

CS628 – Take Home Lab Exam

Disclaimer: This contest aims to familiarize you with some offensive techniques in computer security. You will be carrying out attacks with our permission in a controlled environment. Keep in mind that doing similar attacks on other machines without authorization is a legal offense. You may face disciplinary and legal action for unauthorized attacks.

The exam is in the format of a capture-the-flag security contest. You will be required to solve security related problems most of which are from topics covered in the class. When you successfully complete a challenge, you will get a flag, which is a passphrase that you have to submit to get points for that challenge. Here are the rules for the contest:

- The contest has around 10 challenges & more problems can be added during the CTF.
- The main contest page is at <https://cs628a.cse.iitk.ac.in>
- The challenges are hosted on cs628a.cse.iitk.ac.in, To solve these challenges, you have to SSH into this machine with the credentials mailed to you. Your task is to read the file `flag.txt` for challenges.
- Teams are not allowed in this CTF. This is an individual event.
- All flags are of the format `cs628a{ }`. For example, if you see `cs628a{supersecret}` on solving a challenge, submit `cs628a{supersecret}` on the contest page. It is important that you submit the flags as you capture them. Don't delay the submission.
- The contest will be active till 11:55 pm, 12 September.
- To maintain the integrity of the contest, anyone can be called randomly by the TAs to give a demo of the exploit used by them.
- Collaboration is not allowed. If a student is found to have shared his/her work with another student, both will be given 0 for this lab. There are several monitoring mechanisms in place to detect cheating. We will be checking your entire history of commands on the server.
- If you feel lost and are looking for hints feel free to ask on Piazza. You can also send direct messages to Bidya Sarkar (bidya@), Dixit Kumar (dixit@), Hariom (hariom@), Mayank Rawat (mayankr@), Nirjhar Roy (nirjhar@), Krishna Kumar Tayal (ktayal@) and Supriya Suresh (ssuresh@).
- If you face any issue in the ctf server or flag submission portal, contact Mayank(mayankr@) or Krishna(ktayal@).
- Any attempts to DoS the contest infrastructure will attract penalties.
- If you find any weakness in the contest infrastructure, let us know without trying to misuse it. You may be given bonus marks for this.
- In order to ensure availability for everyone, your accounts on the contest server have some resource limits. Let us know if you find them to be too restrictive.

Deliverables: You should submit a zip file containing subdirectories with the name of problem. Each subdirectory should have a file `answer.txt` describing in not more than 5 lines how you solved or attempted to solve the challenge. If you wrote any small code/script for that challenge, include it in the subdirectory.

Include a file `'it.txt'` in the root directory mentioning the maximum penalty under the Indian IT Act, 2000 for "Hacking with computer system" and "Securing access or attempting to secure access to a protected system".