International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 2 | Jan-Feb 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

JomSecurity: Localized Attack of IPS

Siew, J. X.
School of Computing & Creative Media, KDU
University College, Jalan Kontraktor U1/14,
Seksyen U1, Shah Alam, Selangor, Malaysia

Lim, J. T.
Faculty of Information & Communication
Technology, University Tunku Abdul
Rahman, Kampar, Perak, Malaysia

ABSTRACT
Internet became a vital part of our life so from a small to big company has set up their own network. Thus, to prevent the company's network security breached and private information might leak out it is important to implement good network security. The current limitation of IPS only relies on the global signature to determine packet. A mix mode method will be used to collect primary data via survey and interview. The sample size selection criteria for the questionnaire is Private University Students, lecture and industry experts who have networking knowledge. Furthermore, the simulation test will be done using virtualization to simulate the network environment to implement the self-updated IPS to protect the server. This helps to validate the workability of the proposed. Last with the implementation of the security measure of a network that able to help the user to gain the trust towards the digital society.

KEYWORDS: *VSS; VRRP; HSRP; GLBP; ICT infrastructure; high availability; business continuity; network; routing protocol; Intrusion Prevention System, academic*

1. INTRODUCTION ON THE IMPORTANCE OF NETWORK SECURITY FOR KDU University College

University student becoming the target of cyber-attack rate is increasingly high rate because university student spends more time on the Internet.[1] Furthermore, recently there is a largest 1Tbps DDoS attacked happened attacker use a lot of smart devices included IoT devices to launch a huge DDoS attacked.[2] Moreover, nowadays cloud computing is so popular, there is so many companies subscribe to cloud storage and services but even these cloud hosting company also have the risk that gets a DDoS attack.[3] From cases above able to know that DDoS will make a company have a big loss in financial and it is difficult to avoid. In a questionnaire conducted by Association of Governing Boards of Universities and Colleges and United Educators found that there are more universities increasingly engage in cyber risk.[4] KDU University College is a medium-size company that main business is education. They had set up their own network and servers. Thus, there are a chances that KDU University College became a target and get attack by a hacker. Normally hacker will not attack things that are not beneficial to them. So once the attack succeeds private information may leak out, the system may break down and the victim will have loss of trust, KDU University College may have Image and reputation damage, and business may not able to continue for some period due to the breakdown of the system. Thus, KDU University College needs some security to prevent these unpredictable attack. Psad is an intrusion detection software that contains 3 lightweight daemons and it also able to perform log analysis. Besides that's, iptables is an application work with a Linux firewall and allow the system administrator to configure the tables, chain, and rules that are stored. Currently, iptables is able to support ipv4 and ipv6. In this research will using Psad and iptables provide an emergency temporary solution to protect servers from unpredictable attacks.

IPS is a technology security to secure all hosts from attack. The job for IPS is to examine network traffic flows to scan and to prevent vulnerability exploits by an attacker. So suppose a network had set up an IPS and the network should be secured and any attack may not able to attack the network. However, it is not working like that in reality and this is the major problem statement. In a network, that setup IPS but still has chances that get an attack. For example, a DDoS attack is one type of attack that not sending malicious packet but it still able to attack servers. Since IPS are working like first need to scan packets and if that packet is malicious then drop it and if the packets are not malicious then let it go into the network. Therefore, IPS will keep allowing those packets that are not malicious but keep repeating come in so when the server not able to sustain the traffic it will break down. In the response to this problem, our study proposed identifying what are the ways able to reduce the chances that important host get an attack. Furthermore, this project will also look into which is the most effective way to mitigate the problem stated above.

The research aims to deliver the following objectives as shown below.

RO1: To improve the efficiency of security by implementing a IPS to learn the actual attack methods that are actually happening on site of in the KDU network
RO2: To trim down the administrative burden of KDU network to the network administrator.
RO3: To mitigate the possible financial implication from the effect of the intrusion

Currently, most of the IPS detect threat is based on the global signature. Thus, if there is an attack the signature is not Inside database of the IPS signature to KDU University College server. IPS not able to detect it and the attack will successfully attack the server. To having a IPS that could learn the real attack able to prevent this case happen.

To monitor a whole network is an important job for the network administrator. Once the network had anything happens network administrator have to solve it as fast as possible. It is because any problem in the network may affect the whole business not able to run normally. However, normally a medium size enterprise IT department does not have that many staff so the IT staff in medium size company may need to monitor the network also need to handle desk inquiry and some technical support. Hence, trim down the administrative burden of network IT staff able to spend the time work on another task.

Normally a hacker will not attack a target for fun, normally they have attacked for something for example money, information, or other valuable things that will benefit the attacker. Attacker benefits something from attack the target will lose something. Therefore, by reducing the chance and risk that KDU University have a huge loss from the effect of attack security of the network is a key to protecting the asset of KDU University College.

This paper aims to answer the above research objective via the research question as shown below: -

RQ1: How to improve the efficiency of security for KDU server?

RQ2: How to automate the detection to allow network administrators to have more time to focus on another task?

RQ3: How to reduce negative financial impact from the effect of intrusion?

2. LITERATURE REVIEW

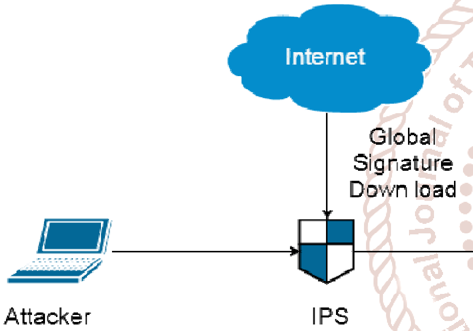


Figure 1: Conventional Topology

Figure 1 shown current topology that implemented IPS in the network. There are only 2 categories of IPS which is network based and host based.[5] In this project, the implementation will focus on host-based IPS. The normal IPS is download signature from the internet and scan the packets that coming in and out. Once the packet has the code that matches with IPS signature it will block it to coming in or going out. However, not all attack is recorded in the signature. Some attack like ping it looks harmless but if there is a machine keep ping the server the server may not able to sustain with the traffic it may cause server down. Thus, since KDU University College have their own private network and servers, therefore may have a chance to get an attack.

In a work published by JosephNg PS & Kang CM (2016) stated that "*This ITconomic paradox has been long debated over its tangible and intangible contributions, yet information technology continues to be a major user of costly capital expenditure and laggard operating expenses in today's electronic economy*."[6] From the statement above know that nowadays information technology system is widely used in any sector. There are a lot of business able to grow bigger is because technology helped them to centralized data makes things manageable.

To choose an IPS first need to know which area want IPS to protect. For network-based IPS is monitor a part of network devices or segments. Network-based IPS will detect and block any suspicious activity that happened in the area that IPS protected.[7]. Besides that, wireless IPS is like network-based IPS but it only monitors the wireless network to identify any suspicious activities involved in a wireless network. However, wireless IPS is not able to identify suspicious activity in applications or higher level of protocols. Moreover, THE next type of IPS is network behaviour analysis this kind of IPS will observe network traffic to detect threats that produce abnormal traffic flow like DDoS attack and also able to detect certain malware like backdoors and worms. Normally this kind of IPS is set up to monitor internal network flow. Last is host-based IPS this kind of IPS only monitors a single host to identify this machine have any suspicious activity. This type of IPS able to detect suspicious activity from application and network. Host-based IPS are the last line of defence of a server. Normally this kind of IPS only set up in a critical host. In this project the IPS will use for KDU University College is a host-based IPS. There are an open source host-based IPS called PSAD + Iptables. It is very popular and it is well documented for Linux.

PSAD is an IDS that able to identify attacker IP from Log. Since it is an IDS so it does not provide any action that able to prevent the attack. However, Psad is able to integrate with Iptables. Iptables is a Linux firewall, it only knows to allow or block. Since Psad able to identify and Iptables able to do action so Psad and iptables work together it works same as IPS. If there is an attacker trying to attack server but the attacker wants to do an active recon attack to the server so the attacker use port scanning software to scan the server to obtain information of the server to do the next step like, try to obtain what service and version of software is using to do the next level of attack. So in this situation if the server is installed Psad IPS it will block the attacker IP do not allow the connection of attacker to the server since Psad IPS know that this IP is malicious. Thus, the attacker not able to perform the next attack and the server is safe on that night.

3. METHODOLOGY

In this section will discuss research methodology that will be used in this project. Furthermore, this topic also will talk about what technique will be used for data collection and the reason for choosing it. For this project, a mixed methods design is chosen. Thus, quantitative and qualitative research method is used in this project. There are three methods chosen for research which is a questionnaire, interview, and experiment. In 2016 Professor Janice Morse stated

"A mixed method design, if conducted with deliberate care, is a stronger design than one that uses the single method because the supplemental component enhances the validity of the project by enriching or expanding our understanding or by verifying our results from another perspective."

The data is to be collected via the following methodology as summarized in

Table below.

Table 1: Research Methodology [6], [8]–[13]

Research Dimension	Explanatory Sequential Design
Research Methodology	Quantitative Generalization Qualitative Reasoning
Data Collection	Online Survey

	Personalized Interview
Result Validation	Experimental Simulation

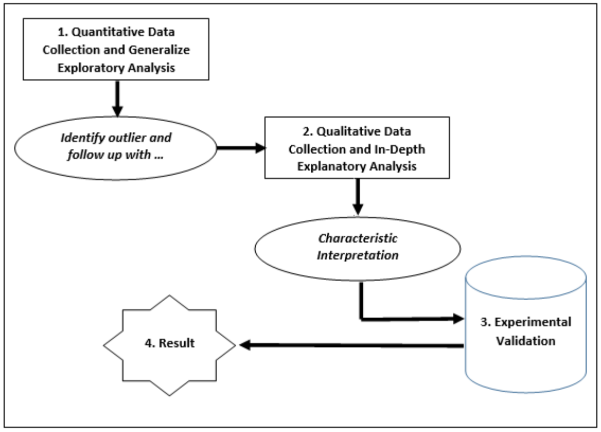

1. Quantitative Data Collection and Generalize Exploratory Analysis
Identify outlier and follow up with ...
2. Qualitative Data Collection and In-Depth Explanatory Analysis
Characteristic Interpretation
3. Experimental Validation
4. Result

Figure 2 : Sequential Design [6], [8]–[11],[13]

The figure above is the sequential design methodology diagram for this project [6], [8]– [11], [13]. Since this project is using mixed methods, so both the quantitative and qualitative technique will be used in this project for data collection. Furthermore, Professor Janice Morse in the year (1991) also stated "A sequential explanatory design is typically used to explain and interpret quantitative results by collecting and analyzing follow-up qualitative data. It can be especially useful when unexpected results arise from a quantitative study".[14] Moreover, from the figure above able to see that before anything starts the first step of research is to generalize exploratory analysis. Basically, is doing data collection by using quantitative data collection technique and from the result simplify the whole idea of research. Next, after generalized exploratory analysis need to detect outliers and anomalies from the resulting follow-up with reasoning. After that, qualitative data collection needs to be conducted. The reason to conduct qualitative data collection is to do the in-depth explanatory analysis for reasoning the previous result from quantitative. Therefore, characteristics interpretation is done by using the depth-explanatory analysis. Next, after collecting data and analyzed it need to do experimental validation. Experimental validation is to validate data that collected previously by experiment. From experiment able to know data that collected previously is true or false. So after experiment then able to get the result from the experiment and make a conclusion to know is the idea able to work or not.

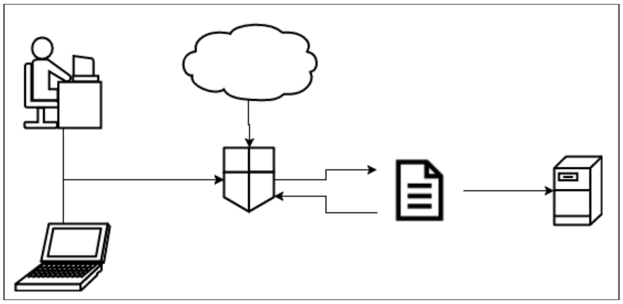


Figure 3: Network Topology

The testing will be conducted via a virtual machine. In the testing environment will be set up 2 attackers, 1 IPS that installed on the server machine. All machine will connect with each other as the figure below except the cloud symbol that is for explaining the purpose. The first thing wants to test is all of them is connected with each other so use ping to test the connectivity. Furthermore, the different between Psad IPS and normal IPS is it will revise log to block the localized attack. From the figure below able to see that there are two categories of machine connect to a server which is attacker and staff. The IPS that in the middle of the diagram is actually a software that installed on the server. IPS able to download global signature and revise their own log so anyone want to connect to server IPS will check is there any pattern that matches global signature and their own log if not then the IPS will allow it go into the server.

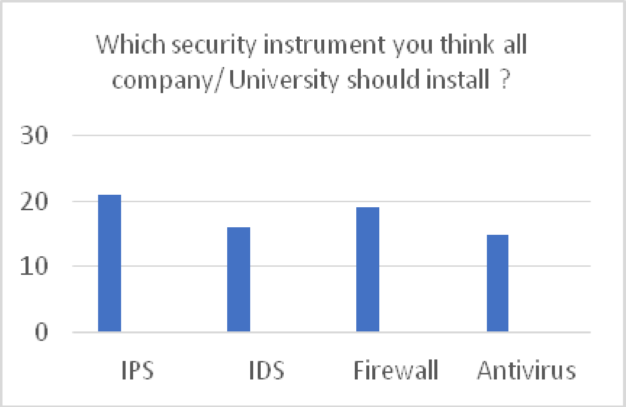


Figure 3: Corporate Security System Trend

In figure 3 this question is asking respondent what are the security system should install in a company or university environment. From the respond of this question know that IPS get the most voted which 67% of respondent voted IPS and follow with firewall get 61%, 51% of respondent voted IDS and 48% of respondents voted Antivirus and there is an others selection no respondent vote it. Furthermore, from this result also able to know that people have the trust with IPS so implement IPS into the network it not only will help to secure the network also able to build the trust of the network security with the user.

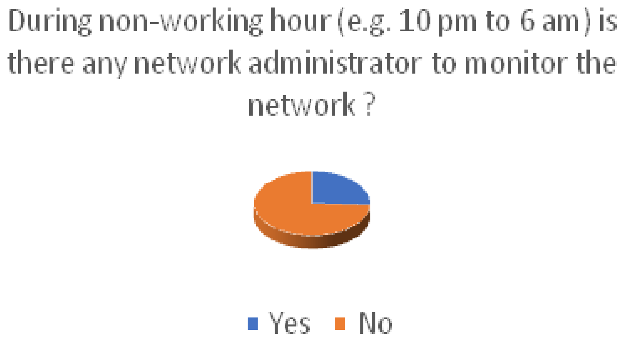
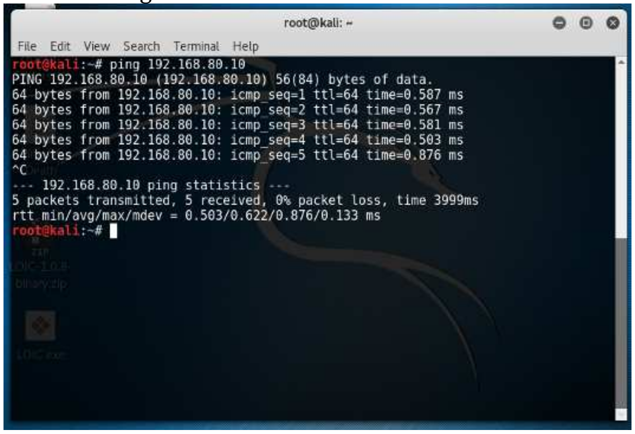


Figure 4: Administrator Burden of Network

In figure 4 question is during non-working hour any network administrator monitors the network? The majority of the respondent choose no it is up to 74%. From this question, we are able to know that most of the company do not have a network administrator on duty after working hour. However, there are 26% of respondents chose during nonworking hours also have network administrator to monitor the network. It means that some company network is very critical to their business. Furthermore, the 74% of respondents do not have anyone to monitor the network during the non-working hours. It means that in this period network security is rely on the security system. In this time is easier for an attacker to launch an attack since there is no one to stop the attack if the attacker launches a localized attack in this time will easily attack the main server.

4. RESULTS AND FINDINGS

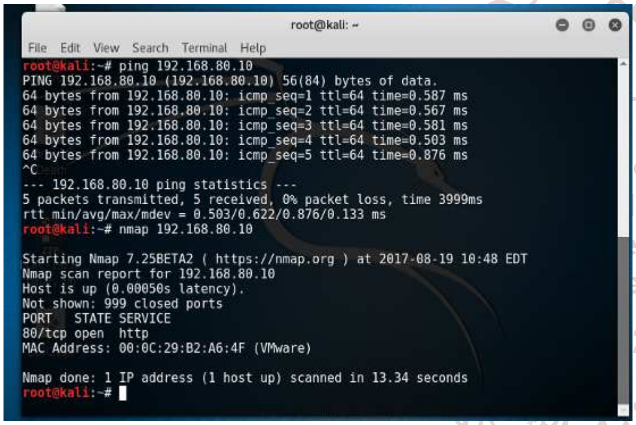
Port Scanning attack



```
root@kali:~# ping 192.168.80.10
PING 192.168.80.10 (192.168.80.10) 56(84) bytes of data.
64 bytes from 192.168.80.10: icmp_seq=1 ttl=64 time=0.587 ms
64 bytes from 192.168.80.10: icmp_seq=2 ttl=64 time=0.567 ms
64 bytes from 192.168.80.10: icmp_seq=3 ttl=64 time=0.581 ms
64 bytes from 192.168.80.10: icmp_seq=4 ttl=64 time=0.503 ms
64 bytes from 192.168.80.10: icmp_seq=5 ttl=64 time=0.876 ms
^C
--- 192.168.80.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.503/0.622/0.876/0.133 ms
root@kali:~#
```

Figure 5: Pretest

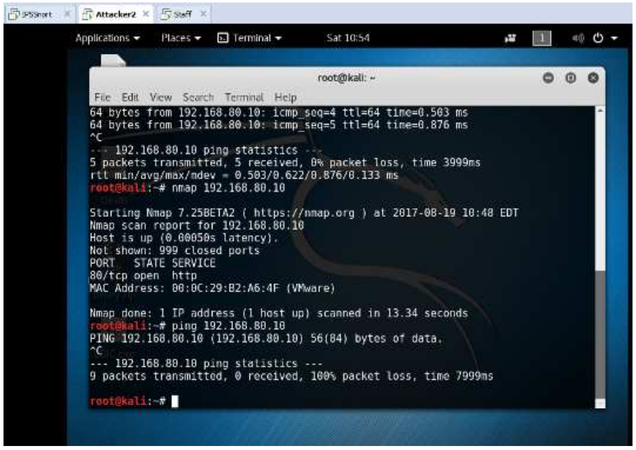
In figure 5 able to see that attacker machine before the attack, the server the connection between attacker and server is up.



```
root@kali:~# ping 192.168.80.10
PING 192.168.80.10 (192.168.80.10) 56(84) bytes of data.
64 bytes from 192.168.80.10: icmp_seq=1 ttl=64 time=0.587 ms
64 bytes from 192.168.80.10: icmp_seq=2 ttl=64 time=0.567 ms
64 bytes from 192.168.80.10: icmp_seq=3 ttl=64 time=0.581 ms
64 bytes from 192.168.80.10: icmp_seq=4 ttl=64 time=0.503 ms
64 bytes from 192.168.80.10: icmp_seq=5 ttl=64 time=0.876 ms
^C
--- 192.168.80.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.503/0.622/0.876/0.133 ms
root@kali:~# nmap 192.168.80.10

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-08-19 10:48 EDT
Nmap scan report for 192.168.80.10
Host is up (0.00050s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:B2:A6:4F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
root@kali:~#
```

Figure 6: Port Scan Attack

From figure 6 able to see that the attacker successfully port scan the server. From the content of the terminal able to see that the server port 80 is open and another 999 port is closed.

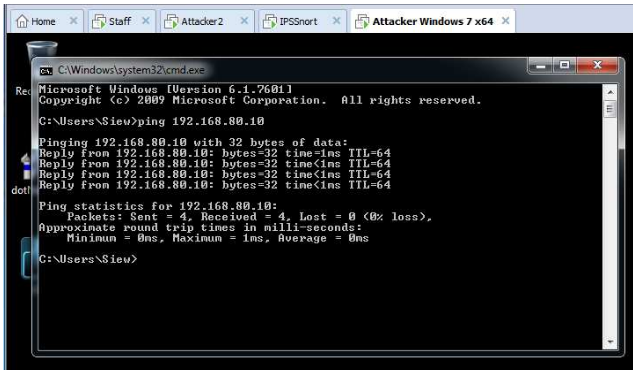


```
64 bytes from 192.168.80.10: icmp_seq=4 ttl=64 time=0.503 ms
64 bytes from 192.168.80.10: icmp_seq=5 ttl=64 time=0.876 ms
^C
--- 192.168.80.10 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3999ms
rtt min/avg/max/mdev = 0.503/0.622/0.876/0.133 ms
root@kali:~# nmap 192.168.80.10

Starting Nmap 7.25BETA2 ( https://nmap.org ) at 2017-08-19 10:48 EDT
Nmap scan report for 192.168.80.10
Host is up (0.00050s latency).
Not shown: 999 closed ports
PORT   STATE SERVICE
80/tcp open  http
MAC Address: 00:0C:29:B2:A6:4F (VMware)

Nmap done: 1 IP address (1 host up) scanned in 13.34 seconds
root@kali:~# ping 192.168.80.10
PING 192.168.80.10 (192.168.80.10) 56(84) bytes of data.
^C
--- 192.168.80.10 ping statistics ---
9 packets transmitted, 0 received, 100% packet loss, time 7999ms

root@kali:~#
```

Figure 7: Post Attack Testing

Figure 7 shows that the attacker machine is unable to ping the server after the attack. It proved that the IPS blocks the connection from attacker IP automatically. The attacker had sent 9 pings and the server did not give any response to the attacker so there show 9 packets are sent and 100% packet loss.

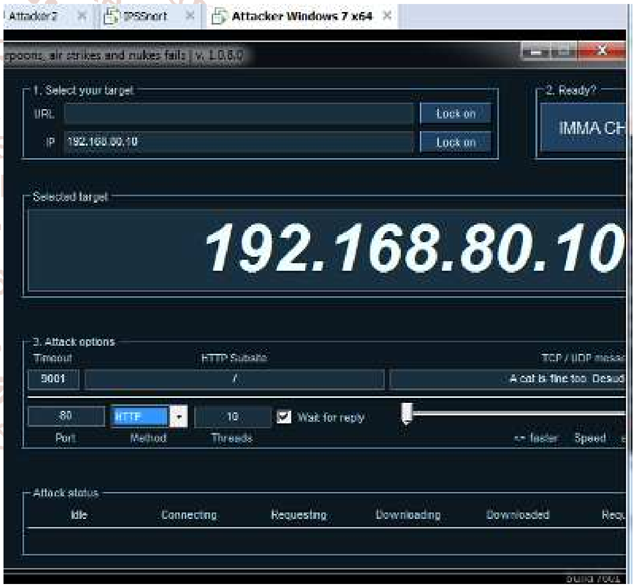
DOS attack



```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Users\Siew>ping 192.168.80.10

Pinging 192.168.80.10 with 32 bytes of data:
Reply from 192.168.80.10: bytes=32 time=1ms TTL=64
Reply from 192.168.80.10: bytes=32 time<1ms TTL=64
Reply from 192.168.80.10: bytes=32 time<1ms TTL=64
Reply from 192.168.80.10: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.80.10:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Users\Siew>
```

Figure 8: Pretest

Figure 8 shows that the attacker Pc is successfully pinged the server before the attack. It means that the connection from an attacker with the server is up.



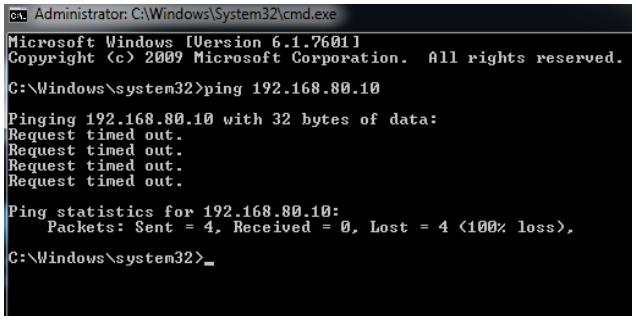
URL
IP 192.168.80.10

Selected target
192.168.80.10

Timeout 9001
HTTP Subsite /
TCP / UDP messa A cat is fine too. Desud
Port 80
Method HTTP
Threads 10
☑ Wait for reply

Figure 9: DOS Attack

In figure 9 showed the Windows attacker start attack with LOIC software. This is an open source stress testing software for the server by launching Dos attack to the server. From the figure above shows that attacker is Lock on the server IP and chose port 80 and HTTP types of packets sent to the server.

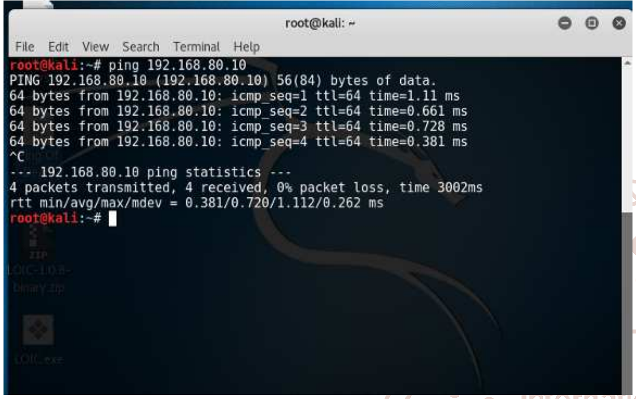


```
Microsoft Windows [Version 6.1.7601]
Copyright (c) 2009 Microsoft Corporation.  All rights reserved.

C:\Windows\system32>ping 192.168.80.10

Pinging 192.168.80.10 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.80.10:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\system32>_
```

Figure 10: Post Test

Figure 10 is using attacker to ping server after the Dos attack. From this screenshot able to see that the attacker is failed to ping the server. The result from attacker to ping server after the attack it shown request timeout.

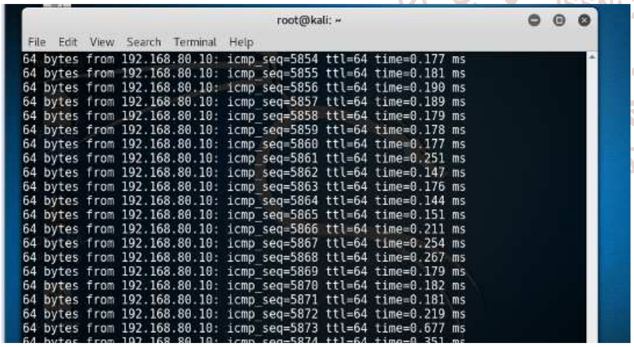
Ping of Death



```
root@kali:~# ping 192.168.80.10
PING 192.168.80.10 (192.168.80.10) 56(84) bytes of data.
64 bytes from 192.168.80.10: icmp_seq=1 ttl=64 time=1.11 ms
64 bytes from 192.168.80.10: icmp_seq=2 ttl=64 time=0.661 ms
64 bytes from 192.168.80.10: icmp_seq=3 ttl=64 time=0.728 ms
64 bytes from 192.168.80.10: icmp_seq=4 ttl=64 time=0.381 ms
^C
--- 192.168.80.10 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3002ms
rtt min/avg/max/mdev = 0.381/0.720/1.112/0.262 ms
root@kali:~# █
```

Figure 11: Pretest

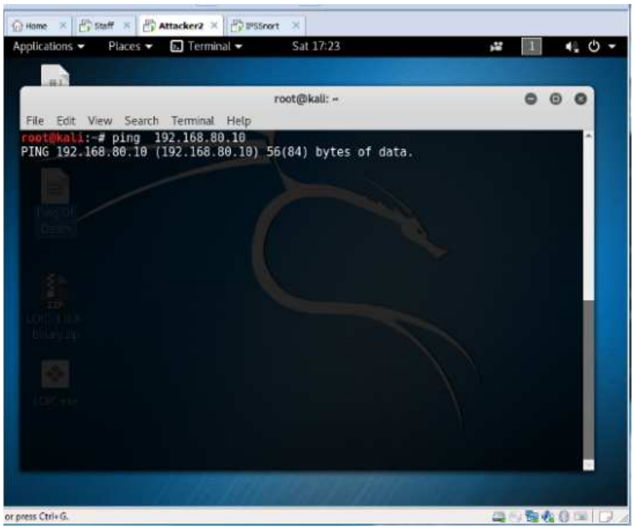
The figure 11 is the attacker pc try to ping the server and from the screenshot able to see that the ping from attacker to the server before the attack is successful.



```
64 bytes from 192.168.80.10: icmp_seq=5854 ttl=64 time=0.177 ms
64 bytes from 192.168.80.10: icmp_seq=5855 ttl=64 time=0.181 ms
64 bytes from 192.168.80.10: icmp_seq=5856 ttl=64 time=0.190 ms
64 bytes from 192.168.80.10: icmp_seq=5857 ttl=64 time=0.189 ms
64 bytes from 192.168.80.10: icmp_seq=5858 ttl=64 time=0.179 ms
64 bytes from 192.168.80.10: icmp_seq=5859 ttl=64 time=0.178 ms
64 bytes from 192.168.80.10: icmp_seq=5860 ttl=64 time=0.177 ms
64 bytes from 192.168.80.10: icmp_seq=5861 ttl=64 time=0.251 ms
64 bytes from 192.168.80.10: icmp_seq=5862 ttl=64 time=0.147 ms
64 bytes from 192.168.80.10: icmp_seq=5863 ttl=64 time=0.176 ms
64 bytes from 192.168.80.10: icmp_seq=5864 ttl=64 time=0.144 ms
64 bytes from 192.168.80.10: icmp_seq=5865 ttl=64 time=0.151 ms
64 bytes from 192.168.80.10: icmp_seq=5866 ttl=64 time=0.211 ms
64 bytes from 192.168.80.10: icmp_seq=5867 ttl=64 time=0.254 ms
64 bytes from 192.168.80.10: icmp_seq=5868 ttl=64 time=0.267 ms
64 bytes from 192.168.80.10: icmp_seq=5869 ttl=64 time=0.179 ms
64 bytes from 192.168.80.10: icmp_seq=5870 ttl=64 time=0.182 ms
64 bytes from 192.168.80.10: icmp_seq=5871 ttl=64 time=0.181 ms
64 bytes from 192.168.80.10: icmp_seq=5872 ttl=64 time=0.219 ms
64 bytes from 192.168.80.10: icmp_seq=5873 ttl=64 time=0.677 ms
64 bytes from 192.168.80.10: icmp_seq=5874 ttl=64 time=0.351 ms
```

Figure 12: Launch Ping of Death

Figure 12 shows the attacker use the Ping of Death method from attacker to server. This is an attack keep on sending a ping packet to the server. The command for this attack shown below.
Command: ping –I 0 (server ip)
Example: ping –I 0 192.168.80.10



```
root@kali:~# ping 192.168.80.10
PING 192.168.80.10 (192.168.80.10) 56(84) bytes of data.
```

Figure 13: Post Test

From figure 13 show that the attacker no longer able to ping server after the attack. This also shown that the experiment for this attack also successful. From above shown 3 types of attacks to servers. These 3 types of attacks experiment are not only 1 to 1 machine testing. For all 3 experiments also included another 1 machine act as company staff to test the connection to prevent the IPS will block all the connection including local staff connection.

5. Limitation

The limitation for this project is not enough memory resources to perform the DOS attack due to some attack need high memory consumption. So may have some delay error during the experiment. Furthermore, due to the time limitation of this project only 31 respondents for the questionnaire and only 3 attacks is tested.

REFERENCE

[1] T. Hunt, "Cyber Security Awareness in Higher Education," *Central Washington University*, 2016.

[2] A. VERMA, "World's Largest 1Tbps DDoS Attack Launched From 152,463 Hacked Devices," *Foss Bytes*, 2016. [Online]. Available: https://fossbytes.com/1tbps-worlds-largest-ddos-attack-launched-152000-hacked-iot-devices/. [Accessed: 30-Sep-2016].

[3] Kang, C.M., JosephNg, P.S. & Issa, K. (2015), A study on integrating penetration testing into the information security framework for Malaysian higher education institution, International Conference on Mathematical Sciences and Computing Research (ISMSC), pp. 156-161

[4] M. Darwish, A. Ouda, and L. F. Capretz, "Cloud-based DDoS attacks and defences," *Inf. Soc. (i-Society), 2013 Int. Conf.*, pp. 67–71, 2013.

[5] B. Y. L. J. Diaz, M. C. Anderson, J. T. Wolak, and D. Opderbeck, "The Risks and Liability of Governing Board Members to Address Cyber Security Risks in Higher Education.," *JC UL*, vol. 43, p. 49, 2017.

[6] Panda, B. Kumar, M. Pradhan, and S. Pradhan, *Network Security Attacks and Countermeasures*. IGI Global, 2016.

[7] JosephNg, P.S. (2018), EaaS Optimization: Available yet hidden information technology infrastructure inside medium size enterprise, *Technology Forecasting and Social Changes,* 132(7), pp. 165-173

[8] JosephNg, P.S. *et al.*, (2016), EaaS : Available yet Hidden Infrastructure inside MSE, *ACM International Conference on Network, Communication, and Computing, Kyoto, Japan*, 2016, vol. 17, no. 21, pp. 17–21.

[9] JosephNg, P.S. & Kang, C.M. (2016), Beyond Barebone Cloud Infrastructure Services: Stumbling Competitiveness During Economic Turbulences, *Journal of Science & Technology*, 24(1), pp. 101-121.

[10] JN, P.S. *et al.,* (2016), Exostructure Services for Infrastructure Resources Optimization, *Journal of Telecommunication, Electronic and Computer Engineering*, 8(4), pp. 65-69

[11] Joseph, N.P.S.; Choo, P.Y.; Wong, S.W.; Phan, K.Y. & Lim, E.H. (2012), Hibernating ICT infrastructure during rainy days, *Journal of Emerging Trends in Computing & Information Sciences,* 3(1); pp. 112-116

[12] X. Jia, D. Ren, Y. Yang, H. Li, and S. Guozi, “DFIPS : Toward Distributed Flexible Intrusion Prevention System in Software Defined Network,” *SEKE*, pp. 124–127, 2016.

[13] S. K. Batumalai *et al.*, (2015), IP Redundancy and Load Balancing With Gateway Load Balancing Protocol, *Int. J. Sci. Eng. Technol.*, 4(3), pp. 218–222

[14] A. M. A. Mohamed et al., (2015), Hot Standby Router Protocol for a Private University in Malaysia, *Int. J. Sci. Eng. Technol.*, 4(3), pp. 172-174

[15] SHR Abdullaa et al., (2013), Implementing of Virtual Router Redundancy Protocol in a Private University, Journal of Industrial and Intelligent Information, 1(4), pp. 255-259

[16] Siew, J. X. et al., (2016). ECO QR Car Park System. International Journal of Scientific Engineering and Technology, 6(5), 176-180.

[17] L. Lim et al., (2016) “ScareDuino: Smart Farming with IOT,” International Journal of Scientific Engineering and Technology, 6(5), 207-210.

[18] J. M. Morse, “Approaches to qualitative-quantitative methodological triangulation,” *Natl. Multi-Specialty Nurs. Conf. Urin. Cont.*, vol. 40, no. 2, pp. 120–123, 1991.