

Using Nessus For Host Discovery

◀ Previous Post

If an exploit falls in the forest,
does anyone hear it being
patched?

[Blog Home](#)

Next Post ▶

[Tenable Network Security
Podcast - Episode 62](#)



By [Paul Asadoorian](#) on December 9th, 2010

 TWEET

 SHARE

 SHARE

A

Nessus user recently contacted me about performing a scan that would simply discover hosts on the network. This is a very low impact scan that does not look for vulnerabilities or enumerate ports. There are a few good reasons to run this type of scan:

Systems protected by a network or host-based firewall may only respond on a single port or to an ICMP echo request. Hosts that only respond to an ICMP ping will not show up in the default Nessus scan report. By enumerating these hosts you can include them in the report to show that scans were attempted but did not find any results, then determine if this is normal behavior or not.

Your internal policies may provide specific time windows when vulnerability scanning can occur. By tuning a scan that only discovers live hosts, you can check that your Nessus server is set up properly, collect a list of hosts to scan and stay within your vulnerability scanning policy guidelines.

To configure a scan that will only test if hosts are alive, use the following policy settings:

The screenshot shows the Nessus policy configuration interface for a policy named 'Host Discovery'. The interface is divided into several sections:

- Basic:** Name is 'Host Discovery', Visibility is 'Private', and Description is empty.
- Scan:** A list of checkboxes for scan options:
 - Save Knowledge Base: ☐
 - Safe Checks: ☐
 - Silent Dependencies: ☒
 - Log Scan Details to Server: ☐
 - Stop Host Scan on Disconnect: ☐
 - Avoid Sequential Scans: ☐
 - Consider Unscanned Ports as Closed: ☐
 - Designate Hosts by their DNS Name: ☒
- Network Congestion:**
 - Reduce Parallel Connections on Congestion: ☐
 - Use Kernel Congestion Detection (Linux Only): ☐
- Port Scanners:**
 - TCP Scan: ☐
 - SNMP Scan: ☐
 - Ping Host: ☒
 - UDP Scan: ☐
 - Netstat SSH Scan: ☐
 - SYN Scan: ☐
 - Netstat WMI Scan: ☐
- Port Scan Options:** Port Scan Range is set to 'default'.
- Performance:**
 - Max Checks Per Host: 5
 - Max Hosts Per Scan: 80
 - Network Receive Timeout (seconds): 5
 - Max Simultaneous TCP Sessions Per Host: unlimited
 - Max Simultaneous TCP Sessions Per Scan: unlimited

Click for larger image

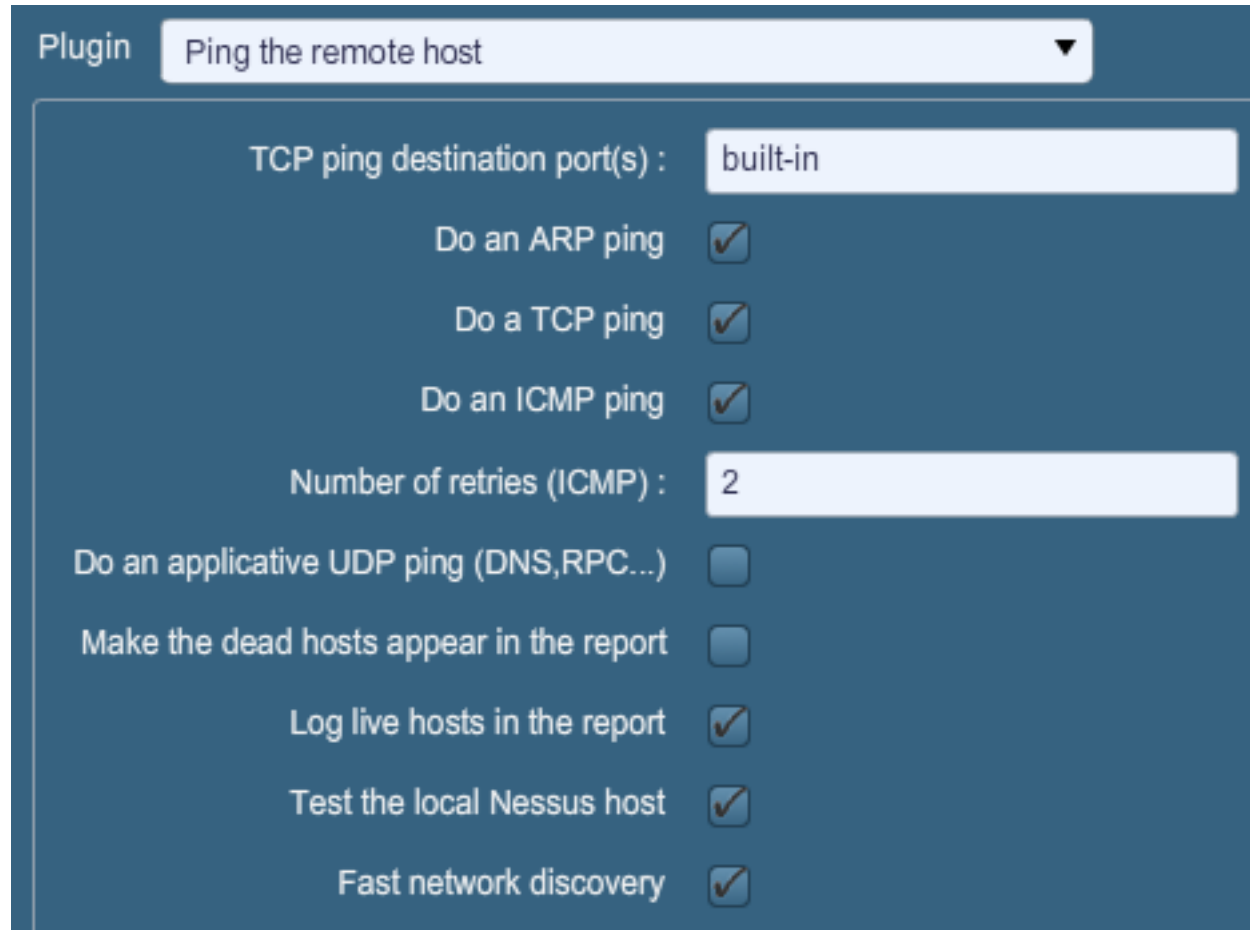
In the main policy configuration screen above the only setting in the "Port scanners" section enabled is "Ping host", which tells Nessus not to portscan the target hosts but only send packets that will test if the hosts are alive or not. I've also increased the "Max checks per host" setting from the default of 40 to 80. Since we are only performing tests to check if a host is alive, scanning more hosts per scan will make the scan run much faster with little impact on the network or local Nessus scanner machine.



Click for larger image

All plugins can be disabled in the plugins section. This may seem odd at first, but the "Ping host" checkbox in the first configuration screen will take care of host discovery without any plugins being enabled. You could easily extend this scan to perform operating system identification by enabling the appropriate plugins, but be cautioned that this will trigger several more checks and increase your scan time as well as send

more invasive scans to each host.



The image shows a configuration window for the 'Ping the remote host' plugin in Nessus. The window has a dark blue header with the text 'Plugin' and a dropdown menu showing 'Ping the remote host'. Below the header, there are several settings:

- 'TCP ping destination port(s) :' with a text input field containing 'built-in'.
- 'Do an ARP ping' with a checked checkbox.
- 'Do a TCP ping' with a checked checkbox.
- 'Do an ICMP ping' with a checked checkbox.
- 'Number of retries (ICMP) :' with a text input field containing '2'.
- 'Do an applicative UDP ping (DNS,RPC...)' with an unchecked checkbox.
- 'Make the dead hosts appear in the report' with an unchecked checkbox.
- 'Log live hosts in the report' with a checked checkbox.
- 'Test the local Nessus host' with a checked checkbox.
- 'Fast network discovery' with a checked checkbox.

In the preferences tab under "Ping the remote host", you can tune the host discovery settings. I've checked "Log live hosts in the report", which causes Nessus to report on hosts that respond to a discovery ping, which is not the default behavior. I've also enabled "Fast network discovery", which disabled some of the more advanced features of host discovery, such as proxy server detection.

Processing the results

This is a great scan to run on a regular basis on your network to discover new hosts (and if you enable operating system detection, will tell you the type of hosts appearing on the network). If you are a penetration tester, you may also wish to export the IP addresses to a file for processing by other tools, or even quickly see which type of host discovery test was successful. By exporting the data to an NBE (download the report and save as an NBE file from within the Nessus GUI) file, I came up with two quick Linux (or other UNIX compatible shell) command line tricks to extract this information:

The following command will extract the IP address and the method of discovery:

```
$ awk -F "|" '/10180/ {print $2 $7}'
HostDiscoveryResults.nbe | sed -e 's/Synopsis//' | cut -d:
-f1,7 | sed -e 's/\\n/ /g'
xbox-basement.myinternaldomain.com : The remote host is up
The remote host replied to an ICMP echo packet
madmonk.myinternaldomain.com : The remote host is up The
remote host emitted a UDP packet from port 53 going to port
33609
linky.myinternaldomain.com : The remote host is up The
remote host replied to an ICMP echo packet
johnnymo.myinternaldomain.com : The remote host is up The
remote host replied to an ICMP echo packet
```

```
hanzo.myinternaldomain.com : The remote host is up The
remote host replied to an ICMP echo packet
gogo.myinternaldomain.com : The remote host is up The host
is the local scanner.
192.168.1.81 : The remote host is up The remote host
replied to an ICMP echo packet
192.168.1.79 : The remote host is up The remote host
replied to an ICMP echo packet
```

The following command will extract just the IP addresses:

```
$ awk -F "|" ' /10180/ {print $2 }' HostDiscoveryResults.nbe
xbox-basement.myinternaldomain.com
madmonk.myinternaldomain.com
linky.myinternaldomain.com
johnnymo.myinternaldomain.com
hanzo.myinternaldomain.com
gogo.myinternaldomain.com
192.168.1.81
192.168.1.79
```

The nice part about the commands above, is that you can run this against any Nessus scan result file that you've enabled "Ping host" for and it will extract the live host information. This is done with the parameter sent to awk of "/10180/", which is the plugin ID associated with this option. Keep in mind you will be missing the hosts that only responded to host discovery unless you enable the option "Log live hosts in the report".

Conclusion

Knowing what's on your network is extremely important. If you don't know what is on your network, how do you know what needs to be managed, secured or monitored? The data can be used in all sorts of meaningful ways, such as tracking growth on the network or discovering hosts being plugged into the network that need to be scanned later. This is a great use of the new scan scheduling feature of Nessus, or an additional scan in your SecurityCenter. Finally, you may also want to read the post titled, [Scanning Large Networks with Nessus](#), which also contains some tips useful for customizing Nessus scans in this way.

Filed Under: [Nessus](#),

 TWEET

 SHARE

 SHARE

[◀ Previous Post](#)

[If an exploit falls in the forest,
does anyone hear it being
patched?](#)

[Blog Home](#)

[Next Post ▶](#)

[Tenable Network Security
Podcast - Episode 62](#)

More from the Tenable Blog

Enabling Actionable with SecurityCenter Continuous

Tenable Announces the
Industry's First Assurance
Report Cards in
SecurityCenter 5

By [Narayan Makaram](#) on April 14, 2015

View™

By [Manish Patel](#) on July 16, 2015

Attribution is Hard, Part 2

By [Marcus J. Ranum](#) on January 20, 2015

Products

- [Product Overview](#)
- [SecurityCenter Continuous View](#)
- [SecurityCenter](#)
- [Nessus Cloud](#)
- [Nessus Manager](#)
- [Nessus Professional](#)
- [Passive Vulnerability Scanner](#)

Product Resources

- [Integrations](#)
- [SecurityCenter Dashboards](#)
- [SecurityCenter Report Templates](#)
- [Assurance Report Cards](#)
- [Nessus Download](#)
- [Nessus Report Templates](#)

Support

- [Support Portal](#)
- [Professional Services](#)
- [Tenable Discussions Forum](#)
- [Nessus Documentation](#)
- [Nessus FAQ](#)
- [System Status](#)
- [Security Advisories](#)

Customer Education

- [Overview](#)
- [Free On-Demand Training](#)
- [Instructor-Led Training](#)

[Configuration Audits](#)

[LCE Plugins](#)

[Nessus Plugins](#)

[PVS Plugins](#)

Partners

[Partner Overview](#)

[Become a Partner](#)

[Resellers](#)

[Partner Login](#)

[Find an Alliance Partner](#)

Solutions

[Education](#)

[Finance](#)

[Government](#)

[Healthcare](#)

[PCI](#)

[Energy](#)

Resources

[Resource Library](#)

[Case Studies](#)

[Whitepapers](#)

About

[About Tenable](#)

[Leadership](#)

[Board of Directors](#)

[Awards & Certifications](#)

[Careers](#)

[Other](#)

News & Events

[Media Room](#)

[Blog](#)

[Webinars](#)

[Events/Conferences](#)

[Recruiting Events](#)

[RSS Feeds](#)

[Newsletter Signup](#)

Contact

[Contact Us](#)

