

Padernos Andre T.

BS601

Laboratory Exercise

Active Attack Vs Passive Attack

Objective:

At the end of the exercise, the students should be able to:

- Describe each classification of security attacks.

Requirement:

- Microsoft Word

Procedures:

1. Read the blog post entitled “Active Attack Vs Passive Attack” by Hassan, N. below.

The internet is full of risks! Whenever you go online, there is a possibility that you will encounter a risk. Within that range of risks, there are different types of computer threats with varying associations of damaging effects. For example, some threats may damage or corrupt your installed operating system and force you to reinstall it. Another type may steal your credentials and saved passwords. Still, other threats may not bring any harm to your PC; instead, they will track your online activities and invade your privacy.

Today, criminals are smarter than ever before, and malicious programs are more sophisticated. Modern malware can infect a target PC and remain undetected for a long time; the advance of computing power makes it possible to crack difficult passwords in a fraction of seconds. The motive behind the majority of cyberattacks nowadays is not to damage your machine, but instead to steal your money, access your private information, or acquire your login credentials. Conceptually, cybersecurity risks can be divided into two main categories: passive and active attacks.

In a passive attack, an intruder monitors a system and network communications and scans for open ports and other vulnerabilities. For example, they might exploit an unpatched system or take advantage of an expired certificate on a security device. Once the intruder has infiltrated the network, they can collect information in a couple of ways. In a footprinting passive attack, the intruder will try to collect as much intelligence as they can to use it later to attack the target system or network in a later step. Detecting a passive attack is very difficult and impossible in many cases because it does not involve data alteration in any way. However, you can implement protective measures to stop it, including:

- Using encryption techniques to scramble messages, making them unreadable for any unintended recipients.
- Avoid posting sensitive information publicly (e.g., private and company information) that can be used by outside hackers to invade your private network.

An active attack involves using information gathered during a passive attack to compromise a user or network. Hackers attempt to modify the integrity and availability of the information they have intercepted to gain access or greater privileges. Although a user will more likely become aware of an active attack than a passive one, the root cause of active attacks is hard to determine without proper monitoring and protection

of human and machine identities. To avoid this attack, the attitude of individuals and organizations needs to change to prevent cyber-attacks. There must be a fundamental understanding that, when online, everyone is a target and that none of us are too small or unimportant.

2. Answer the following questions:

- a. What is the article all about? Summarize the article in at least seven (7) sentences.

The article is all about active attack vs passive attack, there is a chance that you will be exposed to a risk whenever you go online. There are other types of computer dangers within that risk range, each with its own set of detrimental effects. Some attacks, for example, can harm or corrupt your installed operating system, forcing you to reinstall it. We all know that we live in a modern world right now where technology is very innovative, so is the criminals they're also smarter than ever before and malicious programs are more sophisticated.

Cybersecurity threats are divided into two categories: passive and active attacks. In a passive assault, no data is modified, and the target is unaware of it unless they have a mechanism in place to monitor and safeguard machine identities. During an active attack, system resources and data are manipulated or otherwise damaged, causing the system to stop functioning normally. Although an active attack is more likely to be detected than a passive attack, the root cause of active attacks is difficult to pinpoint without effective monitoring and protection of human and machine identities.

- b. Compare and contrast active and passive attacks.

Active vs. Passive Assaults The main distinction between active and passive attacks is that in active attacks, the attacker intercepts the connection and alters the data. In contrast, in a passive attack, the attacker intercepts transit data with the aim of reading and analyzing it rather than modifying it. Threats, attacks, and vulnerabilities of numerous forms exist to corrupt and breach system security. Computer assaults that compromise the system's security are known as security attacks. Security attacks can be divided into two types: active and passive attacks, in which the attacker gains unauthorized access to the system's resources.

The key differences between active and passive attacks

1. The message is modified as part of the active attack. In passive attacks, on the other hand, the attacker does not make any changes to the intercepted data.
2. The active attack does significant damage to the system, whilst the passive attack has no effect on the system's resources.
3. A passive attack is regarded as a danger to data security. An active attack, on the other hand, poses a threat to the data's integrity and availability.
4. In the case of an active attack, the attacked entity is aware of the attack. In the passive attack, on the other hand, the victim is completely oblivious of the attack.
5. The active attack is carried out by taking physical control of the communication channel in order to intercept and insert data. In a passive attack, on the other hand, the attacker just needs to observe the transmission.

Active and passive attacks can be distinguished based on what they are, how they are carried out, and how much harm they inflict to system resources. However, the active attack mostly alters information and does significant harm to system resources, potentially affecting its operation.

- c. What are your recommendations to prevent these attacks?

Using strong network encryption technologies is the best strategy to prevent a Passive attack. This means that the original communication should be well encrypted at the sender's end into an unintelligible language, and then decoded into an understandable language at the receiver's end. Active attacks can be prevented and protected with the deployment of powerful firewalls and a strong intrusion prevention system.

3. Place your answer on MS Word. Once done, save your work with the filename <**Last name_First name_TP2**> (ex. Magpili_Carlo_Lab3) and call the attention of your instructor. Have it saved on his/her FTP account.

GRADING RUBRIC:

Criteria	Performance Indicator	Points
Content	Correct ideas, concepts, descriptions, and feedback were included.	20
Relevance	The student's explanation is relative to the correct concepts.	20
Organization	Ideas and concepts were presented in an organized manner.	10

Total	50
-------	----

Reference:

Hassan, N. (2020, July 1). *Active attack vs passive attack*. Retrieved from <https://www.venafi.com/blog/active-attack-vs-passive-attack/> on February 24, 2021