TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 9448 - 9453

Network Analysis Using Raspberry Pi

M. Sucharitha, M. Ch. Vamsi, B. V. Rakesh, Dr. N. Neelima

[1,2, 3] student, Information Technology, Velagapudi Ramakrishna Siddhartha Engineering College, A.P, India.
[4] Assistant Professor, Information technology, Velagapudi Ramakrishna Siddhartha Engineering College, A.P, India.

Article Info
Volume 83
Page Number: 9448 - 9453
Publication Issue:
May - June 2020

Article History
Article Received*: 19 November 2019*
Revised*: 27 January 2020*
Accepted*: 24 February 2020*
Publication*: 18 May 2020*

Abstract:
This paper states about the usage of Raspberry pi in which a network scanner is used to know about the hosts and networks connected and also used to perform the traffic analysis. For testing the network, these testing methodologies are implemented. The results of the performed tests are sent to the tester via mail. In context, we are going to develop our shell script in such a way that scanning results are sent automatically to the tester. By this tester can quickly know the network status as well as he can comfortably access the results.

Keywords*: Network scanner, Shell script, Python code.*

Introduction:

Penetration testing is a way in which we can test the network for security vulnerabilities. The penetration testing is used to test the web application or system for any vulnerabilities and report it to the particular owner. This testing is mainly crucial in every organization to control security theft. The penetration testing is mostly done by the penetration tester who is hired by the organization. Penetration testing comes under the field of ethical hacking.The penetration testing mainly focuses on the entry point of the particular system, to know the shortcomings in the network.[1]

Purpose of penetration testing:

The primary purpose of penetration testing is to find security breaches in anyorganization. Due to this security breaches, the organization may face data leakage, which is confidential and therefore result in company losses; hence many organization hires penetration testers to find the vulnerabilities. [1]

Penetration tester:

An infiltration analyser is a kind of system security advisor that attempts to break into or discoverpotential endeavours in various PC frameworks and programming. You can consider them a sort of moral programmer. They, by and large, are relied upon to run various tests, for the most part, based around arrange infiltration, and round out evaluation reports about what they have found. While they will frequently be running pre-decided kinds of tests, they will likewise be planning their own tests a huge bit of the time, which requires innovativeness and creative mind, alongside an eminent degree of specialized information and skill.[2].

Raspberry Pi:

The Raspberry Pi is an affordable computer that may lend itself to several light & medium-duty tasks.it's supported a Broadcom SOC (System on a Chip) that features an ARM7 core, a Video core iv GPU, and a USB controller. it's either 256MB or 512MB on the board and an SD card slot for storage.[3]

Network Security:

A specialized field in networking that involves securing a computer network infrastructure.Network security is usually handled by a network administrator or computer user who implements the protection policy, network software and hardware needed to shield a network and also the resources accessed through the system from unauthorized access and also make sure that employees have

May – June 2020
ISSN: 0193-4120 Page No. 9448 - 9453

adequate access to the network and resources to figure.[4]

II. LITERATURE SURVEY

A. Ethical Hacking and penetration testing using raspberrypi

In this the kali is booted into raspberry pi. ARM RPI light image is used for booting kali into raspberry pi. Kali depends on Debian; however, not at all like Debian, it's centered around crime scene investigation. Hence Kali preinstalls bundles necessary for legal sciences. Kali likewise effectively looks for bugs in crime scene investigation related packages. In this manner, Kali spares you from finding and introducing scientific bundles. It additionally keeps you educated about bugs in these bundles. Besides, it gives a network stage to those curious about crime scene investigation. [5]

B. WIRELESS SECURITY AUDIT AND PENETRATION TEST USING RASPBERRYPI.

Wireless networks are very convenient but have risksand
vulnerabilities. The hardware we use nowadays is getting very minute and very strong so in this Wi-Fi audit helps us. Wi-Fi auditor gives us a place for testing and reporting.

With the increase in wireless technology, we face the risk of security guidelines of the technology.

Though the Wi-Fi provides us with convenience, they also come with many vulnerabilities. The Wi-Fi acts as less space taking devices and also provides us with excellent ease; they have many security breaches. Therefore, in this case, they use the Wi-FI auditor to mitigate the problems.[6].

C. Analysis of Attack and Protection Systems in Wi-Fi Wireless Networks under the Linux OperatingSystem.

In Backtrack, there are remote systems assaulting apparatuses that go through orders executed by the assailant, however predominantly there are devices with agreeable UIs that encourage the assault procedure; that is the reason Fern Wi-Fi Cracker and Ettercap devices have been picked. Furthermore, in WLAN the aggressors mostly search for access to the system so as to acquire more up to date benefits and gets to or catch data that is of their advantage. By getting the secret phrase, the aggressor approaches the system and the licenses characterized by the system.

Being in correspondence permits the assailant to get to the trading data of an objective customer. To accomplish the activities referenced above, Fern Wi-Fi Cracker and Ettercap fit well [7].

D. Detecting Rogue Access Points UsingKismet

Kismet has the entirety of the highlights that you'd anticipate from an ordinary bundle channel. However, it likewise has numerous highlights that were explicitly intended for remote systems. The product is additionally intended to interpret WEP parcels on the fly as those bundles are caught. Essentially, individuals who *i*ntroduce a rebel passage with malignant purpose some of the time attempt to shroud the passageway's SSID. Kismet can retaliate against this method since it bolsters SSID [8].

E.Analysis and Impact of Vulnerability Assessment and Penetration Testing.

The fast increment of the apparatus, whether its versatile or PC frameworks have brought progressively advance and productive Windows, Web, and Mobile applications, yet it likewise expands the intricacy in structures which at last prompts vulnerabilities that aggressors use to misuse the casualty frameworks. In decades, the employments of web applications and web hacking exercises have been intensified quickly. In this day and age, associations and establishments end up in complicated circumstances for making sure about their framework and information from expanding vulnerabilities; that is the reason it is smarter to find and distinguish these vulnerabilities ahead of time before the assailant can misuse them. Hence defenselessness evaluation and entrance testing

May – June 2020
ISSN: 0193-4120 Page No. 9448 - 9453

methods cause it to decide if the game plans in making sure about framework are working appropriately or not by fixing those security holes. This paper will be on examining and investigating about existence pattern of VAPT procedure and VAPT instruments for discovering vulnerabilities in the framework. We will likewise center its significance at different authoritative levels for reception prerequisite of refreshing safety efforts so as to give insurance from various digital assaults.[9].

F. Penetration and Security of OpenSSH Remote Secure Shell Service on Raspberry Pi 2.

This exploration presents an infiltration testing approach to protect OpenSSH administration on Raspberry Pi 2. The examination talks about a method for entering Debian v7.1p2, introduced in Raspberry Pi 2, utilizing Kali Linux. We misuse the powerlessness found in SSH convention trade keys, because of which numerous CRLF infusions in Raspberry Pi 2 Model B, permitting remote verified clients to sidestep planned shell-order limitations through all around made X11 information sending. Here they propose an inventive security model to comprehend the issues of authorising remote confirmation to get to utilizing SSH convention trade keys without influencing the scrambled conventions transmissions. We finish up with proposals on the best way to safely moderate MITM assaults using our safe proposed model [10].

III. NEED FOR RASPBERRY PI

Penetration tester's role is to test the network by scanning. For that, the tester uses several tools to test, and report generation is to be done. It is a vast process. To reduce this by developing a script and creating a report and send the report to the tester mail can reduce the time and effort of the tester. The scanning of network and developing a script for that in a pc is not a great thing. So raspberry, which is a microcontroller, can also scan the network, and it is very cost-efficient as shown in Fig.1.

Fig. 1. Raspberry pi 3.

May – June 2020
ISSN: 0193-4120 Page No. 9448 - 9453

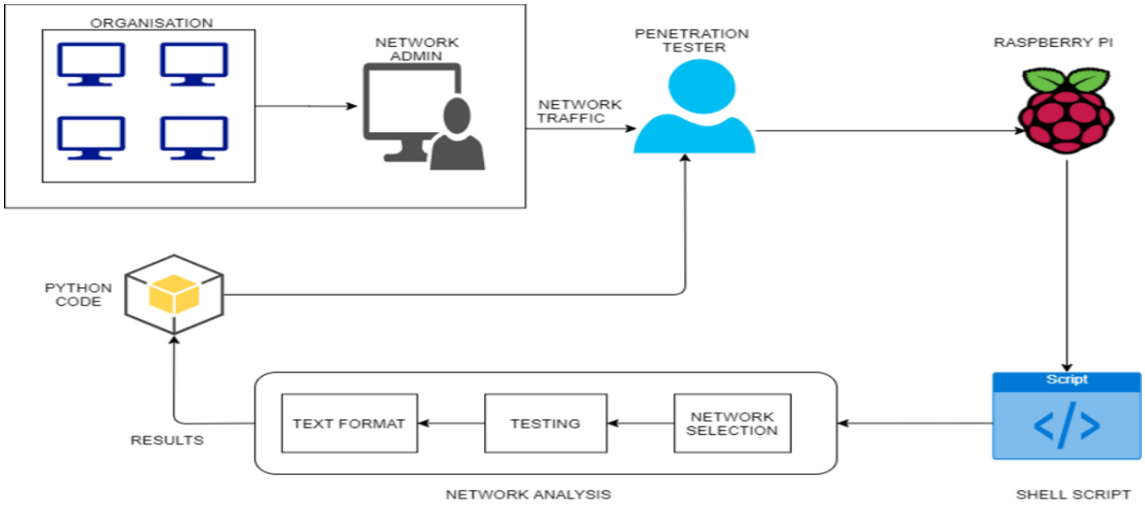


Fig.2. Architecture diagram

Architecture diagram:

As shown in the architecture diagram, a network admin can access the entire system in an organization. Pen tester takes access from the network admin and perform penetration testing. For that, he needs to execute the shell script. The execution process involves network selection, which means to which network testing is to do. The next step is network testing, which engages with the traffic monitoring. Later, results converted to text format. In the next level, a python code that contains the code to send the results to tester mail and submitting the reports to the particular organization, as shown in Fig.2.

IV. PROCEDURE

Firstly, when an organization offers a pen tester to test the network, the tester is to be ready at any time. So, firstly tester needs to set up with the requirements. The requirements setup and procedure are as shown below.

Etcher:

An etcher is an open-source tool that is used to send the .iso files to the storage devices like pen drives and Sd cards. Now, by using this tool, the operating system (kali) is dumped to the raspberry pi as shown in the Fig.3.

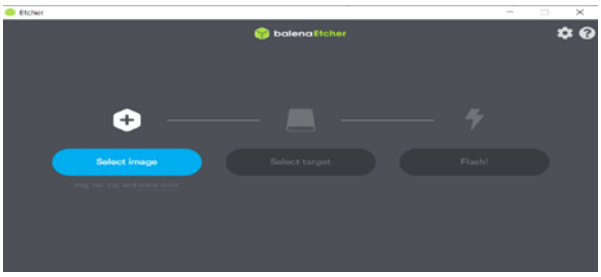


Fig. 3. Balena Etcher

VNC viewer:

A vnc viewer is a tool that establishes a connection between raspberry pi and our pc. It is one of the best tools because it contains a good GUI with a password protection feature. We can access the tool by entering the IP address of the specific device. The connection to VNC viewer is as shown in Fig.4

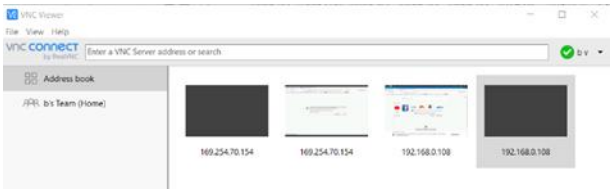


Fig.4.VNC Viewer

After connecting to VNC viewer, open the terminal and run the shell script as shown in the Fig.5.

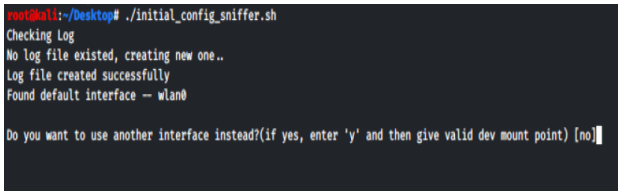


Fig.5. executing shell script

TEST Engineering & Management

May – June 2020
ISSN: 0193-4120 Page No. 9448 - 9453

After the execution, a message is displayed as "Do you want to use another interface instead? (if yes, enter 'y' and then give the valid dev mount point) [no]". Choose the option based on the requirement. And later, it will ask for the required network to monitor. For that choose the BSSID and channel number as shown in the below Fig.6.

Here BSSID means MAC address of the particular network and channel denotes the path at which data flows.

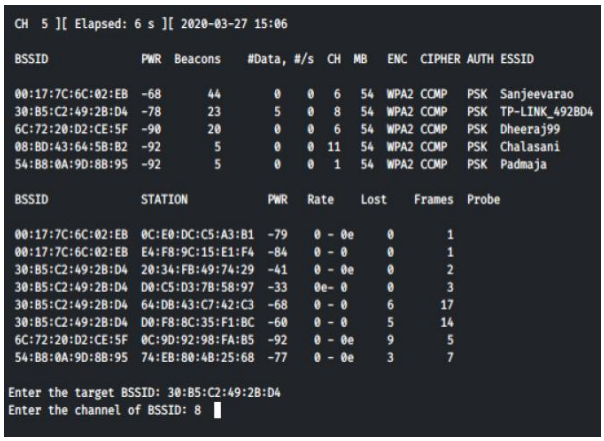


Fig.6. Monitoring mode

Now, a message is displayed as "Enter the number of packets to capture?". After entering the number of packets, the results are stored in text files automatically as shown in Fig.7.

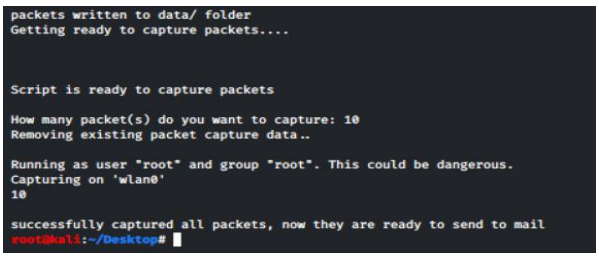


Fig.7. packet capturing

The script ends here, and now tester wants to execute the python file.

Python code:

Python code contains the mail credentials of the sender and the receiver. And also, the path for the text file i.e., the result file of the shell script. The execution of python code is as shown in Fig.8.

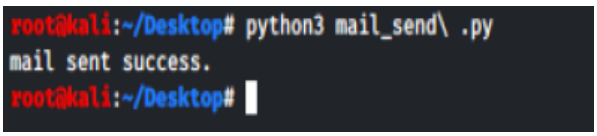


Fig.8.executing python code

Algorithm:

The algorithm describes the easy way to understand the procedure. So, the step by step procedure to test the network is as shown below.

1: Start shell script
2: Check dependencies, if there is error
    return{error}
3: Create logfile
4: Detect wireless interface and assign to INTR

    if found
        proceed to next step
    elseif
        prompt user to enter manual WIFI interface
    else
        return{error}

5: Start monitor mode on INTR, if there is error
    return{error}
6: Update INTR to monitor mode &start dumping nearby targets
7: Read BSSID
8: Read Channel
9: Create two directories as 'results' and 'data'
10: Set target network to BSSID and on Channel
    return captured packets to 'data' folder
11: Disable monitor mode, if there is error
    return{error}
12: Restart network manager
13: Check tshark, if there is error
    return {error}
14: Read packet count to capture
    do
        Capture all data traffic &save to 'results' directory

May – June 2020
ISSN: 0193-4120 Page No. 9448 - 9453

15: exit(script)
16: start python code
17: do
send mail to admin
else
return{error}
18: {error}: If any error, print ‘error occurred’ and exit with code ‘1’
else exit with code ‘0’
19: end ().

Output:

The first step is to start the testing. Then check for dependencies. If there is error call error function. Then create a logfile. After that, detect wireless interface and assign to INTR. If found proceed to step 5 or enter the interface, else call error function. Now read BSSID and channel. The next step is to create two directories as ‘results’ and ‘data’. Now, set target network to BSSID and on Channel and return captured packets to ‘data’ folder. The next step is disable monitor mode, if there is error call error function. Now restart network manager. After that, read the packets count and capture all data traffic &save to ‘results’ directory. The next step is to exit script. Now start python code, if there is error return the error function else display message “mail sent successfully”. Now end the python code.

V. RESULTS

The python code for sending mail is successful. Now tester can check the mail for the result as shown in Fig.9.

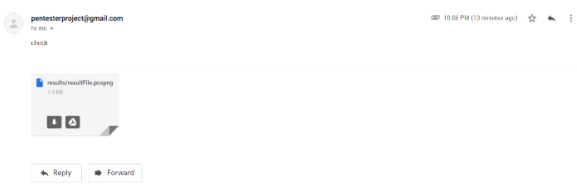
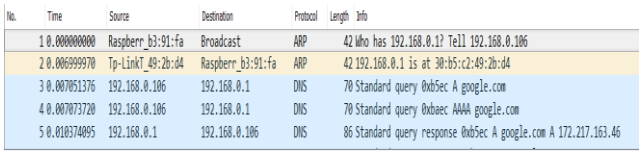


Fig.9.results file sent to mail

Now download the file and view the file the testing results are displayed in Fig.10.



No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000000	Raspberr_b3:91:fa	Broadcast	ARP	42	Who has 192.168.0.1? Tell 192.168.0.106
2	0.006999970	Tp-LinkT_49:2b:d4	Raspberr_b3:91:fa	ARP	42	192.168.0.1 is at 30:b5:c2:49:2b:d4
3	0.007051376	192.168.0.106	192.168.0.1	DNS	70	Standard query 0xb5ec A google.com
4	0.007073720	192.168.0.106	192.168.0.1	DNS	70	Standard query 0xbaec AAAA google.com
5	0.010374095	192.168.0.1	192.168.0.106	DNS	86	Standard query response 0xb5ec A google.com A 172.217.163.46

Fig.10. Result

CONCLUSION

Finally, it is a simple tool created using shell script and python to reduce the work of the pen tester. By this, the tester can generate the report and send it to the mail. Till now, scanning and packet analysis is done. Further developments were concentrating on adding more testing features and providing the graphical user interface to the tool.

REFERENCES

1. Margaret Rouse. (October 2018). SearchSecurity. https://searchsecurity.techtarget.com /definition/penetration-testing
2. Infosec. https://www.infosecinstitute.com/career-profiles/penetration-tester/
3. https://en.wikipedia.org/wiki/Raspberry_Pi
4. Josh Fruhlinger. (2018, July 15). CSO. https://www.csoonline.com/article/3285651/what-is-network-security-definition-methods-jobs-and-salaries.html
5. Ethical Hacking and penetration Testing using Raspberry pi, 2017.
6. Wireless Security Audit & Penetration Test using Raspberry Pi.
7. Detecting Rouge Access Points using Kismet, 2015.
8. Analysis of Attack and Protection Systems in Wi-Fi wireless Networks under the Linux Operating System., 2016.
9. Analysis and Impact of Vulnerability Assessment and penetration testing, 2019.
10. Penetration and Security of OpenSSH Remote Secure Shell Service on Raspberry Pi 2, 2018