Volume 2, Issue 8, August 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

An Overview on Intrusion Detection System and Types of Attacks It Can Detect Considering Different Protocols

Amrita Anand*
Department of Computer Science, M.E (4th sem)
S.R.I.T, Jabalpur, R.G.P.V University, *India*

Brajesh Patel
Department of Computer Science, HOD (M.E),
S.R.I.T, Jabalpur, R.G.P.V University, *India*

ABSTRACT: **Intrusion Detection System (IDS) has been used as a vital instrument in defending the network from this malicious or abnormal activity. it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks With the ability to analyze network traffic and recognize incoming and ongoing network attack, majority of network administrator has turn to IDS to help them in detecting anomalies in network traffic In this paper, we focus on different types of attacks on IDS this paper gives a description of different attack on different protocol such as TCP ,UDP,ARP and ICMP.**

Keywords- Attack, DoS, Intrusion detection , NIDS, Protocols.

I. INTRODUCTION

Intrusion detection systems (IDSs) are usually deployed along with other preventive security mechanisms, such as access control and authentication, as a second line of defense that protects information systems. There are several reasons that make intrusion detection a necessary part of the entire defense system. First, many traditional systems and applications were developed without security in mind. In other cases, systems and applications were developed to work in a different environment and may become vulnerable when deployed Intrusion detection complements these protective mechanisms to improve the system security. Moreover, even if the preventive security mechanisms can protect information systems successfully, it is still desirable to know what intrusions have happened or are happening, so that we can understand the security threats and risks and thus be better prepared for future attacks.

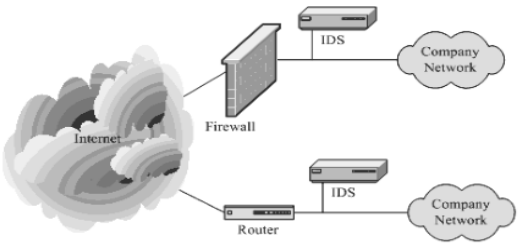

Fig 1:- IDS

The attack can be launched in term of fast attack or slow attack. Fast attack can be defined as an attack that uses a large amount of packet or connection within a few second [1]. Meanwhile, slow attack can be defined as an attack that takes a few minutes or a few hours to complete [1] . Both of the attack gives a great impact to the network environment due to the security breach decade. As in Fig:-1, Currently IDS is used as one of the defensive tools in strengthens the network security especially in detecting the first two phases of an attack either in form slow or fast attack An intrusion detection system can be divided into two approaches which are behavior based (anomaly) and knowledge based (misuse) [2], [3]. The behavior based approach is also known as anomaly based system while knowledge based approach is known as misuse based system [4], [5].The misuse or signature based IDS is a system which contains a number of attack description or signature that are matched against a stream of audit data looking for evidence of modeled attack [6]. The audit data can be gathered from network traffic or an application log. This method can be used to detect previous known attack and the profile of the attacker has to be manually revised when new attack types are discovered. Hence, unknown attacks in network intrusion pattern and characteristic might not be capture using this technique [8].Meanwhile, the anomaly based system identifies the intrusion by identifying traffic or application which is presumed to be normal activity on the network or host . The anomaly based system builds a model of the normal behavior of the system and then looks for anomalous activity such as activities that do not confirm to the established model. Anything that does not correspond to the system profile is flagged as intrusive. False alarms generated by both systems are major concern and it is identified as a key issues and the cause of delay to further implementation of reactive intrusion detection system [9].

Therefore, it is important to reduce the false alarm generated by both of the system . Although false alarm is a major concern in developing the intrusion detection system especially the anomaly based intrusion detection system, yet the system has fully met the organizations' objective compared to the signature based system [10]. The false positive generated by the anomaly based system is still tolerable even though expected behavior is identified as anomalous while false negative is intolerable because they allow attack to go undetected An attack that uses a large amount of packet or connection within a few second scanning attack, DOS attack , DDOS attack worm attack are some of fast attack Code Red Worm and NIMDA worm are another breed of DoS attacks on Internet infrastructure after the Morris Worm. Code Red Worm has a fast rate of propagation and infection via network scanning to detect and automatically exploit

II. ATTACK TYPES

A. Scanning Attack

Scanning attacks can be used to assimilate information about the system being attacked. Using scanning techniques, the attacker can gain topology information, types of network traffic allowed through a firewall, active hosts on a network, OS and kernel of hosts on a network, server software running, version numbers of software, etc... Using this information, the attacker may launch attacks aimed at more specific exploits. The above was gathered by launching a stealth SYN scan. This scan is called stealth because it never actually completes TCP connections. This technique is often referred to as half open scanning, because the attacker does not open a full TCP connection. The attacker sends a SYN packet, as though you he were opening up a real TCP connection. If the attacker receives a SYN/ACK, this indicates the port is listening. If no response is received, the attacker may assume that the port is
closed

B. Denial of Service Attack

There are two main types of denial of service (DoS) attacks: flooding and flaw exploitations. Flooding attacks can often simply implement. For example, one can launch a DoS attack by just using the ping command. This will result in sending the victim an overwhelming number of ping packets. If the attacker has access to greater bandwidth than the victim, this will easily and quickly overwhelm the victim. As another example, a SYN flood attack sends a flood of TCP/SYN packets with a forged source address to a victim. This will cause the victim to open half open TCP connections - the victim will send a TCPSYN/ACK packet and wait for an ACK in response. Since the ACK never comes, the victim eventually will exhaust available resources waiting for ACKs from a nonexistent host.

C. Penetration Attack

Penetration attacks contain all attacks which give the unauthorized attacker the ability to gain access to system resources, privileges, or data. One common way for this to happen is by exploiting a software flaw. This attack would be considered a penetration attack. Being able to arbitrarily execute code as root easily gives an attacker to whatever system resource imaginable. In addition, this could allow the user to launch other types of attack on this system, or even attack other systems from the compromised system.

III. DIFFERENT PROTOCOL ATTACKS

A. ICMP

ICMP is used by the IP layer to send one-way informational messages to a host[12]. There is no authentication in ICMP which leads to attacks using ICMP that can result in a denial of service, or allowing the attacker to intercept packets. There are a few types of attacks that are associated with ICMP shown as follows:

ICMP DOS Attack: Attacker could use either the ICMP "Time exceeded" or "Destination unreachable" messages. Both of these ICMP messages can cause a host to immediately drop a connection. An attacker can make use of this by simply forging one of these ICMP messages, and sending it to one or both of the communicating hosts. Their connection will then be broken. The ICMP redirect message is commonly used by gateways when a host has mistakenly assumed the destination is not on the local network. If an attacker forges an ICMP "Redirect" message, it can cause another host to send packets for certain connections through the attacker's host.

Ping of death: An attacker sends an ICMP echo request packet that's larger than the maximum IP packet size. Since the received ICMP echo request packet is larger than the normal IP packet size, it's fragmented. The target can't reassemble the packets, so the OS crashes or reboots.

ICMP nuke attack**:** Nukes send a packet of information that the target OS can't handle, which causes the system to crash.
ICMP PING flood attack: A broadcast storm of pings overwhelms the target system so it can't respond to legitimate traffic

B. TCP

If one application wants to communicate with another via TCP, it sends a communication request. This request must be sent to an exact address. After a handshake between the two applications, TCP will set up a full-duplex communication between the two applications. The full-duplex communication will occupy the communication line between the two computers until it is closed by one of the two applications. There are security problem in tcp[11], some attack are describe below

TCP SYN or TCP ACK Flood Attack - This attack is very common. The purpose of this attack is to deny service. The attack begins as a normal TCP connection: the client and the server exchange information in TCP packets. The TCP client continues to send ACK packets to the server, these ACK packets tells the server that a connection is requested. The server thus responds to the client with a ACK packet, the client is supposed to respond with another packet accepting the connection to establish the session. In this attack the clients continually send and receive the ACK packets but it does not open the session. The server holds these sessions open, awaiting the final packet in the sequence. This cause the server to fill up the available connections and denies any requesting clients access.

TCP Sequence Number Attack - This is when the attacker takes control of one end of a TCP session. The goal of this attack is to kick the attacked end of the network for the duration of the session. Only then will the attack be successful. Each time a TCP message is sent the client or the server generates a sequence number. The attacker intercepts and then responds with a sequence number similar to the one used in the original session. This attack can then hijack or disrupt a session. If a valid sequence number is guessed the attacker can place himself between the client and the server. The attacker gains the connection and the data from the legitimate system

TCP Hijacking - This is also called active sniffing, it involves the attacker gaining access to a host in the network and logically disconnecting it from the network. The attacker then inserts another machine with the same IP address. This happens quickly and gives the attacker access to the session and to all the information on the original system.

TCP reset attack: This is also known as "forged TCP resets", "spoofed TCP reset packets" or "TCP reset attacks". These terms refer to a method of tampering with Internet communications.

C. ARP

ARP maps any network level address (such as IP Address to its corresponding data link address. Some ARP attack are given below

ARP flooding

Processing ARP packets consumes system resources. Generally, the size of an ARP table is restricted to guarantee sufficient system memory and searching efficiency. An attacker may send a large number of forged ARP packets with various sender IP addresses to cause an overflow of the ARP table on the victim. Then the victim cannot add valid ARP entries and thus fails to communicate .An attacker may also send a large number of packets with irresolvable destination IP addresses. When the victim keeps trying to resolve the destination IP addresses to forward packets, its CPU will be exhausted.

User spoofing: An attacker may send a forged ARP packet containing a false IP-to-MAC address binding to a gateway or a host. The forged ARP packet sent from Host A deceives the gateway into adding a false IP-to-MAC address binding of Host B. After that, normal communications between the gateway and Host B are interrupting.

In DoS attack target hosts are denied from communicating with each other, or with the Internet. This is done simply by corrupting their ARP caches with fake entries including nonexistent MAC addresses, or by disabling the IP packet routing option in the malicious host, so that received redirected traffic will not be forwarded to its real destination.

Connection Hijacking and Interception

Packet interception is the act in which client can be victimized into getting their connection manipulated in a way that it is possible to take complete control aver

D. UDP

UDP uses a simple transmission model without implicit handshaking dialogues for providing reliability, ordering, or data integrity. Thus, UDP provides an unreliable service and datagram may arrive out of order, appear duplicated, or go missing without notice. UDP assumes that error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level.[13].some UDP attacks are describe below

UDP flood attack**:** Similar to ICMP flood attack, UDP flood attack sends a large number of UDP messages to the target in a short time, so that the target gets too busy to transmit the normal network data packets.

Fraggle - A fraggle attack is similar to a smurfing attack with the exception that the User Datagram Protocol (UDP) is used instead of ICMP.

Teardrop - A teardrop type of DoS attack The attack works by sending messages fragmented into multiple UDP packages. Ordinarily the operating system is able to reassemble the packets into a complete message by referencing data

in each UDP packet. The teardrop attack works by corrupting the offset data in the UDP packets making it impossible for the system to rebuild the original packets. On systems that are unable to handle this corruption a crash is the most likely outcome of a teardrop attack.

IV. ANALYSIS

A. Traffic Data

We used two-way traffic traces provided by the Umass Trace Repository . The traces were measured at the Umass Internet gateway router. The UMass campus is connected to the Internet through Verio, a commercial ISP, and Internet . Both of these connections are Gigabit Ethernet links. In particular, we used the "Gateway Link 3 Trace" that was measured every morning from 9:30 to 10:30 from July 16, 2004 to July 22, 2004. All of these data are manually labeled, but we did not use the labels with the proposed method.

B. Effectiveness of the Time-Periodical Packet Sampling

First, we confirmed our conjecture that the time-periodically sampled traffic would contain normal packets with higher ratio than the original traffic before sampling. For comparison, the mixing ratio of the anomalous packets to the original traffic and randomly sampled traffic of which the sampling rate per packet is *p*. The mixing ratio of anomaly packets to the time-based sampled traffic is much smaller than that to the original traffic before sampling, whereas the mixing ratio of anomaly packets to the randomly sampled traffic is almost identical to that to the original traffic before sampling. This result indicates that the time-periodical packet sampling is useful for extracting normal packets from the unlabeled original traffic which may include anomalous traffic. However, we have to remember that the time-periodically sampled traffic might be biased towards a specific aspect of normal traffic. Therefore, we investigated the performance of baseline distributions that were trained with time-periodically sampled traffic data. e numbers of normal behaviors incorrectly identified as anomalies (FP: False Positive) and missed anomalies (FN: False Negative) regarding TCP SYN packets for the baseline distributions trained with different types of traffic data, i.e., normal traffic data, original traffic data before sampling, 10 sets of time-periodically sampled traffic data, and 10 sets of randomly sampled traffic data

C. Effectiveness of Ensemble Anomaly Detection

This indicates that the unsupervised ensemble method can avoid the worst performance of the individual baseline distributions for the time-periodically sampled traffic. In addition, the resulting performance for the time-periodically sampled traffic is nearly identical to when the baseline distribution is trained by using the normal traffic data.
Note that the unsupervised ensemble anomaly detection is effective even when the baseline distribution is trained by using randomly sampled traffic data. However, the resulting performance for the randomly sampled traffic is nearly identical to when the baseline distribution is trained with the original traffic data. Therefore, we still cannot provide any justification for using randomly sampled traffic data to train the baseline distributions.

V. CONCLUSION and FUTURE WORK.

Before determining a network traffic is a potential threat to a network or not, there is a need for IDS to have a method in differentiating whether it is malicious or not. Therefore, this research has introduced a new methodology to identify a fast attack intrusion using time based detection. The method used to identifies anomalies based on the number of connection made in 1 second.. For further validation, the methodology will be implemented on a different set of real network traffic. In view of the fact that this research only concentrate on the TCP connection only, in the near future the researcher are planning to investigate use other protocol and other flag to recognize the fast attack intrusion activity. Inspecting other protocol and flag it may help to detect fast attack intrusion activities that launch 88using UDP or ICMP protocol. Finally the approach introduce in this research will be implemented on a production network for accessing the performance on the anomalies detection using time based detection.

References

[1] Faizal, M.A., Mohd Zaki M., Shahrin Sahib, Robiah, Y., Siti Rahayu, S., and Asrul Hadi, Y. "Time Based Intrusion Detection on Fast Attack for Network Intrusion Detection System", Second International Conference on Network Applications, Protocols and Services, IEEE, 2010.

[2] Cuppen, F. & Miege, A. (2002). Alert Correlation in a Cooperative Intrusion Detection Framewok. In Proceeding of the 2002 IEEE Symposium on Security and Privacy. IEEE, 2002]

[3]. Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.

[4] Yeophantong, T, Pakdeepinit, P., Moemeng, P & Daengdej, J. (2005).Network Traffic Classification Using Dynamic State Classifier. In Proceeding of IEEE Conference

[5] Farah J., Mantaceur Z. & Mohamed BA. (2007). A Framework for an Adaptive Intrusion Detection System using Bayesion Network. Proceeding of the Intelligence and Security Informatics, IEEE, 2007.

[6] Cabrera, J.B.D., Ravichandran, B & Mehra R.K. (2000). Statistical Traffic Modelling for Network Intrusion Detection. In Proceeding of the IEEE Conference.

[7] Wang Y., Huang GX. & Peng DG. (2006). Model of Network Intrusion Detection System Based on BP Algorithm. Proceeding of IEEE Conference on Industrial Electronics and Applications, IEEE, 2006.

[8] Sekar, R., Gupta, A., Frullo, J., Shanbhag, T., Tiwari, A., Yang, H. & Zhou, S. (2002). Spesification-based Anomaly Detection: A New Approach for Detecting Network Intrusions. In Proceeding of CCS ACM Conference.

[9] Karl Levitt. (2002). Intrusion Detection: Current Capabilities and Future Direction. Proceeding of IEEE Conference of the 18th Annual Computer Security Application, IEEE, 2002.

[10] Garuba, M., Liu, C. & Fraites, D. (2008). Intrusion Techniques: Comparative Study of Network Intrusion Detection Systems. In Proceeding of Fifth International Conference on Information Technology: New Generation, IEEE, 2008

[11] "Security Problems in the TCP/IP Pro-tocol Suite", Bellovin, S., Computer Communica-tions Review, April 1989.

[12] Postel, J. Internet Control Message Protocol, RFC 792. http:// tools.ietf.org/html/rfc0792

[13] RFC 768: User Datagram Protocol, August 1980. Available on the world-wideweb at http://www.freesoft.org/CIE/RFC/768/".

