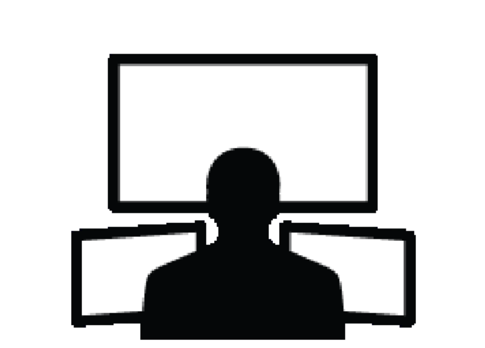
UNIVERSITY OF ŽILINA
Faculty of Management Science
and Informatics

Prednáška 8
Vulnerability assessment, technologies and protocols



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

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 a vyhodnocovať 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

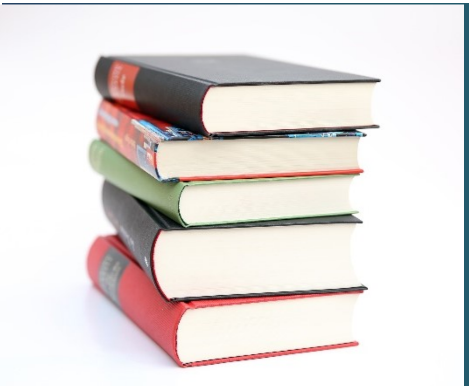
- Prerekvizity:
  - Princípy IKS, Počítačové siete 1, Úvod do OS

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

Week	CyberOps Modules in Lectures	Exam from:
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) Chapter 28 Digital Forensics and Incident Analysis and Response	24-25
11	Expert talk (invited lecture)	26-28



Obsah dnešnej prednášky

Čo prejdeme spolu na prednáške:

- **Chapter 23 Endpoint Vulnerability Assessment**
- **Chapter 24 Technologies and Protocols**

Module 23: Endpoint Vulnerability Assessment

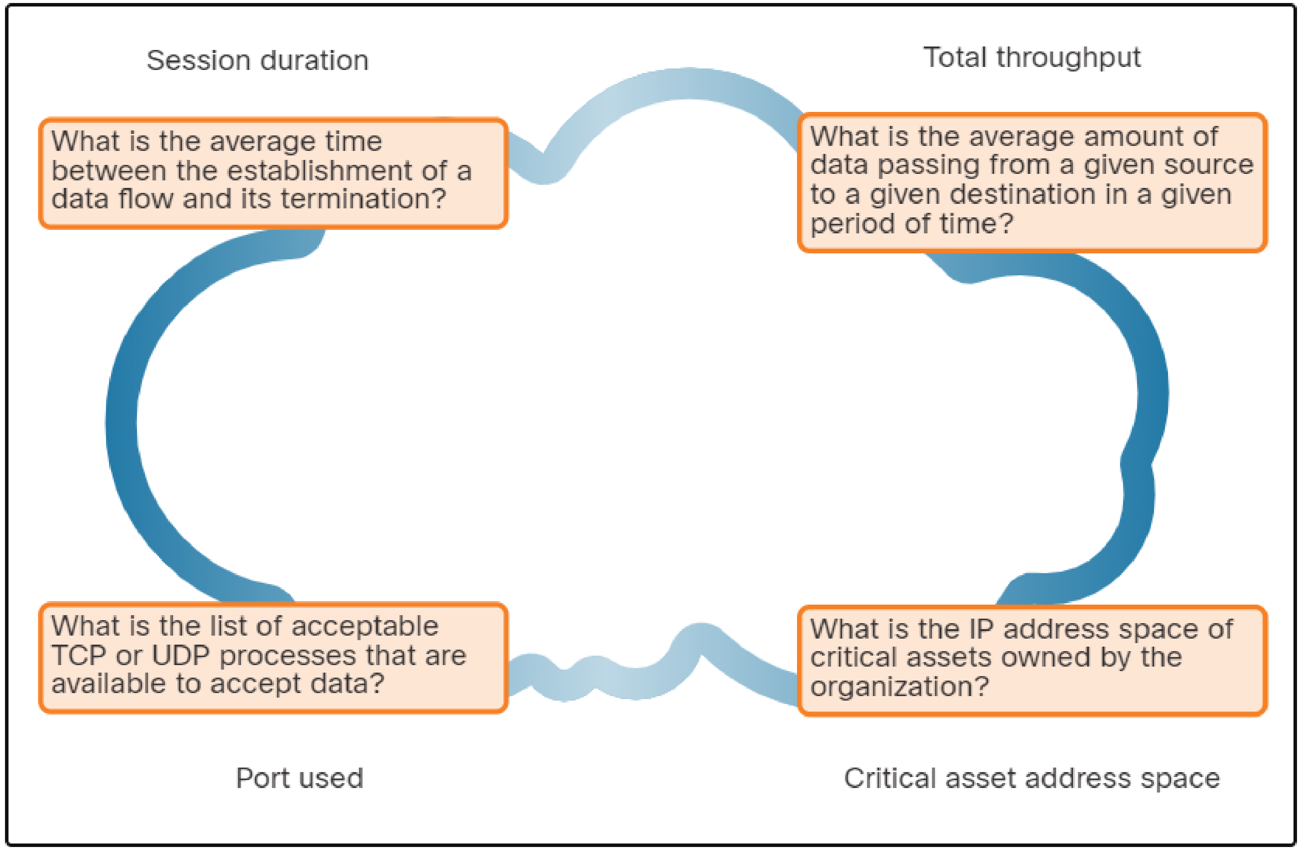
Module Objective: Explain how endpoint vulnerabilities are assessed and managed.

Topic Title	Topic Objective
Network and Server Profiling	Explain the value of network and server profiling.
Common Vulnerability Scoring System (CVSS)	Explain how CVSS reports are used to describe security vulnerabilities.
Secure Device Management	Explain how secure device management techniques are used to protect data and assets.
Information Security Management Systems	Explain how information security management systems are used to protect assets.

23.1 Network and Server Profiling

Network Profiling

- Network and device profiling provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Elements of network profile:
  - Session duration
  - Total throughput
  - Critical asset address space
  - Typical traffic type



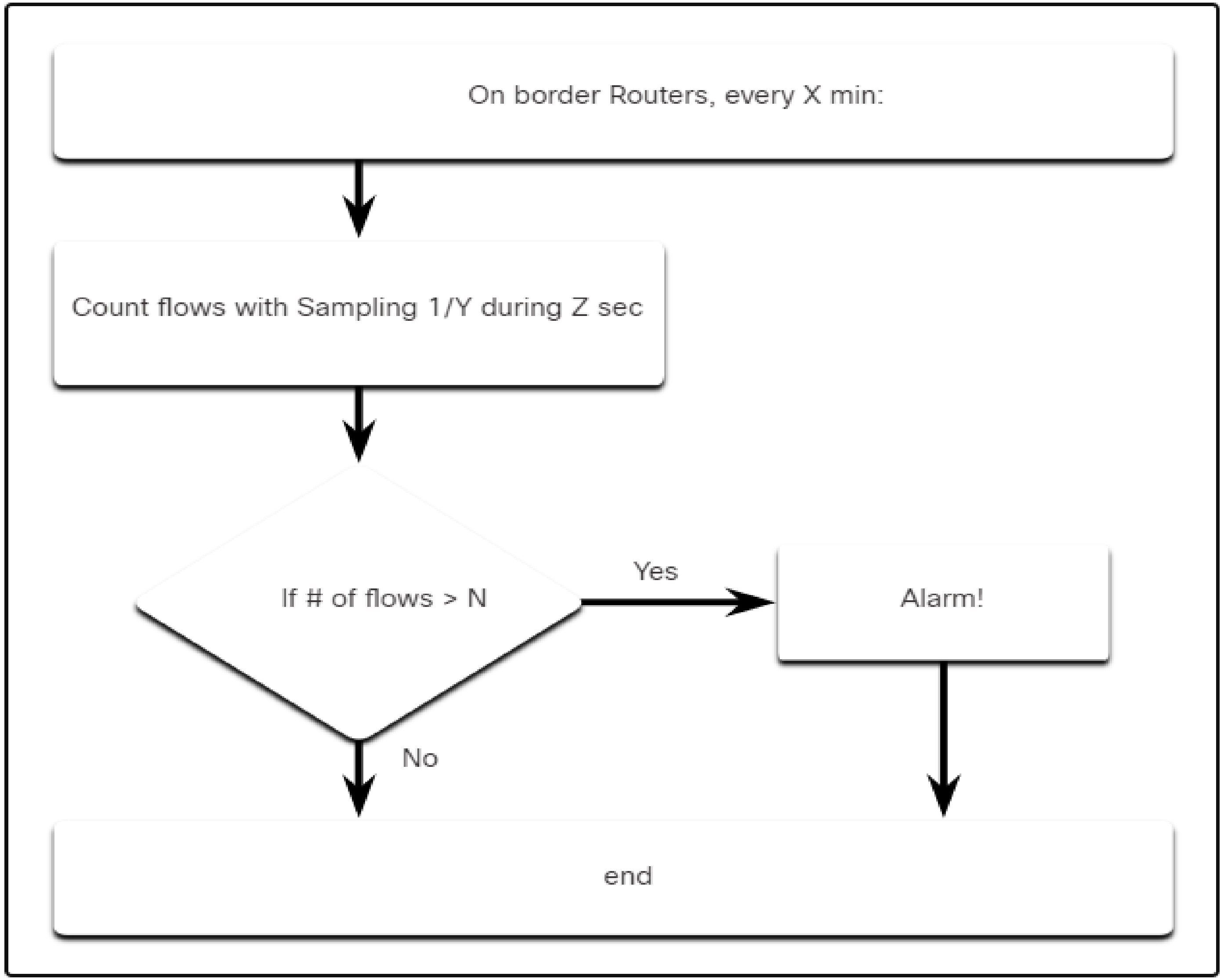
Elements of a Network Profile

Server Profiling

- A server profile is a security baseline for a given server.
- Server profiling is used to establish the accepted operating state of servers.
- The server profile elements are as follows:
  - Listening ports
  - Logged in users and accounts
  - Service accounts
  - Software environment

Network Anomaly Detection

- Network behavior is described by a large amount of diverse data such as the features of packet flow, features of the packets themselves, and telemetry from multiple sources.
- Big Data analytics techniques can be used to analyze this data and detect variations from the baseline.
- Anomaly detection can identify infected hosts on the network that are scanning for other vulnerable hosts.
- The figure illustrates a simplified version of an algorithm designed to detect an unusual condition at the border routers of an enterprise.



Network Vulnerability Testing

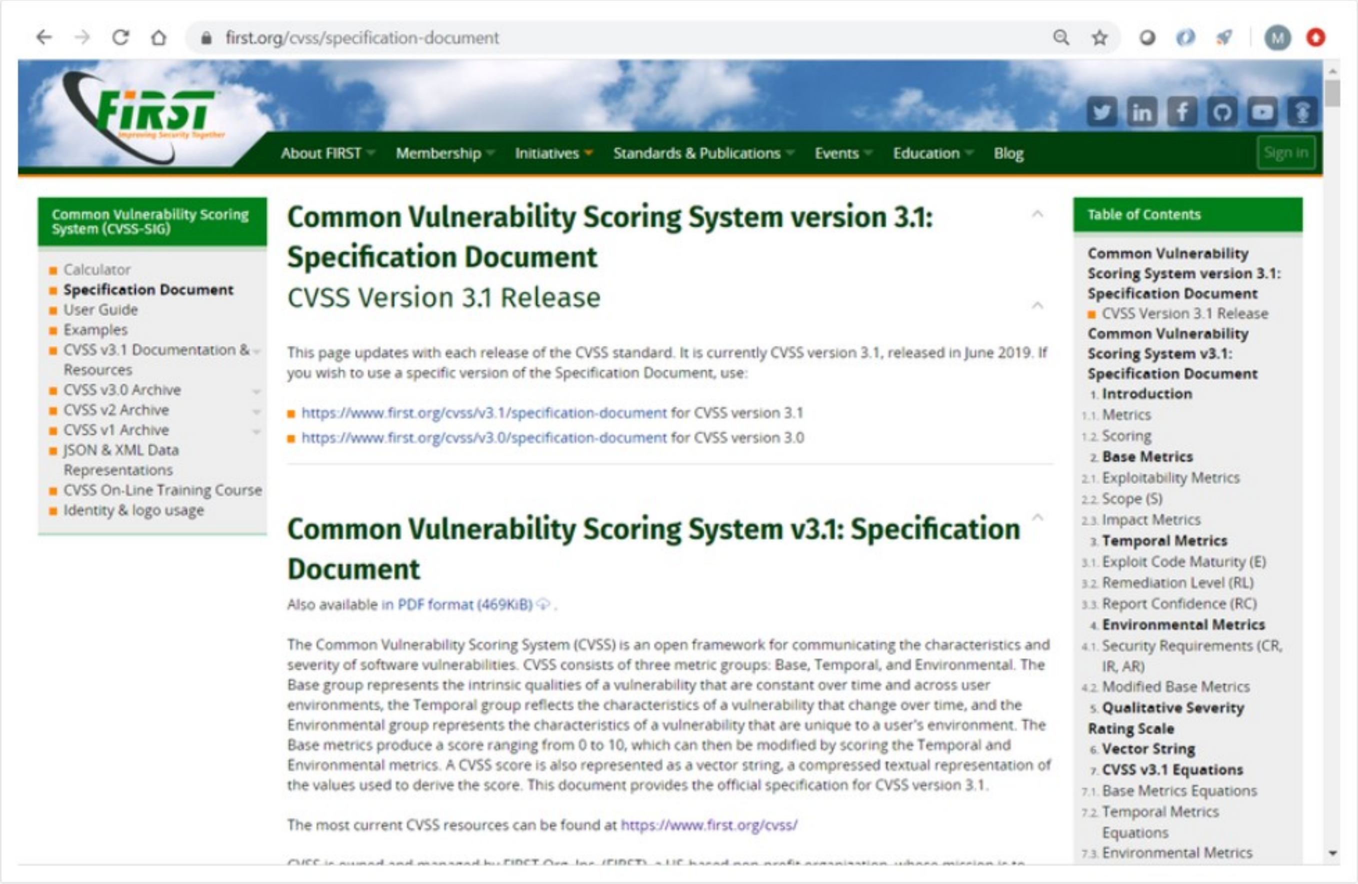
- Network Vulnerability Testing includes Risk Analysis, Vulnerability Assessment and Penetration Testing.
- The table lists examples of activities and tools that are used in vulnerability testing:

Activity	Description	Tools
Risk analysis	Individuals conduct comprehensive analysis of impacts of attacks on core company assets and functioning	Internal or external consultants, risk management frameworks
Vulnerability Assessment	Patch management, host scans, port scanning, other vulnerability scans and services	OpenVas, Microsoft Baseline Analyzer, Nessus, Qualys, Nmap
	Use of hacking techniques and tools to penetrate network	Metasploit, CORE

23.2 Common Vulnerability Scoring System (CVSS)

CVSS Overview

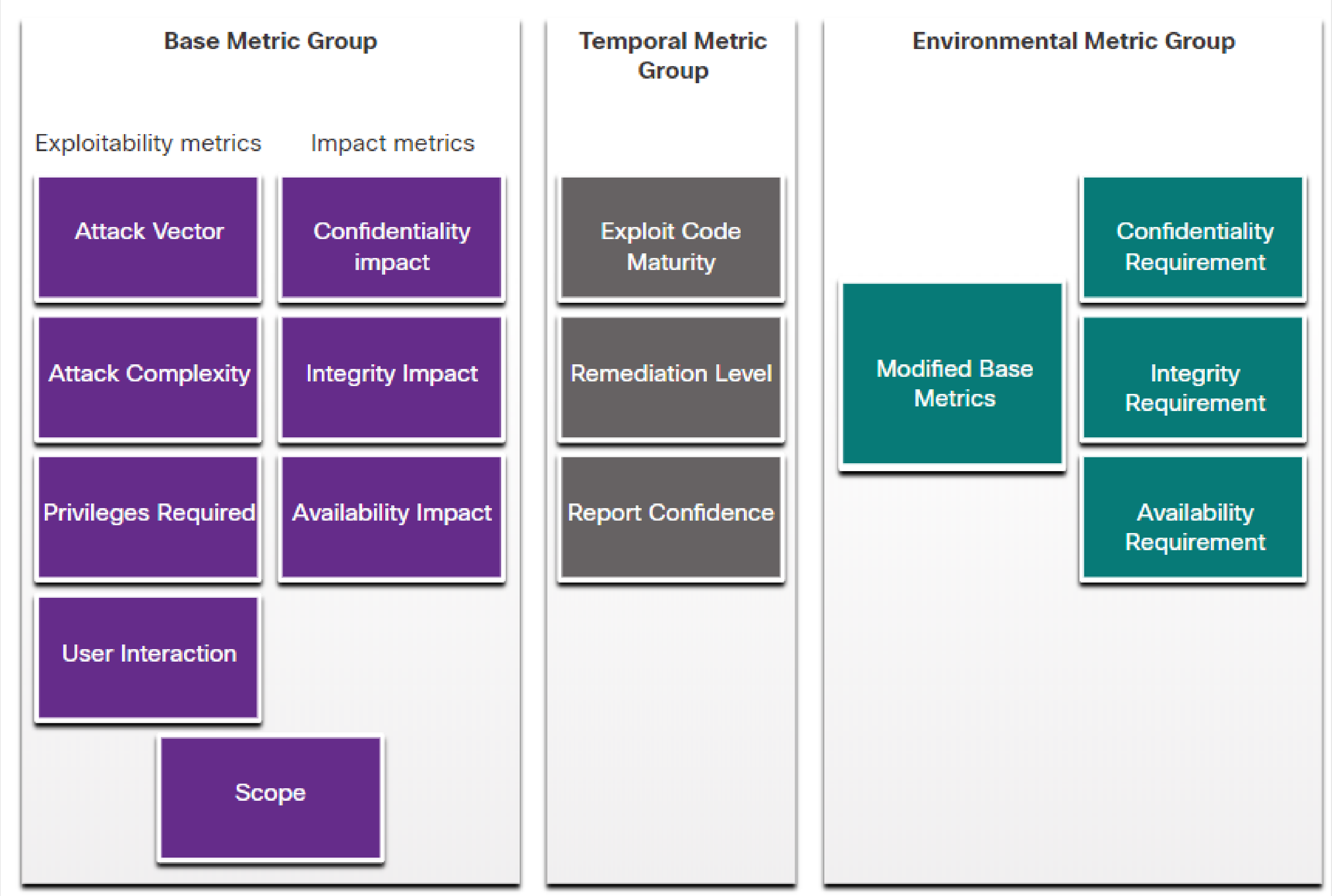
- The Common Vulnerability Scoring System (CVSS) is a risk assessment toc designed to convey the common attributes and severity of vulnerabilities i computer hardware and software systems.
- CVSS provides standardized vulnerabilit scores.
- It provides an open provides an open framework with metrics to all users.
- CVSS helps prioritize risk.
- The Forum of Incident Response and Security Teams (FIRST) has been designated as the custodian of the CVSS to promote its adoption globally.



Common Vulnerability Scoring System (CVSS)

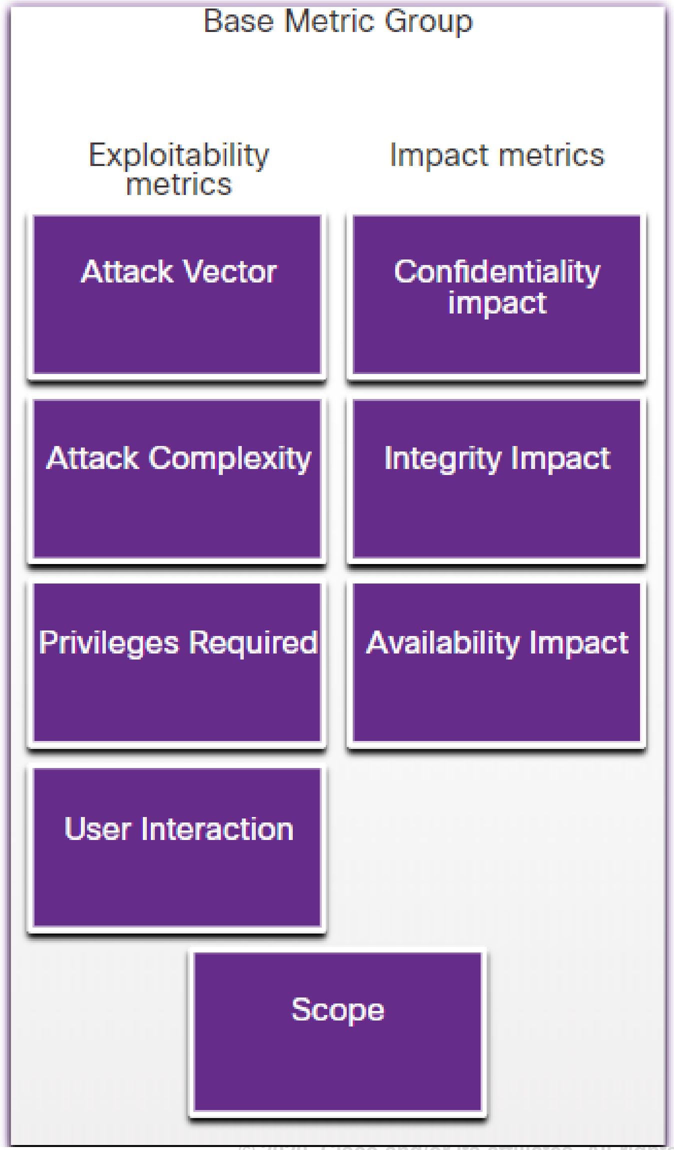
CVSS Metric Groups

- The CVSS uses three groups of metrics to assess vulnerability.
  - **Base Metric Group**: Represents the characteristics of a vulnerability that are constant over time and across contexts.
  - **Temporal Metric Group**: Measures the characteristics of a vulnerability that may change over time, but not across user environments.
  - **Environmental Metric Group**: Measures the aspects of a vulnerability that are rooted in a specific organization's environment.



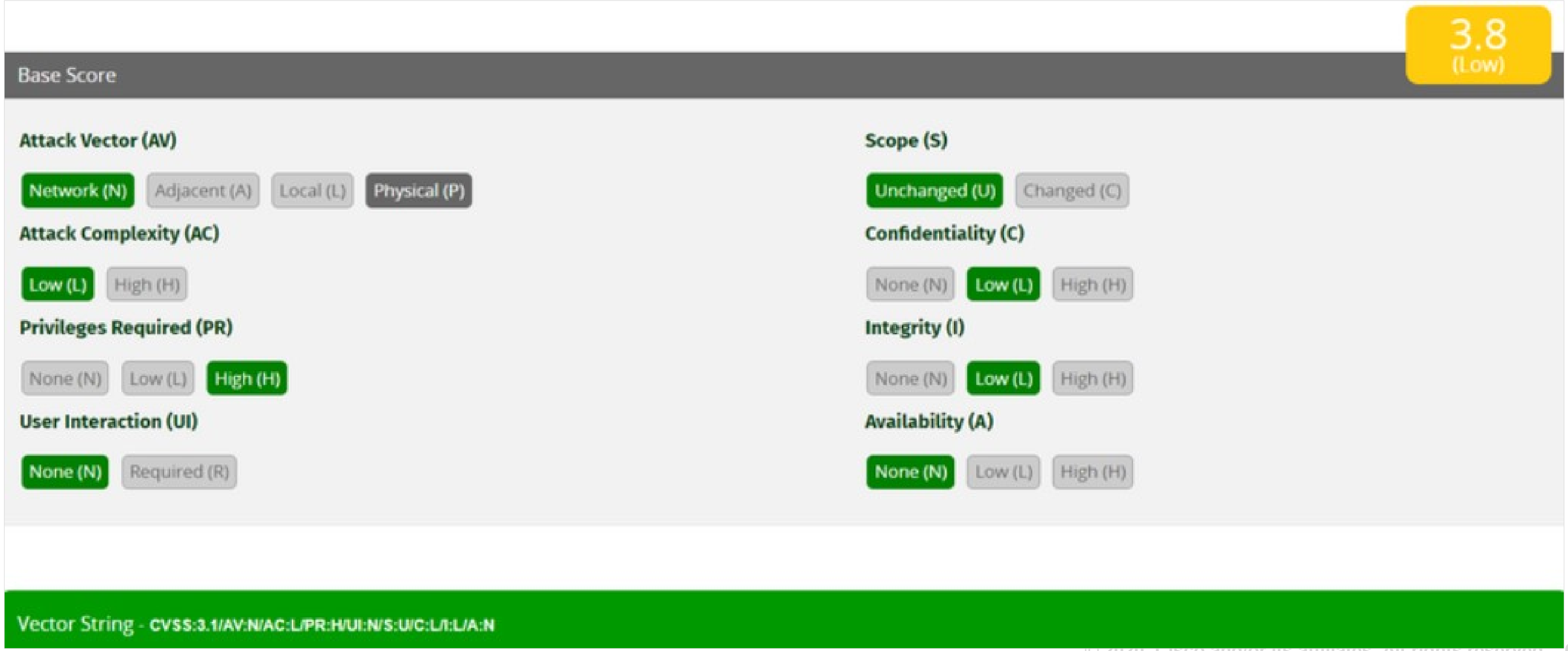
CVSS Base Metric Group

- Base Metric Group Exploitability metrics include the following criteria:
  - Attack vector
  - Attack complexity
  - Privileges required
  - User interaction
  - Scope
- Base Metric Group Impact metrics components include the following criteria:
  - Confidentiality Impact
  - Integrity Impact
  - Availability Impact



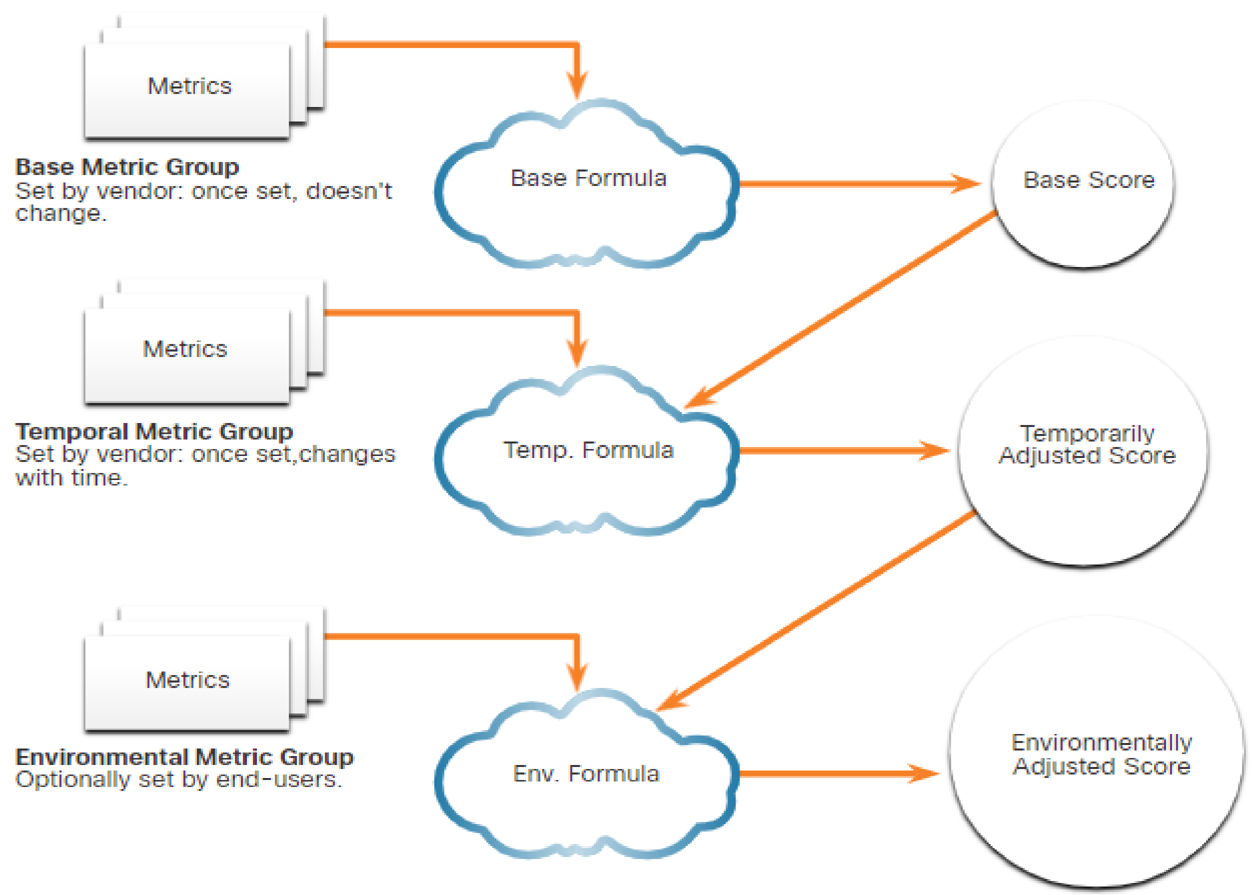
The CVSS Process

- The CVSS process uses a tool called the CVSS v3.1 Calculator.
- The calculator is like a questionnaire in which the choices are made that describe the vulnerability for each metric group.
- Later, a score is generated and numeric severity rating is displayed.



The CVSS Process (Contd.)

- After the Base Metric group is completed, the Temporal and Environmental metric values modify the Base Metric results to provide an overall score.



Source: www.first.org

CVSS Reports

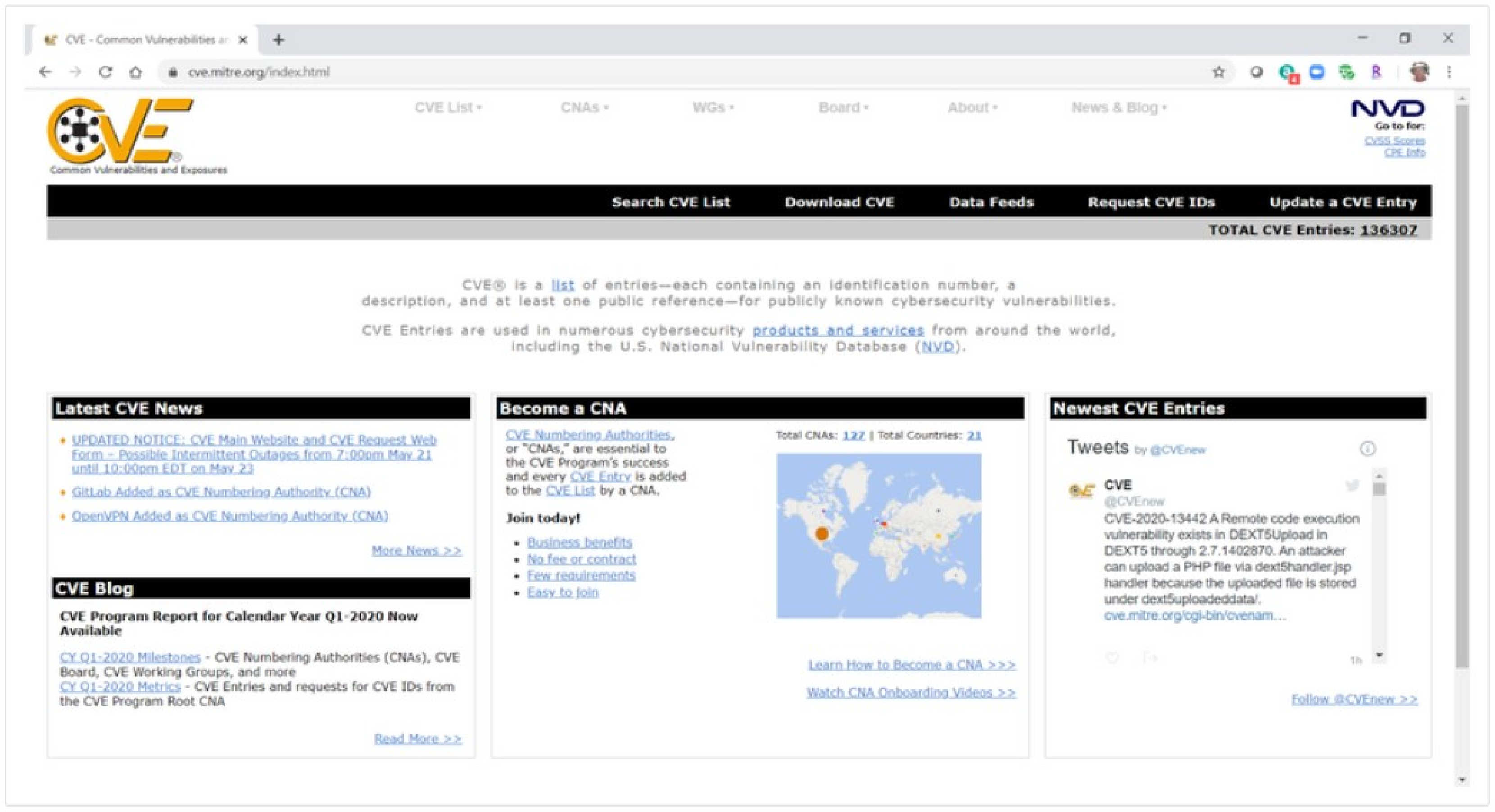
- The higher the severity rating, the greater the potential impact of an exploit and the greater the urgency in addressing the vulnerability.
- Any vulnerability that exceeds 3.9 should be addressed.
- The ranges of scores and the corresponding qualitative meaning is shown in the table:

Rating	CVSS Score
None	0
Low	0.1 – 3.9
Medium	4.0 – 6.9
High	7.0 – 8.9
Critical	9.0 – 10.0

Other Vulnerability Information Sources

Common Vulnerabilities and Exposures (CVE):

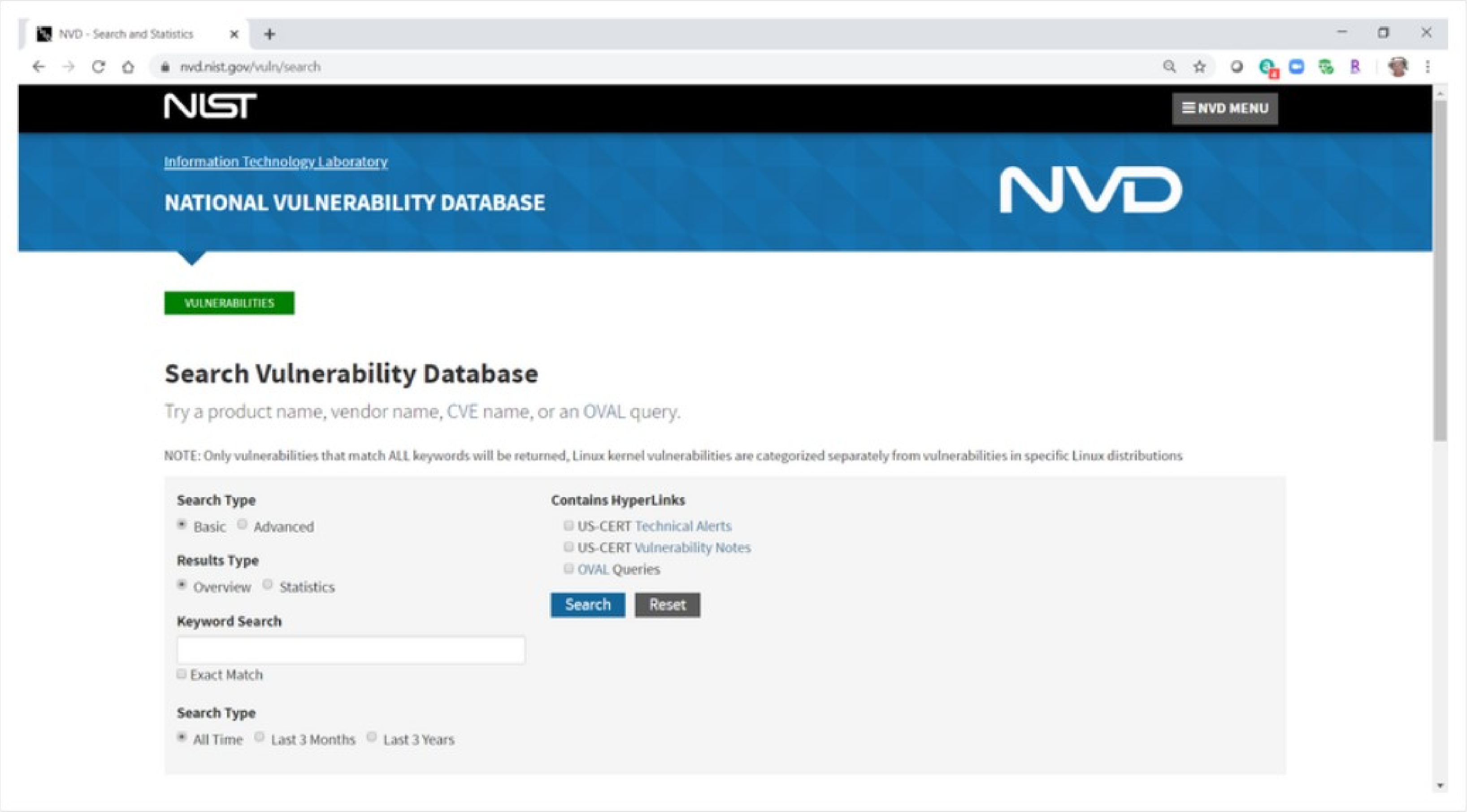
- CVE identifier provides a standard way to research a reference to vulnerabilities.
- Threat intelligence services use CVE identifiers, and they appear in various security system logs.
- The CVE Details website provides a linkage between CVSS scores and CVE information.



Other Vulnerability Information Sources (Contd.)

National Vulnerability Database (NVD):

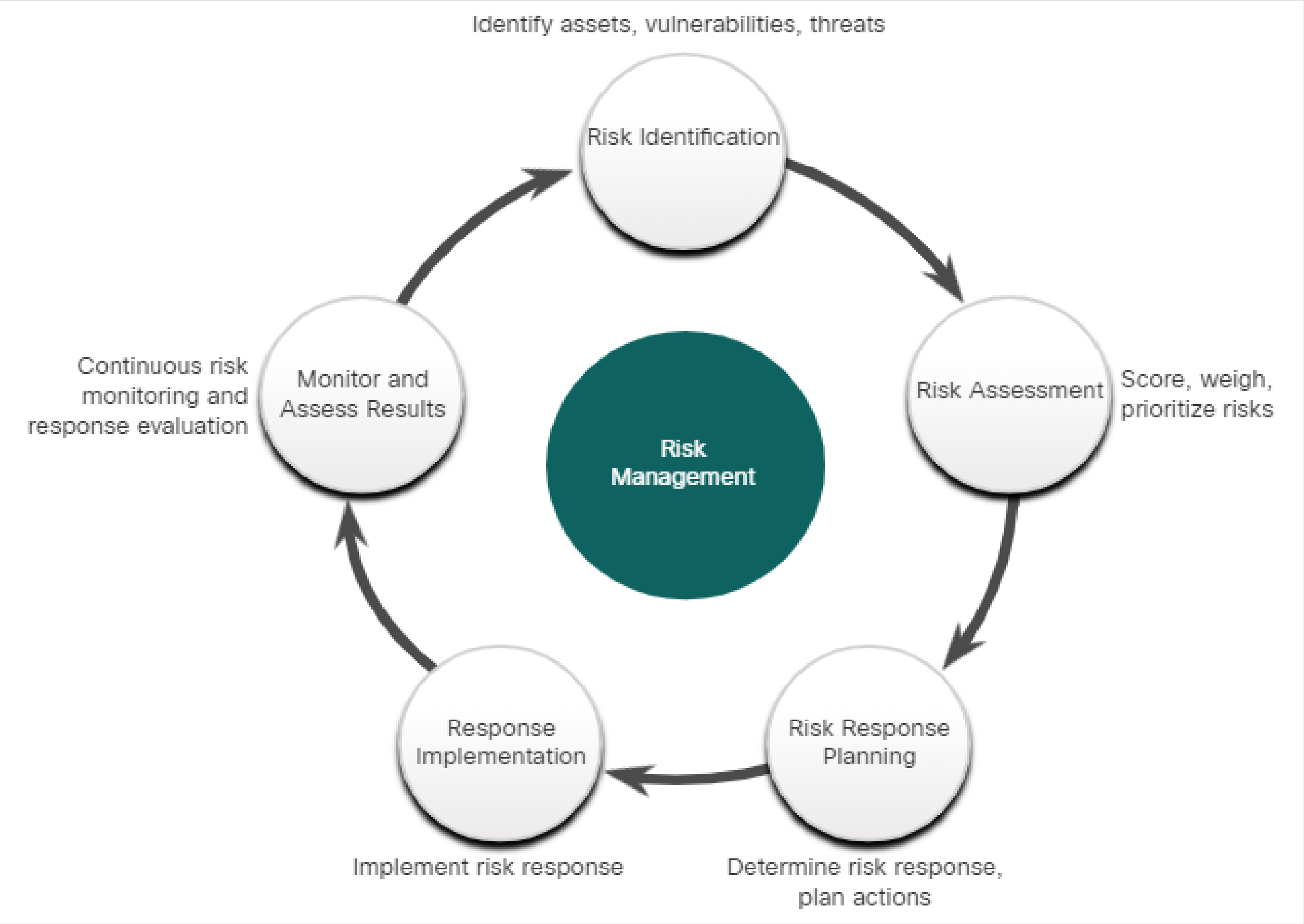
- This utilizes CVE identifiers and supplies additional information on vulnerabilities such as CVSS threat scores, technical details, affected entities, and resources for further investigation.
- The database was created and is maintained by the U.S. government National Institute of Standards and Technology (NIST) agency.



23.3 Secure Device Management

Risk Management

- Risk management involves the selection and specification of security controls for an organization.
- A mandatory activity in risk assessment is to identify threats and vulnerabilities.
- Ways to respond to identified risks:
  - **Risk avoidance** - Stop performing the activities that create risk.
  - **Risk reduction** - Take measures to reduce vulnerability.
  - **Risk sharing** - Shift some risk to other parties.
  - **Risk retention** - Accept the risk and its consequences.



Vulnerability Management

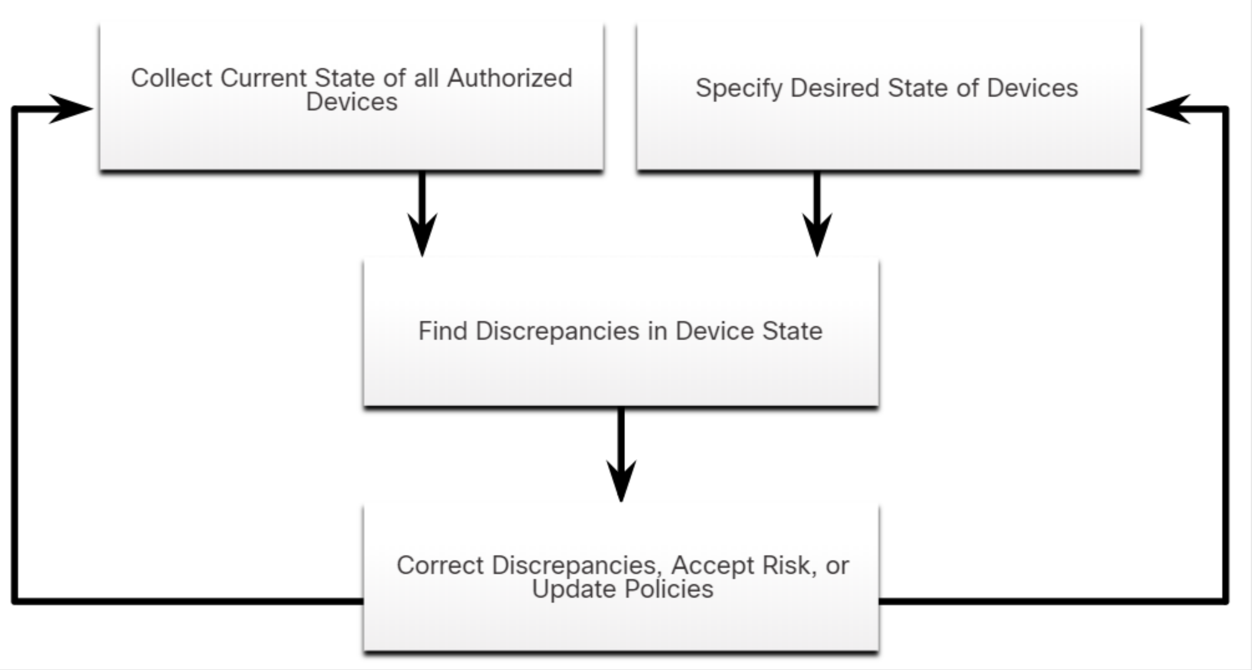
- Vulnerability management is a security practice designed to proactively prevent the exploitation of IT vulnerabilities.
- The steps in the Vulnerability Management Life Cycle:
  - **Discover** - Develop a network baseline. Identify security vulnerabilities on a regular automated schedule.
  - **Prioritize Assets** - Categorize assets into groups or business units, and assign a business value based on their criticality to business operations.
  - **Assess** - Determine a baseline risk profile to eliminate risks based on asset criticality, vulnerability, threats, and asset classification.

Vulnerability Management (Contd.)

- **Report** - Measure the level of business risk associated with your assets according to your security policies. Document a security plan, monitor suspicious activity, and describe known vulnerabilities.
- **Remediate** - Prioritize according to business risk and address vulnerabilities in order of risk.
- **Verify** - Verify that threats have been eliminated through follow-up audits.

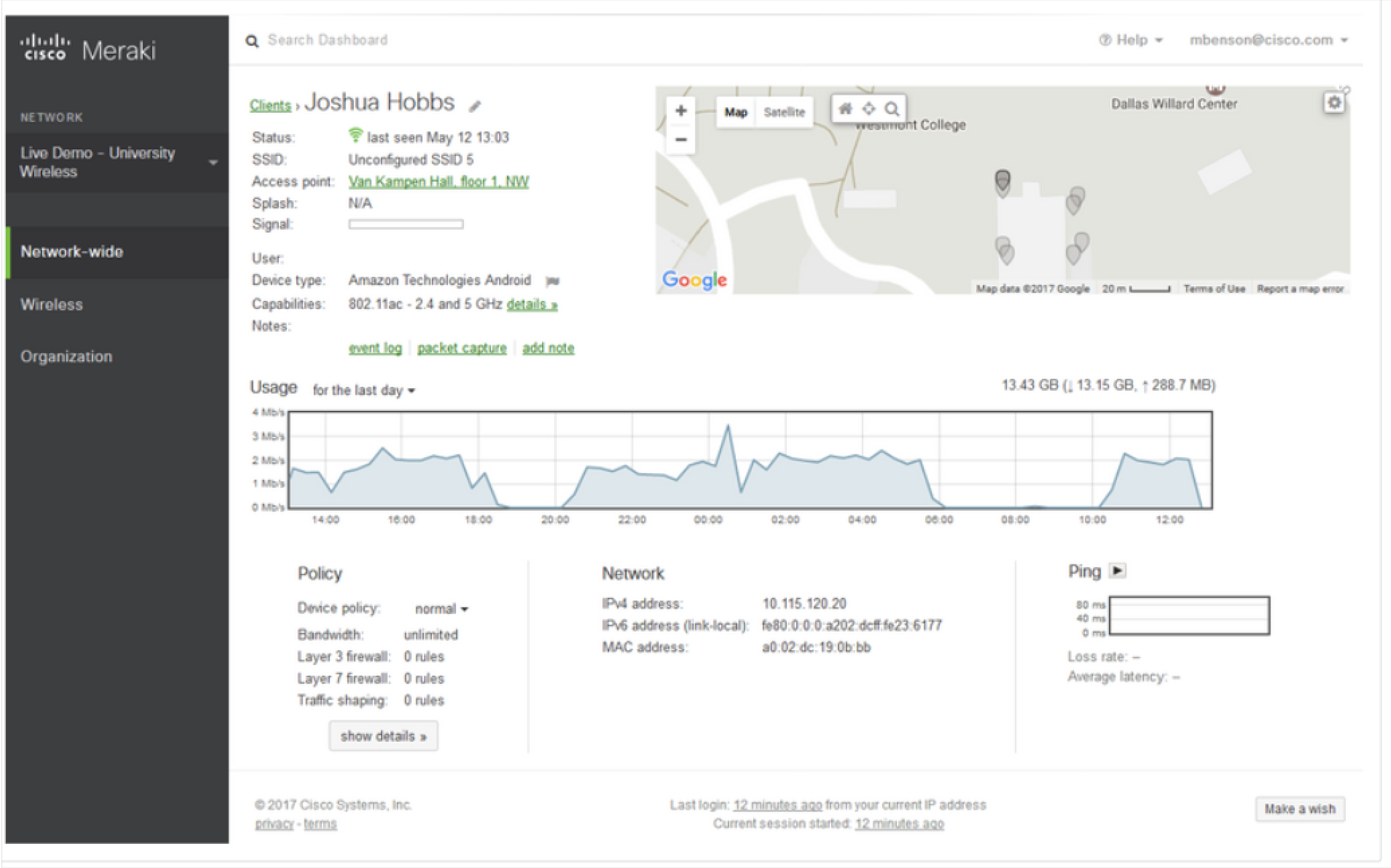
Asset Management

- Asset management involves the implementation of systems that track the location and configuration of networked devices and software across an enterprise.
- **Tools and Techniques for Asset management:**
  - Automated discovery and inventory of the actual state of devices
  - Articulation of the desired state for those devices using policies, plans, and procedures in the organization's information security plan
  - Identification of non-compliant authorized assets
  - Remediation or acceptance of device state, possible iteration of desired state definition
  - Repeat the process at regular or ongoing intervals



Mobile Device Management

- Mobile devices cannot be physically controlled on the premises of an organization.
- MDM systems, such as Cisco Meraki Systems Manager, allows the security personnel to configure, monitor and update a very diverse set of mobile clients from the cloud.



Configuration Management

- **Configuration Management**: As defined by NIST, configuration management:

  Comprises a collection of activities focused on establishing and maintaining the integrity of products and systems, through control of the processes for initializing, changing, and monitoring the configurations of those products and systems.

- **Configuration tools** : Puppet, Chef, Ansible, and SaltStack

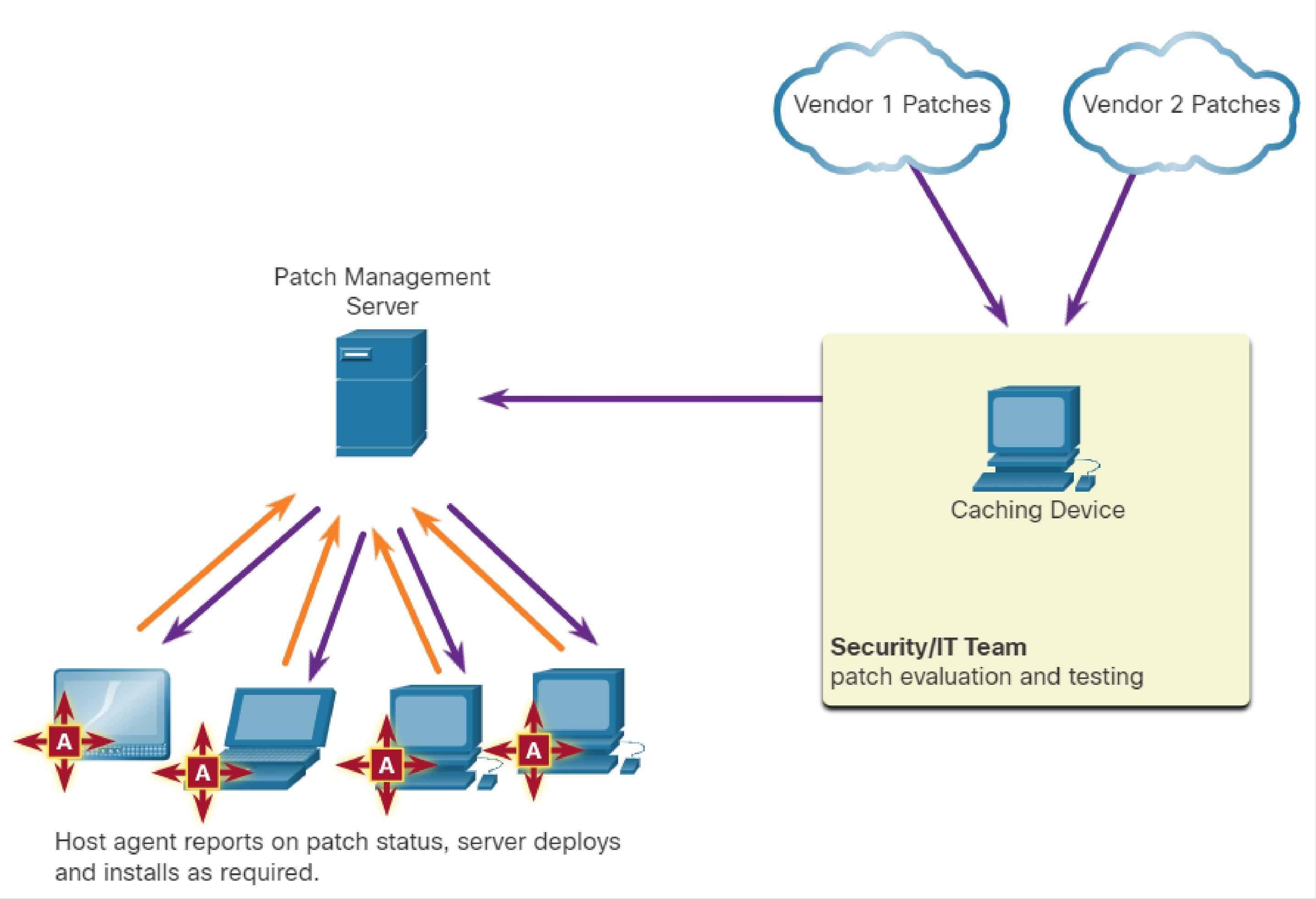
Enterprise Patch Management

- Patch management involves all aspects of software patching, including identifying required patches, acquiring, distributing, installing, and verifying.
- Patch management is required by some compliance regulations such as Sarbanes Oxley (SOX) and the Health Insurance Portability and Accountability Act (HIPAA).

Patch Management Techniques

Agent-based:

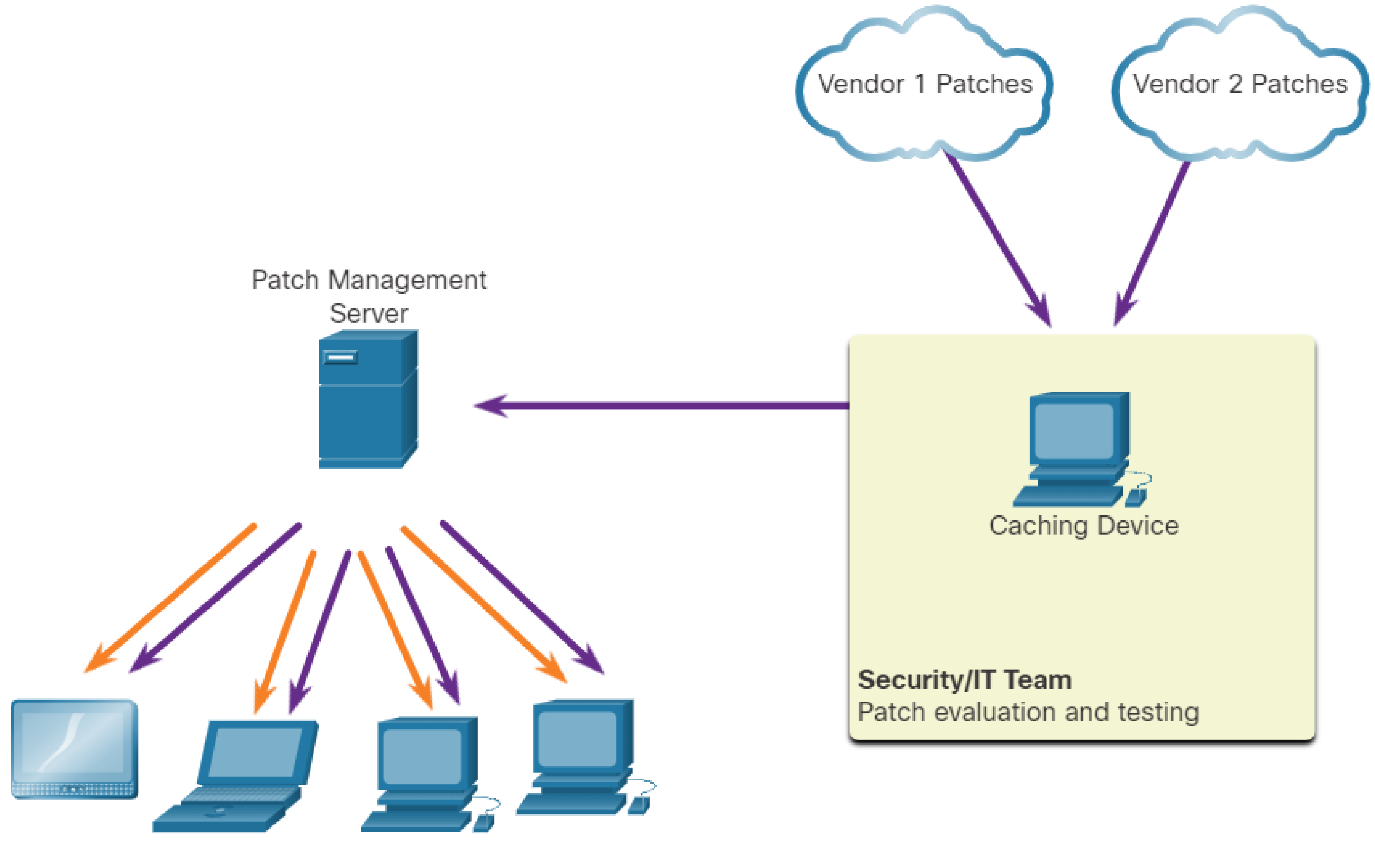
- This requires a software agent to be running on each host to be patched.
- The agent reports whether vulnerable software is installed on the host.
- The agent communicates with the patch management server and determines if patches exist that require installation, and installs the patches.
- Agent-based approaches are the preferred means of patching mobile devices.



Patch Management Techniques

Agentless Scanning:

- Patch management servers scan the network for devices that require patching.
- The server determines which patches are required and installs those patches on the clients.
- Only devices that are on scanned network segments can be patched, which can be a problem for mobile devices.

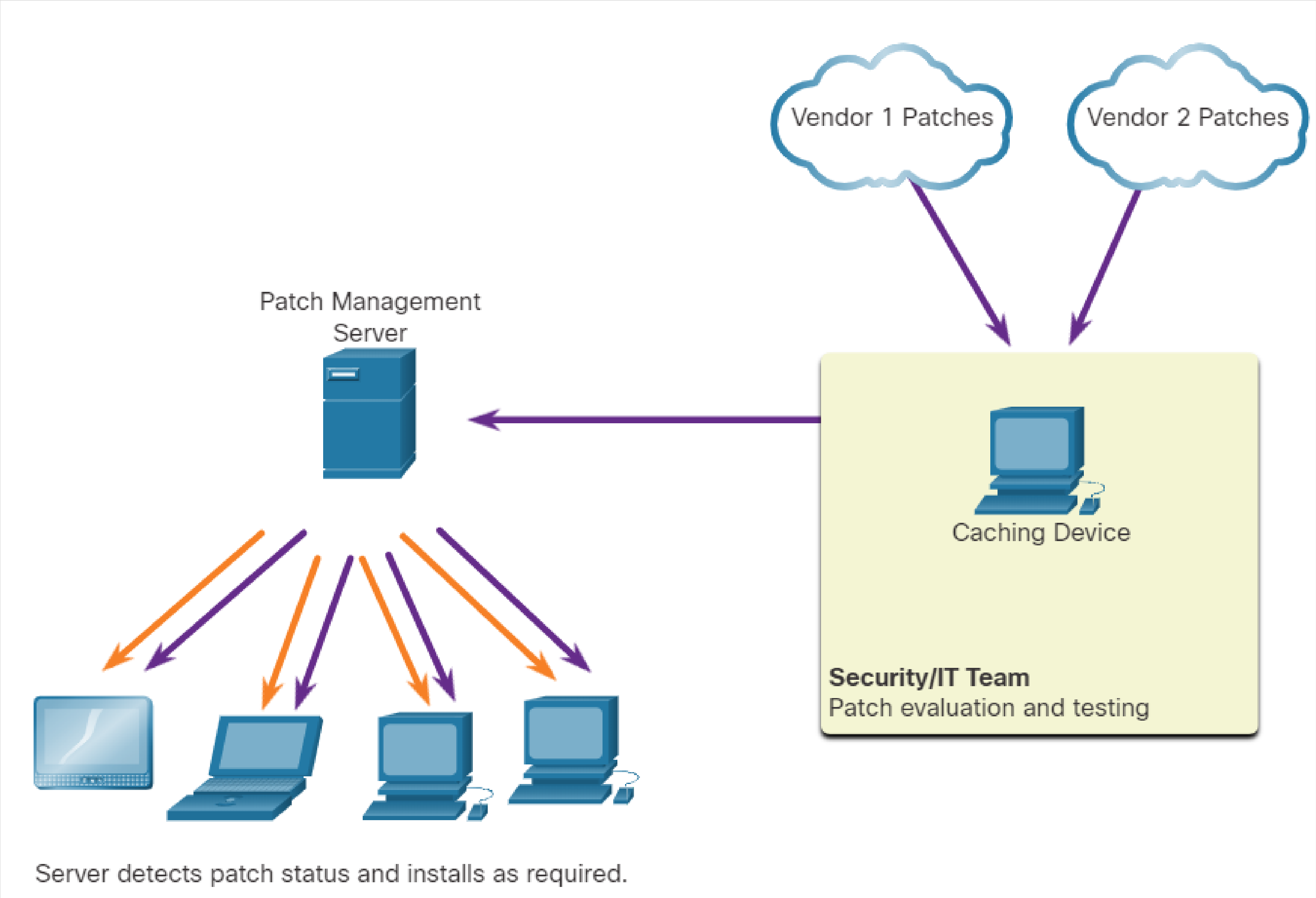


Server detects patch status and installs as required.

Patch Management Techniques

Passive Network Monitoring:

- Devices requiring patching are identified through the monitoring of traffic on the network.
- This approach is only effective for software that includes version information in its network traffic.

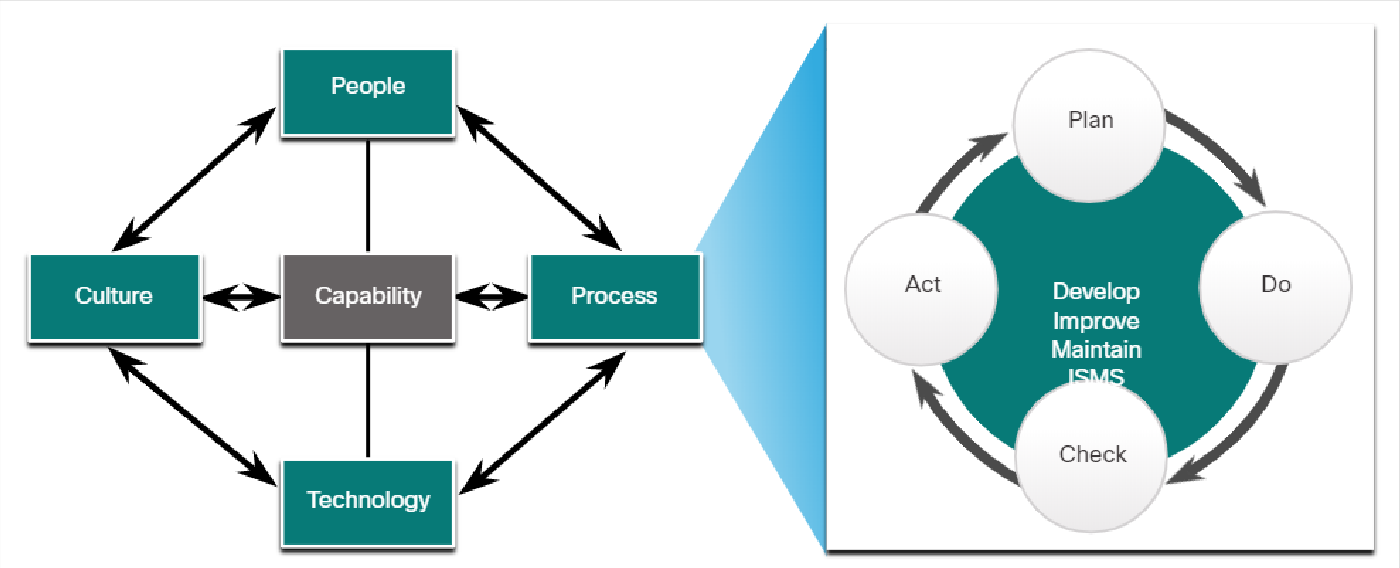


23.4 Information Security Management Systems

Security Management Systems

- An Information Security Management System (ISMS) consists of a management framework to identify, analyze, and address information security risks.

- ISMSs provide conceptual models that guide organizations in planning, implementing, governing, and evaluating information security programs.
- It incorporates the “plan-do-check-act” framework, known as the Deming cycle.
- ISM is seen as an elaboration on People-Process-Technology-Culture model of organizational capability



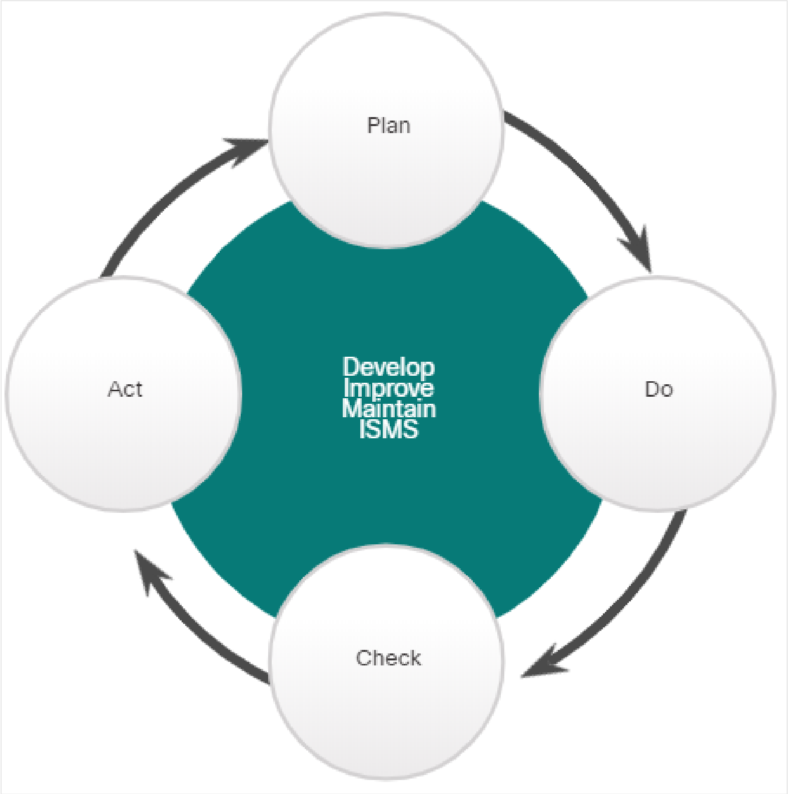
A General Model for Organizational Capability

Information Security Management Systems

ISO-27001

- ISO/IEC 27000 family of standards – internationally accepted standards that facilitate business conducted between countries. The ISO 27001 - global, industry-wide specification for an ISMS.

Plan	Do	Check	Act
• Understand business objectives • Define activities scope • Access and manage support • Assess and define risk • Perform asset management and vulnerability assessment	• Create and implement risk management plan • Establish and enforce risk management policies and procedures • Train personnel, allocate resources	• Monitor exécution • Compile reports • Support external certification audit	• Continually audit processes • Continually improve processes • Take corrective action • Take preventive action



NIST Cybersecurity Framework

- **NIST Cybersecurity Framework** – is a set of standards designed to integrate existing standards, guidelines, and practices to help better manage and reduce cybersecurity risk.
- The below table describes the core functions in NIST Cybersecurity Framework:

Core Function	Description
IDENTIFY	Develop an organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.
PROTECT	Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.
DETECT	Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.
RESPOND	Develop and implement the appropriate activities to act on a detected cybersecurity event.
RECOVER	Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

23.5 Endpoint Vulnerability Assessment Summary

Endpoint Vulnerability Assessment Summary

- Network and device profiling provides statistical baseline information that can serve as a reference point for normal network and device performance.
- Network security can be evaluated using a variety of tools and services.
- Vulnerability assessment uses software to scan Internet-facing servers and internal networks for various types of vulnerabilities.
- The Common Vulnerability Scoring System (CVSS) is a vendor-neutral, industry standard, open framework for rating the risks of a given vulnerability by using a variety of metrics to calculate a composite score.
- Vulnerabilities are rated according to the attack vector, attack complexity, privileges required, user interaction, and scope.
- Risk management involves the selection and specification of security controls for an organization.

Endpoint Vulnerability Assessment Summary (Contd.)

- Vulnerability management is a security practice that is designed to proactively prevent the exploitation of IT vulnerabilities that exist within an organization.
- Organizations can use an Information Security Management System (ISMS) to identify, analyze, and address information security risks.
- Standards for managing cybersecurity risk are available from ISO and NIST.
- NIST has also developed the Cybersecurity Framework, which is similar to the ISO/IEC 27000 standards.

Module 24:
Technologies and Protocols

Module Objective: Explain how security technologies affect security monitoring.

Topic	Topic Objective
Monitoring Common Protocols	Explain the behavior of common network protocols in the context of security monitoring.
Security Technologies	Explain how security technologies affect the ability to monitor common network protocols.

24.1 Monitoring Common Protocols

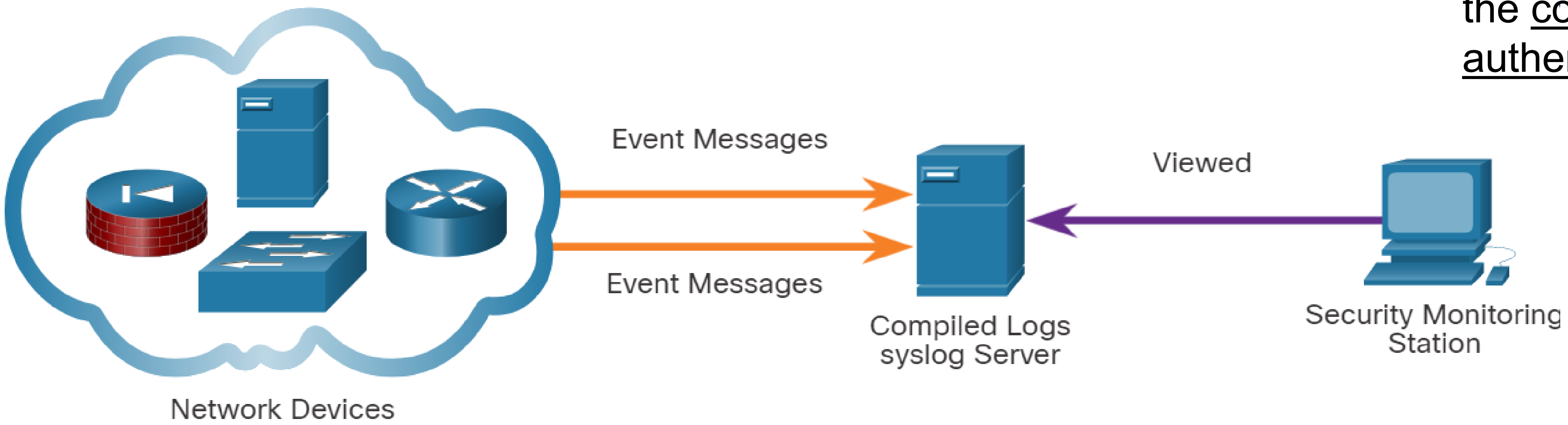
Technologies and protocols

Syslog and NTP

- Syslog and Network Time Protocol (NTPv4) are **essential** to the work of the cybersecurity **analyst**.

The **syslog** standard

- is used for logging event messages from network devices and endpoints.
- allows for a system-neutral means of transmitting, storing, and analyzing messages.
- Many types of devices from many different vendors can use syslog to send log entries to **central servers** that run a **syslog daemon**.
  - This centralization of log collection helps to make security monitoring practical.
  - Servers that run syslog typically listen **on UDP port** 514.



Network Time Protocol (**NTP**)

- Syslog messages are usually timestamped
- messages come from many devices => important that the devices share a consistent timeclock - achieved by NTP

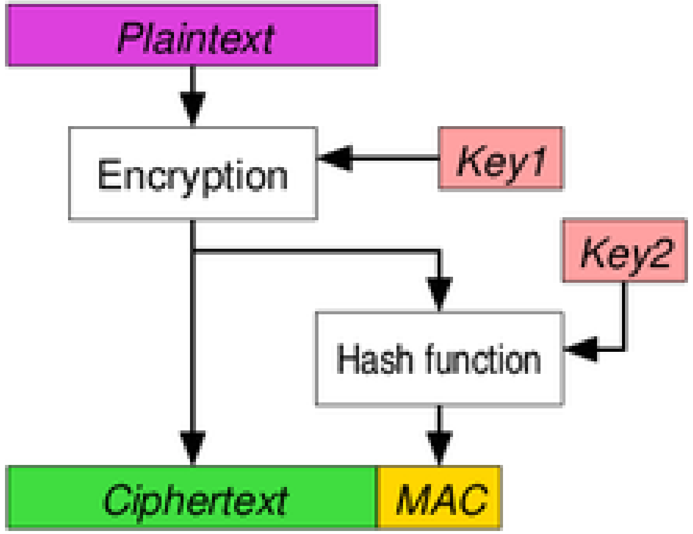
Network Time Security (**NTS**)

- secure version of NTP
  - with **TLS** and **AEAD**
- Authenticated Encryption with Associated Data (AEAD)
  - form of encryption which simultaneously assure the confidentiality and authenticity of data

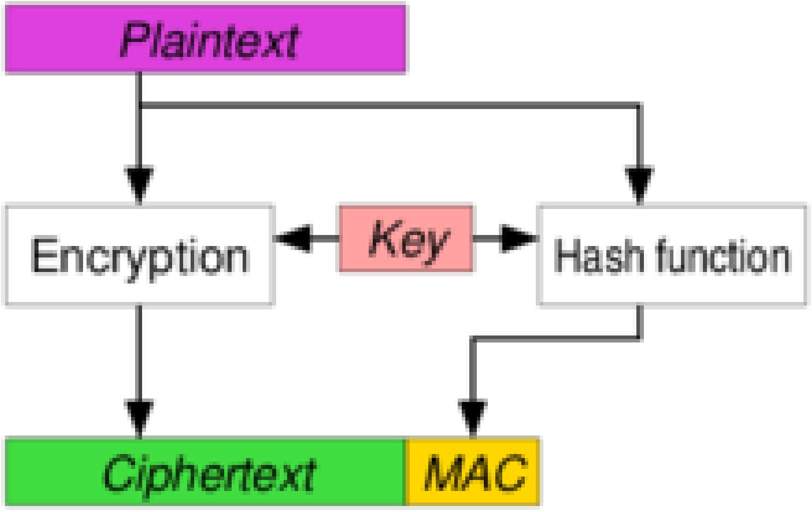
AEAD - Authenticated Encryption with Associated Data

- required, for example, by network packets or frames where
  - the **header** needs visibility
  - the **payload** needs confidentiality
  - and **both** need integrity and authenticity
- MAC = message authentication code

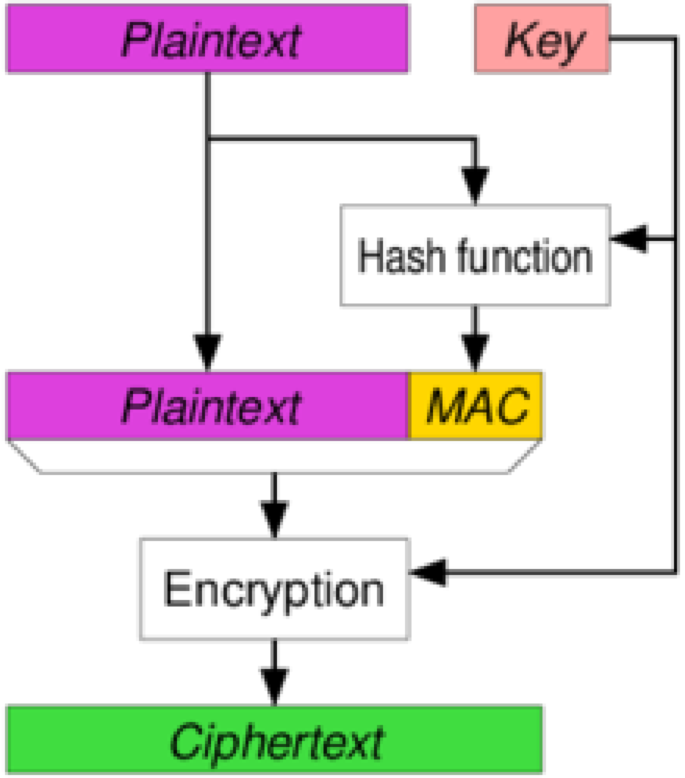
Encrypt-then-MAC (EtM)
used in SSHv2



Encrypt-and-MAC (E&M)
used in SSH



MAC-then-Encrypt (MtE)
used in TLS/SSL



https://en.wikipedia.org/wiki/Authenticated_encryption

Syslog attacks

WHAT:

- syslog is so important to security monitoring
  - => syslog servers may be a target for threat actors.

WHY:

- **data exfiltration** can take a long time to complete
  - due to the very slow ways in which data is secretly stolen from the network.
  - => attackers may try to hide the fact that exfiltration is occurring
    - attack the syslog servers
    - that contain the information that could lead to detection of the exploit.

HOW:

- Hackers may attempt
  - to block the transfer of data from syslog clients to servers
  - tamper with *(zasiahnuť do)* or destroy log data
  - tamper with the software that creates and transmits log messages.

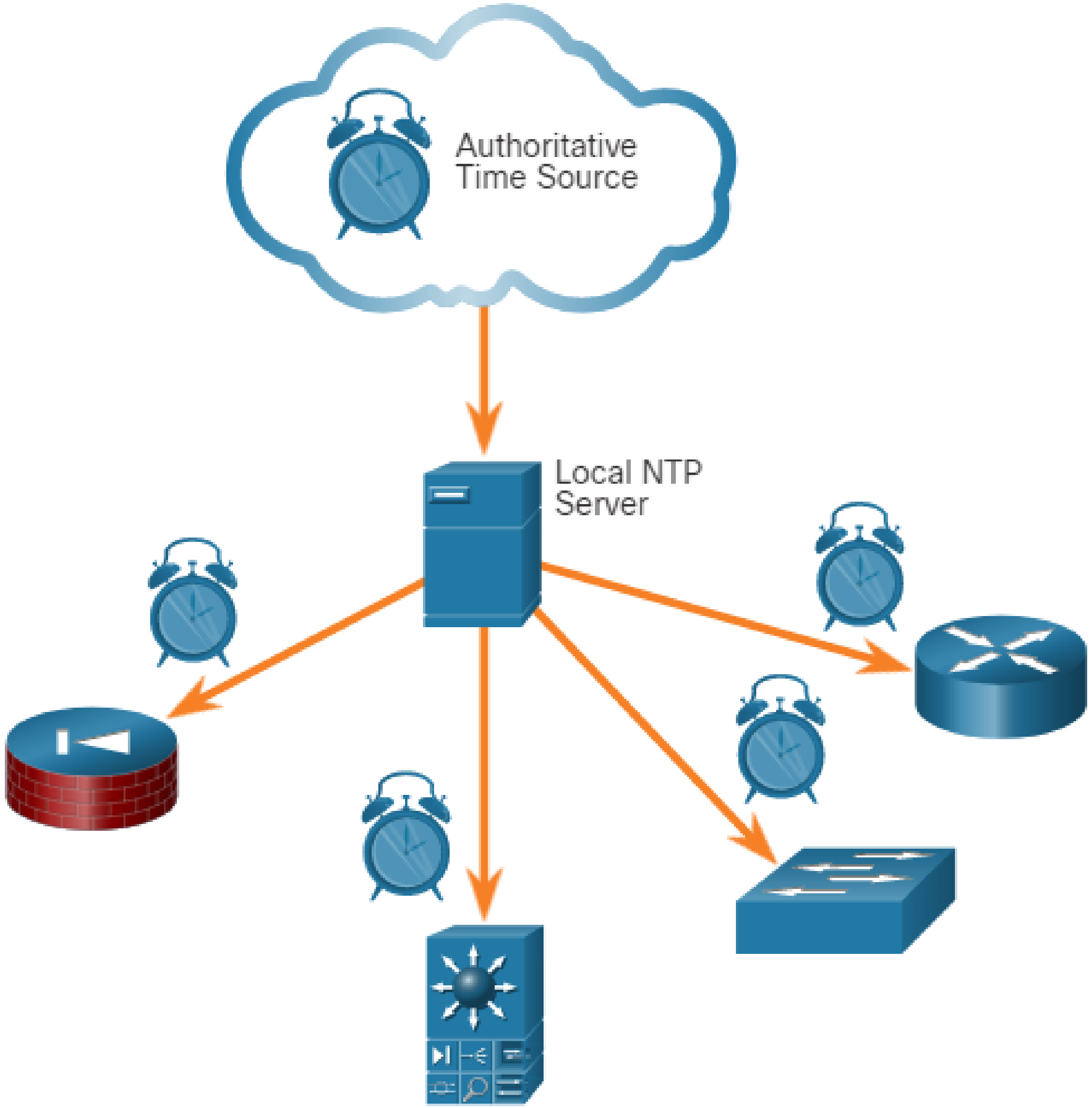
DEFENCE:

- The next generation (ng) syslog implementation, known as syslog-ng, offers enhancements that can help prevent some of the exploits that target syslog.

NTP attacks

- NTP (udp, port 123) uses a hierarchy of **authoritative** time sources
  - => to **share** time information between devices on the network
- Threat actors may attempt
  - **to attack** the NTP infrastructure
    - to corrupt time information used to correlate logged network events
      - Expirated certificate for web… and others
  - **to use** NTP systems
    - to direct DDoS attacks through vulnerabilities in client or server software

    = NTP amplification attack



NTP amplification attack

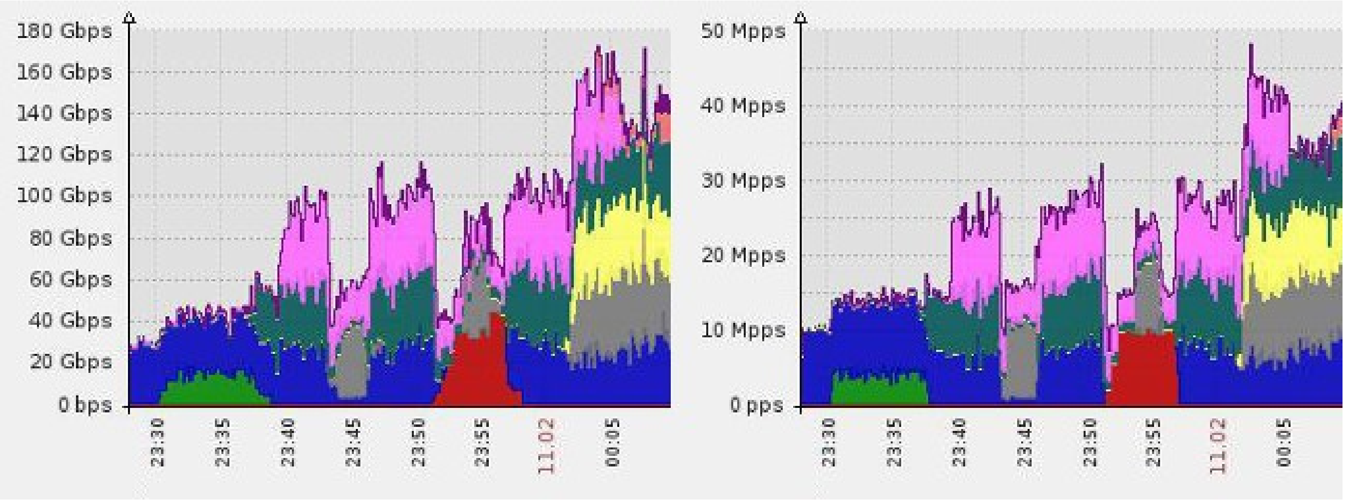
WHAT:

- a type of DDoS attack
  - the attacker exploits publically-accessible NTP servers to overwhelm the target (victim) with UDP traffic

HOW:

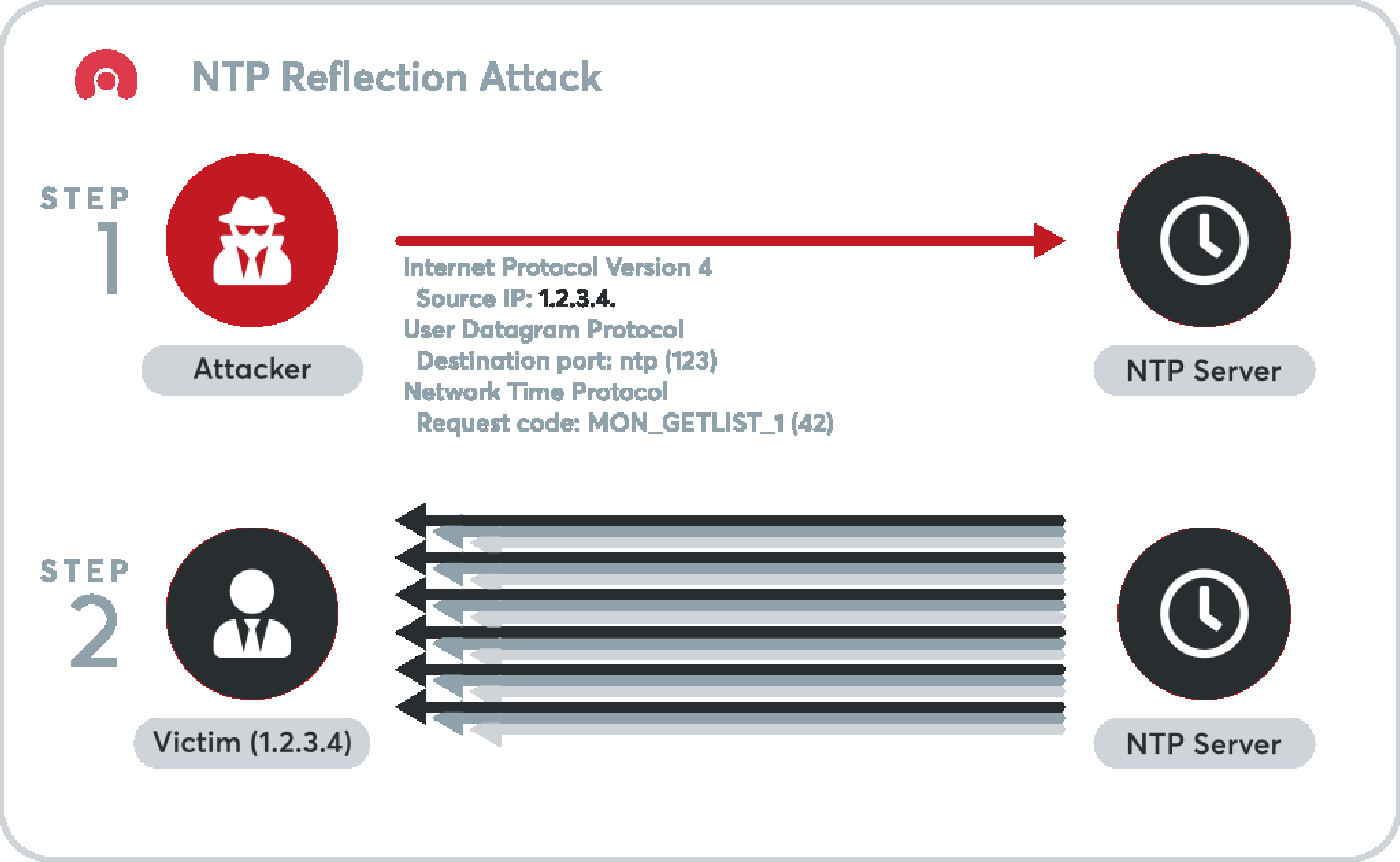
- In addition to clock synchronization, older versions of NTP support a monitoring service
  - enables administrators to query NTP server for a traffic count
    - command “get monlist”

      => sends the requester a list of the last 600 hosts
      - that connected to the queried server
    - Response >> request
      - ratio of query size to response size is between 20:1 and 200:1



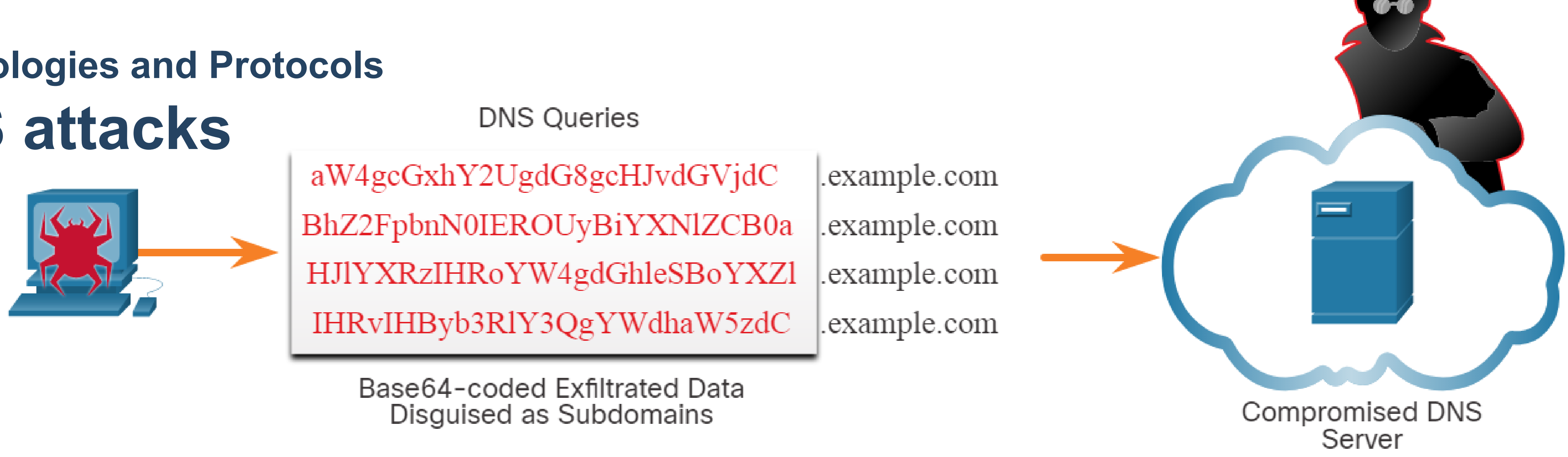
- IMPACT:
- attacker who controls 1 machine with 1Gbps could effectively direct 200Gbps of traffic toward the targeted server
- DEFENSE:
- Challenging: ostensibly legitimate traffic from valid servers
- **overprovisioning and traffic filtering**
- **scrubbing (deflect and** absorb**)**

NTP amplification attack



Technologies and Protocols

DNS attacks



WHAT:

- used by many types of malware
  - some use DNS to communicate with command-and-control (CnC) servers and to exfiltrate data in traffic disguised *(zamaskované)* as normal DNS queries.

HOW:

- Malware could encode stolen data as the subdomain portion of a DNS lookup
  - for a domain where the nameserver is under control of an attacker
- DNS lookup for ‘long-string-of-exfiltrated-data.example.com’ would be forwarded to the nameserver of example.com (attacker)
  - which would record ‘long-string-of-exfiltrated-data’ and reply back to the malware with a coded response
  - exfiltrated data is the encoded text shown in the box. The threat actor collects the encoded data, decodes and combines it, and now has access to an entire data file.

Technologies and Protocols

DNS

ANALYSIS:

- It is likely that the subdomain part of such requests would be
  - **much longer** than usual requests.
- Cyber analysts can use the **distribution** of the lengths of subdomains within DNS requests
  - to construct a mathematical model that describes **normality** *(normálnosť)*

DEFENSE:

- What to consider as suspicious:
  - DNS queries for **randomly generated** domain names
  - **extremely long** random-appearing subdomains
    - Better: Non-normality (math model)
  - especially if their **occurrence spikes** dramatically on the network.
- **DNS proxy logs** can be analyzed to detect these conditions.
- Alternatively, services such as the Cisco Umbrella passive DNS service can be used to **block requests** to suspected CnC and exploit domains.

Technologies and Protocols

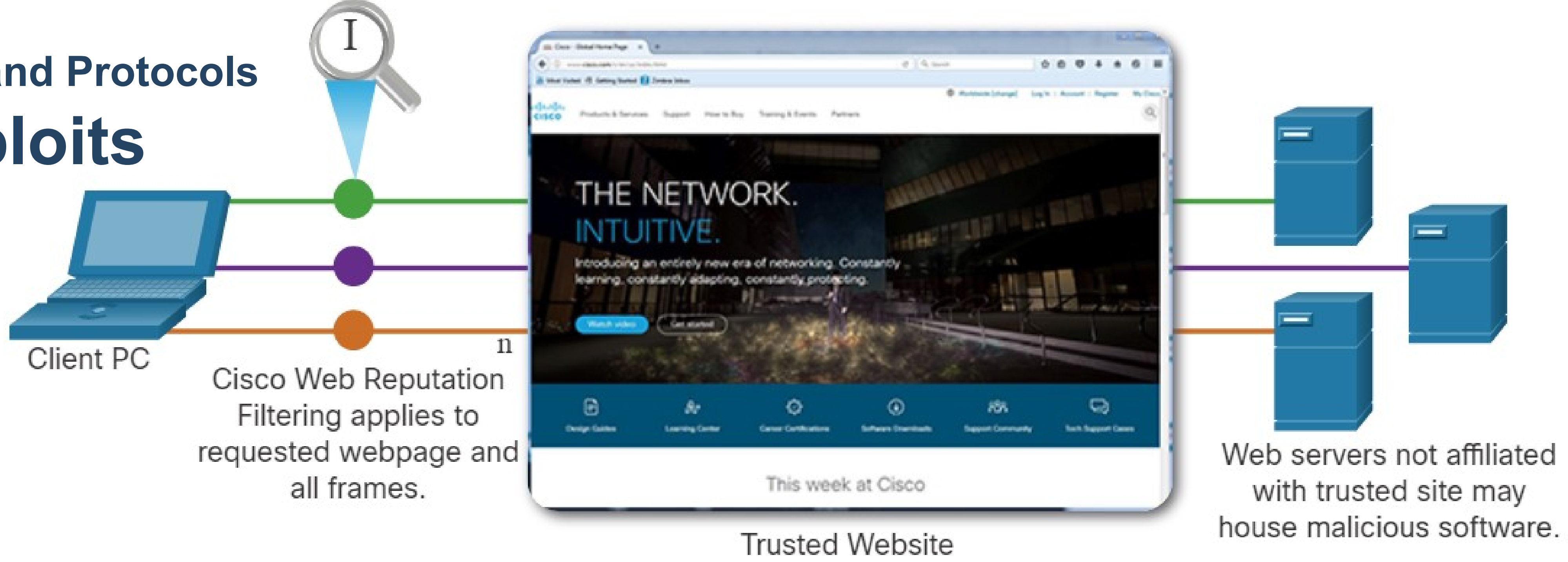
HTTP

Damn known informations:

- Hypertext Transfer Protocol (HTTP) is the backbone protocol of the World Wide Web.
- All information carried in HTTP is transmitted in plaintext from the source computer to the destination on the internet.
- HTTP does not protect data from alteration or interception by malicious parties, which is a serious threat to privacy, identity, and information security.
- All browsing activity should be considered to be at risk.

Technologies and Protocols

HTTP exploits

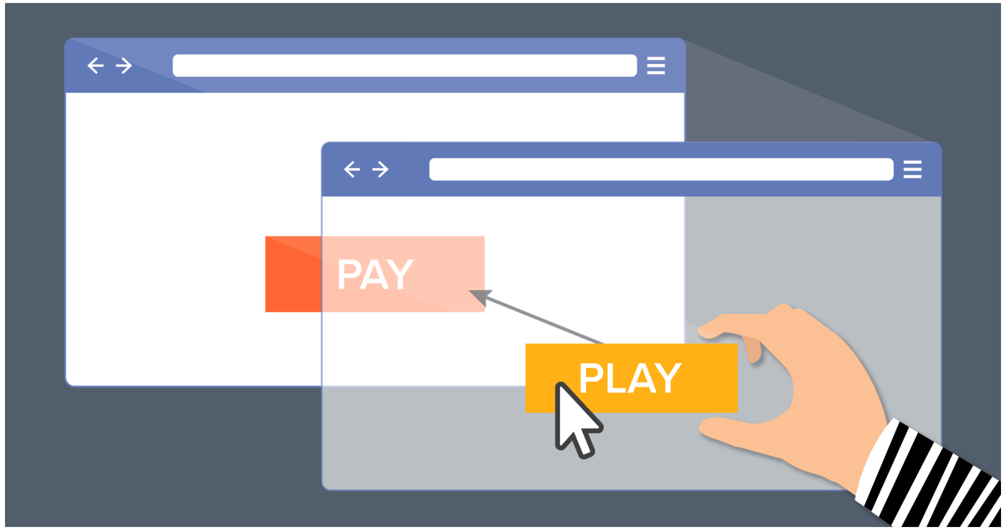


- iFrame (inline frame) injection
  - threat actor compromises a webserver
  - and plants malicious code
    => which creates an invisible iFrame on a commonly visited webpage.
- iFrame **loads** => malware is **downloaded**
  - frequently from a **different URL** than the webpage that contains the iFrame code.
- Network security services can detect when a website attempts to send content from an **untrusted website** to the host, even when sent from an iFrame
  - For example: Cisco Web Reputation filtering

DEFENSE:

- use HTTPs and forbid iFrame in HTTP https://www.w3.org/TR/CSP2/#directive-frame-ancestors

HTTP and HTTPS



- Content-Security-Policy (CSP) with frame-ancestors *(predchodcovia)*
  - CSP HTTP header was initially developed to protect against XSS and other data injection attacks
  - However, it also provides a frame-ancestors directive
    - for specifying sources that are permitted to embed a page
    - in a <frame>, <iframe>, <object>, <embed>, or <applet> element
    - The syntax is simple:

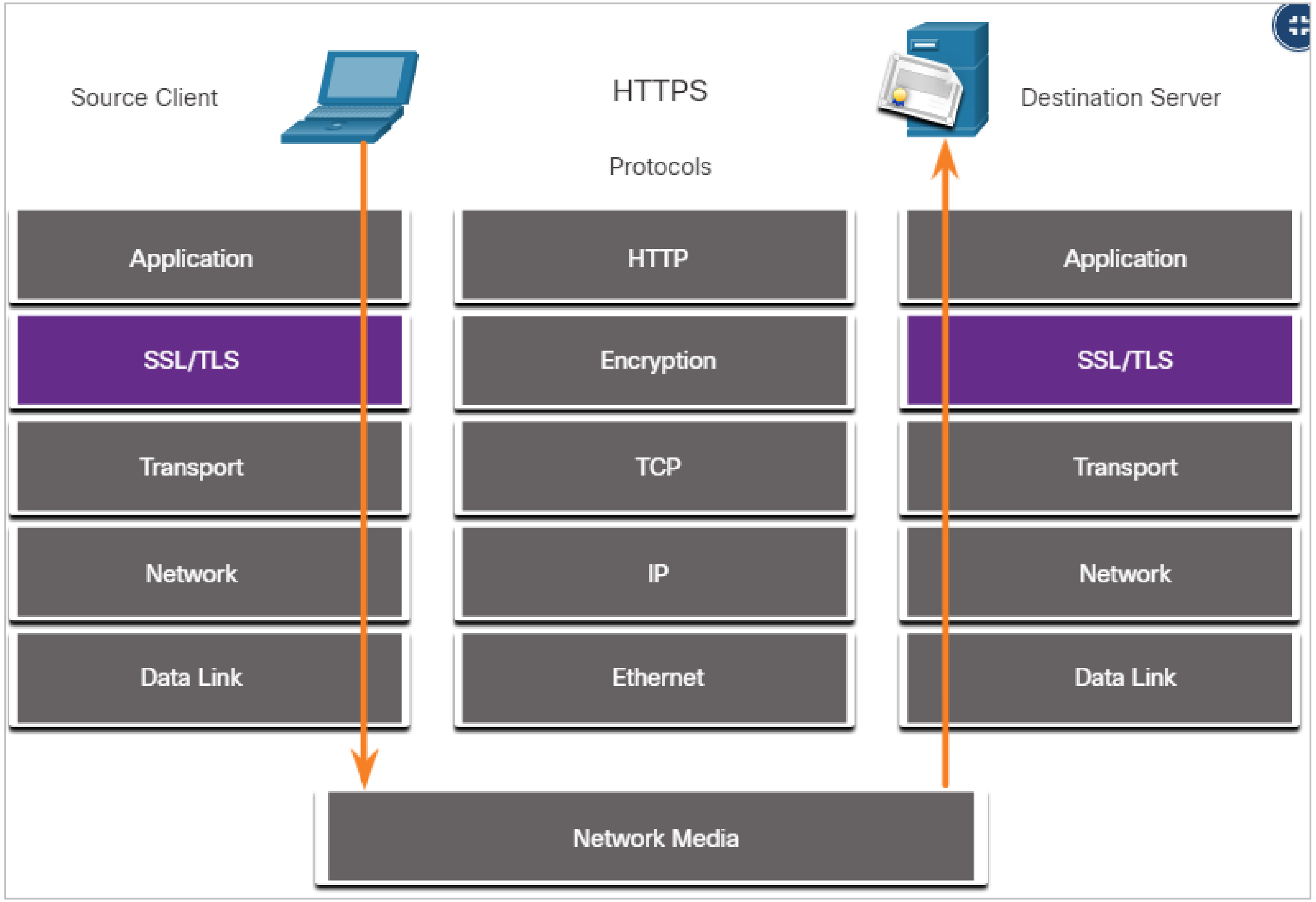
Content-Security-Policy: frame-ancestors <source1> <source2> ... <sourceN>;

Technologies and Protocols

HTTPS

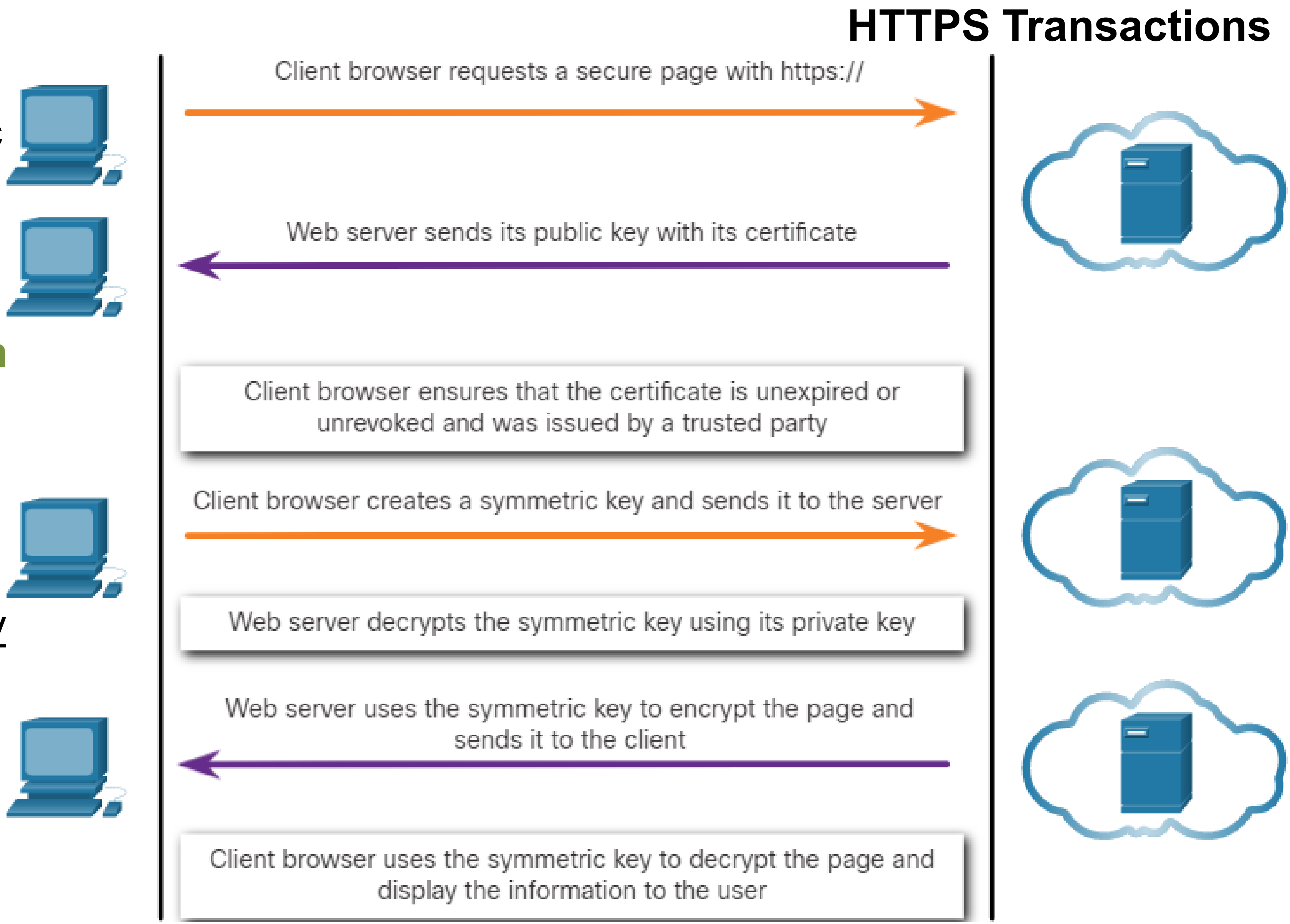
- implement HTTPS-only policies to protect visitors to websites and services.
- HTTPS adds a layer of encryption to the HTTP protocol by using Secure Socket Layer (SSL), as shown in the figure.
- This makes the HTTP data unreadable as it leaves the source computer until it reaches the server.
- HTTPS **is not a mechanism for web server security**. It only secures HTTP protocol traffic while it is in transit.

HTTPS Protocol Diagram



Technologies and Protocols

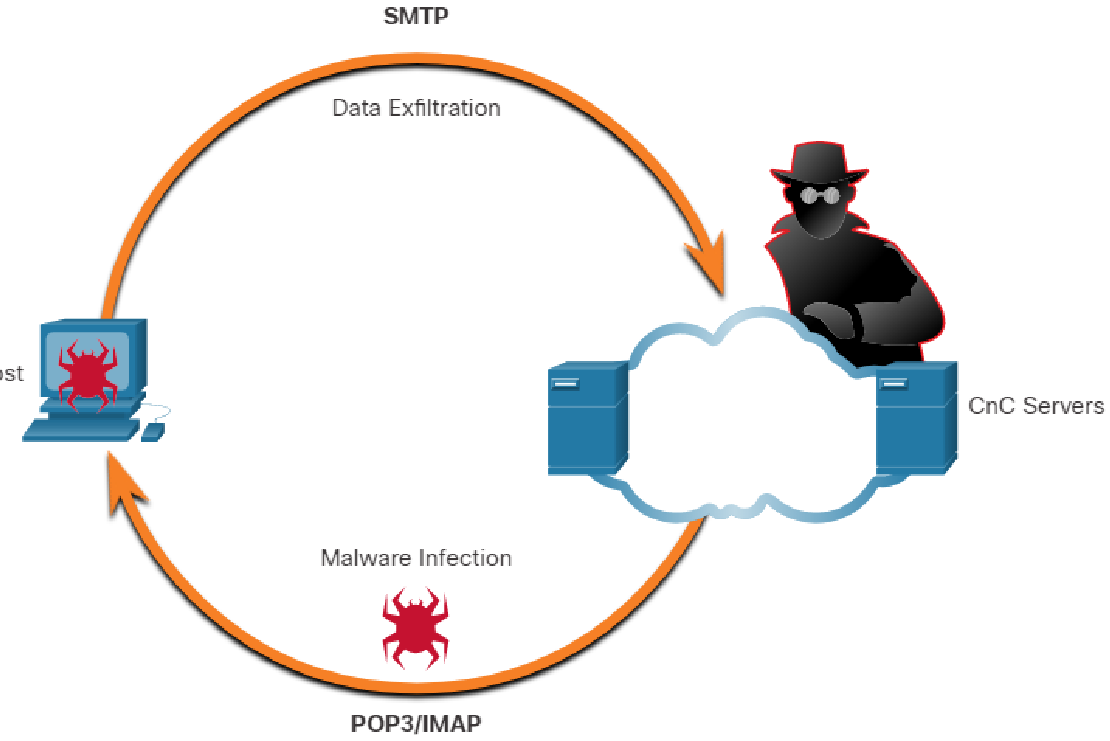
- encrypted HTTPS traffic **complicates** network security monitoring.
- Some security devices include **SSL decryption and inspection**; however, this can present processing and privacy issues.
- HTTPS adds complexity to packet captures due to the additional messaging involved in establishing the encrypted connection.



Email Protocols

- SMTP, POP3, IMAP
  - can be used by threat actors to
    - spread malware
    - exfiltrate data
    - provide channels to malware CnC servers, as shown in the figure.
- SMTP sends data from a host to a mail server and between mail servers.
- IMAP and POP3 are used to download email messages from a mail server to the host computer. They are the application protocols that are responsible for bringing malware to the host.
- Security monitoring can identify when a malware attachment entered the network and which host it first infected.

Email Protocol Threats

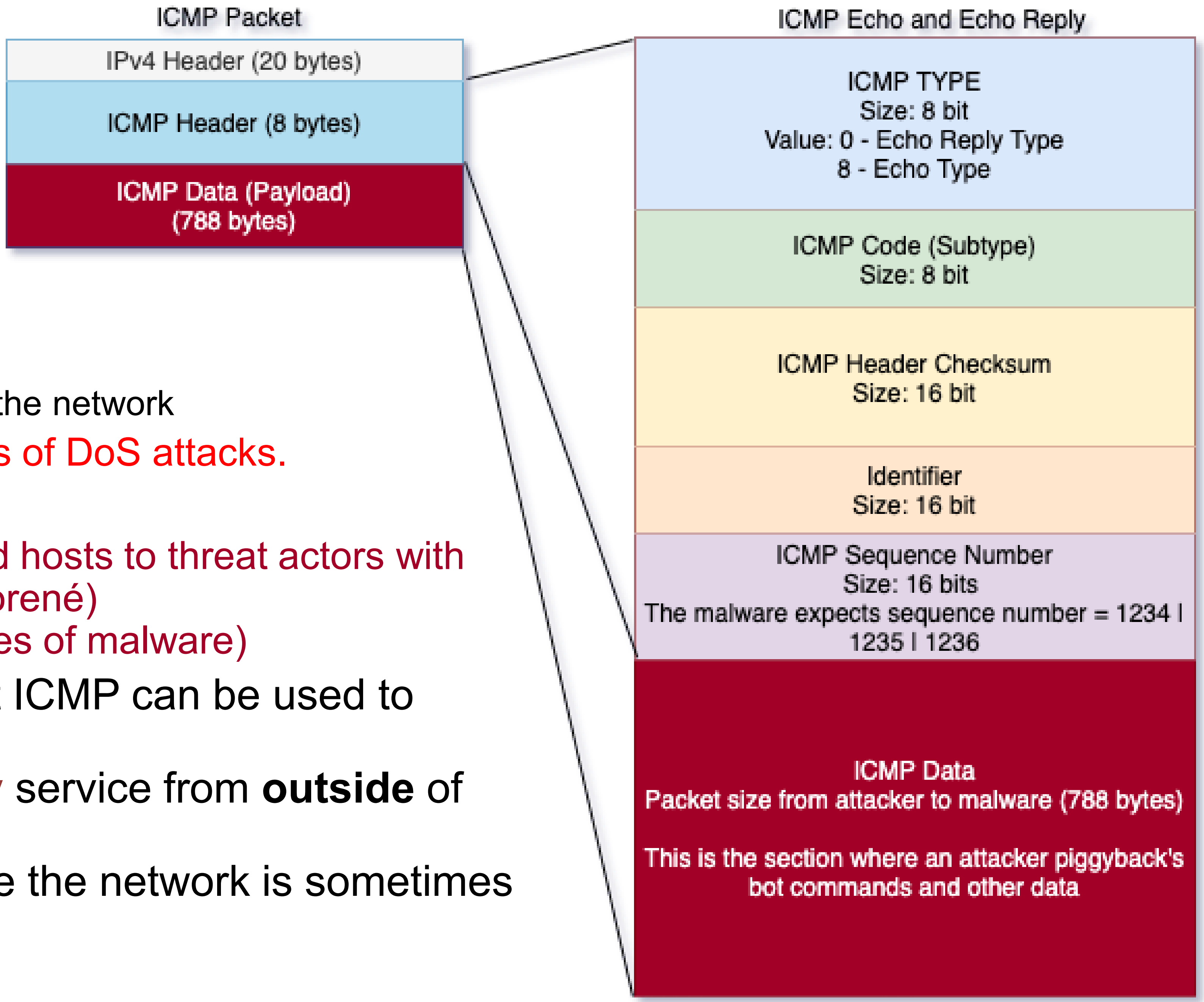


Technologies and Protocols

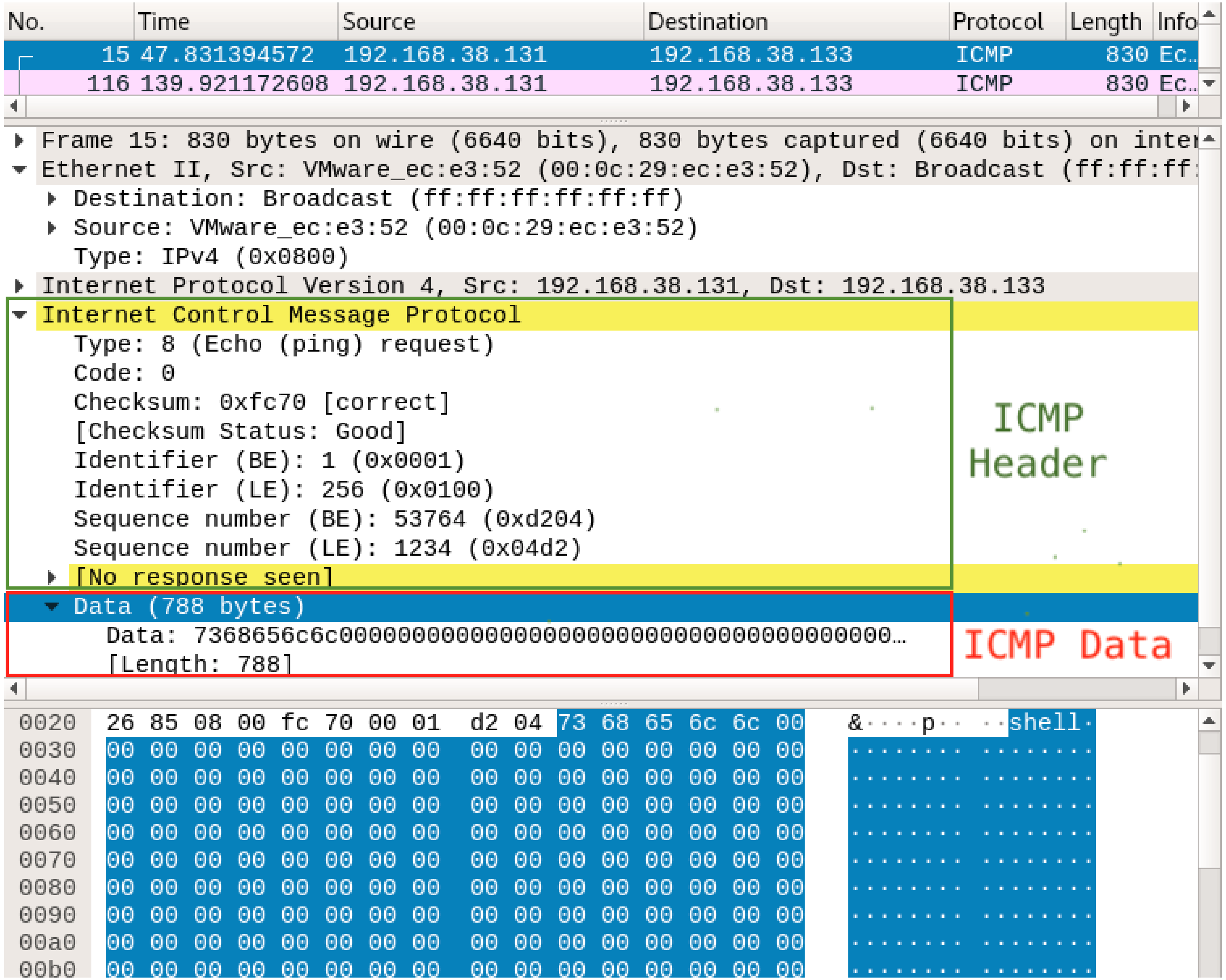
ICMP

- ICMP can be used
  - to identify
    - hosts on a network
    - structure of a network
    - operating systems at use on the network
  - as a vehicle for various types of DoS attacks.
  - for data exfiltration
  - To transfer files from infected hosts to threat actors with crafted packets (umelo vytvorené) = ICMP tunneling (some types of malware)
- Because of the concern that ICMP can be used to surveil *(sledovať)* => security defenders **deny** service from **outside** of the network BUT: ICMP traffic from inside the network is sometimes overlooked

  and it shouldn't be



ICMP tunneling analysis, backdoor at the end of ICMP tunnel



https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/backdoor-at-the-end-of-the-icmp-tunnel/

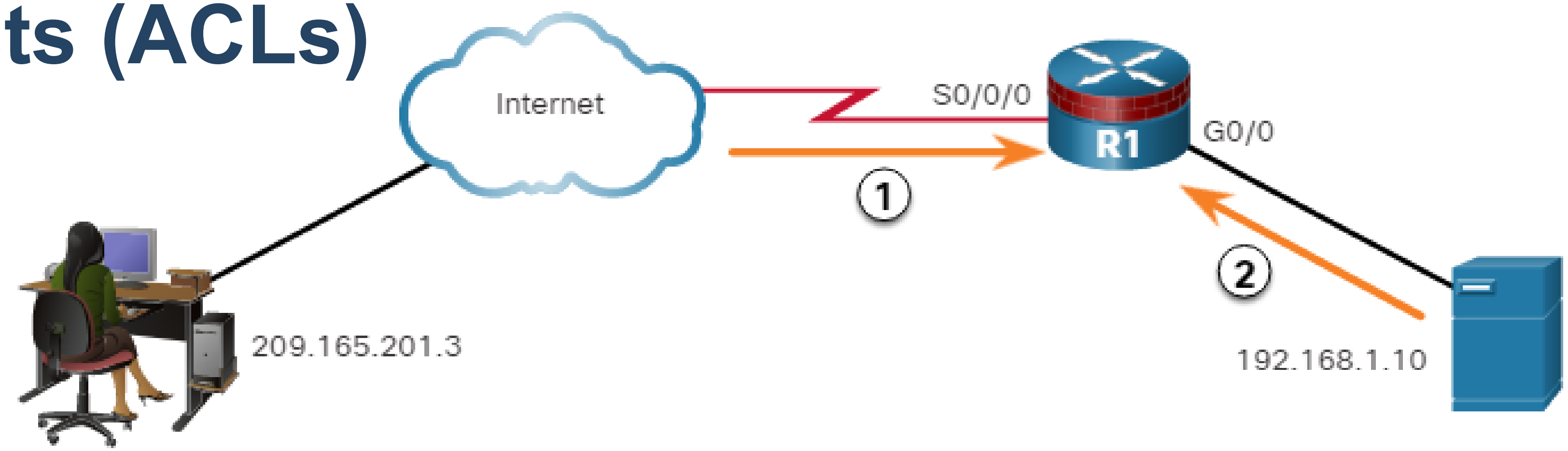
24.2 Security Technologies

Security Technologies

Access control lists (ACLs)

Mitigating ICMP Abuse

- ACLs and packet filtering are technologies that contribute to an evolving set of network security protections.
- **source Quench**
  - packets can not be forwarded due to buffers overload
  - TCP sender should decrease its send window to the respective destination in order to limit outgoing traffic.
- **parameter-problem**
  - incorrect usage of an IP option



1. Rules on R1 for ICMP traffic from the Internet

```
access-list 112 permit icmp any any echo-reply
access-list 112 permit icmp any any source-quench
access-list 112 permit icmp any any unreachable
access-list 112 deny icmp any any
access-list 112 permit ip any any
```

2. Rules on R1 for ICMP traffic from inside the network

```
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any echo
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any parameter-problem
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any packet-too-big
access-list 114 permit icmp 192.168.1.0 0.0.0.255 any source-quench
access-list 114 deny icmp any any
access-list 114 permit ip any any
```

Security Technologies

ACLs

PROBLEM:

- Attackers can determine which IP addresses, protocols, and ports are allowed by ACLs
  - either by port scanning or penetration testing, or through other forms of reconnaissance.

IMPACT:

- Attackers can craft packets that use spoofed source IP addresses.
- Applications can establish connections
  - on arbitrary ports
  - with manipulated established flag in TCP segments
- Rules cannot be anticipated *(predpokladané)* and configured for all emerging packet manipulation techniques.
  - the shortcomings of rule-based security measures

DEFENCE:

- In order to detect and react to packet manipulation
  - more sophisticated behavior
  - and context-based measures need to be taken Additional network elements included

Advanced sollutions:

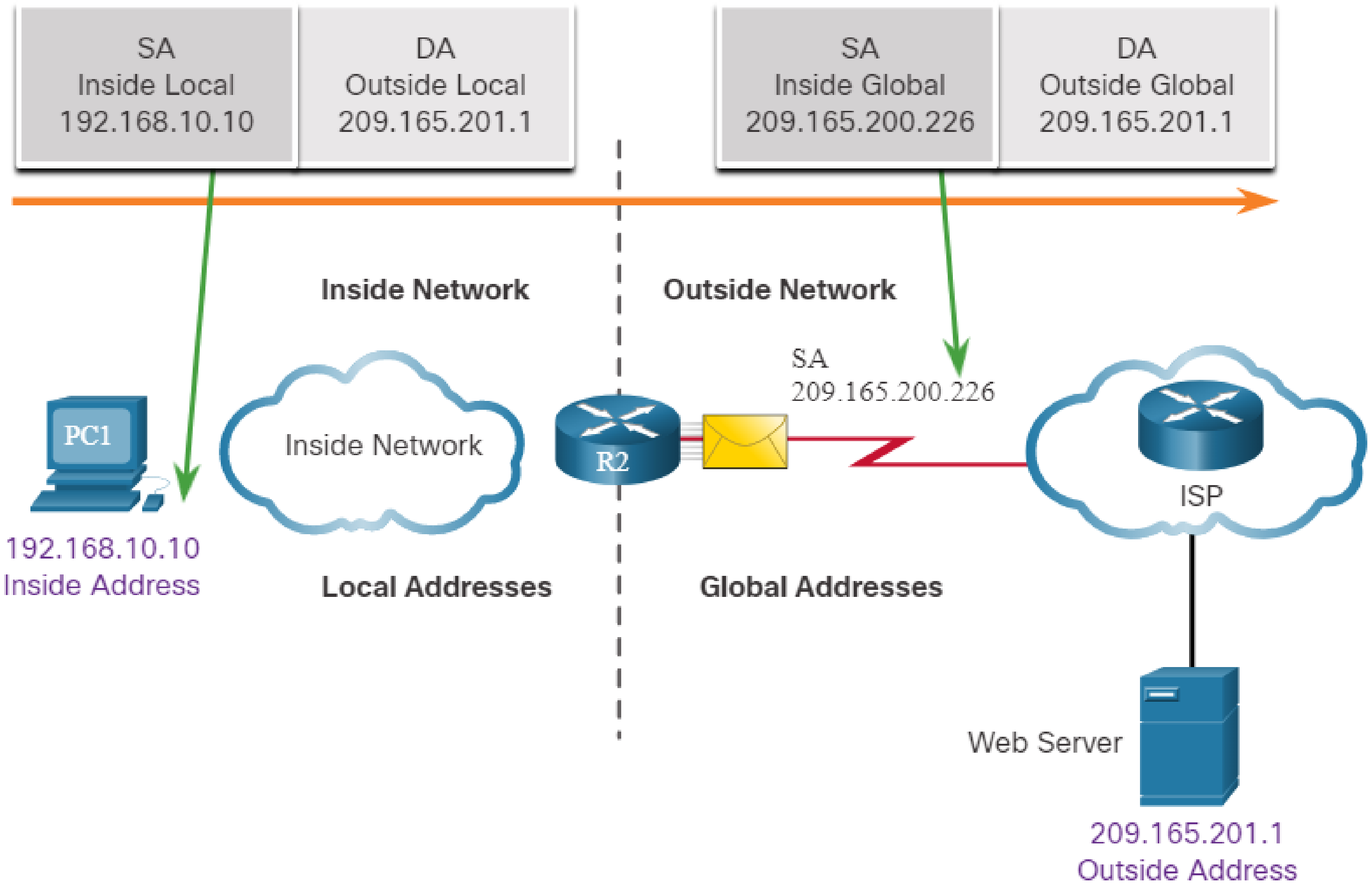
- Cisco Next Generation FW (NGFW)
- Antimalware Protection (AMP)
  - Protection from viruses and malware
- Email Security Appliance (ESA)
  - SPAM mails filtering before they reach the endpoint
- Web Security Appliances (WSA)
  - Website filtering and blacklisting
- Network Admission Control (NAC)
  - Perform network access decisions
  - Only authorized and compliant systems may connect

Security Technologies

NAT and PAT

PROBLEM:

- can complicate security monitoring
- If PAT is in effect, it could be **difficult to log the specific inside device** that is requesting and receiving the traffic when it enters the network.
  - Remember our simple iptables rules in the labs... Against DDoS
- This problem can be relevant with **NetFlow** data
  - NetFlow flows are **unidirectional** and are defined by the addresses and ports that they share.



Possible SOLLUTIONs:

- Nothing much
- To be aware of...
- Do monitoring inside our network (not behind NAT)

Encryption, Encapsulation, and Tunneling

ONLY PROBLEMs:

- **Encryption** => challenges to security monitoring by making packet details unreadable
- **VPN** establishes a virtual point-to-point connection between networks over public facilities
  - Encryption
    - is part of VPN technologies - IP is used to carry encrypted traffic.
    - makes the traffic unreadable to any other devices but the VPN endpoints.

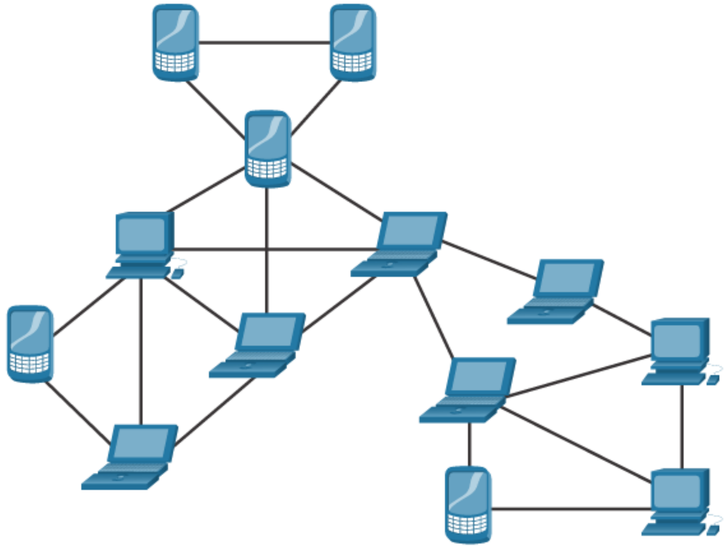
MORE PROBLEMs:

- A similar technology can be used by threat actors (with malware) to create
  - **virtual point-to-point** connection **between** an **internal host** and **threat actor** devices.
  - encrypted tunnel that rides on **a common and trusted protocol**
    - Threat actor use it to exfiltrate data from the network

Security Technologies

Peer-to-Peer Networking

- P2P
  - hosts can operate in both **client and server** roles
  - is inherently **dynamic**
    - connecting to numerous destination IP addresses
    - can also use dynamic port numbering
- types of P2P applications/operation
  - file sharing
    - **BitTorrent**
  - processor sharing
    - donate processor cycles to distributed computational tasks
    - examples:
      - Cancer research
      - searching for extraterrestrials
      - scientific research
  - instant messaging
    - legitimate value within organizations that have geographically distributed project teams
  - **Bitcoin** is a P2P operation



PROBLEM:

- P2P network activity can **avoid** *(vyhnúť sa)* **firewall** protections
- common **vector** for the spread of **malware**

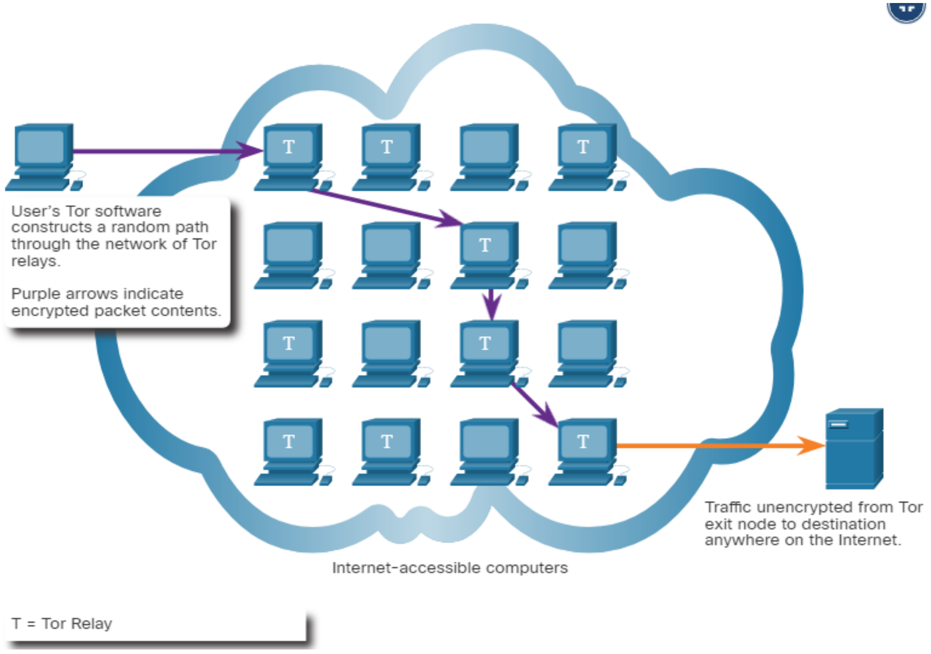
DEFENCE:

- File-sharing P2P applications should not be allowed on corporate networks
- specialized IM applications, such as the Webex Teams platform, which are more secure than IM that uses public servers

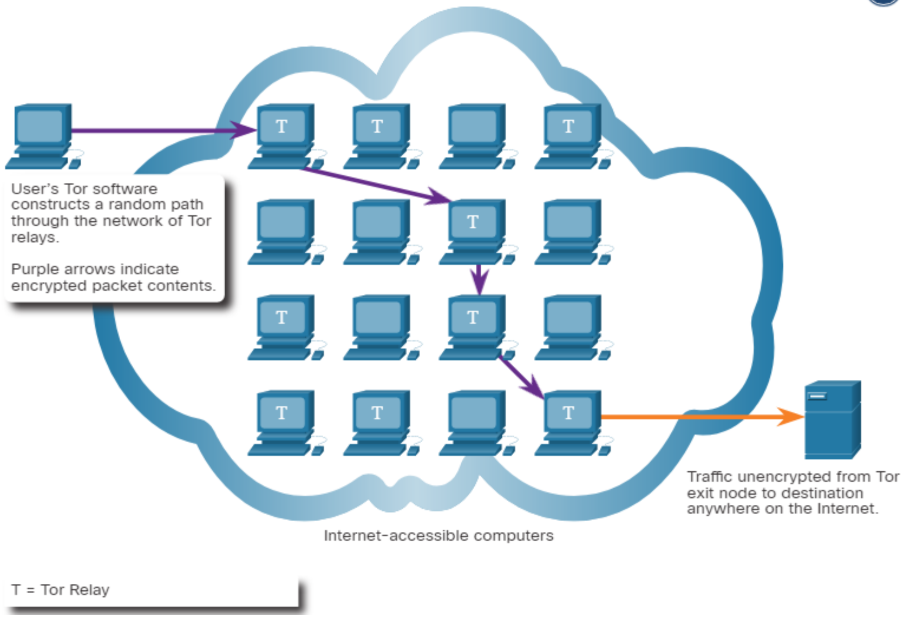
Security Technologies

Peer-to-Peer Networking and Tor

- Tor
  - software platform
  - network of P2P hosts
  - Hosts function as internet routers
  - allows users to browse the internet anonymously
    - special browser is needed
- When browsing begins, the browser constructs a layered end-to-end path across the Tor server network that is encrypted
  1. **encryption** to ensure privacy of data within the Tor network
  2. **authentication** so clients know they're talking to the relays they meant to talk to,
  3. **signatures** to make sure all clients know the same set of relays



Peer-to-Peer Networking and Tor



- all connections in Tor use **TLS** link encryption
  - **PROBLEM**: observers can't look inside to see which circuit a given cell is intended for
- Tor client establishes an ephemeral encryption key with each relay in the circuit
  - these extra layers of encryption mean that
    - only the exit relay can read the cells
  - Both sides discard the circuit key when the circuit ends
    - **PROBLEM**: so logging traffic and then breaking into the relay to discover the key won't work
- no single device knows the entire path to the destination
  - routing information is readable only by the device that requires it
- at the end of the Tor path, the traffic reaches its internet destination
  - When traffic is returned to the source, an encrypted layered path is **again constructed**.

MORE PROBLEMs for SOC analysts:

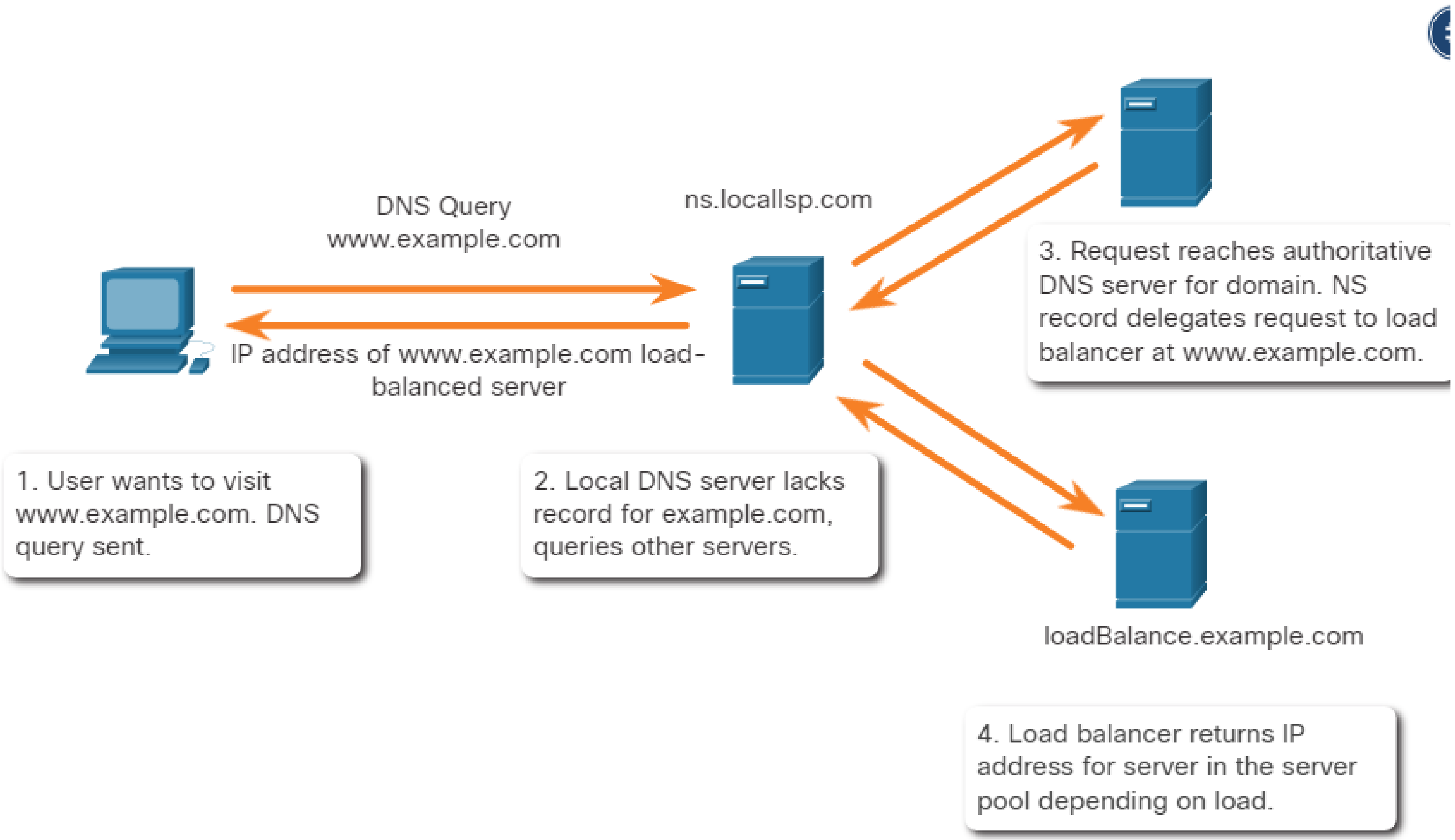
- Tor is widely used by criminal organizations on the "**dark net**"
- Tor has been used as a **communications channel** for malware CnC
- It **avoids blacklisting** that have been configured on security devices
  - *destination IP address* of Tor traffic is **confused by encryption**
    - only the next-hop Tor node is known

Security Technologies

Load Balancing

- Load balancing involves the distribution of traffic between devices or network paths to prevent overwhelming network resources with too much traffic.
- If redundant resources exist, a load balancing algorithm or device will work to distribute traffic between those resources, as shown in the figure.
- One way this is done is through techniques that use DNS
  - to send traffic to resources that
    - have the same domain name
    - but multiple IP addresses.

Load Balancing with DNS Delegation



Load Balancing

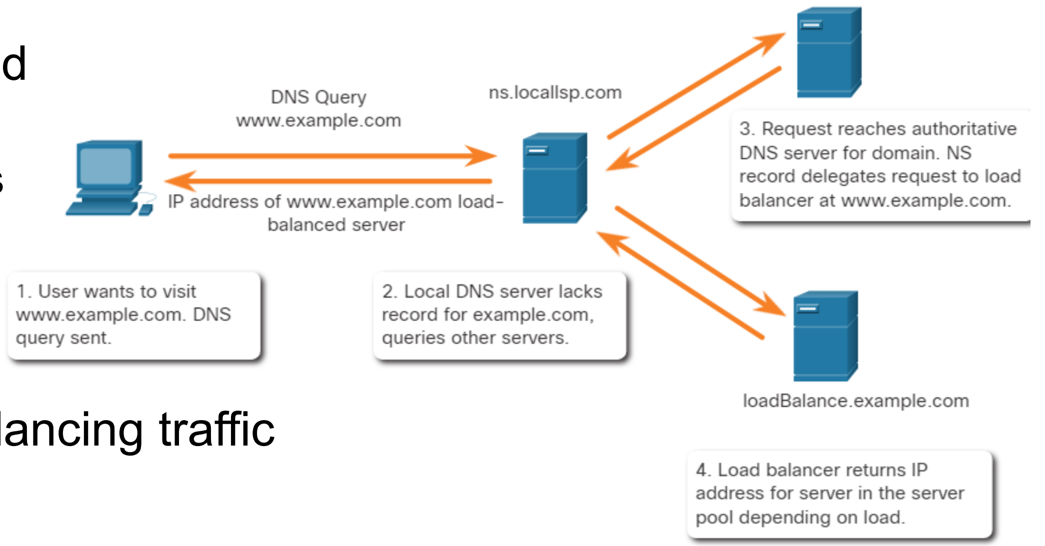
Load Balancing with DNS Delegation

- In some cases, the distribution may be to servers that are distributed geographically.
  - it results in single internet transaction which is represented
    - by multiple IP addresses on the incoming packets
    - It may cause suspicious features to appear in packet captures
- Also, some **load balancing manager (LBM)** devices
  - use probes to test for the performance of different paths
    - and the health of different devices.
  - may send probes to the different servers that it is load balancing traffic to
    - in order to detect that the servers are operating.

  to avoid sending traffic to a resource that is not available.

PROBLEM:

- These probes can appear to be suspicious traffic if the cybersecurity analyst is not aware that this traffic is part of the operation of the LBM.



24.3 Technologies and Protocols Summary

What Did I Learn in this Module?

- Syslog is used to send log entries to central servers that run a syslog daemon. This centralization of log collection helps to make security monitoring practical. As syslog is so important to security monitoring, syslog servers may be a target for threat actors.
- Syslog messages are usually timestamped. As the messages come from many devices, it is important that the devices share a consistent timeclock by using Network Time Protocol (NTP).
- Attackers encapsulate different network protocols within DNS to evade security devices.
- DNS is now used by many types of malware. Some varieties of malware use DNS to communicate with command-and-control (CnC) servers and to exfiltrate data in traffic disguised as normal DNS queries.
- An exploit of HTTP is called iFrame (inline frame) injection. To address the alteration or interception of confidential data , HTTPS should be adopted.
- HTTPS adds a layer of encryption to the HTTP protocol by using secure socket layer (SSL), making the HTTP data unreadable.

Technologies and Protocols Summary

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

- Email protocols such as SMTP, POP3, and IMAP can be used by threat actors to spread malware, exfiltrate data, or provide channels to malware CnC servers.
- ICMP can be used to identify hosts on a network, the structure of a network, and determine the operating systems at use on the network.
- It can also be used as a vehicle for various types of DoS attack and can also be used for data exfiltration.
- Attackers can determine which IP addresses, protocols, and ports are allowed by ACLs. This can be done either by port scanning or penetration testing, or through other forms of reconnaissance.
- Network Address Translation (NAT) and Port Address Translation (PAT) can complicate security monitoring.
- This problem can be especially relevant with NetFlow data which are unidirectional and are defined by the addresses and ports that they share.

Technologies and Protocols Summary

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

- Encryption can present challenges to security monitoring by making packet details unreadable. Encryption is part of VPN technologies.
- In peer-to-peer (P2P) networking, hosts can operate in both client and server roles.
- Three types of P2P applications exist: file sharing, processor sharing, and instant messaging.
- Tor is a software platform and network of P2P hosts that function as internet routers on the Tor network. This allows users to browse the internet anonymously.
- Load balancing involves the distribution of traffic between devices or network paths to prevent overwhelming network resources with too much traffic.
- This can be achieved through various techniques that use DNS to send traffic to resources that have the same domain name but multiple IP addresses.
- Some load balancing manager (LBM) devices use probes to test for the performance of different paths and the health of different devices.

UNIVERSITY OF ŽILINA
Faculty of Management Science and Informatics

Ďakujem za pozornosť

Obsahom boli moduly:
- Chapter 23 Endpoint Vulnerability Assessment
- Chapter 24 Technologies and Protocols

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

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