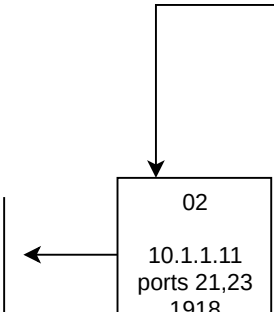
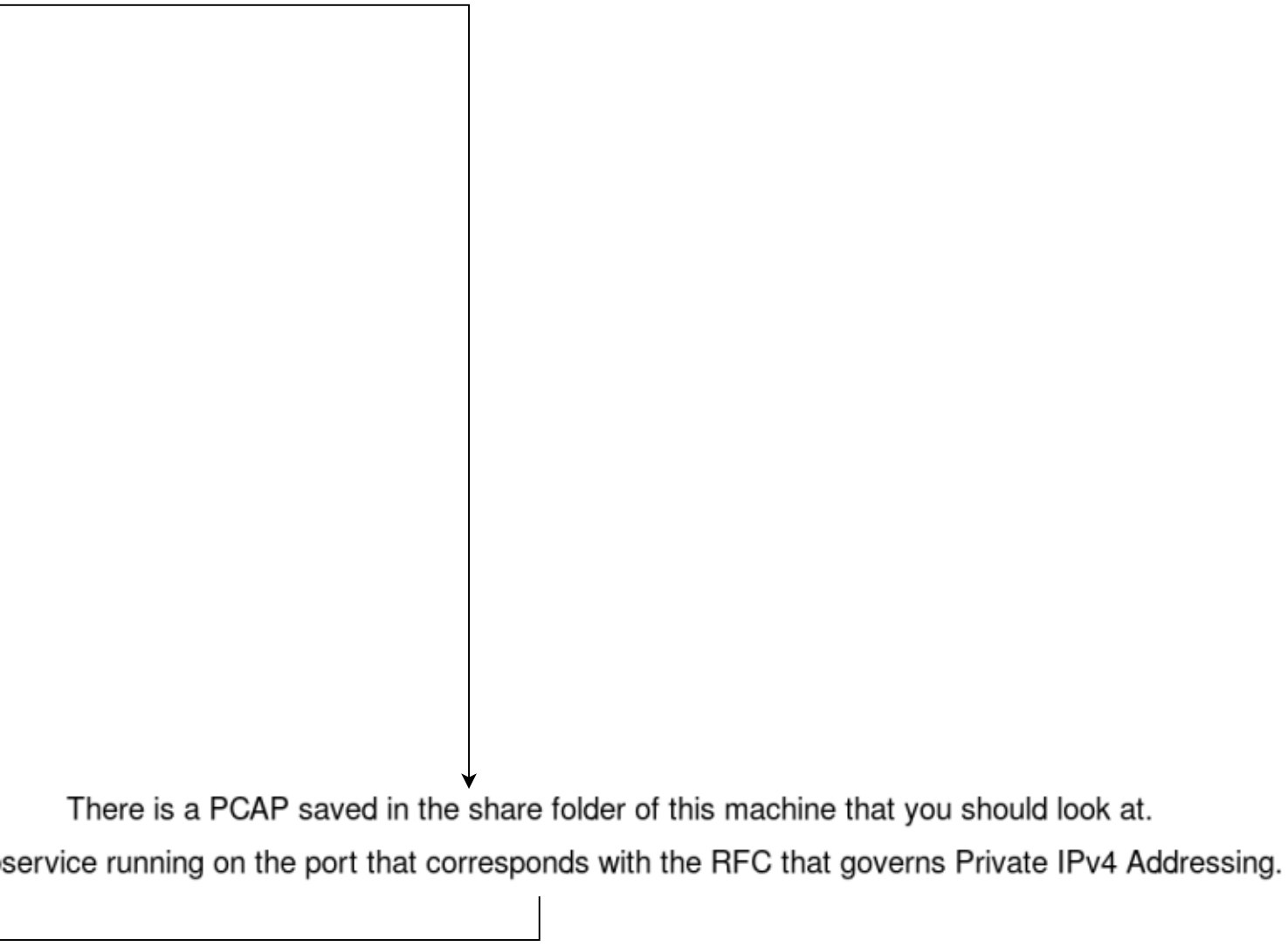
```
Flag-02f.txt
To answer these 4 questions, you will need to use
```

```
tcpdump and BPF's against the capstone-bpf.pcap fi
le.


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

Question 1:

Using BPF's, determine how many packets with a DSC
P of 26 being sent to the host 10.0.0.103.

Provide the number of packets converted to BASE64.

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

Question 2:

What is the total number of fragmented packets?

Provide the number of packets converted to BASE64.

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

Question 3:

How many packets have the DF flag set and has ONLY
 the RST and FIN TCP Flags set?

Provide the number of packets converted to BASE64.

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

Question 4:

An attacker is targeting the host 10.0.0.104 with
either a TCP full or half open scan. Based off the
 pcap, how many ports are open?

Provide the number of ports converted to BASE64.

------------------------------------------------
```

There is a web





APIPA uses the IP network range of 169.254.0.0/16. What RFC number governs this?

IPv6 Uses SLAAC to resolve its Global address from the Router. What multicast destination address does it use to Solicit the router?

Which type of ARP is sent in order to perform a MitM attack?

An attacker built a FRAME that looks like this:

| Destination MAC | Source MAC | 0x8100 | 1 | 0x8100 | 100 | 0x0800 | IPv4 Header | TCP Header | Data | FCS |

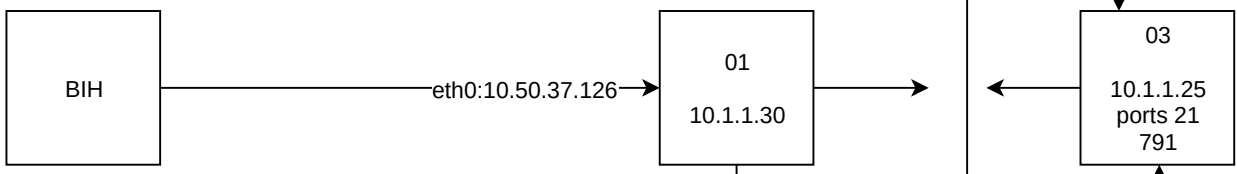
What form of attack is being performed? Supply your answer in ALL CAPS and convert to BASE64.

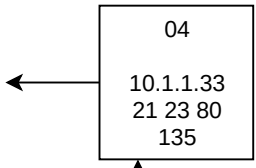
SSH is ru

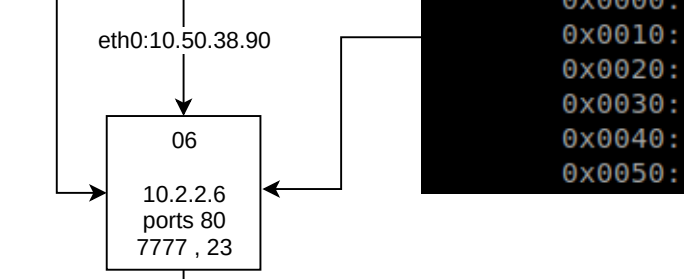
The Flag

nning on a higher port although it only seems to accept connections when it looks like its coming from a Cisc

for this system is the SSH Port number.







co Device's TTL. Try using iptables to adjust your sending TTL.

A router receives a 5000 byte packet on eth0. The MTU for the outbound interface (eth1) is 1500. What would the fragmentation offset increment be with the con
Origional packet Size = 5000 bytes
MTU for outboud interface = 1500
Packet IHL = 7

is a webservice running on the port that corresponds with the RFC that governs IPv4 Header Structure

is another hint in the student home drive. There is no SSH access to this system so try using FTP with your

RAW Sockets are created in _____ space. Specify the one word BASE64 conversion of your answer in ALL CAPS.

Which module would you need to import to convert data into a corresponding 2-digit hex representation?
Specify the module in lowercase and converted to BASE64.

Specify the answer in the proper case. Include only what is between the single or double quotes and not the quotes themselves or the "!".

What is the default (and most common) encoding used when converting data to be sent over the network.

Provide your answer in ALL CAPS and converted to BASE64.

What type of header does TCP build to perform the checksum function?

i.e. [ANSWER] Header

Provide your answer in ALL CAPS and converted to BASE64.

is a listening TCP port on this system that waiting for connections.
a Python3 TCP Stream sender and send it thru your tunnel to say Hi.
your message as a bytes-like object and decode the response to/from UTF-8 to get the
e-encoded message. You can use CyberChef to help you decode the message to Human
able message.

There is another box (Capstone-05) on a different network (that only this system can see) trying to attack thi
box, on one of the port(s) associated with the W32/Blaster Worm. Use a sniffing tool to try to find the messa
to send.

RIPv2 seems to be running on the 10.1.1.0/25 network.
Try to sniff out the traffic to find out what networks its advertising in its updates.
What you find will be the IP address of the next environment pivot to access from your INTERNET_HOST.

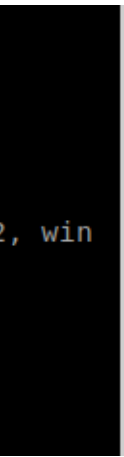
```
 IP (tos 0x10, ttl 64, id 62755, offset 0, flags [DF], proto TCP (6), length 74)
014 > 10.2.2.6.telnet: Flags [P.], cksum 0x184d (incorrect -> 0x284f), seq 94:116, ack 117
ons [nop,nop,TS val 3633703626 ecr 2595770788], length 22
  fa16 3e24 0714 fa16 3ed1 c61b 0800 4510  ..>$....>.....E.
  004a f523 4000 4006 2d6a 0a02 0207 0a02  .J.#@.@.-j......
  0206 84de 0017 d59c e1fd 4e4f 45b3 8018  ..........NOE...                    13:5
  01fb 184d 0000 0101 080a d895 eaca 9ab8  ...M............
  51a4 4830 6c64 2037 3368 2064 3030 723f  Q.H0ld.73h.d00r?                    507,
  0d00 6578 6974 0d00                      ..exit..
```

ditions below?

student credentials.

s
ge it is trying

```
    0x0010:  0047 b501 4000 4006 6d8f 0a02 0206 0a02  .G..@.@.m.......
    0x0020:  0207 0017 84e6 c9db a673 9a72 88b9 8018  .........s.r....
    0x0030:  01f7 184a 0000 0101 080a 9ab9 8bbe d897  ...J............
    0x0040:  24e4 6361 7073 746f 6e65 2d30 3620 6c6f  $.capstone-06.lo
    0x0050:  6769 6e3a 20                             gin:.
5:57.708647 IP (tos 0x10, ttl 64, id 12477, offset 0, flags [DF], proto TCP (6), length 52)
10.2.2.7.34022 > 10.2.2.6.telnet: Flags [.], cksum 0x1837 (incorrect -> 0x2031), seq 79, ack 92
 options [nop,nop,TS val 3633784037 ecr 2595851198], length 0
    0x0000:  fa16 3e24 0714 fa16 3ed1 c61b 0800 4510  ..>$....>.....E.
    0x0010:  0034 30bd 4000 4006 f1e6 0a02 0207 0a02  .40.@.@.........
    0x0020:  0206 84e6 0017 9a72 88b9 c9db a686 8010  .......r........
    0x0030:  01fb 1837 0000 0101 080a d897 24e5 9ab9  ...7........$...
    0x0040:  8bbe                                     ..
```


2, win

SSH is running on the port that correspond
The flag for this system is the port number

> This system seems to be a

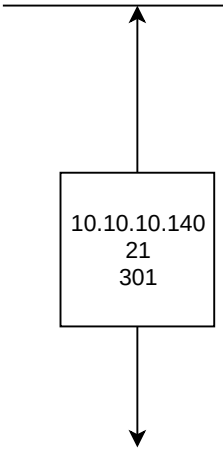
There is a web service running on this machine that is

SSH is running on a highe
It also seems to use differ
How can we intercept thes
Maybe another system ha
The Flag for this system is
Credentials for this systen

```
2: et
    l
    i

    i

3: et
    l
    i

    i
```

ls with the HTTP status code for Moved Permanently.
converted to BASE64. hint-08a.png

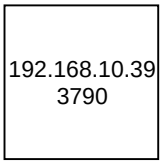
a pivot for the Network Reconnaissance section.
hint-08b.png



SSH is running on the
The flag for this system

This system seems to be

the same port that Metasploit uses for its webservice.



There is a webservice running

<h2>Question 1</h2>

<hr>

r port but it is not accessible from the outside.
rent username and password than what the other systems use.
se credentials?
s a tool that can help us.
s the password you find converted to BASE64.
n will be exactly what you find.

```
h0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pf
ink/ether fa:16:3e:d1:c6:1b brd ff:ff:ff:ff:ff:ff
net 10.2.2.7/28 brd 10.2.2.15 scope global eth0
  valid_lft forever preferred_lft forever
net6 fe80::f816:3eff:fed1:c61b/64 scope link
  valid_lft forever preferred_lft forever
h1: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1450 qdisc pf
ink/ether fa:16:3e:a5:63:51 brd ff:ff:ff:ff:ff:ff
net 10.10.10.129/25 brd 10.10.10.255 scope global eth1
  valid_lft forever preferred_lft forever
net6 fe80::f816:3eff:fea5:6351/64 scope link
  valid_lft forever preferred_lft forever
```

10.2.2.7
23, 80
2222

10.10.10.129

port that corresponds with the HTTP status code for Not Found.
n is the port number converted to BASE64. **hint-10a.png**

e a pivot for the Movement and Redirection section. **hint-10b.png**

10.10.10.167
80
404

SSH is running
The flag for thi

This system

on the port that corresponds with the default port for Proxy-chains.

11
192.168.10.80


```
<h2>Question 1</h2>
<p></p>
```

13:5

win

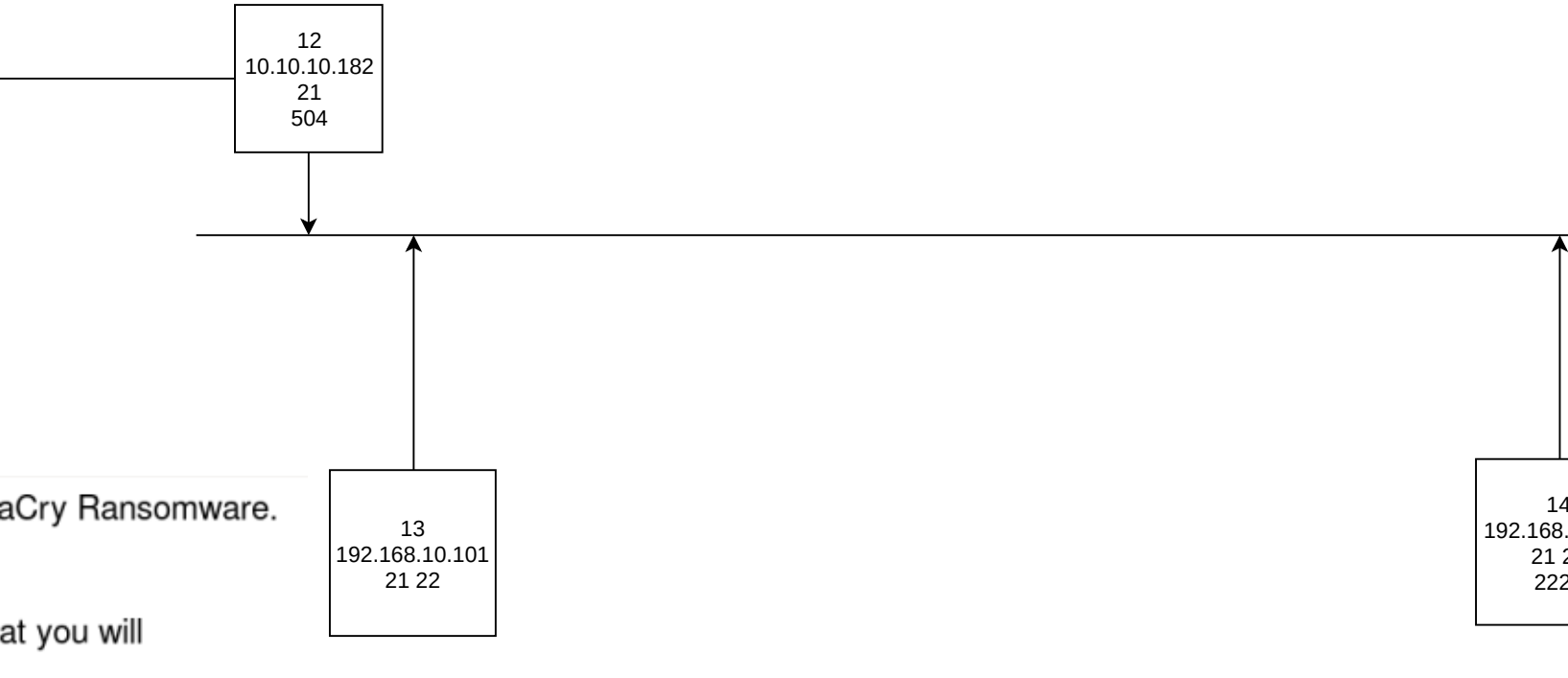
g on the port that corresponds with the HTTP status code for Gateway Timeout.
is system is the port number converted to BASE64. hint-12a.png

n seems to be a pivot for the Network Analysis and Filtering sections. hint-12b.png

There is a webservice running on the port that is the sum of the 2 SMB ports used by the Wanna

There is a Hex-Encoded PCAP saved in the share folder of this machine th
need to extract, decode with XXD, and open with Wireshark.

```
5:57.708678 IP (tos 0x10, ttl 64, id 12478, offset 0, flags [DF], proto TCP (6), length 67)
10.2.2.7.34022 > 10.2.2.6.telnet: Flags [P.], cksum 0x1846 (incorrect -> 0x3fc1), seq 79:94, ac
507, options [nop,nop,TS val 3633784037 ecr 2595851198], length 15
    0x0000:  fa16 3e24 0714 fa16 3ed1 c61b 0800 4510  ..>$....>.....E.
    0x0010:  0043 30be 4000 4006 f1d6 0a02 0207 0a02  .C0.@.@.........
    0x0020:  0206 84e6 0017 9a72 88b9 c9db a686 8018  .......r........
    0x0030:  01fb 1846 0000 0101 080a d897 24e5 9ab9  ...F........$...
    0x0040:  8bbe 6e65 744e 5f63 6f6d 7261 6465 580d  ..netN_comradeX.
```



aCry Ransomware.

at you will

```
ck 92,
```

4
10.111
22
23

There is a webservice running on the port that that falls in the Expanded Extended Cisco Numbered

Snort is running on this machine. Maybe you should take a look through its file locations.

To answer these a questions, you will need to examine the Snort

d ACL Range.

<p>You are performing ARP scans and sending Grat

<p>Provide the 2 wor

<p>What is the typical flag response (if any) woul
<p>Provide the 3 letter abbreviated name of the FLAG(s) i

<p>What command line tool can be u
<p>Provide the com

<p>Which NMAP scan is able to determine open ports on a t
<p>Provide the scan

<p>A cyber analyst wants to us Netc
<p>Provide the exact command (without switches and in

uitous ARPs to perform a MitM attack. Which phase of reconnaissance are you in?

d phase in ALL CAPS and converted to Base64.

<h2>Question 2</h2>

d a Linux host perform when receiving a Stealth scan on an CLOSED port?
in ALL CAPS, separated by / (use “NONE” if no response) and converted to Base64.

<h2>Question 3</h2>

sed to pull DNS information from the server using TCP port 43?
mand in ALL CAPS and converted to Base64.

<h2>Question 4</h2>

arget by spoofing packets to make them looks as if they came from a zombie machine?
name in ALL CAPS and converted to Base64.

<h2>Question 5</h2>

at to perform a banner grab on a target IP of 10.1.0.1 port 1111.
cluding spaces) you would perform on the command line and converted to Base64.

Whic

Which SSH syn

Of the 2 types of en

What exact SCP command would you u

Provide the command exactly as

h SSH syntax will properly setup a Local port forward from the “Outside Host” to access to the Internal Website?

<pre>
| Outside | | FW | | Inside | | Web |
147.25.99.1 192.168.1.27 188.8.8.8
</pre>

A.) ssh outside@192.168.1.27 -L 1234:188.8.8.8:80 -NT
B.) ssh inside@147.25.99.1 -L 9876:188.8.8.8:1234 -NT
C.) ssh outside@147.25.99.1 -L 1234:188.8.8.8:80 -NT
D.) ssh inside@192.168.1.27 -L 1234:188.8.8.8:80 -NT

Provide only the LETTER answer in ALL CAPS and converted to Base64.

Which op

What is the name

<h2>Question 2</h2>

tax will properly setup a Remote port forward from the “Inside Host” to give “Outside Host” access to the Internal Website?

<pre>
| Outside | | FW | | Inside | | Web |
147.25.99.1 192.168.1.27 192.168.1.10
</pre>

A.) ssh Outside@147.25.99.1 -R 9876:192.168.1.10:80 -NT
B.) ssh Inside@147.25.99.1 -R 9876:192.168.1.10:80 -NT
C.) ssh Outside@192.168.1.10 -R 9876:147.25.99.1:80 -NT
D.) ssh Inside@192.168.1.27 -R 9876:192.168.1.10:80 -NT

Provide only the LETTER answer in ALL CAPS and converted to Base64.

A network a

What type of n

<h2>Question 3</h2>

ncryption, which encryption type does SSH use to verify and authenticate each other, and to encrypt and pass the shared key?
Provide the 1 word in ALL CAPS and converted to Base64.

<h2>Question 4</h2>

use to copy a file called “secret.txt” from the 'tgt' home directory, to your current working directory, using the Dynamic tunnel you have established.

<pre>
| outside | | FW | | inside | | tgt |
147.25.99.1 192.168.1.27 192.168.1.10
</pre>

outside$: ssh inside@192.168.1.27 -D 9050 -NT

you would run in from the command line (including any appropriate spaces and all lower case) using proxychains and converted to Base64.

proxychains scp {username}@{ip}:{path}/{filename} {target location}

<h2>Question 5</h2>

Which tool adds “FTP Like” services to SSH?

Provide the exact tool acronym in ALL CAPS and converted to Base64.

To answer these 8 questions, you will nee

<h2>Question 1</h2>

ption in Wireshark could you use if you wanted to identify which IP address are communicating with each other?
Specify your answer in ALL CAPS and converted to Base64.

<h2>Question 2</h2>

of the data type that is a Cisco proprietary protocol used for collecting IP traffic information and monitoring network flow?
Specify your answer in ALL CAPS and converted to Base64.

<h2>Question 3</h2>

A method of data collection where this device can be placed in line on the wire to capture traffic?
What is this device called?
Specify your one word answer in ALL CAPS and converted to Base64.

<h2>Question 4</h2>

admin starts to notice an increase in requests for certain files, changes to the registry and unusual tasks being run.
This anomaly is an Indicator of _____?
Specify your 1 word answer in ALL CAPS and converted to Base64.

<h2>Question 5</h2>

malware doesn't use an encryption key but is capable of rewriting its code and signature patterns with each iteration?

Specify your 1 word answer in ALL CAPS and converted to Base64.

/usr/share/cctc/Flag-13f.txt
d extract the capstone-analysis-HEX-Encoded.pcap file that you will need extract, decode with XXD, and open with Wireshark.

<p>In I

Question 1:

Which ip address initiated the attack against the FTP server?

Provide the ip address in the x.x.x.x format and converted to Base64.

Question 2:

How many failed attempts to guess the FTP password?

Provide number and converted to Base64.

Question 3:

What is the correct FTP password?

Provide the exact password and converted to Base64.

Question 4:

What is the system IP that was compromised?

Provide the ip address in the x.x.x.x format and converted to Base64.

Question 5:

What is the FTP version?

Provide the version number only and converted to Base64.

Question 6:

What is the name of the file taken by the attacker?

Provide the filename exactly as shown and converted to Base64.

Question 7:

What was the message contained within the extracted file?

Provide the message exactly as shown and converted to Base64.

Question 8:

What is the name of the file uploaded by the attacker?

Provide the filename exactly as shown and converted to Base64.

14

<h2>Question 1</h2>

NAT, which Hook would I place a rule to change the source IP for all traffic thru this host?
Specify your 1 word answer in ALL CAPS and converted to Base64.

<h2>Question 2</h2>

Which Hook would I apply rules that are destined for the ‘localhost’?
Specify your 1 word answer in ALL CAPS and converted to Base64.

<h2>Question 3</h2>

What recognition method do IDS/IPS primarily use to detect malicious traffic?
Specify your 1 word answer in ALL CAPS and converted to Base64.

<h2>Question 4</h2>

In iptables, which Table would I use if I wanted to preform packet alterations?
Specify your 1 word answer in ALL CAPS and converted to Base64.

<h2>Question 5</h2>

What is the default family for NFTables?
Specify your 1 word answer in ALL CAPS and converted to Base64.

To answer these s questions, you will need to examine the Short

---

Question 1:

How many rule files are on the syste

Provide the number converted to Base64 as

Question 2:

How many of the rules are currently in use to m

Provide the number converted to Base64 as

Question 3:

Which rule will look for someone doing a n

Provide only the filename as your answer (i.e. ‘file.rules’) a

---

Question 4:

What is the exact Alert Message that is being trigge

Convert the exact message as you see it and convert it to

Question 5:

From what IP is the attack coming fr

Provide your answer in the x.x.x.x format and con

---

services running on this system.

---

em?

your answer.

---

atch on traffic?

your answer.

---

ull scan ?

and converted to Base64.

---

red on the system?

Base64 for your answer.

---

om?

verted to Base64.
