

Introduction to Networking

1. Introduction

Networking is the backbone of modern communication systems, enabling computers to connect and exchange information efficiently. This report delves into the fundamentals of networking, covering various aspects such as networking overview, setup considerations, and practical examples of network configurations.

2. Networking Structure

A network encompasses diverse elements including topologies, mediums, and protocols. Topologies such as mesh, tree, and star define the layout of connections between devices, while mediums like ethernet, fiber, coax, and wireless dictate the physical transmission channels. Protocols such as TCP, UDP, and IPX govern data transmission and reception. Understanding these components is crucial for security professionals as network failures can occur silently, potentially leading to oversight of security breaches.

3. Networking Workflow

Setting up a large, flat network may seem straightforward but can pose security risks akin to building a house on an unsecured plot. Segregating networks into smaller segments with Access Control Lists (ACLs) fortifies defense mechanisms, making it harder for attackers to pivot silently. Analogies such as fences, lights, and deterrents illustrate the importance of network segmentation and monitoring for detecting suspicious activities.

4. Addressing

Network addressing plays a pivotal role in directing data packets to their destinations. Understanding subnetting, subnet masks, and IP addressing schemes is essential for designing efficient and secure networks. Misconfigurations, such as setting incorrect subnet masks, can lead to connectivity issues and oversight of network segments, as illustrated by real-world penetration testing oversights.

5. Protocols & Terminology

Protocols govern the rules and conventions for communication between devices on a network. Familiarity with protocols like TCP (Transmission Control Protocol), UDP (User Datagram Protocol), and IPX (Internetwork Packet Exchange) is imperative for troubleshooting and securing network communications.

6. Connection Establishment

Establishing connections between devices involves various stages, including addressing, routing, and data transmission. Understanding the workflow of connection establishment aids in diagnosing connectivity issues and optimizing network performance.

7. My Workstation

This section explores practical considerations for securing individual workstations within a network environment. Topics include network segmentation, firewall configurations, and best practices for workstation security.

The screenshot shows a web browser window with multiple tabs open. The active tab is 'academy.hackthebox.com/module/34/section/297'. The page content is titled 'Fun Story' and describes a physical penetration test during COVID. The text reads: 'During COVID, I was tasked to perform a Physical Penetration Test across state lines, and my state was under a stay at home order. The company I was testing had minimal staff in the office. I decided to purchase an expensive printer and exploited it to put a reverse shell in it, so when it connected to the network, it would send me a shell (remote access). Then I shipped the printer to the company and sent a phishing email thanking the staff for coming in and explaining that the printer should allow them to print or scan things more quickly if they want to bring some stuff home to WFH for a few days. The printer was hooked up almost instantly, and their domain administrator's computer was kind enough to send the printer his credentials!'. Below this, it states: 'If the client had designed a secure network, this attack probably would not have been possible for many reasons:'. A bulleted list follows: '• Printer should not have been able to talk to the internet', '• Workstation should not have been able to communicate to the printer over port 445', and '• Printer should not be able to initiate connections to workstations. In some cases, printer/scanner combinations should be able to communicate to a mail server to email scanned documents.'. At the bottom of the content area, there are two buttons: 'Next →' and 'Mark Complete & Next'. The footer of the page says 'Powered by HACKTHEBOX'. The browser's taskbar at the bottom shows the time as 12:13 on 2 Jun 2024.

academy.hackthebox.com/module/34/section/298

geographical proximity; that is, nodes are individual machines of a company connected to a LAN via router. High-performance routers and high-performance connections based on glass fibers are used, which enable a significantly higher data throughput than the Internet. The transmission speed between two remote nodes is comparable to communication within a LAN.

Internationally operating network operators provide the infrastructure for MANs. Cities wired as Metropolitan Area Networks can be integrated supra-regionally in Wide Area Networks (WAN) and internationally in Global Area Networks (GAN).

PAN / WPAN

Modern end devices such as smartphones, tablets, laptops, or desktop computers can be connected ad hoc to form a network to enable data exchange. This can be done by cable in the form of a Personal Area Network (PAN).

The wireless variant Wireless Personal Area Network (WPAN) is based on Bluetooth or Wireless USB technologies. A wireless personal area network that is established via Bluetooth is called Piconet. PANs and WPANs usually extend only a few meters and are therefore not suitable for connecting devices in separate rooms or even buildings.

In the context of the Internet of Things (IoT), WPANs are used to communicate control and monitor applications with low data rates. Protocols such as Insteon, Z-Wave, and ZigBee were explicitly designed for smart homes and home automation.

← Previous Next → [Mark Complete & Next](#)

Powered by HACKTHEBOX

academy.hackthebox.com/module/34/section/299

Daisy Chain Topology

```
graph TD; A[Host A] --- B[Host B]; B --- C[Host C]; C --- D[Host D]; D --- E[Host E];
```

← Previous Next → [Mark Complete & Next](#)

Powered by HACKTHEBOX

How to Install and R... x HG8145V x Preparing Your Dow... x ChatGPT x Introduction to Net... x CSA2-2024: Assignm... x Word | Microsoft 36... x

academy.hackthebox.com/module/34/section/300

Host B

HTTP Request

(Non-) Transparent Proxy

All these proxy services act either **transparently** or **non-transparently**.

With a **transparent proxy**, the client doesn't know about its existence. The transparent proxy intercepts the client's communication requests to the Internet and acts as a substitute instance. To the outside, the transparent proxy, like the non-transparent proxy, acts as a communication partner.

If it is a **non-transparent proxy**, we must be informed about its existence. For this purpose, we and the software we want to use are given a special proxy configuration that ensures that traffic to the Internet is first addressed to the proxy. If this configuration does not exist, we cannot communicate via the proxy. However, since the proxy usually provides the only communication path to other networks, communication to the Internet is generally cut off without a corresponding proxy configuration.

Previous

Next

Mark Complete & Next

Powered by HACKTHEBOX

How to Install and R... x HG8145V x Preparing Your Dow... x ChatGPT x Introduction to Net... x CSA2-2024: Assignm... x Word | Microsoft 36... x

academy.hackthebox.com/module/34/section/301

process continues to the **Physical Layer** or **Network Layer**, where the data is transmitted to the receiver. The receiver reverses the process and unpacks the data on each layer with the header information. After that, the application finally uses the data. This process continues until all data has been sent and received.

Packet Transfer

The diagram illustrates the packet transfer process through the seven layers of the OSI model. On the left, the 'Sender' side shows data being processed from the top layer (Application) down to the bottom layer (Physical). The layers are: Application (Data), Presentation (Data), Session (Data), Transport (Data), Network (IP), Data Link (MAC), and Physical (Binary Transmission). On the right, the 'Receiver' side shows the reverse process, where data is received from the Physical layer and moves up through the layers to the Application layer. The layers are: Physical (Binary Transmission), Data Link (MAC), Network (IP), Transport (TCP), Session (Data), Presentation (Data), and Application (Data). In the center, the data is shown as a 'Packet' being transmitted over the 'Ethernet' network. The packet structure is shown as a sequence of layers: Data, TCP, IP, and MAC, which are encapsulated into a 'Frame' and then a 'Packet' before being sent over the 'Ethernet' network.

For us, as penetration testers, both reference models are useful. With **TCP/IP**, we can quickly understand how the entire connection is established, and with **ISO**, we can take it apart piece by piece and analyze it in detail. This often happens when we can listen to and intercept specific network traffic. We then have to analyze this traffic accordingly, going into more detail in the **Network Traffic Analysis** module. Therefore, we should familiarize ourselves with both reference models and understand and internalize them in the best possible way.

Previous

Next

Mark Complete & Next

Powered by HACKTHEBOX

How to Install and R... x HG8145V x Preparing Your Dow... x ChatGPT x Introduction to Net... x CSA2-2024: Assignm... x Word | Microsoft 36... x

academy.hackthebox.com/module/34/section/303

1. Layer Physical

Network Card

Authentication Protocols

TCP/UDP Connections

Cryptography

The most important tasks of TCP/IP are:

| Task | Protocol | Description |
|----------------------|----------|--|
| Logical Addressing | IP | Due to many hosts in different networks, there is a need to structure the network topology and logical addressing. Within TCP/IP, IP takes over the logical addressing of networks and nodes. Data packets only reach the network where they are supposed to be. The methods to do so are network classes , subnetting , and CIDR . |
| Routing | IP | For each data packet, the next node is determined in each node on the way from the sender to the receiver. This way, a data packet is routed to its receiver, even if its location is unknown to the sender. |
| Error & Control Flow | TCP | The sender and receiver are frequently in touch with each other via a virtual connection. Therefore control messages are sent continuously to check if the connection is still established. |
| Application Support | TCP | TCP and UDP ports form a software abstraction to distinguish specific applications and their communication links. |
| Name Resolution | DNS | DNS provides name resolution through Fully Qualified Domain Names (FQDN) in IP addresses, enabling us to reach the desired host with the specified name on the internet. |

Previous

Next

Mark Complete & Next

My Workstation

OFFLINE

Start Instance

1 / 1 spawns left

Powered by HACKTHEBOX

How to Install and R... x HG8145V x Preparing Your Dow... x ChatGPT x Introduction to Net... x CSA2-2024: Assignm... x Word | Microsoft 36... x

academy.hackthebox.com/module/34/section/302

2. Data Link

1. Physical

The central task of layer 2 is to enable reliable and error-free transmissions on the respective medium. For this purpose, the bitstreams from layer 1 are divided into blocks or frames.

The transmission techniques used are, for example, electrical signals, optical signals, or electromagnetic waves. Through layer 1, the transmission takes place on wired or wireless transmission lines.

The layers 2-4 are **transport oriented**, and the layers 5-7 are **application oriented** layers. In each layer, precisely defined tasks are performed, and the interfaces to the neighboring layers are precisely described. Each layer offers services for use to the layer directly above it. To make these services available, the layer uses the services of the layer below it and performs the tasks of its layer.

If two systems communicate, all seven layers of the **OSI** model are run through at least **twice**, since both the sender and the receiver must take the layer model into account. Therefore, a large number of different tasks must be performed in the individual layers to ensure the communication's security, reliability, and performance.

When an application sends a packet to the other system, the system works the layers shown above from layer 7 down to layer 1, and the receiving system unpacks the received packet from layer 1 up to layer 7.

Previous

Next

Mark Complete & Next

IPv4 Addresses

Subnetting

MAC Addresses

IPv6 Addresses

Protocols & Terminology

Networking Key Terminology

Common Protocols

Wireless Networks

Virtual Private Networks

Vendor Specific Information

Connection Establishment

Key Exchange Mechanisms

Authentication Protocols

TCP/UDP Connections

Cryptography

My Workstation

The screenshot shows a web browser window with multiple tabs. The active tab is 'academy.hackthebox.com/module/34/section/1879'. The page content discusses network spoofing techniques. It states that one does not need to establish a connection before sending data. It mentions that using `traceroute` with UDP results in 'Destination Unreachable' and 'Port Unreachable' messages. The section is titled 'Blind Spoofing' and describes it as a data manipulation attack where false information is sent. It gives an example of sending a TCP packet with false source/destination ports and a false Initial Sequence Number (ISN). It explains that the ISN is a field in the TCP header used to specify the sequence number of the first packet. This attack is used to disrupt connections or intercept information.

not need to establish a connection between the sender and the receiver before sending data. Instead, the data is sent directly to the target host without any prior connection.

When `traceroute` is used with UDP, we will receive a **Destination Unreachable** and **Port Unreachable** message when the UDP datagram packet reaches the target device. Generally, UDP packets are sent using `traceroute` on Unix hosts.

Blind Spoofing

Blind spoofing, is a method of data manipulation attack in which an attacker sends false information on a network without seeing the actual responses sent back by the target devices. It involves manipulating the IP header field to indicate false source and destination addresses. For example, we send a TCP packet to the target host with false source and destination port numbers and a false **Initial Sequence Number (ISN)**. The **ISN** is a field in the TCP header that is used to specify the sequence number of the first TCP packet in a connection. The ISN is set by the sender of a TCP packet and sent to the receiver in the TCP header of the first packet. This can cause the target host to establish a connection with us without receiving the connection.

This attack is commonly used to disrupt the integrity of network connections or to break connections between network devices. It can also be used to monitor network traffic or to intercept information sent by network devices.

Navigation buttons: Previous, Next, Mark Complete & Next.

Powered by HACKTHEBOX

The screenshot shows a web browser window with multiple tabs. The active tab is 'academy.hackthebox.com/module/34/section/2026'. The page content is a table of cipher modes. A 'Spectacle' screenshot tool window is overlaid on the page, showing a list of capture settings.

| Cipher Mode | Description |
|----------------------------------|--------------------------------|
| Electronic Code Book (ECB) mode | ECB m Furthe clear- - |
| Cipher Block Chaining (CBC) mode | CBC m default |
| Cipher Feedback (CFB) mode | CFB m encryp BitLoa |
| Output Feedback (OFB) mode | OFB m is cons PKCS t |
| Counter (CTR) mode | CTR m real-ti |
| Galois/Counter (GCM) mode | GCM i: commu |

Each mode has its characteri
depends on the application's

Navigation buttons: Previous, Finish.

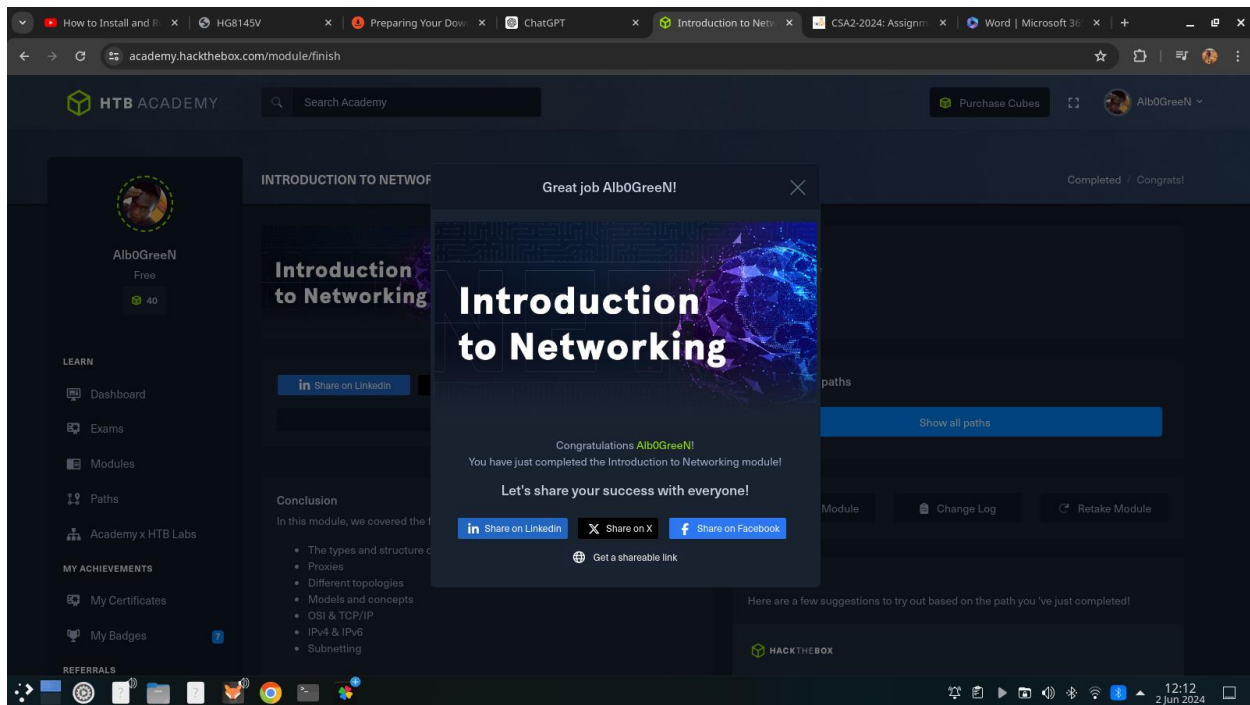
Powered by HACKTHEBOX

Spectacle Screenshot Tool Settings:

- Take a new screenshot:
 - Rectangular Region
 - Full Screen
 - Active Window
 - Window Under Cursor
- Capture Settings:
 - ☐ Include mouse pointer
 - ☒ Include window titlebar and borders
 - ☐ Capture the current pop-up only
 - ☐ Quit after manual Save or Copy
 - ☐ Capture on click
- Delay: No Delay

cs-sa07-24019

John_Mbithi_Mutave



Shareable link - <https://academy.hackthebox.com/achievement/1296187/34>

Conclusion

In conclusion, mastering the fundamentals of networking is essential for security professionals and network administrators alike. By understanding the structure, workflow, and protocols of networks, individuals can design, deploy, and maintain robust and secure communication infrastructures.