TryHackMe — Networking Essentials | Cyber Security 101 (THM)

Z3pH7 · Follow

9 min read · Oct 24, 2024

Listen Share More

Hey everyone! TryHackMe just announced the **NEW Cyber Security 101** learning path, and there are tons of giveaways this time! This article might help you out, but I've kept the summary short for easy understanding. Enjoy hacking!

Introduction

Have you ever wondered how your computer can dynamically configure its network settings when you turn it on or connect it to a new network? Have you ever wanted to know how many devices and countries your packets passed through before reaching their destination? Are you curious how all your home devices can access the Internet even though your ISP gives you a single IP address?

If you want to know the answers to these questions, among others, then this room is for you.

This room is the second room in a series of four rooms about computer networking:

- Networking Concepts
- Networking Essentials (this room)
- Networking Core Protocols
- Networking Secure Protocols

Learning Prerequisites

To benefit from this room, we recommend that you know the following:

- ISO OSI model and layers
- TCP/IP model and layers
- Ethernet, IP, and TCP protocols

In other words, starting this room after Networking Concepts is the recommended approach.

Learning Objectives

The objective of this room is to teach you about various standard protocols and technologies that glue things together:

- Dynamic Host Configuration Protocol (DHCP)
- Address Resolution Protocol (ARP)

- Network Address Translation (NAT)
- Internet Control Message Protocol (ICMP)
- Ping
- Traceroute

DHCP: Give Me My Network Settings

DHCP automates the network configuration process, such as setting up an IP address, Subnet Mask, Default Gateway, and DNS Server, so users don't need to manually configure these settings every time they connect to a new network. This helps avoid IP address conflicts and is particularly useful for mobile devices like smartphones and laptops.

Example: When you connect to a coffee shop's Wi-Fi, your device automatically requests an IP address from the shop's DHCP server. The server responds with an available IP address and necessary network settings.

DHCP Process (DORA):

- **DHCP Discover**: The client sends out a DHCPDISCOVER broadcast message to find a DHCP server.
- **DHCP Offer**: The DHCP server responds with a DHCPOFFER containing an available IP address.
- **DHCP Request**: The client replies with a DHCPREQUEST to accept the offered IP address.
- **DHCP Acknowledge**: The server sends a DHCPACK to confirm the assignment of the IP address and other settings(DHCP).

The following packet capture shows the four steps explained above. In this example, the client gets the address `192.168.66.133`.

```
user@TryHackMe$ tshark -r DHCP-G5000.pcap -n
    1   0.000000      0.0.0.0 → 255.255.255.255 DHCP 342 DHCP Discover - Transa
    2   0.013904 192.168.66.1 → 192.168.66.133 DHCP 376 DHCP Offer    - Transac
```

```
3   4.115318      0.0.0.0 → 255.255.255.255 DHCP 342 DHCP Request  - Transa
4   4.228117 192.168.66.1 → 192.168.66.133 DHCP 376 DHCP ACK      - Transac
```

- **tshark:** This is the command to start the TShark program.
- **-r DHCP-G5000.pcap:** The `-r` option tells TShark to read from a specified file, in this case, `DHCP-G5000.pcap`, which is a packet capture file that logs network traffic.
- **-n:** The `-n` option prevents TShark from resolving hostnames or converting IP addresses to domain names. This makes the output faster by not requiring DNS lookups.

Benefits of DHCP:

- Automates network configuration, saving time.
- Prevents IP conflicts when multiple devices are connected.
- Especially useful in dynamic environments like public Wi-Fi.

Answer the questions below

> *How many steps does DHCP use to provide network configuration?*

Answer: 4

> *What is the destination IP address that a client uses when it sends a DHCP Discover packet?*

Answer: *255.255.255.255*

> *What is the source IP address a client uses when trying to get IP network configuration over DHCP?*

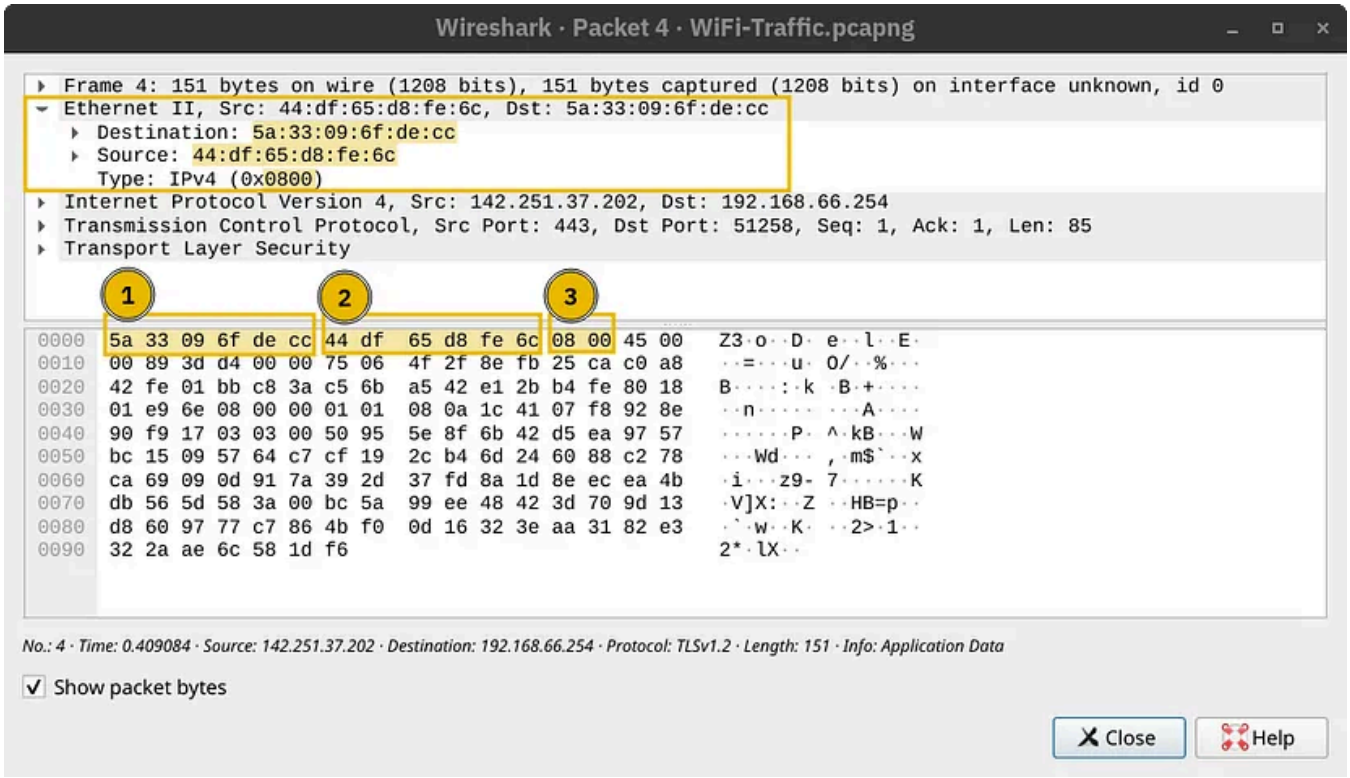
Answer: 0.0.0.0

ARP: Bridging Layer 3 Addressing to Layer 2 Addressing

ARP is a protocol used to map a device's IP address to its MAC (Media Access Control) address. When a device wants to communicate with another device on the same local network, it needs the MAC address to create a data link layer frame.

As a reminder, in the screenshot below, we see an IP packet within an Ethernet frame. The Ethernet frame header contains:

- Destination MAC address
- Source MAC address
- Type (IPv4 in this case)



Example: If your computer wants to send data to a device with IP address 192.168.66.1 but doesn't know the MAC address, it will send an ARP Request. The device with the matching IP will respond with an ARP Reply, including its MAC address.

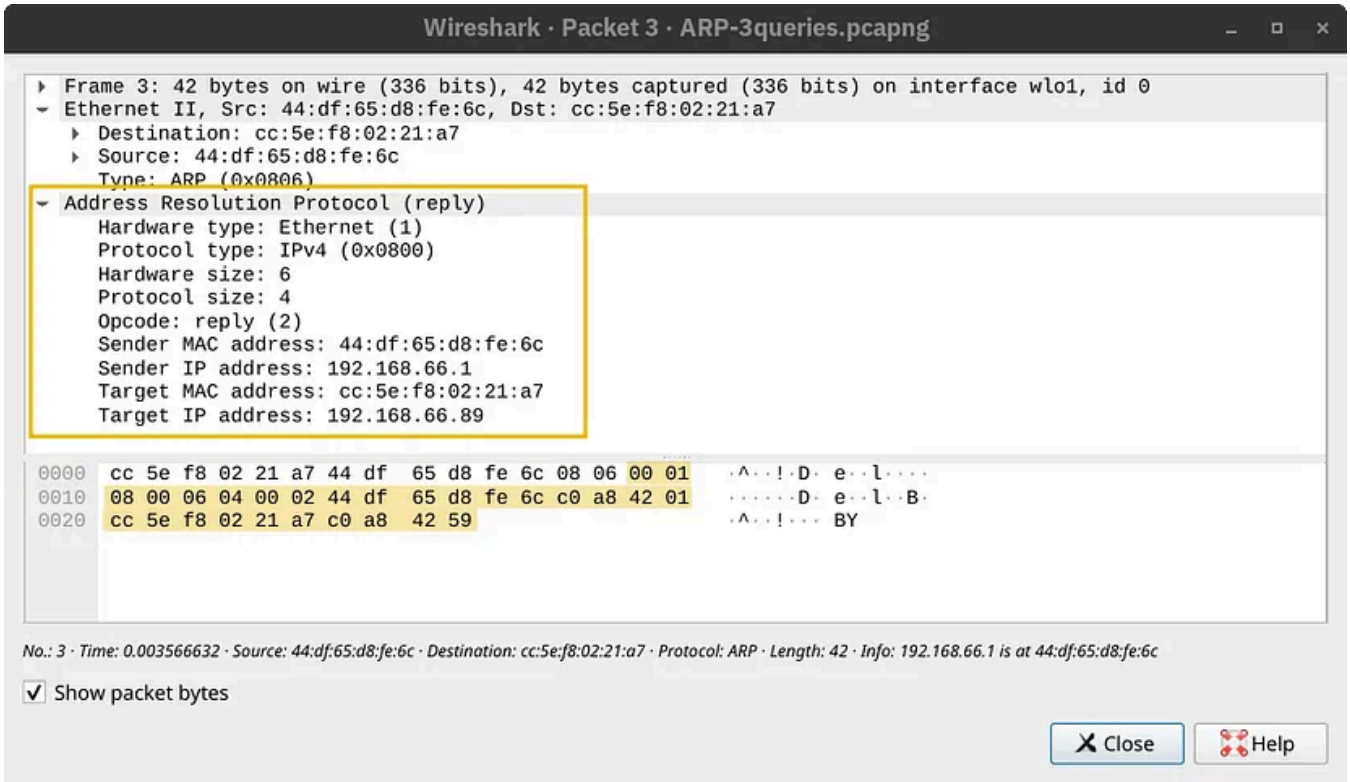
```
user@TryHackMe$ tshark -r arp.pcapng -Nn
    1 0.000000000 cc:5e:f8:02:21:a7 → ff:ff:ff:ff:ff:ff ARP 42 Who has 192.168.
    2 0.003566632 44:df:65:d8:fe:6c → cc:5e:f8:02:21:a7 ARP 42 192.168.66.1 is
```

If we use `tcpdump`, the packets will be displayed differently. It uses the terms ARP **Request** and ARP **Reply**. For your information, the output is shown in the terminal below.

```
user@TryHackMe$ tcpdump -r arp.pcapng -n -v
17:23:44.506615 ARP, Ethernet (len 6), IPv4 (len 4), Request who-has 192.168.66
17:23:44.510182 ARP, Ethernet (len 6), IPv4 (len 4), Reply 192.168.66.1 is-at 4
```

- **tcpdump**: The command to run tcpdump, which is used to capture or analyze network traffic.
- **-r arp.pcapng**: The `-r` option specifies the packet capture file (`arp.pcapng`) to read from.
- **-n**: Just like in TShark, the `-n` option disables DNS lookups, preventing IP addresses from being resolved into hostnames.
- **-v**: This enables **verbose** mode, meaning more detailed output. It will show extra information about the packets, like packet size, and detailed protocol information.

An ARP Request or ARP Reply is not encapsulated within a UDP or even IP packet; it is encapsulated directly within an Ethernet frame. The following ARP Reply shows this.



ARP Process:

- **ARP Request**: The device sends a broadcast message asking for the MAC address associated with the known IP address.
- **ARP Reply**: The device that has the IP address responds with its MAC address (DHCP).

Answer the questions below

> *What is the destination MAC address used in an ARP Request?*

Answer: ff:ff:ff:ff:ff:ff

> *In the example above, what is the MAC address of* `192.168.66.1` *?*

Answer: 44:df:65:d8:fe:6c

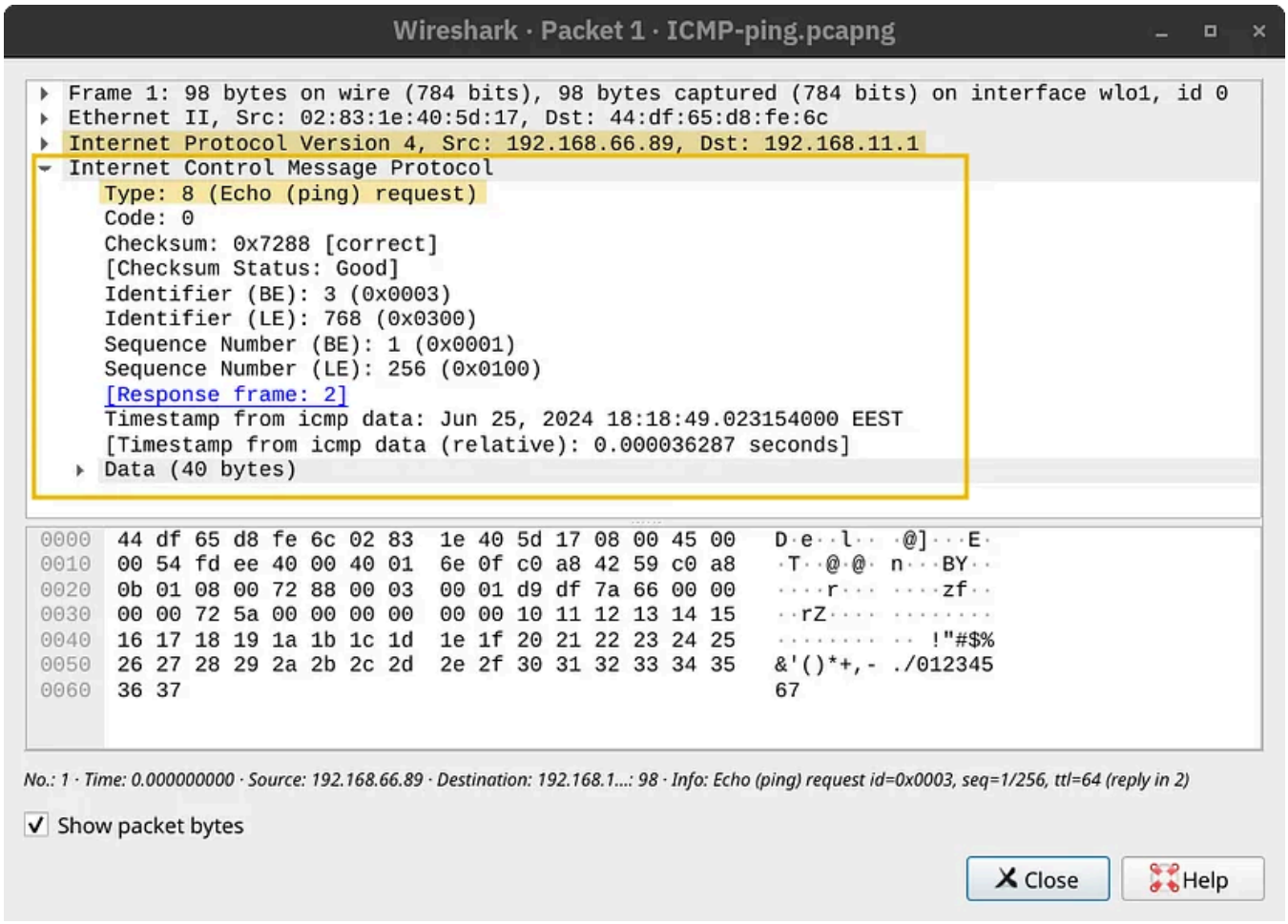
ICMP: Troubleshooting Networks

ICMP is primarily used for network diagnostics and troubleshooting. Two common commands that rely on ICMP are:

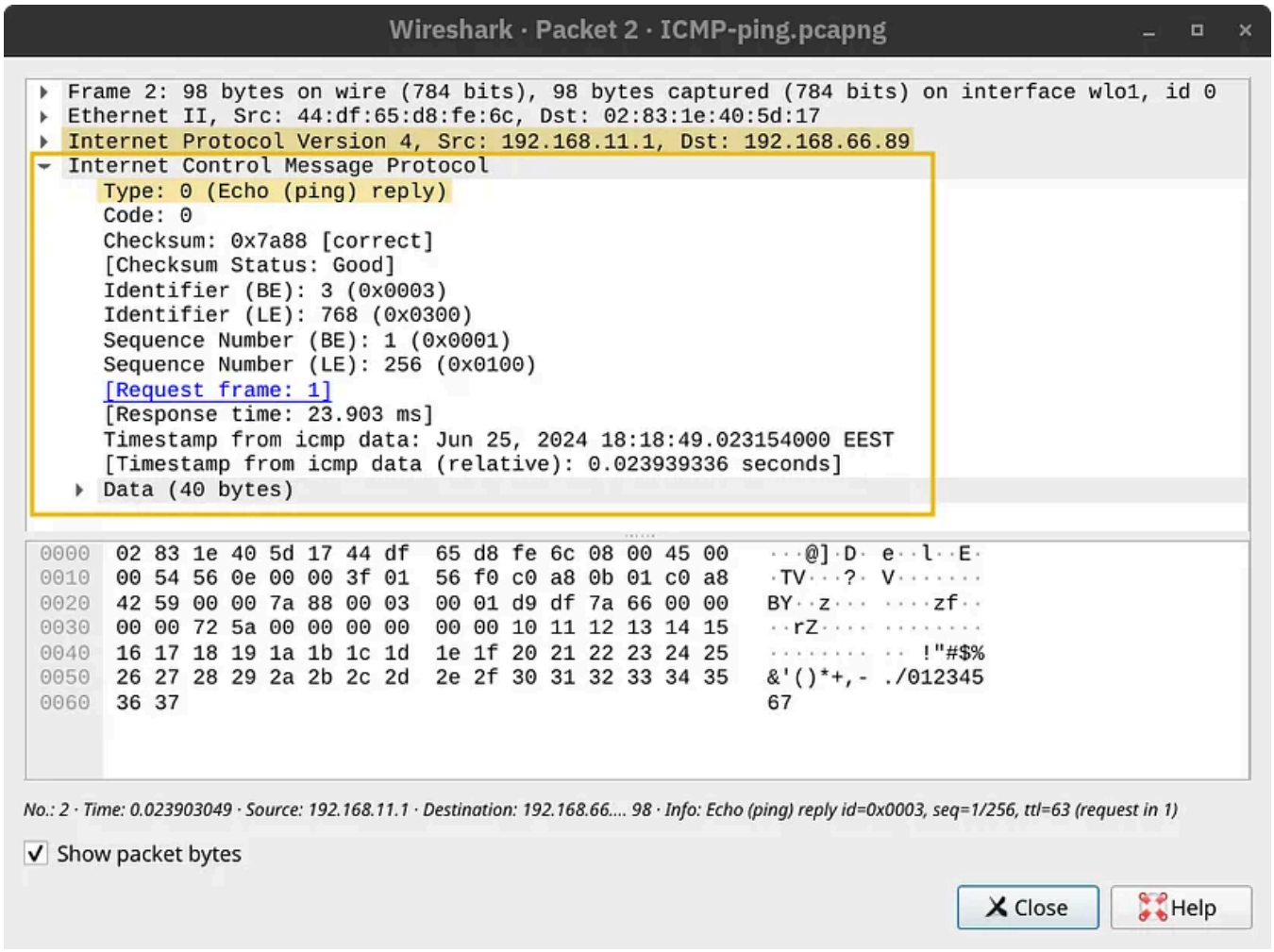
- **Ping**: Tests the connectivity between your device and a target system. It sends an ICMP Echo Request and waits for an ICMP Echo Reply.
- **Traceroute**: Finds the path data takes from your device to a target system by identifying each router along the way.

Ping Example:
You can use the `ping` command to check if a server is online. By typing `ping example.com`, the system sends ICMP Echo Requests to the server, and if the server is reachable, it replies with ICMP Echo Replies(DHCP).

The `ping` command sends an ICMP Echo Request (ICMP Type `8`). The screenshot below shows the ICMP message within an IP packet.



The computer on the receiving end responds with an ICMP Echo Reply (ICMP Type `0`).



Many things might prevent us from getting a reply. In addition to the possibility of the target system being offline or shut down, a firewall along the path might block the necessary packets for `ping` to work. In the example below, we used `-c 4` to tell the `ping` command to stop after sending four packets.

```
user@TryHackMe$ ping 192.168.11.1 -c 4
PING 192.168.11.1 (192.168.11.1) 56(84) bytes of data.
64 bytes from 192.168.11.1: icmp_seq=1 ttl=63 time=11.2 ms
64 bytes from 192.168.11.1: icmp_seq=2 ttl=63 time=3.81 ms
64 bytes from 192.168.11.1: icmp_seq=3 ttl=63 time=3.99 ms
64 bytes from 192.168.11.1: icmp_seq=4 ttl=63 time=23.4 ms
--- 192.168.11.1 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3003ms
rtt min/avg/max/mdev = 3.805/10.596/23.366/7.956 ms
```

- **ping**: The command that sends an ICMP Echo Request to test network connectivity.
- **192.168.11.1**: The target IP address of the device you are trying to reach.

- **-c 4:** The `-c` option specifies the number of ping requests to send. In this case, it will send 4 packets and stop.

Traceroute Example:
If you want to find out the path your data takes to reach `example.com`, the `traceroute` command will show each router the data passes through.

The Internet protocol has a field called Time-to-Live (TTL) that indicates the maximum number of routers a packet can travel through before it is dropped. The router decrements the packet's TTL by one before it sends it across. When the TTL reaches zero, the router drops the packet and sends an ICMP Time Exceeded message (ICMP Type `11`). (In this context, "time" is measured in the number of routers, not seconds.)

```
user@TryHackMe$ traceroute example.com
traceroute to example.com (93.184.215.14), 30 hops max, 60 byte packets
 1  _gateway (192.168.66.1)  4.414 ms  4.342 ms  4.320 ms
 2  192.168.11.1 (192.168.11.1)  5.849 ms  5.830 ms  5.811 ms
 3  100.104.0.1 (100.104.0.1)  11.130 ms  11.111 ms  11.093 ms
 4  10.149.1.45 (10.149.1.45)  6.156 ms  6.138 ms  6.120 ms
 5  * * *
 6  * * *
 7  * * *
 8  172.16.48.1 (172.16.48.1)  5.667 ms  8.165 ms  6.861 ms
 9  ae81.edge4.Marseille1.Level3.net (212.73.201.45)  50.811 ms  52.857 ms 213.
10  NTT-level3-Marseille1.Level3.net (4.68.68.150)  93.351 ms  79.897 ms  79.80
11  ae-9.r20.parsfr04.fr.bb.gin.ntt.net (129.250.3.38)  62.935 ms  62.908 ms  6
12  ae-14.r21.nwrknj03.us.bb.gin.ntt.net (129.250.4.194)  141.816 ms  141.782 m
13  ae-1.a02.nycmny17.us.bb.gin.ntt.net (129.250.3.17)  145.786 ms ae-1.a03.nyc
14  ce-0-3-0.a02.nycmny17.us.ce.gin.ntt.net (128.241.1.14)  148.692 ms ce-3-3-0
15  ae-66.core1.nyd.edgecastcdn.net (152.195.69.133)  141.100 ms ae-65.core1.ny
16  93.184.215.14 (93.184.215.14)  140.574 ms  140.543 ms  140.514 ms
17  93.184.215.14 (93.184.215.14)  140.488 ms  139.397 ms  141.854 ms
```

The traversed route might change as we rerun the command.

Answer the questions below

> *Using the example images above, how many bytes were sent in the echo (ping) request?*

Answer: 40

> *Which IP header field does the `traceroute` command require to become zero?*

Answer: TTL

Routing

Routing protocols help routers determine the best path for data to travel within a network or across the internet. Key routing protocols include:

- **OSPF (Open Shortest Path First):** Finds the shortest path for data transmission by sharing information about the network topology.
- **EIGRP (Enhanced Interior Gateway Routing Protocol):** A Cisco proprietary protocol that helps routers determine the best path using various metrics.
- **BGP (Border Gateway Protocol):** The main routing protocol of the internet, enabling ISPs to exchange routing information.
- **RIP (Routing Information Protocol):** A simple routing protocol that finds the route with the fewest hops between devices, often used in smaller networks (DHCP).

Example:
OSPF is used in enterprise networks to calculate the shortest and most efficient path for data transmission between devices on different subnets.

Answer the questions below

> *Which routing protocol discussed in this task is a Cisco proprietary protocol?*

Answer: EIGRP

NAT

NAT allows multiple devices on a private local network to share a single public IP address to access the internet. This helps conserve public IP addresses, which are limited in number under the IPv4 system.

Example: In an office with 50 computers, all the devices can access the internet through a single public IP address using NAT. The router keeps track of which internal device is making each request and translates it to the public IP for communication with external servers(DHCP).

In the diagram below, multiple devices access the Internet via a router that supports NAT. The router maintains a table that maps the internal IP address and port number with its external IP address and port number. For instance, the laptop might establish a connection with some web server. From the laptop perspective, the connection is initiated from its IP address `192.168.0.129` from TCP source port number `15401`; however, the web server will see this same connection as being established from `212.3.4.5` and TCP port number `19273`, as shown in the translation table. The router does this address translation seamlessly.

Answer the questions below

> *In the network diagram above, what is the public IP that the phone will appear to use when accessing the Internet?*

Answer: 212.3.4.5

> *Assuming that the router has infinite processing power, approximately speaking, how many **thousand** simultaneous TCP connections can it maintain?*

Answer: 65

Closing Notes

This room introduced various protocols that we constantly use directly or indirectly. We have covered ICMP, DHCP, ARP, NAT, and routing. Although we use the Internet daily without coming across most of this room's acronyms, these protocols are the foundation for a functional network.

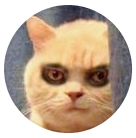
Answer the questions below

> *Click on the **View Site** button to access the related site. Please follow the instructions on the site to obtain the flag.*

Answer: THM{computer_is_happy}

Thank You!

Tryhackme | Tryhackme Walkthrough | Cyber Security 101 | Networking



Follow

Written by Z3pH7

234 Followers · 7 Following

Cybersecurity | Pentester | Student

Responses (1)

What are your thoughts?

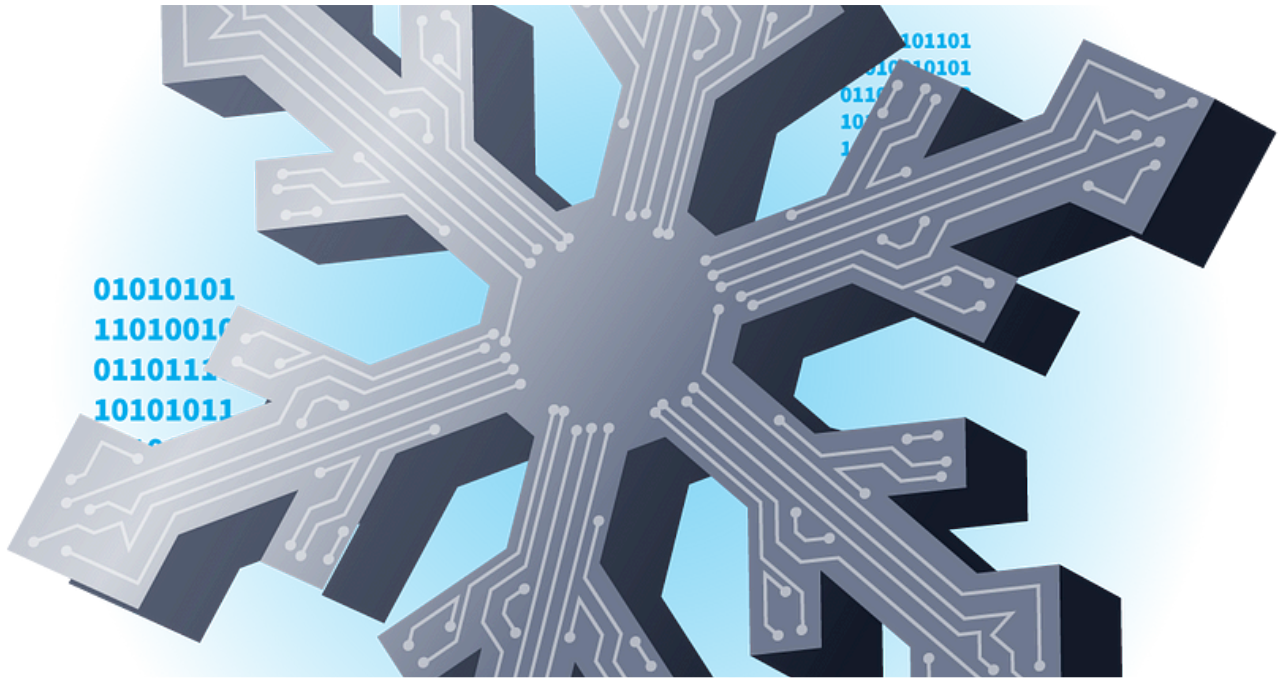
Respond

Sai kiran he/him
2 months ago

Productive

Reply

More from Z3pH7



Z3pH7

TryHackMe—Hashing Basics | Cyber Security 101 (THM)

Hey everyone! TryHackMe just announced the NEW Cyber Security 101 learning path, and there are tons of giveaways this time! This article...

Oct 29, 2024 101 1

Z3pH7

TryHackMe—Networking Core Protocols | Cyber Security 101 (THM)

Hey everyone! TryHackMe just announced the NEW Cyber Security 101 learning path, and there are tons of giveaways this time! This article...

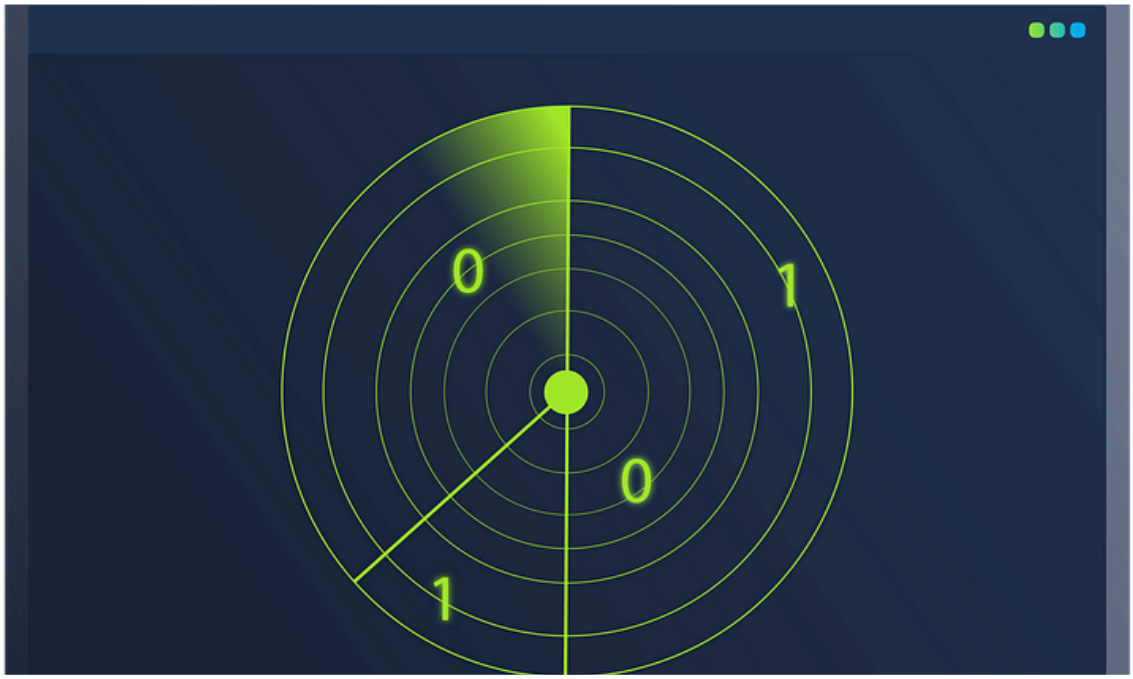
Oct 25, 2024 11

Z3pH7

TryHackMe—Public Key Cryptography Basics | Cyber Security 101 (THM)

Hey everyone! TryHackMe just announced the NEW Cyber Security 101 learning path, and there are tons of giveaways this time! This article...

Oct 28, 2024 75



Z3pH7

TryHackMe—Nmap: The Basics | Cyber Security 101 (THM)

Hey everyone! TryHackMe just announced the NEW Cyber Security 101 learning path, and there are tons of giveaways this time! This article...

Oct 25, 2024 4

See all from Z3pH7

Recommended from Medium

In T3CH by Axoloth

TryHackMe | Training Impact on Teams | WriteUp

Discover the impact of training on teams and organisations

Nov 5, 2024 60

rutbar

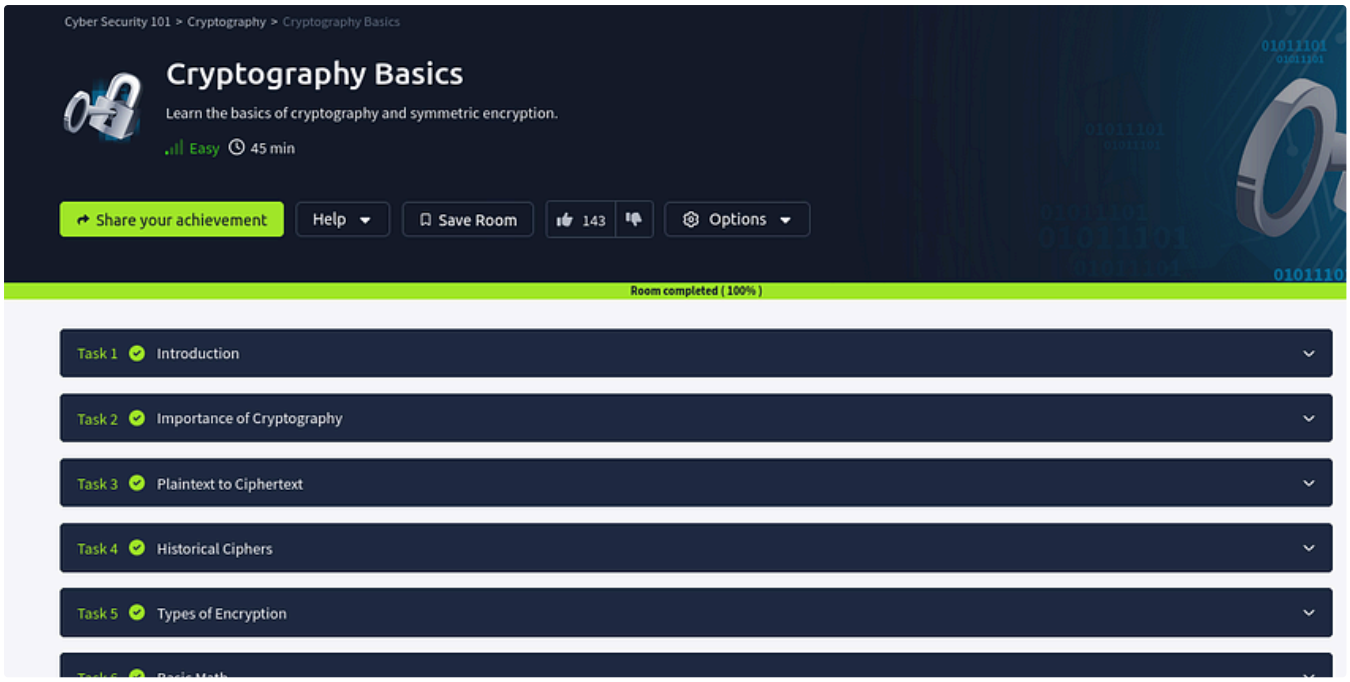
TryHackMe—CAPA: The Basics | Cyber Security 101 (THM)

Tool Overview: How CAPA Works

Lists

Business 101

25 stories · 1334 saves

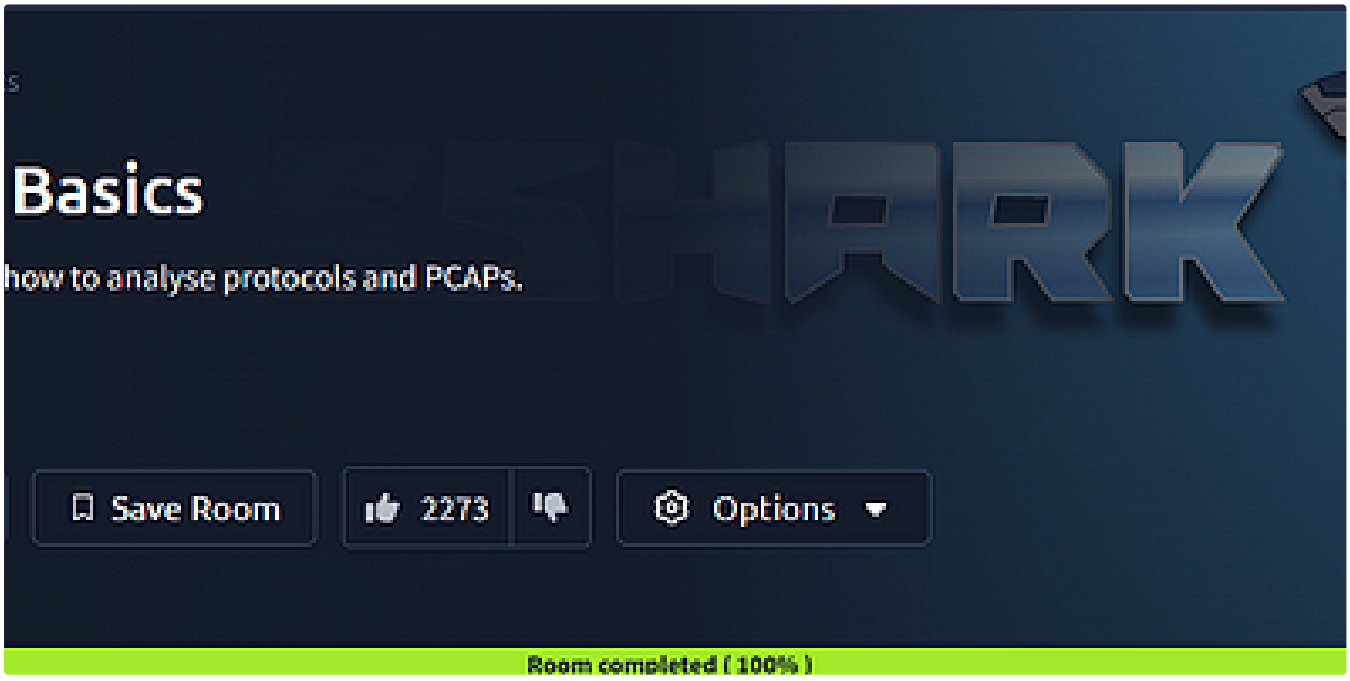


Jawstar

Cryptography Basics | Tryhackme Write Up | By jawstar

CYBER SECURITY 101

Oct 29, 2024 2

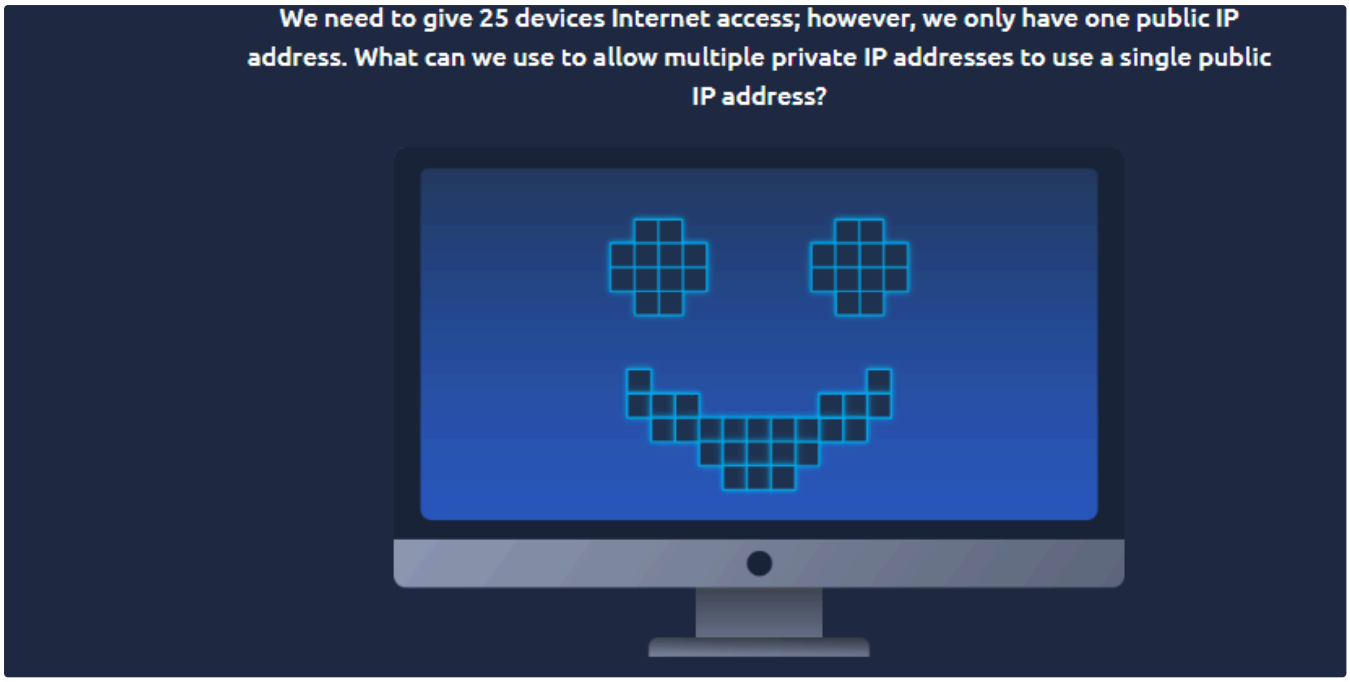


TRedEye

Wireshark: The Basics — Tryhackme Walkthrough

Tryhackme Walkthrough

Oct 29, 2024 50

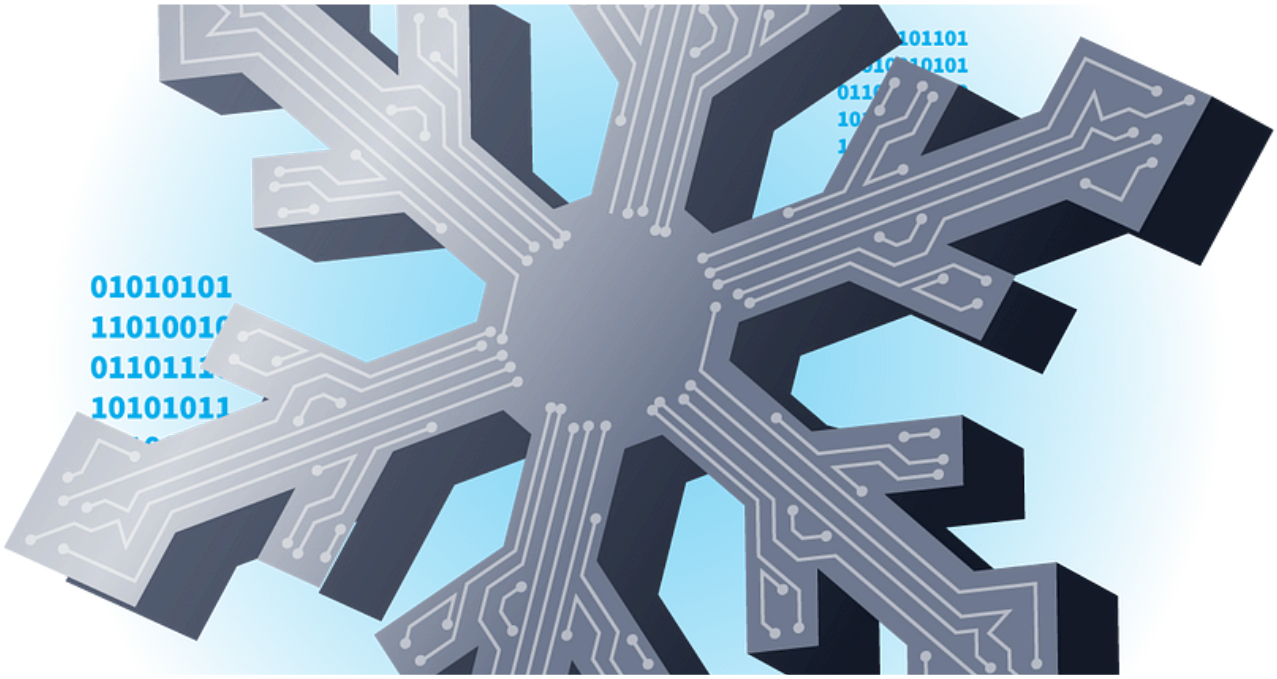


embossdotar

TryHackMe—Networking Essentials—Writeup

Key points: Networking protocols | DHCP | ARP | NAT | ICMP | Ping | Traceroute. Networking Essentials by awesome TryHackMe! 🎉

Oct 22, 2024 1



Z3pH7

TryHackMe—Hashing Basics | Cyber Security 101 (THM)

Hey everyone! TryHackMe just announced the NEW Cyber Security 101 learning path, and there are tons of giveaways this time! This article...

Oct 29, 2024 101 1

See more recommendations