University of Sindh Journal of Information and Communication Technology (USJICT)
Volume 4, Issue 1, January 2020
ISSN-E: 2523-1235, ISSN-P: 2521-5582
Website: http://sujo.usindh.edu.pk/index.php/USJICT/

Prevention Mechanism For RUDY Attack And Its Comparison.

Sheena Qadir Memon, Liaquat Ali Thebo, Syed Naveed Jafri, Hyder Zaman Brohi

Department of Computer System Engineering, MUET, Jamshoro, Pakistan
sheenamemon20@gmail.com, liaquat.thebo@faculty.muet.edu.pk, sayednaveed@feculty.muet.edu.pk, hyder.zaman@isra.edu.pk

Abstract: Rapid growth in the area of information technology causes IT professionals to make greater efforts to secure their network from Hackers. IT world called that attack RUDY (R U Dead Yet) attack Basically, RUDY attack is used by hackers to block or disrupt web-server services. Hacker is also trying to attack a web server using open ports. Each web server in the world has its exposed client ports (80, 8080,443 and 4433), and hackers use these ports to target web servers. You may want to use a web server on Microsoft Based Server (IIS) or Linux Based Server (Apache). RUDY attack on the 7th layer of HTTP traffic (DoS) attack, which basically injects POST body traffic to the server at a low rate to create so many sessions on the server. In this proposed work, a RUDY attack would be undertaken and tested for its impact on the Microsoft Based Web-server as well as the Linux Based Web-server at the end of which the key would be bounced to lock the Web-server..

Keywords: RUDY attack, HTTP,web server;

I. INTRODUCTION

For computer network security concern, the most common types of attacks are Denial of Service (DoS). DoS attacks the consume resources of the system, services on a server become unavailable for legal clients. Therefore, the entire company or network can be killed easily. Data theft or other safety breach these types of attacks mostly do not result, huge loss of money and time is targeted computer or network. In the past few years, these DoS application layer attacks have been increased these attacks have disturb the real human activity and compelled for adhere to protocol that results more difficult to detect. In the OSI model [1] among seven layers 7th layer named "application layer" works at the user end to interact with user applications, file transfer and email that are the major services of the layer. The main function of this is to transfer information and data by use of different protocols such as; SNS, SMTP, Telnet, HTTP, FTP, etc. A network requires several hundred bots to be carried out whereas a single attacker can attack by activating the device without the need for extra bots. Hence layer 7 becomes more popular DoS attack strategy, as the World Wide Web is based on Hypertext Transfer protocol [2]. Where, as this is connection-oriented protocol has similar
Vulnerability to TCP. When connection initiates the server allocate resources to it till the connection is open it remain allocated. To take the advantage of RUDY attacks the vulnerability is built.POST HTTP connections to HTTP server and delay to submit open by RUDY. Hence Server becomes busy because this attack sends many small packets to keep the link open. Therefore, as compared to flooding Dos attack it is comparatively hard to detect this low and slow attack [3].

II. RELATED WORK

Wrapper-based feature is of two types selection methods used are SEM-based ranker and Ranker based as discussed in (Sung and Mukkamala 2002). In the performance based ranker, elimination is done only on the input feature at a time, then testing of the classifier and training is done. To compare the performance of this classifier with original classifier carries all features is based on this performance. The first feature is primarily classified as "important" and secondary as "an important". Using Neural networks SVM and Classification models are created and are analyzed by using important features. In result accuracy of normal class increases and testing time decreases whereas the performance of the other classes depends upon the overall feature set. The important features are not defined for each specific class [4]. A ranking mechanism to guess competency of different features to detect the different types of attacks was given by (Ghorbani and Onut 2007). Their ranking process is statistical feature and ranked as 3-tier method. To compute the chances for the capability of the individual feature is to identify the type of attacks hence higher the chances, feature becomes better. When calculated the probabilities rank feature is done on the probability resulting values. DoS attack mostly correlate with the Internet Control Message Protocol (ICMP) i.e. ICMP NUMBER. of packets sent by the source ICMP or IP and number. of bytes sent by the source IP[5].
In order to investigate the correlate set of features for the detection of DOS attacks (Garg and Bhoria 2013) applied NSI KDD dataset with no specific feature selection method. Three sets of features compared and modeled together. First set contain 41 features and second contains28 features in the KDD data set, selected by adding time based basic traffic features. Third set includes 8 features whereas selection

technique has not been prescribed by author yet. With the help of these all, the decision tree algorithm is applied with cross validation to calculate performance values. To calculate performance values, decision tree algorithm is applied on these three sets of features with cross validation. Therefore, it can be summarized from the results that set includes 8 features takes shortest classification time and provides best classification accuracy [6]. For detection of RUDY attacks in 2016 (Najafabadi, Taghi M. Khoshgoftaar) used machine learning algorithm to create predictive models. The accuracy detection method gives faster analysis, increase with the least number of features, and shows the essential characteristics of the RUDY attack that are beneficial for its detection [7]. Hameed and Ali [19] introduced a framework called HADEC to detect live high-rate DDoS attack that occurs in network and application layers, such as TCP-SYN, HTTPGET, UDP, and ICMP. Sreeram and Vuppala[20] proposed a machine-learning matrix with a bio-inspired bat algorithm to allow fast and early detection of HTTP DDoS attacks. The time interval is incorporating by work instead of user sessions, packet patterns to generate a detection algorithm. A value of maximum sessions for one-time interval and computing a number of sessions in one-time interval to detect DDoS attack at the application layers the time interval uses machine-learning matrix. Matrix accounts for two pages of HTTP GET request. The frequency of a web page accessed by users and the time gap between first page request and the second page is determined to monitor user behavior. Am and Djuraev [21] proposed a detection technique based on the workload of the source node. The technique is used at multiple levels to protect a web server. The first layer allowed or rejected a received connection by inspecting the source IP address to the whitelist. The registered IP addresses were allowed to establish a connection with web servers to obtain service, while the connection of non-registered IP addresses was dropped. IP addresses allowed were inspected, and if they behaved maliciously, the connection would be dropped, and the IP addresses would be blacklisted.

III. METHDOLOGY

To keep an eye on monitoring HTTP traffic towards web-server is challenging task. It is hard to find that which packet or data is coming for collecting data from web-server either by Hacker or by real client. If RUDY attack is succeeded to break the security barrier it will reach to the web-server and there is no way to secure that effected web-server. The only way is to restart your web-server and change its IP address.

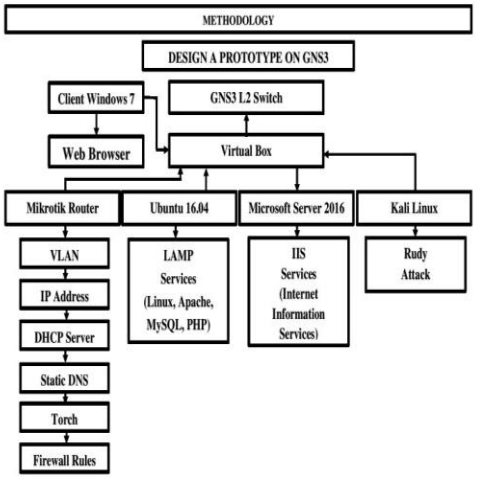

Figure 1. Proposed work flow

In this proposed work security is being provided to the web servers to block the RUDY attack automatically through the Mikrotik router. In this proposed work we used Mikrotik Router for networking and packet monitoring over the network. In Mikrotik router we configure VLAN,IP address, DHCP server static DNS torch and firewall rule. Torch is a built in tool in Mikrotik router for the packet filtering, "Ubuntu 16.04 server edition and Microsoft Server 2016".For Web Services, LAMP (Linux, Apache, MySQL, and PHP) should be installed in Ubuntu 16.04 and Kali Linux for RUDY Attack preparation in kali Linux we used Slowris.pl tool that is built in tool in kali Linux and the all operating systems should be installed on Virtual Box.

Step 1

In this step designed a prototype on GNS3 to diagnose the RUDY attack over the Network

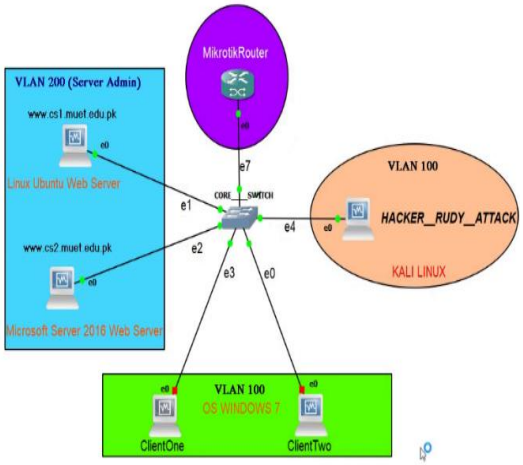

Figure 2.Network diagram of project

The above diagram shows different Virtual machines "MIKROTIK Router, Web Server (Ubuntu 16.04), Microsoft Server 2016, Client PCs (Windows 7) and Hacker System (Kali LINUX)".

Step 2

Web Servers and their IP address and configuration of local DNS Server on MIKROTIK Router.

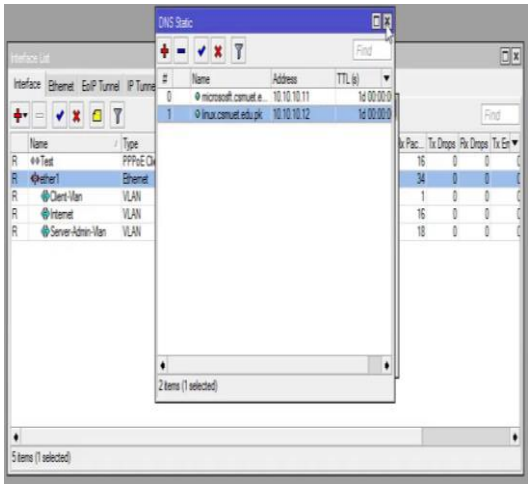

Figure 3. DNS Entry On Mikrotik Router

The local DNS server shown above is added to the Mikrotik router so that it can be easily accessed via domain base webs. It is easy to remember a domain instead of an IP address

http://linux.csmuet.edu.pk

http://microsoft.csmuet.edu.pk

Step 3

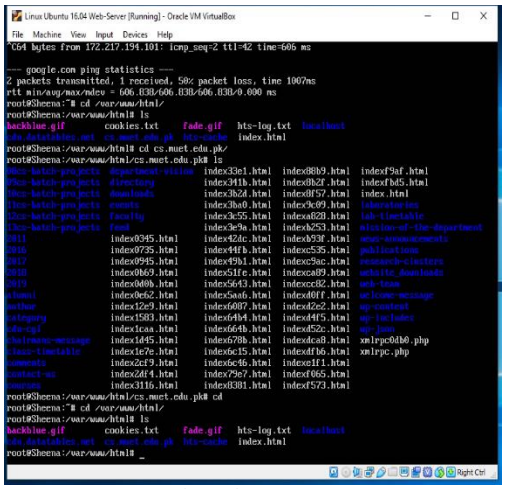

Figure 4. All files of web site at ubuntu directory

The image above shows that all web access files have been uploaded to the Ubuntu web server in /var/www/html directory and that apache web services are already installed on Ubuntu to run web services. The directory is not created by default /var/ww/html, we get this directory after installation of lamp services. All the data is copied and placed in this directory such data from MUET web. Whereas we have used HTTracker software from where we have copied all the content of web pages. With the installation of LAMP (Linux, Apache, MySQL, and PHP), services a sever will work as a web server.

Step 4

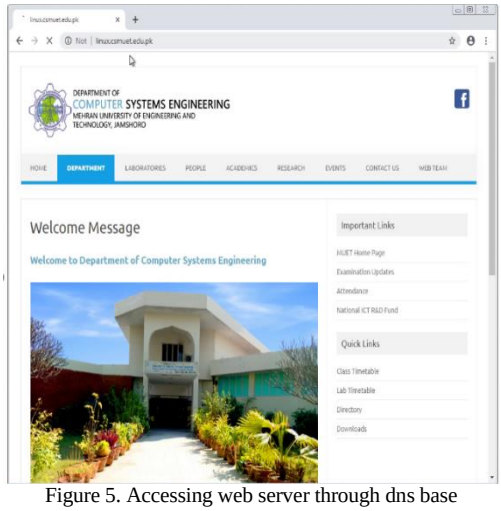

Figure 5. Accessing web server through dns base

The figure above shows that a web server created is working and a Web server based on Linux is ready to test the RUDY attack impact.

Step 5

Enable the IIS service and put all web files in the directory C:\inetpub\wwwroot\

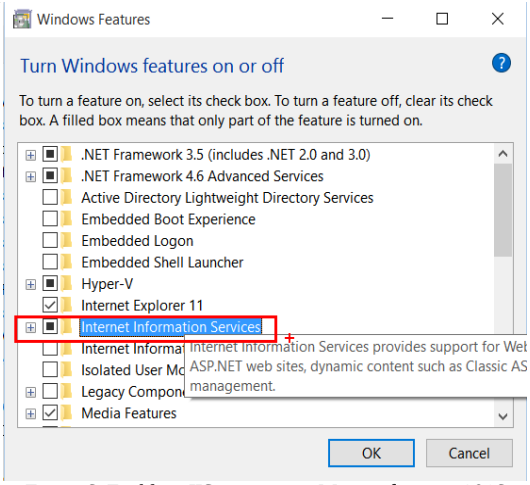

Figure 6: Enabling IIS services on Microsoft server 2016

Enable IIS service on the 2016 Microsoft Based Server. If the organization wants a web server on a Microsoft OS based, the IIS service must be enabled.

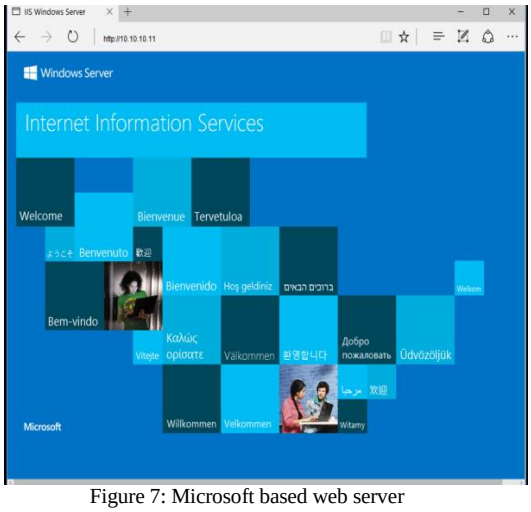

Figure 7: Microsoft based web server

The figure above indicates that Microsoft based web server 2016 under the IP address 10.10.10.11has been developed and is ready to test the effect of the RUDY attack.

Step 6

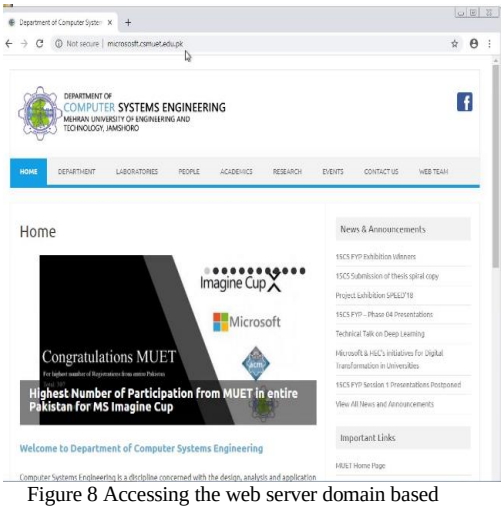

Figure 8 Accessing the web server domain based

The above figure shows that created web server is working and Microsoft based Web server is ready to test the RUDY attack impact the servers are ready to work, compile and compare the results of the RUDY attack on the Linux Based Server (Apache) and the Microsoft Based Server (IIS).

IV. RESULTS

Now test the single user to access the web server so we can see that how many sessions are required to access a web server.

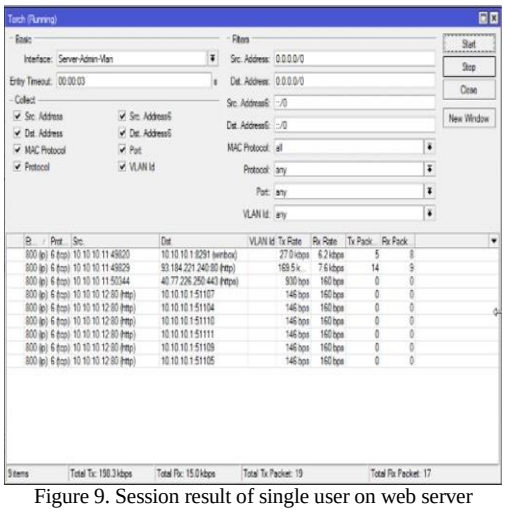

Figure 9. Session result of single user on web server

If a single user access a web server the sessions will create up to 20 sessions. The figure above shows that single user sessions on server and their impacts on server.

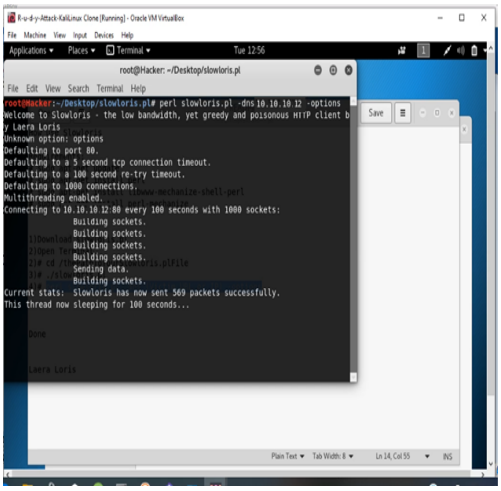

Figure 10. RUDY attack on server ip address from Kali Linux

The Server IP address is 10.10.10.12 as shown in the figure , now see the result after the RUDY attack.

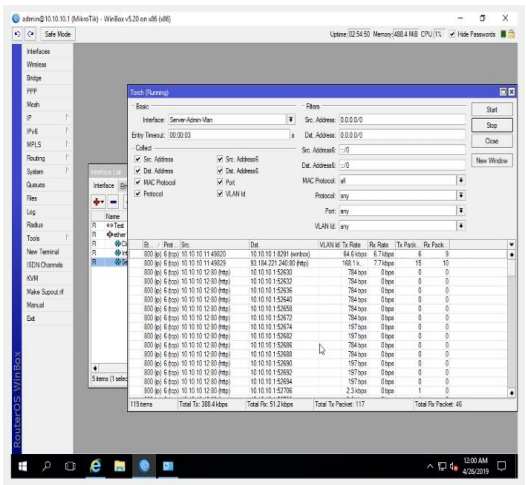

Figure 10. Sessions from Kali Linux to Linux based web server

Sessions that are created on the web server using Kali Linux within 5 seconds it creates 119 sessions on the web server if it will run up to 100 seconds then it will create lots of traffic on the web server.

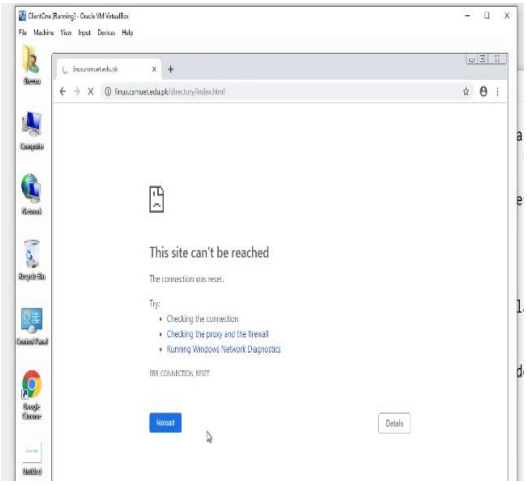

Figure 11.After RUDY attack on Linux based web server

The figure above shows that within a few seconds it creates a lot of sessions on the server so the server is too busy to respond to anyone else.

Now provide the solution to stop the RUDY attack by using the MIKROTIK Router Firewall rule.

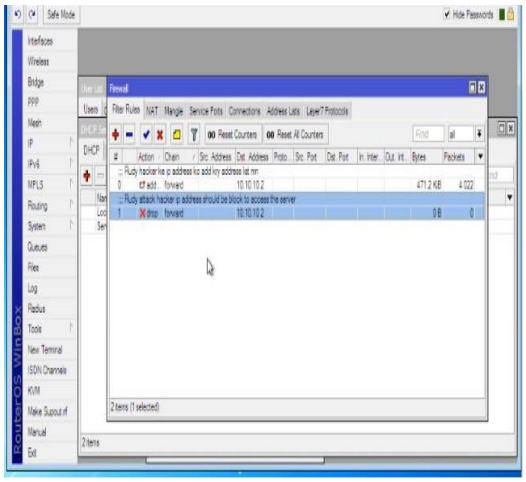

Figure 12. Firewall rule to block the Rudy attack

We configure the firewall rule on Mikrotik router. If a user access 10.10.10.12 and create more than 30 sessions on the web server then it should highlight and block that IP address. Normally, if we go through Google 15 or 20 sessions are created, but when RUDY attack works within seconds it creates more than 1000 sessions hence server becomes down.

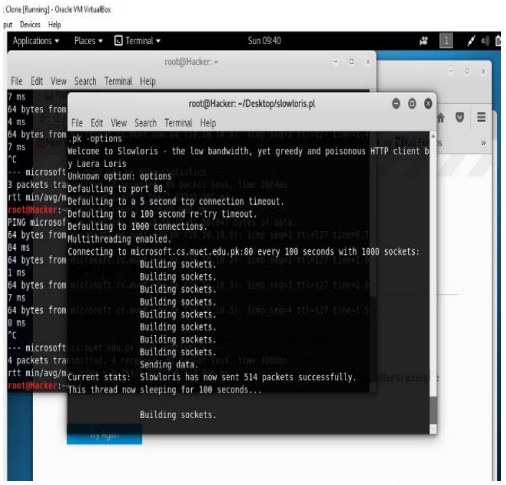

Figure 13. RUDY attack on microsoft.cs.muet.edu.pk

The fig above shows how RUDY effects on Microsoft Based web server every 100 seconds it creates lots of sessions on the server.

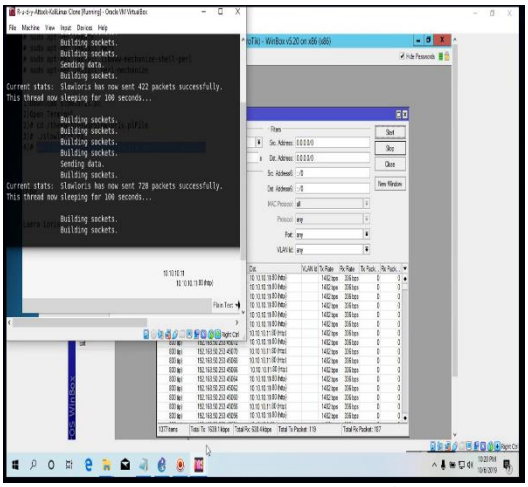

Figure 14: Sessions are created on web server after RUDY attack

The figure above shows that web server sessions are created by RUDY attack are 1377 sessions, but their affect does not interrupt the web services as they affects the Linux based web server.

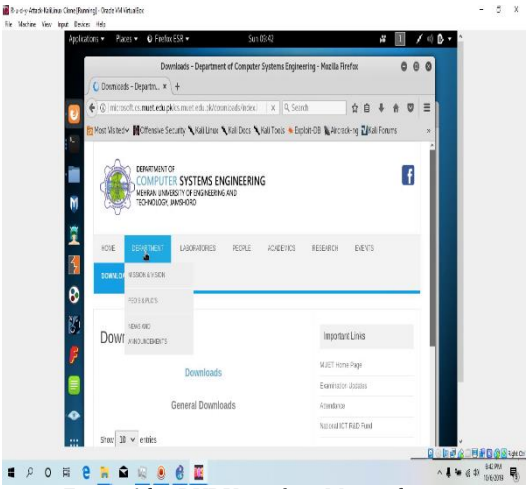

Figure After RUDY attack on Microsoft server

Our server is still responding after creating 1377 sessions on IIS server . Attacks like RUDY are almost ineffective against Microsoft web servers, since such threats are designed to seize all available connections the server is able to simultaneously serve. Since IIS is able to potentially manage thousands of connections simultaneously

V. CONCLUSION

The RUDY attack relates to application layer attack that exhausts the server with a slower connection, injecting POST body traffic to the server at a low rate to create so many sessions on the server. In this research , we proposed a solution that blocks RUDY attack, and designed a prototype on GNS3 to test the RUDY attack on the LAN and WAN network, used Kali Linux to prepare the RUDY attack, configured the Mikrotik firewall to analyze the Rudy packet over the network. Automatically blocked RUDY attacks before creating a violation over the web services, and secured the servers. After the RUDY attack, the Linux-based server (Apache) was no longer available. Whereas the Microsoft based server (IIS) after RUDY attack is slow but not inaccessible. The impact of the RUDY attack on (IIS) service is nothing buffer won't be overfelow. In the future, we'd like to find a buffer overfelow RUDY tool on Microsoft based server.

REFERENCES

[1] C M P Books, Grigonis, R. 2000 computer telephony encyclopedia edition1st.

[2] Fielding,R.;Mogul,J.;Gettys,J.;Masinter, L.;Frystyk,H.;Berners-Lee,andLeach, P.; T. 1999. http/1.1. Request for Comments:2616

[3] H.R, N.; Shetty, S.; and K.C, P. 2014. Study on distributed denial of defense mechanisms and service attacks.

[4] International journal of computer applications (0975 8887) 15–20.A comprehensive study on distributed denial of defense mechanisms and service attacks.

[5] Mukkamala, S., and Sung, A. H. 2002. To study feature selection for intrusion detection using support vector machinesandneural networks. Research journal of the transportation research Board, Transportation record. (1822 33–39).

[6] Ghorbani, A. A. And Onut, I.-V. 2007 features vs. attacks: Feature selection model for networkbasedintrusion detection systems. ISC 2007 (volume 4779, 19–36. Springer)10th International Conference.

[7] Garg,K.,andBhoria,M.P.2013.Determiningfeaturesetof dos attacks. International Journal of Advanced Research in Comp. Sc. and Software Engg3(5)(875–878).

[8] Maryam M., Najafabadi, et al"Rudy attack, detection at the network level and its important features." The twenty-ninth international flairs conference. 2016.

[9] Goldstein, M.; Levine, D. Berenson.;andM. L 1983 intermediate statistical methods and applications: A computer package approach 2nd edition. PrenticeHall.

[10] Dale, J.; Damon, E.; Laron, E.;Land, N.; Mache, J.; and Weiss, R. 2012 hands-on denial of service lab exercises by use ofslow Loris and Rudy. InformationSecurityCurriculumDevelopmentConferenceIn 2012,in-foSecCD '12, 21–29. New York, NY, USA:ACM.

[11] Elisseeff, A,andGuyon, I.2003 introduction to feature and variable selection. Learn. Res. J. Mach. 3:1157–1182.

[12] Pfahringer, B.; Witten, I. H; Reutemann,P.; Frank, E.; Holmes, G.; and Hall, M.;2009, study weka data mining software:An update. SIGKDD Explor. Newsl. 11(1):10–18.

[13] Seliya, N.; Khoshgoftaar, T. M.; Kemp, C.; Zuech, R; and Najafabadi, M. M.2014 to detecting brute force attacks at the network level by Machine learning. In 2014Bioinformatics and Bioengineering, Internationalconferenceon-workshoponBigDataanddataanalyticsapplications, (379–385).

[14] Khoshgoftaar, T. M.; Seliya, N; and Najafabadi, M. M.; 2016 carry out evaluating feature selection methods for network intrusion detection with Kyoto data. International Journal ofQuality Reliability, and Safety Engineering.

[15] Khoshgoftaar, T. M.; Najafabadi, M. M.;andWheelus,C.2015 studied Attackcommonalities:Extractingnewfeaturesfornetwork intrusion detection. In 21st ISSAT international conference on qualityandreliabilityin de- sign,46–50.

[16] Mukkamala, S. and Sung, A. H.,2002 feature selection for intrusiondetectionusingneuralnetworksandsupportvectormachines.

Transportation record research journal of the transportation research board (182233–39).

[17] Lin, C.-Y.; Hsu, Y.-F.; Tsai, C.-F.; and Lin, W.-Y. 2009; Review,Intrusion detection by machine learning, A review. ExpertSystems with Applications 36(10):(11994–12000).

[18] T. M.; Zuech, R.; Khoshgoftaar, Wheelus, C.; and Najafabadi, M. M. 2014 studied session based approach for aggregating network traffic data - the Santa dataset. In Bioinformaticsand Bioengineering, 2014InternationalConference on - workshop on Big Data and data analytics applications, 369–378.

[19] U. Ali and S. Hameed "Hadoop-based live DDoSdetection framework:HADEC" vol. 2018, no. 1, p. 11, 2018, EURASIP Journal on Information Security.

[20] V. P. K. Vuppalaand I. Sreeram, Applied Computing andInformatics, 2017, in press. "HTTP flood attack detectionin application layer using machine learning metricsand bio inspired bat algorithm".

[21] S. Djuraev and S. Y. Nam, KSII Transactions on Information and Internet Systems.Vol. 8, no. 7, pp. 2512–2531, 2014.

HTTP defending web serversagainst DDoS attacks by busy period-based attack flowdetection.