Security Fundamentals — Introduction

- **Jeremy's IT Lab** is a free, complete course for the CCNA.
- This video covers **security fundamentals**.
- The CCNA is **not a cybersecurity certification**, but it requires candidates to learn some fundamentals of **network and system security** necessary to work as an IT professional.
- **Exam topics covered in this video:**
  - Key security concepts
  - Security program elements
  - Passwords and user authentication
  - AAA concepts: **authentication**, **authorization**, and **accounting**
- This video is a **brief introduction** to many different security topics.
- If you haven't studied this material before, there will be many **new terms** to learn and memorize.
- **Recommendation:** take notes to keep all of the information organized.

Specific Coverage Order

1. **Key security concepts and terms**
2. **Common attacks** targeting an enterprise's systems and information
3. **Passwords and multi-factor authentication**
4. **AAA** — Authentication, Authorization, and Accounting
5. **Security programs** implemented by enterprises to secure systems and educate staff

- Watch until the end of the video for a **bonus question** from **Boson Software's ExSim for CCNA**.

Why Security?

- The purpose or goal of security in an enterprise is grounded in the **CIA triad**, which forms the **foundation of security**.
- Note: This is not the American Central Intelligence Agency. In this case, CIA stands for **Confidentiality**, **Integrity**, and **Availability**.

C — Confidentiality

- **Confidentiality** means that **only authorized users** should be able to access data.
- Some information and data is **public** and can be accessed by anyone.
    - Example: information put on the company website
- Some information is **secret** and should only be accessed by specific people.
- There are **degrees in the middle** — some information is more secret, some is less secret.

I — Integrity

- **Integrity** means that data should **not be tampered with** and should **not be modified** by unauthorized users.
- Data should be **correct and authentic**, not modified by an attacker.

A — Availability

- **Availability** means that the enterprise network and systems should be **operational and accessible** to authorized users.
    - Example: staff should be able to access the internal resources they need to perform their duties
    - Example: the company's website should be up and running and available to customers

Summary of the CIA Triad

- The CIA triad is **Confidentiality**, **Integrity**, and **Availability**.
- **Attackers can threaten** the confidentiality, integrity, and availability of an enterprise's systems and information.
- How attackers do that will be covered when looking at **common attacks**.

Key Security Concepts

- In addition to the **CIA triad**, there are some fundamental security concepts you should understand, and these are explicitly stated in the exam topics.

Vulnerability

- A **vulnerability** is any potential weakness that can compromise the **CIA** of a system or information.
- A potential weakness on its own isn't a problem.
    - Example: The windows of a house are vulnerabilities — potential weaknesses — but houses continue to have windows.

Exploit

- An **exploit** is something that can potentially be used to exploit the vulnerability.
- Something that can potentially be used as an exploit isn't a problem on its own.
    - Example: A rock can exploit the weakness of a window and be used to enter a house, but rocks aren't problems on their own.

Threat

- A **threat** is the potential of a vulnerability to be exploited. This ties it all together.
    - Example (window and rock analogy): A threat is a robber who wants to use a rock to break a window and enter your house.
    - Example (more relevant): A hacker exploiting a vulnerability in your system is a threat.

Mitigation Techniques

- A **mitigation technique** is something that can protect against threats.
- There are various mitigation techniques, and they depend on the threat that is being defended against. Some techniques will be covered in this video and the next few videos on security.
- Appropriate mitigation techniques should be implemented everywhere a vulnerability can be exploited.
    - Example: client devices, servers, switches, routers, firewalls
    - Example: preventing unauthorized people from getting physical access to the devices by keeping them in a secure rack behind a secure door, etc.

- **Important:** No system is perfectly secure. Systems can be more secure or less secure, but there are no guarantees in security.
    - Example: You can implement malware detection on your network firewall and have the best antivirus software on client PCs, but the chance of the PCs getting infected with malware is never 0.

Common Attacks

- These are **threats** which can potentially exploit **vulnerabilities** to compromise the **confidentiality**, **integrity**, or **availability** (CIA) of an enterprise's systems and information.
- There are many more potential attacks than just these, but these are some of the **main attack categories**.
- Let's take a brief look at each one individually.

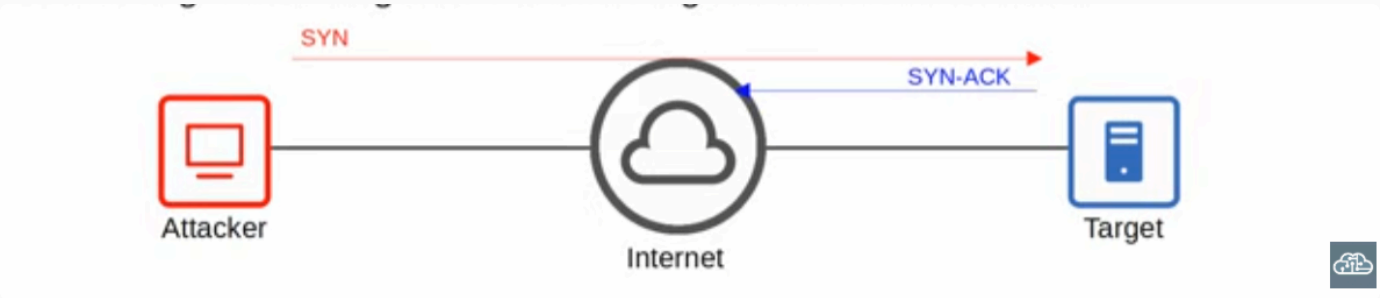
Denial-of-Service (DoS) Attacks

- **DoS attacks** threaten the **availability** of a system — the **A** of the CIA triad.
- There are many kinds, and a few will be shown, but one common DoS attack is the **TCP SYN flood**, which exploits the **TCP three-way handshake**.
- The three-way handshake is **SYN**, **SYN-ACK**, and **ACK**.

TCP SYN Flood

- In a **TCP SYN flood**, the attacker sends countless **TCP SYN messages** to the target.
- The target sends a **SYN-ACK message** in response to each SYN it receives.
- The attacker **never replies with the final ACK** of the handshake.
- The target waits for the final ACK of each handshake, and the **incomplete connections fill up the target's TCP connection table**.
- The incomplete connections will timeout and be removed from the table after a certain period of time, but the attacker **continues sending SYN messages** to fill up the table.
- In the end, the target is **no longer able to make legitimate TCP connections** because it has reached the maximum number of TCP connections it can maintain.

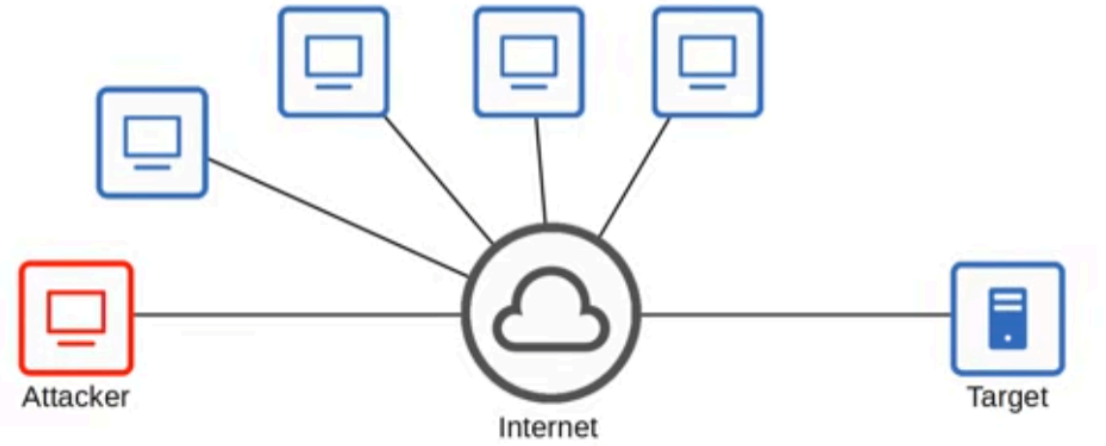
- ***Example (diagram demonstration):***



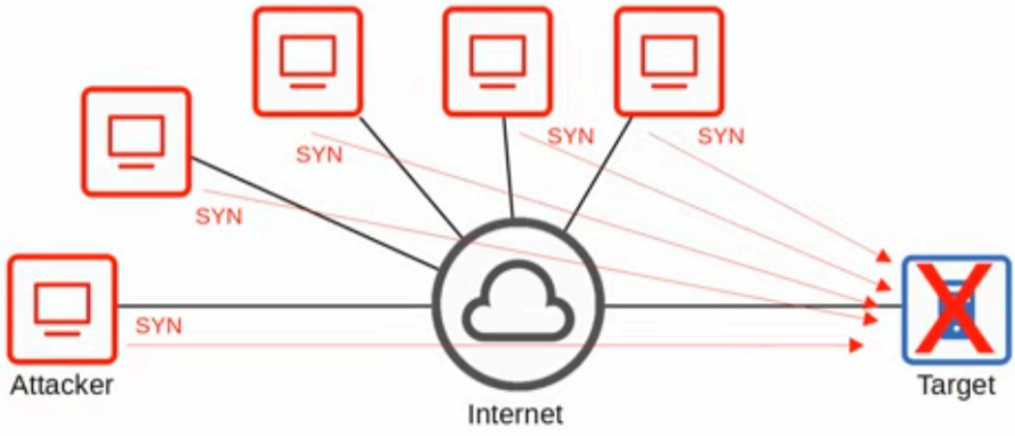
  - *For each SYN message the attacker sends:*
    - *The target puts an entry in its TCP connection table*
    - *The target sends a SYN-ACK message*
    - *The target then waits for an ACK to complete the connection*
  - *The ACK never comes*

  - *The attacker keeps sending SYN messages, and the target keeps sending SYN-ACK messages*
  - *Eventually, the target's TCP connection table fills up*
  - *The denial-of-service has been achieved*
- **Note (spoofing):** The SYN-ACK arrows were drawn not reaching the attacker because the attacker likely **spoofs their IP address**, meaning they use a **fake IP address**, so the SYN-ACK messages don't return back to them. Spoof attacks will be discussed after DoS attacks.

Distributed Denial-of-Service (DDoS) Attacks



- A denial-of-service like that is **usually not done by a single attacker**. A much more powerful kind of attack is the **DDoS**.
- In a **DDoS (distributed denial-of-service)** attack, the attacker **infects many target computers with malware** and uses them all to initiate a denial-of-service attack, for example a **TCP SYN flood attack**.
- This group of infected computers is called a **botnet**.
- ***Example (DDoS attack):***



1. *The attacker infects many PCs with malware through separate attacks.*
2. *All infected PCs together start flooding the target with TCP SYN messages.*
3. *The target server is no longer able to respond to legitimate TCP connection requests.*

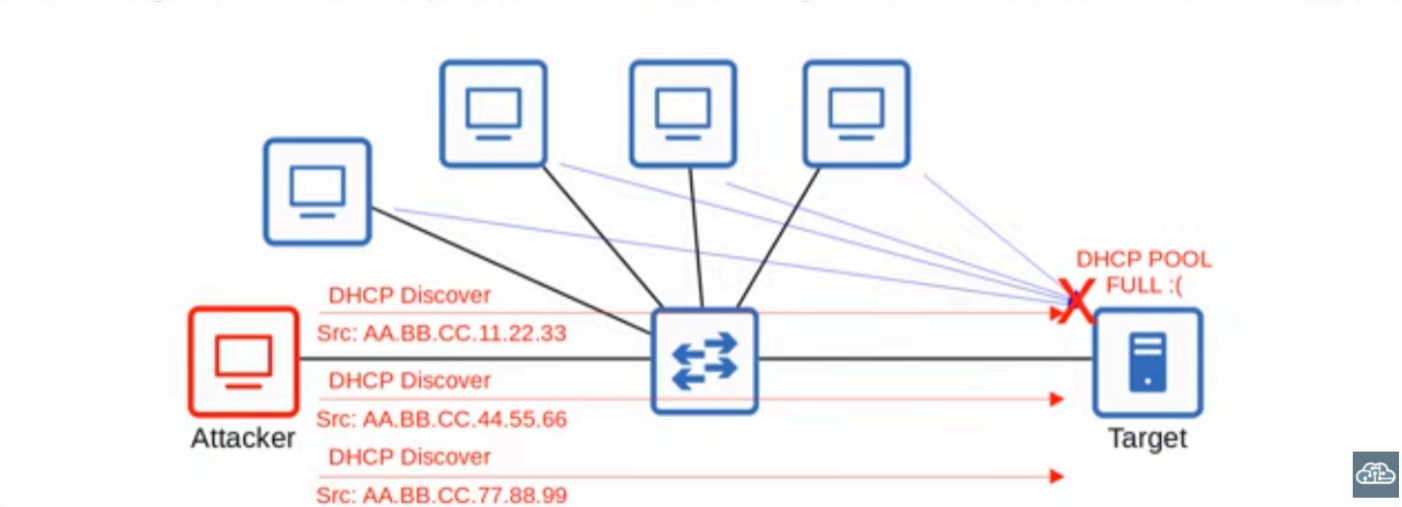
- **Summary:** Denial-of-service attacks attack the **availability** of a system — the **A** of the CIA triad.

Spoofing Attacks

- To **spoof** an address is to use a **fake source address**, for example a fake **IP** or **MAC address**.
- There are numerous attacks that involve spoofing — it is **not a single kind of attack**.

DHCP Exhaustion Attack

- An example of a spoofing attack is a **DHCP exhaustion attack**.
- It is **similar to the TCP SYN flood attack**.
- An attacker uses **spoofed MAC addresses** to **flood DHCP Discover messages**.
- Then, the target server's **DHCP pool becomes full**, resulting in a **denial-of-service** to other devices — they won't be able to get an IP address.
- **Note:** Spoofing attacks don't have to be denial-of-service attacks, but this type is.

> ***Example (demonstration):***
>
> 
>
>
> 1. ***The attacker sends a DHCP Discover message with a fake source MAC address***
> 2. ***Then it sends another with a different fake source MAC address***
> 3. ***Then it does it again, with another fake source MAC address***
> 4. ***It keeps sending these at a very quick pace***
> 5. ***The server replies to each Discover with a DHCP Offer message***

> 6. ***While the server is offering an IP address, it will not assign that address to other devices***
> 7. ***If legitimate PCs send DHCP Discover messages to get IP addresses, the server cannot give them IP addresses because its DHCP pool is full***

- **Example (scale):** Maybe the server had **250 IP addresses** to lease to clients, but they are **all taken by the attacker**.

Connections to Other Attack Types

- This is just **one example** of a spoofing attack.
- In the previous **TCP SYN flood** example, **source IP addresses were spoofed** too, so actually it is **also a spoofing attack**.
- This **DHCP exhaustion attack** resulted in a denial-of-service, so it is **also a DoS attack**.
- Some of these attack types are **connected and related** — they aren't totally separate.
- Once again, this attacks the **availability** — the **A** of the CIA triad.
- **Note:** Not all spoofing attacks are DoS attacks. Later the professor will show **another type of spoofing attack** that targets the **confidentiality and integrity** of a system, not the availability.

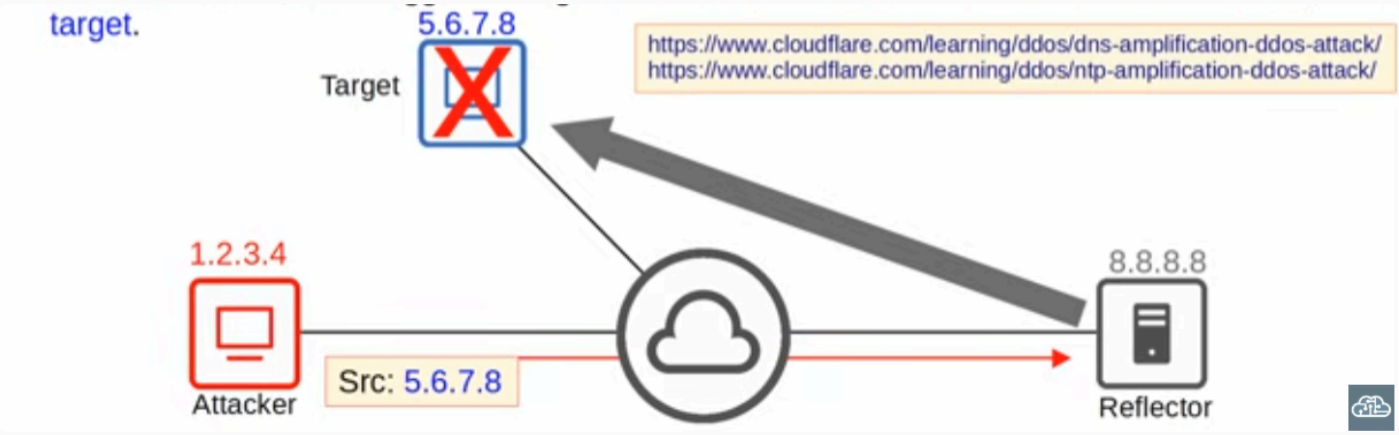
Reflection and Amplification Attacks

- In a **reflection attack**, the attacker sends traffic to what's called a **reflector** and **spoofs the source address** of its packets using the **target's IP address**.
- Then the reflector — for example, a **DNS server** — sends the reply to the **target's IP address**.
- **Purpose of the attack:**
  - If the amount of traffic is large enough, this can result in a **denial-of-service** to the target.

Amplification Attack

- A **more powerful form** of reflection attack is called an **amplification attack**.
- A reflection attack becomes an **amplification attack** when:
  - The amount of traffic sent by the attacker is **small**
  - But it triggers a **large amount of traffic** to be sent from the reflector to the target

- This is how it can trigger a **denial-of-service**.

> ***Example (demonstration):***
>
> 
>
>
> 1. ***The attacker's IP address is 1.2.3.4***
> 2. ***The attacker uses source IP address 5.6.7.8 to send a message to a server at 8.8.8.8, which becomes the reflector***
> 3. ***5.6.7.8 is the IP address of the target of the attack***
> 4. ***The attacker's message causes the reflector to send a large amount of traffic to the target***
> 5. ***This results in a denial-of-service***

Vulnerabilities Used for Amplification Attacks

- There are **DNS and NTP vulnerabilities** which can be exploited for **amplification attacks** like this.
- **Resources:** Cloudflare articles on these topics can be found by searching for **"DNS amplification attack"** or **"NTP amplification attack"**.

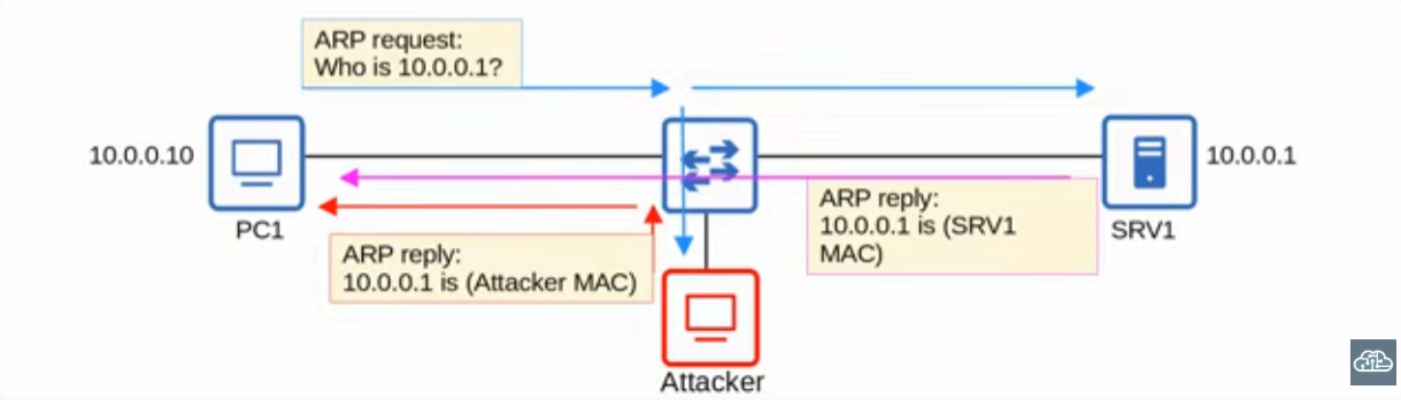
Man-in-the-Middle Attacks

- In a **man-in-the-middle attack**, the attacker places **himself between the source and destination** to **eavesdrop on communications**, or to **modify traffic** before it reaches the destination.

ARP Spoofing (ARP Poisoning)

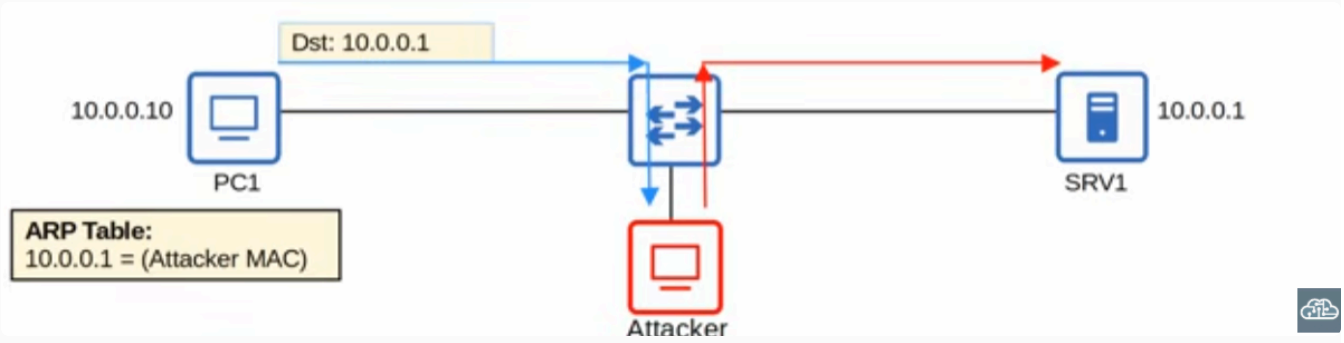
- A common example of a man-in-the-middle attack is **ARP spoofing**, also known as **ARP poisoning**.
- This is **yet another kind of spoofing attack**.

Example (ARP spoofing demonstration):



- ***Setup: PC1 is asking for the MAC address of 10.0.0.1, which is SRV1.***

1. ***PC1 sends an ARP request asking for the MAC address of 10.0.0.1 (SRV1)***
2. ***Because ARP request messages are broadcast, the switch floods the frame, so both SRV1 and the attacker receive it***
3. ***The target of the ARP request, SRV1, sends an ARP reply to inform PC1 of SRV1's MAC address***
4. ***The attack: The attacker waits briefly and then sends another ARP reply after the legitimate replier***
5. ***If the attacker's ARP reply arrives last, it will overwrite the legitimate ARP entry in PC1's ARP table***



6. ***Now, in PC1's ARP table, the entry for 10.0.0.1 has the attacker's MAC address, not the real SRV1's MAC address***

> 7. ***When PC1 tries to send traffic to SRV1, it is forwarded to the attacker instead***
> 8. ***The attacker can then:***
>   - ***Inspect the messages, read their contents, and then forward them on to SRV1***
>   - ***Modify the messages before forwarding them to SRV1***

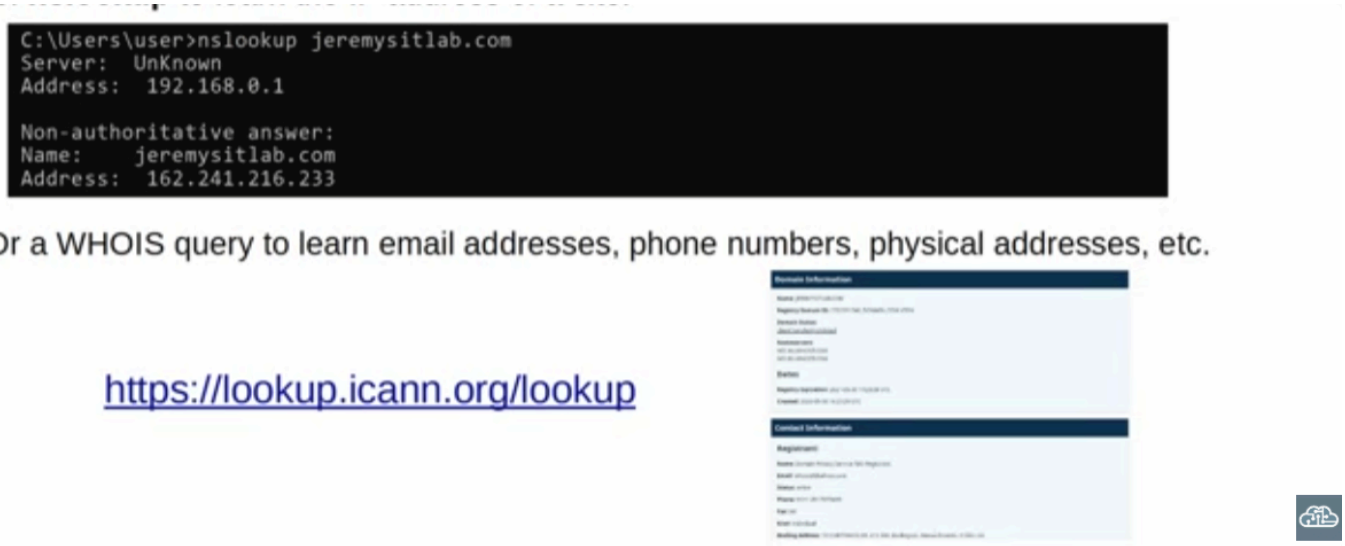
Effect on the CIA Triad

- In this example, the threat is **not** to the **availability** of the CIA triad.
- This kind of attack compromises the **confidentiality** and **integrity** — the **C and I** — of the communications between PC1 and SRV1.
- It compromises **confidentiality** because an **unauthorized user** (the attacker) has access to the communications between PC1 and SRV1.
- It compromises **integrity** because that unauthorized user can also **modify the data** before it reaches the destination.

Reconnaissance Attacks

- **Reconnaissance attacks** aren't attacks themselves, but they are used to **gather information** about a target which can be used for a **future attack**.
- This is often **publicly available information**, which is why it's not really an attack itself — the information isn't actually confidential.

> ***Example (information gathering):***



- ***You can perform an NSLOOKUP to learn the IP address of a site***
- ***From there, you can probe for open ports which are potential vulnerabilities***
- ***You could also perform a WHOIS query to learn:***
  - ***Email addresses***
  - ***Phone numbers***
  - ***Physical addresses, etc.***
- ***You can perform a WHOIS query at this website here — for example, the professor did a lookup of his own website***

- Once **contact information** is known, some of the so-called **'social engineering' attacks** — which will be looked at soon — can be carried out to **threaten the target enterprise**.

Malware

- **Malware**, which means **malicious software**, refers to a variety of **harmful programs** that can infect a computer.
- Here are a few types:

Viruses

- **Viruses** are malware that infects other software, called a **host program**.

- The virus spreads as the software is **shared by users**, or **downloaded from malicious websites**, etc.
- Once the virus has infected the device, it can do various harmful things, such as **corrupting or modifying files** on the target computer.

Worms

- **Worms** are different than viruses in that they **don't require a host program**.
- They are **standalone malware** and are also able to **spread on their own**, without user interaction.
- The spread of worms from device to device can **congest the network**.
- In addition, if the worm has a **'payload'** — other malicious code within the worm — it can cause **additional harm** to target devices.

Trojan Horse

- A **trojan horse** is **harmful software disguised as legitimate software**.
- Trojan horses spread through **user interaction**, such as:
  - Opening **email attachments**
  - Downloading a **file from the Internet**

Note on Malware Types

- These types of malware are defined mostly by **how the malware infects a system and how it spreads**, not the attacks they carry out after infecting the system.
- The above malware types can exploit various vulnerabilities to threaten **any of the CIA triad** of the target device.
- There are many types of malware — these three are just a **few large categories** of malware.

Social Engineering

- **Social engineering attacks** target the most vulnerable part of any system — **the people**.
- This is something you have to be aware of when designing a **security policy**.

- No matter how many security features you configure on your **routers, switches, firewalls, servers, PCs**, etc., people are always a **vulnerability** that can be exploited.
- Social engineering attacks involve **psychological manipulation** to make the target **reveal confidential information** or **perform some action** the attacker tells the target to do.
- As with the previous attack types, there are various kinds of social engineering attacks.

Phishing

- **Phishing** involves **fraudulent emails** that appear to come from a **legitimate business**, maybe Amazon, your bank, or your credit card company, for example.
- These emails contain **links to a fraudulent website** that seems legitimate.
    - Example: The website may look identical to the real login page of your bank's website
- Users are told to login to the fraudulent website, therefore **providing their login credentials** to the attacker.

Spear Phishing

- **Spear phishing** is a type of phishing that is **more targeted**.
- Not mass emails sent out to anybody, but perhaps **emails sent to employees of a specific company**, for example.

Whaling

- **Whaling** is another kind of phishing targeted at **high-profile individuals**, for example a **company president**.

Vishing

- **Vishing**, or **voice phishing**, is phishing performed over the **phone**.
- The attacker could pretend to be from the target's bank, or maybe another department in the company.

> ***Example (vishing attack):***
>
> - ***The attacker might say something like: "Hi, this is Jeremy from the IT department. Due to company policy we need to reset your password, could you tell me the password you're currently using and I'll reset it for you?"***

> - ***Note: The professor notes that a real attacker would be more convincing than that, but it's just an example.***

Smishing

- **Smishing**, or **SMS phishing**, is phishing performed using **SMS text messages** to the target's cell phone.

Watering Hole Attacks

- **Watering hole attacks** compromise **sites that the target victim frequently visits**.
- If a malicious link is placed on a **website the target trusts**, they might not hesitate to click it.
- This kind of attack takes advantage of the **user's trust** in the website they frequently visit — they don't think twice about clicking the link.

Tailgating Attacks

- **Tailgating attacks** involve entering **restricted, secure areas** by simply **walking in behind an authorized person** as they enter.
- Any company that has restricted areas will have rules against this, but often the target will **hold the door open** for the attacker to be polite, assuming the attacker is also authorized to enter.

Summary of Social Engineering

- Social engineering attacks are attacks that **don't directly exploit a company's IT systems** — instead, they **exploit the employees**.

> ***Example (phishing email):***

Пн 09.12.2019 18:57

AmazonWebService <no-reply@[redacted].com>

Suspicious Activity Detected!

To [redacted]

amazon

Dear [redacted]

Case ID : **2887655768,**

Four your safety, your Amazon has been locked because we found some suspicious activity on your account. Someone accessing your account and make some change on your account information. This the details :

Country	:	Dominica
IP Address	:	64.250.251.208
Date and Time	:	09/12/2019 15:59:36
Browser	:	Google Chrome

If you did not make these action or you believe an unauthorized person has accessed your account, you should login to your account as soon as possible to verify your information.

Verify Account Information

Regard

Amazon Support

1. ***The email says the target's Amazon account has been locked due to a suspicious login***
2. ***There is a link at the bottom requesting that the target verify their account information***
3. ***If the target clicks on that link and enters their login information, the attacker now has access to their Amazon account***

- ***Note: Anyone who has an email address has seen emails like this — it's something we all have to watch out for.***

Password-Related Attacks

- The **final kind of attack** covered is **password-related attacks**.
- Most systems use a **username and password combination** to authenticate users.
- The username itself is often **simple and easy to guess**.
  - Example: the user's email address
- The **strength and secrecy of the password** is relied on to provide the necessary security.
- Attackers can learn a user's password through **multiple methods**.

Methods of Password Attacks

- **Guessing:**
  - The attacker could simply **guess the password**.
  - Successfully guessing a password should be **extremely rare**, but it is a possibility.
- **Dictionary attack:**
  - A program runs through a **dictionary**, which is a **list of common words and passwords**, to guess the target's password.
  - It tries each one, hoping to find the correct password.
- **Brute force attack:**
  - Involves trying **every possible combination** of letters, numbers, and special characters to find the target's password.
  - This requires a **very powerful computer**.
  - If the password is **sufficiently strong**, the chances of it working are **very low**, because it takes so much time.

Strong Password Characteristics

- **Strong passwords** should:
  - Contain **at least 8 characters** — definitely not less, but **preferably more than 8**
    - The more characters, the **harder it is to brute force** attack the password
  - Have a **mix of uppercase and lowercase letters**
  - Have a **mixture of letters and numbers**
  - Have **one or more special characters** such as question marks, exclamation points, etc.
  - Be **changed regularly**
- Most enterprises will **enforce rules like these** on their employees.
- It's also **recommended** to follow rules like these when making your own personal passwords.

Summary of Attacks

- The professor notes that was **a lot of potential attacks**.
- To help review, there is a **basic summary of each attack**.
- If you want to know more about each kind of attack, a **Google search** will give you all kinds of great resources.
- For our purposes, just a **basic understanding** of each attack type is sufficient for now.
- **Important:** Make sure you know these **basic attack types**.

Multi-Factor Authentication

- **No matter how secure the password**, there is still a chance it **gets into the hands of an attacker**.
- That's why **multi-factor authentication** is becoming **more and more wide-spread**.
- **Multi-factor authentication** involves providing **more than just a username and password** to prove your identity.
- It usually involves providing **two of the following**, in which case it's called **two-factor authentication**.

Factor 1 — Something You Know

- Example: a **username and password combination** or a **PIN**

Factor 2 — Something You Have

- Example: pressing a **notification** that appears on your phone using an **authenticator app**, or perhaps a **badge** that is scanned

Factor 3 — Something You Are

- These are **unique characteristics** about you.
- Example: **biometrics** such as:
  - **Face scan**
  - **Palm scan**
  - **Fingerprint scan**
  - **Retina scan**, etc.

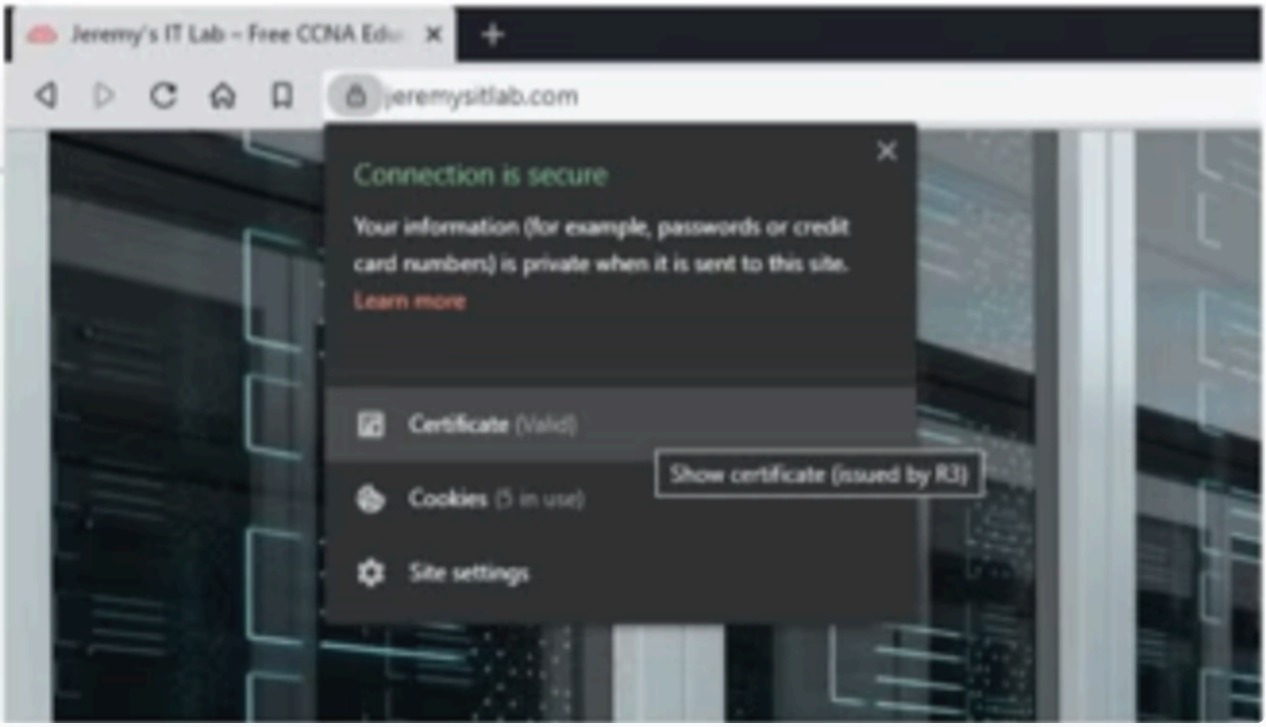
Benefits of Multi-Factor Authentication

- Requiring **multiple factors** of authentication **greatly increases the security**.
- Even if an attacker **learns the target's password**, they **won't be able to login** to the target's account.

Digital Certificates

- Another form of authentication involves the use of **digital certificates**, which are used to **prove the identity of the holder** of the certificate.
- They are **mainly, but not exclusively**, used for **websites** to verify that the website being accessed is **legitimate**.

> ***Example (certificate issuance process):***



1. ***Entities that want a certificate — for example, a company with a website — send a CSR (certificate signing request) to a CA (certificate authority)***
2. ***The CA will generate and sign the certificate***

- When you access a website, **modern browsers display a symbol** to indicate that the website is **secure and has a valid certificate**.
- **Example:** The professor's website has a **valid certificate**, and if you click on it you will be able to **inspect the certificate**.
- This is how you can know that the website you're accessing is really **jeremysitlab.com**, not a **fake website pretending to be jeremysitlab.com**.

AAA — Authentication, Authorization, and Accounting

- The professor has been mentioning **authentication** a lot, and it is one part of an important framework needed for the CCNA.
- **AAA** stands for **Authentication**, **Authorization**, and **Accounting**.
- It is a **framework for controlling and monitoring users** of a computer system, such as a network.

Authentication

- **Authentication** is the process of **verifying a user's identity**.
- Example: When a user logs in, ideally using **multi-factor authentication**, that is authentication.

Authorization

- **Authorization** is the process of **granting the user the appropriate access and permissions**.
- Example: Granting the user access to some files and services, but **restricting access to other files and services**, is authorization.

Accounting

- **Accounting** is the process of **recording the user's activities** on the system.
- Example: Logging when a user **makes a change to a file**, or recording when a user **logs in or logs out**, is accounting.

AAA Servers and Protocols

- Enterprises typically use a **AAA server** to provide AAA services.
- Example: **ISE (Identity Services Engine)** is Cisco's AAA server.
- These AAA servers typically support the following **two AAA protocols**:
  - **RADIUS** — an **open standard protocol** that uses **UDP ports 1812 and 1813**
  - **TACACS+** — a **Cisco proprietary protocol** that uses **TCP port 49**
- **Note:** The professor recommends remembering the **names of these protocols and their ports**, but for the CCNA that is all you need to know about them.
- **Important:** Make sure you know the **differences between authentication, authorization, and accounting** — they are stated directly in the exam topics list.

Security Program Elements

- A **security program** is an enterprise's **set of security policies and procedures**.
- For the CCNA, there are a few elements you have to be aware of.

User Awareness Programs

- **User awareness programs** are designed to make employees aware of **potential security threats and risks**.
- Not all employees are **cyber-security experts**.
    - Example: Someone working in the HR department is probably not aware of all of the cyber threats the company is facing.
- User awareness programs will help make those employees aware.

> ***Example (user awareness program):***
>
> 1. ***A company might send out false phishing emails to make employees click a link and sign in with their login credentials***
> 2. ***Although the emails are harmless, employees who are tricked by the false emails will be informed that it is part of a user awareness program***
> 3. ***They should be more careful about phishing emails in the future***

User Training Programs

- **User training programs** are **more formal** than user awareness programs.
- Example: **dedicated training sessions** which educate users on:
    - The **corporate security policies**
    - How to create **strong passwords**
    - How to **avoid potential threats**
- These should happen:
    - When employees **enter the company**
    - At **regular intervals during the year**

Physical Access Control

- **Physical access control** protects **equipment and data** from potential attackers by only allowing **authorized users** into protected areas.
- Protected areas include:
    - **Network closets**
    - **Data center floors**

- This is **not just to prevent people outside of the organization** from gaining access to these areas.
- **Even within the company**, access to these areas should be **limited to those who need access**.
- **Multifactor locks** can protect access to these restricted areas.

> ***Example (multifactor lock):***
>
> - ***A door that requires users to swipe a badge and scan their fingerprint to enter***
> - ***That is something you have — a badge***
> - ***And something you are — your fingerprint***

- **Badge systems** are very flexible, and **permissions granted to a badge can easily be changed**.
  - Example: Permissions can be easily **removed when an employee leaves the company**, whether they return the badge or not.
- This allows for **strict, centralized control** of who is authorized to enter where.

Review of Covered Topics

- Before moving on to the quiz, the professor reviews what was covered.

Key Security Concepts

- First covered some **key security concepts**, including:
  - The **CIA triad**
  - **Vulnerabilities**
  - **Exploits**
  - **Threats**
  - **Mitigation techniques**

Common Attacks

- Then looked at some **common attacks**:
  - From **common network attacks**
  - To **social engineering attacks** which target **people, not devices**

Passwords and Multi-Factor Authentication

- Then covered **passwords and multi-factor authentication**:
  - Includes a combination of:
    - **Something you know**
    - **Something you have**
    - **Something you are**

AAA

- Then introduced **AAA**:
  - **Authentication** — the process of **verifying a user's identity**
  - **Authorization** — the process of **controlling what that user is allowed to do** in the system
  - **Accounting** — **keeping track of what the user does**

Security Program Elements

- Finally introduced some elements of an enterprise's **security programs**, such as:
  - **User awareness**
  - **User training**
  - **Physical access control**

Closing Notes

- That was **a lot to cover**.
- If you learn the information in this video, you should be **ready to answer questions** about any of these exam topics.
- In the next few videos, we'll take a **closer look at some network attacks** and **what we can do to stop them**.

- Make sure to watch until the end of the quiz for a **bonus practice question** from **Boson Software's ExSim for CCNA**.
