Name : Pratik Shriram Sakhare  Class: BE COMP II (Q)
Subject: CSDF (C2)  RN: 29  PRN: F19112046
Experiment No: 1

Q.1. Why are email headers so important in computer forensics?

Ans: 1) Email headers contain important information about the origin and path an email took before arriving at its final destination, including the sender's IP address, internet service provider, email client, and even location.
2) The information could be used to block future emails from the sender (in the case of spam) or to determine the legitimacy of a suspicious email.
3) A review of the headers can also help to identify 'header spoofing', a strong indication the email was sent with malicious client.

Q.2. How can an email header analysis be used in the legal process?

Ans.
1) To investigate cases related to cyber crimes where emails are being used, digital forensic experts scan relevant emails for evidence.
2) Since criminal often forge messages to avoid detection, email forensic experts need to perform email header analysis to extract and collect crucial evidence.
3) Email headers contain vital information about the path that the message has traversed before reaching its final destination.
4) This information includes recipients and senders name,

tag, in particular, to decide whether to ... helps email service provid... ...ocating Security Payload (ESPs) ...

time of sending and receiving the email message, email client, internet service provider (ISP), IP address of sender, etc.

5) This information and other email header fields can help in determining the legitimacy of a suspecious or malicious email.

---

Q.3. How the use of email header information could be used by a digital forensic professional in an investigation?

Ans. 1) Email headers contain important information including name of the sender and receiver, the trail (servers and other devices) through which the message has traversed, etc.

2) The vital details in email headers can help investigators and forensic experts in email investigation.

3) Example- the delelivered-to field contains email address of recepient and therefore received-by field contains last visited SMTP server's IP address, its SMTP ID, and therefore the date and time at which the email is received.

4) Similarly, the Received: from field may provide key details like IP address of sender and host name.

5) Such information are often instrumental in identifying the culprit and collecting evidence.

---

Name: Pratik Shriram Sakhare Class: BE COMP II (Q)

Subject: CSDF (C2) RN: 29 PRN: F19112046

Experiment No. 2

Q.1. What's the purpose of CAPTCHA technology and how does it work?

Ans. 1) CAPTCHA (Completely Automated Public Turing Test to tell Computers and Humans Apart) is a type of security measure known as challenge-response.

2) The purpose of CAPTCHA is to protect user from spam and password decryption by asking user to complete a simple test that proves user is a human and not a computer trying to break into a password protected account.

3) Classic CAPTCHAs, which are still in use on some web properties today, involve asking users to verify letters. The letters are distorted so that bots are not likely to be able to identify them.

4) To pass the test, users have to interpret the distorted text, type the correct letters into a form field, and submit the form. If the letters don't match, users are prompted to try again.

5) The idea is that a computer program will be unable to interpret the distorted letters, while a human being will usually be able to identify them.

Q.2. How attackers defeat CAPTCHAs?

Ans 1) There are multiple ways CAPTCHA can be defeated. A common method is to use a CAPTCHA solving service,

which utilizes low-cost human labour in developing countries to solve CAPTCHA images.

2) Cybercriminals subscribe to a service for CAPTCHA solutions, which streamline into their automation tools via APIs, populating the answers on the target website.

3) These shady enterprises are so ubiquitous that many can be found with a quick Google search including:

(i) DeathbyCAPTCHA
(ii) 2Captcha
(iii) Kolotibablo
(iv) ProTypers
(v) Antigate

Name : Pratik Shriram sakhare  Class: BE COMP II (Q)
Subject: CSDF (C2)  RN: 29  PRN: F19112046
Experiment No. 6

Q.1. What should I look for in Wireshark capture?

Ans. 1) Wireshark shows you three different panes for inspecting packet data. The packet list, the top pane, lists all the packets in the capture.

2) When you click on the packet, the other two panes change to show you the details about the selected packet. User can also tell if the packet is part of a conversation.

3) Here are details about each column in top pane- Number, Time, Source, Destination, Protocol, Length, Info.

4) Packet details, the middle pane, shows as much readable information about the packet as possible, depending on the packet type.

5) The bottom pane, Packet bytes, displays the packet exactly as it was captured in hexadecimal.

6) When looking at a packet that is part of conservation, user can right click the packet and select Follow to see only the packets that are part of that conversation.

Q.2. How do you analyze packet captures?

Ans. 1) Once the packets are captured, Wireshark organizes them in a detailed packet list pane that's easy to read

2) If user wants to access information regarding a single packet, all he have to do is to locate it on list & click.

3) You can further expand the tree to access details of each protocol contained within the packet.

4) For a more comprehensive overview, go through the following steps—

(i) Select the packet from the list with cursor, then right click

(ii) Open the "View" tab from the toolbar above.

(iii) Select "show packet in New window" from drop-drown menu.

5) There are these 5 ways to analyze packets in the Wireshark—

(i) Use a custom wireshark profile

(ii) Get first information from 3-way handshake.

(iii) Check how many packet have been lost.

(iv) Open the Expert information

(v) Open the Round trip time graph.