ISSN 2395-1621

Infrastructure Security Using IDS, IPS and Honeypot

#1K. D. Yesugade, #2Medankar Sanika Avinash, #3Nagarkar Sanika Satish,
#4Shah Charmi Sandeep, #5Surabhi Malav

[1]kiran_yesugade@yahoo.com
[2]sanika23feb@gmail.com
[3]sanikanagarkar95@gmail.com
[4]charmishah1994@gmail.com
[5]bittudhakad@gmail.com

#12345Computer Department, Bharati Vidyapeeth's College of Engineering for Women, Pune-43, India

ABSTRACT

Various exploits are being used to compromise the network. These exploits are capable of breaking into any secured networks. Thus, to secure the network we are combining features, functions and methodology of IDS, IPS and Honeypot and making Intrusion Detection System more effective, accurate and responsive. Honeypot are mirrored servers which appear as actual servers for attackers and maintains logs of intruding activities. IDS detects the attack, and IPS takes actions as configured. Intrusion detection system (IDS) monitors the data packets and looks for intrusion, when such event occurs an alarm will get triggered resulting analysis of captured packets and corrective action taken by IPS if necessary. This alert will activate IPS which will take preventive actions depending on the type of attack. Featuring log analysis and capturing into our proposed system will enable security expert to investigate such events sophisticatedly.

ARTICLE INFO

Article History

Received :28th April 2016

Received in revised form :

30th April 2016

Accepted : 2nd May 2016

Published online :

4th May 2016

Keywords – IDS, IPS & Honeypot

I. INTRODUCTION

In present era, many attackers attack the network so as to gain the information or damage the system. There are many existing standalone systems to detect and prevent the network from attacks like Firewall, Intrusion-Detection-System(IDS) and Intrusion-prevention-System(IPS).To increase the security, we are combining the features of IDS,IPS and Honeypot. The system analyses and tracks the behavior of the attacker by monitoring the network and capturing the log. The propose system has the sophisticated framework for investigating intruders as well as intrusion events.

II.COMPONENT

1. Intrusion Detection System
   - ➢ Capture
   - ➢ Decode
   - ➢ Preprocessor
   - ➢ Detect
2. Intrusion Prevention System
3. Honeypot
4. Web page with connectivity (Interface)
   - ➢ Webpage
   - ➢ Database of Authentication Information
   - ➢ Trigger Software

III. DESCRIPTION

1. Intrusion Detection System:

This module will detect if any attacker tries to intrude the host. It consists of following sub-modules:

a. Capture:

The incoming packets from the network are captured and verified using the length of the packet.Once the packet is captured the module will scan the packetand store the information like size of packet, size of header, type of flag related to file system, etc in the local buffer for decoding the packet.As the task of decoding the packet is done the memory allocated to the pervious packet gets free and is reallocated for new packet.

b. Decode:

The captured packet will get decoded by calculating payload length, fragmentation andchecksum type. There are many decoding rules with unique sequence Id (Sid) and group id (Gid), defined to alert and drop the packet.

c. Preprocessor:

Proposed system uses different types of preprocessors like Normalize, Performance, Session, Arpspoof, Fragmentation, Httpinspect preprocessor etc. Depending on the decoding information of the packet the preprocessor will extract essential information by using its preprocessor rules.

d. Detection Engine:

This software uses SIGNATURE based pattern matching algorithm to detect the vulnerability of the packet. The information that is extracted from preprocessor is compared with signature database to analysis the behavior of packet.

2. Intrusion Prevention System:

As IDS will alert the intrusion, the IPS will be checking for false-positive of the alert generated. According to the result, the action will be performed as configured.

3. Honeypot:

Honeypot are mirrored servers which appear as actual servers for attackers.In proposed system, Honeypot will analysis and capture the logs of all the incoming packets to the host through network.

4. Web page with connectivity (Interface):

a. Web page:

The web page will display gateway page for authenticated users and signup for new user registration purpose. There will be only one administrator who would have the configuration and maintenance access to the software and other users can only access statistical data.

b. Database of Authenticated Information:

The database will store username, password and all other details related to detection and prevention of an event or intrusion. Later on this information will be required for authenticating the user as well as to feed dashboard with statistical representation of captured, detected and handled event or intrusion. It will also store the login and logout timestamp of the registered user along with the role for further validation and auditing.

c. Trigger Software:

There will be different access rights are maintained for administrator and other users. Administrator will be having access to configure as well as to manage the software. Using sophisticated framework various commands for configuring and maintaining the software will be fired manually or automatically on command line at backend and result will be displayed on web frontend. Other users can only view the statistical data and not having rights to modify the same.

IV. ARCHITECTURE OF PROPOSED SYSTEM

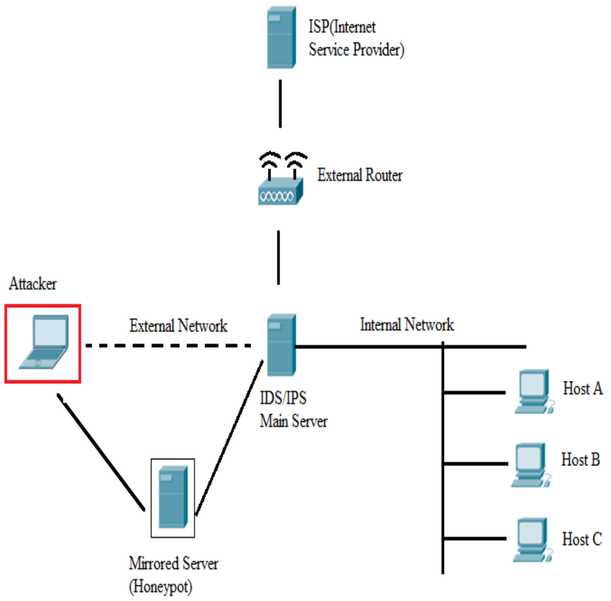
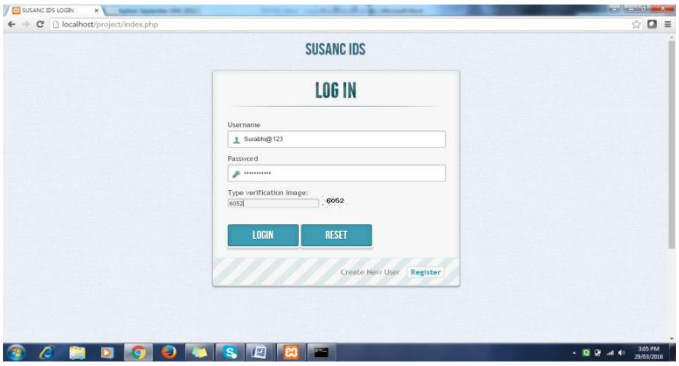


Fig.1. Architecture of proposed system

The architecture of proposed system consists of main server and its own mirrored image as Honeypot. IDS and IPS are eventually deployed on the gateway for analyzing incoming network traffic. The main server will be connected to ISP (Internet Service Provider) through external router. All incoming packets from external network will be first arriving on the mirror server i.e. Honeypot to a capture the logs. These packets will be passed to IDS, IPS to detect intrusion and to take preventive measures. If alert is generated the action will be performed by IPS as configured and if it is innocent packet then it will be passed to main server. The log of all intruding packets will be captured at IDS and same will be send to security administrator for further investigation.

V.RESULT

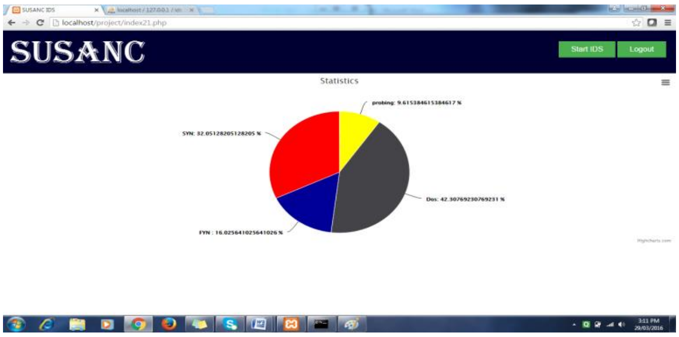
1. User login page : Only authenticated users can able to login the SUSANC IDS.



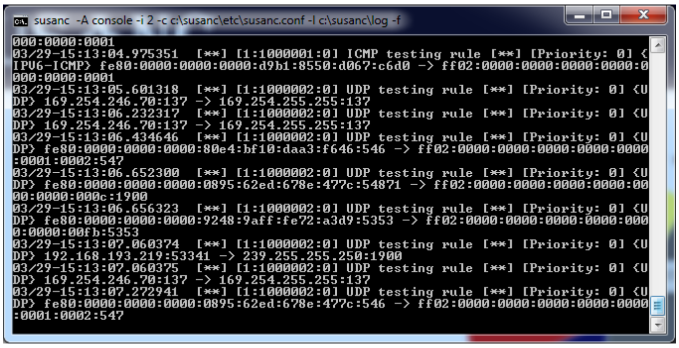
Username
Surabhi@123
Password
••••••••••••
Type verification image:
6052 6052

2. Start IDS : Only administrator has access rights to start IDS and able to watch the result of every user by statistical data in form of pie charts and tables. User has rights to analysis and watch it's own IDS results in form of pie charts as shown

.

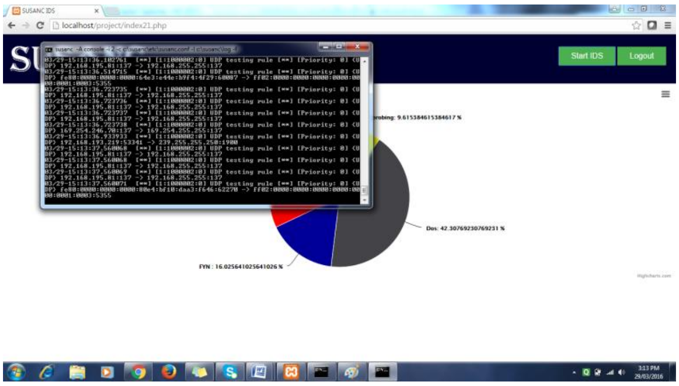


3. Technical result of IDS :

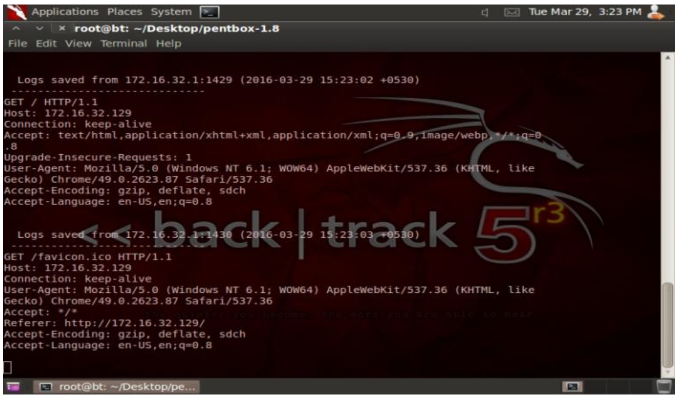

susanc -A console -i 2 -c c:\susanc\etc\susanc.conf -l c:\susanc\log -f

```
000:0000:0001
03/29-15:13:04.975351  [**] [1:1000001:0] ICMP testing rule [**] [Priority: 0] {
IPV6-ICMP} fe80:0000:0000:0000:d9b1:8550:d067:c6d0 -> ff02:0000:0000:0000:0000:0
000:0000:0001
03/29-15:13:05.601318  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] {U
DP} 169.254.246.70:137 -> 169.254.255.255:137
03/29-15:13:06.232317  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] {U
DP} 169.254.246.70:137 -> 169.254.255.255:137
03/29-15:13:06.434646  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:80e4:bf10:daa3:f646:546 -> ff02:0000:0000:0000:0000:0000
:0001:0002:547
03/29-15:13:06.652300  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:0895:62ed:678e:477c:54871 -> ff02:0000:0000:0000:0000:00
00:0000:000c:1900
03/29-15:13:06.656323  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:9248:9aff:fe72:a3d9:5353 -> ff02:0000:0000:0000:0000:000
0:0000:00fb:5353
03/29-15:13:07.060374  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] {U
DP} 192.168.193.219:53341 -> 239.255.255.250:1900
03/29-15:13:07.060375  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] {U
DP} 169.254.246.70:137 -> 169.254.255.255:137
03/29-15:13:07.272941  [**] [1:1000002:0] UDP testing rule [**] [Priority: 0] {U
DP} fe80:0000:0000:0000:0895:62ed:678e:477c:546 -> ff02:0000:0000:0000:0000:0000
:0001:0002:547
```

4. Dynamic update of result :


SUSANC IDS
localhost/project/index21.php
Start IDS
Logout
probing: 9.615384615384617 %
Dos: 42.30769230769231 %
FYN : 16.025641025641026 %
Highcharts.com
3:13 PM
29/03/2016

5. Honeypot results :


Applications Places System
Tue Mar 29, 3:23 PM
root@bt: ~/Desktop/pentbox-1.8
File Edit View Terminal Help
<< back | track 5 r3
root@bt: ~/Desktop/pe...

```
  Logs saved from 172.16.32.1:1429 (2016-03-29 15:23:02 +0530)
 -----------------------------
GET / HTTP/1.1
Host: 172.16.32.129
Connection: keep-alive
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,*/*;q=0
.8
Upgrade-Insecure-Requests: 1
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/49.0.2623.87 Safari/537.36
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8


  Logs saved from 172.16.32.1:1430 (2016-03-29 15:23:03 +0530)
 -----------------------------
GET /favicon.ico HTTP/1.1
Host: 172.16.32.129
Connection: keep-alive
User-Agent: Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/49.0.2623.87 Safari/537.36
Accept: */*
Referer: http://172.16.32.129/
Accept-Encoding: gzip, deflate, sdch
Accept-Language: en-US,en;q=0.8
```

VI. TEST CASES

Test id	**Test case**	**Expected Result**	**Actual Result**	**Pass/Fail**
1	If user enter correct username and password	User Authentication and login	User login	Pass
2	If user enter incorrect username and correct password	Message display incorrect username or password	Message display incorrect username or Password	Pass
3	If user enter incorrect password and correct username	Message display incorrect username or password	Message display incorrect username or password	Pass
4	Registration	a. If register, then registration successful message. b. If not registered successfully, then message should be shown.	a. If register, then registration successful. b. If not registered successfully the message shown to fill details properly.	Pass
5	SQL injection to username and password	Login failed.	Login failed.	Pass
6	Appropriate access rights to particular user. For example: To view detailed log and to start application is allowed only for administrator.	Data visible to logged in users according to his access rights.	Data visible to logged in users according to his access rights.	Pass

7	Start application	Command fired on command prompt which is then executed and application starts running.	Command fired on command prompt which is then executed and application starts running.	Pass
8	Detect the packets coming to the host	Packets with its IP address are displayed on command prompt.	Packets with its IP address are displayed on command prompt.	Pass
9	Log detected packet in file	A log file is generated which will log the details of detected packet.	A log file is generated which will log the details of detected packet.	Pass
10	Logs stored by Honeypot.	Logs stored successfully by Honeypot	Logs stored successfully by Honeypot	Pass.

VII. CONCLUSION

The existing software systems are not able to properly identify intrusion as they are overburdened with other security controls and rolls. To overcome the same drawback, proposed system has introduced two highlighting modules:
1) Mirrored module
2) Detection Module
The proposed system is more stable and precise on operating system platform also on detection ratio.Inherited use of two modules, proposed system has increased its efficiency in detection and low response time with high ROI. Along with this the proposed system have introduced a sophisticated and interactive user friendly interface to configure and monitor the software and also to analyze and log the behavior of the intruder and intruding events. Also the Honeypot module gives ability to proposed system to successfully mirror deployed platform and attract attackers for further RnD.

ACKNOWLEDGEMENT

The authors would like to thank Mr. AmeyTambe Director (Information Security) for his help. This work was sponsored by Intelligent Quotient System Pvt. Ltd. (R & D) Information Security Department.

REFERENCES

[1] "An implementation of intrusion detection system using genetic algorithm"
Mohammad Sazzadul Hoque1, Md. Abdul Mukit2 and Md. Abu Naser Bikas3 1Student, Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh sazzad@ymail.com 2Student, Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh mukit.sust027@gmail.com 3Lecturer, Department of Computer Science and Engineering, Shahjalal University of Science and Technology, Sylhet, Bangladesh bikasbd@yahoo.com

[2] International Journal of Advanced Research in Computer Science and Software Engineering Research Paper www.ijarcsse.com
"Study and Comparison of Virus Detection Techniques"
Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad, Vinayak N Malavade

[3] "Honeypot back-propagation for mitigating spoofing distributed Denial-of-Service attacks" SherifKhattaba, Rami Melhema, Daniel Mosséa, TaiebZnatia,Department of Computer Science, University of Pittsburgh, PA 15260, USA Department of Information Science and Telecommunications, University of Pittsburgh, PA 15260, USA

[4] "A Dynamic Honeypot Design for Intrusion Detection", IyadKuwatly, MalekSraj, Zaid Al Masri American University of Beirut Department of Electrical and Computer Engineering P.O.Box 11-0236 / 3623 Riad El-Solh / Beirut 1107 2020 Lebanon Emails {imk01, mas44, zoa01} @aub.edu.lb

[5] "A Technique for Detecting New Attacks in Low-Interaction Honeypot Traffic", S. Almotairi, A. Clark, G. Mohay, and J. Zimmermann Information Security Institute, Queensland University of Technology Brisbane, Queensland, Australia {s.almotairi, a.clark, g.mohay, j.zimmerm}@isi.qut.edu.au

[6]"Distributed Denial of Service Prevention Techniques", B. B. Gupta, Student Member, IEEE, R. C. Joshi, and ManojMisra, Member, IEEE

[7] NavneetKambow et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 5 (5) , 2014, 6098-6101, "Honeypots: The Need of Network Security" Navneet ,Kambow, LavleenKaurPassi , Deparment of Computer Science, Shaheed Bhagat Singh State Technical Capmus, Ferozepur, India- Department of Computer Science ,AryabhattaInstitte of Engineering and Technology, Barnala, India

[8] "HoneyDroid - Creating a Smartphone Honeypot"
Collin Mulliner, Steffen Liebergeld, and Matthias Lange TechnischeUniversita¨t Berlin / Deutsche Telekom Laboratories {collin,steffen,mlange}@sec.t-labs.tu-berlin.de

[9] "Denial-of-Service Attacks in Bloom-Filter-Based Forwarding"
MarkkuAntikainen, Tuomas Aura, and MikkoSärelä

[10] “Honeypots: Concepts, Approaches, and Challenges” IyatitiMokube Computer Science Armstrong Atlantic State University Savannah, GA 31419 im3871@students.armstrong.edu

[11] “Security Enforcement and Query Forwarding While Preserving System Wide Privacy” Prof. K. D. Yesugade, Ms.S. Bhosale, Ms. Sayali P Gavhane, Department of computer engineering, Bharati Vidyapeeth’s College Of Engineering for Women, Pune, India. International Journal of Computer Science and Mobile Computing (IJCSMC) vol 3, issue 12, December 2014, page 245-253, ISSN 2320-088X