Journal of Information & Communication Technology
Vol. 3, No. 1, (Spring 2009) 01-10

Reliable and Security-Based Myren Network Traffic Management using Open Source Tools

Mohamed Othman*
Mostafa Nikpour Kermanian*
Department of Communication Technology and Network,
Faculty of Computer Science and Information Technology,
University Putra Malaysia, Malaysia

ABSTRACT

Network Security is one the main issues in each network and should be implemented based on the infrastructure design of the target network. Most of computer networks suffer from the shortage of a tight security policies. This paper is based on a practical improvement which is done in University Putra Malaysia to secure Malaysian National Research and Education Network (Myren) networks' transactions. In this improvement, layer two to layer seven of Open System Interconnection (OSI) layer are secured based on Cisco devices and open source utilities. Linux iptables package not only controls accesses from internet users to data-center servers but also controls local area network users' transactions to the data-center servers. This firewalling package protects all inside users from outside intruders' threats. Firewall packages can not detect and prevent protocol weakness, denial of service and viruses attacks. To overcome these firewalling weaknesses, intrusion prevention system which is bases on snort package is used to improve the security of the UPM server-farm. After implementing the proposed infrastructure of Myren network, it is obvious that most of network attacks are dropped by firewalling and intrusion prevention system mechanisms.

INSPEC Classification : C3110, C5620, C3370, D4045

Keywords : Linux iptables firewall, snort Instruction Prevention System (IPS), Monitoring tool

1. INTRODUCTION

Network security is one of the hottest issues in networks infrastructure design where places have a lot of invaluable assets to be protected from inside and outside threats. Most of the attacks (about 80%) are generated in Local Area Network (LAN), and 20% are Internet menaces. Firewall systems are essential tools to protect networks and reduce network traffics by defined rules and Quality of Service (QoS) mechanism on them. Firewall types are divided in three categories (Feinstein, L. and D. Schnackenberg, 2005), (Rajan, S., 2005), (Nutanong, S., 2004).

- Stateful packet filter
- Application proxy
- Hybrid

* The material presented by the authors does not necessarily portray the viewpoint of the editors and the management of the Institute of Business and Technology (BIZTEK) or University Putra Malaysia, Malaysia.

*Mohamed Othman : mothman@fsktm.upm.edu.my

*Mostafa Nikpour Kermanian : m_nickpour@yahoo.com

Packet inspection / filtering gateways are not able to process the packet to the application level to make a filtering decision. Instead, packet inspection gateways tend to process the data to the network / transport layer and make filtering decisions based on the protocol and the port numbers contained in the packet header only. Application proxies are identified by their ability to read and process an entire packet to the application level and make filters decision based on the actual application data, not just the packet header (Nutanong, S., 2004). Application proxies receive all incoming packets and completely decode them to the application layer. The actual application data can then be scrutinized to determine whether it is legitimate data. If this data is legitimate, the firewall will rebuild the packet and forward it accordingly. More and more firewalls today fall into the hybrid category. Although they typically perform stateful packet filtering / inspecting for making filtering decision, they may have some application proxy functionalities built in for specific high-risk protocols and services such as HTTP and FTP. Most attacks which are generated in Layer 2, are critical and should be controlled with layer 2 devices (Döring, C., 2005) . Switches are layer 2 devices which should detect these kinds of attacks and drop them. Most of the layer two switches do not have ability to reduce layer two attacks; they just decrease collision and work in full duplex. Some brands like Cisco, Nortel and Foundry can protect the networks from layer two attacks (Cisco Company, 2008). Layer 2 attacks:

- CAM table overflow
- VLAN hopping
- Spanning-Tree Protocol manipulation
- Media Access Control (MAC) Address spoofing
- Private VLAN
- DHCP "starvation"

The content addressable memory (CAM) table in a switch contains information such as the MAC addresses available on a given physical port of a switch, as well as the associated VLAN parameters. When a Layer 2 switch receives a frame, the switch looks in the CAM table for the destination MAC address. If an entry exists for the MAC address in the CAM table, the switch forwards the frame to the port designated in the CAM table for that MAC address. If the MAC address does not exist in the CAM table, the switch forwards the frame out every port on the switch, effectively acting like a hub. If a response is seen, the switch updates the CAM table.

CAM tables are limited in size. If enough entries are entered into the CAM table before other entries are expired, the CAM table fills up to the point that no new entries can be accepted. Typically a network intruder will flood the switch with a large number of invalid-source MAC addresses until the CAM table fills up. When that occurs the switch will flood all ports with incoming traffic because it cannot find the port number for a particular MAC address in the CAM table. The switch, in essence, acts like a hub. If the intruder does not maintain the flood of invalid-source MAC addresses, the switch will eventually time out older MAC address entries from the CAM table and begin to act like a switch again. CAM table overflow only floods traffic within the local VLAN so the intruder will see only traffic within the local VLAN to which he or she is connected (Cisco Company, 2008).

In May of 1999 the tool macof was released. It was written in approximately 100 lines of PERL code and was later ported to C language code and incorporated into the dsniff package. This tool floods a switch with packets containing randomly generated source and destination MAC and IP addresses. When the switch's CAM table fills up with these addresses, the switch begins to forward all frames it receives to every port. The CAM table-overflow attack can be mitigated by configuring port security on the switch. This option provides for either the specification of the MAC addresses on a particular switch port or the specification of the number of MAC addresses that can be learned by a switch port. When an invalid MAC address is detected on the port, the switch can either block the offending MAC address or shut down the port. Specifying MAC addresses on switch

ports is far too unmanageable a solution for a production environment. Limiting the number of MAC addresses on a switch port is manageable. A more administratively scalable solution would be the implementation of dynamic port security at the switch. To implement dynamic port security, specify a Maximum number of MAC addresses that will be learned (Cisco Company, 2008).

1.1 VLAN Hopping

VLAN hopping is a network attack whereby an end system sends out packets destined for a system on a different VLAN that cannot normally be reached by the end system. This traffic is tagged with a different VLAN ID to which the end system belongs. Or, the attacking system may be trying to behave like a switch and negotiate trunking so that the attacker can send and receive traffic between other VLANs (Cisco Company, 2008).

Switch Spoofing - In a VLAN hopping attack, the network attacker configures a system to spoof itself as a switch. This requires that the network attacker be capable of emulating either ISL or 802.1q signaling along with Dynamic Trunk Protocol (DTP) signaling. Using this method a network attacker can make a system appear to be a switch with a trunk port. If successful, the attacking system then becomes a member of all VLANs.

Double Tagging - Another version of this network attack involves tagging the transmitted frames with two 802.1q headers in order to forward the frames to the wrong VLAN. The first switch to encounter the doubletagged frame (1) strips the first tag off the frame and forwards the frame. The result is that the frame is forwarded with the inner 802.1q tag out all the switch ports (2) including trunk ports configured with the native VLAN of the network attacker. The second switch then forwards the packet to the destination based on the VLAN identifier in the second 802.1q header. Mitigating VLAN hopping attacks requires several modifications to the VLAN configuration. One of the more important elements is to use dedicated VLAN IDs for all trunk ports. Also, disable all unused switch ports and place them in an unused VLAN. Set all user ports to nontrunking mode by explicitly turning off DTP on those ports (Cisco Company, 2008).

1.2 Spanning-Tree Protocol Manipulation

Another attack against switches involves intercepting traffic by attacking the Spanning-Tree Protocol. This protocol is used in switched networks to prevent the creation of bridging loops in an Ethernet network topology (Cisco Company, 2008). Upon bootup the switches begin a process of determining a loop-free topology. The switches identify one switch as a root bridge and block all other redundant data paths.

By attacking the Spanning-Tree Protocol, the network attacker hopes to spoof his or her system as the root bridge in the topology. To do this the network attacker broadcasts out Spanning-Tree Protocol Configuration/Topology Change Bridge Protocol Data Units (BPDUs) in an attempt to force spanning-tree recalculations. The BPDUs sent out by the network attacker's system announce that the attacking system has a lower bridge priority. If successful, the network attacker can see a variety of frames. By transmitting spoofed Spanning-Tree Protocol packets, the network attacker causes the switches to initiate spanning-tree recalculations that then result in the two connections to the network attacker's system to forward packets. To mitigate Spanning-Tree Protocol manipulation use the root guard and the BPDU guard enhancement commands to enforce the placement of the root bridge in the network as well as enforce the Spanning-Tree Protocol domain borders. The root guard feature is designed to provide a way to enforce the root-bridge placement in the network.

The Spanning-Tree Protocol BPDU guard is designed to allow network designers to keep the active network topology predictable. While BPDU guard may seem unnecessary given that the administrator can set the bridge priority to zero, there is still no guarantee that it

will be elected as the root bridge because there might be a bridge with priority zero and a lower bridge ID. BPDU guard is best deployed towards user-facing ports to prevent rogue switch network extensions by an attacker (Cisco Company, 2008).

1.3 MAC Spoofing Attack

MAC spoofing attacks involve the use of a known MAC address of another host to attempt to make the target switch forward frames destined for the remote host to the network attacker (Cisco Company, 2008). By sending a single frame with the other host's source Ethernet address, the network attacker overwrites the CAM table entry so that the switch forwards packets destined for the host to the network attacker. Until the host sends traffic it will not receive any traffic. When the host sends out traffic, the CAM table entry is rewritten once more so that it moves back to the original port.

Use the port security commands to mitigate MAC-spoofing attacks. The port security command provides the capability to specify the MAC address of the system connected to a particular port. The command also provides the ability to specify an action to take if a port-security violation occurs. However, as with the CAM table-overflow attack mitigation, specifying a MAC address on every port is an unmanageable solution. Hold-down timers in the interface configuration menu can be used to mitigate ARP spoofing attacks by setting the length of time an entry will stay in the ARP cache. However, hold-down timers by themselves are insufficient. Modification of the ARP cache expiration time on all end systems would be required as well as static ARP entries. Even in a small network this approach does not scale well. One solution would be to use private VLANs to help mitigate these network attacks (Cisco Company, 2008).

1.4 Private VLAN Attacks

While private VLANs are a common mechanism to restrict communications between systems on the same logical IP subnet, they are not a full-proof mechanism. Private VLANs work by limiting the ports within a VLAN that can communicate with other ports in the same VLAN. Isolated ports within a VLAN can communicate only with promiscuous ports. Community ports can communicate only with other members of the same community and promiscuous ports. Promiscuous ports can communicate with any port. One network attack capable of bypassing the network security of private VLANs involves the use of a proxy to bypass access restrictions to a private VLAN (Cisco Company, 2008).

- Proxy Attack-In this network attack against private VLANs, frames are forwarded to a host on the network connected to a promiscuous port such as a router.

Configure Access Control Lists (ACLs) on the router port to mitigate private VLAN attacks. Virtual ACLs can also be used to help mitigate the effects of private VLAN attacks. An example of using ACLs on the router port is if a server farm segment were 172.16.34.0/24, then configuring the following ACLs on the default gateway would mitigate the private VLAN proxy attack.

1.5 DHCP Starvation

A DHCP starvation attack works by broadcasting DHCP requests with spoofed MAC addresses (Cisco Company, 2008). This is easily achieved with attack tools such as gobbler. This is a simple resource starvation attack just like a SYN flood is a starvation attack. The network attacker can then set up a rogue DHCP server on his or her system and respond to new DHCP requests from clients on the network. Exhausting all of the DHCP addresses is not required to introduce a rogue DHCP server, though. As stated in RFC 2131: "The client collects DHCPOFFER messages over a period of time, selects one DHCPOFFER message from the (possibly many) incoming DHCPOFFER messages and extracts the server address from the 'server identifier' option in the DHCPOFFER message. The times

over which the client collects messages and the mechanism used to select one DHCPOFFER are implementation dependent."

By placing a rogue DHCP server on the network, a network attacker can provide clients with addresses and other network information. Since DHCP responses typically include default gateway and DNS server information, the network attacker can supply his or her own system as the default gateway and DNS server resulting in a "man-in-the-middle" attack.

The techniques that mitigate CAM table flooding also mitigate DHCP starvation by limiting the number of MAC addresses on a switch port. As implementation of RFC 3118, Authentication for DHCP Messages, increases, DHCP starvation attacks will become more difficult.

Additional features in the Catalyst family of switches, such as the DHCP snooping command, can be used to help guard against a DHCP starvation attack. DHCP snooping is a security feature that filters untrusted DHCP messages and builds and maintains a DHCP snooping binding table. The binding table contains information such as the MAC address, IP address, lease time, binding type, VLAN number and the interface information corresponding to the local untrusted interfaces of a switch. Untrusted messages are those received from outside the network or firewall and untrusted switch interfaces are ones that are configured to receive such messages from outside the network or firewall.

Other Catalyst switch features such as IP Source Guard can provide additional defense against attacks such as DHCP starvation and IP spoofing. Like DHCP snooping, IP source guard is enabled on untrusted Layer 2 ports. All IP traffic is initially blocked except for DHCP packets captured by the DHCP snooping process. Once a client receives a valid IP address from the DHCP server a per-port and VLAN access control list (PACL) is applied to the port. This restricts the client IP traffic to those source IP addresses configured in the binding. Any other IP traffic with a source address other than the addresses in the binding will be filtered.

One method of preventing a rogue DHCP server from responding to DHCP Requests utilizes VACLs (Cisco Company, 2008). While the use of VACLs does not entirely eliminate the possibility of a rogue DHCP server since IP spoofed DHCP messages are still possible but more difficult to successfully implement. The VACLs can be used to limit DHCP replies to legitimate DHCP servers and deny these same replies from all others. A more effective method of defending against rogue DHCP servers is the application of DHCP snooping. This provides an excellent defense against potential rogue DHCP servers by placing all ports on the switch into an "untrusted" state and blocking any DHCP replies that servers make. Such replies would be DHCP OFFERs, ACK's or NAC's.

1.6 Intrusion Prevention Systems

Are firewall devices enough to have a secure network? This is a question in most system administrators' minds (Cisco Company, 2008). Although most of companies have a firewall to secure their inside resources from inside and outside threats, most of the times we see that their internal services are hacked by intruders. Although firewall machines reduce a huge number of attacks, they can not detect protocol weaknesses, denial of service attacks and neither viruses. These kinds of attacks are recognized and dropped by neural network devices. Intrusion Prevention Systems (IPS) are such neural network devices which can protect networks from these noted firewall weaknesses. They check all signatures of the packets and if they do not have any hacking signature, permit them to pass IPS interface otherwise; drop them. IPS rules should be updated periodically to improve networks' security. Snort is an open source Intrusion detection system which can be installed in GNU license and monitor networks' traversed packets and also with Snort-inline module it can be as an IPS. This module not only monitors traversed packets but also drop intruders'

attacks to the network resources. You can find useful information about snort package in the following website: http://www.snort.org

2. MYREN NETWORK

All universities of Malaysia are connected to each other by Myren link in order to share their databases for each other. This link not only connects Malaysian universities to each other but also it connects Malaysian research network to the international research communities in Asia Pacific, Europe and North America via the Trans Eurasia Information Network 2 (TEIN2) (Myren Network, 2008). University Putra Malaysia (UPM) has a connection to this research area through Myren link. Although inside users could access online databases of other Universities and also outside users could access UPM research databases, this connection was in lack of proper security mechanisms.

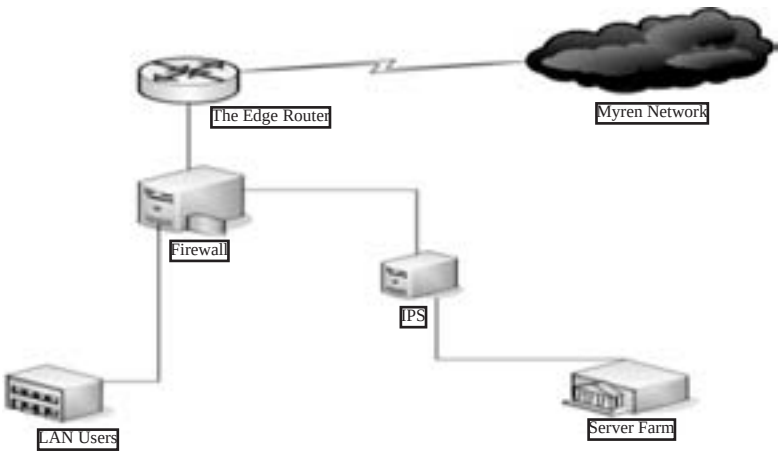
3. PROPOSED NETWORK INFRASTRUCTURE FOR MYREN NETWORK

To improve security in the proposed network infrastructure which is depicted in Fig 1, a new virtual local area network (VLAN) is implemented for data-center servers. This VLAN not only separates the servers of the server-farm from Internet users but also separates server-farm resources from local area network (LAN). In the other hand, all the requests from LAN should be routed to the server-farm zone to reach the resources of the servers. This routing of LAN packets is done on by the firewall machine.

The operational ports of the server-farm servers are opened by iptables package to NAT the traffic with trusted destination port to the proper server in the server-farm. This firewall package is a stateful packet filter which controls the states of all packets to increase network security. After that, those packets which are allowed by the firewall to reach the servers should be checked by intrusion prevention machine to be granted to reach the servers. To permit the traffic to the server-farm servers, snort checks the signatures of the packets. If the signatures of the packets do not have any hacking pattern, they are allowed by snort package to be transmitted to their destinations otherwise; those are dropped by IPS rules.

All internal and external requests to the server-farm servers should be checked by firewall and intrusion prevention systems to access to the resources of servers in the server-farm.

Fig. 1
Proposed Myren Network Infrastructure



4. DESIGN AND IMPLEMENTATION

To implement the proposed network infrastructure, layer two attacks are controlled and prevented by Cisco switches. To achieve this goal, VTP domain is implemented on LAN Cisco switches. In this case, some powerful switches are selected as VTP servers and the rest of network switches are configured as VTP clients. All VLAN configurations are passed from VTP servers to VTP clients automatically to reduce network administrators' overhead. To mitigate layer two attacks, following commends are used on these switches.

VLAN HOPPING
IOS(config-if)# switchport mode access

SPANNING TREE MANIPULATION
IOS(config)# spanntree portfast
IOS(config)# spanning-tree bpduguard enable

MAC SPOOFING
IOS(config-if)#port security max-mac-count 1
IOS(config-if)#port security violation shutdown
IOS(config-if)#arp timeout 30

DHCP SNOOPING
IOS(config)#ip dhcp snooping
IOS(config)#ip dhcp snooping vlan 1
IOS(config-if)#ip dhcp snooping trust
IOS(config-if)#ip dhcp snooping limit rate 100

PRIVATE VLAN ATTACK
IOS(config)#access-list 101 deny ip 192.168.0.1 0.0.0.255 log
IOS(config)#access-list 101 permit ip any any
IOS(config)#ip access-group 101 in

CISCO DISCOVERY PROTOCOL
IOS(config)#no cdp run
IOS(config-if)#no cdp enable

VLAN TRUNKING PROTOCOL
IOS#vtp password Pass

After protecting LAN users and server-farm servers from layer two attacks, WAN perimeter router is secured by upgrading its IOS to the IOS with firewall feature. This kind of IOS has deep-inspection mechanism to drop most of network attacks. Deep-inspection mechanism is based on Context Based Access Control (CBAC). CBAC provides advanced traffic-filtering functionality and can be used as an integral part of networks firewall. Furthermore, all unnecessary services are disabled on Cisco edge router. To access to the router, different users with different privileges (access level permission) are defined on router and also by enabling syslog feature on edge router, all the events would be recorded in the syslog server to be loged and monitored for feature reports. SSH protocol is enabled on Cisco router instead of telnet protocol for remote management because telnet is one of the unsecured mechanisms to access Cisco devices remotely. In telnet mechanism, all username, passwords and data are transferred in clear text mode.

Firewall package which is based on Linux iptables is enabled on firewall machine to protect ingress and egress data transmissions. In this network infrastructure design, iptables is in route mode and ip_forward feature is enabled on Linux kernel. Invalid sessions and also

icmp protocols are controlled by following firewall rules in order to increase network security by dropping unwanted traffics.

-A INPUT -p tcp -m tcp ! --tcp-flags SYN,RST,ACK SYN - m state --state NEW -j DROP
-A INPUT -p tcp -m state --state INVALID -j DROP
-A INPUT -p icmp -m icmp --icmp-type 8 -j DROP
-A INPUT -p icmp -m icmp --icmp-type 3/4 -j ACCEPT
-A FORWARD -p icmp -m icmp --icmp-type 0 -j DROP

Essential rules are applied to protect servers of the server-farm from outside and inside threats. After implementing firewall machine, IPS mechanism is applied to the Myren network infrastructure to improve its security.

Although firewall package is a reputed stateful packet filter to secure the transactions of the network, it has the following weakness:

- Can not detect protocol weaknesses
- Can not detect Denial Of Service Attacks
- Can not detect viruses, Trojans

Overcoming to these weaknesses can be done by using intrusion prevention systems. Snort package with snort_inline module is installed as the IPS package to protect the server-farm services. In this case, all trusted traffics which are passed through the firewall machine should be checked with snort package to reach services. IPS package is configured as Network Intrusion Detection and Prevention System (NIPS). All logs of snort package are in text mode and analyzing them is very difficult. To make these logs understandable, ACID package is installed and configured to show them in categorized mode.

To increase the security of servers, a version of Host based Intrusion detection and Prevention System (HIPS) is installed and configured on each machine. This HIPS is based on Blackice software with the capability of attack prevention to drop the intruders' threats. If snort package dose not have a proper rule to drop an attack, Blackice package would detect and prevent that threat. Not only these three levels of intrusion prevention systems which are configured on the Router, IPS machine and servers but also two levels of firewalling which are implemented on network switches and the edge firewall of the network can improve the security of services which are accessible in UPM University.

5. RESULTS AND DISCUSSIONS

Fig. 2
shows the traffic of Myren network before applying this proposed infrastructure design.

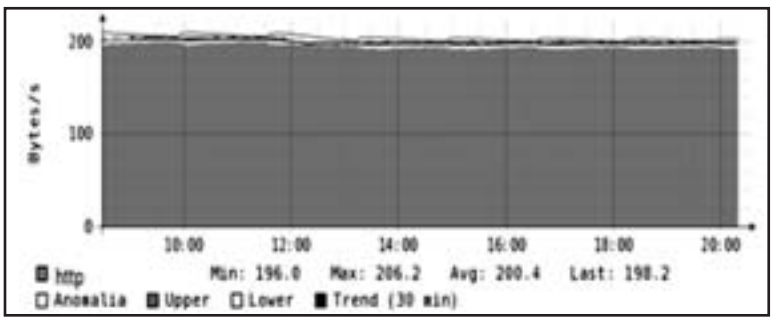


Fig 2 Traffic flow before applying firewall rules

As Fig. 2 shows, the traffic and bandwidth usage of Myren network which was engaged by many untrusted traffics.

After implementing the proposed network infrastructure which is depicted in Fig 1, network security and service reliability increased. Many attacks dropped by the router IPS module, Linux firewall and intrusion prevention system. Penetration tests were used to check the hardening of proposed design.

tcpdum on firewall machine is used to monitor the traversed traffic during the period of attacking to the system resources from inside and outside of the campus. The following logs show that unwanted traffics are dropped by *iptables* firewall module on firewall machine:

Mar 2 10:06:40 linux kernel: SuSE-FW-DROP-DEFAULT IN=eth0 OUT=eth1
MAC=00:50:da:c5:9d:8b:00:0c:6e:8c:d4:61:08:00 SRC=x.x.x.x
DST=192.168.1.108 LEN=40 TOS=0x08 PREC=0x00 TTL=64 ID=45106 PROTO=TCP
SPT=1321 DPT=80 WINDOW=512 RES=0x00 SYN URGP=0

Mar 2 10:24:30 linux kernel: SuSE-FW-DROP-DEFAULT IN=eth0 OUT= eth1
MAC=00:50:da:c5:9d:8b:00:0c:6e:8c:d4:61:08:00 SRC=x.x.x.x
DST=192.168.1.108 LEN=28 TOS=0x10 PREC=0x00 TTL=64 ID=47873
PROTO=UDP SPT=2180 DPT=53 LEN=8

These outputs show that firewall works properly. To monitor the trend of protection of Myren network by IPS machine, we checked the dropped packets log. The following logs show that snort_inline package could drop intruders' attacks.

Log 1:
[**] [119:4:1] (http_inspect) BARE BYTE UNICODE ENCODING [**]
01/16-14:40:35.353241 00-14-A5-D5-39-24:33478 -> 00-14-A5-D5-39-32:80
TCP TTL:240 TOS:0x10 ID:0 IpLen:20 DgmLen:106
AP Seq: 0x804AF2DF Ack: 0x3061FFC7 Win: 0x16D0 TcpLen: 20

Log 2:
[**] [1:2274:1] POP3 login brute force attempt [**]
[Classification: An attempted login using a suspicious username was detected] [Priority: 2]
01/16-14:48:16.763825 00-14-A5-D5-39-24:33663 -> 00-14-A5-D5-39-32:110
TCP TTL:64 TOS:0x0 ID:46834 IpLen:20 DgmLen:74 DF
AP Seq: 0xA10E020F Ack: 0xED46058A Win: 0x16D0 TcpLen: 32 TCP Options (3) => NOP NOP TS: 1291491 925414768

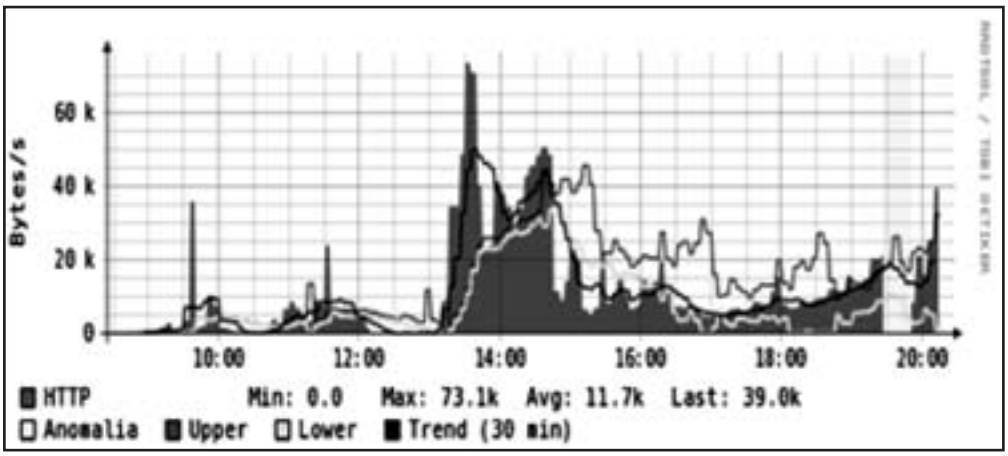
Log 3:
[**] [1:1201:7] ATTACK-RESPONSES 403 Forbidden [**]
[Classification: Attempted Information Leak] [Priority: 2]
01/16-15:38:17.652364 00-14-A5-D5-39-24:80 -> 00-14-A5-D5-39-32:33796
TCP TTL:114 TOS:0x0 ID:11570 IpLen:20 DgmLen:398 DF
AP Seq: 0x3146A645 Ack: 0x5D1A0CEB Win: 0xFAF0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 15728304 1591586

Log 4:
[**] [1:1560:4] WEB-MISC /doc/ access [**]
[Classification: access to a potentially vulnerable web application] [Priority: 2]
01/16-16:27:27.831581 00-14-A5-D5-39-24:33932 -> 00-14-A5-D5-39-32:80
TCP TTL:64 TOS:0x0 ID:57581 IpLen:20 DgmLen:560 DF
AP Seq: 0x16202966 Ack: 0xB4CE8C70 Win: 0x16D0 TcpLen: 32
TCP Options (3) => NOP NOP TS: 1886611 369328338

[Xref => http://www.securityfocus.com/bid/318][Xref => http://www.bia2.com=CVE-1999-0678]

Http, pop3 login brute force attack and injection attacks are dropped by IPS system according to these logs. Fig. 3 shows the Myren traffic flow after applying firewalling and intrusion prevention mechanisms on this link.

Fig 3
Traffic flow after applying firewall rules



As Fig 3 shows the traffic of the Myren network which is become normal and also its bandwidth usage is saved after applying the proposed infrastructure design.

6. CONCLUSION

After analyzing captured data by firewall and intrusion systems it is obvious that, in this infrastructure design of the Myren networks, most of the threats were dropped by firewall and IPS devices. Furthermore, the Blackice HIPS which was installed on the servers as the third layer of intrusion prevention mechanism could recognize those threats which were not dropped by the upper two IPS systems.

As the future works, we should make clusters of firewall and IPS machines to overcome the single point of failure problem of this proposed infrastructure design.

REFERENCES

Feinstein, L. and D. Schnackenberg, Security and DOS control. 2004: Boeing Company.
Rajan, S., Linux firewall. 2005, Texas State University-San Marcos, Dept. of Computer Science
Nutanong, S., Effectiveness of network security frameworks across skill levels. 2004, Osaka University, Japan
Döring, C., Improving network security by using honey nets. 2005, University of Wisconsin-Platteville.
Cisco Company. 2008 [cited; Available from: www.cisco.com].
Myren Network. 2008 [cited; Available from: www.myren.net.my].