International Journal of Scientific Engineering and Applied Science (IJSEAS) – Volume-2, Issue-1, January 2016
ISSN: 2395-3470
www.ijseas.com

LOAD BALANCING ALGORITHM (LBA) AS A LOCAL SPOOFING THREATS & PREVENTION SOLUTION FOR DoS AND DDoS PAQUETS

Mourad Henchiri[a]
Abdallah Al Amri[b]
[a,b]Universty of Nizwa, Nizwa, Sultanate of Oman

Abstract-- Hijack the property on a network is a crucial and a vital technical behavior, that starts with the first necessity to scan the network for all available security risks, any logical ports availability check... it is considered to be a strong tool for rising up the on-question network security. We present here, in our research, the strength of a such technical tool in infiltrating into; a PC, a network, an intranet, an extranet, a distant host,... At this level, we define the tool in a world of activity and necessity, the facts and reasons for which is founded and implemented, and on the other side, we present this same tool when applied in spoofing and hijacking the hosts authentication and data packets. Preventing the negative apply of a such tool is a crucial and vital consideration that should be kept in mind all the way while implementing a security for a computer network. By checking the modifications on a given group of packets while transactions in a transmission process is the key not to our given solution for detecting the spoofed packets. [1, 3, 11]

KEYWORDS-- Spoof, Hijack, intranet, extranet, threat, packet.

Introduction-- the spoofed security reside on facing a data packet coming from a destination that you trust, while you cannot prove this destination authenticity, nor can you affirm its falseness. Spoofed security is the usage and the referral to this weak logical access point to the targeted host (victim).

The technical tools for spoofing authenticity over networks are an effective solution for passing fire walls, solving restrictions, scanning networks, and so many technical cases. This is an effective way to test weaknesses and failing policies at a designated network.

Applying this technology needs a proficiency level and a well understanding in networks topology and network protocols. So here, and in the network context, the spoofing is the unauthenticated access. Yet, in network security context, spoofing is an unauthenticated attack.[3]

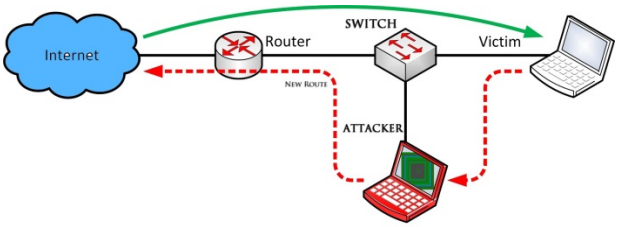

Figure I:-spoofed attack through internet

To accomplish the spoofed access, an attacker has to have an infiltration point to the communication medium which would give the starting key for retrieving the sender's email and replacing it within the

current communication; and here the all the potential has moved to the hacker to present as the real node within the same network.

LAN Protocols

The IP Spoofing technique is recognized as a network hacking (security check up) tool. Thus, the miss functioning of such tool could cause disastrous consequences; for this, the protocols implemented in ensuring the usage of the spoofing technique are selected carefully, while working on a LAN, the NTLM (NT LAN Manager) could be a high level secure authentication process adopted along with your scan and checkup techniques.

IP Spoofing threats [1]

Extracting the real and non-fake authenticity of each interfering member in the communicated packets in a designated network is a major issue. Techniques available are satisfying certain level and sector of such domain. Each attack needs resources to rich destination and achieve goals; from that the TTL(Time To Live), which we are taking consideration in our algorithm to detect the spoofed packets.

TTL Attacks [1]

The variety of techniques ameliorated to make a machine unavailable to its users is pretended by a process based on the usage of the available features. The IP is used to add the Time To Live (TTL) size at the header part for the purpose of terminating and controlling the transmission of packets.

This attack would create an expiry behavior against the network equipment, while flooding targeted victims within a non-wanted communications till it reaches the over potential activity which is known as DoS or the Denial of Service.

The Time To Live is a feature engineered to give a life cycle duration to a specified transmitted packet over a network; which, here, imposes the imposes the integrity of each packet to be under questionnaire. even over an encrypted communication; every and each single communicated packet is seen within all network scan system and techniques, and here the infiltration of a third and unwanted party to the communication could happen and take effect if the security policy is not raised up and well configured. Thus, and for the fundamental settings, if a router gets a packet with a 0 value of the TTL it discards the packet by rejecting it and send an ICMP (v4/v6) message to the initial sender; here, and when attacked by a huge number of packets with TTL less than 1, the devices under attack CPU become busy by processing packets and sending replies. Which would conclude to an affection to all the network activities than to stopped status to all the network activities.[2]

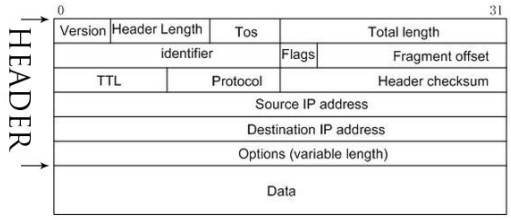

Figure II: Data packet diagram.

Even the checksum header could not guarantee the integrity of each packet; while it protects the data against corruption, yet, it could not be used as a weapon to fight the IP Spoofing technology.

IP Spoofing attacks

Each spoofing project starts at testing the ability of each host in a network of sending fake and spoofed packets, besides the test of ingress and egress filtering of packets from

those hosts; here, usually we would like to keep the mind on that the routes has been deviated and changed.[6, 7]
The wide range of data resources available in the public networks gives the chances to new attack techniques; the IP spoofing is a crucial malicious attack used within all the new technological targets. Raising the status of a targeted machine or an application to a non-responding is the secret behind the DoS or DDoS attack.
Taking the identity of a node in a detected communication on a given network medium is the spoofing act; which is the success of taking the a real node role in a communication over a network, then getting and sending messages with the fake ID.
Here, and in a practical and real plane, every and each web site uploaded and published for a public use and distribution, is highly presented to an unwanted attack like so; the DoS or DDos attack. Thus, the presented attack and malicious infiltration has to be fought took into high consideration at each level and when needed.

REALIZATION

After a deep study on the RBF (Route Based packets Filtering) defense techniques[9], usually we would like to remember that routes has been changed when trying to stop a spoofed communication or even a single spoofed packet.[4] Since and though that the targeted victims in a such technology are software and especially web sites; solutions and remedial also has to be in software wise.
Programming exceptions is a good solution that reaches a high level of trustiness toward the replies to each and every 0 TTL packet. Here, still system failures occurs, which would implies that the programmed exceptions, and after the detected fake packets, are not enough for prohibiting such system failure. The load balancing technique is an amazing technology that we have to adopt in front of each gateway that leads to the system in question.
To achieve the load balancing technique we adopted in our research the scheduling algorithms and data structure methodologies that would subdivide the available load into the available back-end servers to do the necessary assigned tasks.
The realization stands out with an algorithm that presents the consideration of the triggers and exceptions along with the load balancing technology, working together to provide the best high responsive system activity at any situation.[5, 8]

Triggers and Exceptions

Exceptions and triggers programmed as a solution for error handling are too many, yet here are categorized, and the one taken into consideration is a user defined exception to take in value the packets set to 0 TTL value. [1, 12]
The technical reason for a such scenario; is that the triggers and exceptions has to act in first order and first call; and this would be the key of the spoofed IPs detector. [13]

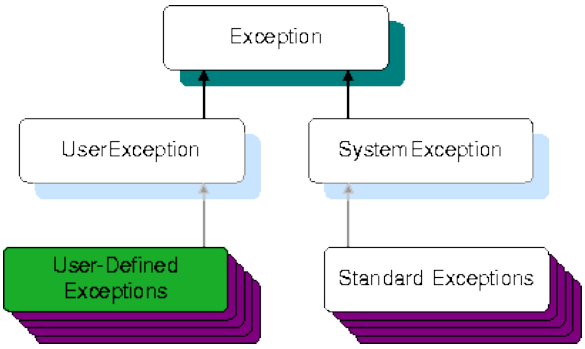

Figure III: Exceptions categories.

Load Balancing Algorithms

The data structure gives the key for ameliorating each system security solution

against the failures in replies or in actions. Here we implement the FIFO prototype in our algorithm and it gives considerable results in time measuring. [10, 12]

Figure IV: FIFO diagram for data processing.
Each process gets the appropriate order that would organize the activity of each processor within time slots and periods.

Round-robin scheduling

The algorithm assigns a periodic time sets per process and cycles through those sets;

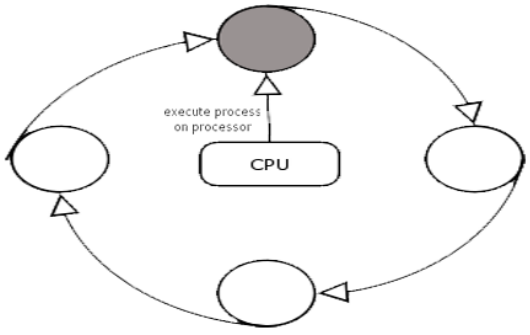

Figure V: Round Robin scheduler diagram.

Adopted Working Solution Architecture

#Libraries
#Global declarations
Triggers
Packet Reception Check Up Function
Main Calls
Exceptions
#Rewind

Conclusion

The available resources on every public network do have the risk of being faced to the risk of an excessive attack that leads to a system failure in case of non-reply and non-reaction. Spoofing identity is a technology used for a variety of purposes all along for negative usage; here, we presented the malicious attacks that has been treated and taken in consideration within a sophisticated solution that has an intelligent integration methodology in a software wise environment. Even for encrypted communications, all passing packets are viewed by all network scanning tools, and then are managed within the desired behavior; when used to spoof the IPs identity is exposed and when used to manage the packet features data integrity is exposed and especially the receiving targets are exposed and their replies are strongly affected.

References

[1] niversity of Oregon Route Views Project, http://www.RouteViews.org

[2] B. White, J. Lepreau, L. Stoller, R. Ricci, S. Guruprasad,M. Newbold, M. Hibler, C. Barb, and A. Joglekar, “An integrated experimental environment for distributed systems and networks,” in the proceedings of the OSDI02, Dec. 2002, USENIX Association, pp. 255—270.

[3] S. Shakkottai and R. Srikant and N. Brownlee and A. Broido and kc claffy, “The RTT Distribution of TCP Flows in the

Internet and its Impact on TCP based Flow Control," CAIDA Technical Report, TR-2004-02.

[4] ARIN WHOIS Database, http://www.arin.net/whois/

[5] NLANR – National Laboratory for Applied Network Research, http://www.nlanr.net

[6] P. Ferguson, and D. Senie. "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing," RFC 2267

[7] J. Li and J. Mirkovic and M. Wang and P. Reiher and L. Zhang, "SAVE: Source Address Validity Enforcement Protocol," Proceedings of INFOCOM, June 2002.

[8] A. Perrig and D. Song and A. Yaar. "StackPi: A New Defense Mechanism against IP Spoofing and DDoS Attacks," Carnegie Mellon University Technical Report, CMU-CS-02-208, February 2003.

[9] K. Park and H.Lee, "On the effectiveness of route-based packet filtering for distributed DoS attack prevention in power-law internets," In Proceedings of SIGCOMM 2001.

[10] C. Jin and H. Wang and K.G. Shin, "Hop-count filtering: an effective defense against spoofed DDoS traffic," Proceedings of the 10th ACM conference on Computer and communications security, 2003.

[11] A. Bremler-Barr and H. Levy, "Spoofing Prevention Method," In Proceedings of INFOCOM'05, March 2005.

[12] Z. Duan and X. Yuan and J. Chandrashekar, "Constructing InterDomain Packet Filters to Control IP Spoofing Based on BGP Updates," Proceedings of INFOCOM'06, April 2006.

[13] W. Feller, "An Introduction to Probability Theory," Wiley 1968