World Applied Sciences Journal 29 (Computer Sciences, Engineering and Its Applications): 25-29, 2014
ISSN 1818-4952

DOI: 10.5829/idosi.wasj.2014.29.csea.2211

# IT Security and Audit

*R. Udayakumar, K.P. Thooyamani Khanaa and A.V. Allin Geo*

School of Computing Science, Bharath University, Chennai - 73, India

**Abstract:** Vulnerabilities in networked software create a risk of compromise of information security. Thus, the security of networked software components should be analyzed, preferably before they are deployed. This paper entitled "IT SECURITY AND AUDIT" is mainly related to data security, systems security, network security and web security. The goals of this paper are to identify the techniques and toolset to analyze the network attacks. In this paper we have identified tools that help in finding specific network vulnerabilities and critical operating points. Our user-friendly toolset with GUI includes monitoring and simulation based approaches, which is used to discover attack points (or vulnerabilities) and impact of faults along with attacks on network performance and services.

- A faster port scanner tool that is equally effective on all platforms, servers, routers and mainframes can be developed to scan the open ports and analyze the vulnerabilities in the network.
- A tool to monitor the network for the various services offered by the servers, routers, mainframes and network hosts can be developed.
- A graphical output can be simulated to depict the results of monitoring.

In general the objective of this paper is to identify the package that is useful in performing the first step of auditing an Enterprise network, port scanning to determine its depth of security and also to provide a choice of monitoring the network hosts.

**Key words:** Security · Auditing · Vulnerability · Scanning · Monitoring

## INTRODUCTION

**Security and Auditing:** Vulnerabilities in networked software create a risk of compromise of information security. Thus, the security of networked software components should be analyzed, preferably before they are deployed.

The process of independently verifying the results of security initiatives, is to ensure that all requirements are satisfied and validating whether the deliverables meet their security objectives to do this analysis. This can help to identify deficiencies in the security initiatives and help to correct weaknesses early by evaluating the company's security architecture, policies, procedures and implementation.

Monitoring tools monitor computers or networks for any unauthorized entry points, unauthorized file modification such as Session Hijacks and Service Denial Threats, monitoring network requests thus preventing Network Jamming attacks.

The best security procedures are of limited value if those procedures are not tested to ensure that they work properly. The system must be continuously monitored to ensure that procedures provide the level of security that is required. Testing security procedures and monitoring their effectiveness are the two aspects of auditing. Auditing is an essential element of an overall security policy. Without good auditing procedures, a system is left vulnerable to attacks.

**Corresponding Author:** R. Udayakumar, School of Computing Science, Bharath University, Chennai – 73, India.

One important part of auditing involves monitoring the system. This includes monitoring access to network resources (such as files), as well as monitoring specific actions by users. The auditing information is written to a security log and is known as logging. These security logs include information such as the identity of the user, the date and time of the action and what action to take place [1, 2].

In addition to monitoring, another important part of auditing involves scanning the system. Network and system security scanning will reveal the vulnerabilities of the current system. Scanning also provides the following benefits.

- Enables corrective action to take place in a timely fashion.
- Reduces the risk of attacks.
- Avoids litigation from customers.
- Reduces performance problems.
- Qualifies for information protection insurance.
- Reveals upgrades needed for future expansion.

System scanning involves two procedures. First procedure uses well-known network and system assessment tools. This system scan gathers information about the system and network configuration to determine vulnerable entry points that a hacker could use to gain access. Secondly, system scanning uses Penetration Testing [3,4]. Tools (like port scanner) which are commonly used by hackers are used to simulate an actual intruder attack, but in a controlled and safe environment. System scanning tools are also referred as Security Vulnerability Assessment, Security Audit or Online Penetration Testing Tools. The audit gives the information on the tools used, the vulnerabilities scanned so far and the list of vulnerabilities under the risk level.

Audit usage is also a key part of auditing. Audit usage monitors the usage of the system and provides valuable information for future capacity planning. The information provided helps to determine whether investments in new applications provide a positive return by tracking when and how they are being used [5, 6].

**Port Scanners:** First of all, to build a complete auditing tool we need to be aware of any unauthorized activity on the network and the Web servers. Port scanners are used to footprint the environment and determine whether there are any doors left open to the intruders via the ports. These scanners detect rogue machines running on the server and the rouge servers running on the network. This is done by initiating TCP connections to the ports, using the specified IP address ranges and checking whether each port has an open connection or not.

We should specify only the ports that make sense for us on the target scan list. For example, we need not scan the entire range of 65,535 available ports, so limit the target range to the ones that concerns us the most (e.g., ports 80,8080,443 and 3128 are common Web-related service ports and various other well-known ports).

The port scanners will return a wealth of data. Some of them can identify the operating system running on a target machine or even retrieve the banner of a connected, but unauthorized server. However, the most useful information a scanner will produce for security purpose is the servers IP addresses, corresponding open ports and the corresponding vulnerabilities from the servers. With these three pieces of data, one can gain a big picture of understanding the Web-related activity on the network [7, 8].

**Vulnerability Analysis:**. In this connected world of Internet, a few malicious individuals may lead to major network security concerns for administrators. The recent denial of service attacks on many of the web's most popular sites makes this clearer than ever before. Many of these attacks generate large volumes of TCP/IP traffic. Commonly the targeted site may seem unavailable to the Internet because of the saturation of its network segment. Internally, however, the web servers may hardly seem to be affected by the attack.

The value of a computer's information determines its desirability as a target for hacking, but only in certain parts. Even valueless machines can serve as jumping-off sites for additional attacks once compromised, or be used to gather information about an ostensibly "private" network in preparation for a later intrusion. And of course, mischief is an endless source of motivation. Knowledge of what the network should look like is worthless unless regularly compared to the way it is. The term "network" is used here to refer to the sum of all networked computers, not to router and switch security, which is a completely different matter. "Securing the network," in this sense, means preventing remote users from gaining access to your machines.

**Monitoring Tools:** Monitoring models provide a lower-cost first-step approach to the traffic management for companies and service providers that need to understand their network congestion and application performance bottlenecks. These new models deliver all the traffic

classification, monitoring and robust reporting features of standard Net Enforcers. It also features Allot's intuitive, an award-winning graphical user interface. With full Layer 2-7 capabilities, these units provide tremendous depth and flexibility to analyze the traffic by user, department, protocol, application, time-of-day and a host of other metrics.

In most cases, users are alarmed to discover the depth and breadth of their congestion and network performance issues. Uncontrolled bandwidth usage, unapproved applications and protocols, Denial of Service (DoS) attacks, network-borne viruses and poor application performance are some of the problems that are easily pinpointed by Allot's monitoring solutions. Armed with this information, network managers can upgrade their units via a simple software license key to unlock the Allot's industry-leading traffic shaping and QoS capabilities and deploy these powerful capabilities from their existing hardware [11, 12].

"Traffic management is rapidly evolving from nice-to-have, to must-have status in most business-critical networks," said Udi Levin, Director of Marketing for Allot Communications. Most users reach that conclusion once they deploy the technology in monitoring mode and begin to understand the complexity and severity of their performance problems. Monitoring a system helps us to understand the traffic management problems and intelligently address those problems.

**Port Scanning with Vulnerability Listing:**

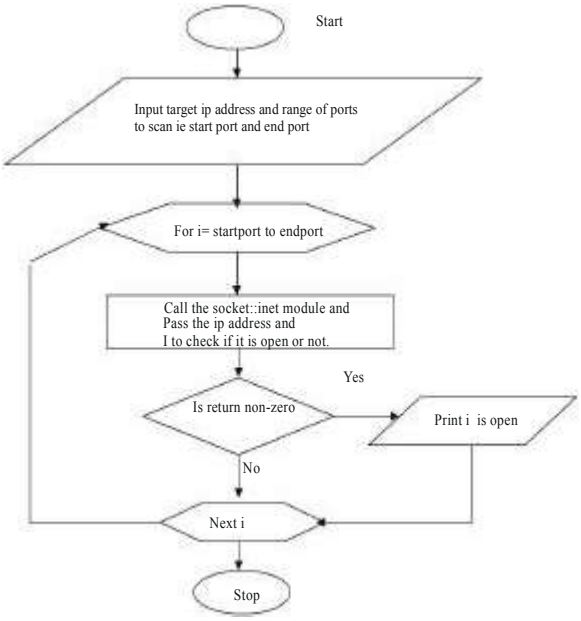


Fig. 1: Port scanning with vulnerability listing

**Well Known Ports - Scanning:** Port scanning is similar to a thief going through your neighborhood and checking every door and window on each house to see which ones are open and which ones are locked. Transmission control protocol and user datagram protocol are two of the protocols that make up the TCP/IP protocol suite, which is used universally to communicate on the Internet. Each of these has ports 0 through 65535 available.

The scanning can be limited for the first 1024 TCP ports which are called the well-known ports associated with standard services such as FTP, HTTP, SMTP or DNS. Some of the addresses over 1023 also have commonly associated services, but the majority of these ports is not associated with any service and is available for a program or application to use and to communicate [13,14].

**Auditing a Network:**

*Step 1*: The first step of performing an Audit is to develop a port scanning software, which in its most basic state, simply sends out a request to connect to the target computer on each port sequentially and makes a note of which ports responded or seem open. By setting different TCP flags or sending different types of TCP packets the port scan generate different results or locate open ports in different ways. A SYN scan will tell the port scanner which ports are listening and which is not, depending on the type of response generated. A FIN scan will generate a response from closed ports, but ports that are open and listening will not send a response, so the port scanner will be able to determine which ports are open and which are not. The INET module uses SYN scan and thus a return of "1" implies open port and a "0" implies closed port. We can monitor for SYN scans by logging any attempt to send a SYN packet to a port that is not open or listening.

*Step 2*: Once we find out what ports respond as being open by port scanning our own network, we can determine whether that particular port is actually necessary to be accessible from outside the network. If they are not necessary we should shut them down or block them.

*Step 3*: If they are necessary you can then begin researching what sorts of vulnerabilities and exploits that the network is open to, by having these ports accessible and work to apply the appropriate patches or mitigation to protect your network as much as possible [15].

**Cpu Utilization Monitoring with Gnuplot:** This module is to build the tool on Unix and GNU / Linux Systems.in Perl to do remote monitoring of CPU Utilization.

**Existing Tools in the Market:** Auditing Tools: Argus, Linux Security Auditing Tool (Lsat) Etc. Port Scanners: Nmap, Fscan And Superscan, Nessus, Wotweb Etc.

**Monitoring Tools:** Mrtg, Alertmobile, Acespy, Spyanywhere, Spyagent.

## CONCLUSION

The Port scanner tool is designed to scan only the wellknown port range of 0 to 1024. The audit is limited with scanning of ports and determining the associated vulnerabilities. The monitoring tool has been built using the concept of establishing the telnet session to a remote machine and running the vmstat command in that machine. This method itself may take a major amount of CPU Utilization if it is run continuously for a long time and so the data obtained will be slightly approximate. The monitoring tool mentioned will work and monitor only *IX platform supporting systems. This is because of the usage of vmstat command, which is Unix specific.

This is just an auditing tool, which is used to determine how securely a network's security has been established. It will only specify the open ports and its vulnerabilities. It does not specify any method to either detect the presence of an intruder or stop one from intruding.

## REFERENCES


1. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Application of Soft Computing Techniques in weather forecasting : Ann Approach, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1845-1850.
2. Tooyamani, K.P., V. Khanaa and R. dayakumar, 2013. Improving Web Information gathering for personalised ontology in user profiles, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1675-1679.
3 Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Detection of Material hardness using tactile sensor, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1713-1718
4. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Blue tooth broad casting server, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1707-1712.
5. Thooyamani, K.P., V. Khanaa and R. Udayakumar, 2013. Weed control system of tea garden using GIS based database Management system, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1702-1706.
6. Saravanan, T. and R. Udayakumar, 2013. Comparision of Different Digital Image watemarking techniques, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1684-1690.
7. Saravanan, T. and R. Udayakumar, 2013. Optimization of Machining Hybrid Metal matrix Composites using desirability analysis , Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1691-1697.
8. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. Images segmentation via Gradient watershed hierarchies and Fast region merging, Middle-East Journal of Scientific Research, ISSN:1990-9233, 15(12): 1680-1683.
9. Saravanan, T., V. Srinivasan and R. Udayakumar, 2013. A Approach for Visualization of Atherosclerosis in Coronary Artery, Middle-East Journal of Scientific Research, ISSN:1990-9233, 18(12): 1713-1717.
10. Saravanan, T., G. Saritha and R. Udayakumar, 2013. A Robust H-Infinity Two Degree of Freedom Control for Electro Magnetic Suspension System, Middle-East Journal of Scientific Research, ISSN:1990-9233, 18(12): 1827-1831.
11. Udayakumar, R., V. Khanna, T. Saravanan and G. Saritha, 2013. Retinal Image Analysis Using Curvelet Transform and Multistructure Elements Morphology by Reconstruction, Middle-East Journal of Scientific Research, ISSN:1990-9233, 16(12): 1798-1800.
12. Udayakumar, R., V. Khanna, T. Saravanan and G. Saritha, 2013. Cross Layer Optimization For Wireless Network (Wimax), Middle-East Journal of Scientific Research, ISSN:1990-9233, 16(12): 786-1789.
13. Udayakumar, R., A. Kumaravel and Rangarajan, 2013. Introducing an Efficient Programming Paradigm for Object-oriented Distributed Systems ,Indian Journal of Science and Technology, ISSN: 0974-6846, 6(5S): 4596-4603.

14. Udayakumar, R., V. Khanaa and K.P. Kaliyamurthie, 2013. Performance Analysis of Resilient FTTH Architecture with Protection Mechanism ,Indian Journal of Science and Technology, ISSN: 0974-6846, 6(6): 4737-4741.

15. Udayakumar, R., V. Khanaa and K.P. Kaliyamurthie, 2013. Optical Ring Architecture Performance Evaluation using ordinary receiver, Indian Journal of Science and Technology, ISSN: 0974-6846, 6(6): 4742-4747.