Networking Fundamentals, Skill Labs

Course Specifications

Course Number: ACI76-044SL_rev1.0
Lab Length: Approximately 16 hours

Configuring Port Redirection

Introduction
Objective

CompTIA Network + Domain:

Domain 1: Networking Concepts
Domain 5: Network Troubleshooting and Tools

CompTIA Network + Objective:

Objective 1.1: Explain the purposes and uses of ports and protocols.
Objective 5.2: Given a scenario, use the appropriate tool.
Objective 5.4: Given a scenario, troubleshoot common network service issues.

Overview

In this lab, you will be testing the firewall from the external network or WAN (wide area network), testing connectivity with ping, and configuring port redirection on pfSense. Configuring port redirection is the process of redirecting a port on the firewall from one network to another port on the internal network. You will be using a pcap file in Wireshark to explore the network traffic that was already captured.

Outcomes:

In this lab, you will learn to:

1. Test a firewall from an external network.
2. Allow ICMP/ping in a firewall.
3. Configure port redirection on a 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

	Key Term	Description
		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

	Key Term	Description
		between hosts

IPv4 vs IPv6 – Calculating, Configuring, and Testing

Introduction
Objective

CompTIA Network + Domain:

Domain 1: Networking Concepts
Domain 5: Network Troubleshooting and Tools

CompTIA Network + Objective:

Objective 1.4: Given a scenario, configure the appropriate IP addressing components.
Objective 5.2: Given a scenario, use the appropriate tool.

Overview

This lab will compare Internet Protocol (IP)v4 and IPv6 addressing concepts such as subnetting, configuration, and testing. Students will assign addresses, test connectivity, and examine the results. Students will compare IPv4 and IPv6, addressing concepts such as subnetting, configuring, and testing. Students will assign addresses, test connectivity, and examine the results.

Outcomes:

In this lab you will learn to:

1. Use decimal, binary, and hexadecimal conversions.
2. Subnet IPv4 addresses.
3. Apply and test IPv4 subnet addresses.
4. Subnetting IPv6 addresses.
5. Apply and test IPv6 subnet addresses.

	Key Term	Description
1	Subnetting	The process of logically dividing a large network into smaller sub-networks by modifying the subnet mask (IPv4) or prefix length (IPv6).
2	Binary number system	A method of representing numbers using only the digits 0 and 1; also known as the base 2 number system.
3	Hexadecimal number system	A method of representing numbers using the digits 0 through 9 and characters A through F; also known as the base 16 number system.
4	Internet Protocol version 4 (IPv4)	A 32-bit number system represented in 4 groups of 8 bits each used to address nodes on an IP network.

	Key Term	Description
5	Subnet mask	A 32-bit number that is logically "AND" ed with an IPv4 address used to determine the network an address belongs to.
6	Internet Protocol version 6 (IPv6)	A 128-bit number system represented in 8 groups of 16 bits each used to address nodes on an IP network.
7	Subnet prefix length	The number of bits in an IPv6 address used to determine the network an address belongs to.

Network Management

Introduction
Objective

CompTIA Network + Domain:

Domain 4.0: Network Security
Domain 5.0: Network Troubleshooting and Tools

CompTIA Network + Objective:

Objective 4.5: Given a scenario, implement network device hardening.
Objective 5.2: Given a scenario, use the appropriate tool.

Overview

This lab explores concepts in network management including baselines, performance monitoring, logs, and implementation of patches and upgrades as a mitigation technique to security threats. By the end of this lab, students will be able to use the Performance Monitor to analyze network and Central Processing Utilization, the Event Viewer to view various logs, and Windows Update to manage operating system patches and updates.

Outcomes:

In this lab, you will learn to:

1. Analyze CPU and network utilization with Performance Monitor.
2. Use the Event Viewer to view logs.
3. Manage patches and updates.

	Key Term	Description
1	Baseline	a documented reference of resource utilization from which we can compare
2	Counter	an object in the Performance Monitor that represents a system resource, such as CPU, Memory, or Network and can be added to the graph area to

	Key Term	Description
		view resource utilization
3	Critical Updates	This type of update patches known vulnerabilities to the operating system and should be implemented immediately to mitigate security threats.
4	Event Viewer	allows users to view event logs in Windows operating systems, which include application, system, and security logs, among others
5	Idle/Idling	the state of the computer (CPU) when not in use by a program or user. System resource utilization should be little to none. Documenting what resource utilization looks like when idling can be important when establishing baselines.
6	Performance Monitor/Resource Monitor	used to monitor system resource utilization in Windows operating systems. Both provide a graphical reference to resource utilization. The Performance Monitor is more advanced and customizable, whereas the Resource Monitor provides a more user-friendly interface.
7	Recommended Updates	In Windows operating systems, recommended updates are classified as updates to hardware, such as device drivers and other hardware information.
8	Service Pack	a "bundle" of patches and updates for the operating system, downloadable as a single installable package, service packs may provide hundreds of updates and patches in one convenient download.
9	Windows Update Utility	used to find and apply patches and updates to the Windows operating system. The Windows Update Utility is accessible through the Control Panel.

Business Continuity - Disaster Recovery

Introduction
Objective

CompTIA Network + Domain:
Domain 3.0: Network Operations
Domain 4.0: Network Security

CompTIA Network + Objective
Objective 3.3: Compare and contrast business continuity and disaster recovery techniques.
Objective 4.6: Explain common mitigation techniques and their purposes.

Overview

Catastrophes of various types such as fires, floods, illness, and terrorism or server crashes, hard drive failure, viruses, and downed networks can upset an organization's ability to meet business needs causing disruptions to regular operational conditions. It is necessary for businesses, whether large or small, to have plans in place to mitigate the effects of potential catastrophes. Business continuity and disaster recovery plans are important components of any business plan to prevent major disruptions.

The purpose of this lab is to characterize some key points in disaster recovery plans and demonstrate the need for implementation. Students will create and restore a data backup. They will examine the importance of virus and malware protection and test antivirus software.

Outcomes:

In this lab, you will learn to:

1. Create a data backup.
2. Restore data from a data backup.
3. Download a virus test file to test antivirus software.

	Key Term	Description
1	Data Backups	copying files from a computer's hard drive onto other digital media that is stored in a secure location
2	Data Recovery	the process of restoring data that is lost through accidental or no accidental means
3	Adware	a software program that delivers advertising content in a manner that is unexpected and unwanted by the user
4	Antivirus (AV)	software that can examine a computer for any infections as well as monitor computer activity and scan new documents that might contain a virus
5	Computer Virus	malicious software program that reproduces itself on a single computer and can spread by sharing the infected files and usually infects program executable files
6	Rootkit	a set of software tools used by an attacker to hide the actions or presence of other
7	Signature File	file that contains known patterns or sequences of bytes (strings) found in viruses; used by antivirus software to identify malware
8	Spyware	general term used to describe software that spies on users by gathering information without consent, thus violating their privacy
9	Trojan	an executable program advertised as performing one activity but actually does something else (or it may perform both the advertised and malicious activities)
10	Worm	malicious program designed to take advantage of vulnerability in an application or an operating system in order to enter a computer

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).

	Key Term	Description
5	DNS	The Domain Name System converts IP addresses to names and names to IP addresses.

Closing Ports and Unnecessary Services

Introduction
Objective

CompTIA Network + Domain:

Domain 3.0: Network Operations

Domain 4.0: Network Security

CompTIA Network + Objective:

Objective 3.4: Given a scenario, use remote access methods.

Objective 4.3: Explain authentication and access controls.

Objective 4.4: Summarize common network attacks.

Overview

In this lab, you will secure the Windows Server by removing insecure and unneeded protocols. You will use Kali Linux to demonstrate the protocols that are open and how they are after they are disabled in Windows Server.

Outcomes:

In this lab, you will learn to:

1. Scan networks for open ports and services.
2. Connecting to the open ports and services using Telnet and FTP.
3. Closing unnecessary ports and services.

	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

	Key Term	Description
5	ping	an operating system utility that allows you to test for TCP/IP connectivity between hosts

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:

1. Secure the Windows login process.
2. Audit login failures.
3. 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	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

Network Security – Firewalls

Introduction
Objective

CompTIA Network + Domain:
Domain 2.0: Infrastructure

CompTIA Network + Objective:
Objective 2.2: Given a scenario, determine the appropriate placement of networking devices on a network and install/configure them.

Overview

This lab will explore firewalls in the IT environment. 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 Kali 2 operating environment using the uncomplicated firewall (UFW).

Outcomes:

In this lab, you will learn to:

1. Enable Windows Firewall using the Control Panel.
2. View Windows Firewall features using the Control Panel.
3. Configure Windows Firewall using the Control Panel.
4. View and configure Windows Firewall with Advanced Security (WFAS) using Administrative Tools.
5. Enable a firewall on a Linux system and enable firewall rules.

	Key Term	Description
1	Firewall	hardware component or software program running on a device that inspects network traffic and allows or blocks traffic based on a set of rules or exceptions
2	Network-based Firewall	located between the internal and external networks and is used to inspect traffic as it flows between networks, not to protect individual computers or computers on the same network
3	Host-based firewall	software that resides on an individual computer primarily to protect that computer from malicious traffic that manages to get through a perimeter firewall or originates on its own network or computer system
4	Firewall Rules (Exceptions)	created and used to allow and block traffic
5	Inbound Traffic	network data that originates from the external host and is addressed to a host on an internal network
6	Outbound Traffic	traffic an internal host sends to external hosts over the network

	Key Term	Description
7	Stateful Firewall	remembers attributes about the packet it is looking at, as well as the previous packets, and creates a stateful table used to determine if the incoming connection is active or inactive. It checks incoming traffic against its state table and blocks any traffic that does not match the state of the conversation.
8	Windows Firewall with Advanced Security	a bidirectional host-based stateful firewall with CLI and GUI interface options for configuration. It is used to secure hosts from attack as well as control what traffic is going in and out of the systems. Profiles and multiple high-level default exceptions are features of the Windows Firewall with Advanced Security
9	Windows Firewall Profiles (Windows Server 2008 R2 and Windows 7)	Profiles are a way to group settings in the firewall such as firewall rules. They are applied to the computer depending on the type of network the NIC is connected to. Each profile has default rules that are applied when the firewall is enabled. Three profiles exist in Windows Firewall and Windows Firewall with Advanced Security. They are • Domain – applied to the network adapter when the computer is connected to a network that has a domain controller and it can contact the domain • Private – applied to the network adapter when the computer is connected to a network not on a domain, not directly connected to the internet, but behind a network firewall or some type of security device. The private profile should be more restrictive than a domain profile. • Public – applied to a network adapter when it is connected to a public network like an airport hotspot. This should be the most restrictive because of the lack of security control.

Network Troubleshooting

Introduction
Objective

CompTIA Network + Domain:
Domain 5.0: Network Troubleshooting and Tools

CompTIA Network + Objective:
Objective 5.1: Explain the network troubleshooting methodology.
Objective 5.1: Given a scenario, use the appropriate tool.

Overview

Networks are important to business processes, and when they are not fully operational, it is costly and frustrating to the users. Network administrators need to understand not just how to keep the network functional but also how to approach troubleshooting problems when a network is not fully operational.

This lab will review troubleshooting and a methodology that will provide ideas on where to start in the problem-solving effort. This methodology will be used as a guide in troubleshooting two protocols widely used in networks, and it is important to be able to diagnose issues with them. Domain Name System (DNS) and Dynamic Host Configuration Protocol (DHCP) are the two protocols we will focus on in this exercise.

Outcomes:

In this lab, you will learn to:

1. Use the problem-solving process to troubleshoot a suspected DNS issue using CLI utilities and resolve the issue.
2. Configure an operational DHCP scope of addresses.
3. Observe the effects of a deactivated DHCP scope and resolve the problem.

	Key Term	Description
1	Domain Name Service (DNS)	the protocol used to resolve and map hostnames and domain names into IP addresses on the Internet. DNS uses UDP port 53 for initiating requests. Name servers, or DNS servers, are servers that contain databases of associated names and IP addresses and provide this information to resolvers (hosts) on request.
2	nslookup	a utility used to perform query testing of DNS servers and obtain detailed responses at the command prompt. This information can be useful for diagnosing and solving name resolution problems.
3	Dynamic Host Configuration Protocol (DHCP)	protocol used to automatically assign network configuration parameters to devices on a network. Parameters include IP address, subnet mask, default gateway, server addresses such as DNS, and lease time. DHCP uses port number 67 to communicate from client to server and port 68 from server to client.
4	DHCP Scope	the consecutive range of possible IP addresses that the DHCP server can lease to clients on a network or subnet. Scopes typically define a single physical subnet on your network to which DHCP services are offered. Scopes are the primary way for the DHCP server to manage distribution and assignment of IP addresses and any related configuration parameters to DHCP clients on the network.
5	Command Line Interface (CLI)	a text-based method of accessing the shell of an operating system. Usually, CLI provides a more powerful, direct way of executing programs and utilities.
6	Universal Resource Locator (URL)	the named address of a resource on the Internet

	Key Term	Description
7	Fully Qualified Domain Name (FQDN)	the complete domain name for a specific computer, or host, on the Internet. The FQDN consists of two parts: the hostname and the domain name.
8	ipconfig	The ipconfig command is used to view or modify a computer's IP addresses, to release and then renew the IP address, and to flush the DNS resolver cache.
9	Ping	used to verify basic TCP/IP connectivity to a network host.
10	APIPA (Automatic Private IP Addressing)	A Microsoft Windows feature used when there is a failure in DHCP servers, allowing DHCP clients to obtain IP addresses. APIPA allocates IP addresses in the private range 169.254.0.1 to 169.254.255.254 and are displayed in ipconfig /all as autoconfiguration IPv4 addresses. When the DHCP server is operational, clients correctly update their addresses automatically.

TCP/IP Utilities

Introduction
Objective

CompTIA Network + Domain:
Domain 5.0: Network Troubleshooting and Tools

CompTIA Network + Objective:
Objective 5.2: Given a scenario, use the appropriate tool.

Overview

This lab will identify common commands used to gather information about nodes on a network. Students will execute these commands in both Windows and Linux environments to compare and contrast their commands and outputs.

Outcomes:

In this lab, you will learn to:

1. Display computer information using the CLI.
2. Display IP information using the CLI.
3. Display DNS information using the CLI.
4. Display network connections using the CLI.
5. Use commands to test network connectivity.
6. Observe the ARP process using Wireshark.

	Key Term	Description
1	Cat	a Linux utility that concatenates and lists files
2	Man Pages	Manual Page, a form of software documentation found on Linux machines used to provide help with concepts such as programs or command syntax
3	Domain Name System (DNS)	the protocol used to map hostnames and domain names into IP addresses on the Internet. DNS uses UDP port 53 for initiating requests.
4	Fully Qualified Domain Name (FQDN)	the domain name that specifies the exact location of the specified node in the DNS hierarchy
5	Authoritative DNS Server	the master DNS server that hosts a specified domain
6	Nonauthoritative DNS Server	a secondary DNS server that responds to DNS queries using cached DNS information
7	Alias	a secondary name assigned to a host within DNS; allows an administrator to provide multiple names that the same host can respond to
8	in-addr.arpa	the reverse lookup zone used by IPv4 to map IP addresses to DNS names
9	Socket	the combination of an IP address and a TCP or UDP port number separated by a colon (ex. 192.168.12.10:53)
10	Internet Control Message Protocol (ICMP)	a protocol within the TCP/IP suite that resides at the OSI Network Layer (Layer 3) used to send query or error messages to network nodes
11	Time to Live (TTL)	a mechanism to specify the lifetime of data on a network
12	Address Resolution Protocol (ARP)	a protocol within the TCP/IP suite that resides at the OSI Network Layer (Layer 3) used to resolve network layer addresses (IP addresses) into link layer addresses (MAC addresses)
13	Media Access Control (MAC) Address	the physical address burned into the ROM of an Ethernet network card; used by switches at the Data Link layer of the OSI model to move information between nodes on the same network
14	Wireshark	‟is a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It has a rich and powerful feature set and is world's most popular tool of its kind. It runs on most computing platforms including Windows, OS X, Linux, and UNIX. Network professionals, security experts, developers, and educators around

	Key Term	Description
		the world use it regularly. It is freely available as open source, and is released under the GNU General Public License version 2." Reference: http://www.wireshark.org

The OSI Model

Introduction
Objective

CompTIA Network + Domain:
Domain 1.0: Networking Concepts

CompTIA Network + Objective:
Objective 1.1: Explain devices, applications, protocols, and services at their appropriate OSI layers.

Overview

This lab will utilize Wireshark to review network traffic. Wireshark is a network protocol analyzer licensed under GNU General Public License. A network protocol analyzer is used to capture data packets on a network. Students will review several layers of the OSI model during this lab. Students will be able to describe the encapsulation process and the function of specific protocols that operate within particular layers of the OSI model.

Outcomes:

In this lab you will learn to:

1. Explain the application, presentation, and session layers.
2. Explain the transport layer.
3. Explain the network layer.
4. Explain the data link layer.
5. Explain the physical layer.

	Key Term	Description
1	Connection-oriented data transfer	a transfer of data that requires the establishment of a connection between communicating endpoints, before the transfer can begin
2	Connectionless data transfer	a transfer of data that is serviced without requiring a verified session and without guaranteeing delivery of data
3	De-encapsulation	the process of each layer of the OSI model removing the control information headers on incoming information for the corresponding layer at the destination

	Key Term	Description
4	Encapsulation	the process of each layer of the OSI model adding control information headers to outgoing network data
5	IANA	Internet Assigned Numbers Authority; a government-funded group responsible for managing IP address allocation and the Domain Name System (DNS)
6	IEEE	Institute of Electrical and Electronics Engineers; one of the leading standards-making organizations in the world
7	IP	Internet Protocol; a core protocol of the TCP/IP suite that resides at the Network layer of the OSI model and provides information about how packets should be routed between networks
8	MAC address	Media Access Control; the physical address burned into the ROM of an Ethernet network card; used by switches at the Data Link layer of the OSI model to move information between nodes on the same network
9	OSI	Open System Interconnect; developed by the International Standards Organization (ISO)
10	OUI	Organizationally Unique Identifier; the first 24 bits (or 3 bytes) of a MAC address assigned by IEEE that identifies the network card's manufacturer
11	PDU	Protocol Data Unit; a term used to describe the product of encapsulation at a given layer of the OSI model
12	TCP	Transmission Control Protocol; the connection-oriented protocol of the TCP/IP suite that resides at the Transport layer of the OSI model
13	UDP	User Datagram Protocol; the connectionless protocol of the TCP/IP suite that resides at the Transport layer of the OSI model
14	Wireshark	a network protocol analyzer. It lets you capture and interactively browse the traffic running on a computer network. It has a rich and powerful feature set and is world's most popular tool of its kind. It runs on most computing platforms including Windows, OS X, Linux, and UNIX. Network professionals, security experts, developers, and educators around the world use it regularly. It is freely available as open source, and is released under the GNU General Public License version 2." Reference: http://www.wireshark.org

TCP/IP Protocols - The Core Protocols

Introduction
Objective

CompTIA Network + Domain:

Domain 1.0: Networking Concepts

Domain 3.0: Network Operations

CompTIA Network + Objective:

Objective 1.1: Explain the purpose and uses of ports and protocols.

Objective 3.3: Explain common scanning, monitoring, and patching processes and summarize their expected outputs.

Overview

This lab will review protocols that operate at the internetwork and transport layers of Transmission Control Protocol/Internet Protocol (TCP/IP). These protocols are internetwork layer protocols such as Address Resolution Protocol (ARP), Internet Control Message Protocol (ICMP), and Internet Protocol (IP), and transport layer protocols such as User Datagram Protocol (UDP) and Transmission Control Protocol (TCP). Students will review Internet Protocol (IP) address configurations, discover facts about network communication using ICMP and the ping utility, and examine the TCP/IP layers and become familiar with their status and function on a network.

Outcomes:

In this lab, you will learn to:

1. Use network utilities and protocols from the TCP/IP suite.
2. Use a network packet analyzer, Wireshark, to examine the ARP protocol.
3. Capture and analyze transport layer packets.

	Key Term	Description
1	TCP/IP	The Internet protocol suite is the conceptual model and set of communications protocols used in the Internet and similar computer networks.
2	ARP	The Address Resolution Protocol is a communication protocol used for discovering the link layer address, such as a MAC address, associated with a given internet layer address, typically an IPv4 address.
3	ICMP	The Internet Control Message Protocol is a supporting protocol in the Internet protocol suite. It is used by network devices, including routers, to send error messages and operational information indicating success or failure when communicating with another IP address.
4	IP	The Internet Protocol is the principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries. Its routing

	Key Term	Description
		function enables internetworking, and essentially establishes the Internet.
5	TCP	The Transmission Control Protocol is a connection-oriented protocol that runs at the transport layer of the OSI model.
6	UDP	The User Datagram Protocol is a connection-less protocol that runs at the transport layer of the OSI model

TCP/IP Protocols – Other Key Protocols

Introduction
Objective

CompTIA Network + Domain:
Domain 1.0: Networking Concepts

CompTIA Network + Objective:
Objective 1.1: Explain the purposes and uses of ports and protocols.
Objective 1.8: Explain the functions of network services.

Overview

This lab will introduce students to additional key services and protocols used on Transmission Control Protocol/Internet Protocol (TCP/IP) networks. These services include Dynamic Host Configuration Protocol (DHCP) and Domain Name Service (DNS).

Outcomes:

In this lab, you will learn to:

1. Create and test a DHCP scope.
2. Create and test a DHCP reservation.
3. Create and test DNS records.

	Key Term	Description
1	Dynamic Host Configuration Protocol (DHCP)	a protocol that allows devices to automatically obtain network settings (such as IP address, default gateway, etc.) so they can communicate on the network. DHCP uses UDP ports 67 (Server) and 68 (Client).
2	Reservation	with DHCP, the process where an administrator assigns an address for DHCP to give to a client
3	Media Access Control (MAC)	the physical address burned into the ROM of an Ethernet network card; used by switches at the Data Link layer of the OSI model to move

	Key Term	Description
	Address	information between nodes on the same network
4	Domain Name System (DNS)	the protocol used to map hostnames and domain names to an IP address on the Internet. DNS uses UDP port 53 for initiating requests.
5	Fully Qualified Domain Name (FQDN)	the domain name that specifies the exact location of the specified node in the DNS hierarchy
6	Forward Lookup Zone	the zone used by DNS clients to obtain information such as IP addresses that correspond to DNS domain names or services in the zone
7	Host (A) Record	the DNS record that links an FQDN to an IPv4 address
8	Host (AAAA) Record	the DNS record that links an FQDN to an IPv6 address
9	Alias	a secondary name assigned to a host within DNS; allows an administrator to provide multiple names the same host can respond to
10	Reverse Lookup Zone	the zone that provides mapping from IP addresses back to DNS domain names
11	in-addr.arpa	The reverse lookup zone used by IPv4 to map IP addresses to DNS names
12	Pointer (PTR) Record	the DNS record that links an IP address to a FQDN; used for reverse lookups

Types of Networks

Introduction
Objective

CompTIA Network + Domain:
Domain 1.0: Networking Concepts

CompTIA Network + Objective:
Objective 1.5: Compare and contrast the characteristics of network topologies, types, and technologies.

Overview

This lab will identify common functions of peer-to-peer and client/server networks. Students will create and access file and print shares as well as access a web and File Transfer Protocol server.

Outcomes:

In this lab, you will learn to:

1. Create a shared file.
2. Testing the share and reassigning permissions.
3. Map a drive to a server.
4. Sharing a printer.
5. Installing the shared printer.
6. Accessing a web and FTP server.

	Key Term	Description
1	Peer-to-Peer Network	a network type where two or more computers share resources (such as files or printers) and each computer in the network is responsible for their own access and security. These networks are simpler and cheaper than client/server networks but are less efficient when lots of users exist or large amounts of resources need to be shared.
2	Client/Server Network	a network where one centralized computer (called a server) controls access and security to shared resources. Other computers (called clients) connect to this central server to access shared resources.
3	Simple File Sharing	a wizard-based file sharing method that enables nontechnical users the ability to easily share files over the network
4	Advanced File Sharing	a file sharing method used by administrators to provide more granular control of shared files over the network
5	Universal Naming Convention (UNC)	a standard for identifying shared resources over the network. The UNC path uses double backslashes to precede the computer name then single backslashes to separate the shared path to the resource. UNC names do not use drive letters to identify resources.
6	Permissions	the rights granted to a user or group to access a resource
7	New Technology File System (NTFS)	the primary Windows file system. NTFS includes its own set of file/folder permissions.
8	Line Print Terminal (LPT)	the logical named assigned to the parallel port on a PC. Parallel ports were typically used to attach local printers, although they have become obsolete and replaced with USB.
9	Universal Serial Bus	a type of serial interface that is used to connect peripheral devices to a PC

	Key Term	Description
	(USB)	
10	HyperText Markup Language (HTML)	the language used for documents on the World Wide Web
11	HyperText Transfer Protocol (HTTP)	the protocol used to transfer web files over the Internet. HTTP uses TCP port 80 for initiating requests.
12	Universal Resource Locator (URL)	the named address of a resource on the Internet
13	Domain Name System (DNS)	the protocol used to map hostnames and domain names into IP address on the Internet. DNS uses UDP port 53 for initiating requests.
14	File Transfer Protocol (FTP)	the protocol used to send and receive files from another computer on the Internet. FTP uses TCP port 21 to set up the exchange process and TCP port 20 to exchange the actual data.
15	Internet Information Services (IIS)	Microsoft's web server

Remote Access – RDP

Introduction
Objective

CompTIA Network + Domain:
Domain 3.0: Network Operations

CompTIA Network + Objective:
Objective 3.4: Given a scenario, use remote access methods.

Overview

This lab will explore Remote Desktop Protocol (RDP) as a remote access method. RDP can be used to remotely connect to a Windows-based PC and navigate the GUI using your local keyboard and mouse. By the end of this lab, students will be able to use the Remote Desktop Connection client on Windows to access a remote machine. Students will also learn how to allow or block RDP using the Windows Firewall as well as allow specific users to connect remotely using RDP.

Outcomes:

In this lab, you will learn to:

1. Connect to another machine using RDP.
2. Configure the Routing and Remote Access (RRAS) server role.
3. Use the built-in VPN client to create a VPN connection.

	Key Term	Description
1	Firewall Exception	an exemption from a specific firewall rule. Exceptions can be made based on IP address or hostname, etc. Exceptions are configured from within the firewall.
2	Firewall Rule	In the firewall, a rule is what is created when we explicitly allow or block a connection. A firewall works based on the rules provided. A single firewall may have dozens, hundreds, or even thousands of rules depending on how much is allowed or blocked.
3	OSI	Open System Interconnect; developed by the International Standards Organization (ISO)
4	Remote Desktop Protocol (RDP)	protocol developed by Microsoft to provide remote control of Windows-based PCs using a graphical interface
5	Terminal Server	In the context of this lab, the terminal server is the remote machine that will be controlled over RDP.
6	Terminal Server Client	software installed on the local machine that provides the function of connecting to the remote machine. Remote Desktop Connection is the default Terminal Server Client for the Remote Desktop Protocol.
7	Terminal Services	used to define the software and features that provide remote access to a computer from the client to the server. Remote Desktop is part of Microsoft's Terminal Services.