International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

Network Security Auditing and Assurance

Urvashi Chauhan [1], Chandresh Parekh [2], Kaushal Bhavsar [3]
[1]*Post Graduation, Cyber Security, M. Tech, Raksha Shakti University, Ahmedabad, Gujarat, India*
[2]*Assistant Professor, Raksha Shakti University, Ahmedabad, Gujarat, India*
[3]*PhD Research Scholar at GLS school of research of innovation, Ahmedabad, Gujarat, India*

Abstract: ***Network auditing is done to analyze, study and gather data about a network. This paper includes mapping of both software and hardware. Information is gathered about what machines and devices are connected to the network, which operating systems are running and to what service pack/patch level. We analyze what user accounts and groups are on each machine, what policies affect that machine and whether it is a physical or a virtual machine. Study of ports of each machine which one is listening/active mode and what software is actually running at the time of the audit. Further which printers, fax machines, routers, access points, network storage and any other device that has connected with the network. The main aim was to scan all the devices which were present in the network and find the drawback and vulnerability which were present in it. After scanning and finding the vulnerabilities then the next step was to patch those devices. This helps in securing the devices which were present in those networks.***

Keywords: ***Auditing, Network operating system, Security of data, Information Security, Network Diagram, Network Scanning, Network Tools***

I. INTRODUCTION

With the rapid development of information technology, the Internet is changing at an alarming rate of people working and living. From government, business institutions to individuals, more and more people dependent on the Internet or access to information. When we enjoy the convenience of the network, while at the same time to encounter a variety of network security issues. Especially in the computer network has become a must-have facility for the development of the country, As the network security problems caused by the increasing loss, the network has become an important topic. At present, the main settlement of network security technology has taken a firewall, intrusion detection system(IDS), encryption applications, These measures has a certain effect to prevent the intrusion system, but in monitoring and dealing with the special needs of the users are powerless, such as monitoring network Internal users access external networks, to prevent disclosure of important information by users. As a result, network security audit (NSA) began widespread attention. Traditional network security audit system is an internal network user to monitor a variety of network behavior, such as restrictions on certain users browse the Internet site, open or close the SMTP, POP3, FTP, SSH, TELNET, DNS and other ports.

Network auditing is the collective measures done to analyze, study and gather data about a network with the purpose of ascertaining its health in accordance with the network/organization requirements. It is a process in which your network is mapped both in terms of software and hardware. The administrator needs to know what machines and devices are connected to the network.

Network auditing works through a systematic process where a computer network is analyzed for:

A. Security
B. Implementation of control
C. Availability
D. Management
E. Performance

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.177
Volume 7 Issue V, May 2019- Available at www.ijraset.com

II. NEED A NETWORK AUDI

1) *Inventory:* As organizations and their demands grow, mergers take place or devices passed from one operational team to another, so does the Network Devices may be added on the fly to the Network and at some point, administrators may be in the dark as to what is running on their Network enter Network Audit.
2) *Network Upgrade Refresh:* Like every other thing, there is a tendency for Networks to just fall into the operational state where administrators are concerned with the day-to-day running of such Networks. To keep up with demands, such Networks will need to be upgraded from time to time. Before upgrading, you will want to perform a Network Audit to know what is really going on in your Networks, which devices are still supported by the, which devices to replace, which ones to upgrade and so on.
3) *Problem Resolution:* I once had a client call me into their office to help resolve a problem, they were having with Internet access. This client wasn't technical say they had someone come in to help setup the Network and this individual was not accessible anymore. Before I could resolve the problem, I needed to first know what made up their Network and performing a Network Assessment was the way to go.
4) *Compliance:* Depending on the kind of business an organization is into, they may be required to comply with certain standards (e.g. PCI DSS). A Network Audit will be used both by the company (to prepare for the audit) and external auditors (to assess the compliance of the organization).

III. NETWORK AUDIT TOOLS

Network auditing tools is somewhat you use to audit the network and all its components: computers, servers, computer peripheral devices like printers and scanners and the network equipment: routers, hubs and other devices. There could be different software and hardware network auditing tools used for different purposes, but the main role plays the software tools. Different software tools implement different auditing tasks like Nmap, Nessus, Advanced IP scanner and more.

IV. NETWORK SCANNING

Network scanning refers to the use of a computer network to gather information regarding computing systems. Network scanning is mainly used for security assessment, system maintenance, and also for performing attacks by hackers.

A. Network scanning processes, like port scans and ping sweeps, return details about which IP addresses map to active live hosts and the type of services they provide. Another network scanning method known as inverse mapping gathers details about IP addresses that do not map to live hosts, which helps an attacker to focus on feasible addresses.

B. Network scanning is one of three important methods used by an attacker to gather information. During the footprint stage, the attacker makes a profile of the targeted organization. This includes data such as the organization's domain name system (DNS) and e-mail servers, in addition to its IP address range. During the scanning stage, the attacker discovers details about the specified IP addresses that could be accessed online, their system architecture, their OSs and the services running on every computer. During the enumeration stage, the attacker collects data, including routing tables, network user and group names, Simple Network Management Protocol (SNMP) data and so on. After all sorts of scanning, we have network devices like Firewall, Router, Switches, and more Devices.

V. NETWORK DIAGRAM

A network diagram is a visual representation of network architecture. It maps out the structure of a network with a variety of different symbols and line connections. It is the ideal way to share the layout of a network because the visual presentation makes it easier for users to understand how items are connected.

A network diagram demonstrates how one computer or system is affiliated with others. This is especially useful when trying to track down problems or when designing a new system. Often the root of a problem can be traced more easily by observing and analyzing how the computers and components in the system are connected.

Here, we have used EDraw Max tool for creating Network Diagram.

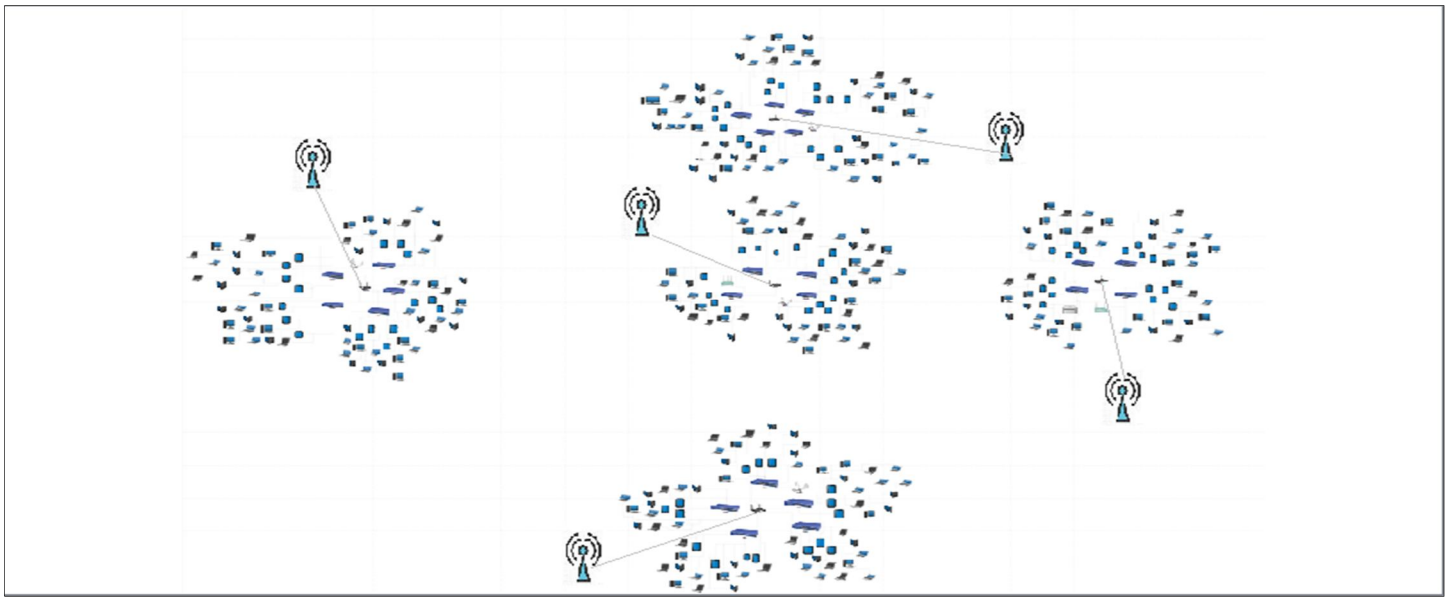

Fig 1 Network Diagram

VI. VULNERABILITY/TESTING

I found vulnerability in my network after scanning all those devices.

A. The first vulnerability found in switches. It is made from Aruba a Hewlett Packard enterprise company.
B. The second vulnerability found in SonicWALL Firewall and the vulnerability is slow Loris DOS attack.

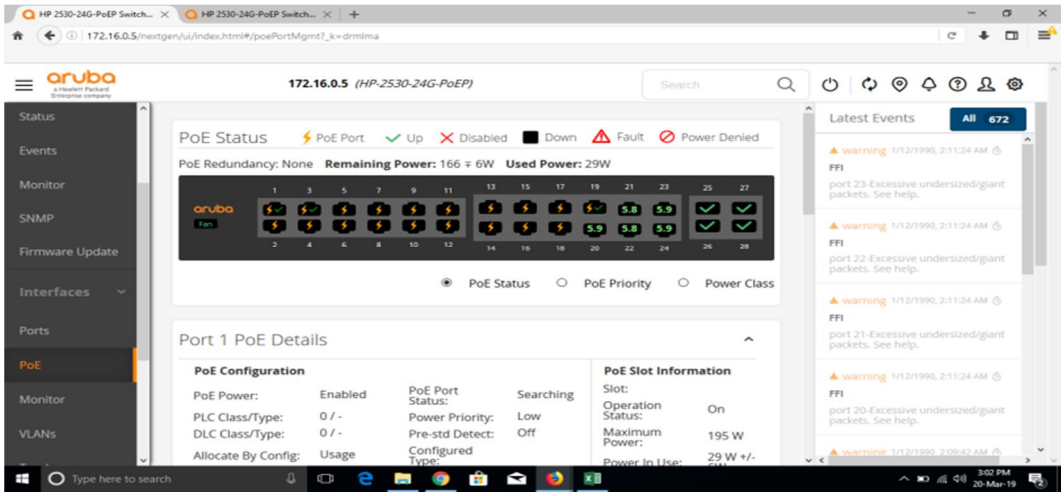

Fig 2 Vulnerability in Switch

VII. CONCLUSION

In this paper, I have provided and overview of security audit, described about scope of auditing, methodologies, techniques, process and literature covering design, issues and recommendation.

The paper provides purpose of auditing in an organization. The scope includes type of data and network to be protected, availability of time and experienced and expertise auditor. Also, purpose the phases and strategies of network auditing.

I succeeded doing a random network scan, visualizing a rough network diagram and ended up with finding vulnerabilities in that particular network.

In near future those vulnerabilities can be exploited. And further vulnerabilities can be found.

VIII. FUTURE WORK

In near future those vulnerabilities can be exploited and further more vulnerabilities can be found. Tools can also developed which allows user to scan a wider range of IPs at a time. Also tools like Nessus, nmap can be upgraded to add such features. With the evolving technology, new network tools can be designed and integrated.

REFERENCES

[1] J. Picciotto, "THE DESIGN OF AN effective auditing subsystem," 1987 IEEE Symposium on Security and
[2] Privacy, p. 10, 4 1987.
[3] J. Zhang, D. Fang and L. LIiu, "Intelligent content filtering model for network security audit system," *Knowledge Discovery and Data Mining, 2009. WKDD 2009. Second International Workshop on*, p. 3, 1 2009
[4] V. A. U. S. A. B. W. M. M. C. M. V. A. U. S. A. S.I. Schaen Mitre Corp., "Network auditing: issues and recommendations," Proceedings Seventh Annual Computer Security Applications Conference, p. 14, 12 2-6 Dec. 1991
[5] M. K. Franklin and D. Malkhi, "Method and apparatus for secure and auditable metering over a communications network," p. 14, 9 2000
[6] B. H. Smith and F. H. Smith, "System and method for installing an auditable secure network," p. 51, 3 2003.
[7] J. Depaolantonio, "Network audit tool," p. 24, 9 2005.
[8] D. A. Jury, S. Ali and J. Seigel, "Network change auditing system," p. 20, 8 2017.