

Another one got caught today, it's all over the papers.

"Teenager Arrested in Computer Crime Scandal"

"Hacker Arrested after Bank Tampering..."

Damn kids. They're all ALIKE...

But did you, in your three-piece psychology and 1950's techNObrain, ever take a look behind the eyes of the hacker?

Did you ever wonder what made him tick, what forces shaped him, what may have molded him?

I am a hacker, enter my World. . . .

ASSIGNMENT NUMBER 02

Damn underachiever. They're all alike.

I'm in junior high or high school.

NETWORK SCANNING REPORT

Damn kid.

"No, Ms. Smith, I didn't show my work. I did it in my head..."

BY ANKIT RAJ

I made a discovery today. I found a computer. Wait a second, this is cool. It does what I want it to. If it makes a mistake, it's because I screwed it up.

Not because it doesn't like me... Or feels threatened by me.. Or thinks I'm a smart ass.. Or doesn't like teaching and shouldn't be here...

Damn kid. All he does is play games. They're all alike.

And then it happened... a door opened to a world... rushing through the phone line like heroin THROUGH AN ADDICT'S VEINS,

an electronic pulse is sent out, a refuge from the day-to-day incompetencies is sought... a board is found.

"This is it... this is where I belong..."

I know everyone here... even if I've never met them, never talked to them, may never hear from them again... I know you all...

You bet your ass we're all alike...

Damn kid. Tying up the phone line again. They're all alike.

we've been spoon-fed baby food at school when we hungered for steak... the bits of meat that you did let slip through were pre-chewed and tasteless

We've been dominated by sadists, or ignored by the apathetic. The few that had something to teach found us willing pupils, but those few are like drops of water in the desert.

This is our world now... the world of the electron and the switch, the beauty of the baud. We make use of a service already existing without paying for what could be dirt-cheap if it wasn't run by profiteering gluttons, and you call us criminals.

We explore...

We seek after knowledge.

and You call us criminals.

We exist without skin color, without nationality, without religious bias...

You build atomic bombs, you wage wars, you murder, cheat, and lie to us and try to make us believe it's FOR OUR OWN GOOD, yet we're the criminals.

Yes, I am a criminal. My crime is that of curiosity.

My crime is that of judging people by what they say and think,

My CRIME is that of outsmarting you,

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

I am a hacker, and this is my manifesto.

You may stop this individual, but you can't stop us all...

after all...

WE'RE ALL ALIKE...

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

```
(root㉿ankeymaccy)-[~/home/err04]
# nmap -sT -sV -T5 -O -p 1-65535 -vv 192.168.5.135 -oX TCP.xml
Starting Nmap 7.92 ( https://nmap.org ) at 2022-06-30 15:45 IST
NSE: Loaded 45 scripts for scanning.
Initiating ARP Ping Scan at 15:45
Scanning 192.168.5.135 [1 port]
Completed ARP Ping Scan at 15:45, 0.04s elapsed (1 total hosts)
Initiating Parallel DNS resolution of 1 host. at 15:45
Completed Parallel DNS resolution of 1 host. at 15:45, 2.15s elapsed
Initiating Connect Scan at 15:45
Scanning 192.168.5.135 [65535 ports]
Discovered open port 80/tcp on 192.168.5.135
Discovered open port 25/tcp on 192.168.5.135
Discovered open port 139/tcp on 192.168.5.135
Discovered open port 3306/tcp on 192.168.5.135
Discovered open port 5900/tcp on 192.168.5.135
Discovered open port 21/tcp on 192.168.5.135
Discovered open port 53/tcp on 192.168.5.135
Discovered open port 22/tcp on 192.168.5.135
Discovered open port 445/tcp on 192.168.5.135
Discovered open port 23/tcp on 192.168.5.135
Discovered open port 111/tcp on 192.168.5.135
Discovered open port 512/tcp on 192.168.5.135
Discovered open port 2049/tcp on 192.168.5.135
Discovered open port 513/tcp on 192.168.5.135
Discovered open port 5432/tcp on 192.168.5.135
Discovered open port 33493/tcp on 192.168.5.135
Discovered open port 1099/tcp on 192.168.5.135
Discovered open port 2121/tcp on 192.168.5.135
Discovered open port 37554/tcp on 192.168.5.135
Discovered open port 8787/tcp on 192.168.5.135
Discovered open port 6667/tcp on 192.168.5.135
Discovered open port 1524/tcp on 192.168.5.135
Discovered open port 8180/tcp on 192.168.5.135
Discovered open port 514/tcp on 192.168.5.135
Discovered open port 52324/tcp on 192.168.5.135
Discovered open port 6000/tcp on 192.168.5.135
Discovered open port 3632/tcp on 192.168.5.135
Discovered open port 6697/tcp on 192.168.5.135
Discovered open port 8009/tcp on 192.168.5.135
Discovered open port 57533/tcp on 192.168.5.135
Completed Connect Scan at 15:45, 1.23s elapsed (65535 total ports)
Initiating Service scan at 15:45
Scanning 30 services on 192.168.5.135
Completed Service scan at 15:47, 126.14s elapsed (30 services on 1 host)
Initiating OS detection (try #1) against 192.168.5.135
```

Command Used

2. SCAN FOR RUNNING SERVICES

```
root@ankeymacyy:/home/err04
Discovered open port 8009/tcp on 192.168.5.135
Discovered open port 57533/tcp on 192.168.5.135
Completed Connect Scan at 15:45, 1.23s elapsed (65535 total ports)
Initiating Service scan at 15:45
Scanning 30 services on 192.168.5.135
Completed Service scan at 15:47, 126.14s elapsed (30 services on 1 host)
Initiating OS detection (try #1) against 192.168.5.135
NSE: Script scanning 192.168.5.135.
NSE: Starting runlevel 1 (of 2) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.47s elapsed
NSE: Starting runlevel 2 (of 2) scan.
Initiating NSE at 15:47
Completed NSE at 15:47, 0.02s elapsed
Nmap scan report for 192.168.5.135
Host is up, received arp-response (0.00034s latency).
Scanned at 2022-06-30 15:45:25 IST for 129s
Not shown: 65505 closed tcp ports (conn-refused)

PORT      STATE SERVICE      REASON  VERSION
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 smptd
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/druby)
33493/tcp open  mountd     syn-ack 1-3 (RPC #100005)
37554/tcp open  nlockmgr   syn-ack 1-4 (RPC #100021)

root@ankeymacyy:/home/err04
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/druby)
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)
```

3. SCAN FOR OS DETAILS

```
root@ankeymacy: /home/err04
root@ankeymacy: /home/err04 x

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/drbs)
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)

MAC Address: 00:0C:29:C0:28:48 (VMware)
Device type: general purpose
Running: Linux 2.6.X
OS CPE: cpe:/o:linux:linux_kernel:2.6
OS details: Linux 2.6.9 - 2.6.33
TCP/IP 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%
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=0%A
OS:=S+F=AS%RD=0%Q=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%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%IP=164
OS:%UN=0%RIPL=G%RID=G%RIPCK=G%RUCK=G%RUD=G)IE(R=Y%DFI=N%T=40%CD=S)

Uptime guess: 0.001 days (since Thu Jun 30 15:46:45 2022)
Network Distance: 1 hop
TCP Sequence Prediction: Difficulty=199 (Good luck!)
IP ID Sequence Generation: All zeros
Service Info: Hosts: metasploitable.localdomain, irc.Metasploitable.LAN; OSs: Unix, Linux; CPE: cpe:/o:linux:linux_kernel

Read data files from: /usr/bin/../share/nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 131.61 seconds
    Raw packets sent: 20 (1.626KB) | Rcvd: 16 (1.338KB)
```

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 #10000
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/druby
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=7.92E=4%D=6/38%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=C%GD=1%ISR=CC%TI=Z%CI=Z%II=I%T
OS : S=7)OPS(01=M5B45T11NW5%02=M5B45T11NW5%03=M5B44NT11NW5%04=M5B45T11NW5%05=
OS : M5B45T11NW5%06=M5B45T11)WIN(W1=16A0%W2=16A0%W3=16A0%W4=16A0%W5=16A0%W6=1
OS : 6A0)ECN(R=Y%DF=Y%T=40%W=16D0%0=M5B4NNSNW5%CC=N%Q=)T1(R=Y%DF=Y%T=40%S=0%A
OS : =S+1%F=A5%RD=0%0=)T2(R=N)T3(R=Y%DF=Y%T=40%W=16A0%S=0%A=S+1%F=A5%0=M5B45T11
OS : NW5%RD=0%0=)T4(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%0=)T5(R=Y%DF=Y%T=40
OS : %W=0%S=Z%A=S+F=AR%0=%RD=0%Q=)T6(R=Y%DF=Y%T=40%W=0%S=A%A=Z%F=R%0=%RD=0%Q
OS : =)T7(R=Y%DF=Y%T=40%W=0%S=Z%A=S+F=AR%0=%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

The screenshot shows the Exploit-DB website interface. The search bar at the top contains the query 'vsftpd'. Below the search bar, there are filters for 'Verified' and 'Has App'. The main content area displays a table of exploit entries for 'vsftpd'. The columns include Date, D, A, V, Title, Type, Platform, and Author. The table lists 7 entries, with the first few being:

Date	D	A	V	Title	Type	Platform	Author
2021-04-12	✓	✓	✓	vsftpd 2.3.4 - Backdoor Command Execution	Remote	Unix	HerculesRD
2021-03-29	✓	✓	✓	vsftpd 3.0.3 - Remote Denial of Service	Remote	Multiple	xynmaps
2008-05-21	✓	✓	✓	vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (2)	DoS	Windows	Praveen Darshanam
2008-05-21	✓	✓	✓	vsftpd 2.0.5 - 'deny_file' Option Remote Denial of Service (1)	DoS	Windows	Martin Nagy
2011-07-05	✓	✓	✓	vsftpd 2.3.4 - Backdoor Command Execution (Metasploit)	Remote	Unix	Metasploit
2011-03-02	✓	✓	✓	vsftpd 2.3.2 - Denial of Service	DoS	Linux	Maksymilian Arciemowicz
2008-06-14	✓	✓	✓	vsftpd 2.0.5 - 'CWD' (Authenticated) Remote Memory Consumption	DoS	Linux	Praveen Darshanam

At the bottom of the page, there are links for 'Downloads', 'Certifications', 'Training', and 'Professional Services'.

BELOW :-

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

The screenshot shows a Firefox browser window with the URL <https://www.exploit-db.com/exploits/49757>. The page title is "vsftpd 2.3.4 - Backdoor Command Execution". Key details from the page header include:

EDB-ID:	CVE:	Author:	Type:	Platform:	Date:
49757	2011-2523	HERCULESRD	REMOTE	UNIX	2021-04-12

Below the header, there are buttons for "Exploit" (with download and source code links) and "Vulnerable App". On the left, there is a code snippet for the exploit:

```
# Exploit Title: vsftpd 2.3.4 - Backdoor Command Execution
# Date: 9-04-2021
# Exploit Author: HerculesRD
# Software Link: http://www.linuxfromscratch.org/~thomaspl/blfs-book-xsl/server/vsftpd.html
# Version: vsftpd 2.3.4
# Tested on: debian
# CVE : CVE-2011-2523

#!/usr/bin/python3

from telnetlib import Telnet
import argparse
from signal import signal, SIGINT
from sys import exit

def handler(signal_received, frame):
    # Handle any cleanup here
    print('  [+]\nExiting...')

exit(0)
```

ii.) - PRODUCT NAME - PostgreSQL

- INSTALLED VERSION - V8.3.0 - 8.3.7
- EXPLOIT LIST THAT WORKS ON <=V11.7 and BELOW:-

The screenshot shows a Firefox browser window with the URL <https://www.exploit-db.com/exploits/>. A search bar at the top right contains the text "PostgreSQL". The search results table displays 11 entries:

Date	D	A	V	Title	Type	Platform	Author
2022-03-30				PostgreSQL 9.3-11.7 - Remote Code Execution (RCE) (Authenticated)	Remote	Multiple	b4keSn4ke
2019-05-08				PostgreSQL 9.3 - COPY FROM PROGRAM Command Execution (Metasploit)	Remote	Multiple	Metasploit
2018-08-13				PostgreSQL 9.4-0.5.3 - Privilege Escalation	Local	Linux	Johannes Segitz
2014-06-13				PostgreSQL 8.4.1 - JOIN Hashtable Size Integer Overflow Denial of Service	DoS	Multiple	Bernt Marius Johnsen
2010-01-27				PostgreSQL - 'bitsubstr' Buffer Overflow	DoS	Linux	Intevydis
2009-03-11				PostgreSQL 8.3.6 - Conversion Encoding Remote Denial of Service	DoS	Linux	Afonin Denis
2009-03-10				PostgreSQL 8.3.6 - Low Cost Function Information Disclosure	Local	Multiple	Andres Freund
2005-02-01				PostgreSQL 7.x - Multiple Vulnerabilities	DoS	Linux	ChoiX
2000-04-23				PostgreSQL 6.3.2/6.5.3 - Cleartext Passwords	Local	Immunix	Robert van der Meulen
2009-01-25				PostgreSQL 8.2/8.3/8.4 - UDF for Command Execution	Local	Linux	Bernardo Damele
2005-04-19				PostgreSQL 8.01 - Remote Reboot (Denial of Service)	DoS	Multiple	ChoiX

At the bottom of the page, there are navigation links for "FIRST", "PREVIOUS", "NEXT", and "LAST". Below the table, there are four footer sections: "Downloads", "Certifications", "Training", and "Professional Services".

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

The screenshot shows the Exploit Database interface. At the top, there's a header with the Exploit Database logo and navigation icons. Below the header, the title "PostgreSQL 9.3 - COPY FROM PROGRAM Command Execution (Metasploit)" is displayed. The main content area has several sections: "EDB-ID: 46813", "CVE: 2019-9193", "Author: METASPLOIT", "Type: REMOTE", "Platform: MULTIPLE", and "Date: 2019-05-08". Below these, there are buttons for "EDB Verified: ✓", "Exploit: ⬇ / { }", and "Vulnerable App:". On the left and right sides of the main content area are large orange navigation arrows. At the bottom of the page, there is a code snippet for the exploit module:

```
\##
# 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:-

The screenshot shows the Exploit Database search results for "samba". The search bar at the top contains the text "samba". The results table lists 15 entries, each with columns for Date, D, A, V, Title, Type, Platform, and Author. The entries are as follows:

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	sleepy
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 - ntrans Reply Integer Overflow	DoS	Linux	x90c
2005-05-24	⬇	✓		Sambar Server 5.x/6.0/6.1 - Server Referrer Cross-Site Scripting	Remote	Windows	Jamie Fisher
2005-05-24	⬇	✓		Sambar Server 5.x/6.0/6.1 - logout RCredit 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)

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

Screenshot of the Exploit Database showing details for Samba 3.5.0 - Remote Code Execution (Exploit ID: 42060, CVE: 2017-7494, Author: STEELO, Type: REMOTE, Platform: LINUX, Date: 2017-05-24). The exploit code is displayed in a code editor:

```

#!/usr/bin/env python
# Title : ETERNALRED
# Date: 05/24/2017
# Exploit Author: steelo <knownsteelo@gmail.com>
# Vendor Homepage: https://www.samba.org
# Samba 3.5.0 - 4.5.4/4.5.10/4.4.14
# CVE-2017-7494

import argparse
import os.path
import sys
import tempfile
import time
from smb.SMBConnection import SMBConnection
from smb import smb_structs
from smb.base import _PendingRequest
from smb.smb2_structs import *
from smb.base import *

```

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

Screenshot of the Exploit Database search results for ProFTPD, showing a list of exploits with columns for Date, Denial of Service (D), Author (A), Verified status, Title, Type, Platform, and Author. The search term "ProFTPD" is entered in the search bar.

Date	D	A	Verified	Title	Type	Platform	Author
2021-05-26	⬇️	✓		ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution (2)	Remote	Linux	Shellbr3ak
2021-03-22	⬇️	✗		ProFTPD 1.3.7a - Remote Denial of Service	DoS	Multiple	xynmaps
2015-06-10	⬇️	✓		ProFTPD 1.3.5 - 'mod_copy' Command Execution (Metasploit)	Remote	Linux	Metasploit
2015-04-21	⬇️	✗		ProFTPD 1.3.5 - 'mod_copy' Remote Command Execution	Remote	Linux	R-73eN
2015-04-13	⬇️	✓		ProFTPD 1.3.5 - File Copy	Remote	Linux	anonymous
2009-02-10	⬇️	✓		ProFTPD 1.3 - 'mod_sql' 'Username' SQL Injection	Remote	Multiple	AlpHaNiX
2003-09-23	⬇️	✓		ProFTPD 1.2.7/1.2.8 - 'ASCII' File Transfer Buffer Overrun	DoS	Linux	netris
2002-12-09	⬇️	✓		ProFTPD 1.2.x - 'STAT' Denial of Service	DoS	Linux	Rob klein Gunnewiek
2001-03-15	⬇️	✓		WU-FTPD 2.4/2.5/2.6 / Trolltech ftpd 1.2 / ProFTPD 1.2 / BeroFTPD 1.3.4 FTP - glob Expansion	Remote	Linux	Frank DENIS
2000-12-20	⬇️	✓		ProFTPD 1.2 - 'SIZE' Remote Denial of Service	DoS	Linux	JeT-Li
1999-09-17	⬇️	✓		ProFTPD 1.2 pre6 - 'snprintf' Remote Root	Remote	Linux	Tymo Twillman
1999-08-27	⬇️	✓		ProFTPD 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (2)	Remote	Linux	anonymous
1999-08-17	⬇️	✓		ProFTPD 1.2 pre1/pre2/pre3/pre4/pre5 - Remote Buffer Overflow (1)	Remote	Linux	babcia padlina ltd
1999-02-09	⬇️	✓		WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPD 1.2 pre1 - 'realpath' Remote Buffer Overflow (2)	Remote	Linux	jamez & c0nd0r
1999-02-09	⬇️	✓		WU-FTPD 2.4.2 / SCO Open Server 5.0.5 / ProFTPD 1.2 pre1 - 'realpath' Remote Buffer Overflow (1)	Remote	Linux	smiler & cossack

- 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: 37262	CVE: 2015-3306	Author: METASPLOIT	Type: REMOTE	Platform: LINUX	Date: 2015-06-10
EDB Verified: ✓	Exploit: Download / Source	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	YDHCU
2019-07-03	↓	✓	✗	Apache Tomcat - CGI Servlet 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.

The screenshot shows a exploit database entry for a vulnerability in Apache Tomcat. The details are as follows:

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

Below the details, there are links for "Exploit" (with download and source options) and "Vulnerable App". Navigation arrows are present at the top right.

```
##  
# 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,  
      'Name' => 'Apache Tomcat CGIServlet enableCmdLineArguments Vulnerability',  
      'Description' => %q{  
        This module exploits a vulnerability in Apache Tomcat's CGIServlet component. When the  
      }  
    )  
  end  
  
  # exploit code goes here  
end
```

7. RUN A SCRIPT ENGINE

A.) TARGET - 192.168.5.135

B.) SCRIPT ENGINE NAME - nbstat.nse

The terminal window shows the output of an Nmap scan using the nbstat.nse script against the target host 192.168.5.135. The output includes a table of open ports and their corresponding services and versions.

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 2.2.18 ((Ubuntu) DAV/2) Files. For efficiency, scripts
111/tcp	open	rpcbind	2 (RPC #100000) longs.
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?	are Nmap scripts location Kali?
514/tcp	open	tcpwrapped	
1099/tcp	open	java-rmi	NmJava 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	How to Use VNC (protocol 3.3) e (NSE) Scripts in Linux - Tecmint
6000/tcp	open	X11	(access denied)

```
6000/tcp open  X11      (access denied)
6667/tcp open  irc      https://nmap.org/bundles/nse/
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

People also ask :
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>ripFlags:bn<group><active>
|   WORKGROUP<00>        Flags: <group><active>
|   WORKGROUP<1d>        Flags: <unique><active>
|_  WORKGROUP<1e>        Flags: <group><active>

Feedback
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-----

