Proceedings of
INTERNATIONAL CONFERENCE ON COMPUTING, COMMUNICATION AND ENERGY SYSTEMS
(ICCCES-16)
In Association with IET, UK & Sponsored by TEQIP-II
29th-30th, Jan. 2016

Paper ID: CSEIT01

ATTACK GRAPH ANALYSIS USING -NS2

Miss: Vijaya Desai
M.E.CN (IInd), KJCOE Pisoli, PUNE
Mrs: Jyoti Nighot
Asst.Professor, KJCOE Pisoli, PUNE

Abstract— we describe large network environment needs multiple sensors to monitor network traffic. Deploying and managing sensors in network's demanding task. Attack graph showing all possible paths. This paper investigate how the IDS sensors are placed using attack graph analysis with some evaluation criteria using MOGA with NS2.

Index Terms—Attack graph, IDS, MOGA, Sensor.

I. INTRODUCTION

Attack graphs represent a series of possible paths taken by potential intruders to attack a given asset. [1] Such graphs are constructed in a topological fashion taking into account both vulnerable services that allow nodes to be exploited and used as launch pads, and protective measures deployed to restrict connectivity. The purpose is to enumerate all paths leading to given assets and where optimal placement is devised to monitor all paths using minimal number of sensors. This is seen as a set cover problem: each node allows for monitoring of certain graph edges and the challenge is to find a minimum set of routers that cover all edges in the graph; a greedy algorithm is then used to compute optimal placement. The use of attack graphs provides an efficient mapping of network vulnerabilities in the network. A vulnerability-driven approach to deploying sensors overlooks factors such as traffic load however.[1] As a result the placement is optimized such that the more paths that go through a node the more likely it is chosen for placement.

II. RELATED WORK

A. Attack Graph

Noel and Jajodia [2] propose to use attack graph analysis to find out optimal placement of IDS sensors. Attack graphs represent a series of possible paths taken by potential intruders to attack a given asset. Such graphs are constructed in a topological fashion taking into account both vulnerable services that allow nodes to be exploited and used as launch pads, and protective measures deployed to restrict connectivity. The purpose is to enumerate all paths leading to given assets and where optimal placement is devised to monitor all paths using minimal number of sensors. This is seen as a set cover problem: each node allows for monitoring of certain graph edges and the challenge is to find a minimum set of routers that cover all edges in the graph; a greedy algorithm is then Used to compute optimal placement. The use of attack graphs provides an efficient mapping of network vulnerabilities in the network. A vulnerability-driven approach to deploying sensors overlooks factors such as traffic load however. As a result the placement is optimized such that the more paths that go through a node the more likely it is chosen for placement.

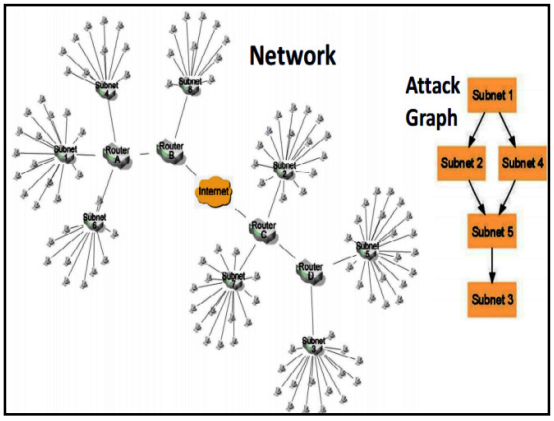

Fig: Attack Graph Diagram

There are 8 subnets, with various hosts in each subnet and routers providing connectivity between them. By the definition of attack graph leading to compromise of given critical assets, vulnerabilities can be ignored. We use network topology for placing sensor to cover all possible paths. To minimize costs, to cover all critical paths using least number of sensors.

B. *Network Security*

Network security affects many organizations, whether they are large, small, or government organizations. If network security is breached an intruder can do all sorts of harm. That is why people need to be aware of and to be educated about network security and how to secure their computer and network. Systems are required to be updated regularly as new security flaws are discovered. Without being up to date, it makes it easy for a *hacker* to gain unauthorized access to the system.There are two main types of attacks whose aim is to compromise the security of a network.

I. Passive attack
II. Active attack.

I. Passive Attack

A passive attack can be split into two types. The first type of passive attack is to simply monitor the transmission between two parties and to capture information that is sent and received. The attacker does not intend to interrupt the service, or cause an effect, but to only read the information. The second type of attack is a traffic analysis. If information is encrypted, it will be more difficult to read the information being sent and received, but the attacker simply observers the information, and tries to make sense out of it; or to simply determine the identity and location of the two communicating parties. A passive attack is usually harder to detect as there is little impact to the information communicated

II. ACTIVE ATTACK

On the other hand, an active attack aim is to cause disruption, and it is usually easily recognized. Unlike a passive attack, an active attack modifies information or interrupts a service. There are four types of an active attack:

- Masquerade – To pretend to be someone else. This could be logging in with a different user account to gain extra privileges. For example, a user of a system steals the System Administrators username and password to be able to pretend that they are them.

- Reply – To capture information to send it, or a copy it elsewhere.
- Modification – To alter the information being sent or received.
- Denial of service – To cause a disruption to the network

C. Common Attack Methods

Common internet attacks methods are broken down into categories. Some attacks gain system knowledge or personal information, such as eavesdropping and phishing.[4] Attacks can also interfere with the system's intended function, such as viruses, worms and Trojans. The other form of attack is when the system's resources are consumes uselessly, these can be caused by denial of service (DoS) attack.[10] Other forms of network intrusions also exist, such as land attacks, teardrop attacks. These attacks are not as well known as DoS attacks, but they are used in some form or another even if they aren't mentioned by name.

D. Simulation

I.IDS PASSIVE SECURITY SOLUTION

An intrusion detection system (IDS) is designed to monitor all inbound and outbound network activity and suspicious patterns that may indicate network or system attack from someone attempting to break into or compromise a system.[11] IDS is considered to be a passive-monitoring system, since the main function of an IDS product is to warn you of suspicious activity taking place – not prevent theme essentially reviews your network traffic and data and will identify probes, attacks, exploits and other vulnerabilities. IDSs can respond to the suspicious event in one of several ways, which includes displaying an alert, logging the event or even paging an administrator. In some cases the IDS may be prompted to reconfigure the network to reduce the effects of the suspicious intrusion.

An IDS specifically looks for suspicious activity and events that might be the result of a virus, worm or hacker. This is done by looking for known intrusion signatures or attack signatures that characterize different worms or viruses and by tracking general variances which differ from regular system activity. The IDS is able to provide notification of only known attacks.

II.IPS ACTIVE SECURITY SOLUTION

IPS or intrusion prevention system, is definitely the next level of security technology with its capability to provide security at all system levels from the operating system kernel to network data packets. [11]It provides policies and rules for network traffic along with IDS for alerting system or network administrators to suspicious traffic, but allows the administrator to provide the action upon being alerted. Where IDS informs of a potential attack, an IPS makes attempts to stop it. Another huge leap over IDS, is that IPS has the capability of being able to prevent known intrusion signatures, but also some unknown attacks due to its database of generic attack behaviors. Thought of as a combination of IDS and an application layer firewall for protection, IPS is generally considered to be the "next generation" of IDS.

I. NETWORK SIMULATOR (NS-2)

Network simulator is software which predict behavior of network. NS is name of Discrete Event Simulators, specifically ns-1, ns-2 and ns-3.We use Network Simulator NS2 [2] to simulate our experimental network as shown in Figure 1. The whole network consists of 180 nodes, where node 0 represents the outside world, nodes 1 to 19 are the routers interconnecting various parts of the network, nodes 20 to 39 are servers offering valuable services to users and therefore critical assets that need to be protected, and nodes 40 to 180 are ordinary clients some of which may be compromised by intruders to attack critical assets. The network is organized as such that the servers are distributed over six subnets and the clients are distributed over seven separate subnets. We simulate real intrusive behavior to analyze how such behaviors could be efficiently detected by the proposed approach. The intrusive behavior we simulated is to do with probing and information gathering, the purpose of which is to assess a potential target's weaknesses and vulnerabilities [8]. For example, an intruder may strive to detect active hosts and networks that are reachable and the services they are running that could be successfully exploited. Detecting and preventing such probes therefore is important both to inhibit exposure of information and prevent attacks that follow.

We simulate a probe attack scenario where various servers are probed from the outside (through node 0) and inside from clients, hence the simulation consists of both external and internal attacks. An intruder may subvert a node in any of the client subnets to probe any of the servers. Intruders (picked randomly) from each of the client subnets, that are client nodes 45, 78, 95, 111, 133, 157 and 178, probe server nodes 20 to 38. In addition, node 45 also attempts a probe on neighbors 46 and 47. A total number of 154 instances of probe attack are injected.

III. EXPERIMENTAL SETUP

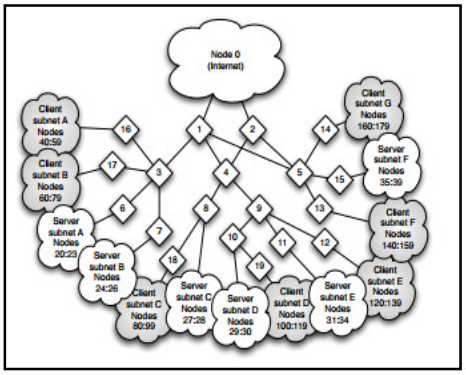

Fig.1.Experimental Network

We implemented a typical network including 15 routers and 800 network nodes, in the NS2 simulation system. In the network, 750 network nodes are reflectors and 50 are legitimate clients.

IV. SIMULATION AND RESULT

We are constructing attack graphs for sensor placement [14].Attack graphs predict the various possible ways of penetrating a network to reach critical assets. We then place IDS sensor to cover all these paths, using the fewest numbers of sensor. We characterize expected monitoring costs for the network. We restrict the costs to a range of values 1 to 10 to express relative monitoring costs for different locations on a network. Router nodes 1 and 2 are assigned a cost of 8,router nodes 3,4,5 and 9 are assigned cost of 7,router nodes 8 and 10 are assigned cost of 6,router nodes 6,11,15 are assigned cost of 5.We assign a flat cost of 4 for all the other subnet router nodes. We are designed different. tcl script through NS2 simulator (For here showing v3.tcl,v4.tcl,v5.tcl,normal1.tcl).For attack Simulation Denial of Service(DOS) attack(eg.Normal1.tcl) is simulated for attack penetration. For probing of attack Worm attack (eg.Worm.tcl) is simulated.

A. Attack Graphs

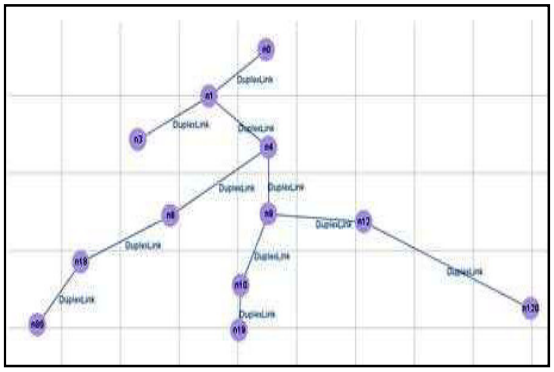

Fig: V5.tcl Attacker Node80client On Server Node120

B.

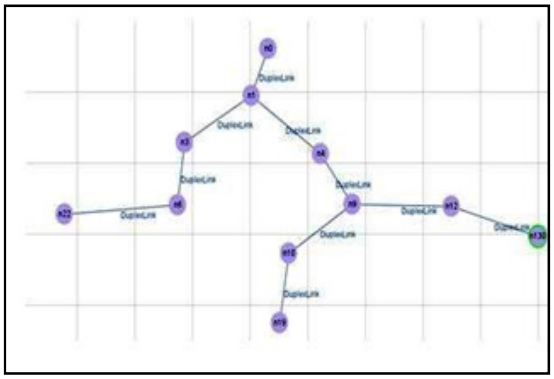

Fig: V3.tcl Attacker Node 130client On Sever Node22

V. CONCLUSION

We focus on critical paths though network that lead to compromise critical assets this analysis support optimal placement of IDS sensors, and effective attack response. By analyzing network traffic, and potential attacker exploit, we predict all possible paths to reach critical assets. We then place IDS sensor to cover all attack paths with minimum number of sensors with minimum cost.

Example	No of sensor	Detection rate	Placement option	Monitoring cost	Energy consumed
V3.tcl	4	88.98%	NODES 1,3,12,19	23	300
V4.tcl	4	91%	NODES 3,8,9,15	25	400
V5.tcl	5	94%	NODES 1,3,12,18,19	27	520
Worm11.tcl	-	76%	-	-	510
Normal1.tcl	-	72%	-	-	510

REFERENCES

[1]Optimising IDS Sensor Placement-Hao Chen, John A. Clark, Siraj A. Shaikh, Howard Chivers, Philip Nobles,

[2]S. Noel and S. Jajodia, "Attack graphs for sensor placement, alert prioritization, and attack response," in Cyberspace Research Workshop, 2007.

[3] L. Zhang, S. Yu, D. Wu, P. Watters, "A survey on latest bottleneck attack and defence," in Proc. 2011 IEEE Conf. on Trust, Security and Privacy in Computing and Communications, pp. 53–60.

[4]V. Paxson , "An analysis of using reflectors for distributed denial-of service attacks," ACM Computer Communication Rev., vol. 31, no. 3, pp. 38–47, 2001.

[5]P. Ferguson and D. Senie, "Network ingress filtering: defeating denial of service attacks which employ IP source addressspoofing."Available: http://www.ietf.org/rfc/rfc2827.txt.

[6] Stateful Inspection Technology (the industry standard for enterprise class network security solutions) Available:http://www.checkpoint.com/products/downloads/Stateful Inspection.pdf

[7] G. V. Rooij, "Real stateful TCP packet filtering in IP filter," in Proc. 2001 USENIX Security Symposium.

[8]T. Vogt, "Application-level reflection attacks." Available:http://www.lemuria.org/security/application-drdos.html

[9] G. E. P. Box, G. M. Jenkins, and G. C. Reinsel, Time Series Analysis: Forecasting and Control, 3rd edition. Prentice Hall, 1994

[10] Parallel Ranking Assist against Distributed Reflection Denial of Service Attack Sumitha.J.S1, D.Devibala2 International Journal of Application or Innovation in Engineering & Management (IJAIEM) Web Site: www.ijaiem.org Email: editor@ijaiem.org Volume 3, Issue 3, March 2014 ISSN 2319 – 4847.

[11]Intrusion Detection (IDS) and **Prevention (IPS) Systems** By Vangie Beal.__Posted July 15, 2005 http://www.webopedia.com/DidYouKnow/Computer_Science/intrusion_detection_prevention.asp