Security Risk Assessment Framework for Network Layer

K.Ram Mohan Rao
Geoinformatics Division
Indian Institute of Remote Sensing
Dehradun, India
Email: rammohan@iirs.gov.in

***Abstract*—Security assessment is a crucial process in the application deployment. The network layer plays an important role in the computer infrastructure. Network infrastructure generally consists of firewall, router, and switches etc. The vulnerabilities and technology gaps in the network assets may lead to serious problems in the security and application deployment. Here we study the risk assessment framework for a network layer for making the network layer more effective and secure. The study led to quantifying risk factor of a network layer.**

***Index Terms*—Network, risk, security, vulnerabilities.**

I. Introduction

A network has been defined as any set of interlinking lines resembling a net, a network of roads, an interconnected system, a network of alliances [1]. The International Standards Organization (ISO) and Open Systems Interconnect (OSI) reference model defines seven layers of communications types, and the interfaces among them. Over the last 25 years, a number of networks and network protocols have been defined and used. Anyone can connect to these public networks, or they can use types of networks to connect their own hosts together, without connecting to the public networks. TCP/IP (Transport Control Protocol/Internet Protocol) is the language of the internet. Anything that can learn to speak TCP/IP can play on the internet. This is functionality that occurs at the network (IP) and transport (TCP) layers in the ISO/OSI reference model. Consequently, a host that has TCP/IP functionality (such as Unix, OS/2, Mac OS, or Windows NT) can easily support applications that use the network. One of the most important features of TCP/IP is not a technological on, the protocol is an open protocol, and anyone who wishes to implement it may do so freely. A number of attacks against these IPs are possible. A packet simply claims to originate from a given address, and there isn't a way to be sure that the host that sent the packet is telling the truth. This isn't necessarily a weakness, but it is an important point, because it means that the facility of host authentication has to be provided at a higher layer on the ISO/OSI reference model. Today, applications that require strong host authentication (such as cryptographic applications) to do this at the application layer. Network infrastructure generally consists of firewall, router, and switches. Firewall sits between a router and application servers to provide access control. Firewalls are originally used to protect a trusted network from the untrusted network. These days, it is becoming more common to protect application servers on their own (trusted, isolated) network from the untrusted networks.

Most of the organizations focus on establishing the perimeter defense such as DeMilitarized Zones (DMZ), firewall and authentication services, intrusion detection systems, and antivirus modules. On the other hand, internal security controls also implemented within the network environment. With the growth of web based applications and intranet, network security has become a major concern. To counter the emerging challenges, mere deployment of firewall systems, access controls and other security systems are not sufficient as they leave many security holes unaddressed. These security holes can allow intruders and threats to access or damage the valuable databases. Therefore network assessment is an essential process to rate the risk that is present in the network layer to understand the risk they are dealing with. The network security assessment helps to identify potential security holes, the technology gaps between different networking devices, to close potential security holes before intruders, worms attempt to exploit the vulnerabilities present in the setup.

In this paper, a modest attempt has been made to quantify the security risk of a network layer. It covers the vulnerability assessment for different network devices such as gateway systems, router, and different networking devices. Then it presents a risk assessment methodology for a network layer. Specifically it is to rate the risk of the network layer comprehensively to protect the organization’s valuable computing resources. Section V explains the security risk assessment methodology for the network layer using different parameters. The security assessment is a comprehensive program that provides to rate the risk by identifying and analyzing vulnerabilities of different devices. Section VI presents results and discussions along with vulnerabilities and its risk factor. These details are key in the remediation plan to minimize the risk factor of the network by eliminating these vulnerabilities. The study highlights the use of different tools for the vulnerability assessment for different networking devices, compiling them for the final risk assessment of the network layer.

II. RELATED WORK

Today there has been tremendous success of web based applications. Most of the applications are deployed using web based technologies. Despite the incorporation of the improved technologies, hacking techniques also gained momentum these days. Web Application Security Consortium [2] gave report on web hacking statistics. These hacking statistics states that the number is gradually increasing from year to year, even with the added security feature technology in networking and application development tools. The trends in hacking techniques are developed according to the usage level of particular technologies at the time [3]. As a consequence network assessts and web servers are becoming popular attack targets. Around 71% of the reported application vulnerabilities have affected the web technologies such as web servers, application servers and web browsers [4]. In the past, organization relied more on gateway defenses, Secure Socket Layer (SSL), Network and Host security to keep the data secured. Unfortunately, majority of the web attacks are application attacks and the mentioned technologies are generally unable to cope up with the security needs against the application attacks [5]. The gateway firewall and antivirus programs through offer protection at network and host level, but not at the application level [6]. Firewall may not detect malicious input sent to a distributed application. Indeed, firewalls are great at blocking ports, of course, some firewall applications examine communications and can provide very advanced indication still. Typical firewall helps to restrict traffic to HTTP, but the HTTP traffic can contain commands that exploit application vulnerabilities. Firewalls are only an integral part of security, but they are not a complete solution [7]. The same holds true for Secure Socket Layer (SSL), which is good at encrypting traffic over the network. However, it does not validate the application's input or protect from a poorly defined port policy. However, when the network and host entries are secure, the public interfaces of the application become the focus of the attack. The Software Unlimited Organization [8] listed the top 10 firewall limitations as it can't tell if there are vulnerabilities that might allow a hacker access to internal network.

Today's client/server technology has progressed beyond the traditional two-tiered concept to three-tier architectures. Web applications have numerous entry points that can put database at risk. Hackers generally look into the different fundamental areas of application to break the security. The general types of attacks are IP access, port access, and application access. Hackers get the IP address of the server and do the telnet to exploit the server. Therefore, network layer plays an important role in the protection of the application database. The major challenges associated with the network layer are their most critical vulnerabilities that are of often the results of Denial of Server, secure configuration, authentication etc [9]. With this background, security assessment has been considered a sub-function of network management, and has been identified as one of the five functional areas of the open system interconnection, management framework. As defined in the OSI management framework, security assessment is concerned not with the actual provision and use of encryption or authentication techniques themselves but rather with their management. Meier et al, 2004 defines security assessment involves holistic approach, applying security at three layers: network layer, host layer, and the application layer [10]. Russ et. al., 2007 concludes security assessment is an organizational level process that focuses on the nontechnical security functions within an organization [11]. In the assessment, it examines the security policies, procedures, architectures, and organizational structure that are in place to support the organization. Although there is no standard metric for rating the risk, there is no standardization of network security assessment process. For example Sloman et al, 1994 defines security assessment as the support for specification of authorization policy, translation of this policy into information which can be used by security mechanisms to control access, management of key distribution, monitoring and logging of security activities [12]. Now, this study enhances the security management of a network layer to quantify the risk associated with all the network devices and generate a comprehensive risk to understand the current security state of the network. This paper emphasizes on defining a framework for network risk measurement taking into account of threat, vulnerability, consequence and risk model.

III. NETWORK THREATS AND VULNERABILITIES

Network security consists of the provisions made in an underlying computer network infrastructure, policies adopted by the network administrator to protect the network and the network-accessible resources from unauthorized access. Securing network infrastructure is similar to securing all possible entry points of a network with tight security practices and guidelines. Attacks could be stopped at the entry points before they spread. RFC 1244 identifies three distinct types of security threats usually associated with network connectivity: Unauthorized access – A break in by any unauthorized person. Disclosure of information - any problem that causes the disclosure of valuable or sensitive information to people who should not have access to the information. Denial of service - any problem that makes it difficult or impossible for the system to continue to perform productive work.

Edwards, 1997 classify the network threats, such as cache, file servers or host systems, viruses, sniffers, Ethernet ports, Backup tapes, wiretapping, hot-swappable and spare components, user passwords and group administrators, share and file permissions, email administrator, unwanted TCP/IP ports, built-in TCP/IP filtering, network binding, the registry, external LAN links, external WAN links [13]. Vulnerability is generally software or hardware bug or a mis-configaration that a malicious individual can exploit [14]. Generally there are two types of vulnerabilities called known vulnerability and unknown vulnerability. Most organizations pay attention to the known vulnerabilities by applying countermeasures or by rectifying the vulnerabilities present in the network. But calculating the unknown window of vulnerability is more important when planning mitigation strategies. Most of the time the underlined vendors will release the corresponding patches to the new vulnerabilities found. But interestingly a good trend has emerged that, third party vendors also releasing patches for new vulnerabilities found in the system. Usually new vulnerabilities in network services are educated by several agencies to the security community. Many organizations namely Security focus, Packet storm, CERT, MITRE etc. provide service to find out potential vulnerabilities in the network.

IV. Risk Assessment Methodology

To counter the emerging challenges in network security, mere deployment of firewalls, access control and other technologies are not enough, as it leaves many security issues unaddressed. Security holes can allow intruders, worms, and other threats to steal or damage critical business information. Network infrastructure vulnerabilities are the foundation for all technical security issues in information systems. These vulnerabilities affect everything running on the site particularly the web applications, which is the main objective of this paper. Many issues are related to the security of network infrastructure. Some issues are more technical and require using various tools to assess them properly. Some issues are easy to assess with a good pair of eyes and some logical thinking. Some issues are easy to see from outside the network, and others are easier to detect form inside the network.

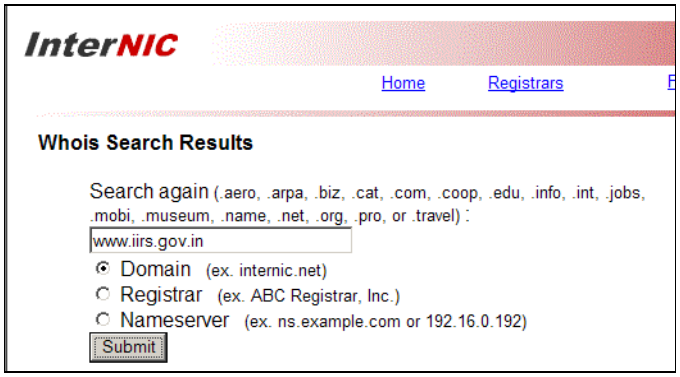
Random procedures are not enough to make the network secure enough, a well defined set of procedures at all levels of network have to be deployed to make the network more secure. Network security involves protecting network devices which act as frontline gatekeepers such as router, firewall and switches [15]. It's all about practicing good security principles with pre identified threats and countermeasures with set of assessment procedures. McNab introduced security as a process, which is the cyclic approach to network security assessment involves discovering a cooperative high level overview of organization being assessed, including assessment of policies, procedures and information flow [16]. The cyclic approach starts with scanning network enumeration, network scanning, and finally specific service/device assessment. The assessment includes assessment of network by scanning network with proper tools. Network scanning is conducted using assessment tools for enumeration and information gathering, and brute-force password guessing. In general enumeration tools are used to gather system information. Brute-force tools are used to compromise account passwords and gain access to shared files and resources. Assessment of firewall, router, and edge switches including placement on the network and how it is configured?

Every security related device must periodically be verified for correctness and integrity. Network vulnerability assessment tools (vulnerability scanners) are excellent for checking the things for known problems with router configuration. ISS, Satan, CyberCop Scanner, and Nmap can be used to scan and test routers on network. Configuring firewall is not enough to guarantee security. Harden routers and switches, too, will tighten the security of application.

V. Vulnerability Assessment

Many organization offer information on discovered vulnerabilities. Some of the organizations are commercial and rest of them is non-commercial. Generally administrators see the latest news for the known vulnerabilities and corresponding remedies for the patch. But for a comprehensive network security, vulnerability assessment is essential. Due to the increasing sophistication of intruder methods and the vulnerabilities present in many applications, it is imperative to regularly assess network security. A variety of vulnerability identification tools are available.

Vulnerability assessment includes the gathering of network details ranging from collection of IP address range, domain details. The next step is the enumeration process, used to determine the target operating system and the application residing on the system. This will substantiate the application residing on the host with information of port policies and determining what application is residing on what ports. Generally Whois Query is used to gather the IP range details with input options of domain, registrar, and name server. The details can be gathered by Whois Query by browsing the site http://reports.internic.net. Fig. 1 shows the who are query against one of the IP address that hosted in the network layer. By performing the Whois query it is possible to gather all required preliminary information of the site hosting the application such as, the physical address, contact information, the IP address range used, the DNS server details.



Whois Search Results

Search again (.aero, .arpa, .biz, .cat, .com, .coop, .edu, .info, .int, .jobs, .mobi, .museum, .name, .net, .org, .pro, or .travel) :

www.iirs.gov.in

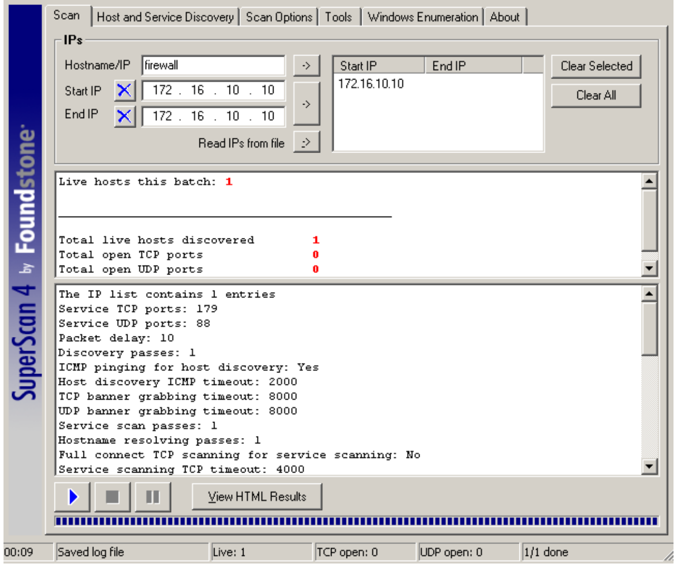
● Domain (ex. internic.net)
○ Registrar (ex. ABC Registrar, Inc.)
○ Nameserver (ex. ns.example.com or 192.16.0.192)

Submit

Fig. 1. Whois Query for IIRS

Using -$P(ping scan) switch within map also can conduct the ping sweep of the target network. In addition to Nmap ping scan, -$V (service / version info) switch to determine the application ports. Now the point is identifying the vulnerabilities in the network is a big process. There are several vulnerability assessment tools (both commercial and open source), but deploying the selected tool in selected location will not compile the total vulnerabilities present. This is because an enterprise site may contain tens of servers and hundreds of hosts. Instead of automated scanning to an enterprise network, leverage the organization's existing vulnerability management. The individual vulnerability of the site may be carried out, by compiling the total security vulnerabilities.

Firewalls are a mandatory component of network security. However, mis-configarations and poor policies and deployment architectures can lead to a false sense of security. A firewall must be configured to allow or deny appropriate traffic. The configuration process can be highly susceptible to human error. In a dynamically changing environment, system managers routinely reconfigure firewalls without regard to security implications. Access control lists on a firewall can be numerous and confusing. It should be continuously monitored that the firewall has been set up correctly, and that it is performing well. However, a firewall must be correctly configured to provide effective protection. Firewall Scanner has added a number of firewall security checks to the base intranet scanner tests, including source porting, source routing, SOCKs, TCP sequence prediction (IP spoofing), and Denial of Service Attacks. Fig. 2 shows the enumeration analysis using SuperScan tool.



Hostname/IP: firewall
Start IP: 172 . 16 . 10 . 10
End IP: 172 . 16 . 10 . 10

Start IP	End IP
172.16.10.10	

```
Live hosts this batch: 1

______________________________________

Total live hosts discovered        1
Total open TCP ports               0
Total open UDP ports               0
```

```
The IP list contains 1 entries
Service TCP ports: 179
Service UDP ports: 88
Packet delay: 10
Discovery passes: 1
ICMP pinging for host discovery: Yes
Host discovery ICMP timeout: 2000
TCP banner grabbing timeout: 8000
UDP banner grabbing timeout: 8000
Service scan passes: 1
Hostname resolving passes: 1
Full connect TCP scanning for service scanning: No
Service scanning TCP timeout: 4000
```

```
00:09   Saved log file   Live: 1   TCP open: 0   UDP open: 0   1/1 done
```

Fig. 2. Enumeration analysis

Opens ports are more vulnerable and attract heavy risk for the system. Scan for such open and blocked ports are necessary to ensure firewall system is performing as intended. Most often firewall also involves lot of unknown vulnerabilities even after successful implementation. These vulnerabilities may be found out immediately to patch the security gap before exploitation of the application. Vulnerability detection tools are available to scan firewall system to determine the presence of known vulnerabilities. If patches exist for vulnerabilities that a tool detects, these patches can be installed on firewall system and re-execute the tool. This ensures that the vulnerability has been eliminated permanently. Several open source and commercial tools are available for the vulnerabilities scanning in the firewalls. Nessus and SuperScan are used for finding out vulnerabilities, including TCP, UDP ports, windows enumeration, host and service discovery [17], [18]. Nessus is a fantastic open source tool to scan network for finding out the vulnerabilities, open ports, user details, service details, host vulnerabilities, risk factors, and remedies. Using this information, the security risk determination network layer is done. By evaluating, each vulnerability present in the device one can address each issue by taking necessary remediation to reduce the risk to the application. The open port in the device would be checked and same can be closed, if not important for the transactions, (or) the port can be monitored regularly, if the port is necessary to conduct the business.

VI. Overall Security Assessment

This section brings all together by integrating router, firewall, and switch security assessment for GWIS environment by identifying weaknesses and recommendations for short and long term security improvements. This approach demonstrates first identifying security strategy by covering assessment results obtained from various network devices deployed in the network in addition to topics covering across the people, process and technology. Microsoft Security Assessment (MSA) tool is used to identify and addressing the security risks in network environment. MSA follows holistic approach to measure security strategy by covering topics across people, process and technology. Findings are coupled with recommendations mitigation efforts. This tool is not an automated scanning tool, but takes the input from the user/administrator in various fields such as infrastructure, application development, deployment, operations, and people. Now, the risk associated with the network layer is calculated by using simple straight forward formula given by Manzuik et al [19].

$$\text{Risk} = \text{Vulnerability} \times \text{Attacks} \times \text{Threat} \times \text{Exposure}$$

Where

V = Vulnerability, A measure of issues that are considered vulnerabilities.This measure is usually is function of vulnerability assessment.

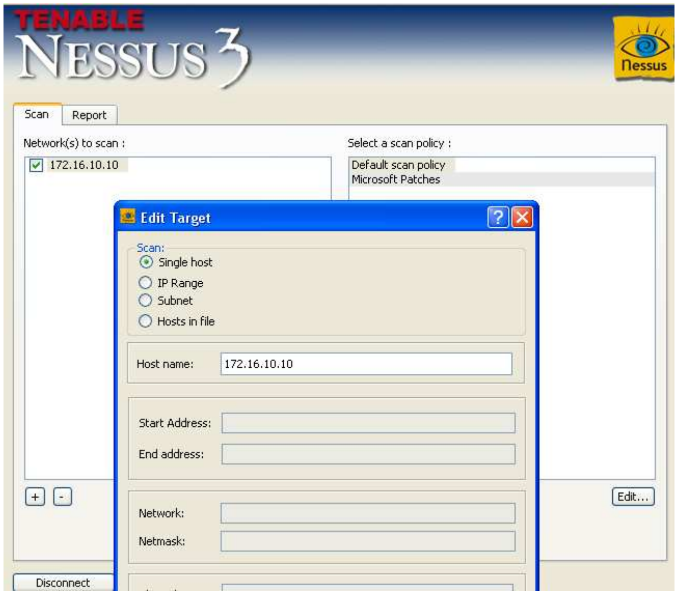
A = Attacks, A measure of actual attacks and dangers, which is typically a function of host/ network based intrusion detection / prevention tool.

T = Threat, A measure of lurking or impending danger. This is known as the threat climate, which comprises such factors as availability and ease of exploit.

E = Exposure, An accounting of organization's vulnerability to attack, or how much periphery must be protected and how poorly it is being protected.

VII. Results and Discussions

Identifying vulnerabilities across the site is a major endeavor. Today's enterprise consists of several system servers, application servers, database servers via several networking circuits with varying speeds. The point is, it is not possible to simply install network or system scanners and scan the total application. This is because, it is not possible to get the required coverage with in the desired time frame with a single scanner. For this reason we cannot simply stop the assessment, knowing that the site consists of 70 percent network vulnerabilities that have not been remediated. Enterprise level assessments are still required. Instead of simply dropping scanners onto network, the process should leverage organizations vulnerability management, its investment in security, patch, and configuration management technologies. Vulnerability scanners are responsible for detecting network hosts, discovering available applications, and ascertaining vulnerabilities. Vulnerability softwares generally run on network devices or on a company own application assets. For this type of network assessment, single type of vulnerability scanner is sufficient for scanning the application. However, larger sites may require multiple vulnerability scanners to support the assessment needs. Now, the point is what is next after fixing the vulnerabilities of the site. The major issue in the security management is finding out the vulnerabilities and fixing them to reduce the security risk posed by these vulnerabilities. Every organization should concern with managing remediation to address the discovered vulnerabilities. Most often traditional vulnerability methodologies and its IT security policy suggest some methodology, but the organization should have a mechanism to validate vulnerabilities exposed to a remote entity. Vulnerability assessment reports produce lot of insightful information as listed in fig. 3.



Network(s) to scan :
☑ 172.16.10.10

Select a scan policy :
Default scan policy
Microsoft Patches

Scan:
● Single host
○ IP Range
○ Subnet
○ Hosts in file

Host name: 172.16.10.10

Start Address:

End address:

Network:

Netmask:

Fig. 3. Vulnerability analysis using Nessus

The vulnerability report generally produces the following information regarding:

- Duration of the assessment,
- Number of machines scanned,
- Vulnerabilities by severity,
- List of vulnerabilities identified,
- Vulnerabilities per host.

During the assessment, advanced tools and security assessment methodology for the detection of security issues and exposures within the network are applied to the related runtime platform environment. The summary summarizes application security vulnerability assessment report for the network. Vulnerability assessment need to be supported by an enterprise remediation strategy, and assessment should target not only at windows, Unix, and Linux systems, but also all I.P. connected devices within the site such as routers, gateways and switches. The total network equipment of network environment is scanned, which includes gateway, router, and L3, L2 switching devices. The vulnerabilities present in firewall, router, and L3 switch are respectively, 45 of which are considered as low risk category, 2 are considered as medium level risk, and 4 are considered as high level risk vulnerabilities. Surprisingly 47 ports are found open in the network area. In fig. 4, vulnerabilities are further broken down by risk, percentage, and average number of vulnerabilities by risk category.

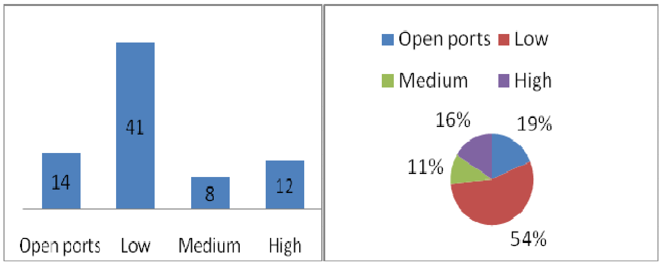


Fig. 4. Vulnerability breakout by count and percentage of network layer

Analyzing vulnerability assessment report further, it is discerned what are most prominent vulnerabilities, as reflected in Table I.

TABLE I
TOP VULNERABILITIES OF NETWORK LAYER

S. No	Vulnerability	Risk factor
1	Remote server does not reply with 404 error code.	None
2	Daytime is running on this port	None
3	DNS server is running on this port	Low
4	Usable remote name server	Medium
5	Version of bind	None
6	RPC service enumeration	None
7	BIND vulnerable to cached RR overflow	High
8	BIND vulnerable to negative cache poison bug	High
9	Default community names of the SNMP agent	High
10	RPC port manager	None
11	SSH server type and version supported	None
12	RPC service enumeration	None
13	Hyper text transfer protocol information	None
14	Checkpiont firewall-1 ICA service detection	None
15	Unknown service banners	None
16	Telenet service detection	Low

Table I provides insightful and more reflective information regarding the true security posture of network at GWIS site. Figure 4 illustrates that 47 ports are open in the network, 45 vulnerabilities of low risk. Detailed breakup list of router, firewall and switch is given in Table II.

TABLE II
DEVICE WISE VULNERABILITIES

Host name	Vulnerabilities	Remarks
Router	Open ports:29 Low :23 Medium :0 High :0	Low severity problem(s) found
Firewall	Open ports:1 Low :3 Medium :0 High :0	Low severity problem(s) found
Switch(es)	Open ports:17 Low :19 Medium :2 High :4	High severity problem(s) found

So vulnerability receives a score of 4 because its impact on the affected systems, attack would receive a score of 2 based on the nature of attack. Threat would receive 4 because of the popularity of the company, exposure in this case receive 2 because the service is not much affected. Therefore,

Risk = Vulnerability x Attacks x Threat x Exposure
So, in this case
Risk = 4 x 2 x 4 x 2
Risk = 64

As per CVE 2005-4560, the maximum risk will always be 625 and minimum will always be 1. The total risk associated with the network layer is 64; therefore overall risk level is LOW. The risk is obtained by integrating the associated network equipment (gateway, router, and switch), and the total risk of the network layer is 64. Hence, the overall severity level is LOW.

VIII. CONCLUSION

Vulnerabilities exist at many layers in the computing world. The first step in securing IT environment is to ensure all application systems and network devices have been properly audited and exposures eliminated. Starting with firewalls, there are two classes of vulnerability mis-configuration, and firmware bugs - that can allow entry to non-authorized users. Most firewall vendors have a list of patches that should be used to bring a firewall up to date. Automated scanners examine the firewall and determine whether the firmware revisions are current.

Network security involves protecting the network devices such as router, firewall, switches, and the data that they forward to provide additional security for host servers. Since the network layer is the first (outer) layer of any application, protecting the network with well defined countermeasures is important. In this process, assessment of each network device plays a major role in finding out the vulnerabilities. These vulnerabilities are fixed out with corresponding countermeasures to make the network security tighter, which ultimately improve the security process of the application.

REFERENCES

[1] A.S.Tanenbaum, Computer Networks, Printece Hall, 2006, pp. 27-55.

[2] WASC, *Web Application Security Consortium, Web Hacking Statistics,* 2008. Accessed from http://www.webappsec.org/projects/whid/statistics.shtml. Accessed on 14.06.2007.

[3] F. Ian, *Protecting The Web Server And Applications*, Computer & Security, 2001,Volume 20, Issue 1, pp. 31-35.

[4] K. Mandeep, *Cenzic Application Security Trends Report - Q4, 2007*, Cenzic Inc. 2008.Whitepaper. Accessed from http://www.Cenzic.com, Accessed on 12.02.2008.

[5] IBM, *Web application security management,: Understanding the web application security*, 2008, Whitepaper. Accessed from http://www.ibm.com Accessed on 12.07.2006.

[6] M. Curphey, D. Endler,, W. Hau, S.Taylor, T. Smith, A. Russel, M. McKenna, R. Parke, K. McLaughlin, N. Tranter, A. Klien, D. Groves, I. By-Gad, S. Huseby, M. Eizner, R. Mcnamara, *A guide to building secure web applications, The open security web application project, V.1.1.1.* 2008. Whitepaper, Available from http://www.first.org/cvss/cvss-guide.html Accessed on 12.04.2007.

[7] J.D.Meier, A. Mackman, S. Vasireddy, M. Dunner, S.Escamilla, A. Murukan, *Improving web application security : Threats and Countermeasures*. 2003. Microsoft Corporation, pp.3.

[8] SoftwareUnlimited, *Firewall Limitations*, Irvine, CA. 2005 Whitepaper. Accessed from http://www.softwareunlimited.com/securityfirewalltop10.htm. Accessed on 06.20.2005.

[9] F. Ricca, P. Tonella, *Web site analysis: structure and evolution,* in: proceedings of the IEEE international Conference on Software maintenance, San Jose, California.2000.

[10] J.D.Meier, A. Mackman, S. Vasireddy, M. Dunner, S.Escamilla, A. Murukan, *Improving web application security : Threats and Countermeasures.* 2003. Microsoft Corporation, pp.4.

[11] R. Russ, D. Ted, G. Miles, M. Greg, *Security Assessment: Case studies for implementing the NSA IAM, Syngress*, Syngress Media, Inc,2007.

[12] M.S. Sloman, *Policy Driven Management for Distributed Systems*. Journal of Network and Systems Management, vol. 2(4), pp. 333-360, December 1994.

[13] M.J.Edwards, *Internet Security with Windows,* Whitepaper, 1997. Accessed on March 2007, http://www.windowsitlibrary.com/Documents/Book.cfm?DocumentID=121

[14] S Manzuik , A Gold, C Gatford, *Network Security assessment: from vulnerability to patch*, Syngress, 2007.

[15] J.D.Meier, A Mackman, S. Vasireddy, M Dunner, S Escamilla, A Murukan, *Improving web application security: Threats and Countermeasures*. Microsoft Corporation, 2003, pp.408-411.

[16] C McNab, *Network Security Assessment*, New York : O'reilly Media Press, 2003, pp.3-7.

[17] Nessus, 2008, *Tenable Network Security*, The Network vulnerability Scanner. Accessed from http://www.nessus.org/nessus/. Accessed on 23.01.2008.

[18] SuperScan, 2008, Symantec, *Confidence in a connected network.* Accessed from http://www.symantec.com/security_response/writeup.jsp?docid=2004-120111-5455-99. Accessed on 23.01.2008.

[19] S Manzuik, A Gold, C Gatford, *Network Security assessment: from vulnerability to patch*, New York : Syngress Press, 2007, pp.75.

Dr. K. Ram Mohan Rao is born in Guntur, India on 25th May 1975. He hold Master of Computer Applications degree from Nagarjuna University, and Doctoral degree in Computer Science from Kumaun University, Nainital, India in 2009. He has research expertise in the fields of Spatial Databases, GIS Customization and dissemination including programming languages, Location Based Services, Distributed GIS and Risk Modeling.

Presently, he is working as Scientist in Indian Institute of Remote Sensing (NRSC), Dehradun, India. His interests include Open source technologies in the field of Geoinformatics. He published 15 research publications in journals and symposiums, and 4 co-edited books have been published to his credits.

Dr. Rao is a member of Indian Society of Geomatics and Indian Society of Remote Sensing.