Generation and Risk Analysis of Network Attack Graph

Keshav Prasad, Santosh Kumar, Anuradha Negi and Aniket Mahanti

Abstract Attack graph describes how an attacker can compromise with network security. To generate the attack graph, we required system as well as vulnerability information. The system information contains scanned data of a network, which is to be analyzed. The vulnerability data contain information about, how exploits can be generated due to multiple vulnerabilities and what effects can be of such exploitation. Multihost multistage vulnerability analysis (MulVAL) tool is used for generating attack graph in this work. MulVAL generated graphs are logical attack graphs based on logical programming and based on dependencies among attack goal and configuration information. The risk of network attack graph is measured through graph topology theoretic properties (connectivity, cycles, and depth), and analysis of possible attacks paths is carried out in this paper.

Keywords Attack graph · Logical attack graph · Network security metrics · Risk analysis · Attack paths

1 Introduction

It is an emerging issue to control network security with growth of network size and numbers of vulnerabilities. The dynamic nature of the attacks and network size are the current challenges for the attack graph generation and analysis of attack graph.

K. Prasad (✉) · S. Kumar · A. Negi
Department of Computer Science & Engineering, Graphic Era University, Dehradun, India
e-mail: kainulyk@gmail.com

S. Kumar
e-mail: amu.santosh@gmail.com

A. Negi
e-mail: anuradhanegi40@gmail.com

A. Mahanti
Department of Computer Science, University of Auckland, Auckland, New Zealand
e-mail: a.mahanti@auckland.ac.nz

S. Das et al. (eds.), *Proceedings of the 4th International Conference on Frontiers in Intelligent Computing: Theory and Applications (FICTA) 2015*, Advances in Intelligent Systems and Computing 404, DOI 10.1007/978-81-322-2695-6_42

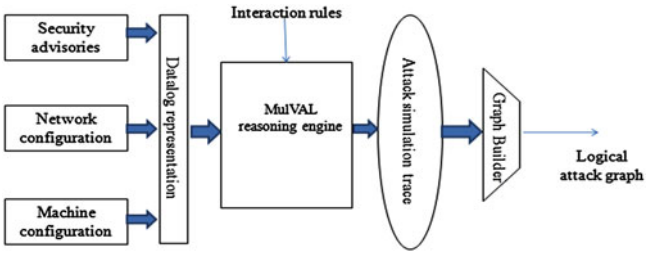

Fig. 1 Logical attack graph generator [1]

Therefore, it is essential to integrate very fast and accurate security approaches to evaluate the existing security state of the network. For this purpose, attack graph [1, 2] is mostly used technique. An attack graph describes how an attacker can gain privileges on a system by linking multiple vulnerabilities [3]. How, a logical attack graph can be generated, the required approach is shown in Fig. 1. There are four phases for logical attack graph generation, phase 1 Data log representation, phase 2 interaction rule with MulVAL and XSB reasoning engine, phase 3 attack simulation traces, and finally phase 4 graph builder as show in Fig. 1.

Phase 1 Datalog Representation It is obtained with integration of three components which are major inputs for an attack graph generator:

First component security advisories: which consists firewall rules, i.e., allow the connection, allow the connection with security check, and block the connection.
Second component network Configuration: which provides description about routers, switches, and other network devices which are involved to control the entire network.
Third component machine configuration: which describes about platform of host machine.

Phase 2 Interaction Rule with MulVAL and XSB Reasoning Engine MulVAL [4, 5] is an end-to-end framework and reasoning system that conducts multihost, multistage vulnerability analysis of a network. The MulVAL reasoning engine takes encoded information as an input from datalog representation and produces complete logical attack graph along with the basic network topology information for analyzing the whole network. Figure 1 shows the complete framework of the MulVAL system. MulVAL system is able to import data from the vulnerability scanners such as Nessus [6], Oval and vulnerability database NVD [7]. The reasoning engine consists of collection of Datalog rules that capture behavior of the operating system and interaction between various components in the network. MulVAL is an integrated system of MulVal software, XSB, and graphviz. XSB is a reasoning system and logical programming of attacks is done in XSB.

Phase 3 Attack Simulation Traces The result of this phase details the vulnerable IP addresses in the network and list of vulnerabilities present in those IP addresses.

Phase 4 Graph builder The attack simulation traces are fed into Graphviz to obtain logical attack graph in various formats.

Logical Attack Graph

Logical attack graph describes logical dependencies among network attack goals and configuration information. A logical attack graph always has size polynomial to the network, which is to be analyzed. The edges of the network attack graphs specify causal relations between network configurations and attackers potential privileges.

Figure 2 shows an example of a simple logical attack graph, nodes p1 and p2 are called as privilege nodes, while nodes e1, e2, and e3 are called exploit nodes. The nodes c1, c2, c3, c4, c5, c6, and c7 are referred to as fact/configuration nodes. In essence, the exploit nodes represent the host machines in the network that can be attacked, while the configuration nodes are sets of configurations (such as firewall rules and IDS configurations) that those hosts have been configured with. The privilege nodes represent the privileges that those host machines are capable of running. In the representation of logical attack graphs, the privilege nodes are treated as OR nodes, which can be satisfied, if any of the child node is true. Exploit nodes are treated as AND nodes which only be satisfied when all of its children are satisfied.

In this paper, we have used Ubuntu 12.04 platform for generation and MATLAB for risk analysis of attack graph. Rest of the paper is organized as follows. Section 2 describes graph theoretic properties-based security metrics [8, 9, 10]. The generated graph analysis and possible attack paths in attack graph [11] are analyzed in Sect. 3. Finally, Sect. 4 concludes the work.

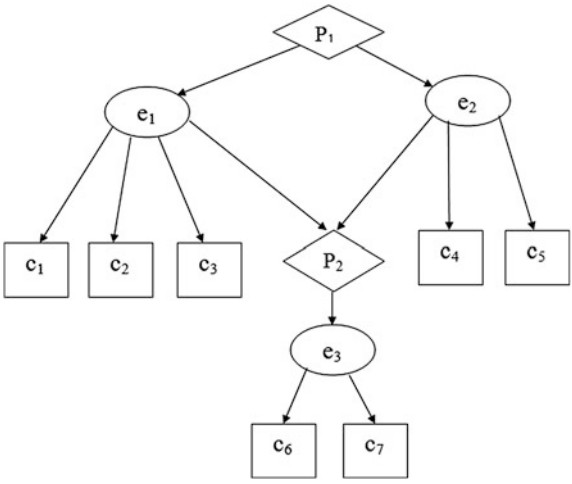

Fig. 2 Logical attack graph

2 Graph Theoretic Properties

Risk analysis over attack graph can be done using graph theoretic properties [8]. Graph theoretic properties only can be applied on directed graph. These properties are useful to determine risk associated with the attack graph. We have calculated the risks on the base of common vulnerability scoring system (CVSS) [12] scale of (0, 10) where 0 signify most secure and 10 signify least secure.

2.1 Connectivity

Connectivity defines the number of connected components in a graph. The worst case (least secure) is when a graph has only single components and best case (most secure) is when the graph is totally disconnected. If w is the number of components in the graph and d is the most possible number of components (total number of nodes) in the graph then connectivity metric is given by equation:

$$\text{Connectivity metric} = 10\left(1 - \frac{w-1}{n-1}\right) \tag{1}$$

An example of the connectivity metric with various components is shown in Fig. 3. In this example, we have found that the connectivity score decreases as the number of connected components increases. Therefore, it is proved by statistical results obtained that single-connected component has the highest connectivity score which signifies high risk.

2.2 Cycles

Cycle is a subgraph of those nodes which are reachable to each others in a graph. The risk of attack graph also depends on the number of cycles in the graph. If a

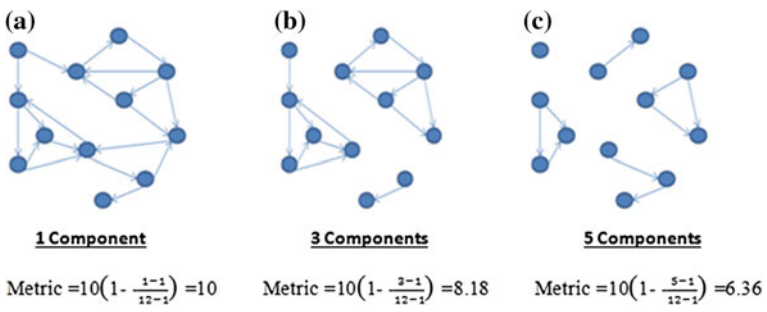

Fig. 3 Connectivity metric

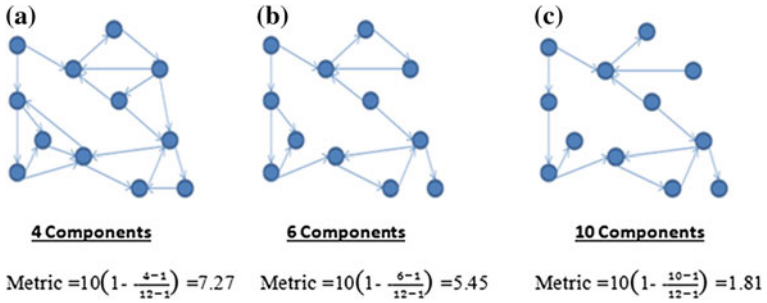

Fig. 4 Cycles metric

number of cycles are less than an attack graph is more risky and if cycles are more then attack graph is more secure. If c is the number of cycles in the graph and d is the most possible numbers of cycles in the graph then cycles metric is given by equation:

$$\text{Cycles metric} = 10\left(1 - \frac{c-1}{d-1}\right) \tag{2}$$

An example of the cycles metric values with various components are shown in Fig. 4. In this example, we have found that the cycle metric score decreases as the number of connected components increases. Therefore, it is proved by statistical results obtained that if the number of cycles in the graph are less then cycles score is high (less secure) and when the number of cycles are more then cycles score is less (more secure).

2.3 Depth

Depth of the graph is the length of maximum shortest path in the graph. It is also known as graph diameter. If n is the total number of components, d is the total number of nodes, c is number of nodes in different components, and s is the depth of the components. Depth metric is calculated by equation:

$$\text{Depth metric} = \frac{10}{nd}\sum_{i}^{n} c_i\left(1 - \frac{s_i}{c_i - 1}\right) \tag{3}$$

Figure 5 shows an example of depth metric with the help of 3 graphs. In this example, the every graph having equal number of nodes, but different number of diameters and components. Figure 5a, b have single connection with different diameter. Figure 5c has two component with different diameters. Result of metric concludes that if attack graph diameter is higher then network is more secure.

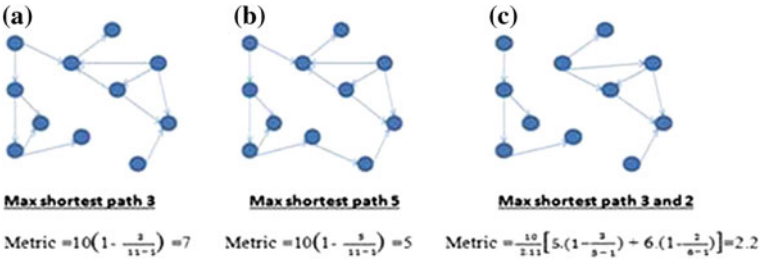

Fig. 5 Depth metric

2.4 Combined Score

It describes the combined score of all considered metrics, i.e., connectivity, cycles, and depth metrics of considered graph. The combined score can be calculated by the following formula

$$\text{Combined score} = 10\sqrt{\frac{\sum_{i=1}^{n}(s_i)^2}{\sum 10^2}} \tag{4}$$

where n is number of considered metrics and s is the individual score of metrics.

Figure 6a has 1 connectivity component, 4 cycles, and 9 diameter; Fig. 6b has 1 connectivity component, 6 cycles, and 6 diameter; and Fig. 6c has 1 connectivity component, 10 cycles, and 6 diameter. Combined score of Fig. 6c is the lowest among the three graph, therefore, this is the more secure attack graph as compare to Fig. 6a, b.

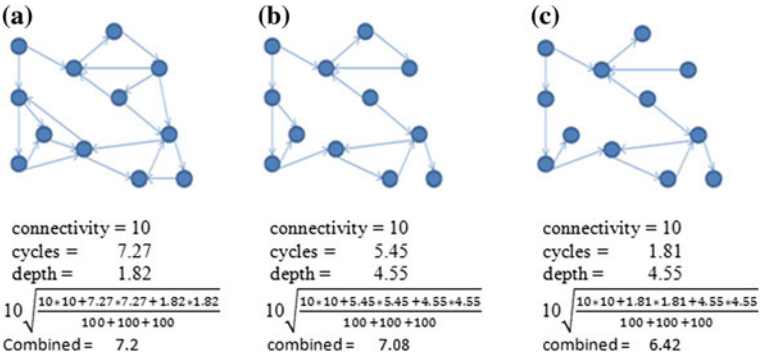

Fig. 6 Combined score metric

3 Results Analysis

The Ubuntu version 12.04 platform is used for logical attack graph generator. We have used Nessus vulnerabilities scanner for scanning the networks. Section 1 of this paper describes the used methodology to generate the logical attack graph. It consists four phases which are shown in Fig. 1. In the present work, the network configuration is done with the creation of a set of host access control list (hostname1, hostname2, protocol, port) and Datalog tuples as input to the MulVAl reasoning engine. The vulnerabilities are obtained with the creation of set of vulExists and vulProperty.

Figure 7a, b represent logical attack graphs generated by MulVAL. This graph has three types of nodes, diamonds nodes are privileged nodes, oval nodes are exploiting nodes, and rectangle nodes are fact or configuration nodes. The logical attack graph shown in Fig. 7a has 12 nodes, 1 connectivity component, 9 cycles and

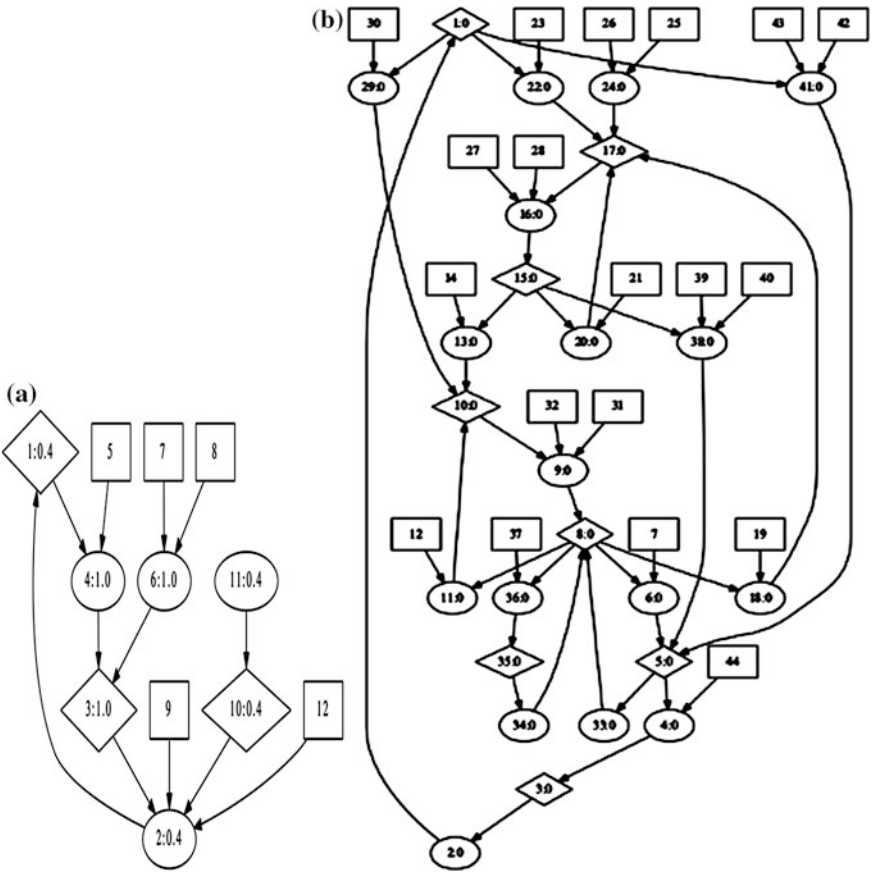

Fig. 7 MulVAL generated logical attack graph

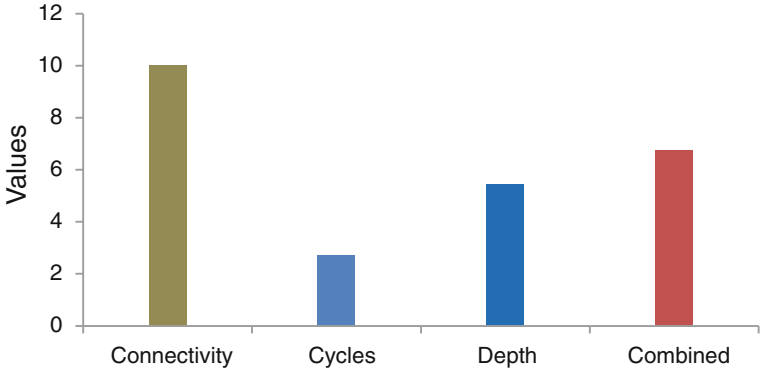

Fig. 8 Score of metrics for logical attack graph of Fig. 7a

5 diameter, and the logical attack graph shown in Fig. 7b has 44 nodes, 1 connectivity component, 21 cycles, and 11 diameter.

In the present analysis, Figs. 8 and 9 represent score of connectivity, cycles, depth, and combined metric of attack graph shown in Fig. 7a, b, respectively.

The connectivity metric score is 10 for 12 nodes and 44 nodes, and therefore, it signifies that there is one connected component in both logical attack graphs, therefore, on the basis of connectivity score network is least secure.

The cycle metric score are 2.73 and 5.35, respectively, for 12 nodes and 44 nodes. In the case of 12 nodes, cycle metric score is less which results there are more cycles or sub graph (all reachable nodes from each others) in the attack graph. Therefore, the network is more secure network. However, the result in Fig. 9 having more cycle score, which signify less secure network.

The depth metric score are 5.45 and 7.44, respectively, for 12 nodes and 44 nodes. In Fig. 8, it is observed that depth metric score are 5.45 which is less score as compare to 44 nodes which conclude the network is more secure. However, the result in Fig. 9 having more depth score, which signifies less secure network.

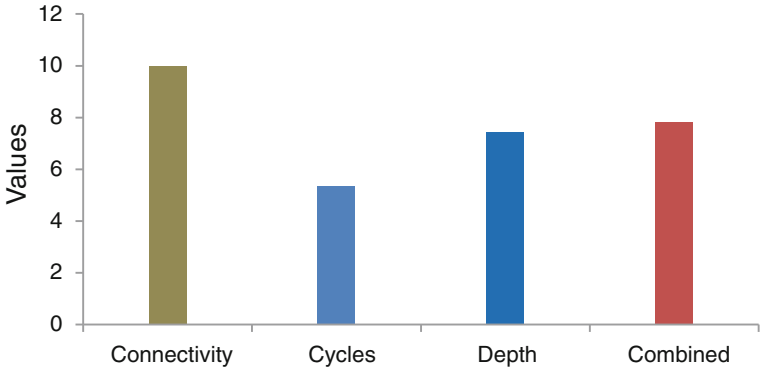

Fig. 9 Score of metrics for logical attack graph of Fig. 7b

The combined scores are 6.76 and 7.83, respectively, for 12 nodes and 44 nodes. In Fig. 8, it is observed that combined scores is 6.76 which is less score as compare to 44 nodes which shows the network is more secure. However, the result in Fig. 9 having more combined score, which signify less secure network.

3.1 Attack Paths Analysis

If we calculate all attack paths in the logical attack graph then we can prevent the attack, which could be happen on the network. In logical attack, graph fact nodes are source nodes for the attacker that means fact nodes (which describe firewall and machine configuration) has to be satisfied for any attack. If fact nodes not satisfied, then no attack is possible. Attacker goal is to gain privileges in the network host machine, therefore, privilege nodes in the logical attack graphs are the destination nodes. In Fig. 2 e1, e2, and e3 are exploiting nodes. Since exploit nodes are AND nodes, so all children nodes must be true for the satisfaction of exploiting node. The exploit node e1 will be true if children c1, c2, c3, and p2 are true. The exploit node e2 will be true if p2, c4, and c5 are true. The exploit node e3 will be true if c6 and c7 are true. Privileges are OR nodes so if any child is true, then condition is true. All attack paths for graph in Fig. 2 are:

(i) e3 –> p2
(ii) e3 –> p2 –> e1 –> p1
(iii) e3 –> p2 –> e2 –> p1

There are three attack paths for a graph given in Fig. 2, but these attacks are only possible when e1, e2, and e3 are logically true.

4 Conclusion

The modeling of logical attack graph gives opportunities to analyze the network with more efficient ways. This work describes how MulVAL runs efficiently for networks with numbers of hosts, and it has discovered an interesting security problem in a real network. We examined risk associated with the network attack graph using graph theoretic properties (connection, cycle, and depth) on the scale of (0–10), where score 0 is fully secure and 10 is worst secure. The analysis has been done on a network with different number of hosts (different numbers of nodes) and the result shows how risk factor heavily depends on depth and cycles present in the graph. All attack paths in logical attack graph also calculated in this work; once we know attack paths, we can prevent them by changing system or firewall setting.

References

1. Ou, X., Boyer, W., McQueen, M.: A Scalable Approach to Attack Graph Generation. ACM (2006)
2. Ingols, K., Lippmann, R., Piwowarsi, K.: Practical attack graph generation for network defense. In: 22nd Annual Conference on Computer Security Application, pp. 121–130 (2006)
3. Zhang, S., Caragea, D., Ou, X.: An Empirical Study on Using the National Vulnerability Database to Predict Software Vulnerabilities. Database and Expert Systems Applications, pp. 217–231. Springer, Berlin (2011)
4. Ou, X., Appel, A.W.: A logic-programming approach to network security analysis. USENIX Security (2005)
5. Ou, X., Govindavajhala, S., Appel, A.W.: MulVAL: a logic-based network security analyzer. In: 14th Usenix Security Symposium (2005)
6. Nessus security scanner. http://www.nessus.org
7. NIST, NVD. http://nvd.nist.gov/cvss.cfm
8. Noel, S., Jajodia, S.: Metrics suite for network attack graph analytics. In: Proceedings of the 9th Cyber and Information Security Research Conference. Oak Ridge National Laboratory, Tennessee (2014)
9. Wang, L., Islam, T., Long, T., Singhal, A.: An Attack Graph-Based Probabilistic Security Metric. Data and Applications Security, pp. 283–296. Springer, Berlin (2008)
10. Wang, L., Singhal, A., Jajodia, S.: Measuring the overall security of network configurations using attack graphs. Lecture Notes in Computer Science, vol. 4602, pp. 98–112. Springer, New York (2007)
11. Williams, L., Lippmann, R., Ingols, K.: GARNET—a graphical attack graph and reachability network evaluation tool. In: Proceedings of the 5th International Workshop. Springer, Cambridge (2008)
12. Common Vulnerability Scoring System (CVSS). http://www.first.org/cvss