

Forum:[Hack Forums](#)

Thread: [What Does It Actually Mean to Scan a Public IP?](#)

APInoob42 - August 19, 2026, 4:59 pm

Hey everyone,

I've been learning cybersecurity for a while now and I'm pretty comfortable with tools like Nmap, Metasploit, and Wireshark. I also spend a lot of time doing Hack The Box labs and have learned quite a lot about networking, ports, services, routing, private IPs, NAT, etc.

One thing I still don't fully understand is what it actually means in practice to scan a public IP address.

For example, on a home network, multiple devices have private IP addresses such as 192.168.x.x or 10.x.x.x, but they can all appear on the Internet behind the same public IP because of the router/NAT.

So when someone runs something like an Nmap scan against a public IP:

What exactly are they scanning?

Are the open ports normally services running on the router itself, or can they represent devices behind the router because of port forwarding/NAT?

How does an attacker go from discovering an exposed service on a public IP to understanding which internal device is actually providing that service?

In real-world pentesting, how different is scanning a public-facing IP compared with scanning machines inside a LAN?

I understand the basic theory of NAT and port forwarding, but I'm trying to connect that theory to what actually happens during reconnaissance.

I'd also be interested in hearing hacking stories from people who have found interesting exposed services through public-IP reconnaissance. What did you discover, and what did the network topology look like behind that IP?

I'm mainly trying to understand the networking side better rather than just blindly running tools.

Thanks!

DramaKing - August 19, 2026, 6:26 pm

Using a typical home router with no forwarded ports as an example, there should be no open ports. If you want to go deeper, I recommend taking a networking course.

Bastille - August 20, 2026, 4:55 am

Quote:What exactly are they scanning?

When you scan public IP addresses you'll go through different ports (from 0 to 65 535) to find open ports and exposed servers / services (such as : websites, mail server, ftp server, VPN services, ...).

Quote:Are the open ports normally services running on the router itself, or can they represent

devices behind the router because of port forwarding/NAT?

It depends about the network configuration, and also if we're speaking about individuals or companies.

1. Individuals : you, me, have a router at home, and usually they run nothing on themselves, except if you configure some services. Some ISP can offer features to configure a VPN access to your home, things like that, and some routers from ISP can run VMs on themselves.
2. Companies : they usually work with a router AND a firewall, there is two type of configuration. Most of the time everything goes through the router, then the firewall allows or block, this is what we call a "transparent" or "bridge" configuration.

Then, 1 public port = 1 service, but this service can have many servers (exemple : if you're a big company and you host a website, you'll need more than 1 web server to run to handle the traffic), but on the WAN side the web site will always go through port 443 (HTTPS), and then the firewall / servers will redirect to different servers (this is a notion we call "load balancing").

Speaking about services running on routers themselves, a good example is firewalls with a VPN feature, for remote working. People work from home but need to access companies' servers and data, so they go through the firewall to access the internal network. The firewall is running a service (a VPN).

Quote: How does an attacker go from discovering an exposed service on a public IP to understanding which internal device is actually providing that service?

Once you've scanned the IP and got some open ports (reconnaissance) the next step is to get an entry point through :

- misconfiguration (SMB shares , no bruteforce protection, ...)
- default configuration (default passwords)
- outdated systems (old Fortigate running an old FortiOS version which is vulnerable : <https://www.cvedetails.com/version-list/0/6632/1/>)
- weak or compromised credentials

After getting an initial access you can then discover the internal network.

Aside of that, during the reconnaissance, sometimes you can get information about servers (misconfiguration, exposed information on github or inside the source code of a website, or hidden pages you've found through fuzzing, internal notes, and so on ...)

With nmap, you can try to get information about services and machines with parameters like -sV (version)

With other protocols, like telnet, you can also get banner information.

Quote: In real-world pentesting, how different is scanning a public-facing IP compared with scanning machines inside a LAN?

First of all, it's illegal.

Then, there are many protection features like honeypots, firewalls, IDS, IPS, SIEMs, rules, conditions, ... For example : if the IT did a good job, you shouldn't be able to access anything related to IT administration. A good example is the firewall administration page, even if the port is open, there should be a rule configured that allow only few and trusted IP addresses to access the admin dashboard, this is called whitelisting.

Other mechanisms are like blacklisting IP addresses. If the monitoring devices (SIEM, firewalls, IDS, ...) see someone querying every port of the IP address, this will be considered as malicious and will be blocked. This is why you have different aggressivity modes on nmap (from T0 to T5). Aside of aggressivity modes, hackers usually don't scan every port with 1 IP address, they use many IP addresses so you don't trigger alerts on the SIEM like "This IP scanned 100 ports, this is suspicious", instead you scan 5 ports and it might not trigger the alert.

Quote:I'd also be interested in hearing hacking stories from people who have found interesting exposed services through public-IP reconnaissance. What did you discover, and what did the network topology look like behind that IP?

Not allowed to brag about internet crimes : <https://hackforums.net/showthread.php?tid=5981318>
But you can find free report from authorities or cybersecurity companies about real-case scenarios, like :

- <https://thedfirreport.com/reports/>

I also recommend you this website to understand what methods attackers use :

<https://attack.mitre.org/matrices/enterprise/>

You can also find information about hacking software, hacking groups and hacking campaigns here :

- <https://attack.mitre.org/software/>

- <https://attack.mitre.org/groups/>

- <https://attack.mitre.org/campaigns/>

This matrice is very important by the way, this is all techniques and methods used :

<https://attack.mitre.org/matrices/enterprise/>

You have the equivalent from the defensive side : <https://d3fend.mitre.org/>

Finally, you never scan with your own IP address. Be aware that some VPN log their customer activity, if a company file a complaint the authority could ask the VPN provider the logs related to the malicious activity. Hackers usually go with no log VPNs, VPS, or proxies.

I hope it helped, feel free to ask if you have any question. If you want to practice on your side you can, just get some firewall VMs or physical appliances (Fortigate, pfSense, OPNsense, D-link, or whatever), and then configure services and try to hack them from your internal network. The difference with real-case scenarios will only be the IP address that will be private instead of public.

DramaKing - August 20, 2026, 7:06 am

One small addition: If a user behind a router with PAT and UPNP-enabled uses an application with UPNP, it could open a port on the router. There's also IPv6 GUA addresses, which have no need of NAT/PAT. Firewall rules are the only things blocking inbound connections. I have a printer with a printer port allowed through the firewall. It doesn't wake from standby over the network, and few hackers care about printers I imagine, so I don't really worry about it.

APInoob42 - August 23, 2026, 2:56 am

Thanks y'all for replying, it helped a lot!