Week 1: Reconnaissance, Information Gathering, and Scanning

INT302: Kali Linux Tools and System Security – Lab 1: Reconnaissance (Information Gathering)

Lab Overview

This lab will guide you through essential reconnaissance techniques to gather preliminary information about a target system or domain during penetration testing. You'll learn to identify IP addresses, retrieve domain registration details, and perform DNS lookups using popular Linux tools such as ping, whois, and nslookup. This hands-on experience will help you gather data that is crucial for vulnerability assessment and further penetration testing.

Lab Objectives

By the end of this lab, you will:

1. Use the ping command to determine the IP address of a domain.
2. Retrieve domain registration details using the whois command.
3. Perform DNS lookups using nslookup to gather information about a domain's DNS records.

Tools Used

- **Kali Linux**: A Linux distribution used for penetration testing.
- **Terminal**: The command-line interface in Kali Linux to run Linux commands.

Prerequisites

- Basic familiarity with Kali Linux and its command-line interface.
- Internet access to run domain lookups.
- An installed and working Kali Linux environment.

Lab Steps

Step 1: Get the IP Address of a Domain Using ping

The ping command helps you verify the reachability of a domain and returns its IP address.

Instructions:

1. Open your **Terminal** in Kali Linux.
2. Run the ping command followed by the domain name you want to investigate.

Command Syntax:

ping <domain>

Example:

ping google.com

Expected Output:
The terminal should return the IP address of the domain along with statistics about packet transmission. For example, google.com might return an IP like 142.250.186.206.

Exercise 1:

Use the ping command to find the IP addresses of the following domains:

- facebook.com
- twitter.com
- amazon.com

Record Your Answers:

1. facebook.com: _____
2. twitter.com: _____
3. amazon.com: _____

Step 2: Retrieve Domain Registration Details Using whois

The whois command fetches domain registration details such as registrar, creation date, and expiration date.

Instructions:

1. In the terminal, use the whois command followed by the domain name.

Command Syntax:

whois <domain>

Example:

whois facebook.com

Expected Output:
You'll see details like:

- Registrar information (e.g., MarkMonitor Inc.)
- Domain creation and expiration dates
- Registrant information (if available)

Exercise 2:

Run the whois command for the following domains:

- github.com
- linkedin.com
- apple.com

Answer These Questions:

1. What is the registration expiration date for github.com? _____
2. Who is the registrar for linkedin.com? _____
3. What country is the registrant of apple.com from? _____

Step 3: Perform a DNS Lookup Using nslookup

The nslookup command queries DNS servers to retrieve DNS records and IP addresses.

Instructions:

1. Run the nslookup command followed by the domain name.

Command Syntax:

nslookup <domain>

Example:

nslookup microsoft.com

Expected Output:
You will see details like:

- The IP address(es) of the domain
- Name servers (NS)
- DNS record information

Exercise 3:

Use nslookup to look up DNS information for the following domains:

- bbc.co.uk

- netflix.com

Answer These Questions:

1. What is the IP address for bbc.co.uk? _____
2. What are the name servers (NS) for netflix.com? _____

Submission Instructions

Submit your results for the exercises above, including:

- IP addresses retrieved using ping
- Domain registration details from whois
- DNS information from nslookup

Conclusion

In this lab, you learned the fundamentals of information gathering using basic Linux networking commands. These reconnaissance techniques are essential in any penetration testing engagement, providing crucial details before moving on to more advanced stages of security analysis.

INT302: Kali Linux Tools and System Security – Lab 2: Website Enumeration and Information Gathering

Lab Overview

This lab focuses on website enumeration and information gathering techniques that are essential in the reconnaissance phase of penetration testing. You will learn to detect web technologies used by a target website and perform aggressive scanning to gather detailed information. We will utilize the whatweb tool, a powerful utility designed for identifying web technologies.

Lab Objectives

By the end of this lab, you will:

1. Detect web technologies used by a website or server using the whatweb command.
2. Perform aggressive scanning on a target IP address or URL to extract detailed information about its web technologies.

Tools Used

- **Kali Linux**: A Linux distribution tailored for penetration testing.
- **Terminal**: The command-line interface to execute commands.

Prerequisites

- Basic knowledge of Kali Linux and command-line operations.
- Internet access to perform scans on live web servers.
- whatweb installed in your Kali Linux environment (it usually comes pre-installed).

Lab Steps

Step 1: Detect Web Technologies Using whatweb

The whatweb command allows you to identify the technologies used by a web application, including the server type, programming languages, and content management systems.

Instructions:

1. Open your **Terminal** in Kali Linux.
2. Use the whatweb command followed by the target IP address or URL.

Command Syntax:

whatweb <IP address or URL>

Example:

whatweb 192.168.1.1

Expected Output:
The output will display various technologies detected on the specified web server, including web server software, programming languages, frameworks, and more.

Exercise 1:

Run the whatweb command to detect technologies for the following targets:

- example.com
- stackoverflow.com
- github.com

Record Your Findings:

1. **example.com**: _____

2. **stackoverflow.com**: _____
3. **github.com**: _____

Step 2: Perform Aggressive Scanning Using whatweb

The --aggression option allows for more thorough scanning by enabling additional checks, which can reveal more information about the target.

Instructions:

1. In the terminal, run the whatweb command with the --aggression option.

Command Syntax:

whatweb --aggression 3 -v <IP address or URL>

Example:

whatweb --aggression 3 -v example.com

Expected Output:
The command will provide a verbose output with more detailed information about the technologies detected on the web application.

Exercise 2:

Perform an aggressive scan on the following targets:

- google.com
- facebook.com

Record Your Findings:

1. **google.com**: _____
2. **facebook.com**: _____

Submission Instructions

Submit your results from both exercises, including:

- Detected web technologies from the whatweb command.
- Detailed findings from the aggressive scans.

Conclusion

In this lab, you explored important techniques for website enumeration and information gathering using the whatweb tool. Understanding the technologies and software running on target systems is crucial for developing effective penetration testing strategies.

INT302: Kali Linux Tools and System Security – Lab 3: Subdomain Hunting

Lab Overview

In this lab, you will learn how to identify subdomains associated with a target domain using various tools. Subdomain hunting is a crucial part of reconnaissance in penetration testing, as it helps identify additional attack surfaces that may not be immediately visible. We will utilize sublist3r for subdomain enumeration, dirb for directory discovery, and theHarvester for gathering information from public sources.

Lab Objectives

By the end of this lab, you will:

1. Perform subdomain enumeration using sublist3r.
2. Discover hidden directories on a target web server using dirb.
3. Utilize theHarvester to gather additional information about the target domain.

Tools Used

- **Kali Linux**: A Linux distribution tailored for penetration testing.
- **sublist3r**: A tool designed for subdomain enumeration.
- **dirb**: A web content scanner for discovering hidden directories.
- **theHarvester**: A tool for gathering emails and subdomains from public sources.

Prerequisites

- Basic knowledge of Kali Linux and command-line operations.
- Internet access to perform scans on live web servers.
- Tools sublist3r, dirb, and theHarvester installed in your Kali Linux environment (they usually come pre-installed).

Lab Steps

Step 1: Subdomain Enumeration Using sublist3r

sublist3r is an effective tool for finding subdomains of a target domain.

Instructions:

1. Open your **Terminal** in Kali Linux.
2. Use the sublist3r command followed by the target domain.

Command Syntax:

sublist3r -d <target domain>

Example:

sublist3r -d example.com

Expected Output:
The output will display a list of subdomains associated with the specified domain.

Exercise 1:

Run the sublist3r command for the following domains:

- github.com
- google.com

Record Your Findings:

1. **Subdomains for github.com**:
    - _____
2. **Subdomains for google.com**:
    - _____

Step 2: Directory Discovery Using dirb

dirb is a powerful tool for discovering hidden directories and files on web servers.

Instructions:

1. In the terminal, run the dirb command followed by the target URL.

Command Syntax:

dirb <target URL>

Example:

dirb https://example.com

Expected Output:
The command will return a list of directories and files found on the web server.

Exercise 2:

Perform a directory discovery scan on the following targets:

- http://example.com
- http://example.org

Record Your Findings:

1. **Directories for example.com**:
    - _____
2. **Directories for example.org**:
    - _____

Step 3: Information Gathering Using theHarvester

theHarvester is a tool for gathering emails, subdomains, and other relevant information from search engines.

Instructions:

1. In the terminal, run the theHarvester command followed by the target domain.

Command Syntax:

theharvester -d <target domain> -b google

Example:

theharvester -d example.com -b google

Expected Output:
The output will show collected emails and other information about the specified domain.

Exercise 3:

Use theHarvester to gather information on the following domain:

- example.com

Record Your Findings:

- **Emails and Information Gathered**:

-

Submission Instructions

Submit your results from all exercises, including:

- Detected subdomains from sublist3r.
- Discovered directories from dirb.
- Information gathered using theHarvester.

Conclusion

In this lab, you explored techniques for subdomain hunting and directory discovery using various tools. This knowledge is essential for identifying potential vulnerabilities and attack vectors in a target's infrastructure.