
ACAS NESSUS PARSER USER GUIDE

Author: Jennifer Gregorio

7/17/2017

Getting Started

Nessus is a security scanning tool which scans a computer and finds any vulnerabilities that hackers could use to gain access to computers you have connected to a network. The Nessus Parser is a tool that parses one or more files from a Nessus Scan into a format that can be imported into other applications. For each device recorded within the Nessus file, a series of data points are collected and formatted for an import into another application.

Among the collected data points are the MAC addresses, which are used to match a device to a vendor designated by the organization unique identifier. The vendor is then recorded and used to create the appropriate Qualified name for the device, based on the vendor information. The oui.csv file contains the first six alphanumeric characters of the MAC address and pairs it with a vendor. The vendors.csv file contains a list of vendors and the qualified names for each.

To use the Nessus Parser, you must have the oui.csv, vendors.csv, NessusParser_vendor_oui.jar (executable jar file), and the Nessus files that you want parsed installed on your computer.

Run the NessusParser_vendor_oui.jar file. The window that opens will look like Figure 1:

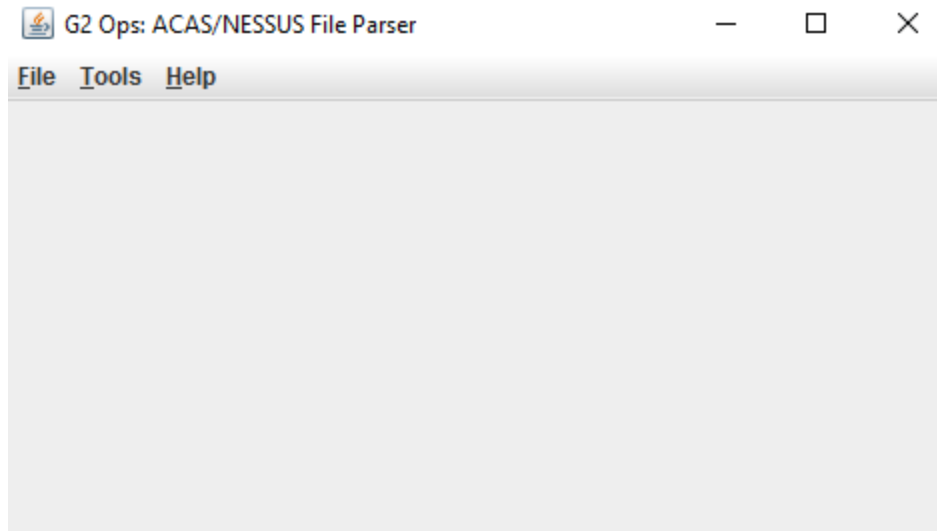


Figure 1

Before you begin using this tool, you want to make sure you have the most recent version of the oui.csv file which includes the list of MAC addresses and vendors. In the top left corner click the **Tools** dropdown menu and click **Update MAC Address Data** as seen in Figure 2.

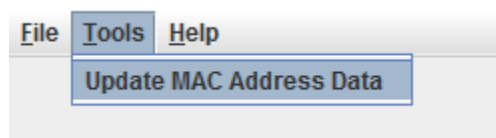


Figure 2

The window seen in Figure 3 will pop up with instructions on how to update your oui.csv file:

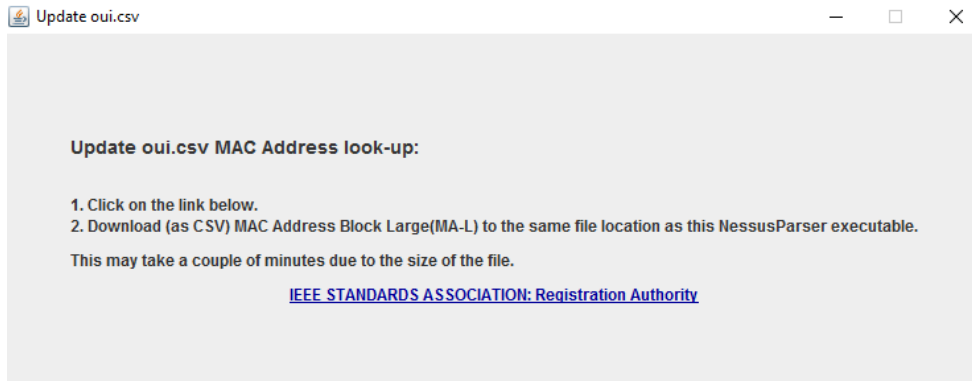


Figure 3

Upon clicking the link, you will be brought to the website (Figure 4) where you can download the most recent version of the oui.csv. The blue arrow shows which file you should be downloading. Make sure your oui.csv, vendors.csv, and NessusParser_vendor_oui.jar files are all saved in the same directory.

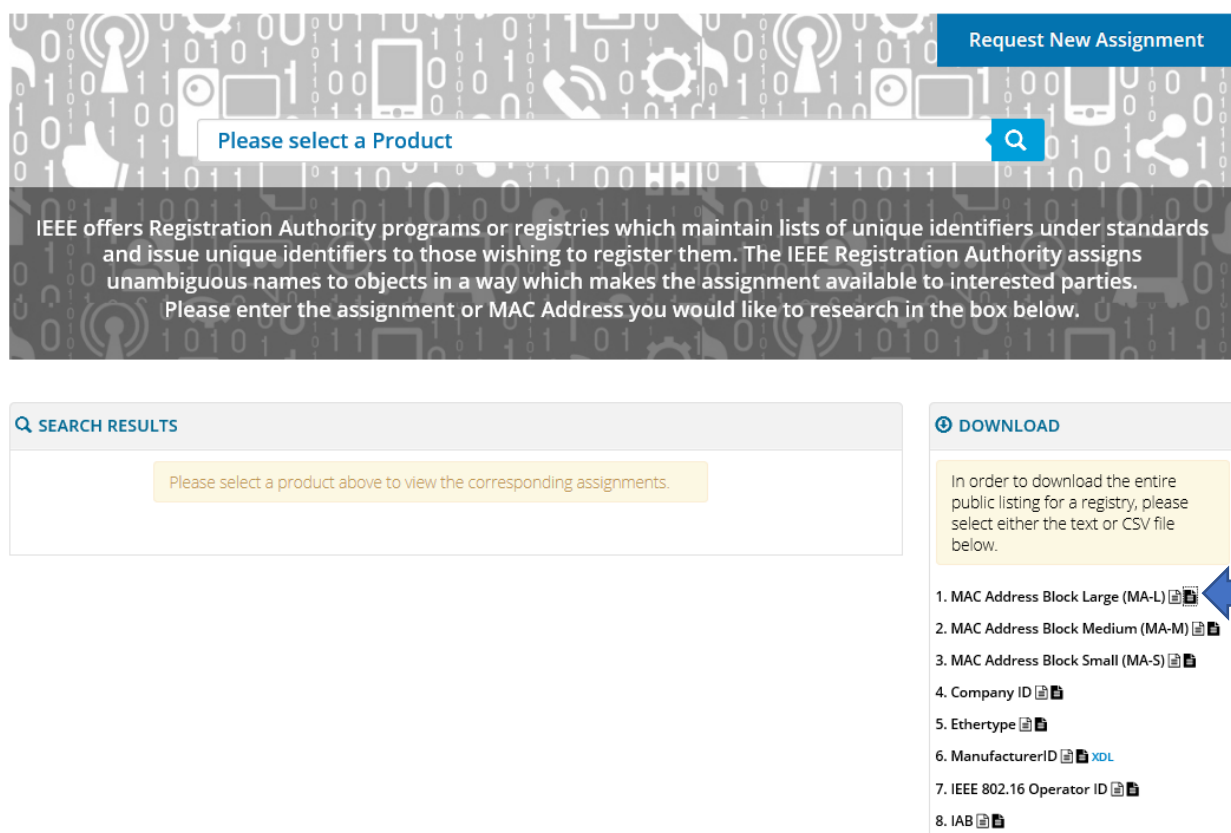


Figure 4

To open the Nessus files that you need parsed, click the **File** dropdown menu in the top left corner and click **Open**.

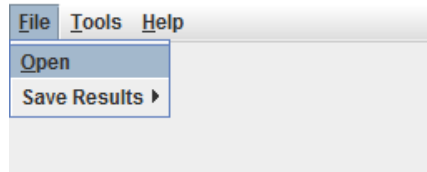


Figure 5

A File Chooser will pop up as seen in Figure 6. From here you can navigate to the directory where you have your Nessus files.

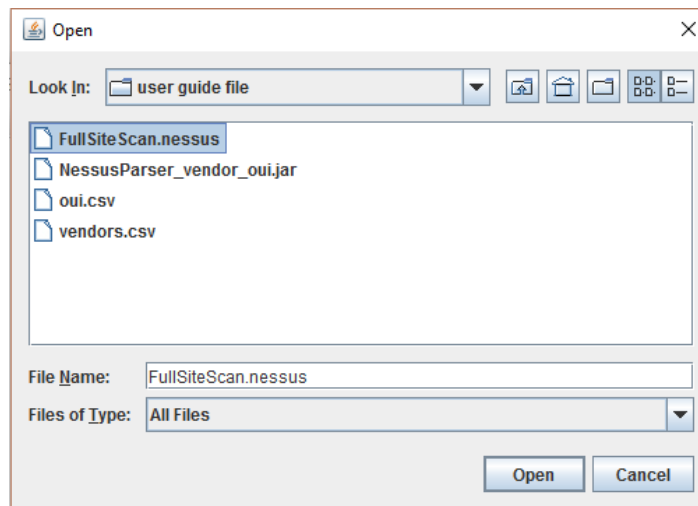


Figure 6

Select one or more Nessus files that you need and click **Open**, the following screen (Figure 7) will show up:

host	vendor	macAddress	qualifiedName	IP-Address	O/S	operatingSystem
10.107.4.1	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.4.1	mac	Cisco IOS XE Cisco IOS Software
10.107.0.2	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.0.2	mac	Cisco IOS XE Cisco IOS Software
10.107.16.2	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.16.2	mac	Cisco IOS XE Cisco IOS Software
10.107.16.3	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.16.3	mac	Cisco IOS XE Cisco IOS Software
10.107.4.3	Cisco Systems	00:6b:f1:99:32:f3	Communications Profile::Vendor ...	10.107.4.3	linux	CISCO IOS 15.6(1)S2
10.107.1.1	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.1.1	mac	Cisco IOS XE Cisco IOS Software
10.107.1.3	Cisco Systems	00:6b:f1:46:1f:20	Communications Profile::Vendor ...	10.107.1.3	linux	CISCO IOS 15.6(1)S2
10.107.0.1	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.0.1	mac	Cisco IOS XE Cisco IOS Software
10.112.243.3				10.112.243.3	linux	
10.112.243.2				10.112.243.2	linux	
10.112.243.1				10.112.243.1	other	
10.112.242.3				10.112.242.3	linux	
10.112.242.2				10.112.242.2	other	
10.112.242.1				10.112.242.1	linux	
10.112.240.3				10.112.240.3	linux	
10.112.240.2				10.112.240.2	other	
ovb3850-1t.headquarters.com				10.121.0.3	linux	
ovb1001-1b.headquarters.com				10.121.0.2	other	
ovb1001-1t.headquarters.com				10.121.0.1	other	
10.112.244.3				10.112.244.3	other	
10.112.244.2				10.112.244.2	other	
10.112.244.1				10.112.244.1	other	
10.107.24.2	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.24.2	mac	Cisco IOS XE Cisco IOS Software
10.107.25.2	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.25.2	mac	
10.107.18.3	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.18.3	mac	Cisco IOS XE Cisco IOS Software

Figure 7

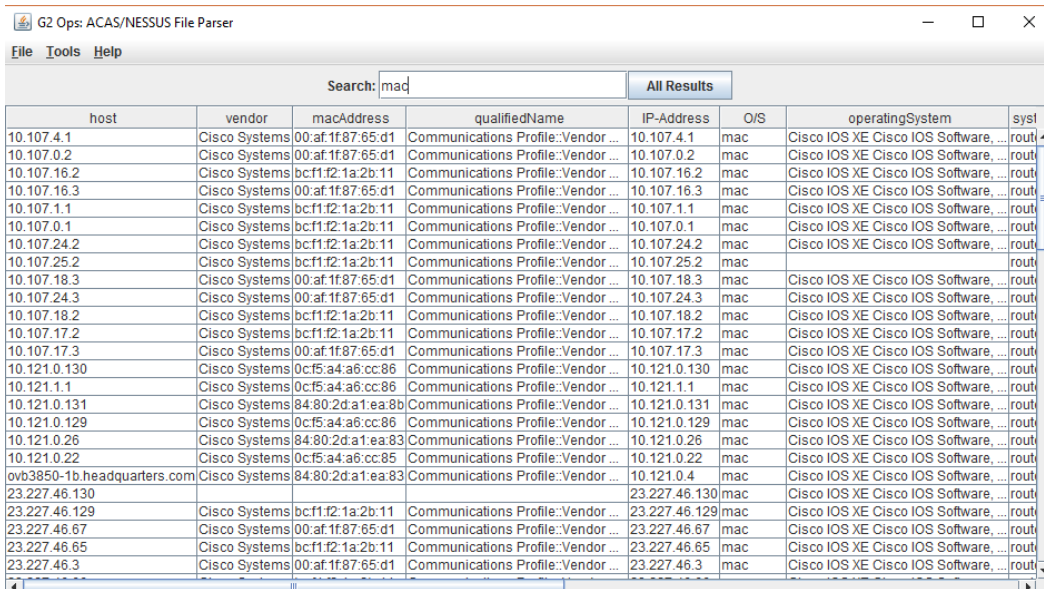
To create the vendor file needed for the Nessus Parser, navigate to the communications profile inside MagicDraw. Create a report to extract vendors and set the file layout to include columns for the sequence names, vendor names, and MagicDraw qualified names. The first few rows should look like Figure 8.

	A	B	C
1	1		Communications Profile::Vendor Hardware & Software::Vendor Folder::
2	2	3Com	Communications Profile::Vendor Hardware & Software::Vendor Folder::3Com
3	3	ADC	Communications Profile::Vendor Hardware & Software::Vendor Folder::ADC
4	4	ADC Fibermux Corp.	Communications Profile::Vendor Hardware & Software::Vendor Folder::ADC Fibermux Corp.
5	5	Adobe Systems Incorporated	Communications Profile::Vendor Hardware & Software::Vendor Folder::Adobe Systems Incorporated

Figure 8

Filtering Results

In some cases, you may want to filter the results to only see a certain type of operating system, vendor, FQDN, etc. At the top of the window in the **Search** bar you can type in a keyword and press Enter on your keyboard to filter the results. As an example, Figure 9 shows the data filtered by the word “mac”:



The screenshot shows a window titled "G2 Ops: ACAS/NESSUS File Parser" with a search bar containing "mac" and an "All Results" button. Below the search bar is a table with the following columns: host, vendor, macAddress, qualifiedName, IP-Address, O/S, operatingSystem, and syst. The table contains 25 rows of data, all of which have "mac" in the O/S column.

host	vendor	macAddress	qualifiedName	IP-Address	O/S	operatingSystem	syst
10.107.4.1	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.4.1	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.0.2	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.0.2	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.16.2	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.16.2	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.16.3	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.16.3	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.1.1	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.1.1	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.0.1	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.0.1	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.24.2	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.24.2	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.25.2	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.25.2	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.18.3	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.18.3	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.24.3	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.24.3	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.18.2	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.18.2	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.17.2	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	10.107.17.2	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.107.17.3	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	10.107.17.3	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.121.0.130	Cisco Systems	0c:f5:a4:a6:cc:86	Communications Profile::Vendor ...	10.121.0.130	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.121.1.1	Cisco Systems	0c:f5:a4:a6:cc:86	Communications Profile::Vendor ...	10.121.1.1	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.121.0.131	Cisco Systems	84:80:2d:a1:ea:8b	Communications Profile::Vendor ...	10.121.0.131	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.121.0.129	Cisco Systems	0c:f5:a4:a6:cc:86	Communications Profile::Vendor ...	10.121.0.129	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.121.0.26	Cisco Systems	84:80:2d:a1:ea:83	Communications Profile::Vendor ...	10.121.0.26	mac	Cisco IOS XE Cisco IOS Software, ...	rout
10.121.0.22	Cisco Systems	0c:f5:a4:a6:cc:85	Communications Profile::Vendor ...	10.121.0.22	mac	Cisco IOS XE Cisco IOS Software, ...	rout
ovb3850-1b.headquarters.com	Cisco Systems	84:80:2d:a1:ea:83	Communications Profile::Vendor ...	10.121.0.4	mac	Cisco IOS XE Cisco IOS Software, ...	rout
23.227.46.130				23.227.46.130	mac	Cisco IOS XE Cisco IOS Software, ...	rout
23.227.46.129	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	23.227.46.129	mac	Cisco IOS XE Cisco IOS Software, ...	rout
23.227.46.67	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	23.227.46.67	mac	Cisco IOS XE Cisco IOS Software, ...	rout
23.227.46.65	Cisco Systems	bc:f1:f2:1a:2b:11	Communications Profile::Vendor ...	23.227.46.65	mac	Cisco IOS XE Cisco IOS Software, ...	rout
23.227.46.3	Cisco Systems	00:af:1f87:65:d1	Communications Profile::Vendor ...	23.227.46.3	mac	Cisco IOS XE Cisco IOS Software, ...	rout

Figure 9

To get back to the original table without any filter results click in the **All Results** button to the right of the Search bar.

Saving Results as MBSE CSV Import

In the top left corner click **File**, then go to **Save Results**, and click **MBSE CSV Import** as seen in Figure 10.

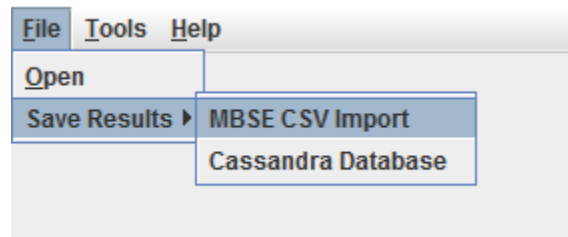


Figure 10

A File Saver will pop up as seen in Figure 11. From here you can navigate to the directory where you want to save the csv files and click **Save**.

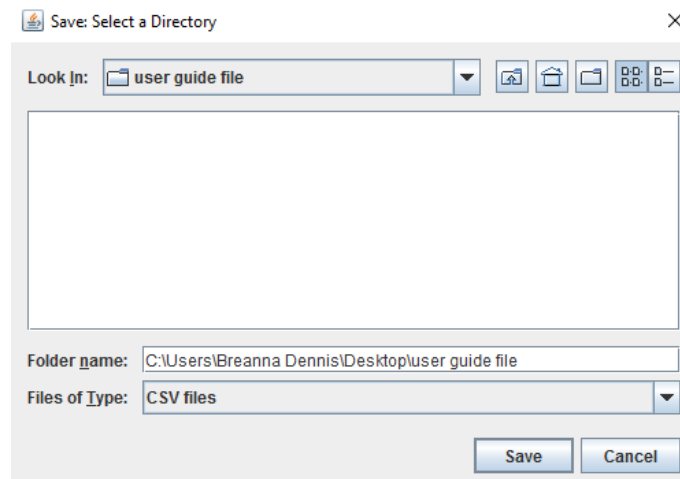


Figure 11

A message will pop up telling you that three csv files have been saved to the directory path that you selected. Now, when you navigate to the directory that you selected (Figure 12), you will see that a connector-ends.csv, host-ports.csv, and an importSpreadsheet.csv file appear, which can now be imported into other applications.

Name	Date modified	Type	Size
connector-ends.csv	7/11/2017 11:01 AM	Microsoft Excel C...	46 KB
host-ports.csv	7/11/2017 11:01 AM	Microsoft Excel C...	446 KB
importSpreadsheet.csv	7/11/2017 11:01 AM	Microsoft Excel C...	42 KB
NessusParser_vendor_oui.jar	7/10/2017 9:58 AM	Executable Jar File	4,719 KB
FullSiteScan.nessus	6/29/2017 8:26 AM	NESSUS File	35,677 KB
oui.csv	6/29/2017 8:18 AM	Microsoft Excel C...	2,012 KB
vendors.csv	6/29/2017 8:18 AM	Microsoft Excel C...	13 KB

Figure 12

The importSpreadsheet.csv includes the information that is displayed within the window of the Nessus Parser; connector-ends.csv records network connections between devices; and host-ports.csv collects the port, protocol, and service name within each host. Note that if you imported multiple Nessus files to be parsed, these files will be aggregated to the same three export csv files.

Here is what the first few lines of each file should look like:

importSpreadsheet.csv:

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	host	vendor	macAddress	qualifiedName	IP-Address	O/S	operatingSystem	systemType	FQDN	scanDate	installedS	traceRout	CVSSBase	CVSSTemporalScore	
2	10.107.4.1	Cisco Systems	00:af:1f:87:6f	Communications	10.107.4.1	mac	Cisco IOS XE Cisco IOS Software,router			Thu Jan 5	cpe:/o:ci	10.101.6	5	4.8	
3	10.107.0.2	Cisco Systems	00:af:1f:87:6f	Communications	10.107.0.2	mac	Cisco IOS XE Cisco IOS Software,router			Thu Jan 5	cpe:/o:ci	10.101.6	5	4.8	
4	10.107.16.2	Cisco Systems	bc:f1:f2:1a:2f	Communications	10.107.16.	mac	Cisco IOS XE Cisco IOS Software,router			Thu Jan 5	cpe:/o:ci	10.101.6	5	4.8	
5	10.107.16.3	Cisco Systems	00:af:1f:87:6f	Communications	10.107.16.	mac	Cisco IOS XE Cisco IOS Software,router			Thu Jan 5	cpe:/o:ci	10.101.6	5	4.8	

connector-ends.csv:

	A	B	C	D	E	F	G
1	Source	SourceName	BlockName	Target	TargetName	Owner	Diagram
2	10.101.61.125	Site::EndPoint_83	EndPoint_83	10.101.0.197	Site::EndPoint_84	Site	Site::Diagram
3	10.101.0.197	Site::EndPoint_84	EndPoint_84	10.101.0.181	Site::EndPoint_85	Site	Site::Diagram
4	10.101.0.181	Site::EndPoint_85	EndPoint_85	10.127.216.202	Site::EndPoint_86	Site	Site::Diagram
5	10.127.216.202	Site::EndPoint_86	EndPoint_86	10.107.1.1	Site::EndPoint_5	Site	Site::Diagram

host-ports.csv:

	A	B	C	D
1	host	ports	serviceName	protocol
2	10.107.4.1	0	general	tcp
3	10.107.4.1	0	general	tcp
4	10.107.4.1	0	general	tcp
5	10.107.4.1	22	ssh	tcp

In future versions of the Nessus Parser, you will be able to save results into a Cassandra Database.