masterskill
education through innovation

aci LEARNING | SKILL LABS

Ethical Hacking and Systems Defense, Skill Labs

Course Specifications

Course Number: ACI76-049SL_rev1.0
Lab Length: Approximately 15 hours

Performing Reconnaissance from the WAN

Introduction
Objective

CEH Exam Domain:

Domain 2: Analysis/Assessments
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:

Objective 2.2 Information Security Assessment Process
Objective 4.3 Information Security Tools

Overview

In this lab, you will be performing reconnaissance from an external IP address from the WAN (wide area network) within this topology, You will also use tools to capture user credentials, and with those captured credentials, log into and compromise the system.

Outcomes:

In this lab, you will learn to:

1. Use nmap to perform banner grabbing.
2. Use nmap to determine the operating system and applications running on a system.
3. Use tools to capture credentials on a system.
4. Use remote desktop to log in to a system from captured credentials.

1	Key Term	Description
1	TELNET	A protocol where the data is transmitted between two machines over in clear text. The use of TELNET, which uses port 23, should be avoided on networks because it is not secure.
2	Kali	A Linux distribution used for penetration testing or for hacking.
3	Zenmap	A GUI front end for nmap; will allow you to scan for open ports and services.
4	Metasploit	A framework that contains exploits for various information systems.

1	Key Term	Description
5	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.

Scanning the Network on the LAN

Introduction
Objective

CEH Exam Domain:
Domain 2: Analysis/Assessment
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:
Objective 2.2 Information Security Assessment Process
Objective 4.3 Information Security Tools

Overview

In this lab, you will be scanning for hosts on a Local Area Network (LAN). Figure 1 shows the lab topology for this lab. You are using a distribution of Linux called Kali, which is primarily used for penetration testing. You will scan the network with Kali. You will use Metasploit and Armitage to exploit a machine with vulnerabilities.

Outcomes:

In this lab, you will learn to:

1. Use nmap to do a ping scan.
2. Use Metasploit and Armitage to exploit vulnerabilities and breach a system.

	Key Term	Description
1	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.
2	port	In computer networking, a port is an endpoint of communication in an operating system associated with an IP address of a host and the protocol type of the communication.
3	Zenmap	A GUI front end for nmap; will allow you to scan for open ports and services.
4	TCP	Transmission Control Protocol is a network protocol designed to send and ensure end-to-end delivery of data packets over the Internet.
5	Metasploit	A framework that contains exploits for various information systems.

Enumerating Hosts Using Wireshark, Windows, and Linux Commands

Introduction
Objective

CEH Exam Domain:
Domain 2: Analysis/Assessments
Domain 4: Information Security Tools

CEH Objective Mapping:
Objective 2.2 Information Security and Communication Technologies
Objective 4.3 Information Security Tools

Overview

In this lab, you will learn to enumerate or list various resources on a target host.

Outcomes:

In this lab, you will learn to :

1. Use Armitage to scan a network.
2. Use system commands to enumerate or list resources on a target system.

	Key Term	Description
1	ifconfig	Interface Configuration is a system/network utility in the Linux operating systems to configure, manage, and query network interface parameters.
2	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.
3	Kali Linux	An Advanced Penetration Testing Linux distribution designed for digital forensics and penetration testing, ethical hacking, and network security assessments.
4	Wireshark	A free and open-source protocol analyzer which will allow a user to capture network traffic or to analyze a capture file.
5	PostgreSQL	Is an open-source object-relational database management system. As a database server, its primary function is to store data securely.

Remote and Local Exploitation

Introduction
Objective

CompTIA Security+ Domain
Domain 1: Attacks, Threats, and Vulnerabilities

Domain 2: Tools and Technologies
Domain 5: Risk Management

CompTIA Security Objective Mapping

Objective 1.4 Penetration Testing Concepts
Objective 2.2 Security Assessment Tools
Objective 5.4 Incident Response Procedures

CEH Exam Domain

Domain 1: Background
Domain 2: Analysis/Assessments
Domain 4: Tools/Systems/Programs

CEH Objective Mapping

Objective 1.2 Information Security Threats and Attack Vectors
Objective 1.3 Information Security Technologies
Objective 2.2 Information Security Assessment Process
Objective 4.3 Information Security Tools

Overview

In this lab, you will exploit a vulnerable Postgres service on a Linux server, the Metasploit framework on Kali Linux. After getting in as the attacker, you will also leverage the Metasploit framework to do a privileged execution.

Outcomes:

In this lab, you will learn to:

1. Use nmap and OpenVas to scan a system.
2. Use Greenbone to determine vulnerabilities of a system.
3. Use Metasploit to exploit a system.
4. Use Meterpreter to breach a system.

	Key Term	Description
1	nmap	Nmap is used to discover hosts and services on a network.
2	Metasploit Project	The Metasploit Project is a computer security project that provides information about security vulnerabilities and aids in penetration testing and IDS signature development.
3	Meterpreter	Meterpreter is a Metasploit attack payload that provides an interactive shell from which an attacker can explore the target machine and execute code.
4	Greenbone	The Greenbone Security Assistant is a web application that connects to the OpenVAS Manager to provide for a full-featured user interface for vulnerability management.

Crafting and Deploying Malware Using a Remote Access Trojan (RAT)

Introduction
Objective

CompTIA Security+ Domain:
Domain 1: Attacks, Threats, and Vulnerabilities
Domain 2: Technologies and Tools

CompTIA Security+ Objective Mapping:
Objective 1.3 Explain threat attack types and attributes.
Objective 1.4 Explain penetration testing concepts.
Objective 2.2 Given a scenario, use appropriate software tools to assess the security posture of an organization.

CEH Domain:
Domain 1: Background
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:
Objective 1.2 Information Security Threats and Attack Vectors
Objective 4.3 Information Security Tools

Overview

In this lab, you will breach and compromise a host on the network. First, you will use the scanning tool nmap/Zenmap in order to determine the open ports on the pfSense firewall from an external address. Then, the lab uses Bruter, a GUI-based network brute-forcing tool for Windows systems to determine the password for the administrator using a dictionary attack. After Bruter determines the password of the administrator account, the attacker can leverage the credentials through an RDP session.

Outcomes:

In this lab, you will learn to:

1. Use nmap/Zenmap to scan a network.
2. Deploy malware on a system.
3. Use Bruter to exploit a system vulnerability.
4. Use remote desktop to breach a system.

1	Key Term	Description
1	netstat	A command line tool in Windows and terminal tool in Linux that will provide you with connection information.
2	RDP	The Remote Desktop Protocol, which allows you to a remote computer though a GUI.
3	Bruter	A program which will allow you to perform a dictionary or brute force attack

1	Key Term	Description
		against a remote system.
4	DarkComet	Malware that will allow an attacker to command and control a victim's system.
5	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.

Capturing and Analyzing Network Traffic Using a Sniffer

Introduction
Objective

CEH Exam Domain:
Domain 2: Analysis/Assessments
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:
Objective 2.1 Information Security Assessment and Analysis
Objective 4.3 Information Security Tools

Overview

In this lab, you will capture and analyze traffic using a sniffer. The sniffer used in this lab is Wireshark. A sniffer is a passive scanner that just listens and records traffic on a network. On a network with a hub, all traffic is sent to all machines. In order to see all of the traffic sent to all machines, a SPAN port will need to be configured.

Outcomes:

In this lab, you will learn to:

1. Configure the network interface to allow a sniffer to capture packets.
2. Generate and capture traffic on the network.
3. Analyze captured traffic in Wireshark.

1	Key Term	Description
1	root	User name or account which has access to all commands along with read and write privileges to all files on a Linux or other Unix-like operating system.
2	TELNET	A protocol where the data is transmitted between two machines over clear text. The use of TELNET, which uses port 23, should be avoided on networks because it is not secure.
3	Wireshark	A free and open-source protocol analyzer which will allow a user to capture network traffic or to analyze a capture file.

1	Key Term	Description
4	POP	Post Office Protocol is an application layer Internet protocol used by local e-mail clients to retrieve e-mail from a remote server over a TCP/IP connection.
5	TCP	Transmission Control Protocol is a network protocol designed to send and ensure end-to-end delivery of data packets over the Internet.

Social Engineering Using SET

Introduction
Objective

CompTIA Security+ Domain:
Domain 3: Threats and Vulnerabilities

CompTIA Security+ Objective Mapping:
Objective 3.3: Summarize social engineering attacks and the associated effectiveness with each attack.

CEH Exam Domain:
Social Engineering

Overview

Social engineering is a technique that attackers use to entice individuals, often with a lack of knowledge of computer security, to run programs, click links, or give out sensitive information. This lab demonstrates how social engineering techniques can be utilized.

Outcomes:

In this lab, you will learn to:

1. Compromise a Windows Server with the Social Engineering Toolkit
2. Execute a spear-phishing attack
3. Exploit the malware to steal data on a system

1	Key Term	Description
1	Social Engineering Toolkit	tools that can be used by an attacker to exploit victims
2	meterpreter	A meterpreter payload can be used by an attacker for control over a victim's system.
3	Kali	a Linux distribution used for penetration testing or for hacking
4	Opera	a free browser and email client
5	spear phish	used to entice an individual to check a link or open an attachment in

1	Key Term	Description
		an email

Performing a Denial of Service Attack from the WAN

Introduction
Objective

CEH Exam Domain:
Domain 1: Background
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:
Objective 1.2 Information Security Threats and Attack Vectors
Objective 4.3 Information Security Tools

Overview

In this lab, you will perform various denial-of-service attacks from a wide area network. A denial-of-service attack is an attacker overwhelms one or more services on a host so it stops responding to requests.

outcomes:

In this lab, you will learn to:

1. Use a TCP flood to perform a denial-of-service attack.
2. Use a UDP flood to perform a denial-of-service attack.
3. Use an HTTP flood to perform a denial-of-service attack.

	Key Term	Description
1	TCP	Transmission Control Protocol is a network protocol designed to send and ensure end-to-end delivery of data packets over the Internet.
2	UDP	User Datagram Protocol is a transport layer protocol and simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues and is used where error checking and correction is either not necessary or is performed.
3	HTTP	The protocol used by the World Wide Web. HTTP defines how messages are formatted and transmitted and how Web servers and browsers should respond to requests.
4	Denial of Service	Is an interruption in an intended user's access to a computer network, typically

	Key Term	Description
	(DoS)	one caused with malicious intent.
5	Low Orbit Ion Cannon	An open-source network stress testing and denial-of-service attack application.

Using Browser Exploitation to Take Over a Host's Computer

Introduction
Objective

CEH Exam Domain:

Domain 1: Background
Domain 2: Analysis/Assessments
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:

Objective 1.2 Information Security Threats and Attack Vectors
Objective 1.3 Information Security Technologies
Objective 2.2 Information Security Assessment Practices
Objective 4.3 Information Security Tools

Overview

In this lab, you will exploit a browser to take over a host's computer. In ethical hacking and penetration testing, white hat hackers use vulnerabilities in systems to test defenses and report on those weaknesses to a client. Black hat hackers use vulnerabilities to cause harm to an organization's systems and network. The main reason for hackers to attack machines and networks is for financial gain. In this lab, you will use an Internet Explorer vulnerability to take over a victim's machine.

Outcomes:

In this lab, you will learn to:

1. Use Metasploit to exploit a web browser vulnerability.
2. Use spear phishing to trick a user into launching a web browser vulnerability.
3. Breach a host's computer using the web browser vulnerability.

	Key Term	Description
1	Spear phishing	Used to entice an individual to check a link or open an attachment in an e-mail.
2	Meterpreter	A Meterpreter payload can be used by an attacker for control over a victim's system.

	Key Term	Description
3	Kali	A Linux distribution used for penetration testing or for hacking.
4	Opera	A free browser and e-mail client.
5	XAMPP	An open-source web server package consisting mainly of the Apache HTTP Server, MariaDB, and interpreters for scripts written in the PHP and Perl programming languages.

Attacking Webservers from the WAN

Introduction
Objective

CEH Exam Domain:
Domain 1: Background
Domain 4: Tools/Systems/Programs
Domain 5: Procedures/Methodology

CEH Objective Mapping:
Objective 1.2 Information Security Threats and Attack Vectors
Objective 1.3 Information Security Tools
Objective 5.2 Information Security Assessment Methodologies

Overview
In this lab, you will attack a web server from the wide area network, or WAN, with a Kali Linux Attack Machine and use Microsoft Remote Desktop Connection (RDP) to connect to the victim machine.

Outcomes:
In this lab, you will learn to:

1. Use nmap/Zenmap to scan a wide area network.
2. Use Bruter to exploit SMTP.
3. Use remote desktop with captured credentials to deface a web site.
4. Cover your tracks from the hack you just performed.

	Key Term	Description
1	Remote Desktop Connection (formerly Microsoft Terminal Services Client)	Allows a user to remotely log into a networked computer running the terminal services server.
2	Port	In computer networking, a port is an endpoint of communication in an operating system associated with an IP

	Key Term	Description
		address of a host and the protocol type of the communication.
3	Zenmap	A GUI front end for nmap; will allow you to scan for open ports and services.
4	Metasploit	A framework that contains exploits for various information systems.
5	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.

Exploiting a Vulnerable Web Application

Introduction
Objective

CEH Exam Domain:

Domain 1: Background

Domain 4: Tools/Systems/Programs

CEH Objective Mapping:

Objective 1.2 Information Security Threats and Attack Vectors

Objective 4.3 Information Security Tools

Overview

In this lab, you will learn how to exploit a vulnerable web application. You are using the external Kali attack machine on the wide area network, or WAN, to attack a web application on the network. You will use Armitage, which is a front end for Metasploit, to exploit a machine using XAMPP WebDAV PHP Upload exploit.

Outcomes:

In this lab, you will learn to:

1. Use nmap to scan a network.
2. Use Metasploit and Armitage to exploit a common web server vulnerability.
3. Use Meterpreter to breach a system.

	Key Term	Description
1	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.
2	Zenmap	A GUI front end for nmap; will allow you to scan for open ports and services.

	Key Term	Description
3	Kali Linux	An Advanced Penetration Testing Linux distribution designed for digital forensics and penetration testing, ethical hacking, and network security assessments.
4	Metasploit	A framework that contains exploits for various information systems.
5	Meterpreter	A tool that is packaged together with the Metasploit framework and provides an advanced, dynamically extensible payload that uses in-memory DLL injection stagers and is extended over the network at runtime.

Breaking WEP and WPA and Decrypting the Traffic

Introduction
Objective

CompTIA Security+ (SY601) Domain:
Domain 1.0: Attacks, Threats, and Vulnerabilities

CompTIA Security+ (SY601) Objective Mapping:
Objective 1.4: Given a scenario, analyze potential indicators associated with network attacks

CEH Domain:
Domain 1: Background
Domain 4: Tools/Systems/Programs
Domain 5: Procedures/Methodology

CEH Objective Mapping:
Objective 1.1 Network and Communication Technologies
Objective 1.3 Information Security Technologies
Objective 4.3 Information Security Tools
Objective 5.2 Information Security Assessment Methodologies

Overview

In this lab, you will learn how to exploit flaws in the Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) wireless security protocols using different tools in Kali Linux.

Outcomes:

In this lab, you will learn to:

1. Decrypt wireless network traffic that uses WEP.
2. Decrypt wireless network traffic that uses WPA.

	Key Term	Description

	Key Term	Description
1	FTP	File Transfer Protocol is a clear text protocol used to transfer files between systems.
2	TELNET	TELNET is a clear text protocol that is used to remotely administer a machine.
3	WEP	Wired Equivalent Privacy is a wireless network security standard. A WEP key is a kind of security passcode for Wi-Fi devices.
4	SSID	Service Set Identifier is a unique identifier attached to the header of packets sent over a wireless local area network (WLAN).
5	DNS	The Domain Name System converts IP addresses to names and names to IP addresses.

Attacking the Firewall and Stealing Data Over an Encrypted Channel

Introduction
Objective

CEH Exam Domain:
Domain 1: Background
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:
Objective 1.2 Information Security Threats and Attack Vectors
Objective 1.3 Information Security Tools

Overview

In this lab, you will attack a firewall and steal data over an encrypted channel. Figure 1 shows the network topology for this lab. You are using the external Kali Attack Machine on the wide area network, or WAN, to attack a web application on the network. You will use Metasploit and a Meterpreter payload to exploit a machine using an XAMPP WebDAV PHP Upload exploit. This exploit uses default WebDAV credentials on XAMPP servers. It uses supplied credentials to launch a Hypertext Preprocessor (PHP) Meterpreter payload.

Outcomes:

In this lab, you will learn to:

1. Use nmap/Zenmap to scan a network.

2. Use metasploit/meterpreter to exploit a vulnerability on a target.

	Key Term	Description
1	Kali Linux	An Advanced Penetration Testing Linux distribution designed for digital forensics and penetration testing, ethical hacking, and network security assessments.

	Key Term	Description
2	Privilege escalation	Gaining a higher level of access (possible administrative access) from account with less permissions and rights.
3	Zenmap	A GUI front end for nmap; will allow you to scan for open ports and services.
4	Metasploit	A framework that contains exploits for various information systems.
5	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.

Using Public Key Encryption to Secure Messages

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objective Mapping
Objective 3.9: Given a scenario, implement public key infrastructure

CEH Exam Domains:
Domain 1: Background
Domain 3: Security
Domain 4: Tools/Systems/Programs
Domain 5: Procedures/Methodologies

CEH Objective Mapping:
Objective 1.3 Information Security Technologies
Objective 3.3: Information Security Attack Prevention
Objective 4.3: Information Security Tools
Objective 5.1 Information Security Procedures

Overview

In this lab, you will use encryption to protect data and sensitive information. Data protection is imperative for companies and organizations. Encryption is used as a part of layered security architecture in an organization's networks.

outcomes:

In this lab, you will learn to:

1. Use PKI to generate a certificate for a student and administrator.
2. Use PKI to encrypt and decrypt a file.

	Key Term	Description

	Key Term	Description
1	Social Engineering Toolkit	Tools that can be used by an attacker to exploit victims.
2	Kleopatra	A certificate manager and a universal crypto graphical user interface (GUI). Kleopatra supports management of X.509 and OpenPGP certificates in the GpgSM and GPG keyboxes and for retrieving certificates from LDAP and other certificate servers.
3	Certificate	An electronic document used to authenticate ownership of a public key. The certificate includes information about the key, information about its owner's identity, and the digital signature of an entity that has verified the certificate.
4	Opera	A free browser and e-mail client.
5	Public key encryption	A cryptographic system that uses two keys—a public key known to everyone and a private key known only to the recipient of the message. These keys are related in that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.

Performing SQL Injection to Manipulate Tables in a Database

Introduction
Objective

CEH Exam Domain:
Domain 1: Background
Domain 3: Security
Domain 4: Tools/Systems/Programs

CEH Objective Mapping:
Objective 1.2 Information Security Threats and Attack Vectors
Objective 1.3 Information Security Technologies
Objective 4.3 Information Security Tools

Overview

In this lab, you will be performing SQL (Structured Query Language) injection to manipulate tables in a database. You are using a Kali Attack Machine which is on the external network, or WAN (Wide Area Network), to scan and attack a MySQL database on port 3306. You will use Metasploit's MySQL login auxiliary module to exploit a database.

Outcomes:

In this lab, you will learn to:

1. Use nmap to scan a network.

2. Use brute force to crack a user name and password of a MySQL database.
3. Use the harvested credentials to exploit and breach a database.

	Key Term	Description
1	nmap	A port scanner which will indicate whether ports are open or closed on a remote system.
2	Zenmap	A GUI front end for nmap; will allow you to scan for open ports and services.
3	Kali	A Linux distribution used for penetration testing or for hacking.
4	Metasploit	A framework that contains exploits for various information systems.
5	SQL injection	Is a code injection attack, used to attack data-driven applications, in which malicious SQL statements are inserted into an entry field for execution.