Krutarth Panchal

CIS 450

Week 3 - Chapter 3 - Exploitation Process

1. According to Mile2 (or any cited cyber/information security source), what is evasion?

(West, 2019) According to the Mr. Samuel West in the article titled “ What is Evasion Technique” evasion is cyberattack which uses malicious payloads to avoid the detection from the system like Sandboxing services.

West, S. (2019, December 2). *What is an Evasion Technique?* Libraesva. <https://www.libraesva.com/what-is-an-evasion-technique/>

1. What are the key metrics for pen testing purpose?

The key metrics for pen testing purpose are focusing on the path, and the act of establishing access to a host bypassing security restricted set by administrator. It is important to have a defined path to avoid the detection of a breach by the system administrator. The metrics for pen testing purpose could be access high value assets, establish Network Access, bypass security restrictions ,and identify and exploit vulnerable systems.

1. What are six tactics to bypass/fool anti-virus?

The six tactics to bypass/fool anti-virus are Encoding, Packing, Encrypting, Whitelist Bypass, Process Injection, Memory Resident.

1. What are some social engineering tactics (sometimes called a Red Team tactic) that can be used during pen testing?

Some of the social engineering tactics that can be used during pen testing are Pretesting, phishing, spear-phishing, and baiting.

1. What is a WAF? How can a pen tester counter a WAF?

WAF is Web Application Firewalls which is a firewall which can be hardware or software-based applications that is used to inspect and filter traffic flowing to or from web-based application. A pen tester can counter a WAF in three ways, which are Pre-processor exploitation by input validation bypass, impedance mismatch by http parameter fragmentation, and rule set bypass by brute-force rules.

1. What does it mean to make a pen test a Precision Strike?

Precision Strike is all about understanding the target host and using right tool against them to stay quiet and undetectable as possible. While pen testing it is very important to be precise which mean to have accurate and detail information about the target and also understanding what exploits need to be run onto the wire and what will be the outcomes of the exploits.

1. How does one customize their pen test exploitation?

As per mile2 preparation guide customized exploitation is the process of crafting the exploit to the scenario that presents itself. A pen tester have to take into account of all possible variables associated with the exploitation scenario then he/she should have a clear picture with as many variables enumerated as possible to enable exploitation. The variable could be who own the system, what the system is using for and which time, is the system running physically or logically (Virtual environment), how to gain access to the system and what is the purpose of getting into in the system.

1. A custom exploit that succeeds against your target network but is known by the security industry is still a zero-day. (T or F)

False

1. What are at least eleven examples of attacks?

The eleven examples of attacks are:

1. Web Application Attacks
2. Social Engineering
3. In-Memory Based Exploits
4. Man-in-the-Middle
5. VLAN Hopping
6. USB/Flash Drive Deployment
7. Reverse Engineering Zero-Day Angle
8. Attacking the User
9. Traffic Analysis
10. Firewire Routing Protocols
11. Phishing with Pretexting Employee Impersonation
12. What is or should be the overall objective of a pen test?  (Logic and Book Question)

The overall objective of a pen test should be first clearly communicating with the client. Then identifying the path of resistance into the organization without detection then represents the vector how the company or client can suffer losses through a targeted attack.

‌