INTERNATIONAL CONFERENCE ON COMBINATORICS, CRYPTOGRAPHY AND COMPUTATION

Iran University of Science &Technology

Proceedings of the 2nd International Conference on Combinatorics, Cryptography and Computation (I4C2017)

Attack Graph Based system for Risk Assessment of Multi-Step Attacks

Marjan Keramati
Semnan University/Department of Computer Science
Semnan Province, Semnan, Iran
Keramati_marjan@semnan.ac.ir

ABSTRACT

Daily increasing of number of vulnerabilities in computer networks and dependency of person's lifestyle to computer networks has made network hardening a necessity. So, because of the budget limitation, minimum cost network hardening has always been one of the worth mentioning challenges for security administrators. Prioritizing the vulnerabilities by the aim of finding the most perilous ones, makes the minimum cost network hardening possible. Common Vulnerability Scoring System or CVSS is the most widely used system that is used for risk assessment of exploiting known vulnerabilities. But, CVSS only considers the intrinsic characteristic of vulnerabilities and temporal features such as probability of exploitation tools availability is ignored. So, efficient vulnerability isolation is not possible by the use of CVSS Scores only. Lack of scores diversity is another important weakness of CVSS. Besides, CVSS only scores the one step attacks and risk assessment of real attacks (multi-step attacks) is not feasible with CVSS. In this paper, by the aim of improving CVSS, one risk assessment system is introduced. The proposed system makes dynamic risk analysis of multi-step attacks possible by considering the temporal features of their vulnerabilities besides the intrinsic ones. The introduced risk scoring system has been developed based on attack graphs. Defining some attack graph based security metrics is one of the most noticeable novelty of the proposed method that makes the risk assessment of multi-step attacks feasible. Risk assessment of multistep attack is done by attack graph analysis of the considered network, probability estimation of vulnerability exploits availability and extracting the Impact of vulnerability exploitation on security parameters of the network. Using Multiple Criteria Decision Analysis for aggregation of the defined security metrics can be considered as another innovation in the proposed method.

KEYWORDS: Risk Assessment, Vulnerability, Attack Graph, Security metric, CVSS

1 INTRODUCTION

Computer networks development has always been considered as the main reason of daily increasing number of cyber-attacks in companies and organizations (Abraham, Nair ,2015). The main cause of attack occurance in computer networks are vulnerabilities. Software vulnerabilities usually origins from numerous problems such as, errors in software design, inappropriate configuration of systems or other shortcomings that are generally recognized as bug (Frühwirth, Männistö , 2009). Vulnerability exploitation because of

its disruptive effects on Confidentiality, Integrity and Availability of systems may be costly (Ghani et al., Luna, Suri, 2013). For example Denial of Service attack, in an internet based organization may interrupt business operations (Houmb, Franqueira, 2009). Daily increasing of vulnerabilities have always been considered as a challenge for public and private organizations. But, patch is not available for all the indexed vulnerabilities. So, because of the rapid growth of software vulnerabilities, it is necessary for security administrators to focus on the most perilous vulnerabilities (Spanos et al., Sioziou, Angelis ,2013). There are some standard databases that can be useful for this purpose. OSVBD and CVE are two examples (Web-1) (Web-2). Penetration test tools are responsible for scanning the network and providing a brief description of each vulnerability in accordance of their CVE number (Web 3). However, using these databases is not efficient and suitable. This is because, not scoring the vulnerabilities makes it difficult for the network administrator to determine the most perilous vulnerabilities (Web 3). Security Analysis and eliminating the most perilous vulnerabilities is considered as one of the most complicated issues in the security management process of every organization and most importantly it is a costly task (Frühwirth, Männistö , 2009).

Availably of appropriate countermeasure for each vulnerability by considering the vulnerabilitiy's intensity is an emergency. Also it is necessary to prioritize vulnerabilities based on their danger level (Ghani et al., Luna, Suri, 2013). On the other hand, security investment must be in accordance with likely damages.

Vulnerabilities must be prioritized base on their risk for the network. Risk is calculated by probability estimation of vulnerability exploiting and their impact on Security parameters of the network [11]. The basic problem is that, till now there is no standard and widely accepted method for risk assessment. Also, the most important problem with the existing approaches is that, they are incapable of performing dynamic risk assessment (Considering temporal features of vulnerabilities)

It is noticeable that, real attacks in computer networks are multi-step attacks which exploits a sequence of vulnerabilities to penetrate the network. They are called as multi-step attacks or chain of vulnerabilities (Idika, Bhargava, 2010). The possible vulnerability chains of each network can be extracted by the analysis the attack graph of the network. This is because, attack graph is representative of all possible attacks in the network and the methods of penetrating a network. In each organization, Attack Graph can be used in order to determine the security posture. Also, the security administrator will be capable of suggesting solutions for risk reduction in that organization. By utilizing the attack graph based security metrics, it is also possible to compare the security level of two different configuration of each network. Another noteworthy challenge in the world of network security is the lack of widely accepted quantifiable security metrics for risk assessment of computer networks. The current approaches provides the qualified ones and subjective methods for security assessment (Pamula, et al., Jajodia, Ammann, Swarup, 2006). Due to the high importance of security analysis of information systems, majority of organizations, companies and researchers have implemented security scoring services. Security scoring systems come into two major categories: qualitative and quantitative. Qualitative approaches reflects the dangerous level of each vulnerability. Quantitative methods provide the set of numerals for vulnerability description (Spanos et al., Sioziou, Angelis ,2013). ISS X-Force and Qualys are two examples of qualitative systems (Web 4) , (Web 5). Examples of quantitative methods are US-CERT's and CVSS (Web-5). As CVSS, provides more detailed and coherent detailed information about each vulnerability, it is used by the vast majority of security community members. CVSS, reflects the risk of each vulnerability by considering its intrinsic features (Web -5). CVSS doesn't take into account the temporal features of the vulnerability. But, temporal factors are so important to be considered in the process of vulnerability scoring. Because, the risk of each vulnerability changes significantly over the years and by situating in different network topologies. Note that, the risk of each vulnerability is influenced over the years and by the probability of patch availability and also the exploitability of tools in each point of time (Frühwirth, Männistö , 2009).On the other hand, CVSS is only capable of scoring one step attacks and this in the case that, the vast majority of attacks are multi step attacks. another serious issue is that, CVSS provides limited number of scores for risk estimation of thousands and thousands of vulnerabilities. So, it doesn't do vulnerability isolation efficiently.

In this paper, with the aim of improving the existing vulnerability scoring systems, one novel attack scoring system has been developed that provides dynamic and quantitative risk assessment of multi-step attacks by considering some temporal features of vulnerabilities over the years (probability of exploit tools

availability). The presented scoring system is an attack graph based one. This is the existence of some quantifiable security metrics which makes efficient attack scoring possible. By applying the proposed method on each network attack graph, determining the most perilous multi-step attacks and predicting the future security level of network attacks will be possible. Defining some quantifiable security metrics and choosing mathematical methods for aggregating the security parameters is considered as the most substantial novelty for this paper. These security metrics can be measurable quantitatively by analysing the network's attack graph.

In the following, after a brief review on some similar works and attack graph's related concepts AND CVSS, in the sections 2, 3, 4, the proposed method is introduced in section 5. Also a comparison of the proposed method with CVSS is provided in section 6 by the aim of demonstrating the effectiveness of the proposed method.

2 RELATED WORKS

As stated earlier, scoring systems come into two categories: qualitative and quantitative. One example of qualitative scoring systems is Mozilla. By using Mozilla, security level of each system is specified in four levels (critical, medium, high and low).

First, we have a brief review on some non-standard methods that has been proposed for risk assessment of computer networks. In the process of risk estimation, the most important issue to consider is, estimating the probability of attack occurring, the consequence of attacks and the effectiveness of security measures in a quantitative way. Addressing this issue is possible by defining some quantifiable security metrics. Based on SSECMM, a security metric reflects the security features of each network component (Idika, Bhargava, 2010). Defining and measuring such security metrics makes the comparison of different network topologies possible. Three proposed security metrics in (Idika, Bhargava, 2010) such as, the shortest path metrics, total number of paths and the average of attack paths length are used to answer the most basic questions in the field of network security. The shortest path metric reflects the minimum effort needed for the attacker to penetrate the network. Also, the Number of paths specifies the diversity of available ways for the attacker. All of such metrics have some shortcomings. For example, the mentioned security metrics neglects both the complexity degree of vulnerability exploitation and the length of all possible attack paths. By the aim of overcoming such challenges, a risk assessment framework has been proposed that performs security analysis by aggregating the defined security metrics and considering the effects of them simultaneously in risk assessment.

In (Abraham, Nair ,2015), there is a risk assessment framework that performs dynamic probability estimation by considering the temporal features of vulnerabilities.

In (Houmb, Franqueira, 2009), one Markova model based risk assessment method is proposed that uses conditional probability for risk estimation of multi-step attacks in the network. In (Pamula, et al., Jajodia, Ammann, Swarup, 2006), risk assessment is performed by estimating one attack graph based security metric which specifies the security strength of each network based on the weakest adversary which can penetrate the network.

In (Ghani et al., Luna, Suri, 2013), economical damages is used for quantitative risk assessment of each vulnerability. The various economic factors are used for risk estimation and Multiple Criteria Decision Analysis method is used for aggregating the effects of such metrics.

(Spanos et al., Sioziou, Angelis ,2013) is a vulnerability scoring system in which the diversity of scores have been improved by modifying the CVSS equations. Lack of considering temporal factors and incapability of it for risk assessment of multi-step attacks can be mentioned as the main shortcomings of this approach.

In (Liu, Zhang,2011), a vulnerability scoring system is introduced by the aim of improving CVSS and reconciling its scores with normal distribution.

The most important essential requisites for a security administrator for doing minimum cost network hardening is performing dynamic risk assessment for multi-step attacks. Currently, there

is the lack of such comprehensive scoring system. The vulnerability scoring system of this paper is an improvement over the existing approaches. It has been developed in such a way to perform dynamic risk assessment for multi-step attacks. In the present vulnerability scoring system, quantitative risk assessment is done by analyzing the network's attack graph and measuring some related security metrics.

Each network's attack graph is built from the networks topology information and its associated vulnerabilities. The network vulnerabilities is extractable by the use of network monitoring systems like Nessus (Web 3). Also there are some databases which contains comprehensive information about the networks vulnerabilities. NVD is one such example (Web-9).Next section is a brief introduction to attack graphs and its associated basic concepts.

3 ATTACK GRAPHS

An attack graph is a mathematical model, which demonstrates all possible attacks in the network based on the interrelationship between the networks vulnerabilities. Defining some attack graph based security metrics in a quantitative way is a conventional method for risk assessment of every network.

Three following factors are required for attack graph construction: (Idika, Bhargava, 2010)

- The vulnerabilities of each host
- Interconnectivity of hosts
- At least on security policy (target point)

State based attack graphs and exploit based attack graphs are two ,most well-known types of attack graphs. The complexity of constructing and analysis of attack graphs is polynomial in terms of number of vulnerabilities and security conditions. It is such a low complexity of exploit based attack graphs generation and analysis which makes attack graphs based methods scalable and so suitable for using in security analysis.

An exploit based attack graph which is known as compact attack graph contains two types of nodes: security conditions and exploitable vulnerabilities. Security conditions come into two types: (Idika, Bhargava, 2010)

- Initial conditions: such security conditions are required for exploiting some of the vulnerabilities of the network and they are not the consequence of exploiting another conditions.
- Intermediate conditions: they are the consequence of exploiting some networks vulnerabilities that they themselves are the consequence of exploiting another vulnerabilities of the network.

Another substantial concept about attack graph is a security path. An attack path is a set of vulnerabilities which are exploited in a predetermined manner for penetrating the network. An attack path is also known as a vulnerability chain.

One example of compact attack graph is shown in Figure 1. C1, C2, C3 are examples of initial conditions and C4 is one example of intermediate condition. Exploitable vulnerabilities are shown in Ti format. T1, T3 is one example of attack path, by exploiting it the attacker gains C7 in the network.

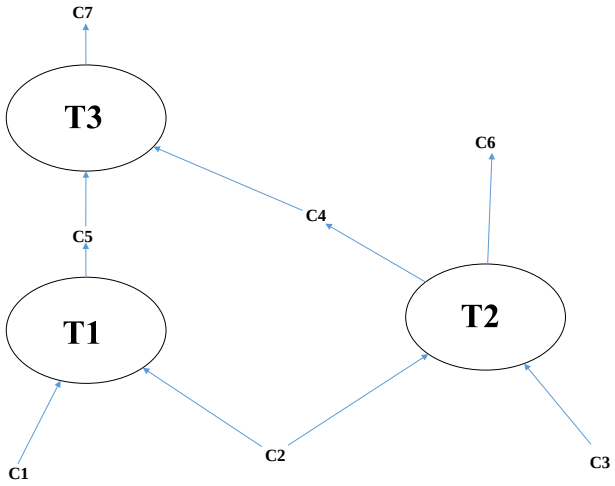

Figure 1 sample example of compact attack graph

4 COMMON VULNERABILITY SCORING SYSTEM

Classifying and prioritizing the vulnerabilities by the aim of finding the most dangerous ones is a critical issue. Currently, CVSS version 2 is available for ranking all vulnerabilities and version 3 can be used for risk assessment of only some the newest ones (Web-5). CVSS provides the risk of each vulnerability in three different groups: Base Scores, Temporal Scores and Environmental ones. Base Scores specifies the intrinsic features of each vulnerability which is constant over the time and also situating in different computer networks. Exploitability and Impact of exploiting the vulnerability on three security parameters, Confidentiality, Availability and Integrity are two major groups of Base Score group. Temporal Scores are the ones which varies over the time. Examples of temporal scores are the probability of exploit tools availability and the probability of patch existence which reduces and increases the vulnerability risk respectively. The Environmental scores varies by situating in different computer networks. Basic Group assigns each vulnerability a score between zeros to ten. One of the most basic problems with CVSS is that, Temporal and environmental scores are not scored in CVSS. So, CVSS does not accurately reflects the vulnerability risk. On the other hand, dynamic risk assessment is not possible by using CVSS only. Also, CVSS performs risk assessment only for single step attacks. AS a result, in this paper by the aim of improving CVSS risk scores, one dynamic vulnerability scoring system is proposed which performs risk assessment for multi-step attacks by considering the temporal features of the vulnerability.

5 THE PROPOSED METHOD

The present vulnerability scoring system is the dynamic one which makes predicting the vulnerability risk in the future possible. This vulnerability scoring system has been developed based on the formal definition of risk.

The formal definition of risk is shown in Eqs(1):

$$Risk = Likelihood\ of\ an\ adverse\ event \times Impact\ of\ the\ adverse\ event\ . \quad (1)$$

The intrinsic features of vulnerabilities are extractable by the CVE identifier from CVSS . In order to make the vulnerability scoring system compatible with both versions of CVSS, we picked the common scores for defining the security metrics.

Dynamic risk evaluation of multi-step attacks requires risk assessment of every involved vulnerability in the attack path and combining the result in a suitable manner. Defining security metrics for quantitative risk assessment of individual vulnerabilities and inventing a method for combining them in order to assess the risk of one multi-step attack is a critical challenge in the world of network security. To overcome the challenge, here we presented some quantifiable security metrics and a method for combining them in a suitable manner. First, we introduce presented security metrics for dynamic risk assessment of individual vulnerabilities that have been done based on both intrinsic and temporal features of each vulnerability. Here the parameter "Access Complexity" which is common between both versions of CVSS is as considered as an indicator of the intrinsic feature of the vulnerability. In the process of risk assessment it should be noticed that, the lowest the Access Complexity (The higher the associated numeric value) of a vulnerability, and the higher the probability of exploit tools availability, the higher the probability of exploiting the vulnerability. So, security metric in Eqs (2) has been defined for probability estimation. also, security metric in Eqs (3) reflects the simplicity degree of exploiting each vulnerability too.

$$Prob(V_i) = AccessComplexity(V_i) \times Exploitability(V_i) \quad (2)$$

$$EaseOfExploitDegree(V_i) = 100 \times Prob(V_i) \quad (3)$$

Exploitability parameter of CVSS in Temporal Scores group is representative of the quality of exploit tools availability. But Temporal group are not scored in CVSS yet. So, in this paper we tried to have an estimation of this parameter by using Pareto distribution shown in Eqs (4). In this equation 'x' is the age of the vulnerability that is equal to the numbers of day from the birth of each vulnerability.

The proposed method for risk estimation of multi-step attacks has been developed by the aim of improving the risk assessment approach in (Idika, Bhargava, 2010), which performs risk assessment based on some attack path based security metrics. The main shortcoming of (Idika, Bhargava, 2010) is that, it ignores the nature (intrinsic and temporal features) of the vulnerability. On the other that, they assume that, the simplicity degree of exploitability is the same for all the attack path's vulnerabilities. by considering such a basic weak point we defined security metric in Eqs (3) for estimating the simplicity degree of each individual vulnerability by considering the intrinsic and temporal features of each vulnerability simaltenously. So, this paper as an improvement over the scoring system in (Idika, Bhargava, 2010), utilizes weighted attack paths for risk evaluation.

$$F(x) = 1 - \left(\frac{k}{x}\right)^{\alpha}. \quad (4)$$

$$k = 0.00161\,, \quad \alpha = 0.260$$

In each network, more than one attack path is associated with each multi-step attack. So, in this paper, all the possible paths have been considered altogether in risk assessment. In the presented risk assessment framework, the risk of each possible attack path is extracted from the ease degree of involved vulnerabilities.

It can be claimed that, the ease degree of each attack path has a direct relationship with the mode of its containing vulnerabilities ease degree ($mode\ (V_i)$ in Eqs(5)). The more the diversity of attack path vulnerabilities, the higher the difficulty degree of exploiting the attack path. So, here, the diversity degree of vulnerabilities of each attack path or the percentage of individual vulnerabilities is considered in the process of estimating the ease degree (Eqs(6)).

$$EaseOfExploitDegree(path) = mode\left(EaseOfExploitDegree(V_i)\right)_{i=1:n} \times (1 - Diversity\,(path)) \quad (5)$$

$$Diversity\,(path) = \frac{Number\ of\ unique\ vulnerabilities(path)}{Total\ Number\ of\ Vulnerabilities(path)} \quad (6)$$

The ease degree of each multi-step attack is calculated by using the MCDA (Multiple Criteria Decision Analysis) methods. Such methods are concerned with the task of ranking a finite number of decision alternatives, each of which is explicitly described in terms of different characteristics called decision criteria which have to be taken account simultaneously. MCDA problems can be stated as below (Triantaphyllou, Baig,2005). There are a number, say m, of alternatives to be evaluated in terms of a number, say n, of decision criteria. Each criterion is associated with a weight of importance, denoted as w_i. The higher the weight is, the more important the criteria is assumed to be. These weights are normalized. So, they add up to one or we have $\sum_{i=1}^{n} w_i = 1$. There are various MCDA methods. By considering the requirement of the attack path ease degree estimation, we chose the weighted product model (WPM)

The ease degree of each multi-step attack is calculated by Eqs(8).The contained variables in Eqs(8) are:

- $LLength$ و $SLength$:they are respectively the length of the shortest and longest attack paths.
- $TrimedMean$: it is calculated by eliminating the shortest and the longest attack paths and calculating the arithmetic mean over the length of the other paths.
- LPP و SPP: They are respectively the percentage of the longest and shortest attack paths.
- TMP : it is calculated by Eqs(9).

$$\prod_{i=1}^{n} {a_{ij}}^{w_i} \quad و \quad \sum_{i=1}^{n} w_i = 1 \quad (7)$$

$$EaseOfExploitDegree(MultiStageAttack) = SLength^{SPP} \times TrimedMean^{TMP} \times LLength^{LPP} \quad (8)$$

$$TMP = 1 - (SPP + LPP) \quad (9)$$

$$Prob(MultiStageAttack) = \frac{EaseOfExploitDegree(MultiStageAttack)}{100*0.71} \quad (10)$$

Based on the (Idika, Bhargava, 2010), the shortest path and the mean of attack path length metric ignores the number of ways the attacker can penetrate the network. So, in this paper, the other paths (except the shortest ones) are also considered in probability estimation (Eqs(8)).

Based on Eqs(1), the Impact of exploiting a vulnerability on three security parameters of the considered network is also needed for the risk assessment of each vulnerability. Fortunately the Impact of exploiting each known vulnerability is available in CVSS.

6 COMPARING THE PROPOSED METHOD WITH CVSS

One basic and challenging, shortcoming with CVSS is the lack of scores diversity. In other words, in CVSS, only a limited number of scores are available for risk assessment and discriminating the huge number of vulnerabilities. So, efficient risk assessment is not possible by using CVSS only. Considering temporal features of the vulnerability in risk assessment not only increases the accuracy of risk assessment but also, improve the scores diversity of CVSS considerably. Based on Eqs (4), the range of the pareto distribution is [0.8122,1]. Due to the infinite

number of scores in the mentioned range and as pareto is an injective function, ehere,,the infinitive number of scores are available for risk assessment of the vast number of vulnerabilities. our risk assessment method have been used for risk estimation of some network examples which have been used in similar works (Ghosh, Ghosh, 2009). The results for one network example are shown and described in the next section. The results are compared with CVSS method. Instead of quantitative risk assessment, CVSS provides qualitative risk assessment too (TABLE 1).

7 EXPERIMENTAL RESULTS

The implementation of the proposed method has been done in a computer system with 8 GB RAM and 2.2 GHz CPU. The proposed risk assessment framework performs risk assessment by analyzing the network attack graph. The network example and its associated attack graph for obtaining root access on Host 2 are shown in Figure 2, Figure 3 respectively. The network topology information, its associated vulnerabilities information and risk assessment results are shown in TABLE 1, 2, 3 respectively. By analyzing the TABLE 3 we can conclude that:

- It is obvious that the diversity level is considerably higher than that of CVSS. The present vulnerability scoring system isolate the 16 multi-step attacks by 12 different scores. This is in the case that, CVSS separatSe them by only 4 scores.
- Regardless of the low diversity of CVSS Impact scores, the proposed method improved the risk scores diversity in comparison to CVSS considerably.

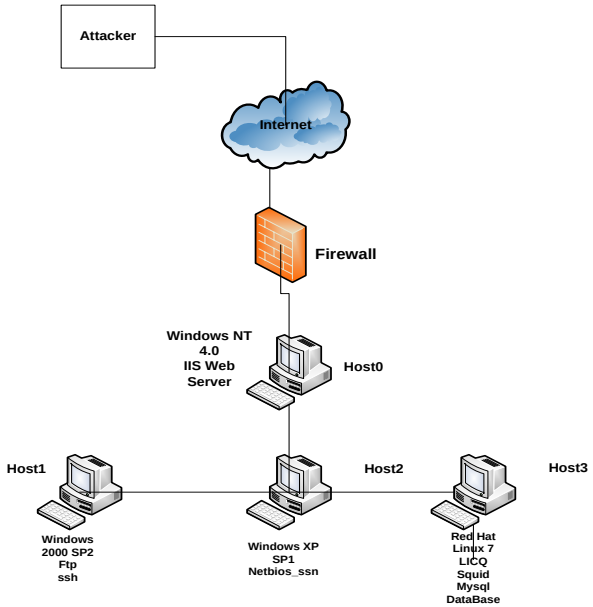

Figure 2 sample network example (Ghosh, Ghosh, 2009)

Table 2 Configuration information of Figure 2

Host	Attacker	H0	H1	H2	H3
Attacker	localhost	IIS	none	none	none
H0	all	localhost	ftp,ssh	all	Squid, LICQ
H1	all	IIS	localhost	all	Squid, LICQ
H2	all	IIS	ftp,ssh	localhost	Squid, LICQ
H3	all	IIS	ftp,ssh	all	localhost

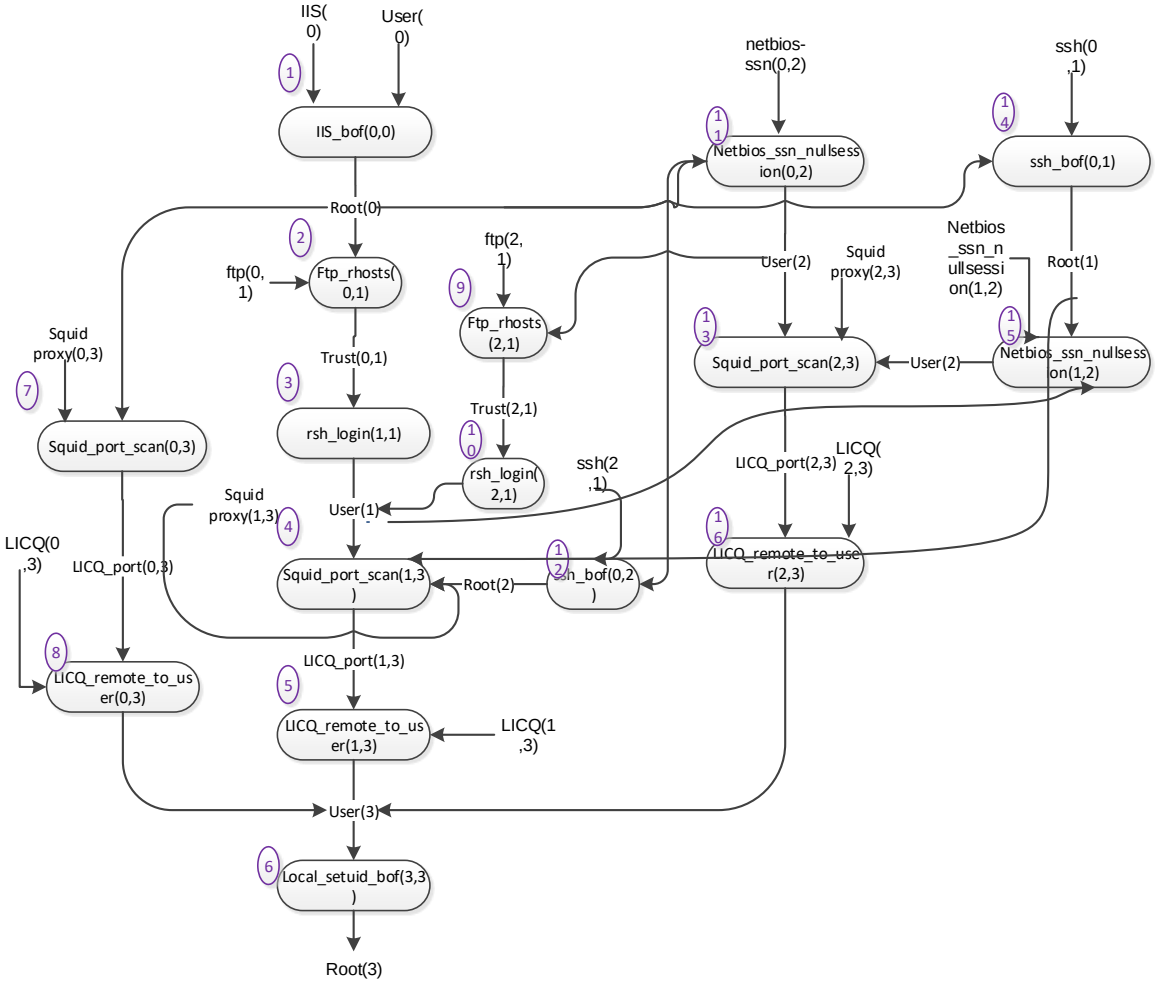

Figure 3 network example's attack graph (Ghosh, Ghosh, 2009)

Table 2 Vulnerability information of Figure 2

CVE	vulnerability	Access Complexity	Age by (10/20/2017)
CVE-2002-0364	IIS buffer overflow	0.71	4854
CVE-2008-1396	ftp rhost overwrite	0.61	2768
CVE-1999-1455	Sshd bufferoverflow	0.71	6401
CVE-2003-0661	Net bios ssn nullsession	0.71	5766
CVE-1999-0180	rsh login	0.71	6226
CVE-2001-0439	LICQ remote to user	0.71	5220
CVE-2001-1030	Squid-port-scan	0.71	5234
CVE-2006-3368	Local – setuid-bof	0.71	3391

Table 2 Risk Assessment of Figure 2 by the proposed method

Vul-number	CVSS Base Score	$Prob$	$Impact$	$Risk$	Elimination priority proposed) (method
1	7.5	0.6953	6.4	4.44992	4
2	4.3	0.5954	2.9	1.72666	10
3	7.5	0.6966	6.4	4.45824	1
4	7.5	0.4761	6.4	3.04704	8
5	7.5	0.5117	6.4	3.27488	6
6	5	0.5374	2.9	1.55846	11
7	7.5	0.6956	6.4	4.45184	3
8	7.5	0.6956	6.4	4.45184	3
9	4.3	0.5954	2.9	1.7266	10
10	7.5	0.6966	6.4	4.45824	1
11	5	0.6949	2.9	2.01521	9
12	7.5	0.6960	6.4	4.4544	2
13	7.5	0.4863	6.4	3.11232	7
14	7.5	0.6960	6.4	4.4544	2
15	5	0.4548	2.9	1.31892	12
16	7.5	0.5239	6.4	3.35296	5

8 CONCLUSION AND FUTURE WORKS

Nowadays because of implementing computer networks in various important aspects of our life, economical, educational, business, network immunization against possible attacks is considered as an inevitable requirement. Due to the limitations in the organizations financial resources, doing network hardening in a minimum cost way is required. Such a goal is reachable by risk assessment of possible attacks and finding the most dangerous ones. Currently CVSS performs risk assessment for the known vulnerabilities. But it has some major shortcoming which make it inefficient for risk evaluation. First, it ignores the temporal features of the vulnerability such as the probability of patch existence. Also, its low scores diversity makes it unusable for separating the vulnerabilities. On the other hand, CVSS is incapable of performing risk assessment for multi-step attacks which are real attacks in network. In this paper, by the aim of improving the CVSS, we implemented an attack graph based risk scoring framework for dynamic risk assessment of multi-step attacks in the network. As the proposed method considers the probability of exploit tools availability, its scores diversity and accuracy of scores are considerably higher than those in CVSS.

In the future we are going to improve the accuracy of the proposed method by considering other temporal features such as the probability of patch availability and the environmental factors such as the privacy of the considered network. Also, by considering the low scores diversity of Impact parameter in CVSS, we are going to propose a method for improving the Impact score diversity in CVSS.

REFERENCES

Abraham S. and Nair S. (2015). “A Predictive Framnework for Cyber Security Analytics Using Attack Graphs”, in International Journal of Computer Networks & Communications (IJCNC), Vol.7, No.1.

Albanese M., Jajodia S., Singhal A., Wang L., (2014) “An Efficient Framework for Evaluating the Risk of Zero-Day Vulnerabilities”, in E-Business and Telecommunications, Springer. PP. 322-340.

Chen F., Liu D., Zhang Y. and Su J.(2010), “A Scalable Approach to Analyzing Network Security using Compact Attack Graphs”, in Journal Of Networks, pp. 543-550.

Frei S., May S., Fiedler U., Plattner B. (2006). “Large-scale vulnerability analysis”, in LSAD ’06: Proceedings of the 2006 SIGCOMM workshop on Large-scale attack defense. pp. 131–138.

Frühwirth C., Männistö T. (2009), “Improving CVSS-based vulnerability prioritization and response with context information”, in Proceedings of International Workshop on Security Measurement and Metrics (MetriSec), PP. 535-544.

GALLON L.(2010), “Vulnerability discrimination using CVSS framework", in New Technologies”, Mobility and Security (NTMS), 4th IFIP International Conference, pp. 1 –6.

Ghani H., Luna j., Suri N. (2013), “Quantitative assessment of software vulnerabilities based on economic-driven security metrics”, in International Conference on Risks and Security of Internet and Systems (CRiSIS), pp. 1-8.

Ghosh N., Ghosh S.K.,(2009), "An Approach for Security Assessment of Network Configurations Using Attack Graph”, in 1st International Conference on Networks and Communications, IEEE, pp. 283-288.

Hamid T., Maple C., Sant P.(2012), “Methodologies to Develop Quantitative Risk Evaluation Metrics”, in International Journal of Computer Applications, Vol.48, No.14, pp.17-24,.

Houmb S. H., Franqueira V. N. L.(2009), “Estimating ToE Risk Level Using CVSS”, in International Conference on Availability, Reliability and Security, pp.718-725.

Idika N., Bhargava B. (2010), “Extending Attack Graph-based Security Metrics and Aggregating Their Application”, in IEEE Transactions on Dependable and Secure Computing, pp. 1-12.

Joh H., Malaiya Y. K., (2011) “Defining and Assessing Quantitative Security Risk Measures Using Vulnerability Lifecycle and CVSS Metrics”, in Proc. Int. Conference on Security and Management. pp. 10-16.

Liu Q., Zhang Y. (2011), “VRSS: A new system for rating and scoring vulnerabilities”, in Computer Communications, Vol. 34, No. 3, PP. 264-273.

Nzoukou W., Wang L., Jajodia S., Singhal A.,(2013), “A unified framework for measuring a network's mean time-to-compromise”, in Proc. 32nd Int'l. Symp. on Reliable Distributed Systems (SRDS). pp. 215-224.

Pamula J., Jajodia S., Ammann P., and Swarup V. (2006), "A Weakest-Adversary Security Metric for Network Configuration Security Analysis", in Proc. Second ACM Workshop Quality of Protection, pp. 31-38.

Scarfone K., Mell P., (2009), “An Analysis of CVSS Version 2 Vulnerability Scoring,” in Proceeding of 3rd International Symposium on Empirical Software Engineering and Measurement, PP. 516 – 525.

Spanos G., Sioziou A., Angelis L. (2013), “WIVSS: a new methodology for scoring information systems vulnerabilities”, in Panhellenic Conference on Informatics, PP. 83-90.

Triantaphyllou E., Baig K.,(2005),” The Impact of Aggregating Benefit and Cost Criteria in Four MCDA Methods”, in IEEE Transactions on Engineering Management, Vol.52, No.2, pp. 213-226.

Xie L., Xie X., Zhang J., (2013),” Network Security Risk Assessment Based on Attack Graph”, in Journal of Computers, Vol. 8, No. 9, pp. 2339-2347.

Web sites:

Web-1: https://cve.mitre.org/, consulted, 5 October 2017.

Web-2:http://osvdb.org/, consulted, 5 October 2017.

Web-3:http://www.tenable.com/products/nessus-vulnerability-scanner, consulted, 5 October 2017.

Web-4:http://www-935.ibm.com/services/us/iss/xforce/faqs.html, consulted, 5 October 2017.

Web 5: http://www.qualys.com/research/knowledge/severity/, consulted, 5 October 2017.

Web 6:https://www.first.org/cvss, consulted, 5 October 2017.

Web 7:https://cve.mitre.org/, consulted, 5 October 2017.

Web 8: http://www.mozilla.org/security/announce/, consulted, 5 October 2017.

Web 9: https://nvd.nist.gov, consulted, 5 October 2017.