International Journal of Future Generation Communication and Networking
Vol. 8, No. 5 (2015), pp. 51-60
http://dx.doi.org/10.14257/ijfgcn.2015.8.5.05

An Integrated Approach to ARP Poisoning and its Mitigation using Empirical Paradigm

Goldendeep Kaur[1] and Dr. Jyoteesh Malhotra[2]

[1]*CSE Department, Guru Nanak Dev University, Regional Campus, Jalandhar*
[2]*ECE Department, Guru Nanak Dev University, Regional Campus, Jalandhar*
[1]*goldenchugh@gmail.com*, [2]*jyoteesh@gmail.com*

Abstract

The primary objective of Cyber Security is to protect data in transit. If a network is vulnerable at layer two, the good fortune opens wide up for an attacker. With the easy availability of refined offensive tools that can exploit these vulnerabilities to create havoc in networks, there is a dire need of mitigative measures that can cope up with increasing threats. ARP Protocol violation is among the most hazardous onslaughts in the wireless networks today. This paper is an effort to implement the mechanism of ARP poisoning and its mitigation by enabling DHCP Snooping and Dynamic ARP Inspection. The attack has been demonstrated under test environment using Cain & Abel, Wireshark and NetworkMiner tools because of their merits. The paper also describes the mechanism of Dynamic ARP Inspection to mitigate man-in-the-middle attacks.

Keywords: *ARP Spoofing, Cain and Abel, Wireshark, NetworkMiner, DHCP Snooping, Dynamic ARP Inspection*

1. Introduction

Evolvement of computer networks and the variety of services they provide to the users have strengthened the need for Local Area Networks in the world today. Subsequently, security of LANs in this new era of heightened stakes has also grown into a major concern. Address Resolution Protocol plays a significant role in successful communication between clients within a Local area network. In spite of the fact that the importance of ARP protocol for communication in Wireless Networks cannot be deserted, it can be shaped up to carry out the most dangerous attacks such as Man in the Middle and Denial of Service Attacks. Since the ARP protocol is a stateless protocol that receives and processes ARP replies without issuing ARP requests [8], the manipulation of the IP-MAC bindings by the attackers become unsophisticated and easy.

The authentication mechanisms have been made stronger due to the increase in the number of online crimes. Earlier, authentication involved sending the user login information in clear text. This led to variety of credential harvesting attacks by the hackers. Thus, to provide additional security Transport Layer Security/Secure Sockets Layer (TLS/SSL) was brought in. This protocol (SSL) is still in use and authenticates the server to the client and vice a versa. In SSL, each party uses a digital certificate which is signed by a trusted third party. However with the new intrusion tools developed, the SSL can be stripped apart. A large variety of tools like Cain & Abel, Ettercap, Wireshark are available that allows easy recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using brute force, cryptanalysis and dictionary attacks thereby rendering the use of SSL digital certificates unfruitful. So, the vulnerability is not limited to HTTP connections, rather HTTPS connections can be hijacked very easily.

Most existing wireless Intrusion Detection Systems are used to detect the false bindings. Snort-wireless is a much popular choice because of its open source characteristics. However it simply matches the legitimate control list. When the attacker

ISSN: 2233-7857 IJFGCN

changes legitimate AP's MAC address using MAC Spoofing technique, nothing can be done to identify a MITM attack in a particular network. Other Kernel based patches such as Antidote and Anticap are used to avoid updating of host ARP cache that contains a MAC address different from the one already in the cache. But these patches are only used with some specific Kernel.

When a device needs to communicate with any other device on the same wireless network, it checks its ARP cache to find the MAC Address of the destination device. If the MAC address is found in the cache, it is used for communication. But if it is not found in local cache, the source machine generates an ARP request. The source broadcasts this request message to the local network. The message is received by each device on the LAN since it is a broadcast. As ARP is a stateless protocol; therefore all client operating systems update their cache if a reply is received, inconsiderate of whether they have sent request for it or not. Since ARP does not offer any method for authenticating replies in the network, these replies are vulnerable to be manipulated by other hosts on a network [5].

The main contribution of this paper is to comprehend the underlying mechanism of ARP poisoning and to check the vulnerability of the hosts with these attacking tools. The research also illustrates how to root out this problem by adopting appropriate mitigation technique.

Section 2 of this paper gives a brief introduction about tools used for ARP Spoofing, its vulnerabilities and mitigation. Section 3 provides the mechanism involved in ARP poisoning, Section 4 describes its mitigation using DHCP Snooping Dynamic ARP Inspection and Section 5 concludes the paper.

2. Related Work

Nowadays, network attack tools have improved tremendously which made this black art of ARP poisoning very easier to accomplish. A number of windows and Linux based tools are available freely that can handle the attack mechanism. The attacker no longer requires the sophisticated knowledge to use these tools. Every network whether it is public, residential or organizational is susceptible to ARP Spoofing. One of the simplest and windows based tool is Cain & Abel. [14] Cain & Abel is a free and simple password recovery tool that will be quite useful for network administrators, professional penetration testers, forensic staff and security software vendors. It allows recovery of various kinds of passwords by sniffing the network, cracking encrypted passwords using various types of attacks, analyzing routing, protocols, recording VoIP conversations, revealing password boxes, uncovering cached passwords etc. It has several built in utilities that can initiate a number of intelligent attacks on the target computer.

Wireshark [15] and NetworkMiner [16] are other important tools used in this paper in ARP attack mechanism with Cain & Abel. Wireshark is open source packet analyzer that is used for network troubleshooting and analysis. It allows the user to put the network interface card in promiscuous mode in order to see all traffic visible on that interface, not just the traffic addressed to one of the interface's configured addresses. NetworkMiner is Forensic Analysis Tool that can be used as passive packet capturing tool in order to detect sessions, operating systems, hostnames etc without putting any traffic on the network. It collects the data about hosts on the network rather than to collect data regarding the traffic on the network.

On the other hand, a survey has been conducted on the tools used to detect and mitigate these attacks so that the networks can be secured to larger extent. But it has been observed that there is no universal defense against these attacks. In fact one of the simplest methods is to use static ARP entries. As static entries cannot be updated, spoofed ARP replies can be ignored. But this method is not suitable practically for large networks to manually add each entry into the cache.

Free Intrusion Detection Systems like Snort [2], ARPWatch [11], XArp are working on detection mechanism but not able to provide complete defense. Kernel based patches like Anticap [12] and Antidote [10] prevents ARP poisoning by rejecting the ARP replies that contains a MAC address different from the current entry in the cache for same IP address. But this solution is also available for a limited number of specific kernels.

On the other hand, Port Security detects MAC cloning but does not able to prevent ARP Spoofing. High end Cisco switches proposed a feature known as Dynamic ARP Inspection [7] that allows the switch to block invalid <IP, MAC> pairings. It uses local pairing table that is built using a feature known as DHCP snooping to detect which pairings are invalid.

From the survey conducted, it can be inferred that out of all the schemes Dynamic ARP Inspection is the best for the mitigation of these attacks. Its mechanism is far better than all other available solutions.

The step by step procedure of ARP attack mechanism performed in an residential network has been described in section 3 and after that the steps used to mitigate these attacks using the apt technique has been described in section 4.

3. Mechanism of ARP Spoofing

We used Cain & Abel as windows based penetration testing utility to check the network configuration vulnerability for the ARP Spoofing attack. The methodology has been illustrated by means of algorithm and flowchart.

Algorithm 1: Working of Cain
Input: Captured ARP Packets
Output: Capturing user credentials in plain text

1: Scan all the hosts in the subnet.

2: for i=1, n where n= number of hosts in subnet

Add to list (i);

End for

3: Move to APR section.

4: for i=1, n

Select victim host (i) and add i to left list;

Select gateway IP (i) and add it to right list;

End for

5: Start ARP poisoning.

6: Steal user credentials, images, sessions *etc*.

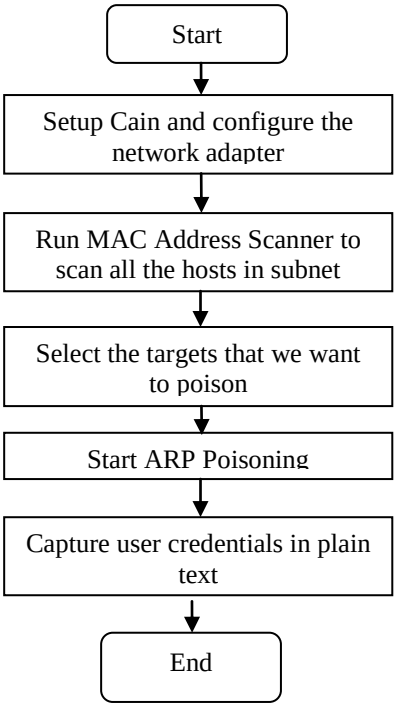

Figure 1. Flowchart

The steps involved in run time environment are explained as follows.

1) To do a man-in-the-middle attack against the target host, start Cain and we will find the sniffer tab on the main panel. We have to activate the sniffer tab to allow the software to sniff packets. We need to select the active network adapter by clicking on the configure option as shown in Figure 2.

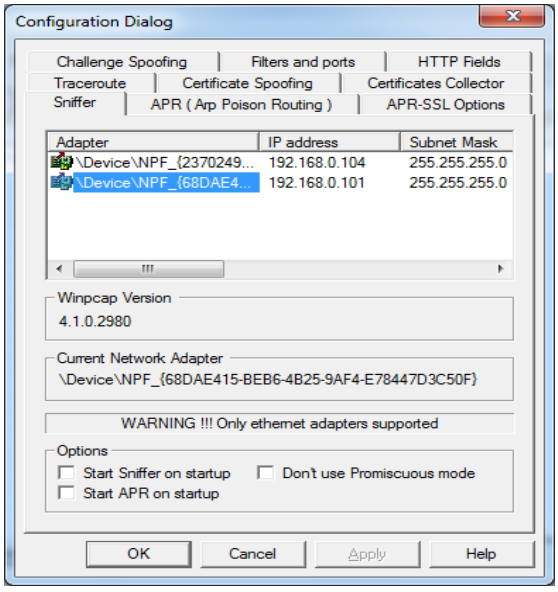

Figure 2. Selecting the Network Adapter

2) After selecting the active network adapter, we will start scanning for all the active hosts in our subnet. To do this, we will click on the blue "+" icon. A dialog box will appear and we have to select "All hosts in my subnet" and then click OK as shown in Figure 3.

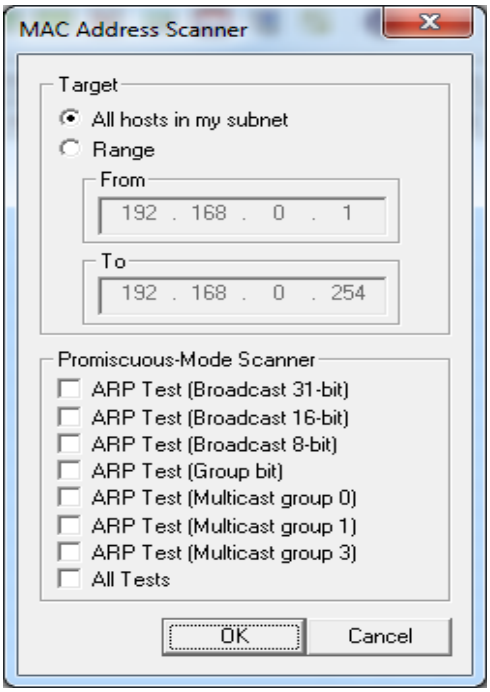

Figure 3. Scanning for Active Hosts

3) After pressing OK button, all the active hosts in subnet will start adding in the list. The result will appear like this as shown in Figure 4. The MAC addresses are kept hidden in order to avoid any kind of misuse.

Figure 4. Hosts List

4) Now we have to go to APR section on the lower left corner. From the top menu we have to select the add-to-list button to configure the communication segment we want to poison. Select the IP of the target host from the left pane and that of gateway router IP address from the right pane and click “OK” as shown in Figure 5.

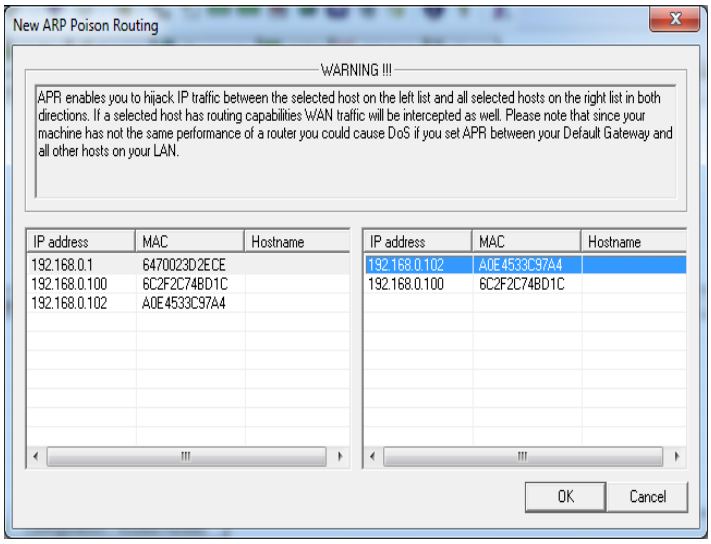

Figure 5. Arp Configuration Screen

5) The target IP is 192.168.0.102 and that of gateway is 192.168.0.1. Now click on the APR icon in the top menu to start poisoning the ARP table.

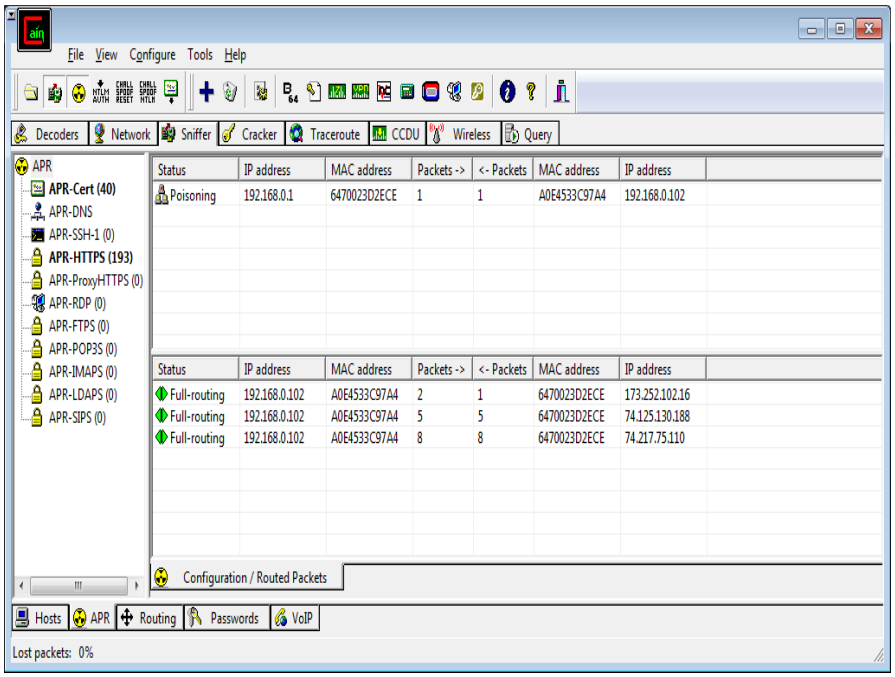

Figure 6. Arp Poisoning Initiated

6) While the Cain is performing all the poisoning, run Wireshark to capture the packets between the target host and the gateway router. Before start capturing the packets, disable “Capture packets in promiscuous mode” in the capture options. This is done to capture the packets only among three systems (target host, gateway and our pc).

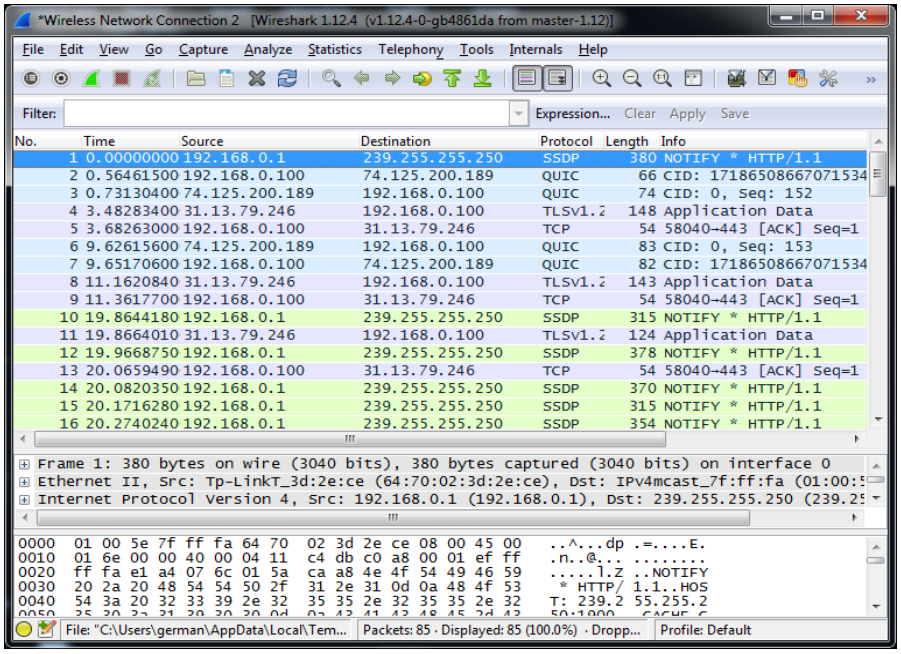

Figure 7. Wireshark Capturing Traffic

7) Stop capturing when enough packets have been captured and save it as .pcap file. Start NetworkMiner and open the .cap file. After few minutes we will see host details, plain data like credentials, pictures, OS fingerprints etc. from the .pcap file as shown in Figure 8.

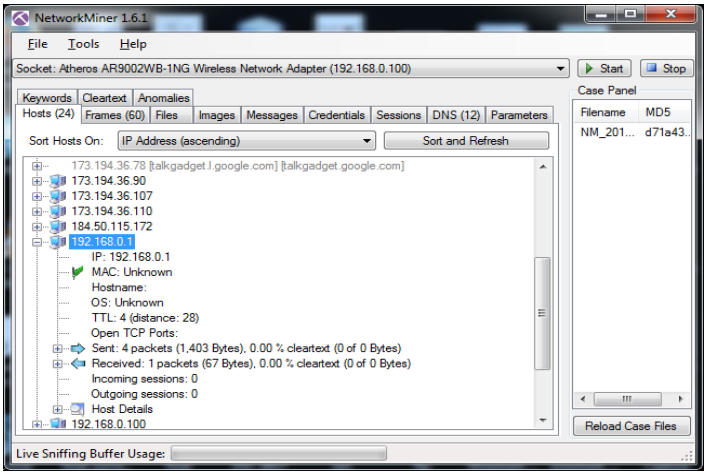

Figure 8. PCAP File Showing All Hosts

Similarly we can see the images, DNS, files, credentials entered by the user, sessions etc by clicking on the specific tab. In this way the whole mechanism of ARP attack is performed.

Table 1. Comparison Summary of Tools

Tool	Use	Pros/Cons
Cain & Abel	Capturing and monitoring traffic for passwords, recording voice over IP (VoIP) conversations, cracking encrypted passwords etc.	Free Windows based password recovery tool; Various techniques available to crack passwords; Requires Rainbow tables that must be downloaded from other sources online; Bit more complicated to use as some built in features might be difficult for invoice users.
Wireshark	Fantastic open source packet analyzer that allows you to examine the data from a live network.	Troubleshoot network problems; Debug protocol implementations; Used to learn network protocol internals; Must be able to capture an interface which is not in existence presently; Must have compressor to compress the data while writing to hard disk.
NetworkMiner	Passive forensic analysis tool that works in the background to check the packets coming from host server to dig out data such as operating system, sessions, open ports etc.	Does not put any burden on the network and works silently; Parse the files for off-line analysis; Host centric rather than packet centric; Young tool, still numerous functionality enhancements pending

4. Mitigation Mechanism

The Cisco IOS Software features that are used to mitigate the man-in-middle attacks are DHCP Snooping and Dynamic ARP Inspection. [7] Dynamic ARP Inspection prevents ARP poisoning by verifying the authenticity of all ARP requests and responses before updating switch's ARP cache or forwarding to the intended destinations. It is dependent on DHCP Snooping. To run Dynamic ARP Inspection, the feature DHCP Snooping must be enabled. DAI verifies the authenticity by intercepting the ARP packet and comparing its <IP, MAC> binding with the information contained in the trusted binding table. This trusted binding table is maintained by DHCP Snooping. DAI has another important feature that includes implementing a configurable rate-limit function on the number of incoming packets. The default rate is 15pps on untrusted interfaces. This is an important feature because all the authentication checks are carried out by CPU, without this function switch would be at risk to Denial of Service attacks. If the number of incoming packets exceeds the specified limit, the switch places the port in error-disabled state.

The process of mitigation starts by logging into the Cisco Catalyst Switch and enabling the DHCP Snooping as shown in Figure 9.

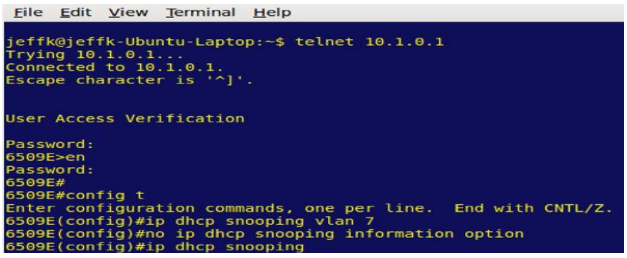

Figure 9. Enabling DHCP Snooping

The next step is to enable Dynamic ARP Inspection.

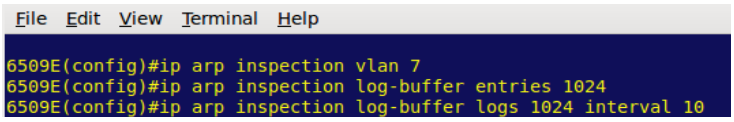

Figure 10. Enabling Dynamic Arp Inspection

As DAI imposes a rate limit function on the untrusted ports the commands that are used on the trusted ports are shown as follows

Figure 11. Commands Used on the Trusted Port

In this way the MITM attacks are tackled by enabling Dynamic ARP Inspection in the Cisco switches.

5. Conclusion

It has been observed that Address Resolution Protocol is susceptible to spoofing attacks. Although ARP is inevitable in the network protocol architecture, measures and mechanism need to be devised to protect this vulnerable protocol against spoofing attacks. In this paper, a test bed to check the vulnerabilities of the residential, organizational or private networks to ARP spoofing attacks has been created. In this work the scope of spoofing has been extended to HTTPS unlike commonly available tools which are limited to HTTP connections only. Various techniques have also been presented in this paper to protect the users from such vulnerabilities like man-in-the-middle attacks, MAC cloning etc. Mostly, the available mitigation software's are applicable to specific kernel and require persistent traffic monitoring. A versatile mitigation technique that is suitable for almost every kernel has been used here and it is able to provide complete defense to these spoofing attacks. Its only disadvantage is the high cost of switches. So the work is in progress to develop a novel algorithm to mitigate such attacks taking into account cost factor as well. The present work can also be taken to advantage to improve the efficiency of existing techniques.

References

[1] S. Whalen, "An introduction to ARP spoofing", 2600: The Hacker Quarterly, vol. 18, no. 3, Fall 2001,.Available: http://servv89pn0aj.sn.sourcedns.com/_gbpprog/2600/arp spoofing intro.pdf.
[2] Snort Project, "The. Snort: The open source network intrusion detection system", <http://www.snort.org>.
[3] T. Demuth and A. Leitner, "ARP spoofing and poisoning: Traffic tricks", Linux Magazine, vol. 56, July **(2011)**, pp. 26-31.

[4] Y. Bhaiji, LAYER 2 ATTACKS & MITIGATION Techniques http://www.sanog.org/resources/sanog7/yusuf-L2-attack-mitigation.pdf.
[5] D. Plummer, "An Ethernet Address Resolution Protocol", RFC, 826, **(2010)** November.
[6] N. Donato, "Poisoning Attack and Mitigation Techniques", Retrieved from Windows ARP attack tools:http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/white, **(2005)**.
[7] Cisco Systems, "Configuring Dynamic ARP Inspection", Catalyst 6500 Series Switch Cisco IOS Sofware Configuration Guide, Release 12.2SX, chapter 39, **(2012)**, pp. 39:1-39:22.
[8] M. A. Carnut and J. J. C. Gondim, "ARP Spoofing Detection on Switched Ethernet Networks: A Feasibility Study", 5th Symposium on Security in Informatics held at Brazilian Air Force Technology Institute, **(2003)** November.
[9] E. Hjelmvik, "Passive Network Security Analysis with NetworkMiner", Retrieved from: http://www.forensicfocus.com/passivenetworksecurity-analysis-networkminer
[10] I. Teterin, "Antidote, SecurityFocus", http://online.securityfocus.com/archive/1/299929, last accessed, **(2012)** April.
[11] L. N. R. Group, "Arpwatch, The Ethernet Monitor Program; for keeping track of ethernet/ip address pairings", (Last accessed April 17, 2012).
[12] M. Barnaba, "anticap", (accessed 17 April 2013) Online. Available: http://www.antifork.org/anticap.
[13] http://resources.infosecinstitute.com/password-cracking-using-cain-abel/
[14] http://www.oxid.it/cain.html
[15] https://www.wireshark.org/
[16] R. MacRee, "NetwrokMiner: Network Forensic Analysis Tool", Retrieved from: http://holisticinfosec.org/toolsmith/pdf/august2008.pdf.

Authors

Goldendeep Kaur was born in Amritsar, Punjab, India. She is currently pursuing M.tech Computer Science & Engineering from Guru Nanak Dev University, Regional Campus, Jalandhar. She received his B.Tech degree with Distinction from Amritsar College of Engineering & Technology, Amritsar in 2013. Her research areas of interests include Network Security. She has published and presented 9 research papers in scientific journals and International Conferences.

Dr. Jyoteesh Malhotra was born in Jalandhar, Punjab, INDIA. He completed B.Engg. with Distinction from P.R.M Institute of Technology & Research, Amravati and M.Tech. with University Gold Medal from Guru Nanak Dev Enginnering College, Ludhiana. He received PhD from Panjab Technical University in recognition to his contribution in the field of Wireless Communication & Networks. From 1994 to 2007 he was employed with DAVCMC, New Delhi as Lecturer and Panjab University, Chandigarh as Assistant Professor. He joined Guru Nanak Dev University Regional Campus at Jalandhar in July 2007 where he is currently Associate Professor and Head of ECE & CSE Departments.

His research interests are in the broad area of Pervasive Communication systems and Networks with emphasis on Statistical modeling of Fading Channels, Fading mitgitaion techniques, Optimization of High data rate Optical and wireless Communication Systems and Enhancement of QoS aware Wireless networks and Wireless Security. Dr. Malhotra has published and presented more than 100 technical papers in scientific journals and international conferences and authored 02 books. He is a life member of Indian Society for Technical Education (I.S.T.E.) and Editorial Board of many International Journals of repute.

