Attacker use cmd line tool sor ssh to gain acces

Transmission control protocol allow to coom over internet

With host-based SSI detection, the outgoing connections are compared with the incoming connections of the same machine, and then the packets are analyzed to check whether a relayed pair in the outgoing and incoming connections can be found.

approach is that it only focuses on a single host, and thus can easily introduce high false-positive errors because it is well-known that stepping-stones are actually used to access remote servers by some legal applications. Client browsers and Web servers are typical examples of this type of application to access remote serversapproach is that it only focuses on a single host, and thus can easily introduce high false-positive errors because it is well-known that stepping-stones are actually used to access remote servers by some legal applications. Client browsers and Web servers are typical examples of this type of application to access remote servers

The key idea of this type of detection method is to estimate the number of connections from the intruder’s host to the target host (as shown in Fig. 1), which is referred to as the length of a (whole) connection chain. If a connection chain contains three or more connections, then the user attempts to gain access to a remote target host via three or most stepping-stones. The more hosts involved in an interactive session to access a remote server, the slower the data communication process. Legal applications are well-known for never using three or more intermediate hosts to access a remote server. Therefore, if a target host is accessed via three or more stepping-stones from another host, then the possibility that the session is manipulated by a malicious hacker and the target system is under attacks is very high.

Rtt it takes for network request to go from starting pt to desti and back to starting pt

Used by network admin ro determine health and speed of network

Kmeans computes centroid and iterates to find optimal centroid

The first proposed detection algorithm via a network-based approach was presented in Ref. [16] by Yung in 2002. The key idea used in Ref. [16] was to calculate the RTT of a Send packet and try to match this Send with its corresponding ACKnowledgement (ACK) packet transmitted from the next adjacent host in the connection chain. The algorithm in Ref. [16] slightly reduced the false-positive errors. However, this algorithm for SSI detection generates high false-negative errors due to the use of the ACK packet from the next adjacent host, and the actual Echo packet is not used and analyzed

a step-function detection method was proposed to estimate the length of a connection chain in Ref. [17] by Yang and Huang in 2004. Unlike the detection method developed in Ref. [16], the stepfunction approach developed in Ref. [17] reduced the false-positive and false-negative errors in the context of a local area network (LAN). The connection chain was properly established in Ref. [17] so that the corresponding Echo packet of a Send packet can be captured and analyzed. In Ref. [17], the step-function approach is used to calculate the packet RTTs by matching a Send packet with its corresponding Echo packet. The drawback of the detection method proposed in Ref. [17] is that it only works well in LANs

To the best of our knowledge, the clustering and partitioning data mining approach presented in Ref. [19] by Yang and Huang is one of the best-existing connection-chain-based SSI detection approaches. In Ref. [19], the packet RTTs are calculated using the maximum-minimum distance (MMD) clustering algorithm

We choose each new centroid to be as far as possible from existing centroids basically it will find number of points which are well spread out

On the basis of this approach, the number of clusters produced by the MMD algorithm determines the number of connections in the chain. Additionally, the MMD approach proposed in Ref. [19] reduced the falsepositive and false-negative errors significantly

However, this detection approach for SSI requires that many TCP packets must be captured and processed. As a result, the MMD approach proposed in Ref. [19] is inefficient in terms of packet capturing and the processing time of the detection algorithm.

This detection algorithm based on k-Means clustering does not require many packets to be captured and processed, and thus it is efficient.

Because of the high fluctuation caused by the intermediate routers on the Internet, outlier values are unavoidable in the RTTs of the captured packets

The input of this algorithm is a TXT file with two columns including packet timestamps and the packet type (either Send or Echo) obtained from the packets captured in the Internet environment. The output of this algorithm is a TXT file that contains the packet RTTs with most of the RTT outlier values removed. The key idea of this algorithm is that before an RTT value is added to the file of RTT values, we need to check whether it is a possible RTT outlier by determining whether it is tenfold larger than the current average of all the RTT values that have been added to the file. If it is, then it is likely to be an outlier RTT value

SDN is approach to networking that uses software based controllers or ap to communicate with underlying hardware and direct nw traffic

Nfv is replacement of nw appliance hw with virtual machines