CTF: Code Crusade - Conquer the Digital Realm

Welcome, digital adventurers! Are you prepared to embark on a journey into the heart of cyberspace? We're granting you access to a labyrinth of virtual challenges, where cunning minds and deft fingers reign supreme. Picture yourself as a modern-day Sherlock Holmes, deciphering cryptic clues and navigating through intricate puzzles. Your mission, should you choose to accept it, is to breach the defenses, unearth hidden treasures, and claim the elusive flags that await those who dare. Are you ready to pit your wits against the finest minds in the digital realm? The gauntlet has been thrown, the challenge awaits—step forward and prove your mettle in the electrifying world of Capture The Flag!

Tasks:

1. Register on the CTF platform(http://10.200.33.139/ - *Intranet only*)
2. Create a team of three and ask your teammates (you are free to form group with any student, even if you already paired up with him/her as part of other assignments or the term project) to join your team.
3. Hack into a vulnerable virtual machine (*Find VM's IP address in the google classroom, from the TAs*)
4. Access the server (*username ns*)
5. Find and submit the flags to CTF as soon as you find them.
6. There are a total of **8 flags**. You must create a python script to perform the attack(s). The input should be the ip address of your assigned VM and the output should be the first 4 flags. **The last 4 flags need not be scripted.**
7. Faster the submission, higher the scoring points.
8. Draft a report documenting your methods and work distribution among the teammates.
9. Seek help from references or Hints from the CTF platform, but beware of the potential cost to scoring points.
10. Lastly, have fun :D

Hacker's Note:-

1. The CTF is divided into **2 parts**, the first four flags constitute the first part and the last four flags constitute the second part.
2. In the world of cybersecurity challenges, much like in epic gaming sagas, there comes a point where facing the main adversary feels daunting. It's at this juncture that strategic detours into side quests become invaluable.
3. In our cybersecurity challenge, the last four flags serve as crucial side quests.
4. Nonetheless, you must complete all the quests, i.e. retrieve all the 8 flags.

General Tips:

First-Time Hackers, Rejoice! Your Ultimate Guide to CTF Success:

1. *Start with the basics* - review the concepts you've learned in the NS course and get familiar with the tools of the trade.
2. *Don't be afraid to ask for help* - reach out to classmates, references, Github repos, ChatGPT or the TAs for a hint (but remember, sharing is not always caring).
3. *Think outside the box* - the most creative solutions are often the most effective.
4. *Keep a cool head* - hacking can be frustrating, but remember to take breaks and stay focused.
5. *Stay organized* - keep track of your progress and take notes on what worked and what didn't.

Now, suit up and get ready to hack your way to glory! The world of network security is waiting for you to conquer it:-)

Stuck in a rut? Don't worry, references (given below) are at your fingertips to guide you on your journey. Still can't crack the code? Time to call in the big guns! Contact the TAs for a hint, but beware, sharing the wealth may cost you scoring points given. Remember, grading is relative, and every action has consequences. So, choose wisely before dishing out any hints to your fellow hackers.

Deliverables:
As part of your mission, you must create a Python script to automate the process of exploiting the vulnerabilities and gain access to the coveted flag1, flag2, flag3, and flag4. Further, you need to document your methods, for *all the flags*, in a clear and concise **report**(max 5 pages). Teamwork is key, so don't forget to clearly outline the work distribution amongst your team members (Max of 1 page).
Show off your skills and impress your classmates as you become the master of the cyber security world.

Submit a google form with all 8 flags.:https://forms.gle/WFuga9B5P4Nadfzx7
(No marks if flags are not submitted on both google form + CTF)

The flags are in the format flag#{some_random_thing}
Eg. flag4{I_am_a_hacker}
P.S.: Every group has different flags, do not bother wasting time in seeking help from other groups :D

Marks Distribution
Flag 1:25
Flag 2:50
Flag 3:75
Flag 4:100

Flag 5: 25
Flag 6: 50
Flag 7: 50
Flag 8: 75
Script to attack:150(including viva)

Note: Your grade for this assignment will depend on how quickly you submit it compared to your classmates on the CTF platform. If you submit your assignment faster than others, you will receive a higher grade.

ANTI PLAGIARISM STATEMENT <*Include it in your report. This statement has been revised as you are allowed to use any publicly available tools/repos/scripts, including ChaptGPT's help for capturing the flags in this assignment*>

We certify that this assignment/report is our own work, based on our personal study and/or research and that we have acknowledged all material and sources used in its preparation, whether they be books, articles, ChatGPT tips, packages, datasets, reports, lecture notes, and any other kind of document, electronic or personal communication. We also certify that this assignment/report has not previously been submitted for assessment/project in any other course lab, except where specific permission has been granted from all course instructors involved, or at any other time in this course, and that we have not copied in part or whole or otherwise plagiarized the work of other students in this group. We pledge to uphold the principles of honesty and responsibility at CSE@IITH. In addition, We understand my responsibility to report honor violations by other students if we become aware of it.

Names:
Date:
Signature: <keep your initials here>

References:

https://portswigger.net/burp
https://gchq.github.io/CyberChef/
https://www.wireshark.org/
https://www.base64decode.org/
https://www.kali.org/tools/dirbuster/
https://nmap.org/
https://github.com/OJ/gobuster