Available online www.ejaet.com

European Journal of Advances in Engineering and Technology, 2015, 2(1): 30-34

Review Article ISSN: 2394 - 658X

A Review on Zero Day Attack Safety Using Different Scenarios

Harshpal R Gosavi and Anant M Bagade

Department of Information Technology, Pune *Institute of Computer Technology (PICT), Pune, India*
harshgosavi007@gmail.com

ABSTRACT

A zero day attack is the type of attack where people make use of flaw in the software developed by various companies. There is no patch available so it is difficult to tackle such types of attacks even when developers of the company are known to this. For any network such attacks can be possible only way to get through this is to prevent such types of attack. If the network administrator knows that how many such attacks can be possible then he can make some changes in his administrator rights. It is found that more than five thousands vulnerabilities are occurring per day. We are proposing complete novel scenario which can lead to the counting of such vulnerability in very efficient way. Using this method we can easily provide option of network hardening so as to prevent it from unknown vulnerability.

Key words: Network administrator, patch, vulnerability, zero day, network hardening.

INTRODUCTION

Now a day, in any network immeasurable vulnerabilities could be found in services which are working on various components of the system. There are few methods of the security as shown below.

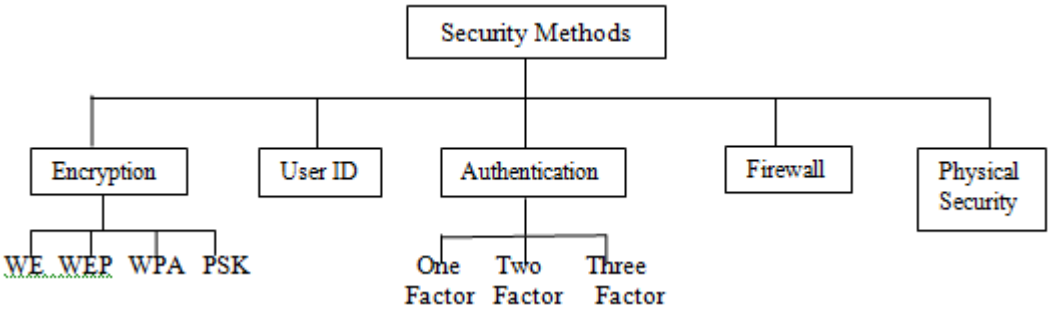

Fig. 1 Types of security methods

Encryption
Encryption is converting useful data into such format so that nobody can understand it. This has four different methods.

Wireless Encryption (WE)
Wireless Encryption is done on wireless network. Various wireless algorithms are developed to implement this encryption.

Wired Equivalent Privacy (WEP)
This also called as Wireless Encryption Protocol. This is the method which states that malicious link should not use.

Wi-Fi Protected Access (WPA)
This generally used to encrypt the secure and source traffic by efficient.

Pre-shared Key (PSK)
In this method the sharing key will be done in the two different machines and security is provided.

User ID
Here it uses the Username and ID to identify the permitted user and according to it he has the rights to access.

Authentication
Authentication has three types. 1) One Factor 2) Two Factor 3) Three Factor. In one factor user knows something to access the network. In two factor anything that user has to physically access the network. In three factor something that user needs like retina scan or finger prints.

Firewall
Firewall blocks unwanted packets and it also analyze the network traffic. It checks incoming packets and give authority that to allow this packets or not.

Physical Security
When somebody breaks something by going physically there. Web applications basically deals with such problems which needs services to run those applications. Web application with injection flaw is widely occurring in the network. Researcher wants to find it from many years to understand it.

Existed Systems
Common Weakness Scoring System (CWSS) is the system where it counts the known vulnerability but say very little about the unknown. Sometimes it was recommended that to merge this into firewall so as client side would not need external security. Modeling network graph can be way to demolish it and has been tested over 40000 hosts to check its compatibility with network [1]. Even if many methods are available to lower down this attacks but no method nearly predict the exact risk of the threat which are acting on the network [2]. NetSPA was one of the tool which uses attack graph to model this threats [3]. It scans the network for the vulnerability and from the preferable input it draws the attack graph to know that vulnerability present over the network [3].

Topological Vulnerability Analysis (TVA) is one of the attack prevention methods which is powerful [4]. This vulnerability can be depending on each other of the different network system. User sometimes even cannot know that how this thing are happening as there is large abstraction in the given applications. In this approach the network is configured and tested for the sequences of the vulnerability. This is shown in the Fig. 2.

Vulnerability Discovery Model is also one of the models to detect count of the vulnerability in any software [5]. So there is always one question can arise that is there any database for measuring the risk of attacks [2]. The attacks related to the exploitation of the vulnerability are common but to make patch of such vulnerability is difficult and cost effective.

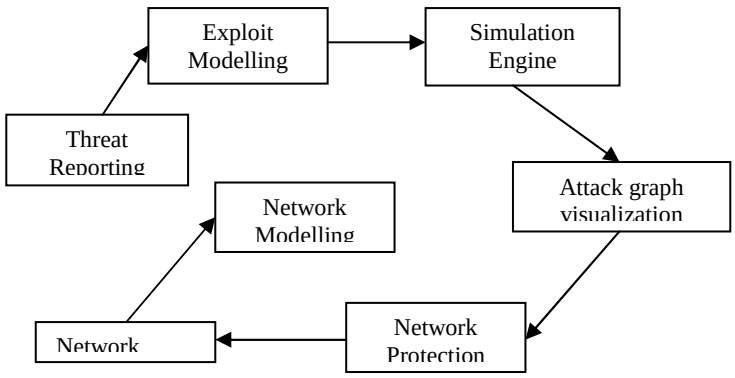

Fig. 2 Process of topological vulnerability analysis

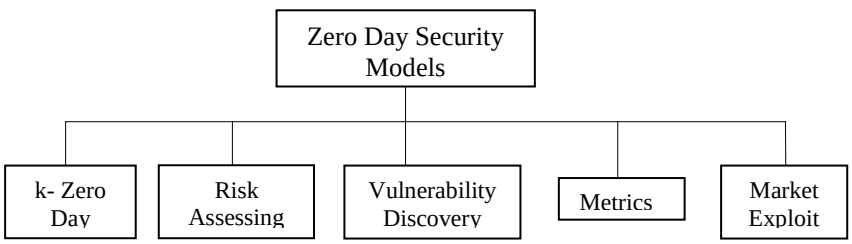

Fig. 3 Zero day Security Methods

APPROACHES OF ZERO DAY MODEL

The zero day safety comes under the firewall security methods. Firewall blocks the unknown packets which are always roaming in the corresponding network. For this type it is further divided into five types of security. It is shown in Fig 3.

k-Zero Day

In this model, the various connected host are measured and different services related to it are detected [1]. The services in which vulnerability can be possible are to be found out. Such count is measured and then it is informed to the corresponding network administrator. The remote services are accessed remotely over the network.

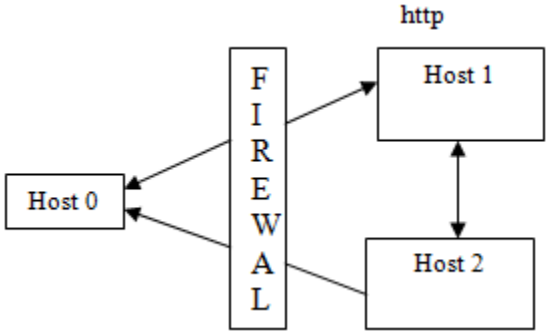

Fig. 4 Example of Zero day vulnerability

As shown in the above fig 4. it is necessary to first make the sequences of the services and corresponding host to determine the distinctness and then it needs to find vulnerability possibilities in the services of those host. The host0 can attack on host1 to exploit vulnerability and to get into root. This vulnerability can again be exploited host2 to gain the access of its privileges. The ways provided to get rid of this is to make an attack graph[3]. It can be exploited like (0,F), (0,1) and then (0,2). It means for first set it is going from host 0 to Firewall. As soon as this services are known which can contain this vulnerability are counted. This metric can be applied to any network and then the administrator can take care of this by using different applications which can prevent further destruction because of these vulnerabilities [1].

Risk Assessment

The risk assessment can be done using the vulnerability in the network whether they exists in large or small quantity [2]. Its functions are based on probability of nodes in the network. Each network node is checked that existing node is true or false for giving access or privileges to another node. Using the probability theory the sample space of a node is calculated and then probability is calculated. In this way a risk of the network can be determined and vulnerabilities can be minimized by prior knowledge of software applications by this node. There are many other factors that are affecting the risk of the network and thus it is very important to analyze the risk of the network.

Vulnerability Discovery Variables

Literature review revels that there are four types of variables for the web applications.

a) Types of the threat and corresponding attacks.
b) People are aware of the vulnerability or not and whether it is in large quantity or not.
c) Security of vulnerability.
d) The mechanisms for such questions.

These are the basic variables for the web applications but there are many types of mechanisms in the survey to discover the vulnerability [5]. Some of them can be Expert Decisions, Construction of maker and scoring information are widely used methods for discovering such zero day vulnerabilities.

Vulnerability Metric by Actual Attacks

This basically relies on the concept of VEA-bility.

V- Vulnerability E- Exploitability A- Attackability

The metric would be done on this three parameters. By using CVSS impact they aggregate the system by individual and all scores are calculated according to its attack graph [1] [3]. The basic equation made by their survey is as follows.

$$A(\text{System}) = \frac{10 \times \sum \text{attack paths}}{\sum \text{Network paths}}$$

From above equation if we know the attack paths and network paths then we can calculate the possible attacks in that network.

Market Zero day Exploit

In the current industries zero days gaining so much popularity thus it is necessary to keep this away from the companies current software because it may leads to the large disaster of the company's assets. There are many arguments like 'for' and 'against' are best explained in corresponding paper. Also there are some tools for checking its availability; it can be named as Cobra effect on credit card and Cobra effect on industry [3]. This approximate includes 15 such effect which are related to avoiding this effects. Even search is a lot but solutions seems to be different because no availability of the definitions of such flaws. The comparison of the markets vulnerability can lead to the efficient knowledge of the existing threats. From this it can be possible to identify the solutions related to the corresponding vulnerability [6].

Table -1 Comparison of Different Methods

Method	Count	Time	Efficiency
k- Zero day	Count unknown attacks	Fast	Best
Risk Assessment	Count risk	Slow	Good
Vulnerability metric	Count by CVSS but not unknown	Moderate	Good
Market Zero day	Count is limited to industry	Moderate	Moderate

PROPOSED APPROACH

There are many flaws in the existing system so there is need of new system which tracks down the flaws in the existing system. Before proceeding it is necessary to know all the services are active on the network. The scenario proposed below is novel scenario and if we go through procedure in fig. 5 then it is easy to count the number of vulnerability possible in the network. Now let's see what is happening in each phase.

Sequences

Every service works differently as according to program that are written into it. Thus, make the different sequences of such services by using set theory. Example if host 1 can exploit the vulnerability on host 2 then in the matrix of n x n we will going to make corresponding field as 1(n is number of host).

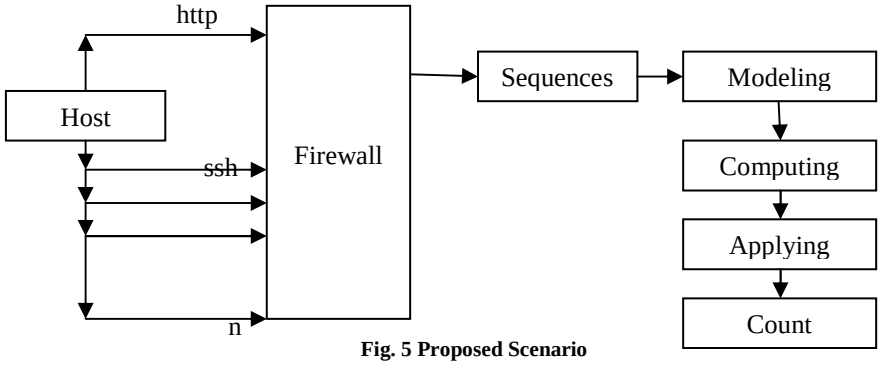

Fig. 5 Proposed Scenario

Modelling

In the modelling, the sequences made in earlier stage are modelled to check the existence of vulnerability. In the first stage network model is to be prepared, it consist of all the information about the network and related routing connections. The connected systems are gathered together to get access and then kept for checking of each and every path of the services. Before checking it has to find that how much privilege it has given to the other systems of the network. Now concentrating on remote system to be check whether the remote systems contains such vulnerability or not. If there exist such vulnerability then it can leads to the exploitation of vulnerability in the destination host.

Computing

Computing is nothing but counting the number of vulnerabilities in the network by deriving various logic propositions rigorousness of the network is determined and vulnerabilities are kept aside. The assets related to it are taken away separately and attack graph tells the exact process of the services [3]. For the next phase determine safety for zero day upto the particular threshold by applying recursive methods. Its complexity will leads to the polynomial in size of zero day attack graph [3]. It means that whatever network assets are available it need to try that this assets would compromise the network upto certain threshold. There are many chances where value of k will become constant. The third phase consists of finding the shortest path via acyclic directed graph (DAG). As the remotely computer requires the privileges, same kind of zero day are arranged in a relation. Any algorithm can be applied to find out shortest path in the attack graph. It would check from node to node and from each node there will be edge for knowing the connections statistics. There should be checking of each node visited or not and the statistic of such visited node have to be considered.

Applying

Here it shows the potential of the metric by applying it to the network hardening. It increases security and it can be done by changing some configuration. It also provides some solutions related to it so that security of the network will increase.

This type of solutions could be valid or invalid thus only valid solutions would be taken into consideration. It takes care of the disabling services then in the network diversity it could be done by taking special care and by terminating each tree services.

Counting

Counting is process of making final attack graph and determines the number of zero day attacks. This would inform to the network administrator to change settings or disabling the services which are acting currently and making vulnerabilities in it [7].

RELATED WORK

The Markov model was the model in which vulnerability identified according to the time and efforts. Currently all are taking efforts on making the attack graph which is little bit different kind to search the network security. The metric is varying day by day as the exploitation of the vulnerability is increasing. The concept of network hardening is currently stayed away but works also in the way to solve [7]. Empirical analysis has been done to know the actual effect of the attack [8]. The most of all are working on to provide security to particular applications but as the network sharing is increased everybody found that to work for the applications which are commonly used. The work was done only on one way to the system but it has to be done parallely. There are some tools need to be there to find it parallel this has been taken in account. Empirical study is aware of the vulnerability occur for the particular time period. Injections of attacks are generally considered as temporary task but it can be blocked by using solution of ant viruses sometimes [9]. The main thing is finding the location of an attacker so as to track such path via different locations [10]. Knowing the IP address of the system of an attacker it can be done but first it needs to find what was the path of the packet which was transmitted from the long distance.

CONCLUSION

This review paper presented novel security scenario for counting the zero day vulnerability and approaches of the zero day attack model. This approaches shows how this zero day can be handled in any given network which includes counting of unknown vulnerability through which we can improve the security. Future work is to develop different technologies for ranking zero day vulnerabilities. There are many situations where uncertain handling of inputs are not considered, this also includes in future work.

REFERENCES

[1] P Mell, K Scarfone and S Romanosky, Common Vulnerability Scoring System, *IEEE Security and Privacy*, **2006**, vol. 4, no. 6, p. 85-89.

[2] Davide Balzarotti, Mattia Monga and Sabrina Sicari, Assessing the Risk of Using Vulnerable Components, *Springer Quality of Protection Advances in Information* Security, **2006,** 23, p. 65-67

[3] K Ingols, M Chu, R Lippmann, S Webster and S Boyer, Modelling Modern Network Attacks and Countermeasures Using Attack Graphs, *IEEE Conf. on Computer Security Applications,* **2009**, p.117-126.

[4] S Jajodia, P Liu, V Swarup and C Wang, Topological Vulnerability Analysis: A Powerful New Approach for Network Attack Prevention, Detection and Response, *Cyber Situational Awareness*, **2010,** p. 139-154.

[5] S Egelman, C Herley and P C Van Oorschot, Market for Zero-Day Exploit: Ethic and Implications, *Proceedings of the 2013 workshop on New Security Paradigms Workshop,***2013,** p. 41-46.

[6] John Homer, Xinmin Qu and David Schmidt, A Sound and Practical Approach to Quantifying Security Risk in Enterprise Networks, *peoplecisksuedu/~xou/publications/tr_homer_0809pdf, **2008.***

[7] L Wang, S Jajodia, A Singhal, P Cheng and S Noel, k-Zero Day Safety: A Network Security Metric for Measuring the Risk of Unknown Vulnerabilities, *IEEE Transaction on Dependable and Secure Computing*, **2014,** Vol.11, Issue1, p. 30-44.

[8] M Ekstedt and H Holm, Empirical Analysis of System-level vulnerability metrics through actual attacks, *IEEE Transactions on Dependable and Secure Computing,***2012**, Vol. 9, Issue 6, p. 825-837.

[9] J Antunes, N Neves, MCorreia, P Verissimo and R Neves, Vulnerability Discovery with Attack Injection, *IEEE Transaction on Software Engineering*, **2010**, Vol. 36, Issue 3, p. 357-370.

[10] T Sommestad, H Holm and M Ekstedt, Effort Estimates for Vulnerability Discovery Projects, *Proc 45th Hawaii International Conference on System Sciences,* **2012,** p. 5564-5573.