Name: Nishant Sanjay Charan enp: 180600283
class: BE/B Sub: CSL Rollno: 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 is cyber attack is to gain access and then escalates to moving through the network undetected.
In almost all such cases, ~~priviledged~~ privileged access is needed because it allows the attackers to move freely within environment.

Page: 1—3 Charan

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

VT-1

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 at 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 :

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

7) Obfuascation :

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,

NChavan

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