ATTACK TECHNIQUES

OVERVIEW

A. Ethical Hacking Phases

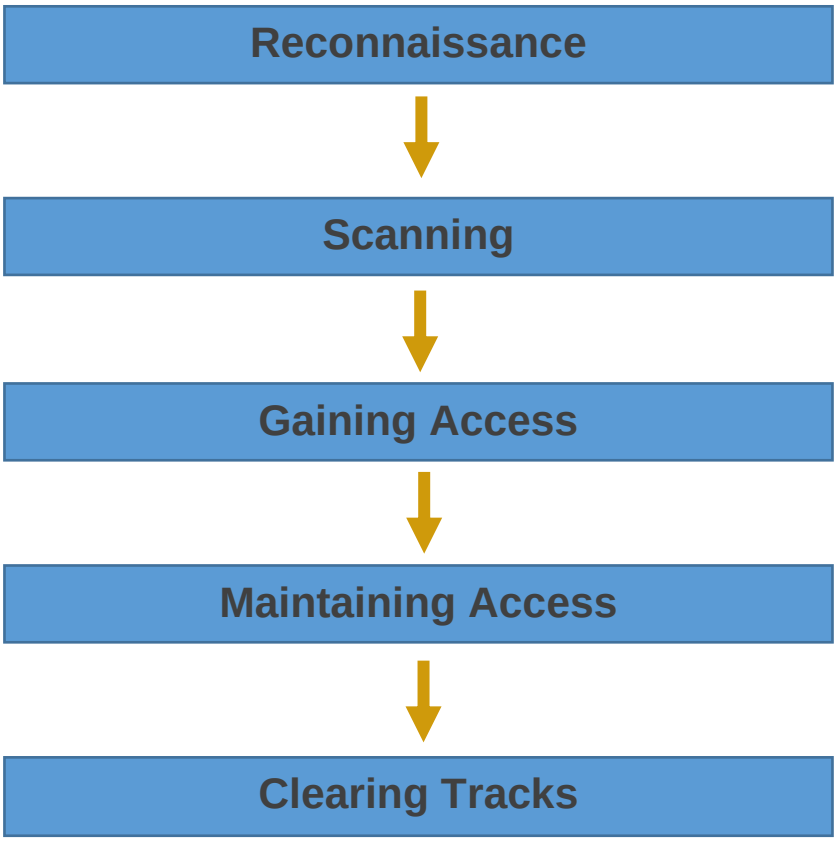
B. Malicious Software

C. Social Engineering

D. Cryptography

Image by rawpixel.com

A. ETHICAL HACKING PHASES



1) Reconnaissance

Also referred to as “footprinting”, reconnaissance is the first step of ethical hacking. This is where we try to obtain as much information as possible about the target. This is a nonintrusive process, meaning we do not access information illegally or attempt to impersonate others with false credentials.

- **Types**
  - **Active** – prodding a target network that may result in logging and alert to your suspicious activities
    - Port Scans, DNS zone xfers..

- **Passive** – obtain information about a target without interacting with its remote systems, typically from other sources

- Tools
  - Nmap, Zenmap, Whois, Recon-ng, Dig, Nessus, OpenVAS
  - Google, Maltego, Domain Dossier, Metis

2) Scanning

Types

- **Port Scanning** – check for open ports, live systems, and other services
- **Vulnerability Scanning** – utilize tools (often automated) to discover potential weaknesses to exploit
- **Network Mapping** – map out the topology of a network and its connected devices

3) Gaining Access

This phase is also associated with the term "**enumeration**". Once sufficient information about the target has been gathered, it can be used to exploit vulnerabilities and enumerate a system. This is where connecting to remote systems takes place.

4) Maintaining Access

Now that a system is compromised, the goal is to maintain access until whatever intended plans were in having attacked the target are fulfilled. In order to do so, the target user(s) must remain unaware of the attacker's presence. Malicious files or programs such as Trojans and Rootkits can help accomplish this.

5) Clearing Tracks

Hackers remove evidence of their activities so as to avoid being caught. Logs will be modified or deleted, alongside changing registry values and removing applications used on the target system.

B. MALICIOUS SOFTWARE

1) Viruses

A virus is a malicious program that attaches onto another program or file; it is incapable of operating or self-replicating without a host presence. That host being a file or separate program.

Viruses are commonly sent through e-mail attachments; where, an unsuspecting user might click a malicious attachment or link that immediately downloads a program with the virus.

2) Worms

A worm is another malicious program; but unlike a virus, it does not need a host to self-replicate or propagate.

3) Trojans

Trojan programs operate largely on social engineering.

This type of malware consists of programs which disguise themselves into fooling users to view them as legitimate. Once a user installs the Trojan program, it can deliver a hidden payload capable of sending confidential information from the target's machine to the attacker's.

4) Spyware

If a user downloaded a program which recorded their confidential information without their knowledge, this would be an example of spyware.

Spyware sends this recorded information from the target to the attacker. Information recorded can be registered from every keystroke a user enters, notably for when they enter their credentials somewhere.

5) Adware

Similar to spyware, adware is downloaded without a user's knowledge. However, adware often alerts the user of its presence and is used primarily to deliver advertisements to a user.

For example, a banner message might display particular content related to a user's purchasing habits (having already been collected).

C. SOCIAL ENGINEERING

Using knowledge of human nature, social engineers aim to exploit unaware or unsuspecting individuals in order to divulge information.

For example, a perpetrator could pose as one of the target company's IT staff members. They would then contact an employee, stressing urgency to help perform "major updates" and gain access to their system.

Techniques used by social engineers include:

1) **Urgency**

   Creating a false sense of urgency to rush the person into explaining or acting on something, thus potentially shaking up their normal thought process and removing raises of suspicion.

2) **Quid pro quo**

   Barter x for x; social engineer promises a product or service in return for information.

3) **Status quo**

   Convince the target into revealing information by making them believe others around them have done the same; prey on group think and social acceptance.

4) **Kindness**

   Show a genuine kindness and care for the target so as to gain their trust.

5) **Position**

   Utilize authority: take on the role of a position high in the company hierarchy to confidently request information --- or, claim that a higher-ranking individual is demanding important information and you (social engineer) are the messenger asking for it.

D. CRYPTOGRAPHY

- **Cryptography** is the process of converting plaintext into ciphertext, which is text that has been encrypted and is unreadable. Sensitive information that organizations or individuals want to keep private should utilize encryption to secure their data.

- **Decryption** is the process of unencrypting ciphertext and turning it back into plaintext.

- **Cryptanalysis** is the process of cracking encryption algorithms. It's not only used by hackers, but also as a way to test how secure an encryption algorithm is. If the resources or time it takes to crack an algorithm is impractical, then the algorithm is considered more secure.

- A **certificate** is a digital file issued by a certification authority (CA). It's used to verify the identities of two parties exchanging data over the Internet. Each certificate has a unique serial number and is required to abide by the X.509 standard.

- A **digital signature** is a way of signing messages using asymmetric encryption.

  First, a message is created to send to a destination along with a hash value. That message's hash value is encrypted with the sender's private key. The receiver uses the sender's public key to decrypt the hash. Then, the receiver verifies that it matches their own calculated hash value of the message. If it matches, the receiver will be able to read the message.

Encryption Algorithms

1) **Symmetric**
   - A single key is used to encrypt/decrypt data
   - Before data can be transmitted, a sender and receiver must agree on the specified key
   - Supports confidentiality, not authentication or nonrepudiation
   - **Examples:** DEA; IDEA, Blowfish, RC5

2) **Asymmetric**
    - Referred to as “public key cryptography”
    - Two keys are used; each either encrypting OR decrypting data
    - Supports authentication and nonrepudation
    - Slower than symmetric algorithms
    - **Examples:** RSA; ElGamal
3) **Hashing**
    - Converts a variable-length input into an output string, also known as **hash value** or **message digest**
    - **Examples**: MD5; SHA-3