Scientific Research Publishing

Journal of Information Security, 2019, 10, 103-116
http://www.scirp.org/journal/jis
ISSN Online: 2153-1242
ISSN Print: 2153-1234

Quantitative Evaluation of Cyber-Attacks on a Hypothetical School Computer Network

Akinjide A. Akinola[1], Adeyemi A. Adekoya[2*], Ayoade O. Kuye[3], Abiodun Ayodeji[4]

[1]University of Lagos, Lagos, Nigeria
[2]Virginia State University, Petersburg, VA, USA
[3]University of Port Harcourt, Port Harcourt, Nigeria
[4]Nuclear Power Plant Development Directorate, Nigeria Atomic Energy Commission, Abuja, Nigeria
Email: *aadekoya@vsu.edu

How to cite this paper: Akinola, A.A., Adekoya, A.A., Kuye, A.O. and Ayodeji, A. (2019) Quantitative Evaluation of Cyber-Attacks on a Hypothetical School Computer Network. *Journal of Information Security*, **10**, 103-116.
https://doi.org/10.4236/jis.2019.103006

Received: January 23, 2019
Accepted: June 14, 2019
Published: June 17, 2019

Abstract

This paper presents the attack tree modeling technique of quantifying cyber-attacks on a hypothetical school network system. Attack trees are constructed by decomposing the path in the network system where attacks are plausible. Considered for the network system are two possible network attack paths. One network path represents an attack through the Internet, and the other represents an attack through the Wireless Access Points (WAPs) in the school network. The probabilities of success of the events, that is, 1) the attack payoff, and 2) the commitment of the attacker to infiltrate the network are estimated for the leaf nodes. These are used to calculate the Returns on Attacks (ROAs) at the Root Nodes. For Phase I, the "As Is" network, the ROA values for both attack paths, are higher than 7 (8.00 and 9.35 respectively), which are high values and unacceptable operationally. In Phase II, countermeasures are implemented, and the two attack trees reevaluated. The probabilities of success of the events, the attack payoff and the commitment of the attacker are then re-estimated. Also, the Returns on Attacks (ROAs) for the Root Nodes are re-assessed after executing the countermeasures. For one attack tree, the ROA value of the Root Node was reduced to 4.83 from 8.0, while, for the other attack tree, the ROA value of the Root Node changed to 3.30 from 9.35. ROA values of 4.83 and 3.30 are acceptable as they fall within the medium value range. The efficacy of this method whereby, attack trees are deployed to mitigate computer network risks, as well as using it to assess the vulnerability of computer networks is quantitatively substantiated.

Keywords

Cyber-Attack, Quantitative Vulnerability Assessment, Attack Trees, Return on Attack, Countermeasures

1. Introduction

One of the most critical concerns of computer and IT professionals today is information security or the lack of it. There is a plethora of evidence to support such a claim. In this day and age, a computer cluster for cracking passwords can generate 350 billion password guesses per second and could break any eight-character password in a maximum of 5.5 hours. Internet web servers must resist thousands of attacks every day, and an unprotected computer connected to the Internet can be infected in fewer than 60 seconds. As it is with different industries and organizations, institutions of higher learning are not immune to this scourge. Moreover, the historic openness of higher education institutions to the public has made their computer networks even more vulnerable to cyber-attacks. Such vulnerabilities are discussed widely in extant literature. Assessment of the adverse impacts of information security vulnerabilities and threats in schools and academic environments has also been presented in contemporary literature. However, much of the reported work has been qualitative. While qualitative research can be useful, their conclusions are often subjective and lack details that provide the necessary impetus for clear and definitive actions, as the research outcomes do not readily lend themselves to risk controls and implementation. Clearly, there is a need to quantify the impacts of cyber-attacks on modern-day establishments, since the rate of cyber-attacks continues to escalate at an alarming rate. Quantitative methods of modeling and analyzing cyber threats have been of great interest to a group of researchers such as Greitzer *et al.* [1], Xynos *et al.* [2], WINS [3] [4] and Roger [5] [6], who have all presented innovative approaches for analyzing cyber threats. Al-Mohannadi *et al.* [7] provided an insight into Cyber-attack modeling techniques. This review advances a significant array of and sheds further light on cyber-attack modeling. Further work by the same author, Al-Mohannadi, *et al.* [8] in particular, enunciated how Cyber Threat Intelligence could be gathered from Honeypot Data.

Furthermore, some quantitative studies carried out by Akinola *et al.*, Baker, Balzarotti *et al,* Dacier *et al.,* Edge *et al.,* LeMay *et al.,* and Mell *et al.* [9]-[15] used attack trees and their variants to examine and extend knowledge on the attributes of cyber-attack prone networks. Attack trees are illustrations of network systems whereby, an asset, or target, may be compromised. Attack trees present interdependencies between attack paths by breaking down the complexity of the network system and decomposing high-level parent goals into the smaller subtasks. Amenaza [16] indicates that the basic premise of an attack tree model is the elucidation of the vulnerability of the system, and ultimately, to isolate and report what is needed to achieve desired remedial outcome and success. A set of tools was developed by Dacierel *et al.* [12] which provides automatic security evaluations of UNIX-based systems. The tools are based on modeling a network system, which transforms the privilege graphs into a Markov chain with all the corresponding possible successful attack scenarios.

Balzarotti *et al.* [11] discusses how relevant information on the attributes of the architecture, and the vulnerabilities inherent in a distributed system can be applied quantitatively, to assess the risk to which the network systems are exposed. The advantage of this approach to risk evaluation is its capability to evaluate the extent to which one should believe in system integrity and trustworthiness, and facilitates a comparative analysis of different evaluative outcomes.

Another line of research is studying security measures for mobile ad-hoc networks, using attack and protection trees. The work of Edge *et al.* [13] indicated that Defense-trees could be used to mitigate or even eliminate vulnerabilities. There are a few limiting factors here, to the extent that some of the defense trees have overpopulated and thereby become redundant. Also, some factors such as the commitment of the attacker, that is, the willpower that the threat agent exhibits, and the time committed to the pursuit of the goal intended are neglected in these models.

Lemay *et al.* [14] calculated the State-based Security metrics of two variants of a Supervisory Control and Data Acquisition (SCADA) system architecture using the AD Versary VIew Security Evaluation (ADVISE) technique. The study demonstrates how the quantitative metrics produced by ADVISE can aid system design and provide much insight on system security. Akinola *et al.* [9] quantitatively evaluated the effect of cyber-attacks on a school network system. Their work involved evaluating information security as proposed by Cremonini and Martini [17], who used the Return-on-Attack (ROA) and the Return-On-Investment (ROI) methodologies and metrics, to assess and measure how an attacker's preference changes with the selected security measure. Furthermore, Akinola *et al.* [9] established that by executing specific countermeasures, the risk of cyber-attacks on a school network attack surface could be greatly reduced. The current work builds on previously established foundations; it applies a similar method to a different environment that is, a dissimilar school network system. It is relevant to point out that, while Akinola *et al.* [9] previous work used single values for the leaf nodes; this study extends the former by using randomly generated values to denote the leaf nodes.

2. Methodology

2.1. Network Description

The network which is the test-bed for the study is a school computer network, consisting of the following elements—an Internet router (Cisco 890), a Fast Ethernet switch 1 (core switch, Cisco SFS3500) and an Ethernet switch 2 (Cisco SFE2000). Included in the network are Wireless Access Points (Linksys WAP300N), a Web server, a database server, and a Mikrotik firewall. The Internet router connects to the web server (Apache HTTP) in the computer laboratory on the school premises. The workstations (running on Windows 2007), are of the ring-based topology. A database server (MYSQL) houses the records of graduates and matriculated students of the school at that time. The attacker pro-

filed for this network is a disgruntled ex-student, whose motivation, is the will to compromise the database server that hosts the students' valuable records, with the aim of modifying some of the data items including his.

2.2. The Attack Tree Model

For the attacker to commit his infamous act, and to compromise the database remotely, the attacker uses one of the wireless access points in the school vicinity. Figure 2 and Figure 3 depict the architecture of the school's network as well as the attack trees. The Attack goal is to compromise the database server—the root node. The tasks needed to achieve success on the attack are spelt out in Figure 2 and Figure 3. Each task is conceptually launched at a node in the attack tree. These are wireless access points 1 and 2 in Figure 1. Figure 2 is a schematic diagram of the various tasks that are involved, and it represents an attack via wireless access points, while Figure 3 depicts an attack through the Internet. In Figure 2 and Figure 3, the nodes that are conjoined by an arc must be performed simultaneously for an attack to be successful, while those that are not, requires either of the nodes for success. Mathematically, this can be represented using the Boolean notations, *i.e.*, "AND" or "OR" respectively. Akinola *et al.* [9] have represented the Return-on-Attack (ROA) formulation used in this work as follows:

$$ROA = P_o CP_s \tag{1}$$

where:

P_o = payoff; C = commitment; P_s = probability of success.

The Commitment, C, is assumed to have a unit value because credible attackers have the capability and the intention to exploit a node contemporaneously. The ROA values range from 1 to 10 and are Low, Medium, High and Very High

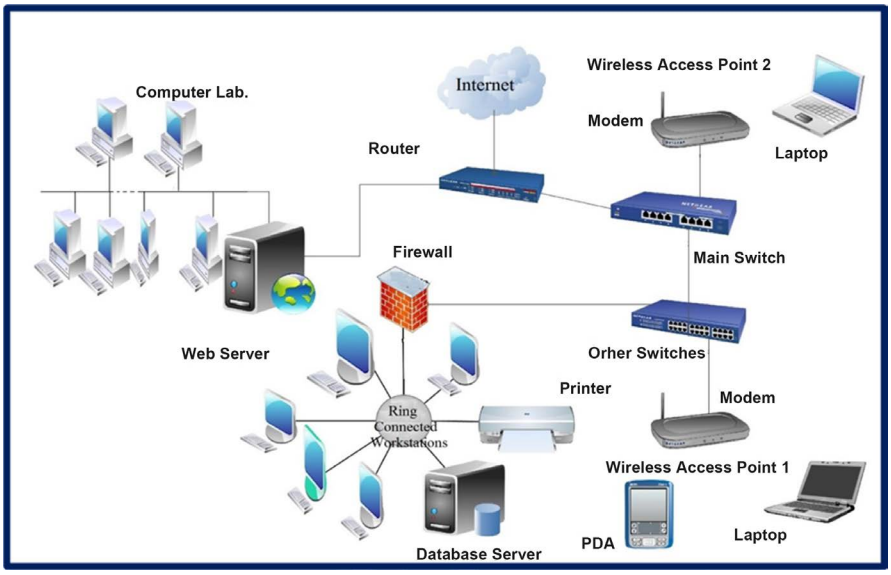

Figure 1. The school network topology.

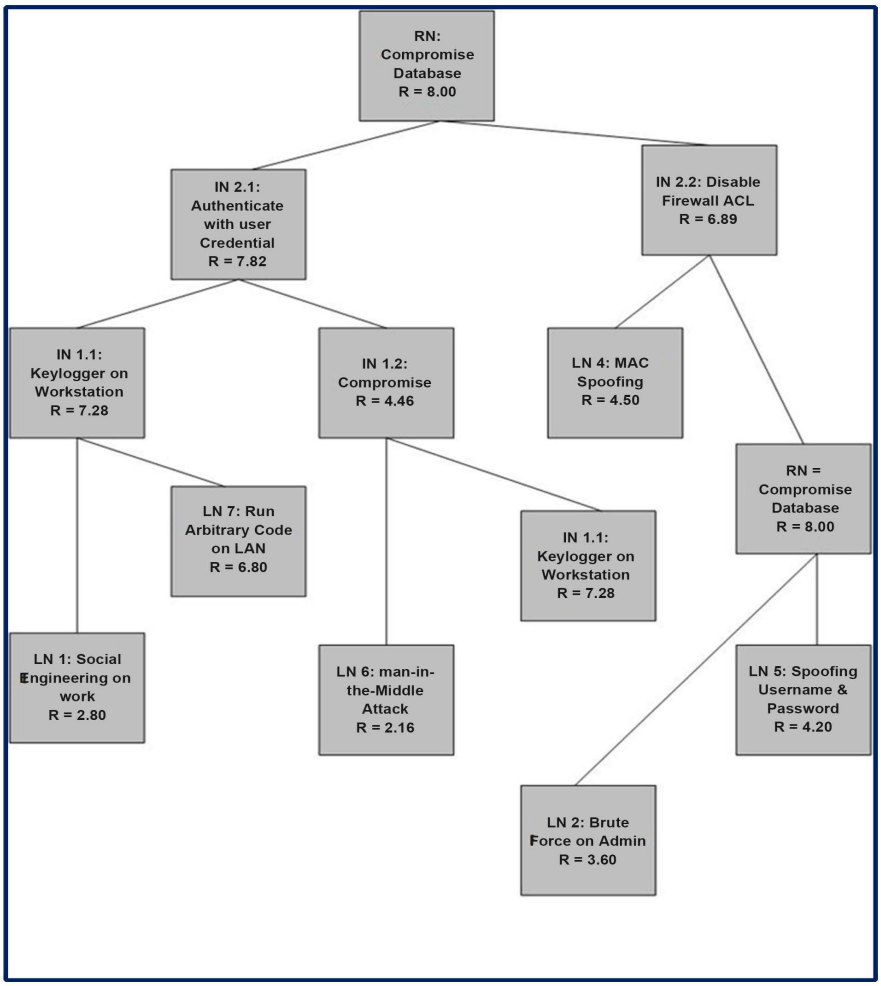

Figure 2. Attack tree diagram a for the school computer network.

[13]. Low ROA values range from 1 - 3. In such a scenario, the attack's impact is minor, and it could easily be detected and repaired. Medium ROA values are between 4 and 6, the attack's impact on the network is usually, "Moderate"; there is typically a reduced performance or interruptions in resource availability. Furthermore, in Attack trees with moderate ROA values, the integrity, confidentiality, and availability of the network require special effort to detect and repair. High ROA values are between 7 and 9. In this case, the attack's impact on the network is "Severe"; leading to significant damage to the network system; there are essential informational access and disclosure to some system files. Considerable effort is required to detect and repair the damage on such networks. When the ROA value is 10, the network system is compromised completely, inoperable or destroyed. The attack vector can render the asset completely unavailable, in this case.

The probability of success is calculated using Equation (2) [9]:

$$P_s = A_{cv} * C_A * A_u \tag{2}$$

where

A_{cv} = Access Vector, C_A = Access Complexity, and A_u = Authentication.

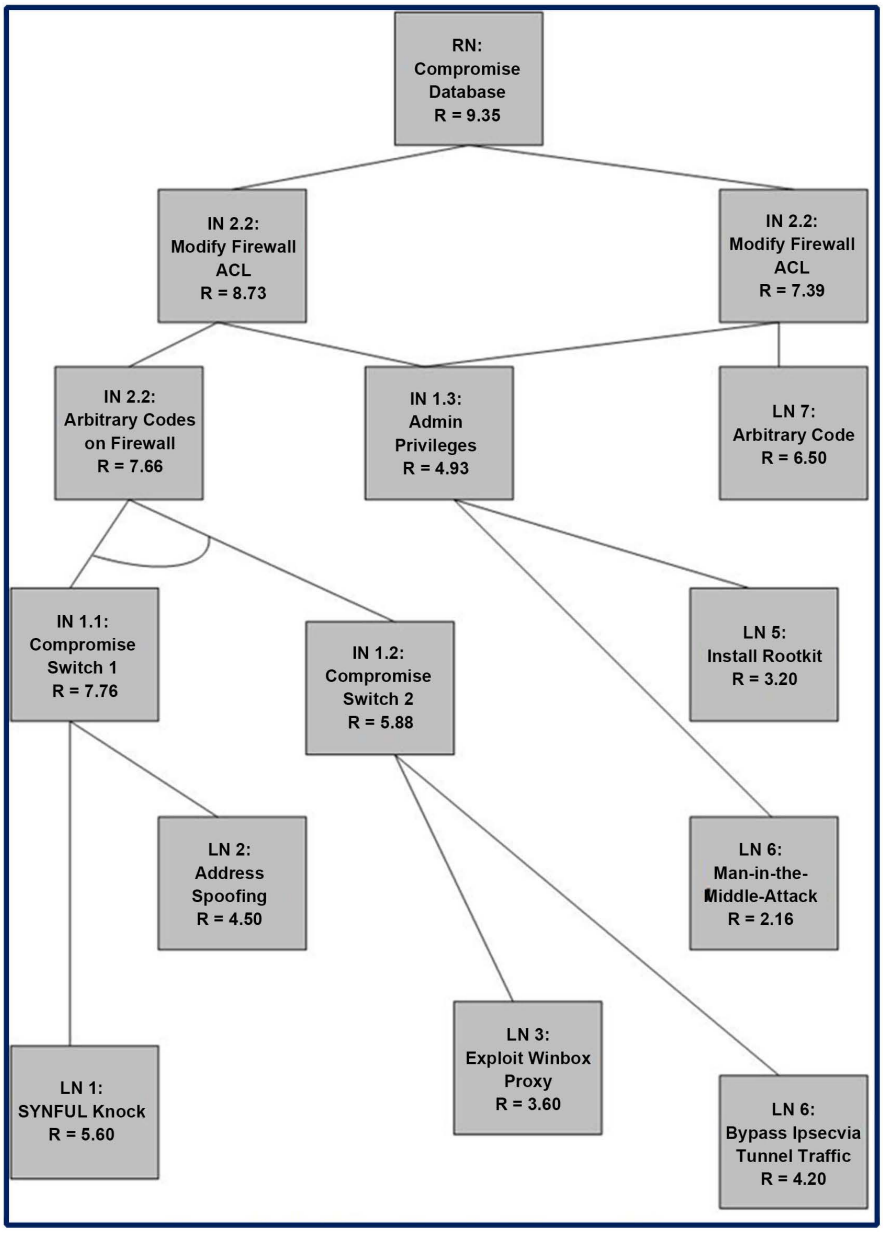

Figure 3. Attack tree diagram b for the school computer network.

The access vector (A_{cv}) shows how vulnerabilities may be exploited. The access complexity (C_A) metric describes how easy or difficult it is to exploit the exposed vulnerability. The number of times that an attacker can be authenticated to a target node for exploitation is indicated by the authentication (A_u) metric. However, successful authentication is not taken into account. For locally exploitable vulnerabilities, this value should only be set to single or multiple values if further authentication is required after initial access. Numerical values for the Access Vector, Access Complexity, and Authentication are derived from a common vulnerability scoring system guide [17]. The probabilities for the intermediate and root nodes P_o and P_s are calculated using Equation (3), (4), (5) and (6) [13]:

For "AND" nodes:

$$P_s = \prod_{i=1}^{k} \text{prob}_i \tag{3}$$

$$P_o = \frac{10^k - \prod_{i=1}^{k} (10 - \text{payoff})}{10^{k-1}} \tag{4}$$

For "OR" nodes

$$P_s = 1 - \prod_{i=1}^{k} (1 - \text{prob}_i) \tag{5}$$

$$P_o = \max_{i=1}^{k} \text{payoff}_i \tag{6}$$

where

$\text{Prob} \in (0,1)$; $\text{Payoff} \in [1,10]$, k = number of leaf nodes.

3. Results and Discussion

Again, Figure 2 and Figure 3, present the two Attack Trees A and B examined in this study. The Payoff, Access Vector, Access Complexity and Authentication values for the two Attack trees which tally with expert opinions, are presented in Table 1 and Table 2. The Payoff, Access Vector, Access Complexity and Authentication values are used to calculate the ROA values for the leaf and intermediate nodes. These values are subsequently used to calculate the ROA values required to compromise the database for Attack Trees A and B (Figure 1 and Figure 2). The ROA values obtained at the root nodes (RN) are 8.00 and 9.35 for Attack Trees A and B respectively. These ROA values fall in the High range, implying that both root nodes can be exploited easily.

With Attack Tree A (Figure 2), the attacker severely impacted the network system thereby, causing considerable informational disclosure and access to many system files, while with Attack Tree B (Figure 3), the attacker rendered the resource completely unavailable.

It must be pointed out that given that the reported values in Table 1 and Table 2, may not reflect the actual real-life situations. Therefore, the access vectors, access complexities, and authentication values were varied randomly within a 5%, 10%, 20%, 30%, 40% and 50% range of the expert opinion values presented

Table 1. Parameters used in calculating ROA for Attack Tree A.

Node	Task name	Payoff	Access Vector (A_V)	Access Complexity (C_A)	Authentication (A_U)
LN1	Social Engineering on Work Station	7	1	0.40	1
LN2	Brute Force on Admin	6	1	0.60	1
LN3	Packet Sniffing	4	1	0.60	1
LN4	MAC Address Spoofing	5	1	0.90	1
LN5	Spoofing Username & Password	7	1	0.60	1
LN6	Man-in-the-Middle Attack	6	1	0.36	1
LN7	Run Arbitrary Code on LAN	8	1	0.85	1

Table 2. Parameters used in calculating ROA for Attack Tree B.

Node	Task name	Payoff	Access Vector (A_V)	Access Complexity (C_A)	Authentication (A_U)
LN1	Synful Knock	8	1	0.70	1
LN2	MAC Address Spoofing	5	1	0.90	1
LN3	Exploit Winbox Proxy	6	1	0.60	1
LN4	Bypass Ipsec via Tunnel Traffic	7	1	0.60	1
LN5	Install Rootkit	8	1	0.40	1
LN6	Man-in-the-Middle Attack	6	1	0.36	1
LN7	Run Arbitrary Code on LAN	8	1	0.80	1

in Table 2 and Table 3. The calculations for ROA were performed 10,000 times to simulate more probable situations. The results obtained are shown in Figure 4 and Figure 5 for Attack Trees A and B respectively.

Figure 4 shows that for Attack Tree A, the maximum and minimum ROA values are 7.98 and 8.00 when the access vectors, access complexities, and authentication values are varied randomly within +50% of expert opinion. The average ROA for the attack path is 7.99. The implication is that for these Attack trees, the ROA value is always high even when errors exist in estimating key parameters.

Also, the maximum and minimum ROA values vary from 9.40 to 5.86 for the Attack Tree B (Figure 5) when the Access Vectors, Access Complexities, and Authentication values are also varied randomly within ±50% of expert opinion values. The average ROA for the Attack path is 9.12, which means that for half of the time, the ROA value is greater than 9.00; a High ROA value which may be unacceptable. Clearly, the ROA values in both the Attack Trees A and B are high. The implication is that an upgrade of the two trees is needed to reduce their vulnerability. Figure 6 and Figure 7, present the suggested upgrade Attack trees.

All things considered, the recommended security upgrades to be implemented on leaf nodes on the Attack Trees are:

1) Adding Intrusion Detection and Prevention Systems (IDPS) at 'sensors' on the network diagram.

2) Adding Remote Access Servers (RAS) before the business processing unit of the digital Network, as all inbound and outbound traffic is routed through this unit.

Again, new Access Vectors, Access Complexities, and Authentication values were obtained for the Attack Trees A and B, by expert judgment. These values are shown in Table 3 and Table 4 for the Attack Trees A and B respectively.

The ROA values for the nodes are re-calculated, and the results are presented in Figure 6 and Figure 7 for the upgraded Attack Trees A and B respectively. The ROA values at the root nodes are 4.32 and 3.30 for Attack Trees A and B respectively. These ROA values are lower than the values reported before the

Table 3. Parameters used in calculating ROA for Attack Tree B after upgrade.

Node	Task name	Payoff	Access Vector (A_V)	Access Complexity (C_A)	Authentication (A_U)
LN1	Social Engineering	7	0.6	0.4	0.4
LN2	Brute Force	6	0.6	0.4	0.7
LN3	Packet Sniffing	4	0.4	0.6	0.4
LN4	MAC Address Spoofing	5	0.6	0.6	0.4
LN5	Spoof Username & Password	7	0.6	0.4	0.7
LN6	Man-in-the-Middle Attack	6	0.6	0.3	0.53
LN7	Run Arbitrary Code on LAN	8	0.85	0.28	0.4

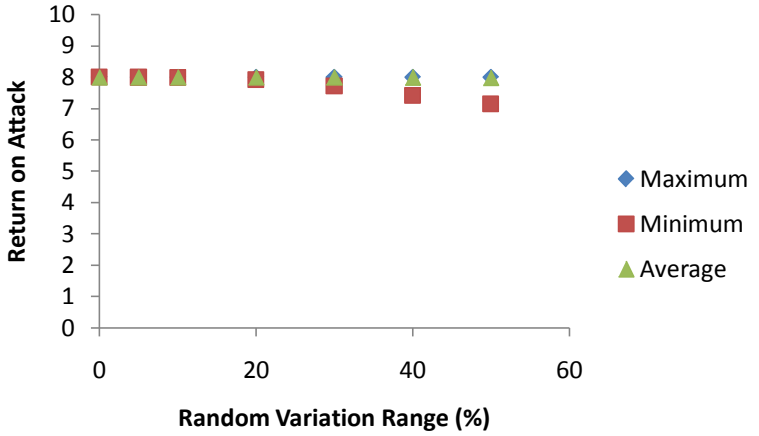

Figure 4. ROA values with random variation in A_{cv}, C_A and A_u values for Attack Tree A.

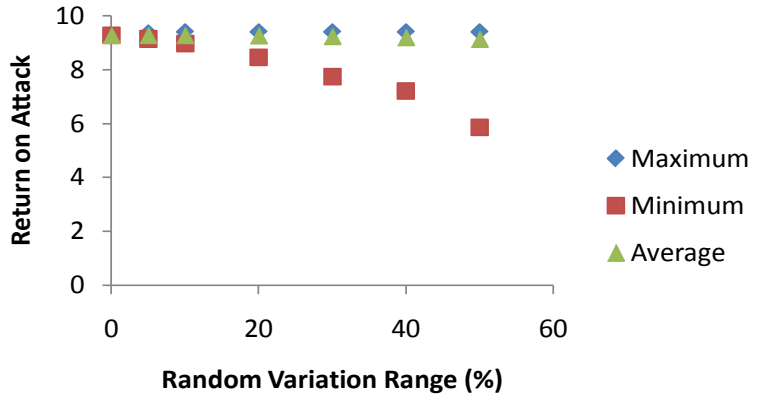

Figure 5. ROA values with random variation in A_{cv}, C_A and A_u values for Attack Tree B.

upgrades, and the ROA values fell to the medium score range for ROA values. Thus, the suggested upgrades were effective. Hence, they did reduce the vulnerability to compromise the Database.

To further obtain better estimates of the ROA values at the Root nodes for each Attack Tree, repeated calculations were performed by randomly varying

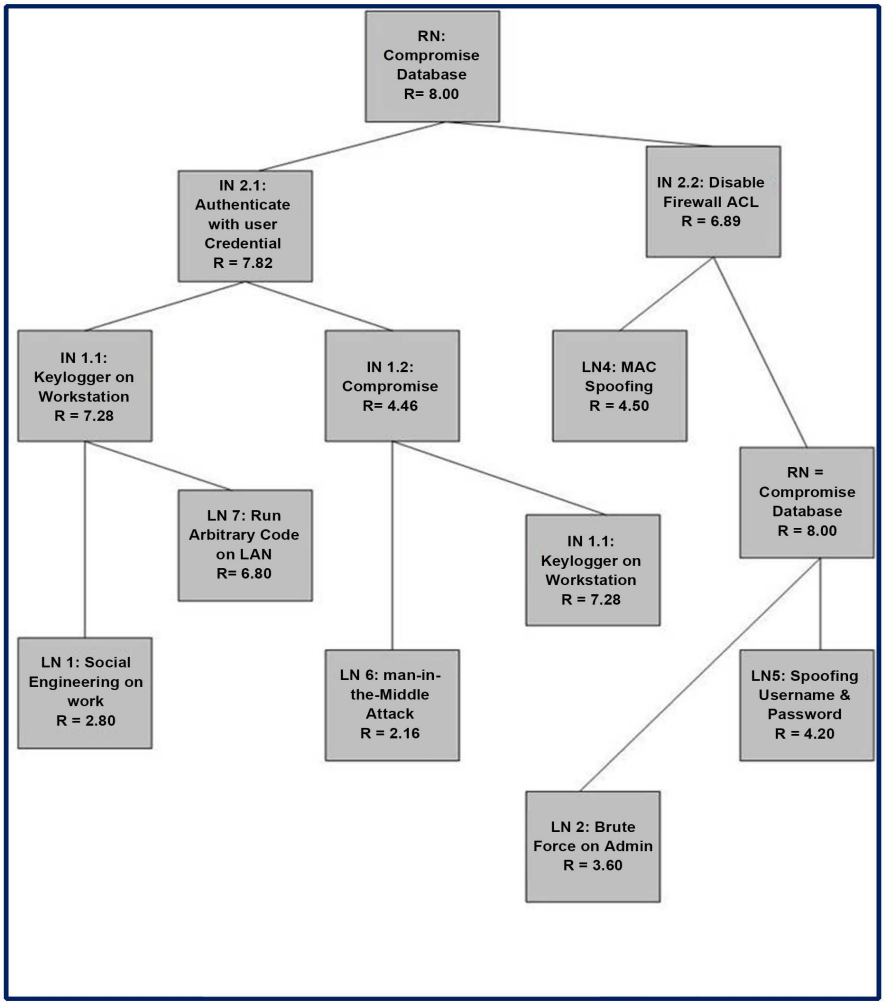

Figure 6. Attack tree diagrams a for school computer network after upgrade.

Access Vector, Access Complexity, and Authentication values up to the +50% range. The calculations were performed 10,000 times with randomly generated values of Access Vectors, Access Complexities, and Authentication. A summary of the results is shown graphically in Figure 8 and Figure 9 for Attacks Trees A and B respectively. Again, the results indicate that the error in ROA value increases proportionally with estimated errors in Access Vector, Access Complexity, and Authentication values; however, the ROA values average out to the values obtained in Figure 6 and Figure 7 for the Attack Tree A and B respectively.

4. Conclusion

Considered in this study, are two attack scenarios on compromising a database in a school network. The networks were analyzed quantitatively, using the attack tree method. The ROA for each attack scenario was determined, and in both cases, they turned out to be >7.0; which meant they are in the high range band. The implication is that the database could be compromised easily. When suggested upgrades were implemented, the ROA values reduced to 4.32 and 3.30 for

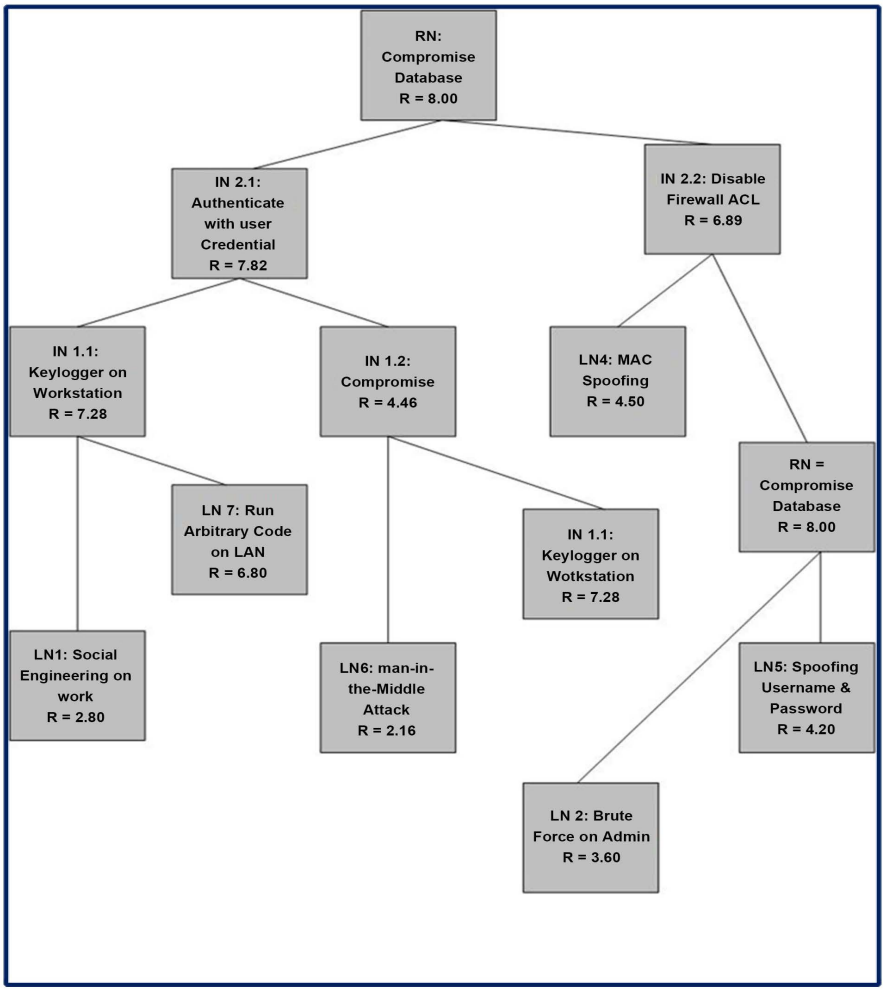

Figure 7. Attack tree diagrams B on school computer network after upgrade.

Table 4. Parameters used in calculating ROA for Attack Tree B after upgrade.

Node	Task name	Payoff	Access Vector (A_V)	Access Complexity (C_A)	Authentication (A_U)
LN1	Synful Knock	8	0.6	0.4	0.4
LN2	MAC Address Spoofing	5	0.6	0.4	0.7
LN3	Exploit Winbox Proxy	6	0.4	0.6	0.4
LN4	Bypass Ipsec via Tunnel Traffic	7	0.4	0.6	0.4
LN5	Install Rootkit	8	0.6	0.4	0.7
LN6	Man-in-the-middle Attack	6	0.6	0.4	0.4
LN7	Run Arbitrary Code on LAN	8	0.6	0.4	0.4

Attack Tree A and Attack Tree B respectively. The ROA values are acceptable because they fall in the Medium range. Even when errors in the Access Vector, Access Complexity, and Authentication values were used to calculate the ROA values, the values fell within the 4 - 7 range, which is an acceptable bound. The

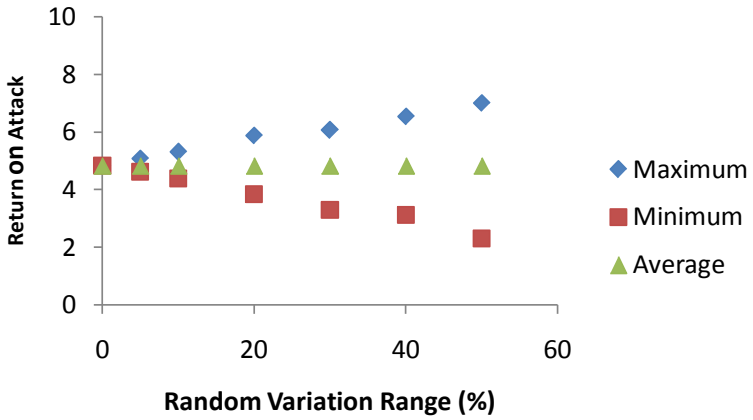

Figure 8. ROA values with random variation in A_{cv}, C_A and A_u values for Attack Tree A after upgrade.

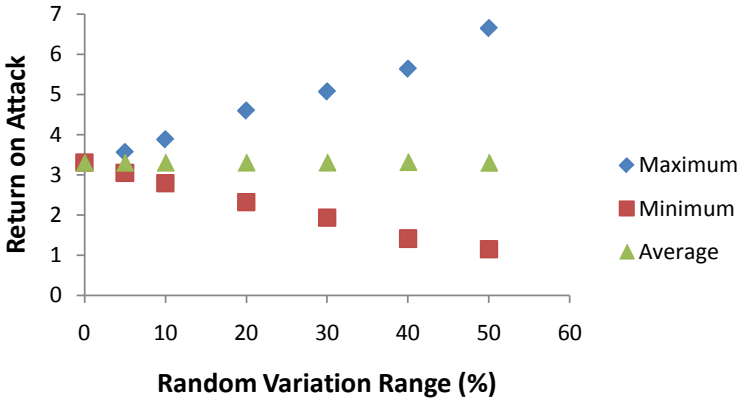

Figure 9. ROA values with random variation in A_{cv}, C_A and A_u values for Attack Tree B after upgrade.

results of the study held steady. The method can, therefore, be used to mitigate, and by extension, to assess the vulnerability of computer networks quantitatively.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Greitzer, F.L., Paulson, P.R., Kangas, L.J., Franklin, L., Edgar, T.W. and Frincke, D.A. (2009) Assessment Challenges: Validating the Model. PNNL Technical Report, Richard.

[2] Xynos, K., Sutherland, I., Read, H., Everitt, E. and Blyth, A.J.C. (2010) Penetration Testing and Vulnerability Assessments: A Professional Approach. *International Cyber Resilience Conference*, Perth, 23-14 August 2010, 126-132.

[3] World Institute for Nuclear Security (2012) Human Reliability as a Factor in Nuclear Security. Presented at the A WINS International Best Practice Guide for Your

Organization. Vienna.

[4] World Institute for Nuclear Security (2015) Managing Internal Threat. A WINS International Best Practice Guide for Your Organization. Vienna.

[5] Roger, G.J. (2010) Changing Security Paradigms. *Journal of Physical Security*, **4**, 35-47.

[6] Roger, G.J. (2010) Being Vulnerable to the Threat of Confusing Threats with Vulnerabilities. *Journal of Physical Security*, **4**, 30-34.

[7] Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A. and Disso, J. (2016) Cyber-Attack Modeling Analysis Techniques: An Overview. *IEEE 4th International Conference on Future Internet of Things and Cloud Workshops*, Vienna, 22-24 August 2016, 69-76. https://doi.org/10.1109/W-FiCloud.2016.29

[8] Almohannadi, H., Awan, I., Al Hamar, J., Cullen, A., Disso, J.P. and Armitage, L. (2018) Cyber Threat Intelligence from Honeypot Data Using Elasticsearch. *IEEE 32nd International Conference on Advanced Information Networking and Applications*, Cracow, 16-18 May 2018, 900-906. https://doi.org/10.1109/AINA.2018.00132

[9] Akinola, A.A., Kuye, A.O. and Ayodeji, A. (2014) Cyber-Attacks Analysis of a School Network. *55th Annual Meeting of Institute of Nuclear Materials Management*, Atlanta, 20-24 July 2014.

[10] Baker, W. (2007) Necessary Measures: Metric-Driven Information Security Risk Peltier Assessment and Decision Making. *Communications of the ACM*, **50**, 101-106. https://doi.org/10.1145/1290958.1290969

[11] Balzarotti, D., Monga, M. and Sicari, S. (2006) Assessing the Risk of Using Vulnerable Components. In: Gollmann, D., Massacci, F. and Yautsiukhin, A., Eds., *Quality of Protection*, Advances in Information Security, Vol. 23, Springer US, Boston, 65-77. https://doi.org/10.1007/978-0-387-36584-8_6

[12] Dacier, M., Deswarte, Y. and Kaâniche, M. (1996) Models and Tools for Quantitative Assessment of Operational Security. In: Katsikas, S.K. and Gritzalis, D., Eds., *Information Systems Security*, Springer US, Boston, 177-186. https://doi.org/10.1007/978-1-5041-2919-0_15

[13] Edge, K.S., Raines, R.A., Baldwin, R.W., Grimaila, M.R., Bennington, R.W. and Reuter, C.E. (2007) Analyzing Security Measures for Mobile Ad Hoc Networks Using Attack and Protection Trees. *Journal of Information Warfare*, **6**, 25-38.

[14] LeMay, E., Ford, M.D., Keefe, K., Sanders, W.H. and Muehrcke, C. (2011) Model-Based Security Metrics Using Adversary View Security Evaluation (ADVISE). *Eighth International Conference on Quantitative Evaluation of Systems*, Aachen, 5-8 September 2011, 191-200. https://doi.org/10.1109/QEST.2011.34

[15] Mell, P., Scarfone, K. and Romanosky, S. (2006) Common Vulnerability Scoring System. *IEEE Security & Privacy*, **4**, 85-89. https://doi.org/10.1109/MSP.2006.145

[16] Amenaza Technologies Limited (2005) Fundamentals of Capabilities-Based Attack Tree Analysis. Calgary, 25.

[17] Cremonini, M. and Martini, P. (2005) Evaluating Information Security Investments from Attackers Perspective: The Return-on-Attack (ROA). *4th Workshop on the Economics on Information Security*, Cambridge, 1-3 June 2005.

Nomenclature

A_{cv}	Access Vector
A_u	Authentication
C	Commitment
C_A	Access Complexity
IN	Intermediate Node
LN	Leaf Node
P_o	Payoff
P_s	Probability of Success
R	Returns on Attack
RN	Root Node
ROA	Returns on Attack
ROI	Return on Investment
WAP	Wireless Access Points