



**Romel Cabling** ▾



[Home](#)

[Home](#) > [My courses](#) > [121 - ITSP2B](#) > [01 Exploring Security Threats](#) > [Lesson Proper for Week 1](#)

# Lesson Proper for Week 1

## EXPLORING SECURITY THREATS

This certification focuses on understanding threats to secure your network using Cisco routers and switches and even configuring and setting up the Cisco Adaptive Security Appliance (ASA). After completion, you'll be able to function as a network security engineer and mitigate and prevent such threats from entering your network. This chapter covers the basic principles of implementing network security in an enterprise network. Security is very important and if no proper security principles are followed, it will lead to financial risks, legal risks, and negative public relations implications. In some cases, the overall business may be placed at risk due to the noncompliance of security policies. The security of an enterprise network can be viewed from different perspectives. For a management team, the network is a tool that enables the business goals of the company. For end users, a network is just a tool for them to complete their job. Unfortunately, if an end user or a management team is not maintaining their data safely, it may lead to several vulnerabilities and security threats. If the hacker compromises and gains access to the data and applications, the security component of the network fails.

The following topics are the three basic concepts of network security:

- **Confidentiality:** The privacy of the data in the network. The data on the network should be protected from unauthorized users and they should not access the data by any means. The data can be protected by encrypting it.
- **Integrity:** The changes made to the data should only be made by the authorized users. If the data in transit is corrupted, it leads to a failure of integrity and a loss of revenue.
- **Availability:** A network, or data, should be available to its authorized users. The term availability refers to the provision of services that are dependent on networks, systems, and data. Any impact on the availability of the leads to heavy loss of business and revenue.



The following diagram illustrates the working mechanism of the network security concept better known as the **CIA triad**:



After completing this chapter, you will:

- Understand the basics of network security
- Understand the different security terminologies
- Understand different types of attack
- Understand the different types of security tools

## IMPORTANT TERMS IN NETWORK SECURITY

Network security is a very broad concept; it starts with authenticating users and authorizing resources. It deals with security threats analysis and vulnerability checks.

### 1. Threats

A **threat** is the potential for an attacker to take advantage of a vulnerability on a system. An example of a threat can be a disgruntled employee who has been given a warning letter in an organization. This person may want to inflict harm to the company's network and has decided to research exploitation.

Some further examples of threats include malware, **Denial of Service (DoS)**, and phishing.

Let's now discuss risk and countermeasure:

- **Risk:** A risk is the likelihood of a threat actor taking advantage of a vulnerability that can attack a network system, which leads to damage to the network.



- **Countermeasure:** A countermeasure can be a combination of a process and a device that can act together as a safeguard against potential attacks, thereby reducing security risks.

## 2. Vulnerability

**Vulnerability** is a weakness of the system, data, or any application, by which unauthorized persons can exploit it. Vulnerability on the network may occur due to various reasons:

- Result of a malicious attack
- Failure of a policy
- Weakness of the system or a policy
- Weakness of a protocol

Vulnerabilities are found in operating systems, routers, switches, firewalls, applications, antivirus software, and so on. An attacker uses these vulnerabilities to create a threat to the network. Generally, vulnerabilities arise due to high complexity or human error while developing an application and designing a network.

## 3. Analyzing Vulnerability

Vulnerability analysis is the process of identifying security weaknesses on a computing platform or network. This aids the internal security team (blue team) in remediating any flaws that have been discovered. A security team is also responsible for conducting a vulnerability assessment to evaluate the cybersecurity risk and try to minimize/mitigate it as much as possible. Vulnerability assessments are usually conducted before and after applying any countermeasures within the organization. This helps with the evaluation process to determine whether the attack surfaces are reduced; it also ensures the proper practices are used and applied correctly.

When an administrator dealing with security installs a patch on the endpoint security tool, there are chances of manual errors or misconfigurations in the tool that may open a door for a hacker to attack the node.

Periodic vulnerability testing/analysis is essential in such situations.

Vulnerability assessments have the following advantages:



- Help administrators to keep their data safe from hackers and attackers, which eliminates business risks.
- Vulnerability assessment tools help administrators to check for loopholes in the network architecture. These tools also examine whether there are any possible destructive actions that can cause damage to your application, software, or network.
- Vulnerability assessment tools detect attack pathways that may get missed in manual assessment, which increases the ROI.

Before performing a vulnerability assessment, the administrators should create a test plan, develop a threat model and verify the URLs, and access credentials.

There are two ways of conducting a vulnerability assessment. The first one is **the automated dynamic scanning** and the other is the manual **Vulnerability** and **Penetration Testing (VAPT)**.

In the automated method, a tool, such as *Burp Suite Pro*, *IBM Rational AppScan*, is used to scan the application and find security flaws. The manual testing is performed in the following steps:

1. Check SQL injection, XML injection, and LDAP injection flaws
2. Inspect poor authentication methods and cracked login processes
3. Inspect cookies and other session details
4. Inspect the default settings in the security configurations in the devices
5. Inspect broken encryption algorithms and other ciphers to secure the communications

Choose either automatic or manual testing methods to verify the scan results, collect evidence, and complete the reports.

## INTRODUCTION TO AN ATTACK

An attack is the process of attempting to steal data, destroy data, gain unauthorized access to a device, or even shut down/disable a system, preventing legitimate users from accessing the resources. An attack can be local, where a malicious user has physical access to the system and either executes a malicious payload or is attempting to gain access into the device. A remote attack requires the malicious user to send a payload over a network connection to the victim device in the hope that the attack would be successful and it would either gain control of the victim device or cause service interruptions (denial of service).



Attacks are mainly distinguished as either:

- Passive attacks
- Active attacks

## 1. Passive Attacks

In a passive attack, the attacker is considered to be in a learning (monitoring) state to understand the details about the potential victim's device, how it performs and operates. This allows the attacker to have a better attack strategy. An example of a passive attack is where an attacker is sniffing the network traffic between a victim machine and its default gateway.

Types of passive attack:

**Sniffing:** Capturing packets unknown to users on the network. The goal is to obtain any sensitive information sent across the network.

**Port scanning:** Checking for open TCP and UDP ports. This will aid the attacker in determining the services running on the target/victim machine.

## 2. Active Attacks

In an active attack, the attacker may have already done enough reconnaissance on the target device and is ready to execute its exploit against the victim. Sometimes, the attack can be a direct attack, meaning the exploit is sent from the attacker's machine to the target, or an indirect attack, where the attacker compromises another machine, making it a zombie, and using the zombie to pivot all the attacks through it. Therefore, the zombie would seem to be the attacker machine from the view of the victim.

Examples of active attacks include:

**Denial of Service:** This attack focuses on exhausting the resources of a system, therefore legitimate users are not given access to the resource.

**Botnet:** The attacker sets up a **Command and Control (CnC)** server to control all its infected machines (zombies) to carry out malicious activities.

## 3. Spoofing Attacks



In a spoofing attack, the attacker uses false information to pretend to be a legitimate or authorized user/machine. When an attacker attempts to exploit a system or deliver a payload, they have to try to trick the user into falling victim to the attack. Sometimes, changing the source IP address and source MAC address of the packets originating from the attacking machine may trick the potential victim into thinking it's from a legitimate user and may disguise the attack's origins.

## **INTERNET PROTOCOL – THE HEART OF INTERNET COMMUNICATION**

Internet Protocol (IP) is a connection protocol that exists at the Network layer (layer 3) of the Open Systems Interconnection (OSI) reference model. Internet protocol is used to assist routers or any layer 3 devices to forward packets to their corresponding destinations. One main characteristic of internet protocol is its nature of being a connectionless protocol, which means it provides delivery using best effort and is not guaranteed to be delivered to the recipient. Since IP is said to be connectionless, it depends on the upper layers to assist with the delivery of data. The layer above the Network layer is known as the Transport layer. There are two sub protocols, which are used primarily for delivery; these are known as the User Datagram Protocol (UDP) and the Transmission Control Protocol (TCP). An IP packet contains the following: source and destination IP addresses, version (IPv4 or IPv6), Time to Live (TTL) value, protocol (TCP, UDP, or ICMP), and flags.

It is through the forging of this source address that hackers are able to break into the network and mislead communication between the source and the destination. Almost all networks use routers as intermediate devices for the transmission of data. When the data is sent via routers, they identify the destination IP address from the header of the IP datagram to forward the packets to that destination. The source address is ignored by the routers. The source address is used only by the destination machine when a reply is sent back for the received packets.

## **HOW IS AN IP DATAGRAM SPOOFED?**

In an IP packet/datagram, the header contains the addressing information, such as the sender's source and the destination's IP address. An IP packet is usually unencrypted, therefore if someone is sniffing the traffic between the sender and the receiver, the contents of the packet and its header information are captured. A malicious user or an attacker can modify the IP address on the IP packets originating from the attacker machine, making it seem to originate from somewhere else, which is known as IP spoofing. It tricks a potential victim into believing the IP packet came from a legitimate or trusted source, but is actually from a malicious user. The operating system has no way of determining whether the IP addresses actually belong to the legitimate machine or not. When the internet protocol was built, security was not a concern at the time, hence IP lacks security features.

There are different types of spoofing attacks:

- Address Resolution Protocol spoofing
- DNS spoofing



## 1. IP Spoofing

Using the following scenario, an attacker sends a specially crafted packet to the web server (200.1.1.1). Within the IP header of the specially crafted packet, it has a source IP address of 203.155.182.1, which belongs to the potential victim machine and not the real IP address of the attacker. When the web server receives the packet and has to respond, it sees the sender's IP address is 203.155.182.1 and sends its response to the victim machine instead of the attacker:



Attackers primarily use IP spoofing as a technique to bypass any filters, access lists, or even security appliances that act as countermeasures for spoofing attacks. The goal is to find a way into a network by tricking the system into believing it's a legit packet.

In this method, the attacker creates IP packets with a fake source IP address to hide the identity of the sender. Attackers use IP spoofing to overcome security measures, such as authentication-based IP networks. Attackers use randomly chosen IP address and spoof the original IP address to perform the DoS attack.

When two computers communicate, information about the IP address is placed on the source field of the packet. In an IP spoofing attack, the source IP address in the packet is not the original IP address of the source computer. By modifying the source IP address, the original sender can make the victim machine think the message originated from another source and therefore the sending machine or the attacker will be protected from being tracked.

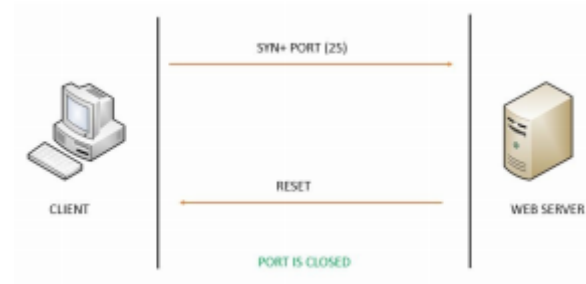
Various options where IP spoofing can be used:

- Scanning
- Hijacking an online session
- Flooding

### A. Scanning



Scanning is a process in which a malicious user sends probes to a victim machine to determine TCP/UDP open ports, the type of operating system and version, services running on the victim machine, and vulnerabilities:



During the scanning phase, the attack may notice whether port 80 is open or not on the target device. If port 80 is open, we can determine there is a web server daemon running on the target device. The attacker can then use the Telnet protocol to perform banner-grabbing on the victim using port 80 as the destination port. This will determine the type and version of the web server, whether it's Microsoft IIS, Apache, or even nginx. Knowing this information will aid the attacker in fine-tuning their payload for the target device.

## B. Hijacking an online session

In a session hijacking attack, an attacker can capture the cookie from a user who has logged on to a website and uses data found inside the cookie to also log on to the same website without having to enter a username and password combination. This would allow the attacker to gain access to the user (victim) account details.

## C. Flooding

In a flooding attack, the attacker sends unsolicited packets to the target continuously until the target is overwhelmed. The target will need to process each packet it receives, but due to the high influx of packets received, the target would eventually be unable to respond to a legitimate request from users or perform any further action.

◀ Preliminary Activity for Week 1

Jump to...



Analysis, Application, and Exploration For Week 1 ▶



## Navigation

Home

Dashboard

Site pages

My courses

121 - CC106

121 - BPM101 / DM103

121 - OAELEC2





121 - ITE3

121 - MUL101

121 - ITSP2B

Participants


 Grades


General

01 Exploring Security Threats

 Preliminary Activity for Week 1

 **Lesson Proper for Week 1**

 Analysis, Application, and Exploration For Week 1

 Generalization for Week 1

 Evaluation for Week 1

 Assignment for Week 1

02 Delving into Security Toolkits

03 Intrusion Prevention System

04 Understanding Security Policies I

05 Understanding Security Policies II

06 - Preliminary Examination

07 Deep Diving into Cryptography

08 Deep Diving into Cryptography: Types of Cipher

09 Implementing the AAA Framework

10 Implementing the AAA Framework: Implementing A...

11 Securing the Control and Management Planes

12 - Midterm Examination

13 Protecting Layer 2 Protocols

14 Protecting the Switch Infrastructure

15 Exploring Firewall Technologies I

16 Exploring Firewall Technologies II

17 Cisco ASA

121 - WEB101 / CCS3218

Courses

---

## Fair Warning

**NOTICE:** Please be reminded that it has come to the attention of the Publishing Team of eLearning Commons that learning materials published and intended for **free use only by students and faculty members within the eLearning Commons network were UNLAWFULLY uploaded in other sites without due and proper permission.**

**PROSECUTION:** Under Philippine law (Republic Act No. 8293), copyright infringement is punishable by the following: Imprisonment of between 1 to 3 years and a fine of between 50,000 to 150,000 pesos for the first offense. Imprisonment of 3 years and 1 day to six years plus a fine of between 150,000 to 500,000 pesos for



the second offense.

**COURSE OF ACTION:** Whoever has maliciously uploaded these concerned materials are hereby given an ultimatum to take it down within 24-hours. Beyond the 24-hour grace period, our Legal Department shall initiate the proceedings in coordination with the National Bureau of Investigation for IP Address tracking, account owner identification, and filing of cases for prosecution.

---

## 2nd Semester Enrollment



visit [www.bcp.edu.ph](http://www.bcp.edu.ph)

# Enrollment registration is now Ongoing

## For 2nd Semester SY 2021 - 2022

We are accepting new students, returnees and transferees.





"Be trained to be the best,  
Be linked to success"

 [bcp-inquire@bcp.edu.ph](mailto:bcp-inquire@bcp.edu.ph)  (8)442-8601 | (8)518-8050

The banner features a blue-tinted background image of a multi-story building with a 'BCP' sign on the roof. A large white diagonal banner contains the main text. At the bottom, there are contact details and a quote. A small circular logo is visible on the right side of the banner.

---

## Activities

-  Assignments
-  Forums
-  Quizzes
-  Resources

