Special Issue of Engineering and Scientific International Journal (ESIJ)
Technical Seminar & Report Writing - Master of Computer Applications - S. A. Engineering College (TSRW-MCA-SAEC) - May 2016
ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

Survey on Ethical Hacking and System Security

R. Edward Andrews [#1], S. Sridhar [*2]

[1]*Master of Computer Applications, S.A. Engineering college, Chennai-77.*
edwardandrewsr@gmail.com
[2]*Asso. Prof., Department of Computer Applications, S.A. Engineering College, Chennai-77.*
sridhar@saec.ac.in

Abstract— This paper explores the survey on the ethical hacking and system security. Hacking is the access to unauthorized system or get the information unethically. Since ethical hacking has been controversial subject over the past few years. Then we are detecting the worms in the vulnerability scanning. A worm is a program that propagates across a network by exploiting security flaws of machines in the network. We suggest and assess an algorithm to perceive extend of worms using actual time traces and simulations.

Keywords— Hacking; Scanning; Vulnerability; Worm.

1. Introduction

Ethical hacking was the process of introspect the security weakness and discovers the potential security vulnerabilities. White hat hacker to find out the weakness in the network or computer. Black hat hacker is a malicious hacker. He/she done for their personal gain. Grey hat hacker is a person who is skilled enough to act as a good or bad in both ways. What are the issues and problems we face in the ethical hacking and the system security we discuss about that. The term "ethical" means legally. Security that protects the confidentiality, integrity & availability of resources.The intent of ethical hacking was to discover vulnerabilities from a malicious attacker's viewpoint to better securing programs.Ethical hackers are mostly people with a good knowledge of operating system and computer technology.

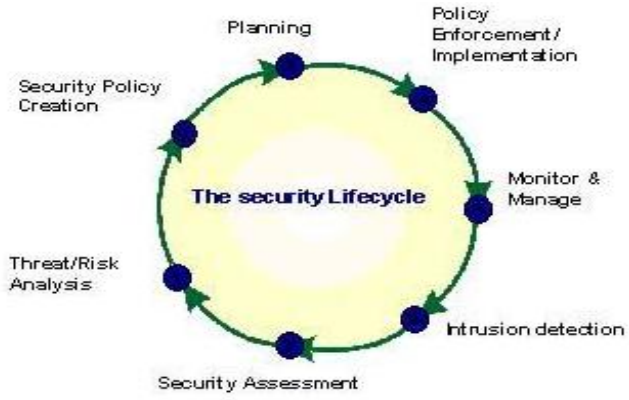

Fig.1: The Security Life Cycle

An Ethical hacker's facts was similar to the one of a "real" hacker.It is identified, that various black hats have been changed to white hats and it is used their facts on how to chop a system in an ethical method. Hiring ex-hackers as ethical hackers is very controversial. They give details report to the owners with the vulnerabilities. It is also called as penetration testing. The need to protect the important data of the same should be addressed with right technology. After, an ethical hacker see sensitive information and needs to be extremely trustworthy.Security policy creation, Plan, policy enforce, monitor & manage, intrusion detection, security, threat / Risk analysis mentioned in fig.1.

2. Literature Survey

Ethical scythe: It is the procedure of introspect the safety flaw and determines the possible safety vulnerabilities for a customer which was accountable for the assaulted in sequence technology surroundings principled hacker is also identified as white hat scythe. Types of penetration testing:White box is closely stimulated to that of an external attacker, give little info or no knowledge about the systems to be tested.Black box is the tester generally provided the information about the network to be tested include the IP address.

2.1 Merits

- Avoid cost of network.
- Preserve the corporate image and customer loyalty.
- Meet the requirements.
- Manage vulnerabilities[1].

Education and training: Teaching students to hack is still a very serious issue that we are faced today. Specialist experiences that they educate students how to get better interruption which unluckily not occurrence. Appreciate the true function of the students was rough to discover outhe grounds why ethical hacking should be used. A problem was thestudents using this approach is that the instructor was effectively providing them Trusting the potential enemy: The need for secure information was important and it plays an important factor in ethical hacking. This information can lead to the problem of who

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

can obtain that information and who should see it.Risk management: Ethical hacker could search vulnerabilities in proceed to minimize the jeopardy[2]. Reconnaissance: To collect all the information of that company whose date need to be hackedScanning: To make an outline of the target network include the IP address of the end or target network which are live. Gaining access: The attackers will get the access of the system or network and it have the ability to spoil the system completely. The system helped.Maintaining access: In this context that hacker can use the target system as launch so that he can scan other system and can damage them.[3]. System security: It secure a system form unknown access by the person who can physically access it.

2.2 Advantages of ethical hacking

- To help in detect the offences taking place through internet.
- It can assist to detect and also to prevent cyber crime.
- Everything it depends upon the knowledge and trustworthiness of the ethical hacker.

2.3 Modes of ethical hacking

- Remote network.
- Local area network.
- Stoled equipment.
- Social engineering.
- Physical entry[5].

Scanning: It is used to find out the weakness or a hole in the system or network. Vulnerability scanning: The hacker will come to know about the kernel method and other linked details of working system such as the service pack is installed or not. The vulnerability scanner was identify the hole of the operating system. So that this can be attacked. Vulnerability scanning refers to which system are connected to host or internet it is scanned .

3. Proposed system and methodology

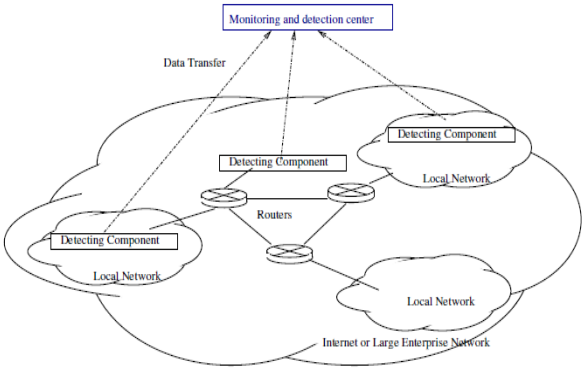

Fig.2: Worm Detection Architecture

Our goal is to detect unknown worms on spreading through the network. We present the general worm detection architecture. The worm is dispersion throughout the network. It contaminates the data obtainable in the host.

4. Generic worm detection architecture

To detect worms, we need to analyze internet traffic. Monitoring traffic towards a single network. The architecture monitors the network behavior at different places.The traffic could appear normal during a worm attack. To reduce the noise, traffic before the inactive addressees was preferred to be used for worm detection. The detection components will pre-analyze the traffic and send initial result or alarms to the control center mentioned in Figure2. Detecting components:The detection components can be implemented on virtual machines or the gateway of local network. Detection components can also be traffic analyzers beside the routers, observing the traffic of a set of addresses. Problems such as where the monitors should be deployed. Address space selection:The number of addresses the system can manage is limited. The worms might use different target spaces. To make packet collection efficient and effective. We need to deploy the detection components. To collect inactive address, IP address blocks that are not assigned or known to be inactive for applications.

4.1 Victim number based algorithm

The algorithm is used to detect the worm spreading through the network. The addresses from the address which is not active it is called victims. If the detection system can trace the number of victims, then the detection system has a good performance. The mall number of packets is not enough to detect [6].

4.2 Victim decision rules

Minimum one packet is received by an inactive host. This is the simplest decision rule. The number of victims is find out by the detection system. It is called one scan decision rule(OSDR). The OSDR can be calculated by using this equation:

$$V_k = \sum_{i=0}^{k} [n_i - n_{i-1}][1 - (1 - D/T)^{(k-i)s}]$$

Where Vk is the number of victims detected by the system up to time tick k. D is the detection network size. The another method is two can decision rule(TSDR). Two scans captured by the host leads to a victims. It is reduces effects by scans or software errors. The number of victims detected by a detection system using TSDR up to time tick k can be calculated by using this equation:

ISSN 2394-187(Online)
ISSN 2394-7179 (Print)

$$V_k = \sum_{i=0}^{k} [n_i - n_{i-1}][1 - \rho^{(k-i)s} - \rho^{(k-i)s-1}(1-\rho)(k-i)s]$$

Where the number of infected host up to time tick i is ni and p=(1-p/t). path rate to be zero and n-1=0. ni-ni-1,is the number of newly infected machines detected at the end of time tick is the sum of machines detected at the end of time tick k is the total number of machines detected at every time tick k is the sum of machines detected at every time tick i before k.

$$\rho^{(k-i)s-1}(1-\rho)(k-i)$$

Denotes the fraction of victims infected during time tick i but only one scan packets has been detected by time tick k.The victim number based algorithm scan all packets with inactive destination address are gathered. The victims are retrieved from the gathered addresses. Inactive address attack is detected. the detection is faster using the method. We test the solution with real traffic traces obtained from worm incident in order to evaluate the detection method. the traffic traces are gathered from the gateways.Scan all packets with inactive destination addresses are gathered. Ti is completed by detection architecture.

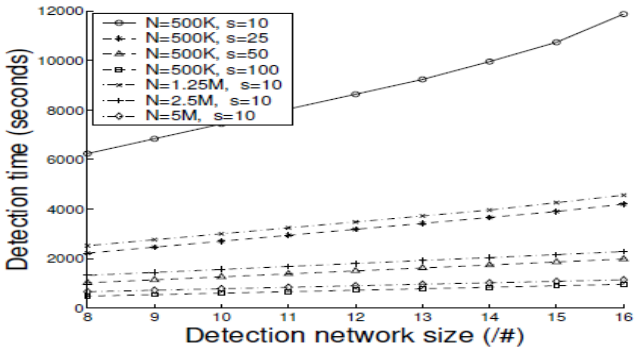

Fig.3: Network Size Detection

The victims are retrieved from the gathered addresses. Adaptive threshold was need to determine when a surge is enough large. During the monitoring of block of inactive addresses, if there is a fast surge in the total number of distinct victims. It is using only inactive addresses. This method requires simple filtering rules to gather suspicious packets and count them. The victim number based algorithm should be reflect it. We need to test the solution with real traffic traces obtained from worm incidents in order to validate the detection method. the traffic traces are gathered from the gateways. Stimulate the number of worm victims detected by a /16 network over time mentioned in Figure 3. Then find that for the case of random scan and routable scan. Finally it completes the detection of the worm by using the victims(number of inactive addresses)

5. Conclusion

Here we used the victim number based algorithm to detect the worms. The worms are detected by using the victim in the way of number of inactive address. The one scan decision and two scan decision rule is the best way to find the worms. Because it is very faster to scan the inactive addressed present in the network. The one scan decision rule is very slow for comparing the two scan decision rule.

6. Future work

The traffic monitoring will be found out the intrusion detection system in future. A consequence of the worm detection method is that the hackers will have to use a limited number of IP addresses to scan the Internet. Therefore, the truth of worm scanning on the Internet traffic will be reduced.

References

[1] U. Murugavel and Dr. Shanthi, "Survey on Ethical Hacking Process in Network Security", Vol.3, July 2014, pp.76-81.
[2] IdimadakalaNagaraju, "Ethics in Ethical Hacking", Vol.4, October 2013, pp.876-881.
[3] D. Moore, The Spread of the Code-Red Worm(CRV2), http// www.caida.org/analysis/secu-rity/code-red/coderedv2/analysis.xml.
[4] D. Moore, "Code-Red: A Case Study on the Spread and Victims of an Internet Worm", http://www.icir.org/vern/imw-2002/imw2002-papers/209.ps.gz.
[5] Internet Protocol v4 Address Space, http://www.iana.org/ assigments/ ipv4-address-space.

R. Edward Andrewsis holding a under graduation degree B.Sc Computer Science from Sri Muthukumaran college of arts & science and pursuing post graduation in Master of computer applications from S.A.Engineering college. This paper is a part of curriculum covered under in (MC7413) Technical Seminar and Report Writing.

S. Sridhar, is a Head of Computer Applications, at S.A. Engineering College, Chennai. He has published many articles in the National and International Journals of Computer Science and presented papers in many Conferences