Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 79 (2016) 781 – 784

Procedia Computer Science

7th International Conference on Communication, Computing and Virtualization 2016

DDoS Attack Analyzer: Using JPCAP and WinCap

Pankaj Shinde[a] ,Thaksen J. Parvat[b],

Computer Engineering
Sinhgad Institute of Technology, Lonavala
S.P.Pune University, (M.S) INDIA- 410401
[a]pankaj.mb.shinde@gmail.com, [b]pthaksen.sit@sinhgad.edu

Abstract

Nowadays, Computers and their Networks leads to being complex and diverse systems that communicate with speed and flexible. There is always room for sophisticated and highly specific network/Packet analyzing tool. Network traffic monitoring is not as straight as they written in theory but also leads to many trends changing changes. Tools are also able to provide the statics and graphic representation of risk and reports. While developing the tools, it is highly important to understand the intrusion attacks conditions, network protocols and systems behavior, the intension of user and user conformability. We are proposing the network traffic detection and analyzing tools that mainly focus on the DDoS attack. We are using JPCAP packet capturing library with WinCap for Detection and analysis of network traffic on a prime target of DDoS Attack.

Peer-review under responsibility of the Organizing Committee of ICCCV 2016

Keywords: Sniffer; Packet Capture; Jpcap; WinCap; Intrusion Detection; DDoS Attacks.

Packet Analyzer or sniffer for the collecting the data [request and response]which traverse the network among the various network devices as well end user systems.[11] These sniffers work on the different protocol data. As data streams flow across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications[3][2]. While analyzing, sniffers encountered packages that should not be part of data or which additionally holding in data for of intrusion, viruses, misbehaviors or any policy violation. Those include network statistics tools, intrusion detection, port knocking daemons, password sniffers, ARP poisoners, trace routers, etc.[1].

* Corresponding author. Tel.: +91 989-001-2124;
E-mail address: Pankaj.mb.shinde@gmail.com

Peer-review under responsibility of the Organizing Committee of ICCCV 2016
doi:10.1016/j.procs.2016.03.103

A Distributed Denial of Service (DDoS) attack is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources.[10][5] They target a wide variety of significant resources, from banks to news websites and present a major challenge to making sure people can publish and access relevant information. [4].
This paper is arranged in section I as an Understanding of WinCap and Jpcap, Section II for proposed algorithm and Section III Experimental Details, followed by Section IV presents results of experiments.

1. WinCap and Jpcap

Windows Packet Capture provides the facility to access low-level network in Windows operating environment. It can transmit network traffic along with protocol stack and process. It allows kernel-level packet filtering. It is windows network utility drivers, which offers low-level network access along with control of kernel of doing it. It been used commercially for many systems as well it also having UNIX version as libcap. As the tools protocol analyzer, traffic analyzer, network traffic monitor, intrusion detection system and mainly in sniffers are integrated by WinCap.[13][14][6]

Java based open source library that implemented in C and Java for access network traffic like capturing and sending over the network. It is mainly used in Java based application along with the WinCap [Windows]/ libcap[UNIX]. Jpcapcaptures Ethernet, TCP, and UDP, IPv4, IPv6, ICMP, ARP/RARP packets, etc. It has been tested on Microsoft Windows (98/2000/XP/Vista), Linux (Fedora, Ubuntu), Mac OS X (Darwin), FreeBSD, and Solaris [9] with successful results.[12]

Jpcap is the collection of java class and interfaces. This collection hides unnecessary details from the user of network traffic capturing, sending across a network, abstracting in protocols. Jpcap is internally handling by many network class and interfaces along with their binding. Java native interface plays a vital role in the binding of all collection of class as interfaces together as the component.[8]

Jpcap on the Java side is made up of several Java classes. These classes peer with native C structures provided by libpcap.[7] So for example, when user retrieves an instance of Pcap object, the object contains a memory pointer to a C pcap_t structure.[7] When any non-static method call on the Java class, will use the stored reference to the native C structure to execute the requested function. Same thing applies to all other structures such as Pcap, If and the remaining. They are all peered and retain a memory reference to their corresponding C structure.[7] For safety purposes and Java protections, the reader is not allowed to access these C structures directly, and all the corresponding *libpcap* library functions are provided as Java methods. Therefore, the is a very close relationship between each Java object and its corresponding native C structure, the same applies to *libpcap* functions and their corresponding Java methods.

We are using the WinCap to get traffic into the system to analyze and to detect particular DDoS. At the functional level, jpcap will analyze the packets by checking out threshold value that likely decides the income packages are suspicious, or they be normal traffic.

2. Proposed Algorithm

1. Obtain and open the network.

```
NetworkInterface[] device = jpcapCaptor.getDeviceList();
captor=JNetPcapCaptor.openDevice(device[index], snaplen, promics, timeout);
        where snaplen= Maximum number of bytes,
        promics= mode to get traffic,
        timeout=timeout values in milliseconds.
```

2. Set the traffic type wireless or Ethernet.

It will allow the user to monitor traffic type either of wireless or Ethernet LAN.

3. Set threshold or it will calculate by default.

4. Check incoming traffic

Verify the Source IP and Destination IP,
Push protocol wise stack and Create thread,
Check Source IP and Destination IP with Port
Check IP: Port same found in stack queue
Push for DDoS calculation.

5. Calculate DDoS Probability and Show report

6. Generate analyzer report based on the detection alerts and notification to the user.

3. Experiments and Results

We use KDD We are in network with internet shared in WAN and LAN via a wireless and wired network. The experiment performed on the Windows-7 64 bit with i3 processor. For Testing, we have deployed dedicated web server that host local website. Attacker system with ping program that execute with targeting host system. We executed both attacker and host programmed and analyzed system for DDoS attack detection.
As we focused on the DDoS attack, we have analysis our proposed solution on the LAN where multiple host is connected and targeting to a particular host for the flooding, pinging continuously.
We can detect the attack as per below generally comes under the DDoS attack:

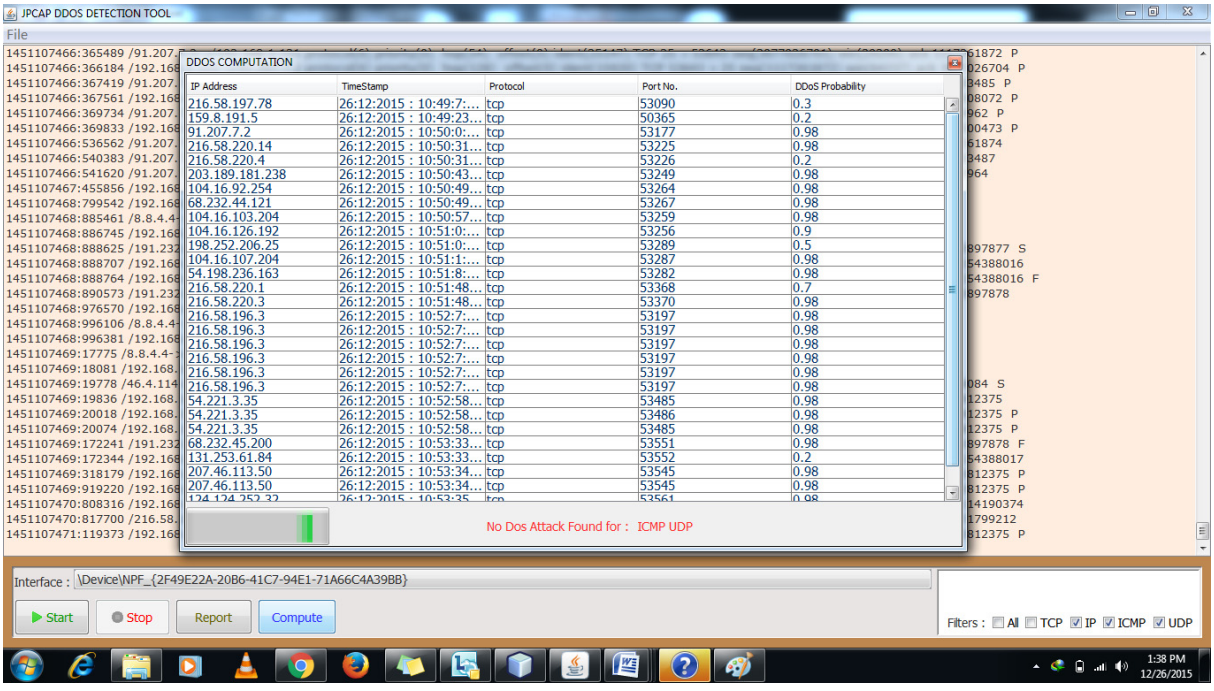

Fig 1: DDoS Attack Detection.

As per Experiment, We have captured live traffic from the network with the internet shared. We have detected DDoS on the ping program system with their IP, timestamp port, and probability which shows how Sevier attack. Our detection for DDoS impressive which able detect TCP, UDP flood more efficiently which majorly found in DDoS attack. ICMP packets can use for multiple attacks like smurf attack; SYN are also effectively detected in traffic our solution.

4. Conclusions

The In this paper, we proposed an algorithmic solution for DDoS detection on the network traffic. As the various parameters varies in the DDoS attack. It should be handled effectively to get an account of vulnerable traffic.
We have an emphasis on the TCP, ICMP and UDP packets that are more susceptible to get flood or pinged for DoS attacked. To handle the DDoS attack we checked with threshold and source and destination address that verifies the authenticated user of the network or not. At the holding point, we can provide a concrete solution to the DDoS detection which ability to set interface, protocol and traffic files.

5. References

[1] Dileep Kumar G et.“Using jpcap API to Monitor, Analyse and Report Network Traffic for DDoS Attacks” IEEE 14

[2] en.wikipedia.org/wiki/IEEE_802.

[3] L.D. Stein, J.N. Stewart, The World Wide Web Security FAQ, version 3.1.2, February 4, 2002, Available from <http://www.w3.org/Security/Faq>.

[4] P. Zaroo, A survey of DDoS attacks and some DDoS defense mechanisms, Advanced Information Assurance (CS 626).

[5] J. Mirkovic and P. Reiher, "A Taxonomy of DDoS Attack and DDoS Defense Mechanisms," ACM SIGCOMM Computer Communications Review(CCR), vol. 34, no. 2, April 2004, pp 39-54.

[6] http://www.winpcap.org

[7] http://jpcap.sourceforge.net/

[8] http://nsilimited.co.uk/Computing/Java/jnetpcap-1.2.rc2-javadoc/overview-summary.html

[9] iac.dtic.mil/iatac/download/intrusion_detection.pdf

[10] M. Sobirey. (2011, Jan.) "Intrusion detection systems". [Online]. Available:http://www-rnks.informatik.tu-cottbus.de/sobirey/ids.html

[11] sectools.org/tag/sniffers/

[12] http://netresearch.ics.uci.edu/kfujii/jNetPcap/doc/tutorial/index.html

[13] www.winpcap.org/docs/docs_41b5/html/group__packetapi.html

[14] dll.paretologic.com/detail.php/WinPcap