NETWORK AUDITING IN PUBLIC AND PRIVATE NETWORK

[1] Urvashi Chauhan, [2] Chandresh Parekh

[1] Post Graduation, Cyber Security, M.Tech, Raksha Shakti University, Ahmedabad, Gujarat, India

[2] Assistant Professor, Raksha Shakti University, 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 gather like what machines and devices are connected to the network, which operating systems are running and to what service pack/patch level. We will analyze what user accounts and groups are on each machine as well as what shares are available and to whom, what hardware makes up 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.

Keywords: Auditing, Network operating system, Security of data, Information Security, Client/Server Approach, Distributed system.

I. INTRODUCTION

A security audit is a systematic evaluation of the security of a company's information system by measuring how well it conforms to a set of established criteria. A thorough audit typically assesses the security of the system's physical configuration and environment, software, information handling processes, and user practices. Security audits are often used to determine regulatory compliance, in the wake of legislation that specifies how organizations must deal with information.
Some of the purpose of audits is listed below:

- Build awareness of current practices and risks
- Reducing risk, by evaluating, planning and supplementing security efforts
- Strengthening controls including both automated and human
- Compliance with customer and regulatory requirements and expectations
- Building awareness and interaction between technology and business teams
- Improving overall IT governance in the organization

An information security audit is an audit on the level of information security in an organization. Within the broad scope of auditing information security there are multiple types of audits, multiple objectives for different audits, etc. Most commonly the controls being audited can be categorized to technical, physical and administrative.

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:

- Security
- Implementation of control
- Availability
- Management
- Performance

The data is gathered, vulnerabilities and threats are identified, and a formal audit report is sent to network administrators.
It is generally done by an information system auditor, network analyst/auditor or any other individual with a network management and/or security background. It uses both manual and automated techniques to gather data and review network posture. It reviews:

- Each node of a network
- Network control and security processes
- Network monitoring processes

- Other data

II. SCOPE

- **Inventory:** Determining what kind of devices were running on the network.
- **Support:** If any of those devices were obsolete.
- **Architecture:** How the devices were connected.
- **Security:** If there were any security concerns they needed to address.

The scope of the audit depends upon:

- Site business plan
- Type of data assets to be protected
- Importance of the data and relative priority
- Previous security incidents
- Time available
- Auditors experience and expertise

III. AUDIT METHODOLOGIES

There are two primary methods by which audits are performed. Start with the overall view of the corporate structure and drill down to the minutiae; or begin with a discovery process that builds up a view of the organization.
Audit methods may also be classified according to type of activity. These include three types:

- **Testing** – Pen tests and other testing methodologies are used to explore vulnerabilities. In other words, exercising one or more assessment objects to compare actual and expected behaviours.
- **Examination and Review** – This include reviewing policies, processes, logs, other documents, practices, briefings, situation handling, etc. In other words checking, inspecting, reviewing, observing, studying, or analysing assessment objects
- **Interviews and Discussion** – This involves group discussions, individual interviews, etc.

IV. AUDITING TECHNIQUES

There are various Auditing techniques used

1. Examination Techniques:

Examination techniques, generally conducted manually to evaluate systems, applications, networks, policies, and procedures to discover vulnerabilities. These techniques include:

- Documentation review
- Log review
- Rule set and system configuration review
- Network sniffing
- File integrity checking

2. Target Identification and Analysis Techniques:

Testing techniques generally performed using automated tools used to identify systems, ports, services, and potential vulnerabilities. They techniques include-

- Network discovery
- Network port and service identification
- Vulnerability scanning
- Wireless scanning
- Application security examination

AUDIT PROCESS

A successful audit will minimally:

- Establish a prioritized list of risks to an organization.
- Delineate a plan to alleviate those risks.
- Validate that the risks have been mitigated.
- Develop an ongoing process to minimize risk.
- Establish a cycle of reviews to validate the process on a perpetual basis.

VI. PHASES OF NETWORK AUDIT AND STRATEGIES

- **Pre-audit agreement stage**
  Agree scope and objective of the audit. Agree on the level of support that will be provided. Agree locations, duration and other parameters of the audit. Agree financial and other considerations. Confidentiality agreements and contracting have to be completed at this stage. Developing/creating a formal agreement to state the audit objectives, scope, and audit protocol.

- **Initiation and Planning stage**
  Conducting a preliminary review of the client's environment, mission, operations, polices, and practices. Performing risk assessments of client environment, data and technology resources; completing research of regulations, industry standards, practices, and issues. Reviewing current policies, controls, operations, and practices; Holding an Entrance Meeting to review the engagement memo, to request items from the client, schedule client resources, and to answer client questions. This will also include laying out the time line and specific methods to be used for the various activities.

- **Data collection and fieldwork (Test phase)**
  This stage is to accumulate and verify sufficient, competent, relevant, and useful evidence to reach a conclusion related to the audit objectives and to support audit findings and recommendations. During this phase, the auditor will conduct interviews; observe procedures and practices, perform automated and manual tests, and other tasks. Fieldwork activities may be performed at the client's worksite or at remote locations, depending on the nature of the audit.

- **Analysis**
  Analyses are performed after documentation of all evidence and data, to arrive at the audit findings and recommendations. Any inconsistencies or open issues are addressed at this time. The auditor may remain on-site during this phase to enable prompt resolution of questions and issues. At the end of this phase, the auditor will hold an Exit Meeting with the client to discuss findings and recommendations, address client questions, discuss corrective actions, and resolve any outstanding issues. A first draft of the findings and recommendations may be presented to the client during the exit meeting.

- **Reporting**
  Generally, the Information Security Audit Program will provide a draft audit report after completing field work and analysis. Based on client response if changes are required to the draft, the auditor may issue a second draft. Once the client is satisfied that the terms of the audit are complied with the final report will be issued with the auditor's findings and recommendations.

- **Follow-through**
  Depending on expectations and agreements the auditor will evaluate the effectiveness of the corrective action taken by the client, and, if necessary, advise the client on alternatives that may be utilized to achieve desired improvements. In larger, more complex audit situations, follow-up may be repeated several times as additional changes are initiated. Additional audits may be performed to ensure adequate implementation of recommendations. The level of risk and severity of the control weakness or vulnerability dictate the time allowed between the reporting phase and the follow-up phase.

VII. NEED A NETWORK AUDIT

- **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.

- **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.

- **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.

- **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. THREE PHASES/STAGES

1. Planning
2. Perform Audit
3. Post-Audit

1. **Planning A Network Audit:**

- Proper Preparation Prevents Poor Performance. This could not hold truer when performing a Network Audit. If you do not get this Planning phase properly
- things to consider during the Planning phase:

  - Do you have buy-in from all stakeholders?
  - Tools to be used
  - Access to the devices
  - What computer will you be using to perform the Network Audit?
  - Observation point

2. **Perform Audit:**

- It shows the performance of the network in the tool.
- Depending on the size, audits can take hours.
- With this basic information, your tool is ready to go to work discovering devices. Depending on the size of the network, your audit can take hours or in some cases, days. I once left my audit computer running all night at a client site because the tool was still working.

3. **Post Audit:**

- **Report:** You need to be able to make sense of all the information that you/your tool pulled up. Like I already mentioned, some of these tools can provide reports for you but you will probably need to present management with a special report that addresses the issues from a business angle, not from a technical point of view.

- **Recommendations:** This is where you highlight next steps. For ex, if you discover obsolete devices, you need to make a case for replacing those devices with newer models. Some of your recommendations can be carried out as "quick fixes". something that can be done immediately to improve the network. For example, during a performance assessment, I discovered that the interface on the router that terminates the ISP's link was faulty. We moved the link to a different interface and there was significant improvement on the client's network.

Access control	Accountability and audit	Application hosting	Application penetration
Application security	Application support	Application testing	Awareness and training
Business continuity	Certification, accreditation and security assessments	Computer assets, servers and storage networks	Configuration management
Content management	Contingency planning	Disaster recovery planning	Endpoints/edge devices
Identification, authentication and access management	Incident response	Infrastructure devices (e.g. routers, firewall services)	Intrusion detection/prevention
Maintenance	Media protection	Messaging	Networks (wired and wireless)
Personnel security	Physical and environmental protection	Risk assessment	Security incident management
Security of infrastructure	Security planning	Software	Storage devices
System and information integrity	System services and acquisition	Systems and communications protection	Third party security management
Web security			

fig. 1 requirement in audits

IX. LITERATURE REVIEW

In this paper dated **1987** titled **The Design Of An Effective Auditing Subsystem**[1], authors talks about the Design and Implementation of the CMW'S auditing Subsystem. This Auditing subsystem was developed in connect with other parts of total CMW project. In this paper the author has spoken about the CMW'S auditing subsystem and there exists anAuditing capability built into the UNIX operating system. Because this system was intended for accounting purpose only, it is far too limited to provide sufficient detailed audit trails to meet the CMW requirements.

In this paper dated **1991** titled **Network Auditing: Issues and Recommendations** [2], authors present their issues on network auditing. The issues are grouped according to collection and storage, integration, protection and analysis. In this, the information describes system activity, authorized users accesses, and unauthorized users attempted penetrations. A security audit trail is a set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to records and reports, and/or backwards from records and reports to their component source transactions.

In **2000** Franklin described how to secure and audit the network in the paper **Method AndApparatus For Secure And Auditable Metering Over Communications Network** [3]. The author mentions that a proxy module intercepts traffic between a client and a server.

The proxy module appends a metering module to the body of information sent from the server to the client. The metering module measures the duration of each visit using a timing function F and a unique Seed generated for each Visit. The metering module returns an auditable result when the client ends the Visit. A log keeper module is used to Store eachresult.

In this paper dated **2003** Titled **System And Method For Installing An Auditable Secure Network**[4], the authors Benjamin Hewitt and Smith present the idea of generating and remotely installing a private secure and auditable network is provided. Node identification, link, and application information is input into a template and a generator generates components using the information in it and the components are remotely installed using an installation Server.

In this paper dated **2005** titled **Network audit tool**[5], authors presents the idea of a method for performing a network audit. The network may comprise a number of different types of devices, each with multiple possible configurations. In one embodiment, each device is queried for its configuration.

In this paper dated **2017** titled **Network change auditing system**[6], authors described a network includes a workflow management system. A network is a workflow which includes management system coupled to an administrator device, and servers coupled to a user device. It receives and stores activity events from the servers that are associated with instructions from user devices to the servers. The network auditing system is associated with two subsets. A first activity event from an administrator device and, in response, provides an identification of the first workflow and at least one second activity event in the first subset of the activity events for display on the administrator deice. It is basically on information handling system.

In this paper dated **2009** titled **Intelligent Content Filtering Model for Network Security Audit System**[7], authors described network security audit system (NSAS) is system that pre control network behaviour for equipment, and later to provide direct electronic evidence and to prevent acts of disavower. It is an important part of the information security system to protect. This paper present a model of intelligent filtering through researching the current network security audit system and information filtering technology, and integrating the feature of network feature of network security audit system. It provides a good solution for content filtering. Network security audit system is composed of identify ,record and check, identification is to capture network packets ,and analyses packets based on their protocol.

X. 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 types of auditing and 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.

Indeed , I had provided just an outline of network auditing and scanned the network of our University

XI. FUTURE WORK

Based on the above observation we feel the need to work in create a secure network and scan the entire network. After this we analyze the entire network. After that we predict the issues in the network while auditing process goes on. Prevent the network after the solve the issues.

XII. REFERENCES

[1] J. Picciotto, "THE DESIGN OF AN EFFECTIVE AUDITING SUBSYSTEM," 1987 IEEE Symposium on Security and Privacy, p. 10, 4 1987.

[2] 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.

[3] M. K. Franklin and D. Malkhi, "Method and apparatus for secure and auditable metering over a communications network," p. 14, 9 2000.

[4] B. H. Smith and F. H. Smith, "System and method for installing an auditable secure network," p. 51, 3 2003.

[5] J. Depaolantonio, "Network audit tool," p. 24, 9 2005.

[6] D. A. Jury, S. Ali and J. Seigel, "Network change auditing system," p. 20, 8 2017.