SEMINAR AND TECHNICAL COMMUNICATION
Review 1

Topic: Effective algorithm to detect stepping stone intrusion by removing packet outliers of packet RTTs

NAME: Atharv Rajkumar Nalwade
Roll No: TC146
Class: TE-1

Research guide:
Prof. Shubadha Mone

CONTENTS:

- Introduction
- Motivation
- Problem Statement
- Scope
- Literature Survey
- Software/Hardware Requirements
- References

Introduction

A network intrusion is an unauthorized penetration of a computer in your enterprise or an address in your assigned domain. It can be active or passive. Some intrusions are simply meant to let you know the intruder was there, defacing your Web site with various kinds of messages or crude images. Others are more malicious, seeking to extract critical information on either a one-time basis or as an ongoing parasitic relationship that will continue to siphon off data until it’s discovered. Attackers on the Internet often launch network intrusions through compromised hosts, called stepping-stones, in order to reduce the chance of being detected. In a stepping-stone attack, an intruder uses a chain of hosts on the Internet as relay machines and remotely log in these hosts using tools such as telnet, rlogin, or SSH. A benefit of using stepping-stones to launch attacks is that intruders can be hidden by a long interactive session and knowing the actual origin of the attack is hard to determine

Motivation

In the 21st century where we are surrounded with an invisible web of internet care should be taken that one does not access your any sorts of private data without your authorization that's where the concept of security clears its picture in the field of computer networks. Any illicit behaviour on a digital network is known as a network intrusion. Any of the following can be considered an intrusion –

- Malware, sometimes known as ransomware, is a type of computer virus.
- Attempts to obtain unauthorized access to a system
- DDOS (Distributed Denial of Service) attacks
- Destruction of cyber-enabled equipment
- Employee security breaches that are unintentional (like moving a secure file into a shared folder)
- Untrustworthy users, both within and external to your company
- Phishing campaigns and other methods of deceiving consumers with ostensibly genuine communication are examples of social engineering assaults.

One such intrusion is stepping stone intrusion where the attacker uses a long chain of compromised hosts to gain access to a remote host which can be prevented effectively up to 85% using the algorithm described in the paper.

Problem Statement

To detect steeping-stone intrusion in a computer networks system using a effective algorithms by removing outliers of packet RTT.

Scope

The algorithms suggested by the author in the research paper titled “Effective Algorithms to Detect Stepping-Stone Intrusion by Removing Outliers of Packet RTTs” by Lixin Wang, Jianhua Yang, Michael Workman, and Pengjun Wan propose an efficient way to eliminate most of the possible RTT outliers of the packets captured in the Internet environment. Then an efficient SSI detection algorithmis used by mining network traffic using an improved version of k-Means clustering. The proposed detection algorithm for SSI is accurate, effective, and efficient in the context of the Internet. Effective rate of our proposed SSI detection algorithm is higher than 85.7% in the context of the Internet.

Literature Survey

Effective Algorithms to Detect Stepping-Stone Intrusion by Removing Outliers of Packet RTTs by Lixin Wang , Jianhua Yang, Michael Workman, and Pengjun Wan

- An effective method to detect stepping-stone intrusion (SSI) is to estimate the length of a connection chain. This type of detection method is referred to as a network-based detection approach. Existing network-based SSI detection methods are either ineffective in the context of the Internet because of the presence of outliers in the packet round-trip times (RTTs) or inefficient, as many packets must be captured and processed. Because of the high fluctuation caused by the intermediate routers on the Internet
- Advantages:The result of the algorithms makes most of the known network-based detection methods for SSI ineffective in the Internet environment
- Disadvantages: During conduction of the experiment in real time it was found that the RTT dataset collected from the connection chain of length two achieves the smallest standard derivation on six of the seven datasets that were captured (only the output generated on on of the dataset is incorrect)

Matching TCP/IP Packets to Detect Stepping-Stone Intrusion

- Author suggest using the technique of matching the TCP/IP Protocols using a Step-Function method, to detect network attackers from using a long connection chain to hide their identities when they launch attacks. The objective of the method is to estimate the length of a connection chain based on the changes in packet round trip times. The key point to compute the roundtrip time of a connection chain is to match a Send and its corresponding Echo packet
- ADVANTAGES:

(i) The ability to detect intruders in real-time,

(ii) The ability to handle encrypted terminal sessions,

(iii) The ability to estimate the length of a chain accurately, and

(iv) The ability to tolerate network traffic fluctuation, network load, and workload of chained hosts.

- DISADVANTAGES

1. We must be able to monitor a packet throughout a connection session in order for this approach to work
2. If the fluctuation of a connection is higher than the additional time to connect to the next host, we will need a better approach to detect the additional host.

Mining Network Traffic with the k-Means Clustering Algorithm for Stepping-Stone Intrusion Detection

- In the research paper “Mining Network Traffic with the k-Means Clustering Algorithm for Stepping-Stone Intrusion Detection” by Lixin Wang, Jianhua Yang, Xiaohua Xu, and Peng-Jun author suggest using k-means clustering algorithm which can accurately determine the length of a connection chain without requiring a large number of TCP packets being captured and processed, so it is more efficient.
  This algorithm is also easier to implement than all existing approaches for stepping-stone intrusion detection. The effectiveness, correctness, and efficiency of our proposed detection algorithm are verified through well-designed network experiments
- Advantages:

1. proposed detection algorithm using the k-means clustering can accurately determine the connection chain length
2. , the proposed algorithm does not require capturing and processing a large number of TCP packets. Therefore, our proposed detection algorithm for SSI is efficient
3. Easy to implement

- Disadvantage

1. the detection methods based on the k-means clustering require that there should be as less outlier values of round-trip times as possible. Therefore, additional algorithms are needed to remove these outlier values of round-trip times from the input file of the detection algorithm

Detecting Stepping Stones

- We develop an efficient algorithm for detecting stepping stones by monitoring a site's Internet access link. The algorithm is based on the distinctive characteristics (packet size, timing) of interactive traffic, and not on connection contents, and hence can be used to find stepping stones even when the traffic is encrypted.
- Advantages:

1. The algorithm runs on a site's Internet access link. It proves highly accurate, and has the major advantage of ignoring the data contents of the connections, which means both that it works for encrypted traffic such as SSH, and that the packet capture load is greatly diminished since the packet filter need only record packet headers.

- DISADVANTAGES

1. Algorithm fails when there is the large number of legitimate stepping stones that users routinely traverse for a variety of reasons
2. It was found that the timing-based algorithm missed a stepping stone simply because the connections were exceedingly short

Stepping Stone Detection for Tracing Attack Sources in Software-Defined Networks

- study aims to adapt some of the existing stepping stone detection and antievasion techniques to software-defined networks which use network function virtualization. We have implemented the stepping-stone detection techniques in a simulated environment and use sFlow for the traffic monitoring at the switches. We evaluate the detection algorithms on different network topologies and analyze the results to gain insight on the effectiveness of the detection mechanisms
- ADVANTAGES

1. Applicable to non-interactive network traffic
2. Effective detection of anomaly due to chaf

- DISADVANTAGES

1. Lack of incorporation of specifics of SDN and NFV environment
2. Limited scalability of the solution
3. Use of data store leads to lot of disk accesses
4. Continuous bandwidth consumption