ABSTRACT

A vulnerability scanner is a computer program designed to assess computers, networks or applications for known weaknesses. These scanners are used to **discover the weaknesses of a given system**. They are utilized in the identification and detection of vulnerabilities arising from mis-configurations or flawed programming within a network-based asset such as a firewall, router, web server, application server, etc.

INTRODUCTION

As time passes, the world is becoming more connected due to internet and new networking technology. Due to open nature of Internet, security of network has hold attention. With the development of new technologies, organization is now moving its business functions to public network, and thus a huge amount of personal, commercial and organization's information are available on networking infrastructures worldwide. Thus a set of precautions are taken to ensure the data cannot be compromised or inaccessible to unauthorized person. Network access in unauthorized by an outside hacker or a disgruntled employee can intentionally harm or destruct exclusive information which adversely influences organization benefit, and upset the proficiency to contend in business. In this manner, Network security is happening to incredible essentialness due to intellectual property that could be gained through the web with some effort. **Network security measures includes** scanning and vulnerability analysis along with penetration testing. Network scanning is fundamental for gathering information about the real state of computer systems or networks. It is a system for identification of active hosts on a network, either with the end goal of security assessment of network. Vulnerability Assessment is a systematic analysis of security status of Information systems. Both techniques are the most comprehensive service for auditing, penetration testing, reporting and patching for any organization's network

1.1SYSTEM SPECIFICATION

1.1.1 HARDWARE SPECIFICATION

Processor : Intel Pentium 4 or Later or Compatible

Hard Disk : 410GB or more

RAM : 4 GB or more

Monitor : LED and LCD Monitor (Touch Screen or Simple)

1.1.2 SOFTWARE SPECIFICATION

Operating System : Linux based any operating system

Programming : shell script

2. SYSTEM STUDY

2.1 EXITSTING SYSTEM

2.1.1 DESCRIPTION

In the manual system, firstly to check the computer services ,and application code verify i staff have to manage information regarding the accounts and transaction of all the customers manually Doing this manual transaction was really tedious job. Secondly information regarding accounts and transactions of customers were to be maintained. This process is time consuming and it requires a great manual effort

2.1.2 DRAWBACKS

- More time is consumed
- More hard work

2.2 PROPOSED SYSTEM

This system tends to replace the existing manual system for the scanning process which is a time consuming, less interactive and highly expensive. the main features of tis system will be creating report and find various type of network based vulnerabilities scanning data, process initiation and after that it generates a report of scanned network

2.2.2 FEATURES

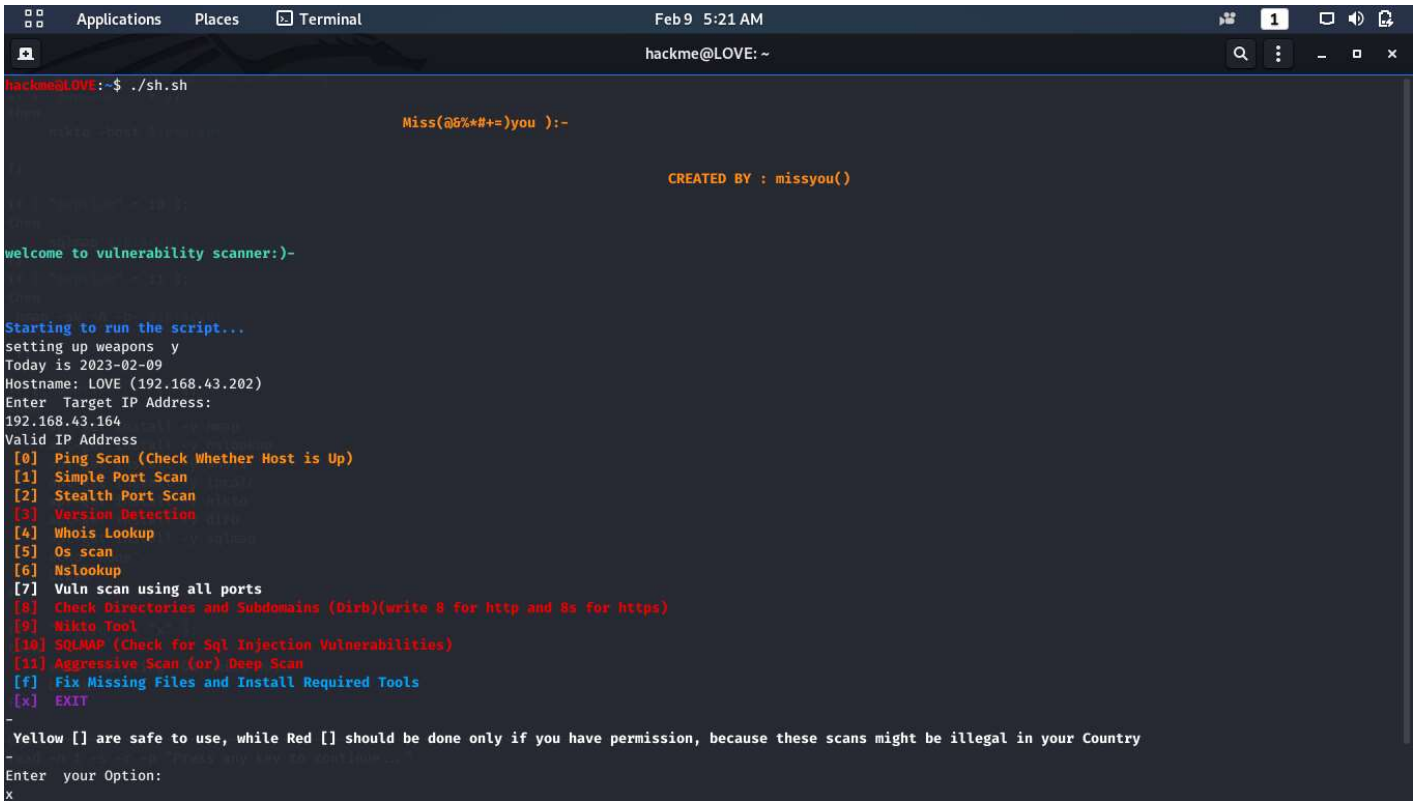
- Less effort to complete scanning
- Less time required and user friendly
- Fastest Scanner

3.SYSTEM DESIGN AND DEVELOPMENT

3.1 FILE DESIGN

As time passes, the world is becoming more connected due to internet and new networking technology. Due to open nature of Internet, security of network has hold attention. With the development of new technologies, organization is now moving its business functions to public network, and thus a huge amount of personal, commercial and organization's information are available on networking infrastructures worldwide. Thus a set of precautions are taken to ensure the data cannot be compromised or inaccessible to unauthorized person. Network access in unauthorized by an outside hacker or a disgruntled employee can intentionally harm or destruct exclusive information which adversely influences organization benefit, and upset the proficiency to contend in business. In this manner, Network security is happening to incredible essentialness due to intellectual property that could be gained through the web with some effort. **Network security measures includes** scanning and vulnerability analysis along with penetration testing. Network scanning is fundamental for gathering information about the real state of computer systems or networks. It is a system for identification of active hosts on a network, either with the end goal of security assessment of network. Vulnerability Assessment is a systematic analysis of security status of Information systems. Both techniques are the most comprehensive service for auditing, penetration testing, reporting and patching for any organization's network

3.2 INPUT DESIGN



3.3 OUTPUT DESIGN

```
Applications  Places  Terminal                Sep 21 05:04
hackme@LOVE: ~/Desktop/testing
Completed Ping Scan at 02:32, 0.01s elapsed (1 total hosts)
Overall sending rates: 212.09 packets / s.
mass_rdns: Using DNS server 192.168.43.1
mass_rdns: Using DNS server 2409:4072:2e95:7655::87
Initiating Parallel DNS resolution of 1 host. at 02:32
mass_rdns: 2.93s 0/1 [#: 2, OK: 0, NX: 0, DR: 0, SF: 0, TR: 2]
Completed Parallel DNS resolution of 1 host. at 02:32, 2.93s elapsed
DNS resolution of 1 IPs took 2.93s. Mode: Async [#: 2, OK: 0, NX: 1, DR: 0, SF: 0, TR: 2, CN: 0]
Initiating Connect Scan at 02:32
Scanning 192.168.43.9 [1000 ports]
Discovered open port 111/tcp on 192.168.43.9
Discovered open port 22/tcp on 192.168.43.9
Discovered open port 3306/tcp on 192.168.43.9
Discovered open port 53/tcp on 192.168.43.9
Discovered open port 5900/tcp on 192.168.43.9
Discovered open port 80/tcp on 192.168.43.9
Discovered open port 445/tcp on 192.168.43.9
Discovered open port 139/tcp on 192.168.43.9
Discovered open port 21/tcp on 192.168.43.9
Discovered open port 23/tcp on 192.168.43.9
Discovered open port 25/tcp on 192.168.43.9
Discovered open port 6667/tcp on 192.168.43.9
Discovered open port 512/tcp on 192.168.43.9
Discovered open port 8009/tcp on 192.168.43.9
Discovered open port 1524/tcp on 192.168.43.9
Discovered open port 1099/tcp on 192.168.43.9
Discovered open port 2121/tcp on 192.168.43.9
Discovered open port 514/tcp on 192.168.43.9
Discovered open port 5432/tcp on 192.168.43.9
Discovered open port 513/tcp on 192.168.43.9
Discovered open port 2049/tcp on 192.168.43.9
Discovered open port 6000/tcp on 192.168.43.9
Discovered open port 8180/tcp on 192.168.43.9
Completed Connect Scan at 02:32, 0.84s elapsed (1000 total ports)
Overall sending rates: 1186.31 packets / s.
Initiating Service scan at 02:32
Scanning 23 services on 192.168.43.9
Got nsock CONNECT response with status TIMEOUT - aborting this service
Completed Service scan at 02:33, 93.63s elapsed (23 services on 1 host)
```

3.4 CODE DESIGN

```
#! /bin/bash

#echo "-----------------------------------------------------------------------------------------------------"



        echo -e  "\e[1;33m

                                        Miss(@&%*#+=)you ):-

\e[0m"

#echo -e "\e                                    Vulnerability Detection Tool                                \e     "

#echo "-----------------------------------------------------------------------------------------------------"

echo -e "\e[1;33m                                                                                    CREATED BY : missyou()
\e[0m"

echo -e  "\e[1;32m

welcome to vulnerability scanner:)-

 \e[0m"

echo -e "\e[1;34mStarting to run the script...\e[0m"

spinner() {

   local i sp n

   sp='missyou '

   n=${#sp}

   printf ' '

   while sleep 0.05; do
```

```
   printf "%s\b" "${sp:i++%n:1}"

    done

}

printf 'setting up weapons '

spinner &

sleep 4  # sleeping for 10 seconds is important work

kill "$!" # kill the spinner

printf '\n'

# VARIABLE ASSIGNMENT

# Show hostname:

HOST=$(hostname)

# User executing the script:

CURRENTUSER=$(whoami)

# Current date:

CURRENTDATE=$(date +%F)

# Host IP address:

IPADDRESS=$(hostname -I | cut -d ' ' -f1)

# SHOW MESSAGES

echo "Today is $CURRENTDATE"

echo "Hostname: $HOST ($IPADDRESS)"

sleep 1echo "Enter  Target IP Address:"
```

```
read iptarget

if [[ $iptarget =~ ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$ ]]; then

  echo "Valid IP Address"

else

  echo "Invalid IP Address. Quitting..."

  exit

fi

#INFINITE LOOP

for (( ; ; ))

do

{

#STARTING

echo -e "\e[1;33m [0]  Ping Scan (Check Whether Host is Up)\e[0m"

echo -e "\e[1;33m [1]  Simple Port Scan \e[0m"

echo -e "\e[1;33m [2]  Stealth Port Scan \e[0m"

echo -e "\e[1;31m [3]  Version Detection\e[0m"

echo -e "\e[1;33m [4]  Whois Lookup \e[0m"

echo -e "\e[1;33m [5]  Os scan \e[0m"

echo -e "\e[1;33m [6]  Nslookup \e[0m"

echo -e "\e[1;37m [7]  Vuln scan using all ports\e[0m"
```

```
echo -e"\e[1;31m [8]  Check Directories and Subdomains (Dirb)(write 8 for http and 8s for https) \e[0m"

echo -e "\e[1;31m [9]  Nikto Tool\e[0m"

echo -e "\e[1;31m [10] SQLMAP (Check for Sql Injection Vulnerabilities)\e[0m"

echo -e "\e[1;31m [11] Aggressive Scan (or) Deep Scan \e[0m"

echo -e "\e[1;36m [f]  Fix Missing Files and Install Required Tools \e[0m"

echo -e "\e[1;35m [x]  EXIT \e[0m"

echo "-"

echo -e "\e[1;37m Yellow [] are safe to use, while Red [] should be done only if you have permission, because these scans might be illegal in your Country \e[0m"

echo "-"

echo "Enter  your Option:"

read option

if [ "$option" = 0 ];

then

    nmap -sn $iptarget

fi

if [ "$option" = 1 ];

then

   sudo nmap -p 1-1000 $iptarget

fi
```

```
if [ "$option" = 2 ];
then
    sudo nmap -sS $iptarget
fi
if [ "$option" = 3 ];
then
    nmap -sV -Pn -T4 $iptarget
fi
if [ "$option" = 4 ];
then
       whois $iptarget
fi
if [ "$option" = 5 ];
then
     echo "NS"
     host -t ns google.com
     echo "MX"
     host -t mx google.com
fi
if [ "$option" = 6 ];
then
```

```
    nslookup $iptarget
fi
if [ "$option" = 7 ];
then
    nmap --script=vuln -p- $iptarget
fi
if [ "$option" = 8 ];
then
    dirb http://$iptarget


fi
if [ "$option" = "8s" ];
then
    dirb https://$iptarget
fi
if [ "$option" = 9 ];
then
    nikto -host $iptarget
fi
if [ "$option" = 10 ];
then
```

```
    sqlmap $iptarget
fi
if [ "$option" = 11 ];
then
 nmap -sV -A -p- $iptarget
 fi
if [ "$option" = "f" ];
then
    apt-get install -y nmap
    apt-get install -y nslookup
    apt-get install -y whois
    apt-get install -y ipcalc
    apt-get install -y nikto
    apt-get install -y dirb
    apt-get install -y sqlmap
    echo "Done"
    break
fi
if [ "$option" = "x" ];
then
    echo "Quitting (OR) miss ou):-"
```

```
    break
fi
echo "-----------------------------------------------------------------"
read -n 1 -s -r -p "Press any key to continue..."
clear
}
done
#INFINITE LOOP
```

3.5 SYSTEM DEVELOPMENT

3.5.1 MODULES

A modules is a collection of source files and build settings that allow you to divided your project into discrete units of functionality .provides a container for your apps source code, resource files, and app settings such as the module –level build file and computer manifest file.

This project includes 13 modules. They are

- Ping Scan
- Port Scan
- Stealth port scan
- Version Detection
- Whoislookup
- Os scan
- Nslookup
- Vuln scan all port
- Check subdomains
- http and https vuln scan

- sql injection vulnerability checker
- Deep scan
- exit

3.5.2 MODULES DESCRIPTION

Ping Scan

This function is mainly used to checking the target online or offline through the internet.

Simple Port Scan

This function is used to show the all port open or close checking process

Stealth Port Scan

This module scan with tcp or udp ports

Version Detection

This function is mainly used running on port in computer to find the port version

Whois Lookup

This module find the domain details ip address ,name server,user information and showing more information

Os scan

This module help to find the or gussing the operating system to the network

Nslookup

This module used to the find the dns information to the network

Vuln scan using all ports

This module help to check all port vulnerabilities or not vulnerabilities

Check Directories and Subdomains

this module help to find the hiden directories in websites or networks

Http and Https vuln scan

This module is mainly used to the port 80 and port 443 vulnerable checking

Sql Injection Vulnerabilities

This module help to check web based sql injection vulnerabilities to the network

Aggressive Scan (or) Deep Scan

This module mainly used to scan with network deep scanning or full scan

EXIT

This module helps to quit the application

4. TESTING

The purpose of testings is to discover errors. Testing is the process of trying to discover ervery conceivable fault or weakness in work product. it provides a way to check the functionality of components, sub assembiles and /or finished profuct it is the process of exercising softwear with the intent of ensuring that the softwear system meets its requirements and user expectations and does not fail in an unacceptable manner . there are various type of test .Each test type addresses a specific testing requirement

TYPES OF TESTS

Integration Testing

Testing is event driven and is more concerned with the basic outcome of screens or fields. integration tests demonstrate that athough the components were individualily satisfaction as shown by successfully unit testing, the combination of components is correct and consistent

Validating Testing

Validation is done at the end of the development process and takes place after verification are completed

```
hen

   nmap -sV -Pn -T4 $iptarget

fi

if [ "$option" = 4 ];

then      whois $iptarget
```

```
fi
if [ "$option" = 5 ];
then
    echo "NS"
    host -t ns google.com
    echo "MX"
    host -t mx google.com
fi
if [ "$option" = 6 ];
then
    nslookup $iptarget
fi
if [ "$option" = 7 ];
then
    nmap --script=vuln -p- $iptarget
fi
if [ "$option" = 8 ];
then
    dirb http://$iptarget
fi
```

```
if [ "$option" = "8s" ];

then
```

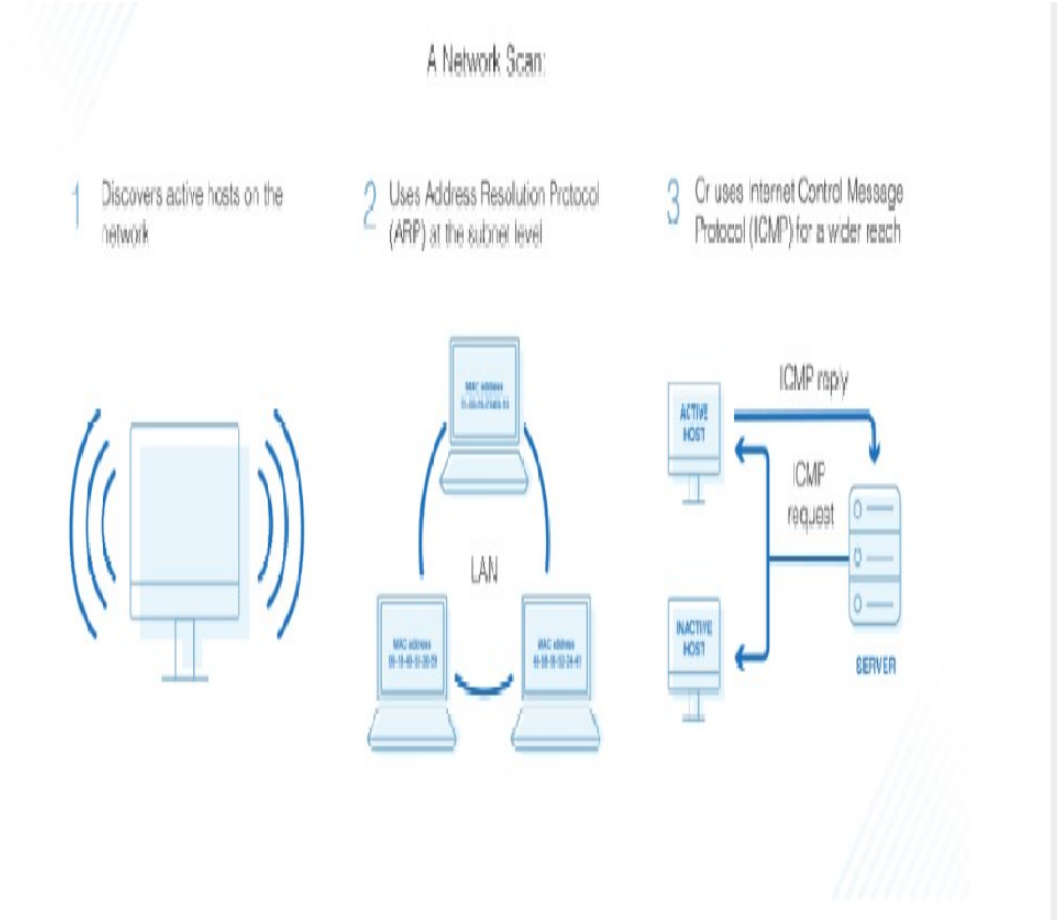
Unit Testing

A unit is the smallest testable part of any softwear. it usually has one or a few inputs and usually a single output

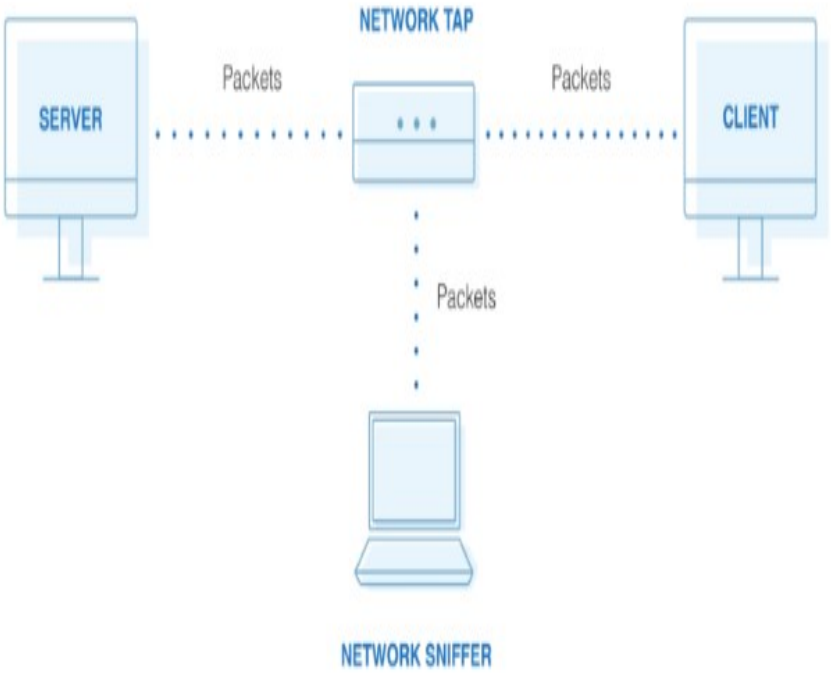
```
echo "Today is $CURRENTDATE"

echo "Hostname: $HOST ($IPADDRESS)"

sleep 1

echo "Enter  Target IP Address:"

read iptarget

if [[ $iptarget =~ ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$ ]]; then

  echo "Valid IP Address"

else

  echo "Invalid IP Address. Quitting..."

  exit

fi

#INFINITE LOOP

for (( ; ; ))

do
```

5. IMPLEMENTATION

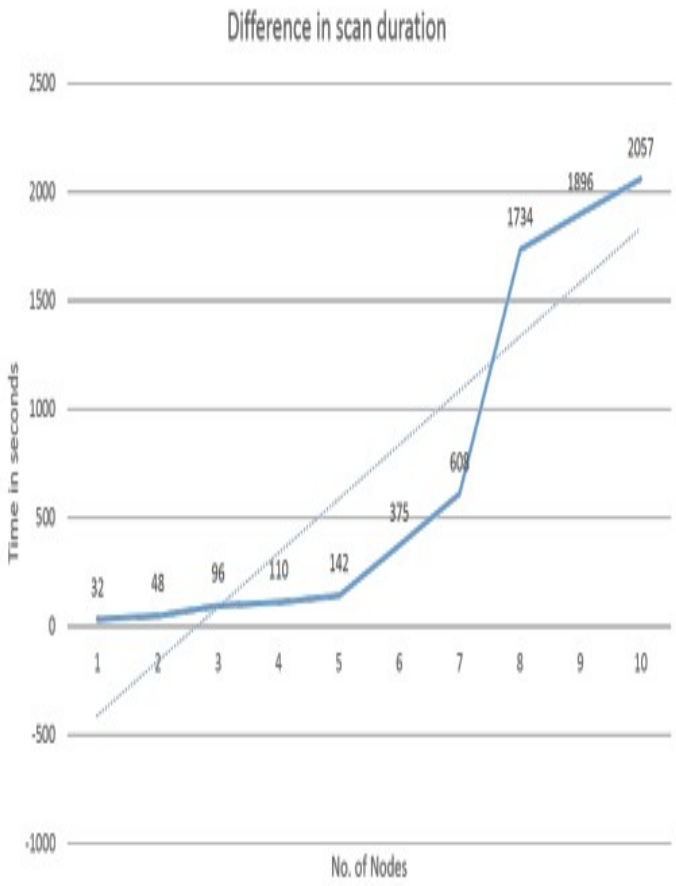
Use case diagram

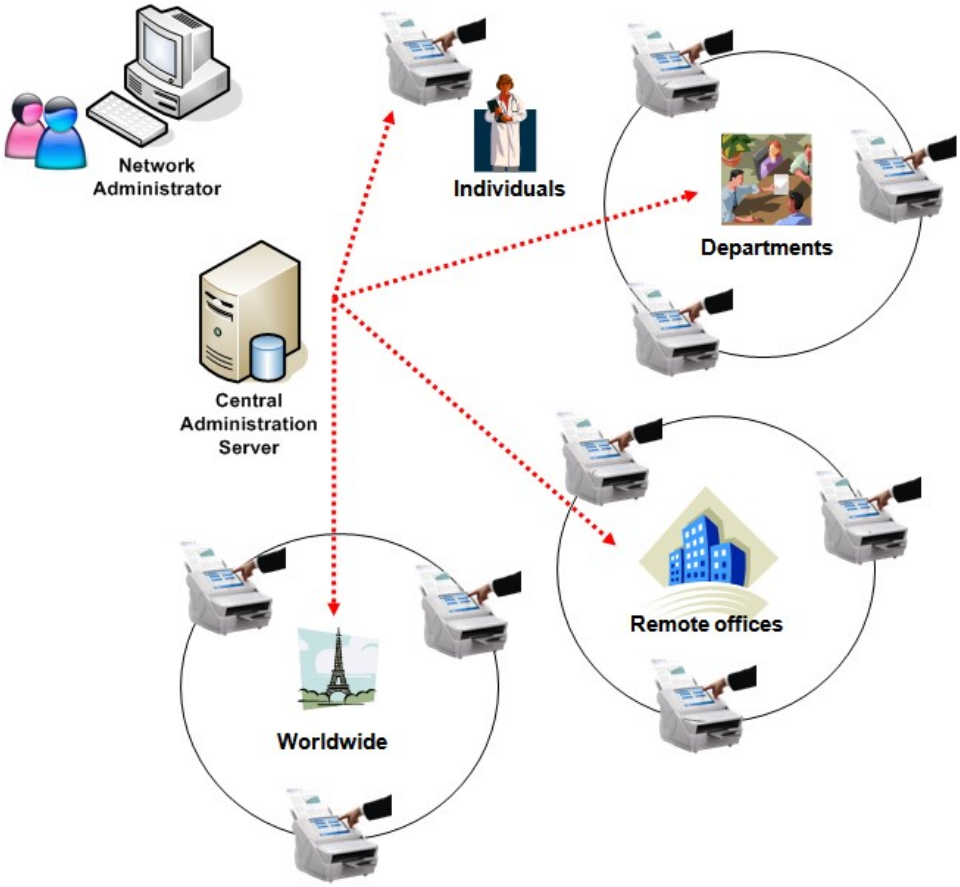


Activity diagram

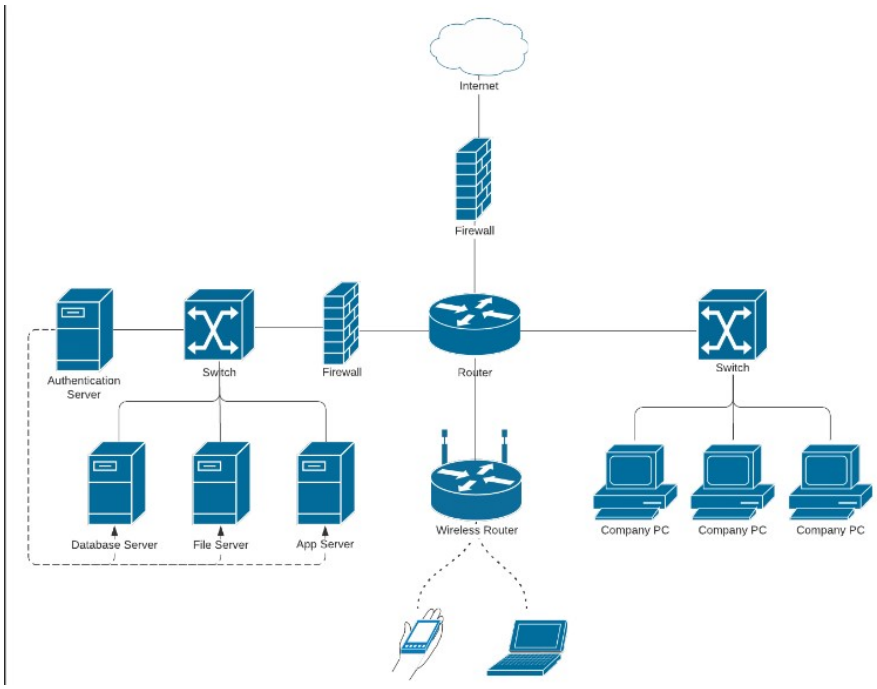


Sequence diagram




Network
Administrator
Individuals
Departments
Central
Administration
Server
Remote offices
Worldwide

Class diagram



B.SAMPLE CODING

```
#! /bin/bash

#echo "-----------------------------------------------------------------------------------------------------------"



          echo -e  "\e[1;33m

                                        Miss(@&%*#+=)you ):-

\e[0m"



#echo -e "\e                                    Vulnerability Detection Tool                                \e     "



#echo "-----------------------------------------------------------------------------------------------------------"

echo -e "\e[1;33m                                                                                    CREATED BY : missyou()
\e[0m"



echo -e  "\e[1;32m

welcome to vulnerability scanner:)-

 \e[0m"

echo -e "\e[1;34mStarting to run the script...\e[0m"

spinner() {

    local i sp n

    sp='missyou '
```

```
    n=${#sp}
    printf ' '
    while sleep 0.05; do
        printf "%s\b" "${sp:i++%n:1}"
    done
}
printf 'setting up weapons '
spinner &
sleep 4  # sleeping for 10 seconds is important work
kill "$!" # kill the spinner
printf '\n'


# VARIABLE ASSIGNMENT
# Show hostname:
HOST=$(hostname)
# User executing the script:
CURRENTUSER=$(whoami)
# Current date:
CURRENTDATE=$(date +%F)
# Host IP address:
IPADDRESS=$(hostname -I | cut -d ' ' -f1)
```

```
# SHOW MESSAGES

echo "Today is $CURRENTDATE"

echo "Hostname: $HOST ($IPADDRESS)"

sleep 1

echo "Enter  Target IP Address:"

read iptarget

if [[ $iptarget =~ ^[0-9]+\.[0-9]+\.[0-9]+\.[0-9]+$ ]]; then

  echo "Valid IP Address"

else

  echo "Invalid IP Address. Quitting..."

  exit

fi

#INFINITE LOOP

for (( ; ; ))

do

{

#STARTING

echo -e "\e[1;33m [0]  Ping Scan (Check Whether Host is Up)\e[0m"

echo -e "\e[1;33m [1]  Simple Port Scan \e[0m"

echo -e "\e[1;33m [2]  Stealth Port Scan \e[0m"

echo -e "\e[1;31m [3]  Version Detection\e[0m"
```

```
echo -e "\e[1;33m [4]  Whois Lookup \e[0m"

echo -e "\e[1;33m [5]  Os scan \e[0m"

echo -e "\e[1;33m [6]  Nslookup \e[0m"

echo -e "\e[1;37m [7]  Vuln scan using all ports\e[0m"

echo -e "\e[1;31m [8]  Check Directories and Subdomains (Dirb)(write 8 for http and 8s for https) \e[0m"

echo -e "\e[1;31m [9]  http and https vuln scan \e[0m"

echo -e "\e[1;31m [10] SQLMAP (Check for Sql Injection Vulnerabilities)\e[0m"

echo -e "\e[1;31m [11] Aggressive Scan (or) Deep Scan \e[0m"

echo -e "\e[1;36m [f]  Fix Missing Files and Install Required Tools \e[0m"

echo -e "\e[1;35m [x]  EXIT \e[0m"

echo "-"

echo -e "\e[1;37m Yellow [] are safe to use, while Red [] should be done only if you have permission, because these scans might be illegal in your Country \e[0m"

echo "-"

echo "Enter  your Option:"

read option

if [ "$option" = 0 ];

then

   nmap -sn $iptarget

fi

if [ "$option" = 1 ];
```

```
then
  sudo nmap -p 1-1000 $iptarget
fi
if [ "$option" = 2 ];
then
   sudo nmap -sS $iptarget
fi
if [ "$option" = 3 ];
then
   nmap -sV -Pn -T4 $iptarget
fi
if [ "$option" = 4 ];
then
      whois $iptarget
fi
if [ "$option" = 5 ];
then
    echo "NS"
    host -t ns google.com
    echo "MX"
    host -t mx google.com
```

```
fi
if [ "$option" = 6 ];
then
    nslookup $iptarget
fi
if [ "$option" = 7 ];
then
    nmap --script=vuln -p- $iptarget
fi


if [ "$option" = 8 ];
then
    dirb http://$iptarget
fi
if [ "$option" = "8s" ];
then
    dirb https://$iptarget
fi
if [ "$option" = 9 ];
then
    nikto -host $iptarget
```

```
fi
if [ "$option" = 10 ];
then
    sqlmap $iptarget
fi
if [ "$option" = 11 ];
then
 nmap -sV -A -p- $iptarget
 fi


if [ "$option" = "f" ];
then
    apt-get install -y nmap
    apt-get install -y nslookup
    apt-get install -y whois
    apt-get install -y ipcalc
    apt-get install -y nikto
    apt-get install -y dirb
    apt-get install -y sqlmap
    echo "Done"
    break
```

```
fi

if [ "$option" = "x" ];

then

    echo "Quitting (OR) miss you):-"

    break

fi

echo "-----------------------------------------------------------------"

read -n 1 -s -r -p "Press any key to continue..."

clear        }

done
```

C.SAMPLE INPUT

```
Applications  Places  Terminal                Sep 21 05:06
hackme@LOVE: ~/Desktop/testing
25/tcp   open  smtp       syn-ack Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN,
|_ssl-date: 2023-02-21T06:03:35+00:00; +1y152d23h28m35s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_DES_64_CBC_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
53/tcp   open  domain     syn-ack ISC BIND 9.4.2
| dns-nsid:
|_  bind.version: 9.4.2
80/tcp   open  http       syn-ack Apache httpd 2.2.8 ((Ubuntu) DAV/2)
| http-methods:
|_  Supported Methods: GET HEAD POST OPTIONS
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
111/tcp  open  rpcbind    syn-ack 2 (RPC #100000)
| rpcinfo:
|_  ERROR: Portmap.Dump: RPC accepted state: remote can't support version.
139/tcp  open  netbios-ssn syn-ack Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn syn-ack Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec?      syn-ack
513/tcp  open  login?     syn-ack
514/tcp  open  shell?     syn-ack
| fingerprint-strings:
|   NULL:
|_    Couldn't get address for your host (LOVE)
1099/tcp open  java-rmi   syn-ack GNU Classpath grmiregistry
1524/tcp open  bindshell  syn-ack Metasploitable root shell
2049/tcp open  nfs        syn-ack 2-4 (RPC #100003)
2121/tcp open  ftp        syn-ack ProFTPD 1.3.1
| ssl-date:
|_  ERROR: Unable to obtain data from the target
3306/tcp open  mysql      syn-ack MySQL 5.0.51a-3ubuntu5
| mysql-info:
```

Applications Places Terminal Sep 21 05:06

hackme@LOVE: ~/Desktop/testing

```
1524/tcp open  bindshell   syn-ack Metasploitable root shell
2049/tcp open  nfs         syn-ack 2-4 (RPC #100003)
2121/tcp open  ftp         syn-ack ProFTPD 1.3.1
| ssl-date:
|_  ERROR: Unable to obtain data from the target
3306/tcp open  mysql       syn-ack MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 9
|   Capabilities flags: 43564
|   Some Capabilities: Speaks41ProtocolNew, SwitchToSSLAfterHandshake, SupportsCompression, SupportsTransactions, Support41Auth, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|_  Salt: UPrnO$`89Ro[Y/|D~p8c
5432/tcp open  postgresql  syn-ack PostgreSQL DB 8.3.0 - 8.3.7
|_ssl-date: 2023-02-21T06:03:36+00:00; +1y152d23h28m35s from scanner time.
5900/tcp open  vnc         syn-ack VNC (protocol 3.3)
| ssl-date:
|_  ERROR: Unable to obtain data from the target
| vnc-info:
|   Protocol version: 3.3
|   Security types:
|_    VNC Authentication (2)
6000/tcp open  X11         syn-ack (access denied)
6667/tcp open  irc         syn-ack UnrealIRCd
| irc-info:
|   users: 1
|   servers: 1
|   lusers: 1
|   lservers: 0
|   server: irc.Metasploitable.LAN
|   version: Unreal3.2.8.1. irc.Metasploitable.LAN
|   uptime: 0 days, 0:44:04
|   source ident: nmap
|   source host: Test-FB6AD55D
|_  error: Closing Link: egjyhllzg[LOVE] (Quit: egjyhllzg)
8009/tcp open  ajp13?      syn-ack
| ajp-auth:
|   ERROR: Failed to connect to AJP server
```

D.SAMPLE OUTPUT

```
Applications  Places  Terminal                Sep 21 05:06
hackme@LOVE: ~/Desktop/testing
8009/tcp open  ajp13?     syn-ack
| ajp-auth:
|_  ERROR: Failed to connect to AJP server
| ajp-methods:
|_  ERROR: Failed to connect to server
8180/tcp open  http       syn-ack Apache Tomcat/Coyote JSP engine 1.1
1 service unrecognized despite returning data. If you know the service/version, please submit the following fingerprint at https://nmap.org/cgi-bin/submit.cgi?new-servi
ce :
SF-Port514-TCP:V=7.80%I=7%D=9/21%Time=61497C66%P=i686-pc-linux-gnu%r(NULL,
SF:2B,"\x01Couldn't\x20get\x20address\x20for\x20your\x20host\x20\(LOVE\)\n
SF:");
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 518d00h43m35s, deviation: 2h30m01s, median: 517d23h28m34s
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|   WORKGROUP<1e>        Flags: <group><active>
| Statistics:
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|   00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
|_  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
| p2p-conficker:
|   Checking for Conficker.C or higher...
|   Check 1 (port 28607/tcp): CLEAN (Couldn't connect)
|   Check 2 (port 33695/tcp): CLEAN (Couldn't connect)
|   Check 3 (port 58545/udp): CLEAN (Failed to receive data)
|   Check 4 (port 32313/udp): CLEAN (Failed to receive data)
|_  0/4 checks are positive: Host is CLEAN or ports are blocked
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
```

Applications Places Terminal Sep 21 05:11

hackme@LOVE: ~/Desktop/testing

```
All 1000 scanned ports on HACKLOVEME (192.168.43.164) are filtered
MAC Address: 3C:91:80:74:80:AF (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 22.07 seconds
hackme@LOVE:~/Desktop/testing$ sudo nmap -sM  192.168.43.164 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-21 05:09 EDT
Nmap scan report for HACKLOVEME (192.168.43.164)
Host is up (0.00065s latency).
All 1000 scanned ports on HACKLOVEME (192.168.43.164) are open|filtered
MAC Address: 3C:91:80:74:80:AF (Liteon Technology)

Nmap done: 1 IP address (1 host up) scanned in 22.70 seconds
hackme@LOVE:~/Desktop/testing$ sudo nmap -o  192.168.43.164 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-21 05:10 EDT
WARNING: No targets were specified, so 0 hosts scanned.
Nmap done: 0 IP addresses (0 hosts up) scanned in 0.34 seconds
hackme@LOVE:~/Desktop/testing$ sudo nmap -O  192.168.43.164 -Pn
Starting Nmap 7.80 ( https://nmap.org ) at 2021-09-21 05:10 EDT
Nmap scan report for HACKLOVEME (192.168.43.164)
Host is up (0.00074s latency).
Not shown: 996 filtered ports
PORT     STATE SERVICE
443/tcp  open  https
902/tcp  open  iss-realsecure
912/tcp  open  apex-mesh
5357/tcp open  wsdapi
MAC Address: 3C:91:80:74:80:AF (Liteon Technology)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: specialized|general purpose
Running (JUST GUESSING): AVtech embedded (87%), Microsoft Windows XP (87%), FreeBSD 6.X|10.X (86%)
OS CPE: cpe:/o:microsoft:windows_xp::sp2 cpe:/o:freebsd:freebsd:6.2 cpe:/o:freebsd:freebsd:10.3
Aggressive OS guesses: AVtech Room Alert 26W environmental monitor (87%), Microsoft Windows XP SP2 (87%), FreeBSD 6.2-RELEASE (86%), FreeBSD 10.3-STABLE (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 1 hop

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.16 seconds
hackme@LOVE:~/Desktop/testing$
```

Conclusion and Future Scope

Every day, vulnerabilities are found in commonly used software products. A network scanner developed in this project is an application which is used to scan the network and report any identified vulnerabilities It is a web-based GUI which deals with two important aspect of network security:- network scanning and vulnerability assessment. Network scanning includes identification of alive hosts in the network, which operating systems is installed on them, and what services are running on them. Throughout the vulnerability check a database of vulnerability signatures is contrasted with the data acquired from a network scan output to produce a list of vulnerabilities that are presumably present in the network. What's more to check whether the vulnerability might be abused or not and on the off chance that it can what are conceivable systems, testing is carried out. It performs functions of both NMAP

BIBLIOGRAPHY

https://github.com/topics/vulnerablilityscanner-project

https://www.wiki.com/networkbasedscanner/

https://www.liunx.com/shellscrpitstoolmakeingreferences/?

https://www.python.com/modulesscanning