

New Discovery Options

Introduction

As at Open-Audit 2.3.2 and later, we have introduced some easy to use and extremely powerful options for discovering devices. These options centre around directing Nmap on *how* to discover devices.

We have grouped these options into what we're calling Discovery Scan Options. We ship seven different groups of options (items) by default that cover the common use-cases.

This benefits Community, Professional and Enterprise customers.

Feature Availability

Feature availability is dependent on license type as per the table below.

Feature	Community	Professional	Enterprise
Match Rules - set default for all discoveries	y	y	y
Discovery Scan Options - set default for all discoveries	y	y	y
Discovery Scan Options - read		y	y
Discovery Scan Options - set per discovery		y	y
Discovery Scan Options - create, read, update, delete			y
Discovery Scan Options - Custom per Discovery			y
Discovery Scan Options - Exclude IP, range, subnet per discovery			y
Discovery Scan Options - Exclude ports per discovery			y
Discovery Scan Options - Set device timeout, per discovery			y
Discovery Scan Options - Custom SSH port per discovery			y
Match Rules - set per discovery			y

Discovery Scan Types

The Discovery Scan Options we ship are detailed in the table below. As above, Enterprise users can create more of these or edit the shipped items.

Attribute	UltraFast	SuperFast	Fast	Medium (Classic) ¹	Medium	Slow	UltraSlow
<i>Approximate</i> time in seconds for remote IP scan	1	5	40	90	100	240	1200
Must Respond to Ping	y	y	y	n	y	y	n
Use Service Version Detection	n	n	n	n	n	y	y
Consider Filtered Ports as Open	n	n	n	y	n	y	y
Timing	T4	T4	T4	T4	T4	T3	T2
Top Nmap TCP Ports		10	100	1000	1000	1000	1000
Top Nmap UDP Ports		10	100		100	100	1000
Custom TCP Ports	22,135,62078	62078	62078	62078	62078	62078	62078
Custom UDP Ports	161			161			
Exclude TCP Ports							
Exclude UDP Ports							
Timeout per Host							
Exclude IP (address, range, subnet)							
Custom SSH Port							

¹The item for Medium (Classic) is similar to the Nmap for Discovery setting available in Open-Audit 2.3.2.

Check the wiki here for a deeper look at [Discovery Scan Options](#).

Example Scanning Improvement

We have a customer who is running discovery on a /22. The scan time to complete when using the original (hard set) options, prior to 2.3.2 was 29 hours. Using 2.3.2's UltraFast option, that scan now takes less than 10 minutes. To say they are impressed would be an understatement! They are now left with a smaller set of unknown devices that they can run a more detailed audit against. And remember, if the audited device is a computer, you will have a list of open ports derived from Netstat, anyway - possibly saving another audit cycle.

Use Cases

Handling Duplicate Serials

Recently we had cause to scan a subnet that was made up of virtual Cisco networking devices. These devices all happened to have identical serial numbers. Using the Match Rules per Discovery (available to Enterprise users) we were able to tweak the ruleset for this discovery only, without affecting other discoveries that rely upon matching a serial number. This ability solved a long-standing issue of working around a less than ideal setup on a network. A serial number, by definition, should be unique.

Filtered Ports

Networks respond differently depending on how they're configured. Some routers and/or firewalls can respond "on behalf" of IPs on the other side of their interfaces to the Open-Audit Server. It is quite common to see Nmap report a probe for SNMP (UDP port 161) to respond as open|filtered for devices that do and do not exist. This is misleading as there is no device at that IP, yet it ends up with a device entry in the database. 99.9% of the time, it is not Open-Audit, nor even Nmap, but the network causing this issue. Now that we have the options to treat open|filtered ports as either open or closed, we can eliminate a lot of this confusion. Enterprise users even have the option to change this on a per discovery basis (more than just using the Medium (Classic) item, as above).

Discovery Enterprise Options

The screenshot below is the Open-Audit discovery page where all the audit configuration is set. I've added ample notes in the page explaining all the options making the tool easy to use for less technical staff.

[Click to enlarge.](#)

Open-AuditIT Enterprise 2.3.2ViewDiscoverReportManageAdminHelpModulesLicensesUser: adminDashboards

Discoveries

NameMy Discovery Name?

Subnet192.168.1.0/24?

Network Addresshttp://127.0.0.1/open-audit/?

SubmitBasic

General Options

OrganisationDefault Organisation?

TypeSubnet?

Devices Assigned to Org?

Devices Assigned to Location?

Nmap Discovery Options

Discovery OptionsUltraFast?

Resulting Nmap Command(s)

```
nmap -n -T4 -sS -p 22,135,62078 (ip)
nmap -n -T4 -sU -p 161 (ip)
```

Must Respond to PingYes?

Use Service Version DetectionNo?

Consider Filtered Ports OpenNo?

TimingAggressive?

Top Nmap TCP PortsNone?

Top Nmap UDP PortsNone?

Custom TCP Ports22,135,62078?

Custom UDP Ports161?

The below attributes of timeout, excluding TCP, UDP & IPs and ssh port detection can be set below and will overwrite the given Discovery Scan Option.

Timeout Per Target (Seconds)?

Exclude TCP Ports?

Exclude UDP Ports?

Exclude IP Addresses?

SSH Running on Ports22?

Device Matching Rules

Match DbusYes?

Match FGDNYes?

Match HostnameYes?

Match Hostname DbusYes?

Match Hostname SerialYes?

Match Hostname UuidYes?

Match IPYes?

Match MacYes?

Match Mac VmwareNo?

Match SerialYes?

Match Serial TypeYes?

Match UuidYes?

About

Discoveries are at the very heart of what Open-AuditIT does.

How else would you know "What is on my network?"

Discoveries are preprepared data items that enable you to run a discovery upon a network in a single click, without entering the details of that network each and every time.

For more detailed information, check the Open-AuditIT Knowledge Base.

Notes

Some examples of valid Subnet attributes are: 192.168.1.1 (a single IP address), 192.168.1.0/24 (a subnet), 192.168.1-3.1-20 (a range of IP addresses).

NOTE - Only a subnet (as per the examples - 192.168.1.0/24) will be able to automatically create a valid network for Open-AuditIT. If you use a single IP or a range, please ensure that before you run the Discovery you have added a corresponding network so Open-AuditIT will accept audit results from those targets.

As of Open-AuditIT 2.3.1, the network address should be set to localhost for Linux and the server's IP for Windows. Only use https if you have configured and enabled HTTPS on this server and HTTP has been disabled from localhost.

Discovery Options

Discovery Preset details are as follows (including an indicative time to scan an individual IP):

UltraFast: 1 second: Scan only the ports that Open-AuditIT needs to use to talk to the device and detect an iOS device (WMI, SSH, SNMP, Apple Sync). A "filtered" port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

SuperFast: 5 seconds: Scan the top 10 TCP and UDP ports, as well as port 62078 (Apple iOS detection). A "filtered" port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Fast: 40 seconds: Scan the top 100 TCP and UDP ports, as well as port 62078 (Apple iOS detection). A "filtered" port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Medium (Classic): 90 seconds: As close to a traditional Open-AuditIT scan as we can make it. Scan the top 1000 TCP ports, as well as 62078 (Apple iOS detection) and UDP 161 (SNMP). A "filtered" port is considered open (and will trigger device detection). Devices are scanned regardless of a response to an Nmap ping. Use aggressive timing.

Medium: 100 seconds: Scan the top 1000 TCP and top 100 UDP ports, as well as port 62078 (Apple iOS detection). A "filtered" port is not considered open. Device must respond to an Nmap ping. Use aggressive timing.

Slow: 4 minutes: Scan the top 1000 TCP and top 100 UDP ports, as well as port 62078 (Apple iOS detection). Version detection enabled. A "filtered" port is considered open (and will trigger device detection). Device must respond to an Nmap ping. Use normal timing.

UltraSlow: 20 minutes: Not recommended. Scan the top 1000 TCP and UDP ports, as well as port 62078 (Apple iOS detection). Devices are scanned regardless of a response to an Nmap ping. Version detection enabled. A "filtered" port is considered open (and will trigger device detection). Use polite timing.

Custom: Unknown time: When options other than as set by a standard discovery preset are altered.

Nmap Timing Options

Nmap timing details are found on the bottom of this linked page <https://nmap.org/book/man-performance.html>. From that page:

If you are on a decent broadband or ethernet connection, I would recommend always using -T4 (Aggressive). Some people love -T5 (Insane) though it is too aggressive for my taste. People sometimes specify -T2 (Polite) because they think it is less likely to crash hosts or because they consider themselves to be polite in general. They often don't realize just how slow -T2 really is. Their scan may take ten times longer than a default scan. Machine crashes and bandwidth problems are rare with the default timing options -T3 (Normal) and so I normally recommend that for cautious scanners. Omitting version detection is far more effective than playing with timing values at reducing these problems.

— Gordon "Tyodor" Lyon

Open-AuditIT Enterprise 2.0.0 is licensed to Opmartek for 12345 Nodes - Expires 18-Jul-2019
Purchase a license for more nodes by clicking [here](#).

Powered by Opmartek

Check the wiki for a more detailed explanation about [Discoveries](#)

Display Improvements

As well as the functional improvements to discovery, we have also revised the Discovery Details page. We have sections for Summary, Details, Devices, Logs and IP Addresses. The Devices section, in particular, is now much more useful. We have added a new type of Unclassified to the list and we use this when we have more than just an IP and/or name for the device. For instance, we may know it's IP, name and the fact that it has port 135 open. This at least is a good indication that the device is likely a Windows machine. So we know "something". More than just "there is something at this IP". That is now an Unclassified device. We still support Unknown devices as always - for those devices we really know nothing about. An example of this screen is below. We also provide a quick link to creating credentials when a service (SSH, WMI, SNMP) has been identified, but we were not able to authenticate to it.

We think these display improvements will go a long way to assisting you to remove any Unknown or Unclassified devices that are on your network.

Click to enlarge.

Open-AuditIT Enterprise 2.3.2

ViewDiscoverReportManage

AdminHelpModulesLicensesUser: admin

Home / Discoveries / 192.168.88.0

192.168.88.0

Summary

Details

Logs

Devices

IP Addresses

Devices

All records per page

Showing 1 to 27 of 27 entries

Search:

FirstPreviousNextLast

View	IP	Name	Identification	Issues	Last Seen
	192.168.88.1 computer	wifi opmantek.com	Computer running Linux from TP-Link Technology	SSH detected but no valid SSH credentials for 192.168.88.1.	2019-02-08 15:43:49
	192.168.88.6 computer	odr opmantek.com	Server from HP		2019-02-08 15:43:52
	192.168.88.7 computer	magni opmantek.com	Computer running Linux from HP	SNMP detected, but no valid SNMP credentials found for 192.168.88.7	2019-02-08 15:43:55
	192.168.88.8 computer	thor opmantek.com	Virtual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials found for 192.168.88.8	2019-02-08 15:43:57
	192.168.88.9 computer	eris opmantek.com	Server from Gigabyte Technology Co., Ltd.		2019-02-08 15:44:01
	192.168.88.10 computer	odin opmantek.com	Server from Gigabyte Technology Co., Ltd.		2019-02-08 15:44:05
	192.168.88.14 computer	snotra opmantek.com	Virtual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials found for 192.168.88.14	2019-02-08 15:44:09
	192.168.88.15 computer	odem opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:12
	192.168.88.20 unclassified	magni-mgmt opmantek.com	Device running SSH	SSH detected but no valid SSH credentials for 192.168.88.20. No valid credentials for 192.168.88.20	2019-02-08 15:44:14
	192.168.88.45 computer	crash-n-burn opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:17
	192.168.88.48 computer	ubuntu opmantek.com	Virtual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials found for 192.168.88.48	2019-02-08 15:44:21
	192.168.88.51 computer	snorri opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:24
	192.168.88.52 unclassified	192.168.88.52	No information could be retrieved.	No management protocols for 192.168.88.52	2019-02-08 15:44:27
	192.168.88.53 computer	red-burn opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:30
	192.168.88.54 computer	sun-burn opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:33
	192.168.88.55 computer	se7en opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:35
	192.168.88.56 unclassified	192.168.88.56	Device running WMI (likely a Windows computer)	WMI detected but no valid Windows credentials for 192.168.88.56. No valid credentials for 192.168.88.56	2019-02-08 15:44:39
	192.168.88.57 computer	idontknow opmantek.com	Virtual server from VMware, Inc.		2019-02-08 15:44:41
	192.168.88.60 unclassified	192.168.88.60	Device running SSH	SSH detected but no valid SSH credentials for 192.168.88.60. No valid credentials for 192.168.88.60	2019-02-08 15:44:44
	192.168.88.62 unclassified	192.168.88.62	Device running SSH	SSH detected but no valid SSH credentials for 192.168.88.62. No valid credentials for 192.168.88.62	2019-02-08 15:44:47
	192.168.88.63 unclassified	192.168.88.63	Device running SSH and WMI (likely a Windows computer)	SSH detected but no valid SSH credentials for 192.168.88.63. WMI detected but no valid Windows credentials for 192.168.88.63. No valid credentials for 192.168.88.63	2019-02-08 15:44:49
	192.168.88.64 unclassified	192.168.88.64	Device running WMI (likely a Windows computer)	WMI detected but no valid Windows credentials for 192.168.88.64. No valid credentials for 192.168.88.64	2019-02-08 15:44:51
	192.168.88.73 computer	hel workgroup	Virtual server from VMware	SSH detected but no valid SSH credentials for 192.168.88.73.	2019-02-08 15:44:54
	192.168.88.106 computer	virtual_elf opmantek.com	Virtual server from VMware, Inc.	SNMP detected, but no valid SNMP credentials found for 192.168.88.106	2019-02-08 15:44:56
	192.168.88.177 iphone	192.168.88.177	iphone from Apple	No management protocols for 192.168.88.177	2019-02-08 15:44:59
	192.168.88.253 switch	midgard opmantek.com	Switch from Cisco Systems		2019-02-08 15:45:01
	192.168.88.254 router	asgard opmantek.com	Router from Cisco Systems		2019-02-08 15:45:03

Showing 1 to 27 of 27 entries

FirstPreviousNextLast

Open-AuditIT Enterprise 2.0.0 is licensed to Opmantek for 12345 Nodes - Expires 19-Jul-2019

Purchase a license for more nodes by clicking [here](#).

Powered by Opmantek

Wrap Up

This new functionality makes Open-AuditIT a powerful and easy to use discovery solution while providing great flexibility for advanced users.

I hope you enjoy the new features as much as our test customers and I do.

Mark Unwin.

