

Forum:[Hack Forums](#)

Thread: [How to find an exact location of a device\(XYZ\)](#)

ATK0L - May 13, 2022, 7:52 am

Does anyone here know how to find a device's exact location (XYZ)(Not a domain a real location)(for educational purposes of course)?

CryptixHacking - May 13, 2022, 7:58 am

From IP "Internet Protocol" address alone ? No getting the external IP of the system is only going to give you the location of the internet service provider "ISP" of said system when doing a GEOIP lookup.

The ISP will have the address "real location" of its paid client getting the address of the system from them is a different story.

Give the system has GPS and GPS services enabled then it could be possible to then get a location of the device within 25 feet. But of course this would require the device has a GPS service and then you would then have to exploit the system to have it dump out its GPS location data to you.

ATK0L - May 13, 2022, 8:12 am

(May 13, 2022 07:58 AM)CryptixHacking Wrote: [\[CITE\]](#) From IP "Internet Protocol" address alone ? No getting the external IP of the system is only going to give you the location of the internet service provider "ISP" of said system.

The ISP will have the address "real location" of its paid client getting the address of the system from them is a different story.

Give the system has GPS and GPS services enabled then it could be possible to then get a location of the device within 25 feet. But of course this would require the device has a GPS service and then you would then have to exploit the system to have it dump out its GPS location data to you.

So I need to be at close range. But what if I put a file (a program or a virus) in the device that will turn on the GPS and send the location to me(I will need to think about how to do that part)? That could work, right?

But there is one more problem, I will need permission from the device so I could turn on the GPS. How can I get that permission?

By the way Thank you for your answer I really appreciate it

CryptixHacking - May 13, 2022, 8:23 am

No your range to the target device has nothing to do with what I said :P

Getting the IP of the system WILL NOT allow you to get the real location of the device only the location of its service provider. So you would then have to request the address of the client device from their ISP.

I guess your location could help if you were doing a ping hop test to triangulate the device but wouldnt work with external IP's so much.

Getting the "real" location of target device without going through IP/ISP could be possible give the device has GPS hardware and services enabled on device. But to then get the "exact/real" GPS location of device you would have to exploit the device to have it give you its GPS location.

Quote:But what if I put a file (a program or a virus) in the device that will turn on the GPS and send the location to me

Yes you are right to get the GPS of the device such a action like you stated would be required.

And yeah you are right if you did such a attack on a mobile device like android your file/app would require to have permission manifest that would allow your file/app to enable GPS on the device if its not enabled. You are right yes.

There are some exploits and ways to bypass this though can depend. I think the most common way of avoiding android app manifest permission request is to have your app use a binary file rather than java/C code from the app itself. Have the app open/run a compiled ARM binary file within the shell of the android system. Then have the ARM binary file do all the dirty background work. This way the app can enabled and turn on GPS without needing to use permission manifest.

ATK0L - May 13, 2022, 8:29 am

(May 13, 2022 08:23 AM)CryptixHacking Wrote: [\[CITE\]](#) No your range to the target device has nothing to do with what I said :P

Getting the IP of the system WILL NOT allow you to get the real location of the device only the location of its service provider. So you would then have to request the address of the client device from their ISP.

I guess your location could help if you were doing a ping hop test to triangulate the device but wouldnt work with external IP's so much.

Getting the "real" location of target device without going through IP/ISP could be possible give the device has GPS hardware and services enabled on device. But to then get the "exact/real" GPS location of device you would have to exploit the device to have it give you its GPS location.

Yes you are right to get the GPS of the device such a action like you stated would be required.

And yeah you are right if you did such a attack on a mobile device like android your file/app would require to have permission manifest that would allow your file/app to enable GPS on the device if its not enabled. You are right yes.

There are some exploits and ways to bypass this though can depend. I think the most common way of avoiding android app manifest permission request is to have your app use a binary file rather than java/C code from the app itself. Have the app open/run a compiled ARM binary file within the shell of the android system. Then have the ARM binary file do all the dirty background work. This way the app can enabled and turn on GPS without needing to use permission manifest.

Brilliant man, thank you again for your magnificent help!

