Cybersecurity SG

Meeting 06

Steps

Penetration Testing

1. Planning and reconnaissance
2. Scanning
3. Gaining Access
4. Maintaining Access
5. Analysis and WAF configuration

Hacking

1. Reconnaissance
2. Scanning and Enumeration
3. Gaining Access / Exploitation
4. Maintaining Access / Persistence
5. Clearing Tracks

Tools

nmap

source

Documentation

> **Info**
>
> Nmap ("Network Mapper") is a free and open source utility for network discovery and security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics.

```
nmap -sC -sV <ip> -oN scan.log
```

ncat

online documentation

> **Description**
>
> Ncat is a feature-packed networking utility which reads and writes data across networks from the command line. Ncat was written for the Nmap Project as a much-improved reimplementation of the venerable Netcat. It uses both TCP and UDP for communication and is designed to be a reliable back-end tool to instantly provide network connectivity to other applications and users. Ncat will not only work with IPv4 and IPv6 but provides the user with a virtually limitless number of potential uses.

Setting up ncat listener

```
nc -lnvp <port>
```

Setting up file transfer :

```
nc -q 0 -lnvp <port> < <file to send>
```

```
nc -q 0 <ip server> <port> > <file to save>
```

nikto

source

Freecodecamp Beginner's Guide

> **Info**
>
> Nikto is an open source web server and web application scanner. Nikto can perform comprehensive tests against web servers for multiple security threats, including over 6700 potentially dangerous files/programs. Nikto can also perform checks for outdated web servers software, and version-specific problems.

```
nikto -h <url>
```

gobuster

source

Documentation

> **Info**
>
> Directory and DNS busting tools written in GO

```
gobuster dir -u <ip>  -w <wordlist>
```

Seclists source

Kali Documentation

linpeas

source

Kali Documentation

> **PEASS-ng - Privilege Escalation Awesome Scripts SUITE new generation**
>
> These tools search for possible **local privilege escalation paths** that you could exploit and print them to you **with nice colors** so you can recognize the misconfigurations easily

---

Pickle Rick

source