Host Discovery

One of the very first steps in any network reconnaissance mission is to reduce a (sometimes huge) set of IP ranges into a list of active or interesting hosts. Scanning every port of every single IP address is slow and usually unnecessary. Of course what makes a host interesting depends greatly on the scan purposes. Network administrators may only be interested in hosts running a certain service, while security auditors may care about every single device with an IP address. An administrator may be comfortable using just an ICMP ping to locate hosts on his internal network, while an external penetration tester may use a diverse set of dozens of probes in an attempt to evade firewall restrictions.

Because host discovery needs are so diverse, Nmap offers a wide variety of options for customizing the techniques used. Host discovery is sometimes called ping scan, but it goes well beyond the simple ICMP echo request packets associated with the ubiquitous ping tool. Users can skip the discovery step entirely with a list scan (`-sL`) or by disabling host discovery (`-Pn`), or engage the network with arbitrary combinations of multi-port TCP SYN/ACK, UDP, SCTP INIT and ICMP probes. The goal of these probes is to solicit responses which demonstrate that an IP address is actually active (is being used by a host or network device). On many networks, only a small percentage of IP addresses are active at any given time. This is particularly common with private address space such as 10.0.0.0/8. That network has 16 million IPs, but I have seen it used by companies with less than a thousand machines. Host discovery can find those machines in a sparsely allocated sea of IP addresses.

If no host discovery options are given, Nmap sends an ICMP echo request, a TCP SYN packet to port 443, a TCP ACK packet to port 80, and an ICMP timestamp request. (For IPv6, the ICMP timestamp request is omitted because it is not part of ICMPv6.) These defaults are equivalent to the `-PE -PS443 -PA80 -PP` options. The exceptions to this are the ARP (for IPv4) and Neighbor Discovery (for IPv6) scans which are used for any targets on a local ethernet network. For unprivileged Unix shell users, the default probes are a SYN packet to ports 80 and 443 using the `connect` system call. This host discovery is often sufficient when scanning local networks, but a more comprehensive set of discovery probes is recommended for security auditing.

The `-P*` options (which select ping types) can be combined. You can increase your odds of penetrating strict firewalls by sending many probe types using different TCP ports/flags and ICMP codes. Also note that ARP/Neighbor Discovery is done by default against targets on a local Ethernet network even if you specify other `-P*` options, because it is almost always faster and more effective.

By default, Nmap does host discovery and then performs a port scan against each host it determines is online. This is true even if you specify non-default host discovery types such as UDP probes (`-PU`). Read about the `-sn` option to learn how to perform only host discovery, or use `-Pn` to skip host discovery and port scan all target addresses. The following options control host discovery:

`-sL` (List Scan)

> The list scan is a degenerate form of host discovery that simply lists each host of the network(s) specified, without sending any packets to the target hosts. By default, Nmap still does reverse-DNS resolution on the hosts to learn their names. It is often surprising how much useful information

simple hostnames give out. For example, `fw.chi` is the name of one company's Chicago firewall. Nmap also reports the total number of IP addresses at the end. The list scan is a good sanity check to ensure that you have proper IP addresses for your targets. If the hosts sport domain names you do not recognize, it is worth investigating further to prevent scanning the wrong company's network.

Since the idea is to simply print a list of target hosts, options for higher level functionality such as port scanning, OS detection, or host discovery cannot be combined with this. If you wish to disable host discovery while still performing such higher level functionality, read up on the `-Pn` (skip host discovery) option.

`-sn` (No port scan)

This option tells Nmap not to do a port scan after host discovery, and only print out the available hosts that responded to the host discovery probes. This is often known as a "ping scan", but you can also request that traceroute and NSE host scripts be run. This is by default one step more intrusive than the list scan, and can often be used for the same purposes. It allows light reconnaissance of a target network without attracting much attention. Knowing how many hosts are up is more valuable to attackers than the list provided by list scan of every single IP and host name.

Systems administrators often find this option valuable as well. It can easily be used to count available machines on a network or monitor server availability. This is often called a ping sweep, and is more reliable than pinging the broadcast address because many hosts do not reply to broadcast queries.

The default host discovery done with `-sn` consists of an ICMP echo request, TCP SYN to port 443, TCP ACK to port 80, and an ICMP timestamp request by default. When executed by an unprivileged user, only SYN packets are sent (using a `connect` call) to ports 80 and 443 on the target. When a privileged user tries to scan targets on a local ethernet network, ARP requests are used unless `--send-ip` was specified. The `-sn` option can be combined with any of the discovery probe types (the `-P*` options) for greater flexibility. If any of those probe type and port number options are used, the default probes are overridden. When strict firewalls are in place between the source host running Nmap and the target network, using those advanced techniques is recommended. Otherwise hosts could be missed when the firewall drops probes or their responses.

In previous releases of Nmap, `-sn` was known as `-sP`.

`-Pn` (No ping)

This option skips the host discovery stage altogether. Normally, Nmap uses this stage to determine active machines for heavier scanning and to gauge the speed of the network. By default, Nmap only performs heavy probing such as port scans, version detection, or OS detection against hosts that are found to be up. Disabling host discovery with `-Pn` causes Nmap to attempt the requested scanning functions against *every* target IP address specified. So if a /16 sized network is specified on the command line, all 65,536 IP addresses are scanned. Proper host discovery is skipped as with the list scan, but instead of stopping and printing the target list, Nmap continues to perform requested functions as if each target IP is active. Default timing parameters are used, which may result in slower scans. To skip host discovery *and* port scan, while still allowing NSE to run, use the two options `-Pn -sn` together.

For machines on a local ethernet network, ARP scanning will still be performed (unless `--disable-arp-ping` or `--send-ip` is specified) because Nmap needs MAC addresses to further scan target hosts. In previous versions of Nmap, `-Pn` was `-P0` and `-PN`.

`-PS <port list>` (TCP SYN Ping)

This option sends an empty TCP packet with the SYN flag set. The default destination port is 80 (configurable at compile time by changing `DEFAULT_TCP_PROBE_PORT_SPEC` in `nmap.h`). Alternate ports can be specified as a parameter. The syntax is the same as for the `-p` except that port type specifiers like `T:` are not allowed. Examples are `-PS22` and `-PS22-25,80,113,1050,35000`. Note

that there can be no space between `-PS` and the port list. If multiple probes are specified they will be sent in parallel.

The SYN flag suggests to the remote system that you are attempting to establish a connection. Normally the destination port will be closed, and a RST (reset) packet sent back. If the port happens to be open, the target will take the second step of a TCP three-way-handshake by responding with a SYN/ACK TCP packet. The machine running Nmap then tears down the nascent connection by responding with a RST rather than sending an ACK packet which would complete the three-way-handshake and establish a full connection. The RST packet is sent by the kernel of the machine running Nmap in response to the unexpected SYN/ACK, not by Nmap itself.

Nmap does not care whether the port is open or closed. Either the RST or SYN/ACK response discussed previously tell Nmap that the host is available and responsive.

On Unix boxes, only the privileged user `root` is generally able to send and receive raw TCP packets. For unprivileged users, a workaround is automatically employed whereby the `connect` system call is initiated against each target port. This has the effect of sending a SYN packet to the target host, in an attempt to establish a connection. If `connect` returns with a quick success or an ECONNREFUSED failure, the underlying TCP stack must have received a SYN/ACK or RST and the host is marked available. If the connection attempt is left hanging until a timeout is reached, the host is marked as down.

`-PA <port list>` (TCP ACK Ping)

The TCP ACK ping is quite similar to the just-discussed SYN ping. The difference, as you could likely guess, is that the TCP ACK flag is set instead of the SYN flag. Such an ACK packet purports to be acknowledging data over an established TCP connection, but no such connection exists. So remote hosts should always respond with a RST packet, disclosing their existence in the process.

The `-PA` option uses the same default port as the SYN probe (80) and can also take a list of destination ports in the same format. If an unprivileged user tries this, the `connect` workaround discussed previously is used. This workaround is imperfect because `connect` is actually sending a SYN packet rather than an ACK.

The reason for offering both SYN and ACK ping probes is to maximize the chances of bypassing firewalls. Many administrators configure routers and other simple firewalls to block incoming SYN packets except for those destined for public services like the company web site or mail server. This prevents other incoming connections to the organization, while allowing users to make unobstructed outgoing connections to the Internet. This non-stateful approach takes up few resources on the firewall/router and is widely supported by hardware and software filters. The Linux Netfilter/iptables firewall software offers the `--syn` convenience option to implement this stateless approach. When stateless firewall rules such as this are in place, SYN ping probes (`-PS`) are likely to be blocked when sent to closed target ports. In such cases, the ACK probe shines as it cuts right through these rules.

Another common type of firewall uses stateful rules that drop unexpected packets. This feature was initially found mostly on high-end firewalls, though it has become much more common over the years. The Linux Netfilter/iptables system supports this through the `--state` option, which categorizes packets based on connection state. A SYN probe is more likely to work against such a system, as unexpected ACK packets are generally recognized as bogus and dropped. A solution to this quandary is to send both SYN and ACK probes by specifying `-PS` and `-PA`.

`-PU <port list>` (UDP Ping)

Another host discovery option is the UDP ping, which sends a UDP packet to the given ports. For most ports, the packet will be empty, though some use a protocol-specific payload that is more likely to elicit a response. The payloads are the same probes used in service and version detection and are defined in the `nmap-service-probes` file. Packet content can also be affected with the `--data`, `--data-string`, and `--data-length` options.

The port list takes the same format as with the previously discussed `-PS` and `-PA` options. If no ports are specified, the default is 40125. This default can be configured at compile-time by changing `DEFAULT_UDP_PROBE_PORT_SPEC` in `nmap.h`. A highly uncommon port is used by default because sending to open ports is often undesirable for this particular scan type.

Upon hitting a closed port on the target machine, the UDP probe should elicit an ICMP port unreachable packet in return. This signifies to Nmap that the machine is up and available. Many other types of ICMP errors, such as host/network unreachables or TTL exceeded are indicative of a down or unreachable host. A lack of response is also interpreted this way. If an open port is reached, most services simply ignore the empty packet and fail to return any response. This is why the default probe port is 40125, which is highly unlikely to be in use. A few services, such as the Character Generator (chargen) protocol, will respond to an empty UDP packet, and thus disclose to Nmap that the machine is available.

The primary advantage of this scan type is that it bypasses firewalls and filters that only screen TCP. For example, I once owned a Linksys BEFW11S4 wireless broadband router. The external interface of this device filtered all TCP ports by default, but UDP probes would still elicit port unreachable messages and thus give away the device.

`-PY <port list>` (SCTP INIT Ping)

This option sends an SCTP packet containing a minimal INIT chunk. The default destination port is 80 (configurable at compile time by changing `DEFAULT_SCTP_PROBE_PORT_SPEC` in `nmap.h`). Alternate ports can be specified as a parameter. The syntax is the same as for the `-p` except that port type specifiers like `S:` are not allowed. Examples are `-PY22` and `-PY22,80,179,5060`. Note that there can be no space between `-PY` and the port list. If multiple probes are specified they will be sent in parallel.

The INIT chunk suggests to the remote system that you are attempting to establish an association. Normally the destination port will be closed, and an ABORT chunk will be sent back. If the port happens to be open, the target will take the second step of an SCTP four-way-handshake by responding with an INIT-ACK chunk. If the machine running Nmap has a functional SCTP stack, then it tears down the nascent association by responding with an ABORT chunk rather than sending a COOKIE-ECHO chunk which would be the next step in the four-way-handshake. The ABORT packet is sent by the kernel of the machine running Nmap in response to the unexpected INIT-ACK, not by Nmap itself.

Nmap does not care whether the port is open or closed. Either the ABORT or INIT-ACK response discussed previously tell Nmap that the host is available and responsive.

On Unix boxes, only the privileged user `root` is generally able to send and receive raw SCTP packets. Using SCTP INIT Pings is currently not possible for unprivileged users.

`-PE`; `-PP`; `-PM` (ICMP Ping Types)

In addition to the unusual TCP, UDP and SCTP host discovery types discussed previously, Nmap can send the standard packets sent by the ubiquitous ping program. Nmap sends an ICMP type 8 (echo request) packet to the target IP addresses, expecting a type 0 (echo reply) in return from available hosts. Unfortunately for network explorers, many hosts and firewalls now block these packets, rather than responding as required by RFC 1122. For this reason, ICMP-only scans are rarely reliable enough against unknown targets over the Internet. But for system administrators monitoring an internal network, they can be a practical and efficient approach. Use the `-PE` option to enable this echo request behavior.

While echo request is the standard ICMP ping query, Nmap does not stop there. The ICMP standards (RFC 792 and RFC 950) also specify timestamp request, information request, and address mask request packets as codes 13, 15, and 17, respectively. While the ostensible purpose for these queries is to learn information such as address masks and current times, they can easily be used for host discovery. A system that replies is up and available. Nmap does not currently implement information request packets, as they are not widely supported. RFC 1122 insists that “a host SHOULD NOT

implement these messages". Timestamp and address mask queries can be sent with the `-PP` and `-PM` options, respectively. A timestamp reply (ICMP code 14) or address mask reply (code 18) discloses that the host is available. These two queries can be valuable when administrators specifically block echo request packets while forgetting that other ICMP queries can be used for the same purpose.

`-PO <protocol list>` (IP Protocol Ping)

One of the newer host discovery options is the IP protocol ping, which sends IP packets with the specified protocol number set in their IP header. The protocol list takes the same format as do port lists in the previously discussed TCP, UDP and SCTP host discovery options. If no protocols are specified, the default is to send multiple IP packets for ICMP (protocol 1), IGMP (protocol 2), and IP-in-IP (protocol 4). The default protocols can be configured at compile-time by changing `DEFAULT_PROTO_PROBE_PORT_SPEC` in `nmap.h`. Note that for the ICMP, IGMP, TCP (protocol 6), UDP (protocol 17) and SCTP (protocol 132), the packets are sent with the proper protocol headers while other protocols are sent with no additional data beyond the IP header (unless any of `--data`, `--data-string`, or `--data-length` options are specified).

This host discovery method looks for either responses using the same protocol as a probe, or ICMP protocol unreachable messages which signify that the given protocol isn't supported on the destination host. Either type of response signifies that the target host is alive.

`--disable-arp-ping` (No ARP or ND Ping)

Nmap normally does ARP or IPv6 Neighbor Discovery (ND) discovery of locally connected ethernet hosts, even if other host discovery options such as `-Pn` or `-PE` are used. To disable this implicit behavior, use the `--disable-arp-ping` option.

The default behavior is normally faster, but this option is useful on networks using proxy ARP, in which a router speculatively replies to all ARP requests, making every target appear to be up according to ARP scan.

`--discovery-ignore-rst`

In some cases, firewalls may spoof TCP reset (RST) replies in response to probes to unoccupied or disallowed addresses. Since Nmap ordinarily considers RST replies to be proof that the target is up, this can lead to wasted time scanning targets that aren't there. Using the `--discovery-ignore-rst` will prevent Nmap from considering these replies during host discovery. You may need to select extra host discovery options to ensure you don't miss targets in this case.

`--traceroute` (Trace path to host)

Traceroutes are performed post-scan using information from the scan results to determine the port and protocol most likely to reach the target. It works with all scan types except connect scans (`-sT`) and idle scans (`-sI`). All traces use Nmap's dynamic timing model and are performed in parallel.

Traceroute works by sending packets with a low TTL (time-to-live) in an attempt to elicit ICMP Time Exceeded messages from intermediate hops between the scanner and the target host. Standard traceroute implementations start with a TTL of 1 and increment the TTL until the destination host is reached. Nmap's traceroute starts with a high TTL and then decrements the TTL until it reaches zero. Doing it backwards lets Nmap employ clever caching algorithms to speed up traces over multiple hosts. On average Nmap sends 5–10 fewer packets per host, depending on network conditions. If a single subnet is being scanned (i.e. 192.168.0.0/24) Nmap may only have to send two packets to most hosts.