



IOT device network scanner

User manual

Bachelor in the IT-Factory
Keuzerichting Cloud and cyber security

Name: Simon Duchateau

Academic year 2020-2021

Campus Geel, Kleinhoefstraat 4, BE-2440 Geel

Table of content

1	INTRODUCTION	2
2	LOGIN	3
3	DASHBOARD	4
4	RESULT TOTAL SCAN	5
5	RESULT RANGE SCAN	7
6	SEARCH	9
7	SPECIFIC VIEW	10
8	UPLOAD CONFIG	11
9	IOT DEVICES	12
10	NETWORK DEVICES	13
11	CLIENT DEVICES	14

1 INTRODUCTION

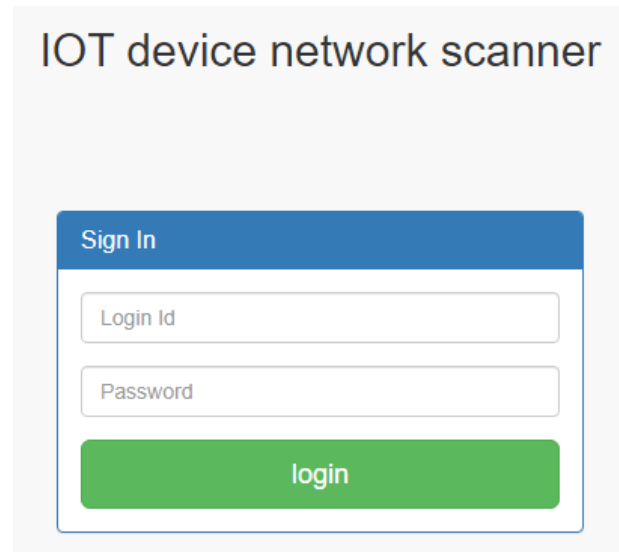
This user manual is designed to provide information about how to use the IOT device network scanner application. This application is designed to have a user friendly output of an detailed nmap scan with the focus on IOT devices.

What are IOT devices and why did we focus on them? IOT devices are devices connected to your network with the aim of making things easier for you. For example a smart thermostat, light switches that you can operate with your phone,... nowadays these devices aren't that rare anymore. But these type of devices need to be secured properly otherwise the possibility that unauthorized people would operate or access these devices would be big.

With this application you can perform a network scan and view all the devices on this network. Not only the devices are shown but also a lot of more information like the scanned port, operating system,... We used a tool called nmap to perform this scan. This is an open source network scanner.

I will briefly explain all the pages of the application. I also will talk about the features this application provides. This document is the continuation of the installation manual where I explain how to install the needed software and the application itself.

2 LOGIN



The screenshot shows a web application interface for an "IOT device network scanner". At the top, the title "IOT device network scanner" is displayed in a large, dark font. Below the title is a "Sign In" form. The form has a blue header bar with the text "Sign In" in white. Inside the form, there are two input fields: "Login Id" and "Password", both with light gray placeholder text. Below these fields is a green button with the text "login" in white.

The first page you are able to see is the login page. We provided this application with a basic login screen. You only need the username and the password of a user. At this point we only provided an admin user. If the company wants to add users they have to contact the administrator.

3 DASHBOARD

IOT device network scanner

Dashboard

Result total scan

Result range scan

Search

Specific view

Upload Config

IOT Devices

Network Devices

Client devices

Logout

WELCOME ADMIN

Total scan

192.168.0.0

Start Scan

Range scan

IP-Adres: 0.0.0.0

Netmask: 24

Start Scan

After u are logged in successfully you enter the Dashboard page of the application. The purpose of this page is to start a scan. You can choose between two different type of scans.

If you want to do a total scan you fill the start IP-address of your preferred network and it will scan this network automatically with the subnet mask of /24.

But if you want to adjust the subnet mask you can chose to use the range scan. With this scan you have the option to manually add the subnet mask as preferred.

Each time you perform a scan all the previous data will be lost. But the data of the total scan won't override the range scan data and vice versa.

4 RESULT TOTAL SCAN

IOT device network scanner

Dashboard
Result total scan
Devices
Ports
Result range scan
Search
Specific view
Upload Config
IOT Devices
Network Devices
Client devices
Logout

WELCOME ADMIN

View Devices

Id	IP address	Mac address	Vendor	Operating System	
1	192.168.0.2	AC:22:05:8C:A8:FF	Compal Broadband Networks	OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)	<input checked="" type="checkbox"/>
2	192.168.0.3	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	<input type="checkbox"/>
3	192.168.0.4	D8:CB:8A:A1:B2:C3	Micro-star Intl	Microsoft Windows XP SP3	<input type="checkbox"/>
4	192.168.0.5	BC:60:A7:01:AD:2B	Sony Interactive Entertainment		<input type="checkbox"/>
5	192.168.0.6	B8:2C:A0:A1:B2:C3	Resideo	Sharp AR-C260M or AR-M351N printer	<input type="checkbox"/>
6	192.168.0.7	40:F5:20:D5:E6:F7	Espressif	ESP-IDF (ESP32, ESP32-S2)	<input type="checkbox"/>
7	192.168.0.8	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	<input type="checkbox"/>
8	192.168.0.9	40:F5:20:D6:E7:F8	Espressif	ESP-IDF (ESP32, ESP32-S2)	<input type="checkbox"/>
9	192.168.0.10	D4:6A:6A:3C:6E:F2	Hon Hai Precision Ind.	VxWorks	<input type="checkbox"/>
10	192.168.0.11	40:F5:20:D7:E8:F9	Espressif	ESP-IDF (ESP32, ESP32-S2)	<input type="checkbox"/>
11	192.168.0.12	D8:CB:8A:A2:B3:C4	Micro-star Intl	Microsoft Windows XP SP3	<input type="checkbox"/>
12	192.168.0.13	D4:A6:51:A1:B2:C3	Tuya Smart	Tuya AIOT	<input type="checkbox"/>
13	192.168.0.14	F4:06:69:D3:86:DC	Intel Corporate	Linux 4.15 - 5.6	<input type="checkbox"/>
14	192.168.0.15	FC:FC:48:A1:B2:C3	Apple Inc.	Apple Mac OS X 10.7.0 (Lion) - 10.12 (Sierra) or iOS 4.1 - 9.3.3 (Darwin 10.0.0 - 16.4.0)	<input type="checkbox"/>































After you performed a total scan you can see all the scanned devices with their information. You can see their IP and MAC address but I also provided the device vendor and the operating system that runs on this particular device.

You can see that the last column contains a few options. For example if you want to have more detailed information about this particular device you can select . This will lead you to a Specific view page of this device.

If you want to select a device because you want to come back on this device on a later date you just can select the select box ☐.

The last button is there if you see a device that isn't important to you. You can easily delete this device from the database. Remember after you have deleted this device all the information is gone from the database including all the ports. If you want this device back you have to rerun the scan.

IOT device network scanner						
Dashboard						
Result total scan						
Devices						
Ports						
Result range scan						
Search						
Specific view						
Upload Config						
IOT Devices						
Network Devices						
Client devices						
Logout						


WELCOME ADMIN						
View Ports						
Id	Device id	Port number	Port state	Port protocol	Port product	
1	1	53	open	tcp	dnsmasq 2.78	 
2	1	5000	open	tcp	MiniUPnP 1.9	 
3	2	53	open	tcp	dnsmasq 2.39	 
4	2	80	filtered	tcp		 
5	2	443	filtered	tcp		 
6	2	333	open	tcp	Netgear POT-(Get/Set) Demo	 
7	3	135	open	tcp	Microsoft Windows RPC	 
8	3	443	open	tcp		 
9	3	445	open	tcp	Microsoft Windows 7 - 10 microsoft-ds	 
10	3	902	open	tcp	VMware Authentication Daemon 1.10	 
11	3	2869	open	tcp	Microsoft HTTPAPI httpd 2.0	 
12	7	53	open	tcp	dnsmasq 2.39	 
13	7	80	open	tcp	OpenWrt uHTTPd	 
14	7	443	open	tcp		 
15	7	3333	open	tcp	Netgear POT-(Get/Set) Demo	 


The total scan also gathers information of all the open ports. On this page you get a table with all the open ports within your network. You don't just see the port but you also get a lot of important information.

The row starts with the device id. This id links the port to the device that uses this port. Next to the device id is the port number. The port number is a very important number because this mostly tells a lot about the service running behind this port.

This application gives you all the needed port information without you having to search for it. As you can see you get the state of the port. Not all ports that are viewed are open they could be filtered as well.

The rest of the information is the port protocol. This way you know how you could connect to the device using TCP or UDP. But you also get the service running behind this port.

If you want to have more information about the device using this port you can easily use the button . This will lead you to the specific view page of this particular device.

You also get the option to delete this port . If you delete a port you delete this row from the database. Take caution if, you want this information back you need to rerun the scan. Deleting a port doesn't influence the other ports from the same device

5 RESULT RANGE SCAN

IOT device network scanner					
WELCOME ADMIN					
Devices					
Id	IP address	Mac address	Vendor	Operating System	
1	192.168.0.2	AC:22:05:8C:A8:FF	Compal Broadband Networks	OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)	🔗 <input checked="" type="checkbox"/> ✖
2	192.168.0.3	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	🔗 <input type="checkbox"/> ✖
3	192.168.0.4	D8:CB:8A:A1:B2:C3	Micro-star Intl	Microsoft Windows XP SP3	🔗 <input type="checkbox"/> ✖
4	192.168.0.5	BC:60:A7:01:AD:2B	Sony Interactive Entertainment		🔗 <input type="checkbox"/> ✖
5	192.168.0.6	B8:2C:A0:A1:B2:C3	Resideo	Sharp AR-C260M or AR-M351N printer	🔗 <input type="checkbox"/> ✖

After you performed a range scan you can see all the scanned devices with their information. You can see their IP and MAC address but you can also see the device vendor and the operating system that runs on this particular device.

If you want to select a device because you want to come back on this device on a later date you just can select the select box ☐.

The last button is there if you see a device that isn't important to you. You can easily delete this device from the database. Remember after you have deleted this device all the information is gone from the database including all the ports. If you want this device back you have to rerun the scan. [✖](#)


IOT device network scanner						
WELCOME ADMIN						
Ports						
Id	Device id	Port number	Port state	Port protocol	Port product	
1	1	53	open	tcp	dnsmasq 2.78	✎ ⓘ
2	1	5000	open	tcp	MiniUPnP 1.9	✎ ⓘ
3	2	53	open	tcp	dnsmasq 2.39	✎ ⓘ
4	2	80	filtered	tcp		✎ ⓘ
5	2	443	filtered	tcp		✎ ⓘ
6	2	333	open	tcp	Netgear POT-(Get/Set) Demo	✎ ⓘ
7	3	135	open	tcp	Microsoft Windows RPC	✎ ⓘ
8	3	443	open	tcp		✎ ⓘ
9	3	445	open	tcp	Microsoft Windows 7 - 10 microsoft-ds	✎ ⓘ
10	3	902	open	tcp	VMware Authentication Daemon 1.10	✎ ⓘ
11	3	2869	open	tcp	Microsoft HTTPAPI httpd 2.0	✎ ⓘ

The range scan also gathers information of all the open ports. On this page you get a table with all the open ports within your range. You don't just see the port but you also get a lot of important information.

The row starts with the device id. This id links the port to the device that uses this port. Next to the device id is the port number. The port number is a very important number because this mostly tells a lot about the service running behind this port.

This application gives you all the needed port information without you having to search for it. As you can see you get the state of the port. Not all ports that are viewed are open they could be filtered as well.

The rest of the information is the port protocol. This way you know how you could connect to the device using TCP or UDP. But you also get the service running behind this port.

You also get the option to delete this port . If you delete a port you delete this row from the database. Take caution, if you want this information back you need to rerun the scan. Deleting a port doesn't influence the other ports from the same device.

6 SEARCH

IOT device network scanner

Dashboard
Result total scan
Result range scan
Search
Specific view
Upload Config
IOT Devices
Network Devices
Client devices
Logout

WELCOME ADMIN

View Devices

Vendor (Separated with :)

Contains

Id	IP address	Mac address	Vendor	Operating System	
1	192.168.0.2	AC:22:05:8C:A8:FF	Compal Broadband Networks	OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)	
2	192.168.0.3	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	
3	192.168.0.4	D8:CB:8A:A1:B2:C3	Micro-star Intl	Microsoft Windows XP SP3	
4	192.168.0.5	BC:60:A7:01:AD:2B	Sony Interactive Entertainment		
5	192.168.0.6	B8:2C:A0:A1:B2:C3	Resideo	Sharp AR-C260M or AR-M351N printer	

If the prevised tables aren't clear because you have too many devices on your network, you can search your devices on device name. This way you can make your search field smaller and more clear.

You have four options to choose from. You can search if the vendor name contains..., does not contain..., equals ., does not equals ... If you completed your search the table will only contain devices that are equal to your search values. We gave you the option to search for multiple Vendor names at the same time. You just have to separate them with a , like shown in the screenshot.

You can see that the last column contains a few options. For example if you want to have more detailed information about this particular device you can select . This will lead you to a Specific view page of this device.

If you want to select a device because you want to come back on this device on a later date you just can select the select box .

The last button is there if you see a device that isn't important to you. You can easily delete this device from the database. Remember after you have deleted this device all the information is gone from the database including all the ports. If you want this device back you have to rerun the scan.

7 SPECIFIC VIEW

IOT device network scanner

Dashboard

Result total scan

Result range scan

Search

Specific view

Specific view total scan

192.168.0.2

192.168.0.3

192.168.0.4

192.168.0.5

192.168.0.6

192.168.0.7

192.168.0.8

192.168.0.9

192.168.0.10

192.168.0.11

192.168.0.12

192.168.0.13

192.168.0.14

192.168.0.15

WELCOME ADMIN

Selects

Device id: 1

IP-adres: 192.168.0.2

MAC-adres: AC:22:05:8C:A8:FF

Vendor: Compal Broadband Networks

Operating System: OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)

id	Device id	Port number	Port state	Port protocol	Port product	
1	1	53	open	tcp	dnsmasq 2.78	
2	1	5000	open	tcp	MiniUPnP 1.9	

If you select the specific view dropdown in the menu bar you get a dropdown. This dropdown contains all the IP addresses of the scanned devices from the total scan. Now you can choose which device you want more information about.

This page is created to get a clear overview about a specific device. First you get a detailed list about the device itself. From mac and IP addresses to the vendor name and Operating System.

The device information is followed by a table with the port information. This table only contains the ports that belong to this particular device. You also have the option to delete unnecessary ports if you wish to.

8 UPLOAD CONFIG

IOT device network scanner

Dashboard
Result total scan
Result range scan
Search
Specific view
Upload Config
IOT Devices
Network Devices
Client devices
Logout

WELCOME ADMIN

Devices

How to format the text files?
You have to write each vendor name on a new line

Vendor name 1
Vendor name 2
Vendor name 3

Browse IOT Devices
Choose File | No file chosen | Upload

IOT Device names in table
Resideo
BehrTech
Edgeworx
FogHorn
Medigate
Ockam
Samsara
ZEDEDA
Softeq
ScienceSoft
Espressif
Tuya Smart

Browse Network Devices
Choose File | No file chosen | Upload

Network Device names in table
Netgear
Compal Broadband Networks
Cisco Systems
TP-Link
D-Link
Linksys
Nokia Networks
Belkin
Hon Hai Precision Ind.

Browse Client Devices
Choose File | No file chosen | Upload

Client Device names in table
Micro-star Intl
Intel Corporate
Lenovo
Samsung
LG Electronics USA Inc.
Dell
Google
Asus
Apple Inc.
Sony Interactive Entertainment

This page is used if you want to define what vendor names are IOT, Network or Client devices. You get an easy to use interface where you can select a .txt file from your local pc and if you click the upload button the application upload your values to a database. You only need to use the format as shown in the example.

9 IOT DEVICES

IOT device network scanner					
Dashboard					
Result total scan <					
Result range scan <					
Search					
Specific view <					
Upload Config					
IOT Devices					
Network Devices					
Client devices					
Logout					
WELCOME ADMIN					
Devices					
id	IP address	Mac address	Vendor	Operating System	
5	192.168.0.6	B8:2C:A0:A1:B2:C3	Resideo	Sharp AR-C260M or AR-M351N printer	✎ <input type="checkbox"/> ⚙
6	192.168.0.7	40:F5:20:D5:E6:F7	Espressif	ESP-IDF (ESP32, ESP32-S2)	✎ <input type="checkbox"/> ⚙
8	192.168.0.9	40:F5:20:D6:E7:F8	Espressif	ESP-IDF (ESP32, ESP32-S2)	✎ <input type="checkbox"/> ⚙
10	192.168.0.11	40:F5:20:D7:E8:F9	Espressif	ESP-IDF (ESP32, ESP32-S2)	✎ <input type="checkbox"/> ⚙
12	192.168.0.13	D4:A6:51:A1:B2:C3	Tuya Smart	Tuya AIOT	✎ <input type="checkbox"/> ⚙





































If you are specifically searching for all the IOT devices within your network you easily can select the IOT devices button in the menu bar. You now get a clear overview of all the IOT devices within your scanned network with the total scan. You can define what an IOT devices is by using the Upload config page.

You can see that the last column contains a few options. For example if you want to have more detailed information about this particular device you can select [✎](#). This will lead you to a Specific view page of this device.


If you want to select a device because you want to come back on this device on a later date you just can select the select box ☐.

The last button is there if you see a device that isn't important to you. You can easily delete this device from the database. Remember after you have deleted this device all the information is gone from the database including all the ports. If you want this device back you have to rerun the scan. [✖](#)


10 NETWORK DEVICES

IOT device network scanner																																			
<div> <div>Dashboard</div> <div>Result total scan <</div> <div>Result range scan <</div> <div>Search</div> <div>Specific view <</div> <div>Upload Config</div> <div>IOT Devices</div> <div>Network Devices</div> <div>Client devices</div> <div>Logout</div> </div>																																			
WELCOME ADMIN																																			
<div>Devices</div> <table> <tr> <th>id</th><th>IP address</th><th>Mac address</th><th>Vendor</th><th>Operating System</th><th></th></tr> <tr> <td>1</td><td>192.168.0.2</td><td>AC:22:05:8C:A8:FF</td><td>Compal Broadband Networks</td><td>OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)</td><td>  </td></tr> <tr> <td>2</td><td>192.168.0.3</td><td>6C:B0:CE:05:0C:4C</td><td>Netgear</td><td>Linux 2.6.13 - 2.6.32</td><td>  </td></tr> <tr> <td>7</td><td>192.168.0.8</td><td>6C:B0:CE:05:0C:4C</td><td>Netgear</td><td>Linux 2.6.13 - 2.6.32</td><td>  </td></tr> <tr> <td>9</td><td>192.168.0.10</td><td>D4:6A:6A:3C:6E:F2</td><td>Hon Hai Precision Ind.</td><td>VxWorks</td><td>  </td></tr> </table>						id	IP address	Mac address	Vendor	Operating System		1	192.168.0.2	AC:22:05:8C:A8:FF	Compal Broadband Networks	OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)	  	2	192.168.0.3	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	  	7	192.168.0.8	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	  	9	192.168.0.10	D4:6A:6A:3C:6E:F2	Hon Hai Precision Ind.	VxWorks	  
id	IP address	Mac address	Vendor	Operating System																															
1	192.168.0.2	AC:22:05:8C:A8:FF	Compal Broadband Networks	OpenWrt Chaos Calmer 15.05 (Linux 3.18) or Designated Driver (Linux 4.1 or 4.4)	  																														
2	192.168.0.3	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	  																														
7	192.168.0.8	6C:B0:CE:05:0C:4C	Netgear	Linux 2.6.13 - 2.6.32	  																														
9	192.168.0.10	D4:6A:6A:3C:6E:F2	Hon Hai Precision Ind.	VxWorks	  																														

Network devices are very important. This is why we created a page with all the network devices within your network. You can define what a network device is using the Upload Config page. If you complete the upload you now can see all the matching devices.

You can see that the last column contains a few options. For example if you want to have more detailed information about this particular device you can select . This will lead you to a Specific view page of this device.

If you want to select a device because you want to come back on this device on a later date you just can select the select box ☐.

The last button is there if you see a device that isn't important to you. You can easily delete this device from the database. Remember after you have deleted this device all the information is gone from the database including all the ports. If you want this device back you have to rerun the scan. 

11 CLIENT DEVICES

IOT device network scanner

Dashboard
Result total scan
Result range scan
Search
Specific view
Upload Config
IOT Devices
Network Devices
Client devices
Logout

WELCOME ADMIN

Devices

Id	IP address	Mac address	Vendor	Operating System	
3	192.168.0.4	D8:CB:8A:A1:B2:C3	Micro-star Intl	Microsoft Windows XP SP3	<input type="checkbox"/>
4	192.168.0.5	BC:60:A7:01:AD:2B	Sony Interactive Entertainment		<input type="checkbox"/>
11	192.168.0.12	D8:CB:8A:A2:B3:C4	Micro-star Intl	Microsoft Windows XP SP3	<input type="checkbox"/>
13	192.168.0.14	F4:06:69:D3:86:DC	Intel Corporate	Linux 4.15 - 5.6	<input type="checkbox"/>
14	192.168.0.15	FC:FC:48:A1:B2:C3	Apple Inc.	Apple Mac OS X 10.7.0 (Lion) - 10.12 (Sierra) or iOS 4.1 - 9.3.3 (Darwin 10.0.0 - 16.4.0)	<input type="checkbox"/>

The last page displays a list of all the devices that are labelled as client devices. Client devices are usually devices that are used for daily use. This could be important because these devices normally don't need a lot of open ports.

You can see that the last column contains a few options. For example if you want to have more detailed information about this particular device you can select . This will lead you to a Specific view page of this device.

If you want to select a device because you want to come back on this device on a later date you just can select the select box ☐.

The last button is there if you see a device that isn't important to you. You can easily delete this device from the database. Remember after you have deleted this device all the information is gone from the database including all the ports. If you want this device back you have to rerun the scan.