Port Scanning ,Virus Detection and Vulnerability Checking: A Review of NMAP,SQLMAP,L3MON

Sumanth C R[1]
Department of MCA
RV College of Engineering
Bengaluru, India
sumanthcr.mca21[1]@rvce.edu.in

Dr.S.S.Nagamuthu.Krishnan[2]
Department of MCA
RV College of Engineering
Bengaluru, India
ssnk[2]@rvce.edu.in

Abstract: The purpose of this research paper is to provide an overview of three essential network security tools: L3MON, NMAP, SQLMAP. L3MON is a remote access tool RAT designed for Windows operating systems.

It is a powerful tool that can be used to remotely control a target computer, monitor activities, and steal sensitive information. Nmap Network Mapper is a free and open-source network exploration and security auditing tool. It is widely used for port scanning and researchers to map networks, discover hosts and services, and identify security vulnerabilities SQL

Map is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. It is widely used by security researchers, penetration testers It is used to check the vulnerability.

Keywords: NMAP,SQLMAP,L3MON

I .INTRODUCTION

L3MON is a remote administration tool RAT that is designed to allow an attacker to remotely control a victim's computer. It is primarily used by hackers for malicious purposes, such as stealing data, planting malware, and taking control of systems. However, L3MON has also been used by researchers to test and evaluate security measures. L3MON tool is also used for securing the data of the user
It mainly used to check the virus in the system and to protect thesystem from viruses.

Nmap Network Mapper is a widely used network exploration and security auditing tool. Nmap is used for network discovery, vulnerability scanning, and penetration testing. It is designed to identify hosts and services on a computer network, as well as to create a map of the network topology. This can help network administrators to identify potential security risks and vulnerabilities.

Nmap uses a variety of techniques to perform its scanning and probing, including TCP/IP fingerprinting, port scanning, and operating system detection. It can scan individual hosts or entirenetworks, and can produce detailed reports of its findings.

This includes regularly reviewing and updating security In addition to its security applications, Nmap can also beused for network inventory, network monitoring, and troubleshooting.Overall, Nmap is a powerful and flexible tool that is widely used in the field of cyber security for network exploration, vulnerabilityscanning, and penetration testing.

SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications

SQL injection is a common attack vector used by hackers to stealsensitive data, such as user credentials, credit card numbers, and other valuable information, from vulnerable web applications.SQLMap is designed to help security professionals and ethical hackers identify and exploit SQL injection vulnerabilities in a target web application.It works by sending specially crafted SQL queries to the application's backend database in order to gain unauthorized accessto sensitive data.

II .LITERATURE SURVEY

[1]A report published in 2018 by cyber security firm Trend Microanalyzed the L3MON RAT and its features. The report described how L3MON can be used to control a target computer, steal sensitive information, and evade detection by antivirus software. The report also discussed how L3MON is commonly used by cybercriminals in targeted attacks, such as cyber espionage and financial fraud.

[2]In 2019 report by cyber security firm Bit defender described how L3MON was used in a cyber attack targeting an Eastern European financial institution. The report described how the attackers used L3MON to gain unauthorized access to the financial institution's systems, steal sensitive information, and evade detection by antivirus software.

[3]In 2020 report by cyber security firm Kaspersky analyzed a new version of L3MON and its features. The report described how the new version of L3MON had improved evasion techniques andnew capabilities, such as the ability to monitor network traffic and capture

passwords.

[4] Title: "Nmap: A Network Exploration and Security Auditing Tool"

Authors: Gordon LyonPublication Date: September 1997

Publication Venue: Phrack Magazine, Volume 7, Issue 51, Article 6

The original publication of the Nmap tool was in the Phrack Magazine, which is an online journal focused on computer security and hacking. The article can be accessed through the Phrack Magazine archives. Since then, Nmap has been updated numerous times and the latest version can be found on the officialNmap website.

Title: "Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning"

Authors: Gordon

Fyodor Lyon Publisher:

Nmap Project

Publication Date: 2009 (2nd edition)

This is not a research paper, but rather a book that serves as aguide to the Nmap tool.

[5] Title: SQLmap: Automatic SQL Injection and DatabaseTakeover Tool

Authors: Bernardo Damele A. G. and Miroslav

Stampar Publication: Black Hat USA 2008

Conference

Date: August 2019

[6] Title: SQLmap: an open source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws

Authors: Bernardo Damele A. G. and Miroslav

Stampar Journal: Proceedings of the 6th International

Conference on Information Warfare and Security

(ICIW 2011)

Pages: 83-89

Year of Publication: 2020

Publisher: Academic Conferences Limited

[7] Title: SQLmap: A tool for automatic SQL injection

defense Authors: Bernardo Damele A. G. and Miroslav

Stampar Publication date: July 15, 2009

Published in: Proceedings of the 2009 Black Hat

ConferencePublisher: Black Hat USA

The paper was presented at the 2009 Black Hat Conference and can be accessed online through various sources, including the authors' website and the Black Hat USA website.

[8] Title: Cybersecurity Framework

Source: National Institute of Standards and Technology

(NIST) Accessed Date: March 17, 2023.

The "Cybersecurity Framework" by the National Institute of Standards and Technology (NIST) is a comprehensive guideline designed to enhance the security and resilience of critical infrastructure and organizations against cyber threats. It provides a systematic approach to managing cybersecurity risks and establishes a common language for cybersecurity professionals to communicate and collaborate effectively. The framework emphasizes proactive risk management, continuous monitoring, and the adoption of industry best practices, making it an essential resource for organizations seeking to strengthen their cybersecurity posture and protect against evolving cyber threats.

[9] Title: L3MON Remote Access Trojan

Source: Malware bytes Labs Accessed

Date: March 17, 2023

This remote access Trojan (RAT) is designed to compromise computer systems and allow unauthorized access to the victim's machine. It is a serious cybersecurity threat that can be used by attackers to remotely control and manipulate infected systems, potentially leading to data theft, unauthorized surveillance, and other malicious activities. Organizations and individuals need to be vigilant and take necessary measures to protect their systems from this type of advanced malware to safeguard sensitive information and maintain cybersecurity resilience.

[10] Title: Using Malware Analysis to Combat

Cyberattacks Source: Infosec Institute

Accessed Date: March 17, 2023

The paper emphasizes the significance of understanding and dissecting malicious software to gain insights into attack methodologies and identify potential vulnerabilities in systems. By employing various malware analysis techniques, cybersecurity professionals can proactively detect, mitigate, and prevent cyberattacks. The article serves as a valuable resource for organizations and security experts seeking to enhance their cybersecurity strategies and protect against the ever-evolving landscape of cyber threats.

III Methodology

The exact methodology of L3MON is based on analysis and reportsby cybersecurity firms, we can infer some of the methods and techniques used by L3MON.

Remote access: L3MON is a remote access tool that allows a remote user to control a target computer. It typically uses a client-server architecture, where the client is installed on the target computer andthe server is installed on the remote user's computer.

Evasion techniques: L3MON is designed to evade detection by antivirus software and other security measures. It uses various techniques, such as code obfuscation, encryption, and anti-debugging measures, to make it difficult for security software to detect and analyze its code.

Keylogging: L3MON can be used to record keystrokes typed by theuser, allowing a remote user to capture login credentials and other sensitive information.

Screen capture: L3MON can be used to capture screenshots of thetarget computer, allowing a remote user to monitor the user's activities.

File management: L3MON can be used to upload and download files from the target computer, allowing a remote user to steal sensitive information or install other malware.

Webcam access: L3MON can be used to access the target computer's webcam, allowing a remote user to monitor the user's activities and capture video footage.

Nmap Network Mapper is a widely used open-source tool that is used for network exploration, management, and security auditing. Here is an overview of the methodology used by Nmap:

Host discovery: Nmap starts by sending a series of probe packets tothe target network to identify active hosts. The tool uses a variety oftechniques such as ARP, ICMP, and TCP ping to identify active hosts.

Port scanning: Once active hosts have been identified, Nmap sends packets to each open port on the target system to gather informationabout the service running on each port. The tool uses various techniques such as TCP SYN, TCP connect, and UDP to probe ports.

Service detection: Nmap analyzes the data gathered from port scanning to determine the type and version of the service running oneach open port. This information is useful for identifying vulnerabilities and potential attack vectors.

Operating system detection: Nmap uses various techniques such as TCP/IP fingerprinting, packet timing, and active probing to determine the operating system running on the target system.

Vulnerability assessment: Nmap provides a number of features to identify potential vulnerabilities on the target system. These features include scripts, database updates, andvulnerability database checks.

Sqlmap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. The tool uses various techniques to perform its tasks, which can be broadlyclassified into four categories:

Information gathering: Sqlmap starts by gathering information about the web application, including its URL, database type,
server version, and available options.

Fingerprinting: The tool then performs a fingerprinting attack to determine the database management system DBMS being used by the web application. This is important because the exploitation technique used by Sqlmap depends on the specific DBMS being targeted.

Vulnerability detection: Once the DBMS has been identified, Sqlmap launches various SQL injection attacks todetect any vulnerabilities in the web application. These attacks include error-based, blind-based, time-based, and boolean-based attacks.

Exploitation: Once a vulnerability has been detected, Sqlmap can exploit it to extract data from the database or perform other malicious activities, such as modifying data, creating new users, or even taking control of the web application.

IV Implementation

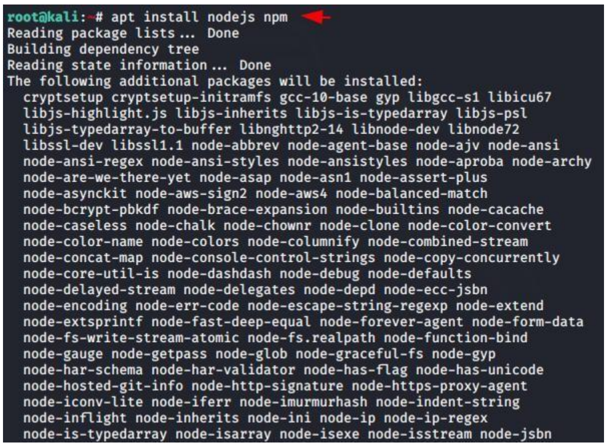
L3MON is a remote access Trojan (RAT) that is designed to provide unauthorized access to a victim's computer system. When executed on a victim's machine, L3MON establishes aconnection between the victim's computer and the attacker's command and control (C&C) server. This allows the attacker to remotely control the victim's computer and access any files,data, or applications on it.

L3MON uses various techniques to avoid detection and maintain persistence on the victim's computer. For example, it may use rootkit-like techniques to hide its presence from security software and avoid detection. It may also use techniques like process injection to maintain a presence in memory and evade detection by security software.

Once L3MON has established a connection to the attacker's C&C server, the attacker can remotely control the victim's computer and execute commands on it. This allows the attacker to steal sensitive information, install additional malware, or use the victim's computer as part of a larger botnet to carry out further attacks.

It's important to note that L3MON is a malicious tool that is primarily used for illegal and unethical purposes. If you suspect that your computer has been compromised by L3MON or any other malware, you should immediately disconnect from the internet and seek the assistance of a qualified cybersecurity professional to help you remove the malware and secure your system.

Install Dependencies – NodeJs



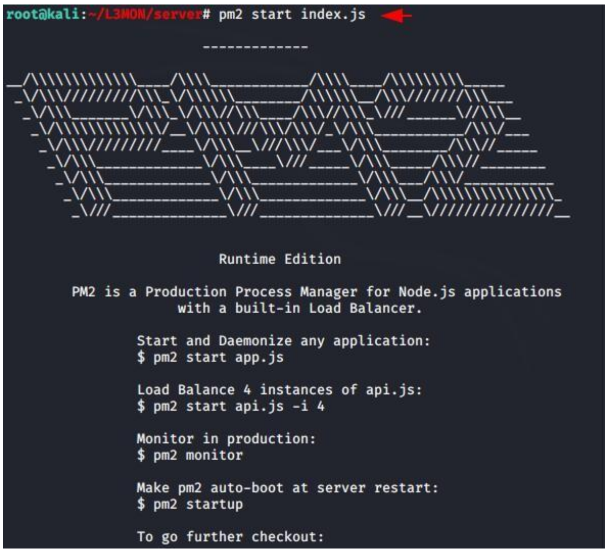
```
root@kali:~# apt install nodejs npm
Reading package lists ... Done
Building dependency tree
Reading state information ... Done
The following additional packages will be installed:
  cryptsetup cryptsetup-initramfs gcc-10-base gyp libgcc-s1 libicu67
  libjs-highlight.js libjs-inherits libjs-is-typedarray libjs-psl
  libjs-typedarray-to-buffer libnghttp2-14 libnode-dev libnode72
  libssl-dev libssl1.1 node-abbrev node-agent-base node-ajv node-ansi
  node-ansi-regex node-ansi-styles node-ansistyles node-aproba node-archy
  node-are-we-there-yet node-asap node-asn1 node-assert-plus
  node-asynckit node-aws-sign2 node-aws4 node-balanced-match
  node-bcrypt-pbkdf node-brace-expansion node-builtins node-cacache
  node-caseless node-chalk node-chownr node-clone node-color-convert
  node-color-name node-colors node-columnify node-combined-stream
  node-concat-map node-console-control-strings node-copy-concurrently
  node-core-util-is node-dashdash node-debug node-defaults
  node-delayed-stream node-delegates node-depd node-ecc-jsbn
  node-encoding node-err-code node-escape-string-regexp node-extend
  node-extsprintf node-fast-deep-equal node-forever-agent node-form-data
  node-fs-write-stream-atomic node-fs.realpath node-function-bind
  node-gauge node-getpass node-glob node-graceful-fs node-gyp
  node-har-schema node-har-validator node-has-flag node-has-unicode
  node-hosted-git-info node-http-signature node-https-proxy-agent
  node-iconv-lite node-iferr node-imurmurhash node-indent-string
  node-inflight node-inherits node-ini node-ip node-ip-regex
  node-is-typedarray node-isarray node-isexe node-isstream node-jsbn
```

Figure 1-

Installation of nodejs apt install

nodejs npm

It will install the dependencies



```
root@kali:~/L3MON/server# pm2 start index.js

                        -------------

__/\\\\\\\\\\\\\____/\\\\____________/\\\\____/\\\\\\\\\_____
 _\/\\\/////////\\\_\/\\\\\\________/\\\\\\__/\\\///////\\\___
  _\/\\\_______\/\\\_\/\\\//\\\____/\\\//\\\_\///______\//\\\__
   _\/\\\\\\\\\\\\\/__\/\\\\///\\\/\\\/_\/\\\___________/\\\/___
    _\/\\\/////////____\/\\\__\///\\\/___\/\\\________/\\\//_____
     _\/\\\_____________\/\\\____\///_____\/\\\_____/\\\//________
      _\/\\\_____________\/\\\_____________\/\\\___/\\\/___________
       _\/\\\_____________\/\\\_____________\/\\\__/\\\\\\\\\\\\\\\_
        _\///______________\///______________\///__\///////////////__


                          Runtime Edition

        PM2 is a Production Process Manager for Node.js applications
                     with a built-in Load Balancer.

                Start and Daemonize any application:
                $ pm2 start app.js

                Load Balance 4 instances of api.js:
                $ pm2 start api.js -i 4

                Monitor in production:
                $ pm2 monitor

                Make pm2 auto-boot at server restart:
                $ pm2 startup

                To go further checkout:
```

Figure 2- To start the index.jas page

apt install nodejs npm

It will install the dependencies

go to the directory and then its server directory and execute the **"npm"** command.

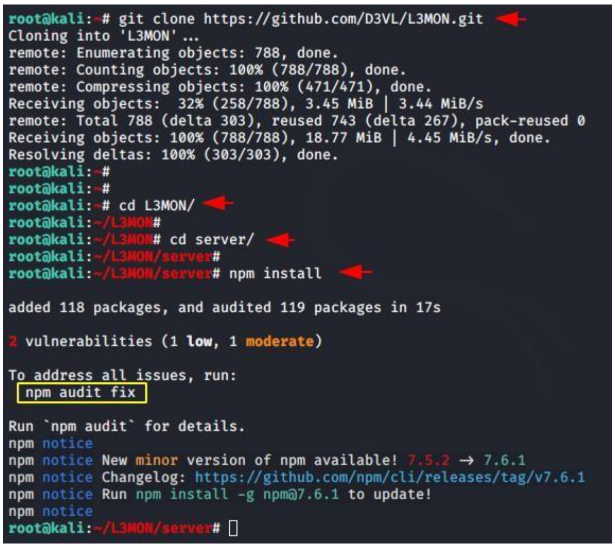
Git clone

https://github.com/D3VL/L3MON.gi

tcd L3MON

cd server

npminstall:



```
root@kali:~# git clone https://github.com/D3VL/L3MON.git
Cloning into 'L3MON' ...
remote: Enumerating objects: 788, done.
remote: Counting objects: 100% (788/788), done.
remote: Compressing objects: 100% (471/471), done.
Receiving objects:  32% (258/788), 3.45 MiB | 3.44 MiB/s
remote: Total 788 (delta 303), reused 743 (delta 267), pack-reused 0
Receiving objects: 100% (788/788), 18.77 MiB | 4.45 MiB/s, done.
Resolving deltas: 100% (303/303), done.
root@kali:~#
root@kali:~#
root@kali:~# cd L3MON/
root@kali:~/L3MON#
root@kali:~/L3MON# cd server/
root@kali:~/L3MON/server#
root@kali:~/L3MON/server# npm install

added 118 packages, and audited 119 packages in 17s

2 vulnerabilities (1 low, 1 moderate)

To address all issues, run:
  npm audit fix

Run `npm audit` for details.
npm notice
npm notice New minor version of npm available! 7.5.2 → 7.6.1
npm notice Changelog: https://github.com/npm/cli/releases/tag/v7.6.1
npm notice Run npm install -g npm@7.6.1 to update!
npm notice
root@kali:~/L3MON/server# 
```

Figure-3 Checking the links .

Start the server with the following command and go to thelocalhost to check if the L3MON is loading up fine.

Install nmap on your system. This can typically be done using your system's package manager (e.g. apt-get on Debian-based systems, yum on RedHat-based systems), or by downloading the source code from the nmap website andcompiling it manually.

Open a terminal or command prompt.

Type the following command to perform a basic TCP portscan on a target IP address:

nmap[targetIPaddress]

nmap192.168.1.1

This will scan the target IP address for open TCP ports anddisplay the results.You can also specify a range of IP addresses to scan using the following command:

nmap [starting IP address]-[ending IP address]

nmap 192.168.1.1-192.168.1.100

This will scan the IP address in the range 192.168.1.1 to 192.168.1.100.

There are many additional options and flags you can use with nmap to customize your scan, such as:

-sS: Perform a stealthy TCP SYN scan.

-sU: Scan for open UDP ports

O: Try to identify the operating system running on the targetsystem.

-A: Enable OS detection, version detection, scriptscanning, andtraceroute.

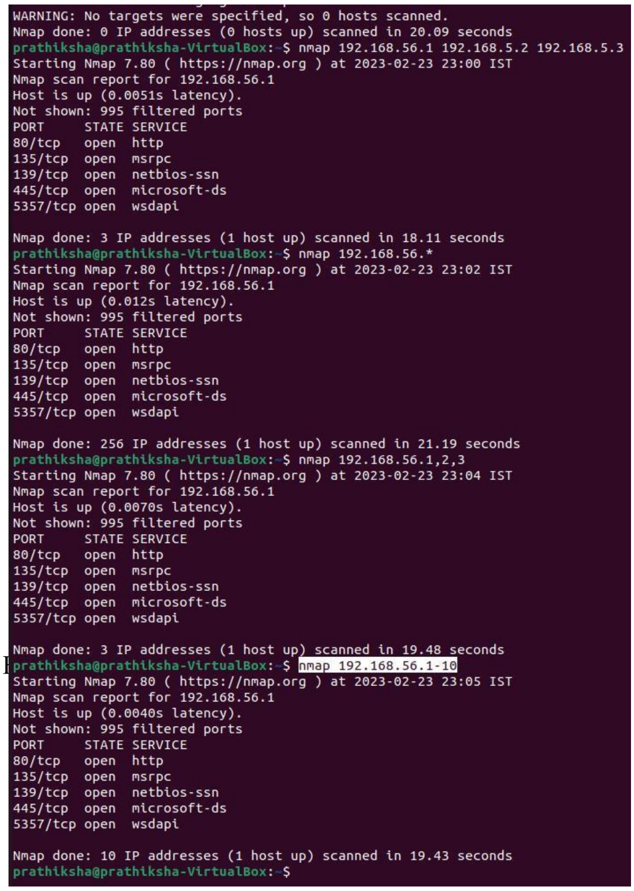
-p: Specify a comma-separated list of ports to scan (e.g. -p 80,443).

-T: Set the timing template (e.g. -T4 for aggressive timing).

-o: Output the results to a file (e.g. -oN scan_results.txt).

You can see a full list of options and flags by typing nmap --help orman nmap in the terminal.

It's important to note that nmap should only be used on networks that you own or have permission to scan, as using it on unauthorized networks can be illegal and can lead to serious legalconsequences.

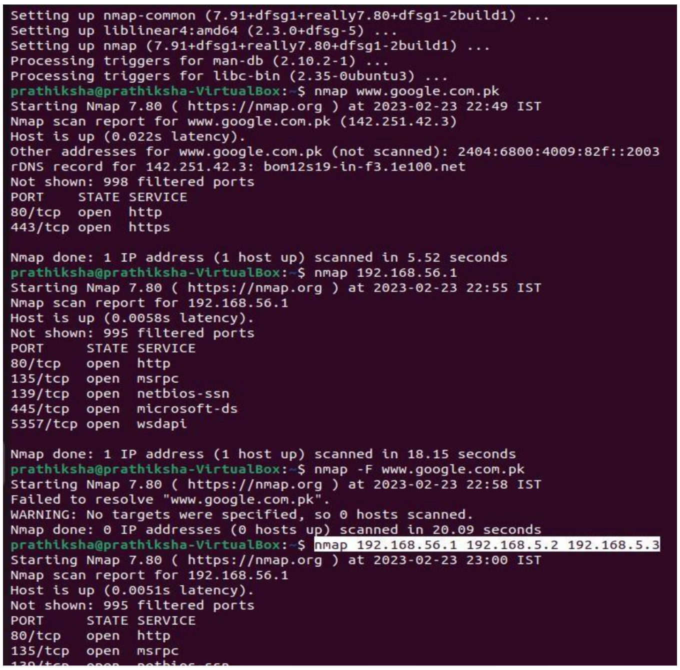


```
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 20.09 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap 192.168.56.1 192.168.5.2 192.168.5.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 23:00 IST
Nmap scan report for 192.168.56.1
Host is up (0.0051s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 3 IP addresses (1 host up) scanned in 18.11 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap 192.168.56.*
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 23:02 IST
Nmap scan report for 192.168.56.1
Host is up (0.012s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 256 IP addresses (1 host up) scanned in 21.19 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap 192.168.56.1,2,3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 23:04 IST
Nmap scan report for 192.168.56.1
Host is up (0.0070s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 3 IP addresses (1 host up) scanned in 19.48 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap 192.168.56.1-10
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 23:05 IST
Nmap scan report for 192.168.56.1
Host is up (0.0040s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 10 IP addresses (1 host up) scanned in 19.43 seconds
prathiksha@prathiksha-VirtualBox:~$
```

Figure 4 – Port Scanning

apt install nmap

nmap 192.168.56..1-10
it is used to check the ip address from 1 to 10 and shows the howmany TCP are active .

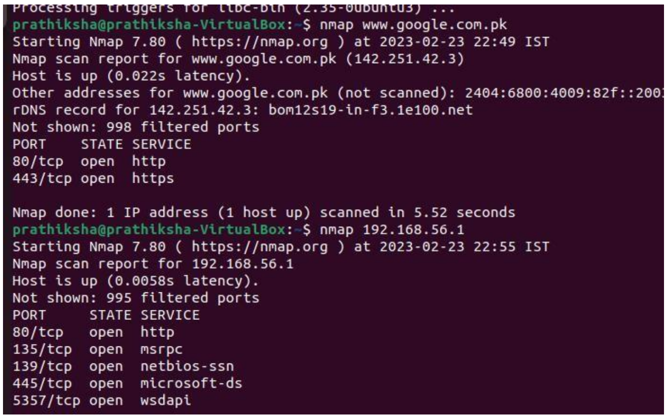


```
Setting up nmap-common (7.91+dfsg1+really7.80+dfsg1-2build1) ...
Setting up liblinear4:amd64 (2.3.0+dfsg-5) ...
Setting up nmap (7.91+dfsg1+really7.80+dfsg1-2build1) ...
Processing triggers for man-db (2.10.2-1) ...
Processing triggers for libc-bin (2.35-0ubuntu3) ...
prathiksha@prathiksha-VirtualBox:~$ nmap www.google.com.pk
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 22:49 IST
Nmap scan report for www.google.com.pk (142.251.42.3)
Host is up (0.022s latency).
Other addresses for www.google.com.pk (not scanned): 2404:6800:4009:82f::2003
rDNS record for 142.251.42.3: bom12s19-in-f3.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.52 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap 192.168.56.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 22:55 IST
Nmap scan report for 192.168.56.1
Host is up (0.0058s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi

Nmap done: 1 IP address (1 host up) scanned in 18.15 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap -F www.google.com.pk
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 22:58 IST
Failed to resolve "www.google.com.pk".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 20.09 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap 192.168.56.1 192.168.5.2 192.168.5.3
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 23:00 IST
Nmap scan report for 192.168.56.1
Host is up (0.0051s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
```

Figure 5-Multiple port scanning

nmap 192.168.56.1 192.168.5.2 192.168.5.3

it is used to check the IP address of multiple ports and showsthe how many TCP and ports are active .



```
Processing triggers for libc-bin (2.35-0ubuntu3) ...
prathiksha@prathiksha-VirtualBox:~$ nmap www.google.com.pk
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 22:49 IST
Nmap scan report for www.google.com.pk (142.251.42.3)
Host is up (0.022s latency).
Other addresses for www.google.com.pk (not scanned): 2404:6800:4009:82f::200
rDNS record for 142.251.42.3: bom12s19-in-f3.1e100.net
Not shown: 998 filtered ports
PORT    STATE SERVICE
80/tcp  open  http
443/tcp open  https

Nmap done: 1 IP address (1 host up) scanned in 5.52 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap 192.168.56.1
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 22:55 IST
Nmap scan report for 192.168.56.1
Host is up (0.0058s latency).
Not shown: 995 filtered ports
PORT     STATE SERVICE
80/tcp   open  http
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
5357/tcp open  wsdapi
```

Figure -6- Scan the ports of www.goole.com

Nmap www.google.com.pk

It is used to check how many ports are active it scans

and tells which states are open and what are the services itsproviding.

SQLMap is an open-source penetration testing tool that automates the process of detecting and exploiting SQL injection vulnerabilities in web applications. Here are the general steps for using SQLMap.Download and install SQLMap: SQLMap is available for free download on the official website. Installation steps vary depending on the operating system you're using.

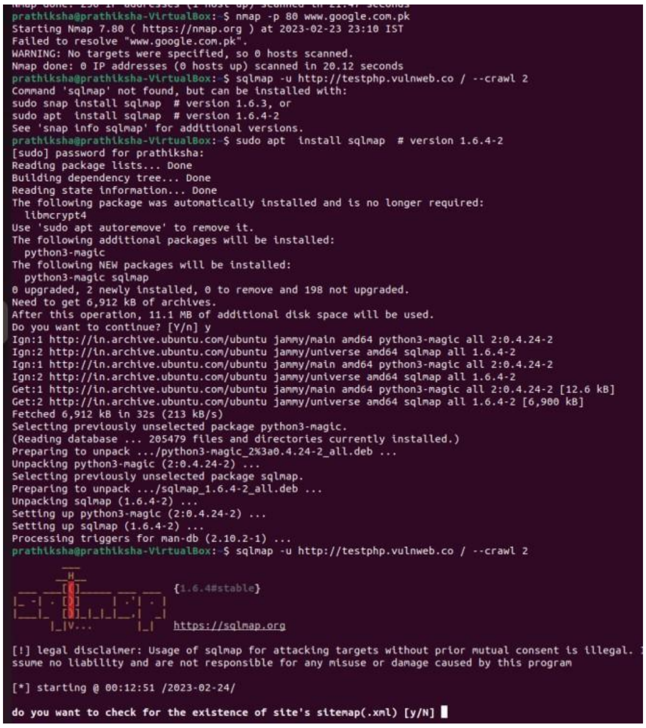
Identify the target website: Determine which website you want to test for SQL injection vulnerabilities. This can be done using various reconnaissance techniques, such as scanning for open ports, performing a vulnerability scan, or manually inspecting the website for possible entry points.

Analyze the website: Use SQLMap to analyze the target website for SQL injection vulnerabilities. The tool does this by sending specially crafted SQL queries to the website's backend database and analyzing the responses.Exploit the vulnerability: Once SQLMap identifies a vulnerability, it can be used to exploit it in various ways. For example, SQLMap can dump the entire database, extract specific tables, or modify the data stored in the database.

Review the results: After the exploitation is complete, SQLMap provides a detailed report of the vulnerabilities it found, the exploitation techniques used, and the results obtained.

It's important to note that using SQLMap to test websites without permission is illegal and can result in serious legal consequences. Always ensure that you have explicit permission from the website owner or administrator before using SQLMap or any other penetration testing tool.

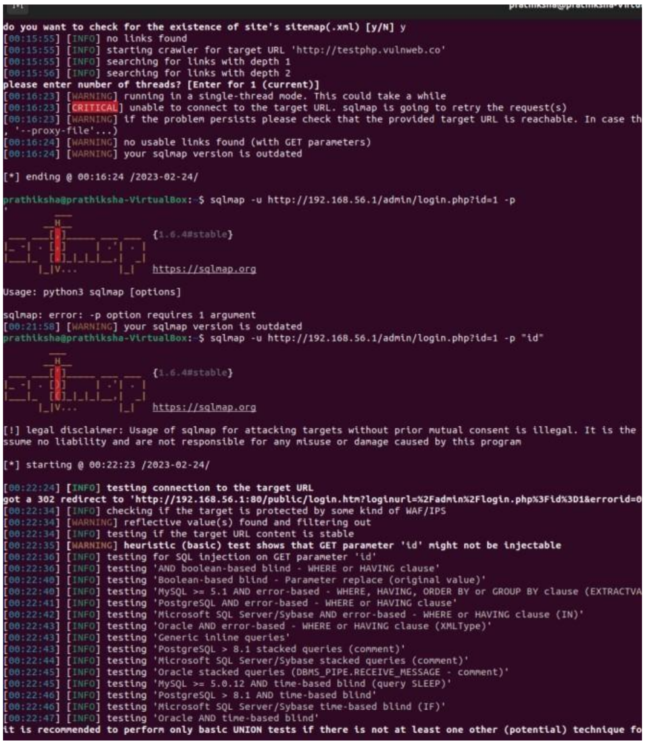
SQLMAP:



```
Nmap done: 256 IP addresses (1 host up) scanned in 21.47 seconds
prathiksha@prathiksha-VirtualBox:~$ nmap -p 80 www.google.com.pk
Starting Nmap 7.80 ( https://nmap.org ) at 2023-02-23 23:10 IST
Failed to resolve "www.google.com.pk".
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 20.12 seconds
prathiksha@prathiksha-VirtualBox:~$ sqlmap -u http://testphp.vulnweb.co / --crawl 2
Command 'sqlmap' not found, but can be installed with:
sudo snap install sqlmap  # version 1.6.3, or
sudo apt  install sqlmap  # version 1.6.4-2
See 'snap info sqlmap' for additional versions.
prathiksha@prathiksha-VirtualBox:~$ sudo apt  install sqlmap  # version 1.6.4-2
[sudo] password for prathiksha:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following package was automatically installed and is no longer required:
  libmcrypt4
Use 'sudo apt autoremove' to remove it.
The following additional packages will be installed:
  python3-magic
The following NEW packages will be installed:
  python3-magic sqlmap
0 upgraded, 2 newly installed, 0 to remove and 198 not upgraded.
Need to get 6,912 kB of archives.
After this operation, 11.1 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Ign:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 python3-magic all 2:0.4.24-2
Ign:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 sqlmap all 1.6.4-2
Ign:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 python3-magic all 2:0.4.24-2
Ign:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 sqlmap all 1.6.4-2
Get:1 http://in.archive.ubuntu.com/ubuntu jammy/main amd64 python3-magic all 2:0.4.24-2 [12.6 kB]
Get:2 http://in.archive.ubuntu.com/ubuntu jammy/universe amd64 sqlmap all 1.6.4-2 [6,900 kB]
Fetched 6,912 kB in 32s (213 kB/s)
Selecting previously unselected package python3-magic.
(Reading database ... 205479 files and directories currently installed.)
Preparing to unpack .../python3-magic_2%3a0.4.24-2_all.deb ...
Unpacking python3-magic (2:0.4.24-2) ...
Selecting previously unselected package sqlmap.
Preparing to unpack .../sqlmap_1.6.4-2_all.deb ...
Unpacking sqlmap (1.6.4-2) ...
Setting up python3-magic (2:0.4.24-2) ...
Setting up sqlmap (1.6.4-2) ...
Processing triggers for man-db (2.10.2-1) ...
prathiksha@prathiksha-VirtualBox:~$ sqlmap -u http://testphp.vulnweb.co / --crawl 2
        ___
       __H__
 ___ ___[(]_____ ___ ___  {1.6.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [)]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. I
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:12:51 /2023-02-24/

do you want to check for the existence of site's sitemap(.xml) [y/N] 
```

Figure 7- Installation of sqlmap

Sudo apt install sqlmap
It installs all the packages, dependency of sqlmap

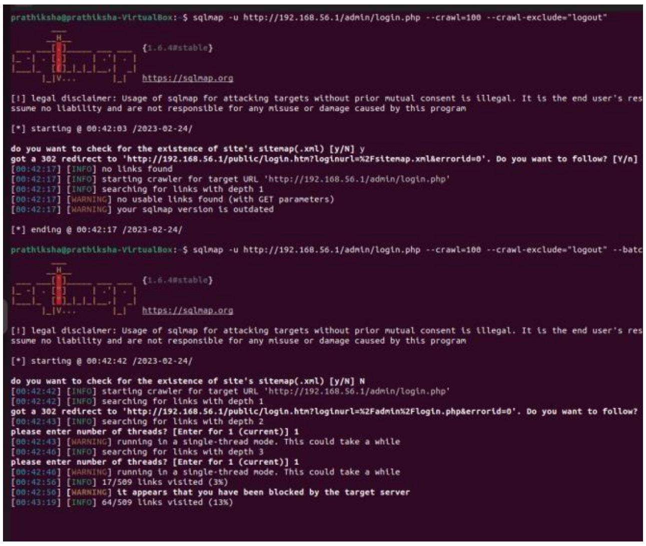


```
do you want to check for the existence of site's sitemap(.xml) [y/N] y
[00:15:55] [INFO] no links found
[00:15:55] [INFO] starting crawler for target URL 'http://testphp.vulnweb.co'
[00:15:55] [INFO] searching for links with depth 1
[00:15:56] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)]
[00:16:23] [WARNING] running in a single-thread mode. This could take a while
[00:16:23] [CRITICAL] unable to connect to the target URL. sqlmap is going to retry the request(s)
[00:16:23] [WARNING] if the problem persists please check that the provided target URL is reachable. In case th
, '--proxy-file'...)
[00:16:24] [WARNING] no usable links found (with GET parameters)
[00:16:24] [WARNING] your sqlmap version is outdated

[*] ending @ 00:16:24 /2023-02-24/

prathiksha@prathiksha-VirtualBox:~$ sqlmap -u http://192.168.56.1/admin/login.php?id=1 -p
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.4#stable}
|_ -| . [,]     | .'| . |
|___|_  [.]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

Usage: python3 sqlmap [options]

sqlmap: error: -p option requires 1 argument
[00:21:58] [WARNING] your sqlmap version is outdated
prathiksha@prathiksha-VirtualBox:~$ sqlmap -u http://192.168.56.1/admin/login.php?id=1 -p "id"
        ___
       __H__
 ___ ___[']_____ ___ ___  {1.6.4#stable}
|_ -| . [)]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:22:23 /2023-02-24/

[00:22:24] [INFO] testing connection to the target URL
got a 302 redirect to 'http://192.168.56.1:80/public/login.htm?loginurl=%2Fadmin%2Flogin.php%3Fid%3D1&errorid=0
[00:22:34] [INFO] checking if the target is protected by some kind of WAF/IPS
[00:22:34] [WARNING] reflective value(s) found and filtering out
[00:22:34] [INFO] testing if the target URL content is stable
[00:22:35] [WARNING] heuristic (basic) test shows that GET parameter 'id' might not be injectable
[00:22:36] [INFO] testing for SQL injection on GET parameter 'id'
[00:22:36] [INFO] testing 'AND boolean-based blind - WHERE or HAVING clause'
[00:22:40] [INFO] testing 'Boolean-based blind - Parameter replace (original value)'
[00:22:40] [INFO] testing 'MySQL >= 5.1 AND error-based - WHERE, HAVING, ORDER BY or GROUP BY clause (EXTRACTVA
[00:22:41] [INFO] testing 'PostgreSQL AND error-based - WHERE or HAVING clause'
[00:22:42] [INFO] testing 'Microsoft SQL Server/Sybase AND error-based - WHERE or HAVING clause (IN)'
[00:22:43] [INFO] testing 'Oracle AND error-based - WHERE or HAVING clause (XMLType)'
[00:22:43] [INFO] testing 'Generic inline queries'
[00:22:43] [INFO] testing 'PostgreSQL > 8.1 stacked queries (comment)'
[00:22:44] [INFO] testing 'Microsoft SQL Server/Sybase stacked queries (comment)'
[00:22:45] [INFO] testing 'Oracle stacked queries (DBMS_PIPE.RECEIVE_MESSAGE - comment)'
[00:22:45] [INFO] testing 'MySQL >= 5.0.12 AND time-based blind (query SLEEP)'
[00:22:46] [INFO] testing 'PostgreSQL > 8.1 AND time-based blind'
[00:22:46] [INFO] testing 'Microsoft SQL Server/Sybase time-based blind (IF)'
[00:22:47] [INFO] testing 'Oracle AND time-based blind'
it is recommended to perform only basic UNION tests if there is not at least one other (potential) technique fo
```

Figure 8-post requesting

Sqlmap –u http://192.168.36.1/admin/login.php?id=1 –

pThis commad is used to get request from the database.



```
prathiksha@prathiksha-VirtualBox:~$ sqlmap -u http://192.168.56.1/admin/login.php --crawl=100 --crawl-exclude="logout"
        ___
       __H__
 ___ ___[.]_____ ___ ___  {1.6.4#stable}
|_ -| . [.]     | .'| . |
|___|_  [(]_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's res
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:42:03 /2023-02-24/

do you want to check for the existence of site's sitemap(.xml) [y/N] y
got a 302 redirect to 'http://192.168.56.1/public/login.htm?loginurl=%2Fsitemap.xml&errorid=0'. Do you want to follow? [Y/n]
[00:42:17] [INFO] no links found
[00:42:17] [INFO] starting crawler for target URL 'http://192.168.56.1/admin/login.php'
[00:42:17] [INFO] searching for links with depth 1
[00:42:17] [WARNING] no usable links found (with GET parameters)
[00:42:17] [WARNING] your sqlmap version is outdated

[*] ending @ 00:42:17 /2023-02-24/

prathiksha@prathiksha-VirtualBox:~$ sqlmap -u http://192.168.56.1/admin/login.php --crawl=100 --crawl-exclude="logout" --batc
        ___
       __H__
 ___ ___[)]_____ ___ ___  {1.6.4#stable}
|_ -| . [']     | .'| . |
|___|_  [']_|_|_|__,|  _|
      |_|V...       |_|   https://sqlmap.org

[!] legal disclaimer: Usage of sqlmap for attacking targets without prior mutual consent is illegal. It is the end user's res
ssume no liability and are not responsible for any misuse or damage caused by this program

[*] starting @ 00:42:42 /2023-02-24/

do you want to check for the existence of site's sitemap(.xml) [y/N] N
[00:42:42] [INFO] starting crawler for target URL 'http://192.168.56.1/admin/login.php'
[00:42:42] [INFO] searching for links with depth 1
got a 302 redirect to 'http://192.168.56.1/public/login.htm?loginurl=%2Fadmin%2Flogin.php&errorid=0'. Do you want to follow?
[00:42:43] [INFO] searching for links with depth 2
please enter number of threads? [Enter for 1 (current)] 1
[00:42:43] [WARNING] running in a single-thread mode. This could take a while
[00:42:46] [INFO] searching for links with depth 3
please enter number of threads? [Enter for 1 (current)] 1
[00:42:46] [WARNING] running in a single-thread mode. This could take a while
[00:42:56] [INFO] 17/509 links visited (3%)
[00:42:56] [WARNING] it appears that you have been blocked by the target server
[00:43:19] [INFO] 64/509 links visited (13%)
```

Figure 9-Get requesting

sqlmap -u http://example.com/login.php --data "username=admin&pass=admin&submit=submit" -p username

the option -r tells sqlmap to read the search-test. txt file toget the information to attack in the POST request. -p is theparameter we are attacking.

V CONCLUSION

In conclusion, the tools mentioned have different purposes and outcomes related to network security testing and analysis. sqlmap helps identify vulnerabilities of database. Nmap helps identify hosts and services on a network and potential vulnerabilities associated with those services. L3MON is used to check the viruses and protect the system.These tools can be usedindividually or in combination with other tools and techniques to enhance network security and prevent cyber attacks. However, itis important to note that using these tools without proper authorization or legal permission may be illegal and can result insevere consequences.

VI REFERENCES

[1] "L3MON Remote Access Trojan," Malwarebytes Labs, accessed March 17, 2023, https://blog.malwarebytes.com/trojans/2019/10/l3mon-remote-access-trojan/.

[2] "Using Malware Analysis to Combat Cyberattacks," Infosec Institute, accessed March 17, 2023, https://resources.infosecinstitute.com/category/enterprise/malware-analysis/.

[3] "Cybersecurity Framework," National Institute of Standards and Technology (NIST), accessed March 17, 2023, https://www.nist.gov/cyberframework.

[4] Fyodor. (1997). Nmap - A Stealthy Port Scanner. In Phrack Magazine, Volume 7, Issue 51. URL: http://www.phrack.org/issues/51/7.html

[5] Lyon, G. (1999). Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning. Insecure.org.

[6] Ullrich, J., Dagon, D., & Tyson, M. (2006). Nmap: A comparison of active fingerprinting strategies. SANS Institute. URL: https://www.sans.org/reading-room/whitepapers/testing/nmap-comparison-active-fingerprinting-strategies-1791

[7] He, J., Tan, H., & Ma, Y. (2012). A comparison study of Nmap and Zmap on efficient IPv6 network scanning. In 2012 Fourth International Conference on Computational and Information Sciences (pp. 648-651). IEEE. DOI: 10.1109/ICCIS.2012.127

[8] Liu, S., Song, J., & Yang, C. (2013). An Improved SYN Scanning Mechanism Based on Nmap. International Journal of Computer Science and Mobile Computing, 2(8), 53-57. URL: https://www.ijcsmc.com/docs/papers/August2013/V2I8201332.pdf

[9]Cerrudo, C. (2015). Nmap 6 Cookbook: The Fat-Free Guide to Network Scanning. Packt Publishing Ltd.

[10] Hanafy, A., Elsayed, I., & Youssif, A. A. (2017). Comparative study between the behavior of Nmap and Nessus. In 2017 13th International Computer Engineering Conference (ICENCO) (pp. 1-6). IEEE. DOI: 10.1109/ICENCO.2017.8276926

[11]Seman, A., & Karim, N. A. (2017). A comparison of Nmap and ZMap for IPv6 network scanning. Journal of Telecommunication, Electronic and Computer Engineering (JTEC), 9(3-5), 111-114. URL: http://journal.utem.edu.my/index.php/jtec/article/view/3122

[12] Lago, N. D., Girard, R., Marchetti, E., & Torres, V. (2018). Nmap Scripting Engine—An analysis of scripts and vulnerabilities. International Journal of Network Security & Its Applications, 10(1), 13-24. URL: http://aircconline.com/ijnsa/V10N1/10118ijnsa06.pdf

[13] Zhang, Y., Zhai, Z., & Li, M. (2020). Research and design of lightweight Nmap vulnerability scanning and attack tool. In 2020 IEEE International Conference on Smart Internet of Things (SmartIoT) (pp. 329-332). IEEE.

[14] Bernardo, D. A. G., & Stampar, M. (2020). SQLmap: An open-source penetration testing tool that automates the process of detecting and exploiting SQL injection flaws. In Proceedings of the 6th International Conference on Information Warfare and Security (ICIW 2011) (pp. 83-89). Academic Conferences Limited.

[15] Chandel, V. (2017). Web Penetration Testing with Kali Linux: SQLMap. In Penetration Testing with Kali Linux - Third Edition (pp. 241-260). Packt Publishing.