Lab 5: The Root of Chaos

1 Introduction

The Hunt has changed, Hunter. We are no longer tracking beasts; we are stealing secrets.

The Guild has identified a fortified stronghold deep within the File Tree Forest. Rumours suggest that the Lords of this domain (the Root users) are hoarding a valuable artifact known as the **The Sovereign Registry**. In the common tongue, this is the `/etc/passwd` file. It is the heart of the system's identity.

Your mission is strictly **Infilration and Extraction**.

You will be dropped into the target zone (the Virtual Machine) with the guise of a commoner, a low-level user with minimal access. Direct combat is futile; the walls are too thick. Instead, you must rely on **Reconnaissance**.

The architects of this fortress were arrogant. They believed their walls were high enough to ignore the cracks in the foundation. You must find those cracks.

Your path is clear. First, you must **survey the terrain**, using your tools to scan for internal weaknesses and misconfigurations. Next, you must **escalate** your standing by finding the flaw in their automation. Exploit it to climb the hierarchy, for you must obtain **Root** privileges to bypass the final locks. Finally, **extract** the prize: seize the contents of `/etc/passwd` and report back to the Guild.

Get in. Get the access. Get the Flag.

2 Notes

Reading the information given in the assignment description and the assignment itself is highly recommended as it includes information specifically related to your assignment.

It is recommended that you record every command that you try, whether successful or not, including a succinct discussion of why that command was chosen and what the expected outcome was. **Good documentation is the mark of a master Hunter**. Your report must be exhaustive and crystal clear; you must not only list your actions but explain your findings in a way that allows the Guild to reproduce your infiltration step-by-step. If a discovery is not written down, it effectively never happened.

The `MAN` pages are painstakingly crafted documentation for most Unix programs filled to the brim with useful information; as such, they are a very good place for information about the usage of commands.

3 Setup

To begin your infiltration, you must seize the sealed Virtual Machine image from the Guild's drop point: The Corrupted Stronghold. This file is a captured snapshot of the fortified server, frozen in time and awaiting your inspection.

Heed this warning: this environment is a quarantine zone. It contains live vulnerabilities and rot. Do not attempt to mount this image directly on your host soil. You must deploy it within your virtualization software (VirtualBox or VMWare) to ensure the corruption remains contained.

Indeed, the Guild mandates that *all* hunters treat this asset with extreme caution to prevent the "wild inodes" from bleeding into your personal systems.

When you are ready to breach the walls, boot the machine. To bypass the outer gates, you must utilize the intercepted credentials: login with the username `master` and the password `icybSnowBoard2023!?`. In an instant, you will be transported to the edge of the system as a low-level user. The tools of the trade, specifically the **LinPEAS** artifact, have been smuggled inside, ready to be wielded against the architecture. Only once the machine is live does the hunt truly begin.

4 LinPEAS

Linux Privilege Escalation Awesome Script(LinPEAS) is a script that looks for privilege escalation vulnerabilities in Linux environments. The script will perform checks to find vulnerable subsystems and components and report back to you. You can see LinPEAS Basic Information for more information. Use this information for subsequent tasks.

5 Deliverables

The Guild demands a full accounting of your operation. You must submit a report of academic standard that details the weaknesses encountered and the strategies used to infiltrate the stronghold.

5.1 The Bounty (Grading Criteria)

Be warned that the architects of this fortress were incredibly careless. There is **not just one** path to power, but several. The Guild rewards thoroughness.

While capturing the Flag proves your success, you will receive a higher bounty (more points) for identifying and documenting **multiple distinct attack vectors**. Do not stop at the first crack you find; map the entire ruin.

5.2 The Report

Your documentation must explain precisely how the security issues were identified and exploited. Furthermore, you are required to propose a robust fix to remedy **each** vulnerability found. Finally, you must present the ultimate proof of your ascension: the content of the `/etc/passwd` file.