{EPITECH}

GAMUT

VIRTUAL MACHINES ADMINISTRATION

GAMUT

Hogwarts Cybersecurity Lore

Introduction

In a time of unprecedented threat, **Hogwarts School of Witchcraft and Wizardry** is determined to protect the **Philosopher's Stone** by reinforcing its digital and magical defenses. Under the wise guidance of **Dumbledore**, Hogwarts has organized its defenses into two main factions : the **blue team**, responsible for defending the stone, and the **red team**, aiming to breach these defenses. Additionally, the school has assembled a **purple team** known as **WAND**, creating a three-way cybersecurity showdown where each team brings a unique approach to this high-stakes mission.

POCHE : The Blue Team

Mission

POCHE, or **Protection Operations and Cybersecurity Hazard Elimination**, serves as Hogwarts' **blue team** and is responsible for fortifying the school's systems against all forms of cyber intrusion. Their role is to build resilient defenses, identify vulnerabilities, and establish layered security measures to keep the Philosopher's Stone safe from hostile attacks.

Leaders : Fred & George

Leading **POCHE** are **Fred and George**, the clever and unpredictable Weasley twins. Known for their tactical minds and inventive flair, they work together to ensure Hogwarts' defenses are both secure and ingeniously tricky. With a mix of humor and skill, the twins set up clever traps and surprises that challenge even the most cunning opponents, making POCHE a force to be reckoned with.

WAND : The Purple Team

Mission

As the school's **purple team**, **WAND** or the **Wizards Acting for Network Defense** —adds an extra layer of agile and creative protection to Hogwarts' security efforts. Known for their flexibility and unconventional methods, WAND is tasked with supporting the defense of the Philosopher's Stone through unique and strategic approaches that enhance the overall security setup.

Leader : Lee Jordan

Leading WAND is **Lee Jordan**, an adept defender with a flair for quick, decisive action. Known for his instinctive approach to problem-solving, Lee brings agility and resourcefulness to the WAND team, making it a powerful complement to Hogwarts' defenses. Lee's focus is on outsmarting opponents with strategic creativity, ensuring that WAND remains an adaptable and resilient force against red team threats.

MIAOU : The Red Team

Mission

MIAOU, or the **Malicious Intrusion and Attack Operations Unit**, serves as the **red team**—a covert and highly skilled faction aiming to breach Hogwarts' defenses and seize the Philosopher's Stone. Using stealth, deception, and vulnerability exploitation, MIAOU embodies the offensive tactics of a real-world red team, testing Hogwarts' defenses to the fullest.

Leader : Dinosaur

The infamous **Dinosaur** leads MIAOU, and he's earned his name for a reason : his monstrous age and vast experience in the field make him a fearsome leader and a master of intrusion tactics. Dinosaur's unparalleled knowledge of both magical and cyber vulnerabilities guides MIAOU's

strategies, making him a nearly insurmountable opponent. His ultimate goal is to outmaneuver Hogwarts' defenders and claim the Philosopher's Stone.

Conclusion

Under Dumbledore's watchful eye, **POCHE**, **WAND**, and **MIAOU** engage in a high-stakes, multi-team battle of wits, skill, and magical prowess. **POCHE** and **WAND** work tirelessly to anticipate and counter every move from **MIAOU**, while Dinosaur's red team pushes the limits, seeking to expose and exploit any weak spots in Hogwarts' defenses.

The outcome of this three-way clash will determine not only the fate of the stone but also the legacy each team leaves in this epic cybersecurity showdown.

Your mission

You are a member of the **POCHE** group. Your mission will be to set up a server which will be used to protect and secure the stone. To do this, you will need to develop

— a server machine composed of a *Debian Server* operating system.
The virtual machine should be named `gamut_${name}` (`${name}` corresponds to your name).
You are free to define the size of this machine's random-access memory and virtual hard drive.
This virtual machine's network interface controller will be configured in *"Bridged""*.
This second virtual machine will contain a Web server and **therefore, should not** have a graphic environment

In order to test the robustness and availability of your server, you will also need a client machine. The latter is described as follows :

— a Dual Boot *Archlinux* and *Parrot OS linux* client machine, which should be set up with the help of **only one** virtual machine named `client_${name}` (`${name}` corresponds to your name).
You are free to define the size of this machine's random-access memory and virtual hard drive.
This virtual machine's network interface controller will be configured in *"Bridged"*.
The system administrator has given us technical characteristics for each operating system that you must comply with (*see below*).

Client machine

1. *Archlinux* operating system

Partitioning a hard drive
Your *Archlinux* operating system will be composed of a 15-Go primary partition and will use the LVM system to create 4 subpartitions :

- a 15 Go journalized *"root"* subpartition equivalent to "/"
- a 5 Go journalized *"home"* subpartition
- a 400 Mo non-journalized *"boot"* subpartition
- a 500 Mo *"swap"* subpartition

Graphic environment
Your *Archlinux* operating system must use the *Plasma KDE* graphic environment and should have a graphic session manager of your choice.

Locales
Archlinux will be in English, the keyboard in your native language and the localization in your time zone.

Groups and users
You must create a *"turban"* user, who belongs to the *"asso"* main group and to the *"Hogwarts"* secondary group.
You must create a *"dumbledore"* user, who belongs to the *"managers"* main group and to the *"Hogwarts"* secondary group.

OS access
The Parrot OS operating system's *"/home"* partition should be automatically accessible when Archlinux is started - either from the file explorer or the terminal.

The system administrator **forbids** you from using a graphic interface to automatically assemble the Parrot OS partition.
You must modify the corresponding file and be able to explain it.

SSH Server
In order to make connections on your client machine from another machine easier, the system administrator has asked you to install an SSH server in your *"Archlinux"* operating system.
Your SSH server should listen on port 42 and be available **only** via the ssh-key Epitech will provide you.

2. *Parrot OS* operating system

Partitioning a hard drive
Your *Parrot OS* operating system will be composed of 4 partitions :
- 25 Go journalized *"root"* partition equivalent to "/"
- 5 Go journalized *"home"* partition
- 500 Mo non-journalized *"boot"* partition
- 500 Mo *"swap"* partition

Locales
Parrot OS linux will be in English, the keyboard in your native language and the localization will be Brazil.

Groups and users
You must create a *"pierre"* user, who belongs to the *"poche"* main group and to the *"Hogwarts"* secondary group.
You must create a *"dinosaur"* user, who belongs to the *"miaou"* main group and to the *"Hogwarts"* secondary group.
You must create a *"lee"* user, who belongs to the *"wand"* main group and to the *"Hogwarts"* secondary group.
You must create a *"fred&george"* user, who belongs to the *"poche"* main group and to the *"Hogwarts"* secondary group.

Permissions
The *"pierre"* user must be able to launch commands as *"dinosaur"* and vice versa.

SSH server
In order to make connections on your client machine from another machine easier, the system administrator has asked you to install an SSH server on your *Parrot OS linux* operating system.
Your SSH server should listen on port 42 and be available **only** via the ssh-key Epitech will provide you.

Server machine - specifications

Web Server
You must set up a Web server that will contain :
- an nginx server
- a database server
- a PHP module
- a database management application

This virtual machine is supposed to be a server. Do you really need a Desktop environment.

You must create your two intranet sites for the Hogwarts school on your Web server :
- **intra.hogwarts.lan**
  This intranet is designed for Hogwarts students. Therefore, it should be accessible from both of the client machine's OS.
  The welcome page should have the following message appear :
  `"Welcome to the Hogwarts students' intranet"`
- **intra-adm.hogwarts.lan**
  This intranet is designed for Hogwarts employees. Therefore, it should be accessible from both of the client machine's OS.
  The welcome page should have the following message appear :
  `"Welcome to Hogwarts's ADM intranet"`

  SSH Server
  In order to make connections from your machine on another machine easier, the system administrator has asked you to install an SSH in your **Debian server** operating system.
  Your SSH server should listen on port 42 and be available **only** via the ssh-key Epitech will provide you.

Bonus

In order to go a little further in this project, you can complete one or more bonuses from the following list.

> The bonuses will **ONLY** be taken into account if the mandatory requirements are **completely** functional.

As a bonus, you can

- **For clients :**
  - Install and configure the zsh shell (see oh-my-zsh)
  - Change the default prompt to : `"username@hogwarts.lan GIT_BRANCH | (EXIT_CODE)"` so that it updates with the current user, the last command executed's return value and the current branch if the user is in a git repository
  - Make an attack report with a list of : security threat, tools used to discover them, solution provided
- **For the server :**
  - Configure security rules (anti DOS, blacklist, SSL/TLS)

v 3.2