CTF – SEPTEMBER 25

PREREQUISTE :

- Metasploitable machine

1 Wireshark:

"Oops! Our network got 'telnapped'! 🥷 Some mischievous intruder thought telnet was still cool, but they left a 'login trail' behind. Your mission: Find the hacker's 'login name' from the attached pcap file and bring them to justice! 💻🚀😂"
HINT: Include ans in SAIT'SCTF{----}
ANS: SAIT'SCTF{tteesstt}

2 Forensics image:

"Looking for the secret flag? It's like finding Waldo in a library! 🥷🗄
Hint: The flag is hiding somewhere inside a file. Start your digital treasure hunt and uncover the flag's sneaky hiding spot! 🔍💾😁"
Image: Picture
Flag: SAIT'SCTF{YouareoneofthebeststudenthereatSAIT}

3Email header

Title: "McAfee Madness: Where in the World is Our Hacker?"
Together we are powerful! 🌐 McAfee alert!! Get 60% discount. An attacker is pulling a fast one by sending you an email about enhancing your security. Can you dig through the digital chaos and uncover the country where this cheeky hacker is sipping cyber-tea and plotting their next move? ☕🥷
ANS: SAIT'SCTF{UKRAINE}

4CRYPTOGRAPHY

Do you know what ROT13 is ? Crypto is necessary.
FNVGPGS{Npgvbavfgursbhaqngvbanyxrlgbnyyfhpprff}
HINT: convert
ANS: SAITCTF{Actionisthefoundationalkeytoallsuccess}

5GENERAL CTF:

Long rambling directory ? Can you loop directories inside a directory ? Find the flag if you can ?ANS :
ANS: SAIT'SCTF{I_am_your_flag}

6REVERSE-ENGINEERING:

"Dr. Evil's Lab - Code Breaker Challenge: Get the Doomsday Blueprint! Dr. Evil's lab is locked down tight! Junior agent got us the code, but it's in VaultDoorTraining.java. Crack the code and unlock the training vault to prove your skills!"
The source code for the training vault is here: VaultDoorTraining.java

HINT : The password is in the program source code.
ANS: SAITCTF{w4rm1ng_Up_w1tH_jAv4_3808d338b46]

7 BINARY:

23249425. Whats next ?
HINT: Mersenne
ANS: SAIT'SCTF{24862048}

8 DATABASE-EN:

"Congratulations! You've stumbled upon the website of the 'World's Messiest Database Enthusiast'! Rumor has it they love collecting databases like others collect stamps. 🧐 Your mission, should you choose to accept it, is to infiltrate their website at http://testphp.vulnweb.com/ and find out how many databases they're currently hoarding. It's rumored to be a secret, but we've heard they've left some clues lying around in plain sight. Happy hunting, detective! 🕵️
HINT: Include the number in SAIT'SCTF{n} ; n= number of databases.
ANS: SAIT'SCTF{2}

9 BASE64:

A Top-secret file encoded as "aXRnZXRzaGFyZGVyZnJvbWhlcmU=". There's an equal sign (=) at the end. Is it just for show, or does it hold the key to unlock the mystery? Can you figure out what's so special about that equal sign?
Hint: Sometimes, even the smallest details can lead to big revelations. Don't underestimate the power of the equal sign!
ANS: SAIT'SCTF{itgetsharderfromhere}

10: METASPLOITABLE:

"Welcome to the 'King SAMBA's Castle' CTF challenge! We've captured an ISO image of the infamous Metasploitable OS, and it seems that Port 445 have been seized by the all-powerful King SAMBA himself. Legend has it that King SAMBA is very proud of his version of Samba, which he believes is the best in all the land. Can you infiltrate his castle and uncover the version of Samba he's bragging about?
ANS: SAIT'SCTF{Samba3.0.20-Debian}
HINT: heard about badlock

11: Dirbuster:

Title: "Virtual Box Voyage: Hunt for the HTTP 300-Code Page!"
Question:
Ahoy, matey! 🕹️ Are ye ready for a digital treasure hunt? Host the ISO file in yer trusty Virtual Box, and embark on a swashbucklin' adventure to penetrate the webserver! Can ye uncover the hidden gem - the number of the HTTP response page with the code 300? 🏴‍☠️🌐💎
Ans : SAIT'SCTF{56}

12:Reverse Engineering:

You've stumbled upon an enigmatic program called "reverse_challenge." It claims to have a flag hidden somewhere. The problem is, the program seems to have developed a sudden shyness. Can you coax it into revealing its flag?
Hint: Look closely; the flag isn't very good at hide-and-seek!
ANS: SAIT'SCTF{Todayis25thSeptember}

13:CRYPTOGRAPHY:

The one time pad can be cryptographically secure, but not when you know the key. Can you solve this? We've given you the encrypted flag, key, and a table to help CAGHZYYELAKUY with the key of AAFZBTABACKU. Can you use this table to solve it?
ANS: SAIT'SCTF{CALGARYFLAMES}

14: DATABASE:

Welcome to the "Wacky Database Adventure"!
You've just been granted access to a super-secret database, but here's the catch—every 5th entry in all the tables of the database is as strange as a penguin in a tutu! Combine all entries and see if you can pull a flag out. Have fun and happy hunting!
ANS: SAIT'SCTF{Calgaryishome}
Hint: ROT13.

15: WEB-APPLICATION:

Analyze the website to pull out the flag.
ANS; SAIT'SCTF{yourockedthectftoday}

16: MITM ATTACK:

We are compromised!!
"Picture this: our system got hit by a mischievous hacker armed with a payload embedded on webserver. Can you decrypt the payload's name ?
ANS; SAIT'SCTF{crack.exe}

17: PEEKINTOBINARY:

In your hands lies a compiled program game, But here's the twist: it has a secret, and that secret is the size of its program header. Can you unveil the program's hidden dimensions.
Flag format: SAIT'SCTF{Xbytes}
ANS: SAIT'SCTF{64bytes}

18:LOG FILE:

You are the network admin and recently there was an unlawful entry. The attacker did played with your system. Before you could do anything, the attacker was able to erase their account, but you had the access logs. Pull out the attacker's name.
HINT: Domain was GMCYBER
ANS: SAIT'SCTF{cinderella}

19 REVERSE ENGINEERING:
Cracker! Cracker!
Here is a cracker. Blast it to get a flag.
ANS: SAIT’SCTF{You_Found_it}

20: REVERSE ENGINEERING:
Boomer! Boomer!
Play with the file and pull the flag out.
ANS: SAIT'SCTF{I_LoVe_PrOgRaMmIng}