18

Best Practices for the Real World

Your journey as an aspiring ethical hacker and penetration tester is only just beginning. You have gained some amazing hands-on skills throughout the previous chapters of this book and have learned various techniques while developing the mindset of a penetration tester. Furthermore, you have learned how to use the most popular penetration testing Linux distribution, Kali Linux, to simulate various real-world cyber-attacks to discover and exploit various security vulnerabilities on systems and networks.

While you have learned a lot, there are a few guidelines and tips I would like to share with you before concluding this book. During the course of this chapter, you will learn about various guidelines that should be followed by all penetration testers, the importance of creating a checklist for penetration testing, some cool hacker gadgets, how to set up remote access to securely access your penetration tester's machine over the internet, and some next steps to move ahead.

In this chapter, we will cover the following topics:

- Guidelines for penetration testers
- Penetration testing checklists

- Creating a hacker's tool bag
- Setting up remote access
- Next steps ahead

Let's dive in!

Technical requirements

To follow along with the exercises in this chapter, please ensure that you have met the following software requirements:

- Kali Linux: **https://www.kali.org/get-kali/**

Guidelines for penetration testers

Having the skill set of an ethical hacker and penetration tester, you need to be aware of the boundaries between ethical and criminal activities. Remember, performing any intrusive actions using a computing system to cause harm to another person, system, or organization is illegal. Therefore, penetration testers must follow a code of conduct to ensure they remain on the ethical side of the law at all times.

Gaining written permission

Before performing a penetration test on a targeted organization, ensure that you have obtained legal written permission from the organization. If additional permission is required from other authorities, please ensure that you acquire all the

legal permission documents. Having legal written permission is like having a get-out-of-jail-free card as a penetration tester, but this comes with a responsibility.

The activities performed by a penetration tester involve simulating real-world cyber-attacks on a targeted organization; this means actually hacking into their systems and networks by using similar tools, techniques, and procedures as real cybercriminals. Some attacks can be very intrusive and may cause damage or network outages; written permission is used to protect yourself legally.

Being ethical

Always be ethical in all your actions as a professional in the industry. During your time practicing your penetration testing skills, I'm sure you have realized that there is a fine line between being a malicious hacker and a penetration tester. The main difference is that penetration testers have a good moral compass and obtain legal permission prior to simulating any cyber-attacks with the intent to help an organization improve its security posture and decrease the attack surface before a real cyber-attack occurs. Being ethical simply means doing the right thing and upholding moral principles.

As technology and legal landscapes evolve, ethical hackers must continually update their knowledge and skills to navigate the complexities of cybersecurity with integrity and lawful conduct.

Penetration testing contract

As an aspiring cybersecurity professional in the industry, ensure that you have a properly written penetration testing contract, inclusive of confidentiality and a **Non-Disclosure Agreement** (**NDA**), reviewed and verified by the legal team of your organization/employer. This ensures the client's (targeted organization's) information is protected and that you (the penetration tester) will not disclose any information about the client unless required by law. Additionally, the NDA builds trust between the client and you, the penetration tester, as many organizations do not want their vulnerabilities known to others.

If, during a business meeting with a new client, they ask about previous penetration tests you have conducted and customer information, do not disclose any details. This would contravene NDAs, which protect your customers and yourself. However, you can simply outline to the new potential client what you can do for their organization, the types of security testing that can be conducted, and some of the tools and methodologies that may be used during the testing phases.

Rules of engagement

During your business meeting with the client (targeted organization), ensure that both you and the client understand the **Rules of Engagement** (**RoE**) prior to the actual penetration test. The RoE are presented in the form of a document created by the service provider (penetration tester) that outlines what types of penetration tests are to be conducted, as well as other specifics. These include the area of the network to be tested, such as the IP addresses and subnets, such as servers, networking devices, security appliances, and workstations. To put it simply, the

RoE document defines the manner in which the penetration test should be conducted and indicates any boundaries in relation to the targeted organization.

Ensure you have obtained contact information for key personnel within the targeted organization so that, in the event there is an emergency or something goes wrong, you can reach out to the client. For instance, if, during a penetration test, the targeted server crashes, contacting the key personnel of the organization would be helpful in rebooting or restoring the server back to an operational state. Furthermore, if there is an unexpected crisis, you may need to contact someone for assistance, such as if you are conducting your tests remotely after working hours.

During a penetration test, if you discover any violations of human rights or illegal activities on targeted organization systems or networks, stop immediately and report it to the local law enforcement authorities. Should you discover a security breach in the network infrastructure, stop and report it to a person of authority within the organization and/or the local authorities. As a penetration tester, you need to have good morals and abide by the law; human rights and safety always come first, and all illegal activities are to be reported to the necessary authorities.

Furthermore, a **Statement of Work** (**SOW**) is provided to the client as a formal agreement before starting any security testing. A typical SOW agreement contains the following information:

- The customer's expectations for the penetration test
- The scope of work, such as which IP addresses, subnets, and systems are to be tested

- The duration/schedule of the penetration test
- The cost for the penetration test
- A list of deliverables to meet the customer's expectations
- Any legal statements between the customer and the service provider
- Signatures of the service provider and customer

The following are common guidelines for data security and confidentiality in penetration testing to establish and maintain trust and integrity during the testing process while safeguarding the client's interests:

- **Data handling procedures**: Ensure you create and maintain clear procedures for handling any sensitive data that will be obtained during penetration testing. Ensure only authorized personnel have access to this sensitive data, use only secure communication channels when transmitting the data, and use encryption technology to securely store data on storage devices.
- **Data storage and retention**: Specify how long the collected data will be stored after the penetration testing process. Ensure you use data encryption technologies to secure the storage of sensitive data.
- **Client communication**: Providing regular updates to the client on the status of the penetration testing process goes a long way. In addition, updates should be provided to only authorized persons and not to just anyone from the organization.
- **Compliance and regulations**: Ensure all the data handling processes and procedures are compliant with industry standards and regulatory requirements, such as **Payment Card Industry Data Security Standard** (**PCI DSS**), **General**

Data Protection Regulation (**GDPR**), and **Health Insurance Portability and Accountability Act** (**HIPAA**), depending on the client's industry.
- **Documentation and reporting**: It's essential to document everything, such as the data handling, data collection, storage, and destruction processes and procedures.

Having completed this section, you have learned about various key guidelines for penetration testers. In the next section, you will learn about some of the key elements when creating a penetration testing checklist.

Penetration testing checklist

When performing a penetration test on a system or network, a set of approved or recommended guidelines is used to ensure the desired outcome is achieved. For instance, you can leverage the following structure in your existing framework or process as it helps with ensuring the critical aspects of penetration testing are addressed:

- **Comprehensive coverage** – Using a checklist helps ensure that all the necessary components of the penetration test are thoroughly covered, such as from the reconnaissance phase all the way to reporting. This will help you create a roadmap, ensuring all important steps are followed and not overlooked.
- **Standardizes procedures** – Standardizing a set of procedures with industry best practices helps you to develop and maintain consistency across various types of penetration testing with each organization. In addition, it helps ensure that all penetration testing is performed in uniformity with a systematic methodology.

- **Facilitates documentation** – Using a checklist helps ensure the penetration tester documents their observations, findings, and activities during the entire process.
- **Improves efficiency** – Checklists can help with staying organized and focusing on the tasks ahead. They help the penetration tester to better utilize the allotted time during each phase of penetration testing.

Following such a checklist ensures that the penetration tester completes all tasks for a phase before moving on to the next. In this book, you started with the information-gathering phase and gradually moved on from there. The early chapters covered the early phases of penetration testing and taught you how to obtain sensitive details about a target using various techniques and resources, while the later chapters covered using the information found to gain access to a target using various methods and tools, and establishing persistence and dominance of the compromised network.

A penetrating testing methodology usually consists of the following phases:

1. Pre-engagement
2. Reconnaissance
3. Enumeration
4. Vulnerability assessment
5. Exploitation
6. Post-exploitation
7. Reporting

Let’s discuss each of these stages in detail.

Pre-engagement

During the pre-engagement phase, the scope and objectives are discussed and mutually agreed upon by both the client and the service provider (employer of the penetration tester). During this phase, it's essential to obtain written legal permission and authorization from the authorities before starting/performing any security assessments.

Reconnaissance

Reconnaissance focuses on collecting as much data as possible on a target and then analyzing the collected data to create meaningful information that can be leveraged by an adversary or threat actor to identify the attack surface and security vulnerabilities on a targeted system, network, or organization. Adversaries use various reconnaissance techniques and tools to collect system information, networking information, and organizational information about their targets. Without first understanding your target and its weaknesses, it'll be challenging to develop cyber-attack methods, including exploits that will be effective in compromising the confidentiality, integrity, and/or availability of the targeted system, network, or organization.

The following are the tasks to be performed prior to and during the reconnaissance phase:

- Gather information that is relevant to the target, such as:
  - Identify domain names and sub-domains.

    - Identify IP addresses and network blocks.
    - Gather email addresses.
    - Identify employee names and their job titles.
    - Identify social media profiles owned and managed by the target.
    - Identify social media profiles owned by employees of the targeted organization.
    - Identify the physical locations of the organization.
- Perform passive reconnaissance using **Open Source Intelligence** (**OSINT**) techniques:
    - Leverage the internet and specialized search engines.
    - Collect data from social media platforms such as Facebook, X, Instagram, and LinkedIn.
    - Identify interesting information from the target's website.
    - Identify data leakage on online forums and discussion groups such as Stack Overflow.
- Perform active reconnaissance:
    - Use network and port scanners to identify live hosts and profile targeted systems.
    - Leverage network mapping tools such as Netcraft and Maltego to profile the public-facing infrastructure of the target.
    - Use email harvesting tools such as Spiderfoot, Recon-ng, and theHarvester to collect employees' email addresses for social engineering simulations.

In the next section, we will take a look at a checklist for enumeration.

Enumeration

By performing enumeration on network services running a targeted system, we'll be able to identify user accounts, network shares, and password policies, and profile the target's operating system. Using the information collected during enumeration helps us to better understand which security vulnerabilities exist and how to improve our plan of attack on the target.

The following is a list of guidelines for performing network enumeration:

- Review the data collected during the reconnaissance phase.
- Identify targeted systems and services for enumeration.
- Perform enumeration on network services such as SMB, LDAP, SNMP, SMTP, and DNS.
- Enumerate DNS records from the target's DNS server to identify sub-domains and unintentionally exposed assets on the internet.
- Perform website and web application scanning using tools such as Burp Suite and Nikto to identify security vulnerabilities.

In the next section, we will take a look at a vulnerability assessment checklist.

Vulnerability assessment

During the vulnerability analysis phase, the ethical hacker or penetration tester performs both manual and automated testing on targeted systems to identify hidden and unknown security flaws. Identifying security vulnerabilities within systems helps organizations to better understand the attack surface, which is the vulnerable points of entry within their systems and network infrastructure.

The following is a list of guidelines for vulnerability assessment:

- Create an inventory of assets that are within the scope of the penetration test.
- Identify an appropriate vulnerability assessment tool based on the targeted systems and environment. Consider automated scanners, manual testing tools, and web application scanners.
- Configure and run scans on targeted systems when working with automated scanning tools.
- Ensure you validate the scan results to identify security vulnerabilities, system misconfigurations, and flaws of the targets.
- Prioritize security vulnerabilities based on their severity, exploitability, and potential impact. Leverage the **Common Vulnerability Scoring System (CVSS)** to help determine the appropriate severity ratings for each security vulnerability found.
- Ensure you identify any false positives. These are security vulnerabilities that are incorrectly reported by the scanning tool.

In the next section, we will take a look at an exploitation checklist.

Exploitation

Using the information about the vulnerabilities, the penetration tester will do their research and create specific exploits that will take advantage of the vulnerabilities of the target – this is exploitation. We use exploits (malicious code) to leverage a vulnerability (weakness) in a system, which will allow us to execute arbitrary code and commands on the targeted system(s).

The following is a list of guidelines for gaining access to a network/system:

- Ensure you review the findings from the vulnerability assessment.
- Perform thorough research using reliable and trustworthy sources on exploiting the security vulnerabilities.
- Verify the exploitability of each identified security vulnerability by performing automated and manual testing. Sometimes, testing can be done within a controlled environment, such as within a virtualized environment, to ensure the exploit is working as expected.
- Select exploitation tools and frameworks based on the target and type of security vulnerability.
- Develop the payloads based on the target and its security vulnerability.
- Test the exploit within a controlled environment.
- Execute the exploit on the real targeted system(s) to determine whether a vulnerability actually exists or not.
- Monitor the behavior of the targeted system during and after launching the exploit and document any findings.

In the next section, we will outline the essentials for a post-exploitation checklist.

Post-exploitation

After exploiting a targeted system or network, performing post-exploitation techniques enables penetration testers to gather sensitive information such as users' login credentials and password hashes, impersonate high-privilege user accounts to gain access to other systems, perform lateral movement to go deeper and ex-

pand the foothold into hidden areas of the network, and use pivoting techniques to perform host discovery and exploitation through a compromised host.

The following is a list of guidelines for maintaining access to a network/system:

- Establish persistence with multiple implants on each compromised system.
- Perform privilege escalation to exploit security misconfigurations.
- Expand the foothold on the network while staying in the scope.
- Set up **Command and Control** (**C2**) operations.
- Perform data exfiltration.

In the next section, we will outline the fundamentals for a covering-tracks checklist.

Covering tracks

Covering tracks focuses on removing any traces, exploits, payloads, and even backdoors that are installed on targeted systems during the penetration test. This phase is important because it focuses on cleaning up any residual traces of evidence that were left behind by the penetration tester with the intention of simulating what a real threat actor will do.

The following is a list of guidelines for covering tracks:

- Ensure you understand the legal and ethical boundaries for clearing all tracking activities on a system. Obtain written legal permission if you are unsure.

- Take a systematic approach to which systems and types of data are to be cleared, how the log data will be cleared, and whether there's any potential impact of this activity.
- Identify tracks for clearing, such as log files, audit trails, temporary files, and forensic artifacts on a system.
- Disable auditing features on the system.
- Clear log files.
- Remove any malware or persistence configurations.
- The systems should be reverted to their state prior to the penetration test.

Next, you will explore the guidelines for report writing.

Report writing

The final phase of a penetration test is reporting and delivering results and helping the organization remediate the findings from the penetration test. In this phase, an official document is created by the penetration tester outlining the following:

- All vulnerabilities found on targeted systems.
- All risks, categorized on a scale of high, medium, and low, based on the CVSS calculator.
- Constructive feedback to the organization as they try to recover/fix things.
- Recommendations to resolve all security vulnerabilities that were found.

Ensure when you are writing your report that it will be understood by anyone who reads it, including non-technical audiences such as senior management and

executive staff members. Managerial staff are not always technical as they are more focused on ensuring the business goals and objectives are met within the organization.

The post-engagement phase of penetration testing is a critical process. This is where the penetration tester communicates the official report, containing all the findings and recommendations to the organization/client for improving their security posture.

The following is the typical post-engagement process in penetration testing:

- **Data analysis and documentation** – This includes the collection and analysis of all findings, including the vulnerability assessment, types of security vulnerabilities found, how each exploit was compromised, their potential impact, and severity ratings. In addition, provide recommendations on how to resolve or mitigate each security issue.
- **Report preparation** – Develop a comprehensive report that summarizes all the findings during the penetration test in an easy-to-understand manner for both technical and non-technical personnel. Furthermore, the report should be organized using the report structure mentioned below and should have appendices containing supporting evidence, references, and further technical information for the client.
- **Review and quality assurance** – Before providing the report to the client, ensure it's reviewed internally to verify its accuracy, completeness, and the consistency of all findings with recommendations. Furthermore, quality assurance

helps validate whether the report is aligned with the client's requirements, using industry standards and best practices.

- **Reporting to the client** – The report should be delivered to the client using secure communication channels to maintain confidentiality. For instance, using secure email services enables you to encrypt email messages with attachments. Furthermore, ensure you schedule a debriefing session with the client to discuss all the findings and recommendations in further detail and to answer any questions or concerns about the penetration testing report.
- **Debriefing session** – The debriefing session includes the client's IT team, key stakeholders, and management team. During this session, the executive report is used to provide an overview of the findings and to emphasize the critical security vulnerabilities that were identified.
- **Remediation planning and follow-up** – Work with the client to develop a remediation plan to resolve all the security vulnerabilities during the penetration test, provide additional support and guidance through this process, and follow up often to monitor the progress of the remediation effects to ensure the organization's security objectives are achieved.

The report should also contain the following:

- Cover sheet
- Executive summary
- Summary of vulnerabilities
- Test details
- Tools used during testing (optional)
- The original scope of work

- The body of the report
- Summary

Further information on penetration testing report writing can be found at **https://www.sans.org/white-papers/33343/**.

Always remember that if you ask 10 different penetration testers how to write a report, they all will give different answers based on their experience and their employers. Be sure not to overwhelm the report with too many images or too many technical terms that will confuse the reader. It should be simple to read for anyone, including the non-technical staff of the organization, and should be actionable.

Having completed this section, you have learned the fundamentals of performing a penetration test on a system and network. Next, we will discuss some tools you may need for your hacker's tool bag.

Creating a hacker's toolkit

Being in the field of ethical hacking and penetration testing won't feel complete without creating your very own hacker's toolkit with some very cool gadgets. Having physical tools and gadgets is not always mandatory, but they help when simulating various real-world cyber-attacks.

ESP8266 microcontroller

The following is an **ESP8266 microcontroller**, running custom firmware created by *Spacehuhn*:

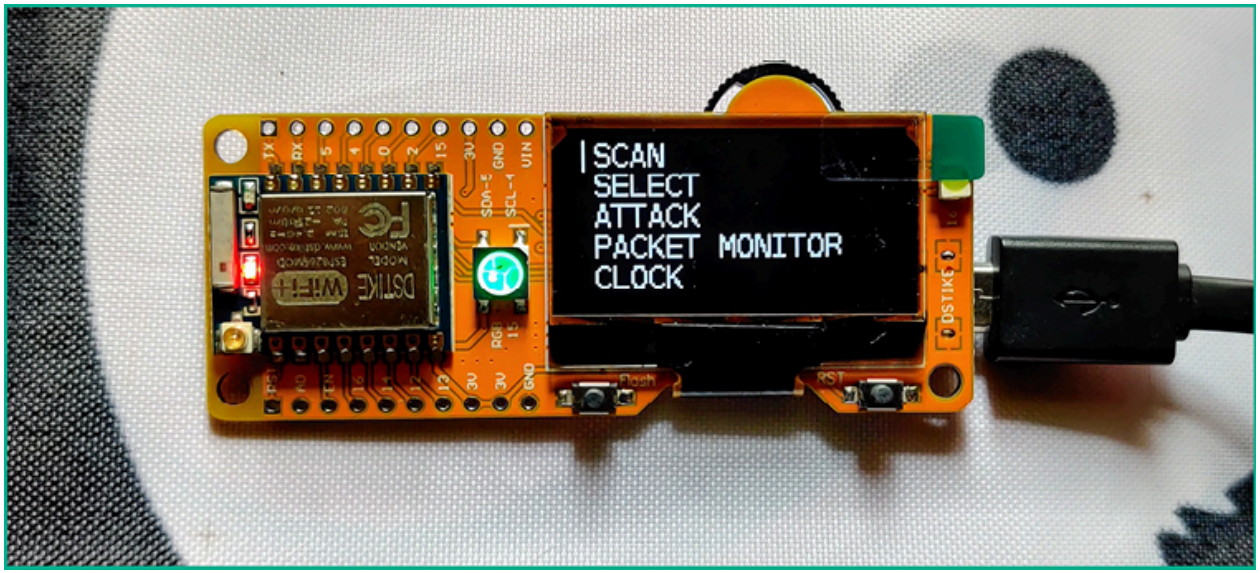

Figure 18.1: ESP8266 microcontroller

This tool assists penetration testers when performing simulated attacks on a targeted wireless network. The custom **Deauther** firmware allows you to perform wireless reconnaissance and de-authentication attacks, capture wireless probes and beacons, perform wireless confusion attacks, and even detect de-authentication attacks by threat actors.

To learn more about Spacehuhn's Deauther firmware for the ESP8266, please see

https://github.com/SpacehuhnTech/esp8266_deauther.

WiFi Pineapple Nano

The following is a **WiFi Pineapple Nano** by *Hak5*, which allows a penetration tester to perform wireless security auditing and testing on both personal and enterprise wireless networks:

Figure 18.2: WiFi Pineapple Nano

This physical tool allows a penetration tester to attach a battery bank to support power to this handheld portal device, which can fit in your backpack or pocket. You can perform wireless reconnaissance on wireless networks, capture wireless security handshakes, create rogue wireless networks, and more.

More details on the WiFi Pineapple can be found at https://shop.hak5.org/products/wifi-pineapple.

Bash Bunny

Another great tool for your hacker's tool bag is the **Bash Bunny** by *Hak5*, a fully operating Linux machine in the form of a physical USB-attached storage device:

Figure 18.3: Bash Bunny

The Bash Bunny looks like a USB flash drive, but when it's connected to a computer, it's recognized as a network. It creates a logical network between the computer and itself, providing a dynamic IP address to the host machine via a preconfigured **Dynamic Host Configuration Protocol** (**DHCP**). This tiny device can be used to perform reconnaissance, scanning, enumeration, device profiling, data exfiltration, and more, all within a few seconds.

To learn more about the Bash Bunny, please see https://shop.hak5.org/products/bash-bunny.

Packet Squirrel

To perform interception of a network-based attack, the **Packet Squirrel** by *Hak5* is another tool equipped with preconfigured scripts for the rapid deployment of network monitoring and attack mitigation tools that runs Linux:

Figure 18.4: Packet Squirrel

The Packet Squirrel is a very tiny tool that allows penetration testers to perform **Man-in-the-Middle** (**MiTM**) attacks. Another very cool feature of this tiny device is the ability to establish **Virtual Private Network** (**VPN**) access between an ex-

ternal device and itself, therefore allowing penetration testers remote access to a network.

To learn more about the Packet Squirrel, please see https://shop.hak5.org/products/packet-squirrel.

LAN Turtle

Another network implant that runs Linux is the **LAN Turtle** by *Hak5*:

Figure 18.5: LAN Turtle

The LAN Turtle is a special device that allows penetration testers to remotely access it via a VPN connection from an external network such as the internet. Additionally, penetration testers are able to simulate various types of real-world cyber-attacks through this device.

To learn more about the LAN Turtle, please see https://hak5.org/products/lan-turtle.

Mini USB-powered network switch

Having a mini USB-powered network switch can be handy at times; the following is an image of a network switch that is only a few inches in size:

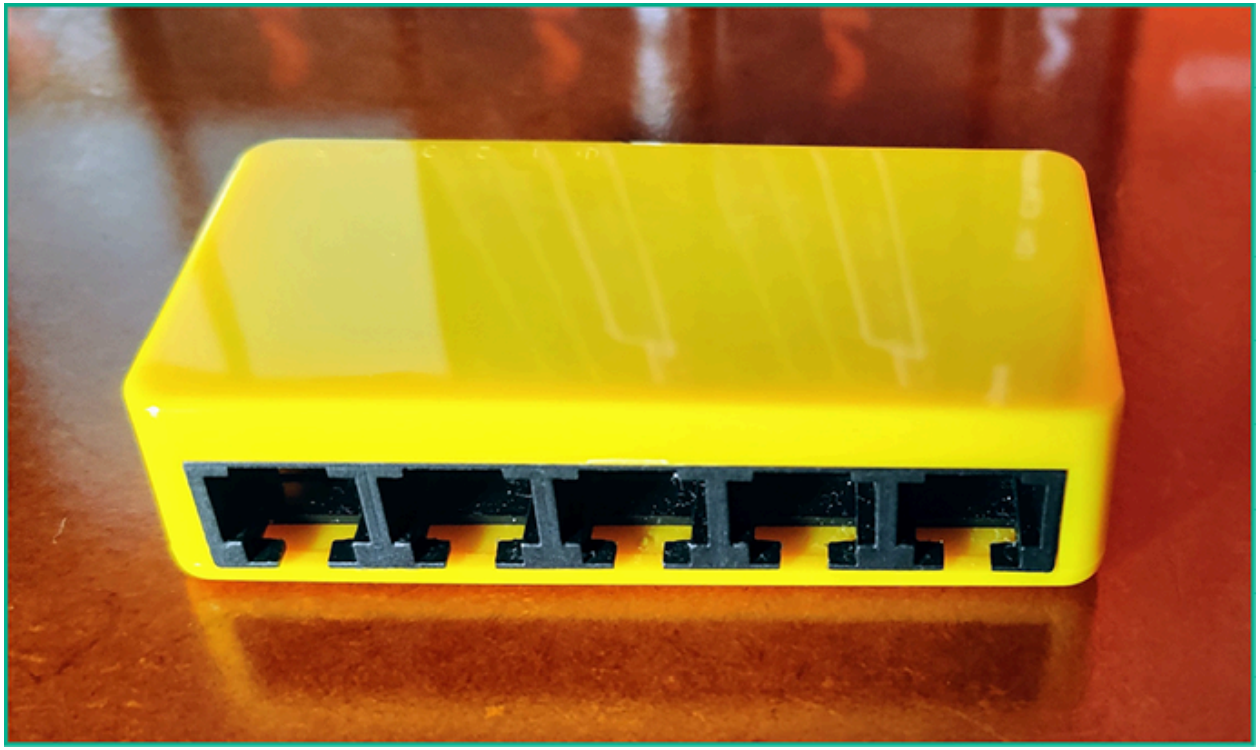

Figure 18.6: Mini USB-powered network switch

There may be a time when you need to interconnect a few devices during your penetration testing exercise and will need a network switch, so having a mini USB-powered network switch will be most useful.

To learn more about the mini network switch, please see https://shop.hak5.org/products/micro-ethernet-switch.

Retractable network cable

Having some networking cables can be handy but sometimes messy, as the cables can become physically entangled with each other. However, a retractable network cable such as the following may be useful:

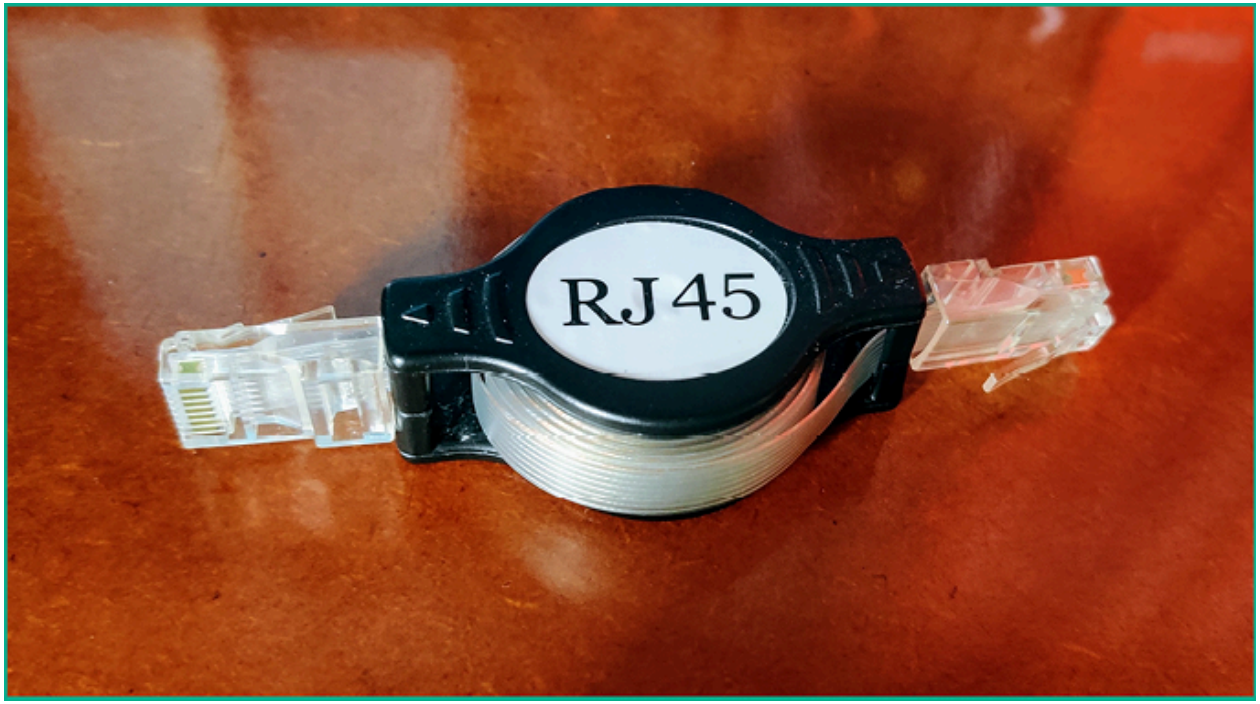

Figure 18.7: Retractable network cable

Flipper Zero

Lastly, there's the popular **Flipper Zero** device that's used for security testing on wireless networks, access control systems, **Near Field Communication** (**NFC**) technologies, **Radio Frequency Identification** (**RFID**) systems, and much more:

Figure 18.8: Flipper Zero

To learn more about the Flipper Zero, please see https://flipperzero.one/.

Sometimes, penetration testers will deploy a **Raspberry Pi** with Kali Linux at their client's location and remotely perform their penetration testing engagements. The component shown in this section is not mandatory but simply an example of some items in a typical penetration tester's backpack.

In the next section, you will learn how to set up end-to-end access between your penetration testing machine at a client's location and your computer.

Setting up remote access

As an aspiring penetration tester, you will be given the opportunity to visit your client's location to perform a penetration test on their network. This means you will need to have a dedicated computer – preferably a laptop or a mini computer – at the client's location for ethical hacking and penetration testing. On this system, you can set up remote access such as **Secure Shell** (**SSH**) and **Remote Desktop Protocol** (**RDP**) to enable you and your team to remotely work without being on-site.

The following are some of my personal recommendations for setting up your penetration-testing machine:

- A laptop running a Microsoft Windows operating system that supports **Remote Desktop**. Keep in mind that Microsoft Windows is a personal choice, and you are free to use any operating system of your personal preference. Ensure there is support for remote access across a network.
- Ensure the laptop supports **BitLocker** (available on Microsoft Windows); store all confidential information within the BitLocker drive. If you're using an operating system other than Microsoft Windows, ensure there is support for data encryption.
- For password cracking using Hashcat, you can collect the password hashes from the targeted systems on the client's network and securely transfer the hashes onto your password-cracking machine at your office for offline pass-

word cracking. Therefore, your password-cracking machine should have a dedicated **Graphics Processing Unit** (**GPU**) to leverage the GPU features of Hashcat.

- If your password-cracking machine is running Microsoft Windows as the host operating system, install and use Hashcat on the host operating system. This enables Hashcat to directly access the power of the GPU during password cracking.
- Use a hypervisor such as VMware Workstation Pro and install Kali Linux as a virtual machine. In my personal experience, VMware Workstation Pro provides direct access to the hardware resources on the host machine as compared to other hypervisors, such as Oracle VM VirtualBox and Microsoft's Hyper-V, and this is a major benefit when working with virtualization technologies.

  For instance, when connecting wireless adapters to a virtual machine, the process is seamless compared to the other hypervisor applications. Using a virtual machine helps manage your snapshots and provides better flexibility for running multiple operating systems on the same physical computer. However, you also have the choice of running Kali Linux on a bare-metal setup on a dedicated laptop or mini computer with remote access.

- Ensure you have one or more wireless network adapters that support packet injection and are compatible with your host operating system and Kali Linux. Also, ensure these wireless adapters operate on the 2.4 GHz and 5 GHz spectrum.
- Configure a VPN to securely access your penetration tester's machine at the client's location from your local office/home.

In this section, you will learn how to set up a host-to-host network service that utilizes features such as VPN and **Software-Defined Networking (SDN)** to ensure you have full end-to-end connectivity between your devices without having to configure your firewall or routing settings. During this exercise, you will learn how to use **ZeroTier** (`www.zerotier.com`) to establish secure network connectivity between your penetration testing machine at your client's location and your computer at your office or home.

The following diagram provides a visual representation of a penetration tester's machine at a client's location with the actual penetration tester working remotely.

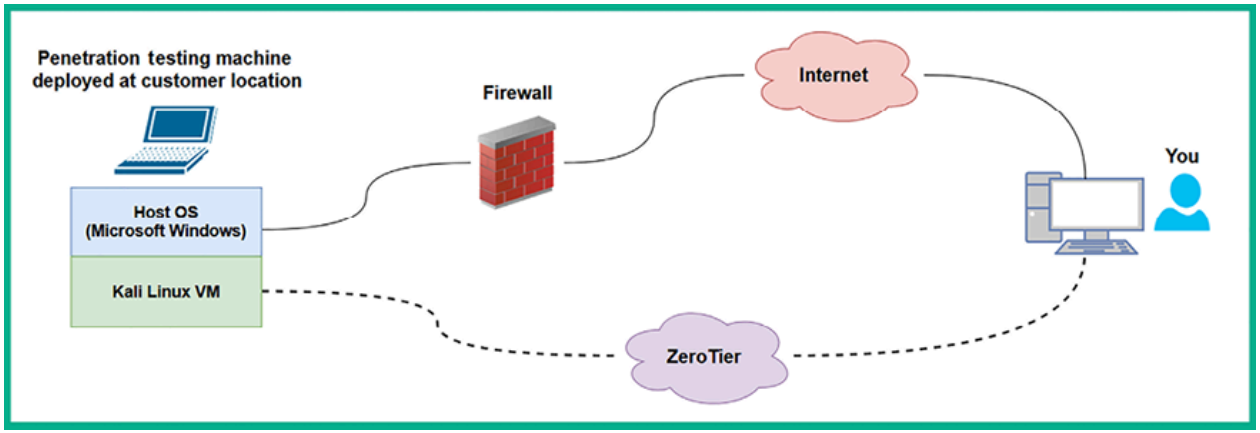

Figure 18.9: Remote access topology

As shown in the preceding diagram, the penetration tester's machine is deployed at a client's location. It is usually behind multiple network devices and security solutions, such as switches, routers, and firewalls. This creates a challenge for the

penetration tester to work remotely because the network-based firewall at the client's location will usually block the connection.

However, ZeroTier enables users to create a virtual network with up to 25 devices within a single virtual network on their platform; therefore, you can add both your penetration tester's machines and another computer, or more. Additionally, ZeroTier is considered to be a push-through VPN service that finds ways to metaphorically punch through a firewall and connect to the ZeroTier servers on the internet. Since this is possible with ZeroTier, you can use this to access any device on any network when an internet connection is available on systems that are running the ZeroTier agent on system boot/startup.

To get started setting up ZeroTier, please use the following instructions as your guide:

1. Firstly, go to the official ZeroTier website at `https://www.zerotier.com/` and click on **Sign Up** to register for a free account.
2. Next, using your newly created user credentials, log in to the user dashboard at `https://my.zerotier.com/`.
3. To create a new network on ZeroTier, click on **Networks** > **Create A Network**, as shown in the following screenshot:

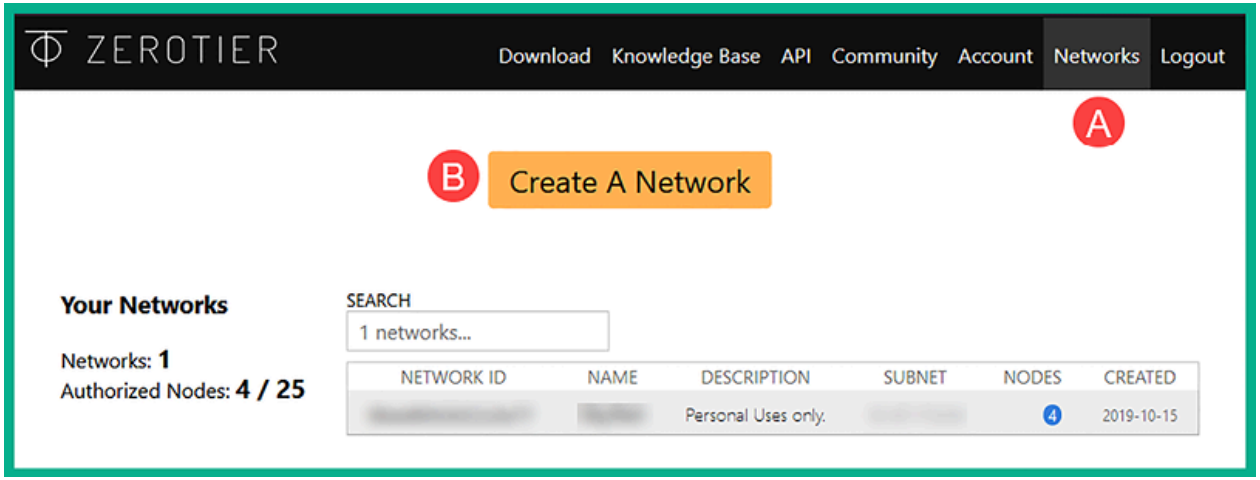

Figure 18.10: ZeroTier dashboard

4. Next, ZeroTier will generate a new network with a random **NETWORK ID** and **NAME**; click on the name of the newly created network ID to access its settings, as shown below:

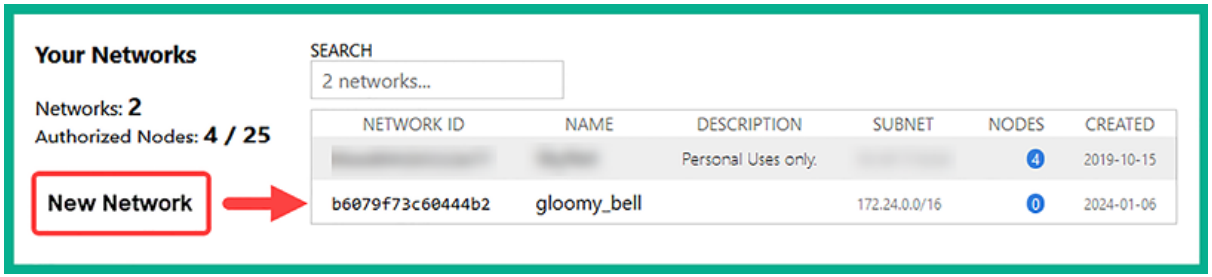

Figure 18.11: New ZeroTier network

I would recommend changing the name of the network to something that helps you better understand the purpose of the network. Additionally, setting a

description is also very beneficial.

5. Next, install the ZeroTier client on the host operating system of your computer at your office location. This computer will be used to remotely access the penetration tester's machine at the client's location. Go to the following ZeroTier downloads page to download and install the agent: https://www.zerotier.com/download/.
6. Once the ZeroTier agent is installed on your computer, launch the application. Once it is running, the ZeroTier agent icon will appear on the taskbar; right-click on the agent, select **Join New Network**, enter the 16-digit network ID, and click on **Join**.
7. Next, head back to the ZeroTier dashboard of your network settings. Scroll down to the **Members** section and you will notice your new client will soon appear. By default, a client's request to join the network has to be manually approved by the creator of the network/account. To authorize the client, click on the checkbox under **Auth?**, as shown in the following screenshot:

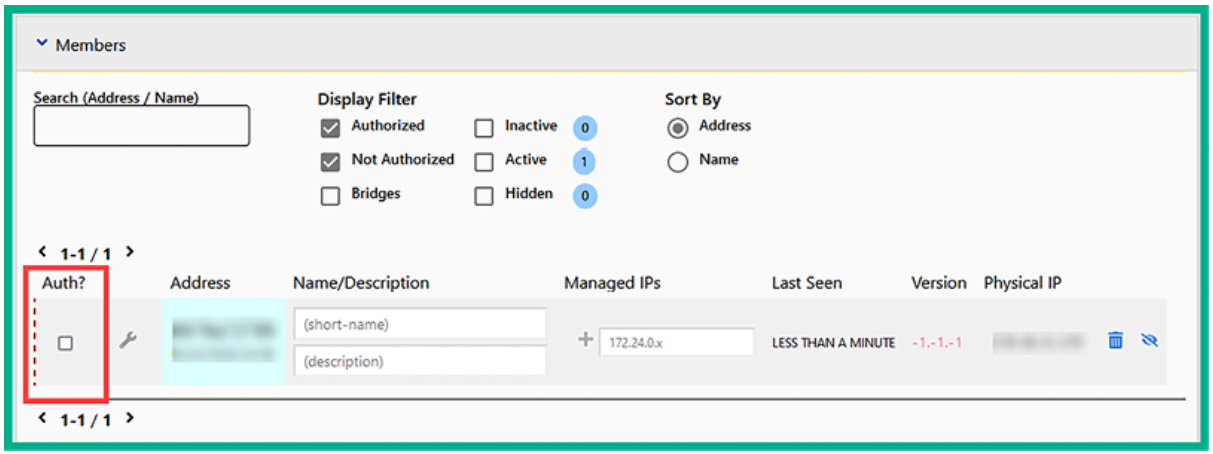

Figure 18.12: New client

Ensure you set a name and description for each approved agent on the ZeroTier network. The naming convention will help you to identify devices, roles, and IP addresses on the ZeroTier network.

8. After a few seconds, ZeroTier servers will automatically assign a private IPv4 address to the newly approved agent, which will be accessible by any device within the same ZeroTier virtual network, as shown below:

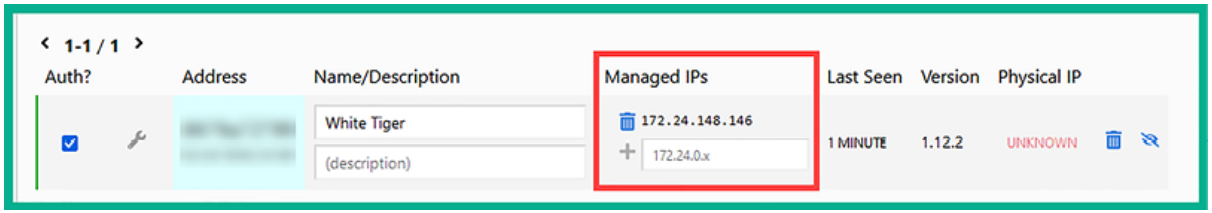

Figure 18.13: Managed IP address

Join more devices, such as the penetration testing laptop or mini computer, to the same network so that they can directly connect to each other via the private IPv4 address assigned by ZeroTier to the client device.

9. Next, if your penetration testing laptop is running Microsoft Windows as the host operating system, use the following link, which contains the official documentation on how to enable Remote Desktop on supported versions of Windows: **https://www.microsoft.com/en-us/windows/learning-center/use-windows-remote-desktop-to-access-pc**.
10. Lastly, ensure the ZeroTier agent is configured to automatically run as a service when your penetration testing machine boots. This allows you to

ship/send your penetration testing machine to your customer and simply inform them to power on and connect it to their network. The ZeroTier VPN and SDN service will automatically connect the ZeroTier servers, and you will be able to see whether the device is online or not via the ZeroTier dashboard. Using another computer on the same ZeroTier network, you can have secure end-to-end connectivity.

You may be wondering whether to set up ZeroTier on the Kali Linux virtual machine too. This is a personal choice based on your preference and how you plan on using both your penetration testing machine and Kali Linux during a real penetration test. You can add both the host operating system and Kali Linux on your penetration testing machine if you wish, as ZeroTier currently supports up to 25 devices on a single ZeroTier account.

Ensure you change the default passwords on Kali Linux and enable SSH if you are going to be remotely accessing your Kali Linux virtual machine. The following are additional useful commands:

- Start the SSH service – `sudo systemctl start ssh.service`
- Restart the SSH service – `sudo systemctl restart ssh.service`
- Stop the SSH service – `sudo systemctl stop ssh.service`
- Automatically start the SSH service when Kali Linux boots – `sudo systemctl enable ssh.service`

To install and set up the ZeroTier agent on Kali Linux, please use the following instructions:

1. Update the software package repository file and install the `libssl3` package:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install libssl3
```

2. Restart Kali Linux.
3. Next, use the following commands to get the ZeroTier agent to install:

```
kali@kali:~$ DV_SAVE=$(cat /etc/debian_version)
kali@kali:~$ echo testing | sudo tee /etc/debian_version >/dev/null
kali@kali:~$ curl -s https://install.zerotier.com | sudo bash
kali@kali:~$ echo $DV_SAVE | sudo tee /etc/debian_version >/dev/null
```

Credit to Airman (**https://airman604.medium.com/about**) for their workaround using the commands in *step 3*. A direct link to the blog post can be found here: **https://airman604.medium.com/install-zerotier-on-kali-linux-ed7bd76845c0**.

4. Next, use the following commands to join the agent with your ZeroTier network:

```
kali@kali:~$ sudo zerotier-cli join <netowkr-ID>
```

To learn more about the ZeroTier CLI, use the `man zerotier-cli` command to view the manual page.

5. Lastly, ensure you authorize the Kali Linux ZeroTier agent via the ZeroTier dashboard, as shown below:

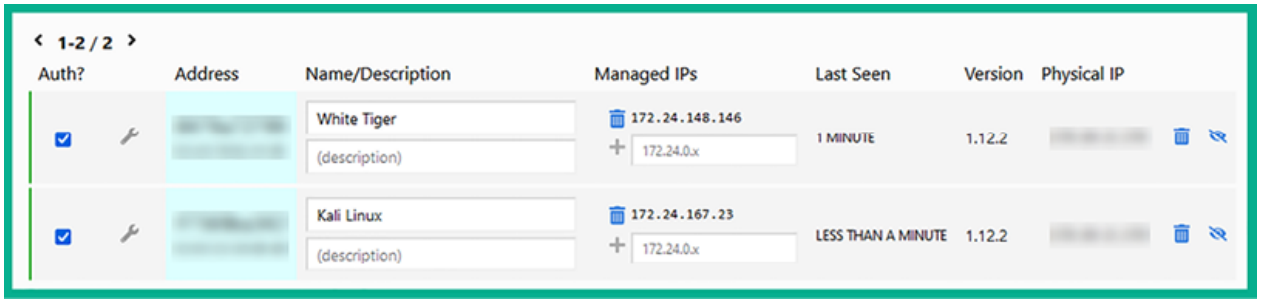

Figure 18.14: ZeroTier agents

Sometimes, a **Graphical User Interface** (**GUI**) is more convenient to use rather a **Command-Line Interface** (**CLI**) on Kali Linux. While SSH is commonly used by IT and cybersecurity professionals within the industry, it would be nice to use the GUI of Kali Linux over a remote session. Unfortunately, Linux-based operating systems do not natively support RDP, as it's a Microsoft application. However, **XRDP** was created for Linux-based systems, which enables IT professionals to establish remote desktop sessions similarly to using RDP on Microsoft Windows.

To set up XRDP on Kali Linux, please use the following commands:

```
kali@kali:~$ sudo apt update
kali@kali:~$ sudo apt install -y kali-desktop-xfce xorg xrdp
kali@kali:~$ sudo sed -i 's/port=3389/port=3390/g' /etc/xrdp/xrdp.ini
kali@kali:~$ sudo systemctl enable xrdp --now
```

At this point, you have set up a host-to-host VPN between your Kali Linux virtual machine, the penetration tester's machine, and your work computer at your office. In addition, you have automatically enabled SSH to run each time Kali Linux boots up and have installed and set up XRDP for remote desktop access.

To learn how to access Kali Linux via a web browser, please see **https://www.kali.org/docs/general-use/**. Check out the Kali Linux Undercover mode: **https://www.kali.org/docs/introduction/kali-undercover/**.

Having completed this section, you have gained the skills to set up secure remote access to your penetration testing machine. In the next section, you will see some recommendations on how to continuously enhance your skills.

Next steps ahead

Never stop learning – there's always something new to learn within the cybersecurity industry. If you want to further your learning and skills, take a look at the following online resources:

- TryHackMe: **https://tryhackme.com/**

- Hack The Box: https://www.hackthebox.com/
- RangeForce Community Edition: https://go.rangeforce.com/community-edition-registration

Both *TryHackMe* and *Hack The Box* are online platforms that help everyone, from beginners to seasoned professionals, gain new skills in various fields of cybersecurity. Both platforms allow learners to complete challenges in a gamified environment to earn rewards. Participating and growing your profile on either platform can be used as part of your portfolio when applying for jobs within the cybersecurity industry.

At the time of writing this chapter, *RangeForce Community Edition* is currently free for anyone to register and complete various cybersecurity blue team learning paths. As an aspiring ethical hacker and penetration tester, understanding the blue team side of cybersecurity will help you gain insight into the tools, technologies, and strategies that are commonly used to detect and mitigate cyber-attacks within organizations.

While there are many cybersecurity qualifications from various educational and academic organizations, be sure to perform research on the learning objectives for each qualification before enrolling, ensuring it aligns with enhancing your skills and knowledge while helping you achieve your goals as a cybersecurity professional. If you're still not sure which qualification to pursue next, research some career paths and jobs in cybersecurity using the following websites:

- LinkedIn Jobs: https://www.linkedin.com/jobs
- Indeed: https://www.indeed.com/

For each interesting job title you find, take a look at the description to better understand whether it's something you would like to do as a professional; also take a close look at the preferred qualifications and skills required for the job. This information will be helpful in understanding what is expected from a professional who is applying for the job role.

Lastly, create a LinkedIn profile and start creating your *personal brand* while networking with like-minded professionals within the industry. You will learn a lot from your connections; start sharing knowledge with others and you will notice a lot of people will begin networking with you too. If you see an interesting job posted on LinkedIn, don't be afraid to connect with the job poster and ask questions about the job. Building a personal brand may seem to be a lot of work, but it's simply demonstrating your skills to the world and standing out from the crowd while showing others you are different in a positive way.

Summary

During the course of this chapter, you have learned about various guidelines that will help you to become a better ethical hacker and penetration tester, and you have also discovered some of the key components of creating a penetration testing checklist, some fun tools for creating a hacker's tool bag, and how to securely access your Kali Linux machine while performing penetration testing remotely.

Lastly, I know the journey of preparing to be an ethical hacker and penetration tester isn't an easy one and there are many challenges along the path on the road to success. I would personally like to thank you very much for your support in purchasing a copy of my book and congratulations on making it to the end while

acquiring all these amazing new skills in ethical hacking and penetration testing techniques and strategies using Kali Linux. I do hope everything you have learned throughout this book has been informative for you and helpful in your journey to becoming super-awesome in the cybersecurity industry and beyond.

Further reading

- Master Services Agreement – https://www.rapid7.com/legal/msa/
- Rules of engagement – https://hub.packtpub.com/penetration-testing-rules-of-engagement/
- Penetration testing methodologies – https://wiki.owasp.org/index.php/Penetration_testing_methodologies
- OWASP testing checklist – https://github.com/tanprathan/OWASP-Testing-Checklist
- PayloadsAllTheThings – https://github.com/swisskyrepo/PayloadsAllTheThings

Join our community on Discord

Join our community's Discord space for discussions with the author and other readers:

https://packt.link/SecNet