Bell Street
DD1 1HG
Dundee
Scotland, UK

SESSION: 2019/2020

System Internals & Cybersecurity

Module Code: CMP408

Raspberry Pi Nmap scanner with S3 storage

Mini Project; submission 4

Student Name: Ekku Jokinen
Student ID: 1703641

.

Note that Information contained in this document is for educational purposes.

.

Contents

.

1 INTRODUCTION

1.1 PROJECT USE CASE

This project is aimed towards a client company with little-to-no cyber security skills/knowledge. They receive a Raspberry Pi (RPi from now on) shipped to them from a cyber security company offering the service and they plug into their network. The RPi has a web server installed with a simple web UI and the Nmap network scanner installed onto it. The client goes to the web UI and selects what type of scan they want to initiate, and the interface crafts the Nmap command for them, and runs it on the selected IP address. After finishing the scan, it uploads the output onto a private Amazon S3 bucket, and the reports can be read from there by the company offering the service. Since the output is accessible online, the company providing the RPi can then interpret the results remotely and advice the client for further action.

By not needing to send employees to the client's company to conduct the scanning in-person, the client saves money and can have simple cyber security testing done for a more affordable price.

1.2 OBJECTIVES / FEATURES

1.2.1 Security

- Private S3 bucket which can only be accessible by authorised personnel
- Client company does not have access to the S3 bucket
- RPi runs with the lowest needed privileges
- RPi utilises a very restricted user for AWS which only allows file uploads
- HTTPS is used by default

1.2.2 Other

- The scanner has a RED LED that lights up during while a scan is running
- The scanner has a YELLOW LED which lights up while a scan output file is being uploaded onto the S3 bucket
- The scanner has a GREEN LED which blinks five times after everything is finished successfully
- Responsive & easy to use web interface

2 PROCEDURE

2.1 RASPBERRY PI SETUP

For the indicator LEDs, three LEDs need to be set up on the RPi (Figure 1).

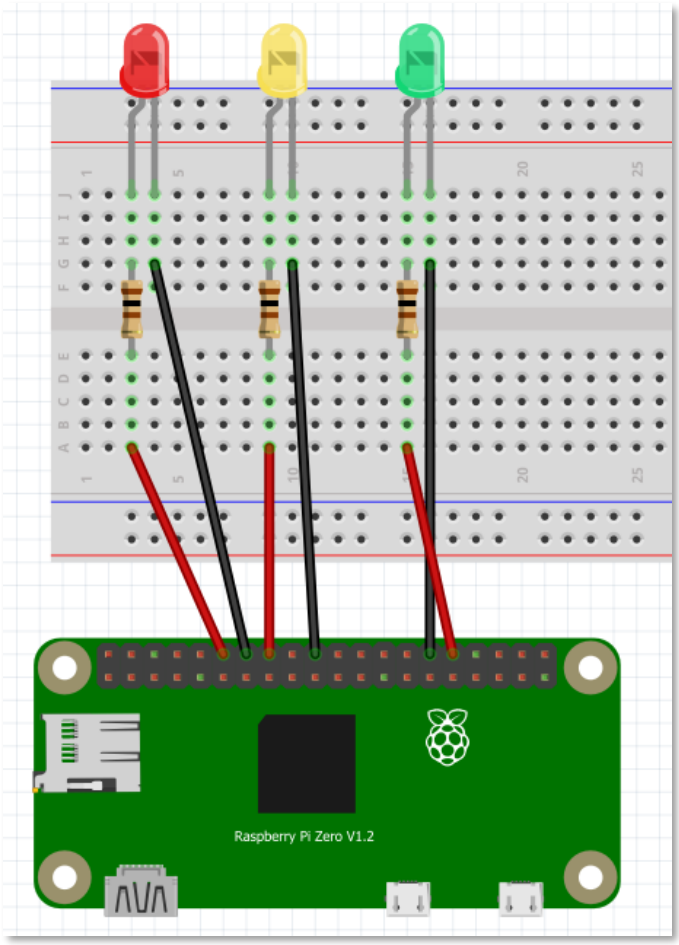

Figure 1 Schematic for the project; version 1.1 was used instead of the pictured 1.2.

For the web UI, Apache needs to be installed and the default user for it (www-data) needs extra permissions so it can run sudo commands. The Apache user also needs the permission to run commands as another user for the AWS CLI upload command to work. This is achieved by adding the following into the /etc/sudoers file:

```
www-data ALL=NOPASSWD: /usr/bin/gpio, /usr/bin/nmap

www-data ALL=(<user2>) NOPASSWD: ALL
```

By restricting www-data privileges to the minimum amount needed improves the security of the product. The second permission could be fine-tuned more by only allowing www-data to execute AWS CLI commands as the second user.

After setting up Apache and copying the web UI files into the default folder, the AWS CLI client needs to be installed. The version 1 of the client can be installed by running:

```
pip3 install --upgrade --user awscli
```

The client needs to be configured to use the access ID and secret access key once the S3 bucket and users have been set up (**section 2.2**). The AWS CLI configuration is initiated by running:

```
/home/darian/.local/bin/aws configure
AWS access Key ID
AWS Secret Access Key
S3 Bucket region name
```

2.2 AWS SETUP

2.2.1 Users and Policy

Two users need to be set up, one for the RPi (RPi-Nmap) so it can upload files to the S3 bucket and the other (RPi-DevUser) for the cyber security company to read the files (Figure 3). The RPi user is setup with programmatic access which allows connections to the S3 bucket using an access key ID and a secret access key (Figure 2).

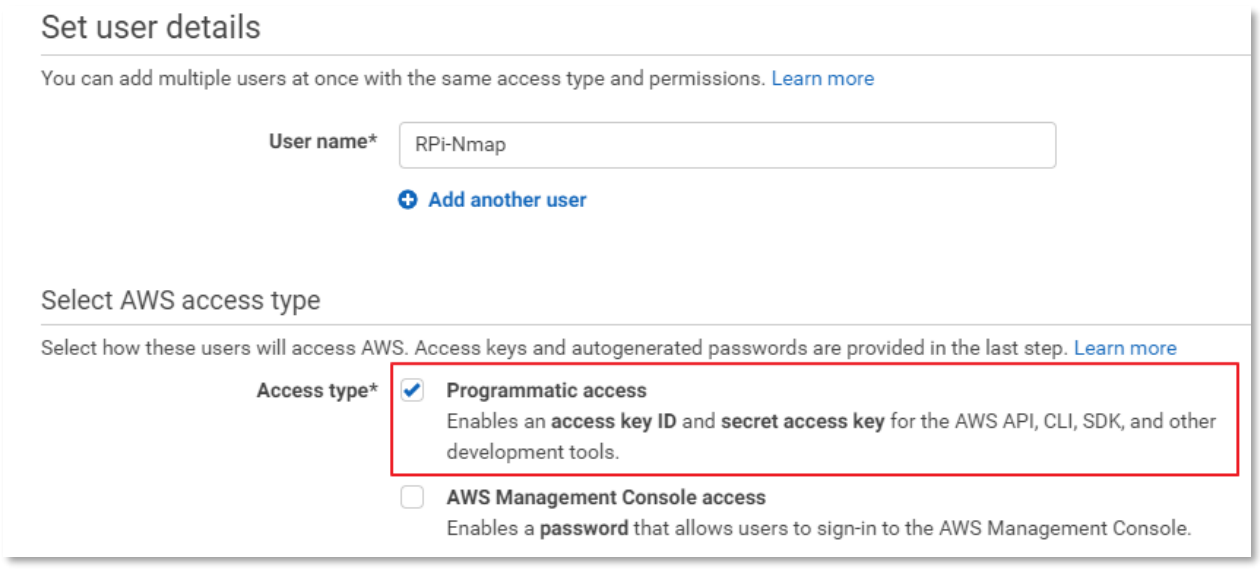

Figure 2 Creating a new low privilege AWS user for the RPi.

Figure 3 The project utilises two users.

The RPi user only needs the rights to upload files to the scanner's bucket so that in the scenario the device is compromised, no harm can be done to the S3 bucket (Figure 4). This also prevents the client from accidentally deleting anything from the S3 bucket or viewing other buckets belonging to the cyber security company. The second user meant for the company can be given all necessary permissions (read/write/list) since they own the device and will be interpreting and acting upon the data in the scans.

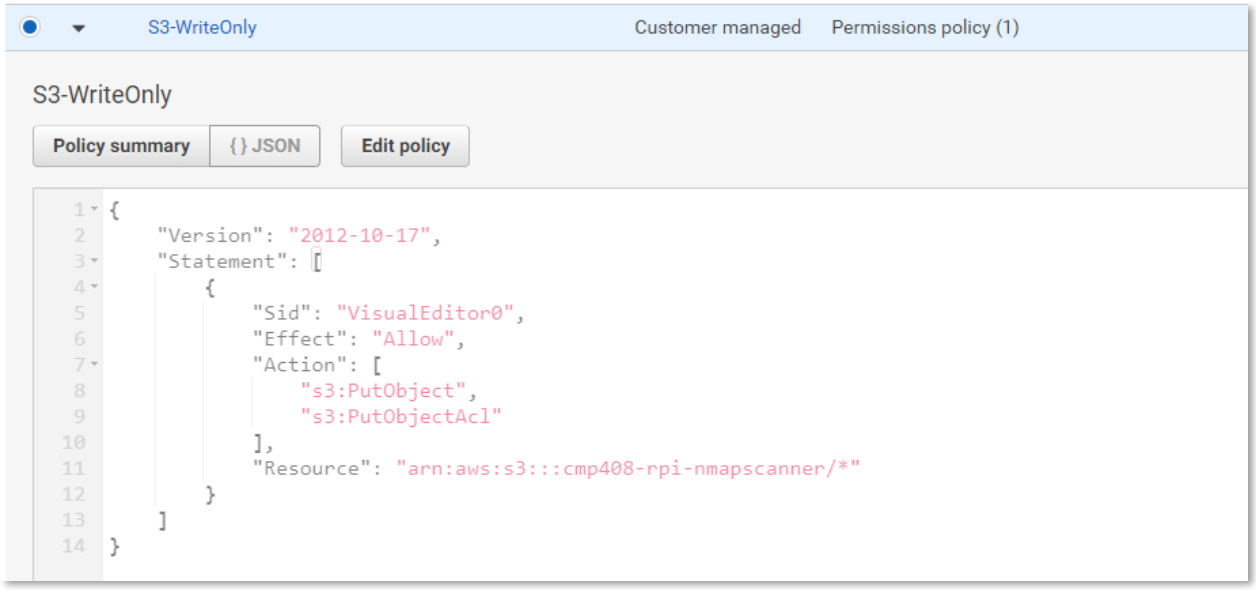

Figure 4 Upload-only user policy for the RPi.

2.2.2 S3 Bucket

An S3 bucket needs to be created for storing the scan output files. As a security feature, a second S3 bucket should also be created to act as a log bucket for any access attempts to the primary S3 bucket. Both buckets are setup to block public access and AES-256 encryption should be enabled for increased security (Figures 5 & 6).

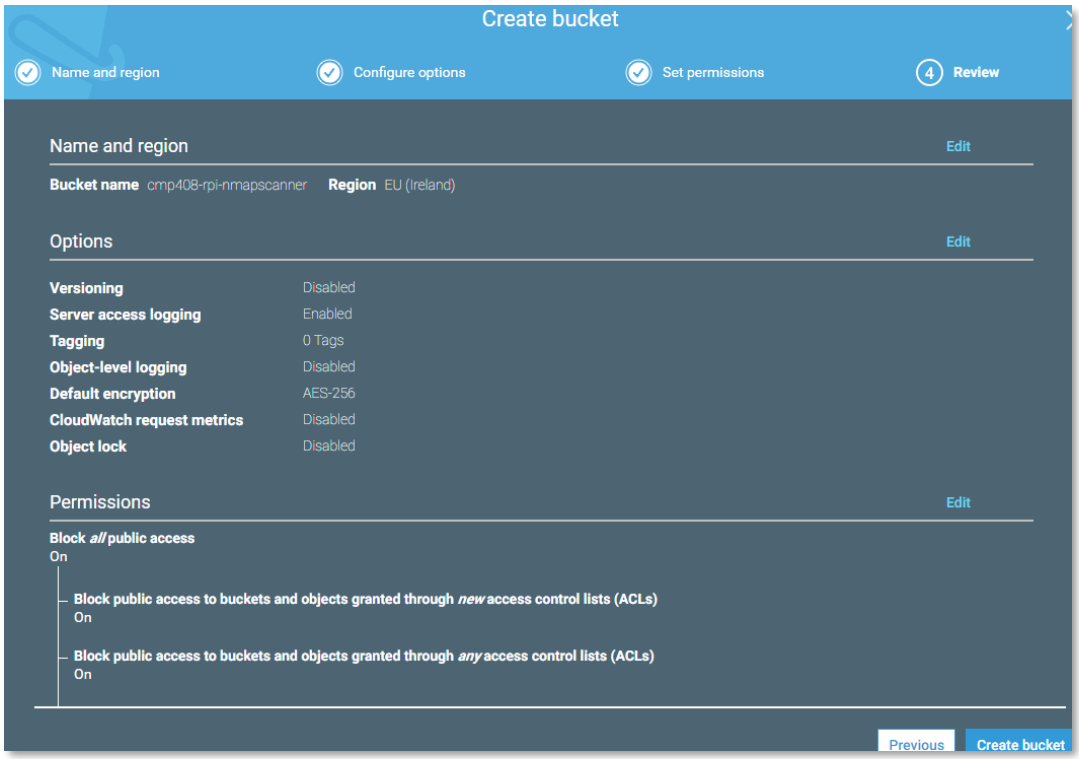

Figure 5 S3 bucket for storing scan outputs.

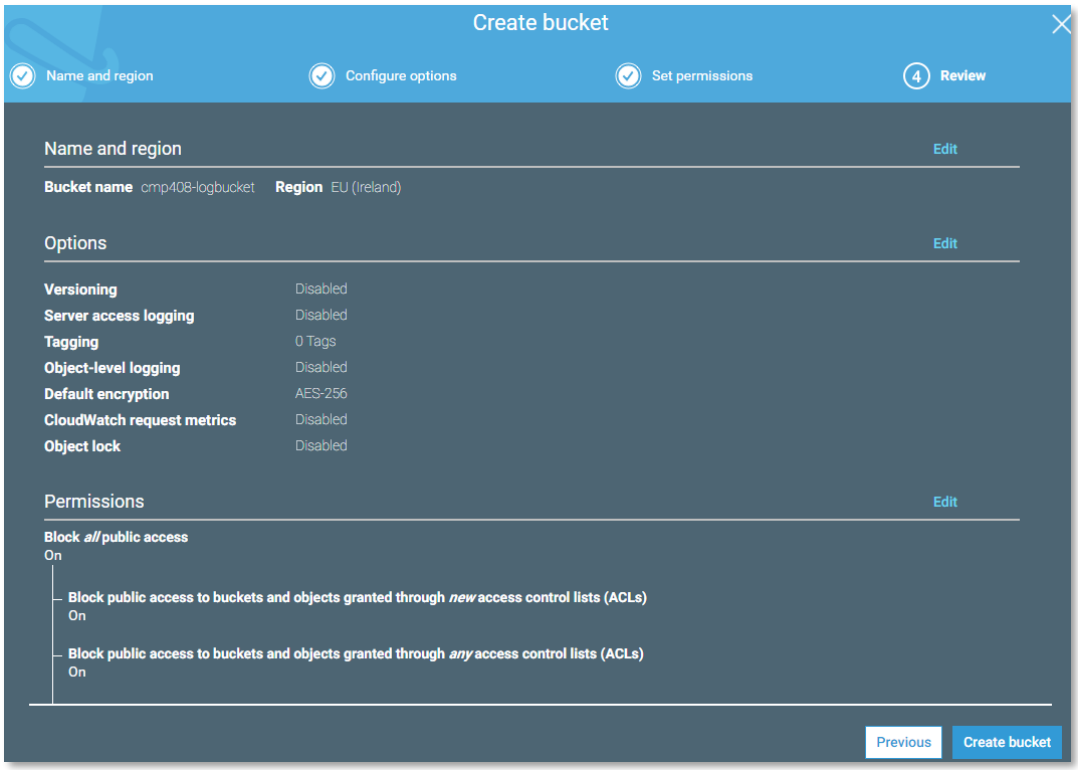

Figure 6 S3 bucket for storing access attempt logs.

Other security practices that should be followed for the AWS account, is to make sure all five categories are checked in the security status dashboard.

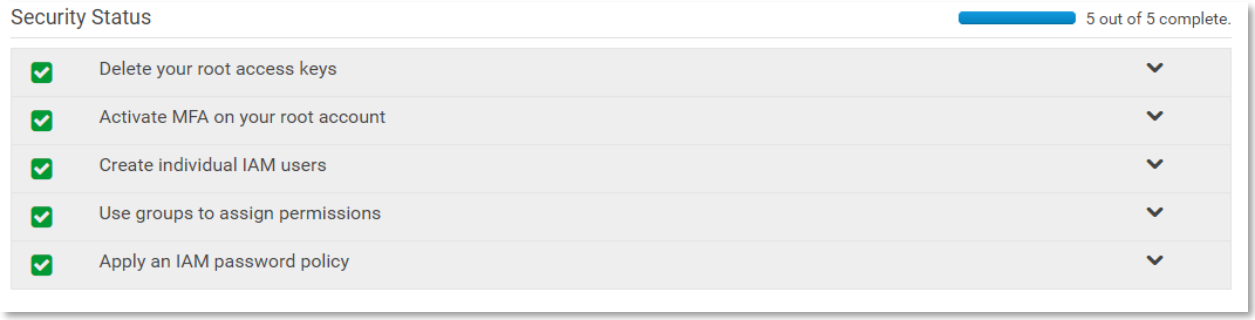

Figure 7 Utilising security best practices.

2.3 USING THE SCANNER

To use the scanner, the user visits the IP address of the RPi and is presented with an easy to use responsive interface. The user can then give the scan a descriptive name and input the IP address that they want to scan. They can then select several different scan options, customise the port ranges and finally select how aggressively the scan is run.

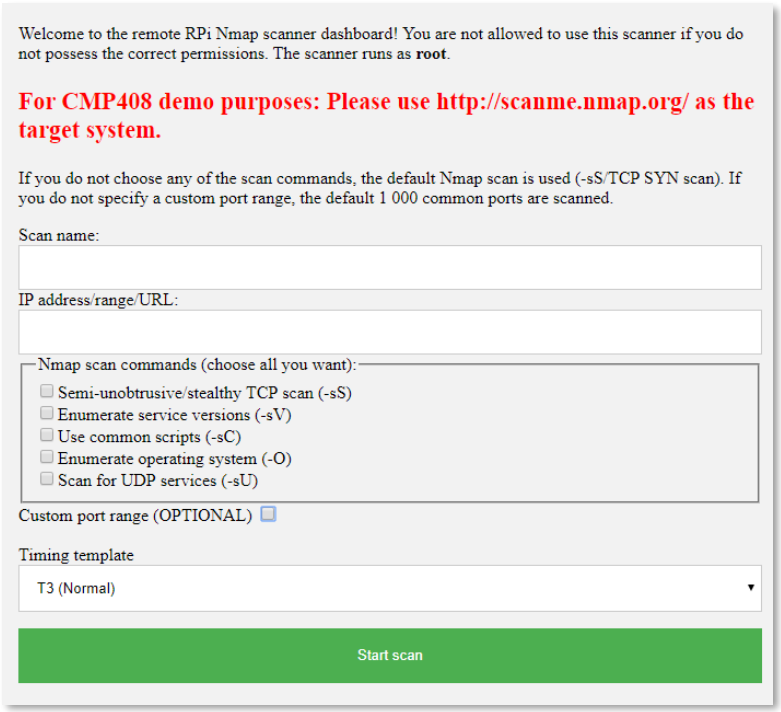

Figure 8 Web UI for the scanner.

During the whole process (scan-upload-done) different LEDs light up to indicate progress. After the yellow LED turns off, the scan results can be read from the bucket using the appropriate user.

3 CONCLUSION

3.1 CONCLUSION

By utilising a cheap single-board computer like the Raspberry Pi as a mobile server and integrating it with a cloud service like AWS, it is quite easy to provide an affordable basic cyber security scanner solution to a company with a low budget and little technical knowledge. The presented solution needs very little modification or setting up from the client, if any at all, and the simple web interface allows them to easily launch different kinds of scans.

The proposed solution meets all of the aims of the product but does have parts that can be improved or extended. The current solution utilises suboptimal ways to interact with the Raspberry Pi (shell_exec/sleep), and although they are fine for a development sample, best practices should be followed if the product is ever meant to be used in a live production environment.

3.2 FUTURE WORK

This solution can be extended further by using a port forwarding service (Raspberry Pi, no date) that would allow the external cyber security company to connect to the RPi which is connected to the clients' local network. However, when implementing such a feature, dashboard authentication and other security concerns need to be addressed very carefully as otherwise a malicious actor can gain an access point into the clients' network by exploiting the RPi.

The web UI could also be extended by adding a section for listing all the finished scans and being able to display them. To accomplish this, the RPi user needs to be given more permissions as the current AWS policy only allows file uploads.

REFERENCES

AWS (2019) *How can I secure the files in my Amazon S3 bucket?* Available at: https://aws.amazon.com/premiumsupport/knowledge-center/secure-s3-resources/ (Accessed: 10 December 2019).

AWS (no date) *How Do I Create an S3 Bucket?* Available at: https://docs.aws.amazon.com/AmazonS3/latest/user-guide/create-bucket.html (Accessed: 10 December 2019).

AWS (no date) *Install the AWS CLI version 1 on Linux*. Available at: https://docs.aws.amazon.com/cli/latest/userguide/install-linux.html (Accessed: 9 December 2019).

Darian Cabot (2017) *AWS S3 UPLOADING AND DOWNLOADING FROM LINUX COMMAND LINE*. Available at: https://dariancabot.com/2017/05/07/aws-s3-uploading-and-downloading-from-linux-command-line/ (Accessed: 9 December 2019).

Ekku Jokinen (2019) *CMP408 assessment 2*. Available on request.

Raspberry Pi (no date) *Access your Raspberry Pi over the internet*. Available at: https://www.raspberrypi.org/documentation/remote-access/access-over-Internet/ (Accessed: 11 December 2019).

StackExchange (2013) *allow sudo to another user without password*. Available at: https://apple.stackexchange.com/questions/82438/allow-sudo-to-another-user-without-password#82527 (Accessed: 11 December 2019).