A Complete Study on Intrusion Detection, Algorithms and Approaches

M. Savitha Devi[1], **R. Thangaraj**[2]

[1]Research Scholar, Mother Theresa Women's University, Kodaikanal, Tamilnadu, India
[2]Computer Science and Engineering, Bannari Amman Institute of Technology, Sathiyamangalam, Tamilnadu, India

Abstract: ***The world is a global village in which accessing, processing and transformation of information is all the way through network. In the past few years there has been a lot of research work took place in the area of wired and wireless Intruders and how they can be detected through different algorithms. According to the study done the intruders can be detected by door contact, Roller door contact, Panic alarm, Passive Infrared detectors, Dual tech, Break glass sensors, Vibration sensors & safe limpet by means of real time network. The intruders use their own creative techniques to intrude the network in the following ways: Targeted with Acquisition, Information gathering, initial access, Privilege escalation, Covering Tracks. The prime objective of the intruders is to Hacking the password. Then they use the hacked password as the gateway to intrude the network.***

Keywords: Intruders, wired and wireless, Infrastructure, Algorithm, Detectors, Networks.

1. Introduction

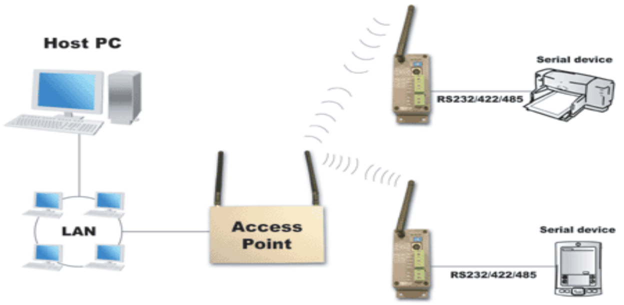
Intruder is a person who attempts to gain unauthorized access to a system. He / She tries to damage the system, disturb the data and tries to hack the system. In general, this person attempts to violate security start from catching the password to access the data then by interfering with system availability, data integrity or data confidentiality. Damage caused by these intruders is the unauthorized modification of system, user files or information and any other system information in network components. Intruders may attack the data by Targeting Acquisition and Information Gathering, Initial Access, Privilege Escalation and Covering Tracks. In this paper we analyze the various approaches followed by the intruders in wired, wireless infrastructure. In addition to this we analyzed the algorithms used for detecting the intruders.

1.1 Network Infrastructure

Based on the Transmission media the network can be classified into Wired and Wireless Transmission.

1.1.1 Wireless infrastructure

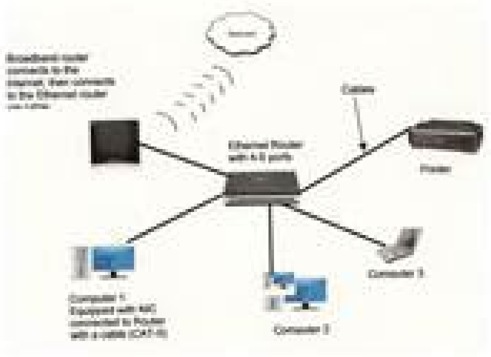
Before configuring a wireless network it is fundamental to mount the wired network as the base network. Setting up an infrastructure mode network requires at least one wireless Access Point (AP). The AP and all local wireless clients must be configured to use the same network name SSID.



The AP is called to the wired network to all wireless clients' access to, for example Internet connections or printers. Additional APs can be joined to this network to increase the reach of infrastructure & support more wireless clients. For example Home network with wireless routes support infrastructure mode automatically as these routers include a built in AP. Compared to the advantages of ad hoc network infrastructure mode networks offer the advantages of scale, centralized security management & improved reach. And also we need to know the disadvantage is the cost to purchase AP network.

1.1.2 Wired Infrastructure

For the wired network we need of network outlets wiring, campus cover network, data centre network and dedicated access to various external networks. In addition to this we need network jacks, copper wiring, fiber cabling, switch infrastructure and connections to the network backbone.


Internet
Broadband router connects to the Internet, then connects to the Ethernet router
Cables
Ethernet Router with 4-8 ports
Printer
Computer 1 Equipped with NIC connected to Router with a cable (CAT-5)
Computer 2
Computer 3

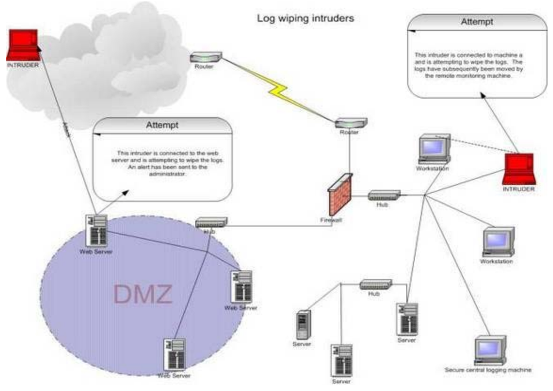
Through these components of network we can access directly the network based resources using wired jacks. However the wireless network is not the perfect alternate to wired network – as a substitute it can reduce the physical components such as edge switches/switch ports and cables/passive.

2. Classes of Intruders

The intruders are classified according to the loop holes for their unauthorized access.

They are;

- Masquerader
- Misfeasor
- Clandestine User


Log wiping intruders
INTRUDER
Router
Attempt
This intruder is connected to machine a and is attempting to wipe the logs. The logs have subsequently been moved by the remote monitoring machine.
Attempt
This intruder is connected to the web server and is attempting to wipe the logs. An alert has been sent to the administrator.
Router
Workstation
INTRUDER
Firewall
Hub
Hub
Web Server
DMZ
Web Server
Web Server
Workstation
Hub
Server
Server
Server
Secure central logging machine

2.1 Masquerader

Unauthorized user who penetrates a system exploiting a legitimate user's account (outside). An individual who is not authorized to use the computer and who penetrates a system's access controls to exploit a legitimate user's account.

2.2 Misfeasor

Legitimate user who makes unauthorized accesses or misuses his privileges (inside). An legitimate user who accesses data, programs, or resources for which such access is not authorized, or who is authorized for such access but misuses his or her privileges.

2.3 Clandestine User

Seizes supervisory control to evade auditing and access controls or suppress audit collection (inside/outside).An individual that seizes supervisory control of the system and uses this control to evade auditing and access controls or to suppress audit collection.

3. Intrusion Detection Systems (IDS)

Intrusion detection systems have become widely recognized as powerful tools for identifying, detecting and deflecting malicious attacks over the network. IDS inspect all inbound and outbound network activities and identifies suspicious pattern that may indicate a network or system attack from someone attempting to break into or compromise the security of a system. The prime classifications of IDS are network based and host based attacks. The network based attack may be either misuse or anomaly based. These attacks are detected from the interconnection of computer systems. The host based attacks are detected only from a single computer system.

3.1 IDS Approaches

IDS can be classified into misuse, anomaly, specification based detections.

3.1.1 Misuse detection

In misuse detection we have analyzed Pattern matching, rule based technique, state based technique and technique based on Data Mining. Pattern Matching reduces the abuse of network with 2.5times faster than the currently used Aho Cora sick algorithm where the pattern matching is done by "partial" or "full" matching is done using data structure CDAWG (Compact Direct Acyclic Word Graph). Rule based detection the first by anomaly it is detected with the analyzation of historical audit records to identify usage patterns and auto generate rules fior them and observe current behavior & match against rules to see if conforms, like statistical anomaly detection does not require prior knowledge of security flaws.

Second is penetration identification uses the expert systems technology with rules identifying known penetration, weakness patterns or suspicious behavior. And compare audit records or state against rules. The rules are generated by expects who interview & codify knowledge of security admin.

Data mining is the tool to detect both misuse and anomaly detection. It classifies the attacker to measure the effectiveness of the system in the area of classification technique. It is easy to estimate the accuracy of the resulting predictive model and to visualize the erroneous predictions. Data Mining and Neural Network plays a vital role.

3.1.2 Anomaly detection

In anomaly detection we analyzed advanced statistical model, Rule based technique, Biological models, learning model. Statistical-Based Systems (SBIDS) can alleviate many of the aforementioned pitfalls of Signature-Based IDS. Statistical-Based systems rely on statistical models such as the Bayes' Theorem, to identify anomalous packets on the network. To identify an anomaly, the system uses data compiled from previous network behavior. The SBIDS identifies and tracks patterns and usage of the network data and then assigns an anomaly score to each packet. Anomalous activity is measured by a number of variables sampled over time and stored in a profile. Based on the anomaly score of a packet, the reporting process will deem it an alert if it is sufficiently anomalous. In Biological model the use of artificial immune system in intrusion detection is an appealing concept for two reasons.

1) The human immune system provides the human body with a high level protection from invading pathogens, in a robust, self-organized and distributed manner.
2) Current techniques used in computer security are not able to cope with the dynamic and increasingly complex nature of computer systems and their security. Genetic algorithm is simulation type system comes under anomaly detection, which exhibit both detection and false positive rate, here we add if then rules that filter the decision of the line as classifies and in that way significantly reduces false positive rate. Improved perception tree (PT) learning model based intrusion detection approach. The binary tree structure of a PT enables the model to divide the intrusion detection problem into sub-problems and solve them in decreased complexity in different tree levels. The expert neural networks (ENNs) embedded in the internal nodes can be simplified by limiting the number of inputs and hidden neurons. Statistical anomaly detection consist two approaches. In first the threshold detection as on count occurrences of specific event over time, and if exceed reasonable value assume intrusion and alone is a crude and Ineffective detector. Second is on profile based on characterize past behavior of users, detect significant deviations from this profile usually its multi parameter.

3.1.3 Specification Based Detection (SBD)

Anomaly detection is capable of detecting novel attacks. However, the use of anomaly detection in practice is hampered by a high rate of false alarms. Specification-based techniques have been shown to produce a low rate of false alarms, but are not as effective as anomaly detection in detecting novel attacks, especially when it comes to network probing and denial-of-service attacks. SBD begins with state-machine specifications of network protocols, and augments these state machines with information about statistics that need to be maintained to detect anomalies. the effectiveness of the approach on the 1999 Lincoln Labs intrusion detection evaluation data, where we are able to detect all of the probing and denial-of-service attacks with a low rate of false alarms.

4. Analyzing Algorithms for Detecting the Intruders

The intruders may be detected by common in public key cryptosystem, digital signature, Fisher Kernel Algorithm and control loop measurement is in progress to detect the intruders and the new trends on the Genetic Algorithm, Bioinformatics, Artificial Immune system etc, among the various algorithms, Fisher Kernel Algorithm is the state of the art technique for detecting the root attacker. Normally, focus on single systems but typically have networked systems.

5. Conclusion

In this paper we present the detailed study on intruders and detection approaches. Also we analyzed the some algorithms that detect and prevent the intruders. Throughout these years many algorithms have been developed to detect intrusions as well as to prohibit hacking. Yet a proper solution has not been reached. Prevention is better than cure. Blocking is the best defense mechanism here. Thus Algorithms have to be developed to Block the intrusions.

6. Acknowledgement

The present work is benefited from the input of, my research guide Dr. R. Thangaraj. I would like to thank him, for his valuable assistance to the undertaking of the study report summarized here. And I thank Mother Teresa Women's University, Kodaikannel for giving the opportunity to present this article. Also I thank our management for their encouragement.

References

[1] J. P. Anderson, "Computer security threat monitoring and surveillance," tech. rep, James P Anderson Co., Fort Washington, Pennsylvania, April 1980
[2] S. Axels son, "Intrusion detection systems: A survey and taxonomy," tech. rep., Department of Computer Engineering, Chalmers University of Technology, 2000
[3] Sundaram, "An introduction to intrusion detection," ACM Crossroads Student Magazine, 1996
[4] J. Baras and M. Rabi, "Intrusion detection with support vector machines and generative models," tech. rep.,

Institute for Systems Research, University of Maryland, 2002

[5] T. Jaakkola and D. Haussler, “Using the Fisher kernel methods to detect remote protein homologies,” in Proceedings of the Seventh International Conference on Intelligent Systems for Molecular Biology, pp. 149–58, 1999

[6] J. C. Burges, “A tutorial on support vector machine for pattern recognition, “in Data Mining and Knowledge Discovery, vol. 2, pp. 121–167, 1998

[7] A survey on intrusion detection approaches, Murali. A Rao. M Computer centre University of Hydrabad-India, 2005-IEEE.org

[8] Network intrusion detection-Mukhergy. B, California Univrsity, Devis. CA, USA Heberlein LT;: Levitt, K.N iEEE1994-ieexplore.ieee.org

[9] www.southwestmicrowave.com

[10] csrc.nist.gov/publications/nistpubs/800-94/SP800-94.pdf

Author Profile

Mrs. M. Savitha Devi has completed MSc (CS)., M. Phli, MCA., She is working as Assistant Professor in Don Bosco College, Dharmapuri, Tamilnadu, India. Now she is doing her research in Network Security in Mother Theresa Women’s University, KodaiKanal, Tamilnadu, India