Information Security Risk Management Framework for University Computing Environment

Umesh Kumar Singh[1], and Chanchala Joshi[2]
(Corresponding author: Chanchala Joshi)

School of Engineering and Technology, Vikram University Ujjain[1]
Madhya Pradesh 456010, India
(Email: chanchala.joshi@gmail.com)
Institute of Computer Science, Vikram University Ujjain[2]
Madhya Pradesh 456010, India

(Received Aug. 22, 2016; revised and accepted Nov. 15 & Dec. 25, 2016)

Abstract

Today's universities are on the forefront of technological advancement which makes University' computing environment vulnerable because of its large open networks. This paper analyzed the security threats specifically evolve in University's network, and with consideration of these issues, proposed risk assessment framework for University computing environment. The proposed framework reduces the risk of security breach by supporting three phase activities; the first phase assesses the threats and vulnerabilities in order to identify the weak point in educational environment, the second phase focuses on the highest risk and create actionable remediation plan, the third phase of risk assessment model recognizes the vulnerability management compliance requirement in order to improve University's security position. The proposed framework is applied on Vikram University Ujjain India's, computing environment and the evaluation result showed the proposed framework enhances the security level of University campus network. This model can be used by risk analyst and security manager of University to perform reliable and repeatable risk analysis in realistic and affordable manner.

Keywords: Security Risk; Security Threats; University Campus Network; Vulnerability

1 Introduction

With increasing development of Information Technology, computing and network applications have become an integral part of universities environment. Today's universities are on the forefront of technological advancement. The greater access to technology results in valuable learning environment, on the other hand can also results vulnerable computing environment with more security threats. University campuses are proving themselves to be some of the most technologically advanced places in the world by providing facilities like extensive Wi-Fi support, online learning using lecture capture software, digital library, classroom virtualization, web conferencing etc [23]. All these advancement makes University's computing environment particularly vulnerable because in contrast to hacking targets like banks, college and university computing environments are often large open networks. Protecting open large university campus against constantly evolving threats and vulnerabilities presents major challenges. On the other hand, the open computing university environment also supports diverse users; mainly the three distinct types of users of university are students, faculty and administration. Each of the user accesses university computing environment with varying level of university resources. Therefore, University campus network must not only provide the secure access to users but also defend them from vulnerabilities and security breaches. In the large University campus network there is need of improving risk posture and security effectiveness. It requires identification of operationally critical threats, assessment of vulnerabilities for measurement of risk level by continuous network monitoring of University campus network.

This paper proposes Quantitative Information Security Risk Assessment Model designed specifically for University computing environment, with the consideration of security dangers presents in large open campus network of University. The proposed model quantitatively measures the security risks by identifying potential threats and information processes within Universities network configuration. This model can be used by risk analyst and security manager of University to perform reliable and repeatable risk analysis in realistic and affordable manner.

2 Related Work

There are various risk assessment models available, some of which are qualitative while others are quantitative in nature; having a common goal of estimating the overall risk value [15]. OCTAVE (Operationally Critical Threat, Asset and Vulnerability Evaluation), developed by CERT is a model for risk-based infosec strategic assessment and planning [1]. OCTAVE defines assets as including people, hardware, software, information and systems. One of the major drawbacks of OCTAVATE is its complexity and it doesn't allow organizations to quantitatively model risk. In order to improve security organization system some standard principles are needed, Joshi et al. [8] analyzed the prominent taxonomies of attacks and vulnerability of computer system and network to improve vulnerability categorization and proposed novel approach towards Standardization of Network and Computer [7]. Harini et al. [5] proposed a simple, fast and efficient protocol for enhanced network architecture for authentication. One another prominent risk assessment model is [4] FAIR (Factor Analysis of Information Risk), provides framework for understanding, analyzing and measuring information risk. FAIR is built to address security concern weaknesses. The framework allows organizations to standardize the risk, apply risk assessment, view in total organizational risk, defend risk determination using advanced analysis and understand how time and money will affect the organization's security profile. The main shortcoming of FAIR is the lack of information about methodology and examples of how the methodology is applied. [6, 12] NIST RMF (National Institute of Standards and Technology's Risk Management Framework) covers a series of activities related to managing organizational risk. [21, 24, 25] TARA (Threat Agent Risk Assessment) is a risk assessment framework created by Intel that helps companies to manage risk by distilling the possible information about security attacks. The major drawback is to be prohibitively expensive and impractical to defend possible vulnerability. One of the primary tasks of risk assessment process is vulnerability scanning; Joshi et al. [9, 10] evaluated the efficiency of web application vulnerability scanners by designing a vulnerable web application. This evaluation assists in choosing vulnerability scanner during first phase of proposed model.

There are numerous risk assessment models; however, there is no mechanism to assist organizations in determining which model is the best to be employed within an organization; also these models considered the security challenges identified in hacking target organizations like banks. Although security risk assessment is crucial for these organizations but these organizations have secure and close network environment. On the other hand, higher educational institutions like Universities where information security risk assessment is major and high priority job are having large and open computing environment. The next section describes the typical scenario of University network environment comprises of diverse small network.

3 University Campus Network Setup

Figure 1 shows an ideal, large and open, University campus network setup, comprises of diverse small networks. With the rapid development of technology, universities strive to develop a convenient and valuable learning environment through IT technologies. University large computing environment includes diverse network devices, various software applications and many servers. University network is large and open, so instead of trying to scan an entire network, we classify the hosts into groups and the scan each group.

- External Scan: Scanning through a router or firewall, 208.91.199.121.
- Internal Scan: The internal scan took place at the School of Engineering and Technology (SoET) location, and was plugged into a server that resides inside Vikram University's network.

In Figure 1 the placement of the blue scanner is inside the firewall, so it can scan internal vulnerabilities and the red scanner is used for external vulnerabilities scan. These internal and external vulnerability scans are used to collect data to assess the effectiveness of current security measures taken at the Vikram University's network. The internal scan took place at the School of Engineering and Technology (SoET) location, and was plugged into a server that resides inside Vikram University's network. The objective is to avoid external security counter measures to get a detailed view at system configurations. The external scan is for determining the security posture through Internet users view. The point behind external scanning is to identify what a hacker would see if he were trying to probe Vikram University's network.

4 Proposed Quantitative Information Security Risk Management Model

The main objective behind designing a security risk assessment framework is, ”Security controls should be selected based on real risks to an organization's assets and operation”. Numerous of security risks assessment models are available but University computing environment is differ from other organizations as it is large, open and consists of several small diverse network with various users. Selecting risk assessment model without analysis, results in implementation of security controls in the wrong places, wasting of resources and leaving an organization vulnerable to unanticipated threats. The proposed risk assessment model initially analyses what is to be assessed, who

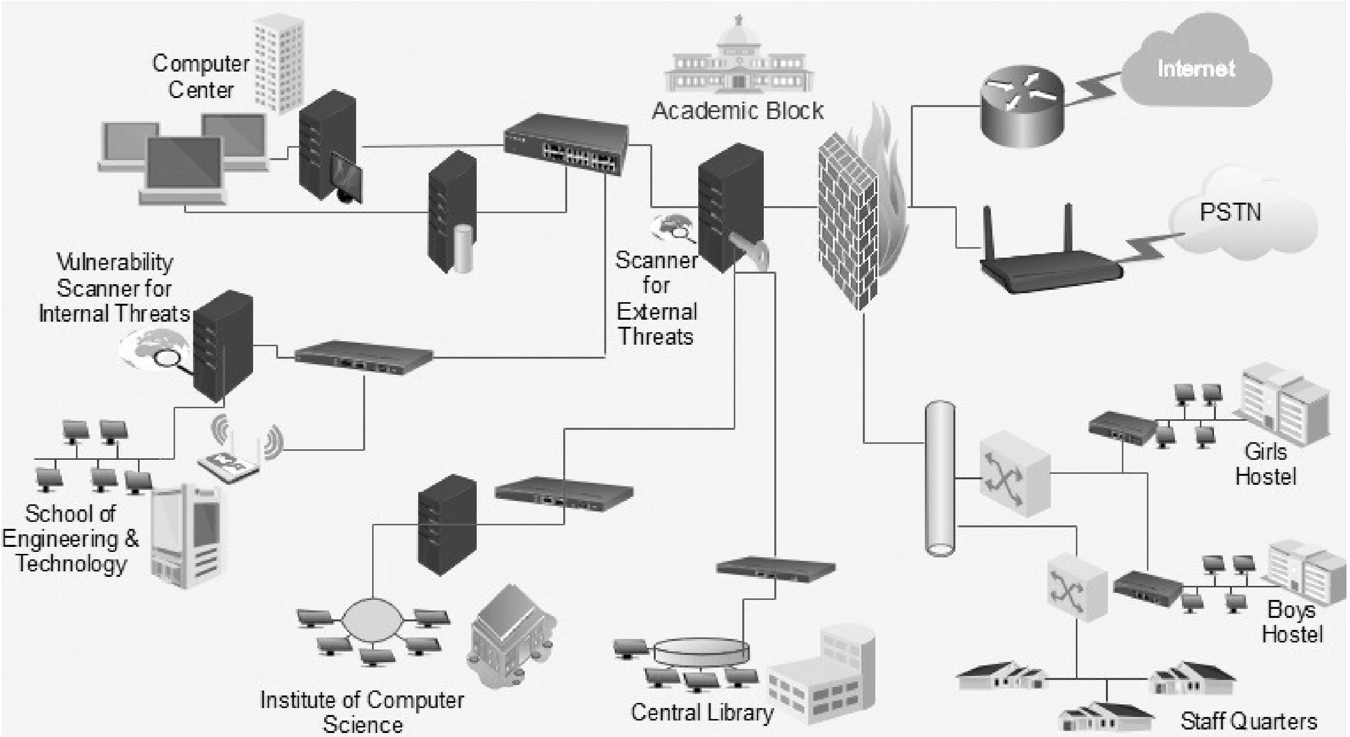

Computer Center
Academic Block
Internet
PSTN
Vulnerability Scanner for Internal Threats
Scanner for External Threats
Girls Hostel
School of Engineering & Technology
Boys Hostel
Institute of Computer Science
Central Library
Staff Quarters

Figure 1: Network setup for Vikram university computing environment

needs to be involved and the criteria for quantifying, qualifying, and comparing severity of risks. The assessment results must be documented properly. The goal of proposed framework is to measure risk level quantitatively that will allow higher educational institutes to understand security risks. The proposed model is based on the most popular risk frameworks in use today, OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation), developed at Carnegie Mellon University. The proposed framework performs three phase activities to make standard model more absolute, and provides a practical approach which can be used in real educational environment.

Figure 2 shows the abstract three phase view of the proposed model: The goal of proposed model is to reduce risks of security breach, this means understanding the cause that makes system vulnerable. The first phase focuses on knowing weak points, even in constantly changing and challenging University's environment. Then the second phase concentrates on understanding which areas are having the highest risks, based on reliable and granular real risk scoring. The proposed framework uses Common Vulnerability Scoring System (CVSS) [13, 14] to validate which vulnerability can be actively exploited. The third phase pivot along the creation of actionable remediation plan over with University environment's unique factor to and finally generate powerful reporting to track recursive risk measurement activities. The central of the proposed risk assessment framework is an objective of assessing University's campus network, recursive mechanism that collects input regarding vulnerabilities and threats and produces quantitative risk level that can be measured and treated. General steps for the proposed framework are: identifying assets and stakeholders, understanding security requirements, assessing vulnerabilities, analyzing the effectiveness of controls, evaluation of risks by estimating frequency and impact of exploit, designing remediation plans and finally drive decisions using powerful reporting. Figure 3 shows the proposed framework for Quantitative Information Security Risk Assessment.

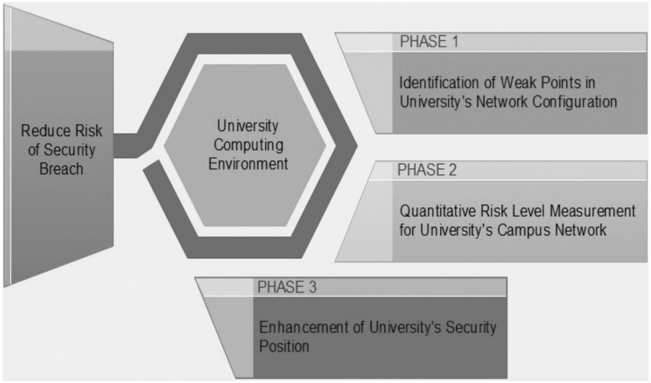

Reduce Risk of Security Breach
University Computing Environment
PHASE 1
Identification of Weak Points in University's Network Configuration
PHASE 2
Quantitative Risk Level Measurement for University's Campus Network
PHASE 3
Enhancement of University's Security Position

Figure 2: Three phases quantitative information security risk assessment model

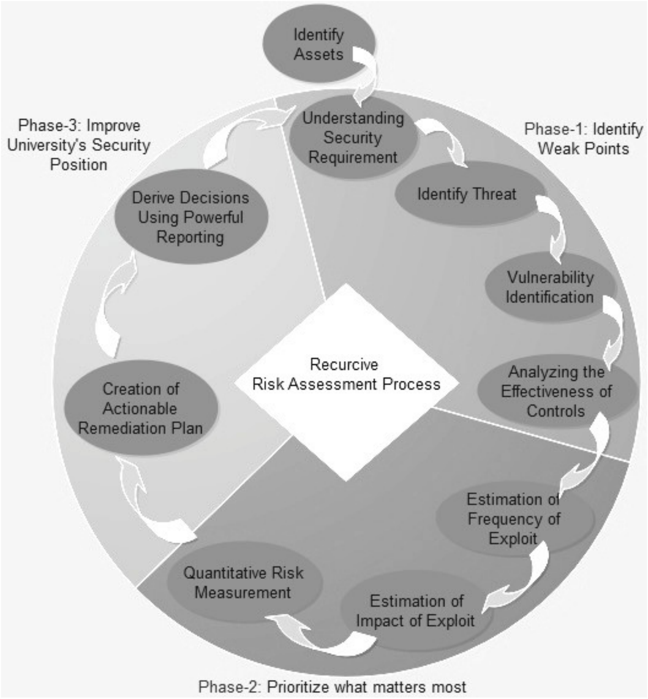

Identify Assets
Understanding Security Requirement
Phase-3: Improve University's Security Position
Phase-1: Identify Weak Points
Identify Threat
Derive Decisions Using Powerful Reporting
Vulnerability Identification
Recurcive Risk Assessment Process
Creation of Actionable Remediation Plan
Analyzing the Effectiveness of Controls
Estimation of Frequency of Exploit
Quantitative Risk Measurement
Estimation of Impact of Exploit
Phase-2: Prioritize what matters most

Figure 3: The proposed framework for quantitative information security risk assessment

4.1 Assets and Stakeholders Identification

The risk assessment techniques require to clearly specifying the assets. This step of proposed model defines the boundaries and contents of the asset to be assessed. In proposed framework information is taken as an asset.

4.2 Understanding Security Requirements

In this step, along with the resources and the information that constitute the system, the boundaries of the IT system will be identified. This step defines the scope of the risk assessment effort and provides information essential to defining the risk. The input for this step is information about hardware, software, data and information, network connections and system interfaces; and the output is a document that describes system mission, system boundary, system functions and information about criticality and sensitivity of data.

4.3 Threats and Vulnerabilities Identification

In this step, threat scenarios are created by listing the most common combinations of attack paths, attack goals and attack actor (attackers or hackers), that might lead to the compromise an asset.

4.4 Analysis of Effectiveness of Controls

In this step of assessment technical controls like authentication and authorization, intrusion detection, network filtering and routing, and encryption are considered and a document is prepared as an output which describes the effectiveness of system in defending against the particular threats.

4.5 Estimation of Frequency of Exploit

In this step, the likelihood that vulnerability can be exploited by the attacker is determined. Frequency of exploit will be calculated using mathematical formula and will be used in determining the quantitative security risk magnitude.

4.6 Estimation of Impact of Exploit

The impact can be measured by using Confidentiality Impact, Integrity Impact, and Availability Impact metrics of the CVSS [20]. The impact estimates how exploitation of a configuration issue could directly affect a targeted system and reflects the degree of loss of confidentiality, integrity, and availability. This step measures the impact of exploit onto the system.

4.7 Quantitative Risk Measurement

By the convergence of frequency and impact of exploit, quantitative security risk level can be measured. With the calculated risk magnitude the qualitative risk level can be determined in the range low to high. This risk level will be further used in creation of remediation plans.

4.8 Creation of Actionable Remediation Plan

Risk magnitude calculated in previous step prioritize the vulnerabilities which assists in defining remediation plans to validate identified vulnerabilities in order to improve system's security level. Second phase of the proposed identifies the areas are having the highest risks using Common Vulnerability Scoring System (CVSS) [20]. This risk magnitude can be used to estimate which vulnerability can be actively exploited and remediation plans will be designed using this information.

4.9 Drive Decisions Using Powerful Reporting

After completion of risk assessment procedure the results should be documented in an official report format. This report will help senior management, the mission owners in making decisions on policy, procedural, budget, and system operational and management changes. As risk assessment is recursive procedure, this final generated report will be used as an input of phase1 of proposed framework in the next cycle of risk assessment procedure.

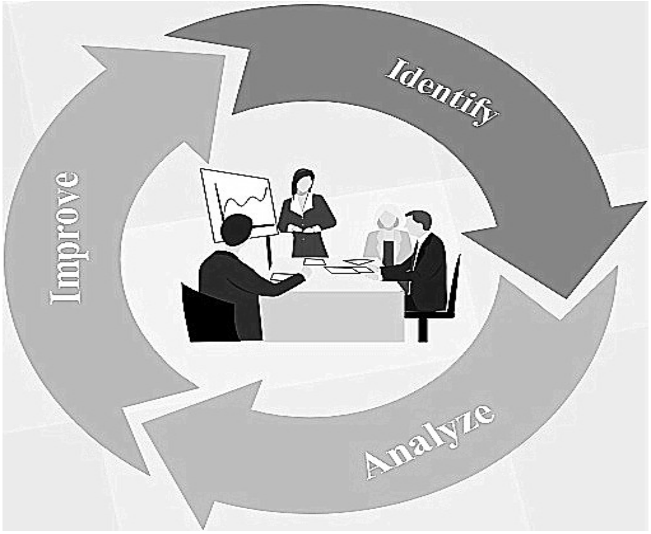


Figure 4: Ongoing risk assessment process

5 Evaluation of Proposed Quantitative Information Security Risk Assessment Model

As discussed in previous Section 2, University's network environment is continuously expanded and modified, its components changed, and its software applications replaced or updated with newer versions; these changes indicate that new risks will emerge and the previously mitigated risks may again become an issue. Thus, the risk management is ongoing and evolving process. This section emphasizes the good practice and need for an ongoing risk evaluation and assessment in order to improve security level. Figure 4 shows recursive model of ongoing risk assessment process.

In order to evaluate the importance and effectiveness of proposed model, it is applied on Vikram University Computing Environment (network setup of Vikram University shown in Figure 1).

5.1 Defining System Boundaries

The first phase of the proposed model identifies weaknesses and vulnerabilities visible and exploitable on the University computing environment. In the first step of first phase, the proposed approach for securing University campus network, determines information as an asset. The second step defines the scope of the effort, in risk assessment process. Characterizing the University's computing system establishes the scope of the risk assessment effort by identifying limits of the computing system along with resources and the information that constitute the network environment. The large and open network environment of Vikram University campus mainly suffers following security threats:

Phishing, ransomware, and malware. Cybercriminals uses emails or Web accounts that spoof official mailings for financial gain [18]. University's young students are at most of being the victim of a phishing attack that results in malware or ransomware downloads.

Wi-Fi. Vikram University provides Wi-Fi access on the University campus which is great in technology advancement view, but it can cause security problems in surprising ways.

Viruses Spreading through Social Media. Young adults of University are most avid users of social media like Facebook, Twitter and YouTube. This implies that in University's network malware can spread like wildfire through social media sites.

So Many Diverse Mobile Devices, so Much Risk. Students are early adopters of technology, and new devices are frequently visible in campus; from iPads to new android phones, daily new launched devices are having upgraded versions of operating systems that can easily infected by smart attacker and also ready to infect University's network.

Embedded Devices are Risks Prone. Embedded connectivity improves the risks for viruses and more threats for network.

5.2 Vulnerability Identification and Assessment

After identification of the plausible security threats in university environment, the next step is to perform vulnerability assessment, which determines the potential impact of loss from a successful attack. Vulnerability scans apprised the administrator to the actual state of security on network and assist in defining remediation before an attacker discovers any vulnerability first. University network is large and open, so instead of trying to scan an entire network, we classify the hosts into groups and the scan each group. It will make scanning process easier. The scanning process is performed in two steps: external scan and internal scan. Since scanning through a router or firewall could hide internal vulnerabilities, therefore, as shown in Figure 1 of Vikram University network setup, the placement of the blue scanner is inside the firewall so it can scan internal vulnerabilities and the red scanner is used for external vulnerabilities scan. These internal and external vulnerability scans are used to collect data to assess the effectiveness of current security measures taken at the Vikram University's network. The internal scan took place at the School of Engineering and Technology (SoET) location, and was plugged into a server that resides inside Vikram University's network. The objective is to avoid external security counter measures to get a detailed view at system configurations. The external scan is for determining the security posture through Internet user's view. The point behind external scanning is to identify what a hacker would see if he were trying to probe Vikram University's network. The vulnerability scan requires the use

Table 1: Discovered hosts by Nexpose

Discovered	IP address	Host Name	OS	Services	Vulns
12/8/16 5:31 PM	208.91.199.121	vikramuniv.net	Unknown	465	72
12/8/16 5:31 PM	192.168.1.4	ICS	Windows Vista	7	23
13/8/16 12:44 AM	192.168.1.1	192.168.1.1	Linux	4	0

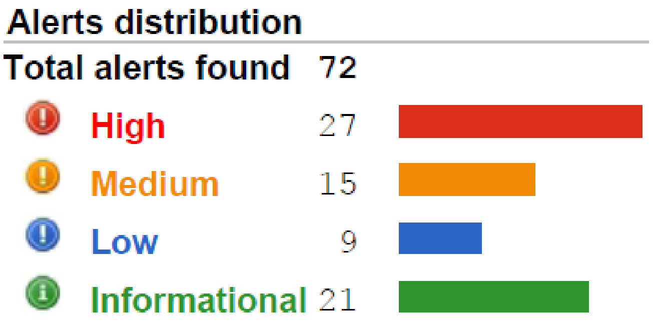
of scanning tools. The tools used to scan Vikram University were [16] Nexpose, [11] Metasploit and [9] Acunetix. The tool Nexpose is used to find hosts on the network have to be scanned for vulnerabilities. Acunetix is used for scanning web vulnerabilities while Metasploit is used along with Nexpose for penetration testing.

5.3 Major Findings

Nexpose placed within contact range of University's router, to find hosts and services on the network, discovered 35 hosts having 587 services, among which the main server of University is running with 27 high, 15 medium and 9 low vulnerability. Table 1 represents the format of result generated by Nexpose with some of the host's details.

Along with these details Nexpose generates details about active services, credentials and successful attacks. Details of vulnerabilities identified by Acunetix at host 208.91.199.121 are shown in Figure 5.

The snap shot of external scan results that summarized the identified alerts of the host 208.91.199.121 shown in Figure 6.



Alerts distribution

Total alerts found 72

High	27	🟥
Medium	15	🟧
Low	9	🟦
Informational	21	🟩

Figure 6: Web scan result of the host 208.91.199.121 by Acunetix web scanner1

Metasploit found 11 vulnerabilities during scan of the same host 208.91.199.121. Of these, 5 were critical, require immediate action because they are relatively easy for attacker to exploit and may provide them full control over the system. 5 vulnerabilities were severe, often harder to exploit and may not provide same access to affected systems. There was one moderate vulnerability discovered, provide information to attacker that may assist them in mounting subsequent attack in University network, so it should also be fixed in timely manner, but not urgent as other vulnerabilities.

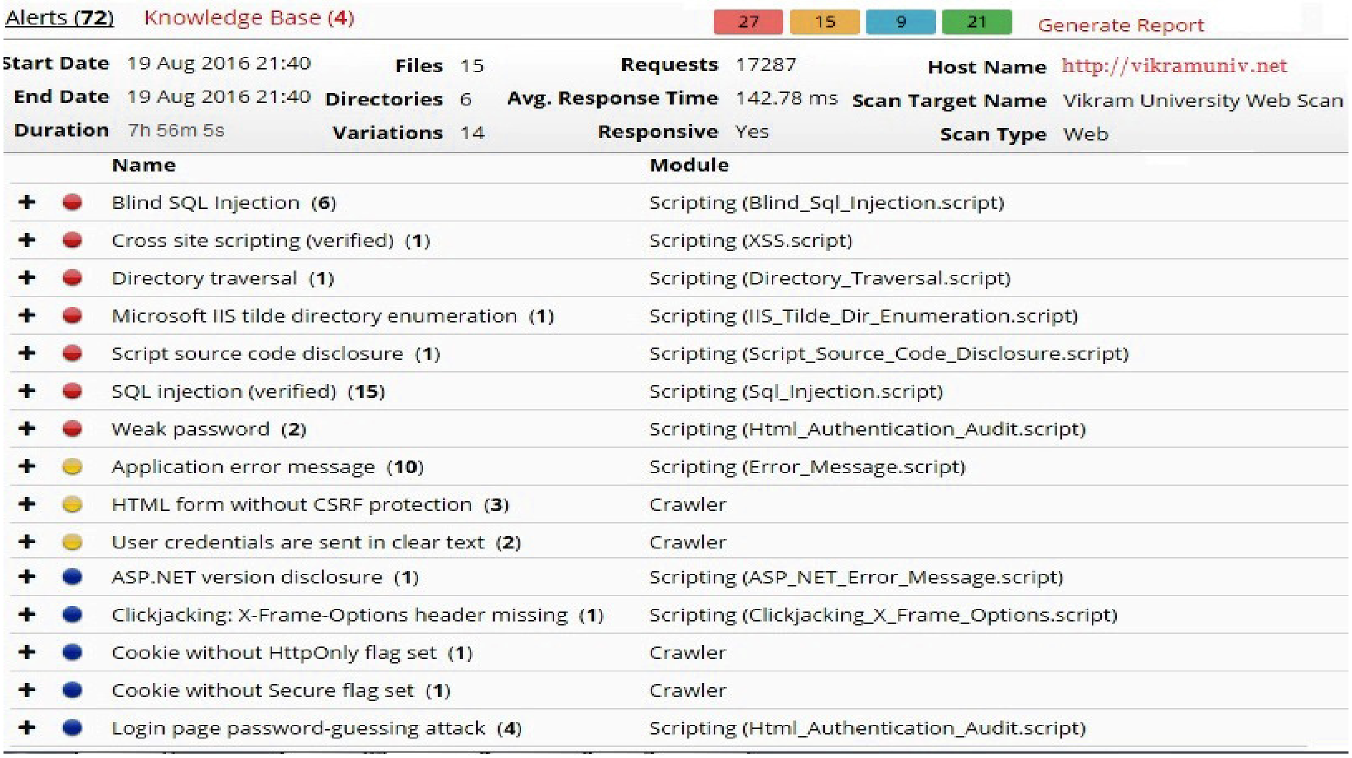
Vulnerability scanners simply identify large numbers of exposures and it is up to security teams to understand the severity of risks, which require knowledge of existing security infrastructure and additional manual effort. After identification of vulnerabilities present in Vikram University network environment, the next phase prioritized security vulnerabilities by calculating risk magnitude, along with estimation of frequency and impact of exploit.

5.4 Quantitative Risk Level Measurement

Risk assessment needed skilled individuals that understand probabilities, statistics and information technology. The first step in risk measurement requires integrating all scan results obtained from different scanners, Nexpose, Acunetix and Metasploit. Table 2 shows the scan results obtained by scanners Nexpose, Acunetix and Metasploit.

With all this vulnerability data gathered from scan results, security professional need to be able to prioritize risk by using as the Common Vulnerability Scoring System (CVSS) along with local network activity and device configurations. The risk level determines, among the identified vulnerabilities which of them actually create danger to the system and further, vulnerabilities are remediated according to the risk magnitude. Risk magnitude depends on the likelihood of the exploit, as the more frequent occurrences of vulnerability make system riskier; also, the Frequency of vulnerability depends on the date of emergence of vulnerability in the system [19]. The frequency and quantitative risk level of vulnerabilities determined by using the mathematical equations of Quantitative Security Risk Level Estimation Model [22], that computed temporal and environmental metrics to augment base CVSS scores and then derived a final risk value. The quantitative risk level score is ranging from 0 to 10; this numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. Table 3 interprets the risk rating values.

In quantitative risk level measurement along with severity of exploit, we are considering many factors like total number of alerts, affected item by exploit, affected parameter and variants identified during vulnerabilities scan. In Vikram University's computing environment the risk assessment method identified SQL injection, weak password and CSRF attacks at High risks.



Alerts (72) Knowledge Base (4) 27 15 9 21 Generate Report

Start Date	19 Aug 2016 21:40	Files	15	Requests	17287	Host Name	http://vikramuniv.net
End Date	19 Aug 2016 21:40	Directories	6	Avg. Response Time	142.78 ms	Scan Target Name	Vikram University Web Scan
Duration	7h 56m 5s	Variations	14	Responsive	Yes	Scan Type	Web

		Name	Module
+	●	Blind SQL Injection (6)	Scripting (Blind_Sql_Injection.script)
+	●	Cross site scripting (verified) (1)	Scripting (XSS.script)
+	●	Directory traversal (1)	Scripting (Directory_Traversal.script)
+	●	Microsoft IIS tilde directory enumeration (1)	Scripting (IIS_Tilde_Dir_Enumeration.script)
+	●	Script source code disclosure (1)	Scripting (Script_Source_Code_Disclosure.script)
+	●	SQL injection (verified) (15)	Scripting (Sql_Injection.script)
+	●	Weak password (2)	Scripting (Html_Authentication_Audit.script)
+	●	Application error message (10)	Scripting (Error_Message.script)
+	●	HTML form without CSRF protection (3)	Crawler
+	●	User credentials are sent in clear text (2)	Crawler
+	●	ASP.NET version disclosure (1)	Scripting (ASP_NET_Error_Message.script)
+	●	Clickjacking: X-Frame-Options header missing (1)	Scripting (Clickjacking_X_Frame_Options.script)
+	●	Cookie without HttpOnly flag set (1)	Crawler
+	●	Cookie without Secure flag set (1)	Crawler
+	●	Login page password-guessing attack (4)	Scripting (Html_Authentication_Audit.script)

Figure 5: Acunetix Web scan result of the host 208.91.199.121

Table 2: Integrated scan results

Vulnerability	Severity	Total Alerts	Category
Weak password	7.5	2	A Brute Force attack
Weak password	7.5	2	Insufficient Authentication
Cross-site Scripting(verified)	4.4	1	Cross-site Scripting
Blind SQL Injection	7.8	6	SQL Injection
SQL injection (verified)	7.8	15	
Microsoft IIS tilde directory enumeration	2.6	1	Information Leakage
Script source code disclosure	2.6	1	
Weak password	7.5	2	
Application error message	5.0	10	
ASP.NET version disclosure	0.0	1	
Microsoft IIS version disclosure	0.0	1	
Password type input with auto-complete enabled	0.0	4	
Directory traversal	6.8	1	Path Traversal
HTML form without CSRF protection	8.6	6	Abuse of Functionality
Clickjacking: X-Frame-Options header missing	6.8	1	
Login page password-guessing attack	6.8	4	

Table 3: Qualitative risk rating scale

Quantitative Risk Magnitude	**Risk Category**	**Description**
9.0 to 10.0	Critical	Risk is totally unacceptable; must require immediate action to reduce likelihood of occurrence.
7.0 to 8.9	High	Risk is unacceptable; should require remediation plan to be implemented as soon as possible.
4.0 to 6.9	Medium	Risk may be acceptable over the short period of time; require that in future actions and budget plans to reduce risk should be included.
0.1 to 3.9	Low	Risks are acceptable; plans to further reduction of risk should be implemented with other security upgrades.

5.5 Recommendations for Up-gradations

Based on the findings from the risk assessment, the next phase of the proposed framework is to identify countermeasure upgrades that will reduce the risk levels. The previous phase of risk assessment identifies SQL injection, weak password and CSRF attacks at High risks in Vikram University's network. This section presents recommendations about identified risks in order to improve University network's security.

SQL injection. Vikram University computing environment identified total 21 SQL injection security alerts and the affected items are: /Login.asp, /Register.asp, /Search.asp, /showforum.asp and /showthread.asp. SQL injection attacks reshape the SQL queries which alter the nature of the program for the benefit of the hacker [2]. Server Side defense using Prepared Statement [9] is the most effective way to protect from SQL Injections, because it ensures that intent of query is not changed.

Weak Password. In University network 6 alerts of weak password are detected in /Login.asp. There are several accounts with passwords older than thirty days and some are even close to a year old. Password cracking is one of the most common elements used to assess the current security posture [3]. The simpler way to overcome weak password vulnerability is to enforce password policies, such as password length should be more than 8 characters, contains at least one capital and one small latter, at least one numeric and one special symbol should be included while choosing password.

CSRF Attacks. Total 6 variants detected with affected items /Login.asp, /Register.asp and /Search.asp. The CSRF vulnerabilities occur when applications allow every valid session identifier request to be processes by the application business logic [17]. The main threat is concerned to the way the browser handles requests. A simple example is a web application uses the GET method in an HTTP request for transferring password information; the browser encodes form data into a URL while using GET. Since form data is in the URL, it is displayed in the browser's address bar, and information leakage occurs. The simplest solution is the use of POST method, while using the POST method, form data appears within the message body of the HTTP request, not the URL.

And finally, the risk assessment results are documented in an official report format which help senior management, the mission owners in making decisions on policy, procedural, budget, and system operational and management changes. As risk assessment is recursive procedure, this final generated report will be used as an input of phase1 of proposed framework in the next cycle of risk assessment procedure.

6 Conclusions

This paper proposed Quantitative Information Security Risk Assessment framework for University's Computing Environment. The goal of proposed model is to reduce risks of security breach, this means understanding the cause that makes University's campus network vulnerable. Applying the proposed framework onto the Vikram University campus network, it is clear that the current approaches of securing the network are ineffective in University environment's concern; as University's computing environment is differ in contrast to hacking targets like banks. The evaluation study addresses the issues found in Vikram University's network, such as enforcement of password policies, remote access management and restricting permissions to mandatory accounts. The proposed model quantitatively measured the risk magnitude for University's network configuration and can be used by risk analyst and security manager of University to perform reliable and repeatable risk analysis in realistic and affordable manner. The proposed framework can be applied to any higher educational organization or University's IT environments; it enables Universities to stay a step ahead of security threats and also to get more value from their security budget, by focusing on critical assets that are truly at risk.

Acknowledgments

The authors are thankful to MP Council of Science and Technology, Bhopal, for providing support and financial grant for the research work.

References

[1] C. Alberts and A. Dorofee, *An Introduction to the Octave Method*, Technical Report PA 15213-3890, Software Engineering Institute, Carnegie Mellon University, Taiwan USA, Aug. 2003.

[2] N. Asha, M. V. Kumar, and G. Vaidhyanathan, "Preventing sql injection attacks," *International Journal of Computer Applications*, vol. 52, pp. 28–32, Aug. 2012.

[3] Y. Asimi, A. Amghar, A. Asimi, and Y. Sadqi, "Strong zero-knowledge authentication based on virtual passwords," *International Journal of Network Security*, vol. 18, pp. 601–616, July 2016.

[4] B. Dixon, "Understanding the fair risk assessment," Nebraska CERT Conference, 2009. (`http://www.certconf.org/presentations/2009/files/TA-2.pdf`)

[5] N. Harini and T. R. Padmanabhan, "3c-auth: A new scheme for enhancing security," *International Journal of Network Security*, vol. 18, pp. 143–150, Jan. 2016.

[6] Joint Task Force Transformation Initiative, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, Technical Report NIST Special Publication 800-37 Revision 1, Feb. 2010.

[7] C. Joshi and U. K. Singh, "Admit - A five dimensional approach towards standardization of network and computer attack taxonomies," *International Journal of Computer Application*, vol. 100, pp. 30–36, Aug. 2014.

[8] C. Joshi and U. K. Singh, "A review on taxonomies of attacks and vulnerability in computer and network system," *International Journal of Advanced Research in Computer Science and Software Engineering*, vol. 5, pp. 742–747, Jan. 2015.

[9] C. Joshi and U. K. Singh, "Analysis of vulnerability scanners in quest of current information security landscape," *International Journal of Computer Application*, vol. 145, pp. 1–7, July 2016.

[10] C. Joshi and U. K. Singh, "Performance evaluation of web application security scanners for more effective defense," *International Journal of Scientific and Research Publications*, vol. 6, pp. 660–667, June 2016.

[11] D. Kennedy, J. O'Gorman, D. Kearns, and M. Aharoni, *Metasploit The Penetration Tester's Guide*, San Francisco: William Pollock, 2011.

[12] Computer Security Division (Information Technology Laboratory), *Risk Management Framework (RMF)*, Technical Report SP 800-37 Rev. 1, Oct. 2016.

[13] P. Mell, K. Scarfone, and S. Romanosky, "Common vulnerability scoring system," *IEEE Security and Privacy*, vol. 4, pp. 85–89, Nov.-Dec. 2006.

[14] P. Mell, K. Scarfone, and S. Romanosky, "Cvss: A complete guide to the common vulnerability scoring system version 2.0," *Forum of Incident Response and Security Teams (FIRST)*, 2007.

[15] F. Nabi, M. M. Nabi, "A process of security assurance properties unification for application logic," *International Journal of Electronics and Information Engineering*, vol. 6, no. 1, pp. 40–48, 2017.

[16] W. Rosenberry, *Nexpose: Vulnerability Management and Penetration Testing System v.5.1 Security Target*, Technical Report 545 Boylston Street, Suite 400 Boston, MA 02116, May 2012.

[17] K. Sentamilselvan, P. S. Lakshmana, and N. Ramkumar, "Cross site request forgery: Preventive measures," *International Journal of Computer Applications*, vol. 106, pp. 28–32, Nov. 2014.

[18] J. Singh, "Cyber-attacks in cloud computing: A case study," *International Journal of Electronics and Information Engineering*, vol. 1, no. 2, pp. 78–87, 2014.

[19] U. K. Singh and C. Joshi, "Quantifying security risk by critical network vulnerabilities assessment," *International Journal of Computer Applications*, vol. 156, no. 13, pp. 26–33, Dec. 2016.

[20] U. K. Singh and C. Joshi, "Information security assessment by quantifying risk level of network vulnerabilities," *International Journal of Computer Application*, vol. 156, pp. 37–44, Dec. 2016.

[21] U. K. Singh and C. Joshi, "Measurement of security dangers in university network," *International Journal of Computer Applications*, vol. 155, no. 1, pp. 6–10, Dec. 2016.

[22] U. K. Singh and C. Joshi, "Quantitative security risk evaluation using cvss metrics by estimation of frequency and maturity of exploit," in *Proceedings of the World Congress on Engineering and Computer Science (WCECS2016)*, San Francisco, USA, Oct. 2016.

[23] D. Stiawan, Y. Idris, H. Abdullah, and M. AlQurashi, "Penetration testing and mitigation of vulnerabilities windows server," *International Journal of Network Security*, vol. 18, pp. 501–513, May 2016.

[24] T. T. Taiwhenua, *Risk Assessment Process*, Technical Report 3.0 NZ, Internal Affairs, NewZealand Government, Information Security, Feb. 2014.

[25] J. Wynn, J. Whitmore, G. Upton, L. Spriggs, and D. McKinnon, *Threat Assessment and Remediation Analysis Tara*, Technical Report 031180SE-K1, Oct. 2011.

Biography

Umesh Kumar Singh received his Doctor of Philosophy (Ph.D.) in Computer Science from Devi Ahilya University, Indore(MP)-India. He is currently Associate

Professor in Computer Science and Director in School of Engineering and Technology, Vikram University, Ujjain(MP)-India. He has authored 6 books and his about 100 research papers are published in national and international journals of repute. He was awarded Young Scientist Award by M.P. council of Science and Technology, Bhopal in 1997. He is reviewer of various International Journals and member of various conference committees. His research interest includes Computer Networks, Network Security, Internet and Web Technology, Client-Server Computing and IT based education.

Chanchala Joshi received her Master of Science in Computer Science and Master of Philosophy in Computer Science from Vikram University, Ujjain(MP)-India. She is currently Junior Research Fellow and doctoral student in Institute of Computer Science, Vikram University, Ujjain(MP)-India. Her research interest includes network security, security measurement and risk analysis.