International Journal of Modern Communication Technologies & Research (IJMCTR)
ISSN: 2321-0850, Volume-2, Issue-11, November 2014

Traffic Analysis of Intrusion Detection Systems

Ahmed Abdelrahaman Eltom Amin Babiker A. Nabi Mustafa

***Abstract*— Securing information system is one of major concerns today specially for sensitive work including confidential or financial information. Although with the huge evolution of enhancing the network security in the past few years hackers have been developing their attack methods making their intrusion detection a difficult mission. Despite of the importance of the firewall device as the guards of the front gate of the system network security intrusion detection system has been proving themselves as a key players in the defense plan in the past few years achieving amazing performance and accuracy to only for detecting sophisticated attacks but giving the advantage of auditing the system security in order to enhance it and making the intrusion as hard as possible. Traffic analysis is essential in that job since the capabilities traffic analysis provide to only help detecting new types of attacks especially but also with proper configuration can help detection attack that has no known patterns or signatures especially with the fact that intruders always develop, evaluate, and upgrade their ways to gain unauthorized access to information system resources. Finally the detailed and vital information about the attack details always help filling the security holes and fixing the system vulnerabilities and enhancing the information system security.**

***Index Terms*— Securing information system, IDS, network investigation**

I. IDS INTRODUCTION

Intrusion can be defined by discovering and responding to incidents and malicious activities targeting the system and compromising information systems resources.

The main function of IDS is to detect unauthorized access to resources and their misusage or any attempts of system intrusion and generate alarm for any action compromising information systems security.

II. IDS TYPES

There are three major types of intrusion detection systems , these three types were classified Based on the sources of the audit information used by each intrusion detection system as a host-based IDS or Network – based IDS or Hybrid IDS .

A. Host Based IDS

Host-based IDS watch over the activity on an individual computer such as a single desktop or server reporting any suspicious activity or incident compromising system security . Due to the fact the HIDS access the local O.S and file structure and it as more platform specific, it has the ability to determine the user and processes concerning any event compromising system security.

B. Network based IDS

Network-based IDS is concerned with the events and activities in the network, monitoring the network activities and the traffic passing through a network in order to compare that traffic with a database of so called signatures known to be associated with malicious activity and the traffic passing through system and scanning packets for patterns indicating any suspicious activity.

C. Hybrid IDS:

Hybrid IDS combines several technologies of both Network based IDS and Host based IDS in a complex way to achieve better discovery of intrusion attempts providing better efficiency and proven as very good method to detect and respond unknown and new intrusion attempts .

III. IDS TECHNIQUES:

These techniques are implemented whether it was Host-based IDS or Network-based IDS.

A. Anomaly Detecting

Anomaly detection depend on defining a profile of normal usage through modeling the normal behavior of the network as a noise characterization and anything significantly deviates from that noise will be considered as suspicious activity or an attempt of intrusion .

The detection of Novell attack is a great advantage of this method along with the ability to detect new threats and unknown attacks the configuration a major and complex issue to decide what can trigger the alarm.

B. Misuse Detection

Depending on the characteristics of known attacks and system vulnerabilities to detect intrusion. They refer to attack following well defined patterns; if a pattern is matched they indicate an intrusion process. Despite the ease of deployment and update there are some disadvantage like need of update and the lack of the ability to detect unknown or new attacks .

C. Target Monitoring

Its main concern is about discovering the modification of a specific file lacking the need of constant observation and mentoring and put in mind an important fact that this action actually takes place after the intrusion process making it more like a corrective action.

D. Stealth Probes

Targeting intruders operating over a long a long period of time, which is a common hacking behavior, time is an important factor especially if the target is well protected and

Manuscript received November 09, 2014.
Ahmed Abdelrahaman Eltom Amin Babiker A. Nabi Mustafa, Neelain University Faculty of Engineering, Department of electronic Engineering

need a lot of intrusion attempt to grant unauthorized access to system resources.
Stealth probes collect a massive amount of data through a considerable long time and inspecting any suspicious behavior.

IV. Traffic Analysis

IDS traffic plays an important role as function that helps achieving the appropriate defense plan. IDS Traffic analysis is vital when performing network investigation due the importance of the information that the IDS can provide regarding any security incident compromising system security and the time of the incident , the source host , the targeted destination and an advance ability to classify the severity of the incidents , so depending on these vital information the appropriate procedures and corrective actions would be taken to immune the security system and make the intrusion process as hard as possible .

A lot of work is done through the sensors accomplishing important tasks like monitoring network traffic and generation alarms in any case of suspicious activity whether it came from inside the network like a legitimate user abusing recourses or from outside the network as an intrusion attempt, helping to take the proper corrective action and save the records for more detailed later investigation in order to fix vulnerabilities and security hole and enhance system security.

V. Port Forwarding

Port forwarding is used to accomplish incoming TCP or UDP connection to distant device. For a connection between a source and a destination port forwarding will allow an intermediate host securing the connection and to forbidding direct connection between source and destination as it resides at the middle specially for cases which the end point is a server which should be secured and its information should remain confidential and at the same time connected and functioning properly by in a secure fashion.

IDS proper configuration of port forwarding will accomplish secure communication between two endpoints listening to ports and forwarding arriving packet to.

VI. Simulation

In this simulation three devices were implemented , the first one is the intruder host using a software of Acunetix Web Vulnerability Scanner in order to attack a victim –the second device -which is an application in a web server over a VMware environment . the third device is the IDS using Smoothec IDS for its functionality and reliability .

In the first step (before implementing IDS) the outsider device can reach the web server directly through its IP address, the next step an IDS was implemented to perform the mission of port forwarding in order to keep confidentiality of server addressing though IDS port listening and fort forwarding restricting the connection through IDS and keeping the web server connected securely.

A proper configuration of Smoothtech IDS is an essential procedure to achieve the desired successful fort forwarding, the next step will be launching attack and observe network traffic analysis in order to catch the attack and generate the alarms regarding the launched attack on the web server in statistical and graphical form .

Fig 1 shows web server configuration using VMware environment (the victim)

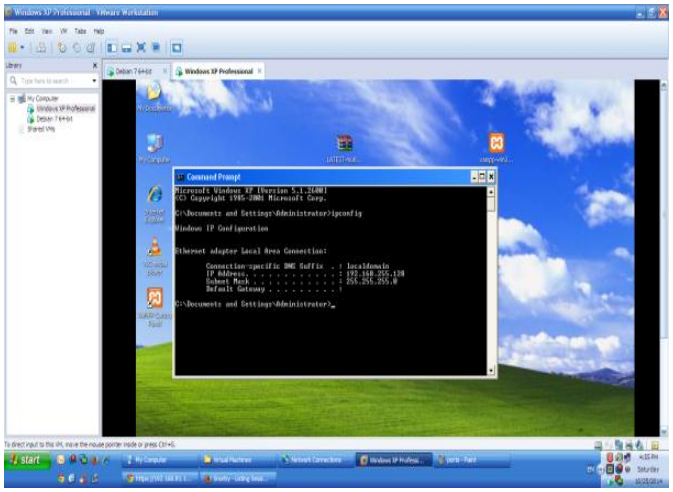


Fig 2 shows web server database

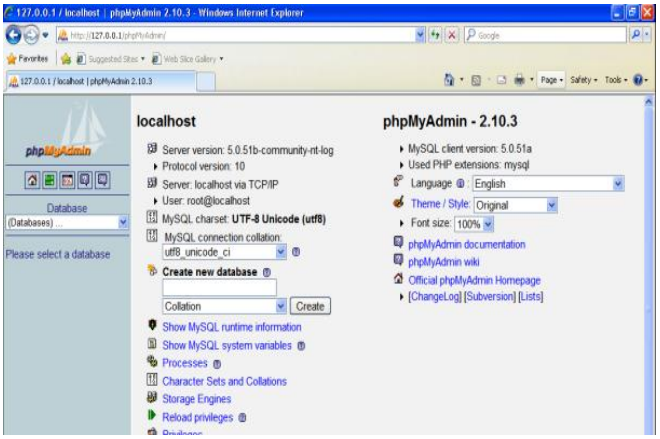


Fig 3 shows application on the web server and displays clearly its IP address.

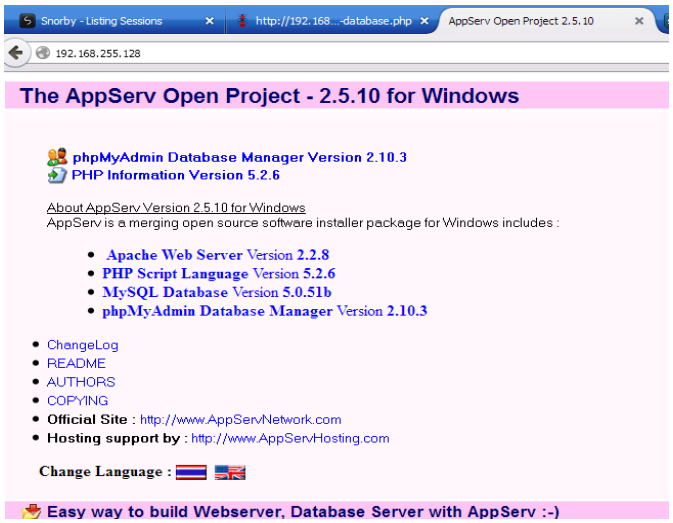


Fig 4 shows logs before attack displaying one activity as physical logging

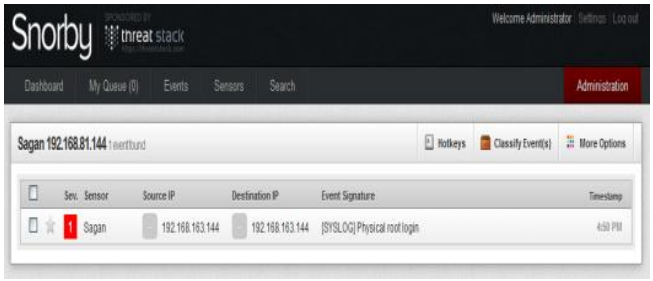


Figure 5 , show Smoothtech IDS IDS ports,

```
[warnble some interfaces ... (warning).
[ ok ] Reconfiguring network interfaces...done.
root@smoothsec64:~# ifconfig |grep addr
eth0      Link encap:Ethernet  HWaddr 00:0c:29:50:7d:7e
          inet addr:192.168.81.144  Bcast:192.168.81.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe50:7d7e/64 Scope:Link
eth1      Link encap:Ethernet  HWaddr 00:0c:29:50:7d:88
          inet addr:192.168.255.130  Bcast:192.168.255.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe50:7d88/64 Scope:Link
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
root@smoothsec64:~# netstat -ant
Active Internet connections (servers and established)
Proto Recv-Q Send-Q Local Address           Foreign Address         State
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          0.0.0.0:*               LISTEN
tcp        0      0 127.0.0.1:3306          127.0.0.1:59335         ESTABLISHED
tcp        0      0 127.0.0.1:59336         127.0.0.1:3306          ESTABLISHED
tcp        0      0 127.0.0.1:59332         127.0.0.1:3306          ESTABLISHED
tcp        0      0 127.0.0.1:59335         127.0.0.1:3306          ESTABLISHED
tcp        0      0 127.0.0.1:3306          127.0.0.1:59336         ESTABLISHED
tcp        0      0 127.0.0.1:3306          127.0.0.1:59332         ESTABLISHED
tcp6       0      0 :::22                   :::*                    LISTEN
tcp6       0      0 :::443                  :::*                    LISTEN
root@smoothsec64:~# _
```

Figure 6, 7, 8 show Smoothtech IDS configuration .

```
          collisions:0 txqueuelen:1000
          RX bytes:3950 (3.8 KiB)  TX bytes:468 (468.0 B)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:167 errors:0 dropped:0 overruns:0 frame:0
          TX packets:167 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:17095 (17.4 KiB)  TX bytes:17895 (17.4 KiB)

root@smoothsec64:~# ifconfig |grep eth
eth0      Link encap:Ethernet  HWaddr 00:0c:29:50:7d:7e
eth1      Link encap:Ethernet  HWaddr 00:0c:29:50:7d:88
root@smoothsec64:~# ifconfig |grep addr
eth0      Link encap:Ethernet  HWaddr 00:0c:29:50:7d:7e
          inet addr:192.168.163.144  Bcast:192.168.163.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe50:7d7e/64 Scope:Link
eth1      Link encap:Ethernet  HWaddr 00:0c:29:50:7d:88
          inet addr:192.168.211.130  Bcast:192.168.211.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe50:7d88/64 Scope:Link
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
root@smoothsec64:~# _
```

```
  GNU nano 2.2.6                File: /root/fw-fin.bak

# Generated by iptables-save v1.4.14 on Sat Oct 25 16:54:52 2014
*nat
:PREROUTING ACCEPT [9:1155]
:INPUT ACCEPT [9:1155]
:OUTPUT ACCEPT [9:644]
:POSTROUTING ACCEPT [14:904]
-A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168$
-A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168$
COMMIT
# Completed on Sat Oct 25 16:54:52 2014
# Generated by iptables-save v1.4.14 on Sat Oct 25 16:54:52 2014
*filter
:INPUT ACCEPT [41:7150]
:FORWARD ACCEPT [23:5853]
:OUTPUT ACCEPT [38:2791]
-A FORWARD -d 192.168.255.128/32 -i eth0 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Sat Oct 25 16:54:52 2014

                [ Read 18 lines ]
^G Get Help  ^O WriteOut  ^R Read File ^Y Prev Page ^K Cut Text  ^C Cur Pos
^X Exit      ^J Justify   ^W Where Is  ^V Next Page ^U UnCut Text^T To Spell
```

```
  GNU nano 2.2.6                File: /root/fw-fin.bak

# Generated by iptables-save v1.4.14 on Sat Oct 25 16:54:52 2014
*nat
:PREROUTING ACCEPT [9:1155]
:INPUT ACCEPT [9:1155]
:OUTPUT ACCEPT [9:644]
:POSTROUTING ACCEPT [14:904]
-A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168$
-A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j DNAT --to-destination 192.168$
COMMIT
# Completed on Sat Oct 25 16:54:52 2014
# Generated by iptables-save v1.4.14 on Sat Oct 25 16:54:52 2014
*filter
:INPUT ACCEPT [41:7150]
:FORWARD ACCEPT [23:5853]
:OUTPUT ACCEPT [38:2791]
-A FORWARD -d 192.168.255.128/32 -i eth0 -p tcp -m tcp --dport 80 -j ACCEPT
COMMIT
# Completed on Sat Oct 25 16:54:52 2014

                [ Read 18 lines ]
root@smoothsec64:~# nano /proc/sys/net/ipv4/conf/eth0/forwarding _
```

Figure 9 show Smoothtech IDS and configuration to implement of port forwarding successfully.

```
root@smoothsec64:/#
root@smoothsec64:/#
root@smoothsec64:/#
root@smoothsec64:/#
root@smoothsec64:/# /etc/init.d/ssh restart
[ ok ] Restarting OpenBSD Secure Shell server: sshd.
root@smoothsec64:/# iptables -t nat -A PREROUTING -p tcp -i eth0 --dport 80 -j D
NAT --to-destination 192.168.255.128:80
root@smoothsec64:/# iptables -A FORWARD -p tcp -d 192.168.255.128 --dport 80 -m
state --state NEW,ESTABLISHED,RELATED -j ACCEPT
root@smoothsec64:/# iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
ACCEPT     tcp  --  anywhere             192.168.255.128      tcp dpt:http state
 NEW,RELATED,ESTABLISHED

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
root@smoothsec64:/# _
```

Fig 10 displaying the application requested by outsider host with the IP address of the IDS instead of the IP address of the server as a result of using port forwarding as configured in the past steps.

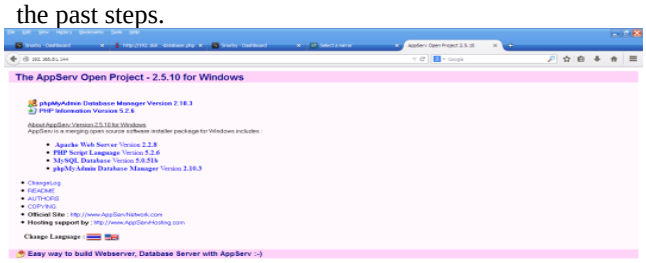


Fig 11 shows the attack launched on the web server through IP address .

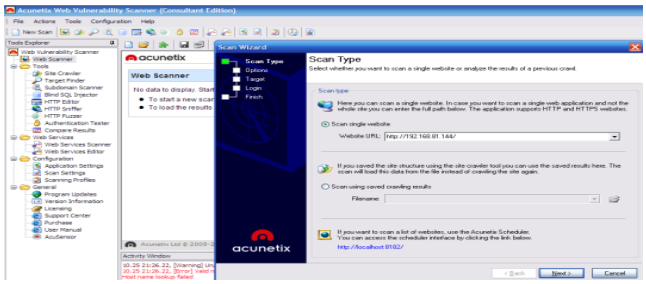


Fig 12 shows the attack launched on the web server and its applications .

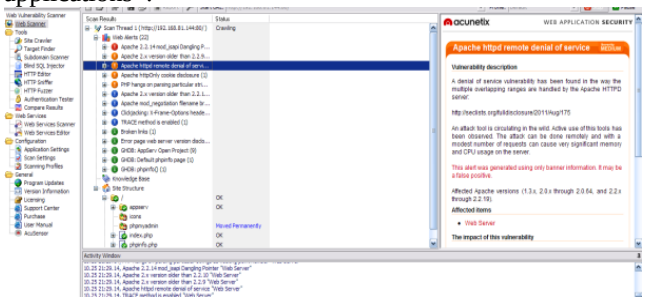
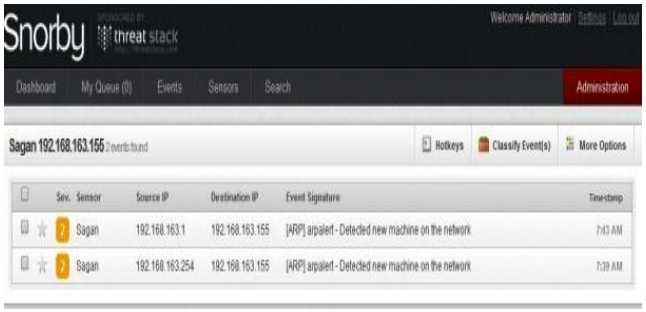
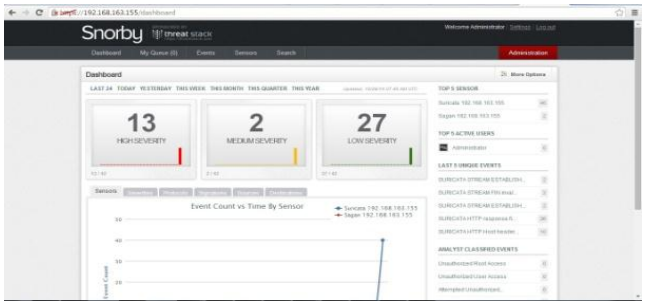
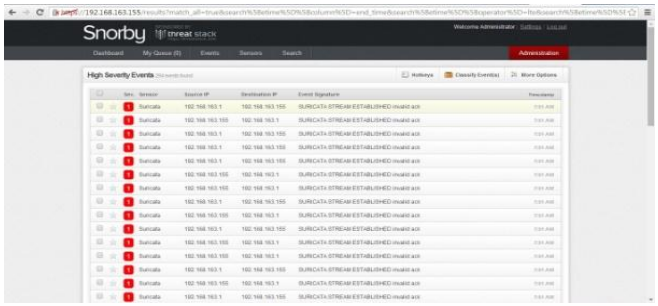
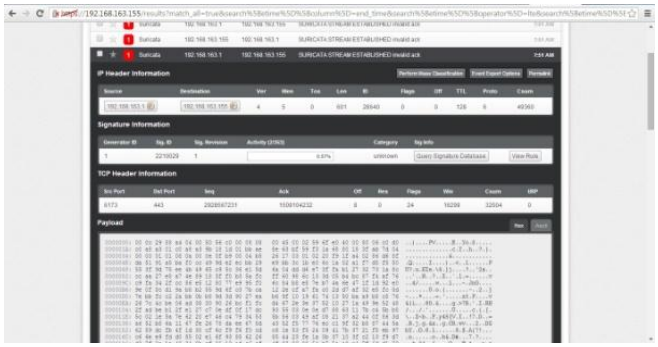


Fig 13 , 14 , 15 , 16 and 17 show the alarms generated due the attack launched on the server classified by the IDS due to the severity of the attack.









VII. Recommednations

Enhancing the security of information system is a major target of using IDS Through live surveillance and network monitoring in order to analyze network traffic reporting any suspicious incident with an alert giving all needed details concerning security incident.

Traffic analysis can definitely improve network security along with the usage of signature matching providing more detection efficiency, whether these analysis took place monitoring the characteristic of a single host or being done over the entire network is essential to identify any activity compromising network security Traffic analysis can also provide high level of intrusion detection on new attacks which a great deal facing IDS techniques due to their usage of signatures making it hard to be discovered, giving the traffic analysis the advantage of the detection of these unknown or new attacks.

By providing detailed information such as attack course, destination, time and generating alerts depending on attack severity IDS traffic analysis provide great assistance and guidance to security analysts, helping them to take the right procedures and the proper actions to fix network vulnerabilities and to secure network resources and protect it from intrusion.

VIII. Conclusion

IDS if perfectly deployed and well configured will contribute greatly in discovering attacks and suspicious activities compromising networks security, intrusion detection systems play a major goal not only reporting suspicious activities and generate alarms in case of any intrusion attempt bust also provide the ability to audit the system security in order to provide much secure environments of information systems.

References

[1] Traffic Analysis: From Stateful Firewall to Network Intrusion Detection System Fanglu Guo Tzi-cker Chiueh Computer Science Department Stony Brook University, NY 11794

[2] Next Generation Intrusion Detection Systems (IDS) By Dr. Fengmin Gong, Chief Scientist, McAfee Network Security Technologies Group

[3] Importance of Intrusion Detection System (IDS) Asmaa Shaker Ashoor (Department computer science, Pune University)