International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V7I3201707
Volume 7 Issue 3 September - October 2017

Preventive Approach against HULK Attacks in Network Environment

Oday A. Hassen
Computer Science and Information Technology
University of Wasit, Iraq

Hussain k. Ibrahim
Department of Information Technology
Ministry of Education, Iraq

Abstract

With the increasing network based communication, the security and privacy are in concern from a long time. Even the network assaults related to ransom ware are prevalent to get the extortion money from system administrators. In addition, the novel algorithm based zero attacks are in process very frequently by the cyber terrorists. With all such information, it is desirable to integrate the unique mechanisms to guard against the web portals against such attacks. One of the very powerful attacks is Distributed Denial of Service Attack (DDoS) which becomes more dangerous when associated with HTTP Unbearable Load King (HULK) as this attack choke down the network bandwidth and communication channels using malicious attempts of network access with the execution of specialized scripts. This research manuscript underlines the assorted dimensions of HULK attacks with the penetration level along with the tools and approaches which can be used to protect the network environment against such attacks.

Keywords:- Distributed Denial of Service Attack, HTTP Unbearable Load King, HULK Attack, Network Strangle Attack

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V7I3201707
Volume 7 Issue 3 September - October 2017

Introduction:-

Now days, the network environments are struggling to cope up with the zero day strangle and denial of service attacks [1] which becomes very effective for cyber criminals to integrate the extortion of money using Ransom ware [2]. As per the recent reports of CNN, more than 99 countries hit by such attacks in recent year 2017. More than 75,000 network assaults damaged the network environment in these countries which lead to the huge decay of money and time of corporate and government infrastructures [3].

There are number of assaults which are traditionally injected in the network based environment. Following is the broad taxonomy of network based attacks

Passive Attack:- The passive attacks include the monitoring of network resources and communication channels as a hidden spy so that all the activities can be monitored. Such attacks are more hazardous as the victim systems do not know about the existence of any attack. The network port sniffing, copying of passwords, route tracing, traffic evaluation and related implementations are done in the passive attacks and the attacked environment is generally not aware with any malicious attempt. HULK attacks are covered under this category because the network choke down is very difficult to evaluate regarding the actual source of attack [4].

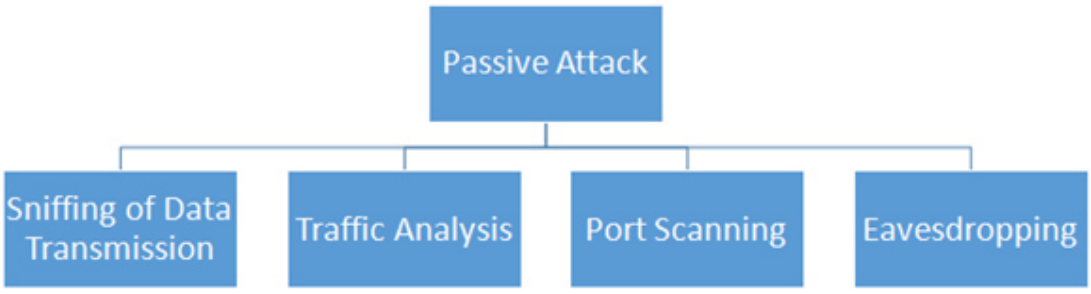

Figure 1: Passive Attacks in Network Environment

Active Attack: The active attacks are used to damage the network environment with actual modification in the communication channels. The deletion or changing of passwords is

implemented in this attack. In addition, the content modification or any other change falls under this category [5].

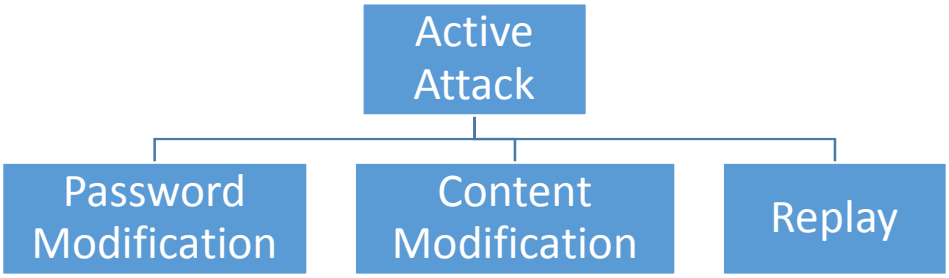

Figure 2: Active Attacks in Network Environment

HTTP Unbearable Load King (HULK) Attacks:-

HTTP Unbearable Load King (HULK) [6] attacks are used to transmit the virtual traffic to the web server so that the actual or genuine users cannot access the services of that web portal. In MySQL database engine, the maximum limit to create the connections is 151. Previously this limit was 100 concurrent connections. It means that the database server will not respond to Apache Web Server if this limit is crossed. Now, using HULK attack, the virtual connections with more than 151 concurrent users (which physically do not exist) can be created using Python, Java, PHP or any other script [7]. By execution of such HULK Scripts, the limit of database engine will be over and the web server will not work as per required operations. Many times, such HULK attacks are injected in the web servers to push back the actual users from using the web services. In PostgreSQL, if limit is set to 1000, this limit can be acquired with the virtual users using such scripts.

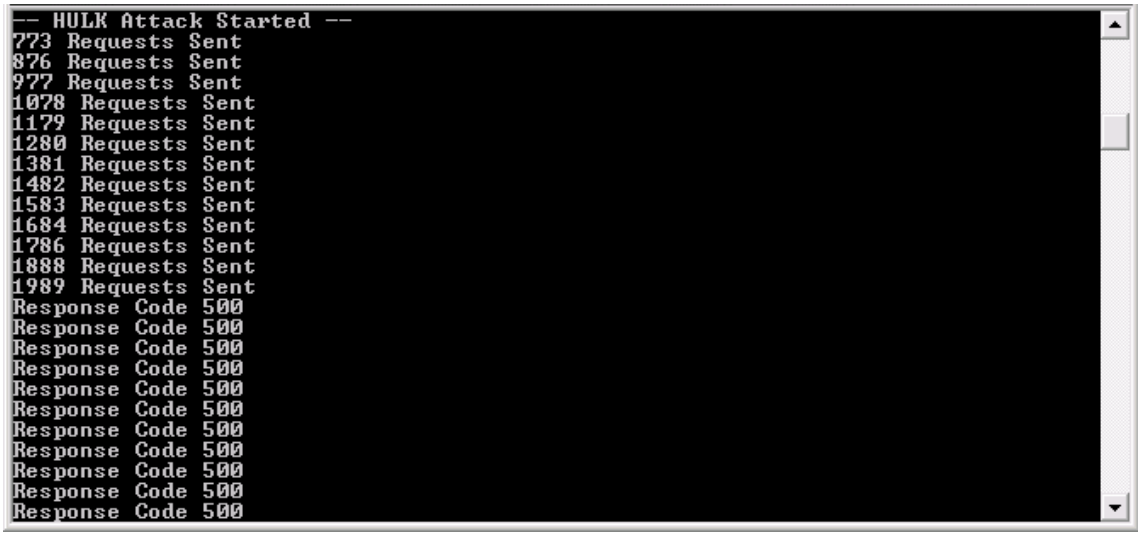

Figure 3: Execution Scenario of HULK Attack

Following is the type of output which is presented by the Web Server because of number of requests made by the HULK Attack.

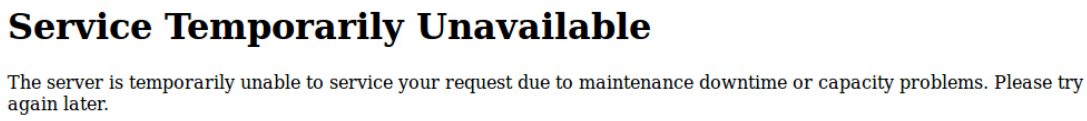

Figure 4: Error Message Presented by Web Server

Free and Open Source Software (FOSS) for HULK Attacks

DDoS Deflate:-

DDoS Deflate is a powerful with analytics based shell script that can be used to evaluate the occurrences of DDoS attack and HULK Attacks in the Web Server environment. The base command of netstat is used to identify the malicious or suspicious traffic with the recognition of IP addresses attempting to create the fake connections with the web servers [8].

<systemdirectory>$ netstat -ntu | awk '{print $5}' | cut -d: -f1 | sort | uniq -c | sort –n

Features of DDoS Deflate includes

- IP Address Identification and Blocking
- Blacklisting and Whitelisting of Sources
- Prior Notification and Alert Mechanisms
- Setting up rules with the IPTables and Policies of System Security
- Configuration Management with ease
- Alerts on E-mail
- Pushing back of fake connections using tcpkill

<systemdirectory>$ cd /usr/local/src/

<systemdirectory>$ wget http://www.inetbase.com/scripts/ddos/install.sh

<systemdirectory>$ chmod 0700 install.sh

<systemdirectory>$ ./install.sh

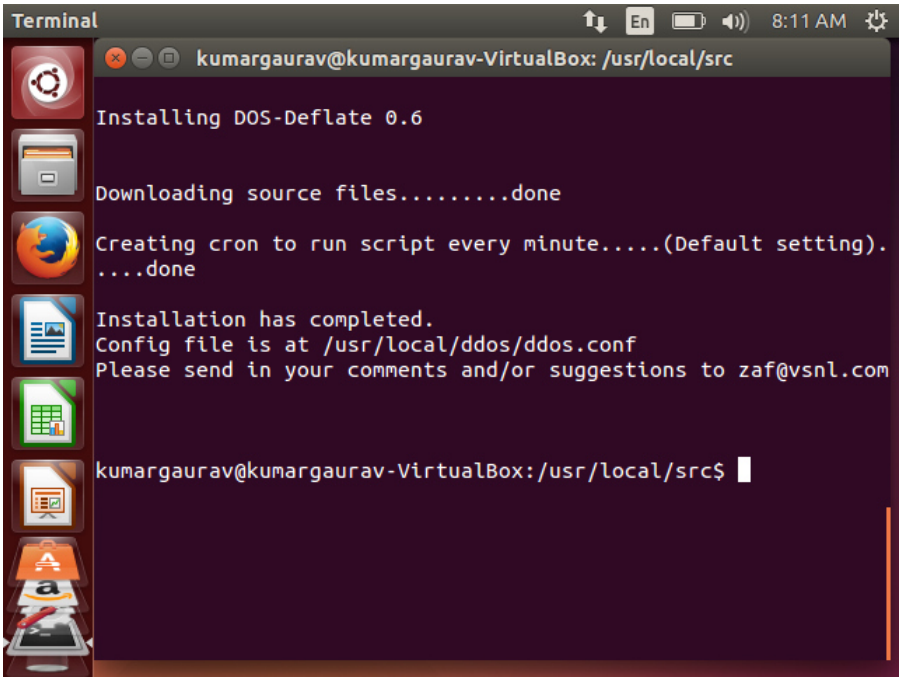

Figure 5: DDoS Deflate Working Environment

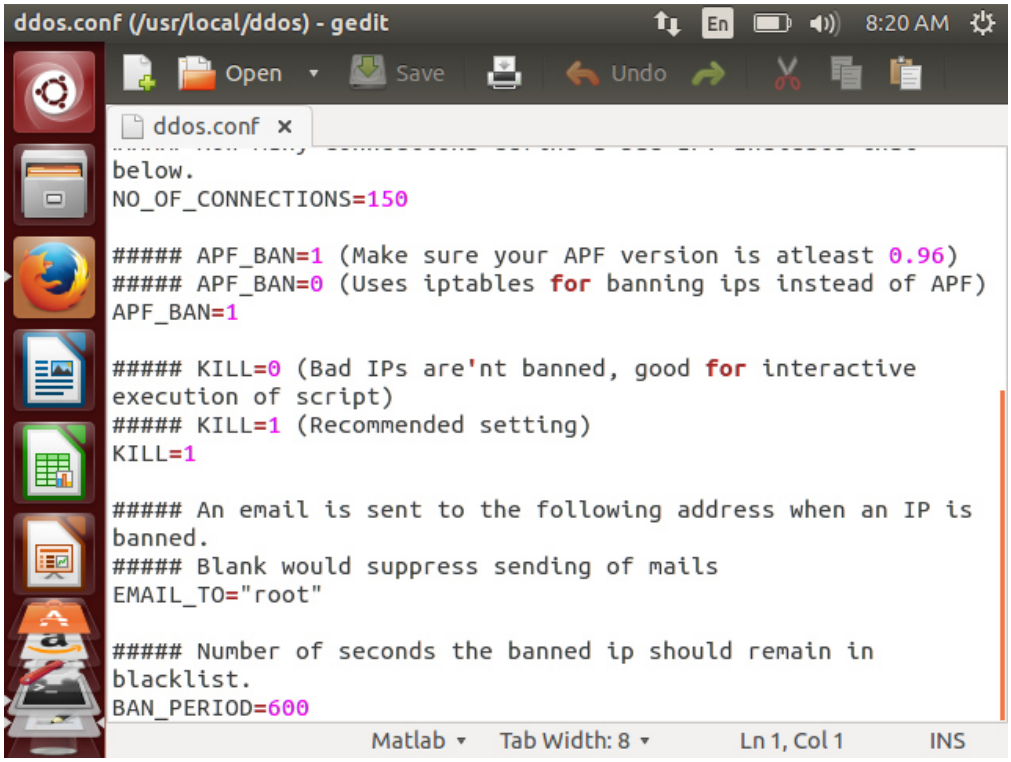

Figure 6: Configuration File of DDoS Deflate

Editing in the Configuration File

<systemdirectory>$ vi /usr/local/ddos/ddos.conf

or

<systemdirectory>$ gedit /usr/local/ddos/ddos.conf

Starting DDoS Deflate Engine

<systemdirectory>$ /usr/local/ddos/ddos.sh –c

Removal of Deflate Engine

<systemdirectory>$ wget http://www.inetbase.com/scripts/ddos/uninstall.ddos

<systemdirectory>$ chmod 0700 uninstall.ddos

<systemdirectory>$ ./uninstall.ddos

View Help Screen and All Options in DDoS

<systemdirectory>$ ddos –help

To View the Whitelisted IP addresses

<systemdirectory> $ ddos -I | –ignore-list

To Evaluate the Blacklisted or Banned IP addresses.

<systemdirectory> $ ddos -b | –bans-list

Initialize Daemon Process for monitoring of connections

<systemdirectory> $ ddos -d | –start:

Stopping the Daemon Process

<systemdirectory>$ ddos -s | –stop

View Current Status of Daemon and PID Running

<systemdirectory>$ ddos -t | –status

Show Active Connections with Server

<systemdirectory>$ ddos -v | –view

Ban or Blacklist all IP addresses with more than n Connections

<systemdirectory>$ ddos -k | –kill:

Fail2Ban:-

Fail2Ban is used to recognize the malicious sources of HULK traffic with the predictive analytics and avoidance mechanisms. The scanning of log files and identification of suspicious traffic is done in this tool with the push back of unauthenticated attempts [9].

Key Features of Fail2Ban

- Deep Evaluation and Parsing of Log Report
- Evaluation of IP with their time zone
- Client-Server Architecture
- Powerful services sshd, vsftpd, apache etc. for effectual evaluation
- Configuration and Administration with ease
- Compatibility
- Blacklisting and Whitelisting of IP addresses
- Push back of Brute Force Attacks
- Support for Powerful Python Programming
- Zone based IP blocking

Installation and Working with Fail2Ban

<systemdirectory>$ sudo apt-get install fail2ban

Fail2Ban service maintains a configuration file in the directory /etc/fail2ban. In this directory, the default configuration file is jail.conf.

After installation, the default configuration file is copied to working configuration file.

<systemdirectory>$ sudo cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local

Configuration Settings at the end of Config File

[http-get-dos] # Rule to be Set

enabled = true # Status

port = http,https # 80,443 (Ports)

filter = http-get-dos # Filter Names

logpath = /var/log/www/vhost.d/mysite.com/site-access_log # Path of Log

maxretry = 5 # Retries Max. Limit

findtime = 10 # 5 retries in 10 seconds from 1 IP Ban or Blacklist

International Journal of Computing and Business Research (IJCBR)
ISSN (Online) : 2229-6166
International Manuscript ID : 22296166V7I3201707
Volume 7 Issue 3 September - October 2017

Proposed Novel Mechanism for Avoidance of HULK

Flow of Work:-

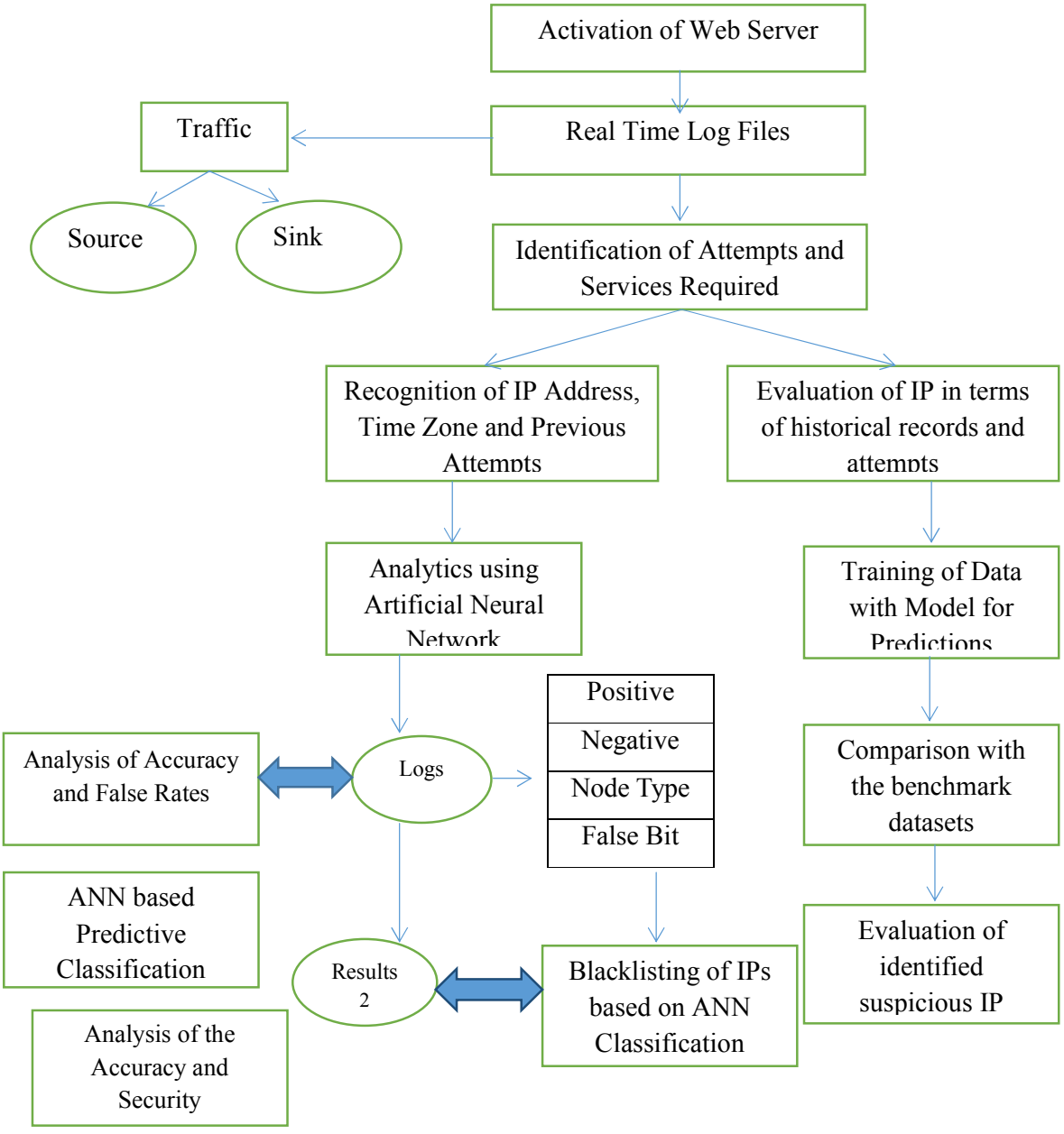

Figure 7: Flow of Proposed Mechanism for HULK Identification

Figure 7 depicts the proposed novel mechanism to guard the network against HULK attacks using Artificial Neural Networks. The benchmark dataset of malware or suspicious IP addresses can be modeled and trained on ANN based integration and then the currently flowing IPs can be evaluated with the dataset model. The accuracy rate of projected traffic can be further evaluated using machine learning and data mining approaches so that the effectual results can be obtained with higher degree of accuracy and integrity.

Conclusion:-

HULK attacks are widely used in number of web server based implementations so push back the actual users of the web service. Using free and open source tools, the HULK attack can be avoided but machine learning and soft computing based approaches can provide the higher degree of accuracy and optimization level.

References:-

[1] Gu Q, Liu P. Denial of service attacks. Handbook of Computer Networks: Distributed Networks, Network Planning, Control, Management, and New Trends and Applications. 2007 Jun;3:454-68.

[2] Cabaj K, Mazurczyk W. Using software-defined networking for ransomware mitigation: the case of cryptowall. IEEE Network. 2016 Nov;30(6):14-20.

[3] Choi KS, Scott TM, LeClair DP. Ransomware against police: diagnosis of risk factors via application of cyber-routine activities theory. International Journal of Forensic Science & Pathology. 2016.

[4] Deng H, Li W, Agrawal DP. Routing security in wireless ad hoc networks. IEEE Communications magazine. 2002 Oct;40(10):70-5.

[5] Jhaveri RH, Patel AD, Parmar JD, Shah BI. MANET routing protocols and wormhole attack against AODV. International Journal of Computer Science and Network Security. 2010 Apr;10(4):12-8.

[6] Elsawwaf AM, Eldessouky AS. Pictorial Presentation of Computer Behavior and Fault Detection Automation Using Genetic Algorithm. InProceedings of the International Conference on Security and Management (SAM) 2013 Jan 1 (p. 1). The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

[7] Cui A, Stolfo SJ. Reflections on the engineering and operation of a large-scale embedded device vulnerability scanner. InProceedings of the First Workshop on Building Analysis Datasets and Gathering Experience Returns for Security 2011 Apr 10 (pp. 8-18). ACM.

[8] Unrein E, Fish D, Boeker J, Sun W. Living in denial-A comparison of distributed denial of service mitigation methods. Issues in Information Systems. 2012;13(1):190-8.

[9] Alieyan K, Kadhum MM, Anbar M, Rehman SU, Alajmi NK. An overview of DDoS attacks based on DNS. In Information and Communication Technology Convergence (ICTC), 2016 International Conference on 2016, Oct 19, (pp. 276-280). IEEE.

ABOUT THE AUTHORS

Hussain K. Ibrahim received the B.Sc. degree in mathematics from the Department of Mathematics, University of ALanbar, Iraq in 1993, and M.Sc from department of information technology, science college, Alexandria University in 2016, Egypt. His research and professional interests include image processing, cryptography, authentication and security technologies.

Oday A. Hassen received the B.Sc. degree in mathematics from the Department of Mathematics, University of Mustansiriyah, Iraq in 2004, and M.Sc from department of information technology, science college, Alexandria University, Egypt. Currently he is PHD student in university Technical Melaka (UTeM), Malaysia. His research and professional interests include image processing, cryptography, authentication and security technologies.