Discovery Scan Options

Introduction

Starting with Open-AudIT 2.3.2 we have introduced sets of preconfigured options for running the discovery scan using Nmap.

As at 3.3.0 we have introduced a "filtered|open" option to discovery scan options with a default of 'y'. Previously we used the "filtered" column to check for open|filtered. This change aligns the discovery scan options with Nmap return strings.

How Does it Work?

When a discovery ius run, the relevant discovery scan option is chosen and those settings used by Nmap to scan the target devices. If no option set is chosen, the default configuration item (discovery_default_scan_option) is selected and used.

If a device is individually discovered using the "Discover Device" link on the device details page, we first check if this device has been discovered previously (by Discoverey) and if so, use the discovery options from that scan. If it has not been previously discovered, we revert to the configuration item discovery_default_scan_option the settings.

Creating a Discovery Scan Options entry

Discovery Scan Options are just another item collection. Enterprise users can create, read, update and delete entries as required. Professional users can read all entries, but not create new entries, update existing entries or delete entries. Community users have no GUI that allows access to this collection.

Roles contain the definitions for users that are allowed to CRUD these items (regardless of license). Just like Baselines, for example.

The attributes for discovery scan options are as below.

Attribute	Description
id	The standard ID of an auto-incrementing integer.
name	The standard 'name' of a collection item. Ideally should be unique.
org_id	The Org that owns this entry.
description	The standard description field.
options	Unused at present. Options fields within the Open-AudIT schema are generally designed to hold a stringified JSON object.
edited_by	The user that created or last edited this entry.
edited_date	The standard date/time this entry was created or last edited.
ping	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.
service_version	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 identifying unclassified devices. This was not previously used.

open|filtered	An open|filtered port is considered open (and will trigger device detection). 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.
filtered	A filtered port is considered open (and will trigger device detection).
timing	The standard Nmap timing options. Previously set at T4 (aggressive).
nmap_tcp_ports	Top Nmap TCP Ports. The top 10, 100, 1000 ports to scan as per Nmaps "top ports" options. Previously we scanned the Top 1000 ports (the Nmap standard).
nmap_udp_ports	Top Nmap UDP Ports. The top 10, 100, 1000 ports to scan as per Nmaps "top ports" options. Previously we scanned UDP 161 (snmp) only.
tcp_ports	Custom TCP Ports. Any specific ports we would liuke scanned in addition to the Top TCP Ports. Comma seperated, no spaces.
udp_ports	Custom UDP Ports. Any specific ports we would liuke scanned in addition to the Top UDP Ports. Comma seperated, no spaces.
	The below fields can be overwritten by an individual discovery, while still "using" a discovery_scan_options item for these if they're not set in the discovery.
timeout	Timeout per Target. Wait for X seconds for a target response.
exclude_tcp	Exclude any ports listed from being scanned. Comma seperated, no spaces.
exclude_udp	Exclude any ports listed from being scanned. Comma seperated, no spaces.
exclude_ip	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(s) 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. Comma seperated, no spaces.

Database Schema

```
CREATE TABLE `discovery_scan_options` (
 `id` int(10) unsigned NOT NULL AUTO_INCREMENT,
 `name` varchar(100) NOT NULL DEFAULT '',
 `org_id` int(10) unsigned NOT NULL DEFAULT '1',
 `description` text NOT NULL,
 `ping` enum('','y','n') NOT NULL DEFAULT 'y',
 `service_version` enum('','y','n') NOT NULL DEFAULT 'n',
 `open|filtered` enum('','y','n') NOT NULL DEFAULT 'n',
 `filtered` enum('','y','n') NOT NULL DEFAULT 'n',
 `timeout` int(10) unsigned NOT NULL DEFAULT '0',
 `timing` int(1) unsigned NOT NULL DEFAULT 4,
 `nmap_tcp_ports` int(10) unsigned NOT NULL DEFAULT '0',
 `nmap_udp_ports` int(10) unsigned NOT NULL DEFAULT '0',
 `tcp_ports` text NOT NULL,
 `udp_ports` text NOT NULL,
 `exclude_tcp_ports` text NOT NULL,
 `exclude_udp_ports` text NOT NULL,
 `exclude_ip` text NOT NULL,
 `ssh_ports` text NOT NULL,
 `options` text NOT NULL,
 `edited_by` varchar(200) NOT NULL DEFAULT '',
 `edited_date` datetime NOT NULL DEFAULT '2000-01-01 00:00:00',
 PRIMARY KEY (`id`)
) ENGINE=InnoDB DEFAULT CHARSET=utf8;
```

API / Web Access

You can access the /discovery_scan_options collection using the normal Open-AudIT JSON based API. Just like any other collection. Please see the API documentation for further details.

Access is provided as part of a roles permissions. Discovery Scan Options is a standard resource and can have create, read, update and delete permissions (by Enbterprise licensed customers).

The API routes below are usable from both a JSON Restful API and the web interface. The Web application routes are specifically designed to be called from the web interface (a browser).

API Routes

Request Method	ID	Action	Resulting Function	Permission Required	URL Example	Notes
POST	n		create	discovery_scan_options::create	/discovery_scan_options	Insert a new discovery_scan_options entry.
GET	y		read	discovery_scan_options::read	/discovery_scan_options/{id}	Returns a discovery_scan_options details.
PATCH	y		update	discovery_scan_options::update	/discovery_scan_options/{id}	Update an attribute of a discovery_scan_options entry.
DELETE	y		delete	discovery_scan_options::delete	/discovery_scan_options/{id}	Delete a discovery_scan_options entry.
GET	n		collection	discovery_scan_options::read	/discovery_scan_options	Returns a list of discovery_scan_options.

Web Application Routes

Request Method	ID	Action	Resulting Function	Permission Required	URL Example	Notes
GET	n	create	create_form	discovery_scan_options::create	/discovery_scan_options/create	Displays a standard web form for submission to POST /discovery_scan_options.