Minor Project

Smart Intrusion Detection System

Prepared by:
18BCE056 Dhruvi Shah
18BCE064 Pranav Gajjar

Contents

- Overview of the Project
- System prerequisites
- Tools and technologies that will be used

What is an Intrusion Detection System (IDS) ?

What is an Intrusion Detection System ?

An intrusion detection system (IDS) is a device or software application that monitors a network for malicious activity or policy violations.

They are used to detect anomalies with the aim of catching hackers before they do real damage to a network.

Alerts when any activity is found.

Overview for our Project

Our aim is to build a Smart Intrusion Detection System that makes it easier for the end user to manage their security and take measures accordingly. We will incorporate various features like:

- Front-end helps administrators to analyze the system in real-time
- Ease of use for performing various IDS-related activities
- In case of any malicious activity, notifies administrator via email and SMS
- Analytical Dashboard with Real time threat analysis Chart
- A solution tip for the user to help secure their network.

System Prerequisites

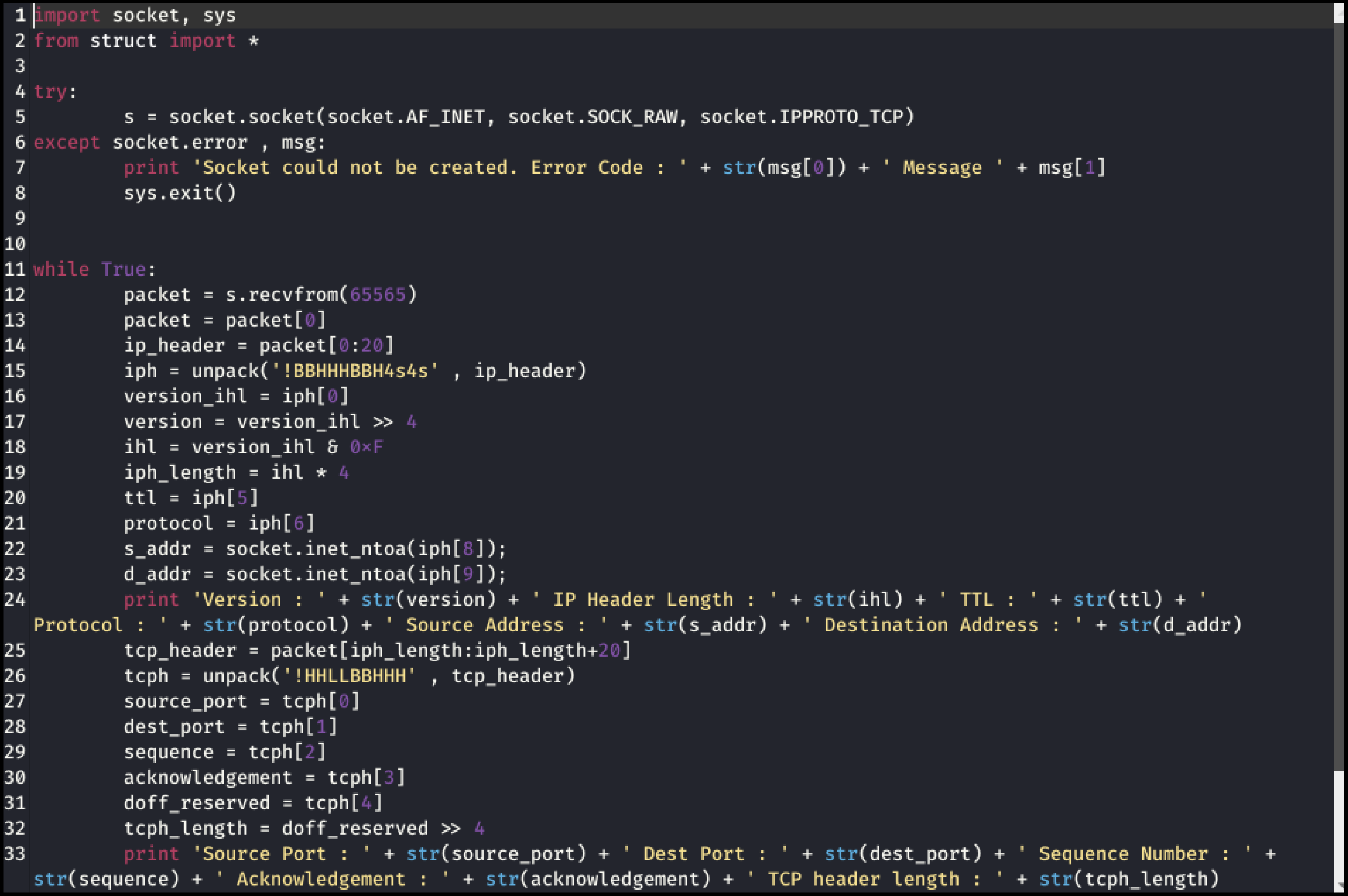
- Any Operating System like
  - Windows,
  - Linux,
  - Mac OS
- Should contain basic programs like
  - Python 3,
  - React,
  - MySQL etc.

Tools and Technologies

- Python3
- React for Front End
- MySQL for Database Management
- Machine Learning for Adaptive and enhance detection
- Network Protocols
- Pre defined Datasets for Training ML Model
- Snort
- Twilio API

What we have done so far?

- Creating python scripts to capture packets.
- Capturing different TCP, UDP, ICMP packets.
- Exploring new and efficient techniques to detect intrusion.
- Exploring existing tools which are available for IDS and trying to integrate that to create efficient IDS system.

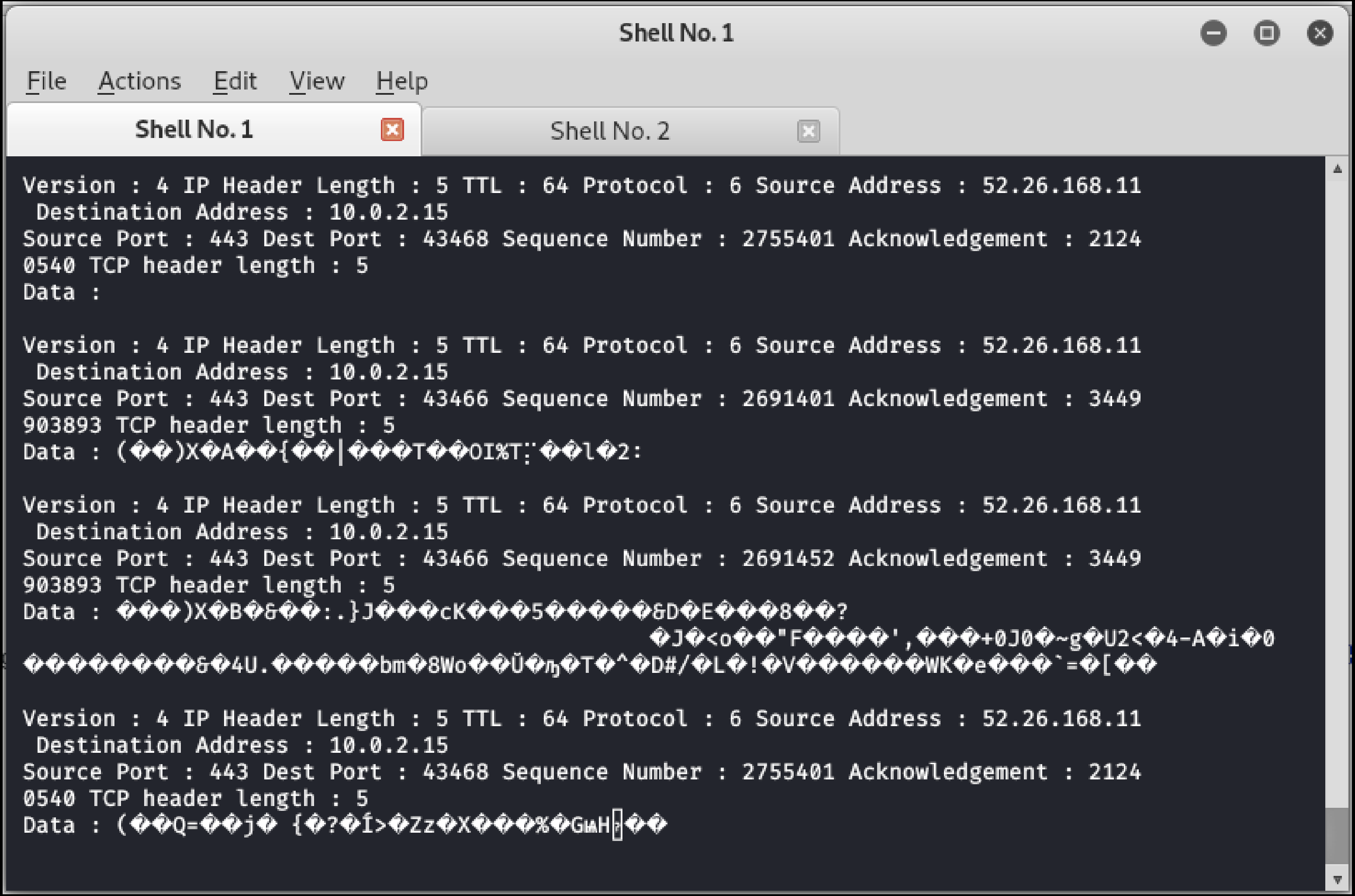


```python
import socket, sys
from struct import *

try:
        s = socket.socket(socket.AF_INET, socket.SOCK_RAW, socket.IPPROTO_TCP)
except socket.error , msg:
        print 'Socket could not be created. Error Code : ' + str(msg[0]) + ' Message ' + msg[1]
        sys.exit()


while True:
        packet = s.recvfrom(65565)
        packet = packet[0]
        ip_header = packet[0:20]
        iph = unpack('!BBHHHBBH4s4s' , ip_header)
        version_ihl = iph[0]
        version = version_ihl >> 4
        ihl = version_ihl & 0xF
        iph_length = ihl * 4
        ttl = iph[5]
        protocol = iph[6]
        s_addr = socket.inet_ntoa(iph[8]);
        d_addr = socket.inet_ntoa(iph[9]);
        print 'Version : ' + str(version) + ' IP Header Length : ' + str(ihl) + ' TTL : ' + str(ttl) + ' Protocol : ' + str(protocol) + ' Source Address : ' + str(s_addr) + ' Destination Address : ' + str(d_addr)
        tcp_header = packet[iph_length:iph_length+20]
        tcph = unpack('!HHLLBBHHH' , tcp_header)
        source_port = tcph[0]
        dest_port = tcph[1]
        sequence = tcph[2]
        acknowledgement = tcph[3]
        doff_reserved = tcph[4]
        tcph_length = doff_reserved >> 4
        print 'Source Port : ' + str(source_port) + ' Dest Port : ' + str(dest_port) + ' Sequence Number : ' + str(sequence) + ' Acknowledgement : ' + str(acknowledgement) + ' TCP header length : ' + str(tcph_length)
```

Writing Scripts for Packer Capture



```
Version : 4 IP Header Length : 5 TTL : 64 Protocol : 6 Source Address : 52.26.168.11
 Destination Address : 10.0.2.15
Source Port : 443 Dest Port : 43468 Sequence Number : 2755401 Acknowledgement : 2124
0540 TCP header length : 5
Data :

Version : 4 IP Header Length : 5 TTL : 64 Protocol : 6 Source Address : 52.26.168.11
 Destination Address : 10.0.2.15
Source Port : 443 Dest Port : 43466 Sequence Number : 2691401 Acknowledgement : 3449
903893 TCP header length : 5
Data : (��)X�A��{��|���T��OI%T:¨��l�2:

Version : 4 IP Header Length : 5 TTL : 64 Protocol : 6 Source Address : 52.26.168.11
 Destination Address : 10.0.2.15
Source Port : 443 Dest Port : 43466 Sequence Number : 2691452 Acknowledgement : 3449
903893 TCP header length : 5
Data : ���)X�B�&��:.}J���cK���5������&D�E����8��?
                                               �J�<o��"F�����',���+0J0�~g�U2<�4-A�i�0
���������&�4U.������bm�8Wo��Ŭ�ŋ�T�^�D#/�L�!�V�������WK�e����`=�[��

Version : 4 IP Header Length : 5 TTL : 64 Protocol : 6 Source Address : 52.26.168.11
 Destination Address : 10.0.2.15
Source Port : 443 Dest Port : 43468 Sequence Number : 2755401 Acknowledgement : 2124
0540 TCP header length : 5
Data : (���Q=���j� {�?�Í>�Zz�X����%�GաH▯��
```

Screenshot of our script Capturing Packet

THANKyou