****

**Concordia Institute for Information Systems Engineering (CIISE)**

**Concordia University**

**INSE 6961 SEMINAR - Report on Ethical Hacking**

Submitted to: **PROFESSOR AYDA BASYOUNI**

Submitted by:

Name: **Bala Krishna Yadav Kunati**

Student ID: **40292128**

Email ID: [**kunatibala101@gmail.com**](mailto:kunatibala101@gmail.com)

**TABLE OF CONTENTS:**

1. Introduction……………………………………………………………………………… 3

2. Setting up a hacking lab…………………………………………………………………. 3

3. Virtual Machine Installation……………………………………………………………... 4

4. Linux Basics……………………………………………………………………………... 4

5. Network Hacking………………………………………………………………………... 5

6. Pre-Connection Attacks…………………………………………………………………. 5

7. Understanding Networks………………………………………………………………… 5

8. MAC Address……………………………………………………………………………. 6

9. Switching to Monitor Mode……………………………………………………………... 6

10.Packet sniffing using Airodump-NG…………………………………………………… 7

11. Deauthentication Attacks………………………………………………………………. 7

12. Limitations of Deauthentication Attacks……………………………………………….. 8

13. Gaining Access…………………………………………………………………………. 8

14. Breaking WEP Encryption……………………………………………………………... 8

15. Exploiting WEP with Aircrack-NG……………………………………………………. 9

16. Breaking WPA and WPA2 Encryption………………………………………………… 10

17. Limitations……………………………………………………………………………... 11

18. Post-Connection Attacks……………………………………………………………….. 11

19. Network Discovery with NetDiscover…………………………………………………. 11

20. Zenmap Quick Scan Plus………………………………………………………………. 12

21. Security Measures……………………………………………………………………… 12

22. Conclusion……………………………………………………………………………... 13

23. References……………………………………………………………………………… 13

**List of Figures**

Figure 1 – Basic Network Structure………………………………………………………... 5

Figure 2 – Output of iwconfig command…………………………………………………... 6

Figure 3 – Cracking WPA/WP2 password…………………………………………………. 11

Figure 4 – ARP Request……………………………………………………………………. 12

**Introduction:**

Ethical Hacking is an important aspect of Cybersecurity, which enables the organizations to identify the vulnerabilities and defend their systems against various attacks. Through the *Learn Ethical Hacking from Scratch 2024* course by Zaid on Udemy, I have gained a practical and thorough understanding of the principles of Cybersecurity, along with a strong theoretical foundation. This has helped me in acquiring necessary knowledge and skills to think in the perspective of a hacker in responsibly uncovering system vulnerabilities.

In this course, hacking is defined as gaining unauthorized access to systems or data. And hackers are classified into three categories based on their intentions and goals. They are classified as follows:

* **Black-Hat Hackers:** These are the individuals or a group of organizations, who exploit systems illegally for personal or financial gain
* **White-Hat Hackers:** These are the security professionals, who test systems with prior permission, to identify vulnerabilities and enhance their security posture.
* **Grey-Hat Hackers:** These hackers are people of good intent, but without permissions test the security of systems and notify the administrators of vulnerabilities, but not exploit or damage the systems.

The increasing dangers of Cyberattacks has resulted in a huge demand for ethical hackers. Organizations such as Google, Facebook and Microsoft actively employ ethical hackers and provide them with bug bounty programs to enhance their overall security posture.

The course is divided into four parts:

1. **Network Hacking:** Understanding network communication, exploiting vulnerabilities in Wi-Fi security protocols and intercepting the data.
2. **Gaining Access:** Identify vulnerabilities, create undetectable backdoors and learn about the social engineering techniques.
3. **Post Exploitation:** After we gain access, we will be exploring the capabilities such as system control, keystroke logging and leveraging compromised systems to escalate it further.
4. **Website Hacking:** Analysing website structures, identifying critical vulnerabilities and implementing robust security measures.

This report highlights the key learnings and skills that I have learned in the online course to contribute responsibly to the field of ethical hacking.

**Setting up a Hacking Lab:**

In the course *Learn Ethical Hacking from Scratch 2024*, one important ideology they taught us is that whatever testing you do, its always good to perform the testing in an isolated environment like Virtual Machines. This is because, in our learning stages, we might do mistakes and those might end up in doing irreversible damages to the systems when tested in a physical machine. This errors or actual damages can be avoided by practicing in a secure, robust and isolated environments, like virtual machines. For this purpose, the chosen platform is Kali Linux, a powerful Linux distribution especially designed for penetration testing and security analysis.

**Why Kali Linux?**

Kali Linux is a Debian based platform and is the first choice for ethical hacking because of its convenience and pre-installed tools. Unlike generic Linux distributions, Kali Linux removes the necessity to manually install and setup the hacking tools, thereby saving our time and reducing our efforts drastically. This helps the learners and even the professional to focus just on the security analysis and penetration testing part instead of spending hours or days in setting up the tools or the environment.

**Virtual Machine Installation:**

For safety purposes and easy of use, we will be installing Kali Linux as a virtual machine (VM), as suggested in the course. This makes sure that, the lab setup is completely isolated from the Host machine. Following are the advantages that a VMs have to offer:

1. **Isolation**: Suppose if the virtual environment is compromised or corrupted, this will not affect the Host machine.
2. **Reconfiguration**: VMs can be reset or deleted without impacting the host system.
3. **Hardware Independence**: Allows running Kali Linux on various operating systems like Windows, Linux or macOS without direct installation.

To install the VM in our host machine, we need a desktop virtualization software. Hence, we will be installing VMware Workstation, which enables us to create, configure and manage multiple Virtual Machines on a single physical machine.  
After, installing the VMware Workstation, I have downloaded the Kali Linux Image provided in the course by Zaid. Importing this Image into the VMware Workstation and allocating resources as per the physical system’s capabilities will create the Virtual Machine. After starting the virtual machine, we can see that the VM comes pre-installed with various hacking tools necessary for this course. This setup ensures that, we focus entirely on mastering cybersecurity techniques without being overwhelmed by complex configuration challenges.

**Linux Basics:**

The terminals or the command prompt were used, even much before the Graphical User Interfaces (GUI) were into the industry. Hence, the terminal is a powerful tool with much advanced functionality and sophistication. The Linux terminal especially is a powerful tool essential for effectively using the Kali Linux distribution. The instructor explains its importance, specifically in the field of cybersecurity and penetration testing, where terminal-based tools are predominant. Below are the list of some important commands and their usage:

**Core Linux Terminal Commands:**

* **pwd** : Used to display the current working directory.
* **ls :** Lists files and directories.
* **cd** : **Navigates** between directories.
* **man** : Displays the manual for a command, explaining its syntax and options.
* **--help** : Provides a brief overview and usage of a command, similar to man command.
* **clear** : Used to clear the terminal screen.

**Installing Programs via the Terminal:**

1. Update the package list:

$ sudo apt-get update

1. Install a program from the package list:

$ sudo apt-get install {program-name}

For example, to install Terminator:

$ sudo apt-get install Terminator

Terminator is a terminal emulator that allows multiple terminal windows within the same interface, enhancing productivity.

**Network Hacking:**

The Network Hacking section is the most important section of the course as nearly all systems, whether personal computers, servers, companies or websites are always connected to the internet, forming a network of systems. Hence, having a solid understanding of networking essentials will make our life easier as a hacker. This section is divided into three subsections, each building upon the previous to equip learners with a comprehensive and thorough understanding of network vulnerabilities and attack procedures. They are:

* **Pre-Connection Attacks:** Focuses on attacks that can be executed without connecting to a network
* **Gaining Access:** Learn to crack the Wi-Fi Encryption to gain access to networks.
* **Post-Connection Attacks:** Exploring attacks that become possible after we gain access to a network.

1. **Pre-Connection Attacks:** This subsection focuses on possible attacks, that an adversary can perform even without connecting to the network. In this section and for the next, we are expected to have a wireless Wi-Fi adapter, using which we will explore various reconnaissance and probing techniques. These techniques help an attacker to gather information about networks, identify vulnerabilities and set the setup for further exploration, even much before accessing the target network.

**Understanding Networks:** Before knowing about the attacks, we need to understand the basic functioning of networks. Networks are designed to connect multiple systems, enabling them to share data between them. A common example of such a resource is the internet which can be accessed via Wi-Fi or wired networks.

**Network Structure:**

A white arrow pointing to the right

Description automatically generated

Figure 1 – Basic Network Structure

1. **Access Point (Router):** the router is a crucial part of the network with direct access to the internet and connects it to all the devices on the network.
2. **Packet Transmission:** Data is transmitted between the clients and the router in the form of packets. These packets can carry requests and responses between the devices in the network.

**Note:** In wireless networks, like the devices that are connected through Wi-Fi, these data packets are transmitted through air. Hence, any device with a wireless network card within range can potentially capture these packets.

**MAC (Media Access Control) Address**: A MAC address is a unique identifier assigned to network devices by the manufacturer. This is independent of the device’s location and the network it is connected to.

MAC addresses are used within local networks to identify devices and route data between them. They help ensure that the data is sent to the correct destination.

Note: While IP addresses are used for communication over the internet, MAC addresses are used on a local network level.

**Switching to Monitor Mode:** During communication between network devices, by default, a wireless device will only capture packets addressed to it. However, if you want to capture all the packets in the network, we need to switch to monitor mode. Below are the steps for enabling monitor mode:

* Check Interface Mode: We have to check the current mode of the wireless adapter using the command *iwconfig*. By default, it is et to Managed, which means that it only captures packets addressed to the device.
* Disable the Interface: We have to disable the interface, before changing the mode. This is done by running : $ ifconfig lan0 down
* Enable Monitor Mode: Now, we can switch to monitor mode, by running: $ iwconfig lan0 mode monitor
* Re-enable the Interface: This can be done using: $ ifconfig lan0 up
* Verify the Mode: Run iwconfig to confirm the interface is now running in monitor mode.

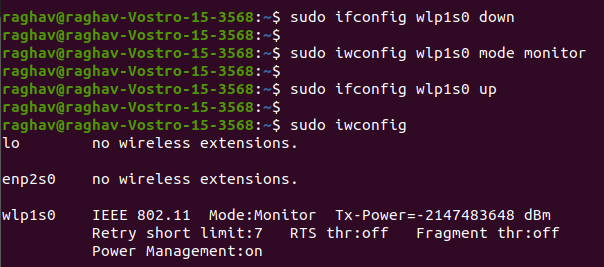


Figure 2 – Output of iwconfig command

**Packet Sniffing using Airodump-NG**: Once we enable the monitor mode, we can capture all the data packets sent within range, even those that are not directed at our device. To perform this step, we use Airodump-NG, a packet sniffer tool from the Aircrack-NG suite. This helps us in capturing useful information like MAC addresses, encryption types and connected clients. Running the command airodump-ng along with the wireless network in monitor mode as an argument, the adapter will start scanning for nearby devices and display information about each device.

The output of the command contains values data like:

* BSSID: MAC address of the network
* ESSID: Network Name
* PWR: Signal strength or power of the network
* Data: Number of data packets captured
* Beacons: This represents the number of frames that are broadcasted by the network
* Channel: Represents the Network’s operating channel
* Encryption: Shows whether the network uses WEP, WPA or WPA2 mode of encryption

**WiFi Bands**: There are two primary frequencies for WiFi networks namely 2.4 GHz and 5GHz. To connect to these networks, the devices must support them.

By default, Airodump-NG captures only the 2.4GHz frequency. If, all the networks around us are not visible, then it might be because your router broadcasts over both 2.4GHz and 5GHz bands, but Airodump-NG only listens to 2.4 GHz by default.

Below are the commands used for sniffing 5GHz networks:

1. $ airodump-ng –band a mon0

This tells Airodump-NG to capture only the 5GHz frequency packets.

1. $ airodump-ng –band abg mon0

Use this command, to list both 2.4GHz and 5GHz networks. However, this operation might slow the system as switching between bore channels consumes mores resources.

**Deauthentication Attacks:** This is a highly powerful pre-connection attack that can disconnect devices from the networks without requiring the network’s password. Below is the working of a deauthentication attack, demonstrating how an attacker tricks the target and the router into disconnecting from each other:

1. **Impersonating the Client:** The attacker spoofs the MAC address of the client and sends a disconnection request to the router.
2. **Impersonating the Router:** Here the attacker repeats the same process of sending a disconnection request but spoofs the router and sends this request to the client or the target device.
3. **Result:** This mutual deauthentication disconnects the target client from the network.

The Deauthentication attack is performed using the following command:

$ aireplay-ng –deauth <packet\_count> -a <router\_MAC> -c <client\_MAC> <interface\_in\_monitor\_mode>

**Key Parameters:**

* --deauth : Specifies a deauthentication attack
* <packet\_count> : This represents the number of deauthentication packets to send to the target. A large value ensures that the target remains disconnected for a long period of time.
* -a <router\_MAC> : This represents the MAC address of the target router
* -c <client\_MAC> : This is the MAC address of the target device that we need to disconnect
* <interface\_in\_monitor\_mode> : This is the wireless adapter in monitor mode.

**Limitations of Deauthentication Attacks:**

* Device Reconnection: Target devices upon disconnecting with the router, may immediately reconnect to another network or switch to mobile data, which makes the attack seems ineffective.
* Network Monitoring: Some networks may detect and block the deauthentication attacks with Intrusion Detection/Prevention Systems (IDS/IPS).

1. **Gaining Access:** This section dives deep into the art of cracking Wi-Fi encryption to gain access to the networks. Bypassing the Wi-Fi security protocols involves understanding the different security protocols. They are:

* **Wired Equivalent Privacy (WEP): This** security protocol was designed to provide a level of security and privacy equivalent to that of wired networks. WEP is highly outdated and is highly insecure due to significant vulnerabilities in its design and implementation.
* **Wi-Fi Protected Access (WPA):** This is a more secure protocol which addresses the shortcomings of WEP, but is still susceptible to certain attacks
* **Wi-Fi Protected Access 2 (WPA2):** This is currently the most used Wi-Fi security protocol, which provides even stronger security by using the Advanced Encryption Standard (AES).

Now, in this section, we will be discussing the steps involved in Breaking each security protocol starting with WEP.

1. **Breaking WEP Encryption:** This protocol uses RC4 algorithm for encryption, which is a weak encryption, due to which WEP can be easily broken. Although, this protocol is outdated, some networks still use WEP, making it an essential and easy topic for any hacker or penetration tester to begin with.

**Working of WEP:**

* WEP uses the RC4 algorithm to encrypt the data packets.
* The sender generates a key stream based on a shared password and an Initialization Vector (IV).
* This key stream is used to encrypt the data, converting it into gibberish that cannot be read by an interceptor without the decryption key.
* The receiver then decrypts these packets using the same key derived from the shared password and the IV.
* This process allows the receiver to get the original data.

**Weakness in WEP:**

* WEP generates a 24-bit IV for each packet to create a unique key stream.
* Due to the limited size of the IV, repetitions occur frequently in busy networks.
* When IVs are reused, attackers can identify patterns and perform statistical analysis to find out the Key stream.
* Since the IVs are transmitted in plain text, an attacker can collect IVs from multiple packets over time.
* By analysing the packets with the same IV, an attacker can identify the key stream and eventually crack the shared password.

**Exploiting WEP with Aircrack-NG:** In this section, we use tools like Aircrack-ng to exploit WEP’s vulnerabilities and recover the network key. The process is as shown below:

**Step 1:** Use Airodump-ng to capture WEP-encrypted packets. The command to run for this step is : $ airodump-ng –bssid <target\_bssid> --channel <channel> --write <output\_file> mon0

**Note:** Replace <target\_bssid> with the MAC address of the target network and <channel> with the network frequency.

**Step 2:** WEP cracking requires a large number of packets to exploit IV reuse. We can use aireplay-ng to create the required traffic and more data packets as shown below:

$ aireplay-ng –arpreplay -b <target\_bssid> -h <your\_MAC> mon0

**Note:** replace <target\_bssid> with the MAC address of the target router and <your\_MAC> with the wireless adapter’s MAC address.

**Step 3:** Once enough packets with repeated IVs are captured, use Aircrack-ng to analyze them and recover the WEP Key. The command for this process is:

$ aircrack-ng <output\_file>.cap

Note: Replace <output\_file> with the name of the file created by Airodump-ng

**Step 4:** This is the final step, where the WEP key is captured. As mentioned earlier, aircrack-ng uses statistical analysis on the captured IVs to determine the WEP key. This process becomes more efficient and reliable when more packets with reused IVs are collected.

1. **Breaking WPA and WPA2 Encryption: Exploiting WPS**

We now know that WPA and WPA2 are more secure that WEP. However, there is a feature called WPS (WiFi Protected Setup), if enabled and misconfigured, can be exploited to recover the key without cracking the encryption.

**What is WPS?**

WPS is a feature designed to simplify the process of connecting devices like printers to networks. Instead of entering the network password, using WPS we can allow authentication using a 8-digit pin. This pin is numeric and is relatively small, thereby enabling us to try all the possible combination of pins within in a short time. Once the pin is recovered, the attacker can use it retrieve the Wi-Fi password.

**Conditions for Exploiting WPS:**

* WPS must be enabled in the network
* The WPS must use PIN authentication instead of Push Button Configuration (PBC). If PBC is enabled, the router will reject all the PIN-based authentication requests, until the WPS button is pushed manually

**Steps for performing the Attack:**

**Step 1**: Identifying WPS-Enabled Networks

* Use the wash tool to scan for networks enabled with WPS. This can be done using: $ wash –interface mon0
* This lists the target networks, where BSSID is the MAC address and Lck if has a value of “No” means that the network is not locked and can be attacked.

**Step 2**: Confirming WPA/WPA2 Encryption

* We have to verify if the target network uses WPA/WPA2 Encryption, as this attack focusses on exploiting WPS, but not cracking the WPA/WPA2 encryption directly.

**Step 3**: Associating with the target

* Run the below command, to perform a fake authentication attack:

$ aireplay-ng –fakeauth 30 -a <BSSID> -h <MAC\_address> mon0

* Using this command output we can make sure that the target network will not ignore connection attempts during the brute force attack.

**Step 4**: Brute Forcing the WPS PIN

* Now running the reaver tool using the below command, will brute force the WPS pin and recove the WPA/WPA2 Key:  
  $ reaver -bssid <BSSID> --channel <channel> --interface mon0 -vvv --no-associate

**Step 5**: Recovering the Key

* Once the correct WPS PIN is discovered, reaver computes and displays the WPA/WPA2 Key.

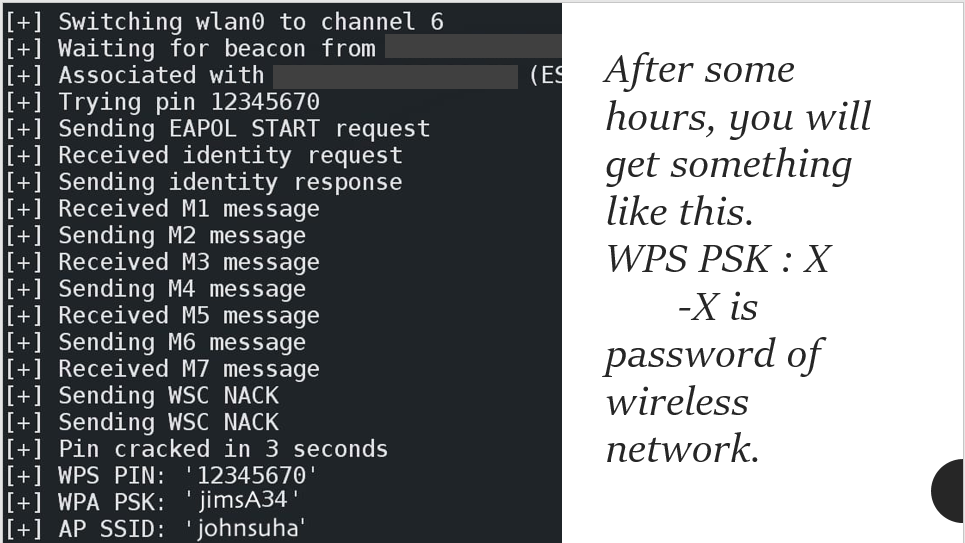


Figure 3 – Cracking WPA/WPA2 Password

**Limitations:**

* This attack works only if WPS is enabled and configured for PIN authentication. This attack will fail, if the network uses PBC or if WPS is disabled in the router.
* Some routers may lock the WPS feature after multiple failed attempts, preventing the network from further brute force attacks.

1. **Post-Connection Attacks**: In the final section of Network Hacking, we explore all the possible attacks that an adversary can perform after gaining access to the target network. These attacks are relevant to both Wi-Fi and wired connections and hence the wireless Wi-Fi adapter isn’t mandatory for this section. Below are the steps that an attacker can do, once he/she has gained access to a network.

* Intercepting Network Traffic: Attacker can capture the data being transmitted within the network, such as usernames, passwords and chat messages.
* Data Manipulation: The attacker can act as man in the middle and modify the data in transit, performing actions like fake server updates, redirecting users to malicious websites or injecting malicious codes into the web pages.
* Advanced Exploits: The adversary can escalate further up in the network by gaining deeper control over connected devices and accessing the sensitive information.

1. **Network Discovery with NetDiscover:** Gathering unauthorized information is one of the key objectives of hackers and penetration testers. To assess a target, understanding the network and its connected devices is necessary. This is the solid foundation necessary to escalate an attack furthermore in the network. NetDiscover is a tool exactly designed for this purpose. It helps identify the devices in a network.

* NetDiscover scans a subnet to identify devices, their IP addresses, MAC addresses and other manufacturer information.
* To run this command, we have to first run “ifconfig” in Kali Linux to find our interface and IP address. For example, an IP address of 10.0.1.34 means the subnet is 10.0.1.0/24.
* Now, we can run the netdiscover command to scan the subnets using:  
  $ netdiscover -r 10.0.1.0/24
* This scans all the IPs from 10.0.1.1 to 10.0.1.254 and lists the connected devices
* The tool displays the IPs, MAC addresses and device manufacturer information, providing a foundation for identifying potential targets for further analysis.

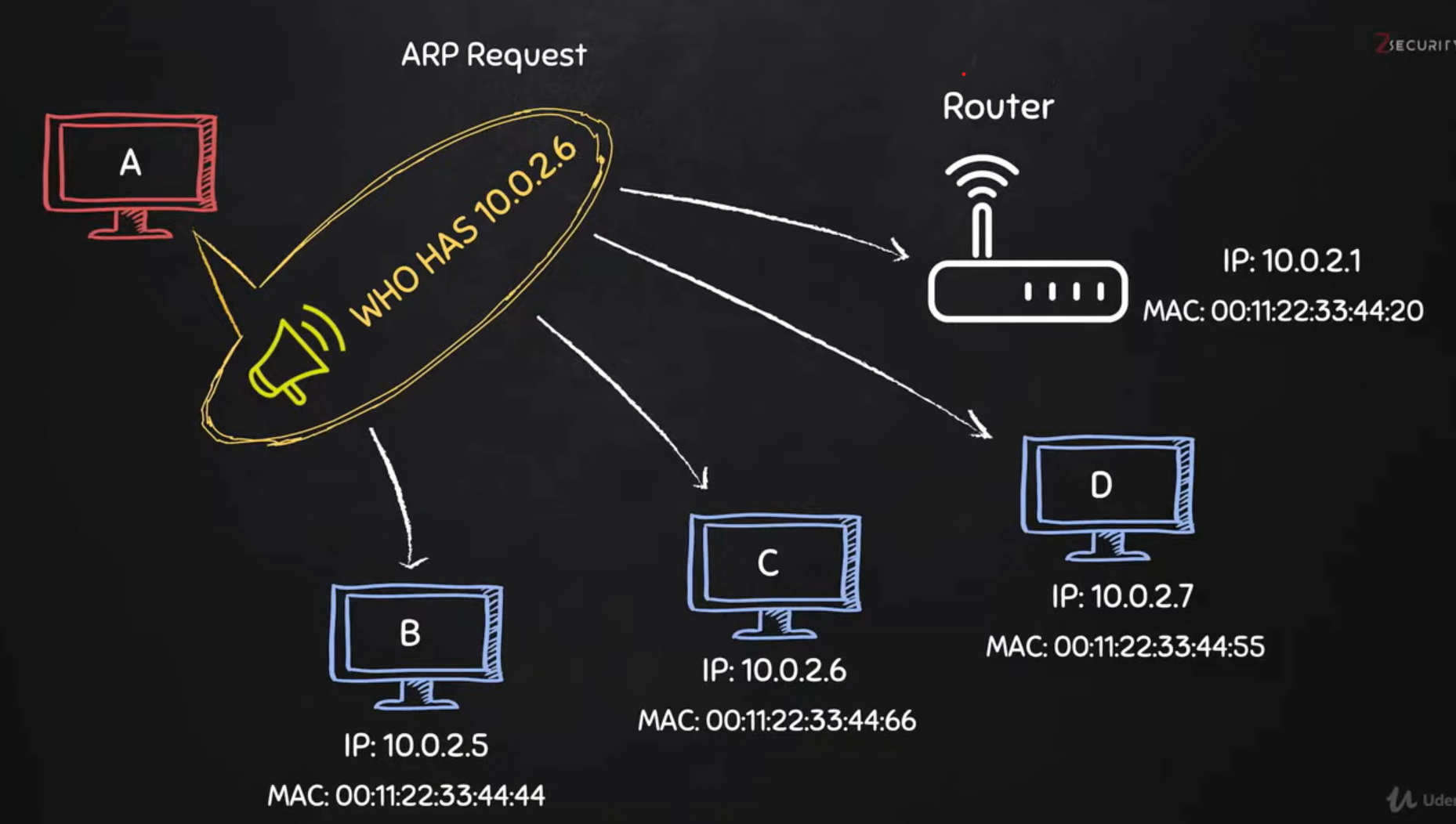


Figure 4 – ARP Request

1. **Zenmap Quick Scan Plus:** Zenmap is an enhanced scan option for gathering detailed information about the devices in a network. Although this method is slower, it provides greater details related to operating systems, device types, service versions and more, which are crucial for exploiting their inherent weaknesses or version specific vulnerabilities.

* For instance, the instructor has demonstrated an example, where an apple iPhone which had OpenSSH running was detected in the network. By leveraging Zenmap’s detailed information, the instructor could attempt a successful SSH login with default credentials, gaining full access to the device.

**Security Measures:**

From this course, I understood that Wireless networks are never secure by default. So, we always have to use Ethernet connections, if possible, to avoid our data being intercepted by other users in close proximity to our premises. However, if we still need to go with Wireless network, we should always make sure that we use WPA/WPA2 or a better security protocol, but not outdated protocols like WEP. We should also change our network password frequently with a strong a long password including a combination of capital, small letters and special characters. One important setting to disable is the WPS mode of authentication, which prevents attackers from successfully brute forcing into our network. Another optional security feature to increase our security posture is to set MAC Filtering in our network, so that only trusted devices can access the network. Moreover, we have to always keep our system and applications up to date, so that we don’t let the attackers to take advantage of the vulnerabilities which might have been fixed in the latest versions.

**Conclusion:**

The *Learn Ethical Hacking from Scratch 2024* course by Zaid has laid an excellent foundation into the world of ethical hacking. This comprehensive course has equipped me with not only theoretical knowledge, but also practical skills necessary to identify, exploit and mitigate security vulnerabilities across various systems and networks. By following a structured approach, I have gained a deeper understanding of how attackers think and operate and how to counteract their attacks responsibly.

This course not only focused on offensive strategies, but also put a strong emphasis on defensive strategies as well. Ultimately, this course has not only improved my technical abilities, but also deepened my appreciation for the ethical dimensions of cybersecurity. This has made be confident in solving the real-world problems making the world a safer place for everyone.

**References:**

[1] <https://www.linkedin.com/pulse/wifi-hacking-using-reaver-rishav-kumar/>

[2] <https://gourav-dhar.com/blogs/man-in-the-middle-attacks-by-arp-spoofing-tutorials-and-examples/>

[3] <https://concordia.udemy.com/course/learn-ethical-hacking-from-scratch/learn/lecture/5306390#overview>