International Journal of Advances in Engineering Research http://www.ijaer.com
(IJAER) 2012, Vol. No. 4, Issue No. II, August **ISSN: 2231-5152**

INTRUSION DETECTION SYSTEM SECURE TECHNIQUES FOR WLAN USING SNORT CONFIG

Dr. Umesh Sehgal Author 1[†] and Mrs. Shilpa Sharma Author2[††],
Prof. Arni University
M.Tech student Arni University

ABSTRACT

A Wireless Local Area Network (LAN) is a Radio frequency (RF) data communications system. WLANs transmit and receive data Over the Air (OTA) and thus collectively combine data connectivity with ease of mobility. Wireless LANs today provide wireless access to vital network resources such as large, multi-location enterprises, small and medium size enterprises as well as Hospitals, Hotel, Airports and homes. Wireless LANs are being widely recognized as a viable, cost-effective general-purpose solution in providing high-speed real-time access to information.[3]An Intrusion Detection System (IDS) is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. IDSs can be classified as the tools and methods that monitor computer systems and network traffic to identify. Snort is an open source network intrusion detection system (NIDS) created by Martin Roesch. Snort is a packet sniffer that monitors network traffic in real time, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies. In my Research work I will define that how snort file used in WLAN system and which types of problems facing in thissystem.

Keywords: - Snort file, Linux operating system, WLAN Tools

INTRODUCTION TO WIRELESS LOCAL AREA NETWORKS (WLAN) AND INTRUSION DETECTION SYSTEM (IDS) AND SNORTFILE

A Wireless Local Area Network (LAN) is a Radio frequency (RF) data communications system. WLANs transmit and receive data Over the Air (OTA) and thus collectively combine data connectivity with ease of mobility. Wireless LANs today provide wireless access to vital network resources such as large, multi-location enterprises, small and medium size enterprises as well as Hospitals, Hotel, Airports and homes. Wireless LANs are being widely recognized as a viable, cost-effective general-purpose solution in providing high-speed real-time access to information. With a WLAN, users can gain access to shared information without being bound to fixed plug-in point. WLANs can be used to replace wired LANs or simply be used as an extension of a wired infrastructure. Added to the convenience and cost advantages over traditional wired Networks some of the benefitsinclude:

- Mobility
- Installation speed, simplicity andflexibility

- Reducedcost
- Scalability

The most distinctive benefit of WLANs is they are easy to understand and use. This can be attributed to the fact that everything to do with wired LANs, with a few exceptions, also applies to aWLAN.

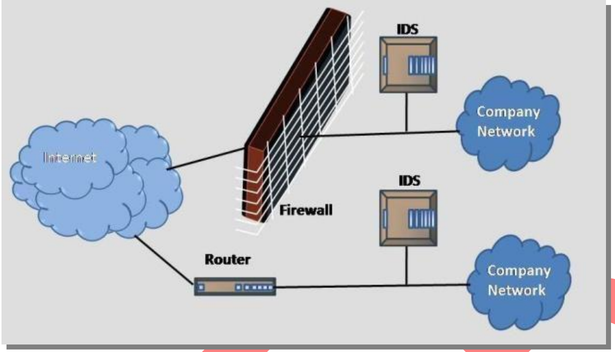

Figure 1.1 IDS Working Environment

INTRUSION DETECTION SYSTEM

An Intrusion Detection System (IDS) is a program that analyzes what happens or has happened during an execution and tries to find indications that the computer has been misused. IDSs can be classified as the tools and methods that monitor computer systems and network traffic to identify and report possible hostile attacks originating from outside the organization and also for system misuse or attacks originating from within theorganization.

The genesis of intrusion detection dates from 1980 commencing with James Anderson's technical report, Computer Security Threat Monitoring and Surveillance for the U.S. Air Force. In 1985, Stanford Research Institute (SRI) was funded by the U.S. Navy to build the initial type of Intrusion Detection Expert System (IDES). Dr. Dorothy Denning assisted in leading this team and a year later published a paper entitled, An Intrusion Detection Model for the 1986 IEEE Symposium on Security and Privacy. This paper is regarded as being the seminal work on intrusiondetection.

Conceptually a wireless IDS is similar to wired IDS but marked differences between wireless and wired-line networks, particularly the "structural and behavioral differences" render current IDS designs unsuitable for wireless networks. Wired intrusion detection systems operate at layer 3 (IP layer) and above of the OSI model whereas WLANs generally refer to the Physical and Data Link layers of the OSI model. A wireless IDS must therefore function at the Data Link layer or even possibly the Physical layer if optimal security is required. There are two main classes of Intrusion:

Misuse (abuse)

Intrusion is well-defined attacks on known weak points of system. All Intrusion which object is to misuse system resources and break it, are fall in this categories. Misuse intruder can be detected by watching for certain action being performed on certain objects and also by doing the pattern matching on audit trail information.

Anomaly

Intrusions are based on observations of deviation from normal system usage pattern. They can be detected by observing significant deviation from the normal behavior. Anomalous Intrusion is harder to detect.

Anomaly or Anomalous may be symptoms of possible Intrusion. Anomaly detection has also been performed through other mechanism such as Neural Network. System's vulnerabilities involve abnormal use of system therefore security violation could be detected from abnormal pattern of system usage.

TYPES OF INTRUSION DETECTION SYSTEM FOR NETWORK BASED

The Five types of IDS are [5]**:-**

Network based IDS

Host based IDS

Hybrid IDS

Network IDS

Signature based IDS

CHALLENGES OF INTRUSION DETECTION

Intrusion detection systems in theory looks like a defense tool which every organization needs. However there are some challenges the organizations face while deploying an intrusion detection system. [1] These are discussed below.

1. IDS technology itself is undergoing a lot of enhancements. It is therefore very important for organizations to clearly define their expectations from the IDS implementation. IDS technology has not reached a level where it does not require human intervention. Of course today's IDS technology offerssomeautomationlikenotifyingtheadministratorincaseofdetectionofamaliciousactivity, shunning the malicious connection for a configurable period of time, dynamically modifying a router's access control list in order to stop a malicious connection etc.

2. The success of an IDS implementation depends to a large extent on how it has been deployed. A lot of plan is required in the design as well as the implementation phase. In most cases, it is desirable to implement a hybrid solution of network based and host based IDS to benefit fromboth.

3. It is important to take care of sensor to manager ratio. There is no thumb rule as such for calculating this ratio. To a large extent it depends upon how many different kinds of traffic is being monitored by each sensor and in what environment. Lot of organizations deploys a 10:1 ratio. Some organizations go for 20:1 and some others15:1.

4. The IDS technology is still reactive rather than proactive. The IDS technology works on attack signatures. Attack signatures are attack patterns of previous attacks. The signature database needs to be updated whenever a different kind of attack is detected and the fix for the same is available. The frequency of signature update varies from vendor to vendor[6].

5. While deploying a network based IDS solution, it is important to keep in mind one very important aspect of the network based IDS in switched environment. Unlike a HUB based network, where a host on one port can see traffic in and out of every other port in the HUB, in a switched network however, traffic in and out of one port cannot be seen by a host in another port, because they are in different collisiondomains.

SNORT FILE CONFIG

Snort is an open source network intrusion detection system (NIDS) created by Martin Roesch. Snort is a packetsniffer that monitors network traffic in real time, scrutinizing each packet closely to detect a dangerous payload or suspicious anomalies.

Snort is based on *libpcap* (for library packet capture), a tool that is widely used in TCP/IP traffic sniffers and analyzers. Through protocol analysis and content searching and matching, Snort detects attack methods, including denial of service,buffer overflow, CGI attacks, stealth port scans, and SMB probes. When suspicious behavior is detected, Snort sends a real-time alert to *syslog*, a separate 'alerts' file, or to a pop-up window.

<u>This script is found as snort-test-auto.sh file [7].</u>

```
#! /bin/sh
#
####################################################################
# You are free to copy and distribute this script under #
# University License until this part is not removed #
# from the script. #
####################################################################
# HOW TO USE #
# #
# Right after installation of Snort, run this script.#
# It is assumed that snort executable is present in the#
# /opt/argus/bin directory and all rules and configuration #
# files are present under /opt/argus/etc/snort directory. #
# if files are in other locations, edit the following location#
# of variables. If you used the installation script provided #
# along with this script, the files will be automatically#
# located in appropriate directories. #
# #
# Note that the script starts and stops Snort by itself and#
# you should make sure that Snort is not running at the time #
# you run this script.#
# #
# It will generate alerts in /tmp/alert file similar #
# to the following: #
# #
# [**] [1:498:3] ATTACK RESPONSES id check returned root [**] #
# [Classification: Potentially Bad Traffic] [Priority: 2] #
# 08/31-15:56:48.188882 255.255.255.255 -> 192.168.1.111 #
# ICMP TTL: 150 TOS: 0x0 ID:0 IpLen: 20 DgmLen: 84#
# Type: 0 Code: 0 ID: 45596 Seq: 1024 ECHO REPLY#
# #
# These alerts are displayed at the end of the script. #
#####################################################################
#

PREFIX=/opt/snort
SNORT=$PREFIX/bin/snort
SNORT_CONFIG=$PREFIX/etc/snort.conf
LOG_DIR=/tmp
ALERT_FILE=$LOG_DIR/alert
ALERT_FILE_OLD=$LOG_DIR/alert.old
ADDRESS="255.255.255.255"

clear

echo "#####################################################################"
echo "# Script to test Snort Installation#"
echo "# Written By #"
echo "##"
echo "# Umesh sehgal#"
echo "#umeshsehgal@sify.com#"
echo "# University#"
echo "# http://www.umeshsehgal.com #"
echo "######################################################################"
echo

echo
echo "######################################################################"
echo "The script generates three alerts in file/tmp/alert"
echo "Each alert should start with message like the following:"
echo
echo " \"ATTACK RESPONSES id check returned root\" "
echo "######################################################################"
echo

if [! -d$LOG_DIR]
then
echo "Creating log directory ..."
mkdir$LOG_DIR

if [$? -ne 0]
then
echo "Directory $LOGDIR creation failed"
echo "Aborting..."
exit 1
fi
fi

if [-f$ALERT_FILE]
then
mv -f $ALERT_FILE $ALERT_FILE_OLD

if [ $? -ne 0 ]
then
echo "Can't rename old alerts file."
echo "Aborting ..."
```

```
exit 1
fi
fi

if [ ! -f $SNORT]
then
echo "Snort executable file $SNORT does not exist."
echo "Aborting..."
exit 1
fi

if [! -f$SNORT_CONFIG]
then
echo "Snort configuration file $SNORT_CONFIG does not exist."
echo "Aborting..."
exit 1
fi
104
if [ ! -x $SNORT]
then
echo "Snort file $SNORT is not executable."
echo "Aborting..."
exit 1
fi
111
echo "Starting Snort..."
$SNORT -c $SNORT_CONFIG -D -l /tmp2>/dev/null
114
if [ $? -ne 0 ]
then
echo "Snort startup failed."
echo "Aborting ..."
exit 1
fi
121
echo
echo "Now generatingalerts."

ping -i 0.3 -n -r -b $ADDRESS -p "7569643d3028726f6f74290a" -c3 2>/dev/ null >/dev/null
```

```

if [ $? -ne 0 ]
then
echo "Alerting generation failed."
echo "Aborting ..."
exit 1
else
echo
echo "Alert generation complete"
echo
fi

sleep 2

tail -n18 $ALERT_FILE 2>/dev/null | grep "ATTACK RESPONSES id check" >/dev/null

if [ $? -ne 0 ]
then
echo "Snort test failed."
echo "Aborting ..."
exit 1
fi

echo "Stopping Snort ..."
pkill snort >/dev/null 2>&1

if [ $? -ne 0 ]
then
echo "Snort stopping failed."
echo "Aborting ..."
exit 1
fi

echo
echo "Done. Snort installation is working properly"
echo
```

As you may have noted, this scripts creates alert file in the /tmp directory which is used to find out if the alert creation was successful. When you run the script and everything is working fine, you will see the followingoutput:

```
############################################################
# Script to test Snort Installation #
# Written By #
# #
# Umesh sehgal #
# umeshsehgal@sify.com #
# University #
# http://www.umeshsehgal.com #
############################################################
############################################################
The script generates three alerts in file /tmp/alert
Each alert should start with message like the following:
"ATTACK RESPONSES id check returned root"
###########################################################
Starting Snort...
Now generating alerts.
Alert generation complete
Stopping Snort...
Done. Snort installation is working properly.
```

This script does a number of things when you run it. First of all it sets values of some variables using lines from line number 36 to 42. After setting these variables, the script goes through the followingsteps:

- Lines 66 to 77 are used to check for the presence of $LOG_DIR directory. The variable LOG_DIR defined in line 39 shows that this directory is /tmp. If the directory does not exist, the script createsit.
- Lines 79 to 89 are used to check for the presence of $ALERT_FILE, which is /tmp/alert. If the file exists, the scripts rename it as/tmp/alert.old.
- Lines91to96areusedtocheckforthepresenceofSnortbinaryfile$SNORT,whichis /opt/snort/bin/snort. If the file is not present, execution is stopped.
- Lines98to103areusedtocheckforthepresenceof$SNORT_CONFIGfile,whichis /opt/snort/etc/snort.conf. If the file does not exist, execution is stopped.
- Lines 105 to 110 make sure that the Snort binary file is indeedexecutable.
- Line number 113 starts Snort.
- Lines 115 to 120 check that Snort was started successfully.
- Line 125 generates alerts as described in the previous section. These alerts are sent to broadcast address.
- Lines 127 to 136 are used to make sure that the alert generation process wassuccessful.

• Line 140 checks the last eighteen lines of the alert file to verify that alerts were generated and log entries are createdsuccessfully.
• Lines 142 to 147 display an error message if the test in line 140failed.
• Line 150 stopsSnort.
• Line 160 displays a message showing that the test generation process wassuccessful.[77]

CONCLUSION

In the light of the objectives proposed for this study, the following methodology will be adapted to study and analysis of the Intrusion Detection Techniques for Wireless LAN.In addition, a number of lesser classifications are possible based on the location of sensors, the nature of events reviewed, the execution timing of monitors, and the correlation of results between resolver units. To study the various Vulnerabilities and attacks on WLANs and their detection using the Intrusion Detection methodologies. There are two major categories of Intrusion Detection methodologies i.e. Misuse Detection and AnomalyDetection.

Misuse Detection: (Also called signature detection or detection by appearance) Misuse Detection attempts to match observed behavior against known intrusive behavioral patterns. A variety of techniques have been used to model and recognize attack patterns in Wireless Local Area Networks. A common element between these techniques is that they attempt to represent the essential nature of a known attack in such a way that variations on that attack can be distinguished from normal behavior. Anything that is not recognized as an attack is accepted as legalbehavior.
A human studies an attack and identifies the characteristics (e.g., behavior and/or content) that distinguish it from normal data or traffic. The combination of these characteristics is known as the signature, and it becomes part of a database of attack signatures. When the IDS encounters data matching the signature, it raises an alarm. Signature systems represent the vast majority of installed IDSs; they are important. All commercial anti-virus products make use of signature detection, as does the network IDS snort.Snort uses rules stored in text files that can be modified by a text editor. Rules are grouped in categories. The Rules belonging to each category are stored in separate files. These files are than included in a main configuration file called snort.
In most of the Intrusion Detection systems, the dominant form of misuse detection used is signature analysis, due to the simplicity of representation and efficiency of implementation possible. A limitation of this approach is that the signature set requires constant review as new attacks develop. In addition, as more attacks and attack variations become available, the number of rules against which an event stream must be checked becomes larger – leading to scaling difficulties.
Anomaly Detection: (also called **detection by behavior**) Anomaly Detection attempts to model the expected behavior of objects (users, processes, network hosts and the like). Any action that does not correspond to expectations is considered suspicious. The strength of these methods lies in their ability to differentiate normal user behavior, anomalous acceptable behavior, and intrusivebehavior.

[2] Anomaly-based IDSs assume that intrusion attempts are rare and that they have different characteristics from normalbehavior

REFERENCES

[1] S. Capkun, L. Buttyan, and J. Hubaux, "*Sector: Secure Tracking of Node Encounters in Multi-hop Wireless Networks. Proc. of the ACM Workshop on Security of Ad Hoc and Sensor Networks,"* 2003.

[2] H. Deng, W. Li, Agrawal, D.P., "*Routing security in wireless ad hoc networks,"* Cincinnati Univ.,OH,USA;IEEECommunicationsMagazine,Oct.2002,Volume:40,page(s):70-75, ISSN: 0163-6804

[3] J.-P. HuBaux, L. Buttyan, and S. Capkun., "*The quest for security immobile ad hoc network,"* In Proc. ACM MOBICOM, Oct.2001.

[4] H. Hsieh and R. Sivakumar, "*Transport OverWireless Networks,"* Handbook of Wireless Networksand Mobile Computing, Edited by Ivan Stojmenovic. John Wiley and Sons, Inc., 2002.

[5] Y. Hu, A. Perrig, and D. Johnson, "*Ariadne: A Secure On-Demand Routing for Ad Hoc Networks,"* Proc. of MobiCom 2002, Atlanta, 2002.

[6] Y. Hu, A. Perrig, and D. Johnson, *"Packet Leashes: A Defense AgainstWormhole Attacks inWirelessAd Hoc Networks,"* Proc. of IEEE INFORCOM, 2002.

[7] IEEE Std. 802.11i/D30, *"Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Specification for Enhanced Security,"*2002.