Quantifying Security Risk by Critical Network Vulnerabilities Assessment

Umesh Kumar Singh
School of Engineering and Technology
Vikram University Ujjain, M.P. India

Chanchala Joshi
Institute of Computer Science
Vikram University Ujjain, M.P. India

ABSTRACT
Network vulnerability is the weaknesses in the network configuration that inadvertently allows dangerous operations and poses serious security threats. An attacker can exploit these vulnerabilities to gain unauthorized access to the system. Hence, detection and remediation of network vulnerabilities is critical for network security. This paper proposed method for effective risk level estimation by using a new introduced metric, the Hazard Metric (HM) which identifies the probability of attacks in user environments. As in network environment the number of attacks scenario increases, there is higher probability of compromising a target and thus the overall security of the network reduces. Thus, there is a need for quantification of security level of a specific network. The HM measures the probability of successful exploits by estimation of impact and likelihood of the attacks, which is to quantify the degree of security strength against vulnerability exploit in a network system. The proposed method prioritizes the mitigation of discovered vulnerabilities according to their risk levels. The methodology is tested in Vikram University Ujjain, India's network environment. The results represent the system trustworthiness.

Keywords
CVSS score; risk level; security measurement; security metrics; vulnerability

1. INTRODUCTION
With the growth of information system most of our everyday activities depend on services provided by computer networks. With increasing dependency on IT infrastructure, the main objective of a system administrator is to maintain a stable and secure network, with ensure that the network is robust enough against malicious network users like attackers and intruders. Security risk management presents a way to manage the increasing threats to infrastructures or system. The first step towards security risk management is the identification of vulnerabilities presents in the system. Now days many network security scanners like Nessus [1], Appscan [2], Acunetix [3], Netsparker [4] etc. provide an efficient way for vulnerabilities detection local to the system. Prioritization of detected vulnerability according to severity level is essential for applying remediation plans to maintain the security level of the system. The Common Vulnerability Scoring System (CVSS) allows administrator to prioritize vulnerabilities by severity score. The CVSS score of vulnerability is a standard measure and not defined for specific network configuration; although the frequency and impact of vulnerability affect the security risk level of specific network. Along with the severity score there are many factors like maturity and frequency of vulnerabilities present in the system [5] and the impact of detected vulnerability on to the system [6] affect the security risk level of the organization's infrastructure. Therefore, for efficient network security risk management, involvement of these factors with CVSS severity score is advisable in the risk level estimation computations. Information about the network architecture and the vulnerabilities affecting the system are the important factors of risks to predict the possible, future occurrence of events; the proposed work integrating this information to Hazard Metric, which determines the adverse effects on vulnerable and exposed elements. Hazard is the component of risk and the intensity of hazard can be determined by network environment degradation and intruder intervention in the system i.e. Hazard defines the chances of system being in danger because of environmental events in a network. Depending on the network environment the severity level of vulnerability varies for different networks because of Hazard events, so the risk level estimation should be personalized for diverse networks. This paper identified network intrinsic factors that can affect the security strength of the specific network system. With these intrinsic characteristics, a new Hazard Metric is defined for effective network security risk level estimation, which measures the probability of attack in user environments. Hazard Metric measures the probability of exploiting the vulnerability by attacker using the critical resources of a specific network. The main attributes of Hazard Metric are, Maturity Level (ML) of vulnerability in specific network environment, Frequency of Exploit (FE) in user's network, exploitability impact (EI) of vulnerability on to the specific network system, amendment level (AL) of a particular network configuration and authentication level (AuL). Amendment Level is an important vector of Hazard Metric which measures the degree of resistance that a specific network have against vulnerability; the Authentication Level measures the level of privileges required by an attacker before successfully exploiting the vulnerability. Having all these attributes Hazard Metric estimates the security strength of specific network by determining the probability of vulnerability exploitation in the specific network environment's circumstances.

With the new proposed Hazard Metric (HM), this paper proposed an algorithm for network security risk level estimation in section IV-B. The proposed approach measures the risk level of the network security in generic environment that may vary from individual systems to organization's wide systems, to the whole geographic. The tool predicts the probability of exploit and computes the risk level to improve security of existing system and to minimize adverse effect from these probable exploits.

2. RELATED WORK
Risk evaluation is an important factor of network security measures; many researchers have done important work in the field. The first step towards network security risk level measurement is vulnerability prioritization, followed by vulnerability categorization. Joshi et al. [7] proposed a five

dimensional approach for vulnerabilities categorization with attack vector, defense, methodology used for vulnerability exploitation, impact of vulnerability on to the system, and the target of attack. In the field of vulnerability categorization [8] evaluates some of the prominent taxonomies, this assessment is helpful for proper categorization of vulnerabilities presents in network system environment. There are many vulnerability scanners available for identification and assessment of vulnerabilities. Selection of these vulnerability scanners plays an important role in network security management. [9] Evaluated the performance of three prominent web vulnerability scanners Netsparker, Acunetix and Burp Suit, the evaluation study suggested that performance of vulnerability scanners vary for different vulnerability categories. Prioritization of vulnerabilities is done according to CVSS severity score. Tripathi et al. [10] analyzed the trends of vulnerability classes across six CVSS base metrics which is helpful in identifying most critical class of vulnerability relative to system environment. In [11] Tripathi et al. proposed a model for quantitative security measurement for prioritization of vulnerability mitigation. In a step further towards risk evaluation Tupper et al. [12] proposed a quantitative security metric, VEA-bility (Vulnerability, Exploitability, Attackability), which measured the desirability of different network configurations that can be used to estimate the comparative desirability of a specific network configuration. Wang et al. [13] have proposed an approach to measures the likelihood of compromising a network in terms of the fraction of attackers reaching the goal, which can be used to estimate the risk level of network system.

Many researchers attempted to evaluate network security; however discussed approaches do not measure the personalized security risk level that can estimate the probability of vulnerability exploitation for specific network environment, although all these research work done in the field of risk level estimation is the inspiration behind our proposed work. In proposed work, we attempt to provide a risk level estimation scheme for security strength measurement and prioritization of risk mitigation.

3. EXISTING STANDARD SECURITY RISKS METRICS

Pagett et al. [13] examined security metrics that IT security managers used most frequently to gauge the effectiveness of their organizations overall security efforts. They stated that there's a strong correlation between security products and metrics. Depending on the network configuration the severity level of vulnerability varies for different networks, so the risk level estimation should be personalized for diverse networks configurations. The main attributes of existing security metrics are: time taken to patch, policy violations, uninfected endpoints, reduction in the cost of security, end users training, and reduction in unplanned system downtime. One of the most prominent risks measuring metric is Common Vulnerability Scoring System (CVSS) [14] that standardize the efforts for vulnerability by providing an open framework for measuring severity of vulnerabilities. CVSS contains three metric groups: Base metric group, Temporal metric group and Environmental metric group. The Base group reflects the intrinsic properties of vulnerability, the Temporal group represents the dynamic behavior of a vulnerability that changes over time, and the Environmental group defines the unique user's environment characteristics of a vulnerability. The Base metrics generate a score 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. However, CVSS generally treat vulnerabilities in isolation, without considering attack interdependencies on target networks.

This paper focuses on network intrinsic factors that can affect the security strength of the specific network system and defined Hazard Metric, which measures the probability of attack in user environments. Hazard Metric measures the probability of exploiting the vulnerability by attacker using the critical resources of a specific network.

4. DEFINING NEW HAZARD METRIC

Literature survey found number of organizational issues which exist with the use of security metrics in measuring security risks level, which can be summarized as follows:

- Metrics used for measuring the security effectiveness are difficult to define.
- Measurement results are difficult to interpret by non-security professionals.
- Metrics effectiveness cannot be easily compared to evaluate the organization's performance.

Computer network security is notoriously difficult to quantify. Literature review finding states that metrics exists to measure risk level of individual vulnerability but in order to evaluate risk level of whole network system, no standard metrics are available. The study in the field concluded that there is a gap in current security metrics and management in a concern that how to measure the effectiveness of security controls. This paper introduces Hazard Metric, which assists security personal in defining the probability of exploits that can danger the security level. Hazard metric predicts the possible, future occurrence of events that may have adverse effects on vulnerable and exposed elements.

4.1 Attributes

The main attributes of Hazard Metric are:

1) Maturity Level (ML)
2) Frequency of Exploit (FE)
3) Exploitability impact (EI)
4) Amendment level (AL)
5) Authentication level (AuL)

Maturity Level (ML) defines the age of vulnerability and can be measured by date of vulnerability exploitation on to the network system. Frequency of Exploit (FE) computes the likelihood of exploit in user's network environment. Exploitability impact (EI) defines the impact of exploit on specific network configuration. Amendment level (AL) measures the degree of resistance that a specific network have against vulnerability. Authentication level (AuL) determines the level of privileges required by an attacker before successfully exploiting the vulnerability. Having all these attributes Hazard Metric estimates the security strength of specific network by determining the probability of vulnerability exploitation in the specific network environment's circumstances.

4.1.1 Metric Computation

The proposed Hazard Metric of security risks level measurement consists of 5 basic vectors: Maturity Level (ML), Frequency of Exploit (FE), Exploitability impact (EI), Amendment level (AL), Authentication level (AuL).

1) Computation of Maturity Level (ML) vector

Maturity Level of vulnerability defines the age of vulnerability, which is the ratio of the date of emergence of vulnerability and date of vulnerability exploitation in the user's network system.

$$\text{Maturity Level} = \frac{\text{total\_days (Emergence Date)}}{\text{total\_days(Date of exploit)}}$$

Date of vulnerability exploitation in system's network can be determined by proper monitoring of network system using an automated tool like vulnerability scanners, in our work we are using Nessus [1] vulnerability scanner for determining date of exploit in our network environment. The emergence date of vulnerability can be taken from vulnerability databases, National Vulnerability Database (NVD) [14] which uses the Common Vulnerabilities and Exposures (CVE) [15] is one of the most prominent databases that accounts the date in which the vulnerability is first reported. The work in the paper, taken published date of vulnerability from NVD.

2) Computation of Frequency of Exploit (FE)

Frequency of Exploit (FE) reflects the likelihood of exploit in user's network environment. The idea behind including frequency of exploit in the proposed Hazard Metric is that the more frequent occurrences of vulnerability make system riskier. We described the method of frequency calculation of exploit in our previous paper [16], by the mathematical formula:

Frequency= (AV * AC * PR) + Temporal Score

Here, Attack Vector (AV), Attack Complexity (AC) and Privileges Required (PR) are the attribute of CVSS Metric [13]. In this paper we modified Temporal score by Maturity Level (ML) vector calculated in previous step:

Frequency= (AV * AC * PR) + ML

Here we are replacing the Temporal Score by Maturity Level vector, because the proposed Hazard Metric computes the probability of exploit in specific network configuration, hence, we are also considering date of emergence in user's environment.

3) Computation of Exploitability Impact (EI)

Exploitability Impact (EI) defines the impact of exploit on specific network configuration. Computation of Exploitability Impact involves the base vector of CVSS metric: Confidentiality Impact (CI), Integrity Impact (II) and Availability Impact (AI), along with the environmental vectors: Confidentiality Requirement (CR), Integrity Requirement (IR) and Availability Requirement (AR). In our paper [17] we described the method of impact computation by the mathematical formula:

Exploitability Impact = ((CI*CR) + (II*IR) + (AI*AR)) * ML

Computation of Exploitability Impact includes additive method because the impact of vulnerability on to the network environment is very important factor. The vulnerabilities having low impact can be avoidable during security risks mitigation plans.

The overall calculated impact value finally product with the Maturity Level of vulnerability, computed in first section of Metric Computation; because, the higher value of maturity of vulnerability is having more impact on the security risks level of system.

4) Computation of Amendment Level (AL)

Amendment Level (AL) measures the degree of resistance that a specific network have against vulnerability. It represents the effort that an attacker requires for successful execution of the exploit. We are computing the Amendment Level vector by using attack graph. Attack graph represents the overall security of network and provides a way to represents correlated attacks [18]; it consists of a number of attack scenarios each of which is represented by an attack path. More number of attack scenarios and corresponding attack paths show the higher probability of security risks [19]. Computation of Amendment Level involves the following steps:

Step1: Exploit condition identification

Step2: Identifying exploits relation with nodes and determining correlated exploits

Step3: Attack graph creation

Step4: Measurement of Amendment Level vector

In order to identify the exploit condition, each node in the network has to be detected and followed safe data transaction rules. Then, the combinations of exploit conditions that occurred on multiple nodes are determined. Every occurred exploits added to the attack graph, which is represented by attack paths; finally, by connecting all individual nodes graph a complete attack graph is generated. This generated graph can be used to classify vulnerabilities, which can occur by possible attacks and it also determines the further attacks measures [20]. This attack graph is tested with different exploit conditions.

We are considering that the Amendment Level of an individual exploit is the set of some initial conditions required for having an exploit; these conditions are generally not implied by other exploits. That means, Amendment Level measures the resistance of individual exploit in user's environment. Suppose, for an exploit e, R (e) represents the resistance of e and CR (e) represents the cumulative resistance of e and C (e) represents the condition for successful exploit; then, we defined an Amendment Level (AL) vector, which maps an exploits to another exploit and its resistance value as:

AL= (R (e) * C (e)) / CR (e)

The calculated vector AL represents the final security resistance strength of the current network.

5) Computation of Authentication Level (AuL)

Authentication Level (AuL) determines the level of privileges required by an attacker before successfully exploiting the vulnerability. We are converging Authentication Level (AuL) vector to the proposed Hazard Metric, because for successful exploits attacker must have to capture Authentication resources. For Authentication Level vector computation, we are considering two basic vectors Privileges Required (PR) and User Interaction (UI) of CVSS metric. We are integrating these two basic vectors to the Environmental metric vectors: Confidentiality Requirement (CR), Integrity Requirement (IR) and Availability Requirement (AR) of CVSS. The quantitative measurement of Authentication Level (AuL) can be calculated as:

AuL= (PR * UI) + (CR* IR * AR)

Here, PR and UI are the primary attributes of Authentication Level computation equation; whether CR, IR and AR vectors represent environment specific requirement for successful exploit.

4.2 Complete Framework of Hazard Metric

Fig 1 shows the complete framework of the proposed Hazard Metric. The Base Metric and Environmental metric are the

component of standard CVSS metric [13]. CVSS generates standard severity score, which is universal. In our work, we are redefining these attributes in specific network environment of user. One of the major activities while calculating Hazard Metric is the computation of Amendment Level, which is measured by generating attack graph. In Hazard Metric computation inclusion of attack graph method gives resistance of individual exploit in user's environment, also, it correlates the exploits. The correlation of exploits reflects the possible conditions that can use by attacker to exploit. The knowledge of Amendment Level improves the security resistance strength of the current network.

Having all these attributes Hazard Metric estimates the security strength of specific network by determining the probability of vulnerability exploitation in the specific network environment's circumstances. Following Fig represents the overall framework of proposed Hazard Metric:

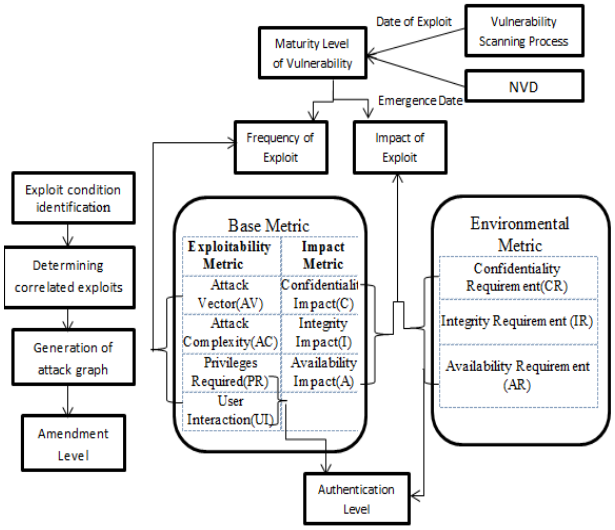

Fig 1: Complete framework of the proposed Hazard Metric

5. SECURITY RISKS MEASUREMENT WITH PROPOSED HAZARD METRIC

Risk management is basically integration of three major activities: the identification of risk, design of strategies to manage risks and mitigation of risk. Risks identification is done by assessment of vulnerabilities, using automated tool such as vulnerabilities scanners. After assessment, vulnerabilities are prioritized in order to make strategy plans to manage risks. The strategies involve estimating probability of risk events occurrences, risk avoiding activities, reducing adverse effect of the risk and determining the consequences of a risk. However, the overall purpose of risk management is to reduce risks to a level accepted by the organization.

All risk management activities are based on one prominent activity, estimating the probability of occurrences of risk events. This paper defines a new Hazard Metric (HM) for quantitative risk measurement, which identifies the probability of occurrences of risk events in user environments. Attributes of Hazard Metric are, Maturity Level (ML) of vulnerability in user environment, frequency of exploit (FE), exploitability impact (EI) of vulnerability on to the users' network, amendment level (AL) of network environment against the attacker and authentication level (AuL) of network system which measures the level of privileges required by an attacker before successfully exploiting the vulnerability. All these factors together measure the probability of occurrences risk events i.e. Hazard in specific network environment.

Hazard Metric= (FE* EI) / (AL + AuL)

Higher frequency of exploit makes system more risky, in the same way exploit having High impact must have to be considerable; therefore, we are multiplying these two major attributes in Hazard Metric computation equation. While the higher value of Amendment Level indicates that system is highly resistance for an exploit, i.e. system considers most of the conditions require to having a successful exploit, therefore reduces the probability of exploit. In the same way, the higher value of Authentication Level reflects that system implements some security plans, so the privileges cannot be easily acquired by the attacker. Hence, higher value of Authentication Level vector also reduces the probability of exploit. With these considerations, we are dividing the sum of Amendment Level and Authentication Level vectors, while measuring the Hazard Metric.

Along with the calculated Hazard Metric and standard CVSS severity score, the final security resistance strength of the current network will be measured.
In our previous paper [17], we derived Risks Measurement equation. Now, with the proposed Hazard Metric having all these network dependent attributes, we are modifying the Risks Measurement equation, which measures the security level of specific network environment:

Risks Level Measures= Minimum ((Hazard x Risk Level), 10)

In Risk Level Measures, risk is therefore characterized by two parameters:

i. The probability of occurrence of risk events computed using proposed Hazard Metric
ii. The severity of the possible adverse consequences calculated using existing Risk Level equation.

The above Risks Level Measures equation calculates the quantitative risk level along with the maturity of exploit, frequency and impact of vulnerability, amendment level and authentication level of system, and severity of exploit. The total risk is the products of the Risk Level multiplied by their probabilities.

6. EVALUATION OF PROPOSED METHOD

The proposed method is implemented in Vikram University Ujjain, India computing environment [21]. The idea behind selection of educational institution is that the large and open network of University's computing environment is particularly vulnerable. 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 fig.2 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 Universitys 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.

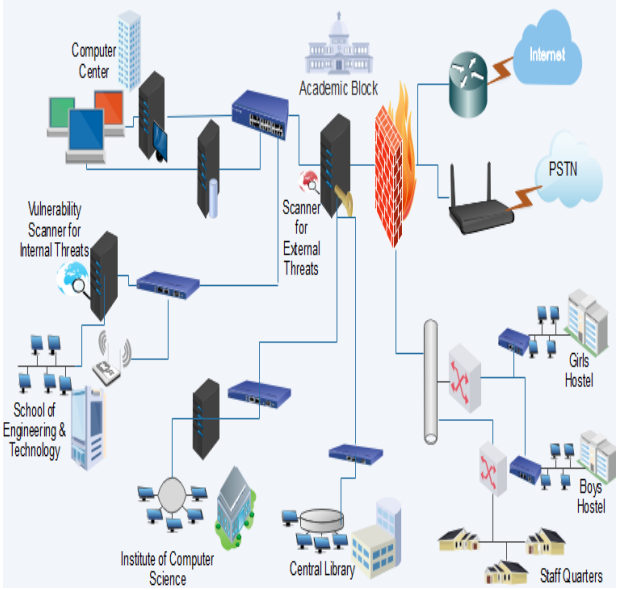

Fig.2. Network Setup for Vikram University Computing Environment

In our work, we are analyzing the security of academic institution Vikram University Ujjain, India campus network's web server 208.91.199.121. We are using Nessus, Acunetix and Nexpose vulnerability scanner for identification of vulnerabilities in university computing environment.

6.1 External Scan

Nessus placed within contact range of University, and generates details about active services, credentials and successful attacks. Scanning activities result that the server 208.91.199.121 has two open ports, tcp80 listening to HTTP traffic and tcp22 listening to SSH traffic. In University system, the SSH connection allows system administrators to do maintenance work remotely from within the subnet administration. The SSH service has vulnerabilities CVE-2012-5975, CVE-2014-6271 and CVE-2015-5600. CVE-2012-5975 allows remote attackers to bypass authentication via a crafted session involving entry of blank passwords; CVE-2015-5600 does not properly restrict the processing of keyboard-interactive devices within a single connection, which makes it easier for remote attackers to conduct brute-force attacks or cause a denial of service; and CVE-2014-6271 allows remote attackers to execute arbitrary code via a crafted environment. HTTP service has vulnerabilities CVE-2016-5387 and CVE-2015-3183. CVE-2016-5387 allows remote attackers to redirect an application's outbound HTTP traffic to an arbitrary proxy server via a crafted Proxy header in an HTTP request; and CVE-2015-3183 allows remote attackers to conduct HTTP request smuggling attacks via a crafted request. Both of these HTTP service vulnerabilities are present in the Apache HTTP Server. Here is the snapshot of the results generated by Nessus:

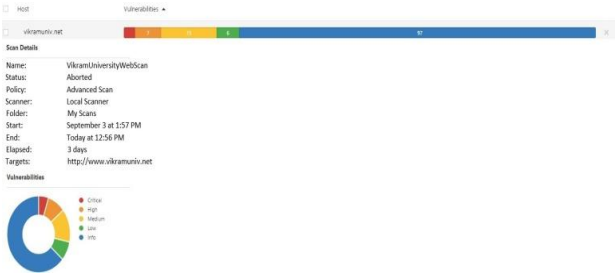

Fig 3: Nessus Scanning Results

The proposed method is regarded by network security persons of Vikram University, as in large and open network of University's environment the primary focus is on availability of information but low demand of confidentiality. The Base vector of CVE-2012-5975 is exploitability AV:N, AC:M, Au:N and impact CI:C, II:C, AI:C; The Temporal vector is E:ND, RL:ND, RC:ND; The Environment vector is CR:L, IR:ND, AR:L. Table II summarizes the input for calculating risks using Network Security Risk Level Estimation Tool:

Table 1. Summary of Inputs for Risk Calculation

CVE-ID / Vectors	CVE-2012-5975	CVE-2014-6271	CVE-2015-5600	CVE-2016-5387	CVE-2015-3183
AV	Network N	Network N	Network N	Network N	Network N
AC	Medium M	Low L	Low L	High H	Low L
Au	None N	None N	None N	None N	None N
CI	Complete C	Partial P	Partial P	Partial P	None N
II	Complete C	Complete C	None N	Partial P	Partial P
AI	Complete C	Complete C	Complete C	Partial P	None N
RL	Low L	NotDefined X	Medium M	NotDefined X	Medium M
IR	NotDefined X	NotDefined X	NotDefined X	NotDefined X	Medium M
AR	Low L	Low L	Medium M	NotDefined X	Medium M
CVSS Severity	9.3 HIGH	10.0 HIGH	8.5 HIGH	8.1 HIGH	5.0 MEDIUM

Besides the severity of vulnerability the major factors that affect system's security and can increase risk level of system failure are: frequency, impact, amendment level and authentication level; these factors represent the security level of organization. For risk evaluation we are considering 3 SSH and 2 HTTP service vulnerabilities; frequency of exploit (FE), exploitability impact (EI) of vulnerability on to the users' network, amendment level (AL) of network environment against the attacker and authentication level (AuL) of network system of these vulnerabilities are calculated using proposed methodology, which are shown in the Table III. The first column of the table represents information about CVE-ID of vulnerability; second column contains CVSS score of vulnerability; third column represents the published date of vulnerability, which is taken from NVD; fourth column shows the likelihood of vulnerability Vikram University's network; fifth column shows the computed impact onto the system; sixth and seventhes columns represent the Amendment Level and Authentication Level against vulnerability respectively.

Table 2. Risk Level Calculation

CVE-ID	CVSS Score	Published Date	FE	EI	AL	AuL	Risk Score
CVE-2012-5975	9.3	12/04/2012	0.73	0.46	Medium	Low	10.0
CVE-2014-6271	10.0	09/24/2014	0.02	0.30	X	X	8.7
CVE-2015-5600	8.5	08/02/2015	0.10	0.64	Low	X	8.9
CVE-2016-5387	8.1	07/18/2016	0.01	0.01	High	X	5.4
CVE-2015-3183	5.0	07/20/2015	0.42	0.80	Medium	Medium	6.4

6.2 Internal Scan

We are using Nessus, Acunetix and Nexpose vulnerability scanner for identification of internal vulnerabilities in university computing environment. Here are the snapshots of the results generated by Acunetix scanner:

Fig 4: Acunetix Web Vulnerability Scanner's scanning results

Acunetix web vulnerability scanner detected total 72 vulnerabilities, out of which 27 are ciritical, 15 are high, 9 are medium while 21 are low priority vulnerabilities.

The following table summarizes the scanning results of Nessus, Acunetix and Nexpose vulnerabity scanners:

Table 3. Internal 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	

6.3 Observations

In Table II, vulnerability "CVE-2016-5387" has severity score 8.1 released on 07/18/2016 and the qualitative severity level of the vulnerability is High. It was discovered that httpd used the value of the Proxy header from HTTP requests to initialize the HTTP_PROXY environment variable for CGI scripts, which in turn was incorrectly used by certain HTTP client implementations to configure the proxy for outgoing HTTP requests. A remote attacker could possibly use this flaw to redirect HTTP requests performed by a CGI script to an attacker-controlled proxy via a malicious HTTP request. The frequency of CVE-2016-5387 is 0.01 in Vikram University's network, as well as Amendment Level is High either because of availability of patch or having very low impact onto the system, the qualitative severity level of vulnerability is High but after applying the proposed method, we found that the frequency and impact of vulnerability in University's computing environment is very low, which results CVE-2016-5387 is medium category vulnerability for Vikram University's network configuration.

The following chart compare the calculated severity score using

proposed Hazard metric with standard CVSS score:

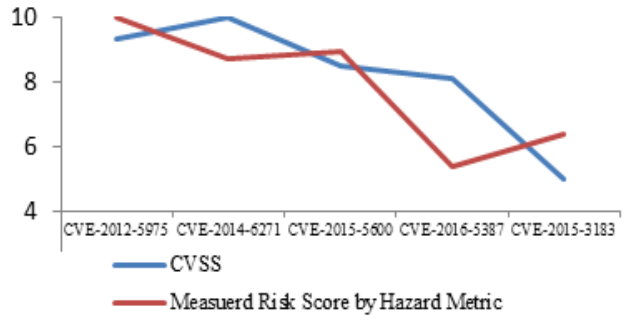

Fig 5. CVSS v/s Hazard Metric

This evaluation study shows that the proposed quantitative risk level estimation will be helpful to network administrator for design and implementation of remediation plans, as it provides an effective way for risk level evaluation.

7. CONCLUSION

This paper proposed method for effective risk level estimation by using Hazard Metric (HM) which identifies the probability of successful exploits in user environments. Along with the proposed Hazard Metric and standard CVSS severity score, the final security resistance strength of the current network will be measured. We evaluate the computation of Hazard Metric in Vikram University, India computing environment [21]. Computation of Hazard Metric vectors identify the loopholes in network security such as Amendment Level, Authentication Level reflects the security level in manageable form. Also, frequency and impact estimation of vulnerability reflects the vulnerable points in network which helps in developing the strategies to manage risks. The strategies involve estimating probability of risk events occurrences, risk avoiding activities, reducing adverse effect of the risk and determining the consequences of a risk. However, the overall purpose of risk management is to reduce risks to a level accepted by the organization.

In present scenario, there is a gap in current security metrics and management in a concern that how to measure the effectiveness of security controls. With all the considerations about the attributes of user's environment that can affect the security of network system, we developed the proposed Network Security Risk Level Estimation Method that measures the security level of specific network environment and enables the assessment of security risks. The proposed approach will help to network administrator by measuring risk level of the network security in generic environment, varying from individual systems to organization's wide systems. The method predicts the probability of exploit and computes the risk level to improve security of existing system and to minimize adverse effect from these probable exploits. The proposed approach for risk evaluation can be used to assess how much one should believe in system trustworthiness.

8. ACKNOWLEDGMENTS

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

9. REFERENCES

[1] Nessus Vulnerability Scanner, http://www.tenable.com/products/nessus-vulnerability-scanner

[2] IBM Rational AppScan, 2008, http://www.ibm.com/software/awdtools/appscan/

[3] Acunetix Web Vulnerability Scanner, 2008,http://www.acunetix.com/vulnerability-scanner/Nmap

[4] Netsparker Web Vulnerability Scanner, 2012, https://www.netsparker.com/web-vulnerability-scanner/

[5] A. Tripathi, and U K. Singh, "Evaluation of severity index of vulnerability categories", Int. J. Information and Computer Security, Vol. 5, No. 4, 2013 pp. 275-289

[6] C. Joshi, and U.K. Singh, "ADMIT- A Five Dimensional Approach towards Standardization of Network and Computer Attack Taxonomies". International Journal of Computer Application (IJCA, 0975 – 8887), Volume 100, Issue 5, August 2014, pp 30-36

[7] 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 (IJRCSSE) Volume 5, Issue 1, January 2015, pp 742-747.

[8] C. Joshi, and U. K Singh, "Performance Evaluation of Web Application Security Scanners for More Effective Defense" International Journal of Scientific and Research Publications (IJSRP), Volume 6, Issue 6, June 2016, ISSN 2250-3153, pp 660-667.

[9] C. Joshi, and U. K Singh, "Analysis of Vulnerability Scanners in Quest of Current Information Security Landscape", International Journal of Computer Application (IJCA 0975 – 8887), Volume 146(2), July 2016, ISBN 973-93-80883-35-9, pp 1-7.

[10] A. Tripathi, and U K. Singh, "A model for quantitative security measurement and prioritisation of vulnerability mitigation" Int. J. Security and Networks, Vol. 8, No. 3, 2013 pp. 139-153.

[11] M. Tupper and A. N. Zincir-Heywood, "VEA-bility Security Metric: A Network Security Analysis Tool," Availability, Reliability and Security, 2008. ARES 08. Third International IEEE Conference on, Barcelona, 2008, pp. 950-957.

[12] J. Pagett, and S.L. Ng , "Improving Residual Risk Management Through the Use of Security Metrics", Royal Holloway Series 2010.

[13] CVSS v3.0 specification document, Available: https://www.first.org/cvss/specification-document.

[14] National Vulnerability Database, Available: http://nvd.nist.gov

[15] CVE - Common Vulnerabilities and Exposures (CVE), Available: https://cve.mitre.org/

[16] U. K. Singh, and C. Joshi, "Quantitative Security Risk Evaluation using CVSS Metrics by Estimation of Frequency and Maturity of Exploit", Proceedings of the World Congress on Engineering and Computer Science 2016 Vol I WCECS 2016, San Francisco, USA, October 19-21, 2016, ISBN: 978-988-14047-1-8, ISSN: 2078-0958 (Print), ISSN: 2078-0966 (Online).

[17] U. K. Singh, and C. Joshi, "Information Security Assessment by Quantifying Risk Level of Network Vulnerabilities", International Journal of Computer

Applications, Volume 156, Issue 2, pp.37-44, December 2016.

[18] Nirnay Ghosh., and S. K. Ghosh . "An Approach for Security Assessment of Network Configurations using Attack Graph", In First International Conference on Networks & Communications (2009).

[19] L. Wang, A. Singhal, and S. Jajodia. "Measuring the overall security of network configurations using attack graphs", In Proceedings of the 21st Annual IFIP WG 11.3 Working Conference on Data and Applications Security (DBSec), July 2007.

[20] N. Ghosh, and S. K. Ghosh. "An Intelligent Technique for Generating Minimal Attack Graph", In proceedings of the 21st annual computer security applications conference(ACSAC 2005)

[21] U. K. Singh, and C. Joshi, "Measurement of Security Dangers in University Network", International Journal of Computer Applications, Volume 155, Issue1, pp.6-10, December 2016.