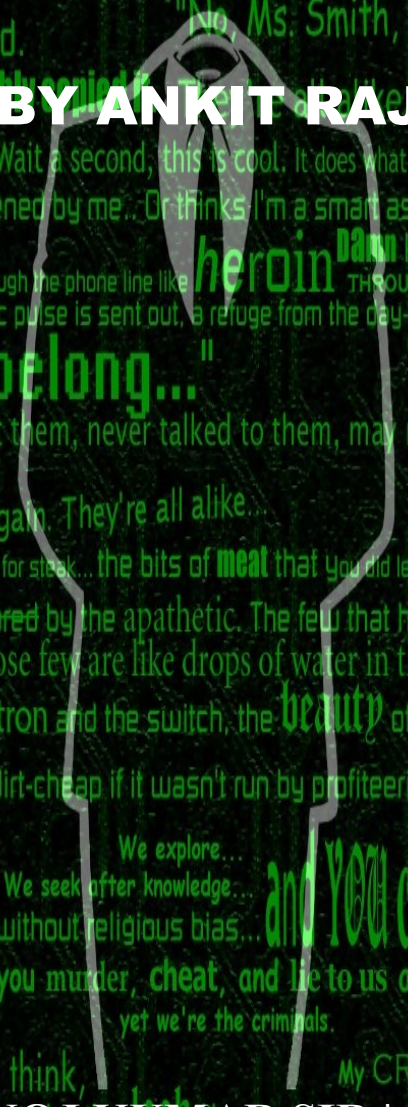
ASSIGNMENT NUMBER 02

NETWORK SCANNING REPORT

BY ANKIT RAJ



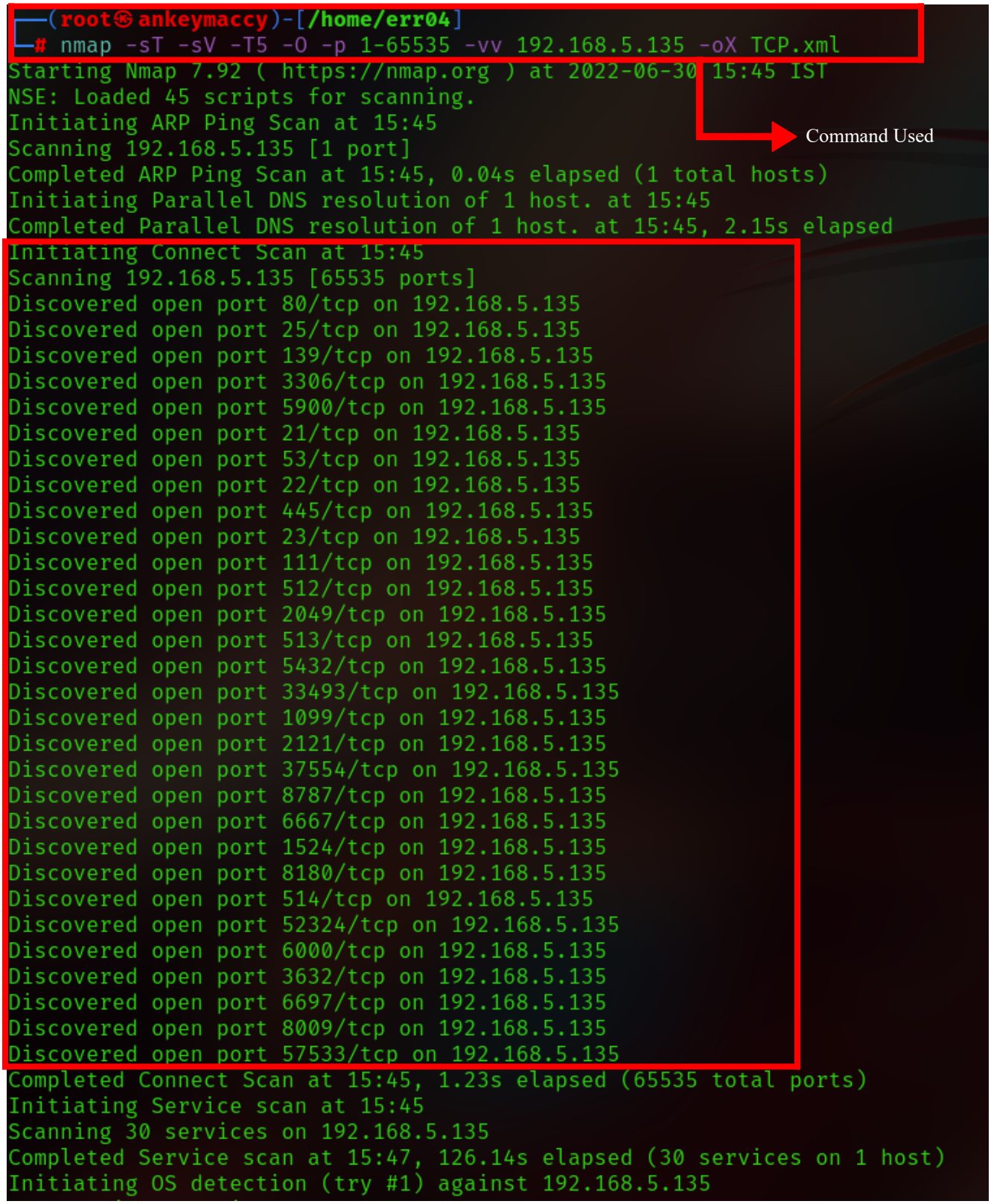
SUBMITTED TO - MANOJ KUMAR SIR | mmanoj.manu26@gmail.com

TARGET - METASPOITABLE 2

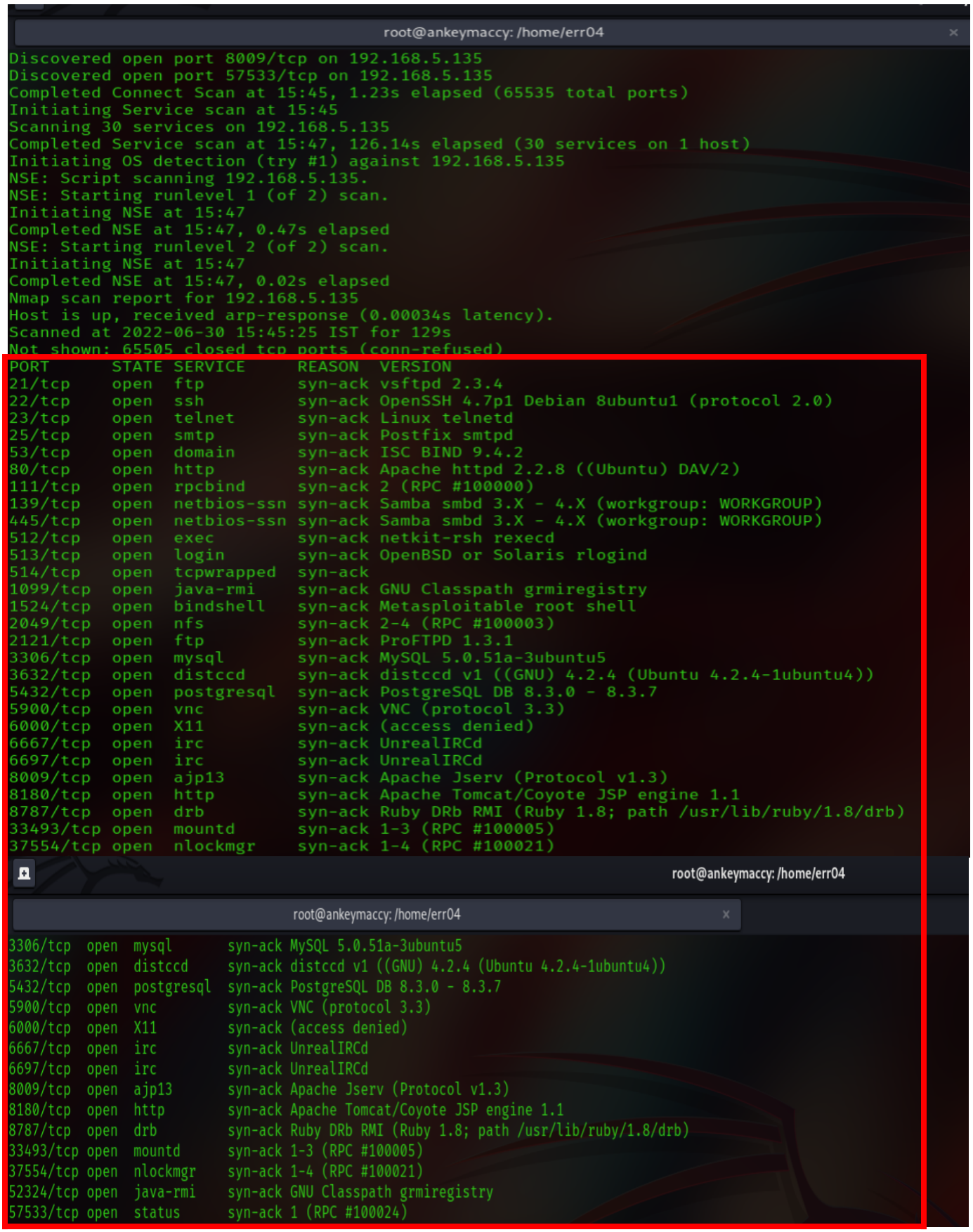
TASKS TO DO AND OTHER INFO :-

1. TARGET'S IP - 192.168.5.135
2. EXISTENCE - LOCAL NETWORK
3. TASK 1 - SCAN FOR OPEN PORTS
4. TASK 2 - SCAN FOR RUNNING SERVICES
5. TASK 3 - SCAN FOR OS DETAILS
6. TASK 4 - CONVERT THE XML SCAN REPORT INTO HTML FILE
7. SCAN SUMMARY
8. TASK 5 - LIST TOP 5 VULNERABILITIES USING EXPLOIT DB
9. ATTACH THE SCREENSHOT ALONG WITH THE HTML REPORT FILE IN THE MAIL
10. RUN A SCRIPT ENGINE

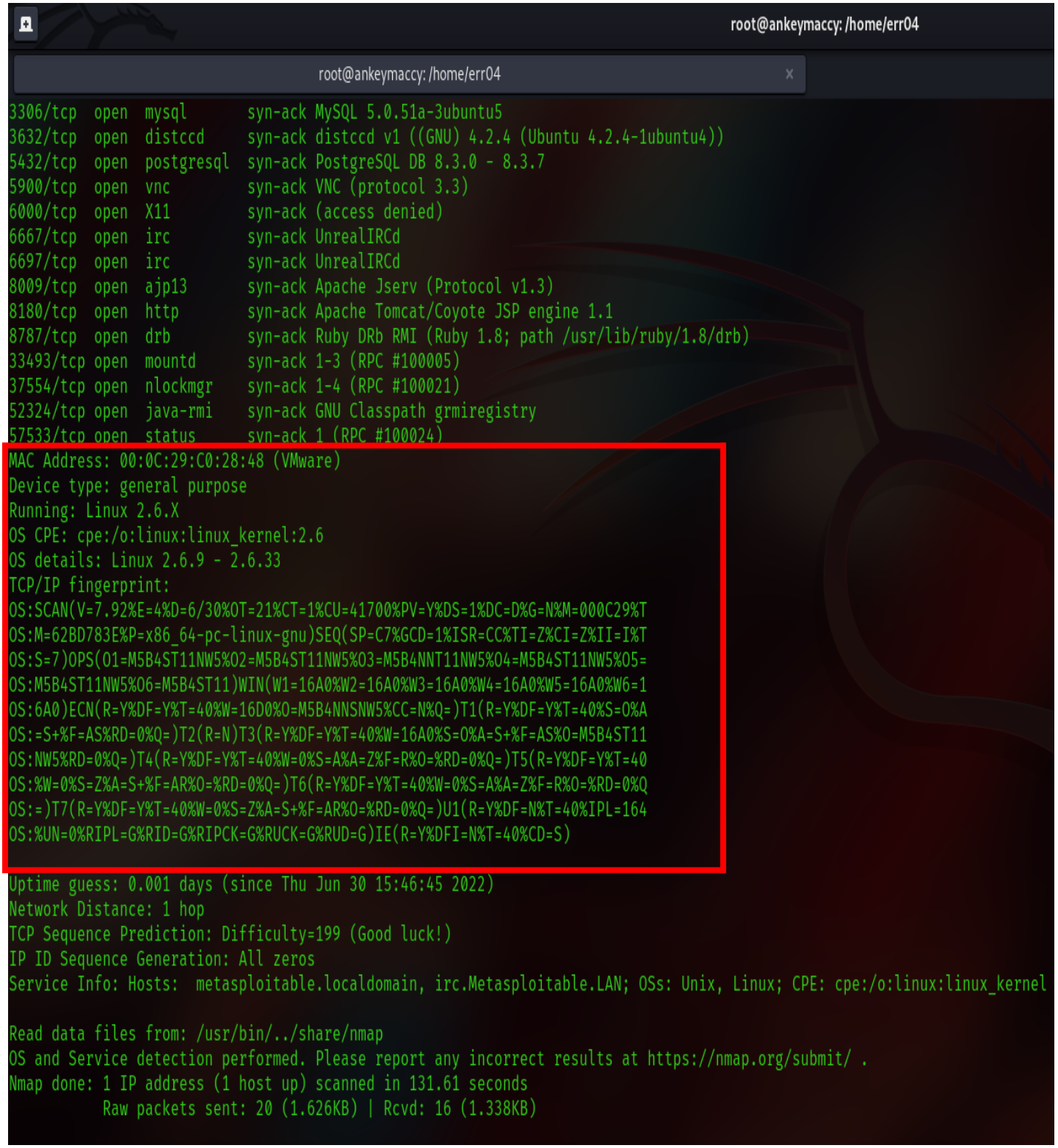
1. SCAN FOR OPEN PORTS



2. SCAN FOR RUNNING SERVICES



3. SCAN FOR OS DETAILS



4. CONVERT THE XML REPORT INTO HTML

```
┌──(root㉿ankeymaccy)-[/home/err04]
└─# xsltproc TCP.xml -o TCP.html

┌──(root㉿ankeymaccy)-[/home/err04]
└─# ls
Desktop  Documents  Downloads  Music  Pictures  Public  TCP.html  TCP.xml  Templates  Videos
```

5. SCAN SUMMARY :-

Scan Summary

Nmap 7.92 was initiated at Thu Jun 30 15:45:22 2022 with these arguments:
nmap -sT -sV -T5 -O -p 1-65535 -vv -oX TCP.xml 192.168.5.135

Verbosity: 2; Debug level 0

Nmap done at Thu Jun 30 15:47:34 2022; 1 IP address (1 host up) scanned in 131.61 seconds

192.168.5.135

Address

- 192.168.5.135 (ipv4)
- 00:0C:29:C0:28:48 - VMware (mac)

Ports

The 65505 ports scanned but not shown below are in state: **closed**

- 65505 ports replied with: **conn-refused**

Port		State (toggle closed [0] | filtered [0])	Service	Reason	Product	Version	Extra info
21	tcp	open	ftp	syn-ack	vsftpd	2.3.4	
22	tcp	open	ssh	syn-ack	OpenSSH	4.7p1 Debian 8ubuntu1	protocol 2.0
23	tcp	open	telnet	syn-ack	Linux telnetd		
25	tcp	open	smtp	syn-ack	Postfix smtpd		
53	tcp	open	domain	syn-ack	ISC BIND	9.4.2	
80	tcp	open	http	syn-ack	Apache httpd	2.2.8	(Ubuntu) DAV/2
111	tcp	open	rpcbind	syn-ack		2	RPC #100000
139	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
445	tcp	open	netbios-ssn	syn-ack	Samba smbd	3.X - 4.X	workgroup: WORKGROUP
512	tcp	open	exec	syn-ack	netkit-rsh rexecd		
513	tcp	open	login	syn-ack	OpenBSD or Solaris rlogind		
514	tcp	open	tcpwrapped	syn-ack			
1099	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
1524	tcp	open	bindshell	syn-ack	Metasploitable root shell		
2049	tcp	open	nfs	syn-ack		2-4	RPC #100003
2121	tcp	open	ftp	syn-ack	ProFTPD	1.3.1	
3306	tcp	open	mysql	syn-ack	MySQL	5.0.51a-3ubuntu5	
3632	tcp	open	distccd	syn-ack	distccd	v1	(GNU) 4.2.4 (Ubuntu 4.2.4-1ubuntu4)
5432	tcp	open	postgresql	syn-ack	PostgreSQL DB	8.3.0 - 8.3.7	
5900	tcp	open	vnc	syn-ack	VNC		protocol 3.3
6000	tcp	open	X11	syn-ack			access denied
6667	tcp	open	irc	syn-ack	UnrealIRCd		
6697	tcp	open	irc	syn-ack	UnrealIRCd		
8009	tcp	open	ajp13	syn-ack	Apache Jserv		Protocol v1.3
8180	tcp	open	http	syn-ack	Apache Tomcat/Coyote JSP engine	1.1	
8787	tcp	open	drb	syn-ack	Ruby DRb RMI		Ruby 1.8; path /usr/lib/ruby/1.8/drb
33493	tcp	open	mountd	syn-ack		1-3	RPC #100005
37554	tcp	open	nlockmgr	syn-ack		1-4	RPC #100021
52324	tcp	open	java-rmi	syn-ack	GNU Classpath grmiregistry		
57533	tcp	open	status	syn-ack		1	RPC #100024

Remote Operating System Detection

- Used port: **21/tcp** (**open**)
- Used port: **1/tcp** (**closed**)
- Used port: **41700/udp** (**closed**)
- OS match: **Linux 2.6.9 - 2.6.33** (**100%**)

- OS identified but the fingerprint was requested at scan time. **(click to expand)**

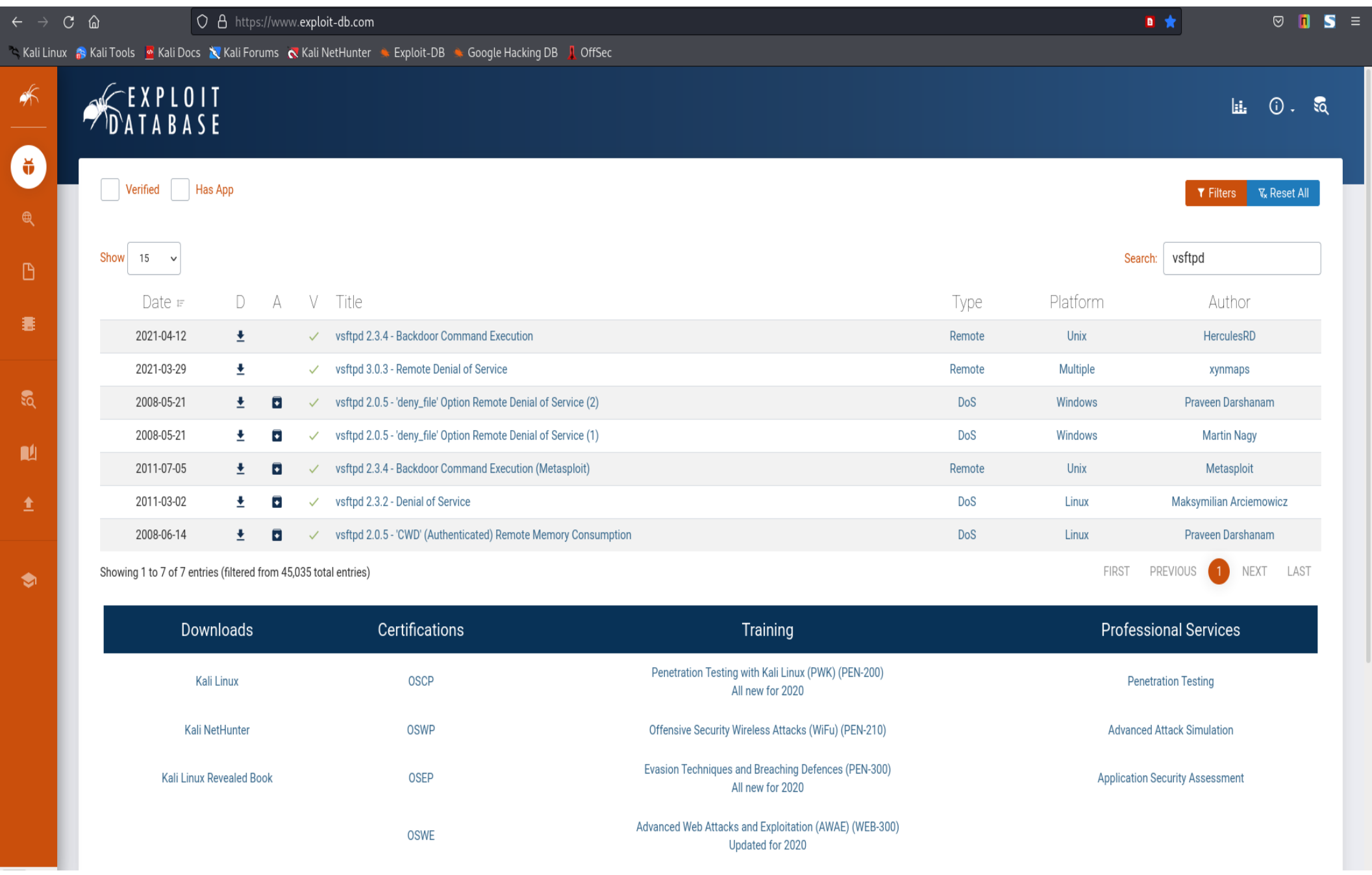
Operating System fingerprint
OS:SCAN(V=7.92%E=4%D=6/30%OT=21%CT=1%CU=41700%PV=Y%DS=1%DC=D%G=N%M=000C29%T OS:M=62BD783E%P=x86_64-pc-linux-gnu)SEQ(SP=C7%GCD=1%ISR=CC%TI=Z%CI=Z%II=I%T OS:S=7)OPS(O1=M5B4ST11NW5%O2=M5B4ST11NW5%O3=M5B4NNT11NW5%O4=M5B4ST11NW5%O5= OS:M5B4ST11NW5%O6=M5B4ST11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=1 OS:6A0)ECN(R=Y%DF=Y%T=40%W=16D0%O=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=O%A OS:=S+%F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=O%A=S+%F=AS%O=M5B4ST11 OS:NW5%RD=0%Q=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q=)T5(R=Y%DF=Y%T=40 OS:%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%O=%RD=0%Q OS:=)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+%F=AR%O=%RD=0%Q=)U1(R=Y%DF=N%T=40%IPL=164 OS:%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Misc Metrics **(click to expand)**

Metric	Value
Ping Results	arp-response
System Uptime	49 seconds (last reboot: Thu Jun 30 15:46:45 2022)
Network Distance	1 hops
TCP Sequence Prediction	Difficulty=199 (Good luck!)
IP ID Sequence Generation	All zeros

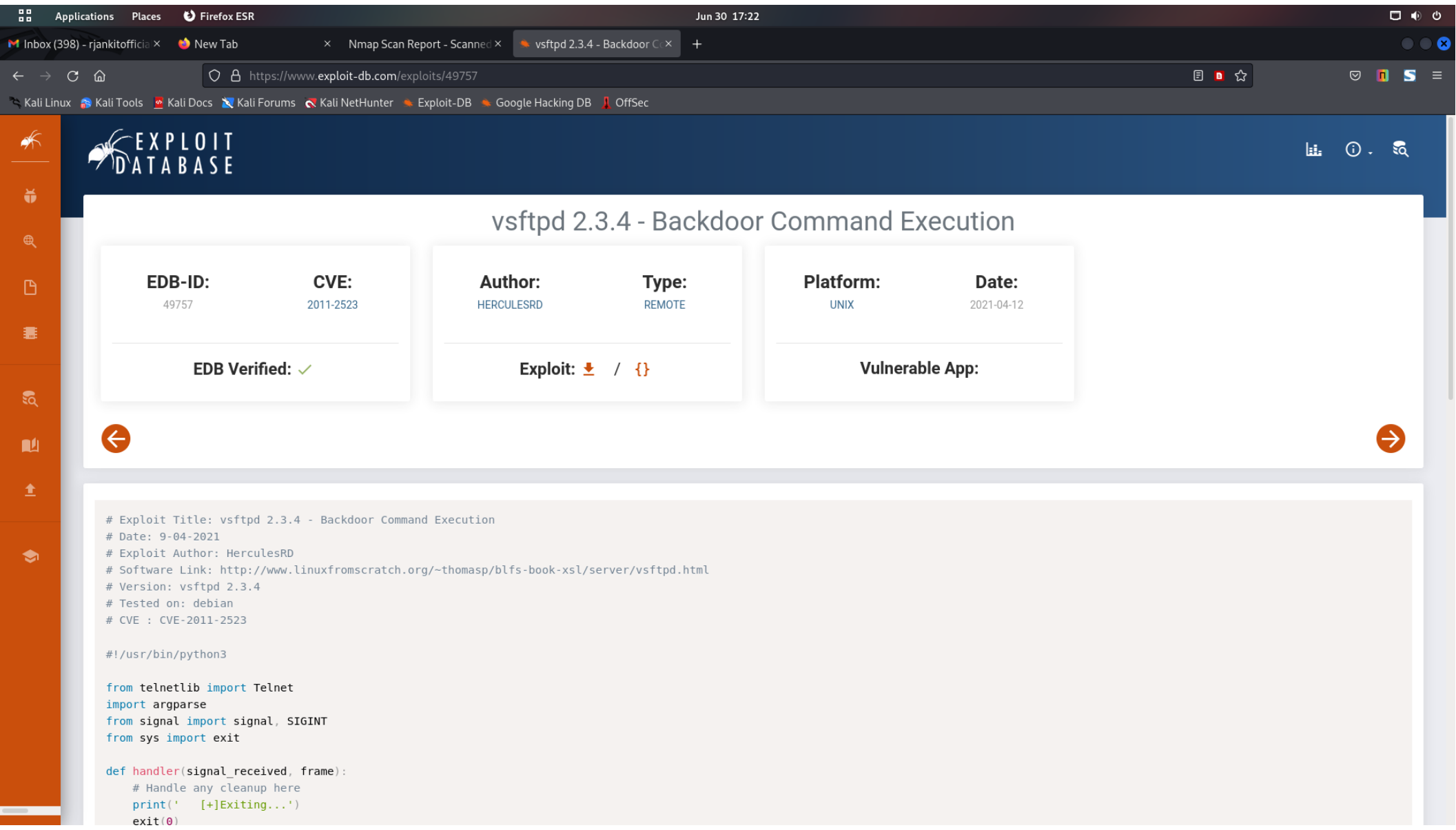
6. LIST TOP 5 VULNERABILITIES ON OUR TARGET USING EXPLOIT DB

i.) - PRODUCT NAME - vsftpd
- INSTALLED VERSION - V2.3.4
- EXPLOIT LIST THAT WORKS ON <= V3.0.5 and



BELOW :-

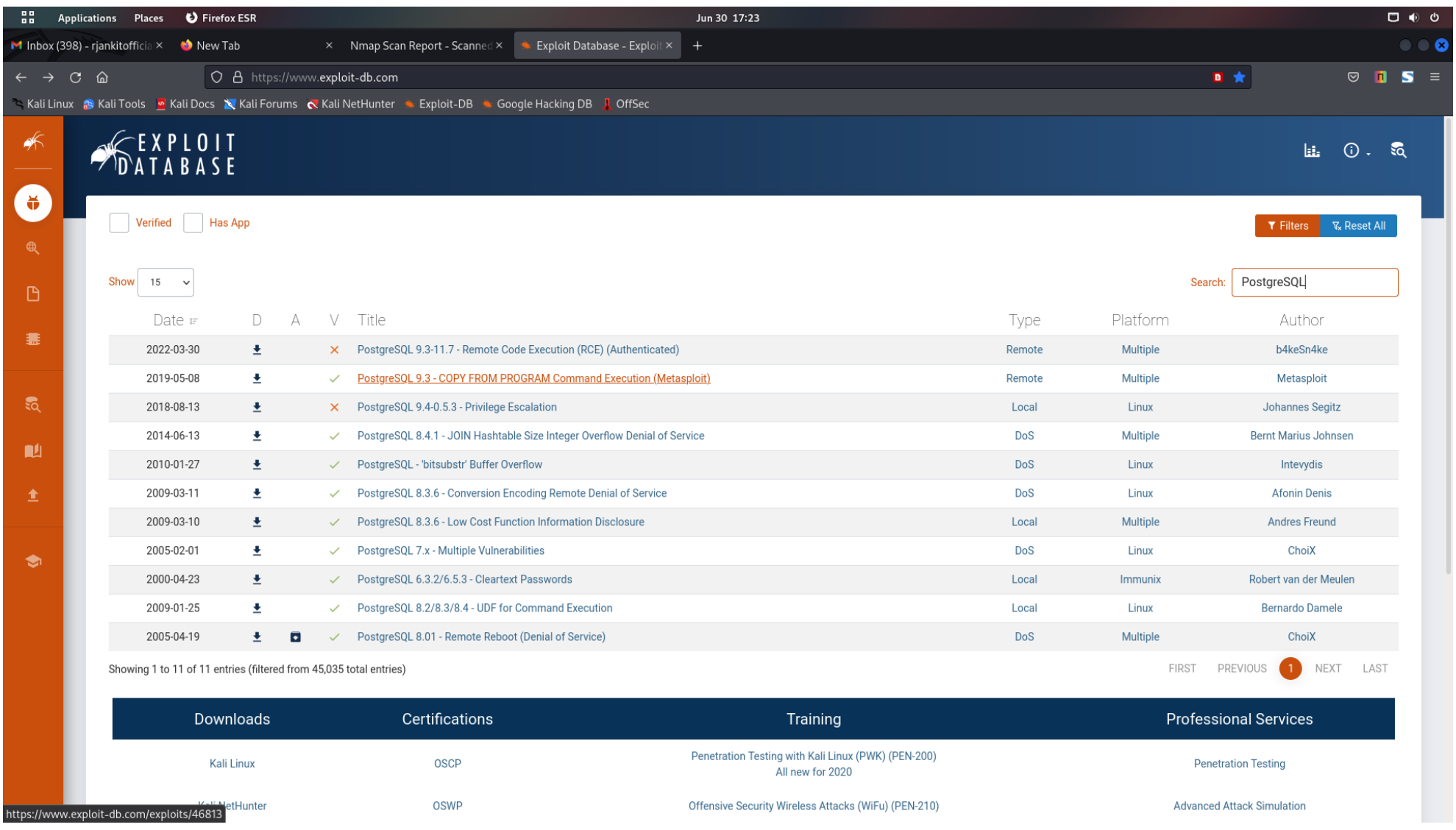
- CVE of vsftpd V2.3.4 is 2011-2523 and it will work on our target



ii.) - PRODUCT NAME - PostgreSQL

- INSTALLED VERSION - V8.3.0 - 8.3.7

- EXPLOIT LIST THAT WORKS ON < =V11.7 and BELOW:-



- CVE of PostgreSQL V9.3 is 2019-9193 and it work on our target as well.

EXPLOIT DATABASE

PostgreSQL 9.3 - COPY FROM PROGRAM Command Execution (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
46813	2019-9193	METASPLOIT	REMOTE	MULTIPLE	2019-05-08

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
\##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core/exploit/postgres'

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::Postgres
  include Msf::Exploit::Remote::Tcp
  include Msf::Auxiliary::Report

  def initialize(info = {})
    super(update_info(info,
```

iii.) - PRODUCT NAME - samba
- INSTALLED VERSION - V3.X - 4.X
- EXPLOIT LIST THAT WORKS ON < =V3.5.0 and BELOW:-

Applications Places Firefox ESR Jun 30 17:27

Inbox (398) - rjankitofficia × New Tab × Nmap Scan Report - Scanned × Exploit Database - Exploit ×

https://www.exploit-db.com

Kali Linux Kali Tools Kali Docs Kali Forums Kali NetHunter Exploit-DB Google Hacking DB OffSec

EXPLOIT DATABASE

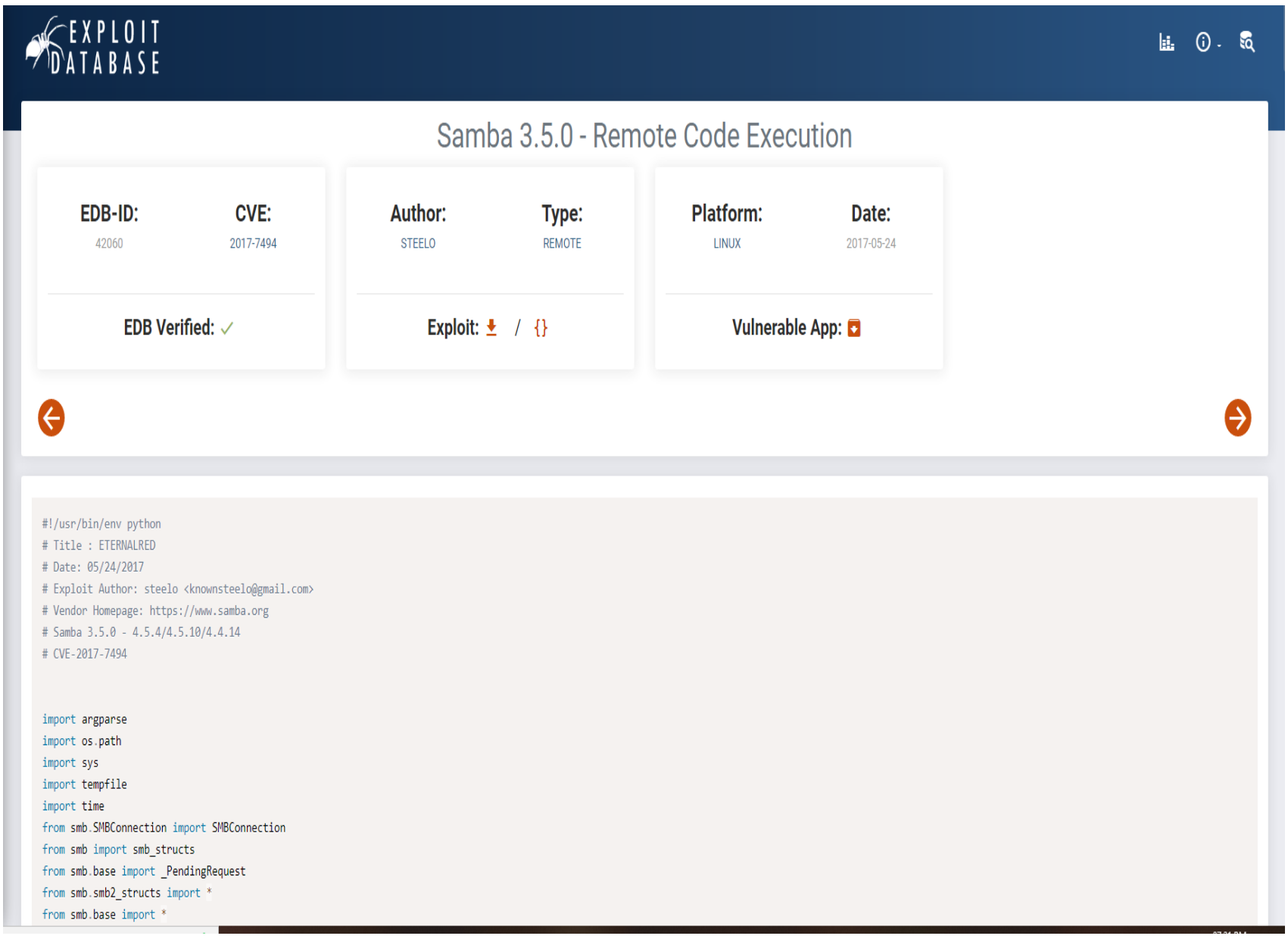
Verified Has App Filters Reset All

Show 15 Search: samba

Date	D	A	V	Title	Type	Platform	Author
2017-05-29			✓	Samba 3.5.0 < 4.4.14/4.5.10/4.6.4 - 'is_known_pipename()' Arbitrary Module Load (Metasploit)	Remote	Linux	Metasploit
2017-05-24			✓	Samba 3.5.0 - Remote Code Execution	Remote	Linux	steelo
2017-03-27			✓	Samba 4.5.2 - Symlink Race Permits Opening Files Outside Share Directory	Remote	Multiple	Google Security Research
2012-09-24			✓	Samba 3.5.11/3.6.3 - Remote Code Execution	Remote	Linux	kb
2015-04-13			✗	Samba < 3.6.2 (x86) - Denial of Service (PoC)	DoS	Linux_x86	sleepya
2010-02-04			✓	Samba 3.4.5 - Symlink Directory Traversal	Remote	Linux	kingcope
2010-02-04			✓	Samba 3.4.5 - Symlink Directory Traversal (Metasploit)	Remote	Linux	kingcope
2009-05-19			✓	Samba 3.3.5 - Format String / Security Bypass	Remote	Linux	Jeremy Allison
2013-08-22			✗	Samba 3.5.22/3.6.17/4.0.8 - nttrans Reply Integer Overflow	DoS	Linux	x90c
2005-05-24			✓	Sambar Server 5.x/6.0/6.1 - Server Referer Cross-Site Scripting	Remote	Windows	Jamie Fisher
2005-05-24			✓	Sambar Server 5.x/6.0/6.1 - logout RCredirect Cross-Site Scripting	Remote	Windows	Jamie Fisher
2005-05-24			✓	Sambar Server 5.x/6.0/6.1 - 'results.stm' indexname Cross-Site Scripting	Remote	Windows	Jamie Fisher
2004-06-01			✓	Sambar Server 6.1 Beta 2 - 'showini.asp' Arbitrary File Access	Remote	Windows	Oliver Karow
2004-06-01			✓	Sambar Server 6.1 Beta 2 - 'showperf.asp?title' Cross-Site Scripting	Remote	Windows	Oliver Karow
2004-06-01			✓	Sambar Server 6.1 Beta 2 - 'show.asp?show' Cross-Site Scripting	Remote	Windows	Oliver Karow

Showing 1 to 15 of 68 entries (filtered from 45,035 total entries) FIRST PREVIOUS 1 2 3 4 5 NEXT LAST

- CVE of samba V3.5.0 is 2017-7494 and it work on our target as well.



iv.) - PRODUCT NAME - ProFTPD
- INSTALLED VERSION - V1.3.1
- EXPLOIT LIST THAT WORKS ON < =V1.3.1 and BELOW:-

- CVE of ProFTPD V1.3.5 is 2015-3306 and it will work on our target as well.

EXPLOIT DATABASE

ProFTPd 1.3.5 - 'mod_copy' Command Execution (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
37262	2015-3306	METASPLOIT	REMOTE	LINUX	2015-06-10

EDB Verified: ✓ Exploit: / {} Vulnerable App:

```
##
# This module requires Metasploit: http://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

require 'msf/core'

class Metasploit3 < Msf::Exploit::Remote

  Rank = ExcellentRanking

  include Msf::Exploit::Remote::Tcp
  include Msf::Exploit::Remote::HttpClient

  def initialize(info = {})
    super(update_info(info,
      'Name'           => 'ProFTPD 1.3.5 Mod_Copy Command Execution',
      'Description'    => %q{
```

v.) - PRODUCT NAME - apache tomcat
- INSTALLED VERSION - V1.1
- EXPLOIT LIST THAT WORKS ON < = V9.0.1 and BELOW:-

EXPLOIT DATABASE

Verified Has App Filters Reset All

Show 15 Search: apache tomcat

Date	D	A	V	Title	Type	Platform	Author
2021-07-13	⬇		✗	Apache Tomcat 9.0.0.M1 - Cross-Site Scripting (XSS)	WebApps	Multiple	Central InfoSec
2021-07-13	⬇		✗	Apache Tomcat 9.0.0.M1 - Open Redirect	WebApps	Multiple	Central InfoSec
2020-11-13	⬇		✓	Apache Tomcat - AJP 'Ghostcat' File Read/Inclusion (Metasploit)	WebApps	Multiple	SunCSR
2020-02-20	⬇		✗	Apache Tomcat - AJP 'Ghostcat File Read/Inclusion	WebApps	Multiple	YDHCUI
2019-07-03	⬇		✓	Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)	Remote	Windows	Metasploit
2017-10-09	⬇		✓	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (2)	WebApps	JSP	intx0x80
2017-09-20	⬇		✗	Apache Tomcat < 9.0.1 (Beta) / < 8.5.23 / < 8.0.47 / < 7.0.8 - JSP Upload Bypass / Remote Code Execution (1)	WebApps	Windows	xxlegend
2017-04-04	⬇		✗	Apache Tomcat 6/7/8/9 - Information Disclosure	Remote	Multiple	justpentest
2016-10-10	⬇		✗	Apache Tomcat 8/7/6 (RedHat Based Distros) - Local Privilege Escalation	Local	Linux	Dawid Golunski
2016-10-03	⬇		✓	Apache Tomcat 8/7/6 (Debian-Based Distros) - Local Privilege Escalation	Local	Linux	Dawid Golunski
2010-11-30	⬇		✓	AWStats 6.x - Apache Tomcat Configuration File Arbitrary Command Execution	WebApps	CGI	StenoPlasma
2010-11-22	⬇		✓	Apache Tomcat 7.0.4 - 'sort' / 'orderBy' Cross-Site Scripting	Remote	Linux	Adam Muntner
2009-09-02	⬇		✓	Apache Tomcat 3.2 - 404 Error Page Cross-Site Scripting	Remote	Multiple	MustLive
2009-06-03	⬇		✓	Apache Tomcat 6.0.18 - Form Authentication Existing/Non-Existing 'Username' Enumeration	Remote	Multiple	D. Matscheko
2008-08-01	⬇		✓	Apache Tomcat 6.0.16 - 'HttpServletResponse.sendError()' Cross-Site Scripting	Remote	Multiple	Konstantin Kolinko

- CVE of apache tomcat V9.0.1 is 2019-0232 and it will work on our target as well.

EXPLOIT DATABASE

Apache Tomcat - CGIServlet enableCmdLineArguments Remote Code Execution (Metasploit)

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
47073	2019-0232	METASPLOIT	REMOTE	WINDOWS	2019-07-03

EDB Verified: ✓ | Exploit: / {} | Vulnerable App:

```
##
# This module requires Metasploit: https://metasploit.com/download
# Current source: https://github.com/rapid7/metasploit-framework
##

class MetasploitModule < Msf::Exploit::Remote
  Rank = ExcellentRanking

  include Msf::Exploit::Remote::HttpClient
  include Msf::Exploit::CmdStager

  def initialize(info={})
    super(update_info(info,
      'Name'           => 'Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability',
      'Description'    => %q{
        This module exploits a vulnerability in Apache Tomcat's CGIServlet component. When the
```

7. RUN A SCRIPT ENGINE

A.) TARGET - 192.168.5.135
B.) SCRIPT ENGINE NAME - nbstat.nse

```
Applications  Places  Terminal   Jun 30 21:31
root@ankeymaccy: /usr/share/nmap/scripts
root@ankeymaccy: /usr/share/nmap/scripts        err04@ankeymaccy: ~

┌──(root㉿ankeymaccy)-[/usr/share/nmap/scripts]
└─# nmap -sV --script=nbstat.nse 192.168.5.135
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-30 21:18 IST
Nmap scan report for 192.168.5.135
Host is up (0.0018s latency).
Not shown: 977 closed tcp ports (reset)
PORT     STATE SERVICE     VERSION
21/tcp   open  ftp         vsftpd 2.3.4
22/tcp   open  ssh         OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
23/tcp   open  telnet      Linux telnetd
25/tcp   open  smtp        Postfix smtpd
53/tcp   open  domain      ISC BIND 9.4.2
80/tcp   open  http        Apache httpd 2.2.8 ((Ubuntu) DAV/2)
|_http-server-header: Apache/2.2.8 (Ubuntu) DAV/2
111/tcp  open  rpcbind     2 (RPC #100000)
| rpcinfo:
|   program version    port/proto  service
|   100000  2            111/tcp   rpcbind
|   100000  2            111/udp   rpcbind
|   100003  2,3,4       2049/tcp   nfs
|   100003  2,3,4       2049/udp   nfs
|   100005  1,2,3      33493/tcp   mountd
|   100005  1,2,3      35779/udp   mountd
|   100021  1,3,4      37554/tcp   nlockmgr
|   100021  1,3,4      47281/udp   nlockmgr
|   100024  1          57533/tcp   status
|_  100024  1          57706/udp   status
139/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
445/tcp  open  netbios-ssn Samba smbd 3.X - 4.X (workgroup: WORKGROUP)
512/tcp  open  exec        netkit-rsh rexecd
513/tcp  open  login?
514/tcp  open  tcpwrapped
1099/tcp open  java-rmi    GNU Classpath grmiregistry
1524/tcp open  bindshell   Metasploitable root shell
2049/tcp open  nfs         2-4 (RPC #100003)
2121/tcp open  ftp         ProFTPD 1.3.1
3306/tcp open  mysql       MySQL 5.0.51a-3ubuntu5
5432/tcp open  postgresql  PostgreSQL DB 8.3.0 - 8.3.7
5900/tcp open  vnc         VNC (protocol 3.3)
6000/tcp open  X11         (access denied)
```

```
6000/tcp open  X11         (access denied)
6667/tcp open  irc         UnrealIRCd
8009/tcp open  ajp13       Apache Jserv (Protocol v1.3)
8180/tcp open  http        Apache Tomcat/Coyote JSP engine 1.1
|_http-server-header: Apache-Coyote/1.1
MAC Address: 00:0C:29:C0:28:48 (VMware)
Service Info: Hosts:  metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Host script results:
| nbstat: NetBIOS name: METASPLOITABLE, NetBIOS user: <unknown>, NetBIOS MAC: <unknown> (unknown)
| Names:
|   METASPLOITABLE<00>   Flags: <unique><active>
|   METASPLOITABLE<03>   Flags: <unique><active>
|   METASPLOITABLE<20>   Flags: <unique><active>
|   \x01\x02__MSBROWSE__\x02<01>  Flags: <group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 11.65 seconds
```

----------END OF REPORT------THANK YOU----------