

Labs: Blue Team

Pablo Fraile Alonso

Create a hardened server.

Create and configure a hardened Linux server with the following requirements:

- Distro: Ubuntu Server.
- SSH must be installed, enabled, and running.
- You must be serving a simple webpage with HTTP traffic on port 80.
- TLS/HTTPS is not required.

You do not need to configure:

- Secure Boot
- Full-disk encryption

These protections are unnecessary because the system will run as a disposable/dummy virtual machine.

You may deploy the web server using containers. If you choose a containerized approach, keep the solution as minimal and security-focused as possible, avoiding unnecessary packages, services, images, and privileges.

Please, be aware that ubuntu server uses AppArmor LSM instead of SELinux. You can see a [simple guide of AppArmor on the debian documentation](#).

Once the installation is complete, you should create a document explaining the measures you implemented and the commands you used to verify that the distribution was configured according to security best practices.

Prometheus, Grafana, and Loki.

Next, clone the server you just configured to create a second instance. You should now have two identical **hardened servers**.

With both servers ready, proceed to set up your **observability stack**. For detailed setup instructions, refer to the [Observability Stack Configuration](#) guide.

IDS

HoneyPots

Adapt “Server 2” to: - Install [cowrie honeypot](#) - Configure cowrie to be an SSH honeypot.
- Enable the prometheus exporter on cowrie. - Create a notification on Prometheus Server (Server 1) so, when someone connects to the honeypot, you get a notification.

Forensic

See the [forensic exercises](#)

Extra Exercises:

- [SadServers Bata exercise](#) (extra-easy, just a linux sysadmin tool)
- [SadServers porto exercise](#) (easy)
- [SadServers annapurna](#) (medium level, keep in mind how docker is configured)
- [SadServers madrid](#) (medium level, capabilities)