Unit : 3

Ethical Hacking and Social Engineering

Marwadi University

Department of CE

Unit no.: 3

Unit title.: Ethical Hacking and Social Engineering

Cyber Security [01CE0604]

Asst. Prof. Krupali Gosai

Hacking

- Hacking is the act of finding the possible entry points that exist in a computer system or a computer network and finally entering into them.
- Hacking is usually done to gain unauthorized access to a computer system or a computer network, either to harm the systems or to steal sensitive information available on the computer.

Ethical Hacking Concepts

- **Ethical Hacking:** Ethical hacking involves finding weaknesses in a computer or network system for testing purpose and finally getting them fixed.
- Most people think hackers have extraordinary skill and knowledge that allow them to hack into computer systems and find valuable information.
- In reality, a good hacker, or security professional acting as an ethical hacker, just has to understand how a computer system works and know what tools to employ in order to find a security weakness.

Ethical Hacking Concepts

- Most ethical hackers are in the business of hacking for profit, an activity known as *penetration testing*, or *pen testing* for short.
- Pen testing is usually conducted by a security professional to identify security risks and vulnerabilities in systems and networks.
- The purpose of identifying risks and vulnerabilities is so that a countermeasure can be put in place and the risk mitigated to some degree.
- Ethical hackers are in the business of hacking and as such need to conduct themselves in a professional manner.

Ethical Hackers

- Ethical hackers are motivated by different reasons, but their purpose is usually the same as that of crackers.
- They're trying to determine what an intruder can see on a targeted network or system, and what the hacker can do with that information.
- This process of testing the security of a system or network is known as a *penetration test*, or *pen test*.

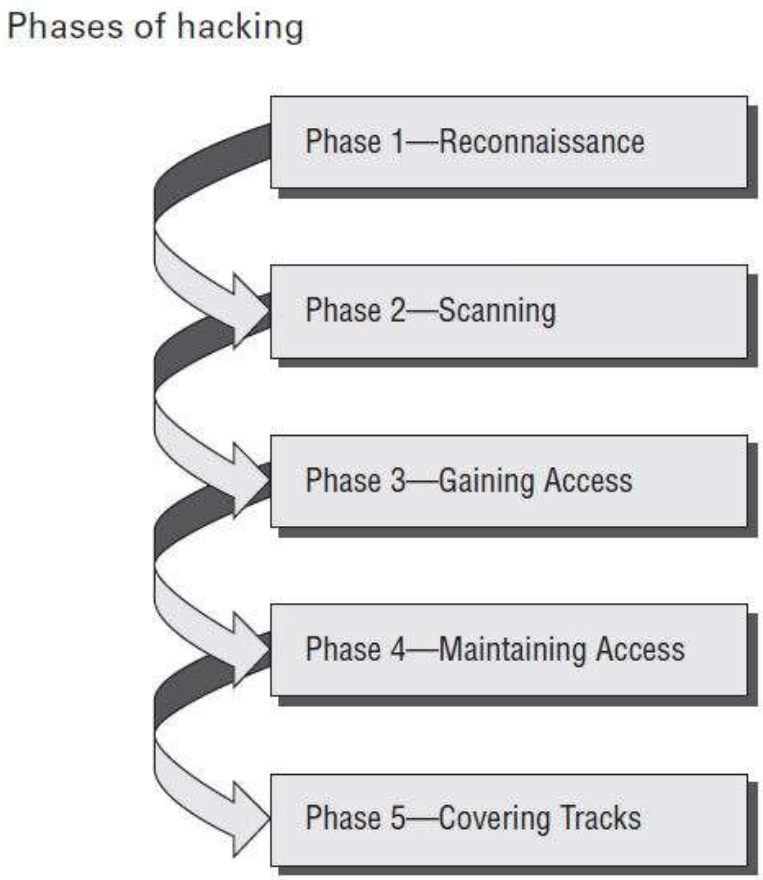
An Ethical Hacker's Skill Set

- Ethical hackers who stay a step ahead of malicious hackers must be computer systems experts who are very knowledgeable about computer programming, networking, and operating systems.
- In-depth knowledge about highly targeted platforms (such as Windows, Unix, and Linux) is also a requirement.
- Patience, persistence, and immense perseverance are important qualities for ethical hackers because of the length of time and level of concentration required for most attacks to pay off.
- Networking, web programming, and database skills are all useful in performing ethical hacking and vulnerability testing.

Ethical Hacking Terminology

- **Threat :** An environment or situation that could lead to a potential breach of security.
- **Exploit :** A piece of software or technology that takes advantage of a bug, or vulnerability, leading to unauthorized access, privilege escalation, or DOS on a computer system.
- **Vulnerability :** The existence of a software flaw, logic design, or implementation error that can lead to an unexpected and undesirable event executing bad or damaging instructions to the system.
- **Attack :** An attack occurs when a system is compromised based on a vulnerability.

The Phases of Ethical Hacking



Phase 1: Passive and Active Reconnaissance

- *Passive reconnaissance* involves gathering information about a potential target without the targeted individual's or company's knowledge.
- Passive reconnaissance can be as simple as watching a building to identify what time employees enter the building and when they leave. However, most reconnaissance is done sitting in front of a computer.

Active reconnaissance

- *Active reconnaissance* involves probing the network to discover individual hosts, IP addresses, and services on the network. This process involves more risk of detection than passive reconnaissance and is sometimes called *rattling the doorknobs*.
- Active reconnaissance can give a hacker an indication of security measures in place but the process also increases the chance of being caught or at least raising suspicion.

Phase 2: Scanning

- *Scanning* involves taking the information discovered during reconnaissance and using it to examine the network. Tools that a hacker may employ during the scanning phase include
  - Dialers
  - Port scanners
  - Internet Control Message Protocol (ICMP) scanners
  - Ping sweeps
  - Network mappers
  - Simple Network Management Protocol (SNMP) sweepers
  - Vulnerability scanners

Phase

- Phase 3: Gaining Access
- Phase 4: Maintaining Access
- Phase 5: Covering Track

How to Be Ethical

- The ethical hacker must follow certain rules to ensure that all **ethical and moral obligations are met**. An ethical hacker must do the following:
- **Gain authorization from the client and have a signed contract giving the tester permission to perform the test.**
- Maintain and **follow a nondisclosure agreement (NDA**) with the client in the case of confidential information disclosed during the test.
- **Maintain confidentiality when performing the test**. Information gathered may contain sensitive information. No information about the test or company confidential data should ever be disclosed to a third party.
- Perform the test up to but not beyond the agreed-upon limits. For example, DoS attacks should only be run as part of the test if they have previously been agreed upon with the client. Loss of revenue, goodwill, and worse could befall an organization whose servers or applications are unavailable to customers as a result of the testing.

MCQ

- **1.** Which of the following statements best describes a white-hat hacker?
- **A.** Security professional
- **B.** Former black hat
- **C.** Former gray hat
- **D.** Malicious hacker

MCQ

- **2.** What is the first phase of hacking?
- **A.** Attack
- **B.** Maintaining access
- **C.** Gaining access
- **D.** Reconnaissance
- **E.** Scanning

MCQ

- **3.** When a hacker attempts to attack a host via the Internet, it is known as what type of attack?
- **A.** Remote attack
- **B.** Physical access
- **C.** Local access
- **D.** Internal attack

MCQ

- **4.** Which term best describes a hacker who uses their hacking skills for destructive purposes?
- **A.** Cracker
- **B.** Ethical hacker
- **C.** Script kiddie
- **D.** White-hat hacker

MCQ

- **5.** MAC address spoofing is which type of attack?
- **A.** Encryption
- **B.** Brute-force
- **C.** Authentication
- **D.** Social engineering

MCQ

- **6.** Which type of person poses the most threat to an organization's security?
- **A.** Black-hat hacker
- **B.** Disgruntled employee
- **C.** Script kiddie
- **D.** Gray-hat hacker

Answer

- **1.** A. White-hat hackers are "good" guys who use their skills for defensive purposes.
- **2.** D. Reconnaissance is gathering information necessary to perform the attack.
- **3.** A. An attack from the Internet is known as a remote attack.
- **4.** A. A cracker is a hacker who uses their hacking skills for destructive purposes.
- **5.** C. MAC address spoofing is an authentication attack used to defeat MAC address filters.
- **6.** B. Disgruntled employees pose the biggest threat to an organization's security because of the information and access that they possess.

Attack Vector

- **Attack vector** is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome.
- Attack vectors enable attackers to exploit system vulnerabilities, including the human element.
- Attack vectors include viruses, E-mail attachments, webpages, pop-up windows, instant messages, chat rooms and deception.
- All of these methods involve programming, except deception, in which a human operator is fooled into removing or weakening system defenses.

Attack Vector

- The most common malicious payloads are viruses, trojan horses, worms and spyware. Payload is the necessary data being carried within a packet or other transmission unit – in this scenario (i.e. attack vector) payload means the malicious activity that the attack performs.

Attack Vector

1. Attack by E-Mail: the hostile content is either embedded in the message or linked to by the message.
2. Attachments (and other files): Malicious attachments install malicious computer code. The code could be a virus, trojan horse, spyware or any other kind of malware.
3. Attack by deception: Deception aimed at the user/operator as a vulnerable entry point. It is not just malicious computer code that one needs to monitor.

Attack Vector

4. Heedless guests (attack by webpage): Counterfeit websites are used to extract personal information. Such websites look very much like the genuine websites they imitate.
5. Attack of the worms: many worms are delivered as E-mail attachments, but network worms use holes in network protocols directly.

Attack Vector

7. Malicious macros: Microsoft word and Microsoft excel are some of the examples that allow macros.
8. Foistware (sneakware): Foistware is the software that adds hidden components to the system. Spyware is the most common form of foistware.
9. Viruses: These are malicious computer codes that hitch a ride and make the payload.

Zero Day Attack

- Zero day or a day zero attack is the term used to describe the threat of an unknown security vulnerability in a computer software or application for which either the patch has not been released or the application developers were unaware of or did not have sufficient time to address.
- Since the vulnerability is not known in advance, the exploits often occur without the knowledge of the users. A zero day flaw is considered as an important component when designing an application to be efficient and secure.

What makes a vulnerability a zero-day?

- The term "zero-day" refers to a newly discovered software vulnerability. Because the developer has just learned of the flaw, it also means an official patch or update to fix the issue hasn't been released.
- So, "zero-day" refers to the fact that the developers have "zero days" to fix the problem that has just been exposed - and perhaps already exploited by hackers.
- Once the vulnerability becomes publicly known, the vendor has to work quickly to fix the issue to protect its users.
- But the software vendor may fail to release a patch before hackers manage to exploit the security hole. That's known as a zero-day attack.

Zero-day attack example

- Stuxnet - a type of zero-day vulnerability - was one of the earliest digital weapons used. Stuxnet is a highly infectious self-replicating computer worm that disrupted **Iranian nuclear plants**. The threat took control of computers. It altered the speed of centrifuges in the plants and shut them down.
- Symantec researchers Eric Chien and Liam O'Murchu analyzed the worm. They discovered that Stuxnet is a well-crafted computer worm that only a national government could create to control large-scale industrial facilities. With a team of cyber security experts, Chien and O'Murchu came up with patches and workarounds to fix the bug.

Thank You

Any Question !!!