International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume 4 Issue 6, September-October 2020 Available Online: www.ijtsrd.com e-ISSN: 2456 – 6470

Remotely Scanning Organization's Internal Network

Sharique Raza[1], Feon Jaison Maliyekkal[2], Nitin Choudhary[1]

[1]Master of Computer Application, [2]Assistant Professor,
[1,2]Jain University, Bengaluru, Karnataka, India

ABSTRACT

This project mainly focuses on remotely scanning the organization's internal network using precise, advanced and most efficient tools built/installed on the Raspberry Pi. Keeping all the security aspects in scope, this tool is built and configured to meet and protect one's required operations through the process. The whole scanning operation is done through the Secured Shell because it's open source and uses open protocol, so it's hard to plant a backdoor attack. The encryption will provide privacy and maintain integrity throughout the operation and will protect against network sniffers, eavesdropping and Man in the Middle Attack. This tool is made to completely eliminate the physical traveling of security team to the client's location and to perform any contractual based security operations.

KEYWORDS: *Network scanning, secured shell, Raspberry Pi, Nmap, Nikto*

How to cite this paper: Sharique Raza | Feon Jaison Maliyekkal | Nitin Choudhary "Remotely Scanning Organization's Internal Network" Published in International Journal of Trend in Scientific Research and Development (ijtsrd), ISSN: 2456-6470, Volume-4 | Issue-6, October 2020, pp.1139-1141, URL: www.ijtsrd.com/papers/ijtsrd33636.pdf

IJTSRD33636

INTRODUCTION

As the world is moving ahead in 21st Century, people are relying more on the internet and new networking technology. Because of the internet it is very easy to store our data in the cloud and access them by sitting anywhere in the world. Whenever there is a large amount of data, there is a risk of data getting hampered especially in transmission of data from a source to a destination. The transmission of data generally takes place through ports. Now there are 65,535 ports in a computer. A hacker can use any one of the ports to penetrate in the system and get access to the desired data. Network scanning is the initial step for gathering information about the network, as it provide the information about the open ports. As we all know that ports are like the doors and windows of our houses, therefore to avoid by kind of intrusion we must scan and secure those open ports on a regular basis.

In this project, I have developed a system that can scan an internal network remotely with the help of Raspberry Pi. Raspberry Pi is a small single chip CPU that increases the power of computing in the present scenario. It does not contain any external hardware like mouse, keyboard, etc. It just contains a processor of different clock rates. Due to its large functions, it can be used to access the remote systems for internal network scanning. This Raspberry Pi has been designed in such a way that any security tools can be embedded in it. In this project, I have used NMap for internal network scanning and Nikto for vulnerability scanning.

Motivation

In a crisis situation like covid-19, when the whole world was in complete lockdown everyone including schools and colleges shifted their mode of work from offline to online. Earlier the scanning of internal networks used to take place by physically travelling to the client's location and do all the required internal scanning which became impossible during this covid-19 situation. So to eliminate this problem and also avoid unnecessary travelling, this project comes into play. In this project, we scan any organizations internal network by sitting at home securely as all the scans will go through the secured shell port and without travelling to the client's place which ultimately reduces the overall cost of the operation.

Existing System

For internal network vulnerability scanning any third party hired/contractual based security team has to be on the client side physically to perform any required security operations, which unnecessarily increases the cost of internal scanning because of travel surcharges. Some penetration testing vendors will add a fee to help cover the cost of consultants while they are traveling to and from your location. At company's critical time like covid-19, Incident Response Team have to travel to the client location to carry out the virtual operations. Every scan returns a precise set of data about the vulnerable hosts. To get a fairly finish picture of targets for more precise analysis, it requires the combination of results from both the tools. The existing system has an issue of not generating a customized report and moreover it takes intensive time. These issues can be addressed in our proposed model.

Proposed System

The solution to the above existing problem is that we can use Raspberry pi as a mediator to access the client's system remotely. The proposed model provides the solution that reduces the travelling surcharge of the security team which eventually saves time. Some tools like OpenVAS takes a lot of time in vulnerability scanning which can be reduced by using the combination of two tools like Nikto and NMap.

- Eliminating the physical appearance of VAPT team
- Centralized system: considering only a single device for complete network scanning and provides complete package of advance vulnerability scanning tools.
- Less client's computer resources utilization.
- Generates very less internal traffic while performing the operations.
- Consistency: Provides the ability to install up-to date tools on demand and allows the team install any new scanning tools any time
- Makes use of SSH connection for entire operations.
- Transparency: As the device is now considered as a part of internal network that means the firewall or any installed security compliance soft-wares can keep the device's activity logs

Hardware Requirements –

- Minimum - 8GB RAM
- Hard Disk/Micro SD Card - 256 GB (min)
- Display and connectivity cable
  - HDMI/DIV interface for display
  - USB interface for keyboard
  - Power supply that can supply at least 3A at 5V

Architecture

As you can see here in the above diagram, the Raspberry Pi is located at the client's location and the security team is handling all the scanning operations requested by the client. As mentioned earlier all operations will go through a secured shell tunnel to avoid network sniffing and man in the middle attack as all the data will be encrypted by the secured shell.

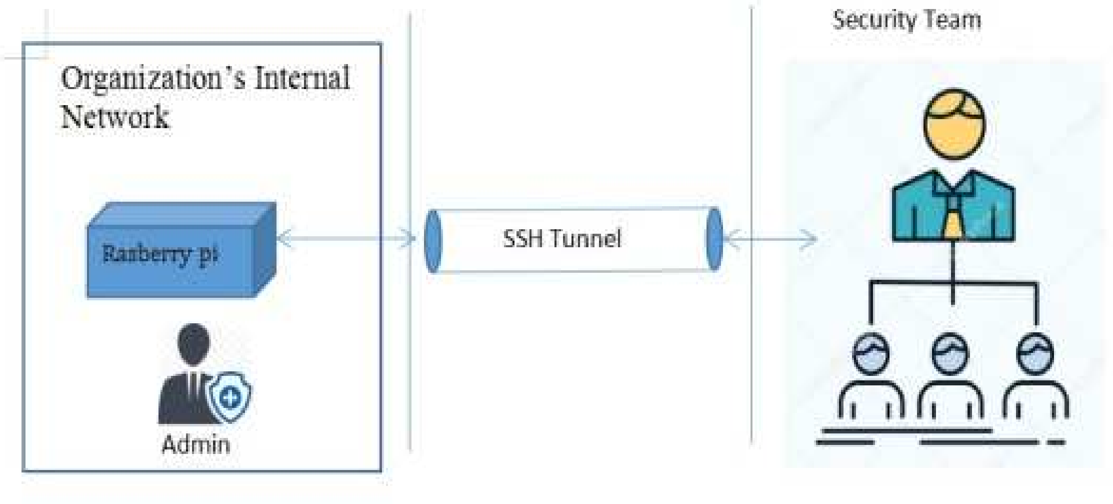


Diagram5.1. Visual Representation Overview

Working Mechanism

The device that will be located on organizations internal network is Rasberry Pi. It is well configured and it only makes use of wired connection on internal network (Version 1.0) to avoid any kind of man-in-the-middle attack on wireless connections (Resetting the 3-way handshake leads to disconnect any connected device). As it is built on Debian based Linux flavour introduces and holds the major security configuration as well as integrity throughout the operation. The Administrator from client's organization need to acknowledge the device's IP address back to the VAPT team. The VAPT team from other side need remote SSH connection client, which will connect to the device over the port 22.

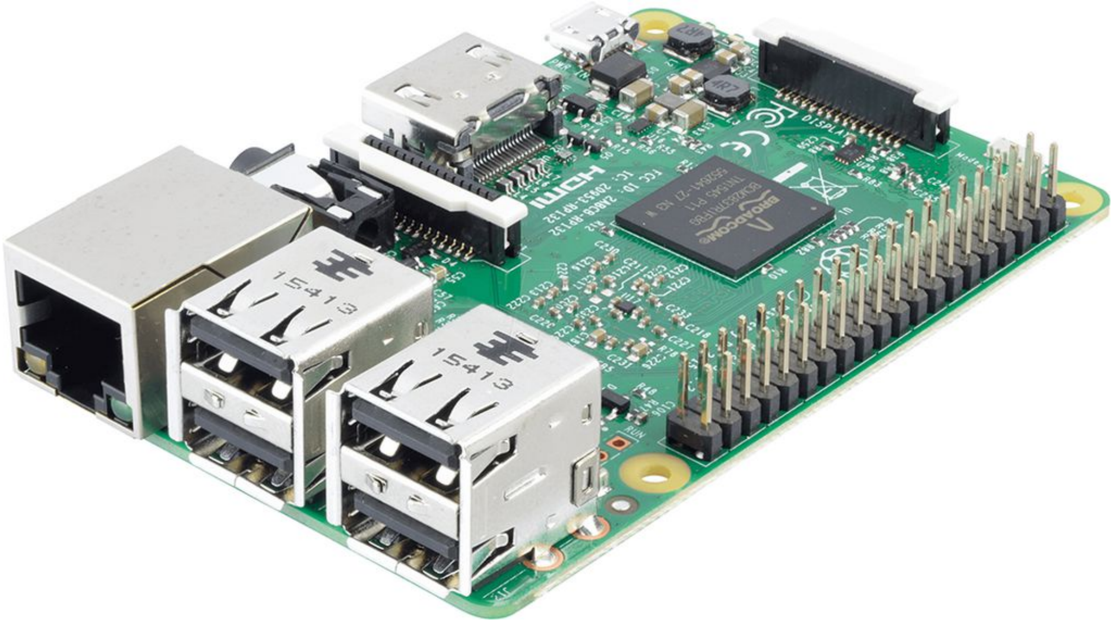
Configuration Process –

1. Before the tool's installation and configuration process begins, need to update and upgrade the operating system, as of now its running kali 2020.2
2. Create a temporary user account for client side administrative team to determine the device's IP address
3. We a SSH client software to connect to Raspberry Pi device when it arrives at client location. For that we can make use of any reliable tool, as of now we are making use of Putty 0.73.

Client Side Work

When Rasberry Pi arrives at the client location, few manual work should be done from administrator. In this first version 1.0, we are only making use of **eth0** interface connection.

- If some services running under ACL or some level of authentication, the administrative team from client location should send all the necessary credentials before beginning the operations.
- Administrator need to connect one of reliable LAN cable to this device
- After successfully connecting, admin should connect other I/O devices like Monitor and Keyboard.
- Now admin should access the temporary user account (credentials given by the VAPT team) and run **ifconfig** command to get the current device IP and send it back to VAPT team to carry out the operations as per the client's requirement.



Rasberry Pi 3

Conclusion

Scanning client's organizations internal network becomes really easy by using this methodology. After performing all the security and scanning operations finally the VAPT team gathers all the scanned details and generates a single precise VAPT report at the end. Here the report will be generated in the XML format. The XML file can later be converted to any desired file extension like HTML. And then the VAPT team can view the report in any browser like Google Chrome before they send it to the client.

Future Scope –

- Wlan support (Wireless connection).
- Automatic IP address acknowledgement to VAPT team.
- All enterprise addition vulnerability scanning tools at one place.
- Can clone any tool from GitHub to perform the required operation.

Acknowledgement

I would like to take this liberty to convey my respect and gratitude to my guide, Mrs. Feon Jaison, Honorable Assistant Professor MCA Department, Jain Deemed to be University Bangalore, for her precious time and valuable suggestions from the start till end. She has provided her constant guidance and support throughout the process. It gives me huge satisfaction in expressing my gratitude to Dr. Lakshmi JVN, Honorable project - Coordinator, MCA Department, Jain Deemed to be University, Bangalore for her extraordinary support continuous encouragement. An exceptional appreciation to Dr. MN Nachappa, Honorable Head of Department, Jain Deemed to be University for the motivation he has elongated during the course of this work.

During the preparation of this project my parents, Mr. Sultan Mahmood & Mrs. Jamila Sultan has been a permanent support. A special thanks to my loving brother Mr. Tarique Raza, who has always been an inspiration to me since my childhood. I don't have enough words to convey my appreciation. It is my duty to thank them enough for providing me the environment to study and possibilities to succeed.

References

[1] P. Zhang, J. Shang, and Z. Liang, "Application of Multi-Agent Model in Vulnerability Detection System", IEEE, First IEEE International Symposium, 2007.

[2] Golnaz Elahi, Eric Yu, and Nicola Zannone, "Security Risk Management by Qualitative Vulnerability Analysis", IEEE, Third International Workshop on Security Measurements and Metrics, 2011.

[3] Nilima R. Patil and Nitin N. Patil, April, 2012. "A comparative study of network vulnerability analysis using attack graph", in Proceedings of National Conference on Emerging Trends in Computer Technology (NCETCT-2012.

[4] Common Vulnerabilities and Exposures (CVE), https://cve.mitre.org, 15-03-2017.

[5] Nessus Open source vulnerability scanner project, http://en.wikipedia.org/wiki/Nessus (software), 10-07-2016.

[6] Peng Li and Baojiang Cui, December, 2010, "A Comparative Study on Software Vulnerability Static Analysis Techniques and Tools", in Proceedings of the IEEE International Conference on Information Theory and Information Security (ICITIS), IEEE International conference, 2010.

[7] Jhala, Nikita. (2014). Network Scanning & Vulnerability Assessment with Report Generation.

[8] R. Yadav, R. N. Verma and A. K. Solanki, "An Improved Model for Analysis of Host Network Vulnerability", International Journal of Computer Applications (IJCA), pp. 12-16, Vol. 148, No.13, August 2016.

[9] Open Vulnerability Assessment System (OpenVAS), http://www.openvas.org/about.html, 10-04-2017.

[10] Nikto Website Scanner, https://hackertarget.com/nikto-website-scanner.html, 19-09-2020.

[11] Vulnerability Scanners – SecTools Top Network Security Tools, https://sectools.org/tag/vuln-scanners/, 19-09-2020.