

Forum:[Hack Forums](#)

Thread: [Find IP address via MAC address.](#)

hack3rcon - May 29, 2019, 12:57 am

Hello.

How can I find the IP address of a device in a local network by its MAC address? For example, I have a mobile MAC address and I want to find its IP.

Thank you.

Asdethprime - May 29, 2019, 1:03 am

Local IP address of the machine (for example 192.168.1.100) or like public IP where you can start sending message to the device?

If its the former, you can use various tools like aircrack-ng ; wireshark etc. All you get is a private IP that can ONLY be access from within the network (be it through a double hop - if you don't know what that is, you can ignore that for now).

If you are looking for a public IP address that you invoke from outside the network, than more than likely it does not exist. On most home network, if you take away smartphones (because sim card can actually provide a public ip) , normal computer do NOT have a public IP address.

When you go to google and type "what is my public address", the IP address you get back is NOT the IP address of your computer, but rather than IP address of your WIFI box.

You might wanna clear few things out on what exactly are you trying here?

hack3rcon - May 29, 2019, 2:52 am

Thank you.

In a local network, We have some mobiles that use WiFi for connect to the internet. I want to know, if I have a mobile MAC address then can I find its local IP address?

CyberStrike - May 29, 2019, 3:03 am

Negative the MAC address is not going to reveal the IP, a MAC address is basically individual to each card. At most you can get the manufacturer of the device perhaps have an idea of what kind of device it is.

Lante - May 29, 2019, 3:06 am

No one noticed he's asking for a local IP? If you're on the same LAN, just run an IP scan (eg. Advanced IP Scanner) and it will display the MAC address and IP address of every found device on the network.

Asdethprime - May 29, 2019, 4:12 am

(May 29, 2019 02:52 AM)hack3rcon Wrote: [\[CITE\]](#) Thank you.

In a local network, We have some mobiles that use WiFi for connect to the internet. I want to know, if I have a mobile MAC address then can I find its local IP address?

Oh just the local IP address, sure there are multiple way to get that.

The easiest would be to use arp -a command that would be the most specific.

If you can perform an arp spoofing to pretend to be the wifi box, you can directly run Wireshark and you can see both MAC and private IP address.

I am a bit keen to understand, why you are hunting for local IP ? Just curious to find out

CyberStrike - May 29, 2019, 4:57 am

Locally even the MAC address will not reveal the local IP, and that was the question. If OP doesn't know he needs to use nmap or scapy and wireshark to scan and analyze the results, then he is out of his league already.

cybermonkey2619 - May 29, 2019, 6:31 am

(May 29, 2019 12:57 AM)hack3rcon Wrote: [\[CITE\]](#) Hello.

How can I find the IP address of a device in a local network by its MAC address? For example, I have a mobile MAC address and I want to find its IP.

Thank you.

generally the mac id is from the manufacturer and the local ip can be set via 2 ways, dynamically when the device connects to a network configured with dhcp and so the device gets a pre assigned IP from the server and the 2nd way is to know the network details which you need to connect the device and configure manually with the local IP address given by the network administrator.

if its a win box u can run ipconfig and on a linux box u can run ifconfig and on a mobile device when you connect via wifi in that place u can see the assigned IP. hope this helps.

Asdethprime - May 29, 2019, 7:43 pm

(May 29, 2019 04:57 AM)CyberStrike Wrote: [\[CITE\]](#) Locally even the MAC address will not reveal the local IP, and that was the question. If OP doesn't know he needs to use nmap or scapy and wireshark to scan and analyze the results, then he is out of his league already.

A mapping of local IP and MAC address is always maintained on a local network in a table called ARP (Address resolution protocol).

You actually have 2 options to get this mapping:

1) you can use the reverse arp (arp -a) and send a message to anyone on the network saying 'Where is Mac 1:2:3:4 tell me '.

This is obviously just an example and the Mac is not even on the correct format but u get the message back saying hey I have this Mac and my IP address is this.

Alternatively, any device joined to the domain can broadcast an ARP query. In simple terms any device can send a network wide message saying

'Who has 192.168.1.2 , please tell 192.168.1.101'

you can keep repeating this till the correct device replies saying I have that IP.

Works either way way.

hack3rcon - May 31, 2019, 1:04 am

(May 29, 2019 04:12 AM)Asdethprime Wrote: [\[CITE\]](#) Oh just the local IP address, sure there are multiple ways to get that.

The easiest would be to use `arp -a` command that would be the most specific.

If you can perform an arp spoofing to pretend to be the wifi box, you can directly run Wireshark and you can see both MAC and private IP address.

I am a bit keen to understand, why you are hunting for local IP ? Just curious to find out I just want to find someone.

(May 29, 2019 07:43 PM)Asdethprime Wrote: [\[CITE\]](#) A mapping of local IP and MAC address is always maintained on a local network in a table called ARP (Address resolution protocol).

You actually have 2 options to get this mapping:

1) you can use the reverse arp (`arp -a`) and send a message to anyone on the networking saying 'Where is Mac 1:2:3:4 tell me '.

This is obviously just an example and the Mac is not even on the correct format but u get the message back saying hey I have this Mac and my IP address is this.

Alternatively, any device joined to the domain can broadcast an ARP query. In simple terms any device can send a network wide message saying

'Who has 192.168.1.2 , please tell 192.168.1.101'

you can keep repeating this till the correct device replies saying I have that IP.

Works either way way.

Can you show me an example in real world? I mean is commands.

Asdethprime - May 31, 2019, 1:31 am

(May 31, 2019 01:04 AM)hack3rcon Wrote: [\[CITE\]](#) I just want to find someone.

Can you show me an example in real world? I mean is commands.

`$ arp -a my:sexy:Mac:address`

The device needs to be connected to the network.

hack3rcon - May 31, 2019, 9:57 pm

(May 31, 2019 01:31 AM)Asdethprime Wrote: [\[CITE\]](#) `$ arp -a my:sexy:Mac:address`

The device needs to be connected to the network.

What is "my:sexy" ? If the MAC address is "00:0a:95:9d:68:16" then:

Code `$ arp -a my:sexy:00:0a:95:9d:68:16` Give me the IP address of the device?

Asdethprime - May 31, 2019, 10:10 pm

(May 31, 2019 09:57 PM)hack3rcon Wrote: [\[CITE\]](#) What is "my:sexy" ? If the MAC address is "00:0a:95:9d:68:16" then:

Code `$ arp -a my:sexy:00:0a:95:9d:68:16` Give me the IP address of the device?

`Arp -a 00:0a:95:9d:68:16`

That's all.

If the device is joined to the same network you will get the Ip address.

hack3rcon - June 1, 2019, 4:41 am

(May 31, 2019 10:10 PM)Asdethprime Wrote: [\[CITE\]](#) Arp -a 00:0a:95:9d:68:16

That's all.

If the device is joined to the same network you will get the Ip address.

How about VLAN? In a VLAN network, when I did that command it show me the switch MAC address and not device MAC address.

Asdethprime - June 1, 2019, 7:57 pm

(Jun 1, 2019 04:41 AM)hack3rcon Wrote: [\[CITE\]](#) How about VLAN? In a VLAN network, when I did that command it show me the switch MAC address and not device MAC address.

You are not on the same broadcast domain if the device is connected to another VLAN so arp won't work.

You need to first join that VLAN for u to access internal network information (and that to even be useful to you)

hack3rcon - June 1, 2019, 10:21 pm

(Jun 1, 2019 07:57 PM)Asdethprime Wrote: [\[CITE\]](#) You are not on the same broadcast domain if the device is connected to another VLAN so arp won't work.

You need to first join that VLAN for u to access internal network information (and that to even be useful to you)

I see.

How can I join to that VLAN? If I set another IP address in that range then?