VAPT of Network, Network Connected Devices using Raspberry Pi & VNC Viewer

Dr. Bhoomi Gupta[1] Ashutosh Kumar Bharti[2] Harsh Bijarnia[3]
[1]Assistant Professor [2,3]Student
[2,3]Department of Information Technology
[1,2,3]MAIT, Rohini, New Delhi, India

Abstract— This paper reviews the general exploitation of unattended networks or network loosely configured. VAPT is employed to such networks to detect and exploit these networks. Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited. Penetration tests attempt to exploit the vulnerabilities in a system to determine whether unauthorized access or other malicious activity is possible and identify which flaws pose a threat to the application. . A penetration test is meant to show how damaging a flaw could be in a real attack rather than find every flaw in a system. Together, penetration testing and vulnerability assessment tools provide a detailed picture of the flaws that exist in an application and the risks associated with those flaws.

Key words: VAPT, Raspberry Pi, VNC, Network, Mobile Devices, Security, Flaws, Vulnerabilities, Kali Linux

I. INTRODUCTION

The information that is present around us in the form of electrical signals in a wire or packets in the air includes very critical and personal information which can lead to catastrophic results if misused by a third party. This interesting topic was chosen to shed some light on the vulnerability of the digital data around us, how it can be hacked and some basic security measures to encounter them. As stated, Vulnerability assessment tools discover which vulnerabilities are present, but they do not differentiate between flaws that can be exploited to cause damage. Penetration tests find exploitable flaws and measure the severity of each. Vulnerability Assessment and Penetration Testing (VAPT) provides enterprises with a more comprehensive application evaluation than any single test alone.. Vulnerabilities can be found in applications from third-party vendors and internally made software, but most of these flaws are easily fixed once found. Using a VAPT provider enables IT security teams to focus on mitigating critical vulnerabilities while the VAPT provider continues to discover and classify vulnerabilities.

A. Raspberry PI

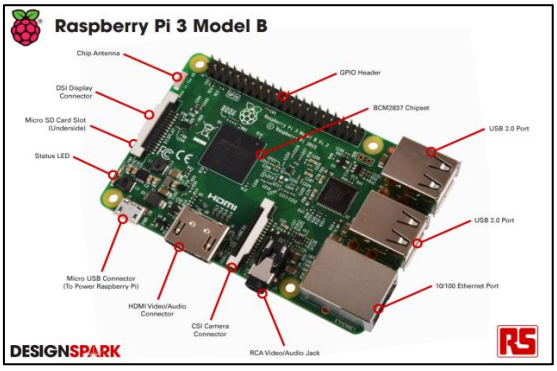

Fig. 1.1: Raspberry Pi 3B Labelled Diagram

As shown in the Fig 1.1 Raspberry Pi is a series of credit card-sized single-board computers developed in the United Kingdom by the Raspberry Pi Foundation. All models feature a Broadcom system on a chip (SoC), which includes an ARM compatible central processing unit (CPU) and an on chip graphics processing unit (GPU). CPU speed ranges from 700 MHz to 1.2 GHz for the Pi 3 and on board memory range from 256 MB to 1 GB RAM. Secure Digital SD cards are used to store the operating system and program memory in either the SDHC or Micro SDHC sizes. Most boards have between one and four USB slots, HDMI and composite video output, and a 3.5 mm phono jack for audio. Lower level output is provided by a number of GPIO pins which support common protocols like I²C. The B-models have an 8P8C Ethernet port and the Pi 3 has on board Wi-Fi 802.11n and Bluetooth.

B. MITM

In cryptography and computer security, a man-in-the-middle attack (MITM) is an attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of man-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones.

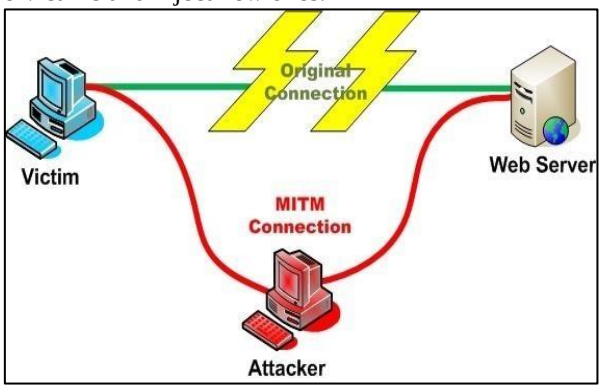

Fig. 1.2: MITM Attack

C. Need of the VAPT

Setting up or connecting to an unsecured Wi-Fi network connection may seem convenient, but that convenience comes at the cost of security. The risks are that much worse when using the connection for business purposes, considering the sensitivity of business data. Primarily, the risks of unsecured network have to do with data interception and network intrusion.

A major risk of connecting to an unsecured network connection comes from using services that require login information. Data transmitted over unsecured network can be intercepted by third parties. These third parties can extract your login information and passwords from this intercepted data and use it to fraudulently access your services. This can include online banking, email and other services that can be used to facilitate identity theft. If your company is operating an unsecured network, you also risk bandwidth theft. When others sign onto your network, the tasks they perform will consume a portion of the available bandwidth. Hosting unsecured network also endangers the data stored on your company's computers. Any unauthorized users will be able to access unsecured resources on your computer network, including the data on any connected computers. Without proper intrusion safeguards, sensitive corporate information can be stolen. Viruses and other malicious software can also be introduced to the network. That is why we would demonstrate how easily a network could be exploited and can be used illicitly.

II. PROCEDURE

As this project is based on VAPT hence the main objective of the project is hijack a network or exploit a loosely configured network. The approach is we create a hosted network, configure the raspberry pi to act as attacker. These are the following steps

1) Install Kali Linux in the Raspberry Pi 3B. This can be done by using downloading the ARM image of the Kali Linux and flash it to the Raspberry Pi.
2) After setting up Kali Linux, we setup a wireless adapter (TP LINK-722N) to work as an antenna to the Raspberry Pi. By executing the command "enable wlan0" in the shell of Kali.

Fig. 2.1: Raspberry Pi Setup

3) Setting the VNC viewer. Virtual Network Computing (VNC) is a graphical desktop sharing system that uses the Remote Frame Buffer protocol (RFB) to remotely control another computer. It transmits the keyboard and mouse events from one computer to another, relaying the graphical screen updates back in the other direction, over a network. We install the VNC viewer our android phone and configure it to accordingly to work with Raspberry Pi.
4) Setting up a victim.
5) Executing several commands to capture the capture the beacons and de-authenticate the connected device to host and capture those .cap files.
6) Executing attack by injecting payload in the network to crack the loosely set WPA hash pass obtained.

III. RESULT

The scripts were properly executed and the attack was successfully executed.

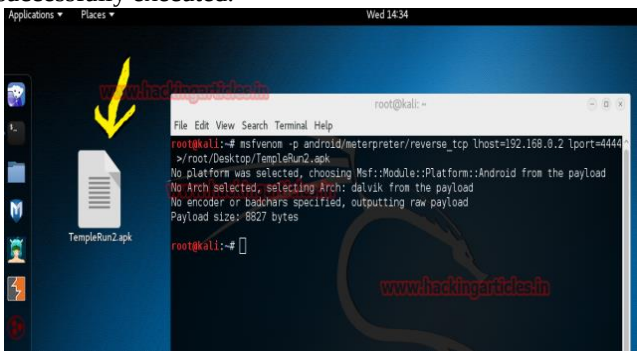

Fig. 3.1: Injecting Payload in the Network.

IV. CONCLUSION

The conclusions are as following

4.1) WPS has been such a security disaster. Since WPS is required for WiFi certification, it is present in all consumer routers. Thus it is best not to use WPS configuration security.

4.2) Default passwords are a huge problem for routers and should not be allowed. Even default passwords that look random are not. Eventually, someone figures out the formula for creating that password and can often use that, combined with public information from the router, to derive the password.

4.3) the router also needs to be protected from malicious web pages that exploit CSRF bugs.

4.4) although every router offers WPA2 encryption with Pre-Shared Key (PSK) there are still things to look for:

4.4.1) Verify that the router offers WPA2 exclusively. If the only option is a combination of WPA and WPA2, then it is not as secure as WPA2.

4.4.2) after opting for WPA2 encryption, a better router will always use AES or CCMP (two terms for the same thing).

4.4.3) some routers offer TKIP as an option with WPA2. TKIP is not as secure. Wi-Fi Analyzer on Android, to see if it is using AES.

ACKNOWLEDGMENT

We acknowledge the efforts and hard work by the experts who have contributed and guided us through the whole process. We take this opportunity to express our gratitude and deep regards to Dr. Bhoomi Gupta (Assistant Professor, IT Department) and Dr. M.L.Sharma (HOD, IT Department) for their constant monitoring and encouragement throughout the course of this project.

REFERENCES

[1] An Internet Of Things (Iot) Based Security Alert System Using Raspberry PI -Arun Raja, R. Naveedhab,

G.Niranjanadevic and V.Roobinid, Asia Pacific International Journal Of Engineering Science ,Vol. 02 (01) (2016).

[2] Banday, M.T., Qadri, J.A., Shah, N.A. (2009). "Study of Botnets and Their Threats to Internet Security,". Sprouts: Working Papers on Information Systems, 9(24).

[3] Brown, E. Top 10 hacker SBC's May 22, 2014 from: http://linuxgizmos.com/top-10/hacker-sbcs-survey-results/

[4] M.G. Williams, A Risk Assessment on Raspberry Pi using NIST Standards, IJCSNS International Journal of Computer Science and Network Security, VOL.15 No.6, June 2015.

[5] C.B. Westphall, "Challenges Towards Secure Internet of Things", IARIA SECURWARE 2014 - PANEL, Lisbon, Portugal, 2014, pp. 1-4 Jan 2015, sshttps://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project#tab=OWASP_Internet_of_Things_Top_10_for_2014

[6] Article title : Setting up Aircrack-ng from - https://nullbyte.wonderhowto.com/how-to/hack-wi-fi-getting-started-with-aircrack-ng-suite-wi-fi-hacking-tools-0147893/

[7] Setting up the payload (Meterpreter) from – https://www.offensive-security.com/metasploitunleashed/about-meterpreter/

