Work assignment

The following table includes a list of proposed assignments that can be done during the course and should be presented in class during the theory sessions.

Topic	Observations
SSH Certificates	Usage of SSH certificates
WireGuard	Lightweight VPN in GNU/Linux
Let's Encrypt	Free TLS certificates
Password Store	Personal password manager
HashiCorp Vault	Credentials storage service
Wireless network cracking frameworks	aircrack-ng, reaver
Password cracking frameworks	hashcat, john
Configuration management	Ansible and Chef

Some considerations about assignments:

- Assignments are intended to be completed by 4 or 5 people.
- The assignment should be 20–30 pages, single-spaced, using a 12-point font.
- The exact deadline will be announced; it will be in December.
- Topics cannot be repeated among groups. The first request (via email or in person) will be granted.
- It is possible to add or modify points the group wants to investigate, but changes must be agreed upon with the professor.
- It is possible to work on a topic not included in the list; this must be agreed upon with the professor.
- Presenting the work orally is required to obtain the grade reserved for class participation. Presentations will take place during the last in-person classes in December.
- All assignments require a demonstration. Unless otherwise authorized, this demonstration must be carried out during the oral presentation.

SSH certificates

The usual way to deploy SSH in an organization is by using public keys. Each user provides their public key to the administrator, who adds them to the `~/.ssh/authorized_keys` file on the nodes the users have access to.

However, SSH certificates are an alternative that significantly improves the use of public keys.

This assignment consists of explaining:

- What SSH certificates are in detail.
- How they are issued and used.

- What security benefits they provide.
- How they compare to other options such as plain public keys or username/password.
- Demonstration.

WireGuard

VPNs are widely used to provide confidentiality and secure access to resources. WireGuard is a "recent" project, adopted in the Linux kernel, that creates VPNs in a simple and very lightweight manner.

This assignment consists of explaining:

- What WireGuard is and how it works.
- How to adopt and use it.
- What security benefits it provides.
- How it compares to other implementations such as IPsec or OpenVPN.
- Demonstration.

Let's Encrypt

Certification authorities for TLS certificates typically require validation and payment. Let's Encrypt aims to make obtaining trusted TLS certificates free and automated.

This assignment consists of explaining:

- What the project is about.
- What tools it offers and how their validation mechanisms work.
- How to adopt and use it.
- What security benefits it provides.
- How it compares to commercial CAs like DigiCert.
- Demonstration.

Password Store

Managing many distinct, secure passwords is challenging. `pass` is a password manager designed for individual use that uses the command line as its primary interface.

This assignment consists of explaining:

- What `pass` is and how it works internally.
- How to use it in its complete form (using `git` and asymmetric encryption with `gpg`).
- What security benefits it provides.
- How it compares to services like LastPass or 1Password.
- Demonstration.

HashiCorp Vault

Managing credentials across an organization is complex. HashiCorp Vault provides centralized secret management with advanced features.

This assignment consists of explaining:

- What HashiCorp Vault is and what it offers.
- Its basic concepts and how information is organized.
- How it works internally.
- What security benefits it provides.
- Demonstration.

Wireless network cracking frameworks

Wireless networks are common and use encryption to keep traffic confidential. However, tools exist that can recover keys and be used for attacks.

This assignment consists of explaining:

- Current wireless security protocols (WPA2, WPA3).
- aircrack-ng:
  - Which tools it provides and their purposes.
  - Detailed explanation of a typical attack.
  - Different supported attacks.
- reaver:
  - Which vulnerability it exploits and how.
  - Detailed explanation of a typical attack.
- Frameworks that automate these attacks (e.g., h4rpy).
- Demonstration. You may need hardware (e.g., access points); consult the professor for alternatives.

Password cracking frameworks

Passwords are usually stored as hashes. If hashes are leaked, tools can attempt to recover passwords.

This assignment consists of explaining:

- hashcat:
  - Supported attack modes.
  - High-level description of how it works.
  - Related tools in the ecosystem (e.g., hcxtools).
  - Demonstration.
- John the Ripper (`john`):
  - What it supports.
  - High-level description of how it works.
  - Demonstration.
- Relationship between both tools.

- Support for accelerator hardware (e.g., NVIDIA CUDA).
- Online services such as https://gpuhash.me.

Configuration management

Configuration management of distributed systems is essential to implement security policies consistently and audibly across many nodes.

This assignment consists of explaining:

- Infrastructure as Code concepts.
- Ansible:
  - Architecture and basic concepts.
  - How it works.
  - Related tools (AWX / Ansible Tower).
  - Demonstration.
- Chef:
  - Architecture and basic concepts.
  - How it works.
  - Related tools (e.g., Chef InSpec).
  - Demonstration.