Club PREMIER UNIVERSITY

CTF Recruitment Examination-2025

ID: 02222100051011209 **BATCH:** 41 **SECTION:** C

CLUE: Once upon a late night in the PUC cyber-lab, an old terminal — where an evil entity was trying to communicate from a distance to recruit members for its team. On its screen there appeared strange questions, but not all of them were true. Some were lies, half-truths, or broken commands planted by a mischievous hacker. For each riddle, the terminal opens a box; that's where your answer belongs. But **beware**: some choices are impostors. If you can spot the lies, you must **repair** them with the correct truth. Besides the truth, every lie you expose, and fix earns you +10 bonus points. Some riddles may hide more than one truth catch them all if you want the full reward.

The first solver claims **+30 points**. Every next solver earns 5 points less — 25, 20, 15… until the bonus fades to **0.**

1. You receive the string: **UHl0aG9uIQ==** what kind of hash ?? 10 + 10 Points

10 ☑ Base 64 ☐ Oracle ☐ SHA 12 ☐ MD5 ☐ bcrypt

SHA512 10

2. You want to fetch a small file from a machine running an HTTP server on port 8000. Suggest a quick client-side command. 10 + 10 = 20 Points

curl - - - - 10

~~wget~~ wget - - - 10

3. During a web test, you find a field that reflects your input back into the page without sanitization. Example: typing <script>alert("hello")</script> pops up an **alert box**. 20 Points

What type of attack is possible?

10 ☐ SQL-inverse Injection ☑ XSS (Cross-Site Scripting) ☐ RFI ☐ CSRF

10

4. A **robots.txt** file in a website is used for: 10 Points

☐ Storing user passwords ☐ Hiding Admin credentials ☐ Detecting malware

10 ☑ Giving instructions to search engine crawlers ☐ Preventing SQL injections ☐ Encrypting data

5. Which of the following protocols can send data **unencrypted**? 30Points

10 ☑ HTTP ☐ HTTPS ☑ FTP ☐ SFTP ☑ Telnet

10 10

6. Which tools could help you test for hidden **directories** on a web server? 40 Points

10 ☑ Gobuster ☑ Dirb ☑ Nikto ☑ Burp Suite ☐ Hydra ☐ Wireshark

10 10 10

7. Which of the following can lead to sensitive **data exposure** on a web app? 40 + 10 Points

10 ☑ SQL Injection ☑ XSS ☐ MSRF ☑ Directory Traversal ☐ HTTPS ☑ Local File Inclusion

10 10 XSRF 10 10

8. You have a suspicious binary file — **Recovery** — which shows only 0s and 1s. What tools can you use to quickly view human-readable strings? 60 Points

☑ strings	10
☐ Elf-read	→ 20 → read-ELF
☐ Dumb-Obj	→ 20 → obj-dumb
☑ hexdumb	10

9. Which of the following can be analyzed in digital forensics to find evidence? 4*10 = 40 Points

10 10 10

10 ☑ Log files ☑ Memory dumps ☑ Network packets ☐ Encrypted passwords ☑ Registry keys

☐ Random JPEG images

10. Which of the following sources/tools can be used to gather open-source intelligence? 40 Points

☑ Google search ☑ Shodan ☑ Social media ☐ Metasploit ☑ WHOIS ☐ Wireshark

11. Below are some GUI and CLI tools, describe them in one line: 10*6 + 20 = 80 Points

a) Nmap ➡ network map
b) Wireshark ➡ Packet capture + analysis
c) Burp Suite ➡ testing framework
d) Hydra ➡ brute force
e) Hydrosploit ➡ metasploit → payload injection
f) Nikto ➡ vulnerability scanner

20

12. Why you wanted to do CTF not in the Competitive Programming Club?? Is there any future goal?? What is the relation between CTF and Cyber Security? 10 + 10 + 20 = 40 Points

13. Suppose you just breached the wall of PUC (although we don't have one) and obtained some credentials, like a username **Kingshuk_Sir** and a password hash **$2a$05$bvIG6Nmid…..** In which way would you attempt to crack the hash in the least possible time? You may type CLI commands if you think you're smart enough or you can do it in the web. For both, you can gain double points. 40 + 40 = 80

hascat / John the ripper 40

Tunnel up → for hash 40
cybershot → for decrypt.

14. An image **photo.png** is given. You're told "not all is seen". What quick commands would you try to find hidden data? For each try (yes, you read that right — for each try) you will get marks. For each line, you will get 10. Now it's up to you how much you can get -_- Unlimited Points

Solved by ↓ Creator @Punih:

strings, exiftool, binwalk, steghide 8

xxd ~~X~~ ztxcy ⟶ many more