PREVENTION OF INTERNET PROTOCOL SPOOFING

ALIAH ALGASSMI

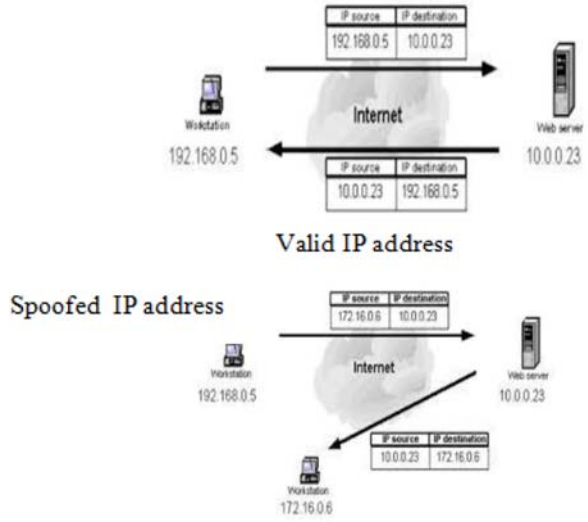
E-mail: Aliah13@windowslive.com

Abstract - The main purpose of writing this paper is to find solutions to detection and prevention spoofing in the internet protocol address (IP). Spoofing, in practical, indicates impersonating another machine or person, regularly by giving false information (IP address, URL or E-mail name). Spoofing can take several patterns in the computer, all of which include some sort false description of information. There are a diversity of approaches and kinds of spoofing. I would like to introduce and explain IP spoofing attacks in this paper. There are no constructive or legal practices for achieving spoofing of any type. Some of the results might be vindication, theft, sport, or another malicious goal. The magnitude of these crimes can be very critical; can cost us millions of dollars. This Paper will describes the detection and prevention of IP spoofing attack.

Index Terms - Spoofing, Filtering, Attacks, Information

I. INTRODUCTION

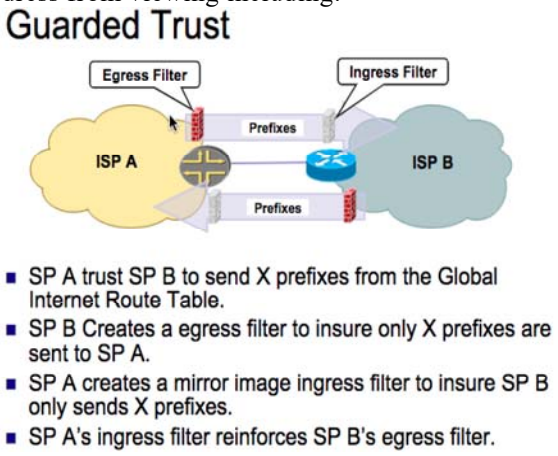
Internet Protocol ("IP") considers the primary protocol for transmitting data over the Internet network and several other computer networks .It is the header of each Internet Protocol source /packet and also consider the destination address of the packet. The source of the IP is usually the place which is the packet transmitted from. In the IP spoofing, by rigging the header to include another address, an intruder can produce it shows that the packet did transmit by another computer. Initially, the computer which gets the packets that became already spoofed, will transfer reply back to the faked address, that indicates this technique is essentially utilized when the criminal does not consider the response or the criminal has some plans of supposing the response. Criminals own hard manipulated the tactic of hiding their real identification, from disguises to nicknames to caller-id blocking. It must look as no wondering then, that criminals who carry their wicked actions on machines must apply such procedures. IP spoofing is a popular kind of online camouflage. through this spoofing, the criminal receives access which is unapproved to a machine or a the specific system by creating it look really trick which that malicious has get with a trusted device or network by doing the spoofing of IP address of that specific computer. In particular instances, it may be probable for the criminal to notice or redirect the response to his own network. In the most common situation is when the criminal makes spoofing attack from LAN or WAN on the same source address. Consequently, the person who did spoofing has illegally access through networks or machine. IP spoofing, in particular, is performing the forged source of Internet Protocol address with the intent of hiding the most important part which is the identification of the sender. In a spoofing attack, the intruder transfers information to a machine indicating that the report has taken from a trusted system. To be successful, the hacked need first find the IP address of a trusted system, and then adjust the packet headers to that it seems that the packets are getting from the trusted system. In reality, the criminal is tricking (spoofing) the distant machine into thinking that they are a true member of the network. The purpose of the attack is to build a connection that will allow the intruder to get root access to the host, allowing the making of a backdoor entry way into the target system. In this paper, I will examine how to defend against IP spoofing through execute ingress filtering, encrypting the Wireless Network, and my proposed solution among them which is monitoring the network traffic.



II. EXECUTE INGRESS FILTERING

IP spoofing is one of the most dangerous challenges that the Internet users face. It is a problem to which there must be plans to decrease its influences and increase awareness of it. There are many ways the user can follow to pretend the IP spoofing, one of them is execute ingress and egress filtering packets. Basically, egress and

ingress take the act of a checking point for the entering and exiting. Indeed, egress filtering works to monitor and control the outgoing information from the network to another, especially the private IP computer network to the Internet. On the other hand, ingress is a type of filtering packet that examine outbound traffic and permits the allowed packet to transfer to the network if they follow the administrator policies. Moreover, Ingress filtering is considering in the first line of network defense strategy. Ingress filtering exploits the Layer 2 IP address filtering capacity of a switch at the network's edge and squares movement that has a high likelihood of being spoofed. It makes this assurance dependent on whether the substance of an IP packet header meet characterized criteria. The packet filter analyzes a few qualities, most outstandingly for this situation the source IP address, if the source address is invalid or doesn't look like the originating network, the filter decides the IP address is spoofed (Rouse, 2017). Furthermore, ingress filtering designed to block various IP address from viewing including:



- The internal IP address
- Private IP address
- Loopback IP address
- Management network IP address
- Multicast IP address

III. ENCRYPTING THE WIRELESS NETWORK

One of the practical ways to prevent IP spoofing from occurring is by encrypting the wireless network so that trusted hosts that are outside my network can securely communicate with my local hosts. Consequently, it's essential to enable encryption when we set up the router by setting a specific password which will be required when we connect to the wireless network. The best way to make sure if we have enabled encryption in the beginning, we have to look for the wireless network name (SSID) in the list of available networks. If we see a padlock icon next to the network name that's a good sign that we're using encryption. Sometimes we have an encryption network turned on but at the same time it's not secure and that's happening when we use an outdated wireless encryption were the network will be easily hacked. Additionally, we have to figure out the different basic types of wireless security which are WPA and WPA2 (an upgraded version of WPA and it's more secure). However, we can easily identify which one we are using when we go to the wireless network configuration. Therefore, setting up a security upgrade is always recommended as we attempt to avoid IP spoofing from happening.

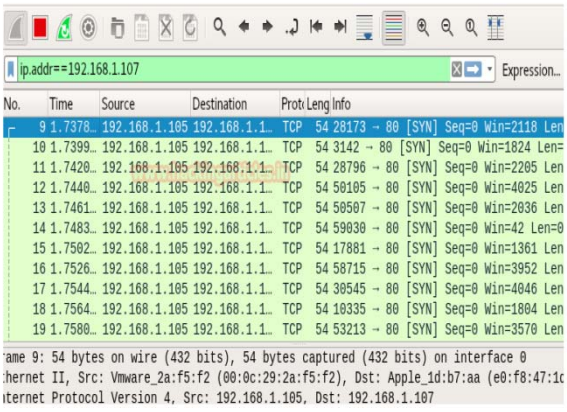
Moreover, relying on encryption as a solution of IP spoofing is really effective if we also enabled Transport Layer Security (TLS), Hypertext Transfer Protocol Secure (HTTPS), Secure Shell (SSH), and Secure Socket Layer (SSL). These protocols can do a great job to eliminate any futures risks by stopping any modification to the packet by encrypting it so the intruder who tries to hack the packet can't do his job anymore. Furthermore, when the packet reached its destination; authentication will be required. In addition, Secure Socket Layer has the ability to stop any communication that's not from a reliable source by providing a digital certificate, and an encryption key (symmetric and asymmetric keys). Besides that, Secure Socket Layer can also stop Man-in-the-Middle spoofing, blind and Non-blind spoofing. On the other hand, HTTPS can be seen on the browser address bar in Firefox, Internet Explorer and other web browsers as a padlock icon. HTTPS is the secure version of HTTP and it guarantees an encrypted connection between the website and the browser. Moreover, HTTPS typically uses an asymmetric Public Key Infrastructure (PKI) for encryption which is provided by one of the secure protocols like TLS or SSL. On the other hand, Secure Shell (SSH) allows users to modify and control their remote servers over the Internet by using some cryptographic techniques to ensure an encrypted communication. It also uses symmetric and asymmetric encryption the same as TLS and SSL. Additionally to that, Secure Shell Connections use a one-way hashing for encryption. Nevertheless, verifying the authenticity of messages is the main goal of hashing in SSH, also when the command received, Hash-based Message Authentication Codes (HMACs) guarantees that the message is not modified or tampered with in any way.

IV. MONITORING THE NETWORK TRAFFIC

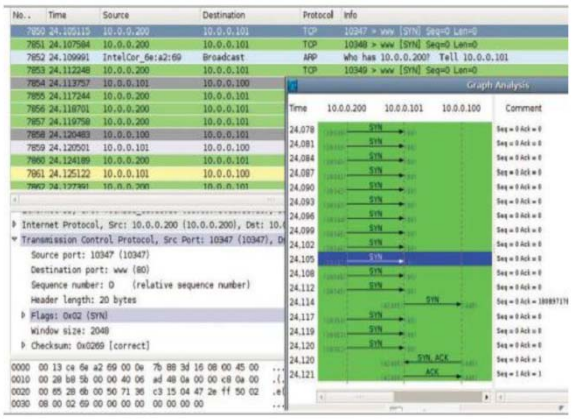
After viewing the previous solutions, I found out that the most effective solution to detect attacks that depends on IP spoofing is monitoring the network traffic manually and analyze the suspicious packets depending on several criteria. I will illustrate some factors that indicates the IP spoofing and how to trace them by using the Wireshark. In my proposal

solution, I use Wireshark as a monitoring tool to track the network packets, analyze the suspicious packets and then block the IP address that has been approved to be spoofed by firewall filtering or router. Wireshark is a network application that is used to capture traffic and analyze the packets to resolve the problems. By default, Wireshark will capture all traffic for a selected interface; this can result in hundreds of thousands of packets in a single capture. Wireshark makes this easy by implementing some filters that assist in breaking up the packets to analyze them. One of the mechanisms to identify whether the malicious packet is spoofed or not is by keeping track of the packet flow information embedded in the IP header. The first thing to investigate when the packet appears suspicious is the MAC address that is related with the packet. If the same IP address sends packets with different MAC addresses, then the packets are spoofed (Febrero, 2011).

The second way to indicate the spoofing attack is tracking the three-way handshake of TCP packets. For each TCP connection, SYN, SYN/ACK and ACK are required to start communication. SYN (Synchronize) is sent from the host to the server in order to initiate a connection, then the server responses to the client by sending SYN and ACK(Acknowledge) which represents an acknowledgment of accepting the connection. After that, the client responses to the server with the acknowledgment number to complete the connection process. In some situation of spoofing attack, the attacker initiates the connection by sending SYN and the server responses with SYN/ACK, but the client does not send the ACK number to the server in order to complete the connection which leads to the DDoS attack. For each connection, the TCP/IP stack of the server must wait for a set time, and when the server receives many packets, the resources of the device stop responding to the new requests (Strech, 2010). This situation can be noticed in Wireshark in illustrated in figure1 where we can see the same source address that sends many requests to overwhelm the server. In the below image you can notice endless SYN packet has sent on target's network on port 80 (Febrero, 2011).

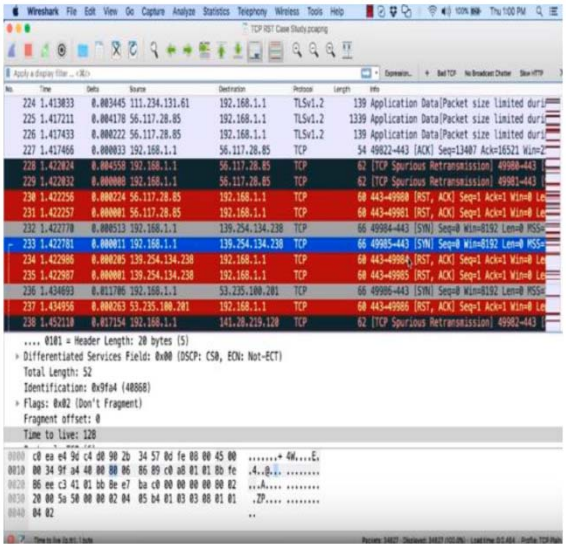


By selecting a certain packet that indicates to be malicious and clicking on the Transmission control protocol, we can follow the three-way handshake clearly to determine whether the packet is spoofed or not.



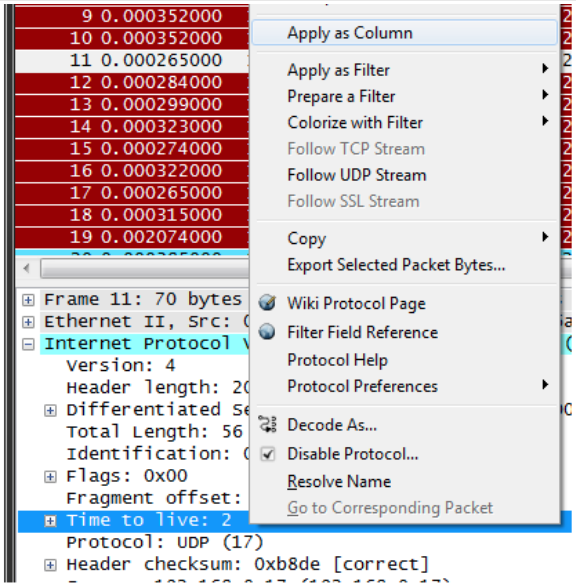
(Febrero, 2011)

The second mechanism to detect the spoofed packet is tracing the lifespan of the IP packet which is known as TTL (Time to Live). The Figure 3 illustrates some SYN and RST packets which means that some new connections to the server are being reset. The reset packet sometimes occurs because a malicious attacker interrupts the connection in the middle and send the rest packet. By examining the TTL in the IP header, we can determine if the packet came from the actual address or not. The TTL refers to the route of the packet which decrements by one number every time the packet moves (Sneha Rana , T. Bansod, 2012). The common TTL start numbers are 255,128 and 64, and for this packet the TTL is 64 which indicates that the packet has not been routed. It means the packet did not come from the actual IP address because each time the packet is routed, the TTL number will decrease by 1 (Gupta, 2012).

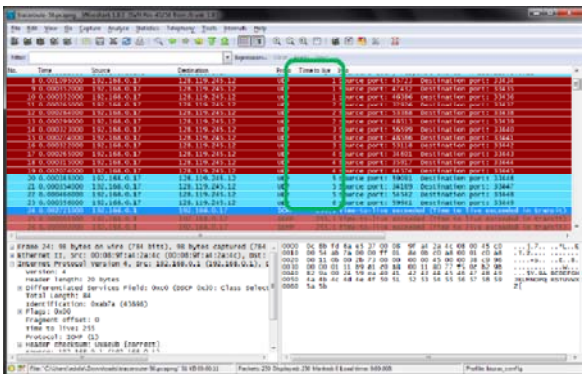


(Gupta, 2012).

By right click on the time to live, we can apply it as a column to check on the time to live and notice which packet is routed and which one is not.



One of the useful services in Wireshark is supporting the geolocalisation which obtains the city and countries of the IP address. This feature is helpful because it gives a visual picture of the origin of the packet. To apply this feature, you need to go to preferences and then name resolution and GeoIP database in the Wireshark to download and add this feature. When you add this feature, the geographical location of the packet will appear when the user right-clicks and selects Enable GeoIP lookups on the suspicious packet. The figure 6 shows the window that illustrates the source location of the packets (Febrero, 2011).





CONCLUSION

This paper illustrates detection and prevention methods of internet protocol (IP) spoofing which is trying to gain unauthorized access. Among the contemporary implementations of spoofing, the network security area must be aware of the potential cost of these sorts of crimes. Users can definitely be monitoring and maintain patching and logs to reduce the possible damage. We believe that my proposed solution which is monitoring the network traffic will be quite effective methods to detect and prevent the internet protocol spoofing and give a safe and secure dealing with the networks and computers.

REFERENCES

[1] Febrero, B. M. (2011, February). Traffic Analysis with Wireshark . Retrieved from https://www.csirtcv.gva.es/sites/all/files/downloads/cert_trafficwireshark.pdf

[2] Gupta, N. (2012, December). Wireshark Packet Capture on Internet Control Message Protocol. Retrieved from https://www.youtube.com/watch?v=7paKmiDQx-4

[3] Sneha Rana , T. Bansod. (2012, June). IP Spoofing Attack Detection using Route Based. Retrieved from http://ijarcet.org/wp-content/uploads/IJARCET-VOL-1-ISSUE-4-285-288.pdf

[4] Strech. (2010, June). Understanding TCP Sequence and Acknowledgment Numbers. Retrieved from http://packetlife.net/blog/2010/jun/7/understanding-tcp-sequence-acknowledgment-numbers/

[5] Rouse, M. (2017). Ingress Filtering, Retrieved from https://searchnetworking.techtarget.com/definition/ingress-filtering

[6] Barak, D., Greene, B, & Prior, M. (2015). Prefix Filtering, Black Holes, and Protecting

[7] Your Business. Slide 36. Retrieved from https://slideplayer.com/slide/4802802/

[8] O'Donnell, A. (2018, April 12). How to Encrypt Your Wireless Network. Retrieved from https://www.lifewire.com/how-to-encrypt-your-wireless-network-2487653

[9] Ladia, A. (2017, November 10). How Does SSH Work. Retrieved from https://www.hostinger.com/tutorials/ssh-tutorial-how-does-ssh-work#gref

[10] Andrew, J. (2017, November 21). How Does SSL Protect Against IP Spoofing? Retrieved from https://itstillworks.com/ssl-protect-against-ip-spoofing-20448.html

★★★