Please Subscribe my Youtube Channel at Protoons (Multi Media)

Diploma in Ethical Hacking Techniques for Beginners and Experts

SUMMARY

BY:
Aminu Aliyu Ahmad
ID: Aminu-Pro-001

- Welcome this comprehensive Ethical Hacking course! This course assumes you have **NO prior knowledge** and by the end of it you'll be able to **hack systems like black-hat hackers** and **secure them like security experts!**
- This course is highly **practical** but it won't neglect the theory; we'll start with ethical hacking basics, breakdown the different penetration testing fields and install the needed software (on Windows, Linux and Mac OS X), then we'll dive and start hacking straight away. You'll **learn everything by example**, by analysing and exploiting different systems such as networks, servers, clients, websites .....etc. We'll never have any boring dry theoretical lectures.
- The course is divided into a number of sections, each section covers a penetration testing / hacking field, in each of these sections you'll first learn how the target system works, the weaknesses of this system, and how to **practically** exploit theses weaknesses to hack this system.
- By the end of the course you will have a strong foundation in most hacking or penetration testing fields and you'll also learn how to **detect, prevent and secure** systems and yourself from the discussed attacks.
- The course is divided into four main sections:
- **1. Network Hacking** - This section will teach you how to test the security of both wired & wireless networks. First, you will learn network basics, how they work, and how devices communicate with each other. Then it will branch into three sub sections:
- Pre-connection attacks: in this subsection you'll learn a number of attacks that can be executed without connecting to the target network and without the need to know the network password; you'll learn how to **gather information** about the networks around you, discover connected devices, and control connections (**deny/allow devices from connecting to networks**).

- Gaining Access: Now that you gathered information about the networks around you, in this subsection you will learn how to **crack** the key and get the password to your target network whether it uses **WEP, WPA** or even **WPA2**.

- Post Connection attacks: Now that you have the key, you can connect to the target network, in this subsection you will learn a number of **powerful techniques** that allow you to gather comprehensive information about the connected devices, **see anything they do on the internet** (such as login information, **passwords**, visited urls, images, videos ....etc), redirect requests, **inject evil code** in loaded pages and much more! All of these attacks work against both wireless and wired networks. You will also learn how to **create a fake WiFi network,** attract users to connect to it and use all of the above techniques against the connected clients.

- **2. Gaining Access** - In this section you will learn two main approaches to **gain full control or hack computer systems**:

- Server Side Attacks: In this subsection you will learn how to **gain full access** to computer systems **without user interaction**. You will learn how to gather useful information about a target computer system such as its operating system, open ports, installed services, then use this information to **discover weaknesses and vulnerabilities** and **exploit** them to gain full control over the target. Finally you will learn how to automatically scan servers for vulnerabilities and generate different types of **reports** with your discoveries.

- Client Side Attacks - If the target system does not contain any weaknesses then the only way to hack it is by interacting with the users, in this subsection you'll learn how to get the target user to install a backdoor on their system without even realising, this is done by **hijacking software updates** or **backdooring downloads** on the fly. This subsection also teaches you how to use social engineering to hack secure systems, so you'll learn how to gather comprehensive information about system users such as their social accounts, friends, their mails.....etc, you'll learn how to **create trojans** by backdooring normal files (such as an image or a pdf) and use the gathered information to spoof emails so they appear as if they're sent from the target's friend, boss or any email account they're likely to interact with, to social engineer them into running your trojan.

- **3. Post Exploitation** - In this section you will learn how to interact with the systems you compromised so far. You'll learn how to **access the file system** (read/write/upload/execute), **maintain your access**, **spy** on the target (capture key strikes, turn on the webcam, take screenshots....etc) and even use the target computer as a **pivot** to hack other systems.

- **4. Website / Web Application Hacking** - In this section you will learn **how websites work**, how to **gather information** about a target website (such as website owner, server location, used technologies ....etc) and how to **discover** and **exploit** the following dangerous **vulnerabilities** to hack websites:

- File Upload.

- Code Execution.

- Local File Inclusion.

- Remote File Inclusion.

- SQL Injection.

- Cross Site Scripting (XSS).

- At the end of each section you will learn how to **detect, prevent and secure** systems and yourself from the discussed attacks.

- All the techniques in this course are **practical** and work against real systems, you'll understand the whole mechanism of each technique first, then you'll learn how to use it to hack the target system. By the end of the course you'll be able to modify these techniques to launch more powerful attacks, and adopt them to suit different situations and different scenarios.

- *Notes:*
- *This course is created for educational purposes only, all the attacks are launched in my own lab or against systems that I have permission to test.*

Learning Outcomes

After completing this module you will be able to:

- Outline the types of hackers.
- Discuss how hackers exploit the basic elements of security.
- Explain the common methods of hacking.
- Recall the ethical hacking terminologies.
- Compare ethical hacking and cybersecurity.
- Summarise the process of data transmission in a network.
- Distinguish between public and private addresses.

Overview of Hacking Methods

- The three types of hackers are:
- White Hats: Ethical hackers. Use their hacking skills for defensive purposes.
- Black Hats: Malicious attackers. Use their hacking skills for illegal or malicious purposes.
- Gray Hats: Typically, self-proclaimed ethical hackers invested in hacker tools, mostly from a curiosity standpoint.
- The four basic elements of security are:
- Confidentiality | Authenticity | Integrity | Availability

Some of the common methods of hacking are:

- Virus/Trojan
- Phishing
- Eavesdropping
- Keylogger
- Social engineering
- Bait and Switch

Introduction to Ethical Hacking

- Cybersecurity focuses on protecting a network from potential attacks and dangers. At the same time, ethical hacking is the act of attempting to break into a network to uncover vulnerabilities that may be present.
-
- Ethical hacking falls under the umbrella of cybersecurity.
-
- Ethical hacking and penetration testing typically refer to the same thing and can be used interchangeably.
-
- Networking Basics
- A network occurs when two or more computers are linked together and can share resources.
- The types of networks are:
- PAN: Personal Area Network
- LAN: Local Area Network
- MAN: Metropolitan Area Network
- WANS: Wide Area Networks

Cont.…

- An IP address is used to identify computers on a network. No two computers can have the same IP address.
-
- The two types of IP addresses are public and private IP addresses.
- Ports allow for the transmission of data over a network. They exist on the TCP and UDP protocols.
-
- At a very high level, data travels across networks in the form of packets. Each packet has two addresses attached to it: the source address and the destination address.
-
- TCP is a connection-oriented protocol built around confirming packet delivery.
-
- UDP is a connectionless protocol. It doesn’t check for failed transmission of packets. So, it is faster than TCP.

Learning Outcomes

- After completing this module you will be able to:
- Define virtual machines and a hacking lab.
- Discuss how to set up your hacking lab.
- Describe the steps in installing and setting up the Kali Linux machine on your computer.
- Recall the vital Linux commands and their functions.
- Explain how to apply the key syntaxes of Bash and Python language in executing commands in Linux.

Setting up your Hacking Lab

- A hacking lab is a network you create that lets you practice your hacking skills in a controlled environment, reducing the risk that arises from practising on real systems.
-
- To run your virtual machine, you will need a virtual machine player. An example of a virtual machine player is the virtual box.
-
- The virtual box is an application that allows you to load and run images of machines on your computer. It can be run on Windows, Mac, and Linux OS.

Basics of Linux

- An operating system is software that directly manages a system's hardware and resources such as CPU, memory and storage.
- A scripting language is a programming language designed for integrating and communicating with other programming languages.
- Some Linux commands you should know are:
- Whoami: Print the username of the current user.
- Pwd: Prints the current directory of a user.
- Rmdlr: Delete the indicated directory.
- Ls: Lists out the element of the current directory.
- Hostname: Prints the hostname of the device.
- Basics of Bash and Python Languages
- Bash is the language that is used to navigate Linux and execute commands.
- All bash scripts typically start with #!/bin/bash.
- Python scripts in Linux always start with #!/usr/bin/python.

Learning Outcomes

- After completing this module you will be able to:
- Discuss how to maintain your privacy on the web.
- Explain how to install the Tor browser and anonsurf on Kali Linux.
- Recognise the significance of virtual private networks and servers in maintaining web anonymity.
- List the common ways that black hackers get access to networks and information.
- Recall how to hack a WEP and WPA network.

Hiding your Identity Online

- The internet is a very public place by default, so you need to take a few steps to remain anonymous.
-
- A Virtual Private Network (VPN) is a connection method that adds security and privacy to private and public networks. With a VPN, the user's initial IP address is replaced with one from the VPN provider.
- The TOR browser is a web browser that allows users to browse the web while preventing surveillance and tracking.
- Anonsurf is a tool that will help you stay anonymous by routing every packet from your computer through the TOR relay. When you use Anonsurf for ethical hacking, all the traffic from your system goes through a TOR proxy server.
- Every device has a unique MacAddress that can identify it. To remain anonymous, it would be wise to change this as well.

Wi-Fi Hacking

- A wireless access point allows wireless devices to connect to the wireless network.
- The common methods that hackers use in hacking Wi-Fi are:
- Spoofing and Wardriving.
- Encryption cracking and Brute force.
- To detect and connect to Wi-Fi with the Kali Linux virtual machine, you must add an external USB Wi-Fi adapter. If you use the Wi-Fi adapter, you will need to use the virtual box extension pack with the kali machine.
- The main flaw of WEP is its use of initialisation Vectors (IV) and small encryption key size. The IV and small encryption key size make it easy for an attacker to decrypt packets on the WEP network. You can easily use the aircrack-ng tool to crack the WEP.
- Once the security flaws of WEP became obvious, WPA/WPA2 was created as replacements. They use stronger encryption methods and can't be easily hacked like the WEP. The best way to hack into a WPA network is to capture the initial 4-way handshake when a user first connects to the access point.

Learning Outcomes

- After completing this module you will be able to:
- Recall the basic steps in performing reconnaissance.
- Distinguish between active and passive reconnaissance.
- List the tools used in conducting passive Reconnaissance on a network.
- Explain how to use vital web tools for passive reconnaissance.
- Discuss how to conduct an active Reconnaissance on a network.

Reconnaissance

- Reconnaissance is a set of processes and techniques used to covertly discover and collect information about a target system.
-
- The steps in performing reconnaissance are:
- Gather initial information
- Determine the network range
- Identify active machines
- Discover open ports and access points
- Fingerprint the operating system
- Uncover services on port
- Map the network
- Passive reconnaissance involves gathering information about a target without forming any connection or contact with them at all.

Cont.....

- Active reconnaissance involves gathering information about a target while initiating connections or contact with them.
- Recon-ng is one of the most powerful tools for conducting passive reconnaissance using open source intelligence.
- Web Tools for Passive Reconnaissance
- Shodan is known as the “Hacker’s Google”. It is a site that literally has information about almost every device that is connected to the internet. It can help you discover known vulnerabilities of a target, all from Open Source Intelligence (OSINT).
- Securityheaders is a tool that allows you to check if a site has its security headers set up correctly to prevent attacks.
- SSLlabs test a server to see if its SSL settings are correctly set and if it accepts a vulnerable version of TLS or SSL.

Cont.…

- Pastebin is simply a place where people worldwide post very random things as basic text docs that anyone can view.
- Active Reconnaissance Tools
-
- Nmap is probably the most important tool in the penetration testing tool. It is a versatile tool that can scan an entire network to discover what ports are open.
-
- Netcat is known as the hacker swiss army knife. It is essential for establishing a remote connection to devices you are going to exploit.
- Network File Share (NFS), which runs over port 111, is typically used to mount network shares and can be exploited when set up incorrectly. You can use Nmap to enumerate NFS information.

Cont…..

- Nikto is a web application scanner that can find vulnerabilities and weaknesses that exists on web servers.
-
- Sparta is a useful tool that combines multiples tools into one interface for faster and more automated information gathering. Some of the tools included are Nmap, Nikto, Hydra, and the screenshot tool.
-
- Nessus is a vulnerability scanner that allows you to scan an entire network to discover vulnerabilities on devices.

Diploma in Ethical Hacking Techniques for Beginners and Experts - First Assessment. Learning Outcomes

- You will be assessed on the following learning outcomes:
- - State the common methods of hacking.
- - Compare ethical hacking and cybersecurity.
- - Outline the ethical hacking terminologies.
- - Discuss how to set up your hacking lab.
- - Describe the steps in installing and setting up the Kali Linux machine on your computer.
- - Explain how to maintain your privacy on the web.
- - Recognise the significance of virtual private networks and servers in maintaining web anonymity.
- - Recall how to hack a WEP and WPA network.
- - Distinguish between active and passive reconnaissance.
- - Summarise how to use vital tools for conducting active and passive reconnaissance on a network.

Learning Outcomes

- After completing this module you will be able to:
- List the five phases of cyberattack.
- Describe how to search for exploits to compromise a target system.
- Explain how to launch cyberattacks with Metasploit.
- Recall the key cyberattack methods.
- Discuss how to conduct post-exploitation activities.

Cyber Attack

- The five phases of cyberattack are:
- Reconnaissance
- Scanning
- Gaining access
- Maintaining access
- Covering tracks
- Reconnaissance is a preparation phase where an attacker gathers information about the target prior to launching an attack.
- Attackers use the information gathered from reconnaissance to identify specific vulnerabilities.
- Access to the targeted devices can be gained locally, offline, or over the internet.
- Social engineering is the act of manipulating users into revealing confidential information that can be used to gain unauthorised access to information.
- Some common social engineering attacks are:
- Phishing | Watering hole | Pretexting
- Outside launching attacks with exploits, you could brute force your way into a system.

Cont…..

- THC Hydra is a program that comes with Kali Linux and allows you to launch brute force attacks.
-
- ARP spoofing can be used to impersonate another computer and potentially intercept information meant to go somewhere else.
-
- Cryptography is the science or study of protecting information by using techniques to render the information unusable to anyone who does not possess the means to decrypt it.
- The two forms of encryption are:
- Symmetric encryption: This uses the same key for encryption and decryption.
- Asymmetric encryption: This uses one key to encrypt and another key to decrypt.
- Post-exploitation is the phase of operation after a victim’s system has been compromised by the cyberattacker.

Cont.…

- The six phases of post-exploitation are:
- Understanding the victim.
- Privilege escalation.
- Cleaning tracks and staying undetected.
- Collecting system information and data.
- Setting up backdooring and rootkit.
- Pivoting to penetrate internal networks.
- Privilege Escalation is the act of attempting to gain root access or system-level access on a system.
-
- A keylogger monitors and records every key pressed on a computer and sends it back to your machine for analysis.

Learning Outcomes

- After completing this module you will be able to:
- List the top 10 OWASP web application vulnerabilities.
- Describe how to use vital web application scanning tools.
- Discuss how to utilise key tools in exploiting the crucial vulnerabilities of web applications.
- State the common methods of mobile phone hacking.
- Recall how to protect your phone from hacking.

Web Application Scanning Tools

- Much like regular penetration testing, you must first gather information on your target web app or website before you attack.
- ZAP and BURP are web-scanning tools that you can use to gather information about web applications or websites. BURP has a paid edition, while ZAP is 100% free.
- Kali Linux comes with a tool called directory buster that enumerates directories that exists on a given website.
- The SQLmap and SQLNinja can be used to enumerate information about a web application that utilises SQL databases and determine if SQL attacks are possible.
- Web Application Attacks
- Command injection involves exploiting a vulnerability that allows for the remote execution of commands into a system.
- SQL injection takes advantage of unsanitised input that is used in an SQL query. This allows a user to execute any SQL command.
- Cross-Site Request Forgery (CSRF) involves using malicious code to take advantage of a user's trusted session inside of their browser.
- Cross-site scripting (XSS) involves injecting malicious code either into a request for a web page or into the web page itself, leading to its execution when the page is loaded.

Cont.…

- The three types of XSS vulnerabilities are:
- Stored XSS | Reflected XSS | DOM-based XSS
- Mobile Phone Hacking and Security
- Some typical attack vectors in mobile devices are:
- Mobile malware from a downloadable app.
- Advertisements inside of apps or on mobile sites.
- Operating system vulnerabilities.
- Phishing via SMS with malicious links.
- Vulnerabilities of installed apps.
- Some of the countermeasures against mobile phone malware are:
- Installing a good anti-malware program.
- Configuring your apps to always auto-update.
- Installing the latest operating system patches as soon as they are released.
- Jail breaking and rooting your phone unlock root access to your phone and make it easier for an attacker to compromise your device.

Assessment Overview Questions

- Distinguish between personal branding and business branding.
- Discuss the methods of gaining more authority and credibility as an ethical hacker.
- State the top bug bounty websites.
- Recall the sites you can get freelance ethical hacking jobs.
- List the key sites where you can practice ethical hacking.
- Explain the processes of starting a career in cybersecurity.

Aminu Aliyu Ahmad

+2348083361925, +234911247589

aminualiyuahmad03@gmail.com, protoons03@gmail.com, protidings@gmail.com