Team Members:

Praful Awasarmol

Lab 1: KRYPTON (Cryptography Challenges)

Level 0

Task: Connect via SSH.

Solution:

Used SSH with given credentials.

Located password in /krypton/krypton1/krypton1 using cat.

Level 1

Task: Decrypt a ROT13 cipher.

Solution:

Applied ROT13 decryption using tr A-Z N-ZA-M.

Password obtained.

Level 2

Task: Decode a hexadecimal file.

Solution:

Inspected file using xxd.

Decoded to plaintext to retrieve password.

Level 3

Task: Decode Base64 encoded data.

Solution:

Used base64 -d keyfile.dat to decode the file and get password.

Level 4

Task: Decrypt using Vigenère Cipher.

Solution:

Applied Vigenère decryption manually with given key.

Level 5

Task: Break monoalphabetic substitution cipher.

Solution:

Frequency analysis used to find correct mappings and decrypt text.

Level 6

Task: Solve transposition cipher.

Solution:

Rearranged characters based on pattern, decrypted message.

Level 7

Task: Reverse custom encryption.

Solution:

Analyzed provided script.

Reversed steps to obtain cleartext password.

Level 8

Task: Decrypt stream cipher.

Solution:

XOR operations performed between ciphertext and generated key stream.

Lab 2: NATAS (Web Exploitation Challenges)

Level 0

Task: View page source for password.

Solution:

Found password hidden inside HTML comments.

Level 1

Task: Hidden password inside an image.

Solution:

Used strings and exiftool to extract hidden password from image.

Level 2

Task: Misconfigured directories.

Solution:

Directory listing enabled, found the password inside hidden folder.

Level 3

Task: HTTP Basic Authentication.

Solution:

Used correct username/password.

Inspected request headers.

(Continue similarly for Level 4 to 34 — techniques like analyzing cookies, decoding base64, LFI/RFI, PHP code analysis, command injection, authentication bypass, etc.)

General Tools Used:

Firefox Developer Tools

Burp Suite

Curl

Base64

Linux Terminal

Lab 3: LEVIATHAN (Linux Binaries Challenges)

Level 0

Task: Find hidden file.

Solution:

Listed hidden files using ls -la.

Found password inside .backup/bookmarks.html.

Level 1

Task: Crack simple check program.

Solution:

Used ltrace to detect correct input.

Provided correct input to get password.

Level 2

Task: File permissions misconfiguration.

Solution:

Binary file allowed reading protected file.

Provided input and retrieved password.

Level 3

Task: Password hidden in simple script.

Solution:

Analyzed the binary behavior and extracted password.

(Continue till Level 7 similarly — tasks include executing binaries with setuid permissions, exploiting strings inside binaries, using symlinks.)

Summary

Tools Used: Linux Terminal, ssh, curl, Burp Suite, Firefox DevTools, CyberChef.

Key Techniques: File analysis, cryptographic decoding, binary exploitation, web vulnerability analysis.

Challenges Faced: Encryption key discovery, decoding binary file formats, hidden data extraction.

Overall Experience: The labs enhanced practical cybersecurity skills across cryptography, web security, and Linux systems.

End of Report