Network Auditing to Secure the Organization Using VAPT

Priyanka Revar[1], Dr.Ravi Sheth[2]

[1] Student, *School of Information Technology and Cyber Security, Raksha Shakti University, Lavad, Gandhinagar, Gujarat, India*

[2] *Assistant Professor, School of Information Technology and Cyber Security, Raksha Shakti University, Lavad, Gandhinagar, Gujarat, India*

***Abstract*- This paper describes Penetration Testing Tools and Approaches to finding the vulnerability of any organization Web Application or network. The paper contains the steps for Penetration Testing and how to secure the web application, organization or network. There are many tools are used for vulnerability finding and penetration testing. It contains the Approaches to provide the security solution for network and it's infra by finding the loopholes. Providing a Network diagram to overcome network traffic. These steps are used in penetration testing is Pre-engagement interaction, information gathering, vulnerability analysis, exploitation of Vulnerability, Reporting. This methodology is used to conduct the Penetration testing of web application and network Auditing. In this paper we are performing Network Audit and give the network solution by reconstructing the network before an attacker are used this vulnerability and exploits it.**

***Index terms*- Network Auditing, Vulnerability Assessment & Penetration Testing**

I.INTRODUCTION

Nowadays, everyone is using the internet so the complexity of the system is increasing day by day. That's why Vulnerability increasing in systems. Attackers use these vulnerabilities to exploit the victim's system. It is better to find out these vulnerabilities in advance before attackers do. The power of vulnerability assessment is usually underestimated. While Vulnerability Assessment and Penetration Testing can be used as a Cyber-defense technology to provide a proactive cyber defense. In this paper we proved Vulnerability Assessment and Penetration Testing (VAPT), how we can find an active vulnerability. Here is a complete life cycle of vulnerability assessment and penetration testing on system or network and proactive action taken to resolve that vulnerability and stop the possible attacks. In this paper we describe different tools and phases used in Penetration testing. Every organization has its own network infrastructure if it not has any loopholes then attackers use that way to enter the system and it may lose your data, any sensitive information, it may also perform the ransomware attack and encrypt your data it is needs to secure our organization safe and secure. Using some techniques we provide the network solution to secure the network.

What is Vulnerability Assessment & Penetration Testing?

VA- It is a process of identifying, Defining, prioritizing and classifying vulnerabilities in the computer system, applications and network infrastructures and providing the organization doing the assessment with the necessary knowledge, awareness and risk background to understand the threat to its environment and react and react appropriately

PT- Penetration Testing is also known as pen-testing. It is used to test the Computer, Web Application, mobile application, Network, finding vulnerability before Attacker use this vulnerability to exploit. Many Automatic tools are also available for pen testing and you can also test the application manually. The main goal of penetration testing is to find the vulnerability before any unauthorized user exploits it.

Phases of Penetration Testing

Pre-Engagement Action:

It is one of the phases of pen testing and it was the most important phase. In this pre-phase start with defining the test's scope. It contains the client outlines what they want to tested and by what methods and tools.

The Reconnaissance Phase

After the scope is complete the legal stuff is out of the way, the next is reconnaissance. In this Phase gather as much info about the subject as possible you can. The best option for information gathering is foot-printing.

The Threat Modeling & Vulnerability Identification Phase

After collecting all sufficient information about the client system, start the making to the modeling of threats that client-facing and identify vulnerabilities that will allow for those. It is before the attack phase in this phase you can get everything ready. And all that data you you collect using reconnaissance is pay off. You can start using scanning tools live hosts or port scanners to find open ports etc. There are also have some tools for vulnerability scanning or find possible vulnerabilities on the network.

The Exploitation Phase

You can begin to exploit those opportunities to gain access to systems.

Dependent upon the scope, you'll want to see just how far you can get. You can get a shell of a computer system, you can get credentials off the system, You can use it to pivot to another computer or server, Or you may try creating an admin account the goal of this phase to gain as high of administrator access as possible.

Post exploitation Phase

After the exploitation phase it is time to prepare a document which method you are using for the Exploiting vulnerability. Prepare a list of devices, tools, ports are used for exploiting the vulnerability. Keep a note and Screenshot especially of attack that worked.

Fig -1: Phases of Penetration Testing

Reporting Phase

It is the most important phase for penetration testing because in this phase you tell your client about their system weakness. After that give the suggestion for how to resolve the vulnerability. You should tell the client exactly what the exploits where you used to compromise their system as well as exactly what steps should be taken to remediate them.

The resolution & re-testing phase

All penetration tester is not doing this phase. In this phase After the specific time duration we are doing re-testing of vulnerability and check this vulnerability is resolve or not. Sometimes the client wants the penetration tester to assist in resolving the issue.

II. WHAT IS NETWORK AUDITING?

The network security audit is a process for checking network security. The process of investigating assets and customer's policies on the network and identify the loopholes that put customers at risk of a security breach.

We need to check the following assets in Auditing.

Device & Platform Identification: In the first step of network Auditing we identify the operating system they used, All the assets that used in the network. It is very important to identify any and all the threats

Security Policy Review: Where your documented policies the policy review, the architecture review step analyzes the actual controls and technologies that are in place. This platform identification process to give you an in-depth analysis of your cyber security measures.

Risk Assessment: In this step, the managed security provider perform a various assessment to characterize your system (process, application, and function), analyze the control environment and identify threats to determine what your risks are and what their potential impact is. This all information is then used to prioritize the fixes from the biggest threat that is easiest to remedy to the smallest threat that is the hardest to resolve.

Firewall Configuration Review: Network firewall is very important to review in-depth. In the firewall it needs to review the firewall's topology, rule-based analyses, configuration, and management processes/procedures.

Penetration Testing: The pen test is used to test the network security architecture, the tester tries to "break" the security architecture so they can find and resolve the previously-undiscovered issues.

Current network Design of Organization

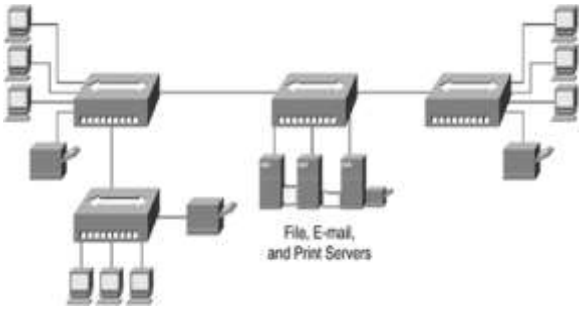

Fig -2: Current Network Design

Vulnerability Available in-network Design

After performing a Security Audit of overall IT Network design. This section details the findings of the security audit together with the gap.

III. FINDINGS VULNERABILITY IN NETWORK OF CLIENT

1 The network design does not have a core and access layer
2 The network design does not have L3 switch
3 L2 switches are running with the default configuration
4 Full network Subnet range are having access for firewalls and other network devices
5 Wide ranges of the subnet being used in the network
6 The Server resides in LAN Zone
7 The high amount of broadcast traffic processed by the firewall
8 IPV6 is enabled on the network
9 Local WIFI Authentication
10 Poor SSID key
11 A Firewall is set as DHCP server
12 No local DNS server available
13 NO BYOD policy

Consequences:

1 Unwanted network broadcast traffic and security issues
2 Unwanted network broadcast traffic and security issues
3 Unwanted network broadcast traffic and security issues
4 Core network devices can be compromised
5 A large amount of broadcast traffic in the network
6 Any user can access the server
7 Load on firewall
8 Unwanted IPV6 traffic available on the network
9 Wi-Fi can be compromised easily
10 Key can be compromised easily
11 Username can't be logged
12 The high amount of public DNS traffic
13 Security Threat

Business Impact

1 Poor network performance & lack of security
2 Poor network performance & lack of security
3 Poor network performance & lack of security
4 Core network devices can be compromised
5 Poor network performance & lack of security
6 Security & data breach threat
7 Poor firewall performance

8 Security & data breach threat
9 Security & data breach threat
10 Security & data breach threat
11 Security & data breach threat
12 Poor network performance & data breach threat
13 Security Threat

Recommendation:
There is a recommendation is to redesign the network as per the industry standard which should have a core & access layer. Define the proper zone at the firewall level and IP sub-netting. The server should be separated from the LAN zone.

Industrial Standard design for Network

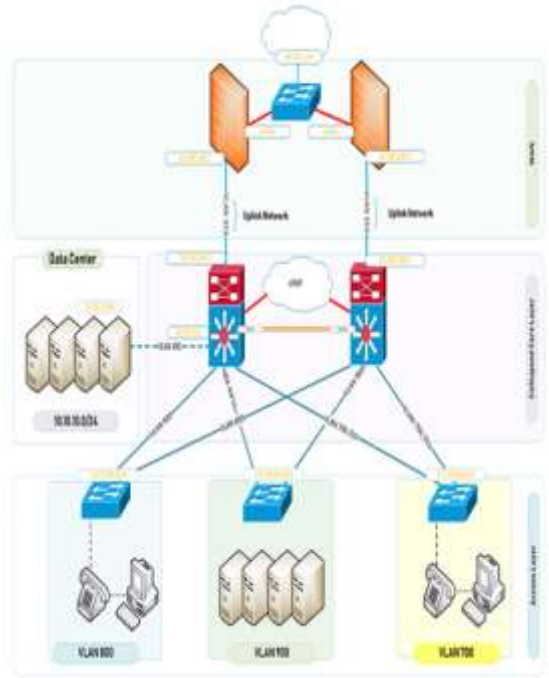

Fig -3: Standard Network Design

IV. TOOLS ARE USED TO FIND THE VULNERABILITIES

A. Network Scanning Tool
Nmap
Nmap is a network mapping tool specially used for scanning. It is used for port scan vulnerability scanning using script etc.

Command for port scanning
Nmap <HOSTNAME>
Command – namp www.rsu.ac.in

Fig -4: Nmap

B. Information Gathering tool
Webbackmachine
This Tool is used for information gathering about the organization

Fig -5: Web back machine

Dnsdumster
This tool is used to find domain server and IP addresses

Fig -6: Dns dumpster

C. Directory Scanning Using Dirbuster

This tool is used to find the directory of any website

Fig -7: Dirbuster

D. Vulnerability scanning tool

Nessus

Nessus Tool is used for the network scan, Network Scan, Advance scanning, malware scanning, etc

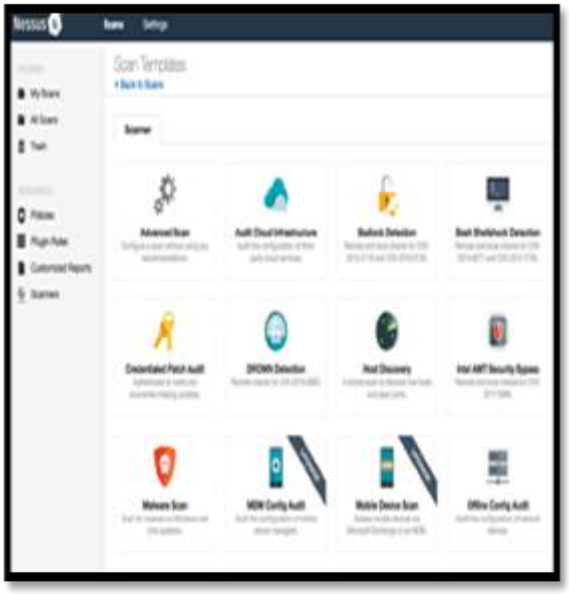

Fig -8: Nessus

VI. SOLUTION AFTER NETWORK AUDITING NETWORK DESIGN

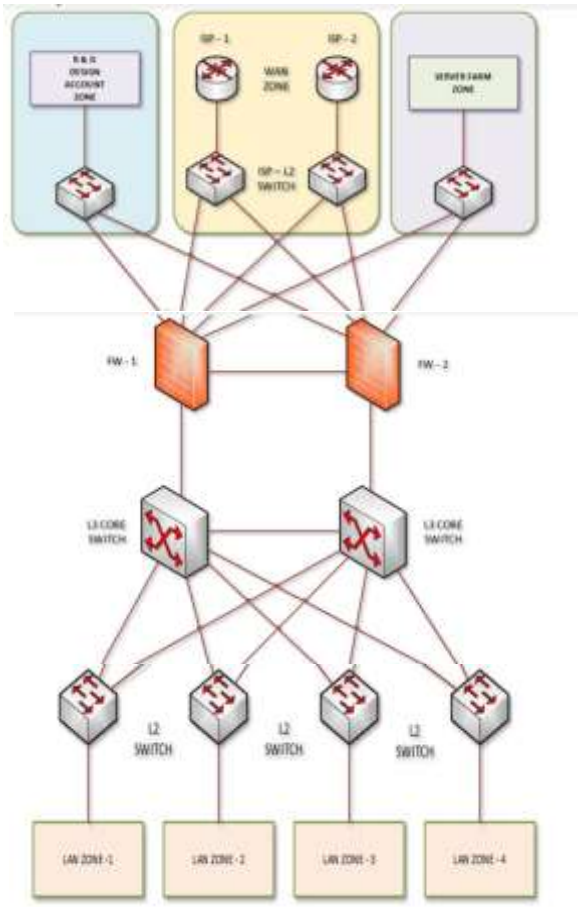

Fig -9: solve Network Design

VII. RESULT

This paper described after network auditing how we can find the vulnerability of any network using the VAPT and using different tool. Providing the solution for specific Vulnerability. For Network Design Vulnerability providing network diagram and reconstruct the network design

VII. CONCLUSIONS

Penetration testing is used to find the vulnerability of the system by using step by step process and exploit the vulnerability before any attacker. Various tools are used for penetration testing. Nmap is used to scan the network or host and check which port is open and which port is closed

Information gathering tool is used to find the information about the target which web server they are using, which language is used in developing the website, which is a public IP address, etc. In the

Network Auditing we are testing the organization network and find out vulnerability of system where attacker easily enter in your network and perform the malicious activity and harm your organization or network after that we provide the solution that problem and reconstruct the network design.

REFERENCES

[1] S. Angel,Dr.S.Sarala,(2011), A study on penetration testing, International Journal of Advanced Research in Computer science,2,396-398

[2] Aileen G. Bacudio, Xiaohong Yuan, Bei-Tseng Bill Chu, Monique Jones,(2011), An Overview of Penetration Testing, IJNSA,3,19-38.

[3] Pawan Kesharwani, Sudhanshu Shekhar Pandey, Vishal Dixit, Lokendra Kumar Tiwari (2018) A Study Of Penetration Testing Using Metasploit framework, IRJET,5,193-200

[4] Brandon F. Murphy,(2013) Network Penetration testing and Research, NASA. John F. Kennedy Space Center, Program USRP Summer.1-12.

[5] Konstantinos Xynos, Iain Sutherland, Huw Read, Emlyn Everitt and Andrew J.C. Blyth, (2010) Penetration Testing And Vulnerability Assessments: A Professional Approach, International Cyber Resilience conference,126-132.

[6] Neha Samant,(2011) AUTOMATED PENETRATION TESTING, San Jose State University SJSU ScholarWorks,180,1-63

[7] Jai Narayan Goela,b, BM Mehtreb, (2015), Vulnerability Assessment & Penetration Testing as a Cyber Defence Technology, 3rd International Conference on Recent Trends in Computing, 57 (2015) 710 – 715.

[8] Nagendran K, Adithyan A, Chethana R, IICamillus P, Bala Sri Varshini K B, (2019), Web Application Penetration Testing, International Journal of Innovative Technology and Exploring Engineering (IJITEE) 8,1029-1035.

[9] Muhammad Zunnurain Hussain, Muhammad Zulkifl Hasan, Muhammad Taimoor Aamer Chughtai, (2017), Penetration Testing In System Administration, INTERNATIONAL JOURNAL OF SCIENTIFIC & TECHNOLOGY RESEARCH, 6, 275-278.