masterskill
education through innovation

aci LEARNING | SKILL LABS

Network Security Fundamentals, Skill Labs

Course Specifications

Course Number: ACI76-042SL_rev1.0
Lab Length: Approximately 15 hours

Configuring a Windows Based Firewall to Allow Incoming Traffic

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

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

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will enumerate hosts on the network using various tools.

Outcomes:

In this lab, you will learn to:

- Set Up System Services on the Internal Network
- Configure and Test the Windows-Based Firewall
- Use Internal Services from an External Machine

	Key Term	Description
1	FTP	FTP stands for File Transfer Protocol. FTP, which uses port 20 and 21, can be used to upload or download files from the command line or a bowser, like Firefox.
2	HTTP	HTTP stands for Hyper Text Transfer Protocol. HTTP, which uses port 80, and is commonly used to download files from a website using browsers like Internet Explorer.
3	nmap	Nmap can be used in Linux, Mac, or Microsoft Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Nmap was used in the movie The Matrix.
4	Port	There are 65,536 ports, numbered from 0–65,535. The first 1,024 ports, ports

	Key Term	Description
		0-1,023 are said to be well-known. They include ports like HTTP (port 80) and FTP (port 21).
5	SSH	Secure Shell uses port 22. SSH provides a much better option than Telnet for remote administration because traffic is encrypted. SSH is native to most Linux systems.

Configuring a Linux Based Firewall to Allow Incoming and Outgoing Traffic

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

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

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, you will be testing the current firewall configuration nmap You will install and configure the Linux-based firewall called Endian which by default blocks all outgoing services except HTTP. You will test those connections with nmap.

Outcomes

In this lab, you will learn to:

- Test the Current Firewall and Install the Linux Firewall
- Configure and Test the Linux-Based Firewall
- Using Internal Services from an External Machine

	Key Term	Description
1	FTP	FTP stands for File Transfer Protocol. FTP, which uses port 20 and 21, and can be used to upload or download files from the command line or a bowser, like Firefox.
2	HTTP	HTTP stands for Hyper Text Transfer Protocol. HTTP, which uses port 80, and is commonly used to download files from a website using browsers like Internet Explorer.
3	nmap	Nmap can be used in Linux, Mac, or Microsoft Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Nmap was used in the movie the Matrix.
4	PORT	There are 65,536 ports, numbered from 0-65,535. The first 1024 ports, ports 0-

	Key Term	Description
		1023 are said to be well-known. They include ports like HTTP (Port 80) and FTP (Port 21).
5	SSH	Secure Shell uses port 22. SSH provides a much better option than Telnet for remote administration because traffic is encrypted. SSH is native to most Linux systems.

Implementing Secure DHCP and DNS

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objectives
Objecting 3.1: Given a scenario, implement secure protocols

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, you will install, configure, and secure Windows DHCP and DNS. A system administrator needs to understand how DHCP and DNS work so they know how to troubleshoot if they run into issues.

Outcomes:

In this lab, you will learn to:

- Install and Configure DCHP
- Secure DHCP
- Install and Configure Secure DNS
- Secure DNS

	Key Term	Description
1	DNS	Domain Name System maps Fully Qualified Domain Names (F.Q.D.N.) to IP Addresses. DNS allows users to connect to websites using names instead of IPs.
2	DHCP	Dynamic Host Configuration Protocol automatically leases IP Addresses to clients on the network. DHCP uses UDP and uses ports 67 (server) and 68 (client).
3	Forward Lookup	A DNS forward lookup provides the IP Addresses for Fully Qualified Domain Names (F.Q.D.N.).
4	Reverse Lookup	A DNS reverse lookup provides the Fully Qualified Domain Names (F.Q.D.N.) for the IP Addresses.
5	Zone Transfer	When information is sent from one DNS server to another to provide a list.

Configuring a Linux Based Firewall to Allow Outgoing Traffic

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

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

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, you will be testing the current firewall configuration nmap You will install and configure the Linux-based firewall called Endian which by default blocks all outgoing services except HTTP. You will test those connections with nmap.

Outcomes:

In this lab, you will learn to:

- Test the Current Firewall and Install the Linux Firewall
- Configure and Test the Linux-Based Firewall
- Using Internal Services from an External Machine

	Key Term	Description
1	FTP	FTP stands for File Transfer Protocol. FTP, which uses port 20 and 21, and can be used to upload or download files from the command line or a bowser, like Firefox.
2	HTTP	HTTP stands for Hyper Text Transfer Protocol. HTTP, which uses port 80, and is commonly used to download files from a website using browsers like Internet Explorer.
3	nmap	Nmap can be used in Linux, Mac, or Microsoft Windows to locate machines on a network. After Nmap is used to discover machines on a network, it can also be utilized to determine which open Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) ports the machine has open. Nmap will give an indication of the operating system the remote machine is using. Nmap was used in the movie the Matrix.
4	PORT	There are 65,536 ports, numbered from 0-65,535. The first 1024 ports, ports 0-1023 are said to be well-know. They include ports like HTTP (Port 80) and FTP (Port 21).
5	SSH	Secure Shell uses port 22. SSH provides a much better option than Telnet for remote administration because traffic is encrypted. SSH is native to most Linux systems.

Configuring Access Control Lists on a Linux Based Firewalls

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

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

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will set up the sniffer, enable services and configure firewall rules, and test those rules.

Outcomes:

In this lab, you will learn to:

1. Set up the network
2. Enable services and configure firewall rules
3. Test the firewall

You should be aware of the common terms that are relevant within the "Configuring Access Control Lists on a Linux-Based Firewalls" lab to successfully complete it.

	Key Term	Description
1	Iptables	a command line tool that allows you to create firewall rules.
2	route add	This command allows you to add a default gateway on a Linux system.
3	netstat	This command will allow you to view active TCP and UDP connections.
4	NAT	Network Address Translation will allow internal hosts to reach the external network through a single IP address. Most firewalls can be configured to perform NAT.
5	nmap	The command will allow you to check for open TCP and UDP ports.

Configuring a Virtual Private Network with PPTP

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objectives
Objecting 3.1: Given a scenario, implement secure protocols

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will install and configure a Linux Firewall.

Outcomes:

In this lab, you will learn to:

- Test the Firewall and Configuring the VPN Server
- Configure the VPN client
- Use Internal Services from an External Machine

	Key Term	Description
1	PPTP	Point-to-Point tunneling protocol is an older VPN technology that allows remote users to connect to a company's VPN server and access internal resources.
2	L2TP	Layer 2 tunneling protocol is a VPN technology that uses IPsec and allows remote users to connect to a company's VPN server and access internal resources.
3	VPN	Most firewalls can be configured to allow incoming traffic on their external interfaces to be redirected to internal hosts.
4	NAT	Network Address Translation will allow internal hosts to reach the external network through a single IP Address. Most firewalls can be configured to perform NAT.
5	IPsec	IPsec is a technology that encrypts IP packets so they are not sent in the clear. Layer 2 tunneling protocol is a VPN technology that uses IPsec.

Configuring a Virtual Private Network with OpenVPN

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objectives
Objecting 3.1: Given a scenario, implement secure protocols

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will install and configure a Linux Firewall.

Outcomes:

In this lab, you will learn to:

- Install the Firewall and Configuring the VPN Server
- Configure the VPN Server and Clients
- Use Internal Services from an External Machine

	Key Term	Description
1	PPTP	Point to Point tunneling protocol is an older VPN technology that allows remote users to connect to a company's VPN server and access internal resources.
2	L2TP	Layer 2 tunneling protocol is a VPN technology that uses IPsec and allows remote users to connect to a company's VPN server and access internal resources.
3	VPN	Most firewalls can be configured to allow incoming traffic on their external interfaces to be redirected to internal hosts.
4	NAT	Network Address Translation will allow internal hosts to reach the external network through a single IP Address. Most firewalls can be configured to perform NAT.
5	IPsec	IPsec is a technology that encrypts IP packets so they are not sent in the clear. Layer 2 tunneling protocol is a VPN technology that uses IPsec.

Implementing RIP, RIPv2, and Securing RIP

Introduction
Objective

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

CompTIA Security+ (SY601) Objective Mapping:
Objective 3.1: Given a scenario, implement security protocols

Overview

RIP stands for Routing Information Protocol. A router is a device that can connect two different networks. Routers are common to all computer networks and help to connect the entire Internet together. A typical router is a hardware device. Cisco and Juniper are two companies who manufacture many of the hardware routers used in company networks and throughout the Internet. It is also important to note that any computer with two network cards can be used as a router. In this lab, you will configure the RIPv1 and RIPv2 routing protocols and implement a password used between the routers.

Outcomes:

In this lab, you will learn to:

1. Configure RIP Version 1
2. Configure RIP Version 2
3. Securing RIP

	Key Term	Description
1	RIPv1	Routing Information Protocol, Version 1, uses a broadcast address to update

	Key Term	Description
		information about routing over UDP (User Datagram Protocol) port 520.
2	RIPv2	Routing Information Protocol, Version 2, uses a multicast address to update information about routing over UDP (User Datagram Protocol) port 520.
3	UDP	User Datagram Protocol is a connectionless oriented protocol in contrast to TCP (Transmission Control Protocol) which is a connection oriented protocol.
4	Wireshark	A protocol analyzer that will allow you to capture traffic.
5	Routing and Remote Access	IPsec is a technology that encrypts IP packets so they are not sent in the clear. Layer 2 tunneling protocol is a VPN technology that uses IPsec.

Intrusion Detection using Snort

Introduction
Objective

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

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

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will enumerate hosts on the network using various tools.

Outcomes:

In this lab, you will learn to:

- Set Up the Sniffer
- Detect Unwanted Incoming Traffic
- Detect Unwanted Outgoing Traffic

	Key Term	Description
1	Wireshark	A protocol analyzer that read binary capture files. Wireshark will also allow you to capture network traffic and runs on Windows, Linux, and on Mac OS X.
2	snort	An Intrusion Detection System, or an IDS, that can be used to analyze and capture traffic. By using signatures, snort can provide information about activity within a capture file. Snort can be downloaded from www.snort.org and is a free and commercial tool. Sourcefire, a Columbia, Maryland–based company, maintains and develops snort.
3	tcpdump	A Linux/UNIX program that allows you to capture network traffic. The tcpdump program comes installed on many Linux distributions by default.

	Key Term	Description
4	Sniffer	A Sniffer is used to capture network traffic on a network. Software programs like tcpdump, Wireshark, and Network Miner can be used to sniff traffic.
5	PCAP File	Programs that can sniff network traffic like tcpdump, Wireshark, and Network Miner allow you to save the network capture to a PCAP file format. In order to read the PCAP format, you need a tool like Wireshark or Network Miner.

Writing Custom Rules

Introduction
Objective

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

CompTIA Security+ (SY601) Objective Mapping:
Objective 1.7: Summarize the techniques used in security assessments

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

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48. In this lab, you will do a basic penetration using nmap and bruter. Then, you will configure a snort rule to alert for a specific user and malicious file. You will use tcpdump to capture the network traffic to a file to be used by snort to find malicious traffic throug alerts.

Outcomes:

In this lab, you will learn to:

- Penetrate a network.
- Write rules to protect the network.
- Generate traffic trigger alerts.

	Key Term	Description
1	Wireshark	A protocol analyzer that read binary capture files. Wireshark will also allow you to capture network traffic and runs on Windows, Linux, and on Mac OS X.

	Key Term	Description
2	Snort	An Intrusion Detection System, or an IDS, that can be used to analyze and capture traffic. By using signatures, snort can provide information about activity within a capture file. Snort can be downloaded from www.snort.org and is a free and commercial tool. Sourcefire, a Columbia, Maryland–based company, maintains and develops snort.
3	tcpdump	A Linux/UNIX program that allows you to capture network traffic. The tcpdump program comes installed on many Linux distributions by default.
4	Sniffer	A Sniffer is used to capture network traffic on a network. Software programs like tcpdump, Wireshark, and Network Miner can be used to sniff traffic.
5	PCAP File	Programs that can sniff network traffic like tcpdump, Wireshark, and Network Miner allow you to save the network capture to a PCAP file format. In order to read the PCAP format, you need a tool like Wireshark or Network Miner.

Host-Based Firewalls

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

This lab will explore firewalls in the IT environment at the host. Students will view and configure the two host-based firewalls that are packaged with the Windows operating systems as well as create a firewall rule within the Linux Ubuntu operating system using the uncomplicated firewall (UFW). Figure 1 shows the topology for this lab.

Outcomes:

In this lab, students will learn to:

1. Learn how the hacker enters the network
2. Write rules to protect the network
3. Learn how the hacker triggers alerts

	Key Term	Description
1	Wireshark	A protocol analyzer that read binary capture files. Wireshark will also allow you to capture network traffic and runs on Windows, Linux, and on Mac OS X.
2	snort	Snort, an Intrusion Detection System (IDS), can be used to analyze and capture traffic. By using signatures, snort can provide information about activity within a capture file. Snort can be downloaded from www.snort.org

	Key Term	Description
		and is a free and commercial tool. Sourcefire, a Columbia, Maryland based company, maintains and develops snort.
3	tcpdump	A Linux/UNIX program that allows you to capture network traffic. The tcpdump program comes installed on many Linux distributions by default.
4	Sniffer	A Sniffer is used to capture network traffic on a Network. Software programs like tcpdump, Wireshark, and Network Miner can be used to sniff traffic.
5	PCAP File	Programs that can sniff network traffic like tcpdump, Wireshark, and Network Miner allow you to save the network capture to a PCAP file format. In order to read the PCAP format, you need a tool like Wireshark or Network Miner.

Configuring RADIUS

Introduction
Objective

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

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will install and configure a Linux Firewall.

Outcomes:

In this lab, you will learn to:

1. Configure the RADIUS Server
2. Set up the Remote Access Policies
3. Connect to the RADIUS Server

	Key Term	Description
1	RADIUS	(Remote Authentication Dial-In User Service) RADIUS can be used for wired or wireless networks to help secure networks and prevent any unauthorized use.
2	Remote Access Policy	Policy that dictates which conditions must be met in order for remote users to connect to the network. For example, users can log on between the hours on 9 A.M. and 5 P.M. Monday through Friday but not during other times.
3	UDP	User Datagram Protocol is a connection-less oriented protocol in contrast to TCP (Transmission Control Protocol) which is a connection oriented protocol.
4	Wireshark	A protocol analyzer that will allow you to capture traffic.

	Key Term	Description
5	Routing and Remote Access	IPsec is a technology that encrypts IP packets so they are not sent in the clear. Layer 2 tunneling protocol is a VPN technology that uses IPsec.

Domain Security

Introduction
Objective

CompTIA A+ (220-1102) Domain:
Domain 2.0: Security

CompTIA A+ (220-1102) Objective:
Objective 2.7: 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 3.7: Given a scenario, implement identity and account management controls

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 join a Windows 8 workstation to a Windows Active Directory Domain Environment and create a user and a group policy.

Outcomes:

In this lab, you will learn to:

1. Join a domain.
2. Create a domain account.
3. Create a group policy.

	Key Term	Description
1	workstation	an end user operating system such as Windows 7, Windows 8, and Windows 10
2	Windows Server	Microsoft has several server operating systems such as Server 2003, 2008, 2012, and 2016.
3	Active Directory	the centralized database for managing users and computers
4	Domain	a centralized unit of security and management
5	Group Policy	allows local or centralized management of users and computer in a Windows environment

Configuring a Site to Branch a Virtual Private Network

Introduction
Objective

CompTIA Security+ (SY601) Domain
Domain 3.0: Implementation

CompTIA Security+ (SY601) Objectives
Objecting 3.1: Given a scenario, implement secure protocols

Overview

This lab is part of a series of lab exercises intended to support courseware for Ethical Hacker training. The development of this document is funded by the Department of Labor (DOL) Trade Adjustment Assistance Community College and Career Training (TAACCCT) Grant No. TC-22525-11-60-A-48.

In this lab, students will install and configure a Linux Firewall.

Outcomes:

In this lab, you will learn to:

- Set up the Branch Office Machines
- Configure the Main Office VPN Server and the Branch Server
- Access Resources on the Remote Network

	Key Term	Description
1	Branch Office	Part of a company's network may be located in a different physical location. This other part of the network is often referred to as a branch office.
2	RIPv2	Routing Information Protocol, Version 2, uses a multicast address to update information about routing over UDP (User Datagram Protocol) port 520.
3	UDP	User Datagram Protocol is a connection-less oriented protocol in contrast to TCP (Transmission Control Protocol) which is a connection oriented protocol.
4	Wireshark	A protocol analyzer that will allow you to capture traffic.
5	Routing and Remote Access	IPsec is a technology that encrypts IP packets so they are not sent in the clear. Layer 2 tunneling protocol is a VPN technology that uses IPsec.

Closing Security Holes

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

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 system over the network and then patch and secure it. You will practice ethical hacking techniques by using Armitage to compromise a Windows Server and cybersecurity defensive techniques of closing ports and installing patches to prevent attackers from compromising systems.

Outcomes:

In this lab, you will learn to:

1. Attack a vulnerable Windows Server with Armitage
2. Close a port on a Windows Server using the Windows Firewall
3. Patch a system with Windows Update

	Key Term	Description
1	nmap	a command line scanning tool that will allow you to determine open ports
2	Windows Server	Microsoft has several server operating systems such as Server 2003, 2008, 2012, and 2016.
3	exploit	a program takes advantage of a weakness or flaw in software code
4	patching	the process of removing a vulnerability from a system
5	firewall	can be used to open and blocks or allows programs