EFFICIENT DEFENSE SYSTEM FOR IP SPOOFING IN NETWORKS

Emil Kuriakose John [1] and Sumaiya Thaseen [2]

[1]School of Information Technology and Engineering,
VIT University, Vellore, Tamil Nadu, India
ekj171@gmail.com
[2] School of Computing Science and Engineering,
VIT University, Chennai, Tamil Nadu, India
sumaiyathaseen@gmail.com

ABSTRACT

In this age of gigabit Ethernet and broadband internet, network security has been the top priority for most of the researchers. Technology advancements have advantages as well as disadvantages. Most of the communication of present world, the e-world, takes place online, through the internet. Thus the context of network intrusions and attacks to hack into servers also came into existence. A technique to perform this activity is made possible by preventing the discovery of the sender's identity through IP Spoofing [7]. Many popular internet sites have been hacked and attackers try to forge or spoof the source addresses in IP packets. Using spoofing detection technique, the user can retrieve the list of IP addresses and able to identify the malicious IP addresses.Hence mechanisms must be designed to prevent hacking. This paper proposes a novel technique to detect IP spoofing based on traffic verification and filtering.

KEYWORDS

Distributed Denial of service attack (DDoS), Replay attack, Blind Spoofing. IP Spoofing, Time to Live (TTL), Hop Count Filtering (HCF).

1. INTRODUCTION

Internet is most widely used in every aspect of life. Over one-third of the world population utilize Internet for daily activities [8]. It is used in services like banking, shopping, transport, health, communications etc. Shifting to the internet era has increased the context of network intrusions and attacks to hack into servers [3]. But in the current scenario, there is no integrated application that provides a network administrator to manage the network from the server or host machine. Unauthorized access made by malicious user to a particular system is IP Spoofing. IP address spoofing or IP Spoofing refers to "the creation of Internet protocol (IP) packets with forged source IP address with the intention of concealing the identity of the sender and impersonate other computing system" [7]. Security for IP Spoofing is essential and demanding.

This paper proposes a promising solution for the detection of malicious IP packets under real time environment. IP Spoofing happens in various ways through Distributed Denial of Service (DDoS) attack, Replay attack and Blind Spoofing [9]. These are the main techniques by which spoofing attempts occurs in the Internet. We provide some efficient and reliable techniques by which these issues are dealt. The aim of the work is to develop an application with a clean GUI that aids the administrator to monitor network traffic and attempts of intrusion, from any system in the network. The developed system will integrate all the necessary tools required by a network

Sundarapandian et al. (Eds): CoNeCo,WiMo, NLP, CRYPSIS, ICAIT, ICDIP, ITCSE, CS & IT 07,
pp. 185–193, 2012. © CS & IT-CSCP 2012 DOI : 10.5121/csit.2012.2416

administrator to know the details of each and every system connected to the network, the traffic from each system, source and destination of packets, source and destination of intrusions and even lets him record the details of traffic and attacks. The administrator can carry out analysis based on the entries in this application and thus provide an efficient defense system against IP Spoofing.

The paper is organized as follows. Section 2 summarizes the comparative study of IP Spoofing. Section 3 discusses about implementation of proposed defense system. Section 4.Results are discussed in section 4.Section 5 concludes the paper.

2. COMPARATIVE STUDY OF IP SPOOFING

IP Spoofing can be handled in many different ways ranging from greater complexity algorithms to simple techniques based on the level of service it has to provide. Here we develop a mechanism for detection of IP Spoofing in real time environment, considering the performance and the resource management constraints [6]. Over the years, network security has been a prime concern and there are four major aspects. They are:-

1. Distributed denial of service(DDoS attack)

   This is a serious attack in IP Spoofing [5]. Our study is limited to the host based approach. In host based approach, it decreases the resource consumption and provides greater resource management by avoiding the malicious traffic [4]. The present host based approach identifies spoofing in the transport layer and layers above and cannot stop the victim server from consuming CPU resource in handling the malicious IP packets. This can very much slow down the victim server [11]. Hence, we detect the spoofed packet at the IP layer itself. This technique lays emphasis on effective usage of resources thus providing greater resource management. One of the host based approach is hop count filtering (HCF). The hop count field is indirectly related to the Time to Live (TTL) field of the IP Header. We design a tool at the receiver end where the Time to Live (TTL) value can be inferred and can check for consistency. If the TTL field gives different values for different packet in a single session then inconsistency prevails and one can suspect of an intruder attempting to make connection with the receiver.

   Hop Count Filter (HCF) runs in two states. In the learning state, HCF watches for the abnormal TTL behavior without discarding any packets. On detection of an attack, HCF switches to the filtering state, where it discards those IP packets with mismatching hop-counts. Over 90% of the spoofed IP packets can be identified. False positive is a term which refers to the legitimate packets that are incorrectly identified as spoofed. Our HCF technique reduces the number of false positives [1]. Thus, HCF can effectively counter the DDoS attack.

2. Replay attack

   A replay attack is defined as “a type of network attack in which data transmission is maliciously repeated” [10]. Theoretically, this issue can be handled using session id. A packet with a session id is valid only for a particular period of time after which the packet is considered invalid and is not fit for transmission. An intruder or malicious user copies a steam of messages between the sender and receiver (two parties) and replay the stream to one or more of the parties.

3. Blind Spoofing

   Blind Spoofing Attack is another type of spoofing attack. This attack may occur by external means where sequence and acknowledgement numbers are unreachable. Attackers send random packets to the end system to identify the sequence numbers. Random sequence number is specified by the operating System and is difficult to predict. If the sequence number is compromised, data could be sent to the target machine.

IP spoofing is incomplete without considering the issues of all the hosts connected in the network as a whole. This is because network intrusion can happen within a particular network as well. So here we provide a scenario to validate the availability of the hosts in that particular network starting from the network address and performing ping operation on every successive IP addresses till the end of the hosts. The next stage follows implementation where we discuss on how these concepts can be implemented for real time systems on resource management.

3. IMPLEMENTATION OF PROPOSED DEFENSE SYSTEM

The design and development of defense system for IP Spoofing is discussed in this section. The proposed system works on real time environment. It works on the platform C#.net (Microsoft Visual Studio 2005). Application is capable of performing the detection of malicious packets arriving at the destination node. The proposed system is capable of monitoring the network traffic and detects any attempts to intrude into the network almost instantaneously. The system combines together all the tools into a single, user-friendly application that can be handled by the administrator. The operation performed is classified into three categories. In the first step, packet analyzer module will filter all the incoming IP packets to the destination. It monitors the network traffic and detects any attempts to intrusion into the network, almost instantaneously. IP Spoofing is incomplete without port scanning of the servers. With port scanning it identifies which all ports are active at a particular time and can validate the existence of an attack (if any) with the packet tracing feature. Apart from these activities, another module is machines on local area network (LAN) which identifies all the machines in the network to which the host is presently connected. This also plays a major role in IP Spoofing as spoofing can happen within the host network as well. These are the proposed issues we wish to handle in the application to be developed.

Generally the phases of fake IP detection can be classified as shown in Figure 1.

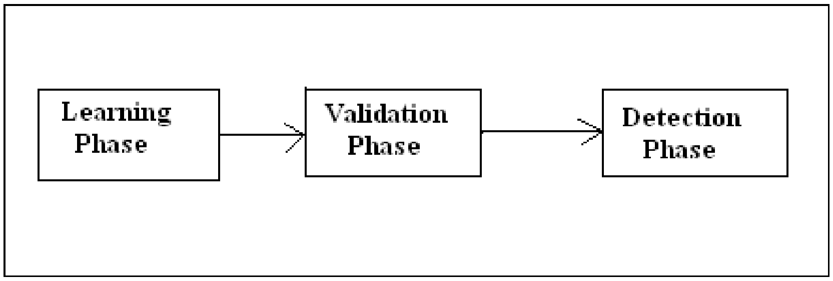


Figure 1. Fake IP Detection process

The general working phases can be categorized into three categories [2].

1. Learning Phase

   During this phase, the information containing the packets in the real time is listed. It is assumed that during normal connection, no attacks occur.

2. Validation Phase

   After performing the listening phase, the packets traced are checked with various detection handling methods. If any detection method gets invoked, it moves to the Detection phase or else it continues to learn the packets.

3. Detection Phase

   The packets obtained from the validation phase and sent to detection phase are considered malicious and are potentially dangerous packets which are highlighted for user's immediate attention.

The proposed system consists of the following modules as shown in the figure 2.This system performs the task of detecting IP Spoofing in a fair and less resource consumed manner.

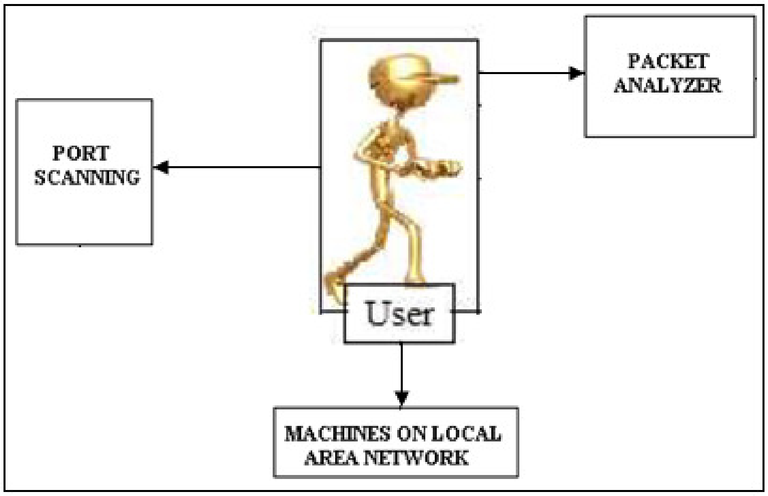


Figure 2. Architecture of Proposed System

Packet Analyzer is the major module of the system performing the following action as shown in the Figure 3.

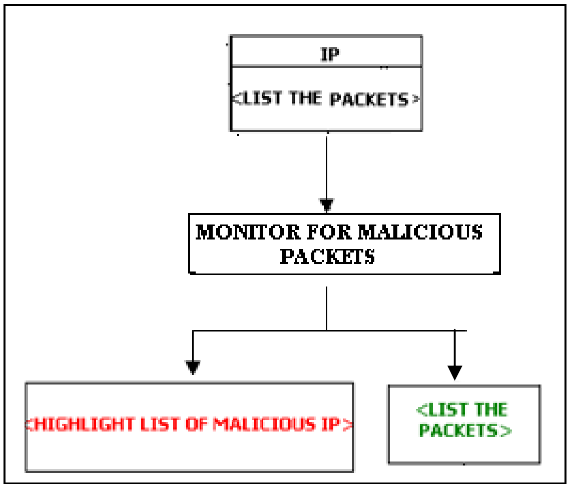

IP
<LIST THE PACKETS>
MONITOR FOR MALICIOUS PACKETS
<HIGHLIGHT LIST OF MALICIOUS IP>
<LIST THE PACKETS>

Figure 3. IP Packet Analyzer

Various guidelines are taken into account for detecting the malicious packet which can result in IP Spoofing. Distributed Denial of service (DDoS) attack can be avoided by using the Hop-count filtering (HCF) technique where the destination system can infer the Time to Live (TTL) information and check for consistency [1] [2]. If it leads to inconsistent values, then it is considered as spoofed IP packet and is highlighted.

Replay attack is also potential attack in network security which needs greater importance. Since the application being developed is worked at the destination level, the technique adopted here is based on the Identification field and the Time to Live (TTL) field of the IP header. A packet arriving at a particular instant has identification field as well as TTL field. A packet arriving next will definitely have different identification value than the previous one. If the detection phase detects any IP Packets with identification field different than the identification field previously coming from the same IP address, then it is considered malicious as there is a possibility of replay attack.

Some other criteria are also taken into consideration. If many packets arrive from a particular source to the destination, then it can be a threat on flooding the network leading to Denial of service (DoS). Although it is not necessary that Denial of Service (DoS) should occur at that point in time rather a large file being downloaded can also be the case. Hence as a precautionary step a message box is displayed to alert the user about the packet transfer from a particular source during a short span of time.

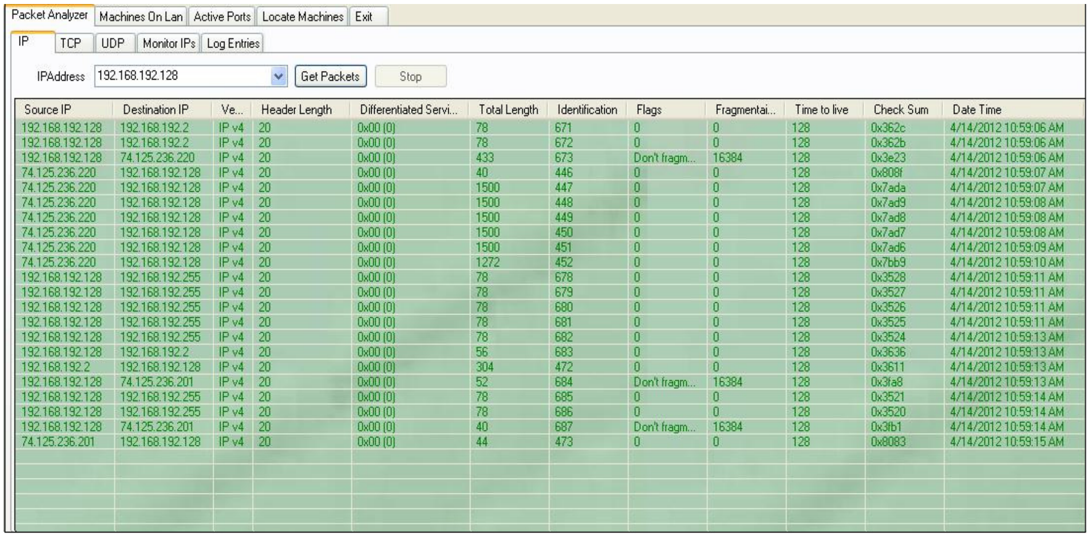
If a user considers that packets arriving from a particular source IP is malicious or wishes to trace, one can manually filter the results by providing the source IP under the monitor IP sub module of the proposed application. This will benefit users for a comparative analysis of the packets leading to greater result accuracy.

It is well known that UDP is connectionless service and communication of services is carried out between ports. Naturally, the server port and the client ports are different. If same port number for both the server and client is used in transfer of packet from source IP address to destination IP address, then such packets may not be secure and are therefore detected.

Apart from the IP packet filtering techniques, a user can also perform scanning of the active machines available. This segment is used to validate the user whether spoofing happens within the network or from outside. The proposed system considers the machines that are scanned from the IP address "192.0.0.0" onwards. This will also facilitate in providing the MAC address of that particular host in the network.

4. RESULTS AND DISCUSSION

An integrated application is developed which collectively handles most of the issues related to spoofing with less resource requirements. User will trace the packets coming to the destination node. Based on the criteria mentioned above detection of spoofing is performed. Results and discussion of the proposed system is discussed below. The main GUI of the implemented system is as shown in Figure 4.



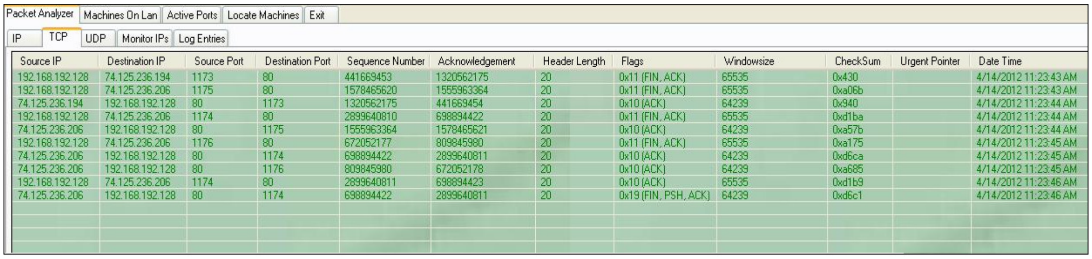
IPAddress 192.168.192.128

Source IP	Destination IP	Ve...	Header Length	Differentiated Servi...	Total Length	Identification	Flags	Fragmentai...	Time to live	Check Sum	Date Time
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	78	671	0	0	128	0x362c	4/14/2012 10:59:06 AM
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	78	672	0	0	128	0x362b	4/14/2012 10:59:06 AM
192.168.192.128	74.125.236.220	IP v4	20	0x00 (0)	433	673	Don't fragm...	16384	128	0x3e23	4/14/2012 10:59:06 AM
74.125.236.220	192.168.192.128	IP v4	20	0x00 (0)	40	446	0	0	128	0x808f	4/14/2012 10:59:07 AM
74.125.236.220	192.168.192.128	IP v4	20	0x00 (0)	1500	447	0	0	128	0x7ada	4/14/2012 10:59:07 AM
74.125.236.220	192.168.192.128	IP v4	20	0x00 (0)	1500	448	0	0	128	0x7ad9	4/14/2012 10:59:08 AM
74.125.236.220	192.168.192.128	IP v4	20	0x00 (0)	1500	449	0	0	128	0x7ad8	4/14/2012 10:59:08 AM
74.125.236.220	192.168.192.128	IP v4	20	0x00 (0)	1500	450	0	0	128	0x7ad7	4/14/2012 10:59:08 AM
74.125.236.220	192.168.192.128	IP v4	20	0x00 (0)	1500	451	0	0	128	0x7ad6	4/14/2012 10:59:09 AM
74.125.236.220	192.168.192.128	IP v4	20	0x00 (0)	1272	452	0	0	128	0x7bb9	4/14/2012 10:59:10 AM
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	678	0	0	128	0x3528	4/14/2012 10:59:11 AM
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	679	0	0	128	0x3527	4/14/2012 10:59:11 AM
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	680	0	0	128	0x3526	4/14/2012 10:59:11 AM
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	681	0	0	128	0x3525	4/14/2012 10:59:11 AM
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	682	0	0	128	0x3524	4/14/2012 10:59:13 AM
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	56	683	0	0	128	0x3636	4/14/2012 10:59:13 AM
192.168.192.2	192.168.192.128	IP v4	20	0x00 (0)	304	472	0	0	128	0x3611	4/14/2012 10:59:13 AM
192.168.192.128	74.125.236.201	IP v4	20	0x00 (0)	52	684	Don't fragm...	16384	128	0x3fa8	4/14/2012 10:59:13 AM
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	685	0	0	128	0x3521	4/14/2012 10:59:14 AM
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	686	0	0	128	0x3520	4/14/2012 10:59:14 AM
192.168.192.128	74.125.236.201	IP v4	20	0x00 (0)	40	687	Don't fragm...	16384	128	0x3fb1	4/14/2012 10:59:14 AM
74.125.236.201	192.168.192.128	IP v4	20	0x00 (0)	44	473	0	0	128	0x8083	4/14/2012 10:59:15 AM

Figure 4. IP Packet Analyzer getting real time packets

Analyzing the above packets, it can be inferred that no Denial of Service takes place because the identification field gives different values in each time. The Differentiated Services field also plays an important role in determining the type of service carried out by every packet. Here, it is 0x00 which represents packets are sent at minimum delay. This is the learning phase.

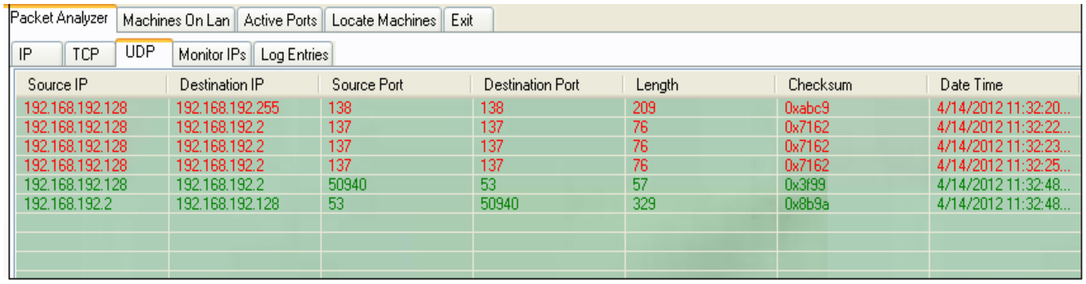
Similarly the TCP and UDP packets can also be listed as shown in Figure 5 and Figure 6 below.



Source IP	Destination IP	Source Port	Destination Port	Sequence Number	Acknowledgement	Header Length	Flags	Windowsize	CheckSum	Urgent Pointer	Date Time
192.168.192.128	74.125.236.194	1173	80	441669453	1320562175	20	0x11 (FIN, ACK)	65535	0x430		4/14/2012 11:23:43 AM
192.168.192.128	74.125.236.206	1175	80	1578465620	1555963364	20	0x11 (FIN, ACK)	65535	0xa06b		4/14/2012 11:23:43 AM
74.125.236.194	192.168.192.128	80	1173	1320562175	441669454	20	0x10 (ACK)	64239	0x940		4/14/2012 11:23:44 AM
192.168.192.128	74.125.236.206	1174	80	2899640810	698894422	20	0x11 (FIN, ACK)	65535	0xd1ba		4/14/2012 11:23:44 AM
74.125.236.206	192.168.192.128	80	1175	1555963364	1578465621	20	0x10 (ACK)	64239	0xa57b		4/14/2012 11:23:44 AM
192.168.192.128	74.125.236.206	1176	80	672052177	809845980	20	0x11 (FIN, ACK)	65535	0xa175		4/14/2012 11:23:45 AM
74.125.236.206	192.168.192.128	80	1174	698894422	2899640811	20	0x10 (ACK)	64239	0xd6ca		4/14/2012 11:23:45 AM
74.125.236.206	192.168.192.128	80	1176	809845980	672052178	20	0x10 (ACK)	64239	0xa685		4/14/2012 11:23:45 AM
192.168.192.128	74.125.236.206	1174	80	2899640811	698894423	20	0x10 (ACK)	65535	0xd1b9		4/14/2012 11:23:46 AM
74.125.236.206	192.168.192.128	80	1174	698894422	2899640811	20	0x19 (FIN, PSH, ACK)	64239	0xd6c1		4/14/2012 11:23:46 AM

Figure 5. Analyzing TCP real time packets

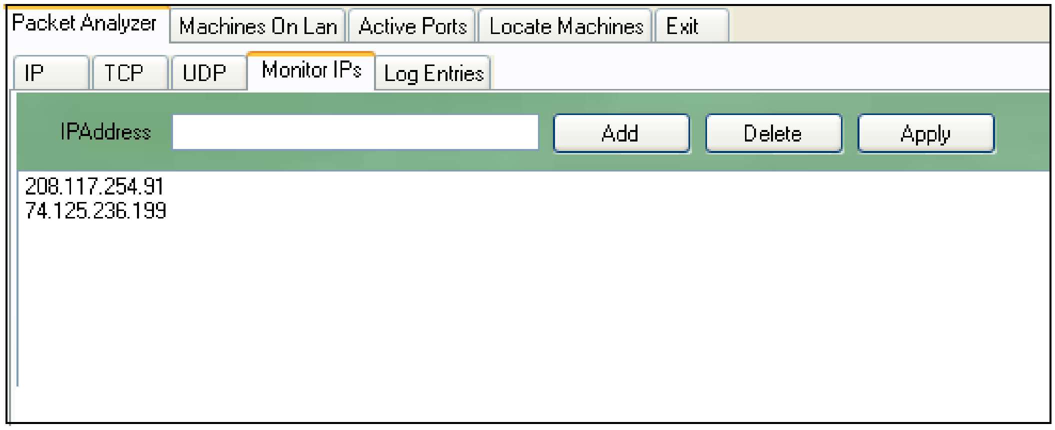
The sequence number field is of great importance as it identifies each packet uniquely.



Source IP	Destination IP	Source Port	Destination Port	Length	Checksum	Date Time
192.168.192.128	192.168.192.255	138	138	209	0xabc9	4/14/2012 11:32:20...
192.168.192.128	192.168.192.2	137	137	76	0x7162	4/14/2012 11:32:22...
192.168.192.128	192.168.192.2	137	137	76	0x7162	4/14/2012 11:32:23...
192.168.192.128	192.168.192.2	137	137	76	0x7162	4/14/2012 11:32:25...
192.168.192.128	192.168.192.2	50940	53	57	0x3f99	4/14/2012 11:32:48...
192.168.192.2	192.168.192.128	53	50940	329	0x8b9a	4/14/2012 11:32:48...

Figure 6. Analyzing UDP real time packets

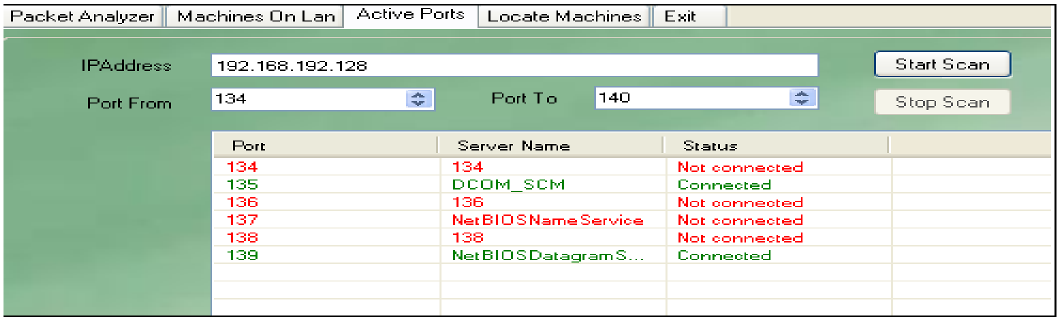
Since the server port and client port cannot be the same, it highlights the packet details. As discussed earlier, once the learning phase is done, validation phase is carried out where the system checks the possibility of the packet to be malicious or not. Detection mechanisms as discussed above have been incorporated in the tool. Apart from this a user interface is developed for users to particularly monitor specific source IP addresses. This is illustrated as shown in Figure 7.



208.117.254.91
74.125.236.199

Figure 7. Monitor IP Address in packet analyzer

Port Scanning is another module that is implemented. Active ports describe the ports which are being connected at that particular point of time. It is illustrated as shown in the Fig.8.



IPAddress 192.168.192.128

Port From 134 Port To 140

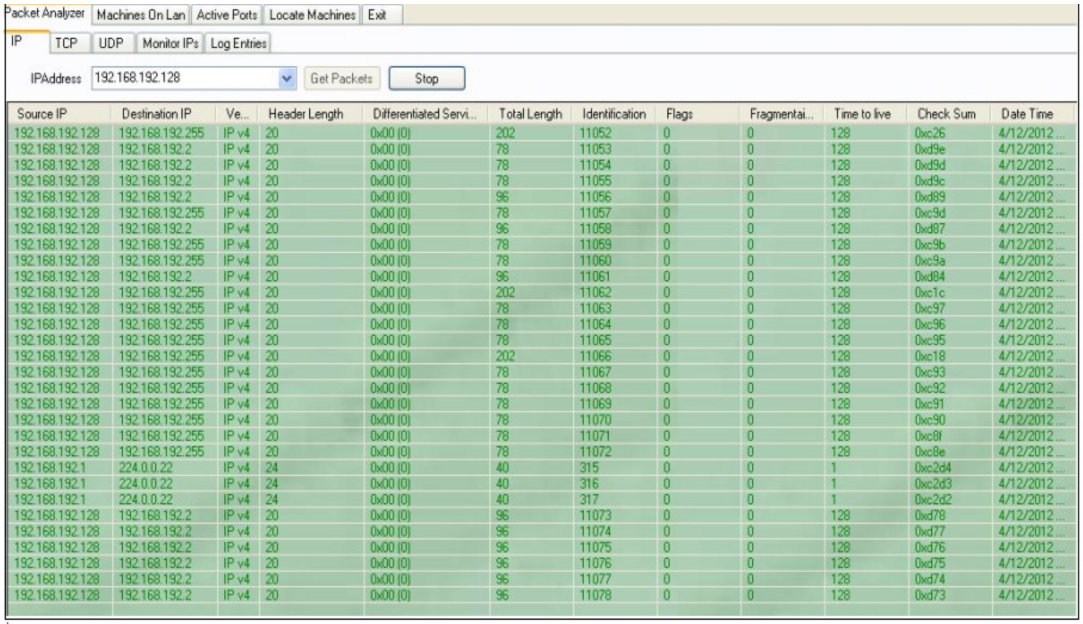
Port	Server Name	Status
134	134	Not connected
135	DCOM_SCM	Connected
136	136	Not connected
137	NetBIOSNameService	Not connected
138	138	Not connected
139	NetBIOSDatagramS...	Connected

Figure 8. Port Scanning

Machines on Local Area Network (LAN) is another module used to validate whether an attack occurs within the system or from externally.

The defects detected during test execution of the proposed application system are described below.

1. Change in hop value- potential chances for Denial of Service (DoS) attack [1]. This is illustrated in Figure 9.

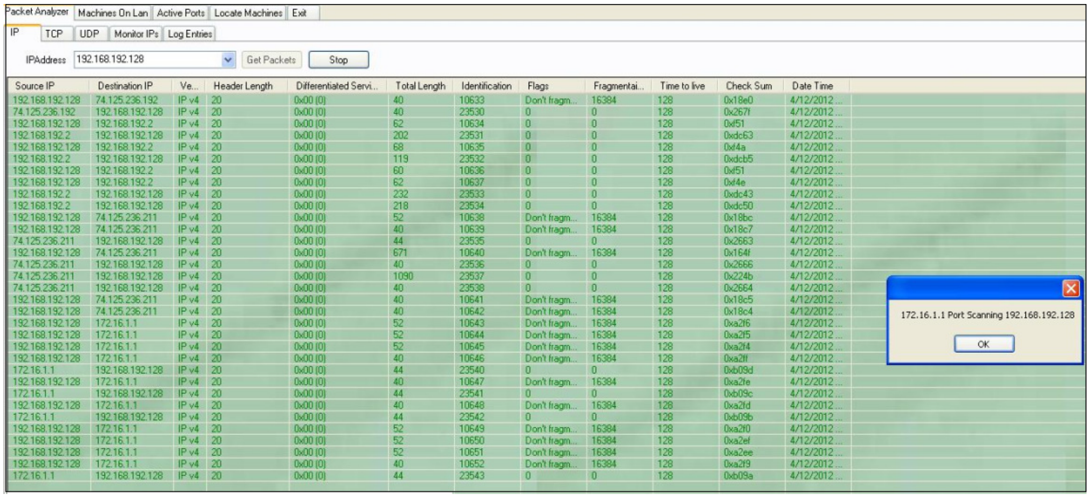


IPAddress 192.168.192.128

Source IP	Destination IP	Ve...	Header Length	Differentiated Servi...	Total Length	Identification	Flags	Fragmentai...	Time to live	Check Sum	Date Time
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	202	11052	0	0	128	0xc26	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	78	11053	0	0	128	0xd9e	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	78	11054	0	0	128	0xd9d	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	78	11055	0	0	128	0xd9c	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11056	0	0	128	0xd89	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11057	0	0	128	0xc9d	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11058	0	0	128	0xd87	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11059	0	0	128	0xc9b	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11060	0	0	128	0xc9a	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11061	0	0	128	0xd84	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	202	11062	0	0	128	0xc1c	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11063	0	0	128	0xc97	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11064	0	0	128	0xc96	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11065	0	0	128	0xc95	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	202	11066	0	0	128	0xc18	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11067	0	0	128	0xc93	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11068	0	0	128	0xc92	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11069	0	0	128	0xc91	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11070	0	0	128	0xc90	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11071	0	0	128	0xc8f	4/12/2012 ...
192.168.192.128	192.168.192.255	IP v4	20	0x00 (0)	78	11072	0	0	128	0xc8e	4/12/2012 ...
192.168.192.1	224.0.0.22	IP v4	24	0x00 (0)	40	315	0	0	1	0xc2d4	4/12/2012 ...
192.168.192.1	224.0.0.22	IP v4	24	0x00 (0)	40	316	0	0	1	0xc2d3	4/12/2012 ...
192.168.192.1	224.0.0.22	IP v4	24	0x00 (0)	40	317	0	0	1	0xc2d2	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11073	0	0	128	0xd78	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11074	0	0	128	0xd77	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11075	0	0	128	0xd76	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11076	0	0	128	0xd75	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11077	0	0	128	0xd74	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	96	11078	0	0	128	0xd73	4/12/2012 ...

Figure 9. Variation in Time to Live (TTL) field for DoS detection

2. Source IP transmitting more packets in a particular time to the destination. This is illustrated in Figure 10.



IPAddress 192.168.192.128

Source IP	Destination IP	Ve...	Header Length	Differentiated Servi...	Total Length	Identification	Flags	Fragmentai...	Time to live	Check Sum	Date Time
192.168.192.128	74.125.236.192	IP v4	20	0x00 (0)	40	10633	Don't fragm...	16384	128	0x18e0	4/12/2012 ...
74.125.236.192	192.168.192.128	IP v4	20	0x00 (0)	40	23530	0	0	128	0x267f	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	62	10634	0	0	128	0xf51	4/12/2012 ...
192.168.192.2	192.168.192.128	IP v4	20	0x00 (0)	202	23531	0	0	128	0xdc63	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	68	10635	0	0	128	0xf4a	4/12/2012 ...
192.168.192.2	192.168.192.128	IP v4	20	0x00 (0)	119	23532	0	0	128	0xdcb5	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	60	10636	0	0	128	0xf51	4/12/2012 ...
192.168.192.128	192.168.192.2	IP v4	20	0x00 (0)	62	10637	0	0	128	0xf4e	4/12/2012 ...
192.168.192.2	192.168.192.128	IP v4	20	0x00 (0)	232	23533	0	0	128	0xdc43	4/12/2012 ...
192.168.192.2	192.168.192.128	IP v4	20	0x00 (0)	218	23534	0	0	128	0xdc50	4/12/2012 ...
192.168.192.128	74.125.236.211	IP v4	20	0x00 (0)	52	10638	Don't fragm...	16384	128	0x18bc	4/12/2012 ...
192.168.192.128	74.125.236.211	IP v4	20	0x00 (0)	40	10639	Don't fragm...	16384	128	0x18c7	4/12/2012 ...
74.125.236.211	192.168.192.128	IP v4	20	0x00 (0)	44	23535	0	0	128	0x2663	4/12/2012 ...
192.168.192.128	74.125.236.211	IP v4	20	0x00 (0)	671	10640	Don't fragm...	16384	128	0x164f	4/12/2012 ...
74.125.236.211	192.168.192.128	IP v4	20	0x00 (0)	40	23536	0	0	128	0x2666	4/12/2012 ...
74.125.236.211	192.168.192.128	IP v4	20	0x00 (0)	1090	23537	0	0	128	0x224b	4/12/2012 ...
74.125.236.211	192.168.192.128	IP v4	20	0x00 (0)	40	23538	0	0	128	0x2664	4/12/2012 ...
192.168.192.128	74.125.236.211	IP v4	20	0x00 (0)	40	10641	Don't fragm...	16384	128	0x18c5	4/12/2012 ...
192.168.192.128	74.125.236.211	IP v4	20	0x00 (0)	40	10642	Don't fragm...	16384	128	0x18c4	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	52	10643	Don't fragm...	16384	128	0xa2f6	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	52	10644	Don't fragm...	16384	128	0xa2f5	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	52	10645	Don't fragm...	16384	128	0xa2f4	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	40	10646	Don't fragm...	16384	128	0xa2ff	4/12/2012 ...
172.16.1.1	192.168.192.128	IP v4	20	0x00 (0)	44	23540	0	0	128	0xb09d	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	40	10647	Don't fragm...	16384	128	0xa2fe	4/12/2012 ...
172.16.1.1	192.168.192.128	IP v4	20	0x00 (0)	44	23541	0	0	128	0xb09c	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	40	10648	Don't fragm...	16384	128	0xa2fd	4/12/2012 ...
172.16.1.1	192.168.192.128	IP v4	20	0x00 (0)	44	23542	0	0	128	0xb09b	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	52	10649	Don't fragm...	16384	128	0xa2f0	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	52	10650	Don't fragm...	16384	128	0xa2ef	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	52	10651	Don't fragm...	16384	128	0xa2ee	4/12/2012 ...
192.168.192.128	172.16.1.1	IP v4	20	0x00 (0)	40	10652	Don't fragm...	16384	128	0xa2f9	4/12/2012 ...
172.16.1.1	192.168.192.128	IP v4	20	0x00 (0)	44	23543	0	0	128	0xb09a	4/12/2012 ...

172.16.1.1 Port Scanning 192.168.192.128

Figure.10 Multiple placket transmission over a period of time

The proposed system can handle or identify almost all malicious packets and thus add on the feature of robustness.

5. CONCLUSION

The proposed system retrieves IP traffic for verification and filters the packet which is identified as malicious. The application can be used for spoofing any type of malicious packets with the key advantage of consuming fewer resources. It is an integrated tool comprising of packet analyzer, active ports and machines on LAN. The system is resistant to Distributed Denial of service attack (DDoS), Replay attack and blind spoofing. Improving the current system with new set of guidelines or methods for packet tracing is our future work.

REFERENCES

[1] Haining Wang, Member, IEEE, Cheng Jin, and Kang G. Shin, Fellow, IEEE, “Defense Against Spoofed IP Traffic Using Hop-Count Filtering”, IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 15, NO. 1, FEBRUARY 2007.

[2] N. Arumugam, C. Venkatesh ,“A Trivial Scheme for Detecting and Preventing Fake IP Access of Network Server Using IPHP Filter”, European Journal of Scientific Research, ISSN 1450-216X Vol.53 No.2 (2011), pp.258-268.

[3] Yao Chen, Shantanu Das, Pulak Dhar, Abdulmotaleb El Saddik, and Amiya Nayak, “Detecting and Preventing IP-spoofed Distributed DoS Attacks,” International Journal of Network Security, Vol.7, No.1, PP.70–81, July 2008.

[4] T.M. Gil and M Poleto, ”MULTOPS: a data-structure for bandwidth attack detection”, hoc.io* USENIX Security Symposium Washington,DC, pp.23-38,Aug,2001

[5] A. Kuzmanovic and E. W. Knightly, “Low-rate TCP-targeted denial of service attacks (the shrew vs. the mice and elephants,” in Proc. ACM SIGCOMM, 2003, pp. 75–86.

[6] G. Banga, P. Druschel, and J. Mogul, “Resource containers: A new facility for resource management in server systems,” in Proc. USENIX OSDI’99, New Orleans, LA, 1999, pp. 45–58.

[7] IP address spoofing. Accessed 02.32 PM http://en.wikipedia.org/wiki/IP_address_spoofing

[8] World Internet Usage Statistics. Accessed 07.45 AM http://www.internetworldstats.com/

[9] Different types of IP Spoofing Accessed 03.01 PM http://www.computerworld.com/s/article/9001021/The_top_five_ways_to_prevent_IP_spoofing

[10] Replay attack. Accessed 04.40 PM http://en.wikipedia.org/wiki/Replay_attack

[11] S. M. Bellavin, “ICMP traceback messages”, Internet Draft, 2001

Authors

[1] Emil Kuriakose John received his B. Tech. from Kerala University, Trivandrum, Kerala, India, in 2010. He is currently doing M. Tech. from VIT University, Vellore, Tamil Nadu, India. His areas of interest are Wireless Mobile Networking, Cryptography and Network Security, Network Programming and Protocols.

[2] Sumaiya Thaseen received her B.E from Madras University and M.Tech from VIT University in 2004 and 2006 respectively. She is currently an Assistant Professor (Senior) in School of Computing Science and Engineering, VIT University, Chennai with 6 years of experience and also pursuing her PhD degree. A life member of Computer Society of India (CSI). Her areas of interests are ad hoc networks, cryptography and network security. She has published several papers in international peer reviewed journals and conferences.