DOI: 10.21917/ijct.2013.0110

AN AUTOMATED NETWORK SECURITY CHECKING AND ALERT SYSTEM: A NEW FRAMEWORK

Vivek Kumar Yadav[1] and B.M. Mehtre[2]
[1]*University of Hyderabad, India*
E-mail: Vivekyadav1989@gmail.com
[2]*Institute for Development and Research in Banking Technology, Established by Reserve Bank of India, India*
E-mail: BMMehtre@idrbt.ac.in

Abstract
Network security checking is a vital process to assess and to identify weaknesses in network for management of security. Insecure entry points of a network provide attackers an easy target to access and compromise. Open ports of network components such as firewalls, gateways and end systems are analogues to open gates of a building through which any one can get into. Network scanning is performed to identify insecure entry points in the network components. To find out vulnerabilities on these points vulnerability assessment is performed. So security checking consists of both activities- network scanning as well as vulnerability assessment. A single tool used for the security checking may not give reliable results. This paper presents a framework for assessing the security of a network using multiple Network Scanning and Vulnerability Assessment tools. The proposed framework is an extension of the framework given by Jun Yoon and Wontae Sim [1] which performs vulnerability scanning only. The framework presented here adds network scanning, alerting and reporting system to their framework. Network scanning and vulnerability tools together complement each other and make it amenable for centralized control and management. The reporting system of framework sends an email to the network administrator which contains detailed report (as attachment) of security checking process. Alerting system sends a SMS message as an alert to the network administrator in case of severe threats found in the network. Initial results of the framework are encouraging and further work is in progress.

Keywords:
Security Assessment, Network Enumerator, Port Scans, OS Fingerprinting

1. INTRODUCTION

In this modern age of computers, most of the networks are connected to the internet for facilitating the network user to connect with any network and system on the internet. The public Internet is a world-wide computer network, i.e., a network that interconnects millions of computing devices throughout the world [7]. In this way Internet made this world a very small place due to worldwide connectivity of people. But as Internet is a public network, it is unsafe and insecure for the private networks to be connected with it. The private networks connected to internet and contain vulnerabilities, which can be dangerous and harmful for the owning organizations. Vulnerability means defect and deficiency that exist in the realization of the hardware, software and protocol or in the system security strategy of the computer system [9]. Attackers can exploit these vulnerabilities to compromise network components. The attackers may be from outside or inside of an organization. Network security checking is also known as network security assessment. It is a process of finding the weakness (vulnerability) of the network, which may be a threat for network security. It is basically an assessment process to get real status of the security of a network. Vulnerability assessment technology can detect potential security vulnerabilities and assess the security situation of network [10]. There are four basic phases to perform network assessment [6]. They are,

- *Reconnaisance* – Collecting basic andvaluable information about network such as domain names, individual contacts, IP addreses etc.
- *Network Scanning* – The network is scanned to identify live hosts, tracing routes and getting open ports and services on live hosts. This is also called Enumeration.
- *Vulnerability Assessment* – Based on the information obtained from network scanning this phase finds out vulnerabilities in the network components.
- *Exploitation* – Vulnerabilities found from vulnerability assessment phase are exploited to know about the effect of them on network. In this way this phase tells how much vulnerability is harmful for the network.

There are lots of commercial and freely available automated tools for network scanning and vulnerability assessment. One technique is not enough for assessment [2]. According to the prior research it is proved that no single assessment tool can give acceptable assessment result. So, these tools may use different techniques and may be applicable on different targets. So using multiple tools instead of one can be a better idea, as multiple tools can cover broader area of target domain and can be able to find sufficient number of vulnerabilities.

The framework basically contains two kinds of tools- Network Scanners and Vulnerability Scanners.

Network Scanner

Network scanning tools are used for scanning the network for discovering the live hosts on the networks, scan various ports to find out accessible TCP and UDP ports on remote hosts, identify services running on them, finding operating platforms on the target hosts and getting configuration of filtering security system[4].

Vulnerability Scanner

Vulnerability scanner discovers the vulnerabilities in various target hosts to determine the threats within the network. Vulnerability scanners are really based on a simple idea: automating the process of connecting to a target system and checking to see if vulnerabilities are present. By automating the process, we can quickly and easily check the target systems for many hundreds of vulnerabilities [5]. Vulnerability scanning tools have an inventory of many system vulnerabilities and goes out across the network to check whether any of these vulnerabilities exists on the target.

This paper proposes a framework for automated network security checking and alert system which allows multiple network scanning and vulnerability scanning tools for security checking process. These tools are integrated together to find the loopholes in the security of the network and provide more reliable report in comparison to the report of a single tool. The report generated from this framework is more reliable because multiple tools contribute for the assessment process and provides acceptable number of vulnerabilities.

The rest of the paper is organized as follows. Section 2 covers the previous research and work done in this field. Section 3 describes proposed framework for network security assessment. Process flow of the framework is described in section 4. Section 5 describes about the advantages of proposed framework on existing framework. Initial experimental results are shown in section 6 and section 7 concludes this paper.

2. PREVIOUS WORK

Lots of research has been done in this field of network security assessment. Traditionally for assessment purpose multiple tools were not used, they used to rely on result of single tool. Major vulnerability assessment tools were then tested by K. Novak [3] in order to find their accuracy and performance. Using these tools he proved that no vulnerability tool could find acceptable number of vulnerabilities, so using more than one scanner can be more accurate and beneficial. Multiple tools can be used to in two ways.

- All the tools are executed consecutively in serial manner. The scanning policies and control for each tool is set separately.
- All tools are executed in parallel manner with common set of policies and control.

After the research of K. Novak multiple tools were used. Initially these tools were used serially one after another. Separate policies were set for each tool for assessment and were controlled separately. The result of these tools were stored and analyzed manually. So this was a time consuming process.

Later on Jun Yoon and Wontae Sim [1] proposed a framework for vulnerability assessment with multiple heterogeneous vulnerability scanning tools. These tools are executed in parallel and common set of policies are used for every tool used. This framework basically contains following components- Vulnerability Scanner Agents, Vulnerability Scanner, Message Relay Server, Scan Result Manager and Management Interface. These components collectively perform vulnerability assessment in local as well as remote network.

The framework presented by Jun Yoon and Wontae Sim performs vulnerability scanning using heterogeneous vulnerability scanners while it does not perform network scanning before vulnerability assessment. So we only get the list of vulnerabilities excluding all other information which we find in network scanning. We don't get any information about the ports, services, OS running on systems and areas of vulnerabilities.

Network scanning process tells about the attack vectors and areas where vulnerability may exist. In this way network scanners provide more specific target to vulnerability scanners to scan the vulnerabilities within the network.

3. PROPOSED FRAMEWORK

The framework presented in this paper is the extension of Jun Yoon's and Wontae Sim's framework. In this framework additional components are network scanners, reporting system and alerting system. Alert system generates alert message on the basis of integrated report generated during the assessment process and send it to the network administrator in the form of SMS. Along with this, detailed report of assessment is sent to the network administrator by email. In this way this framework also makes the network administrator aware about the vulnerabilities existing there in network at the time they are found with the help of SMS alert and email reporting. The report generated through this framework contains list of vulnerabilities along with the result of network scanning which makes the report more significant than the previous existing framework. The overall framework is described in Fig.1.

The proposed framework is designed for assessing the security of network using multiple heterogeneous tools for finding the vulnerability in the network before attacker can exploit them. This framework easily integrates the various network scanning tools and generates a report. This report is basically integration of all the results of network scanners in one common format. This report helps in vulnerability scanning as it points to areas where vulnerabilities may exist. Vulnerability scanners generate vulnerability reports and later on these various vulnerability reports are integrated in one common format after performing correlation analysis. Network Scanner Agent (NSA), Network Scanners (NS), Network Scanner Result Manager (NSRM), Alert System (AS) and Email Reporting System (ERS) are the new components that are added in existing framework.

3.1 MANAGEMENT INTERFACE

Management interface is basically used to manage the applications that are integrated in this framework including NSA, VSA, NSRM and VSRM.

This interface enables network administrator to control the whole system as well as look over the status of network. Management interface allows them to adjust the policies for scanning tools and controls the scanners.

All the network scanners run in parallel, so common policy is set for them. Similarly all the vulnerability scanners execute in parallel so common policy is set for vulnerability scanners too. Management Interface issues commands to network scanners and vulnerability scanners to execute.

3.2 MESSAGE RELAY SERVER

MRS is used to transmit message between the applications that are running in the framework. The information flowing between applications are very crucial as it contains information about the weakness, threats and risks within the network.

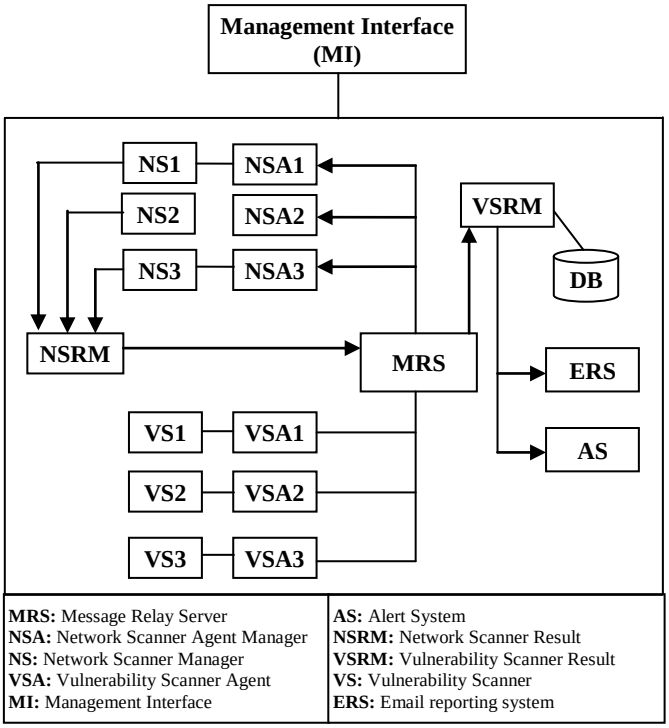

Fig.1. Network security checking and alert system framework

So if any attacker gets this information, then he/she can easily attack on the network and can exploit the vulnerabilities for their personal benefit. That is why only authenticated persons or applications can access this information.

For secure transmission of message MRS uses access control, flow control, secure channel and reliable message transmission [1].

3.3 NETWORK SCANNER AGENTS

NSA is used to control the Network scanners according to the commands issued by MI. It also applies the security policies on the network scanning tools. It accepts the control commands through MRS and applies them on corresponding network scanner.

3.4 NETWORK SCANNERS

Network Scanners are the various tools which are used to find out the attack vectors in the network which are further used for vulnerability discovery. Different scanners available may apply different techniques of scanning. As an example of port scanning there are different technique of port scanning, TCP ports can be scanned using TCP Connect, TCP SYN, TCP FIN, XMAS tree, NULL, TCP ACK[5]. Similarly different scanners may have different scanning domain. One scanning tool may be good in one network scanning task say port scanning while other may be specialized in OS fingerprinting. Multiple network scanners are used in this framework to provide better results.

3.5 NETWORK SCANNING RESULT MANAGER

As there are various kinds of network scanners the reports generated by them are also in different formats. NSRM defines one common format to represent the integrated result.

NSRM collects the network scanning results from various network scanners, and then these results are further analyzed based on the correlation, and a common integrated report is generated. This report is further sent to the MRS. VSAs use this report in vulnerability scanning. Vulnerability scanners find existing vulnerabilities in the areas suggested by this report on the target hosts.

3.6 VULNERABILITY SCANNER AGENTS

VSA performs similar type of task as NSA does, but VSA does it for vulnerability scanners. It controls the vulnerability scanner according to the commands issued by MI and the report of network scanning. After completion of vulnerability scanning it retrieves and formalizes the scan result from VS and sends it to VSRM.

3.7 VULNERABILITY SCANNERS

Vulnerability scanners are the tools to detect the vulnerabilities into the network. These tools are controlled by corresponding VSA. Vulnerability Scanners find the vulnerabilities on the attack vectors given by Network Scanners. Vulnerability Scanners contain inventory of vulnerabilities which were checked across the network to find them in the network.

3.8 VULNERABILITY SCANNING RESULT MANAGER

VSRM is an important component which is used to collect all the result from different vulnerability assessment tools. These collected results are then analyzed and integrated into one common format as there various formats of reports generated from different tools. It also integrates the result of network scanning and vulnerability scanning and generates a common report, this common report is send to ERS for sending a reporting mail to network administrator. Later on vulnerability scanning result is stored into database along with scan policy. These results can be queried from database for analysis of network vulnerabilities.

3.9 SMS ALERT SYSTEM

Alert System module creates alert message based on the reports obtained from the network security checking process. It analyzes the integrated report generated by VSRM and generates a brief alert message. Alert system in this framework is a SMS alert system which sends a limited size message. If there exists any severe vulnerability in the network based on the report generated as a result of assessment, then a SMS is sent to the network administrator to make him aware about the threat in network immediately.

3.10 EMAIL REPORTING SYSTEM

The alert system only sends very brief message in the form of SMS while reporting system of this framework sends a detailed report of network assessment to the network administrator by email. The information shared on email in this framework is very important and crucial, and if any attacker would be able to get it, then he/she would be aware of vulnerable points in network and easily can be able to compromise the

whole network. So email server used for reporting should be very much secure and getting access to email should be almost impossible.

4. PROCESS FLOW

The framework basically contains two important phases of network assessment process that are network scanning and vulnerability scanning. Both of these phases are using multiple heterogeneous tools which complement each other in the network security checking process. But simultaneous use of multiple tools requires a standard process to control and analyze results. There are following process in this framework.

4.1 POLICY SETTING AND MANAGEMENT

Unauthorized system scans pose a threat to the availability, integrity, and confidentiality of organizations' information resources. Unauthorized scans can be a prelude to the disclosure of sensitive data, cause loss of service, and loss of reputation in the global community [11]. The policies are applied on tools to regulate and control their functionality to avoid them from leaving any harmful effect on the network components. These policies are established by the network administrator according to the requirement of organization, network and services running on various hosts on the network.The role of policy in determining the appropriate response is clear: whatever is done must produce a state that the policy allows [8].

For network scanning, policies are defined for the target range of IP address within the network, method of network scanning selected (active scanning, passive scanning), method of port scanning selected (TCP connect, SYN, ACK, Xmas tree, Null etc).

For vulnerability assessment phase, policies are set to make the vulnerability assessment phase safe using Safe check, assigning the speed level for assessment by Scanning time. Other than this, policies are managed for Web service port, Web based scan, Network device based scan if on particular host these services are running.

4.2 NETWORK SCANNING

Network scanning is a procedure for identifying active hosts on a network, either for the purpose of attacking them or for network security assessment. Scanning procedures, such as ping sweeps and port scans, return information about which IP addresses map to live hosts that are active on the Internet and what services they offer[12]. Network scanning in this framework is performed by multiple heterogeneous tools, as single tool is not sufficient. Single tool doesn't provide all kind of network scanning.

Different tools with different functionalities or even with same common functionalities are integrated in this framework, which complements each other and provides an acceptable network scanning result. This result contains the live hosts in the network, status of TCP and UDP ports on these hosts, services running the hosts, OS installed on target hosts.

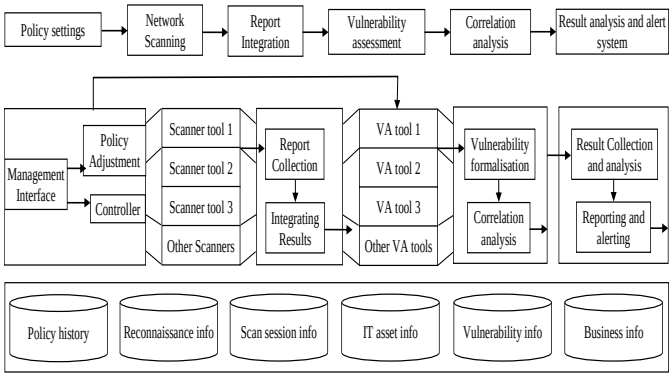

Fig.2. Process flow of the Framework

After completion of network scanning, we have information such as list of addresses for the live hosts on the network, general network topology, list of open ports on live hosts, list of services and versions running on target ports, Operating system types of live hosts etc. This information proves to be very helpful during the vulnerability scanning in the network.

4.3 NETWORK SCANNING REPORT INTEGRATION

Network scanning process is performed by multiple tools which produce reports in different formats. So analyzing the complete report from different formats and multiple places is a very tedious process. So various reports of different formats are collected from each of network scanning tools and integrated in one common format so that analyzing the report would be comfortable and more efficient. This report is used as an input by vulnerability assessment phase.

Common standard format may contain
IPadd, OS, opTCP, opUDP, run_services}

IPadd is the list of live hosts on the network, OS represents the operating system on the corresponding IPaddress, opTCP and opUDP contains list of accessible TCP and UDP ports on the corresponding IP address and run_services tells about the services running on the targeted host. Similarly different standard format can be set.

4.4 VULNERABILITY ASSESSMENT

The vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system. The framework uses various heterogeneous vulnerability assessment tools to identify the vulnerability in hosts in the network based on the report of network scanning process. These tools are controlled by the VSA which carries the command of MI and scanning policies.

4.5 CORRELATION ANALYSIS

The results collected from different VSs are transformed into one common format by each corresponding VSA. The common result format is as follows,

{ScanSessionID, HostIP, VulnerabilityName, ToolName, Severity, Description, PublicID, Port} [1].

According to the framework VSA send the results to the SRM where the correlation analysis is performed. The attribute defined in common format are parsed from the results achieved from VSA. Public ID and port are optional information because each tool does not provide this information so if this is the case No-match ID will be assigned at these places. The hashed value of found vulnerability information is matched with hashed value of vulnerability stored in database, which is already found, if it matches, then existing ID will be assigned to this vulnerability otherwise new ID will be generated for vulnerability and hashed value would be stored in the database for future use [1].

4.6 RESULT ANALYSIS AND ALERT SYSTEM

The results achieved from various tools are converted into common format by correlation analysis and then these results of common format are integrated together to make a generalized report which can be easily analyzed. The result of integration is stored in the database. During the integration phase we can find the same vulnerabilities with different name and different severity level, but reliability level is set for each VS using security manager.

After the integration of results, analysis of output result of integration is performed, based on various factors as business requirements, severity of vulnerability to find the vulnerabilities which may be more harmful for organization and network. Based on this analysis the report is generated and a mail to the network administrator is send automatically by Email reporting system of framework. Parallel to this, based on the report a small SMS message is created if report contains severe vulnerability. This SMS is sent as an alert message to the network administrator's mobile phone. The SMS alert does not reveal the vulnerability information because SMS is a plain text based messaging system which can be easily compromised. It only alerts network administrator if severe vulnerabilities exist. Network administrator needs to read its mail for detailed report.

5. EXPERIMENT AND RESULTS

We have used five systems in LAN for our experiment. One of these systems is used for performing network security checking on the remaining four systems.

Here we are presenting initial results of the experiment. We used NMAP, Superscan and Nbtscan tools for network scanning. All the tools were executed in parallel to each other. Nbtscan tool scanned for open netbios name servers on TCP/IP network.Nmap performed OS fingerprinting and gave three OS guesses out of which one was true for each system.NMAP and Superscan performed port scanning separately on the same range of TCP and UDP ports for each of the four machines.

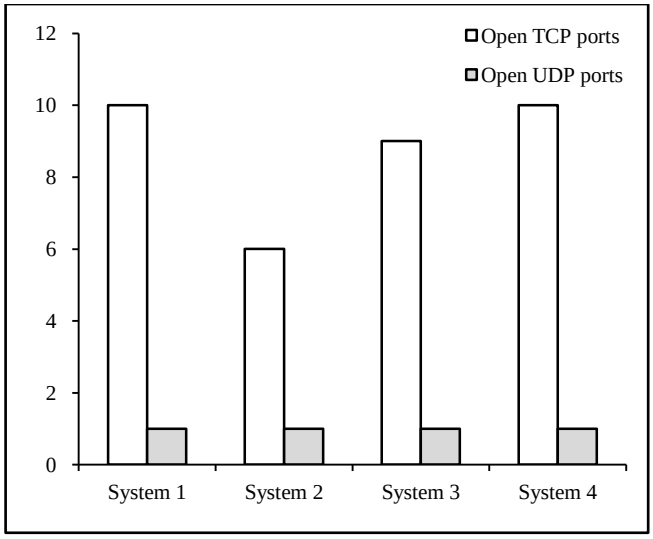

Fig.3. Open TCP and UDP ports discovered by Superscan

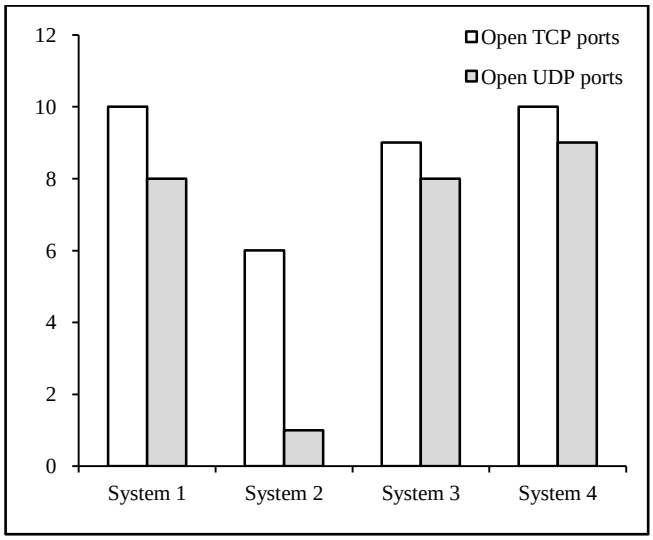

Fig.4. Open TCP and UDP ports discovered by NMAP

Numbers of open ports on each of four systems found by both tools are shown in Fig.3 and Fig.4 respectively. NMAP tool classifies ports in three states as Open, Filtered and Closed. Shaded portion of red color column in Fig. 4 represents filtered UDP ports. Superscan classifies ports only in two states Open and Closed. After looking into the Fig.3 and Fig.4 we can see that there are various similarities in the results of both tools. There are some differences too, as Superscan considered filtered UDP ports as closed ports and discarded them in results while NMAP identified them in separate class mentioned as filtered ports. In both the tools we used vanilla connect (also known as TCP connect()) port scanning to identify open TCP ports on each system. On the other hand to identify open UDP ports, UDP data were sent on the target machines seeking for the reply from well known ports as well as ICMP messages. If ICMP message "ICMP destination port unreachable" is not received back then UDP port is considered as open. Along with the list of open ports these tools also tell about the services running on these ports. There were some ports on which one tool was not able to identify the services running while another did. This is

one of the advantages of using multiple tools for network scanning.

As all the tools were executed in parallel so it took around 466 seconds in scanning the all the four systems, while executing them serially it took around 612 seconds.

The development of integration platform for various tools, based on the proposed framework is in progress. We have developed all the interfaces required, to interact with the system. We have successfully integrated all the network scanning tools used in platform. Fig.5 and Fig.6 are the screenshots of some of the interfaces where the right side window shows the main interface of the platform, which facilitates users to configure network scanners and vulnerability assessment tools, set Email and SMS alert system. We provide IP addresses to platform in one of the three ways that are in range, list or browse form file. Fig.5 shows the interface for configuring scanners used for network scanning, which appears after clicking on "Config Scanners" button of main interface. This interface asks user to select the scanners to run, select port scan (TCP or UDP or both), scanning technique and port numbers which we want to scan. Fig.6 shows the interface which asks details for setting email reporting system. This interface appears after clicking on "Email Settings" button under "Settings" button group of main interface. It demands for the email-ID of recipient including carbon copy recipients, Email Server's IP address etc. Similarly there are other interfaces which allows user to interact with the platform's various components such as SMS alert system, configure vulnerability assessment tools etc.

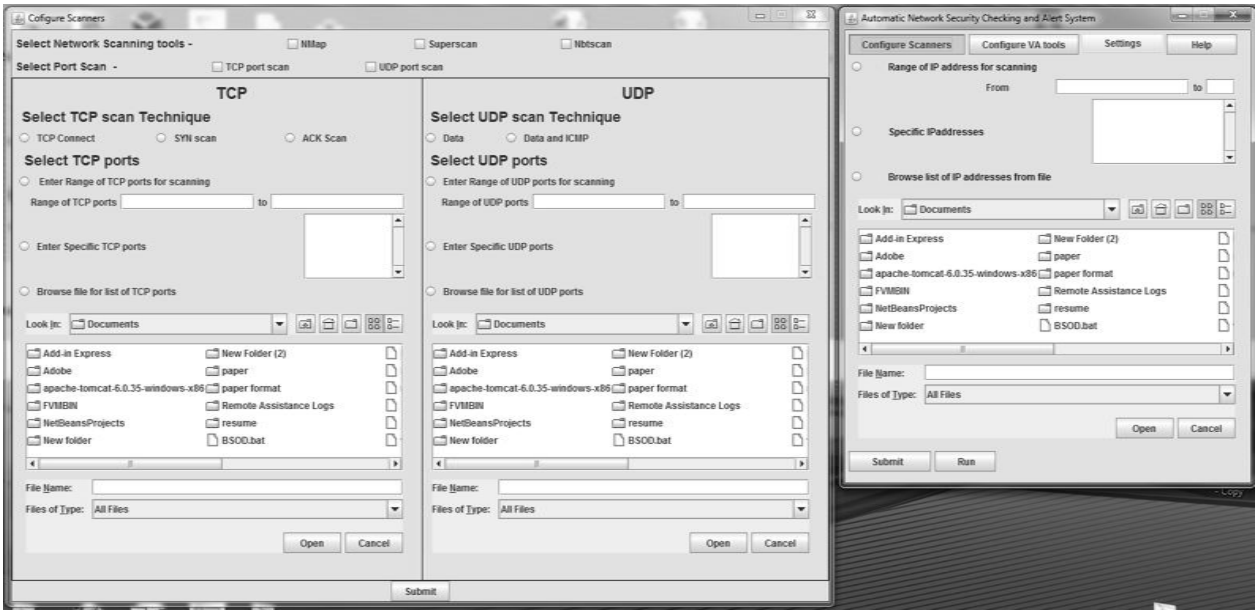

Fig.5. Screenshot of interface for configuring scanners of integration platform

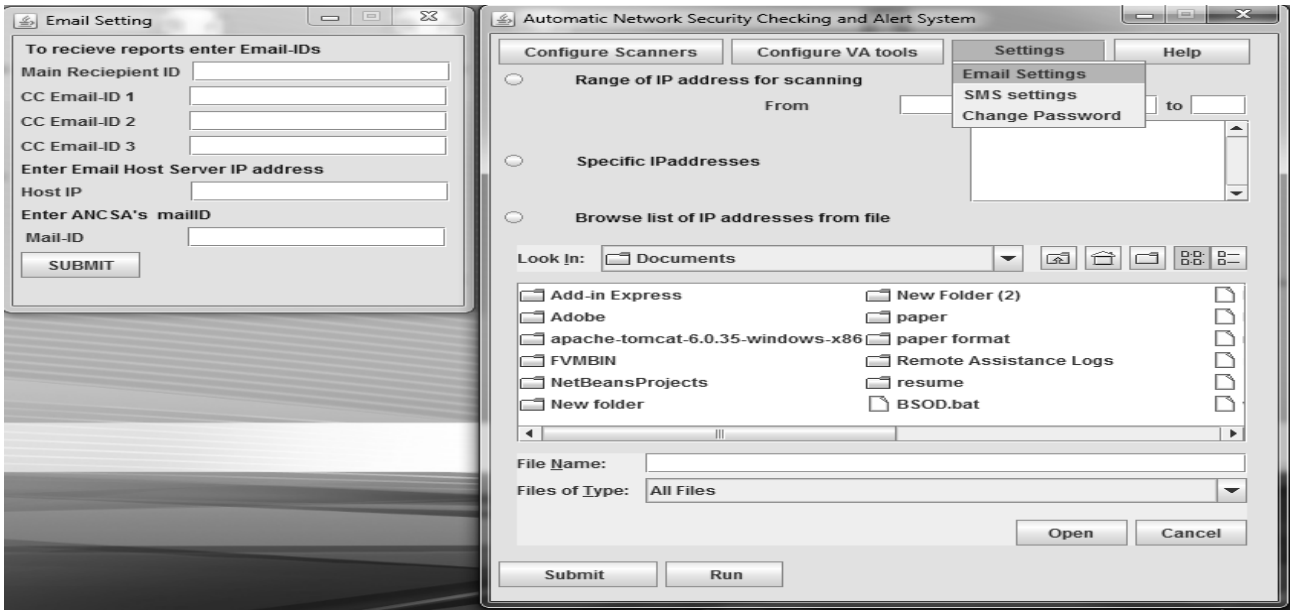

Fig.6. Screenshot of Email-setting interface of integration platform

6. ADVANTAGES OF THE FRAMEWORK

There are various advantages of the proposed framework which signifies the framework. Framework performs network scanning prior to vulnerability assessment which provides clears target network's picture by identifying structure of network, live host in the network, open TCP and UDP ports on live hosts, Services running on these ports and perform OS fingerprinting and other network scanning activities. Port scanning is beneficial, because it finds open ports on an IP address (host), ports that are open on a host represent services, servers, and sometimes internet applications (possibly trojans), therefore a port scanner can inform you of such services, servers, etc. running on a local or remote system. Port scanners may assist you in the detection of trojans and other unwanted servers/applications [13]. In this way, this information helps vulnerability scanners to perform vulnerability assessment in more effective manner. As well as network scanning provides specific targets for vulnerability scanning instead of scanning the whole network for vulnerabilities.

Secondly we are using multiple network scanning tools and these tools together provide better acceptable result of network scanning than using any one tool.

Report generated by this framework is more significant as it contains the list of vulnerabilities along with the network scanning results. This report provides better insight about the network and its vulnerabilities.

This framework also provides a reporting and alerting system, which sends report to the network administrator just after the completion of assessment process as well as it also sends an alert message to network administrator if any severe vulnerability found in the network.

7. CONCLUSION

The paper proposed a new framework for network security checking and alert system for assessment of the security of network with better performance and efficiency along with alert system. This framework can easily integrate multiple network scanners as well as vulnerability scanners. It is a flexible framework which can accept the network security and vulnerability scanner tools according to the requirements. All the network scanning tools execute in parallel and after completion of network scanning, based on network scanning report all vulnerability scanners execute in parallel manner. In this way the parallel execution of tools speeds up the security checking process.

This framework additionally provides alert messages and security checking reports which alerts and reports network administrator anywhere and anytime.

REFERENCES

[1] Jun Yoon and Wontae Sim, "Implementation of the automated network vulnerability assessment framework", *Proceedings of 4th International Conference on Innovations in Information Technology*, pp. 153-157, 2007.

[2] Austin A and Williams L, "One Technique is Not Enough: A Comparison of Vulnerability Discovery Techniques", *Proceedings of International Symposium on Empirical Software Engineering and Measurement*, pp. 97-106, 2011.

[3] K. Novak, "VA Scanners Pinpoint Your Weak Spots", *Network Computing*, 2003.

[4] Chris McNab, "*Network Security Assessment*", Second edition, O'Reilly Media, 2007.

[5] Edward Skoudis and Tom Liston, "*Counter Hack Reloaded: A step-by-step Guide to Computer Attacks and Effective Defenses*", Second Edition, Prentic Hall, 2006.

[6] James S Tiller, "*CISO'S Guide to Penetration Testing: A Framework to Plan, Manage and Maximize Benefits*", CRC Press, Taylor and Francis Group, 2012.

[7] James F. Kurose and Kieth W. Ross, "*Computer Networking: A Top-Down Approach Featuring the Internet*", Third Edition, Pearson Education, 2005.

[8] Matt Bishop, "Trends in academic research: vulnerabilities analysis and intrusion detection", *Computers & Security*, Vol. 21, No. 7, pp. 609-612, 2002.

[9] LV Zhen-Bang, Zhang Jun-cai and Zhang Jun, "Research on Network Security Leak Scan and Vulnerability Analysis", *Aeronautical Computer Technique*, Vol. 2, pp. 118-121, 2005.

[10] Haifeng Wu, "Research of Network security Assessment System Based on Vulnerability Scan", *Proceedings of 3rd International Conference on Advanced Computer Control*, pp. 566-569, 2011.

[11] https://my.tennessee.edu/portal/page?_pageid=40,43717&_dad=portal&_schema=portal

[12] http://searchmidmarketsecurity.techtarget.com/definition

[13] http://www.networkactiv.com/Scanner.html