WEAKNESSES, VULNERABILITIES AND ELUSION STRATEGIES AGAINST INTRUSION DETECTION SYSTEMS

Hossein Jadidoleslamy

Department of Information Technology, Anzali International Branch, The University of Guilan, Rasht, Iran
tanha.hossein@gmail.com

ABSTRACT

One of most important existent issues in information security application domain is Intrusion Detection System (IDS); IDS is a defensive-aggressive system to protect information, verifying and responding to occurring attacks on computer systems and networks. This paper discusses different topics including presenting some strategies against IDSs to passing from them; this leads to improving detection level and performance of IDS; also, this paper considers some intrusion tools, new attacks patterns and tracking prevention techniques. In addition, it discusses vulnerabilities, security holes and IDSs' structural and systemic problems to eliminating defects, reducing penetrates and correcting their behavior. Finally, it leads to increasing the functionality coefficient of IDSs, promoting the security level of computer systems and networks, increasing the trust of authorized users. So, the proposed methods in this paper can apply to improving the IDSs by using inverse engineering methods.

KEYWORDS

Security, Intrusion, Intrusion Detection System (IDS), Detection, Prevention, Computer Network & Intruder.

1. INTRODUCTION

Nowadays, information is the most valuable asset of organizations that needs to protect and supply its security against unauthorized access. Security supply means supplying three basic dimensions including integrity, confidentiality and availability [1]. It can do by two strategies, including violation prevention and violation detection from security policies. In the existent approaches, a defensive-aggressive approach like IDS is an efficient and appropriate tool to monitor intruders' motivations, goals and their tools. Target of an IDS is detecting attacks/intrusions and systems' security problems and then, notifying them to the security manager [1, 5, 7, 10].

In layered-based model of security, different types of IDSs including host, network and application levels are usable. Also, IDS is security equipment which can use in layers 2, 3 and 4 of TCP/IP model. An IDS reinforces the system or network security and increases the functionality coefficient, of course along with other security mechanisms [6]. The main topics of this paper are as follow:

- Introducing IDSs and usual attacks against them to increasing detection, security level and their accurate functionality;
- Considering intrusion tools, attacks patterns and prevention techniques of tracking that used by intruders;
- Discussing IDSs' vulnerabilities, security holes and systemic/structural problems to eliminate their defects, reducing penetration and correcting their behavior;

All of these things conclude to promoting the security level of computer systems and network, increasing the authorized users' reliability and preventing from intruders' misuse. This paper has

DOI : 10.5121/ijcses.2012.3402

been organized as: section2 expressed the intrusion concept; section3 discussed about IDSs and their different dimensions and categorizations; section4 is presented the different intrusion, prevention and elusion techniques against IDSs (some methods about how attackers can pass from IDSs); section5 expressed conclusion and finally, section6 represented the future works.

2. CONCEPT OF INTRUSION

Intrusion, i.e. unauthorized access or login (to the system, or the network or other resources); Intrusion is a set of actions from internal or external of the network, which violate security aspects (including integrity, confidentiality, availability and authenticity) of a network's resource [7, 13]. Different steps of intrusion are:

- Gathering verification/primary information about the target system or network;
- Scanning ports;
- Scanning vulnerabilities and security holes;
- Attacking;
- Acquiring the control of the target system or network;
- Hacking and accessing to the system or network resources;

Intruders are classified into two categories, including internal intruders and external intruders; for example internal employee, hacker and malicious software (malware). Intruders using methods to attack and unauthorized access to the systems or networks, such as software defects, passwords break, eavesdropping, existent weaknesses in design of computers, networks and services [7, 13].

3. INTRUSION DETECTION SYSTEM (IDS)

Intrusion detection is a process which detecting contradictory activities with security policies to unauthorized access or performance reduction of a system or network [4, 7, 11]; the purpose of intrusion detection process is reviewing, controlling, analyzing and representing reports from the system and network activities. Intrusion Detection System (IDS), i.e.:

- A hardware or software or combinational system, with defensive-aggressive approach to protect information, systems and networks [3, 8, 17];
- Usable on host, network [2, 11] and application levels;
- It analyzes the system or network traffic or controls the incoming connections to different ports, and then it detects the occurring sabotage/vandalism;
- It can detects known attacks, unusual traffic, harmful data, misuse and unauthorized access to the systems and networks by internal users or external intruders [2, 7];
- It inferences by using deterministic methods (based on patterns of known attacks) or non-deterministic methods (to detecting new attacks and anomalies);
- It can determine the intruder's identity and tracking him/her/it;
- It informs and notifies to the security manager by different types of warnings or notifications; sometimes, it disconnects the suspicious connections or blocks malicious traffic [2, 3];

In general, three main functionalities of IDSs are including monitoring (evaluation), analyzing (detection) and responding (reporting) to the occurring attacks on computer systems and networks [3, 8]. There are two stages to configure IDS, consisting of attack's signs and management arbitrary events [8]. If IDS has been configured nice, it will show three types of events, including: primary verification events (like stealthy port scan or file content manipulation), attacks (automatic/manual, local/remote) and suspicious events.

3.1. IDS Categorization Based on Their Architecture

According to the **Figure1**, Intrusion Detection Systems (IDSs) by attending to the information gathering source and input data supplier, divided into three categories, as follows.

3.1.1. Host-based Intrusion Detection System (HIDS)

According to **Table1**, HIDS installs on a computer system; it uses processor and memory of that system and protects only the hosting system [4, 7, 9, 11]. It has an abnormal detector part which using statistical methods to detect abnormal behavior of users in comparison to their behavioral records [1, 2, 14]; also, it has an expert system part that detects the security threats and describes the vulnerabilities of the system, but independent from behavioral records of users; of course, it uses a rules-base, too.

3.1.2. Network-based Intrusion Detection System (NIDS)

As **Table1** is showing, NIDS is a software process which installs on a special hardware system; in many cases, it operates as a sniffer and controls passing packets and active communications, and then it analyze network traffic in sophisticated, to find attacks [2, 7, 8, 17]. NIDS can identify attacks, on network level; thus, it includes following steps:

- Setting up the Network Interface Card (NIC) on promiscuous mode and eavesdropping network traffic [2, 11];
- Capturing the transmitting network packets [3, 14];
- Extracting requirement information and properties from the network's packets;
- Analyzing properties and detecting statistical deviation from normal behavior and known patterns (using pattern matching);
- Producing and logging proper events [4];

3.1.3. Distributed Intrusion Detection System (DIDS)

In attention to **Table1**, most important characteristics of DIDS are:

- Combination of HIDS, NIDS and central management system [2, 12];
- Sending the reports of distributed IDSs (HIDSs and NIDSs) to the central management system;
- Based on distributed and heterogeneous resources [3, 12, 14];
- High complexity, variable specifications and agent-based.

In attention to most attackers are targeting routing layer of networks, since they can control passing information into the network. So, disrupting and violating from this process leads to success attacks. As a result, for such networks, most proper architecture for IDS will be NIDS. A NIDS using network's traffic as data source; it eavesdrops and listens to the network traffic, captures packets in real-time, then controls and tests them to detect attacks.

Table 1. A comparison of different IDSs based on their architecture

IDS/properties	**Deployment location**	**Information source**	**Control domain**
HIDS	Under-control system, software process	Local traffic (on OS level) and Log files	Local hosting system
NIDS	Isolated system on network traffic route, software process	Network traffic (raw data packets of the network)	Local segment or whole network
DIDS	Distributed and heterogeneous (host, network and central management system)	Host traffic and network traffic	Network wide (all hosts and different network segments)

3.2. IDS Classification Based on Detection Method

IDSs must be able to differentiate between normal and abnormal activities, to detect malicious efforts, in real-time. As **Figure1** shows, IDSs be partitioned into two categories, based on data analysis and detection method [1, 2, 16]. In following sections, they will be considered.

3.2.1. Anomaly Detection Systems

Anomaly Detection Systems are focused on normal behavioral patterns [2, 16]. According to the expert systems are not able to timeouts update patterns, we will need automatic devices to extract new attacks' patterns. It is possible to using some techniques such as threshold detection (fully heuristic and static), statistical criteria, act/rule-oriented criteria, clustering methods, neural networks, expert systems, machine learning and data mining, to detecting abnormal behaviors [3, 4]; for example, measuring the changes in volume, direction and pattern of communication traffic, can indicate and differentiate attack traffic, easily. In this approach, it is possible to detecting new attacks and also internal attackers; including following steps:

- Identifying normal behaviors [2, 7] (they have deterministic properties) and finding especial rules for them (describing normal behaviors by automated learning, usually);
- Forming some views from normal behaviors of the system, network, users and user groups;
    - Behaviors that following these patterns ⇨ normal behaviors;
    - Activities which have excessive deviation from defined statistical values of these patterns ⇨ abnormal behaviors and intrusion efforts;

➲ The main key to detect abnormal behavior: comparing current traffic and predefined normal behaviors patterns [3, 4, 16].

➲ Problem: how gathering a set of static criteria of normal behaviors?

3.2.2. Signature-based Detection Systems

This method is using deterministic scenarios, rules and patterns of known attacks, which be defined by security expert systems, to detect security threats and attacks [1, 2, 5, 15]; in this model, IDS gathers the properties of attacks and abnormal behaviors and then, make an information base by them [4, 15]. Therefore, to using such systems, user should define and store the templates and requirements actions for security threats. After pattern and properties matching, IDS can report the type of attack, in precise. Thus, the main operation of these systems is comparing observed behavior and known attacks' patterns to each other. Some of characteristics of this approach are:

- Inability to identifying new attacks [3, 8, 16];
- Requiring to a set of predefined patterns [13] (including properties, rules and behaviors) of known attacks into the IDS;
- Necessity of adding new patterns of attacks to the patterns' set, manually and repeatedly;

➲ The main key to detect misuse behavior: comparing current traffic to predefined and pre-known attacks' patterns [2, 16, 17].

➲ Problem: how detecting intrusions' properties and displaying them?

3.3. IDS Categorization Based on Decision Making Techniques

In this section, the paper discusses about who should make final decision if occurring intrusion or not, or if a node is an intruder, really? Is an attack accrued? If ok, what actions must be doing? According to the **Figure1**, there are two approaches for this purpose, as follows.

3.3.1. Cooperative Mechanism

In a cooperative IDS, if a node detects an anomaly, or the existent evidences be inconclusive, a cooperative mechanism triggers to produce a global intrusion detection action along with neighboring nodes; even if a node be sure about the crime of another node, decision making also should be cooperative (again) [2, 3]; because the node which take the decision, maybe be malicious, itself.

3.3.2. Autonomous and Independent Mechanism

In this method, network nodes take decisions, autonomously [3, 4]; they gather evidences and criteria of anomaly and intrusion activities from the network and then, make decision on node-level. Other network nodes do not have cooperated in this decision making process. The main weaknesses of this approach are:

- Security of network nodes is low [2]; attackers can compromise them soon and easy; therefore, this leads to loss of the network control;
- Enforcing excessive processing overhead on some network nodes; therefore, in attending to limited resources and being few key nodes, it leads to their lifetime reduction (energy waste and network node destruction).

3.4. IDS Categorization Based on Response Method

IDSs using events' information and patterns analysis of attacks to react them, as following sections.

3.4.1. Direct Response

These responses prevent from the attackers' activities, directly [2, 3, 8, 16]; for example, session disconnection [4], dynamic reconfiguration of the network, using Honeypot and setting thresholds again (in attention to the user skill, network speed, expected network connections, work load of security manager, sensor sensitivity, security policy, vulnerabilities, information and system sensitivity and fault importance).

3.4.2. Indirect Response

These kinds of responses do not prevent from the attackers' activities, directly [4, 13, 16], like: shunning, logging, notifying through cell phone, email and message to SNMP console [3, 4].

➲ The proposed response approach for the computer networks is using combinational method; i.e. active and passive responses by each others, depending on conditions and attacks' nature; thus, the type of response be determining based on attacks' severity and their damages level. Also, responses can be as a part of policies; i.e. we can define and store responses into the Info-bases such as Policy-base, manually.

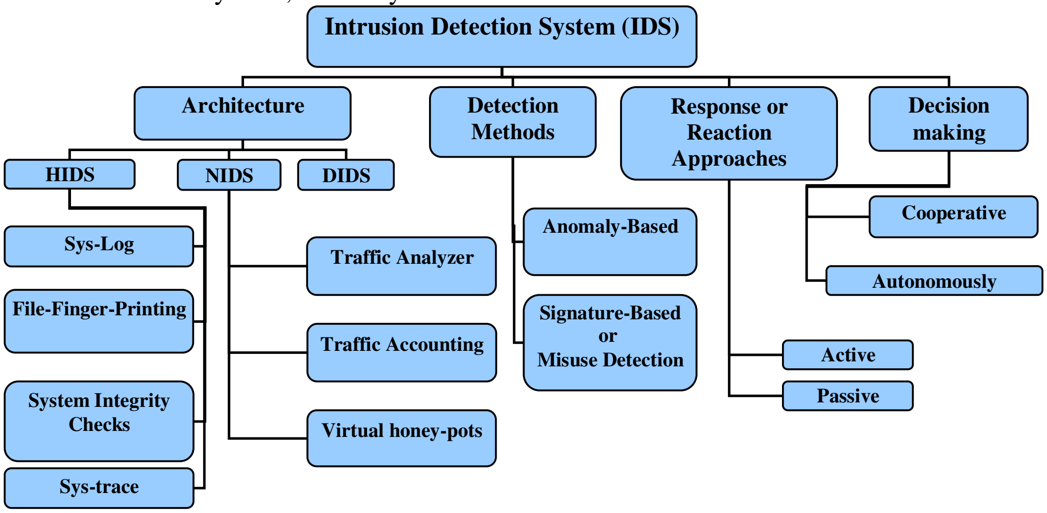

Figure 1. Different categorizations of IDSs

4. ELUSION STRATEGIES AGAINST IDSs

There are many strategies against IDSs which can help intruders to pass from IDSs. Some of their most important have been classified and expressed in following sections.

4.1. Public Elusion Techniques against IDSs

Some of most popular methods which used by intruders to pass from IDSs are:

- Coding requests to attack to applications;
- Fragmentation technique to attack against the services;
- Polymorphic shell code to attack against exploits;
- Misusing errors, security holes and vulnerabilities of IDS to attack to itself and other systems (IDS deception and triggering many wrong notifications);
- Sending much useless data to IDS (DoS attack against IDS ➲ IDS can not analyzing the log files);
- Scanning ports by using Idle method (Bouncing);
- Using the different capabilities of Nmap tool, including:
  - Scanning by FTP Bounce Scan method;
  - Hidden port scanning (TCP SYN Scan);
  - Hiding intruder's traffic through sending many useless/forgery packets, slowly;
  - Using switch –S{x} i.e. source address to forging the IP address;
  - Using switch –f (i.e. fragmentation);
  - Using of switch –sS, i.e. SYS Stealth, stealthy scan mechanism;
- Utilizing the different capabilities of X-Scan tool, consist of:
  - Using switch –t to hide intruder;
- Doing attacks without/with at least changes in volume, direction and pattern of communication traffic;
- Misusing of the IDS's statistical and analysis techniques' weaknesses;
- Using of spyware to verification, stealthy access to systems and network resources (preventing from verifying and tracking intruder by IDS by using the fraud detection capability) and attack (overflow and DoS attacks against IDS) [5, 10];
- Finding threshold range (through social engineering) and inviolate of them to escape of Anomaly Detection;
- Attacking to IDS resources, which leads to resource starvation [5] (IDS crash);
- Doing direct/indirect or active/passive attacks against IDS, such as DDoS and SYN Flood [5, 10, 12];
- Utilizing new tools and unknown patterns;

4.2. Classification Elusion Techniques against IDSs Based on Their Architecture

In attention to the different architecture of IDSs, intruder can pass from them by using some techniques; some of these methods have been written in continue (following sections).

4.2.1. Elusion Strategies against HIDSs

The most important technique against HIDS is verifying its process (by intruder) and disabling it through stopping the information gathering cycle.

4.2.2. Elusion Strategies against NIDSs

There are a lot of methods against NIDSs; the most common techniques of them are including:

- Misusing from difficulties of IDSs' pattern matching algorithm (low or high flexibility) for attack to it;
- Doing attacks in the low layers of the network;

- Network traffic encryption, high transmission/transfer speed and much/high volume;
- Three types attacks against sniffing-based NIDSs are:
    - DoS: disabling the NIDS by sending many useless/false packets/activities to it and resources starvation attacks to disabling the system; flooding/exploiting the NIDS by false/wrong activities; sending flooding traffic to the NIDS, including: Network Resource Exhaustion (such as disk space, memory, CPU cycle and bandwidth) and Abusing Reactive IDSs [5, 10, 11];
    - Insertion: in this method, intruder sends invalid packets through valid packets. Insertion attacks disable protocol analysis and then pattern matching too. These attacks by adding packets to the stream, corrupting the reassemble of the stream and then, lead to completely different reassemble on the target system (destination). Attached packets can change the stream sequence and then, leads to IDS's wrong understand. Also, it is possible that the packets have been inserted as they have overlap with previous data or adding some data to the stream content which they change its mean. Different techniques of insertion attack are: URL Encoding, Reverse Traversal, Self-referencing Directories, Parameter Hiding, Long URLs and Multiple Slashes [10, 12, 13].
    - Evasion: in this way, intruder creates inconsistency between analyzer and the goal system and then, he/she/it attacks to the system; it leading to the NIDS loses some of stream fragments and thus, it prevents from reassemble of the stream by the NIDS. It tries to disable the protocol analysis and pattern matching process as same as the insertion attacks. Besides, intruder causes that the NIDS receives a different information flow of the target system; i.e. the NIDS does not or can not view the important and necessity information to detecting attacks. Also, the main request can be as a non-mean packet/request for the NIDS. The different mechanisms of evasion attack are: Slow Scan, Method Matching, Premature request ending, Http Mis-Formatting, DOS Syntax Directory, Case sensitivity, Fragmentation (enforcing much overhead in fragments reassemble time), Session Slicing and Null Method Processing (ignoring the malicious payload) [5, 13].

4.3. Classification IDSs' Elusion Techniques Based on Intrusion Phases by Intruder

IDS can verify intruder in one of following phases.

4.3.1. Phase1: Primary Verification and Information Gathering

Strategies against IDS verification in this phase are:

- Using new sniffing tools and methods, to finding open ports and vulnerability points;
- Hidden scan and getting the information from open ports and security holes of the target system;
- Using tools which change the intruder's information (forgery information) or tools that they show intruder's information as null [5];
- Utilizing of available IP addresses into the network (during scan);
- Using of social engineering skills (art of deception), specially in system to system communication like spoofing [5, 8];

Some of used tools into this phase are including SamSpade, Net Scan Tools and LAN Surveyor.

4.3.2. Phase2: Attack and Misuse

Strategies against verifying by IDSs into this phase are as following:

- Encrypting the sent/forwarded traffic and using polymorphic shell code;
- Using new attack methods (programmed by intruder);

- Sending much volume of suspicious/unrelated traffic to the target system (in short time interval);
- Stopping or activating logging (by using some tools such as AuditPol);

4.3.3. Phase3: After of Attack

The most important strategy against tracking by IDS is hiding and removing the footprints; including attacking to event logs (change and removing them), changing in shell history files and establishing the hidden channels and infecting the target system to the Root kit. Some of tools which used into this phase are Clear Event Log and Win Zipper.

4.4. Classification IDSs' Elusion Techniques Based on Their Structural Block Diagram

Following figure (**Figure2**) shows the CIDF model of IDSs. If there were a hole in each one of IDS's components, so the IDS is one of logical goals to attack. It is possible to disable it or enforce it to produce false/wrong information/notifications/warnings (in attention to the IDS's failures be classified into two categories including Accuracy, i.e. Number of False Positive Occurrence and Completeness, i.e. Number of False Negative Occurrence).

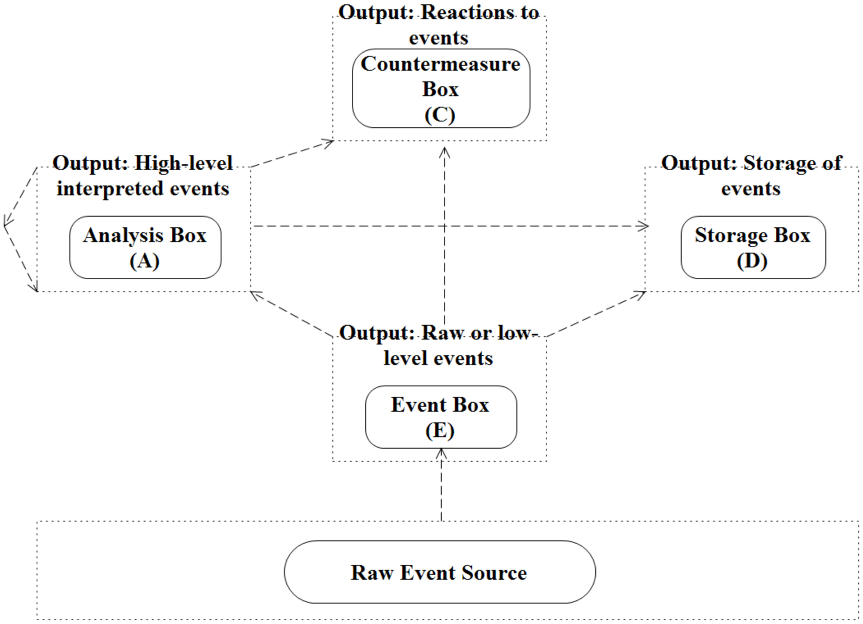
Output: Reactions to events
Countermeasure Box (C)
Output: High-level interpreted events
Analysis Box (A)
Output: Storage of events
Storage Box (D)
Output: Raw or low-level events
Event Box (E)
Raw Event Source

Figure 2. Communications between CIDF Components

In attention to showed architecture in above **Figure2**, some of IDSs' vulnerabilities are [10]:

- Attack to box E (Event Generator): preventing from IDS to get/access to packets or preventing from allocating appropriate code to them;
- Components of box A (Analysis Engine): these components do complex/sophisticated analysis to providing security information; because in otherwise an intruder can escaping from detecting (by its deception); the simple systems be failed in detecting masked and complex attacks;
- Intruder can manipulates the components of box D: it causes prevents from logging the attack details; sometimes, it is possible to change the logged information;

- About box C: i.e. if intruder knows how does not answer to box C, he/she/it can continue to its attack against the IDS, fully safe. Even, it is possible to inverse the capabilities of this box.

4.5. Classification IDSs' Elusion Techniques Based on TCP/IP Model

In attention to the TCP/IP model, intruder can pass from the IDS by using different techniques which some of them have been expressed and classified in following sections.

4.5.1. Routing Layer

Network layer problems are including [1, 2, 10]:

- Attacking by new attacks patterns and new tools that have been written by intruder;
- Using the fragmentation technique (by using tools such as Frag router);
- Insertion and evasion attacks [3, 10], consist of:
    - Simple insertion attack, including: Bad header field (Checksum, TTL36 and DF37), IP options (Time stamp and tracking TCMP responses);
    - MAC addresses: intruder can send forgery packets to the IDS by using/having/knowing its MAC address, simply; thus, intruder can attacked the IDS by buffer overflow or DoS attacks [4, 5];
    - IP fragmentation: it is including Basic reassembles problems, Overlapping fragments, Effect of End System Fragmentation Bugs and IP options in Fragment streams;
    - Forensic information from IP packets: it is possible to change the logged information by intruder (even after attack/intrusion detection); so, that information lose their legal valuable/importance (their importance be destroyed);

4.5.2. Transport Layer

In this layer, intruder tries to confusing the IDS in current stream sequence numbers; i.e. the IDS be desynchronized from the intruder connections. Difficulties of the transport layer are [1, 2, 10]:

- Simple insertion attack [3, 10], including:
    - Malformed header fields: like non-checking the header fields of TCP packets, non-considering the data of a SYN packet and non-calculating the checksum;
    - TCP options: bad options;
- TCP creation [4, 10], consist of:
    - Requiring three-way handshaking: the intruder be undetectable by using different sequence numbers but along with same parameters from/than the real/logged sequence numbers related to the IDS's three-way handshaking [5] (it takes time until the established TCP connection be opened by the intruder);
    - Data synchronization: if the IDS does not be configured correctly, or if the IDS's configuration be inconsistent to real packet filters, the intruder can confuse the IDS by injecting the forgery SYN packets to the network (communication channel);
- TCP stream reassembly [3, 10], including:
    - Basic reassembly problems: intruder can send the data stream non-ordering (then it can be un-understandable for the IDS to detecting attacks);
    - Challenges to reassembly: intruder can send several packet sequences as they are identically same but along with variable data; into these packets their header information will not change (except of checksum); each/any packet will change the state of end system by an exactly same method, but it will be processed only one of that packets by the target system; thus, it is possible to attack to this IDS by insertion attack techniques. So, the IDS will accept the harmful data, it also ignores

  the valid data and it be confused proportional/than real connection (similar to TCP Hijacking);
  - Overlap: intruder can create a stream which it be quite harmless by overlapping TCP segments, also, intruder can overwrite the packet of stream on destination host;
  - Endpoint TCP overlap bugs;
- TCP teardown: intruder prevents from pattern matching by inducing the false end of TCP connection [10, 16].
  - Using TCP connection teardown messages;
  - Relying on timeouts for TCP teardown: intruder leads to the IDS lose the connection state by inducing the time interruption of TCP connections; then the intruder can escape from the IDS (sneakers type attacks). If the intruder establishes a new connection with the same parameters before time outing his/her/its primary connection that it maintains on IDS, the IDS will be confused.

5. CONCLUSION

IDSs are not the sophisticated, complex and silver bullet security solutions; but they only reduce security risks. They have many weaknesses in their design which decrease their efficiency. This paper introduced the IDSs, different intrusion methods, IDSs' weaknesses and vulnerabilities and some strategies against IDSs (elusion techniques). It is possible to utilize from proposed strategies to improving the IDSs (of course by using reverse engineering techniques), increasing security and taking efficient security policies. Some of most important challenges and vulnerabilities of IDSs are:

- Inability to eavesdropping and analyzing the high volume and high speed traffics; it leads to non-real time detection;
- Non-supporting IP version 6.0 and encrypted traffic;
- False positive, false negative and scalability;
- Different/variety attacks against IDSs, like DoS, Buffer overflow, SYN flood and Spoofing;

Some of most important results of this research are:

- Presenting some strategies against IDSs to violate them;
- Proposals for improving and eliminating the IDSs' vulnerabilities (of course, by utilizing from reverse engineering techniques);
- Introducing to IDSs' challenges, vulnerabilities, security holes, their difficulties and disadvantages to thinking about how it is possible to improve their functionality;
- Introducing some of intruders' tools/devices and utilizing them to testing IDSs to finding their problems.

6. FUTURE WORKS

Some of research topics in this regard (by the same token) are as following:

- Presenting some strategies to eliminating the designed defects and preventing from intruders' attack techniques;
- Introducing some methods to tracking intruders and reacting against impersonation (identity forge);
- Presenting the used traffic encryption techniques by intruders;
- Presenting some techniques to detecting attacks of encrypted traffic;

It is hoping which this paper is useful to improving the IDSs' functionalities, their security level and functionality coefficient of computer systems and networks.

REFERENCES

[1] K. Scarfone and P. Mell; Guide to Intrusion Detection and Prevention Systems (IDPS); NIST 800-94; February, 2007.

[2] H. Jadidoleslamy; Designing an Agent-Based Intrusion Detection System for Heterogeneous Wireless Sensor Networks: Robust, Fault Tolerant and Dynamic Reconfigurable; International Journal of Communications, Network and System Sciences (IJCNS), Vol. 4, No. 2, pp 523-543, doi:10.4236/ijcns.2011.48064; August, 2011.

[3] H. Jadidoleslamy; A High-Level Architecture for Intrusion Detection on Heterogeneous Wireless Sensor Networks: Hierarchical, Scalable and Dynamic Reconfigurable; international journal of Wireless Sensor Network (WSN), Vol. 3, No. 7, pp 241-261, doi:10.4236/wsn.2011.37026; July, 2011.

[4] H. Jadidoleslamy; A Hierarchical Intrusion Detection Architecture for Wireless Sensor Networks; International Journal of Network Security & Its Applications (IJNSA), Vol. 3, No. 5, pp 131-154, doi: 10.5121/ijnsa.2011.3511; September, 2011.

[5] G. Maselli, L. Deri and S. Suin; Design and Implementation of an Anomaly Detection System: an Empirical Approach; University of Pisa, Italy; 2002.

[6] V. Chandala, A. Banerjee and V. Kumar; Anomaly Detection: A Survey; ACM Computing Surveys; University of Minnesota; September, 2009.

[7] Ch. Krügel and Th. Toth; A Survey on Intrusion Detection Systems; TU Vienna , Austria; 2000.

[8] P. Prasad; A Dynamically Reconfigurable Intrusion Detection System, Mastee of Science (MSc) Thesis, University of North Carolina State, 2003.

[9] J. Molina and M. Cukier; Evaluating Attack Resiliency for Host Intrusion Detection Systems, Information Assurance and Security Journal (JIAS); 2009.

[10] H. T. Ptacek and N. T. Newsham; Insertion, Evasion and Denial of Service: Eluding Network Intrusion Detection; Secure Networks, Inc.; January, 1998.

[11] J. N. Puketza, K. Zhang, M. Chung, B. Mukherjee and A. R. Olsson; A Methodology for Testing Intrusion Detection Systems; University of California, Davis; September, 1996.

[12] S. Selliah; Mobile Agent-Based Attack Resistant Architecture for Distributed Intrusion Detection System; Master of Science (MSc) Thesis, College of Engineering and Mineral Resources at West Virginia University; 2001.

[13] A. K. Jones and R. S. Sielken; Computer System Intrusion Detection: A Survey; University of Virginia, USA; 2004.

[14] S. Northcutt and J. Novak; Network Intrusion Detection: An Analyst's Handbook; New Riders Publishing; Thousand Oaks, CA, USA; 2002.

[15] S. Zanero and S. M. Savaresi; Unsupervised Learning Techniques for an Intrusion Detection System; ACM Symposium on Applied Computing; 2004.

[16] O. Depren, M. Topallar, E. narim and M. K. Ciliz; An Intelligent Intrusion Detection System for Anomaly and Misuse Detection in Computer Networks; 2005.

[17] R. A. Kemmerer and G. Vigna; Intrusion Detection: A Brief History and Overview; 2002.

Author Biography

H. Jadidoleslamy is a Master of Science of Information Technology (IT). He received his Engineering Degree (Bachelor) in Information Technology (IT) engineering from the University of Sistan and Balouchestan (USB), Iran, in September 2009. He received his Master of Science degree from the University of Guilan, Rasht, Iran, in June 2011. His research interests include Computer Networks (especially Wireless Sensor Network), Information Security (by focusing on Intrusion Detection Systems), and E-Commerce. He may be reached at tanha.hossein@gmail.com or Jadidoleslamy@gmail.com .