Experiment No. 15

Title: Linux Privilege Escalation (Self-Learning)

Roll No.: 16010420075 **Experiments No.: 15**

Aim: To perform privileged escalation on a Linux platform

\

Resources: virtual box, TryHackMe

Theory

What exactly is "privilege escalation"?

Privilege Escalation is the process of moving from a lower permission account to a higher permission account. It's the use of a vulnerability, design defect, or configuration oversight in an operating system or application to obtain unauthorised access to resources that are normally restricted to users.

What is the significance of this?

When executing a real-world penetration test, gaining a foothold (first access) that grants you direct administrative access is extremely rare. Privilege escalation is important because it allows you to get system administrator access, which allows you to do things like:

- Resetting passwords
- Bypassing access controls to compromise protected data
- Editing software configurations
- Enabling persistence
- Changing the privilege of existing (or new) users
- Execute any administrative command

Enumeration is the first step you have to take once you gain access to any system. You may have accessed the system by exploiting a critical vulnerability that resulted in root-level access or just found a way to send commands using a low privileged account. Penetration testing engagements, unlike CTF machines, don't end once you gain access to a specific system or user privilege level. As you will see, enumeration is as important during the post-compromise phase as it is before.

hostname

The hostname command will return the hostname of the target machine. Although this value can easily be changed or have a relatively meaningless string (e.g. Ubuntu-3487340239), in some cases, it can provide information about the target system's role within the corporate network (e.g. SQL-PROD-01 for a production SQL server).

uname -a

Will print system information giving us additional detail about the kernel used by the system. This will be useful when searching for any potential kernel vulnerabilities that could lead to privilege escalation.

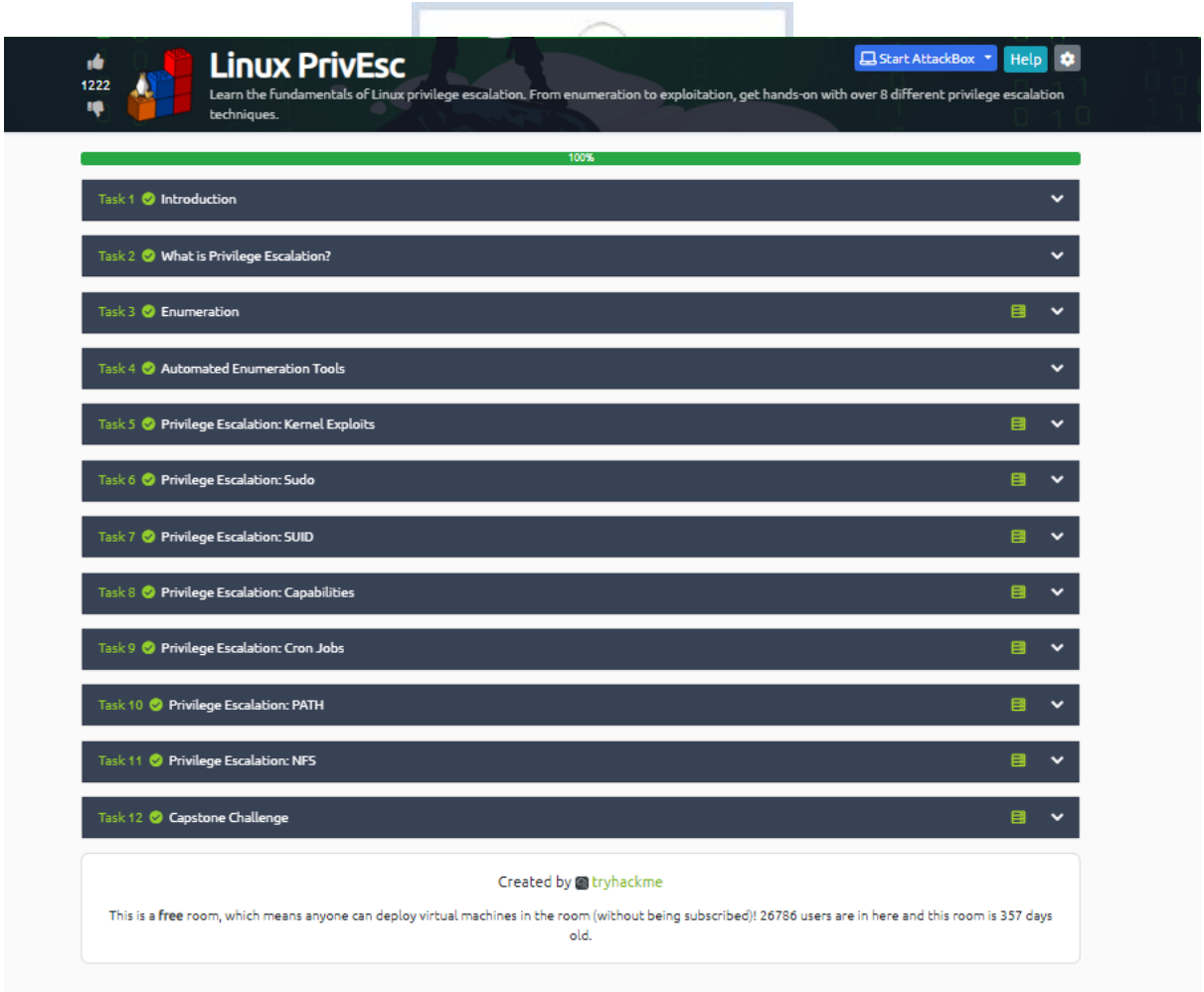
/proc/version

The proc filesystem (procfs) provides information about the target system processes. You will find proc on many different Linux flavours, making it an essential tool to have in your arsenal.
Looking at /proc/version may give you information on the kernel version and additional data such as whether a compiler (e.g. GCC) is installed.

/etc/issue

Systems can also be identified by looking at the /etc/issue file. This file usually contains some information about the operating system but can easily be customized or changes. While on the subject, any file containing system information can be customized or changed. For a clearer understanding of the system, it is always good to look at all of these.

IMPLEMENTATION AND RESULTS:



Outcomes:

CO-3: Understand attack methodology

Conclusion: (Conclusion to be based on the objectives and outcomes achieved)

Escalation of privileges was successfully understood and implemented in Linux.

Grade: AA / AB / BB / BC / CC / CD /DD

Signature of faculty in-charge with date

REFERENCES:

- www.kali.org
- www.tryhackme.com