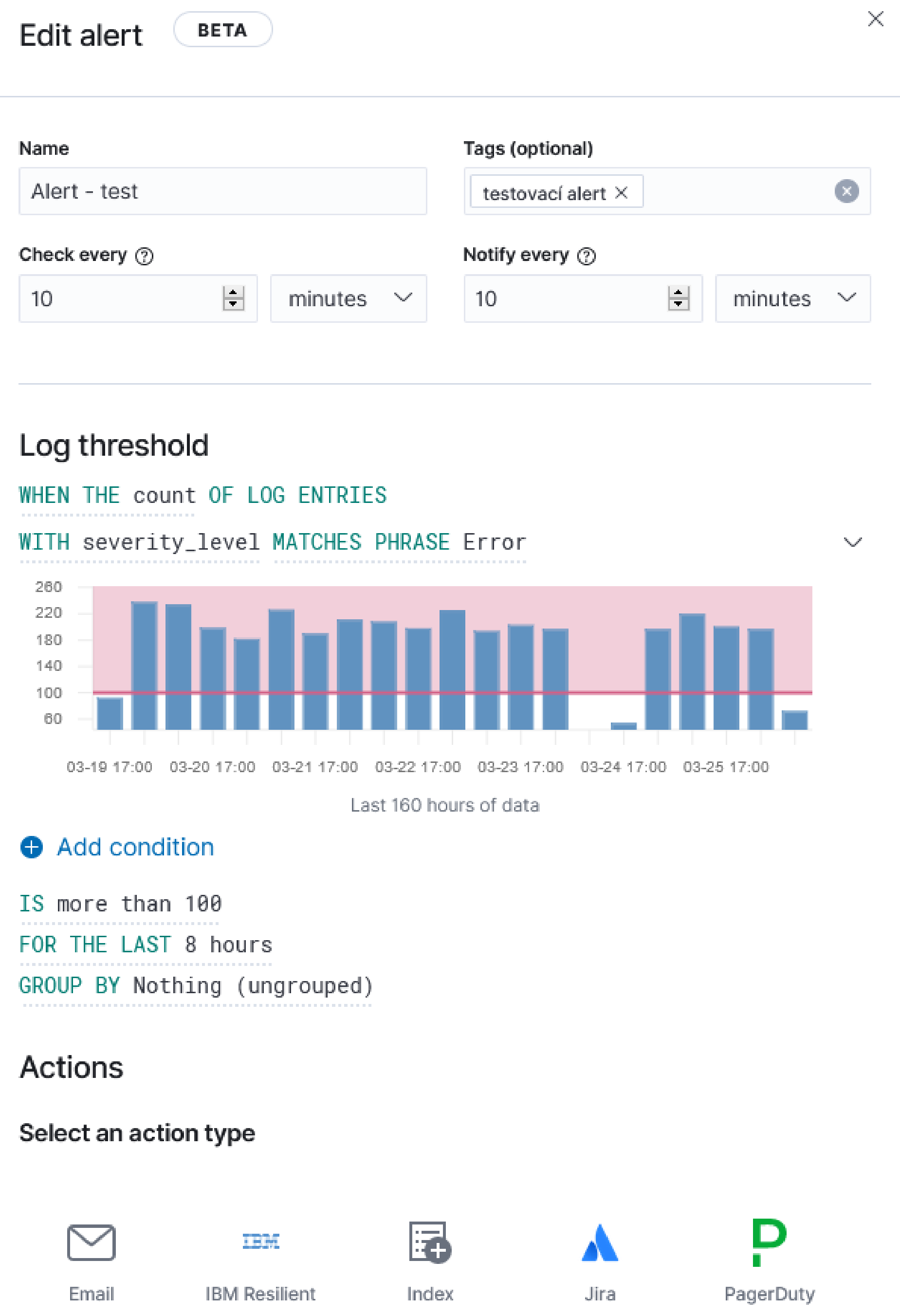
Katedrový elastic stack

- syslog server - prijíma syslog logy z rôznych zdrojov a ukladá ich do vytvorenej štruktúry priečinkov
- Elastic Stack server
  - obsahuje
  - Kibana
  - Elasticsearch
  - Logstash
    - číta uložené logy, parsuje a ukladá ich do ES databá



Kibana - tvoba alertov a reportov

- **Alerts/Create alert**
  - Name
    - názov alertu
  - Tags
    - voliteľné
  - Check every
    - ako často sa vyhodnocuje podmienka
  - Notify every
    - ako často sa generujú alerty pri pretrvávaní splnenia podmienky
  - Log threshold
    - query, v ktorej sa definuje podmienka
    - zobrazuje aj interaktívny graf
  - Actions
    - aká akcia sa v prípade splnenia podmienky vykoná



Edit alert BETA

Name: Alert - test

Tags (optional): testovací alert

Check every: 10 minutes

Notify every: 10 minutes

Log threshold

```
WHEN THE count OF LOG ENTRIES
WITH severity_level MATCHES PHRASE Error
```

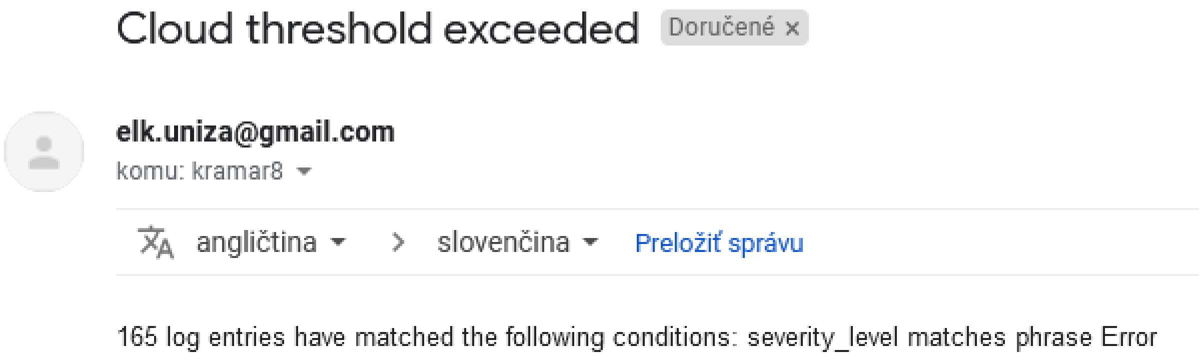
Last 160 hours of data

```
IS more than 100
FOR THE LAST 8 hours
GROUP BY Nothing (ungrouped)
```

Actions

Select an action type

Kibana – vygenerovaný alert



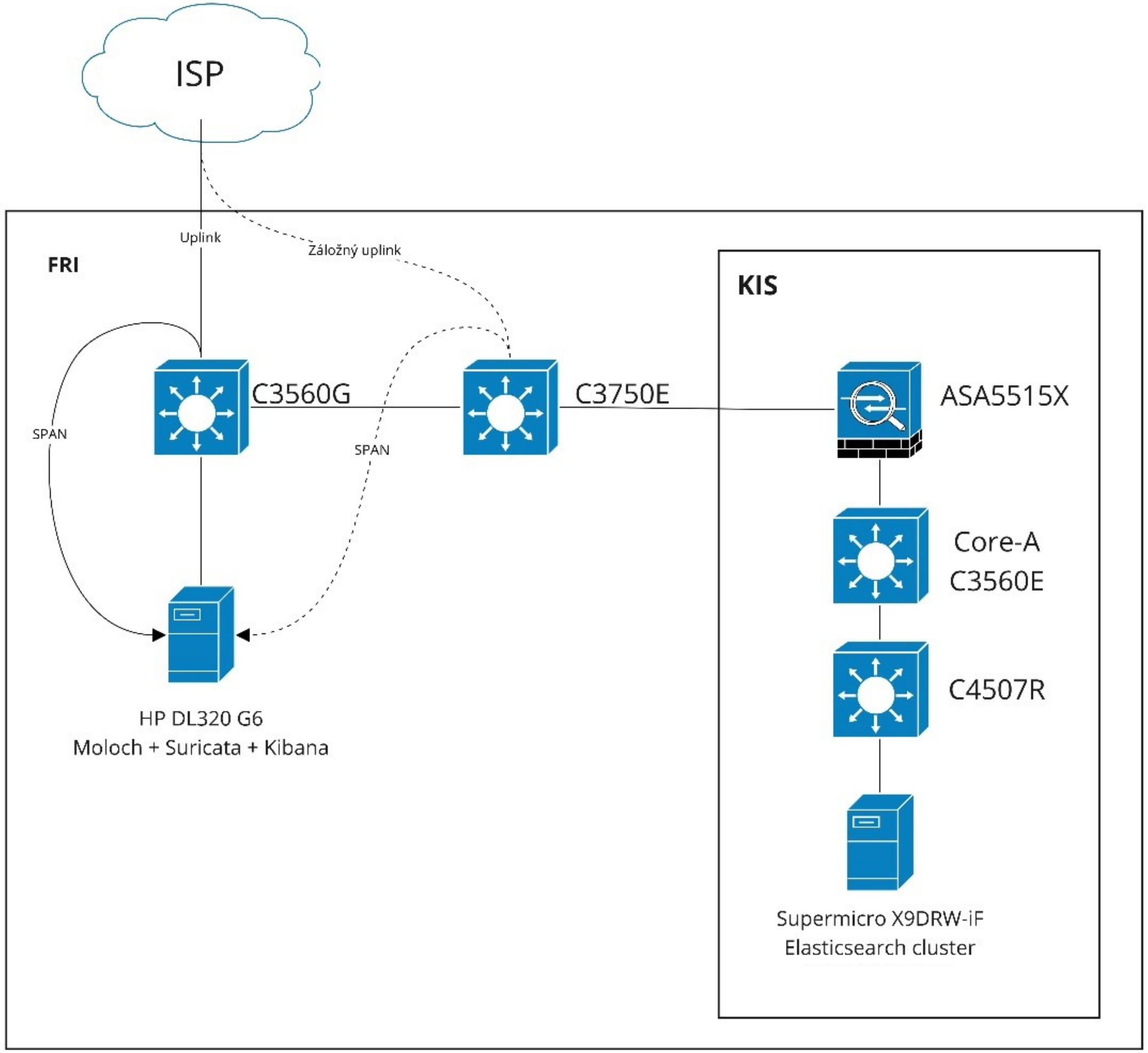
Cloud threshold exceeded

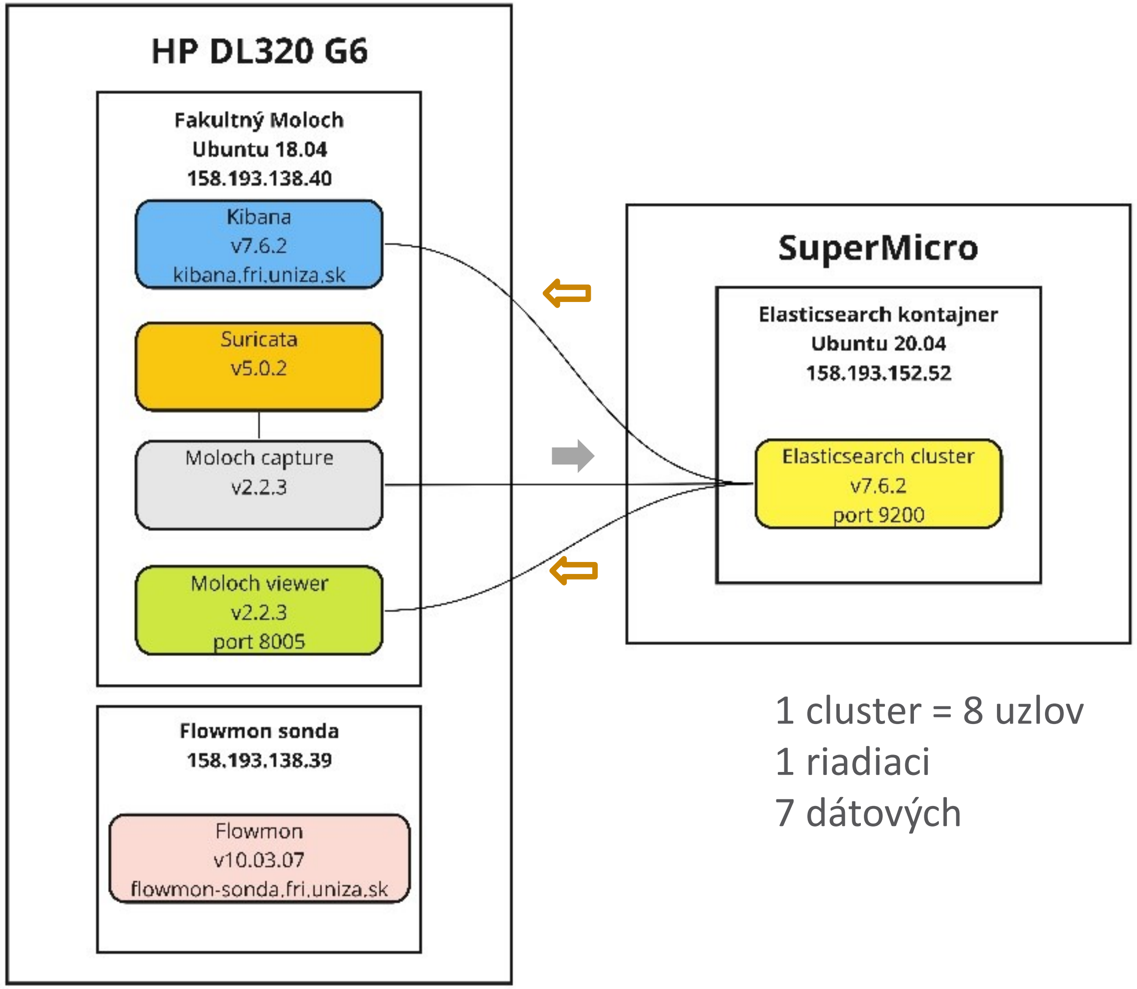
elk.uniza@gmail.com

komu: kramar8

165 log entries have matched the following conditions: severity_level matches phrase Error

Nedávne nasadenie na FRI a KIS

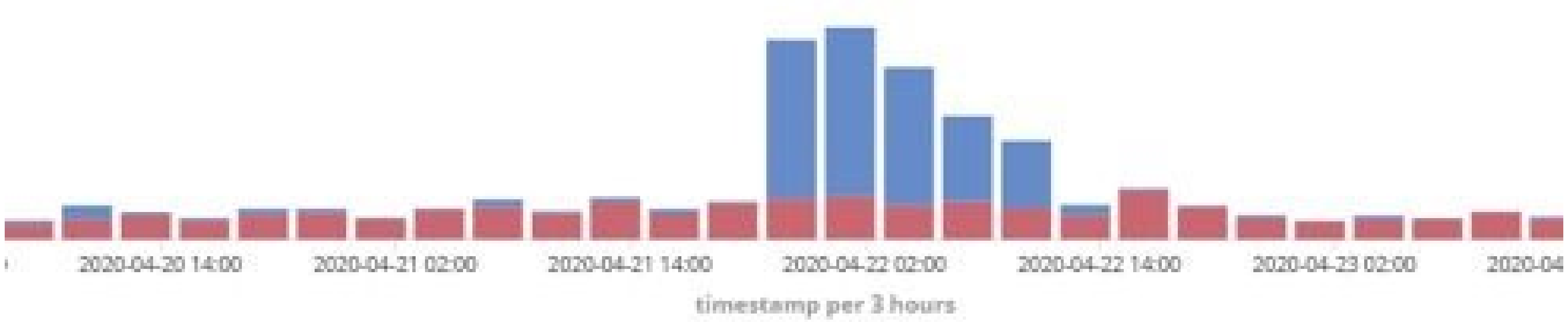




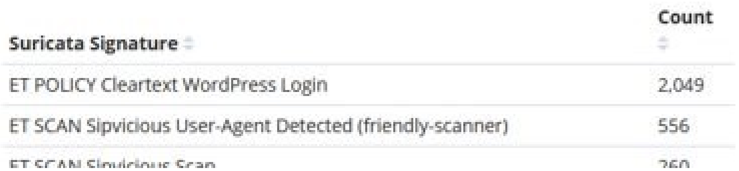
1 cluster = 8 uzlov
1 riadiaci
7 dátových

Analýza incidentov v Kibane – Wordpress útok

- pokus o prihlásenie sa hrubou silou do WordPress aplikácie na serveri
- Počet upozornení v čase

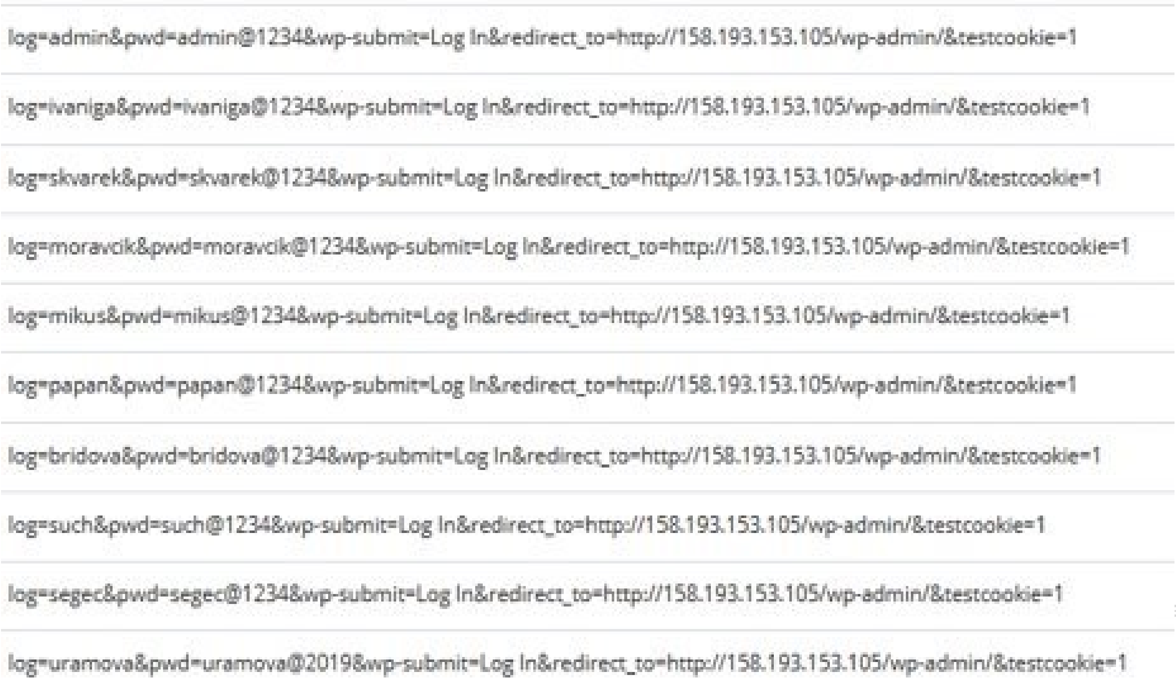


- Počty Suricata upozornení



Suricata Signature	Count
ET POLICY Cleartext WordPress Login	2,049
ET SCAN Sipvicious User-Agent Detected (friendly-scanner)	556
ET SCAN Sipvicious Scan	260

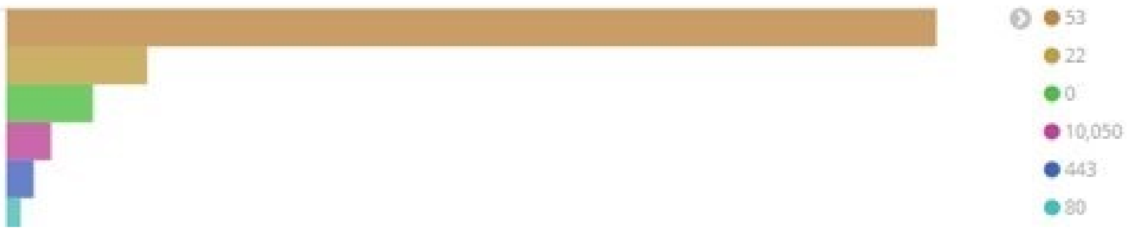
- v Kibane sme si vedeli zobraziť aj detail HTTP requestov



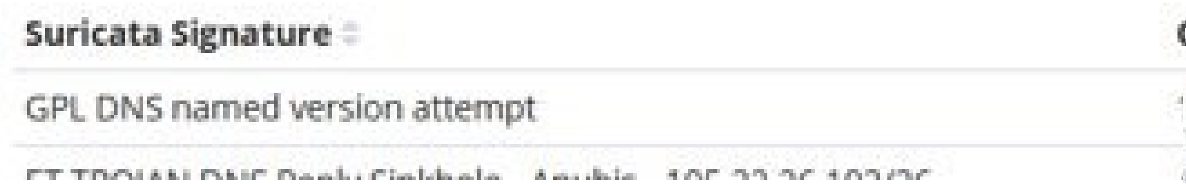
```
log=admin&pwd=admin@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=ivaniga&pwd=ivaniga@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=skvarek&pwd=skvarek@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=moravcik&pwd=moravcik@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=mikus&pwd=mikus@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=papan&pwd=papan@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=bridova&pwd=bridova@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=such&pwd=such@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=segec&pwd=segec@1234&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
log=uramova&pwd=uramova@2019&wp-submit=Log In&redirect_to=http://158.193.153.105/wp-admin/&testcookie=1
```

Analýza incidentov v Kibane – DNS útok

- DNS útok na cieľovú IP adresu v rozsahu katedrového OpenStack cloudu
- vo výraznej miere prevyšovala prevádzka na DNS port 53
  - Počas časového okna približne 14 hodín sa rapídne zvýšila prevádzka

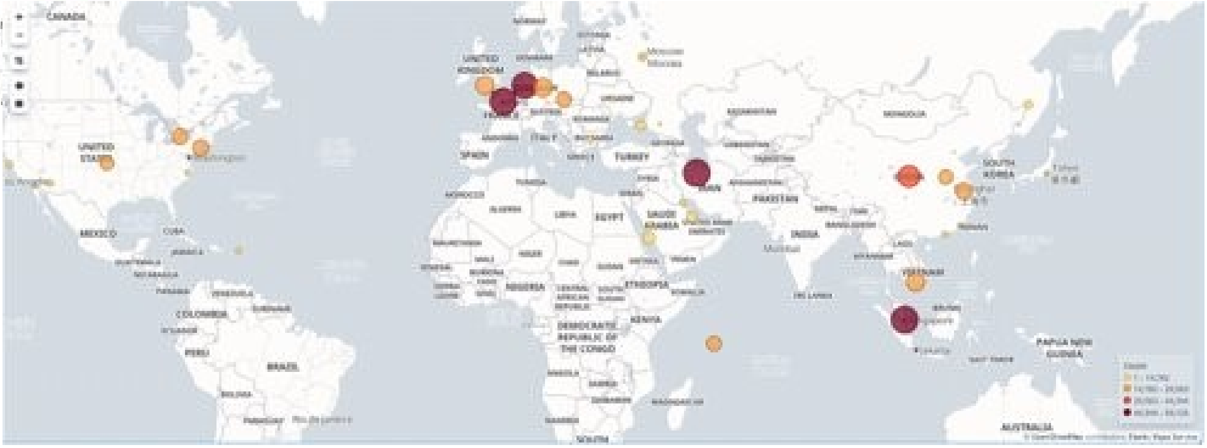


- vygenerované Suricata upozornenia



Suricata Signature	Count
GPL DNS named version attempt	
ET TROJAN DNS Reply Sinkhole - Anubis - 195.22.26.192/26	

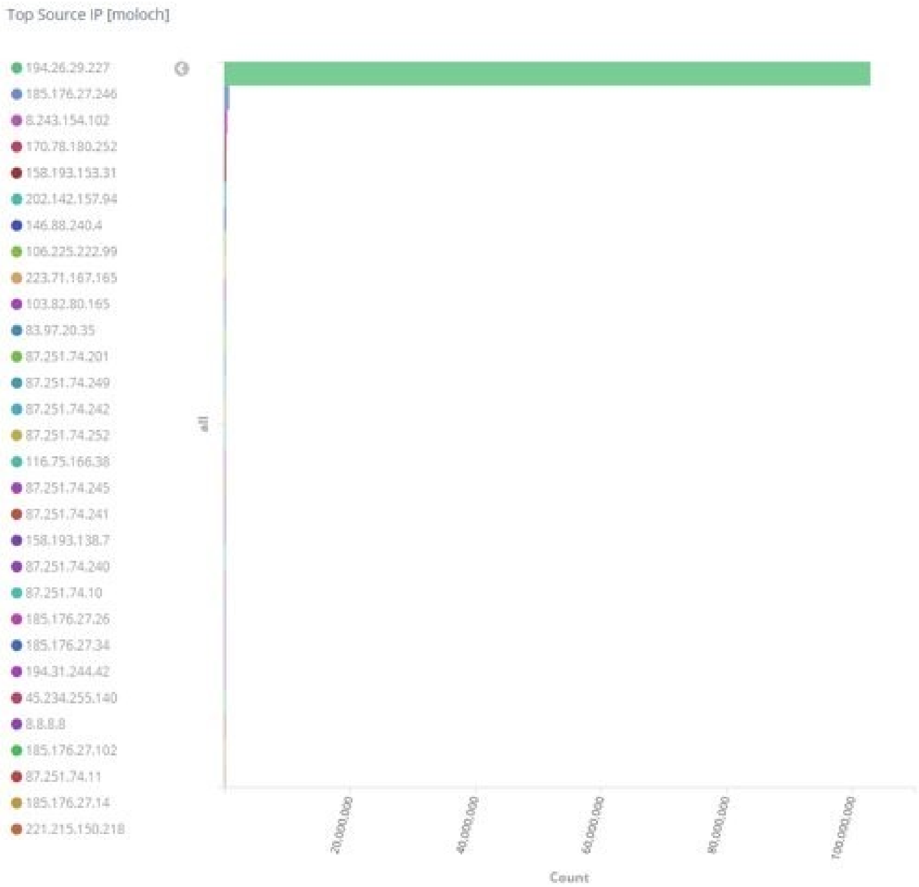
- DNS útok – zdrojové IP adresy na mape

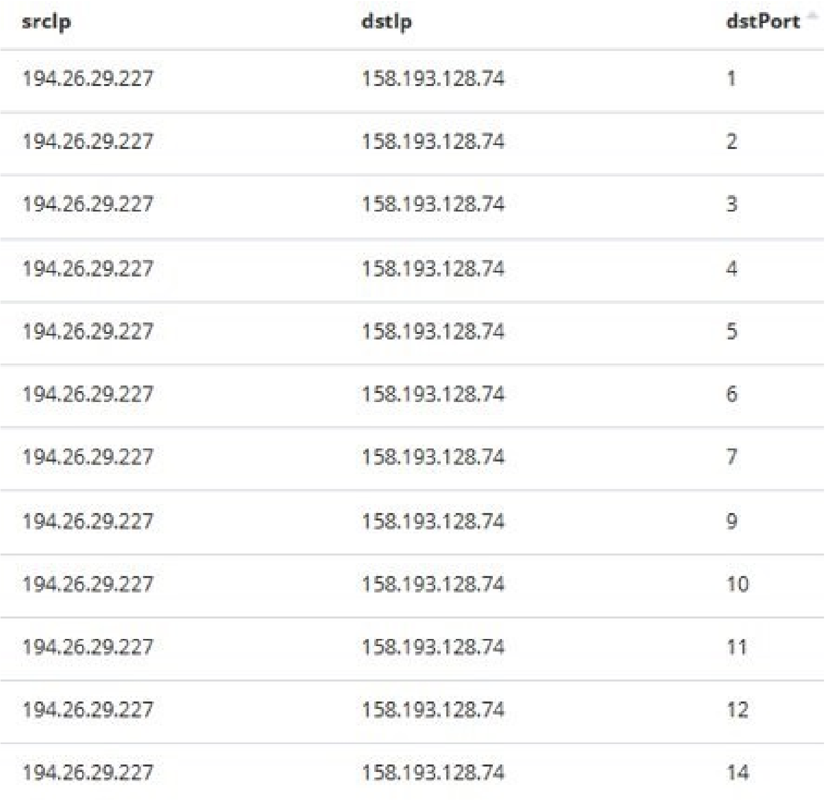


Analýza incidentov v Kibane – DNS útok

- Podľa cieľových portov ani podľa cieľových IP sme nič podozrivé nezistili

- Až pri analýze zdrojových IP sme zistili, že išlo o toky pochádzajúce z jedného zdroja na všetky IP z fakultného rozsahu, na porty od 1 po 65000. Suricata pri tejto podozrivej prevádzke nevygenerovala žiadne signatúry.





srcIp	dstIp	dstPort
194.26.29.227	158.193.128.74	1
194.26.29.227	158.193.128.74	2
194.26.29.227	158.193.128.74	3
194.26.29.227	158.193.128.74	4
194.26.29.227	158.193.128.74	5
194.26.29.227	158.193.128.74	6
194.26.29.227	158.193.128.74	7
194.26.29.227	158.193.128.74	9
194.26.29.227	158.193.128.74	10
194.26.29.227	158.193.128.74	11
194.26.29.227	158.193.128.74	12
194.26.29.227	158.193.128.74	14

15.3 Network Monitoring and Tools Summary

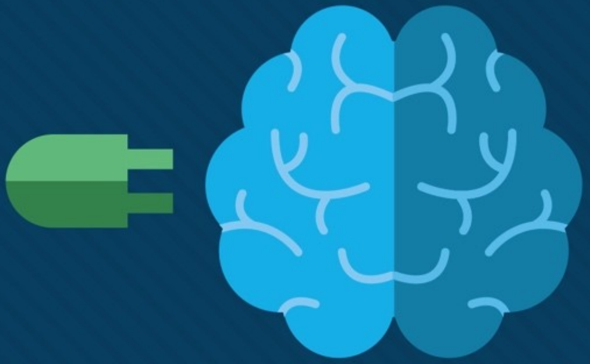
What Did I Learn in this Module?

- To mitigate threats, all networks should be secured and protected using a defense-in-depth approach.
- This requires a security infrastructure that consists of firewalls, IDS, IPS, and endpoint security software.
- A cybersecurity analyst needs to review all alerts that are generated by network devices and validate them.
- Tools such as IDS, packet analyzers, SNMP, NetFlow, and others are used to determine normal network behavior.
- Two common methods that are used to capture traffic and send it to network monitoring devices are network taps and traffic mirroring using Switch Port Analyzer (SPAN) or other port mirroring.

Network Monitoring and Tools Summary

What Did I Learn in this Module? (Contd.)

- Common tools that are used for network security monitoring include network protocol analyzers (Wireshark and Tcpdump), NetFlow, and SIEM.
- Network protocol analyzers are programs that are used to capture traffic.
- Netflow is a Cisco IOS feature that provides 24x7 statistics on packets that flow through a Cisco router or multilayer switch. It can be used for network and security monitoring, network planning, and traffic analysis.
- SIEM is a technology that is used to provide real time reporting and long-term analysis of security events.



Module 16: Attacking the Foundation

Instructor Materials

CyberOps Associate v1.0

Module 16:
Attacking the Foundation

Module Objective: Explain how TCP/IP vulnerabilities enable network attacks

IP PDU Details	Explain the IPv4 and IPv6 header structure.
IP Vulnerabilities	Explain how IP vulnerabilities enable network attacks.
TCP and UDP Vulnerabilities	Explain how TCP and UDP vulnerabilities enable network attacks.
IP PDU Details	Explain the IPv4 and IPv6 header structure.

16.1 IP PDU Details

Attacking the Foundation

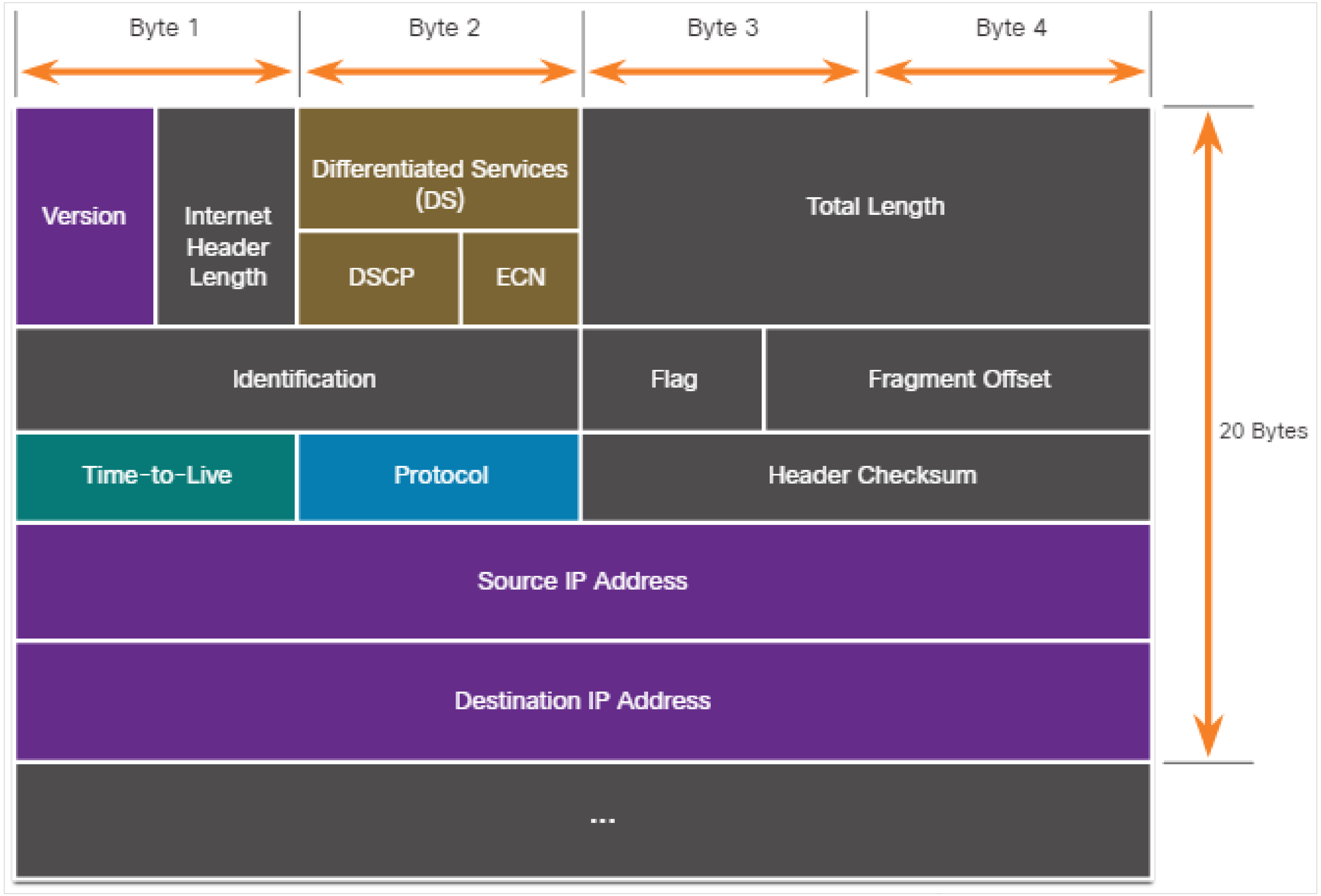
IPv4 and IPv6

- IP was designed as a Layer 3 connectionless protocol. It provides the necessary functions to deliver a packet from a source host to a destination host over an interconnected system of networks.
- IP makes no effort to validate whether the source IP address contained in a packet actually came from that source. For this reason, threat actors can send packets using a spoofed source IP address.
- Also, threat actors can tamper with the other fields in the IP header to carry out their attacks. So, it is important for security analysts to understand the different fields in both the IPv4 and IPv6 headers.

Attacking the Foundation

The IPv4 Packet Header

The fields in the IPv4 packet header are shown in the figure. There are 10 fields in the IPv4 packet header.



Attacking the Foundation

The IPv4 Packet Header (Contd.)

The following table describes the IPv4 header fields:

IPv4 Header Field	Description
Version	• Contains a 4-bit binary value set to 0100 that identifies this as an IPv4 packet.
Internet Header length	• A 4-bit field containing the length of the IP header. • The minimum length of an IP header is 20 bytes.
Differentiated Services or DiffServ (DS)	• Formerly called the Type of Service (ToS) field, the DS field is an 8-bit field used to determine the priority of each packet. • The six most significant bits of the DiffServ field are the Differentiated Services Code Point (DSCP). • The last two bits are the Explicit Congestion Notification (ECN) bits.
Total length	• Specifies the length of the IP packet including the IP header and the user data. • The total length field is 2 bytes, so the maximum size of an IP packet is 65,535 bytes.

Attacking the Foundation

The IPv4 Packet Header (Contd.)

IPv4 Header Field	Description
Identification, Flag, and Fragment offset	• As an IP packet moves, it might need to cross a route that cannot handle the size of the packet. The packet will be divided, or fragmented, into smaller packets and reassembled later. • These fields are used to fragment and reassemble packets.
Time-to-Live (TTL)	• Contains an 8-bit binary value that is used to limit the lifetime of a packet. • The packet sender sets the initial TTL value, and it is decreased by one each time the packet is processed by a router. • If the TTL field decrements to zero, the router discards the packet and sends an Internet Control Message Protocol (ICMP) Time Exceeded message to the source IP address.
Protocol	• Field is used to identify the next level protocol. • This 8-bit binary value indicates the data payload type that the packet is carrying, which enables the network layer to pass the data to the appropriate upper-layer protocol. • Common values include ICMP (1), TCP (6), and UDP (17).

Attacking the Foundation

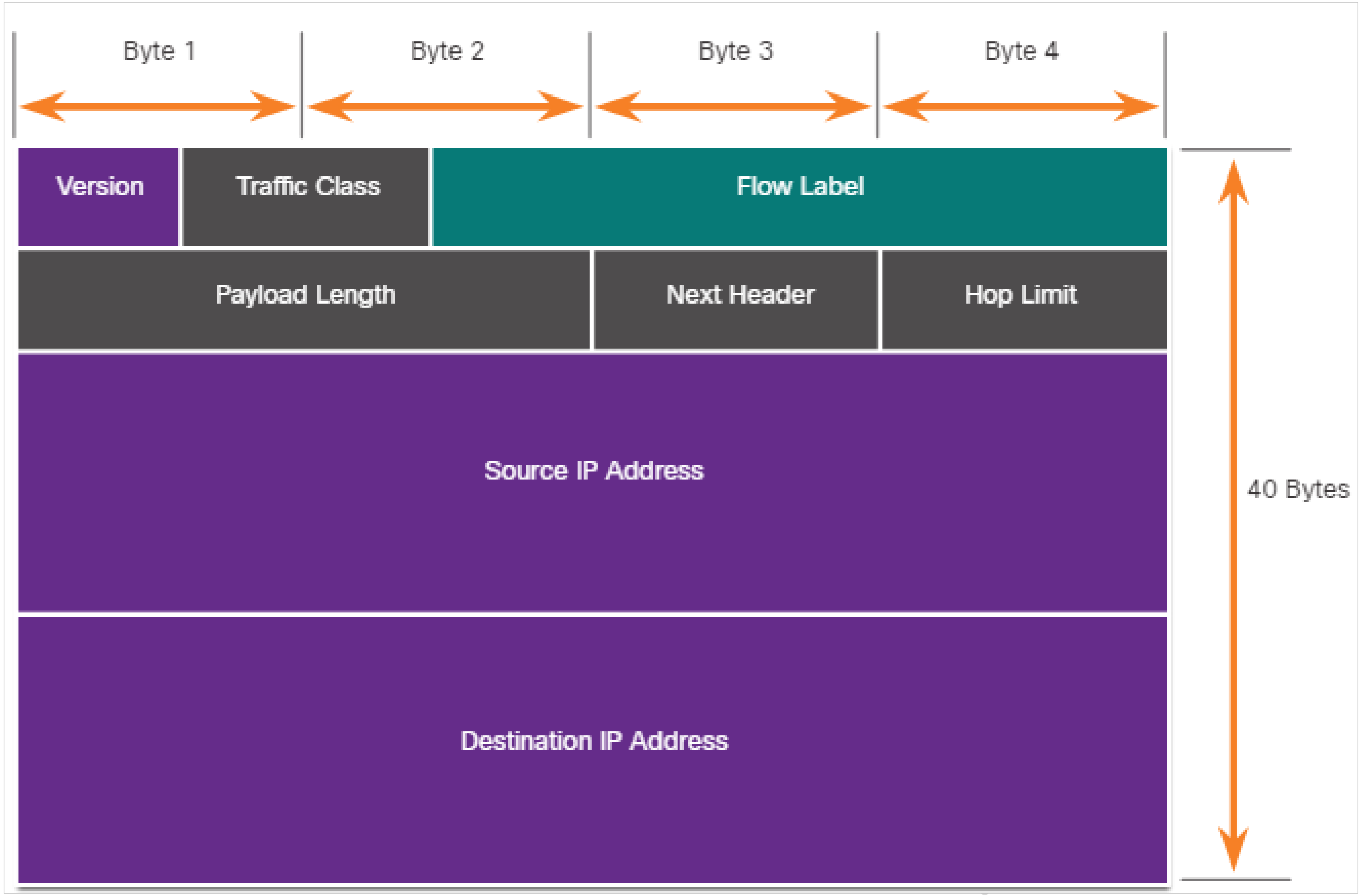
The IPv4 Packet Header (Contd.)

IPv4 Header Field	Description
Header checksum	• A value that is calculated based on the contents of the IP header. • Used to determine if any errors have been introduced during transmission.
Source IPv4 Address	• Contains a 32-bit binary value that represents the source IPv4 address of the packet. • The source IPv4 address is always a unicast address.
Destination IPv4 Address	• Contains a 32-bit binary value that represents the destination IPv4 address of the packet.
Options and Padding	• This is a field that varies in length from 0 to a multiple of 32 bits. • If the option values are not a multiple of 32 bits, 0s are added or padded to ensure that this field contains a multiple of 32 bits.

Attacking the Foundation

The IPv6 Packet Header

There are eight fields in the IPv6 packet header, as shown in the figure.



Byte 1
Byte 2
Byte 3
Byte 4

Version
Traffic Class
Flow Label

Payload Length
Next Header
Hop Limit

Source IP Address

Destination IP Address

40 Bytes

The IPv6 Packet Header (Contd.)

The following table describes the IPv6 header fields:

IPv6 Header Field	Description
Version	•This field contains a 4-bit binary value set to 0110 that identifies this as an IPv6 packet.
Traffic Class	•This 8-bit field is equivalent to the IPv4 Differentiated Services (DS) field.
Flow Label	•This 20-bit field suggests that all packets with the same flow label receive the same type of handling by routers.
Payload Length	•This 16-bit field indicates the length of the data portion or payload of the IPv6 packet.
Next Header	•This 8-bit field is equivalent to the IPv4 Protocol field. •It indicates the data payload type that the packet is carrying,

The IPv6 Packet Header (Contd.)

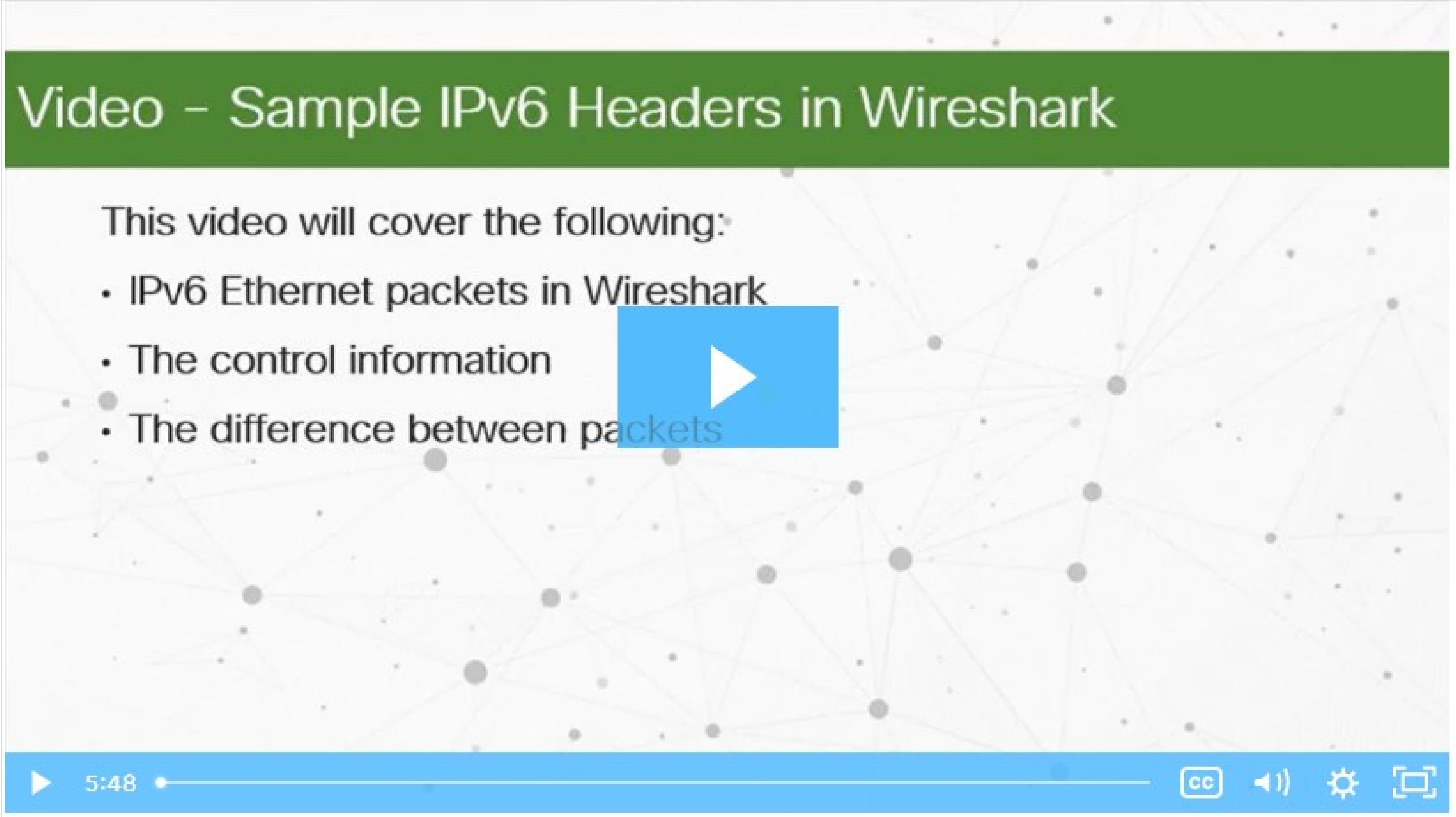
IPv6 Header Field	Description
Hop Limit	•This 8-bit field replaces the IPv4 TTL field. •This value is decremented by a value of 1 by each router that forwards the packet. •When the counter reaches 0, the packet is discarded, and an ICMPv6 Time Exceeded message is forwarded to the sending host, indicating that the packet did not reach its destination because the hop limit was exceeded.
Source IPv6 Address	•This 128-bit field identifies the IPv6 address of the sending host.
Destination IPv6 Address	•This 128-bit field identifies the IPv6 address of the receiving host.

- An IPv6 packet also contain extension headers (EH) that provide optional network layer information.
- Extension headers are optional and are placed between the IPv6 header and the payload. EHs are used for fragmentation, security, to support mobility, and more.

Attacking the Foundation

Video - Sample IPv6 Headers in Wireshark

Click Play in the figure to view a demonstration of examining IPv6 headers in a Wireshark capture.



Video – Sample IPv6 Headers in Wireshark

This video will cover the following:

- IPv6 Ethernet packets in Wireshark
- The control information
- The difference between packets

16.2 IP Vulnerabilities

IP Vulnerabilities

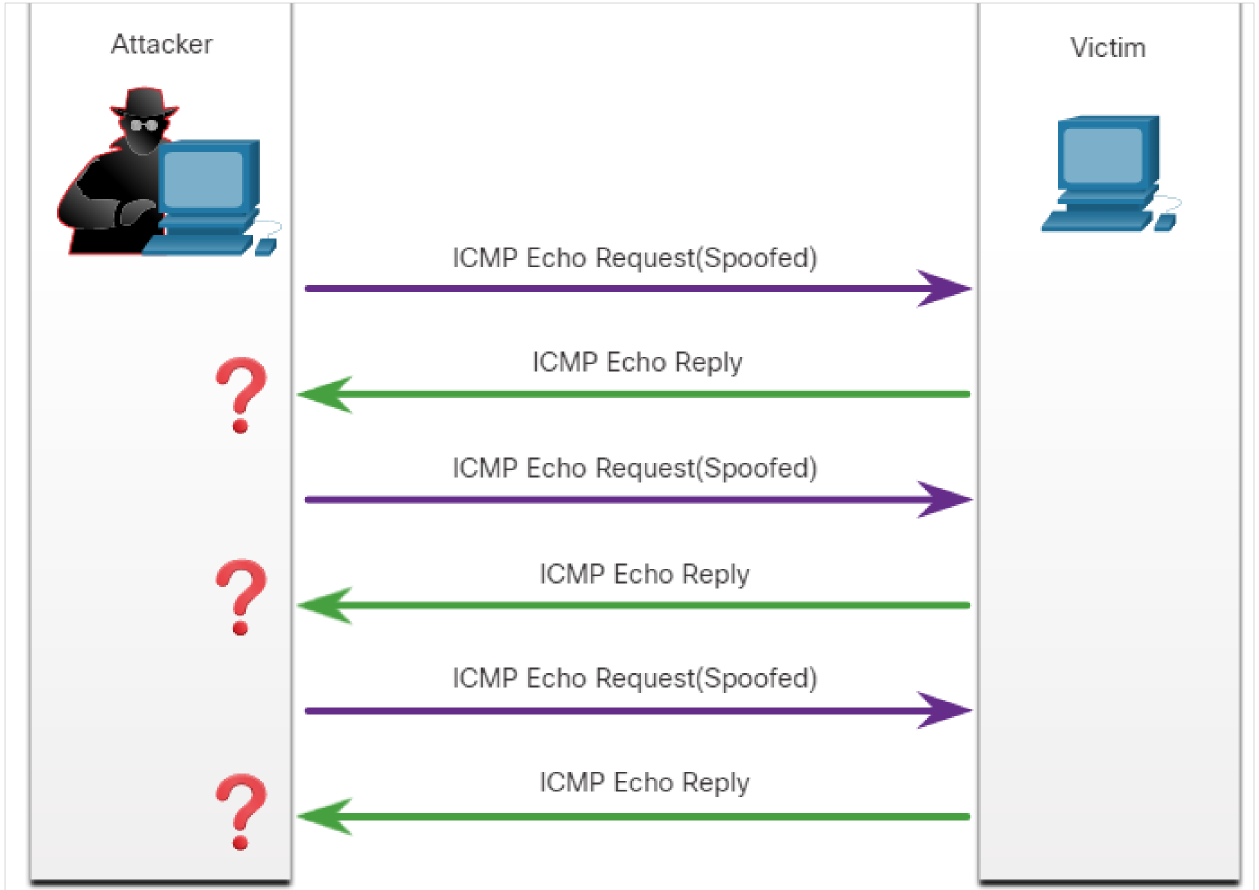
The following table lists some of the common IP-related attacks:

IP Attacks	Description
ICMP attacks	Threat actors use Internet Control Message Protocol (ICMP) echo packets (pings) to discover subnets and hosts on a protected network, to generate DoS flood attacks, and to alter host routing tables.
DoS attacks	Threat actors attempt to prevent legitimate users from accessing information or services.
DDoS attacks	Similar to a DoS attack, but features a simultaneous, coordinated attack from multiple source machines.
Address spoofing attacks	Threat actors spoof the source IP address in an attempt to perform blind spoofing or non-blind spoofing.
Man-in-the-middle attack (MiTM)	Threat actors position themselves between a source and destination to transparently monitor, capture, and control the communication. They could simply eavesdrop by inspecting captured packets or alter packets and forward them to their original destination.
Session hijacking	Threat actors gain access to the physical network, and then use an MiTM attack to hijack a session.

IP Vulnerabilities

ICMP Attacks

- ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable. ICMP messages are generated by devices when a network error or outage occurs.
- The ping command is a user-generated ICMP message, called an echo request, that is used to verify connectivity to a destination.
- Threat actors use ICMP for reconnaissance and scanning attacks.
- Threat actors also use ICMP for DoS and DDoS attacks, as shown in the ICMP flood attack in the figure.


Attacker
Victim
ICMP Echo Request(Spoofed)
ICMP Echo Reply
?
ICMP Echo Request(Spoofed)
ICMP Echo Reply
?
ICMP Echo Request(Spoofed)
ICMP Echo Reply
?

Note: ICMP for IPv4 (ICMPv4) and ICMP for IPv6 (ICMPv6) are susceptible to similar types of attacks.

ICMP Attacks (Contd.)

- Networks should have strict ICMP access control list (ACL) filtering on the network edge to avoid ICMP probing from the internet.

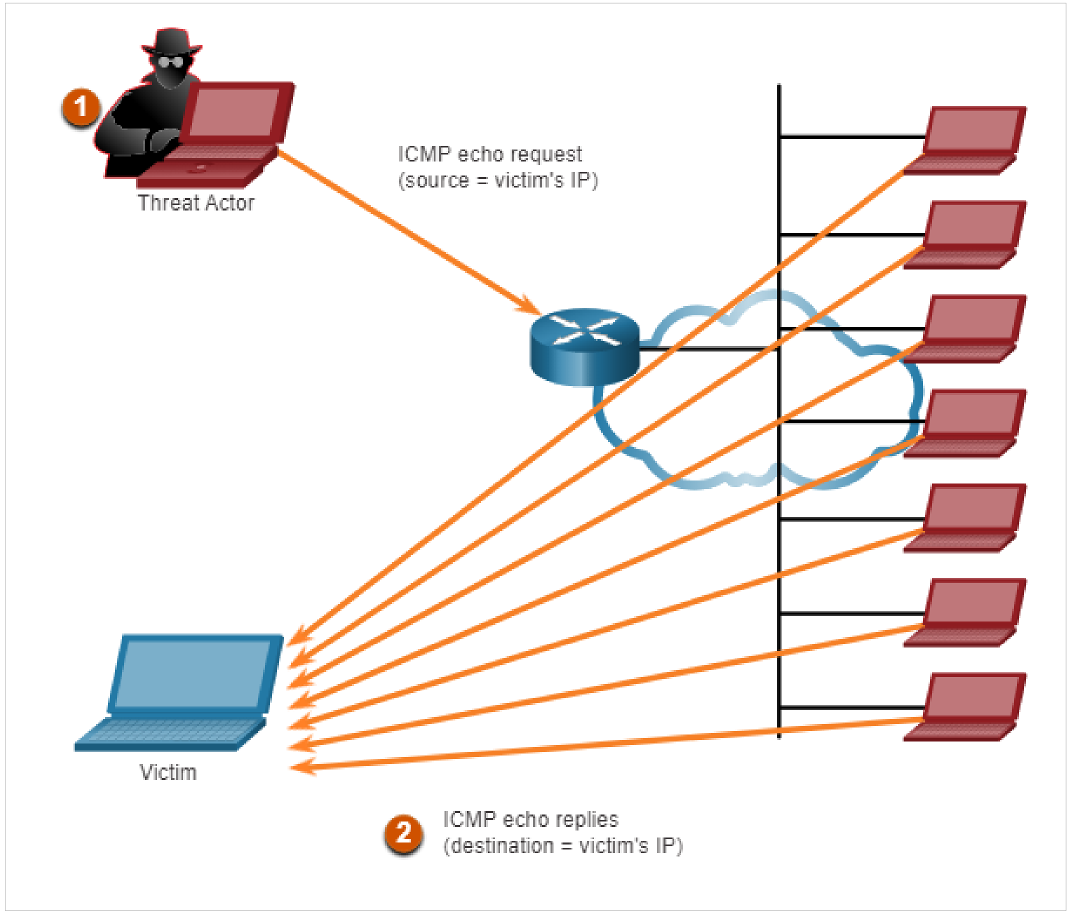
- The following table lists the common ICMP messages of interest to threat actors.

ICMP Message	Description
ICMP echo request and echo reply	This is used to perform host verification and DoS attacks.
ICMP unreachable	This is used to perform network reconnaissance and scanning attacks.
ICMP mask reply	This is used to map an internal IP network.
ICMP redirects	This is used to lure a target host into sending all traffic through a compromised device and create a MITM attack.
ICMP router discovery	This is used to inject bogus route entries into the routing table of a target host.

IP Vulnerabilities

Amplification and Reflection Attacks

- Threat actors often use amplification and reflection techniques to create DoS attacks.
- The figure shows how an amplification and reflection technique called a Smurf attack is used to overwhelm a target host.
  - **Amplification** - The threat actor forwards ICMP echo request messages to many hosts. These messages contain the source IP address of the victim.
  - **Reflection** - These hosts all reply to the spoofed IP address of the victim to overwhelm it.
- Threat actors also use resource exhaustion attacks.



Note: Newer forms of amplification and reflection attacks such as DNS-based reflection and amplification attacks and Network Time Protocol (NTP) amplification attacks are now being used.

IP Vulnerabilities

Address Spoofing Attacks

- IP address spoofing attacks occur when a threat actor creates packets with false source IP address information to either hide the identity of the sender, or to pose as another legitimate user.

- The threat actor can then gain access to otherwise inaccessible data or circumvent security configurations.

- Spoofing is usually incorporated into another attack such as a Smurf attack.

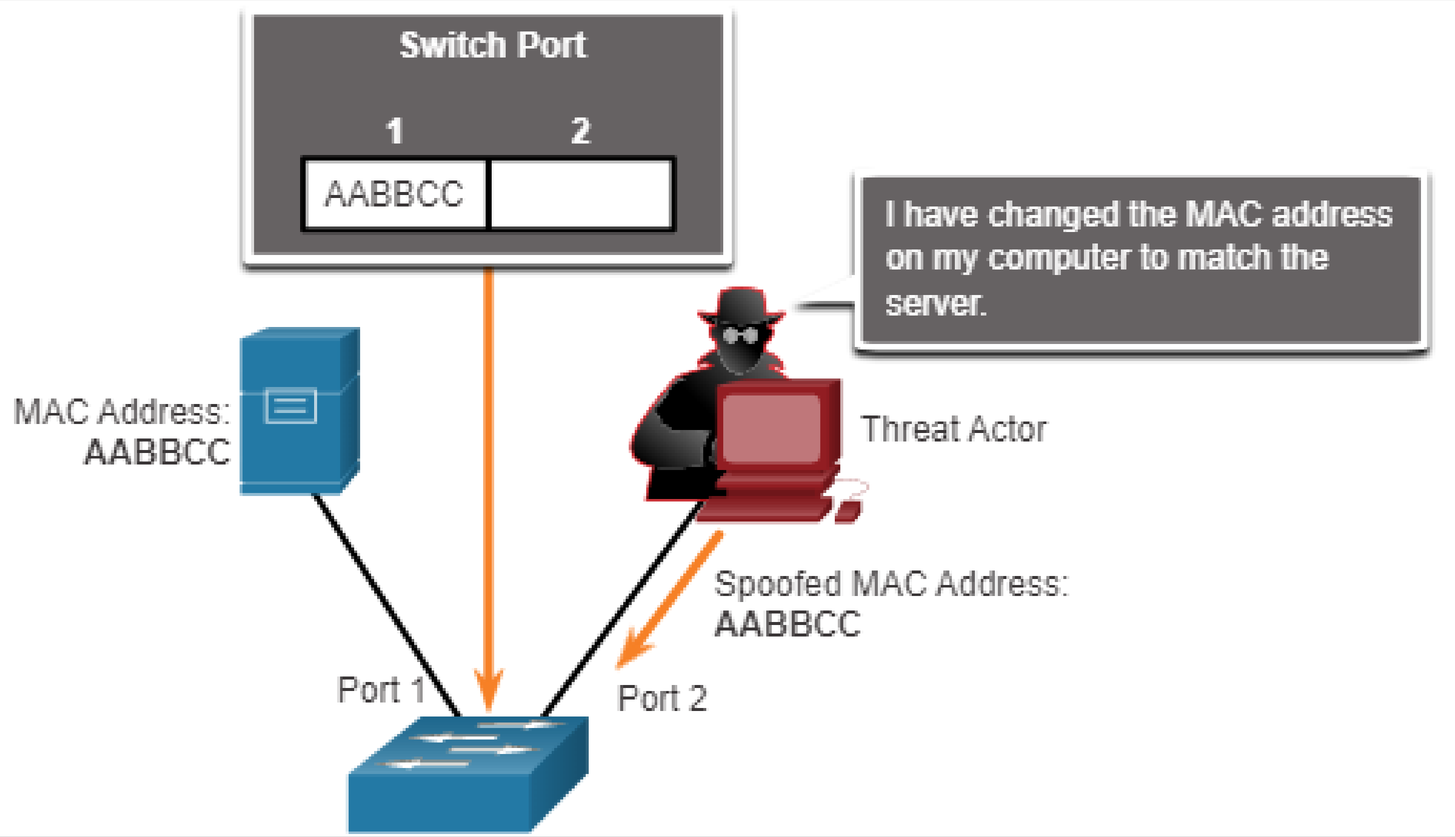
- Spoofing attacks can be non-blind or blind:
  - **Non-blind spoofing** - The threat actor can see the traffic that is being sent between the host and the target. The threat actor uses non-blind spoofing to inspect the reply packet from the target victim. Non-blind spoofing determines the state of a firewall and sequence-number prediction. It can also hijack an authorized session.
  - **Blind spoofing** - The threat actor cannot see the traffic that is being sent between the host and the target. Blind spoofing is used in DoS attacks.

IP Vulnerabilities

Address Spoofing Attacks (Contd.)

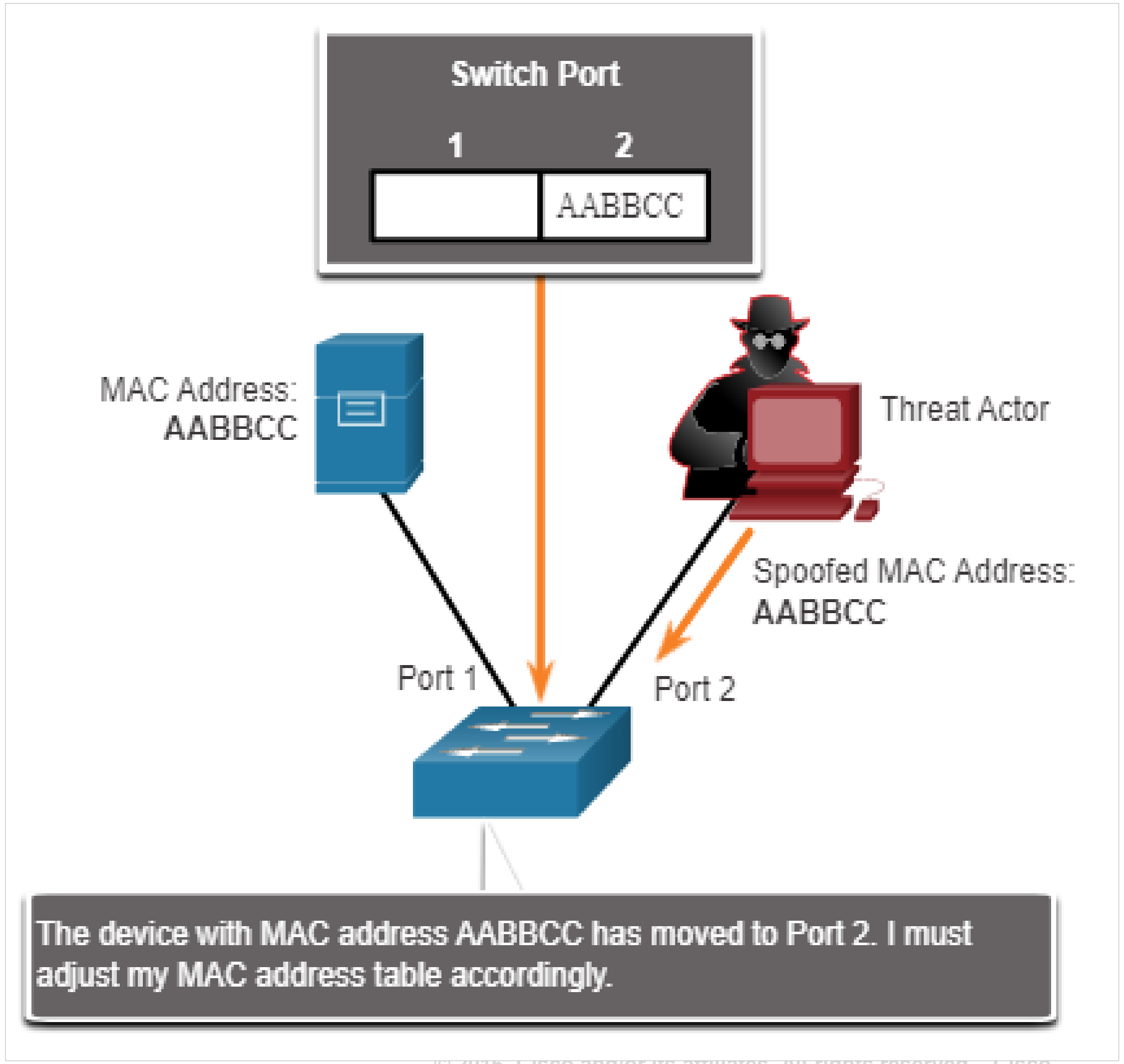
- MAC address spoofing attacks are used when threat actors have access to the internal network.

- Threat actors alter the MAC address of their host to match another known MAC address of a target host, as shown in the figure.
- The attacking host then sends a frame throughout the network with the newly-configured MAC address.
- When the switch receives the frame, it examines the source MAC address.


Switch Port
1
2
AABBCC
I have changed the MAC address on my computer to match the server.
MAC Address: AABBCC
Threat Actor
Spoofed MAC Address: AABBCC
Port 1
Port 2

Address Spoofing Attacks (Contd.)

- The switch overwrites the current CAM table entry and assigns the MAC address to the new port, as shown in the figure.
- It then forwards frames destined for the target host to the attacking host.
- Application or service spoofing is another spoofing example. A threat actor can connect a rogue DHCP server to create an MiTM condition.



The device with MAC address AABBCC has moved to Port 2. I must adjust my MAC address table accordingly.

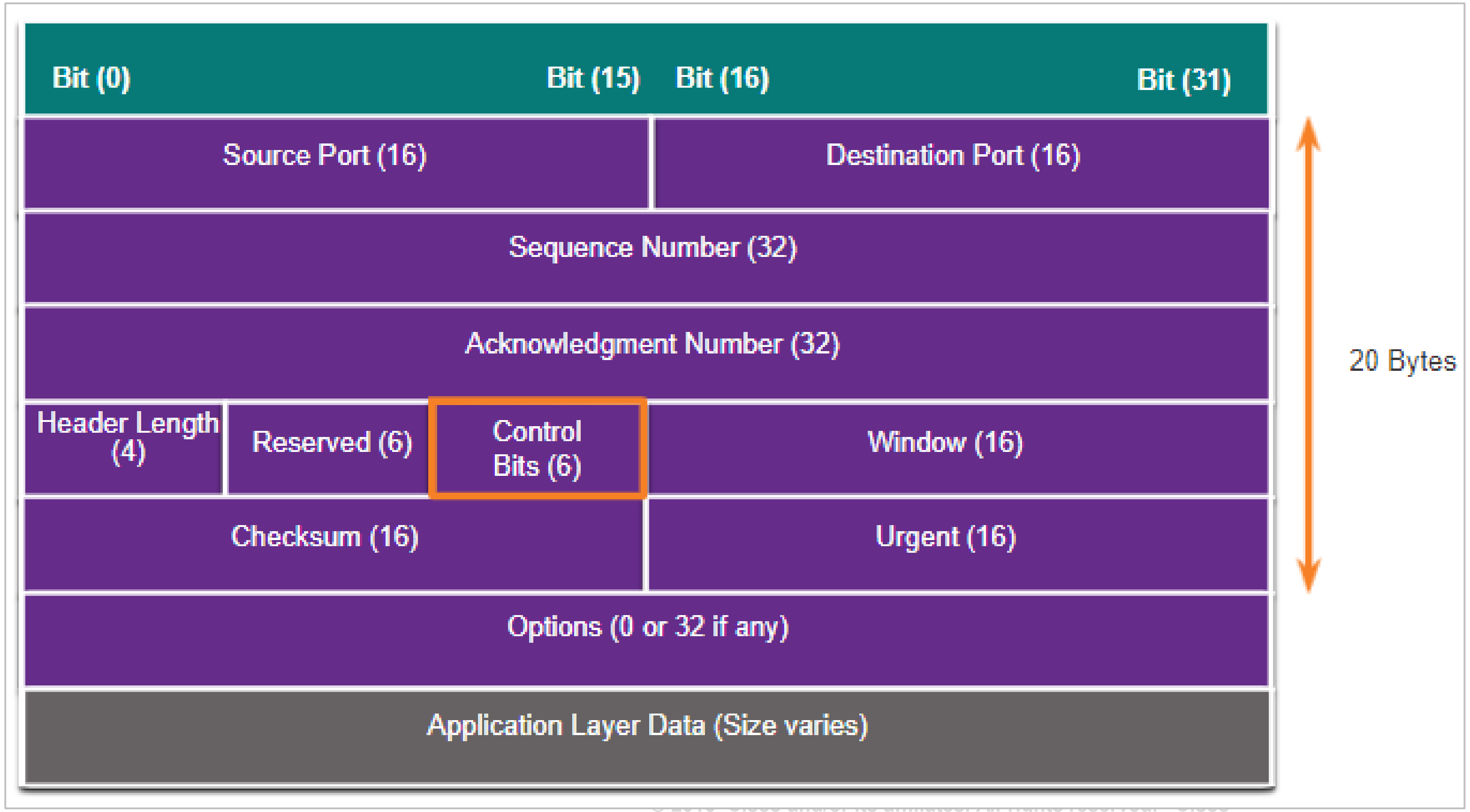
16.3 TCP and UDP Vulnerabilities

TCP and UDP Vulnerabilities

TCP Segment Header

- TCP segment information appears immediately after the IP header. The fields of the TCP segment and the flags for the Control Bits field are displayed in the figure.

- The following are the six control bits of the TCP segment:
  - URG - Urgent pointer field significant
  - ACK - Acknowledgment field significant
  - PSH - Push function
  - RST- Reset the connection
  - SYN - Synchronize sequence numbers
  - FIN - No more data from sender



Bit (0) Bit (15) Bit (16) Bit (31)

Source Port (16) | Destination Port (16)

Sequence Number (32)

Acknowledgment Number (32)

Header Length (4) | Reserved (6) | Control Bits (6) | Window (16)

Checksum (16) | Urgent (16)

Options (0 or 32 if any)

Application Layer Data (Size varies)

20 Bytes

TCP and UDP Vulnerabilities

TCP Services

TCP provides these services:

- **Reliable delivery** - TCP incorporates acknowledgments to guarantee delivery, instead of relying on upper-layer protocols to detect and resolve errors. If a timely acknowledgment is not received, the sender retransmits the data. Requiring acknowledgments of received data can cause substantial delays. Examples of application layer protocols that make use of TCP reliability include HTTP, SSL/TLS, FTP, DNS zone transfers, and others.
- **Flow control** - TCP implements flow control to address this issue. Rather than acknowledge one segment at a time, multiple segments can be acknowledged with a single acknowledgment segment.
- **Stateful communication** - TCP stateful communication between two parties occurs during the TCP three-way handshake. Before data can be transferred using TCP, a three-way handshake opens the TCP connection. If both sides agree to the TCP connection, data can be sent and received by both parties using TCP.

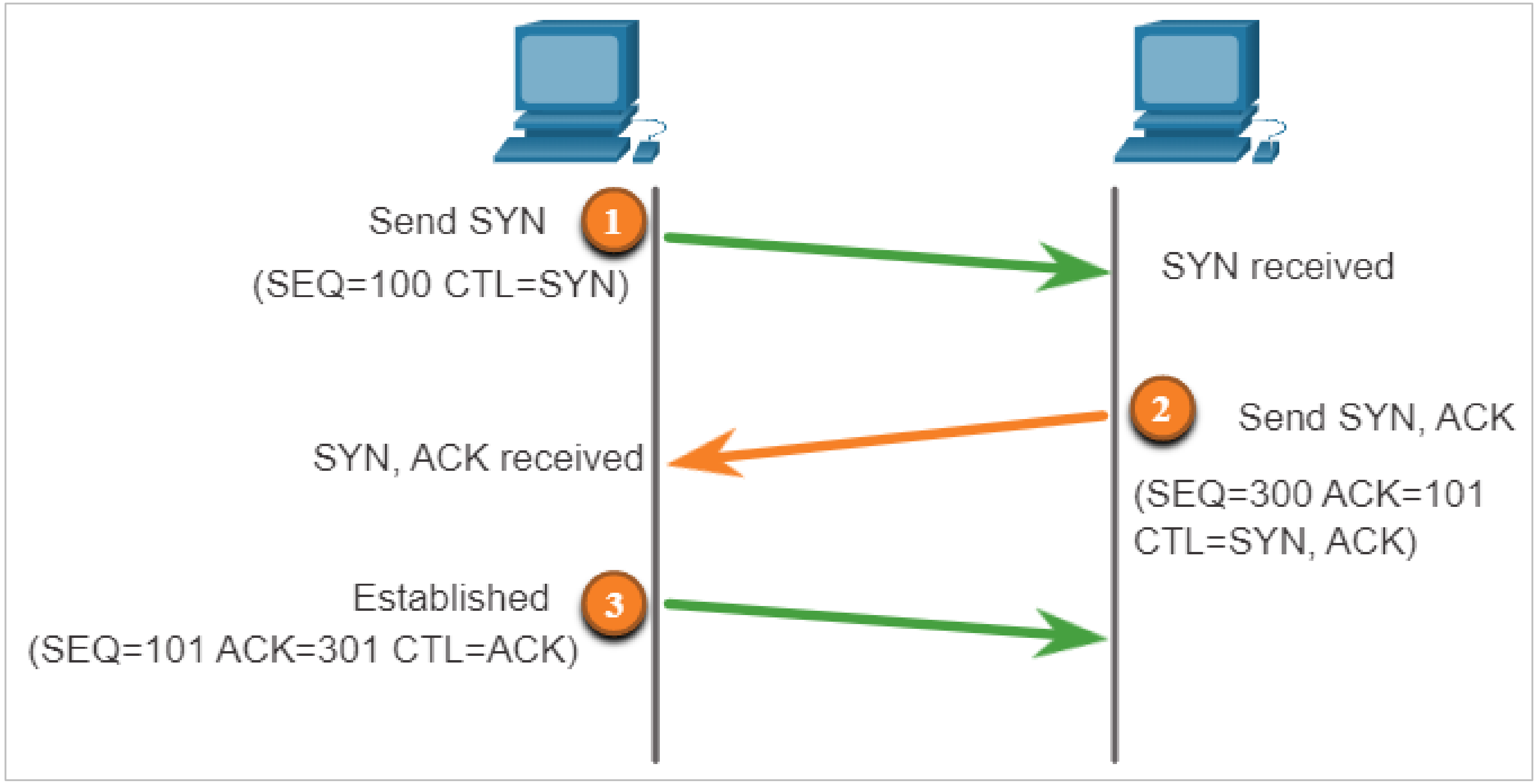
TCP and UDP Vulnerabilities

TCP Services (Contd.)

TCP Three-Way Handshake

A TCP connection is established in three steps:

- The initiating client requests a client-to-server communication session with the server.
- The server acknowledges the client-to-server communication session and requests a server-to-client communication session.
- The initiating client acknowledges the server-to-client communication session.

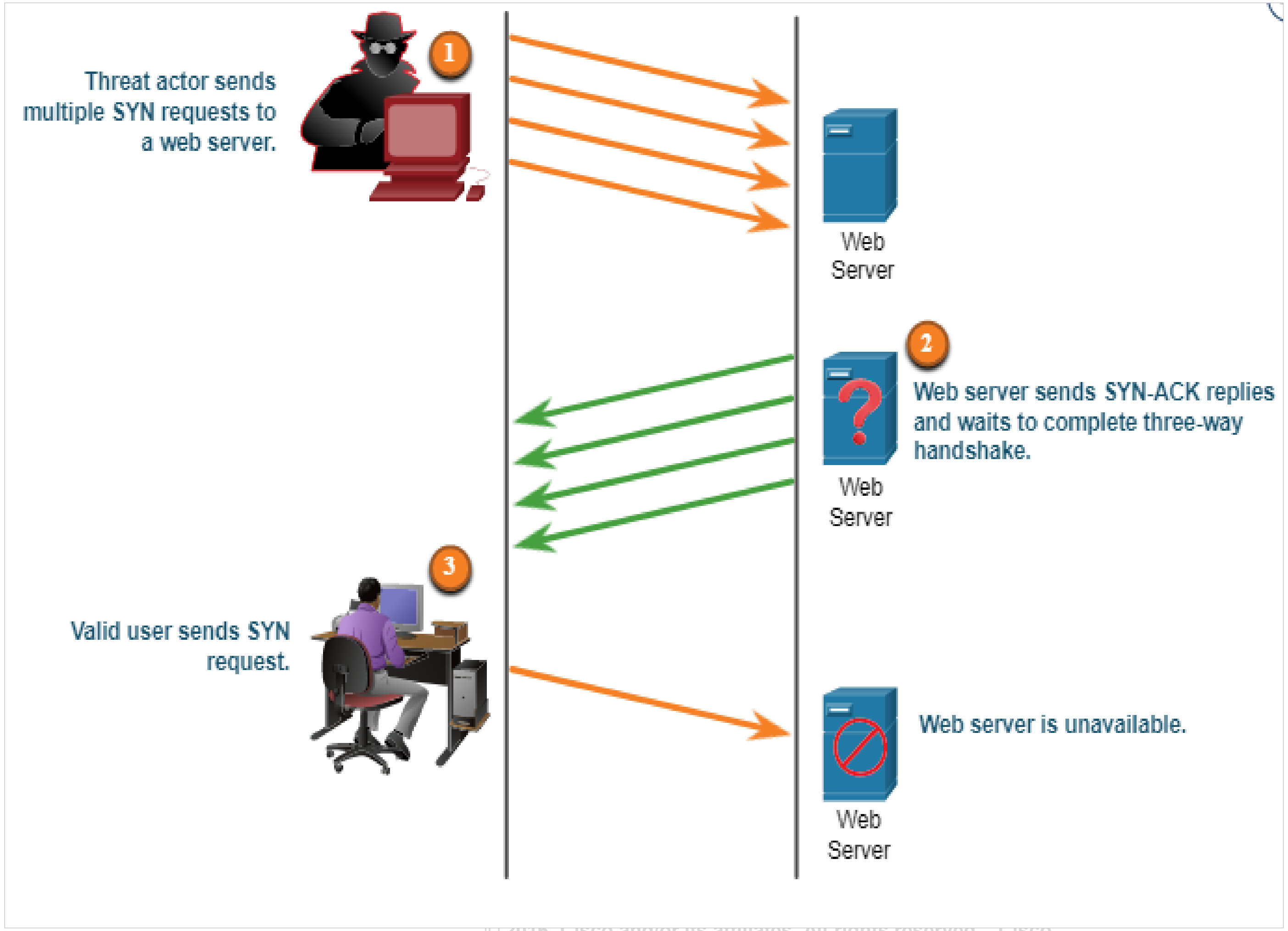


TCP Attacks

Network applications use TCP or UDP ports. Threat actors conduct port scans of target devices to discover which services they offer.

TCP SYN Flood Attack

- **The TCP SYN Flood attack exploits the TCP three-way handshake.**
- The figure shows a threat actor continually sending TCP SYN session request packets with a randomly spoofed source IP address to a target.
- The target replies with a TCP SYN-ACK packet to the spoofed IP address and waits for a TCP ACK packet. Those responses never arrive.
- The target host **has too many** half-open TCP connections, and TCP services are denied to legitimate users.



1 Threat actor sends multiple SYN requests to a web server.

2 Web server sends SYN-ACK replies and waits to complete three-way handshake.

3 Valid user sends SYN request.

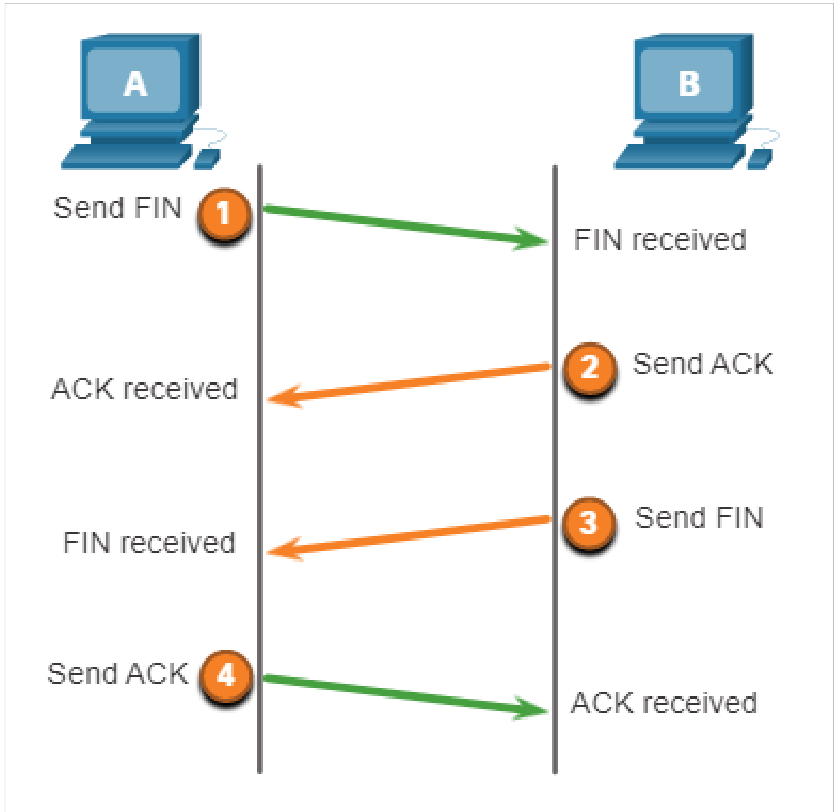
Web server is unavailable.

TCP and UDP Vulnerabilities

TCP Attacks (Contd.)

TCP Reset Attack

- A TCP reset attack can be used to terminate TCP communications between two hosts.
- A threat actor could do a TCP reset attack and send a spoofed packet containing a TCP RST to one or both endpoints.
- Terminating a TCP session uses the following four-way exchange process:
- When the client has no more data to send in the stream, it sends a segment with the FIN flag set.
- The server sends an ACK to acknowledge the receipt of the FIN to terminate the session from client to server.
- The server sends a FIN to the client to terminate the server-to-client session.
- The client responds with an ACK to acknowledge the FIN from the server.



A sends ACK response to B

TCP and UDP Vulnerabilities

TCP Attacks (Contd.)

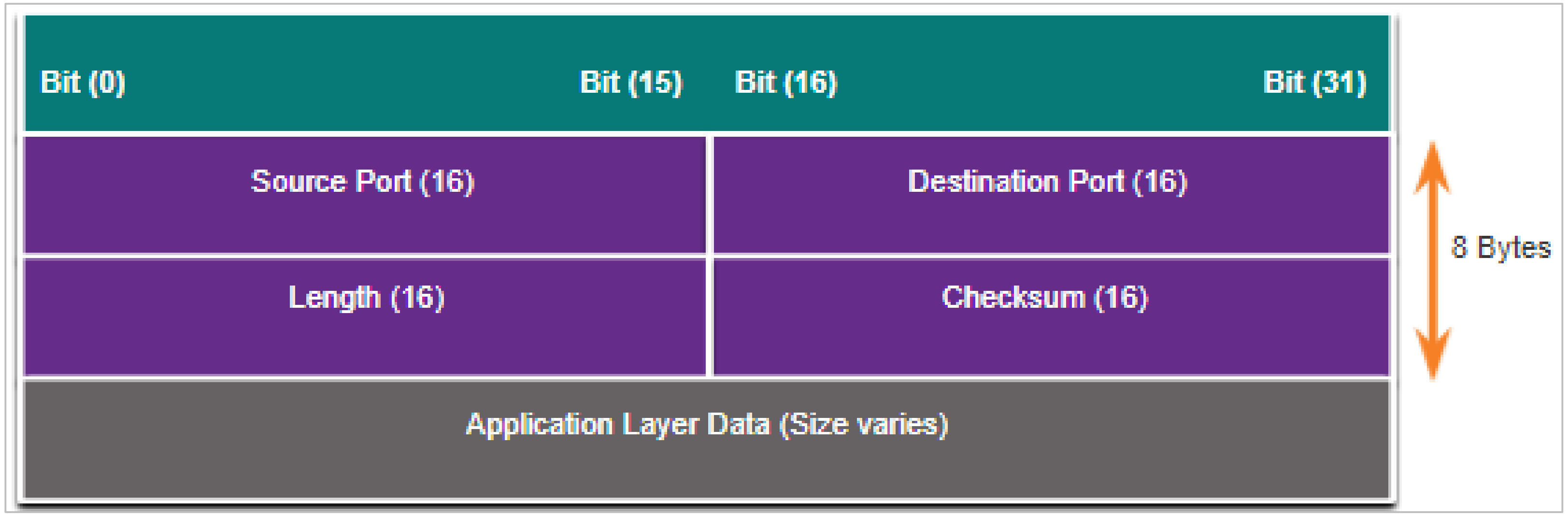
TCP Session Hijacking

- TCP session hijacking is another TCP vulnerability.
- A threat actor takes over an already-authenticated host as it communicates with the target.
- The threat actor must spoof the IP address of one host, predict the next sequence number, and send an ACK to the other host.
- If successful, the threat actor could send, but not receive, data from the target device.

TCP and UDP Vulnerabilities

UDP Segment Header and Operation

- UDP is commonly used by DNS, DHCP, TFTP, NFS, and SNMP.
- It is also used with real-time applications such as media streaming or VoIP. UDP is a connectionless transport layer protocol.
- The UDP segment structure, shown in the figure, is much smaller than TCP.
- Although UDP is normally called unreliable, this does not mean that applications that use UDP are always unreliable. It means that these functions are not provided by the transport layer protocol and must be implemented elsewhere if required.



Bit (0) Bit (15)	Bit (16) Bit (31)
Source Port (16)	Destination Port (16)
Length (16)	Checksum (16)
Application Layer Data (Size varies)	

- The low overhead of UDP makes it very desirable for protocols that make simple request and reply transactions.

TCP and UDP Vulnerabilities

UDP Attacks

- UDP is not protected by any encryption. Encryption can be added to UDP, but it is not available by default.
- The lack of encryption means that anyone can see the traffic, change it, and send it on to its destination.

UDP Flood Attacks

- In a UDP flood attack, all the resources on a network are consumed.
- The threat actor must use a tool like UDP Unicorn or Low Orbit Ion Cannon. These tools send a flood of UDP packets, often from a spoofed host, to a server on the subnet.
- The program will sweep through all the known ports trying to find closed ports. This will cause the server to reply with an ICMP port unreachable message.
- As there are many closed ports on the server, this creates a lot of traffic on the segment, which uses up most of the bandwidth. The result is very similar to a DoS attack.

16.4 Attacking the Foundation Summary

Attacking the Foundation Summary

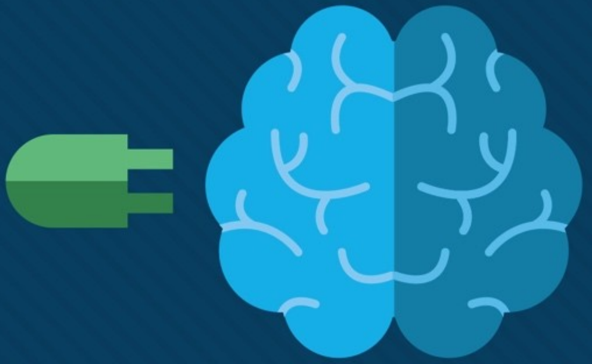
What Did I Learn in this Module?

- IP was designed as a Layer 3 connectionless protocol.
- The IPv4 header consists of several fields while the IPv6 header contains fewer fields. It is important for security analysts to understand the different fields in both the IPv4 and IPv6 headers.
- There are different types of attacks that target IP. Common IP-related attacks include:
  - ICMP attacks
  - Denial-of-Service (DoS) attacks
  - Distributed Denial-of-Service (DoS) attacks
  - Address spoofing attacks
  - Man-in-the-middle attack (MiTM)
  - Session hijacking

Attacking the Foundation Summary

What Did I Learn in this Module? (Contd.)

- ICMP was developed to carry diagnostic messages and to report error conditions when routes, hosts, and ports are unavailable.
- TCP segment and UDP datagram information appear immediately after the IP header. It is important to understand Layer 4 headers and their functions in data communication.
- Threat actors can conduct a variety of TCP related attacks:
  - TCP port scans
  - TCP SYN Flood attack
  - TCP Reset Attack
  - TCP Session Hijacking attack
- The UDP segment (i.e., datagram) is much smaller than the TCP segment, which makes it very desirable for use by protocols that make simple request and reply transactions such as DNS, DHCP, SNMP, and others.



Module 17:Attacking What We Do

Instructor Materials

CyberOps Associate v1.0

Module 17:
Attacking What We Do

Module Objective: Explain how common network applications and services are vulnerable to attack.

Topic Title	Topic Objective
IP Services	Explain IP service vulnerabilities
Enterprise Services	Explain how network application vulnerabilities enable network attacks

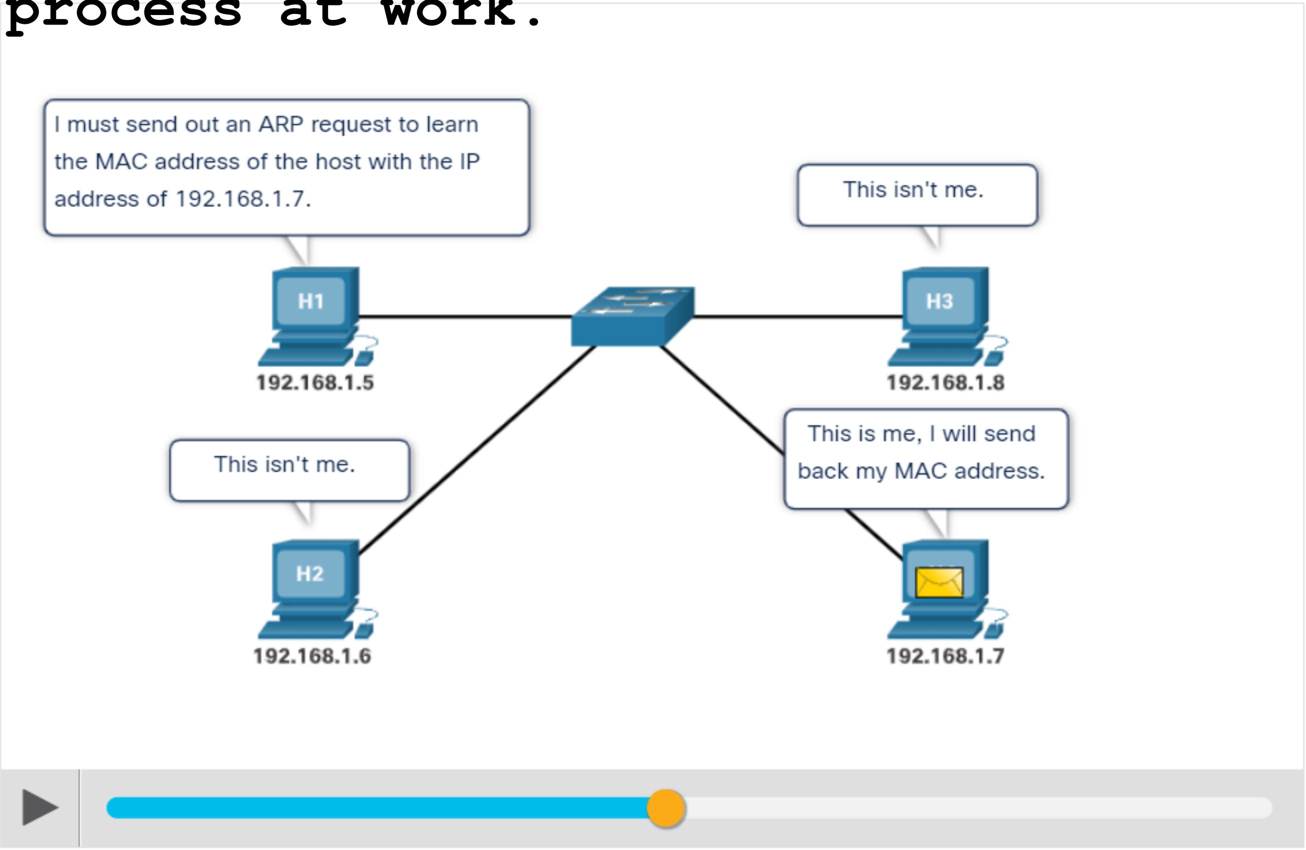
17.1 IP Services

Attacking What We Do

ARP Vulnerabilities

- Hosts broadcast an ARP Request to other hosts on the network segment to determine the MAC address of a host with a particular IP address.
- The host with the matching IP address in the ARP Request sends an ARP Reply called “gratuitous ARP.”
- A threat actor can poison the ARP cache of devices on the local network
- The goal is to associate the threat actor’s MAC address with the IP address of the default gateway in the ARP caches of hosts on the LAN segment.

Play the animation to see the ARP process at work.



I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.
This isn't me.
H1
192.168.1.5
H3
192.168.1.8
This is me, I will send back my MAC address.
This isn't me.
H2
192.168.1.6
192.168.1.7

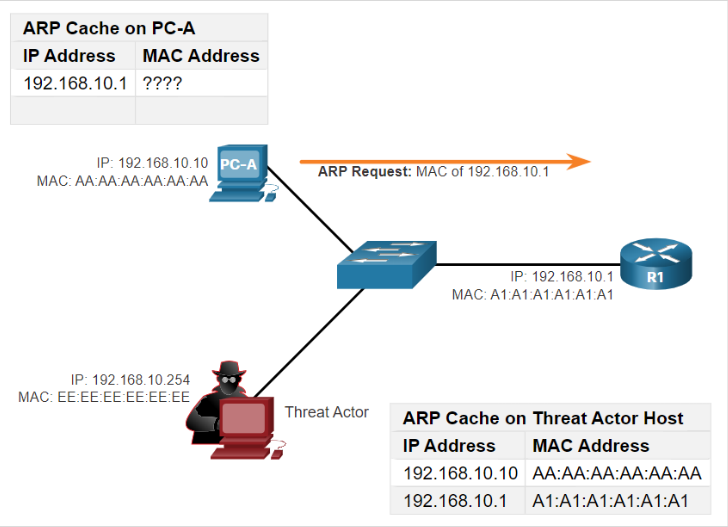
Attacking What We Do

ARP Cache Poisoning

- ARP cache poisoning can be used to launch various man-in-the-middle attacks.

ARP cache poisoning process

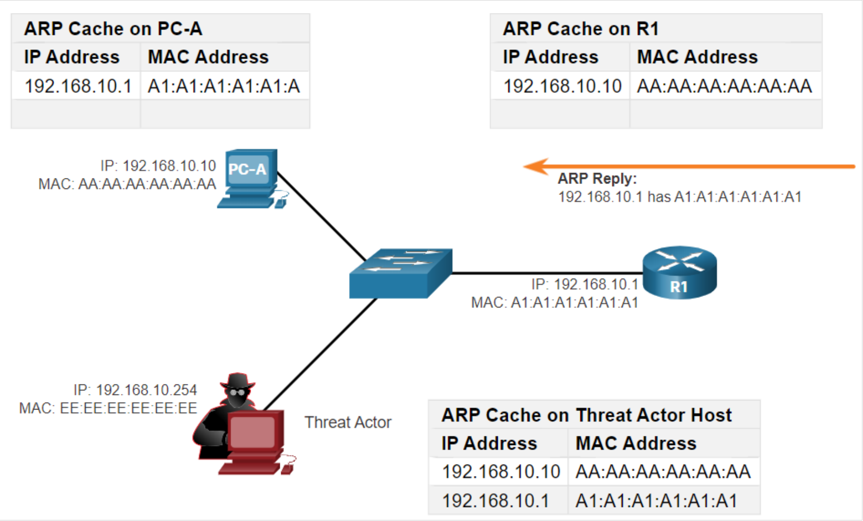
ARP Request



ARP Cache on PC-A	
IP Address	MAC Address
192.168.10.1	????

ARP Cache on Threat Actor Host	
IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA
192.168.10.1	A1:A1:A1:A1:A1:A1

ARP Reply

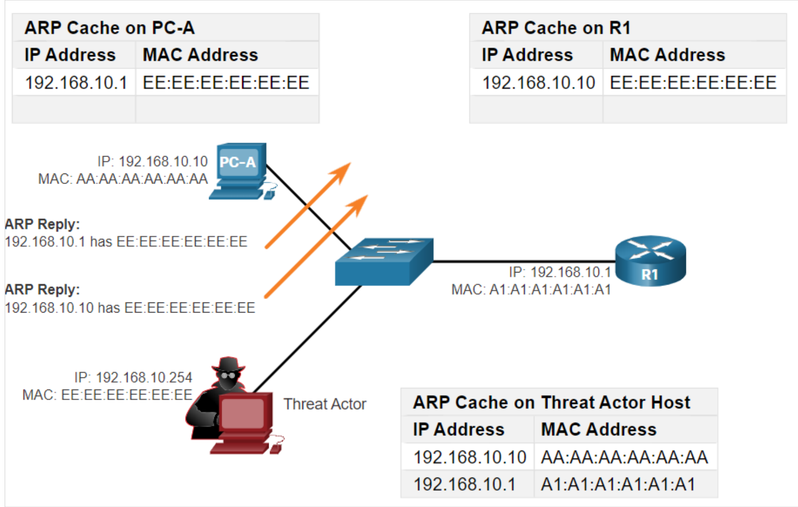


ARP Cache on PC-A	
IP Address	MAC Address
192.168.10.1	A1:A1:A1:A1:A1:A

ARP Cache on R1	
IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA

ARP Cache on Threat Actor Host	
IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA
192.168.10.1	A1:A1:A1:A1:A1:A1

Spoofed Gratuitous ARP replies



ARP Cache on PC-A	
IP Address	MAC Address
192.168.10.1	EE:EE:EE:EE:EE:EE

ARP Cache on R1	
IP Address	MAC Address
192.168.10.10	EE:EE:EE:EE:EE:EE

ARP Cache on Threat Actor Host	
IP Address	MAC Address
192.168.10.10	AA:AA:AA:AA:AA:AA
192.168.10.1	A1:A1:A1:A1:A1:A1

Note: There are many tools available on the internet to create ARP MITM attacks including dsniff, Cain & Abel, ettercap, Yersinia, and others.

DNS Attacks

DNS attacks include the following:

DNS open resolver attacks:

- A DNS open resolver is a publicly open DNS server such as Google DNS (8.8.8.8) that answers client's queries outside its administrative domain. DNS open resolvers are vulnerable to multiple malicious activities described in the table.

DNS Resolver Vulnerabilities	Description
DNS cache poisoning attacks	Threat actors send spoofed, falsified Record Resource (RR) information to a DNS resolver to redirect users from legitimate sites to malicious sites.
DNS amplification and reflection attacks	Threat actors send DNS messages to the open resolvers using the IP address of a target host.
DNS resource utilization attacks	This DoS attack consumes all the available resources to negatively affect the operations of the DNS open resolver.

DNS Attacks (Contd.)

DNS Stealth Attacks

- To hide their identity, threat actors also use the DNS stealth techniques described in the table to carry out their attacks.

DNS Stealth Techniques	Description
Fast Flux	Threat actors use this technique to hide their phishing and malware delivery sites. The DNS IP addresses are continuously changed within minutes.
Double IP Flux	Threat actors use this technique to rapidly change the hostname to IP address mappings and to also change the authoritative name server. This increases the difficulty of identifying the source of the attack.
Domain Generation Algorithms	Threat actors use this technique in malware to randomly generate domain names that can then be used as rendezvous points to their command and control (C&C) servers.

Attacking What We Do

DNS Attacks (Contd.)

DNS Domain Shadowing Attacks

- In Domain Shadowing, threat actor gather domain account credentials in order to create multiple sub-domains which will be used during the attacks.
- These subdomains typically point to malicious servers without alerting the actual owner of the parent domain.

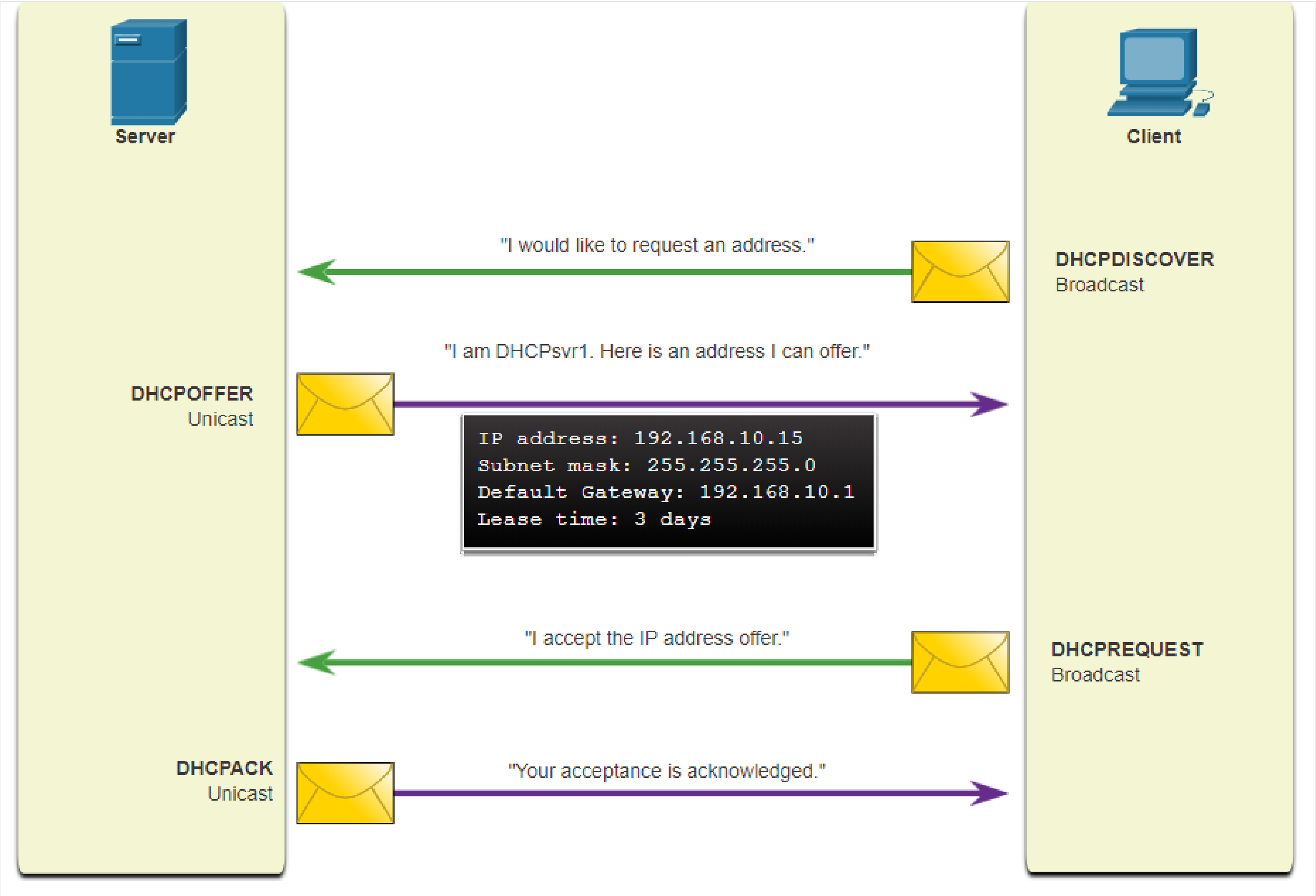
Attacking What We Do

DNS Tunneling

- It is necessary for the cybersecurity analyst to be able to detect when an attacker is using DNS tunneling to steal data, and prevent and contain the attack.
- To accomplish this, the security analyst must implement a solution that can block the outbound communications from the infected hosts.
- Threat actors who use DNS tunneling place non-DNS traffic within DNS traffic. This method often circumvents security solutions.
- For the threat actor to use DNS tunneling, the different types of DNS records such as TXT, MX, SRV, NULL, A, or CNAME are altered. For example, a TXT record can store the commands that are sent to the infected host bots as DNS replies.
- To stop DNS tunneling, a filter that inspects DNS traffic must be used.

DHCP

- DHCP servers dynamically provide IP configuration information to clients.
- In the figure, a client broadcasts a DHCP discover message.
- The DHCP server responds with a unicast offer that includes addressing information the client can use.
- The client broadcasts a DHCP request to tell the server that the client accepts the offer.
- The server responds with a unicast acknowledgment accepting the request.


Server
Client
"I would like to request an address."
DHCPDISCOVER
Broadcast
"I am DHCPsvr1. Here is an address I can offer."
DHCPOFFER
Unicast
"I accept the IP address offer."
DHCPREQUEST
Broadcast
DHCPACK
Unicast
"Your acceptance is acknowledged."

```
IP address: 192.168.10.15
Subnet mask: 255.255.255.0
Default Gateway: 192.168.10.1
Lease time: 3 days
```

Normal DHCP Operation

DHCP Attacks

DHCP Spoofing Attack

- A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.

A rogue server can provide a variety of misleading information such as:

- **Wrong default gateway** - Threat actor provides an invalid gateway, or the IP address of its host to create a MITM (Man In The Middle) attack.
- **Wrong DNS server** - Threat actor provides an incorrect DNS server address pointing the user to a malicious website.
- **Wrong IP address** - Threat actor provides an invalid IP address, invalid default gateway IP address, or both. The threat actor then creates a DoS attack on the DHCP client.

17.2 Enterprise Services

HTTP and HTTPS

- To investigate web-based attacks, security analysts must have a good understanding of how a standard web-based attack works.

Common stages of a typical web attack:

- The victim unknowingly visits a web page that has been compromised by malware.
- The compromised web page redirects the user to a site containing malicious code.
- The user visits this site with malicious code and their computer becomes infected.
- After identifying a vulnerable software package running on the victim's computer, the exploit kit contacts the exploit kit server to download the malicious code.
- After the victim's computer has been compromised, it connects to the malware server and downloads a payload.
- The final malware package is run on the victim's computer.

Enterprise Services

HTTP and HTTPS (Contd.)

- Server connection logs can often reveal information about the type of scan or attack.
- The different types of connection status codes are:
  - **Informational 1xx**
  - **Successful 2xx**
  - **Redirection 3xx**
  - **Client Error 4xx**
- To defend against web-based attacks:
  - Always update the OS and browsers with current patches and updates.
  - Use a web proxy to block malicious sites.
  - Use the best security practices from the Open Web Application Security Project (OWASP) when developing web applications.
  - Educate end users by showing them how to avoid web-based attacks.

Common HTTP Exploits

Malicious iFrames

- An iFrame is an HTML element that allows the browser to load another web page from another source.
- In iFrame attacks, the threat actors insert advertisements from other sources into the page.
- Threat actors compromise a webserver and modify web pages by adding HTML for the malicious iFrame.
- As the iFrame is running in the page, it can be used to deliver a malicious exploit. such as spam advertising, exploit kits, and other malware.

Steps to prevent or reduce malicious iFrames:

- Use a web proxy like to block malicious sites.
- Ensure web developers do not use iFrames.
- Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.
- Ensure the end user understands what an Iframe is.

Common HTTP Exploits (Contd.)

HTTP 302 Cushioning

- Threat actors use the 302 Found HTTP response status code to direct the user’s web browser to a new location.
- The browser believes that the new location is the URL provided in the header. The browser is invited to request this new URL. This redirect function can be used multiple times until the browser finally lands on the page that contains the exploit.

Steps to prevent or reduce HTTP 302 cushioning attacks:

- Use a web proxy to block malicious sites.
- Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.
- Ensure the end user understands how the browser is redirected through a series of HTTP 302 redirections.

Enterprise Services

Common HTTP Exploits (Contd.)

Domain Shadowing

- When a threat actor create a domain shadowing attack, first they compromise a domain. Then they must create multiple subdomains of that domain to be used for the attacks using Hijacked domain registration logins.
- After these subdomains have been created, attackers can use them even if they are found out to be malicious domains. They can simply make more from the parent domain.

Steps to prevent or reduce Domain shadowing attacks:

- Secure all domain owner accounts.
- Use a web proxy to block malicious sites.
- Use a service such as Cisco Umbrella to prevent users from navigating to web sites that are known to be malicious.
- Make sure that domain owners validate their registration accounts and look for any subdomains that they have not authorized.

Enterprise Services

Email

- As the level of use of email rises, security becomes a greater priority.
- The way users access email today also increases the opportunity for the threat of malware to be introduced.

Examples of email threats:

- **Attachment-based attacks** - Threat actors embed malicious content in business files such as an email from the IT department.
- **Email spoofing** - Threat actors create email messages with a forged sender address that is meant to fool the recipient into providing money or sensitive information.
- **Spam email** - Threat actors send unsolicited email containing advertisements or malicious files.
- **Open mail relay server -** This is an SMTP server that allows anybody on the internet to send mail.

Web-Exposed Databases

- Web applications commonly connect to a relational database to access data.
- As relational databases often contain sensitive data, databases are a frequent target for attacks.

Code Injection

- The attacker’s commands are executed through the web application and has the same permissions as the web application.
- This type of attack is used because often there is insufficient validation of input.

SQL Injection

- Threat actors use SQL injections to breach the relational database, create malicious SQL queries, and obtain sensitive data from the relational database.
- A successful SQL injection exploit can read sensitive data from the database, modify database data, execute administration operations on the database, and sometimes, issue commands to the operating system.

Client-side Scripting

Cross-Site Scripting

- Cross-Site Scripting (XSS) is where web pages that are executed on the client-side, within their own web browser, are injected with malicious scripts.
- These scripts can be used by Visual Basic, JavaScript, and others to access a computer, collect sensitive information, or deploy more attacks and spread malware.
- The two main types of XSS are **Stored (persistent)** and **Reflected (non-persistent).**
- **Ways to prevent or reduce XSS attacks**:
  - Ensure that web application developers are aware of XSS vulnerabilities and how to avoid them.
  - Use an IPS implementation to detect and prevent malicious scripts.
  - Use a web proxy to block malicious sites.
  - Use a service such as Cisco Umbrella to prevent users from navigating to malicious websites.

17.3 Attacking What We Do Summary

Attacking What We Do Summary

What Did I Learn in this Module?

- Any client can send an unsolicited ARP Reply called a “gratuitous ARP.”
- A threat actor can poison the ARP cache of devices on the local network, creating an MiTM attack to redirect traffic.
- The Domain Name Service (DNS) protocol uses Resource Records (RR) to identify the type of DNS response.
- DNS open resolvers are vulnerable to multiple malicious activities, including DNS cache poisoning, in which falsified records are provided to the open resolver.
- In DNS amplification and reflection attacks, the benign nature of the DNS protocol is exploited to cause DoS/ DDoS attacks.
- In DNS resource utilization attacks, a DoS attack is launched against the DNS server itself.
- Threat actors use Fast Flux, in which malicious servers will rapidly change their IP address.
- To stop DNS tunneling, a filter that inspects DNS traffic must be used.

Attacking What We do Summary

What Did I Learn in this Module?

- A DHCP spoofing attack occurs when a rogue DHCP server is connected to the network and provides false IP configuration parameters to legitimate clients.
- The compromised web page redirects the user to a site that hosts malicious code which is known as a drive-by download.
- Cross-Site Scripting (XSS) attacks occur when browsers execute malicious scripts on the client and provide threat actors with access to sensitive information on the local host.
- The OWASP Top 10 Web Application Security Risks is designed to help organizations create secure web applications.

UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Ďakujem za pozornosť

Obsahom boli moduly:

- Chapter 15 Network Monitoring and Tools (SIEM, SOAR)
- Chapter 16 Attacking the Foundation (L2, L3 protocols vulnerabilities and attacks)
- Chapter 17 Attacking What We Do (L7 vulnerabilities and attacks)

Vyjadrite spätnú väzbu na prednášku a/alebo cvičenie v anonymnej ankete cez google form: link

Vytvorené v rámci projektu KEGA 026TUKE-4/2021.