Sri Lanka Institute of Information Technology

Individual Assignment

IE3022 – Applied Information Assurance

Submitted by:

Student Registration Number	Student Name
IT20224998	Jayakodi J.A.W.N

Date of submission

22/10/2022

Sentinal Industries
Security Assessment Findings Report

Business Confidential

Contents

Confidentiality Statement

This document is the exclusive property of Sentinal Industries and CyberOps. This document contains proprietary and confidential information. Duplication, redistribution, or use, in whole or in part, in any form, requires consent of both Sentinal Industries and CyberOps.

CyberOps may share this document with auditors under non-disclosure agreements to demonstrate penetration test requirement compliance.

Disclaimer

A penetration test is considered a snapshot in time. The findings and recommendations reflect the information gathered during the assessment and not any changes or modifications made outside of that period.

Time-limited engagements do not allow for a full evaluation of all security controls. CyberOps prioritized the assessment to identify the weakest security controls an attacker would exploit. CyberOps recommends conducting similar assessments on an annual basis by internal or third-party assessors to ensure the continued success of the controls.

Contact information

Name	Title
Bruce Sentinal	Chief Officer
Wimanga Jayakodi	Penetration Tester

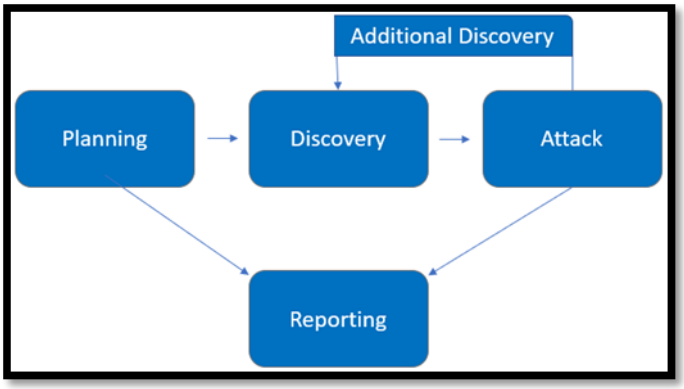
Assessment Overview

From October 2th, 2022 to October 21th, 2022, Sentinal Industries engaged CyberOps to evaluate the security posture of its infrastructure compared to current industry best practices that included an external penetration test. All testing performed is based on the NIST *SP 800-115 Technical Guide to Information Security Testing and Assessment, OWASP Testing Guide (v4), and customized testing frameworks*.

Phases of penetration testing activities include the following:

- Planning – Customer goals are gathered and rules of engagement obtained.
- Discovery – Perform scanning and enumeration to identify potential vulnerabilities, weak areas, and exploits.

- Attack – Confirm potential vulnerabilities through exploitation and perform additional discovery upon new access.
- Reporting – Document all found vulnerabilities and exploits, failed attempts, and company strengths and weaknesses.



Finding Severity Ratings

The following table defines levels of severity and corresponding CVSS score range that are used throughout the document to assess vulnerability and risk impact.

Severity	CVSS V3 Score Range	Definition
Critical	9.0-10.0	Exploitation is straightforward and usually results in system-level compromise. It is advised to form a plan of action and patch immediately.
High	7.0-8.9	Exploitation is more difficult but could cause elevated privileges and potentially a loss of data or downtime. It is advised to form a plan of action and patch as soon as possible.
Moderate	4.0-6.9	Vulnerabilities exist but are not exploitable or require extra steps such as social engineering. It is advised to form a plan of action and patch after high-priority issues have been resolved.
Low	0.1-3.9	Vulnerabilities are non-exploitable but would reduce an organization's attack surface. It is advised to form a plan of action and patch during the next maintenance window.

Severity	CVSS V3 Score Range	Definition
Informational	N/A	No vulnerability exists. Additional information is provided regarding items noticed during testing, strong controls, and additional documentation.

Scope

Assessment	Details
External Penetration Test	10.0.2.8 – Metasploitable 2 Machine 10.0.2.9 – OWASP bwa machine

Executive Summary

CyberOps evaluated Sentinal Industries external security posture through an external network penetration test From October 2th, 2022 to October 21th, 2022. By leveraging a series of attacks, CyberOps found critical level vulnerabilities that allowed full internal network access to the sentinal office. It is highly recommended that Sentinal Industries address these vulnerabilities as soon as possible as the vulnerabilities are easily found through basic reconnaissance and exploitable without much effort.

Scoping and Time Limitations

- Scoping during the engagement did not permit denial of service or social engineering across all testing components.
- CyberOps has assumed that vulnerability which has bellow 7.0 CVSS will be blocked by the Firewalls and they couldn't able to create a high impact on systems.

Testing Summary

The network assessment evaluated Sentinal Industries internal network security posture. From an internal perspective, the CyberOps team performed vulnerability scanning against all IPs provided by Sentinal Industries to evaluate the overall patching health of the network. The team also performed common attacks such as MITM attacks and common port enumerations. Beyond vulnerability scanning the CyberOps evaluated

other potential risks, such as open file shares, default credentials on servers/devices, and sensitive information disclosure to gain a complete picture of the network's security posture.

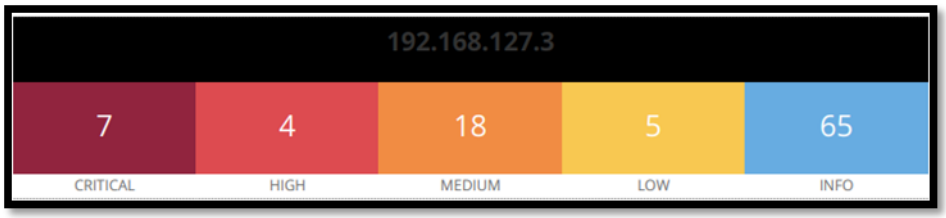
Tester Notes

During testing, two constants stood out: a weak password policy and weak patching. The weak password policy led to the initial compromise of accounts and is usually one of the first footholds an attacker attempts to use in a network [IPT006].

We recommended that Sentinal Industries to re-evaluates their current password policy and considers a policy of 15 characters or more for their regular user accounts and 30 characters or more. Finally, a Privilege Access Management solution should be considered.

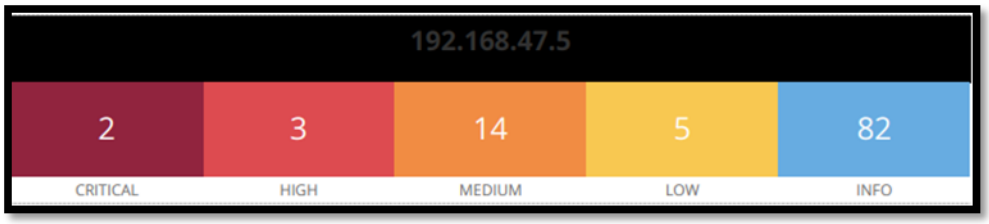
We recommend that the Sentinal Industries team review the patching recommendations made in the Technical Findings section of the report along with reviewing the provided Nessus scans for a full overview of items to be patched. We also recommend that Sentinal Industries improve their patch management policies and procedures to help prevent potential attacks within their network [IPT007, IPT009].

Summary of Findings



Target: 192.168.127.3			
No.	**Findings**	**Severity**	**CVSS**
Internal Penetration Test:			
IPT001	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness	CRITICAL	10.0
IPT002	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)	CRITICAL	10.0
IPT003	VNC Server 'password' Password	CRITICAL	10.0
IPT004	rexecd Service Detection	CRITICAL	10.0
IPT005	Apache Tomcat AJP Connector Request Injection (Ghostcat)	CRITICAL	9.8

IPT006	ISC BIND Service Downgrade / Reflected DoS	HIGH	8.6
IPT007	SSL Medium Strength Cipher Suites Supported (SWEET32)	HIGH	7.5
IPT008	NFS Shares World Readable	HIGH	7.5
Recommendations:			
1	Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.		
2	Secure the VNC service with a strong password.		
3	Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.		
4	Update the AJP configuration to require authorization and/or upgrade the Tomcat server to 7.0.100, 8.5.51, 9.0.31 or later.		
5	Upgrade to the ISC BIND version referenced in the vendor advisory		
6	Place the appropriate restrictions on all NFS shares.		



Target: 192.168.47.5			
No.	**Findings**	**Severity**	**CVSS**
Internal Penetration Test:			
IPT009	Unix Operating System Unsupported Version Detection	CRITICAL	10.0
IPT010	SSL Version 2 and 3 Protocol Detection	CRITICAL	10.0
IPT011	SSL Certificate Signed Using Weak Hashing Algorithm	HIGH	7.0
IPT012	Samba Badlock Vulnerability	HIGH	7.0
Recommendations:			
1	Upgrade to a version of the Unix operating system that is currently supported.		
2	Contact the Certificate Authority to have the SSL certificate reissued.		
3	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.		
4	Reconfigure the affected application, if possible, to avoid use of medium strength ciphers.		

Technical Findings

Internal Penetration Test Findings

Finding IPT001: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness [Critical]

Description:	The remote SSH host key has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to set up decipher the remote session or set up a man in the middle attack.
Risk:	Likelihood: High Impact: Very High
System:	192.168.127.3
Tools Used:	Nessus
References:	[SECURITY] [DSA 1571-1] New openssl packages fix predictable random number generator (debian.org)

Remediation

- Consider all cryptographic material generated on the remote host to be guessable. In particuliar, all SSH, SSL and OpenVPN key material should be re-generated.

Finding IPT002: Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check) [Critical]

Description:	The remote x509 certificate on the remote SSL server has been generated on a Debian or Ubuntu system which contains a bug in the random number generator of its OpenSSL library. The problem is due to a Debian packager removing nearly all sources of entropy in the remote version of OpenSSL. An attacker can easily obtain the private part of the remote key and use this to decipher the remote session or set up a man in the middle attack.
Risk:	Likelihood: High Impact: Very High
System:	192.168.127.3

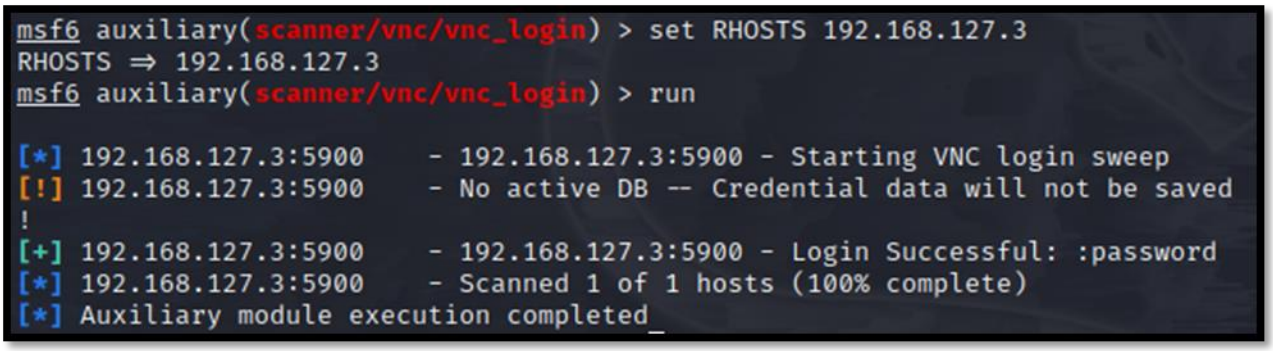
Tools Used:	Nessus
References:	[USN-605-1] Thunderbird vulnerabilities (ubuntu.com)

Finding IPT003: VNC Server 'password' Password [Critical]

Description:	The VNC server running on the remote host is secured with a weak password. Nessus was able to login using VNC authentication and a password of 'password'. A remote, unauthenticated attacker could exploit this to take control of the system.
Risk:	Likelihood: High Impact: Very High
System:	192.158.127.3
Tools Used:	Nessus, Metasploit

Evidence

```
Nessus logged in using a password of "password".
```



Remediation

- Secure the VNC service with a strong password.

Finding IPT004: Rexecd Service Detection [Critical]

Description:	The rexecd service is running on the remote host. This service is design to allow users of a network to execute commands remotely. However, rexecd does not provide any good means of authentication, so it may be abused by an attacker to scan a third-party host.
Risk:	Likelihood: High Impact: Very High
System:	192.168.127.3
Tools Used:	Nessus

Remediation

- Comment out the 'exec' line in /etc/inetd.conf and restart the inetd process.

Finding IPT005: Apache Tomcat AJP Connector Request Injection (Ghostcat) [Critical]

Description:	A file read/inclusion vulnerability was found in AJP connector. A remote, unauthenticated attacker could exploit this vulnerability to read web application files from a vulnerable server. In instances where the vulnerable server allows file uploads, an attacker could upload malicious JavaServer Pages (JSP) code within a variety of file types and gain remote code execution (RCE).
Risk:	Likelihood: High Impact: Very High
System:	192.168.127.3
Tools Used:	Nessus, Metasploit
References:	NVD - CVE-2020-1745 (nist.gov) NVD - CVE-2020-1938 (nist.gov)

Evidence

```
msf6 auxiliary(admin/http/tomcat_administration) > set RHOSTS 192.168.127.3
RHOSTS ⇒ 192.168.127.3
msf6 auxiliary(admin/http/tomcat_administration) > RUN
[-] Unknown command: RUN
msf6 auxiliary(admin/http/tomcat_administration) > run

[*] http://192.168.127.3:8180/admin [Apache-Coyote/1.1] [Apache Tomcat/5.5] [
Tomcat Server Administration] [tomcat/tomcat]
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(admin/http/tomcat_administration) >
```

Finding IPT006: ISC BIND Denial of Service [High]

Description:	A denial of service (DoS) vulnerability exists in ISC BIND versions 9.11.18 / 9.11.18-S1 / 9.12.4-P2 / 9.13 / 9.14.11 / 9.15 / 9.16.2 / 9.17 / 9.17.1 and earlier. An unauthenticated, remote attacker can exploit this issue, via a specially-crafted message, to cause the service to stop responding.
Risk:	Likelihood: High Impact: meduim
System:	192.168.127.3
Tools Used:	Nessus
References:	CVE-2020-8617: A logic error in code which checks TSIG validity can be (isc.org)

Remediation

- Upgrade to the ISC BIND version referenced in the vendor advisory.

Evidence

```
Installed version : 9.4.2
Fixed version     : 9.11.19
```

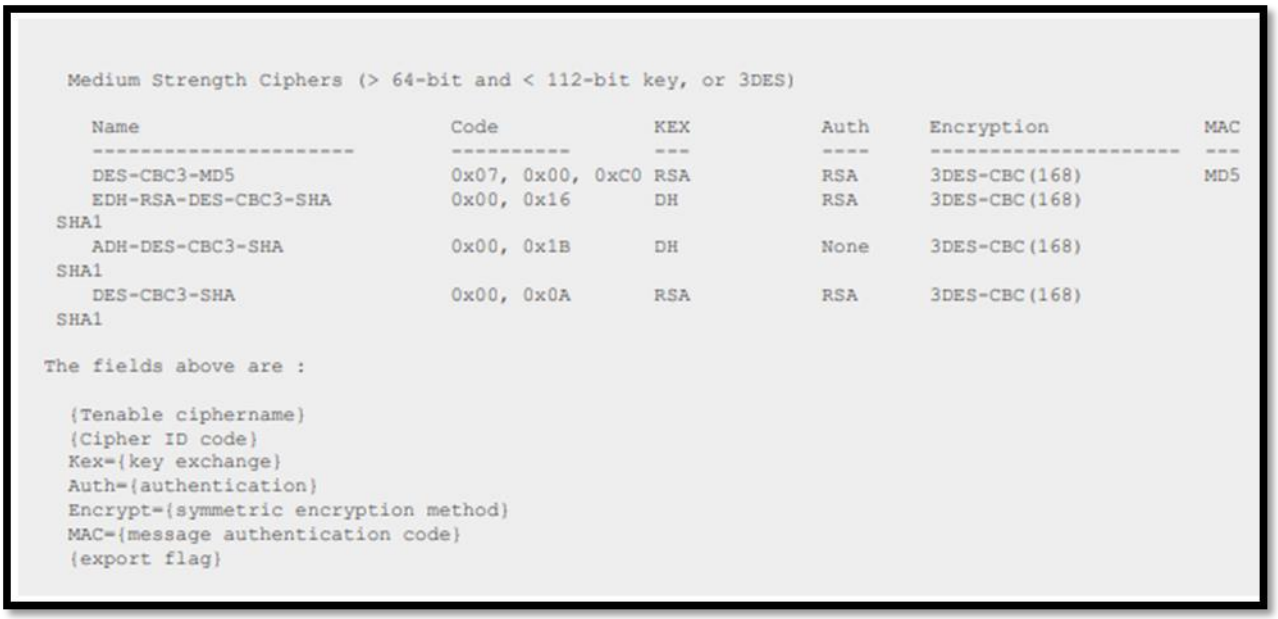
Finding IPT007: SSL Medium Strength Cipher Suites Supported (SWEET32) [High]

Description:	The remote host supports the use of SSL ciphers that offer medium strength encryption. Nessus regards medium strength as any encryption that uses key lengths at least 64 bits and less than 112 bits, or else that uses the 3DES encryption suite. Note that it is considerably easier to circumvent medium strength encryption if the attacker is on the same physical network.
Risk:	Likelihood: High Impact: High
System:	192.168.127.3
Tools Used:	Nessus
References:	The SWEET32 Issue, CVE-2016-2183 - OpenSSL Blog

Remediation

- Reconfigure the affected application if possible to avoid use of medium strength ciphers.

Evidence



```
Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

   Name                         Code              KEX          Auth     Encryption             MAC
   ---------------------------  ----------        ---          ----     --------------------   ---
   DES-CBC3-MD5                 0x07, 0x00, 0xC0  RSA          RSA      3DES-CBC(168)          MD5
   EDH-RSA-DES-CBC3-SHA         0x00, 0x16        DH           RSA      3DES-CBC(168)
SHA1
   ADH-DES-CBC3-SHA             0x00, 0x1B        DH           None     3DES-CBC(168)
SHA1
   DES-CBC3-SHA                 0x00, 0x0A        RSA          RSA      3DES-CBC(168)
SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

Finding IPT008: NFS Shares World Readable [High]

Description:	The remote NFS server is exporting one or more shares without restricting access (based on hostname, IP, or IP range).
Risk:	Likelihood: Medium Impact: High
System:	192.168.127.3
Tools Used:	Nessus
References:	The Linux Documentation Project (tldp.org)

Remediation

- Place the appropriate restrictions on all NFS shares.

Evidence

Finding IPT009: Unix Operating System Unsupported Version Detection [Critical]

Description:	According to its self-reported version number, the Unix operating system running on the remote host is no longer supported. Lack of support implies that no new security patches for the product will be released by the vendor. As a result, it is likely to contain security vulnerabilities.
Risk:	Likelihood: High Impact: Very High
System:	192.168.127.3
Tools Used:	Nessus
References:	XREF IAVA:0001-A-0502 XREF IAVA:0001-A-0648

Evidence

Remediation

- Upgrade to a version of the Unix operating system that is currently supported.

Finding IPT010: SSL Version 2 and 3 Protocol Detection [Critical]

Description:	The remote service accepts connections encrypted using SSL 2.0 and/or SSL 3.0. These versions of SSL are affected by several cryptographic flaws, including: - An insecure padding scheme with CBC ciphers. - Insecure session renegotiation and resumption schemes. An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients. Although SSL/TLS has a secure means for choosing the highest supported version of the protocol (so that these versions will be used only if the client or server support nothing better), many web browsers implement this in an unsafe way that allows an attacker to downgrade a connection (such as in POODLE). Therefore, it is recommended that these protocols be disabled entirely. NIST has determined that SSL 3.0 is no longer acceptable for secure communications. As of the date of enforcement found in PCI DSS v3.1, any version of SSL will not meet the PCI SSC's definition of 'strong cryptography'.
Risk:	Likelihood: High Impact: Very High
System:	192.168.127.3
Tools Used:	Nessus
References:	ImperialViolet - POODLE attacks on SSLv3

Evidence

```
- SSLv3 is enabled and the server supports at least one cipher.
Explanation: TLS 1.0 and SSL 3.0 cipher suites may be used with SSLv3


  Medium Strength Ciphers (> 64-bit and < 112-bit key, or 3DES)

    Name                          Code              KEX          Auth     Encryption             MAC
    ----------------------        ----------        ---          ----     --------------------   ---
    EDH-RSA-DES-CBC3-SHA                            DH           RSA      3DES-CBC(168)
 SHA1
    DES-CBC3-SHA                                    RSA          RSA      3DES-CBC(168)
 SHA1

  High Strength Ciphers (>= 112-bit key)

    Name                          Code              KEX          Auth     Encryption             MAC
    ----------------------        ----------        ---          ----     --------------------   ---
```

```
    DHE-RSA-AES128-SHA                              DH           RSA      AES-CBC(128)
 SHA1
    DHE-RSA-AES256-SHA                              DH           RSA      AES-CBC(256)
 SHA1
    AES128-SHA                                      RSA          RSA      AES-CBC(128)
 SHA1
    AES256-SHA                                      RSA          RSA      AES-CBC(256)
 SHA1
    RC4-MD5                                         RSA          RSA      RC4(128)               MD5
    RC4-SHA                                         RSA          RSA      RC4(128)
 SHA1

The fields above are :

  {Tenable ciphername}
  {Cipher ID code}
  Kex={key exchange}
  Auth={authentication}
  Encrypt={symmetric encryption method}
  MAC={message authentication code}
  {export flag}
```

Remediation

- Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead

Finding IPT011: SSL Certificate Signed Using Weak Hashing Algorithm [High]

Description:	The remote service uses an SSL certificate chain that has been signed using a cryptographically weak hashing algorithm (e.g. MD2, MD4, MD5, or SHA1). These signature algorithms are known to be vulnerable to collision attacks. An attacker can exploit this to generate another certificate with the same digital signature, allowing an attacker to masquerade as the affected service. Note that this plugin reports all SSL certificate chains signed with SHA-1 that expire after January 1, 2017 as vulnerable. This is in accordance with Google's gradual sunsetting of the SHA-1 cryptographic hash algorithm. Note that certificates in the chain that are contained in the Nessus CA database (known_CA.inc) have been ignored.
Risk:	Likelihood: Medium Impact: High
System:	192.168.127.3
Tools Used:	Nessus
References:	Cryptanalysis of SHA-1 - Schneier on Security

Evidence

```
The following certificates were part of the certificate chain sent by
the remote host, but contain hashes that are considered to be weak.

Subject              : CN=owaspbwa
Signature Algorithm : SHA-1 With RSA Encryption
Valid From           : Jan 02 21:12:38 2013 GMT
Valid To             : Dec 31 21:12:38 2022 GMT
Raw PEM certificate :
-----BEGIN CERTIFICATE-----
MIIBnTCCAQYCCQDmhw3dcsK55zANBgkqhkiG9w0BAQUFADATMREwDwYDVQQDEwhvd2FzcGJ3YTAeFw0xMzAxMDIyMTEyMzhaFw0yMj
uafR15KK+k0Yr1xNjjuPd7iX/AKdUh5wAzM0MqoZeEKi72HwiTezYFJFLvpMQ/6PB
+ALtxYnAf7vQkSxmQLsoeKRowKZOV4nIjuEFKCp3ERk7xDbOns5bt62IG9Hxji5cbJMaq4CIMsQc1NHtQIDAQABMA0GCSqGSIb3DQE
+2+oIaiUwN8HDAsaMZGfWzv2rncBQOvyfqxARKzL6H+CZ+Rb5MQos7t5OtwHs1HtRU3A6pPOPLai+/ly1/
aCwmqNTxpghTNFmVLloxT/HJao
-----END CERTIFICATE-----
```

Remediation

Finding IPT012: Samba Badlock Vulnerability [High]

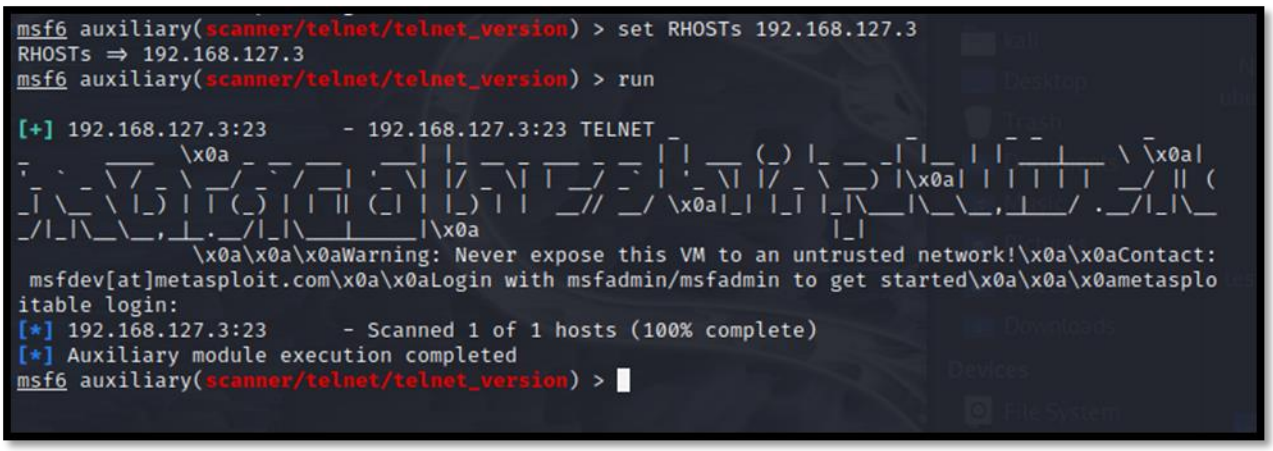
Description:	The version of Samba, a CIFS/SMB server for Linux and Unix, running on the remote host is affected by a flaw, known as Badlock, that exists in the Security Account Manager (SAM) and Local Security Authority (Domain Policy) (LSAD) protocols due to improper authentication level negotiation 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.
Risk:	Likelihood: Medium Impact: High
System:	192.168.127.3
Tools Used:	Nessus
References:	Samba - Security Announcement Archive

Remediation

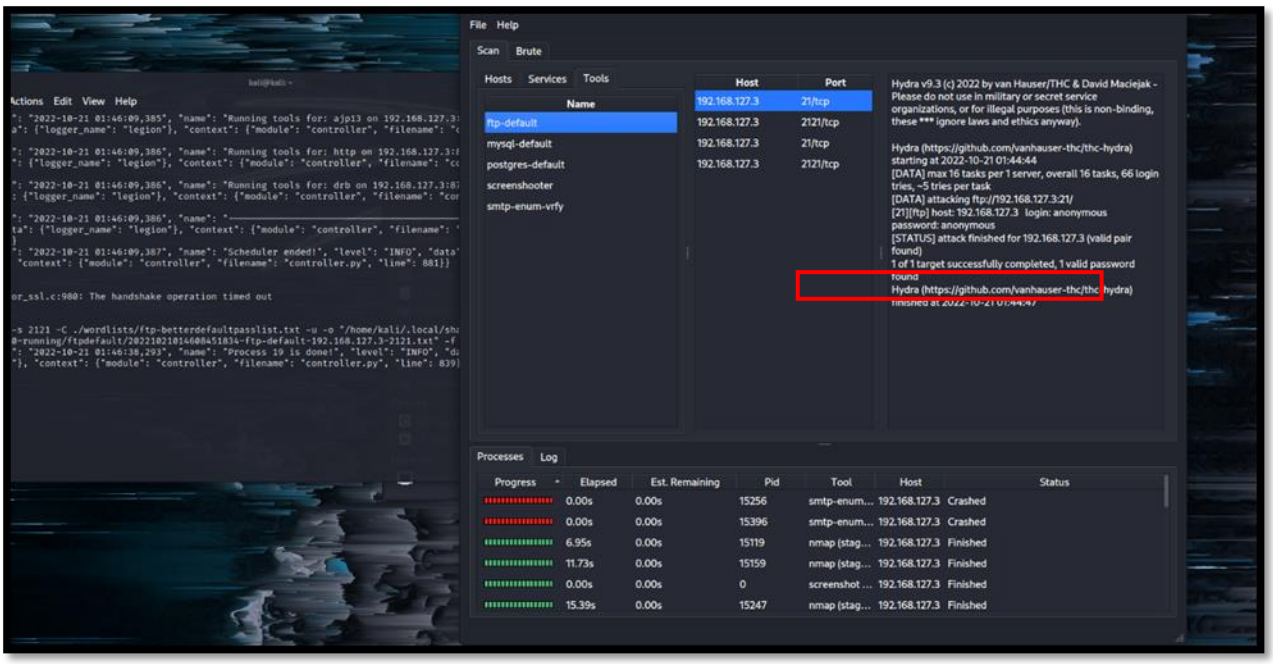
- Upgrade to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

Additional Findings

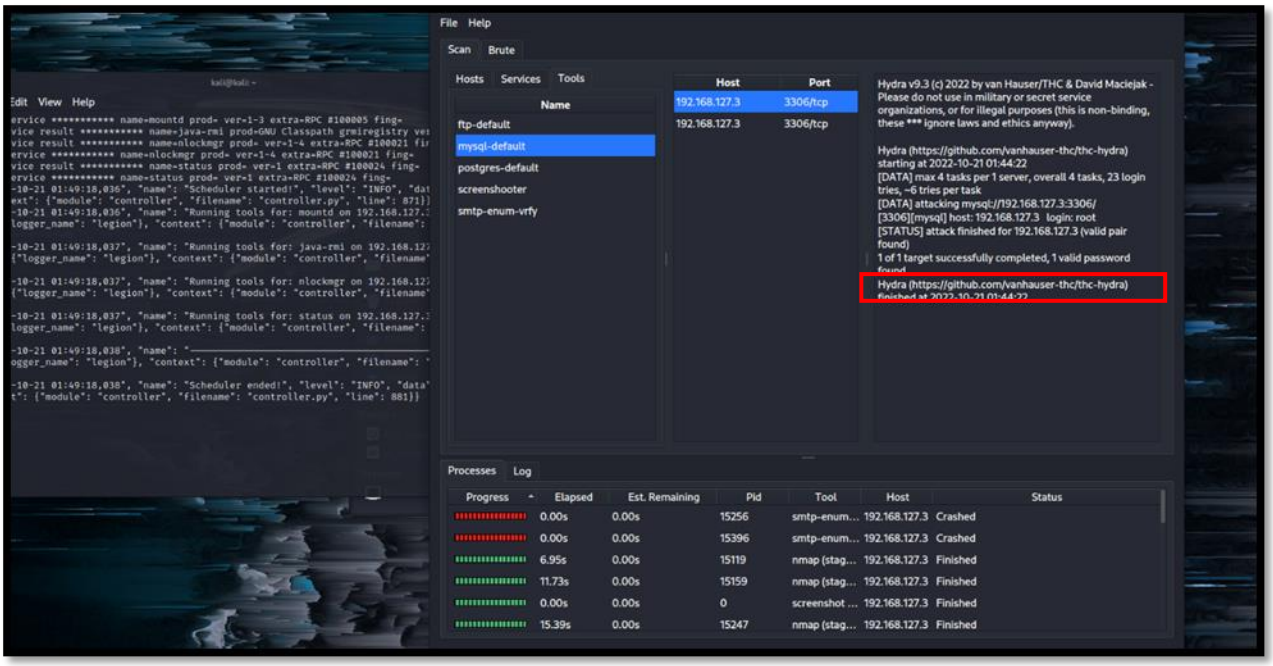
Open Telnet Port -23



Open FTP Port – 21



Postgres Default Credentials



Able to login into MySQL server without passwords.

```
┌──(kali㉿kali)-[~]
└─$ mysql -u root -p -h 192.168.127.3
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 57
Server version: 5.0.51a-3ubuntu5 (Ubuntu)

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MySQL [(none)]>
MySQL [(none)]>
MySQL [(none)]>
MySQL [(none)]>
MySQL [(none)]>
```

Additional Reports and Scans

CyberOps provides all clients with all report information gathered during testing. This includes Nessus files and full vulnerability scans in detailed formats. These reports contain raw vulnerability scans and additional vulnerabilities not exploited by CyberOps.