Practice Labs - Ethical Hacker v10

Introduction to Ethical Hacking

Introduction

Ethical Hacking
Grey Box
White Box
Black Box
Ethics

Welcome to the **Introduction to Ethical Hacking** Practice Lab. In this module, you will be provided with the information needed to develop your knowledge.

Learning Outcomes

In this module, you will complete the following exercises:

- Exercise 1 - Learn About Ethical Hacking

After completing this lab, you will have further knowledge of:

- Ethical Hacking
- The Need for Ethical Hacking
- The Ethical Hacking Methodology
- The Ethical Aspect of Ethical Hacking
- Types of Threat Actors
- The Difference Between Black Box vs. White Box vs. Grey Box Hacking
- Real-life Attacks

Exam Objectives

The following exam objectives are covered in this lab:

- **5.2** Information Security Assessment Methodologies
- **7.1** Ethics of Information Security

> ***Note:*** *Our main focus is to cover the practical, hands-on aspects of the exam objectives. We recommend referring to course material or a search engine to research theoretical topics in more detail.*

Lab Duration

It will take approximately **30 minutes** to complete this lab.

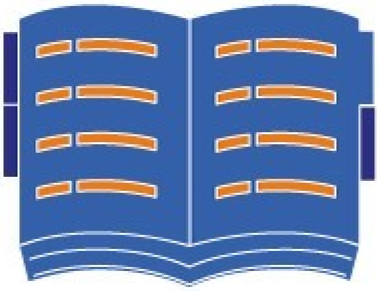
Help and Support

For more information on using Practice Labs, please see our **Help and Support** page. You can also raise a technical support ticket from this page.

> Click **Next** to view the Lab topology used in this module.

Lab Topology

This lab contains supporting materials for Certified Ethical Hacker v10.



> Click **Next** to proceed to the first exercise.

Exercise 1 - Learn About Ethical Hacking

Ethical hacking (also known as penetration testing) is a simulated cyber-attack to exploit the vulnerabilities in a network and the systems. It locates the vulnerabilities, then attempts to exploit them. A person conducting ethical hacking can attempt a breach of applications, protocols, Application Programming Interfaces (APIs), servers, firewalls, and anything else that can be exploited on a network. The core intent is to discover the vulnerabilities before an attacker from the outside, then exploit them to simulate the damage that could be caused.

In this exercise, you will learn about the core fundamentals of ethical hacking.

Learning Outcomes

After completing this exercise, you will have further knowledge of:

- Ethical Hacking
- The Need for Ethical Hacking
- The Ethical Hacking Methodology
- The Ethical Aspect of Ethical Hacking
- Types of Threat Actors
- The Difference Between Black Box vs. White Box vs. Grey Box Hacking
- Real-life Attacks

Task 1 - Ethical Hacking

The fundamental difference between hacking and ethical hacking is permissions. Hacking is when a computer or network is accessed by an unauthorized source, usually for malicious reasons. Ethical hacking is permitted by a person or an organization to explore the possibility of vulnerabilities within a system or a network. The person performing ethical hacking is known as an ethical hacker, who may be contracted or employed by an organization to help them strengthen their security. Ethical hackers work within legal boundaries, ensuring the data they have access to is not exploited or disclosed to any third-parties (unless directed by the organization).

Once discovering the vulnerabilities, the ethical hacker will help the organization with suggestions of how to patch them and therefore prevent attacks. For example, your organization has developed a new Web application for a school. You have been asked to test the Web application and locate vulnerabilities. When you test (hack) the application, you discover that it is prone to SQL Injection attacks. If you had not hacked this application and found the vulnerability to fix, then a hacker could have carried it out, resulting in the data being compromised.

What needs to be protected:

While working, an ethical hacker must preserve the following:

- **Confidentiality**: You must safeguard the information that you have and know. It becomes your responsibility to ensure that the information does not fall into the wrong hands. You can protect the information with appropriate permissions and encryption. If these are not applied, there are chances of disclosure, which allows an unauthorized person to access the information.
- **Integrity**: Keep the information in its original form and do not allow any unauthorized alteration.
- **Availability**: Keep the information available for the authorized individuals to use it. If this is not done, the information can be lost.

Task 2 - The Need for Ethical Hacking

All systems on the internet are considered to be at risk. Attackers are equipped with the latest tools and techniques to attack systems that they find vulnerable. To be able to protect the systems of your organizations, you must know the methods used by the hackers, and the steps that you can take to prevent their attacks.

There are some fundamental answers that you need to know:

- **What to look for** - what are you trying to protect?
- **How to protect** - once you know what needs protecting, how are you going to do that?

It is important to remember that you cannot protect everything. If a vulnerability is unknown, there is no way to protect against it. This is where an ethical hacker comes in. For example, an attacker is able to discover and exploit a zero-day vulnerability in your Web application. This is something that you wouldn’t have thought about, but the attacker was one step ahead of you. An ethical hacker could have discovered this vulnerability beforehand.

As an ethical hacker, you need to:

- Understand and know the systems and processes before starting any activity.
- Know the rules of engagement before starting any activity. You should know what needs to be done.
- Obtain permissions in writing before proceeding with any type of hacking.
- Be able to hack the organization's systems without causing any damage.
- Discover vulnerabilities and help the organization patch them.
- Use the same methods and techniques you think an attacker would use to exploit a system, application, or vulnerability.
- Make sure you do NOT share any discovered vulnerability or information with anyone other than the designated authorities.
- Keep the communication channel open with the respective authorities so that they are aware of the vulnerabilities.
- Present your findings at the end of testing or hacking and share it with the client.

Task 3 - The Ethical Hacking Methodology

Ethical hacking replicates the methodology of an attacker, so there are certain steps that need to be performed. These steps include:

> ***Note**: The steps used by an organization may vary.*

- Reconnaissance and Footprinting - active and passive
- Scanning
- Enumeration
- Hacking / Gaining Access
- Escalation of Privileges
- Maintaining Access
- Covering Tracks
- Backdoor
- Reporting

Reconnaissance and Footprinting

Reconnaissance is gathering information about the target system(s), which is critical in ethical hacking to identify the attack targets. With the amount and type of information the attacker gathers, they can form the strategy for ethical hacking. Footprinting helps to gather information about the size of the organization.

Both of these tasks take place together. For example, when you are gathering information about a network, you get the details of the systems on the network, and at the same time, you get to know the number of systems on there.

There are two types of reconnaissance and footprinting:

Passive

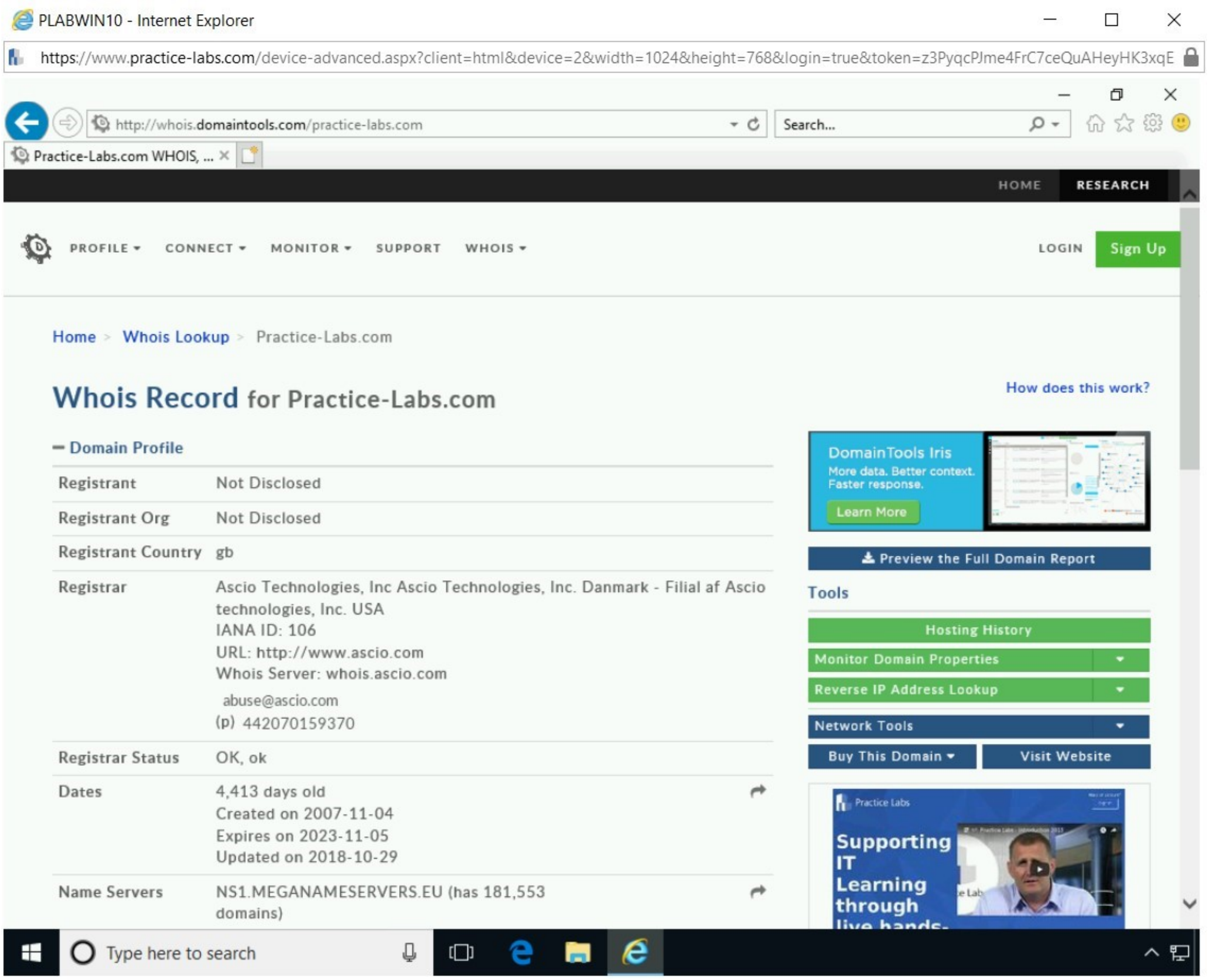
The ethical hacker can use various tools to obtain information without interacting with the system. It is a safer method as you do not expose yourself while collecting the information. The ethical hacker can look for information on various places, such as:

- Whois database
- The target’s website
- Social media profiles of employees
- Google search results
- DNS queries
- Blogs and public forums

The ethical hacker can also use various tools to collect information passively. Some of the key tools are:

- WHOIS
- Social Media
- Shodan
- Google Hacking
- DNS Querying
- The Harvester
- Recon-ng
- Maltego

For example, assume that you want to search for www.practice-labs.com on the whois.domaintools.com website. Notice the output. The result of practice-labs.com is displayed.


PLABWIN10 - Internet Explorer
https://www.practice-labs.com/device-advanced.aspx?client=html&device=2&width=1024&height=768&login=true&token=z3PyqcPJme4FrC7ceQuAHeyHK3xqE
http://whois.domaintools.com/practice-labs.com
Search...
Practice-Labs.com WHOIS, ...
HOME
RESEARCH
PROFILE
CONNECT
MONITOR
SUPPORT
WHOIS
LOGIN
Sign Up
Home > Whois Lookup > Practice-Labs.com
How does this work?
DomainTools Iris
More data. Better context. Faster response.
Learn More
Preview the Full Domain Report
Tools
Hosting History
Monitor Domain Properties
Reverse IP Address Lookup
Network Tools
Buy This Domain
Visit Website
Practice Labs
Supporting IT Learning through live hands-
Type here to search

Whois Record for Practice-Labs.com

– Domain Profile

Registrant	Not Disclosed
Registrant Org	Not Disclosed
Registrant Country	gb
Registrar	Ascio Technologies, Inc Ascio Technologies, Inc. Danmark - Filial af Ascio technologies, Inc. USA IANA ID: 106 URL: http://www.ascio.com Whois Server: whois.ascio.com abuse@ascio.com (p) 442070159370
Registrar Status	OK, ok
Dates	4,413 days old Created on 2007-11-04 Expires on 2023-11-05 Updated on 2018-10-29
Name Servers	NS1.MEGANAMESERVERS.EU (has 181,553 domains)

Figure 1.1: Screenshot of Internet Explorer: Showing information about the searched Website.

Active

In the active reconnaissance method, the ethical hacker connects with the system and collects information. Even though this method provides more accurate information compared to the passive method, the risk of getting noticed and exposed is much higher. One example of active reconnaissance is performing a port scan on a system. In a port scan, the ethical hacker is connecting with the system to obtain the open port information.

There are various tools that can be used in active reconnaissance. Nmap is one of the most sought-after tools for this. Let’s assume, you as the ethical hacker want to scan the 192.168.0.0/24 network and see how many hosts are up using a ping scan. You can use the following command:

Please login to the PLABKALI device using these credentials:

Username:

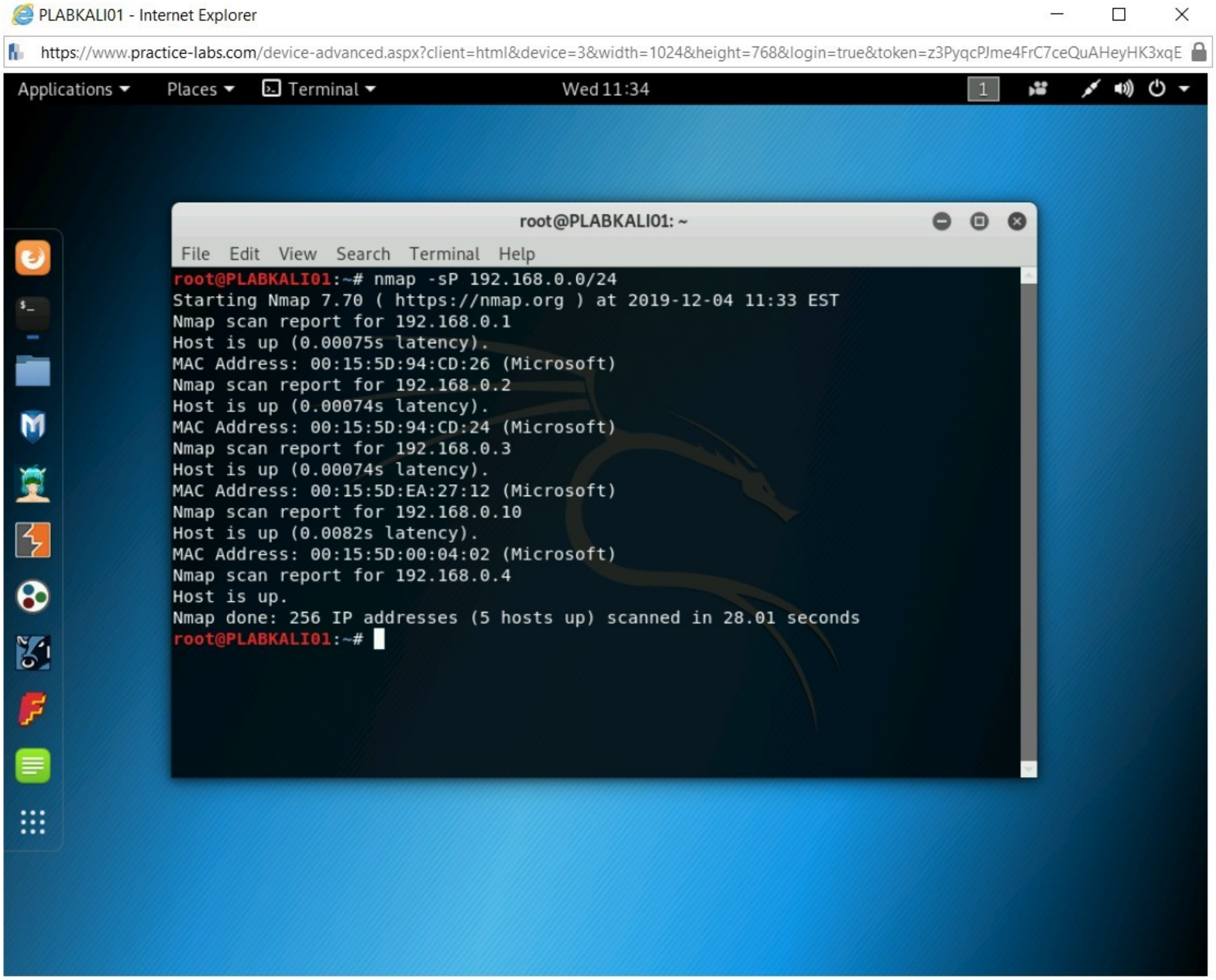
root

Password:

Passw0rd

```
nmap -sP 192.168.0.0/24
```

> ***Note****: the -sP parameter is used for ping scanning. When you use CIDR /24, Nmap will scan all 256 IP addresses on the network.*



PLABKALI01 - Internet Explorer
https://www.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=z3PyqcPJme4FrC7ceQuAHeyHK3xqE
Applications
Places
Terminal
Wed 11:34
1
root@PLABKALI01: ~
File
Edit
View
Search
Terminal
Help

```
root@PLABKALI01:~# nmap -sP 192.168.0.0/24
Starting Nmap 7.70 ( https://nmap.org ) at 2019-12-04 11:33 EST
Nmap scan report for 192.168.0.1
Host is up (0.00075s latency).
MAC Address: 00:15:5D:94:CD:26 (Microsoft)
Nmap scan report for 192.168.0.2
Host is up (0.00074s latency).
MAC Address: 00:15:5D:94:CD:24 (Microsoft)
Nmap scan report for 192.168.0.3
Host is up (0.00074s latency).
MAC Address: 00:15:5D:EA:27:12 (Microsoft)
Nmap scan report for 192.168.0.10
Host is up (0.0082s latency).
MAC Address: 00:15:5D:00:04:02 (Microsoft)
Nmap scan report for 192.168.0.4
Host is up.
Nmap done: 256 IP addresses (5 hosts up) scanned in 28.01 seconds
root@PLABKALI01:~#
```

Figure 1.2 Screenshot of Kali Linux: Showing the output of the nmap -sP command.

The nmap command shown above pings 256 hosts on the network and returns with a list of the hosts that are live at that time.

Scanning and Enumeration

After you have explored the network and identified the live systems on it, you can move on to scanning and enumeration. This is critical for exploitation or gaining access.

Enumeration is also considered part of active reconnaissance. Using enumeration, you can find a lot of details about a device, server, or service.

Enumeration can be used to find information, such as:

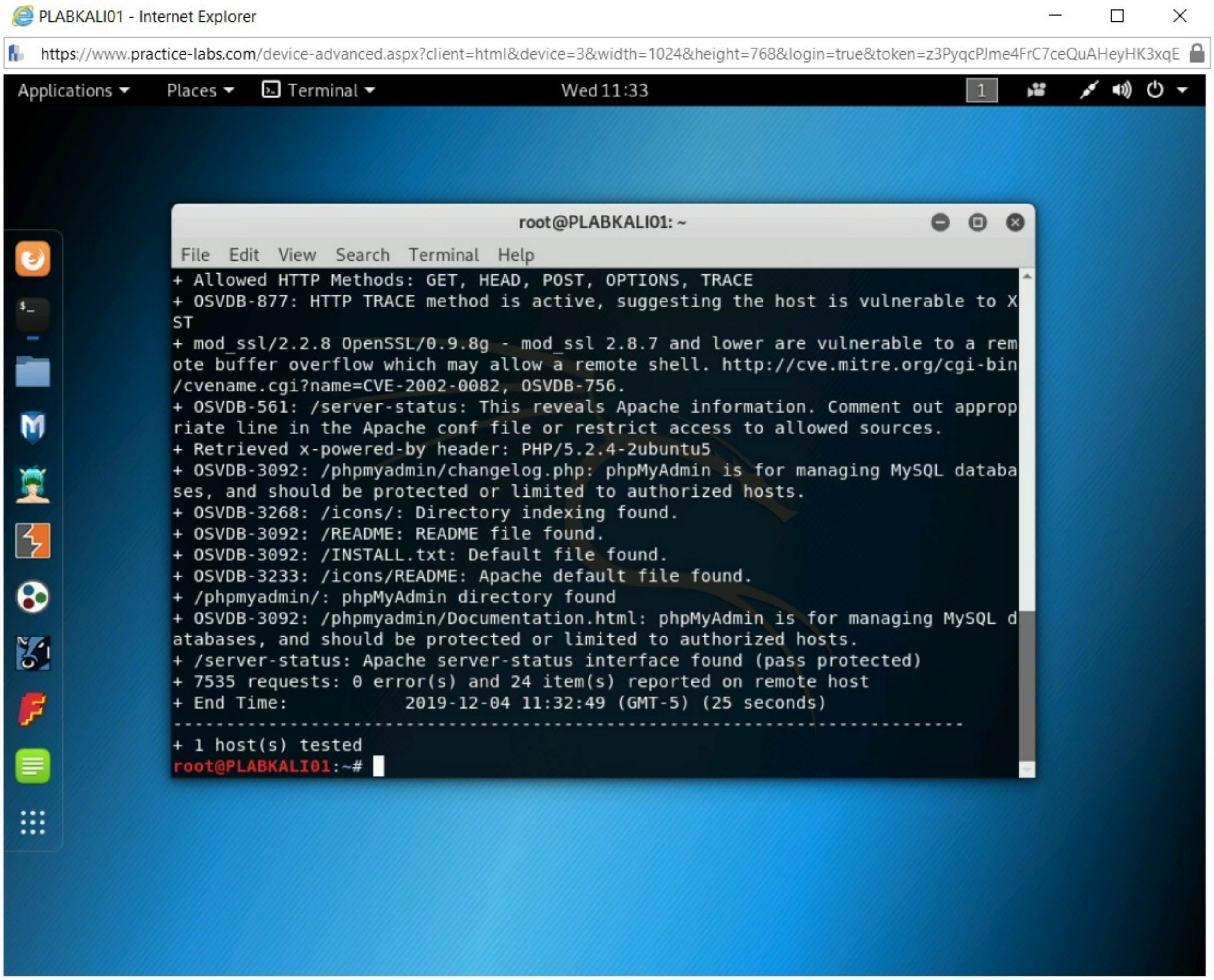
- Operating system information, such as the version
- DNS information
- SNMP information
- Users and groups
- Password hashes and passwords
- Hostnames
- Domain information
- Running services and process

Scanning finds vulnerabilities that can be exploited. For example, you can use Nikto to scan a Web application and find vulnerabilities. Let's look at the example in which you execute the following command:

```
nikto -host http://192.168.0.10
```

Note*: You can host a vulnerable Web application and assign it an IP address. Then, you can use the above command, replacing the IP address with the Web application's IP address.*

The results show the various vulnerabilities discovered.


PLABKALI01 - Internet Explorer
https://www.practice-labs.com/device-advanced.aspx?client=html&device=3&width=1024&height=768&login=true&token=z3PyqcPJme4FrC7ceQuAHeyHK3xqE
Applications
Places
Terminal
Wed 11:33
1
root@PLABKALI01: ~
File Edit View Search Terminal Help

```
+ Allowed HTTP Methods: GET, HEAD, POST, OPTIONS, TRACE
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to X
ST
+ mod_ssl/2.2.8 OpenSSL/0.9.8g - mod_ssl 2.8.7 and lower are vulnerable to a rem
ote buffer overflow which may allow a remote shell. http://cve.mitre.org/cgi-bin
/cvename.cgi?name=CVE-2002-0082, OSVDB-756.
+ OSVDB-561: /server-status: This reveals Apache information. Comment out approp
riate line in the Apache conf file or restrict access to allowed sources.
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5
+ OSVDB-3092: /phpmyadmin/changelog.php: phpMyAdmin is for managing MySQL databa
ses, and should be protected or limited to authorized hosts.
+ OSVDB-3268: /icons/: Directory indexing found.
+ OSVDB-3092: /README: README file found.
+ OSVDB-3092: /INSTALL.txt: Default file found.
+ OSVDB-3233: /icons/README: Apache default file found.
+ /phpmyadmin/: phpMyAdmin directory found
+ OSVDB-3092: /phpmyadmin/Documentation.html: phpMyAdmin is for managing MySQL d
atabases, and should be protected or limited to authorized hosts.
+ /server-status: Apache server-status interface found (pass protected)
+ 7535 requests: 0 error(s) and 24 item(s) reported on remote host
+ End Time:           2019-12-04 11:32:49 (GMT-5) (25 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
root@PLABKALI01:~#
```

Figure 1.3 Screenshot of PLABKALI01: Showing the output of the nikto command.

Gaining Access (Exploitation)

When choosing an attack to use to gain access to the system, the environment and situation have to be considered. Some common attack techniques used in penetration testing are:

- **Social engineering** - This attack sets the base for all other attacks. An attacker can use different methods, such as phishing, to trigger the attack.
- **Web application attacks** - These can include attacks such as SQL injection, XSS, and XSRF. These are applicable if you are performing a penetration test on a Web application.
- **Session hijacking** - This is useful when you have unencrypted sessions. An attacker can perform session hijacking or a man-in-the-middle attack.

- **Password cracking** - This involves some level of access to the server or system, then using various tools to crack the passwords.

A private network is more secure than the public network, which is visible to everyone. When breaking into a private network, the attacker must find various methods to connect. For example, the attacker may use social engineering and deploy malware by sharing an infected USB drive with a user.

If you use a technical method, such as a Web application attack, you need to locate a Webserver first and see if it has a Web application running. You could then exploit the Web application.

In other cases, you may use a social engineering method, such as sending an e-mail to a user, pretending to be from their bank. The e-mail may have a URL the user is instructed to click on. Once they access the URL, the users are navigated to a Website that looks like it is the bank's Website. It could then deploy malware onto their system.

Maintaining Access

Let's assume that you have exploited a vulnerability in the Windows operating system and gained access to the system. There is no guarantee that you will be able to maintain access. In such situations, you need to do something that allows you to maintain access if the vulnerability is patched.

For example, you can create a new user account with administrative access. This will allow you to connect with the exploited system remotely. Alternatively, you install a backdoor or rootkit.

Covering Tracks

In any form of hacking, you are likely to leave traces in the system, possibly resulting in getting stopped or caught. For example, if you create a user account, it will get captured in the log files. One of the key methods used in covering tracks is to clear the log files. However, when logs are cleared, a new entry in the log files is created, mentioning that logs have been deleted.

Reporting

You must report your findings to the organization or person that has requested the ethical hacking test. The report includes vulnerabilities, sensitive data exposure, your access to the sensitive systems, and how to mitigate the threats you were able to pose.

Task 4 - The Ethical Aspect of Ethical Hacking

An ethical hacker must follow professional principles and the code of ethics.

For example, you must not use the organization’s information and data for personal needs or misuse them with malicious intentions. Also, the information must be protected from falling into the wrong hands as a result of the testing. Any misuse of their data or information could result in legal action.

Another critical aspect of ethical hacking is permissions. For example, you must have permission to hack a Webserver that runs a Web application. If you do not have permission, then it is considered as hacking, not ethical hacking.

> ***Note****: The Code of Ethics are available here:*
> ***https://www.eccouncil.org/code-of-ethics/***

If you have the CEH certification and do not adhere to ethics defined by EC-Council, you can lose your certification.

Task 5 - Types of Threat Actors

As an ethical hacker, you must know about different types of threat actors, who are any entity behind a threat, which is a potential danger to an asset. A threat actor can be largely categorized into three categories:

- **Internal Threat** (eg: a rogue employee)
- **External Threat** (eg: a criminal group)
- **Natural Threat** (eg: hurricane or tsunami)

Threat actors look for vulnerabilities to exploit. When a vulnerability or weakness is present in the network, server, or application, it is at risk from the threat actor.

Examples of threat actors

Hackers

There are three types of hacker: black hat, grey hat, and white hat.

Black hat hackers hack the systems with malicious intent. They are also known as crackers.

White hat hackers are ethical hackers or sneakers. They are usually either hired or contracted by organizations to evaluate their security parameters.

Grey hat hackers are a combination of white hat and black hat hackers. They break into systems without seeking permission. Their intentions are not malicious; they want to demonstrate their skills. Their actions are still considered to be illegal, as they do not seek permission to perform their actions.

Script Kiddies

A script kiddie is someone who does not have the expertise of a hacker and relies on ready-made tools as they can't write their own code. Due to a lack of expertise, their attacks are not sophisticated.

Hacktivists

Hacktivists are threat actors who are hackers with a specific mission, which could be political or social. One of the most common attacks they use is a Distributed Denial of Service (DDoS). They are determined to fulfill their cause and can work in groups with like-minded hackers.

Nation-States/State Sponsored

These threat actors are well-funded and well-organized entities that commit their activities with the backing of governments, or similar. State-sponsored attackers typically focus on infiltrating larger organizations with the intent to steal large amounts of mission-critical and sensitive data.

Insider Threats

These threat actors are internal to an organization and can carry out malicious activity intentionally or unintentionally. Some of the activities they could perform include handing out confidential or sensitive information to others unintentionally, or selling information to another threat actor who wants to misuse it.

It is very difficult to detect an insider threat as the person is part of the system. They would have access to the data, along with the knowledge of internal operations and processes. Since they are inside the network, their actions are difficult to track by tools such as firewalls.

Task 6 - The Difference Between Black Box vs. White Box vs. Grey Box Hacking

As an ethical hacker, you may be asked to perform different types of hacking or penetration testing. The organization, after deciding the scope of the task, may also ask you to perform a certain type of hacking or penetration testing, which generally categorized into three types:

- Black box
- Grey box
- White box

Black Box

A black box test is also known as Zero-Knowledge penetration testing. In the black box test, you do not have any information about the network, except for an IP range. You are typically an external entity that needs to exploit the network or systems at the fullest. The organization expects you to gather information on your own, discover vulnerabilities, then exploit them. A black box test takes more time as you do not know anything about the network or its systems. However, it is more effective because you can provide an accurate assessment of the security of the network, and it closely simulates a real-life attack that could occur.

White Box

White box penetration testing is completely opposite to black box testing. It is also known as Full Knowledge Penetration Testing. You have all the information that is required to perform penetration testing. For example, the organization would share the following information:

- Network diagrams
- List of systems with their IP address
- IP ranges
- User credentials to log on to the systems

White box penetration testing takes less time than black box testing because you have the required information available. However, it may not provide accurate results as it is not the same situation an external attacker would be in.

Grey Box

Grey box testing is a combination of black box and white box. You have the limited information to begin with, but do not have user credentials or the configuration details. For example, the organization may share the application name and its IP address but does not provide the application version or the services that it is running. This makes it slightly more accurate than a white box test.

Task 7 - Real-life Attacks

As an ethical hacker, it is useful to understand the minds of hackers. One of the best methods to do this is to study major attacks that have occurred in the past. Some of these major attacks include:

Adobe

In October 2013, Adobe revealed that it had been attacked. Here is a brief summary of the attack:

- Removal of personal information of 2.9 million customers by the attackers - login credentials, names, credit card information including expiration dates
- Customer IDs and encrypted passwords were accessed
- Source code was stolen for ColdFusion, Acrobat Reader, and Photoshop

Sony

Sony had been under major attacks twice.

The first incident occurred in April 2011, which led to the closing of Sony PlayStation, Sony Online Entertainment, and Qriocity for one month.

Here is a brief summary:

- Personal information of 77 million user accounts was leaked
- Thousands of users' bank accounts were compromised

The vulnerability exploited was unencrypted data on the Sony network, which was hijacked using SQL Injection attacks.

November 2014

In the second major attack, Sony Pictures Entertainment was targeted.

Here is a brief summary:

- Attack was conducted using a worm
- Attack was conducted by a hacker group named Guardians of Peace, who ended up stealing more than 100 terabytes of data from Sony
- The vulnerabilities exploited were poor infrastructure management and incorrect configuration

Here are some other big organizations that have been hacked in recent years:

- Facebook
- Google+
- Cambridge Analytica
- MyHeritage
- Quora
- Timehop
- Cathay Pacific Airways
- T-mobile
- British Airways
- Yahoo
- Marriott International
- eBay
- Uber

In the past, the Federal Bureau of Investigation (FBI) has used ex-hackers to track down some of the smartest hackers in the world.

Review

Well done, you have completed the **Introduction to Ethical Hacking** Practice Lab.

Summary

You completed the following exercises:

- Exercise 1 - Learn About Ethical Hacking

You should now have further knowledge of:

- Ethical Hacking
- The Need for Ethical Hacking
- The Ethical Hacking Methodology
- The Ethical Aspect of Ethical Hacking
- Types of Threat Actors
- The Difference Between Black Box vs. White Box vs. Grey Box Hacking
- Real-life Attacks

Feedback