Network Forensic workshop Exam

Q1 Use web site [http://pcap.capanalysis.net](http://pcap.capanalysis.net/) to answer the following

* 1. Out of total traffic, what is the percentage of outbound traffic?
  2. During which hour the outbound traffic volume was highest?
  3. Which IP address is responsible for highest data sent?
  4. How many bytes were sent from IP 192.168.1.76?
  5. The IP 67.180.72.76 is belong to which organization
  6. If this IP generating bad traffic targeting your origination and you want to report to the ORG which email you will use?
  7. The traffic seems to contain some packets/flows from privacy protection technique (or anonymizer solution). Can you identify the technique/solution/tool?
  8. Between 20:00-21:00 on 27 Aguste 2016, traffic can be observed for a popular online shopping service. Can you name the service?
  9. There is also traffic from two file popular file sharing methods. What is their name?
  10. IP address 192.168.1.76 exchanged some traffic with a machine in Canada. What is the IP of that machine?

Q2 referring to Q2.pcap answer the following

2.1 find the leaked data

2.2 What is the source IP address?

2.3 What is the destination IP address?

2.4 Which protocol used to leaking data

Q3 referring to Q3.pcap answer the following

3.1 How many exe files have been downloaded?

3.2 Which file is infected?

3.3 What is the accuracy rate of the infection?

3.4 Which protocol used to transfer the files?

Q4 Find the (supposed to be) confidential data in this Ethernet frame:

 00 05 73 a0 00 00 e0 69 95 d8 5a 13 86 dd 60 00    00 00 00 9b 06 40 26 07 53 00 00 60 2a bc 00 00    00 00 ba de c0 de 20 01 41 d0 00 02 42 33 00 00    00 00 00 00 00 04 96 74 00 50 bc ea 7d b8 00 c1    d7 03 80 18 00 e1 cf a0 00 00 01 01 08 0a 09 3e    69 b9 17 a1 7e d3 47 45 54 20 2f 20 48 54 54 50    2f 31 2e 31 0d 0a 41 75 74 68 6f 72 69 7a 61 74    69 6f 6e 3a 20 42 61 73 69 63 20 59 32 39 75 5a    6d 6b 36 5a 47 56 75 64 47 6c 68 62 41 3d 3d 0d    0a 55 73 65 72 2d 41 67 65 6e 74 3a 20 49 6e 73    61 6e 65 42 72 6f 77 73 65 72 0d 0a 48 6f 73 74    3a 20 77 77 77 2e 6d 79 69 70 76 36 2e 6f 72 67    0d 0a 41 63 63 65 70 74 3a 20 2a 2f 2a 0d 0a 0d    0a

Q5 a twitter authentication session has been captured, you have to retrieve the password from the file Q5.pcap

Q6 you find the configuration file of cisco router you have to decrypt and find the enable secret password, the file is Q6.txt

Q7. Use the Q7.pcap to find the following

7.1 The TTL used to reach the targeted host.

7.2 The TTL used to reply from the targeted host.

7.3 What is the IP address of target host?

7.4 What is the IP address of the source of the ping request?

Q8. Using the Q8.txt file find the following

8.1 Find the password used to authenticate on the SIP infrastructure.

8.2 What is the service that IP 172.25.105.3 trying to register to it.

8.3 Does this service secure or not to use it over internet.

8.4 What is your recommendation as information security engineer to the network administrator to keep your organization secure?

8.5 This traffic sensitive to which type of attack Dos attack or eavesdropping attack or Brute Force Attack.

Q.9 a new critical vulnerability that can affect the Windows systems this vulnerability has been discovered recently your task to search from internet to answer the following.

9.1 What the name of this vulnerability

9.2 What is the CVE of this vulnerability?

9.3 Nearly how many Windows systems are still unpatched from this vulnerability all over the world?

9.4 Dose this vulnerability consider Wormable, that could allow malware to propagate to vulnerable systems just like [WannaCry](https://thehackernews.com/2018/08/tsmc-wannacry-ransomware-attack.html)

The answer is YES or NO

9.5 does Microsoft released the patches for this vulnerability if your answer yes then when.

Q.10 if you passed the exam and get the job are you will invite us for a party or not.

Good luck