International Journal of Research

International Journal of Research (IJR)

e-ISSN: 2348-6848, p- ISSN: 2348-795X Volume 2, Issue 09, September 2015

Available at http://internationaljournalofresearch.org

K- Zero Day Safety: Metric for Measuring the Risk of Unknown Vulnerabilities

Mise Pallavi Ramesh

M.Tech ANURAG Group of Institutions (CVSR College of engineering)

Mrs. N. Swapna Goud

M.Tech Associate Professor

ANURAG Group of Institutions (CVSR College of engineering)

Abstract:

Today's computer networks face intelligent attackers who combine multiple vulnerabilities to penetrate networks with destructive impact. The overall network security cannot be determined by simply counting the number of vulnerabilities. Due to the less predictable nature of software flaws we can't measure the security risk of unknown vulnerabilities. This affects to security metrics, because a safer configuration would be of little value if it were equally vulnerable to zero-day attacks. In this paper, instead of just measuring how much such vulnerability would be required for compromising network assets we can also attempting to rank unknown vulnerabilities. By using collaborative filtering technique to different (types of) zero-day vulnerabilities and novel security metrics for uncertain and dynamic data we propose a Flexible and Robust k-Zero Day Safety security model to rank the zero-day attacks.

Keywords: vulnerability; zero-day attacks; collaborative filtering

Introduction: A COMPUTER network has become the nerve system of enterprise information systems and critical infrastructures on which our societies are highly dependent. The scale of security threats to computer networks have continued to grow same way to tackle with this. Potential consequences of a security attack have also become more and more serious as many high-profile attacks are reportedly focusing on not only computer applications but also industrial control systems at nuclear power plants and military satellites. Main difficulties in securing computer networks are the lack of methods for directly measuring the relative effectiveness of different security solutions in a network under consideration, because “one cannot improve what one can't measure.” Intrusion detection system or firewall can sometimes be obtained through lab-testing, but they are hardly aware of the real effectiveness of the solution when it is deployed in a real world network, which can be very different from the testing environment. .Selecting and deploying a security solution still heavily rely on human experts’ experiences following a trial-and-error approach, which is a task of art, instead of a science. Matrix method is adapted since it would enable a direct measurement and comparison of the amounts of security provided by different security solutions, but it also has some us tackled issues like efforts on network securable on zero day attacks effect of immeasurable threats is that without considering unknown vulnerabilities, a security metric will y metrics typically assign numeric scores to vulnerabilities based on known facts about vulnerabilities. This method is not applicable on zero-day attacks effect of unmeasurable threats is that without considering unknown vulnerabilities, a security metric will have questionable value at best, since it may determine a network configuration to be more secure while that configuration is in fact equally susceptible to zero-day attacks. In this paper we propose a security metric, k-zero day safety, which will address this issue. In this instead of attempting to measure which unknown vulnerabilities are more likely to exist, we start with the worst case consideration that this is not measurable and then metric then matrix simply counts how many zero-day vulnerabilities are required to compromise a network. A larger count will indicate a relatively more secure network, since having more unknown vulnerabilities all available at the same time, applicable to the same network, and exploited by the same attacker, will be lower. We are implementing k-zero day safety metric based on an abstract model of networks and zero-day attacks. We consider the complexity of computing the metric and design heuristic algorithms addressing this complexity in special cases. Contribution of matrix approach to the best of our knowledge is that, this is among the first efforts on network security metrics that is capable of modeling the security risk of unknown zero-day attacks. Secondly the metric would bring about new opportunities to the hardening, quantitative evaluation and design of secure networks.

Motivation: Fig. 1 shows an example where host 1 and host 2 comprise Of internal network. Firewall permits all the outbound Connection requests but it blocks all the inbound requests to host 2. The main security concern here is whether any Of the attacker on host 0 can obtain root privileges on host 2. If we assumed all the services to be free of the known Vulnerabilities, then a vulnerability scanner or an attack graph will draw exactly same conclusion that this network has secure attackers on host 0 hence cannot obtain the root privilege on host 2.

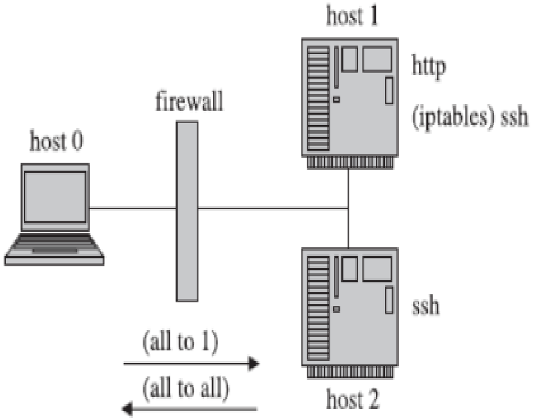

Fig. 1. An example network.

Consider the following two iptables policies:

Policy 1. The iptables rules are left in a default configuration that accepts all the given requests.

Policy 2. The iptables rules are configured which allows specific IPs, excluding host 0, to gain access to the ssh service.

Clearly, the network is already secure, policy 1 is preferred due to its simplicity (no special iptables rules are needed to be configured by the administrator) and functionality (any external host can connect to the ssh service on host 1). However, a different conclusion can be drawn if you compare the two policies with respect to the network’s resistance to zero-day vulnerabilities. Specifically, policy 1. Under policy 1, where each triple indicates an exploit vulnerability, source host, destination host and a pair indicates a host condition, it illustrates three possible ideas for compromising host 2: a. The attackers attacking hosts 0 exploits zero-day vulnerability in the HTTP service on host 1 and then use it as a stepping stone to exploit zero-day vulnerability in the secure shell service on host 2. b. He exploits zero-day vulnerability in the secure shell service on both of the hosts i.e host 1 and host 2. c. He exploited zero-day vulnerability in the firewall (e.g., a default password) to circumvent the traffic blocking it before it compromises host 2. The first and third case require two different and separate zero-day vulnerabilities, whereas the second requires one zero-day vulnerability (in the secure shell service). Therefore, the network may be compromised with at least one zero-day attack under policy 1. 2. Under policy 2, the second case is different: a. the same as 1a. b. The attacker can exploit zero-day vulnerability to circumvent the given iptables rules before exploiting the secured shell service on both hosts i.e. host 1 and host 2. c. The same as 1c. The three cases now require two different zero-day vulnerabilities. The network can, hence, be compromised with at least two zero-day attacks according to policy 2. Consider the fact that each zero-day attack has only a limited lifetime (before the vulnerability is disclosed and fixed), it is reasonable to assume that a large number of distinct zero-day vulnerabilities that is available during same time in this particular network will be significantly smaller (the probability will decrease exponentially if the occurrences of different vulnerabilities can be regarded as independent events; however, the metric will not be dependent on any specific statistical model considering the process to find vulnerabilities is believed to be very chaotic). To revisit the given example, the network is regarded as more secure under policy 2 as compared to policy 1 because the former requires more (two) zero-da attacks to be compromised. The crucial observation is that considering a network's resistance to zero-day vulnerabilities can assist in the relative security of various network configurations, which is otherwise indistinguishable under the existing vulnerability analysis and attack on graph-based techniques. The remainder of this paper is build upon this important observation and addresses the remaining issues.

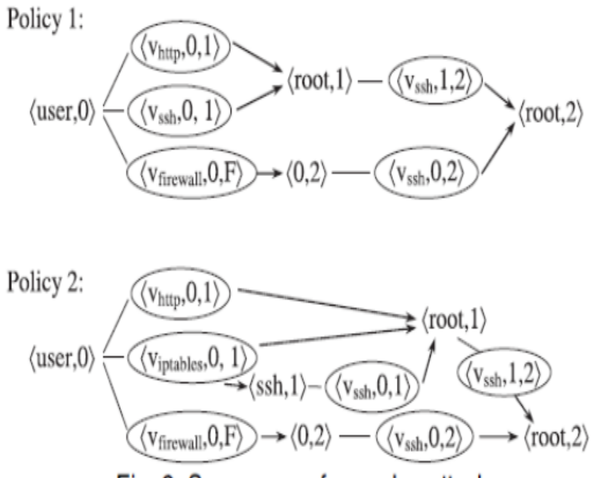

Fig. 2. Sequences of zero-day attacks.

Future Work: All zero-day vulnerabilities are regarded as equally likely due to their common immeasurability, where as in some cases safe assumptions can be made .Assigning different weights and probabilities to different (types of) zero-day vulnerabilities would be a extension to our proposed model. scope of our proposed metric is limited by the three basic considerations about zero-day vulnerabilities and those are the existence of network connectivity, vulnerable services on destination host, and initial privilege on source host .Make the broaden the scope by accommodating other types of attacks is an important future work .

A. Computing k count:

In this model firewall rule list dataset is designed by using network rules and used jpcap and WinPcap software's to capture the data packets travelled in network. After capturing data packets matches their sources and destination ip addresses in the firewall rule list. ip addresses of data packets are allowed can able to attack our system that packets transferring protocol count as vulnerability. Then optimized firewall rule list for security.

B. Calculating Risk of vulnerability

Using captured record in this module we can draw attack graph of vulnerabilities. By Asian network attack graph technique is used to design network attack graph. By using that network graph we can apply probabilistic reasoning to produce a risk measurement of vulnerability.

C. Ranking the vulnerability In this module we can use Collaborative filtering technique is used for ranking the vulnerability.

Conclusion and Future Scope Of Enhancement: In this project we design the security model for zero day attack. We are able to catch the total count of known and dynamic vulnerabilities in network which affect our system security. In previous system we are not able to calculate the risk of vulnerability as well as not able to rank the vulnerabilities for network hardening, this system provide this function. In this model we are using collaborative filtering for ranking vulnerabilities. In this model we are design practical model for firewall system. We configure optimal list of firewall rule list to make our system more secure and find the known as well as unknown and dynamic vulnerabilities in network. The scope of our metric is limited by the three basic assumptions about zero-day vulnerabilities (the existence of network connectivity, vulnerable services on destination host, and initial privilege on source host). The model will be more suitable for application to the evaluation of penetration attacks launched by human attackers or network propagation of worms or bots in mission critical networks. An important future work is to broaden the scope by accommodating other types of attacks (e.g., a time bomb which requires no network connection).

References :

[1] P. Mell, K. Scarfone, and S. Romanosky, “Common Vulnerability Scoring System,” IEEE Security and Privacy, vol. 4, no. 6, pp. 85-89, Nov./Dec. 2006.(24)

[2] MITRE Corp., “Common Weakness Scoring System (CWSS),” http://cwe.mitre.org/cwss/, 2010.(37)

[3] M. Frigault, L. Wang, A. Singhal, and S. Jajodia, “Measuring Network Security Using Dynamic Bayesian Network,” Proc. Fourth ACM Workshop Quality of Protection (QoP ’08), 2008.(9)

[4] Kaur, R.; Singh, M., "Efficient hybrid technique for detecting zero-day polymorphic worms," Advance Computing Conference (IACC), 2014 IEEE International ,pp.95,100, 21-22 Feb. 2014.

[5] J. Homer, X. Ou, and D. Schmidt, “A Sound And Practical Approach to Quantifying Security Risk in Enterprise Networks,” technical report, Kansas State Univ., 2009.(12)

[6] R. Lippmann, K. Ingols, C. Scott, K. Piwowarski, K. Kratkiewicz, M. Artz, and R. Cunningham, “Validating and Restoring Defense in Depth Using Attack Graphs,” Proc. IEEE Conf. Military Comm. (MILCOM’ 06), pp. 981-990, 2006.(20)

[7] N. Poolsappasit, R. Dewri, and I. Ray, “Dynamic Security Risk Management Using Bayesian Attack Graphs,” IEEE Trans. Dependable Secure Computing, vol. 9, no. 1, pp. 61- 74, Jan. 2012.(31)