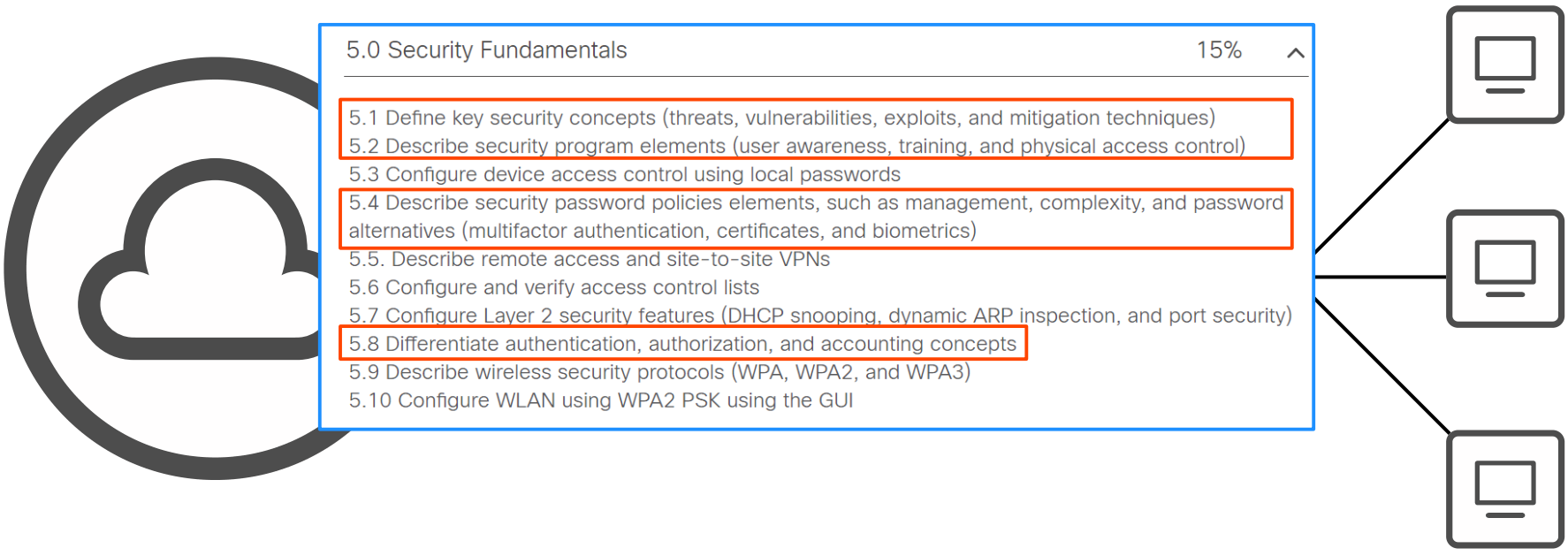
JEREMY'S IT LAB

CCNA Day 48

Security Fundamentals



Things we'll cover

- Key security concepts
- Common attacks
- Passwords/Multi-Factor Authentication (MFA)
- Authentication, Authorization, Accounting (AAA)
- Security Program Elements

Why security?

What is the purpose/goal of security in an enterprise?

The principles of the **CIA Triad** form the foundation of security:

- **C**onfidentiality
  → Only authorized users should be able to access data.
  → Some information/data is public and can be accessed by anyone, some is secret and should only be accessed by specific people.

- **I**ntegrity
  → Data should not be tampered with (modified) by unauthorized users.
  → Data should be correct and authentic.

- **A**vailability
  → The network/systems should be operational and accessible to authorized users.

Attackers can threaten the confidentiality, integrity, and available of an enterprise's systems and information.

Vulnerability, Exploit, Threat, Mitigation

- A **vulnerability** is any potential weakness that can compromise the CIA of a system/info.
  → A *potential* weakness isn't a problem on its own.

- 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 it's own.

- A **threat** is the potential of a **vulnerability** to be **exploited**.
  → A hacker **exploiting** a **vulnerability** in your system is a **threat**.

- A **mitigation technique** is something that can protect against threats.
  → Should be implemented everywhere a vulnerability can be exploited: client devices, servers, switches, routers, firewalls, etc.

<u>No system is perfectly secure!</u>

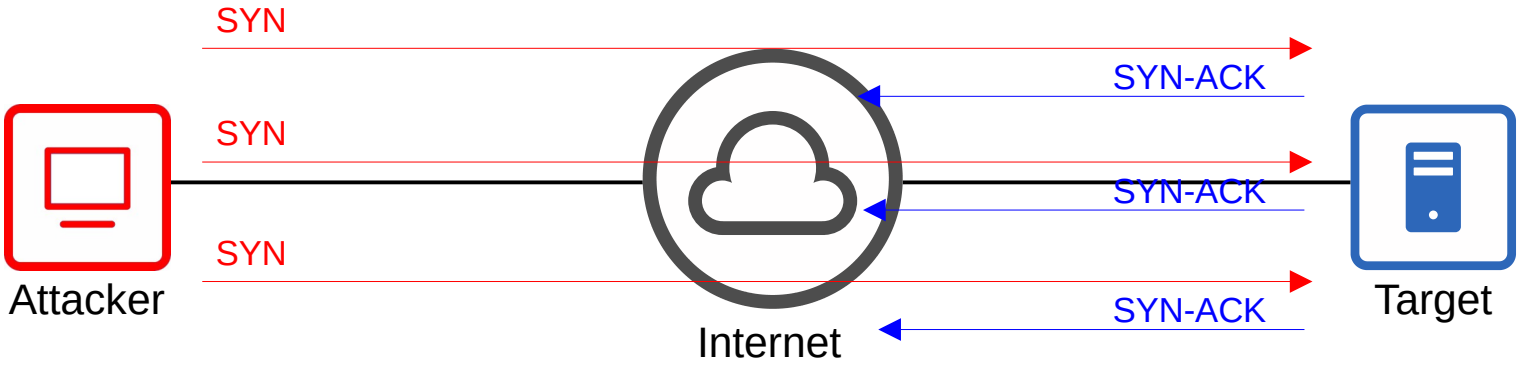
Common Attacks

- DoS (denial-of-service) attacks
- Spoofing attacks
- Reflection/amplification attacks
- Man-in-the-middle attacks
- Reconnaissance attacks
- Malware
- Social engineering attacks
- Password-related attacks

Denial-of-service attacks

- DoS attacks threaten the availability of a system.

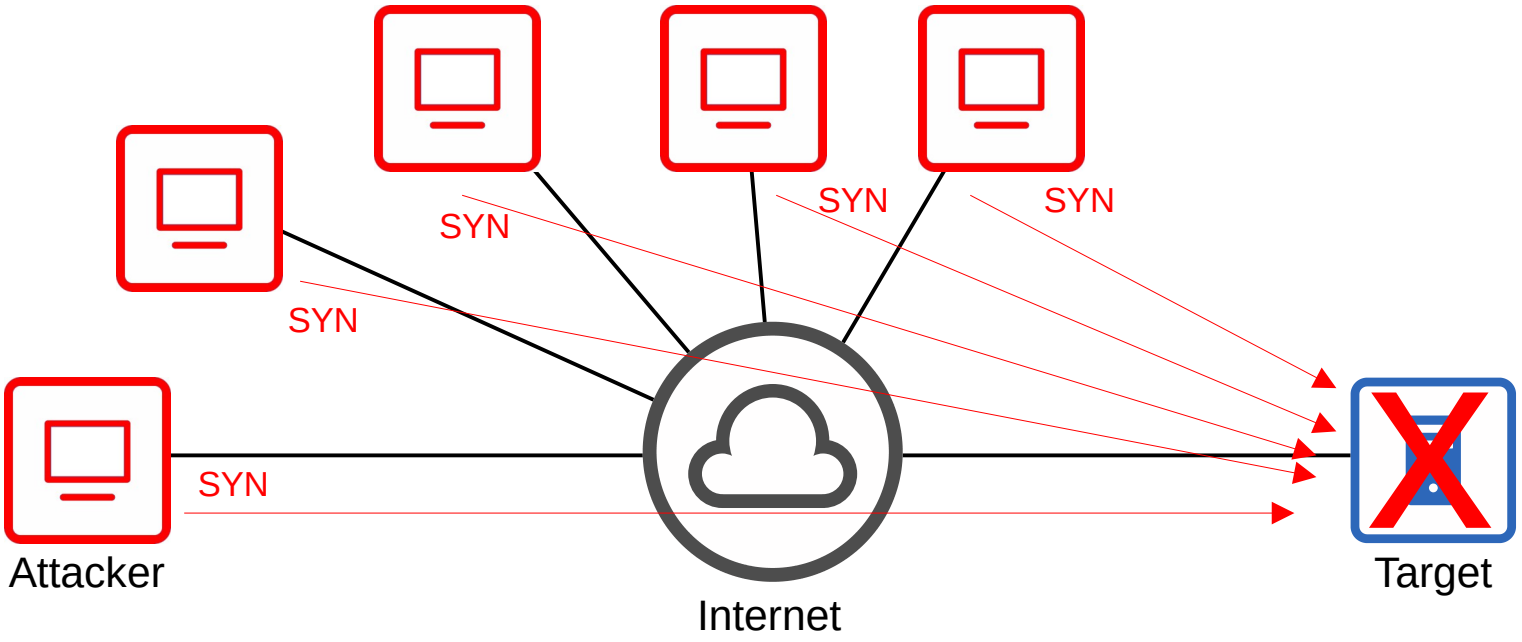
- One common DoS attack is the TCP SYN flood.
  - → TCP three-way handshake: SYN | SYN-ACK | ACK
  - → The attacker sends countless TCP SYN messages to the target.
  - → The target sends a SYN-ACK message in response to each SYN it receives.
  - → The attacker never replies with the final ACK of the TCP three-way handshake.
  - → The incomplete connections fill up the target's TCP connection table.
  - → The attacker continues sending SYN messages.
  - → The target is no longer able to make legitimate TCP connections.



Denial-of-service attacks

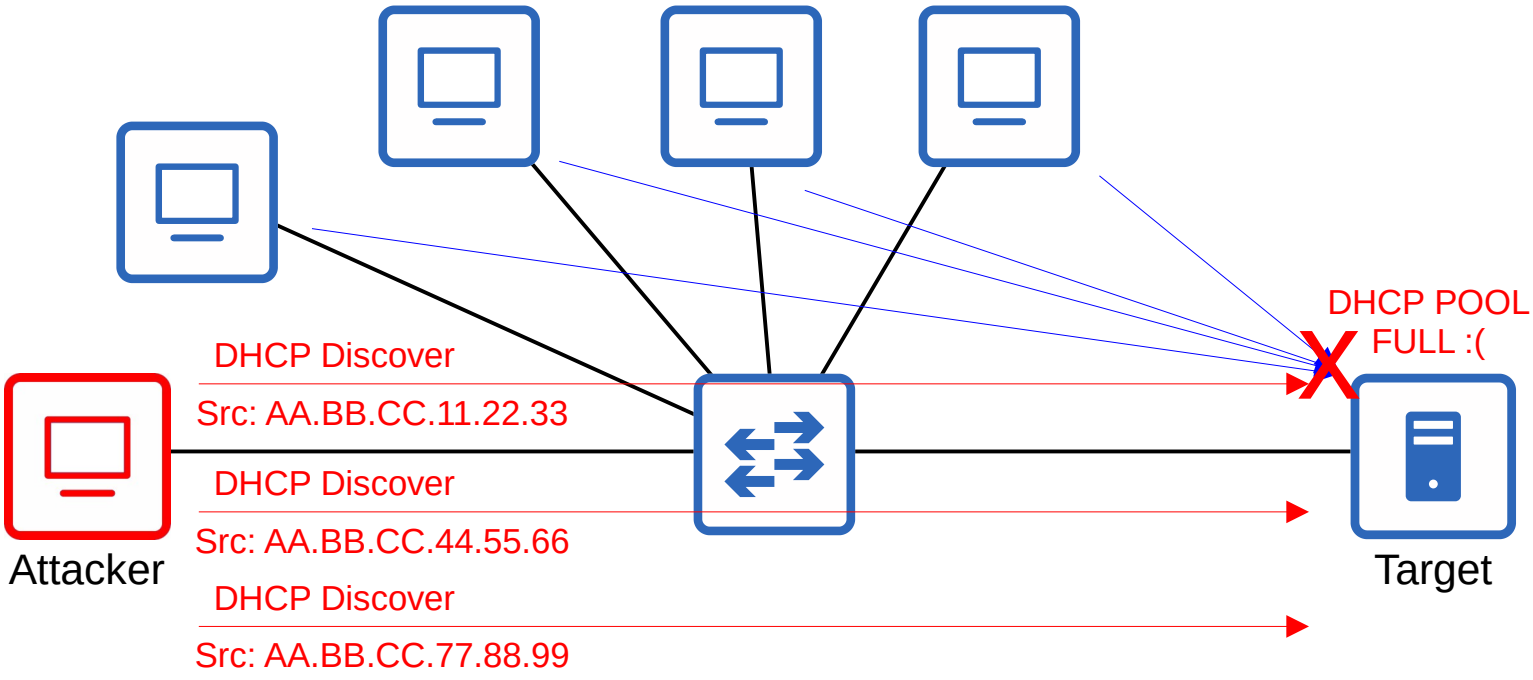
- In a DDoS (Distributed Denial-Of-Service) attack, the attacker infects many target computers with malware and uses them all to initiate a denial-of-service attack, for example a TCP SYN flood attack.

- This group of infected computers is called a **botnet**.



Spoofing attacks

- To **spoof** an address is to use a fake source address (IP or MAC address).
- Numerous attacks involve spoofing, it's not a single kind of attack.
- An example is a **DHCP exhaustion** attack.
- An attacker uses spoofed MAC addresses to flood DHCP Discover messages.
- The target server's DHCP pool becomes full, resulting in a denial-of-service to other devices.

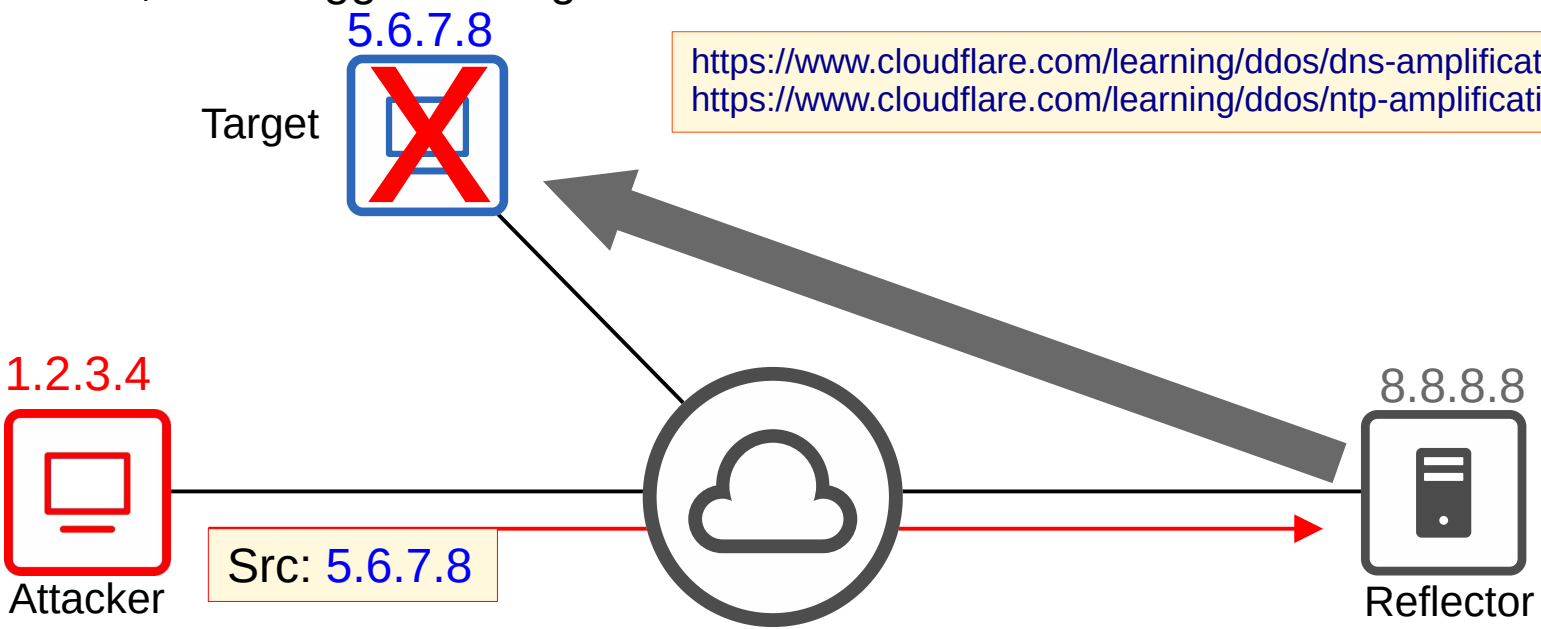


Reflection/Amplification attacks

- In a **reflection** attack, the attacker sends traffic to a reflector, and spoofs the source address of its packets using the target's IP address.
- The reflector (ie. a DNS server) sends the reply to the target's IP address.
- If the amount of traffic sent to the target is large enough, this can result in a denial-of-service.

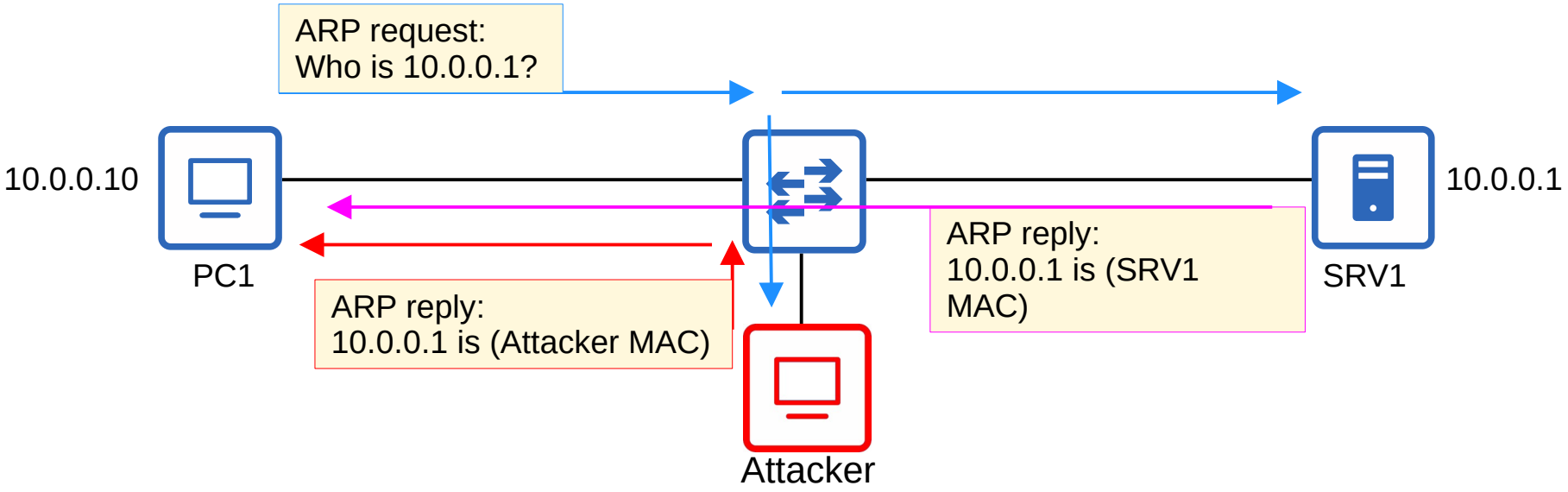
- A reflection attack becomes an **amplification** attack when the amount of traffic sent by the attacker is small, but it triggers a large amount of traffic to be sent from the reflector to the target.

https://www.cloudflare.com/learning/ddos/dns-amplification-ddos-attack/
https://www.cloudflare.com/learning/ddos/ntp-amplification-ddos-attack/



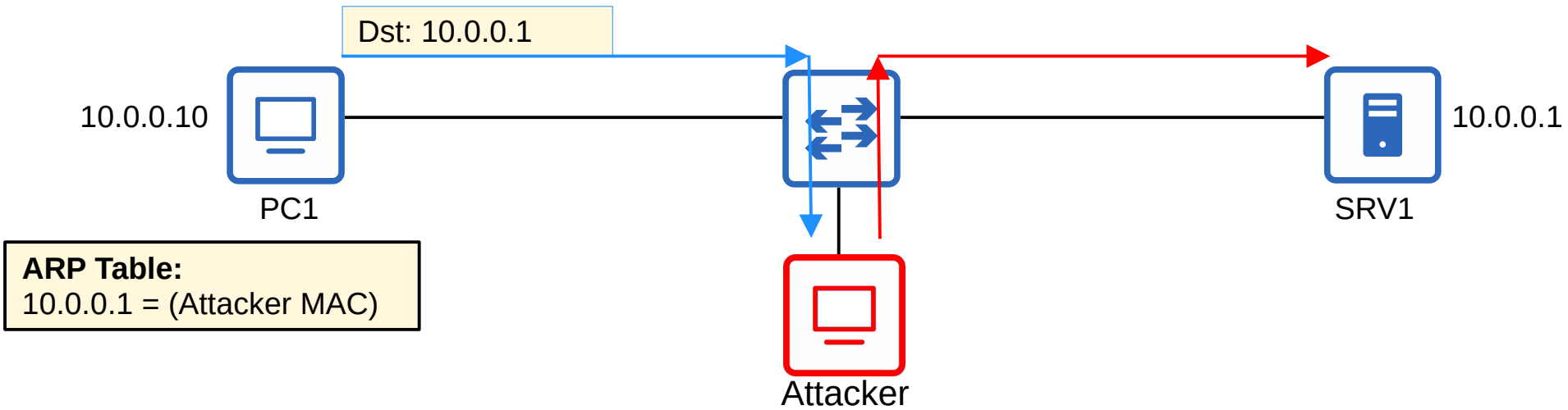
Man-in-the-middle attacks

- 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.
- A common example is **ARP spoofing**, also known as **ARP poisoning**.
- A host sends an ARP request, asking for the MAC address of another device.
- The target of the request sends an ARP reply, informing the requester of its MAC address.
- The attacker waits and sends another ARP reply after the legitimate replier.
- If the attacker's ARP reply arrives last, it will overwrite the legitimate ARP entry in PC1's ARP table.



Man-in-the-middle attacks

- In PC1's ARP table, the entry for 10.0.0.1 will have the attacker's MAC address.
- When PC1 tries to send traffic to SRV1, it will be forwarded to the attacker instead.
- The attacker can inspect the messages, and then forward them on to SRV1.
- The attacker can also modify the messages before forwarding them to SRV1.
- This compromises the **C**onfidentiality and **I**ntegrity of communications between PC1 and SRV1.



Reconnaissance attacks

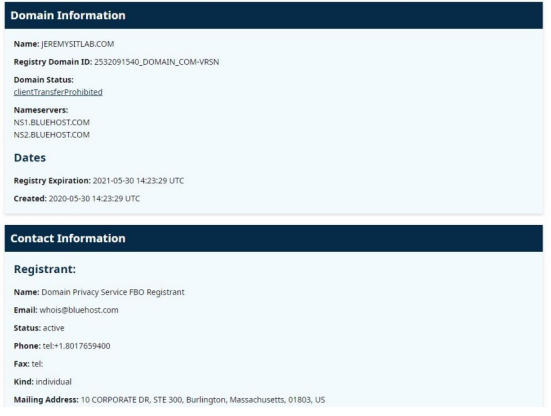
- Reconnaissance attacks aren't attacks themselves, but they are used to gather information about a target which can be used for a future attack.
- This is often publicly available information.
- ie. **nslookup** to learn the IP address of a site:

```
C:\Users\user>nslookup jeremysitlab.com
Server:  UnKnown
Address:  192.168.0.1

Non-authoritative answer:
Name:    jeremysitlab.com
Address:  162.241.216.233
```

- Or a WHOIS query to learn email addresses, phone numbers, physical addresses, etc.

https://lookup.icann.org/lookup



Domain Information

Name: JEREMYSITLAB.COM

Registry Domain ID: 2532091540_DOMAIN_COM-VRSN

Domain Status:
clientTransferProhibited

Nameservers:
NS1.BLUEHOST.COM
NS2.BLUEHOST.COM

Dates

Registry Expiration: 2021-05-30 14:23:29 UTC

Created: 2020-05-30 14:23:29 UTC

Contact Information

Registrant:

Name: Domain Privacy Service FBO Registrant

Email: whois@bluehost.com

Status: active

Phone: tel:+1.8017659400

Fax: tel:

Kind: individual

Mailing Address: 10 CORPORATE DR, STE 300, Burlington, Massachusetts, 01803, US

Malware

- Malware (malicious software) refers to a variety of harmful programs that can infect a computer.

- **Viruses** infect other software (a ‘host program’). The virus spreads as the software is shared by users. Typically they corrupt or modify files on the target computer.

- **Worms** do not require a host program. They are standalone malware and they are able to spread on their own, without user interaction. The spread of worms can congest the network, but the ‘payload’ of a worm can cause additional harm to target devices.

- **Trojan Horses** are harmful software that is disguised as legitimate software. They are spread through user interaction such as opening email attachments, or downloading a file from the Internet.

The above malware types can exploit various vulnerabilities to threaten any of the CIA of the target device.
*there are many types of malware!

Social Engineering attacks

- Social engineering attacks target the most vulnerable part of any system – people!
- They involve psychological manipulation to make the target reveal confidential information or perform some action.

- **Phishing** typically involves fraudulent emails that appear to come from a legitimate business (Amazon, bank, credit card company, etc) and contain links to a fraudulent website that seems legitimate.
  Users are told to login to the fraudulent website, providing their login credentials to the attacker.
  → **spear phishing** is a more targeted form of phishing, ie. aimed at employees of a certain company.
  → **whaling** is phishing targeted at high-profile individuals, ie. a company president.
- **Vishing** (voice phishing) is phishing performed over the phone.
  → '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?'
- **Smishing** (SMS phishing) is phishing using SMS text messages.

- **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.

- **Tailgating** attacks involve entering restricted, secured areas by simply walking in behind an authorized person as they enter.
  Often, the target will hold the door open for the attacker to be polite, assuming the attacker is also authorized to enter.

Social Engineering attacks

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

Password-related attacks

- Most systems use a username/password combination to authenticate users.

- The username is often simple/easy to guess (for example the user's email address), and the strength and secrecy of the password is relied on to provide the necessary security.

- Attackers can learn a user's passwords via multiple methods:
  → Guessing
  → **Dictionary attack**: A program runs through a 'dictionary' or list of common words/passwords to find the target's password.
  → **Brute force attack**: A program tries every possible combination of letters, numbers, and special characters to find the target's password.

- Strong passwords should contain: →at LEAST 8 characters (preferably more).
  →a mixture of UPPERCASE and lowercase letters.
  →a mixture of letters and numbers.
  →one or more special characters (# @ ! ? etc.)
  + should be changed regularly

Common Attacks

- DoS (denial-of-service) attacks
  - → target the availability of a system so users can't access it
- Spoofing attacks
  - → involve using fraudulent source IP/MAC addresses
- Reflection/amplification attacks
  - → involve spoofing a source IP address to cause a reflector to send lots of traffic to the target
- Man-in-the-middle attacks
  - → an attacker intercepts traffic between the source and destination to eavesdrop and/or modify the traffic
- Reconnaissance attacks
  - → used to gather information on the target to perform future attacks
- Malware
  - → malicious software such as viruses, worms, and trojan horses that infect a system
- Social engineering attacks
  - → attacks that use psychological manipulation to target people and make them reveal info or perform an action
- Password-related attacks
  - → attacks such as dictionary attacks and brute force attacks, used to guess the target's password

Multi-factor authentication

- **Multi-factor authentication** involves providing more than just a username/password to prove your identity.
- It usually involves providing two of the following (=two-factor authentication):

- **Something you know**
  → a username/password combination, a PIN, etc.

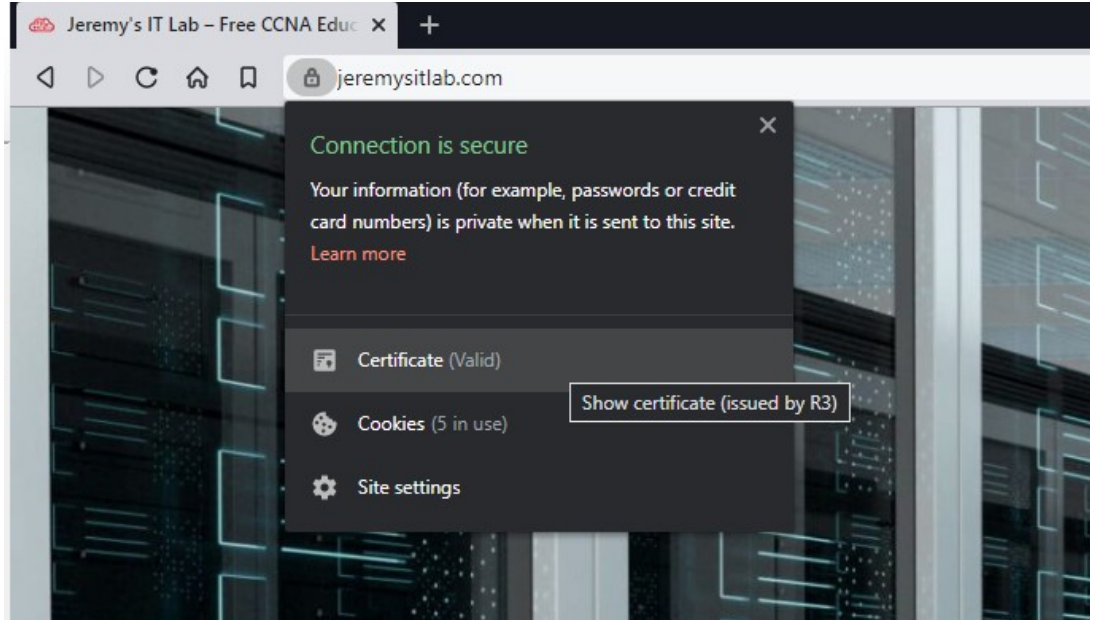
- **Something you have**
  → pressing a notification that appears on your phone, a badge that is scanned, etc.

- **Something you are**
  → biometrics such as a face scan, palm scan, fingerprint scan, retina scan, etc.

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

Digital certificates

- **Digital certificates** are another form of authentication used to prove the identity of the holder of the certificate.
- They are used for websites to verify that the website being accessed is legitimate.
- Entities that want a certificate to prove their identity send a CSR (Certificate Signing Request) to a CA (Certificate Authority), which will generate and sign the certificate.



Controlling and monitoring users with AAA

- **AAA** (triple-A) stands for **A**uthentication, **A**uthorization, and **A**ccounting.
- It is a framework for controlling and monitor users of a computer system (ie. a network).

- **Authentication** is the process of verifying a user's identity.
  → logging in = authentication

- **Authorization** is the process of granting the user the appropriate access and permissions.
  → granting the user access to some files/services, restricting access to other files/services = authorization

- **Accounting** is the process of recording the user's activities on the system.
  → logging when a user makes a change to a file = accounting

- Enterprises typically use a AAA server to provide AAA services.
  → ISE (Identity Services Engine) is Cisco's AAA server.

- AAA servers usually support the following two AAA protocols:
  → RADIUS: an open standard protocol. Uses UDP ports 1812 and 1813.
  → TACACS+: A Cisco propriety protocol. Uses TCP port 49.

- For the CCNA, know the differences between Authentication, Authorization, and Accounting.

Security Program Elements

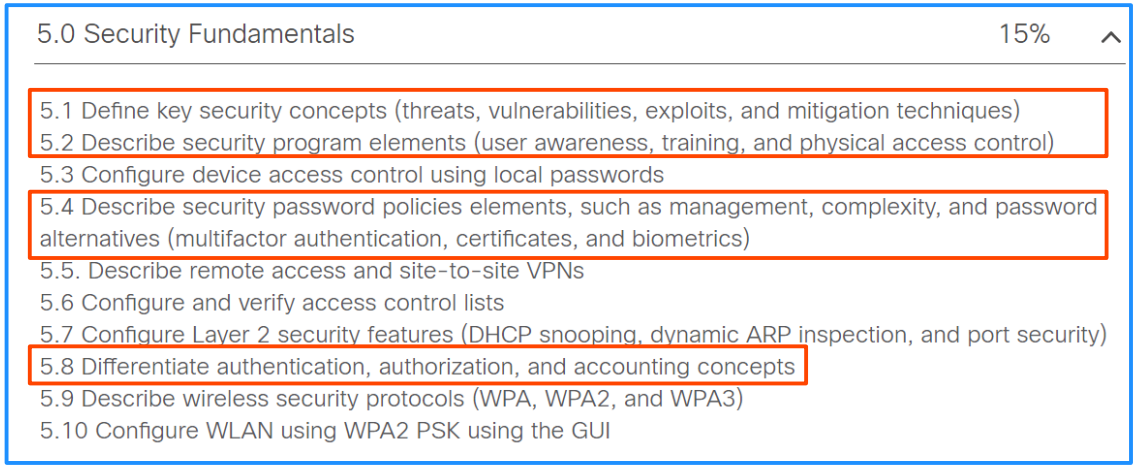
- **User awareness** programs are designed to make employees aware of potential security threats and risks.
  → For example, a company might send out false phishing emails to make employees click a link and sign in with their login credentials.
  →Although the emails are harmless, employees who fall for the false emails will be informed that it is part of a user awareness program and they should be more careful about phishing emails.

- **User training** programs are more formal than user awareness programs.
  → For example, dedicated training sessions which educate users on the corporate security policies, how to create strong passwords, and how to avoid potential threats.

- **Physical access control** protects equipment and data from potential attackers by only allowing authorized users into protected areas such as network closets or data center floors.
  → Multifactor locks can protect access to restricted areas.
    → ie. a door that requires users to swipe a badge and scan their fingerprint to enter.
    → Permissions of the badge can easily be changed, for example permissions can be removed when an employee leaves the company.

Things we'll cover

- Key security concepts
- Common attacks
- Passwords/Multi-Factor Authentication (MFA)
- Authentication, Authorization, Accounting (AAA)
- Security Program Elements



Quiz 1

Which part of the CIA triad ensures that systems are running and accessible by users?

a) Confidentiality

b) Integrity

c) Authentication

d) Availability

e) Authorization

f) Accounting

Quiz 2

Which of the following terms refers to the real possibility that a potential weakness is taken advantage of to attack a system?

a) Threat

b) Vulnerability

c) Exploit

d) Mitigation technique

Quiz 3

Your company implements door locks that require a badge to be scanned and a pass code to be entered. What is this an example of? (select the two best answers)

a) User training

b) User awareness

c) Physical access control

d) Multi-factor authentication

e) AAA

f) Biometrics

Quiz 4

Which of the following is NOT an example of multi-factor authentication?

a) Swiping a key card and then doing a retina scan.

b) Entering a password and then tapping a notification on your phone.

c) Doing a retina scan and then doing a fingerprint scan.

d) Swiping a key card and then entering a PIN.

Quiz 5

Which of the following is considered Accounting in the AAA model?

a) Granting a user permission to modify a file.

b) Using MFA to verify a user’s identity.

c) Restricting a using from viewing a file.

d) Logging the date and time a user logged in to the system.