Name: Nishant Sanjay Chavan Emp: 180600283
Class: BE/B Sub: CSL Rollno: 18

Q.2) Active Attacks	Passive Attacks
1) In active attack, modification in information take place.	1) While in passive attacks, modification in the information does not take place.
2) Active attacks is danger for integrity as well as availability.	2) Passive Attacks is danger for confidentiality.
3) In active attacks attention is on detection.	3) While in passive attacks attention is on prevention.
4) Due to active attack system is always damaged.	4) While due to passive attack, there is no any harm to system.
5) In active attack, victim gets informed about attack.	5) While in passive attack, victim does not get informed about the attack.
6) In active attack, system resources can be changed.	6) While in passive attacks, System resources are not change.

Chavan

Name: Nishant Sanjay Chavan Erp: 180600283
Sub: BE/B Sub: CSL Roll no: 118

UT-1

6) Active attacks influence the service of the system.	7) While in passive attack, information and messages in the system or network are acquired.
8) In active attack, information collected through passive attacks are used during executing.	8) While passive attacks are performed by collecting the information such as passwords, messages by itself.
9) Active attacks is tough to restrict from entering systems or network.	9) Passive attacks is easy to prohibited in comparison to active attacks.

Rchavan

Name: Nishant Sanjay Charan emp: 180600283
class: BE/B Sub: CSL Roll no: 18

UT-1

Q.3) For a successful cyber attack to take place there are seven steps and attacker must perform.

1) Reconnaissance:
The definition of reconnaissance is to check out a situation before taking action. Before launching an attack, hackers first identify a vulnerable target and explore the best way to exploit it. The initial target can be anymon in or connected to an organisation, wheather an executive or an admin or a third party supplier.

2) Scanning:
Once the target is identified, the next step is to identify a weak point that allows the attacker to gain access. This is usually accomplished by scanning an organisation's network with tools easily found on internet to find entry points.

3) Access and escalation:
Now, the weakness in the target network are identified, the next step in cyber attack is to gain access and then escalates to moving through the network undetected.
In almost all such cases, ~~privileged~~ privileged access is needed because it allows the attackers to move freely within environment.

Nsharan

4) Exfiltration:

Within the freedom to move around the network, the attackers can now access systems with an organisation's most sensitive data - to extract it all will. But intruders can take at this time.

5) Sustainment:

The attackes have now gained unrestricted access throughout the target network. Next is Sustainment, or staying in place quietly. To accomplish this, the hackers may secretly install malicious programs like root kits that allow them to return as frequently as they want.

6) Assault:

Fortunately this step is not taken in every cyber attack, because the assault is the stage of an attack when things become particularly nasty. This is when the hackers might alter the functionality of the victim's hardware, or disable the hardware entirely.

7) Obfuscation:

Usually the attackers want to hide their tracks, but this not universally the case - especially if the hackers want to leave a 'calling card' behind the boast about their exploits.

The purpose of trail obfuscation is to confuse,

Name: Nishant Sanjay Charan erp: 18600283
class: BE/B Sub: CSL Roll no: 18

UT-1

disorientate and divert the forensic examination process. Trail obfuscation covers a variety of techniques and tools including log cleaners, spoofing, misinformation, backbone hopping, and more.

@shavan