Computer Science and Information Technologies
Vol. 4, No. 1, March 2023, pp. 69~75
ISSN: 2722-3221, DOI: 10.11591/csit.v4i1.p69-75

Selected advanced themes in ethical hacking and penetration testing

Buthayna AlSharaa, Saed Thuneibat, Rawan Masadeh, Mohammad Alqaisi
Department of Electrical Engineering, Al-Balqa Applied University, As-Salt, Jordan

Article Info

Article history:

Received Oct 23, 2022
Revised Jan 18, 2023
Accepted Jan 31, 2023

Keywords:

Brute force attack
Ethical hacking
Kali Linux
Samba exploits
Telnet exploits

ABSTRACT

Since 1980 cyberattacks have been evolving with the rising numbers of internet users and the constant evolving of security systems, and since then security systems experts have been trying to fight these kinds of attacks. This paper has both ethical and scientific goals, ethically, to raise awareness on cyberattacks and provide people with the knowledge that allows them to use the world wide web with fewer worries knowing how to protect their information and their devices with what they can. Scientifically, this paper includes a deep understanding of types of hackers, attacks, and various ways to stay safe online. This research investigates how ethical hackers adapt to the current and upcoming cyber threats. The different approaches for some famous hacking types along with their results are shown. Python and Ruby are used for coding, which we run on Kali Linux operating system.

Corresponding Author:

Buthayna AlSharaa
Department of Electrical Engineering, Al-Balqa Applied University
As-Salt, Jordan
Email: buthayna-alsharaa@bau.edu.jo

1. INTRODUCTION

The internet made our life easier by making the whole world as big as a small village. Networks are the base of the internet and computers because a computer without an internet connection is almost useless. Networks connect computers to exchange data through cables, and radio waves. Since networks are all about exchanging data that contains personal information, the most important factor of a network is to protect this data from hackers who use it for a variety of reasons [1]. For example, identity theft, black mail and personalize phishing attacks. The most famous and known way to stay safe on the web is to always be ahead of your hacker and think like one.

A hacker is a person who gains or attempts to gain unauthorized access to computer systems. Many cases have reported incidents of hackers not only gaining unauthorized access but also manipulating data which caused different threats to companies and celebrities [1], [2]. On the other hand, the ethical hacker is involved in a workspace, works with a team and certified professionals. Ethical hackers work for the best of their company and do the right thing by trying to find loopholes before the hackers do, there is no personal motive drawing them towards what they are doing. Ethical hackers' goal is to make their system stronger and less affected by threats leading to improvement in the security of the system [3]–[5]. Ethical hackers play an important role in identifying the risks in the system and pointing out their weaknesses [4], [5].

Not every hacker is a cyber-criminal who is willing to take over your personal information, there is more than one category for hackers, and they are divided into six different groups. Black hat, white hat, and grey hat are the main three and the other three are green, blue, and red hats. A black hat hacker is a hacker with a very wide range of knowledge in network protocols and knows how to get into computer systems usually for financial profit and tends to steal and damage personal data by malwares. A white hat hacker or an ethical

hacker is a hacker with great knowledge but chooses to use his knowledge on good terms. He uses the same methods as black hat hackers but with him committed to ethics. Sometimes white hat hackers can be employees whose job is to find security holes in systems, and they perform penetration tests. A grey hat hacker, as known as grey is a color in between black and white so the same goes in our case here, they usually look for weaknesses in the systems without the owner permission and if they find an issue, they report it to the owner and request an amount of money for fixing the problem. This type of hacker does not mean to harm people they just look for credit for issues they find on their own, but still, it is considered illegal because he didn't ask for the permission and authorization of the owner. A green hat hacker is an inexperienced hacker who lacks technical skills. A blue hat hacker is like a white hat hacker but employed by Microsoft to find weaknesses in windows. But in another scenario, blue hats are hackers that seek revenge, so it depends on who you are categorizing. A red hat hacker is a hacker who targets LINUX systems. He tries to attack black hats and stop them from harming people but not by handing them to authorities. They launch attacks against them and destroy their resources [6]–[8].

Article [9] suggest that information security can be thought of as "audit" for computer. Article [10] offers that ethical hacking maybe one of the most effective ways to proactively plug rampant security vulnerabilities in the security of the internet. Systems and hacking skills may be viewed as something like auditing skills as both attempt to uncover issues.

Kali Linux is a tool that can be used for network analysts, penetration testers, or any other cybersecurity and analytics practice. This paper uses Kali to perform Metasploit-related experiments on certain targets as part of Ethical Hacking to exploit their vulnerabilities. A Metasploit framework is an open-source software under Kali that provides a set of tools to perform a penetration test and security auditing [11]–[13].

There are different types of attacks on the internet and for these different attacks there are different solutions. Sometimes these solutions are not the perfect ones. Finding security holes in online applications and object-oriented software that are linked to the internet or other cyber stations is possible with the help of ethical hacking. The key issue is how to secure data in the digital sphere that could be stolen by hackers.

Finding vulnerabilities in web sites and programs that are connected with internet or cyber stations is made possible by ethical hacking. Normal users may be using some important programs to share files and interconnect with each others that may be penetrated. The major contribution of this paper is explaining these systems, and show how they can be penetrated. Finally, we made a set of recommendations for users to prevent them from these attacks [14], [15].

The paper structure is the following: in section 2, the method used is presented. Section 3 details the different experimental results. Finally, the conclusions are presented in section 4.

2. METHOD

2.1. Security testing and penetration

Security testing is software that finds loopholes in systems that can be used by hackers. The main purpose of security testing is to identify possible threats for the developers to fix through coding. Some security test tools are Grabber and Vega.

The terms "ethical hacking" and "penetration testing" are often used interchangeably when referring to the process of verifying an organization's systems, but they are slightly different. Penetration testing is a simulation of a cyber-attack against the system to check for vulnerabilities [16]. Penetration testing is performed by certified professionals, hired by the organization, and given access to a certain amount of privileged information to perform on-site audits to discover and exploit existing vulnerabilities. On the other hand, ethical hackers may not be official employees of the organization. Their purpose in examining organizations' systems may be for entertainment. They may find it tempting to use their discovery for criminal gain - moving from a "white hat" to a "black hat" hacker [17]. Some penetration test tools are Powershell-suite and Zmap [18].

2.2. Phases of hacking

Hacking typically involves five phases. These five procedures don't have to be carried out in order by a hacker. Following it will produce a better outcome because it is a step-by-step method. The five stages of hacking are [17], [19]:

- Information Gathering is the first step of hacking and happens during penetration testing. It has two types: passive and active. The type of information that can be found through passive information gathering is subdomains and public IP addresses, usernames and passwords, emails, phone numbers, and Leaked credentials. The type of information that can be found through active information gathering are API keys, IP address ranges, and technologies used. Tools for information gathering are WHOIS, Google, Maltego, Intercepting Proxies, Web Spiders, and Netcraft.

- Scanning starts after gathering information. We scan for open ports and weak loops to get into the system and after finding the perfect vulnerable spot we go to the next step which is gaining access. Tools for scanning are Acunetix, Solar Winds Network Device Scanner, and PRTG Network Monitor.
- Gaining Access is when the hacker breaks into computing devices through a network using several tools. Every operating system on these devices has some vulnerabilities and gaps that attackers can use to gain access to the system. After gaining access, the attacker must get his way to the administrator level to install an application or get data and can occur locally, offline, or over a network [17]. Examples of attacks for gaining access are password attacks, Stack-based buffer overflows, social engineering, Malware attack, and Session hijacking.
- Maintaining Access starts after entering the system. the hacker should stay in the system without the user noticing until the hacker finishes what he aimed to do, and this can be done using Trojans and Rootkits.
- Installing Backdoors- a backdoor is a hidden entry point that offers access to a website without the user knowing. They are designed in a way to blend in with the rest of the website and they are hard to detect.
- Covering Tracks is the last step. After gaining access and when we are ready to leave the system nothing should be left behind, logs must be deleted. No evidence of an attack should be left behind. Some of the methods used to cover tracks over Network to remain undetectable are installing a reverse hypertext transfer protocol (HTTP) shell on the victim computer, carrying traffic via covert channels using internet control message protocol (ICMP) packets, and using transmission control protocol (TCP) parameters.

2.3. Exploits for Linux targets

One of the best environments used for hacking and penetration testing is Kali Linux distro since it is made specifically for hackers [20], [21]. It has a variety of tools already installed and ready to use. For ethical hacking and penetration testing using virtual box to install Kali Linux as a virtual machine is used for a safe environment to do penetration testing and hacking without the risk of being hacked by more experienced hackers.

2.3.1. Telnet exploit

This vulnerability is only possible due to information disclosure from the target. It happens exclusively when the login information is written on the banner. Steps to hack into a telnet session are:

- Install Telnet on your machine by typing the command “apt-get install telnetd” on the terminal.
- Connect to Telnet by typing “telnet 192.168.1.28”

The IP address used is the IP for the target. When connected to the telnet port successfully, we can see the login info written in the banner then we can login using this information and have full control of the target. This kind of exploit can be avoided by not installing vulnerable software on your computer that can be a gate for hackers into your device. In addition, keep your firewall active at all times because it blocks the connection to port 23 for untrusted networks [22].

2.3.2. Samba exploit

Samba is a free networking tool available for both Unix/Linux and windows. It allows file and resource sharing between these different operating systems [23]. Steps to exploit samba are:

- open Metasploit to search for a scan to help us identify the exact Samba version running on the target by entering the command “msfconsole”.
- choose the right tool for version information by entering the command “auxiliary/scanner/smb/smb_version”.
- Use the scan chosen by entering the command “useauxiliary/scanner/smb/smb_version”.
- Use the command “searchsploit samba 3.0.20” to search for an exploit for the version running on the target
- choose the exploit “use unix/remote/16320.rb”

All versions of samba from 3.5.0 downward are vulnerable to remote code execution exploits [24]. To protect this tool, never open your shares to the public, always keep your samba software up to date, and disable SMBv1 protocol on your Linux by editing the file “/etc/samba/smb.confto” and setting the following:

```
server min protocol = SMB2_10
client max protocol = SMB3
client min protocol = SMB2_10
```

2.3.3. Brute force attack

A brute force attack is when the attacker tries different passwords and usernames combinations to gain access to the target machine [25], [26]. This attack usually works when the attacker knows the target personally and may use personal information as a guess for the password (birthday and nickname). This

attack is also very common with targets using default passwords (password, admin123, and password123). This exploit can be avoided by changing the default password for any downloaded software, choosing your password to be 12 characters or more. Include special characters, numbers, and upper-case letters in your password.

3. RESULTS AND DISCUSSION

In this section, we will go through the five stages of hacking we mentioned above. As mentioned in previous section, each section has a set of operations. We will show how to use the tools available to each stage along with the information obtained.

3.1. Information gathering

In this step, we are looking for any information about the target that can help us with the hacking process. This information can be IP addresses, Emails, Phone numbers, and Technologies used by the target such as the type of software's running, what operating systems they have, how was a certain website built, what programming languages are used. Ping command can be used to get an IP address from a website as shown in Figure 1.

"Whois" is another tool that can be used to get a domain's specific details, such as contract dates, registrant information, and assigned DNS. This information is all collected from a global database that holds it. It also enables an IP to provide us with information about the country from which it originates, the internet service provider in charge of it, and a ton of other technical data. Figure 2 shows the output of this tool.

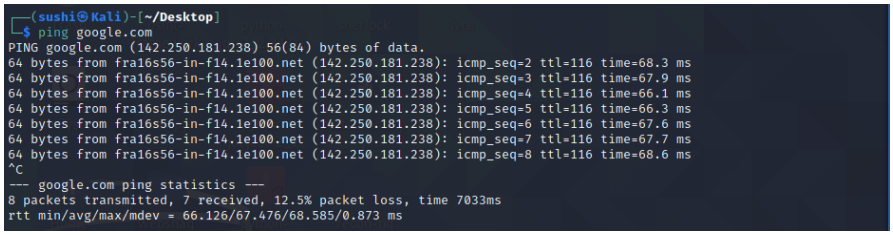

Figure 1. Obtaining IP address from a website

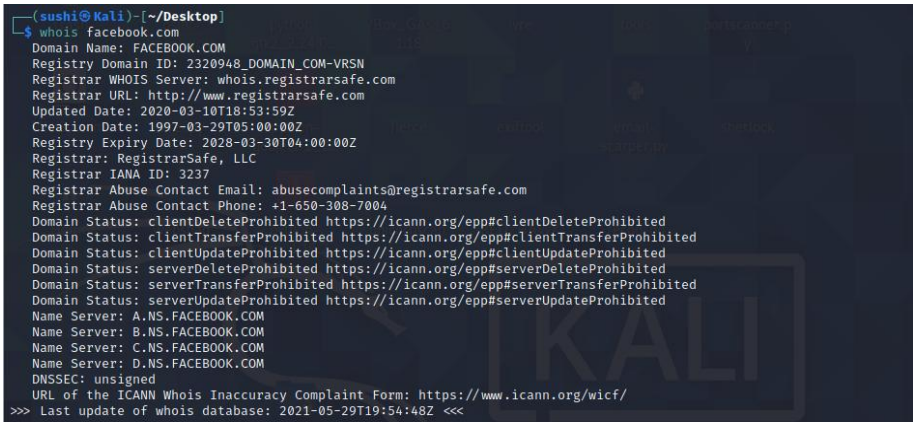

Figure 2. Information gathered using WHOIS

3.2. Scanning

Scanning is the second phase of penetration testing. Certain tools are used to find vulnerabilities in the target. Vulnerabilities can be gateways, open ports, and operating systems. By scanning our target, we can figure out how the target is vulnerable and how we can take advantage of it.

The packets sent to the target will be TCP or user datagram protocol (UDP). In this step, we are looking for open ports and virtual open ports that are used to connect to the internet. Important ports to look for can be port 80, port 443, port 21, and others.

A secure system is a system that has all its ports closed such as home devices because they do not need to host any system. Web pages must have port 80 and port 443 open to be able to be connected to. Large companies have other open ports such as port 21.

Our preferred scanning tool is Nmap which is the Abbreviation of network mapper. Nmap is free and open-source, and it is used to discover hosts and services on a computer network by sending packets and analyzing the responses. Nmap has many modes to choose from for different targets which are all explained in its help menu. Figure 3 shows the Nmap scan output.

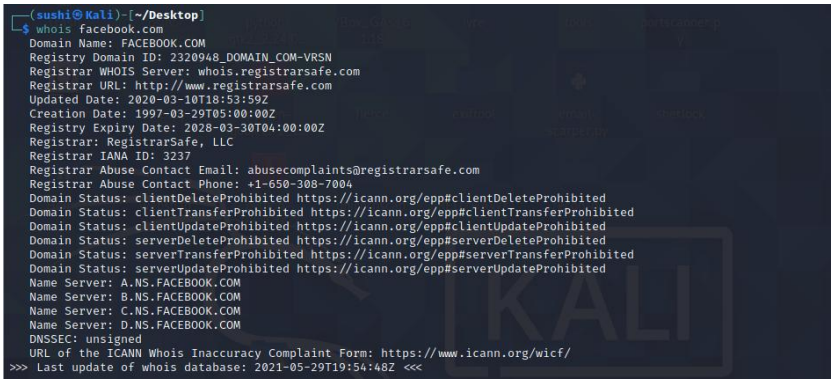

Figure 3. Nmap scan results

3.3. Gaining access

This is the third step in penetration testing, and it allows us to gain access to the target and its data. The hacked target then can be used to attack other devices. After this step, we can say that the penetration test was successful. Exploiting a target is using the target vulnerabilities we discovered to run a payload on it; a payload is a program that we deliver to the target after the exploit, usually, this program is something that allows us to execute commands on the target system and navigate through its files and folders. If the target does not have technical vulnerabilities, we use social engineering to trick the user to open our payload and run it for us. this can be done by a spoof email which is an email address that looks familiar to the user.

The tool used in this step is Metasploit framework, which is a powerful tool used by ethical hackers [26]. It has a lot of ready exploits for the most vulnerable software, and it's a free and open customizable source. Figure 4, shows the Metasploit available options [26].

Figure 4. Metasploit framework help options

3.4. Maintaining access

This step is optional, and it is done if the client wants to know if his network is penetrable. It is commonly done by installing backdoors and planting fruit kits. backdoors and planting fruit kits are programs that will allow us to gain access to that target whenever we want without the need to exploit it again.

3.5. Covering tracks

This step is the final step in penetration testing. All evidence that an attack ever took place is removed. It includes deleting files, editing files, and reverting any changes made to the system.

4. CONCLUSION

Ethical hackers search for loopholes in the network to protect users and systems from any threats. In general, some safe practices on networks include changing passwords periodically and not using the same password for all accounts. It is recommended to use original software and update it regularly. ports should be scanned periodically, and unused ones should be closed to prevent unauthorized access. Firewall can block targeted source IP address when detected. They must be configured correctly to enforce rules to deny traffic from dangerous and unknown sources.

REFERENCES

[1] I. Brown, L. Edwards, and C. Marsden, "Information security and cybercrime," *LAW AND THE INTERNET, 3rd Ed., L. Edwards, C. Waelde, eds., Oxford: Hart*, 2009.

[2] S. M. Furnell and M. J. Warren, "Computer hacking and cyber terrorism: The real threats in the new millennium?," *Computers and Security*, vol. 18, no. 1, pp. 28–34, Jan. 1999, doi: 10.1016/S0167-4048(99)80006-6.

[3] S. Patil, A. Jangra, M. Bhale, A. Raina, and P. Kulkarni, "Ethical hacking: The need for cyber security," in *IEEE International Conference on Power, Control, Signals and Instrumentation Engineering, ICPCSI 2017*, Sep. 2018, pp. 1602–1606. doi: 10.1109/ICPCSI.2017.8391982.

[4] P. Chandra Behera, "Ethical hacking: A security assessment tool to uncover loopholes and vulnerabilities in network and to ensure protection to the system," *Chinmaya Dash International Journal of Innovations & Advancement in Computer Science IJIACS ISSN*, vol. 4, pp. 2347–8616, 2015.

[5] B. Sahare, A. Naik, and S. Khandey, "Study of ethical hacking," *International Journal of Computer Science Trends and Technology*, vol. 2, no. 4, pp. 6–10, 2014, [Online]. Available: www.ijcstjournal.org

[6] R. Banda, J. Phiri, M. Nyirenda, and M. M. Kabemba, "Technological paradox of hackers begetting hackers: A case of ethical and unethical hackers and their subtle tools," *Zambia ICT Journal*, vol. 3, no. 1, pp. 40–51, Mar. 2019, doi: 10.33260/zictjournal.v3i1.74.

[7] X. Zhang, A. Tsang, W. T. Yue, and M. Chau, "The classification of hackers by knowledge exchange behaviors," *Information Systems Frontiers*, vol. 17, no. 6, pp. 1239–1251, Dec. 2015, doi: 10.1007/s10796-015-9567-0.

[8] M. Warren and S. Leitch, "Hacker taggers: A new type of hackers," *Information Systems Frontiers*, vol. 12, no. 4, pp. 425–431, Sep. 2010, doi: 10.1007/s10796-009-9203-y.

[9] P. Logan, "Crafting an undergraduate information security emphasis within information technology," *Journal of Information Systems Education*, vol. 13, no. 3, p. 177, 2002, [Online]. Available: http://proquest.umi.com.library.capella.edu/pqdweb?did=247934171&Fmt=7&clientId=62763&RQT=309&VName=PQD

[10] R. Hartley, D. Medlin, and Z. Houlik, "Ethical hacking: Educating future cybersecurity professionals," in *Proceedings of the EDSIG Conference*, 2017, vol. 2473, no. October, pp. 1–10. [Online]. Available: http://proc.iscap.info/2017/pdf/4341.pdf%0Ahttp://iscap.info

[11] D. Bhatt, "Modern day penetration testing distribution open source platform-Kali Linux-study paper," *International Journal of Scientific and Technology Research*, vol. 7, no. 4, pp. 233–237, 2018.

[12] S. Sinha, S. Sinha, and Karkal, *Beginning ethical hacking with Kali Linux*. Springer, 2018.

[13] P. Cisar and R. Pinter, "Some ethical hacking possibilities in Kali Linux environment," *Journal of Applied Technical and Educational Sciences*, vol. 9, no. 4, pp. 129–149, 2019, [Online]. Available: http://doi.org/10.24368/jates.v9i4.139http://jates.org

[14] M. Bishop, "About penetration testing," *IEEE Security and Privacy*, vol. 5, no. 6, pp. 84–87, Nov. 2007, doi: 10.1109/MSP.2007.159.

[15] M. C. Ghanem and T. M. Chen, "Reinforcement learning for efficient network penetration testing," *Information*, vol. 11, no. 1, p. 6, Dec. 2019, doi: 10.3390/info11010006.

[16] M. Intal tayag and M. emmalyn Asuncion de vigal capuno, "Compromising systems: Implementing hacking phases," *International Journal of Computer Science and Information Technology*, vol. 11, no. 02, pp. 27–35, Apr. 2019, doi: 10.5121/ijcsit.2019.11203.

[17] C. T. Phong, "A study of penetration testing tools and approaches," Auckland University of Technology, 2016. [Online]. Available: http://aut.researchgateway.ac.nz/bitstream/handle/10292/7801/ChiemTP.pdf?sequence=3&isAllowed=y

[18] E. Bash, "Ethical hacking and countermeasures: Attack phases," *PhD Propos*, vol. 1, 2015.

[19] M. Hertzog, Raphael, O'Gorman, Jim, Aharoni, "Kali Linux revealed - Google Books," *Offsec Press*, p. 314, 2017, [Online]. Available: https://www.google.co.uk/books/edition/Kali_Linux_Revealed/6n9atAEACAAJ?hl=en

[20] M. Hammoudeh *et al.*, "Network traffic analysis for threat detection in the internet of things," *IEEE Internet of Things Magazine*, vol. 3, no. 4, pp. 40–45, Dec. 2021, doi: 10.1109/iotm.0001.2000015.

[21] "Linux in a windows world," *Choice Reviews Online*, vol. 43, no. 02, pp. 43–992, Oct. 2005, doi: 10.5860/choice.43-0992.

[22] S. Saito, K. Maruhashi, M. Takenaka, and S. Torii, "TOPASE: Detection and prevention of brute force attacks with disciplined IPs from IDS logs," *Journal of Information Processing*, vol. 24, no. 2, pp. 217–226, 2016, doi: 10.2197/ipsjjip.24.217.

[23] K. T. Dave, "Brute-force attack 'seeking but distressing'','" *Int. J. Innov. Eng. Technol. Brute-force*, vol. 2, no. 3, pp. 75–78, 2013.

[24] S. Nyrbok, "Review: Metasploit framework + armitage - pentesting tools," *PivotPoint Technology Corp*, 2015.
[25] Y. Kolli, T. K. Mohd, and A. Y. Javaid, "Remote desktop backdoor implementation with reverse TCP payload using open source tools for instructional use," in *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference, IEMCON 2018*, Nov. 2019, pp. 444–450. doi: 10.1109/IEMCON.2018.8614801.
[26] R. Seema and N. Ritu, "Penetration testing using metasploit framework: an ethical approach," *International Research Journal of Engineering and Technology(IRJET)*, vol. 06, no. 08, pp. 538–542, 2019, [Online]. Available: https://www.academia.edu/40379823/IRJET-PENETRATION_TESTING_USING_METASPLOIT_FRAMEWORK_AN_ETHICAL_APPROACH

BIOGRAPHIES OF AUTHORS

Buthayna AlSharaa Received her master's degree in computer engineering from Jordan university for science and technology, Jordan in 2006. Now she is an lecturer at Al-Balqa Applied University–Al-huson University College, Jordan. Her research interests include data and network security, Artificial Intelligence, and algorithms, Cloud computing, Routing protocols, Embedded Systems, network programming. She can be contacted at email: buthayna-alsharaa@bau.edu.jo.

Dr. Saed Thuneibat received his BSc in Automatic telecommunication Engineering from Novosibirsk State University in 1994. He received his M.Sc. and Ph.D. in telecommunication/networks engineering from the same university, Russia 2005. Currently, he is an associate professor at the Department of Electrical Engineering at Al-Balqa` Applied University, Jordan. His research interests are fiber optics, digital communication systems, and networking. He can be contacted at email: Saed1970@Bau.edu.jo.

Rawan Masadeh holds a bachelor's degree in communication and Software Engineering from AlBalqa Applied University and currently pursuing a master's in computer science from Kennesaw state university. Research interests: Artificial Intelligence, Cyber Security, Data Science. She can be contacted at email: Rawanmassadeh98@gmail.com.

Mohammad Alqaisi holds a bachelor's degree in communication and Software Engineering from AlBlaqa Applied University and currently works as a Content Moderator at WebHelp Enterprise. Research interests: Cyber Security, Ethical Hacking, Cloud Computing. He can be contacted at email: mohammadalqaissi97@gmail.com.