Rohit Patiballa
21BCI0278

Assignment – 2

Exploring tools of Kali linux

1. **Wireshark –**

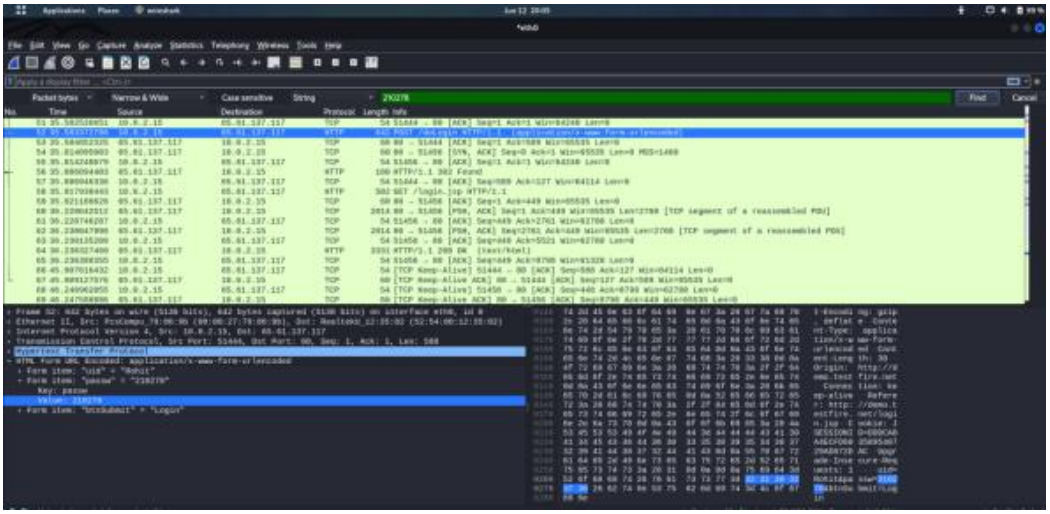
Summarizing what I've explored about wireshark , here are a few highlits -

1. Wireshark is a popular open-source packet analyzer that comes pre-installed on Kali Linux, a specialized Linux distribution for penetration testing and ethical hacking.
2. It allows users to capture and analyze network traffic in real-time, making it a valuable tool for troubleshooting, security analysis, and monitoring network activity.
3. Wireshark supports a wide range of network protocols, enabling users to dissect and inspect packets at various layers of the OSI model.
4. With its user-friendly graphical interface, Wireshark simplifies the process of capturing and analyzing network packets, even for those without extensive networking knowledge.
5. Network professionals use Wireshark to identify network issues, diagnose performance problems, and detect suspicious or malicious activities on a network.
6. Wireshark offers advanced features like packet filtering, color coding, and protocol analysis, making it suitable for both beginners and experts in the field.
7. It can capture traffic from a variety of sources, including Ethernet, Wi-Fi, and USB interfaces, allowing for comprehensive network analysis.
8. Wireshark's "Follow TCP Stream" feature allows users to reconstruct and view the contents of a complete TCP session, aiding in the analysis of data exchanges.

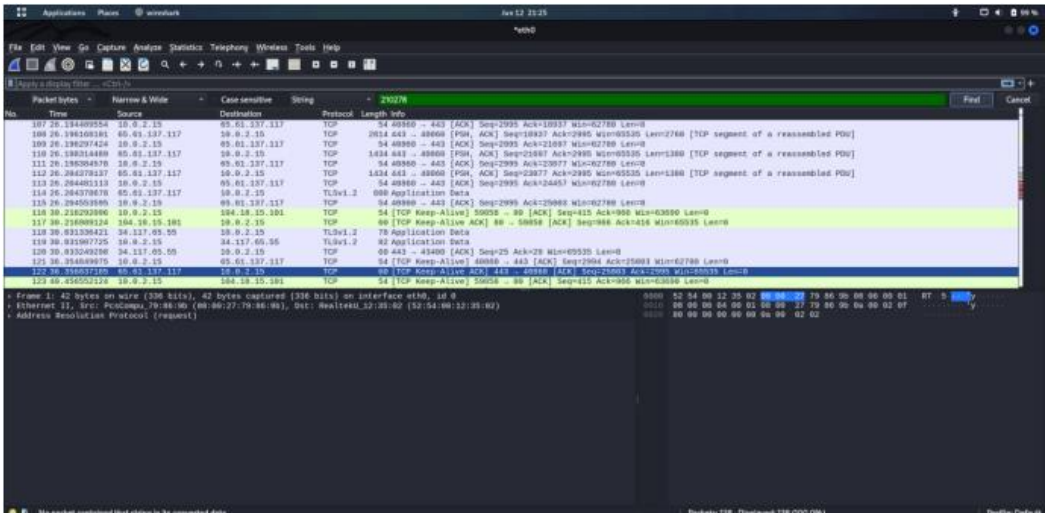
Rohit Patiballa
21BCI0278

9. Kali Linux, with Wireshark, is a powerful combination for ethical hackers and penetration testers, as it helps identify vulnerabilities and assess network security.
10. Continuous updates and a robust community support Wireshark, making it an essential tool for anyone working with network traffic analysis on Kali Linux or any other Linux distribution.

For HTTP protocol -



For HTTPS protocol –



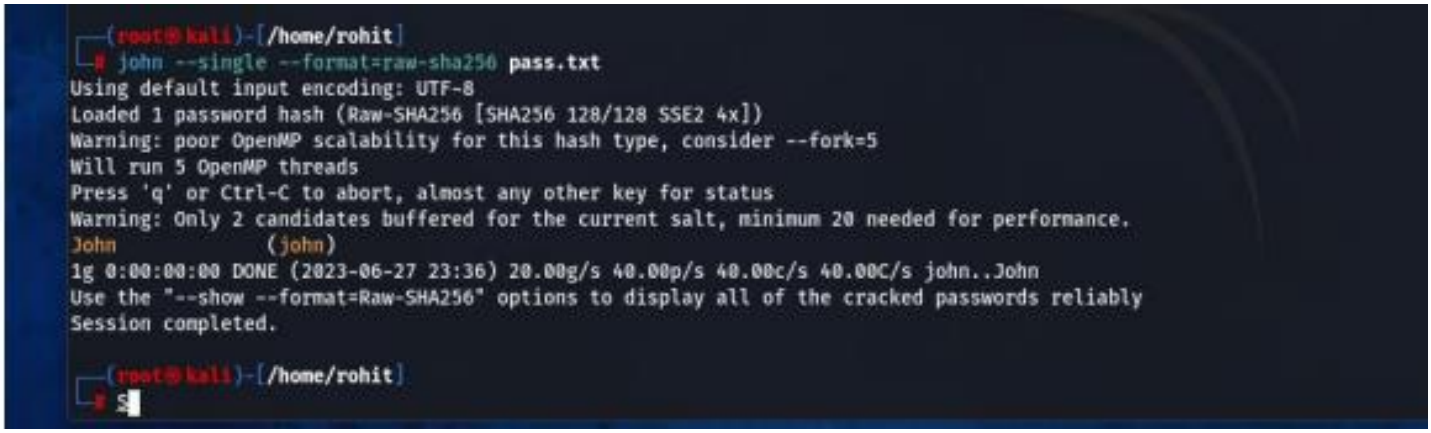
So wireshark works only for HTTP not for HTTPS protocol.

Rohit Patiballa
21BCI0278

2. John Ripper –

Summarizing what I've explored about John the Ripper , here are a few highlits -

1. Password Cracking Tool: John the Ripper is a renowned and versatile password cracking tool available on Kali Linux. It is primarily used for assessing the strength of passwords by attempting to crack them through various methods.
2. Multiple Attack Modes: John offers several attack modes, including dictionary attacks, brute-force attacks, and hybrid attacks. It can systematically guess passwords using wordlists, generate permutations, and adapt to different scenarios, making it a flexible tool for password security testing.
3. Wide Platform Support: John the Ripper is not limited to Kali Linux; it's available on various operating systems, making it a cross-platform tool for password security analysis. This allows security professionals to use it on different systems as needed.
4. Community and Commercial Versions: John the Ripper has both open-source community versions and commercial versions (such as "John the Ripper Pro") with additional features and support. The community version is freely available, while the commercial versions offer enhanced capabilities and support options for organizations and security experts

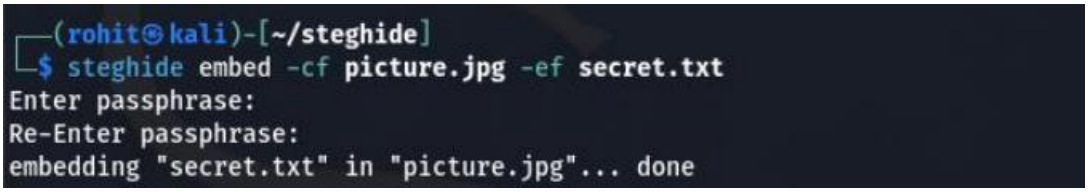


Rohit Patiballa
21BCI0278

3. **Steghide tool –**

Summarizing what I've explored about Steghide tool , here are a few highlits -

1. Concealing Data: Steghide is primarily used for hiding sensitive data within digital images and audio files. It employs steganography techniques to embed information in a way that is not readily apparent to casual observers.
2. Encryption: Steghide can encrypt the data it hides, providing an additional layer of security. This means that even if someone discovers the hidden content, they cannot access it without the decryption passphrase.
3. Wide Format Support: Steghide supports a variety of image and audio formats, making it versatile for concealing data in different types of media files. Common formats include JPEG, BMP, WAV, and more.
4. Passphrase Protection: Users can protect their hidden data by setting a passphrase during the embedding process. This passphrase is required to extract the concealed information from the media file.
5. Use Cases: Steghide is used for various purposes, including secure communication, digital watermarking, and hiding confidential information. Security professionals, researchers, and individuals concerned about data privacy often utilize Steghide to protect their sensitive data.



Rohit Patiballa
21BCI0278