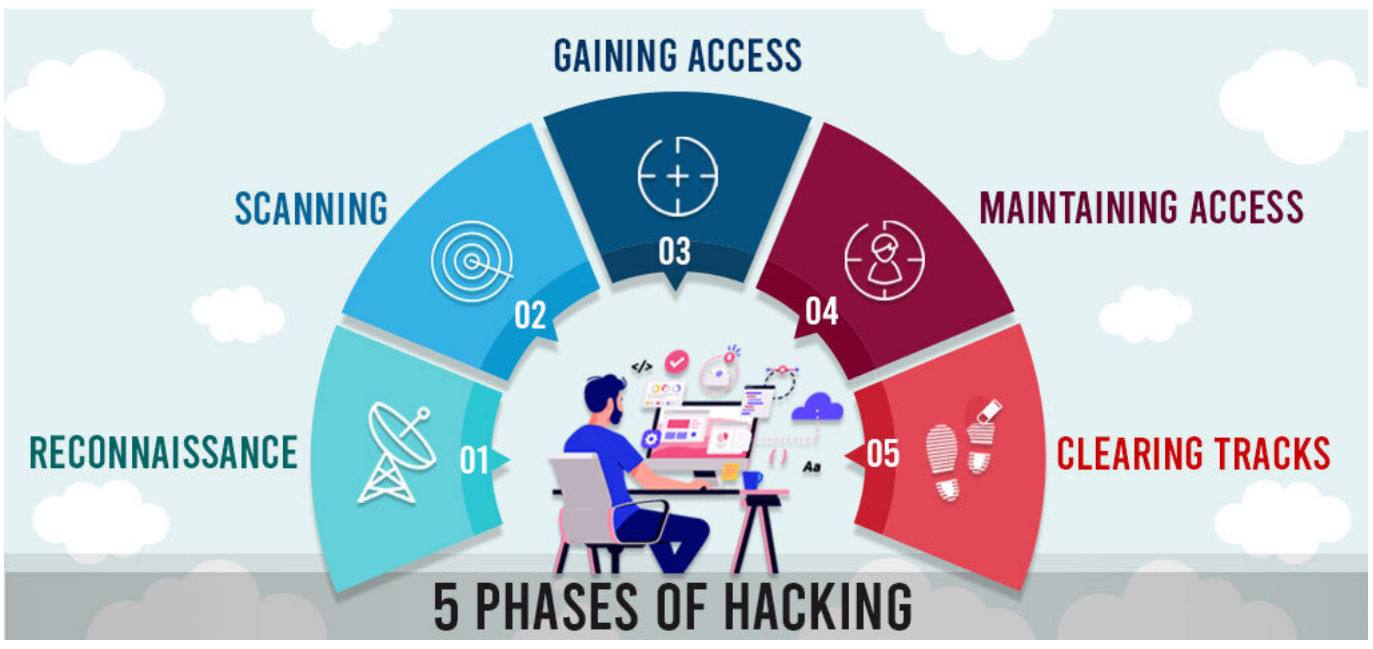
Why this topic?

The Linux Operating System forms the basis of a huge number of the applications that we use every day on the internet. Linux servers are configured for uses as varied as high-performance computing, storage, network routing, and web servers. This flexibility has meant that the management of a Linux server is a complex subject with plenty of room for error. A large number of deployments and configurations has also led to new vulnerabilities being discovered almost every day. To protect a deployment on Linux, a system administrator must ensure that the Linux servers are always up to date with the latest security patches; a single vulnerable service or a minor mistake in configuration could leave the server, and the data residing on it, vulnerable to attack.

As a pentester, it is important to know how to scout for vulnerabilities and the ways they can be exploited.

The Five Phases of Hacking:



Prerequisites

- Basic knowledge of computers and networking

What will you learn?

These Linux Security labs will familiarize you with the basics of **Linux pentesting**. We will go through important Linux concepts and how to use various tools and commands first. Then we will take a look at various phases in the pentesting process one by one.

For the entire section, we will be using a Kali/Ubuntu Attacker machine to attack Linux-based target machines.

References:

- Pentesting with Metasploit
- Pentesting Challenges
- Penetration Testing Execution Standard
- MITRE ATT&CK

While the lab sections can be completed in any order, the recommended order would be:

The objective of the Linux Basics section is to familiarize students with various Linux concepts and commands/tools required to interact with various services and applications.

Reconnaissance

Before attacking any application or service, it is important to gather as much information as possible. The more information an attacker has, the easier it will be to identify any misconfigurations and vulnerabilities. The objective of the reconnaissance section is to familiarize the student with the approach to follow for enumerating web applications and various network services, such as DNS, web servers, databases, caching systems, etc. Using the information, the attack vector and entry points can be identified and then used in the exploitation phase.

Exploitation

The objective of the exploitation phase is to establish access to a system or resource by leveraging a vulnerability or bypassing a security restriction. In this section, the student will learn how to search for exploits based on the information acquired in the reconnaissance phase and use them to compromise the application or service. Once the attacker has compromised a machine, it is possible to attack other machines on the same network which may not be exposed to the internet.

Post-exploitation

A compromised system may contain sensitive information, such as user data, access keys, credentials etc. It may then be possible to use this information to compromise other machines on the same network. The attacker can also turn the machine into a zombie computer and use it to perform attacks on other machines in a planned attack on a future date. The objective of this section is to teach students how to look for sensitive information on a machine, crack password protected files and perform the lateral movement on the network.

Privilege Escalation

On Linux systems, services may be running as a non-root user. For e.g., by default, Apache and Nginx run as the user www-data. Therefore, even if a web application or the service itself is compromised, the attacker will only get access as the www-data user which has limited privileges. To gain full control of a system, it is important to escalate privileges from a user with low privileges to the root user (vertical escalation).
It might not be always possible to escalate from the current user to the root user. In such cases, other users on the machine must be compromised (horizontal escalation), and then used to try to attain root privileges.
The objective of this section is to teach the student the various techniques of privilege escalation in the Linux environment.

Pivoting

In a corporate environment, most of the machines are behind a firewall, which makes it impossible to attack them directly. However, if there is a vulnerable machine exposed to the internet which is also connected to the internal network. It might be possible to pivot through the compromised machine and attack the machines on the internal network. The objective of this section is to teach the various pivoting techniques that can be used to attack machines behind a network.

Maintaining Access

The aim of an attacker is not only to compromise the target machine but also to maintain access to it so that the machine can be used later in a planned attack. Maintaining access to the machine is not a trivial task since the attack vectors might trigger alarms and cause the system administrators to block the vulnerability. This section teaches students the various techniques that can be used to maintain access to a compromised machine.

MITRE ATT&CK

Mitre ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) is a framework developed by Mitre corporation. It consists of threat tactics and techniques based on observations made from real-world attacks. With the Mitre ATT&CK framework, real-world attacks can be broken down into various categories and compared with other attacks. This section familiarizes students with the various techniques from the Mitre ATT&CK Matrix for Linux.

Exploit Research

Based on the information found during the reconnaissance phase or in the post-exploitation phase, a public exploit might not exist for compromising the machine. In such cases, the attacker will have to analyze the files or output and write their own exploit code. In this section, the students will be taught how to debug a process and how to write code to exploit a buffer overflow vulnerability in a program.