Assignment 6 - Incident response

Kerbin Space Agency's systems (10.X.10.95) have seemingly been hacked! Thankfully, they've had logging systems in place: journald and auditd are running on their system. They have hired you back to look through logs to conduct incident response and create a report on your findings. Your tasks are to:

1) Determine the precise time/date of the start of the attack, and the IP address of the attacker.
2) Determine the vulnerabilities which were exploited, and what damage the attacker may have caused (if any).
3) Remediate (patch) the vulnerabilities which enabled the attack.

Your credentials to log in are:

User	**Password**
localuser	password
dev	password
gitea_admin (On Website)	Bui1dFlyDr3am2011!
jhansen	Bui1dFlyDr3am2011!
gkerman	Widen-Ambition-Fiddle

Note that this list does not contain service users used to run the services. Deleting them may cause your services to brick.

Point deductions:
If at any time you require the instructors to reset Kerbin Space Agency's systems (your target box), you will receive a five point penalty per reset. Don't lock yourself out or erroneously delete/remove things!

Extra Credit:
Your penetration testing results (from assignment 4) have been paramount in helping us realize the gaps in Kerbin Space Agency's infrastructure! They would like to invite you back to help *remediate* the vulnerabilities that have been found.

Below is a list of the vulnerabilities. Each successfully remediated vulnerability is worth 2%.

Gitea

- SSH private key exposed in the Gitea instance

File Permissions

- wp-config.php file found on web server with credentials exposed
- localuser (Ludus staging acc) has a bunch of hints and hacking payloads

FTP

- Files in FTP share should not be public
- jhansen has default example password
- FTP users not restricted to webshare (chroot jail)

Web Vulns

- Web server executes dangerous PHP code

Privilege Escalation Vulns

- Pack2TheRoot - CVE-2026-41651
- OverlayFS - CVE-2021-3493
- Cron script
- Sudo baron samedit - CVE-2021-3156