Release Notes for Open-AudIT v2.3.2

Released 2019-02-04

Linux md5sum: b8f7b940820c088c429196a28739170b

Linux SHA256: 3f94938134c147998f7aa28a1c56af38204ef27fbce5a3c379953413eecb813f

Introduction

With Open-AudIT 2.3.2 we have introduced the ability to customise both the scanning options for Nmap and the device matching rules - per discovery.

The Nmap scanning options are contained in a new endpoint (or collection) named nmap_scan_options. You can create your specific options and save them as an item, then use them in your discoveries.

Community users have the ability to select one of the supplied discovery scan options and use it as the default for all scans. Community users will use the default configured matching rules in the configuration as per previous releases for all scans.

Professional users can select an individual discovery scan options entry per scan. Professional users will use the default configured matching rules in the configuration as per previous releases for all scans.

Enterprise users can CRUD (create, read, update, delete) individual discovery scan options as well as customise individual attributes per discovery. Enterprise users can customise the matching rules per scan.

Discovery Scan Options

For more detailed information, go to the Discovery Scan Options page.

The options contained within a discovery scan options entry are as below.

Must Respond To Ping	If set, Nmap will fist attempt to send and listen for an ICMP response. If the device does not respond, no further scanning will occur. Previously a device did not have to respond to a ping for Open-AudIT to continue scanning.
Use Service Version Detection	When a detected port is detected as open, if set to 'y', Nmap will query the target device in an attempt to determine the version of the service running on this port. This can be useful when identifing unclassified devices. This weas not previouslt used.
Consider Filtered Ports Open	Previously, Open-AudIT considered an Nmap response of "open|filtered" as a device responding on this port. This has caused some customers issues where firewalls respond on behalf of a non-existing device, and hence cause false positive device detection. We now have this attribute available to set per scan.
Timing	The standard Nmap timing options. Previously set at T4 (aggressive).
Top Nmap TCP Ports	The top 10, 100, 1000 ports to scan as per Nmap's "top ports" options. Previously we scanned the Top 1000 ports (the Nmap standard).
Top Nmap UDP Ports	The top 10, 100, 1000 ports to scan as per Nmap's "top ports" options. Previously we scanned UDP 161 (snmp) only.
Custom TCP Ports	Any specific ports we would like scanned in addition to the Top TCP Ports. Comma separated, no spaces.
Custom UDP Ports	Any specific ports we would like scanned in addition to the Top UDP Ports. Comma separated, no spaces.
Timout per Target	Wait for X seconds for a target response.
Exclude TCP Ports	Exclude any ports listed from being scanned. Comma separated, no spaces.
Exclude UDP Ports	Exclude any ports listed from being scanned. Comma separated, no spaces.
Exclude IP Addresses	Exclude IP Addresses (individual IP - 192.168.1.20, ranges - 192.168.1.30-40 or subnets - 192.168.1.100/30) listed from being scanned. Comma seperated, no spaces.

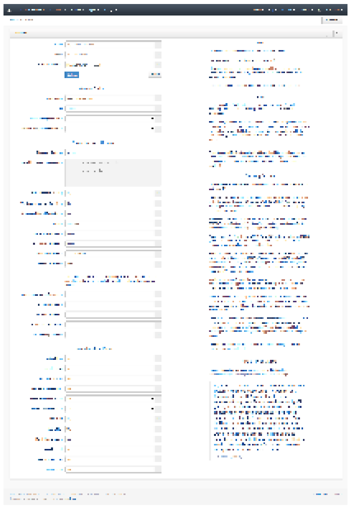
SSH Port	Scan for this port and if detected open, use this port for SSH communication. This is added to the list of Custom TCP POrts above, so there is no need to include it in that listr as well.

When creating a discovery in Enterprise, the screen now looks as below ()after Advanced has been clicked).

As always, you can simply set the name and subnet to be scanned and the defaults (as per the configuration) will be used and you're off and running. If you want to change individual items per scan, click the Advanced button and you have full access to all fields.

Professional users are able to select the Discovery Options from the drop down, but not customize individual attributes.

Click for larger image.



Version	Type	Description
Open-AudIT Enterprise	New Feature	Discovery specific scan and match options.
Open-AudIT	Improvement	Add a 5 second delay for invalid logon attempts.
Open-AudIT Professional	New Feature	Add "Debug" under the users name (top left) which shows JSON output similar to what COmmunity has had for some time.
Open-AudIT Community	New Feature	Add timings for major sections of the response to the META sections of the output (visible using Debug).
Open-AudIT Community	Improvement	Refine processing a device. Do NOT populate "hostname" with "dns_hostname". Populate name with hostname, sysName, dns hostname then IP in that order.
Open-AudIT Community	Improvement	Add a new column - system.identification. Populate upon scan or audit processing.
Open-AudIT Professional	Improvement	Display the "identification" column in the default list when showing the device list.
Open-AudIT Community	Improvement	Improve discovery logging. Log at severity 5 when no working credentials are found or no management protocols (WMI, SSH, SNMP) are returned.

Open-AudIT Community	Improvement	Do not unset the device type if all we have is an Nmap result (ie, MAC manufacturer = Apple or port 62078 is open and device name contains iphone, set device even with just an Nmap scan to iphone).
Open-AudIT Community	Improvement	Use Sodium Compat and Random Compat PHP libraries to enable PHP > 7.2 compatibility. Updated version of phpSecLib installed.
Open-AudIT Community	Improvement	Audit code (in audit_windows.vbs and audit_linux.sh) that correctly parses and inserts as XML the devices open netstat ports. Correspondingly, process this data as per other data with no requirement to parse the raw netstat data within the Open-AudIT server.
Open-AudIT Community	Bug	NMIS export now renders correctly and does not error out.
Open-AudIT Community	Bug	Add the discovery data to the response so when requested from OAP/E, we don't produce an error because of a GET but no data returned.
Open-AudIT Community	Improvement	Remove discovery logs from a JSON read request to discoveries. We should now use the /discovery_log endpoint.
Open-AudIT Professional	New Feature	Add a button on the discoveries_read template to enable use to export all relevant discovery information.
Open-AudIT Community	Improvement	In audit_windows.vbs, wrap attempt to talk to domain in an on error resume next to prevent breakage when talking to an openLDAP domain.
Open-AudIT Community	Bug	Fix broken service, user, route sections on device details page.
Open-AudIT Community	Improvement	Add a new device type of Unclassified. If we have limited information about a device, but Do have something lile a manufacturer derived from a MAC or a port is open, then the device is now classes as Unclassified, not Unknown.
Open-AudIT Community	Improvement	New icon for Unknown devices (warning roadsign with exclamation mark). Reuse old unknown ison for Unclassified devices (blue circle with question mark).
Open-AudIT Professional	Improvement	Show different colurs for an unknown or unclassified device.
Open-AudIT Enterprise	Improvement	Added more items to clouds::read template.
Open-AudIT Enterprise	Improvement	AutoRefresh clouds::read template if status ne completed.
Open-AudIT Professional	Improvement	AutoRefresh discoveries::read template if status ne completed.
Open-AudIT Professional	Improvement	Improve design of discoveries::read template for devices and logs.
Open-AudIT Professional	Bug	On the discoveries::create form, fix the tour for the missing tour_name class.
Open-AudIT Professional	Bug	Provide bulk edit on queries_execute and reports_execute templates.

Open-AudIT Professional	Bug	Restore Support -> Export button on template. Force download instead of display output.
Open-AudIT Professional	Improvement	Added pagination and summary to top of dataTables for discoveries::read template for logs, devices and IPs.
Open-AudIT Professional	Improvement	Add a button that links to credentials create on discoveries devices when discovery log shows no XXX type of credentials.
Open-AudIT Professional	Improvement	Add buildings, floors, rooms and rows to sub menus under Locations.
Open-AudIT Professional	Improvement	Check and automatically fix the Nmap SetUID issue on Linux.
Open-AudIT Professional	Improvement	Add the Nmap Program detected to the Nmap Ports section on the device details template.