ISSN (Online) : 2348 - 2001

International Refereed Journal of Reviews and Research

Volume 9 Issue 1 January 2021

International Manuscript ID : 23482001V9I1012021-153

(Approved and Registered with Govt. of India)

Forensic Analysis of Networks and Programming Patterns Using Python

Ekta Srivastava
Research Scholar
Shri Venkateshwara University
Gajraula, Uttar Pradesh

Dr. Vishal Bhatnagar
Assistant Professor
Shri Venkateshwara University
Gajraula, Uttar Pradesh

Abstract

Network monitoring and digital forensic is one of the prominent areas in the domain of cyber security. A number of software products and tools are available in the technology market which are used to guards the network infrastructure and confidential data against cyber threats and attacks. From long time, the monitoring of servers and forensic analysis of network infrastructure is done using packet capturing (PCAP) tools and intrusion detection systems (IDS). These activities are performed using PCAP and IDS tools available in the market which includes open source software as well as commercial products. As far as the fame and usage of the software suites is concerned, the open source market is getting popularity because of the scope of customization and organization specific personalization the software products.

Keywords : Cyber Security, Forensic Applications, Python Programming

Introduction

Cyber security is important because government, military, corporate, financial, and medical organizations collect, process, and store unprecedented amounts of data on computers and other devices. A significant portion of that data can be sensitive information [1], whether that be intellectual property, financial data, personal information, or other types of data for which unauthorized access or exposure could have negative consequences. Organizations transmit sensitive data across networks and to other devices in the course of doing businesses, and cyber security describes the discipline dedicated to protecting that information and the systems used to process or store it. As the volume and sophistication of cyber attacks grow, companies and organizations, especially those that are tasked with safeguarding information relating to national security, health, or financial records, need to take steps to protect their sensitive business and personnel information. As early as March 2013, the nation’s top intelligence officials cautioned that cyber attacks and digital spying are the top threat to national security, eclipsing even terrorism [2, 3].

In the field of computer network administration, pcap is an application programming interface (API) for capturing network traffic. While the name is an abbreviation of packet capture, that is not the API's proper name [4]. Unix-like systems implement pcap in the libpcap library; for Windows, there is a port of libpcap named WinPcap that is no longer supported or developed, and a port named Npcap for Windows 7 and later that is still supported.

Monitoring software may use libpcap, WinPcap, or Npcap to capture network packets travelling over a computer network and, in newer versions, to transmit packets on a network at the link layer, and to get a list of network interfaces for possible use with libpcap, WinPcap, or Npcap [5].

The pcap API is written in C, so other languages such as Java, .NET languages, and scripting languages generally use a wrapper; no such wrappers are provided by libpcap or WinPcap itself. C++ programs may link directly to the C API or use an object-oriented wrapper [6].

libpcap/WinPcap based software includes

- Tcpdump
- WinDump
- ngrep
- Wireshark
- Snort
- Nmap
- L0phtCrack
- XLink Kai
- iftop
- EtherApe
- Bro IDS
- URL Snooper
- Kismet
- Bit-Twist
- Pirni
- NetSim
- Firesheep
- Suricata
- WhatPulse
- Xplico
- Scapy

Intrusion Detection Systems which are used widely in the network establishments for cyber security and threat analysis includes

- AIDE
- Samhain
- OpenDLP
- OSSEC
- Security Onion
- OpenWIPS-NG
- ACARM-ng
- Fail2ban
- OSSEC HIDS
- Bro NIDS
- Prelude Hybrid IDS
- Samhain
- Snort
- Suricata

Despite a number of tools available for packet capturing and monitoring, still the professional programmers are interested to use their own software developed by coding and scripting [7]. Using self developed and programmed code, there is lots of flexibility in using and personalizing the tool. Many organizations which are sensitive in terms of security, confidentiality and integrity, they do not use any third party software. Rather they develop their own tool using efficient and highly effective programming languages which includes Python, Java, PERL, PHP and many others [8].

As far as the strength and features are there, Python is one of the widely used languages for writing the special scripts that can be used for packet capturing, classification and machine learning [9].

It should be cited that a number of network monitoring and logging software are developed in Python. Shinken and Zenoss are common tools used for watching the hosts, network data collection, alerts and messaging and include lots of active and passive monitoring methods. Currently Shinken is the open source framework used for monitoring and based on Python. This software can perform a large set of operations related to the digital forensics and logging [10, 11].

Some of the features in Shinken include the monitoring of -

- MySQL databases
- Asterisk servers
- DHCP servers
- Active Directory
- Oracle databases
- IIS Server
- Linux Machines and Devices
- Routers
- Switches
- Network Nodes
- Linux Systems using SNMP and Local Agent
- Microsoft Exchange
- SQL database engines
- Windows Machines
- Printers and Fax
- Public Services and Privileges
- VMware hosts and machines
- Windows Nodes using NSClient++
- Windows Nodes using WMI

PYTHON SCRIPTS AND LIBRARIES FOR NETWORK FORENSIC

EDDIE

EDDIE is one of the tools built with Python for network monitoring, logging, high security credential management, and performance evaluation.

The features of the EDDIE Tool includes -

- System monitoring checks
- Filesystem Checking
- HTTP checks
- POP3 tests
- SNMP queries
- RADIUS authentication tests
- Processes Monitoring
- System load
- Network configuration
- Ping checks
- Customized TCP port checks.
- Watching files for changes
- Scanning of logfiles

pypcap (Packet Capture Library) - PyPCAP is a python wrapper with object-oriented integration for libpcap.

pypcap can be installed easily -

```
$ pip install pypcap
```

Using Python PCAP, the packets can be captured with a few lines of code

```
>>> import pcap
>>>   for ts, pkt in pcap.pcap():
        print ts, `pkt`
```

LinkChecker

Using LinkChecker library in Python, the recursive and deep checking of the server pages can be done. Using LinkChecker, the site crawling is made easy with features of integrating the regular expressions and filtering. The output can be generated in multiple formats including HTML, XML, CSV, SQL or simply the sitemap graph.

WebScraping

Python is used by the researchers and practitioners for collecting the live data for research and development. For example, we can fetch the live records of stock market, price of any product from E-Commerce websites. Such data collected is the foundation of BigData Analytics. If a researcher is doing research on big data analysis, the live data can be fetched using Python Script and then it can be processed based on the research objectives.

Here is the code snippet to fetch the live stock exchange data from the website timesofindia.com using Python

```
from bs4 import BeautifulSoup
import urllib.request
from time import sleep
from datetime import datetime
def getnews():
    url = "http://timesofindia.indiatimes.com/business"
    req = urllib.request.urlopen(url)
    page = req.read()
    scraping = BeautifulSoup(page)
    price = scraping.findAll("span",attrs={"class":"red14px"})[0].text
    return price
with open("bseindex.out","w") as f:
    for x in range(2,100):
        sNow = datetime.now().strftime("%I:%M:%S%p")
        f.write("{0}, {1} \n ".format(sNow, getnews()))
        sleep(1)
```

Fetching Live Data from Social Media

In the same way, the twitter live feeds can be fetched using Python APIs. Using twitter developer account, the new app can be created and then the Python Script is mapped with the Twitter App

```
from tweepy import Stream
from tweepy import OAuthHandler
from tweepy.streaming import StreamListener

#setting up the keys
consumer_key = 'XXXXXXXXXXXXXXXXXXXX'
consumer_secret        = ' XXXXXXXXXXXXXXXXXXXX '
access_token           = ' XXXXXXXXXXXXXXXXXXXX '
access_secret          = ' XXXXXXXXXXXXXXXXXXXX '

class TweetListener(StreamListener):
    # A listener handles tweets are the received from the stream.
    #This is a basic listener that just prints received tweets to standard output

    def on_data(self, data):
        print data
        return True

    def on_error(self, status):
        print status

#printing all the tweets to the standard output
auth = OAuthHandler(consumer_key, consumer_secret)
auth.set_access_token(access_token, access_secret)
```

```
stream = Stream(auth, TweetListener())
stream.filter(track=['research'])
```

Using this Python Code, the keyword ‘research’ is extracted from Twitter and the output is sent in JSON Format. JSON (JavaScript Object Notation) File Format is a special format that is used by many NoSQL and unstructured data handling engines. Once the JSON is obtained, after that using Refine Tool or any other tool the intelligence can be created and further predictions can be done.

Conclusion

There is huge scope of research and development using Python scripts and specialized APIs for assorted applications including cyber security, data mining, Internet of Things, cloud simulation, grid implementation and many others. Python is one of the effective programming languages that can process and handle any type of data stream.

References

[1] "IANA record of application for MIME type application/vnd.tcpdump.pcap".

[2] McCanne, Steve. "libpcap: An Architecture and Optimization Methodology for Packet Capture" (PDF). December 27, 2013.

[3] "TCPDUMP/LIBPCAP public repository". December 27, 2013.

[4] "WinPcap News". November 6, 2017.

[5] "WinPcap internals". December 27, 2013.

[6] "Riverbed Expands Further Into The Application-Aware Network Performance Management Market with the Acquisition of CACE Technologies" (Press release). Riverbed Technology. 2010-10-21. Archived from the original on 2013-03-08. 2010-10-21.

[7] "Win10Pcap: WinPcap for Windows 10".

[8] Win10Pcap: WinPcap for Windows 10 (NDIS 6.x driver model): SoftEtherVPN/Win10Pcap, SoftEther VPN Project, 2019-12-31, 2020-01-09

[9] Kevin J. Connolly (2003). Law of Internet Security and Privacy. Aspen Publishers. p. 131. ISBN 978-0-7355-4273-0.

[10] "Network Segment Definition". www.linfo.org. January 14, 2016.

[11] "Packet Sniffing". www.networxsecurity.org. October 12, 2019.