Application Layer Based Packet Analysis And Intrusion Detection

BONTHAGORLA VENKATA KOTESWARAO[#1], SHAIK SALMA BEGUM[#2]

[1] M.Tech (CSE),Gudlavalleru Engineering College, Gudlavalleru
[2] Assistant professor, Gudlavalleru Engineering College, Gudlavalleru.

ABSTRACT:

Network forensics is basically a new approach when it comes to the network information security, because the IDS and firewall cannot always discover and stop the misuse in the whole network. This proposed work is used to capture and analyze the data exchanged among the many different IP traceback techniques like packet marking that assist a forensic investigator to recognize the promicious ip source packets. The proposed network forensics only focus on the network traffic capture,arp spoofing,mac spoofing,attack alerting and traffic replay, that often results in the performance of forensics analysis difficulties. In this particular paper, the frameworks of distributed real time network intrusion forensics system, that's deployed in local area network environment is analyzed and investigated.

I INTRODUCTION

Network forensics is the "capture, recording, and analysis of network events in an effort to find out the source of security attacks or any other problem incidents" [1]. Wherein the security relevant to an organization is bothered, the role of network forensics is complementary to intrusion detection – where intrusion detection fails, network forensics is advantageous for obtaining tips on the attack, dependent on how the source of the attack can be identified and of course the damage can possibly be contained[7].

The idea of network forensics handles the data found across a network connection mostly ingress and egress traffic from one host to a different one. Network forensics analyzes traffic that data logged through firewalls or intrusion detection systems or at network devices like routers. The aim is to traceback in the way to obtain the attack to ensure that cybercriminals are prosecuted. Network forensics is defined in [14] as "the using scientifically proven techniques to collect, fuse, identify, examine, correlate, analyze, and document digital evidence from multiple, actively processing and transmitting digital sources when considering uncovering facts associated with the planned intent, or measured success of unauthorized activities meant to disrupt, corrupt, and or compromise system components as well as providing information to support for a or recovery from these activities". Ranum [17] is known to cause defining network forensics as "the capture, recording, and analysis of network events so that you can learn the method to obtain security attacks." Network forensics involves monitoring network traffic and determining in case there is an anomaly among the traffic and ascertaining whether or not it indicates an attack. Whether it is in that case the nature of one's attack is likewise determined. Network traffic is captured, preserved, analyzed and an incident response is invoked immediately.

Much progress is being made in reducing network risks with a style of security tools, for example the firewall, intrusion detection system, but these efforts mainly concentrate on the prevention and detection of one's network intrusion. The active response of the network misuse is seldom considered. Current incident response is always later on attacks, which lose some important data of the intrusion. To address the dilemma, we'd like result-oriented approaches to enhance the investigation of all the network attack. Network forensics technology with active and real-time response characteristics is most definately a new approach that can be used for that purpose[8].

Computer forensics will be the application of computer investigation and analysis techniques within the interests of determining potential legal evidence [1]. Computer forensic science will be the science of acquiring, preserving, retrieving, and presenting data which has been processed electronically and stored on computer media. Network forensics is often designed to describe the duty of analyzing information collected on active networks from various intrusion detection, auditing, and monitoring capabilities when considering protection[4].

There four elements within the network intrusion forensics system. They are network forensics server, network forensics agents, network monitor, network investigator. Network forensics server integrate the forensics data and analysis them. In addition it guides the network packet filter and captures behavior by the network monitor. It could launch the investigation program upon the network investigator as the response to the sensitive attacks.

Network forensics agents are engine of all the data gathering, data extraction and data secure transportation. It also allows the mechanism of digital signature to data integration, communication, command and control. Agents resident by the monitored host and network Network monitor serves as a packet capture machine to adaptively capture the network traffics. Network investigator is the network survey machine. It can provide you with the mapping topology data and so on. It could actively investigate target when server allows the

command. It could launch the real-time investigation reaction to the network intrusion.

II BACKGROUND AND RELATED WORK

Network forensics is naturally a dedicated investigation technology that enables capture, recording and analysis of network packets and events for investigative purposes. It involves monitoring network traffic and determining if there is an anomaly in the whole traffic and ascertaining it doesn t matter if it indicates an attack. When it is after that the natural phenomena as to the attack can be determined. When attacks are successful, forensic techniques enable investigators to catch the attackers. The most effective goal really should be to provide sufficient evidence to let the perpetrator as being prosecuted [1]. The network forensic analysis process involves preparation, collection, preservation, examination, analysis, investigation and presentation phases [2]. The gathering, examination and analysis phases are most challenging and difficult. A data reduction technique for Intrusion Detection System (IDS) has been introduced by Lam et al [3]. Similarly there exists a would need to develop techniques to collect and retain sufficient data for analysis and forensics in just a storage efficient manner. Data can't be selectively collected as vital information can be lost. Every data aren't collected as storage requirements are not infinite. Useful attack information needs to be collected or extracted from packet captures like protocol types, header information, number of data transferred, number of packets transferred, length of the link in time, and statistics on specific addresses, protocol flags and login attempts assist in forensic processes [4].
Ethereal is definitely an open source software and frequently used currently being a network packet analyzer. It captures packets live direct from network. It displays the knowledge in the whole headers of most the protocols employed in the transmission of one's packets captured. It filters the packets counting on user needs. Ethereal allows surf for packets using some specifications[6,7].

Existing system Problems:

- Existing system packet information does not specify order or sequence information so that it becomes easy to attacker to send packet as an anomalous user.
- Existing system does not provides real time filtering techniques.
- Existing system does not tested on open source packages like winpcap and snort etc.
- Existing system does not recognize packet information whether the packet belongs to application layer protocol or not.

3. PROPOSED FRAMEWORK

When application layer sends data towards the other end as to the session, the data will certainly be processed by each layer due to top to the bottom consequently. First, the application layer data are sent in the transport layer, just for instance TCP layer, that's responsible for the reliability of two communication parties from end to finish[4]. The application data processed by TCP layer will generate data segments. Then, an idea segment is delivered to the network layer, which is responsible to process the particulars of data translation within the network, packet routing for instance. Network layer processes received data and generates data fragments, which may be handed to the data link layer. Data link layer, together with physical layer take care of the data packets' concrete transmission in network. As the network adapter works in data link layer in general, the data packet captured is the link-layer packet. In addition to the application layer data, it also contains data link layer header, IP header, as well as the TCP or UDP header above IP layer, and the application layer may also\ define its own frame structure[4,8].
Capture program is achieved by the data packet capture driver running on Windows core layer, which don't use a special data gathering system, but captures data packets with the network card. Therefore, there must be an efficient and low packet loss rate packet capture driver.

Model

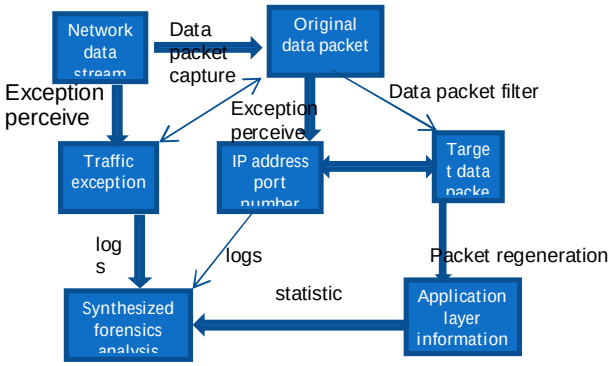

Fig 1:Application layer information forensics model

1. ARP Sniffer module: This sniffs all ARP traffic from the network.
2. MAC - ARP header anomaly detector module: This module classifies the ARP traffic into Inconsistent Header ARP packets and Consistent Header ARP packets.
3. Known Traffic Filter module: This filters most of the traffic, that's already learnt. It certainly will either drop the packet if the Ip to MAC mapping is coherent along with the learnt Host Database or raise an alarm generally if there are any contradictions. Most of the new ARP packets with unknown addresses are sent in the Spoof Detection Engine for verification.
4. Spoof Detection Engine module: This is the main detection engine.We feed the Consistent Header ARP packets to it as input.
5. Add to Database Module: Legitimate ARP entries verified by the Spoof Detection Engine are added to the Host Database by this module.
6. Spoof Alarm Module: This module raises an alarm on detection of ARP spoofing[9-11].

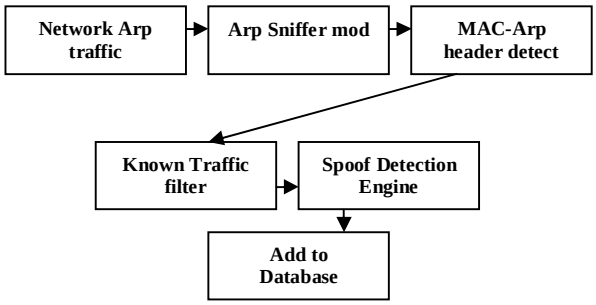

Fig 2:Arp Spoof Methodology

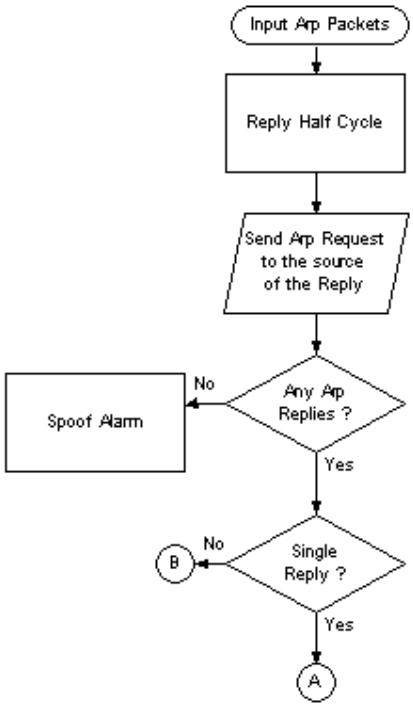

Fig 3: Arp replay detection flow

The Spoof Detection Engine applies our detection algorithm to detect ARP spoofing. The newly seen Consistent Header ARP packets are input to this module. The engine now internally bunches these packets into the three categories namely Full ARP Cycle, Request and Response Half Cyclepackets. After applying the detection algorithm the Spoof Detection engine either sends the ARP entry to the Add to Database module or the Spoof Alarm module. The Add to Database module will add these verified MAC and IP address mapping to the Host Database.

According to the "Type" field of the Ethernet frame header, decide IP, ARP, or RARP packet which one should be constructed. If it's IP packet, read in all the bytes from the 15th byte to the final byte in the buffer zone, and construct IP object based on the IP packet format. Afterwards, in the light of the "Protocol" field in the IP packet, determines TCP, UDP, or ICMP packet which one should be constructed. If it's TCP packet, read in the data contents of IP packet, and construct TCP object in accordance with the TCP Packet Format.

4. EXPERIMENTAL RESULTS

All experiments were performed with the configurations Intel(R) Core(TM)2 CPU 2.13GHz, 2 GB RAM, and the operating system platform is Microsoft Windows XP Professional (SP2).

```
Packet #1 (1).
-------------------------------------------------------------------------------
08 86 3B AF   - 86 00 C4 46   - 19 77 A9 88   - 08 00 45 00     ..;....F.w....E.
-
00 30 7C 32   - 00 00 FF 01   - BA 44 C0 A8   - 02 04 C0 A8
.0|2.....D.....  -
02 01 08 00   - D6 F3 00 01   - 4E 91 4B 61   - 73 70 65 72
........N.Kasper  -
73 6B 79 20   - 70 69 6E 67   - 20 64 61 74   - 61 00          sky ping data.

Packet #2 (2).
-------------------------------------------------------------------------------
C4 46 19 77   - A9 88 08 86   - 3B AF 86 00   - 08 00 45 00     .F.w....;.....E.
-
00 30 0C 56   - 00 00 40 01   - E9 21 C0 A8   - 02 01 C0 A8
.0.V..@..!.....  -
02 04 00 00   - DE F3 00 01   - 4E 91 4B 61   - 73 70 65 72
........N.Kasper  -
73 6B 79 20   - 70 69 6E 67   - 20 64 61 74   - 61 00          sky ping data.

Packet #3 (20).
-------------------------------------------------------------------------------
08 86 3B AF   - 86 00 C4 46   - 19 77 A9 88   - 08 00 45 00     ..;....F.w....E.
-
00 30 7C 34   - 00 00 FF 01   - BA 42 C0 A8   - 02 04 C0 A8
.0|4.....B.....  -
02 01 08 00   - D6 F2 00 01   - 4E 92 4B 61   - 73 70 65 72
........N.Kasper  -
73 6B 79 20   - 70 69 6E 67   - 20 64 61 74   - 61 00          sky ping data.

Packet #4 (21).
-------------------------------------------------------------------------------
C4 46 19 77   - A9 88 08 86   - 3B AF 86 00   - 08 00 45 00     .F.w....;.....E.
-
00 30 0C 57   - 00 00 40 01   - E9 20 C0 A8   - 02 01 C0 A8     .0.W..@..
.....  -
02 04 00 00   - DE F2 00 01   - 4E 92 4B 61   - 73 70 65 72
........N.Kasper  -
73 6B 79 20   - 70 69 6E 67   - 20 64 61 74   - 61 00          sky ping data.

Packet #5 (54).
-------------------------------------------------------------------------------
08 86 3B AF   - 86 00 C4 46   - 19 77 A9 88   - 08 00 45 00     ..;....F.w....E.
-
00 30 7C 35   - 00 00 FF 01   - BA 41 C0 A8   - 02 04 C0 A8
.0|5.....A.....  -
02 01 08 00   - D6 F1 00 01   - 4E 93 4B 61   - 73 70 65 72
........N.Kasper  -
73 6B 79 20   - 70 69 6E 67   - 20 64 61 74   - 61 00          sky ping data.

Packet #6 (55).
-------------------------------------------------------------------------------
C4 46 19 77   - A9 88 08 86   - 3B AF 86 00   - 08 00 45 00     .F.w....;.....E.
-
00 30 0C 58   - 00 00 40 01   - E9 1F C0 A8   - 02 01 C0 A8
.0.X..@.....  -
02 04 00 00   - DE F1 00 01   - 4E 93 4B 61   - 73 70 65 72
........N.Kasper  -
73 6B 79 20   - 70 69 6E 67   - 20 64 61 74   - 61 00          sky ping data.

Packet #7 (63).
-------------------------------------------------------------------------------
```

08 86 3B AF - 86 00 C4 46 - 19 77 A9 88 - 08 00 45 00 ..;....F.w....E.
-
00 30 7C 3A - 00 00 FF 01 - BA 3C C0 A8 - 02 04 C0 A8
.0|:.....<..... -
02 01 08 00 - D6 F0 00 01 - 4E 94 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #8 (64).

C4 46 19 77 - A9 88 08 86 - 3B AF 86 00 - 08 00 45 00 .F.w....;.....E.
-
00 30 0C 59 - 00 00 40 01 - E9 1E C0 A8 - 02 01 C0 A8
.0.Y..@..... -
02 04 00 00 - DE F0 00 01 - 4E 94 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #9 (138).
---
08 86 3B AF - 86 00 C4 46 - 19 77 A9 88 - 08 00 45 00 ..;....F.w....E.
-
00 30 7C 67 - 00 00 FF 01 - BA 0F C0 A8 - 02 04 C0 A8 .0|g.....
-
02 01 08 00 - D6 EF 00 01 - 4E 95 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #10 (139).

C4 46 19 77 - A9 88 08 86 - 3B AF 86 00 - 08 00 45 00 .F.w....;.....E.
-
00 30 0C 5A - 40 00 40 01 - A9 1D C0 A8 - 02 01 C0 A8
.0.Z@.@..... -
02 04 00 00 - DE EF 00 01 - 4E 95 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #11 (435).
---
08 86 3B AF - 86 00 C4 46 - 19 77 A9 88 - 08 00 45 00 ..;....F.w....E.
-
00 30 7D 11 - 00 00 FF 01 - B9 65 C0 A8 - 02 04 C0 A8 .0}.....e.....
-
02 01 08 00 - D6 EE 00 01 - 4E 96 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #12 (436).

C4 46 19 77 - A9 88 08 86 - 3B AF 86 00 - 08 00 45 00 .F.w....;.....E.
-
00 30 0C 5B - 00 00 40 01 - E9 1C C0 A8 - 02 01 C0 A8
.0.[..@..... -
02 04 00 00 - DE EE 00 01 - 4E 96 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #13 (587).
---
08 86 3B AF - 86 00 C4 46 - 19 77 A9 88 - 08 00 45 00 ..;....F.w....E.
-
00 30 7D 73 - 00 00 FF 01 - B9 03 C0 A8 - 02 04 C0 A8 .0}s.....
-
02 01 08 00 - D6 ED 00 01 - 4E 97 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #14 (588).

C4 46 19 77 - A9 88 08 86 - 3B AF 86 00 - 08 00 45 00 .F.w....;.....E.
-
00 30 0C 5C - 00 00 40 01 - E9 1B C0 A8 - 02 01 C0 A8
.0.\..@..... -
02 04 00 00 - DE ED 00 01 - 4E 97 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #15 (612).
---
08 86 3B AF - 86 00 C4 46 - 19 77 A9 88 - 08 00 45 00 ..;....F.w....E.
-
00 30 7D 86 - 00 00 FF 01 - B8 F0 C0 A8 - 02 04 C0 A8 .0}.....
-
02 01 08 00 - D6 EC 00 01 - 4E 98 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #16 (613).

C4 46 19 77 - A9 88 08 86 - 3B AF 86 00 - 08 00 45 00 .F.w....;.....E.
-
00 30 0C 5D - 00 00 40 01 - E9 1A C0 A8 - 02 01 C0 A8
.0.]..@..... -
02 04 00 00 - DE EC 00 01 - 4E 98 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #17 (666).
---
08 86 3B AF - 86 00 C4 46 - 19 77 A9 88 - 08 00 45 00 ..;....F.w....E.
-
00 30 7D 8B - 00 00 FF 01 - B8 EB C0 A8 - 02 04 C0 A8 .0}.....
-
02 01 08 00 - D6 EB 00 01 - 4E 99 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #18 (667).

C4 46 19 77 - A9 88 08 86 - 3B AF 86 00 - 08 00 45 00 .F.w....;.....E.
-
00 30 0C 5E - 00 00 40 01 - E9 19 C0 A8 - 02 01 C0 A8
.0.^..@..... -
02 04 00 00 - DE EB 00 01 - 4E 99 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #19 (673).
---
08 86 3B AF - 86 00 C4 46 - 19 77 A9 88 - 08 00 45 00 ..;....F.w....E.
-
00 30 7D 90 - 00 00 FF 01 - B8 E6 C0 A8 - 02 04 C0 A8 .0}.....
-
02 01 08 00 - D6 EA 00 01 - 4E 9A 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Packet #20 (674).

C4 46 19 77 - A9 88 08 86 - 3B AF 86 00 - 08 00 45 00 .F.w....;.....E.
-
00 30 0C 5F - 40 00 40 01 - A9 18 C0 A8 - 02 01 C0 A8
.0._@.@..... -
02 04 00 00 - DE EA 00 01 - 4E 9A 4B 61 - 73 70 65 72
.....N.Kasper -
73 6B 79 20 - 70 69 6E 67 - 20 64 61 74 - 61 00 sky ping data.

Fig 4: Home view of SNIFFER

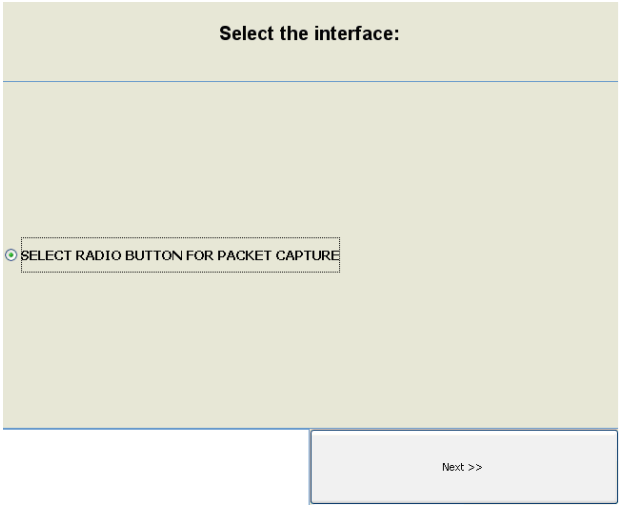

Fig 5: Selecting network interface card

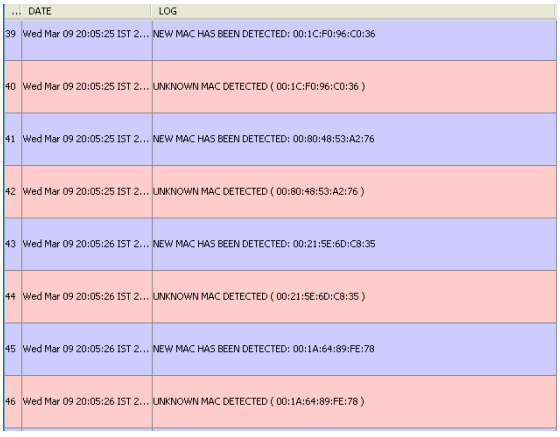

Fig 6: Alerts classification

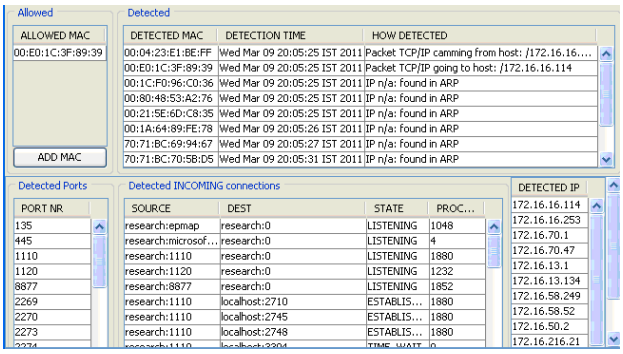

Fig 7: Adding ports and mac details

5. CONCLUSION AND FUTURE WORK

The major challenge in network forensics is handling the massive size of network packet capture. It is difficult to store, manage and analyze. We address this problem by reducing the packet capture file size by marking the attack packets using the packet header information only. For marking the attack packets, we correlated various attacks and its corresponding identified significant features.This system captures network packets, analyze the application layer packets information and then identifies the attacks in the layer with alerts. This proposed work is succefully identifies the arp ,mac spoofs in the network. In future this work can be extended to identify the web application vulnerabilities to detect flaw points in the applications.

REFERENCES

[1] Yanet Manzano and Alec Yasinsac, “Policies to Enhance Computer and Network Forensics”, The 2nd Annual IEEE Systems, Man, and Cybernetics Information Assurance Workshop, at the United States Military Academy, June 2001

[2] S. Ioannidis, K. G. Anagnostakis, J. Ioannidis, and A. D. Keromytis. “xPF: packet filtering for lowcost network monitoring”. In Proceedings of the IEEE Workshop on High-Performance Switching and Routing (HPSR), pages 121--126, May 2002.

[3] 10.S. McCanne and V. Jacobson. The BSD packet filter: A new architecture for user-level packet capture. In Proc. of the USENIX Technical Conf., Winter 1993

[4] D.Wang, R.Hao, D.Lee. Fault detection in rule-based software systems. *Information and Software Technology*. 2003. 45(12): 865- 871.

[5]Application Layer Information Forensics based on Packet Analysis Ruining Guo, Tianjie Cao, Xuan Luo, 2010 International Conference of Information Science and Management Engineering

[6]IEEEStd1003.1.2001.http://standards.ieee.org/reading/ieee/std/posix/1003.1-2001_vol3.pdf

[7] W.Ren, H.Jin. Distributed Agent-based Real Time Network Intrusion Forensics System Architecture Design. In *Proceedings of the 19th International Conference on Advanced Information Networking and Applications (AINA’05)*. Taipei, Taiwan.

[8] Postel, J. Internet Control Message Protocol, RFC 792. http://tools.ietf.org/html/rfc0792

[8] Comer, D.E. and Stevens, D.L. 1991. Internetworking with TCP/IP.

[9] SANS Institute Reading Room. ICMP attack illustrated. http://www.sans.org/reading_room/whitepapers/threats/icmp_attacks_illustrated_477?show=477.php&cat=threats

[10] Kenney, M. Ping of death. http://www.insecure.org/sploits/ping-o-death.html.

[11] Kumar, S. 2007. Smurf-based Distributed Denial of Service (DDoS) Attack Amplification in Internet. In Proceedings of International Conference on Internet Monitoring and Protection.