Gulshan Kumar, International Journal of Computer Science and Mobile Applications,

Vol.2 Issue. 11, November- 2014, pg. 18-23 ISSN: 2321-8363

Intrusions in Computer Networks - A Perspective

Gulshan Kumar
Assistant Professor, Shaheed Bhagat Singh State Technical Campus, Ferozepur, Punjab, INDIA

Abstract

Nowadays, the Internet is the thing that we all want and like. Today, we are dependent on its abilities to publish, and find the information. We are using its ability to perform online shopping, and communication. Unfortunately, most of the popular softwares contain flaws and mis-configuration. These flaws fail to work with all possible conditions, especially unusual user input. Finding and patching of all software flaws is a major problem of the industry. The intruders exploit flaws in software to mount a variety of intrusions into computer networks. The intrusions affect the users in multiple ways. The protection from intrusions enforces the organizations to bear the additional costs. But, the cost involved in protection from the intrusions is often insignificant when equated with the actual cost of a successful intrusion.

In this paper, we explored various types of intrusions and categorized them based upon their behavior and method. Motive behind the intrusions are uncovered. The paper highlights the need of effective intrusion detection. The study in this paper will help the better understanding of different types of intrusions and motivation behind them. The findings of this paper provide useful insights into literature and are beneficial for those who are interested in applications and development of IDSs and related fields.

Keywords: Data Breaches, Intrusions, Intrusion detection, Intrusion detection system, Network Security, Security Threats

1. Introduction

The Internet helps to achieve resource sharing and effective communication, so its usage is increasing in our daily life day by day. Nowadays, the Internet is thing that we all want and like. In most of cases, we are dependent on its abilities like the ability to publish and find the information, the ability to perform online shopping, and the ability to communicate with others (Schneider, 2012). With the passage of time, new Internet technologies and application software are developed. The enhanced software result the networks become more and more complex. But, most of popular software contains vulnerabilities and configuration errors. The basic cause of these vulnerabilities is the software flaws. These flaws fail to work with all possible conditions, especially unusual user input. Finding and patching of all software flaws is a well-known problem of the industry. Software flaws are categorized as either known or unknown (also called zero-day) vulnerabilities. Known vulnerabilities are generally published by companies. Software updates are launched to fix the flaws. Unknown flaws of newly released software are potentially more harmful. These flaws can be easily exploited until new software patches are not launched. The malicious users can also exploit the configuration of networks, servers and clients. Network devices, such as routers and home gateways, come with a default password. Generally, these passwords are not changed in practice. Users with access to a network device can cause all traffic through it to be sent through their own servers, allowing 'man in the middle' attacks. Similarly, mis-configured servers can allow intruders to disable or modify web sites, inserting code of their own choosing. Such code is usually intended to steal data from associated databases (Schneider, 2012). Vulnerabilities in software and easy access of network resources are exploited by the intruders to misuse Internet resources and launch attacks against them (Ramamohanarao et al., 2007). The vulnerabilities in popular software and vast interconnection made possible by the Internet, however, provide the opportunity for intruders and attackers to perform malicious actions (Schneider, 2012). As a result, the number of attack incidents over the Internet is increasing day by day (Cert, 2012). In addition to these factors, availability of free attack software tools over the Internet made these attacks more simple and easy. So, it is becoming more and more difficult for conventional intrusion detection techniques to detect complex attacks efficiently. Efficient detection of attacks or intrusions requires more intelligent and effective techniques (Gupta, 2009). The protection from intrusions enforces the organizations to bear additional costs. But, cost involved in protecting from intrusions is often insignificant when equated with the actual cost of a successful intrusion. This factor also reinforces the necessity to develop more powerful intrusion detection systems.

Since 1980's, many researchers proposed different techniques to develop effective and efficient intrusion detection system (Anderson, 1980; Axelsson, 2000; Jones and Sielken, 2000; Kabiri and Ghorbani, 2005; Sherif and Dearmond, 2002; Siponen and Oinas-Kukkonen, 2007; Lunt, 1993; Lundin and Jonsson, 2002). But, still intrusion detection has to face many challenges. To identify various research challenges & issues related to intrusion detection, the relevant literature of intrusion detection techniques especially AI based techniques is reviewed by keeping major aspects of IDSs in consideration. For example, the important issues with respect to intrusion detection are low detection rate, high false positive rate and efficiency of the system.

Article overview: following this introduction, section 2 highlights the different types of intrusions. Description of various intrusions and their method is provided. Section 3 highlights motivation factor behind the intrusions. Section 4 gives a brief description of intrusion detection systems, functions and its need. Finally, Section 5 summarizes the paper.

2. Intrusions and their type

The intrusion can be defined in terms of basic security objectives viz. Confidentiality, Integrity and Availability. Intrusion is defined as a set of actions that attempt to bypass security objectives of computer system (Hernández-Pereira et al., 2009; Kumar et al., 2010; SANS, 2012; Singh et al., 2012). An intrusive action performs or attempts to perform the followings:

Breach of confidentiality: If it allows to access system resources in an unauthorized manner.

Breach of integrity: If it allows changing the state of resources in an unauthorized manner.

Breach the availability: If it prohibits legitimate users to access resources or services, residing in a computer.

Intrusion detection (ID) is a process of monitoring the actions or events occurring in a computer system or network and analyzing them for signs of intrusions. An intrusion detection system (IDS) is a software or hardware that automates the process of monitoring and analyzing of events (Halme, 1995; Bojkovic et al., 2008). Intrusions can take many forms, which make it difficult to provide a single meaning of the term. Generally, a successful intrusion passes through many stages as described below (Asaka et al., 1999; Kruegel et al., 2005; Engen, 2010).

Probe stage: At this stage, the intruders scan the victim computer systems for potential flaws in software to collect information about the victim.

Exploitation stage: If any flaw is found during the probe stage then it can be further exploited to control the victim computer system. An intruder can easily get control of the victim computer system and violate the security objectives.

Action stage: After getting the control over the victim computer system, the intruder can easily sniff the sensitive information, modify/delete important data, install any malware or drive the victim computer system to further attack other systems (Asaka et al., 1999).

Masquerading stage: In this stage, the intruder tries to remove traces of attack, for example, deleting log entries that reveal the intrusion.

Thus, intrusions can be classified into following categories (Kendall, 1999; Lippmann et al., 2000).

Probe: The probe or scan attacks automatically scan a network of computers, a DNS server to find valid IP addresses, active ports, host operating systems for known vulnerabilities. Such attacks are generally performed using multiple services to find the computer systems which are responding to a network. Information obtained from surveillance is useful to an attacker in launching a variety of automated attacks (Mukkamala and Abraham, 2006). Such attacks help the attackers to find active machines on the network and might deteriorate services for legitimate users. Common probing attacks are IPsweep, Lsdomain, Mscan, Portsweep, Queso, Satan etc.

Denial of Service (DoS): DoS attacks are the network level attacks in which the intruders use a large number of compromised computers to send malicious traffic to a web server or any other server (Schneider, 2012; Kendall, 1999; Engen, 2010; Sachdeva et al., 2009). The purpose of such attack is to disrupt the services or availability of resources partially or completely to legitimate users. If such attacks are attempted from a single compromised system, then the attack is called a DoS attack. Whereas involvement of multiple systems for flooding attack traffic leads to Distributed DoS (DDoS) attack. According to Internet World Stats, the worldwide Internet population in June of 2010 was close to 2 billion users (Schneider, 2012). Many users browse the Internet without appropriate security software, or use operating systems and software that are not properly updated. Attackers employ automated techniques/tools to trace such systems and use known vulnerabilities to install DDoS tools for identified systems. Such compromised computers are typically referred to as zombie computers, or bots. Zombie computers report back to a Command and Control (C & C) server. After they are logged on, they become part of a remotely controlled botnet. The most common C & C servers are Internet Relay Chat (IRC) servers, although some are web servers and even Twitter has been used as a C & C channel. Through the remote control of hundreds or thousands of infected computers that have been previously compromised by worms or trojans, it's possible to coordinate large DDoS attacks. Larger botnets can exceed 1,00,000 zombie computers, which can generate aggregated traffic from 10Gbps to 100Gbps - more than most ISPs can handle. McAfee's third quarter 2010 report indicated that 18 million new zombies were created during that period - an average of 2,00,000 new zombies per day (Schneider, 2012). The zombie computers were primarily used to generate spam, but their purpose could be easily changed by the botnet controller to generate DDoS attacks. To increase the effectiveness of the attack, vulnerabilities are often used to obtain control of the web servers for the purpose of installing trojans or worms that add the server to the controlled botnet. Generally, server machines have the advantage of better computing resources and higher available bandwidth. Further, attack traffic is generated from trusted IP addresses. A large number of DDoS enabling tools are also available on the Internet. The most common ones include Tribe FloodNetwork (TFN) and its newer version TFN2K, Trinoo (Trin00), Stacheldraht, myServer, Mstream, Omega, Trinity, Plague and derivatives etc. Common DoS/DDoS attacks are Address Resolution Protocol (ARP) flooding attack, TCP SYN flooding attack, UDP flooding attack, Ping flooding attack, Smurf attack, ICMP Destination Unreachable attack, ICMP Time Exceeded attack, Teardrop attack, DNS flooding attack and SIP flooding attacks etc.

User to Root (U2R): Such attacks exploit flaws in operating systems and software. Here, a local user on a machine is able to obtain administrator privileges. The attack consists of accessing the special files reserved for security policy of the victim (Kendall, 1999; Ciza, 2009). Common U2R attacks are Ntfsdos, Sqlattack, Buffer overflow attack etc.

Remote to Local (R2L): There are some similarities between this class of intrusion and U2R.
However, in this case, the intruder does not have an account on the host. He attempts to obtain local access across a network connection. To achieve this, the intruder can execute buffer overflow attacks, exploit mis-configurations in security policies or engage in social engineering (i.e., obtaining data by tricking a human operator, rather than targeting software flaws) (Kendall, 1999). Common R2L attacks are Guest, NT PowerPoint macro attack (ppmacro), A man-in-the-middle web browser attack, An NT Trojan installed re- mote administration tool, A Linux Trojan SSH server (sshtrojan) etc.

Similar taxonomy of the attacks has also been proposed by (Lee and Stolfo, 2000), which categorizes intrusions that occur in the DARPA Intrusion Detection Evaluation data set (DARPA, 2012).

It is observed during the analysis that different intrusions behave differently. For example, probe type of intrusions is likely to exhibit limited change as it comprises establishing connections to a large number of computer systems in a stipulated period. In U2R type of intrusions, root privileges are obtained by unauthorized users. Therefore, in both probe and U2R type intrusions, a small number of instances in training data can make possible for classification technique to learn their behavior easily. While both DoS and R2L type intrusions exploit the flaws of a set of computer systems offering different type of services belonging to different networks. Here, the characteristics of these attacks are very specialized. Hence, it is very difficult for classification technique to learn general behavior from a limited number of instances in the training data. Therefore, some of the zero day attacks remain undetected. Major cause of failure of detection of these attacks is the variation in their behavior. Even the best IDS for the DARPA evaluation (DARPA, 2012) shows that less than 10% of new R2L intrusion attempts have been detected (Ciza, 2009). Hence, detection of new attacks is more significant in determining the quality of an IDS.

3. Motivation behind intrusions

A successful intrusion generally compromises a set of computer systems by breaching into one or more security objectives namely confidentiality, integrity or availability. Once anyone of the security objectives is breached, the intruder may result many unpleasant activities. For example, he can steal important information that may be further used to steal money, either through fraudulent credit card transactions or bank transfer transactions. The services of the compromised systems may get disrupted partially or completely for legitimate users, which may require significant time to re-establish again. Most of the intruders are gaining profits by performing malicious actions in the following ways (Schneider, 2012):

- Unauthorized bank & credit card transactions by manipulating the related information.
- Advance fees, as in the Nigerian scam (now originating from many countries) that request money to cover the transfer of millions of ’unclaimed’ funds.
- Product sales from scare ware and web-based enticements.
- Criminal services that allow the creation and use of malware, including malware toolkits, such as the Zeus Trojan toolkit.
- Resale of stolen credit card and bank account related information.
- Captcha breaking services - Captcha is a technique that presents an image with an embedded word or number. This ensures that a human is involved in the interaction. Criminal elements are now offering software services to defeat this interaction.
- Virus testing services - these are online services that determine whether a candidate virus/malware file will be detected by 40 or more anti-virus programs.
- Search redirection - these are services that poison Google and other search engine lookups so that they may direct users to the target websites. Valid institutions may be perceived as insecure by their customers.

There may be some other motivational factors for the intruders as listed below:

- Fame - Looking for the fame among the community of intruders.
- Political - Some country may try to disrupt the services of popular servers for some specific reasons. For example, services of energy, transport, banking, telecom, defense, space and other sensitive areas.
- Ideology - that characterizes the thinking of a group or nation. It may also be one of the primary attack motivation.
- Vandalism
- Online gambling

- Frustration
- Fun and many more.

4. Intrusion Detection System (IDS)

The notion of intrusion detection was originally suggested by (Anderson, 1980). He proposed that audit trails contain vital information that can be used to detect the intrusions. The same concept was further extended by (Denning, 1987) at SRI International. He suggested a solution to secure the computer systems by proposing the first model for an IDS called Intrusion Detection Expert System (IDES). The proposed IDS model is independent of any intrusion, the system and its environment. The model is based on the concept that the intrusion is the abnormal usage of system resources. The model proved as an abstract model for further improvements. In 1988, Haystack IDS was developed at Lawrence Liver more Laboratories (Smaha, 1988). The concept of single IDS was further enhanced for Distributed Intrusion Detection System (DIDS) for client server architecture by releasing Stalker IDS (Innella et al., 2001). Then, many commercial IDSs were introduced into the market. For example, Network Security Monitor (NSM), Net Ranger, Real Secure, Snort and many more (Innella et al., 2001; Heberlein et al., 1990; McHugh, 2001). Different IDSs possess different characteristics for meeting the requirements of an ideal IDS that involve the following (Debar et al., 1999):

- Accurate: No False Positives.
- Complete: No False Negatives.
- Performance: Real Time Detection.
- Fault tolerance: The IDS not becoming security vulnerability itself.
- Scalability/Timeliness: Process large amounts of audit data quickly to propagate intrusion information for counter measures.

In spite of many efforts till date, IDSs have to face many challenges in meeting the requirements of an ideal IDS.

5. Conclusions

The aim of this paper is three fold. First aim is to present various intrusions and their types. The intrusions are classified into four categories namely Probe, DoS, U2R, and R2L. Secondly, the paper is to present the motivation behind the intrusions. The motives of the intruders are of wide range. The motives vary from fame, political, ideology, vandalism, frustration, fun and many more. Finally, the paper aimed to brief history of IDSs, their need, important examples and characteristics of ideal IDS. The paper provides clues for the readers to explore their research in the field of intrusion detection.

References

[1] Anderson, J.P., 1980. Computer security threat monitoring and surveillance. Technical Report 79F26400. James P. Anderson Co., Fort Washington. URL: http://csrc.nist.gov/publications/history/ande80.pdf.

[2] Asaka, M., Taguchi, A., Goto, S., 1999. The implementation of ida: An intrusion detection agent system, in: Proc. of the 11th Annual FIRST Conference on Computer Security Incident Handling and Response (FIRST99), Citeseer. Axelsson, S., 2000. Intrusion detection systems: A survey and taxonomy. Technical Report. Technical report.

[3] Bojkovic, Z.S., Bakmaz, B.M., Bakmaz, M.R., 2008. Security issues in wireless sensor networks. International Journal of Communications 2, 106–115.

[4] Cert, 2012. Cert/cc statistics. URL: http://www.cert.org/stats/.

[5] Ciza, T., 2009. Performance Enhancement of Intrusion Detection Systems using Advances in Sensor

Fusion. Ph.D. thesis. Supercomputer Education and Research Centre, Indian Institute of Science, Bangalore.

[6] DARPA, 2012. Intrusion detection evaluation. URL: http://www.ll.mit.edu/IST/ideval/.

[7] Debar, H., Dacier, M., Wespi, A., 1999. Towards a taxonomy of intrusion-detection systems. Computer Networks 31, 805–822.

[8] Denning, D., 1987. An intrusion-detection model. IEEE Transactions on Software Engineering , 222–232.

[9] Engen, V., 2010. Machine learning for network based intrusion detection: an investigation into discrepancies in findings with the KDD cup'99 data set and multi-objective evolution of neural network classifier ensembles from imbalanced data. Ph.D. thesis. Bournemouth University.

[10] Gupta, K., 2009. Robust and efficient intrusion detection systems. Ph.D. thesis. University of Melbourne, Department of Computer Science and Software Engineering.

[11] Halme, L., 1995. Ain't misbehaving–a taxonomy of anti-intrusion techniques. Computers and Security 14, 606–606.

[12] Heberlein, L., Dias, G., Levitt, K., Mukherjee, B., Wood, J., Wolber, D., 1990. A network security monitor, in: Proc. Of IEEE Computer Society Symposium on Research in Security and Privacy, IEEE. pp. 296–304.

[13] Hernández-Pereira, E., Suárez-Romero, J., Fontenla-Romero, O., Alonso-Betanzos, A., 2009. Conversion methods for symbolic features: A comparison applied to an intrusion detection problem. Expert Systems with Applications 36, 10612–10617.

[14] Innella, P., et al., 2001. The evolution of intrusion detection systems. SecurityFocus, November 16.

[15] Jones, A., Sielken, R., 2000. Computer system intrusion detection: A survey. Computer Science Technical Report .

[16] Kabiri, P., Ghorbani, A., 2005. Research on intrusion detection and response: A survey. International Journal of Network Security 1, 84–102.

[17] Kendall, K., 1999. A database of computer attacks for the evaluation of intrusion detection systems. Ph.D. thesis. Massachusetts Institute of Technology.

[18] Kruegel, C., Vigna, G., Robertson, W., 2005. A multi-model approach to the detection of web-based attacks. Computer Networks 48, 717–738.

[19] Kumar, G., Kumar, K., Sachdeva, M., 2010. The use of artificial intelligence based techniques for intrusion detection: a review. Artificial Intelligence Review 34, 369–387.

[20] Lee, W., Stolfo, S., 2000. Data mining approaches for intrusion detection. Defense Technical Information Center, dept of computer science, Columbia university, New York.

[21] Lippmann, R., Fried, D., Graf, I., Haines, J., Kendall, K., McClung, D., Weber, D., Webster, S., Wyschogrod, D., Cunningham, R., et al., 2000. Evaluating intrusion detection systems: The 1998 darpa off-line intrusion detection evaluation, in: Proc. of DARPA Information Survivability Conference and Exposition (DISCEX'00), IEEE. pp. 12–26.

[22] Lundin, E., Jonsson, E., 2002. Survey of Intrusion Detection Research. Technical Report 02-04. Chalmers University of Technology. Department of Computer Engineering.

[23] Lunt, T., 1993. A survey of intrusion detection techniques. Computers & Security 12, 405–418.

[24] McHugh, J., 2001. Intrusion and intrusion detection. International Journal of Information Security 1, 14–35.

[25] Mukkamala, S., Abraham, A., 2006. Cyber security challenges: designing efficient intrusion detection systems and antivirus tools. Vemuri, V. Rao, Enhancing Computer Security with Smart Technology , 125–163.

[26] Ramamohanarao, K., Gupta, K., Peng, T., Leckie, C., 2007. The curse of ease of access to the internet. Information Systems Security , 234–249.

[27] Sachdeva, M., Kumar, K., Singh, G., Singh, K., 2009. Performance analysis of web service under ddos attacks, in: Proc. of International Advance Computing Conference (IACC), IEEE. pp. 1002–1007.

[28] SANS, 2012. Intrusion detection faq. URL: http://www.sans.org/security-resources/idfaq/.

[29] Schneider, D., 2012. The state of network security. Network Security 2012, 14–20.

[30] Sherif, J., Dearmond, T., 2002. Intrusion detection: systems and models, in: Proc. of eleventh IEEE International Workshops on Enabling Technologies: Infrastructure for Collaborative Enterprises, 2002. WET ICE 2002., IEEE. pp. 115–133.

[31] Singh, J., Kaur, L., Gupta, S., 2012. A cross-layer based intrusion detection technique for wireless networks. The International Arab Journal of Information Technology 9, 201–207.

[32] Siponen, M., Oinas-Kukkonen, H., 2007. A review of information security issues and respective research contributions. ACM Sigmis Database 38, 60–80.

[33] Smaha, S., 1988. Haystack: An intrusion detection system, in: Proc. of fourth Aerospace Computer Security Applications Conference, IEEE. pp. 37–44.