Bypass SSH Restriction by Port Relay

posted in KALI LINUX , PENETRATION TESTING on MARCH 7, 2018 by RAJ CHANDEL

SHARE

Today we are going to access the ssh port which is blocked by the firewall and is forwarded to another port through Port relay tool. Netcat relay is quite useful tool to connect with any remote system by evading the firewall restriction.

Attacker: Kali Linux (IP: 192.168.1.2)

Victim: Ubuntu Server (IP: 192.168.1.7)

Connect to SSH via port 22

Lets first try to get the normal SSH shell. As you can see in the given screenshot we successfully get a ssh shell on the port 22 of the Server 192.168.1.7.

Command: ssh pavan@192.168.1.7

```
root@kali:~# ssh pavan@192.168.1.7
pavan@192.168.1.7's password:
Welcome to Ubuntu 17.10 (GNU/Linux 4.13.0-36-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage


0 packages can be updated.
0 updates are security updates.

*** System restart required ***
Last login: Sat Mar  3 09:46:37 2018 from 127.0.0.1
pavan@ubuntu:~$
```

Block Port 22 for Incoming TCP Packet

Now let's block SSH service Port 22 for Incoming TCP Packet using Iptables. Here we are making an inbound rule to block the tcp packets on the port 22 if the packet source is Kali (192.168.1.2)

Command: iptables –A INPUT –s 192.168.1.2 –p tcp –dport 22 –j DROP

```
root@ubuntu:~# iptables -A INPUT -s 192.168.1.2 -p tcp --dport 22 -j DROP
```

After Blocking the port let's try to get a shell. From given below image you can observe that we got a **Connection Time Out Error** as the packets are dropped by the firewall.

```
root@kali:~# ssh pavan@192.168.1.7
ssh: connect to host 192.168.1.7 port 22: Connection timed out
```

Allow TCP Packets on another port

Now let's make a rule in the firewall to accept the tcp packets on the port 4444 if the packet source is Kali (192.168.1.2).

Command: iptables –I INPUT 1 –s 192.168.1.2 –p tcp –dport 4444 –j ACCEPT

```
root@ubuntu:~# iptables -I INPUT 1 -s 192.168.1.2 -p tcp --dport 4444 -j ACCEPT
```

Check Netcat communication between Attacker and Client

Let's check if we can get a netcat session on the port 4444 to the Kali (192.168.1.2).

Command: nc –v –l –p 4444

```
root@ubuntu:~# nc -v -l -p 4444
Listening on [0.0.0.0] (family 0, port 4444)
Connection from 192.168.1.2 59660 received!
5
connection success
```

Command: nc 192.168.1.7 4444

As you can see in the given Image that we have received a netcat session on the port 4444 from SSH server on the Kali (192.168.1.2).

```
root@kali:~# nc 192.168.1.7 4444
5
connection success
^C
```

Use Netcat Relay backpipe to access SSH service

Now we will have to make a Relay. But first, let's understand, what the commands depicted below do?

Categories

- BackTrack 5 Tutorials
- Best of Hacking
- Browser Hacking
- Cryptography & Stegnography
- CTF Challenges
- Cyber Forensics
- Database Hacking
- Domain Hacking
- Email Hacking
- Footprinting
- Hacking Tools
- Kali Linux
- Nmap
- Others
- Penetration Testing
- Social Engineering Toolkit
- Trojans & Backdoors
- Website Hacking
- Window Password Hacking
- Windows Hacking Tricks
- Wireless Hacking
- Youtube Hacking

The First command makes a special type of file called a FIFO or **named pipe**. We call it backpipe because it is going to carry our responses back through the relay.

Now the second command makes a netcat listener that is allowed through the firewall. This Netcat listener will connect its standard input (0<) to the backpipe. We then forward the standard output of this Netcat listener to Netcat client, which connects to our localhost (127.0.0.1) on TCP port 22 where sshd listens. We then use the forward pipe (1>) to send data and receive responses simultaneously. We need a back and forward pipe because Netcat provides a two-way communication.

Command: mknod /tmp/backpipe p

[p]: Tells the mknod to create a FIFO

Command: nc –l –p 4444 0</tmp/backpipe | nc localhost 22 1>/tmp/backpipe

[-l]: Listener

[-p]: Port

```
root@ubuntu:~# mknod /tmp/backpipe p
root@ubuntu:~# nc -l -p 4444 0</tmp/backpipe | nc localhost 22 1>/tmp/backpipe
```

Access SSH through Netcat Relay

Now let's try to connect the ssh connection through the port 4444.

Command: ssh pavan@192.168.1.7 –p 4444

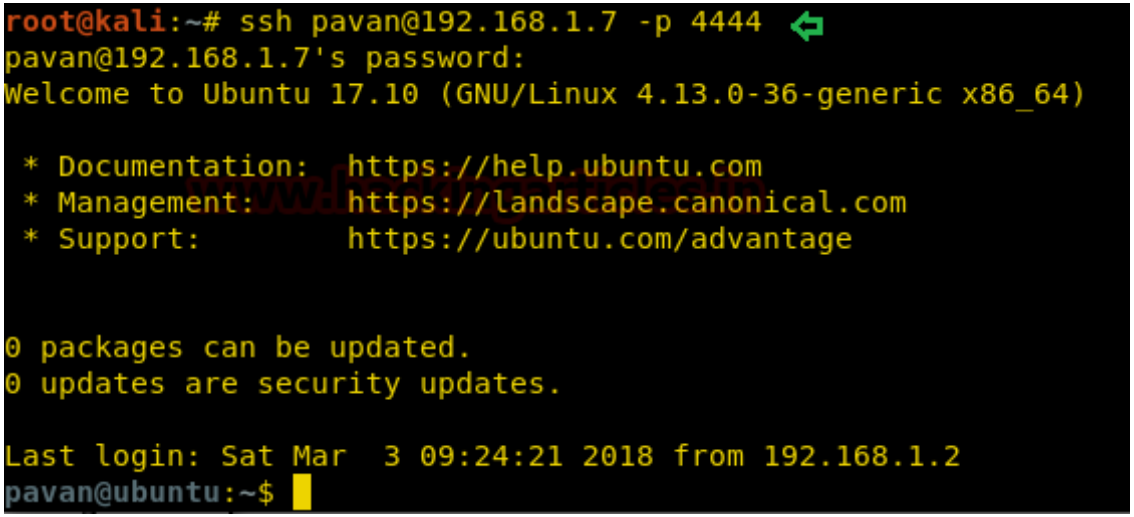
[-p]: To specify Port

Articles

Select Month

Facebook Page

Be the first of your friends to like this



Author: Pavandeep Singh is a Technical Writer, Researcher and Penetration Tester
Contact **here**

Share this:

Like this:

Loading...

ABOUT THE AUTHOR

RAJ CHANDEL

Raj Chandel is a Skilled and Passionate IT Professional especially in IT-Hacking Industry. At present other than his name he can also be called as An Ethical Hacker, A Cyber Security Expert, A Penetration Tester. With years of quality Experience in IT and software industry

PREVIOUS POST
← GENERATING SCAN REPORTS USING NMAP (OUTPUT SCAN)

NEXT POST
5 WAYS TO HACK MYSQL LOGIN PASSWORD →

Leave a Reply

Your email address will not be published. Required fields are marked *

Comment

Name *

Email *

Website

Save my name, email, and website in this browser for the next time I comment.

POST COMMENT

Notify me of follow-up comments by email.

Notify me of new posts by email.