masterskill
education through innovation

aci LEARNING | SKILL LABS

Information Security Fundamentals, Skill Labs

Course Specifications

Course Number: ACI76-050SL_rev1.0
Lab Length: Approximately 15 hours

Securing the pfSense Firewall

Introduction
Objective

CompTIA Security+ (SY601) Domain:
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objective Mapping:
Objective 3.3: Given a scenario, implement secure network designs

Overview

In this lab, you will secure the pfSense Firewall by removing insecure and unneeded protocols. pfSense is an open source, BSD based, firewall that is a very popular and widely used security appliance.

Outcomes:

In this lab, you will learn to:

1. Use nmap to scan for open ports on a pfSense firewall.
2. Close unnecessary ports on a pfSense firewall.
3. Add a secure service to a pfSense firewall.

	Key Term	Description
1	firewall	A firewall can block traffic or redirect traffic to hosts on the internal network. pfSense is an open source firewall that uses a BSD-based firewall.
2	SSH	Secure shell uses port 22 and encrypts traffic, which typically provides a terminal interface.
3	nmap	an open source and free scanner that allows you to determine open ports on a remote host
4	zenmap	a GUI port scanner that is a front end for the free and open source Nmap scanner
5	ping	an operating system utility that allows you to test for TCP/IP connectivity between hosts

Implementing NAT and Allowing Remote Access

Introduction
Objective

CompTIA Security+ (SY601) Domain:
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objective Mapping:
Objective 3.3: Given a scenario, implement security network designs

Overview

NAT stands for Network Address Translation and allows many machines with private IP addresses to use a single Public IP Address to connect to the Internet. In this lab, you will implement NAT on a firewall.

Outcomes:

In this lab, you will learn to:

1. Configure NAT.
2. Use Wireshark to understand how NAT works.
3. Use remote desktop on a network.

	Key Term	Description
1	firewall	A firewall can block traffic or redirect traffic to hosts on the internal network. pfSense is an open source firewall that uses a BSD-based firewall.
2	NAT	Network Address Translation can be used to allow internal IP addresses access to the WAN.
3	VPN	Virtual Private Network allows you to connect to a LAN for the Internet and access resources.
4	pfSense	an open source firewall that is widely used in the industry
5	ping	an operating system utility that allows you to test for TCP/IP connectivity between hosts

Implementing Common Protocols and Services

Introduction
Objective

CompTIA Security+ (SY601) Domain:

Domain 3.0: Implementation

CompTIA Security+ (SY601) Objectives:

Objective 3.1: Given a scenario, implement security protocols

Overview

Telnet and SSH are two protocols that can be utilized to remotely administer a server. However, there is a huge difference between them. TELNET sends all information over the wire in clear text and SSH communication between two systems is encrypted. During this lab, you will utilize TELNET, SSH, and FTP to perform functions between two systems on a network. After completing the tasks, you will examine how the traffic looks with Wireshark, an open source Protocol Analyzer.

Outcomes:

In this lab, you will learn to:

1. Use Telnet and SSH on a network and understand why you would use one over the other.
2. Use FTP and SCP on a network and understand why you would use one over the other.
3. Use Wireshark to capture and observe network traffic.

	Key Term	Description
1	SSH	Secure shell uses port 22 and encrypts traffic, which typically provides a terminal interface.
2	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.
3	PuTTY	a free SSH client for Windows. Although Microsoft Windows does come with a TELNET client, it lacks an SSH client. For this reason, a third party application like PuTTY needs to be utilized in order for a Windows machine to connect to an SSH server.
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	WinSCP	WinSCP is a free program for Microsoft Windows, which will allow you to securely transfer files over an encrypted connection. The use of SCP is preferred over using FTP because the file will be transmitted over an encrypted channel.

Examining Wireless Networks

Introduction
Objective

CompTIA Security+ (SY701) Domain:

Domain 1: Network Security

CompTIA Security+ (SY701) Objective Mapping:

Objective 1.5: Given a scenario, troubleshoot security issues related to wireless networking.

Overview

In this lab, you will analyze a network capture file containing wireless traffic. You will examine protocols, IP addresses, MAC addresses, as well as analyze other information from traffic. You will also learn how to extract an image from http traffic.

Outcomes:

In this lab, you will learn to:

1. Use Wireshark to explore wireless traffic.
2. Use Wireshark to export an image from HTTP traffic.

	Key Term	Description
1	FTP	File Transfer Protocol is a clear text protocol used to transfer files between systems.
2	TCP	Transmission Control Protocol is a network protocol designed to send and ensure end-to-end delivery of data packets over the Internet.
3	SSID	Service Set Identifier is a unique identifier attached to the header of packets sent over a wireless local area network (WLAN).
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	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.
6	Beacon Frame	one of the management frames in a wireless LAN. It contains all the information about the network.

Implementing Security Policies on Windows and Linux

Introduction
Objective

CompTIA Security+ (SY601) Domain:

Domain 5.0: Governance, Risk, and Compliance

CompTIA Security+ (SY601) Objective Mapping:

Objective 5.5: Explain privacy and sensitive data concepts in relation to security

Overview

In this lab, you will secure operating systems running Microsoft Windows and Linux. You will learn how to secure the logon process and also use the highly vulnerable Metasploitable machine (from Rapid7) to do some basic security hardening on Linux.

Outcomes:

3. Secure the Windows login process.
4. Audit login failures.
5. Secure Linux.

	Key Term	Description
1	netplwiz	a command in Windows that will allow you to set logon parameters
2	gpedit.msc	opens the Group Policy Management Console on a Microsoft Windows operating system
3	Event Viewer	7. contains log files that contain information about activities on the computer
4	telnet	allows remote administration of Linux and Windows systems through the command line
5	useradd	a command to add a user on a Linux/Unix system

Data Backups in Windows, BSD, and Linux

Introduction
Objective

CompTIA A+ (220-1102) Domain:
Domain 1.0: Operating Systems

CompTIA Security+ (SY601) Domain:
Domain 2.0: Architecture & Design

CompTIA A+ (220-1102) Objective Mapping:
Objective 1.11: Given a scenario, identify common features and tools of the Linux client/desktop OS

CompTIA Security+ (SY601) Objective Mapping:
Objective 2.5: Given a scenario, implement cybersecurity resilience

Overview

Backing up data and configurations is a critical part of a company or organization's IT policy. A system administrator should always have a disaster recovery plan in place in case of a loss or in case they need to deal with a network compromise or ransomware attack. It should be part of the organization's overall security policy. It should periodically review and update when needed. In this lab, you will back up data

on Windows, Linux, and BSD-based systems. Backing up data is critical, regardless of the operating system used.

Outcomes:

In this lab, you will learn to:

1. Backup pfSense Firewall.
2. Backup files in Linux.
3. Backup files in Windows.

	Key Term	Description
1	pfSense	an open source BSD-based firewall
2	net use	built-in Windows command for mapping drives
3	WinSCP	WinSCP is a free program for Microsoft Windows which will allow you to securely transfer files over an encrypted connection. The use of SCP is preferred over using FTP because the file will be transmitted over an encrypted channel.
4	dir	built-in internal command in Windows that allows you to view files and folders
5	copy	built-in internal command in Windows that allows you to copy files

Incident Response Procedures, Forensics, and Forensic Analysis

Introduction
Objective

CompTIA Security+ (SY601) Domain:

Domain 4.0: Operations and Incident Response

CompTIA Security+ (SY601) Objective Mapping:

Objective 4.1: Summarize the importance of policies, processes, and procedures for incident response

Overview

In this lab, you will exploit a remote system, analyze web logs, and perform incident response on a compromised host.

Outcomes:

In this lab, you will learn to:

1. Scan a network with nmap/zenmap.
2. Exploit a system using Bruter.
3. Use remote desktop using the stolen credentials from Bruter.

	Key Term	Description
1	netstat	A command line tool in Windows and terminal tool in Linux that will provide you with connection information.
2	tasklist	This command, which is built into Windows, will display running processes.
3	ipconfig	These command line Windows tools will display the IP Address and MAC Address of the system.
4	path	This internal command will allow you to set a new path or to display the current path.
5	md5sum	This is a hashing tool that is not native to the Windows operating system.

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.

	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 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.

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
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.

Deep Dive in Packet Analysis - Using Wireshark and Network Miner

Introduction
Objective

CompTIA Security+ (SY601) Domain:
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objective Mapping:
Objective 3.3: Given a scenario, implement secure network designs

Overview
Packet Analysis is the process of sifting through network traffic and finding relevant artifacts. Analyzing network traffic is critical to the protection of information systems.

Outcomes:
In this lab, you will learn to:

1. Use Wireshark to view protocol traffic.
2. View protocols using Wireshark.
3. Parse objects from network traffic.
4. Use NetworkMiner.

	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	ping	uses internet control message protocol to check for connectivity between two systems
4	SSH	Secure shell is used to securely transfer files between two systems.
5	DNS	The Domain Name System converts IP addresses to names and names to IP addresses.

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.

Patching, Securing Systems, and Configuring Anti-Virus

Introduction
Objective

CompTIA Security+ (SY601) Domain:
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objective Mapping:
Objective 3.2: Given a scenario, implement host or application security solutions.

Overview
In this lab, you will begin on the red team side by exploiting a Windows server that has not been properly patched. After seeing the damage that an attacker can do to an unpatched system firsthand, you will jump on the blue team side and you will harden and patch a Windows Server operating system to secure it from attack.

Outcomes:
In this lab, you will learn to:

1. Exploit a Windows server that is not properly patched
2. Harden a Windows server by patching the vulnerability

	Key Term	Description
1	netplwiz	a command in Windows that will allow you to set log on parameters
2	gpedit.msc	opens the Group Policy Management Console on a Microsoft Windows operating system
3	Event Viewer	contains log files that contain information about activities on the computer
4	telnet	allows remote administration of Linux and Windows systems through the command line
5	useradd	a command to add a user on a Linux/Unix system

Using Active Directory in the Enterprise

Introduction
Objective

CompTIA A+ (220-1102) Domain:
Domain 1: Operating Systems
Domain 2: Security

CompTIA A+ (220-1102) Objective Mapping:
Objective 1.3: Given a scenario, use features and tools of the Microsoft Windows 10 operating system (OS).
Objective 2.6: Given a scenario, configure a workstation to meet best practices for security.

CompTIA Security+ (SY601) Domain:
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objective Mapping:
Objective 3.8: Given a scenario, implement authentication and authorization protocols

Overview
Active Directory is a database, which can be used to centrally manage a Microsoft Windows network, users, groups, computers, printers, and other objects and resources. In this lab, you will examine the Active Directory objects and group policies at the domain and organizational unit level. Windows System Administrators commonly use Active Directory in their daily work.

Outcomes:
In this lab, you will learn to:

1. Create an Organizational Unit and Users in Active Directory
2. Set a Domain Level Policy in Active Directory
3. Set an Organizational Level Policy in Active Directory

	Key Term	Description
1	organizational unit	An Active Directory container that can hold users, groups, and computers.
2	dsa.msc	the command to open Active Directory Users and Computers
3	Active Directory Users and Computers	database which can be used to centrally manage a Windows network
4	Net user	A Built in Windows command to manage and create users
5	gpupdate	the command to update group policy

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
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.