IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101257

# A RASPBERRY PI NETWORK SCANNER & CLOUD STORAGE

**Timothy Sewe Ogode[1], M. Bhavana[2], P. Ananya[3], Dr. Vijay Kumar[4]**

Department of Computer Science and Engineering, FET- Jain University Bangalore, Karnataka, India[1-4]

**Abstract: -** Users benefit from the rapid expansion of computer network systems, but they will also face new security threats. The problem of network security encompasses both network system and data security. Tools and techniques are used to scan the network and its devices for vulnerabilities during network scanning and vulnerability testing. Due to the identification of weaknesses, this aids in the refinement of any organization's security policy. In this project we make use of the portability feature of a Raspberry Pi and configure it as a Network Scanner using Kismet Tool to be able to scan networks wherever possible given the permission. We further add an additional feature to the Raspberry such that the raspberry pi can act as a personal cloud storage. It's becoming increasingly popular to use online storage with personal cloud providers such as Dropbox, Google Drive, or Amazon Drive. With these services, users can store their files in a cloud. This can be accessed at any time, using nothing more than a computer or mobile device with internet access. However, it's not uncommon for users to raise concerns regarding the reliability of their cloud hosting provider. A common criticism is that customers don't know who else has access to the saved data, and whether the files are really removed from the server when they're deleted. This is particularly important when it comes to the storage of sensitive data. As the protection of your privacy becomes harder and harder, you may be thinking of moving your files to a private cloud storage and in this case, then this Raspberry Pi is perfect for such.

## 1. INTRODUCTION

In the United Kingdom, the Raspberry Pi Foundation collaborated with Broadcom to create a line of small single-board computers. The **Raspberry Pi project** was established to promote the teaching of fundamental computer science in schools and underdeveloped nations. For diagnostic and research reasons, a Network Scanner is a software application that discovers and categorises what devices are running on a network. The user typically enters a list of IP addresses to be scanned into the tool, and the scanner scans the list in order, determining if each IP address has an active device. Cloud storage is a type of computer data storage in which digital data is stored in logical pools known as "the cloud."A hosting business often owns and manages the physical environment, which consists of several servers (occasionally in different countries). These cloud storage providers are in charge of maintaining the data safe, secure, and operational, as well as the physical environment. All combined, this **Raspberry Pi Network Scanner & Cloud Storage** project will be demonstrating how one can utilize a software package called **Kismet** and **Owncloud** to improve on their basic home or office network security and security of their private data on cloud. The Network Scanner works with the Kismet software, uses your network interfaces, such as your Wi-Fi adapter and Bluetooth adapter, to scan for all accessible devices across all available frequencies. Kismet will read in device information and monitor their packet flow. It will also keep track of information such as the frequencies they use and other details. The Cloud storage utilizes Owncloud free file-hosting application that users can use to create a personal online data storage space, with access to their files via a web interface. However, you can also upload and download data and synchronize files over desktop clients and mobile apps.

## 2. LITERATURE SURVEY

By identifying active hosts on a network, Network Scanning helps to improve the infrastructure security of a network. Open internet give helpful channels through which attacker can bargain internal end-systems. Moreover, inner network clients can deliberately or unknowingly undermine the network and its end-systems through their movements. If there is possibility that one of the internal devices on the network is compromised, it can turn into a risk to whatever is left of the network. As a result, both the internet and intranet provide convenient avenues for attackers (both external and internal) to infiltrate end-systems. As a result, network security is critical in any firm. The following are some reviews of articles and related works that focus on the subject.

Kyle Coffey, Richard Smith and Helge Janicki's Vulnerability Analysis of Network Scanning on SCADA Systems. Industrial control systems (ICSs) and supervisory control and data acquisition (SCADA) have regulated and managed Critical National Infrastructure settings for decades. With the requirement to control and monitor remote facilities, companies have continued to incorporate Internet technology into their ICS and SCADA systems, allowing their operations to cross international borders and meet current living needs.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101257

Ashiqur Rahman, Kantibhusan Roy Kawshik, Atik Ahmed Sourav and Al-Amin Gaji's Advanced Network Scanning. Network scanning is a method of locating active hosts on a network, either for the purpose of attacking them or assessing network security. Ping sweeps and port scans, for example, reveal which IP addresses relate to real-world Internet hosts and what services they offer. Another scanning method is inverse mapping, which provides information on which IP addresses do not map to live hosts, allowing an attacker to make informed estimates about viable addresses. Scanning is one of three components of intelligence collection for an attacker. During the foot printing phase, the attacker creates a profile of the target organization's DNS and e-mail servers, as well as its IP address range. The majority of this material may be found on the internet.

## 3. MATERIALS & METHODOLOGY

Some of the materials/tools to be used in this are mentioned as follows.

A **Raspberry Pi chip or virtualized Raspberry Pi VM.** We will be using the Raspberry Pi gadget in this project. It may be used both physically and virtually. Because it is a "extremely portable" gadget, Raspberry comes in useful. It's about the same size as a deck of cards. This can be carried in our pockets or installed on/next to routers with ease. It can do everything a desktop computer does, including accessing the internet and watching high-definition video, as well as spreadsheets, word processing, and gaming. **Kismet**, since we rely on software that scans for all available devices across all accessible frequencies using network interfaces such as your Wi-Fi adapter and Bluetooth adapter. Kismet will read the devices' information and follow their packet travel. It will also keep track of information like the frequencies they use and other details. Kismet is a passive device, which sets it apart from other wireless network detectors. Without transmitting any loggable messages, it can detect the existence of both wireless access points and wireless clients and associate them with one another. It's also the most widely used and most up-to-date open-source wireless monitoring tool available. Basic wireless IDS features in Kismet include identifying active wireless sniffer applications, such as Net Stumbler, as well as a variety of wireless network assaults. Kismet has the ability to log all intercepted packets and store them in a format that is compatible with tcpdump/Wireshark or Airsnort. Kismet can also capture "Per-Packet Information" headers. A **wireless adapte**r is a network interface controller that connects to a wireless network like Wi-Fi or Bluetooth instead of a wired network like Token Ring or Ethernet. We won't be able to use the Raspberry Pi's built-in Wi-Fi for this project since it lacks the ability to be put into a "monitoring" mode. It is not Ethernet compatible. **Owncloud,** by using owncloud we will be able to host our own private storage on our Raspberry Pi machine which could be easily accessed only by us or users we provide with access. **Shell Scripting,** since we are using a Linux based operating system (Raspbian OS) we will make use of the shell scripting in the terminal. A shell script is a computer programme that runs on the Unix shell, which is a command-line interpreter.

**Network Scanner.**

Setting up the Raspberry Pi Network Scanner. First, we make sure that the Pi is up to date and upgraded via the terminal. Next, we'll check to see whether our wireless adapter supports network scanning. Let's examine if the wireless device we wish to use can handle the monitoring mode we require now that we know its physical address (iw phy phy0 info). We look for the portion marked as Supported interface in the result of the phy0 info command. modes: Under it also search for monitor. Finding it means our adapter can support monitor mode.

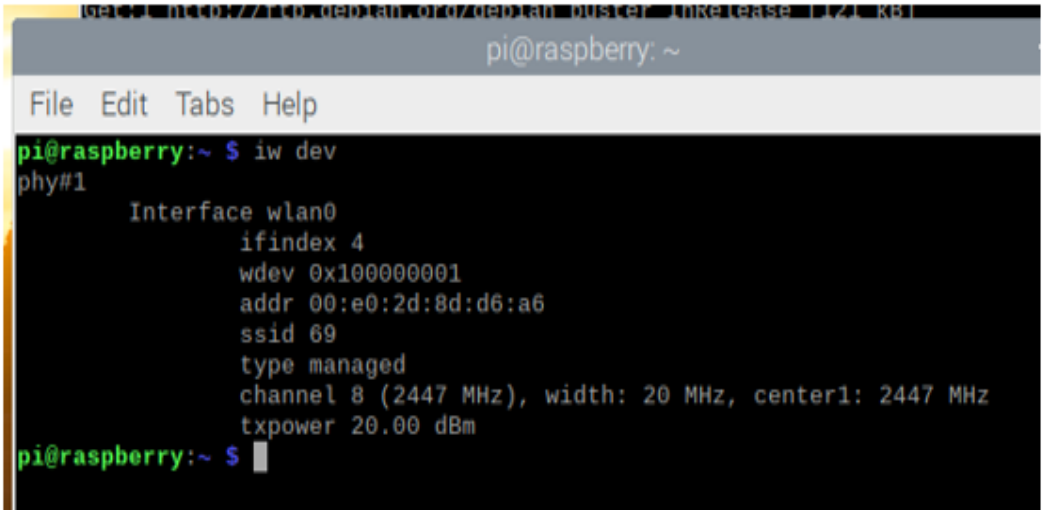



Figure 1. Identifying The Interface

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101257

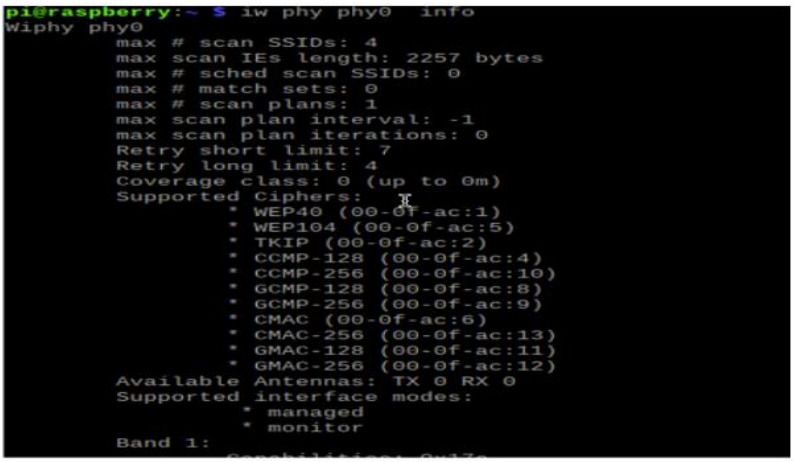



Figure 2. Checking for mon mode

Next step Prepare your wireless monitor for network scanning We need to modify our interfaces file by (sudo nano /etc/network/interfaces) and add some more lines to this file which will modify the wlan0 interface.

allow-hotplug wlan0
iface wlan0 inet manual
pre-up iw phy phy0 interface add mon1 type monitor
pre-up iw dev wlan1 del
pre-up ifconfig mon1 up

Save, exit and reboot the machine. After reboot type ifconfig. From this we should now be able to spot mon1. Now we are ready for monitoring a network. After setting all this we then proceed to install the monitoring tools packages. Here are the packages to download.

sudo apt-get install -y build-essential git libmicrohttpd-dev pkg-config zlib1g-dev
sudo apt-get install -y libnl-3-dev libnl-genl-3-dev libcap-dev libpcap-dev libncurses5-dev
sudo apt-get install -y libnm-dev libdw-dev libsqlite3- dev libprotobuf-dev libprotobuf-c-dev
sudo apt-get install -y protobuf-compiler protobuf-c- compiler libsensors4-dev
sudo apt-get install -y libusb-1.0-0-dev

To get kismet's source code from their official GitHub, we'll have to use GIT to ensure that we have a most recent version of Kismet software(git clone https://github.com/kismetwireless/kismet.git)

Now open a browser and input the ip address which loads kismet network scanner interface on the Raspberry Pi machine. (http://<ipaddress>:2501.).

You'll be asked to create a username and password when you first log in. Following that, you'll notice that the table has been updated to include all WIFI and Bluetooth devices detected by your adapter. By clicking on any gadget, you may learn more about it. We may also obtain the pcap files from a device (packet capture).

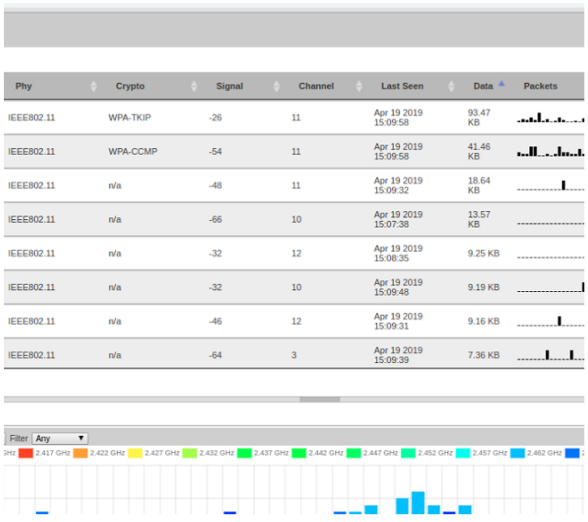



Figure 3. Network Scanning.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101257

**Cloud Storage**

As our first step we need to have both NGINX and PHP in our Raspberry Pi machine. The two will be helpful in running our Owncloud services. To start off the process we add www-data user to www-data group. These will help run Raspbian Buster Now we move on to installing packages that are needed to run Owncloud which are php7.3 and its modules. We then will be configuring NGINX to be compatible with Owncloud and also so that it can support HTTPS connections as well and also create an SSL certificate.

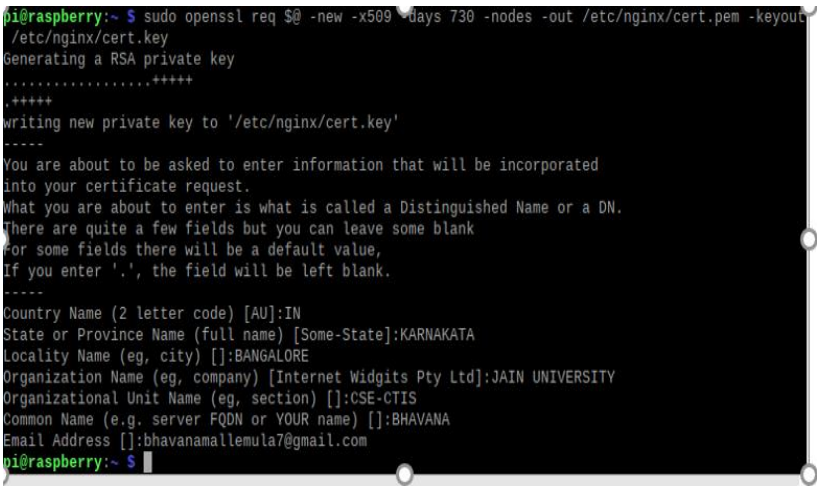



Figure 4. SSL Certificate

K We also must create a custom dhparam that will help ensure our SSL connections are kept Secure. We will generate a 2048 byte long dhparam then we'll chmod the three cert files we just generated and then configure the web server so it could run Owncloud smoothly. After setting up your SQL server, log in to your interface (sudo mysql -u root -p.) and configure your database as per your requirements.

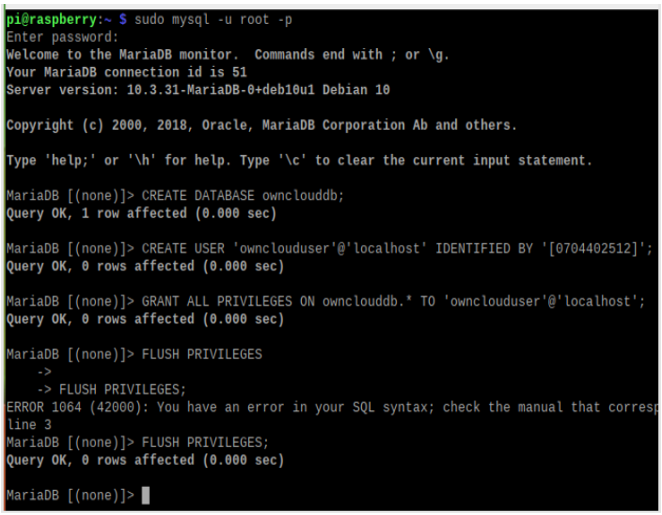



Figure 5. SQL Database.

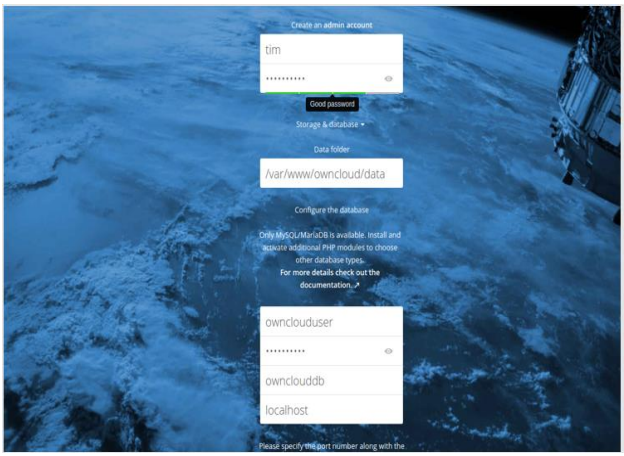
Reboot cd to /var/www/ then use wget to download owncloud and using Tar extract it. Ensure that www-data owns these files; sudo chown -R www-data:www-data /var/www. The update max file sizes to 2000M.; sudo nano /var/www/owncloud/.user.ini To access the cloud storage now using your browser go to your Pi's IP (hostname -I). As it is the first time opening owncloud you need to do your configurations now like username and password for admin. Now you can access your personal storage from anywhere.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Vol. 10, Issue 12, December 2021

DOI: 10.17148/IJARCCE.2021.101257




## 4. FUTURE SCOPE & CONCLUSION

Experts predict that by 2020, the cyber security business would be worth $170 billion. In the past, five years, Cyber Security specialists have earned more money than the average IT professional. And, to put it mildly, the average income disparity across the difference is 9%. The market for network security is always expanding, and new network security solutions are being embraced as servers become more virtualized. The massive increase in the usage of smartphones, as well as the growing demand for integrated security solutions, are predicted to propel the global network security system forward. Furthermore, the rise is projected to be fueled by a large increase in regulatory compliance needs. The requirement for good network security will increase as our reliance on the Internet develops. Breaches are far too common and the amount of consumer information sitting on servers is only growing. We need to be careful.

In conclusion, the basic function of a network is to enable access to sharing of data quickly and with as little user involvement as possible. The ability to do all this stems largely from connecting all the component parts together using wires and cables, then connecting workstations to distributed servers and fixed mainframes using networking devices and communications software. As the network became more widely accepted for doing internal business, there was a growing desire for faster, more seamless, and transparent communications for all users. The network scanner with all this feature is a handy tool that will help the administrator to get a clear understanding of the network. With features like bandwidth monitoring the administrator can trace the malicious usage of the bandwidth. The purpose of network scanning is to manage, maintain, and secure the system using data found by the scanner. Network scanning is used to recognize available network services, discover and recognize any filtering systems in place, look at what operating systems are in use, and to protect the network from attacks. The rapid proliferation of digital data brought with it the unprecedented risk of the most sensitive information ending up in the hands of the wrong people. As per our data privacy, we are not always 100% certain that our data is private via the cloud storage providers, hence when you own your own cloud storage that you could access from anywhere and have confidential files that you wouldn't want anyone to access, then this project would be of good help.

## 5. REFERENCES

1. C. Leckie and R. Kotagiri, "A probabilistic approach to detecting network scans," 2002, pp. 359- 372
2. M. de Vivo, E. Carrasco, G. Isern, and G. O. de Vivo, "A review of port scanning techniques,"
3. Alhawi, O.M.K., Baldwin, J., Dehghantanha, A., 2018. Leveraging machine learningtechniques for Windows ransomware network traffic detection. In:Dehghantanha, A., Conti, M., Dargahi
4. Aaron Wheeler, Michael Winburn, in Cloud Storage Security, 2015.
5. Ric Messier, in Collaboration with Cloud Computing, 2014
6. https://www.dictionary.com/browse/kismet#:~:text=Kismet%20means%20fate%20or%20destiny,why%20such%20a%20thing%20happened
7. https://www.kismetwireless.net/docs/readme/quickstart//
8. https://www.kismetwireless.net/docs/readme/starting_kismet/
9. https://www.linode.com/docs/guides/start-service-at-boot/
10. https://owncloud.com/