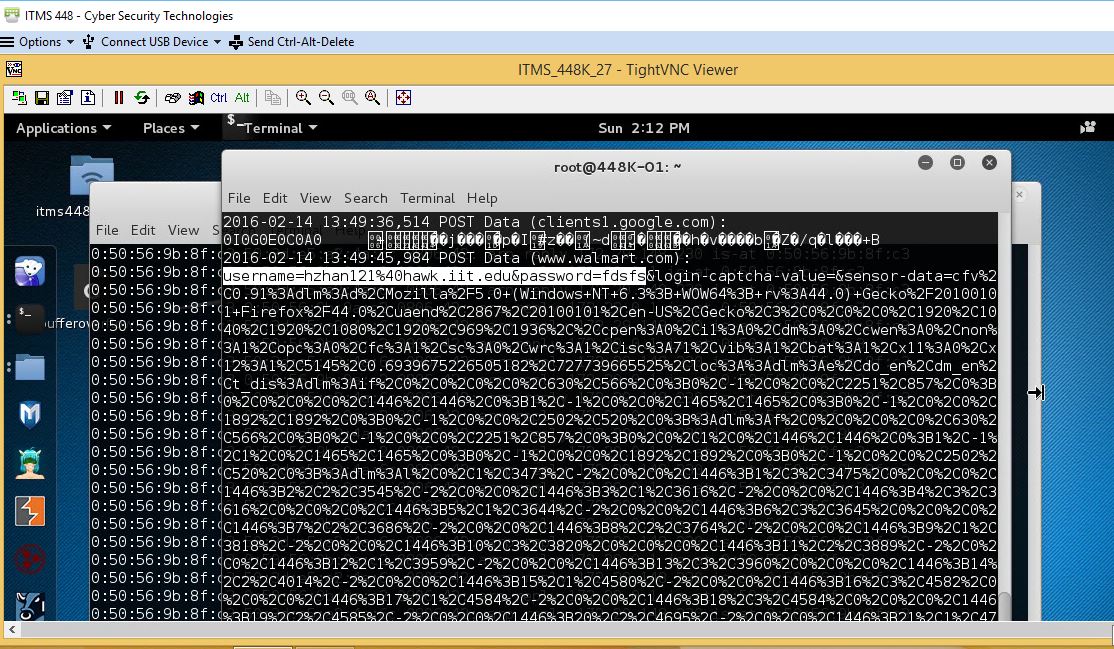
**QUESTION 1**

Download the HW5\_Lab\_Instructions from the Lab Instructions folder in Blackboard.  Complete all of the steps in the lab and submit the requested screenshot from step 19 to answer this question.



**QUESTION 2**

Step 23 from Lab 5:  Did HTTPS-Everywhere in Firefox prevent the victim's email address and password from being captured by sslstrip for the Walmart site during logon?

 True

 False

**QUESTION 3**

Download the following pcap file by clicking on the following link: [lab5capture.pcap](https://blackboard.iit.edu/bbcswebdav/pid-380557-dt-content-rid-2063531_1/xid-2063531_1)  to answer this question through question 12.

Open the pcap in Wireshark in your Student VM or on your personal computer.

Network Admin's Computer = 172.29.0.105 with original MAC of 00-50-56-a4-f8-df

ColaMaster's Production Server = 172.29.148.10 with original MAC of 00-50-56-A4-22-55

Attacker's Computer = 172.29.0.106

\*\*note I removed all traffic from 172.29.0.106 from this capture so that you wouldn't be overrun with the VNC traffic that was necessary for me to put together this lab.\*\*

Now it is story time.  Once upon a time there was a network administrator that logged on to a production machine for a soda company one evening.  That machine held the secret ingredients配料 for ColaMaster which were supposed to be held under tight guard.  Your boss obtained a packet capture that the attacker had taken and forgot to delete.  He wants you to analyze it to see what happened.

Filter for arp traffic in wireshark.  Based on looking at the traffic, what attack was happening here?  Also, based on this information what do you think the MAC address of the attacker was?

This attack is ARP Cache Poisoning. The MAC address of the attacker was 00:50:56:a4:31:e7.

**QUESTION 4**

What protocol did the Network Admin use to connect to the production server?

|  |  |  |
| --- | --- | --- |
|  |  | ssh |
|  |  | ftp |
|  |  | telnet |
|  |  | rlogin |

**QUESTION 5**

What was the username and password that the Network Admin used to logon to the production machine?

login: nneettwwoorrkkadmin[4 bytes missing in capture file]n

password: intheclear

**QUESTION 6**

The Network Admin started out at the C:\Documents and Settings\networkadmin directory.  He then performed the same command twice to end up at C:\.

What was the command he typed twice?

dir

**QUESTION 7**

The Network Admin listed the files in the C:\ directory with the dir command.  What was the directory that he changed into next?

C:\SuperSecretFiles

**QUESTION 8**

There was one file in the directory that the Network Admin most recently changed into.  What was that file's name?

SecretSodaRecipe.txt

**QUESTION 9**

The Network Admin ran the **type** command against the file mentioned in the previous question.  What does the **type**command do?

The type command is used to find out if command is builtin or external binary file. It also indicate how it would be interpreted if used as a command name.

**QUESTION 10**

The last file the Network Admin looked at contained the secret ingredients for ColaMaster.  What are those two ingredients?

12 ounces Coke Rebottle as ColaMaster.

**QUESTION 11**

Explain why it was a bad idea for the Network Admin to use the protocol he selected to logon to the Production Server.  Also, explain a more secure protocol he could have used to logon and why that protocol would have been more secure.

Telnet server could not log you in using NTLM authentication.

He can use  SSH or TLS 1.1+ to logon because they are all use encryption.

**QUESTION 12**

Explain at least one thing the ColaMaster company could have done to mitigate against the initial attack that allowed the attack to monitor the session between the Network Admin and the Production Server.

The Network Admin use type command to hide the file and let the attack miss in capture file

**QUESTION 13**

Explain how an IP Fragmentation Attack such as the Ping of Death works.

Attacker sends a datagram to Victim’s system which is greater than the Max IPv4 packet size. Because the packet is fragmented into several smaller 1500 byte datagrams to travel across Ethernet LAN, the Victim’s system will allow it enter. After Victim’s system receives the fragmented datagrams, these datagrams are reassembled into the original one. Since the datagram is greater than the Max IPv4 packet size, the system crashes.

**QUESTION 14**

The Ping of Death attack is primarily a denial of service against:

|  |  |  |
| --- | --- | --- |
|  |  | The recipient's network bandwidth |
|  |  | The recipient's computer's availability |
|  |  | The recipient's passwords |
|  |  | The recipient's secret files |

**QUESTION 15**

In order for an attacker to use ARP cache poisoning to receive both incoming and outgoing traffic for the entire LAN, what three things need to occur?

•Attacker sends two Gratuitous ARP responses:

First one to update Victim’s ARP cache

oHey, the Gateway’s IP is at attacker’s MAC address!

Second one to update Gateway’s ARP cache

oHey, the Victim’s IP is at attacker’s MAC address!

•Attacker enables IP forwarding on their host to intercept and forward all incoming and outgoing traffic

**QUESTION 16**

Webspy allows an attacker to view the victim's actual browser window as if they were sitting behind the victim.

 True

 False

**QUESTION 17**

What is the danger of Replay Attacks?

Could replay the pcap to pass a victim’s authentication credentials or session cookies in order to authenticate as the victim.

**QUESTION 18**

During the first week, I provided a timeline for your individual project.  This information is also listed in the "Project Info" folder in blackboard.  The first deadline is:

"You should have your service installed, functioning, and understand the default options before class on Feb 15th."

This assignment is due on the 21st, so by now you should have everything installed.

To answer this blackboard question, upload a screenshot of your individual project service running along with a text file open next to it containing your name.  (Most likely your project will be running in either a server or desktop OS running in a VM on your personal system.)  Remember, you should not use RADISH to work on your individual project.