CMT310 Lab Instructions

Introduction:

This work is expected to be completed in 1:30 hours. Please pay attention to the tasks need to be performed. Their expected time duration is also specified along with each task.

Learning Outcomes:

1. The students will learn/revise some important filters of Wireshark, and will attempt to understand the packet communications in a .pcap file.

2. The students will be able to create attack scenarios for insider and outsider threats, single and coordinate attacks, understand attacker's motivation and capabilities, and explore possible vulnerabilities/threats in the system.

TASK 1: 60 min.

Go through Wireshark guide (Introduction) available on Learning Central. Note that Current software version may change, hence, snapshots might be different than what is shown in the document.

Open "Wireshark", and then use the "File" menu and the "Open" command to open the file "Exercise One.pcap" (uploaded on Learning Central). You should see 26 packets listed. This set of packets describes a 'conversation' between a user's client and a central server. This entire conversation happens automatically, after a user types something and hits enter. Look at the packets to answer the following questions in relation to this conversation. In answering the following questions, use brief descriptions. For example, "In frame X, the client requests a web page, and in frame Y, the server delivers the content of the page."

a) What is the IP address of the client that initiates the conversation?

b) Use the first two packets to identify the server that is going to be contacted. List the common name, and three IP addresses that can be used for the server.

c) What is happening in frames 3, 4, and 5?

d) What is happening in frames 6 and 7?

e) Ignore frame eight. However, for your information, frame eight is used to manage flow control.

f) What is happening in frames 9 and 10? How are these two frames related?

g) What happens in packet 11?

h) After the initial set of packets is received, the client sends out a new request in packet 12. This occurs automatically without any action by the user. Why does this occur? See the "Hits Versus Page Views" in the Appendix of the guide "Wireshark Introduction".

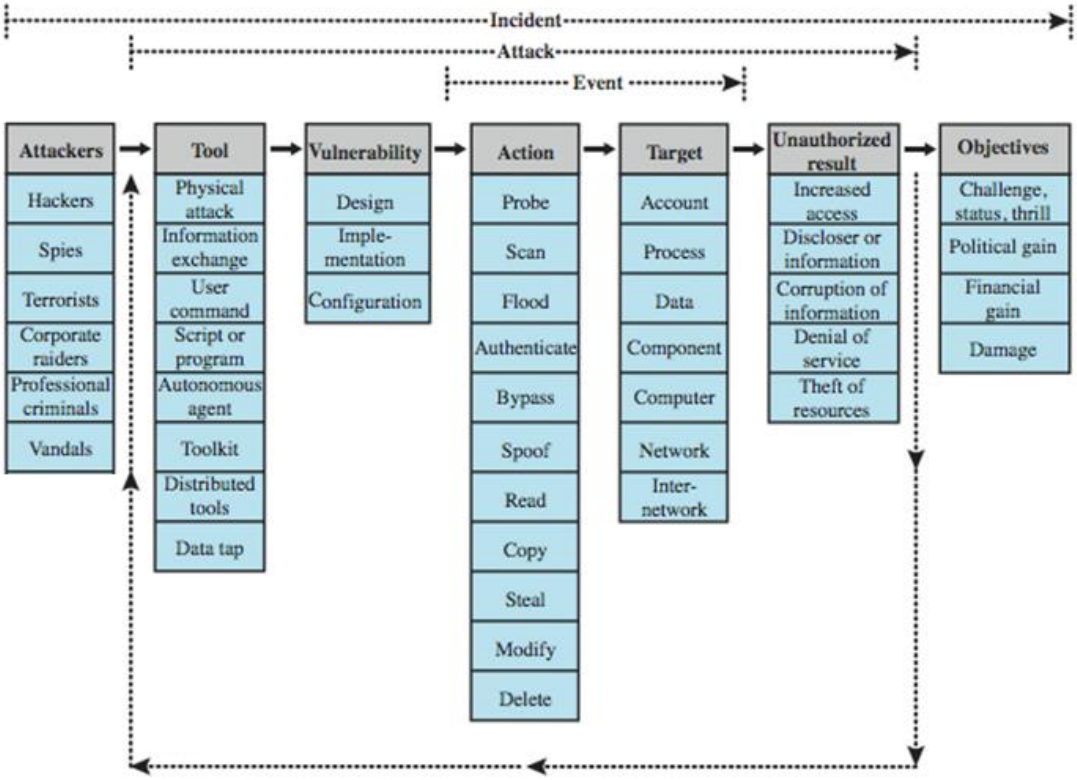
i) What is occurring in packets 13 through 22?

j) Explain what happens in packets 23 through 26. See the "Hint" in the Appendix.

k) In one sentence describe what the user was doing in (j) (Reading email? Accessing a web page? FTP? Other?).

TASK 2: 30 min.

Carefully look at the below figures and perform actions as asked at the end:



Threat Consequence	Threat Action (Attack)
Unauthorized Disclosure A circumstance or event whereby an entity gains access to data for which the entity is not authorized.	**Exposure:** Sensitive data are directly released to an unauthorized entity. **Interception:** An unauthorized entity directly accesses sensitive data traveling between authorized sources and destinations. **Inference:** A threat action whereby an unauthorized entity indirectly accesses sensitive data (but not necessarily the data contained in the communication) by reasoning from characteristics or byproducts of communications. **Intrusion:** An unauthorized entity gains access to sensitive data by circumventing a system's security protections.
Deception A circumstance or event that may result in an authorized entity receiving false data and believing it to be true.	**Masquerade:** An unauthorized entity gains access to a system or performs a malicious act by posing as an authorized entity. **Falsification:** False data deceive an authorized entity. **Repudiation:** An entity deceives another by falsely denying responsibility for an act.
Disruption A circumstance or event that interrupts or prevents the correct operation of system services and functions.	**Incapacitation:** Prevents or interrupts system operation by disabling a system component. **Corruption:** Undesirably alters system operation by adversely modifying system functions or data. **Obstruction:** A threat action that interrupts delivery of system services by hindering system operation.
Usurpation A circumstance or event that results in control of system services or functions by an unauthorized entity.	**Misappropriation:** An entity assumes unauthorized logical or physical control of a system resource. **Misuse:** Causes a system component to perform a function or service that is detrimental to system security.

- A **threat model** helps in analyzing a security problem, design mitigation strategies, and evaluate solutions.
- Steps:
  - Identify attackers, assets, threats and other components
  - Rank the threats
- Solution:
  - Choose mitigation strategies
  - Build solutions based on the strategies

Perform the following actions:

1. Develop attack scenarios for
   - insider and outsider threats
   - single and coordinated attacks
2. Think about the attacker motivation and capabilities