Network Security Technology for Wi-Fi and LAN

Major Project Report

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology

In

Electronics And Communication Engineering

(Communication Engineering)

By

Lalwani Punit Jaikishan

(08MECC07)

Department of Electronics & Communication Engineering

Institute of Technology

Nirma University

Ahmedabad-382 481

May 2010

Network Security Technology for Wi-Fi and LAN

Major Project Reprot

Submitted in partial fulfillment of the requirements

For the degree of

Master of Technology

In

Electronics And Communication Engineering

(Communication Engineering)

By

Lalwani Punit Jaikishan

(08MECC07)

Under the Guidance of

Prof. Sachin Gajjar

Department of Electronics & Communication Engineering

Institute of Technology

Nirma University

Ahmedabad-382 481

May 2010

Declaration

This is to certify that

i) The thesis comprises my original work towards the degree of Master of Technology in Communication Engineering at Nirma University and has not been submitted elsewhere for a degree.

ii) Due acknowledgement has been made in the text to all other material used.

Lalwani Punit Jaikishan

Certificate

This is to certify that the Major Project entitled "**Network Security Technology for Wi-Fi and LAN**" submitted by Lalwani Punit Jaikishan (08MECC07), towards the partial fulfillment of the requirements for the degree of Master of Technology in Electronics & Communication Engineering (Communication) of Nirma University, Institute of Technology, Ahmedabad is the record of work carried out by him under my supervision and guidance. In my opinion, the submitted work has reached a level required for being accepted for examination. The results embodied in this major project, to the best of my knowledge, haven't been submitted to any other university or institution for award of any degree or diploma.

Date: Place: Ahmedabad

Internal Guide

(Prof.Sachin Gajjar)
Assistant Professor, EC

External Guide

(Prof.V.H.Patel)
Senior Faculty
BISAG,Gandhinagar

HOD

(Prof. A. S. Ranade)
Professor, EC

Director

(Dr. K. Kotecha)
Director, IT, NU

Abstract

Network security is one of the most important areas of concern in the communication field, as it is important to protect the users data and information. The thesis presents the technologies for the network security and the tools to find the vulnerabilities in the network. The types of firewall and Intrusion detection system for the protection are explained. The definition of virus , worms and Trojans are also explained . The wireless security is explained with the vulnerabilities and the countermeasures to protect it. The tools like NetStumbler which works on windows platform is used which detects and marks the relative position of the wireless network with GPS, AiroPeek tool which works on the windows platform is a comprehensive packet analyzer for IEEE 802.11 wireless LAN and Airsnort which works on windows platform is a tool used to recover encryption keys are used for the Wi-Fi security.

In the second phase of the project secure file transfer module has been created using the Linux operating system. Also the Intrusion Detection and Prevention System has been implemented by installing and configuring snort, which is a free and open source network intrusion prevention system and network intrusion detection system capable of performing packet logging and real time traffic analysis of IP network.

Acknowledgements

I am deeply indebted to my thesis supervisor Prof. Sachin Gajjar for his constant guidance and motivation. He has devoted significant amount of his valuable time to plan and discuss the thesis work. Without his experience and insights, it would have been very difficult to do quality work.

I would like to express my endless thanks to the external guide of my project thesis Prof. V. H. Patel, senior faculty of BISAG for his sincere and dedicated guidance throughout the project development.

Also I would like to express my gratitude and sincere thanks to Prof. A. S. Ranade Head of Electrical Engineering Department and Dr. D. K. Kothari Coordinator M.Tech Communication Engineering program for allowing me to undertake this thesis work and for his guidelines during the review process.

I would like to express my gratitude and sincere thanks to Mr. T. P. Singh, Director of BISAG (Bhaskaracharya Institute of Space Application and Geo-Informatics) for giving me an opportunity to work under to guidance of renowned people in the field of communications and for providing all the resources for the project development.

I wish to thank all the people of BISAG and Nirma university , my classmates and all those people who have directly or indirectly helped me during my project thesis.Last, but not the least, no words are enough to acknowledge constant support and sacrifices of my family members because of whom I am able to complete the degree program successfully.

Lalwani Punit Jaikishan

08MECC07

Contents

List of Figures

Chapter 1

Introduction

1.1 Background

Network security is one of the most important areas of concern in the communication field, as it is important to protect the user's data and information.Traditionally, information security was provided primarily by physical and administrative means. Due to the widespread use of computers, new requirements have emerged in recent times. We need automated tools to protect the security of files, data, and other stored information. Networks and communications facilities require measures to protect the security of data during transmission.

There are three categories of Security:

- **Computer Security:**Security measures designed to protect data stored in computers.
- **Network (Internet) Security:**Security measures designed to protect data during their transmission over networks (like Internet).
- **Information Security:**A generic term, including both of computer security and network security (and cryptography).

According to the statistics by CERT (the Computer Emergency Response Team), every year there are numerous security-related incidents. Moreover, the sophistications of attacks are growing while the skill and knowledge needed to mount an attack are decreasing. With the ready tools available people having less knowledge of programming can also use the tools for finding the vulnerabilities in the network or a system.

1.2 Motivation

Network security is one of the most important parameter of concern in the telecommunication and Information Technology industry. With the rapid growth of the Internet and mobile communication market it is important to protect the user's data and make the transactions safe and secure. It is a challenge to keep oneself and the organization protected from the hackers and crackers. As a Communication Engineer it is my responsibility to study the various areas in the aspect of network security, find the loopholes and also find a solution to the vulnerability.

1.3 Problem and approach

The objective of the project thesis is to study the various areas involved in the process of the network security. This involves the study of various types of firewall and the Intrusion detection system, port scanning techniques and wireless LAN. To find out the various loopholes and to implement a solution for the security by using sniffing tools like wireshark [4], port scanning tools like nmap for testing the wireless LAN security.

1.4 Gantt Chart

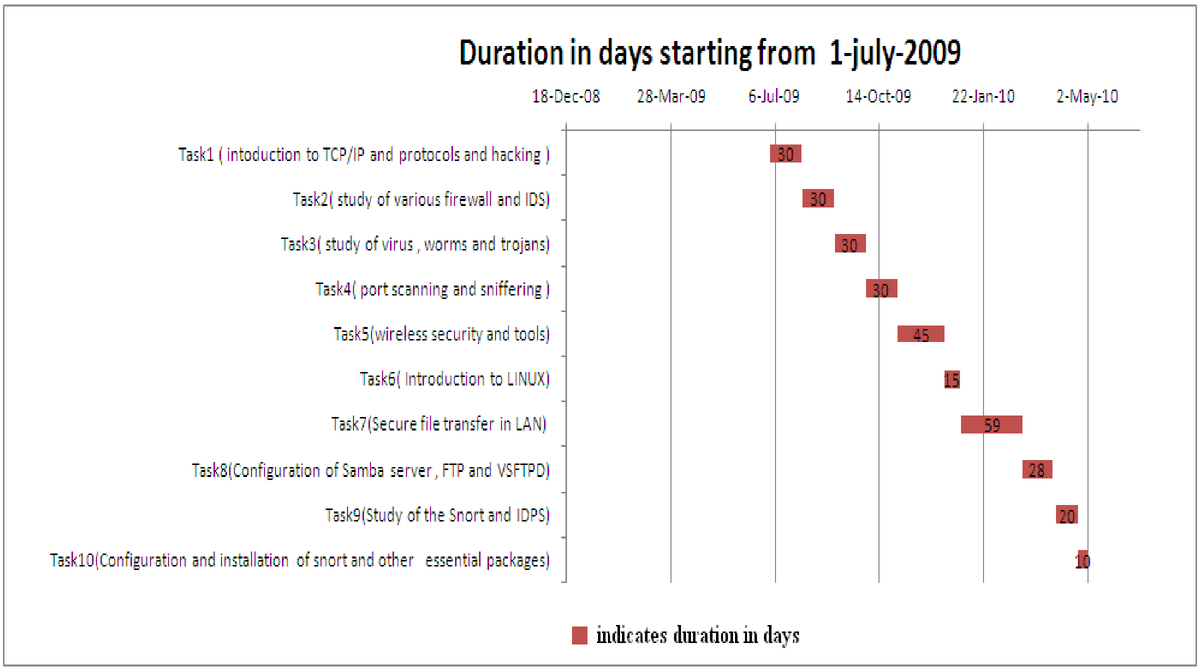


Figure 1.1: Project work planning

1.5 Contents of Thesis

The project report contains the following contents chapter wise

Chapter 2 covers the introduction of network security, the security trinity, why it's needed and how it can be achieved.

Chapter 3 discusses about Sniffers, which is a type of a network analyzer or packet analyzer, how it can be used in Local area network and wireless network. Wireshark which is one of the examples of sniffers is discussed with working and figures.

Chapter 4 covers the various types of viruses, Trojans and worms with the working of each. Also the different levels of protections used in network security are discussed.

Chapter 5 discusses about the Wi-Fi security, loopholes in it, with the tools used to hack the Wi-Fi network and the countermeasures to protect it.

Chapter 6 covers the secure file transfer model created using the Linux platform. This model is used for secure file transfer where different permissions to access the data are given to different users to read or write files from the server.

Chapter 7 shows the working of the IDPS (Intrusion Detection and Prevention System) by using the snort tool. Various steps for configuration and the interface used for creating IDPS are shown with the help of figures.

Chapter 8 discusses the conclusion, contribution and future scope of the project.

Chapter 2

Network Security

2.1 What is Network Security ?

Network security is the implementation of security devices, policies and processes to prevent unauthorized access to network resources or alteration or destruction of resources or data. Computer and network security is important for the following reasons.

2.1.1 Why it is needed ?

- **To protect company assets:**One of the primary goals of computer and network security is the protection of company assets. The assets are comprised of the "information" that is housed on a company's computers and networks. Information is a vital organizational asset. Network and computer security is concerned, above all else, with the protection, integrity, and availability of information. Information can be defined as data that is organized and accessible in a coherent and meaningful manner.

- **To gain a competitive advantage:**: Developing and maintaining effective security measures can provide an organization with a competitive advantage over its competition. Network security is particularly important in the arena of

Internet financial services and e-commerce.

- **To comply with regulatory requirements and fiduciary responsibilities:**Corporate officers of every company have a responsibility to ensure the safety and soundness of the organization. Part of that responsibility includes ensuring the continuing operation of the organization. Accordingly, organizations that rely on computers for their continuing operation must develop policies and procedures that address organizational security requirements. Such policies and procedures are necessary not only to protect company assets but also to protect the organization from liability. For example, most financial institutions are subject to federal regulation. Failure to comply with federal guidelines can result in the seizure of a financial institution by federal regulators.

- **To keep up the job :**Finally, to secure one's position within an organization and to ensure future career prospects, it is important to put into place measures that protect organizational assets. One thing to keep in mind is that network security costs money, It costs money to hire, train, and retain personnel; to buy hardware and software to secure an organization's networks; and to pay for the increased overhead and degraded network and system performance that results from firewalls, filters, and intrusion detection systems (IDS).

2.2 How Network Security can be achieved through the Security Trinity ?

The three legs of the "security trinity," prevention, detection, and response, comprise the basis for network security. The security trinity should be the foundation for all security policies and measures that an organization develops and deploys.

2.2.1 Prevention

The foundation of the security trinity is prevention. In order to provide some level of security, it is necessary to implement measures to prevent the exploitation of vulnerabilities. In developing network security schemes, organizations should emphasize preventative measures over detection and response: It is easier, more efficient, and much more cost-effective to prevent a security breach than to detect or respond to one. Remember that it is impossible to devise a security scheme that will prevent all vulnerabilities from being exploited, but companies should ensure that their preventative measures are strong enough to discourage potential criminals-so they go to an easier target.

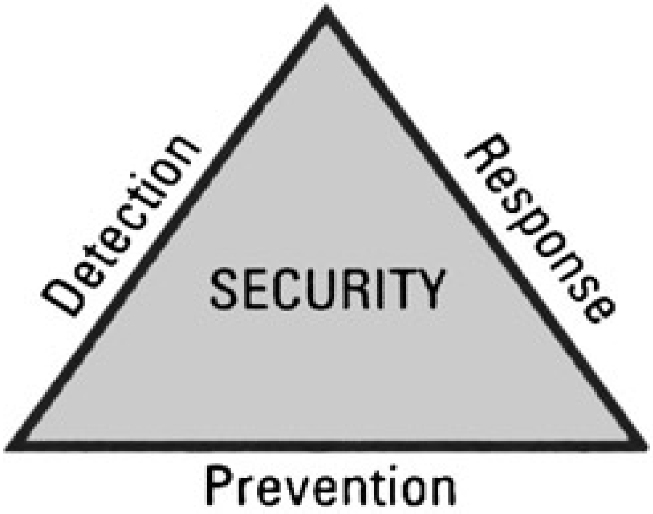


Figure 2.1: Security Trinity

2.2.2 Detection

Once preventative measures are implemented, procedures need to be put in place to detect potential problems or security breaches, in the event preventative measures fail. As later chapters show, it is very important that problems be detected immediately. The sooner a problem is detected the easier it is to correct and cleanup.

2.2.3 Response

Organizations need to develop a plan that identifies the appropriate response to a security breach. The plan should be in writing and should identify who is responsible for what actions and the varying responses and levels of escalation.

Chapter 3

Sniffers

3.1 Sniffers

A sniffer (also known as a network analyzer or packet analyzer or for particular types of networks, an Ethernet sniffer or wireless sniffer) is computer software or computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams flow across the network, the sniffer captures each packet and eventually decodes and analyzes its content according to the appropriate RFC or other specifications.

3.1.1 The Functioning

- On wired broadcast LANs, depending on the network structure (hub or switch), one can capture traffic on all or just parts of the network from a single machine within the network; however, there are some methods to avoid traffic narrowing by switches to gain access to traffic from other systems on the network (e.g. ARP spoofing)

- For network monitoring purposes it may also be desirable to monitor all data packets in a LAN by using a network switch with a so-called monitoring port, whose purpose is to mirror all packets passing through all ports of the switch.

- When systems (computers) are connected to a switch port rather than a hub the analyzer will be unable to read the data due to the intrinsic nature of switched networks. In this case a shadow port must be created in order for the sniffer to capture the data.
- On wireless LANs, one can capture traffic on a particular channel.
- On wired broadcast and wireless LANs, in order to capture traffic other than unicast traffic sent to the machine running the sniffer software, multicast traffic sent to a multicast group to which that machine is listening, and broadcast traffic, the network adapter being used to capture the traffic must be put into promiscuous mode; some sniffers support this, others don't.
- On wireless LANs, even if the adapter is in promiscuous mode, packets not for the service set for which the adapter is configured will usually be ignored; in order to see those packets, the adapter must be put into monitor mode.

3.1.2 Uses

- Analyze network problems.
- Detect network intrusion attempts.
- Gain information for effecting a network intrusion.
- Monitor network usage.
- Gather and report network statistics.
- Filter suspect content from network traffic.
- Spy on other network users and collect sensitive information such as passwords (depending on any content encryption methods which may be in use).
- Reverse engineer proprietary protocols used over the network.

- Debug client/server communications.
- Debug network protocol implementations

3.1.3 A packet sniffer:

- Can be used in education to demonstrate how network protocols work.
- It is often used in the development and debugging of networking software.
- For a token ring network, can detect that the token has been lost or the presence of too many tokens (verifying the protocol).
- Can detect that messages are being sent to a network adapter; if the network adapter did not report receiving the messages then this would localize the failure to the adapter.
- Can detect excessive messages being sent by a port, detecting an error in the implementation.
- Can collect statistics on the amount of traffic (number of messages) from a process detecting the need for more bandwidth or a better method.
- Can be used to extract messages and reassemble into a complete form the traffic from a process, allowing it to be reverse engineered.
- Can be used to diagnose operating system connectivity issues such as HTTP, FTP, SQL, Active Directory, etc.
- Can be used to analyze data sent to and from secure systems in order to understand and circumvent security measures, for the purposes of penetration testing or illegal activities.
- Can passively capture data going between a web visitor and the web servers, decode it at the HTTP and HTML level and create web log files as a substitute for server logs and page tagging for web analytics.

3.1.4 Wireshark:

- Wireshark is a free packet sniffer computer application. It is used for network troubleshooting, analysis, software and communications protocol development, and education. In June 2006 the project was renamed from Ethereal due to trademark issues.

- The functionality Wireshark provides is very similar to tcpdump, but it has a graphical front-end, and many more information sorting and filtering options. It allows the user to see all traffic being passed over the network (usually an Ethernet network but support is being added for others) by putting the network interface into promiscuous mode.[**?**]

Features

Wireshark is software that "understands" the structure of different networking protocols. Thus, it is able to display the encapsulation and the fields along with their meanings of different packets specified by different networking protocols. Wireshark uses pcap to capture packets, so it can only capture the packets on the networks supported by pcap.

- Data can be captured "from the wire" from a live network connection or read from a file that records the already-captured packets.

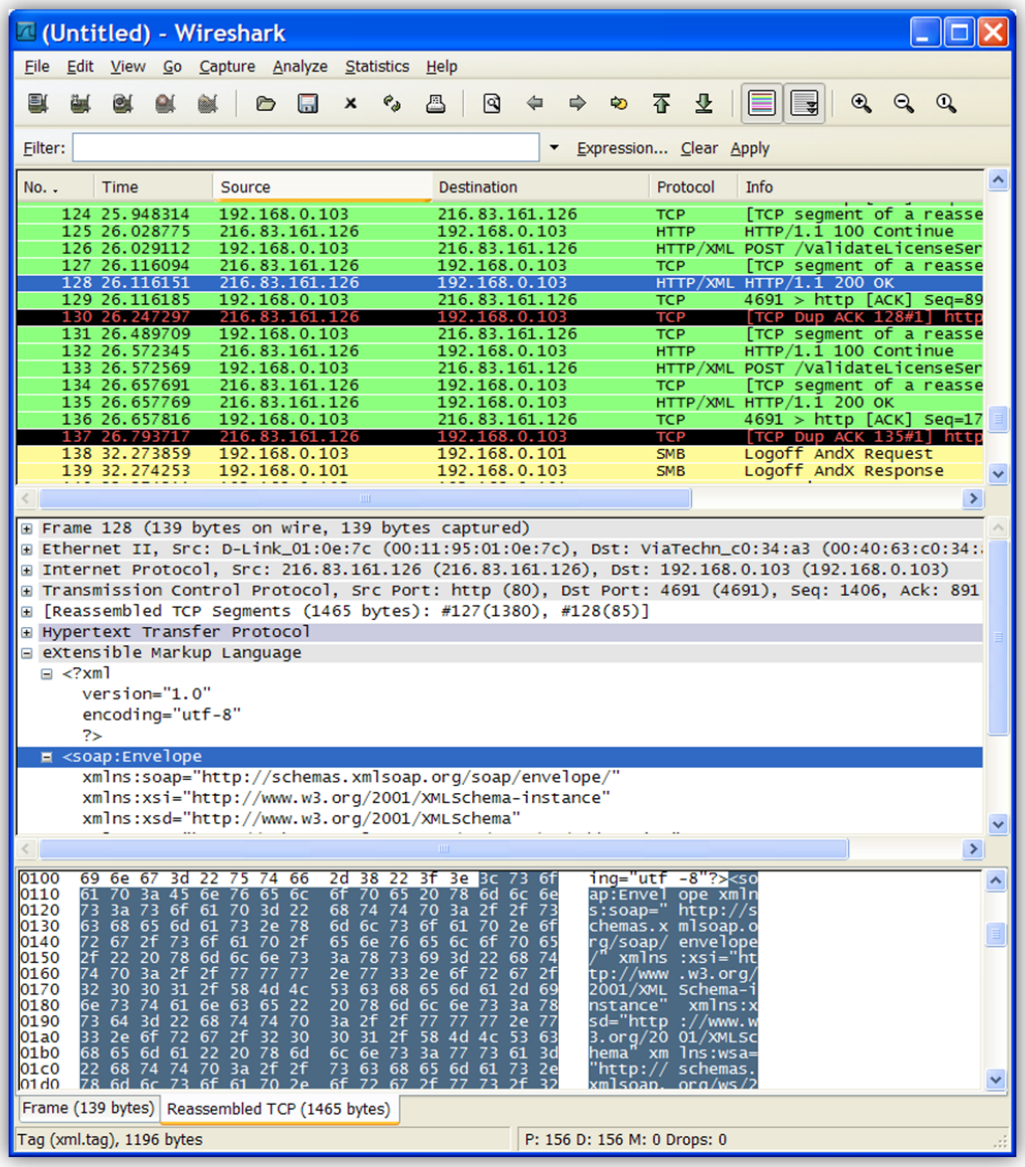
- Live data can be read from a number of types of network, including Ethernet, IEEE 802.11, PPP, and loopback.

- Captured network data can be browsed via a GUI, or via the terminal (command line) version of the utility, tshark.

- Captured files can be programmatically edited or converted via command-line switches to the "editcap" program.

- Display filters can also be used to selectively highlight and color packet summary information.
- Data display can be refined using a display filter.
- Hundreds of protocols can be dissected.

3.1.5 Screen shorts Of wireshark


(Untitled) - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply
Frame (139 bytes)
Reassembled TCP (1465 bytes)

```
No. .  Time       Source          Destination     Protocol Info
  124 25.948314   192.168.0.103   216.83.161.126  TCP      [TCP segment of a reasse
  125 26.028775   216.83.161.126  192.168.0.103   HTTP     HTTP/1.1 100 Continue
  126 26.029112   192.168.0.103   216.83.161.126  HTTP/XML POST /ValidateLicenseSer
  127 26.116094   216.83.161.126  192.168.0.103   TCP      [TCP segment of a reasse
  128 26.116151   216.83.161.126  192.168.0.103   HTTP/XML HTTP/1.1 200 OK
  129 26.116185   192.168.0.103   216.83.161.126  TCP      4691 > http [ACK] Seq=89
  130 26.247297   216.83.161.126  192.168.0.103   TCP      [TCP Dup ACK 128#1] http
  131 26.489709   192.168.0.103   216.83.161.126  TCP      [TCP segment of a reasse
  132 26.572345   216.83.161.126  192.168.0.103   HTTP     HTTP/1.1 100 Continue
  133 26.572569   192.168.0.103   216.83.161.126  HTTP/XML POST /ValidateLicenseSer
  134 26.657691   216.83.161.126  192.168.0.103   TCP      [TCP segment of a reasse
  135 26.657769   216.83.161.126  192.168.0.103   HTTP/XML HTTP/1.1 200 OK
  136 26.657816   192.168.0.103   216.83.161.126  TCP      4691 > http [ACK] Seq=17
  137 26.793717   216.83.161.126  192.168.0.103   TCP      [TCP Dup ACK 135#1] http
  138 32.273859   192.168.0.103   192.168.0.101   SMB      Logoff AndX Request
  139 32.274253   192.168.0.101   192.168.0.103   SMB      Logoff AndX Response
```

```
⊞ Frame 128 (139 bytes on wire, 139 bytes captured)
⊞ Ethernet II, Src: D-Link_01:0e:7c (00:11:95:01:0e:7c), Dst: ViaTechn_c0:34:a3 (00:40:63:c0:34:
⊞ Internet Protocol, Src: 216.83.161.126 (216.83.161.126), Dst: 192.168.0.103 (192.168.0.103)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 4691 (4691), Seq: 1406, Ack: 891
⊞ [Reassembled TCP Segments (1465 bytes): #127(1380), #128(85)]
⊞ Hypertext Transfer Protocol
⊟ eXtensible Markup Language
  ⊟ <?xml
      version="1.0"
      encoding="utf-8"
      ?>
  ⊟ <soap:Envelope
      xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/"
      xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
      xmlns:xsd="http://www.w3.org/2001/XMLSchema"
```

```
0100  69 6e 67 3d 22 75 74 66  2d 38 22 3f 3e 3c 73 6f   ing="utf -8"?><so
0110  61 70 3a 45 6e 76 65 6c  6f 70 65 20 78 6d 6c 6e   ap:Envel ope xmln
0120  73 3a 73 6f 61 70 3d 22  68 74 74 70 3a 2f 2f 73   s:soap=" http://s
0130  63 68 65 6d 61 73 2e 78  6d 6c 73 6f 61 70 2e 6f   chemas.x mlsoap.o
0140  72 67 2f 73 6f 61 70 2f  65 6e 76 65 6c 6f 70 65   rg/soap/ envelope
0150  2f 22 20 78 6d 6c 6e 73  3a 78 73 69 3d 22 68 74   /" xmlns :xsi="ht
0160  74 70 3a 2f 2f 77 77 77  2e 77 33 2e 6f 72 67 2f   tp://www .w3.org/
0170  32 30 30 31 2f 58 4d 4c  53 63 68 65 6d 61 2d 69   2001/XML Schema-i
0180  6e 73 74 61 6e 63 65 22  20 78 6d 6c 6e 73 3a 78   nstance"  xmlns:x
0190  73 64 3d 22 68 74 74 70  3a 2f 2f 77 77 77 2e 77   sd="http ://www.w
01a0  33 2e 6f 72 67 2f 32 30  30 31 2f 58 4d 4c 53 63   3.org/20 01/XMLSc
01b0  68 65 6d 61 22 20 78 6d  6c 6e 73 3a 77 73 61 3d   hema" xm lns:wsa=
01c0  22 68 74 74 70 3a 2f 2f  73 63 68 65 6d 61 73 2e   "http:// schemas.
01d0  78 6d 6c 73 6f 61 70 2e  6f 72 67 2f 77 73 2f 32   xmlsoap. org/ws/2
```

Tag (xml.tag), 1196 bytes

P: 156 D: 156 M: 0 Drops: 0

Figure 3.1: Screen short of working of Wireshark Tool

Figure 3.1 shows the source and destination IP with the relevant information with graphical front-end,and many more information sorting and filtering options. It allows the user to see all the traffic being passed over the network.

Chapter 4

Technologies For Network Security

4.1 Network Worms

A worm is a self replicating program that does not alter files but resides in active memory and duplicate it self.Worms can be classified according to the propagation method they use, i.e. how they deliver copies of themselves to new victim machines. Worms can also be classified by installation method, launch method and finally according to characteristics standard to all malware: polymorphism, stealth etc.Many of the worms which managed to cause significant outbreaks use more than one propagation method as well as more than one infection technique.

4.1.1 Email worms

Email worms spread via infected email messages. The worm may be in the form of an attachment or the email may contain a link to an infected website. However, in both cases email is the vehicle.

In the first case the worm will be activated when the user clicks on the attachment.In the second case the worm will be activated when the user clicks on the link leading to the infected site.

Email worms normally use one of the following methods to spread:

- Direct connection to SMTP servers using a SMTP API library coded into the worm
- MS Outlook services
- Windows MAPI functions

Email worms harvest email addresses from victim machines in order to spread further. Worms use one or more of the following techniques:

- Scanning the local MS Outlook address book
- Scanning the WAB address database
- Scanning files with appropriate extensions for email address-like text strings
- Sending copies of itself to all mail in the user's mailbox (worms may even 'answer' unopened items in the nbox)

While these techniques are the most common, some worms even construct new sender addresses based lists of possible names combined with common domain names.

4.1.2 Instant Messaging (ICQ and MSN) Worms

These worms have a single propagation method. They spread using instant messaging applications by sending links to infected websites to everyone on the local contact list. The only difference between these worms and email worms which send links is the media chosen to send the links.

4.1.3 Internet Worms

Virus writers use other techniques to distribute computer worms, including:

- Copying the worm to networked resources
- Exploiting operating system vulnerabilities to penetrate computers and/or networks
- Penetrating public networks
- Piggy-backing: using other malware to act as a carrier for the worm.

In the first case, the worms locate remote machines and copy themselves into folders which are open for read and write functions. These network worms scan all available network resources using local operating system services and/or scan the Internet for vulnerable machines. They will then attempt to connect to these machines and gain full access to them. In the second case, the worms scan the Internet for machines that have not been patched, i.e. have operating systems with critical vulnerabilities still open to exploitation. The worm sends data packets or requests which install either the entire body of the worm or a section of the worm's source code containing downloader functionality. If this code is successfully installed the main worm body is then downloaded. In either case, once the worm is installed it will execute its code and the cycle continues.

Worms that use Web and FTP servers fall into a separate category. Infection is a two-stage process. These worms first penetrate service files on the file server, such as static web pages. Then the worms wait for clients to access the infected files and attack individual machines. These victim machines are then used as launch pads for further attacks.

Some virus writers use worms or Trojans to spread new worms. These writers first identify Trojans or worms that have successfully installed backdoors on victim machines. In most cases this functionality allows the master to send commands to the victim machine: such zombies which have backdoors installed can be commanded to download and execute files - in this case copies of the new worm. Many worms use two or more propagation methods in combination, in order to more efficiently penetrate potential victim machines.

4.1.4 IRC Worms

These worms target chat channels, although to day IRC worms have been detected. IRC worms also use the propagation methods listed above - sending links to infected websites or infected files to contacts harvested from the infected user. Sending infected files is less effective as the recipient needs to confirm receipt, save the file and open it before the worm is able to penetrate the victim machine.

4.1.5 File-sharing Networks or P2P Worms

P2P worms copy themselves into a shared folder, usually located on the local machine. Once the worm has successfully placed a copy of itself under a harmless name in a shared folder, the P2P network takes over: the network informs other users about the new resource and provides the infrastructure to download and execute the infected file.

More complex P2P worms imitate the network protocol of specific file-sharing networks: they respond affirmatively to all requests and offer infected files containing the worm body to all comers.

4.1.6 Virus and how it differs from worms

A virus is a program that replicates, i.e. it spreads from file to file on your system and from PC to PC. In addition, it may be programmed to erase or damage data.
Worms are generally considered to be a subset of viruses, but with certain key differences. A worm is a computer program that replicates, but does not infect other files.

Instead, it installs itself once on a computer and then looks for a way to spread to other computers.

In the case of a virus, the longer it goes undetected, the more infected files there will be on the computer. Worms, however, create a single instance of their code. Moreover, unlike a virus, a worm code is stand-alone. In other words, a worm is a separate file while a virus is a set of code which adds itself to existing files.

4.1.7 Trojan

Trojans can't spread by themselves, which is what distinguishes them from viruses and worms. Trojans are typically installed secretly and deliver their malicious payload without your knowledge. Much of today's crimeware is comprised of different types of Trojans, all of which are purpose-built to carry out a specific malicious function. The most common are Backdoor Trojans (often they include a keylogger), Trojan Spies, password stealing Trojans and Trojan Proxies that convert your computer into a spam distribution machine.
Network security technologies can be broadly classified into four categories:

- Packet level protection, such as routers' Access Control Lists (ACL) or stateless firewalls
- Session level protection, such as stateful inspection firewalls
- Application level protection, such as proxy firewalls and intrusion prevention systems (IPS) File level protection, such as gateway antivirus systems

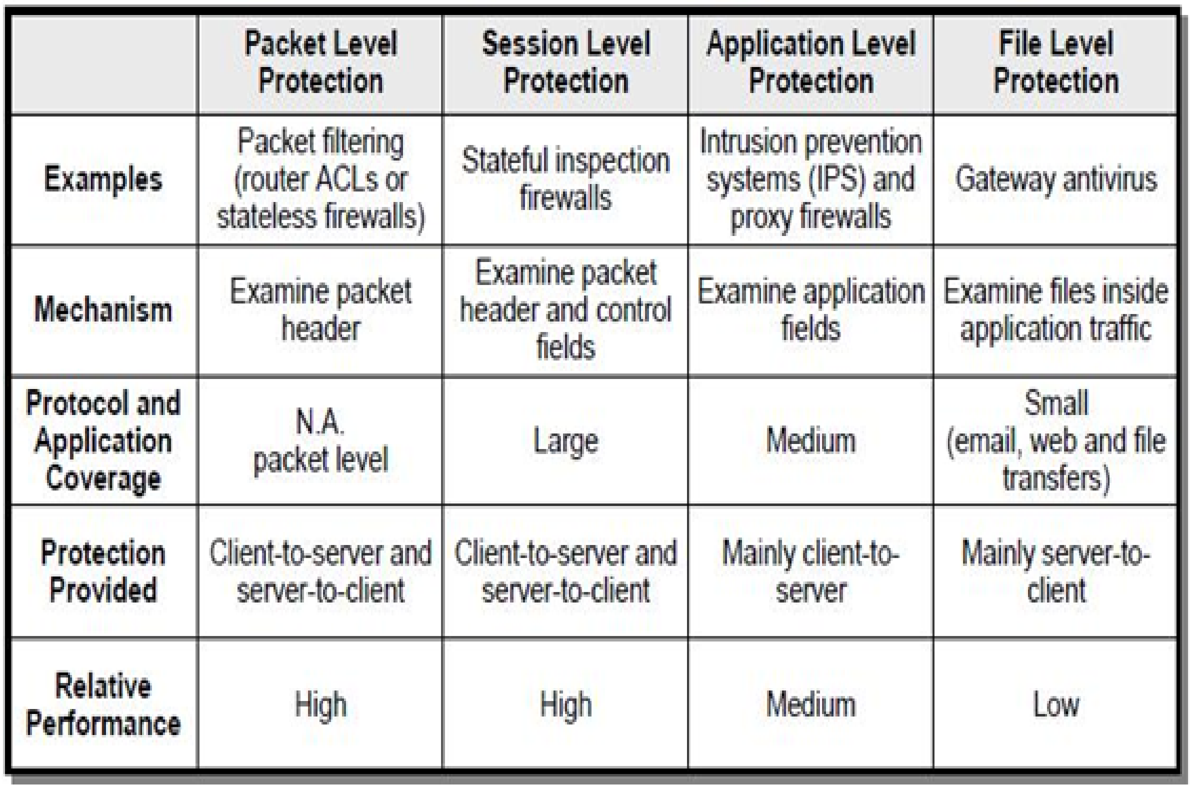
Figure 4.1 compares the four categories of network security technologies. Evaluation of each category by coverage of protocols/applications, level of protection, and relative performance enables organizations to choose the appropriate network security technologies to protect their networks.

4.1.8 Packet Level Protection

Packet level protection, also known as packet filtering, is one of the most widely used means of controlling access to a network. The concept is simple: determine whether a packet is allowed by comparing some basic pieces of information in the packet headers. Cisco IOS Access Control List (ACL) is one of the most used packet filters. IPChains is also a popular packet filter application, which comes bundled with many versions of Linux.

Two-way communication presents a challenge for network security based on packet filtering. If one blocks all incoming traffic, one prevents responses to outgoing traffic from coming in, disrupting communication. Consequently, one has to open two holes, one for outgoing traffic and one for incoming traffic, without enforcing any association of the incoming traffic with existing outgoing connections in the network. Packet filtering thus can allow in crafted malicious packets that appear to be part of existing sessions, causing damage to protected resources.

Packet filtering devices do not track dynamic protocols, where a server and a client negotiate a random port for data transmission. Examples of protocols that use dynamic ports include FTP, RPC, and H.323. To enable these applications to pass through packet filtering systems, one has to open a very large hole, significantly reducing the security protection provided by packet-filtering systems. For instance, in order to allow in standard FTP, one must let through any traffic with a destination port greater than 1,023 (1,023 - 65,500) and source port of 20, thus opening a significant security hole in the network.



	Packet Level Protection	Session Level Protection	Application Level Protection	File Level Protection
Examples	Packet filtering (router ACLs or stateless firewalls)	Stateful inspection firewalls	Intrusion prevention systems (IPS) and proxy firewalls	Gateway antivirus
Mechanism	Examine packet header	Examine packet header and control fields	Examine application fields	Examine files inside application traffic
Protocol and Application Coverage	N.A. packet level	Large	Medium	Small (email, web and file transfers)
Protection Provided	Client-to-server and server-to-client	Client-to-server and server-to-client	Mainly client-to-server	Mainly server-to-client
Relative Performance	High	High	Medium	Low

Figure 4.1: Comparison of various network security technologies

4.1.9 Session Level Protection

Session level protection technologies control the flow of traffic between two or more networks by tracking the state of sessions and dropping packets that are not part of a session allowed by a predefined security policy. Firewalls that implement session-level protection keep state information for each network session and make allow/deny decisions based on a session state table. The most common systems for session level protection are stateful inspection firewalls. Note that session level protection technologies are ”session based,” meaning that firewalls go beyond individual TCP connections to involve many such connections. Session-level firewalls support dynamic protocols by identifying port change instructions in client-server communication and comparing future sessions against these negotiated ports. For instance, to track FTP sessions, the firewall inspects the control connection, used for issuing commands and negotiating dynamic ports, and then allows in various data connections for transferring files.Because session level protection provides all the benefits of packet level protection without the limitations, it renders packet level protection unnecessary for most networks.

4.1.10 Application Level Protection

Application level protection technologies monitor network traffic and dynamically analyze it for signs of attacks and intrusions. Within the network security infrastructure, two common technologies for application level protection are proxy firewalls and Intrusion Prevention Systems (IPS).

Proxy firewalls are network systems that act on behalf of the client accessing a network service and shield the client and the server from direct peer-to-peer connection. The client establishes a connection with the proxy server, and the proxy server establishes a connection with the destination server. The proxy then forwards the data between the parties. IPS are network devices that can accept or deny traffic based on IP addresses, protocol/service, and application level analysis and verification. IPS receive traffic from the network, reassemble the traffic streams and look at application primitives and commands to detect suspicious fields that warrant some predefined action. These actions vary from logging suspicious events to dropping the connection completely.

Proxy firewalls and IPS examine control and data fields within the application flow to verify that the actions are allowed by the security policy and do not represent a threat to end systems. By understanding application-level commands and primitives, they can identify content out of the norm and content that represents a known attack or exploit. Proxy firewalls and IPS perform IP de-fragmentation and TCP stream reassembly as well as eliminating ambiguity within traffic, which can be used by malicious users trying to conceal their actions. Proxy firewalls usually support the common Internet applications, including HTTP, FTP, telnet, rlogin, email and news. Yet, a new proxy must be developed for each new application or protocol to pass through the firewall, and custom software and user procedures are required for each application.

IPS generally support a wider range of protocols and applications, including those required to protect the network against attacks from the Internet. New applications can be allowed through an IPS without requiring changes to the user workstations. In this way, IPS are more transparent to the network than proxy firewalls.
Proxy firewalls and IPS can detect certain viruses or Trojans by looking at application service fields. For instance, IPS can look at the subject field, attachment name, or attachment type within email traffic to detect characteristics of known viruses. However, application level protection does not do a detailed analysis at the file level, which is also required to detect the large number of viruses in existence.

4.1.11 File Level Protection

File level protection provides the ability to extract files within traffic and inspect them to detect malware, including viruses, worms or Trojans3. A common technology for file level protection in a network is gateway antivirus.An antivirus system looks for virus signatures - a unique string of bytes that identifies a virus - and zaps the virus from the file. Most antivirus scanning systems catch not only the initial virus but also many of its variants, since the signature code usually remains intact.[6]

Chapter 5

Wi-Fi Security

5.1 Introduction

Wireless networking technology is becoming increasingly popular but at the same time has introduced many security issues. The popularity in wireless technology is driven by two primary factors - convenience and cost. A Wireless local area network (WLAN) allows workers to access digital resources without being locked into their desks. Laptops could be carried into meetings or even into Starbucks cafe tapping into the wireless network. This convenience has become affordable.

Wireless LAN standards are defined by the IEEE's 802.11 working group. WLANs come in following flavors:

- **802.11b**

  Operates in the 2.4000 GHz to 2.2835GHz frequency range and data rate supported is up to 11 megabits per second.

- **802.11a**

  Operates in the 5.15-5.35GHz to 5.725-5.825GHz frequency range and data rate supported is up to 54 mega bits per second.

- **802.11g**

  Operates in the 2.4GHz frequency range (increased bandwidth range) and data rate supported is up to 54 megabits per second.

- 802.11i

  Improves WEP encryption by implementing wifi protected access 2(WPA2).Data Encryption with advanced encryption standard.

- 802.11n

  600 Mbps speed by Implementing MIMO & channel bonding/40 Mhz operation to the physical layer & frame aggregation to MAC layer.Improves security using WPA & WPA2.

  When setting up a WLAN, the channel and service set identifier (SSID) must be configured in addition to traditional network settings such as IP address and a subnet mask.

- The channel is a number between 1 and 11 (1 and 13 in Europe) and designates the frequency on which the network will operate.

- The SSID is an alphanumeric string that differentiates networks operating on the same channel.

- It is essentially a configurable name that identifies an individual network. These settings are important factors when identifying WLANs and sniffing traffic.

5.1.1 SSIDs

The SSID is a unique identifier that wireless networking devices use to establish and maintain wireless connectivity. SSID acts as a single shared password between access points and clients. Security concerns arise when the default values are not changed, as these units can be easily compromised. A non-secure access mode, allows clients to connect to the access point using the configured SSID, a blank SSID, or an SSID configured as ”any.” **Attacker’s Point of view:** If the target access point responds to a Broadcast SSID Probe, then he might just be in luck. This is because most wireless card drivers are configured with an SSID of ANY so that they will be able to associate with the wireless network. When the SSID is set to ANY, the driver sends a probe request to the broadcast address with a zero-length SSID, causing most access point that will respond to these requests to issue a response with its SSID and info. Though this configuration makes it easier for the user, as the user does not have to remember the SSID to connect to the wireless LAN, it makes it much simpler for attackers to gather SSIDs. Some of the common default passwords:

3Com AirConnect 2.4 GHz DS (newer 11mbit, Harris/Intersil Prism based)
Default SSID: ’comcomcom’
3Com other Acccess Points
Default SSID: ’3com’
Cisco Aironet 900Mhz/2.4GHz BR1000/e, BR5200/e and BR4800
Default SSID: ’tsunami’; ’2’
Console Port: No Default Password
Telnet password: No Default Password
HTTP management: On by default, No Default Password
Apple Airport
Default SSID: ’AirPort Network’; ’AirPort Netzwerk’
BayStack 650/660 802.11 DS AP
Default SSID: ’Default SSID’
Default admin pass: none
Default Channel: 1
MAC addr: 00:20:d8:XX:XX:XX
Compaq WL-100/200/300/400
Default SSID: ’Compaq’

5.2 WEP(Wired Equivalent Privacy)

WEP is a component of the IEEE 802.11 WLAN standards. Its primary purpose is to provide for confidentiality of data on wireless networks at a level equivalent to that of wired LANs.Wired LANs typically employ physical controls to prevent unauthorized users from connecting to the network and viewing data. In a wireless LAN, the network can be accessed without physically connecting to the LAN. IEEE chose to employ encryption at the data link layer to prevent unauthorized eavesdropping on a network. This is accomplished by encrypting data with the RC4 encryption algorithm.

5.2.1 How WEP works

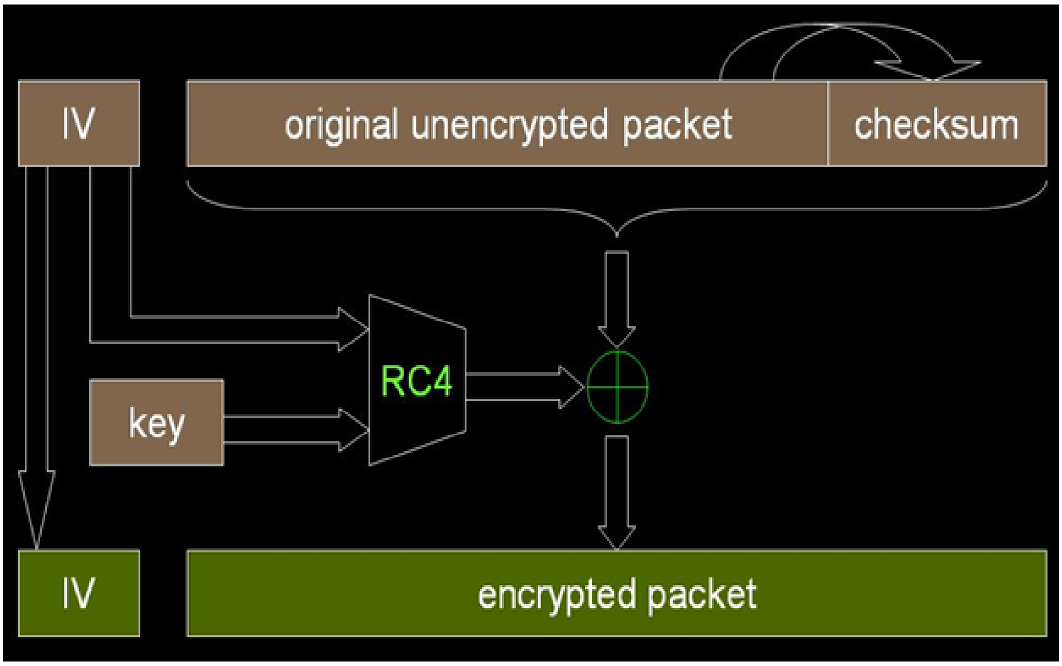


Figure 5.1: Working of WEP

WEP uses the RC4 [9]algorithm to encrypt the packets of information as they are sent out from the access point or wireless network card. As soon as the access point receives the packets sent by the user's network card it decrypts them.

Each byte of data will be encrypted using a different packet key. This ensures that if a hacker does manage to crack this packet key the only information that is leaked is that which is contained in that packet.

The actual encryption logic in RC4 is very simple. The plain text is XOR-ed with an infinitely long keystream. The security of RC4 comes from the secrecy of the packet key that's derived from the keystream.

5.2.2 Packet key

The packet key is formed by combining a pre-shared password, a state array and an initialization vector (IV). Let's first understand each of these terms:

5.2.3 Pre-shared Password:

The same pre-shared password is used by all users for each packet that is transmitted.

5.2.4 State Array:

It's a series of numbers which are scrambled and then used by RC4 to construct the key stream.

5.2.5 Initialization Vector (IV):

The IV is a 3-byte random number generated by the computer. It's either prepended or appended to the cipher text and sent to the receiver who strips the IV off before decrypting the cipher text. The RC4 algorithm consists of 2 main parts:

5.2.6 The Key Scheduling Algorithm:

The KSA process involves creating a scrambled state array . This state array will now be used as input in the second phase, called the PRGA phase.

5.2.7 The Pseudo Random Generation Algorithm:

The state array from the KSA process is used here to generate a final key stream. Each byte of the key stream generated is then Xor'ed with the corresponding plain text byte to produce the desired cipher text.

5.2.8 Key Scheduling Algorithm

The IV is calculated using a state array and properties of the pre-shared password. This is accomplished by creating an array of values equal to the index you want to use in the algorithm. The Index for WEP by default is 256. The components required for the KSA are the values of the variables i and j, the index value, the pre-shared password and its length. The algorithm which uses these values to generate a final keystream is outlined below.

```
Initialization:
For i=0....index-1
S(i)=i
j=0
Scrambling:
For i=0 ... index-1
J = j + state[i] + K[I mod length]
Swap(state[i] , state[j])
```

A loop first runs from 0 to index-1 to initialize the state array with values from 0 to index. For eg. If index =4 the state array will be filled with values from 0 to 3. Therefore the array values will be as follows:

s[0]=0 s[1]=1 s[2]=2 s[3]=3

The value of j is set to 0. Another loop is then started. For every time through the loop, the value of j is calculated, and the array value held in state[i] is swapped for the value held in state[j] .

5.2.9 Pseudo Random Generation Algorithm (PRGA)

A pseudorandom number generator (PRNG) is an algorithm that generates a random sequence of numbers. The PRGA is responsible for creating the streaming values used to encrypt the plaintext, which is based on the state array, the output of the KSA . The methodology that the PRGA follows is outlined below.

```
Initialization:
I=0 j=0 index=4
Generation Algorithm
I=(i+1) mod index
J=(j+state[i]) mod index
Swap(state[i], state[j])
Z=state[state[i] + state[j]mod index]
```

The streaming value is created by looping through the algorithm for each byte of the packet. The variables i and j are initialized to 0. For each packet the value of j is calculated, and the array value held in state[i] is swapped for the value held in state[j] . The output z is then calculated for each packet. At the end of the process we have a PRGA stream.

The PRGA stream is then Xor'ed with the plain text to generate cipher text which is transmitted to the other party.

5.2.10 Example

Let's illustrate the above concepts in the form of an example. The plain text that is to be encrypted is TEST. The password which will be used here is 6258. The initial values of our variable are as follows:

i=0 j=0 password=6258 pass length=4 index=4

Following the algorithm we get:

Step-1

State array: State[0]=0 State[1]=1 State[2]=2 State[3]=3

Password: K[0]=6 K[1]=2 K[2]=5 K[3]=8

j = [0 + S[0] + K[0]] mod 4 = 6 mod 4 = 2

Swap(State[0] , State[2]) = Swap(0,2)

State[0]=2 State[1]=1 State[2]=0 State[3]=3

Step-2

i=1 j=2

State array: State[0]=2 State[1]=1 State[2]=0 State[3]=3

Password: K[0]=6 K[1]=2 K[2]=5 K[3]=8

j = [2 + S[1] + K[1]] mod 4 = 5 mod 4 = 1

Swap(State[1], State[2]) = Swap(1,0)

State[0]=2 State[1]=0 State[2]=1 State[3]=3

Step 3

i=2 j=1

State array: State[0]=2 State[1]=0 State[2]=1 State[3]=3

Password: K[0]=6 K[1]=2 K[2]=5 K[3]=8

j = [1 + State[2] + K[2]]mod 4 = 7 mod 4 = 3

Swap(State[2], State[3]) = Swap(1,3)

State[0]=2 State[1]=0 State[2]=3 State[3]=1

Step 4

i=3 j=3

State array: State[0]=2 State[1]=0 State[2]=3 State[3]=1

Password: K[0]=6 K[1]=2 K[2]=5 K[3]=8

j = [3 + State[3] +K[3]]mod 4 = 12 mod 4 = 0

Swap(State[3], State[0]) = Swap(1,2)

State[0]=1 State[1]=0 State[2]=3 State[3]=2

Final State Array: State[0]=1 State[1]=0 State[2]=3 State[3]=2

Once the KSA state array is ready, the PRGA procedure is initialized. The procedure is as follows:

Initially i=0 j=0

K[0]=6 K[1]=2 K[2]=5 K[3]=8

First Loop:

State[0]=1 State[1]=0 State[2]=3 State[3]=2

i=1 j=0+State[1]=0+0=0

Swap(State[1], State[0]) = Swap(0,1)

State[0]=0 State[1]=1 State[2]=3 State[3]=2

z = State[State[1] + State[0] mod 4] = State[1] = 1

z1 = 00000001

Second Loop:

State[0]=0 State[1]=1 State[2]=3 State[3]=2

i=2 j=0+State[2]=3

Swap(State[2], State[3]) = Swap(3,2)

State[0]=0 State[1]=1 State[2]=2 State[3]=3

z = State[State[2] + State[3] mod 4] = State[1] = 1

z2 = 00000001

Third Loop:

State[0]=0 State[1]=1 State[2]=2 State[3]=3

i=3 j=3+State[3]=6 mod 4 = 2

Swap(State[3],State[2]) = Swap(3,2)

State[0]=0 State[1]=1 State[2]=3 State[3]=2

z = State[State[3] + State[2]] mod 4 = State[1] = 1
z3=00000001

Fourth Loop:
State[0]=0 State[1]=1 State[2]=3 State[3]=2
i=4 j=2+State[4]=2+State[4 mod 4] = 2+State[0] = 2
Swap(State[4],State[2]) = Swap(State[0],State[2]) = Swap(0,3)
State[0]=3 State[1]=1 State[2]=0 State[3]=2
z4 = State[State[4] + State[2]] = State[State[0] +... State[2]] = State[3] = 2
z4=00000010

The outputs z1-z4 at the end of each loop must be Xor'ed with the ASCII of each character of plain text which in our case is TEST. Hence the cipher text for the plain text TEST will be as follows:
$Txorz1 = 01010100xor00000001 = 01010101 = U$
$Exorz2 = 01000101xor00000001 = 01000100 = D$
$Sxorz3 = 01010011xor00000001 = 01010010 = R$
$Txorz4 = 01010100xor00000010 = 01010110 = U$
The word TEST when encrypted with WEP is UDRU.

This article was just an introduction to WEP and the exact procedure in which encryption takes place in WEP. In the next part we'll address the question that's uppermost in your minds: "Why is WEP insecure? What risks am I exposed to if I use WEP?"

5.2.11 Deficiencies of WEP

- IV is too short, even not protected from reuse.

- The per packet key is constructed from IV,making it susceptible to weak key attacks.

- No effective detection message.
- No inbuilt provision to update key in all wireless clients connected to access point.
- No protection against message replay

5.3 WPA (Wi-Fi Protected Access) and WPA2

WPA stands for Wifi Protected Access. It is defined in IEEE 802.1X. It is basically a RC4 stream cipher with 128 bit and 48 bit IV. It uses TKIP - temporal key integrity protocol and Message integrity code (MIC) Micheal to ensure data integrity.

5.3.1 How WPA works

The Wi-Fi Alliance's WPA2 security spec is a major improvement over WEP (Wired Equivalent Privacy), the security standard in IEEE's original 802.11 . WEP was susceptible to attacks and poorly implemented by vendors, and never took off in the enterprise. WEP's weaknesses and the ease with which they've been exploited led to the 802.11i standard, which was approved and published in 2004. The Wi-Fi Alliance created WPA, a subset of the draft version 802.11i, and later, WPA2, which provided stronger security than the first version of WPA.

WPA came with support for TKIP (Temporal Key Integrity Protocol), which uses the RC4 cipher, and it can be implemented in software with just a driver or firmware update. Keys are rotated frequently, and the packet counter prevents packet replay or packet re-injection attacks. WPA provides integrity checking using MIC (Message Integrity Code), sometimes nicknamed "Michael." Although this checksum method can be attacked with brute-force methods, network traffic is halted automatically for a minute and the session keys reset if a WPA-based access point detects more than one TKIP MIC failure within 60 seconds, so the risks are minimal.

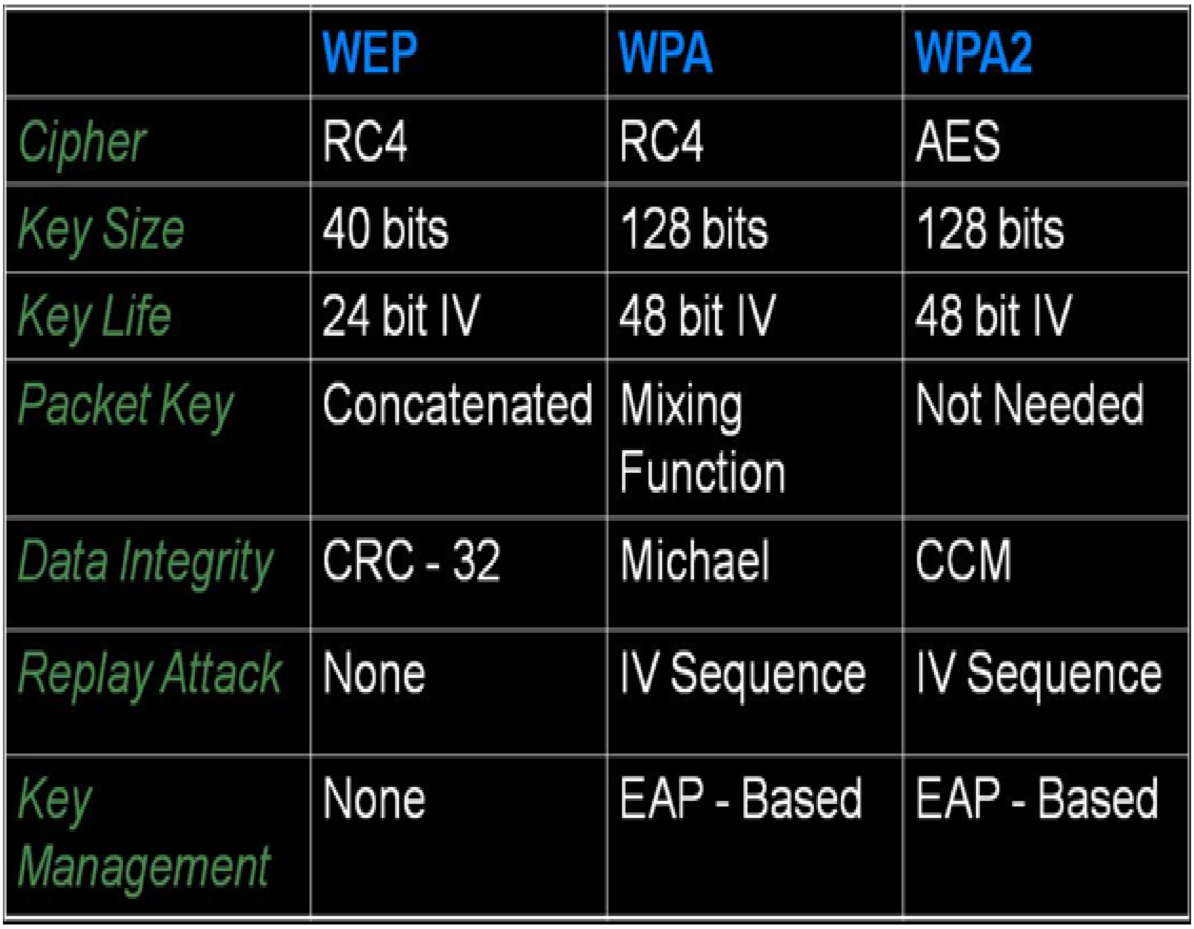
WPA2, meanwhile, uses a new encryption method called CCMP (Counter-Mode with CBC-MAC Protocol), which is based on AES (Advanced Encryption Standard), a stronger encryption algorithm than RC4.

Both WPA and WPA2 include two authentication modes: personal and enterprise. WPA2-Personal generates a 256-bit key from a plain-text pass phrase, sometimes called a PSK, or preshared key. The PSK (as well as the Service Set Identifier and SSID length) form the mathematical basis for the PMK (pairwise master key) that's used to initiate a four-way handshake and generate the PTK (pairwise transient key)–or session key–between the wireless user device and access point. WPA2-Personal, like static WEP, poses challenges in key distribution and maintenance, making it a fit for small offices but not the enterprise.

WPA2-Enterprise, meanwhile, addresses concerns regarding distributing and managing static keys, and controls access on a per-account basis by tying in to most organizations' authentication services. This mode requires credentials, such as a user name and password, a certificate or a one-time password, and authentication occurs between the station and central authentication server. The access point or wireless controller monitors the connection and directs authentication packets to the appropriate authentication server, typically a RADIUS server. The framework for this is 802.1X, which supports user and machine authentication with port-based control that works for both wired switches and wireless access points.

5.3.2 MAC Sniffing & AP Spoofing

MAC addresses are easily sniffed by an attacker since they must appear in the clear even in when WEP is enabled. An attacker can use those "advantages" in order to masquerade as a valid MAC address by programming the wireless card, and get into the wireless network and use the wireless pipes. Spoofing MAC address is very easy. Using packet-capturing software, an attacker can determine a valid MAC address using one packet. To perform a spoofing attack, an attacker must set up an access



	WEP	WPA	WPA2
Cipher	RC4	RC4	AES
Key Size	40 bits	128 bits	128 bits
Key Life	24 bit IV	48 bit IV	48 bit IV
Packet Key	Concatenated	Mixing Function	Not Needed
Data Integrity	CRC - 32	Michael	CCM
Replay Attack	None	IV Sequence	IV Sequence
Key Management	None	EAP - Based	EAP - Based

Figure 5.2: Comparison of WEP, WPA and WPA2

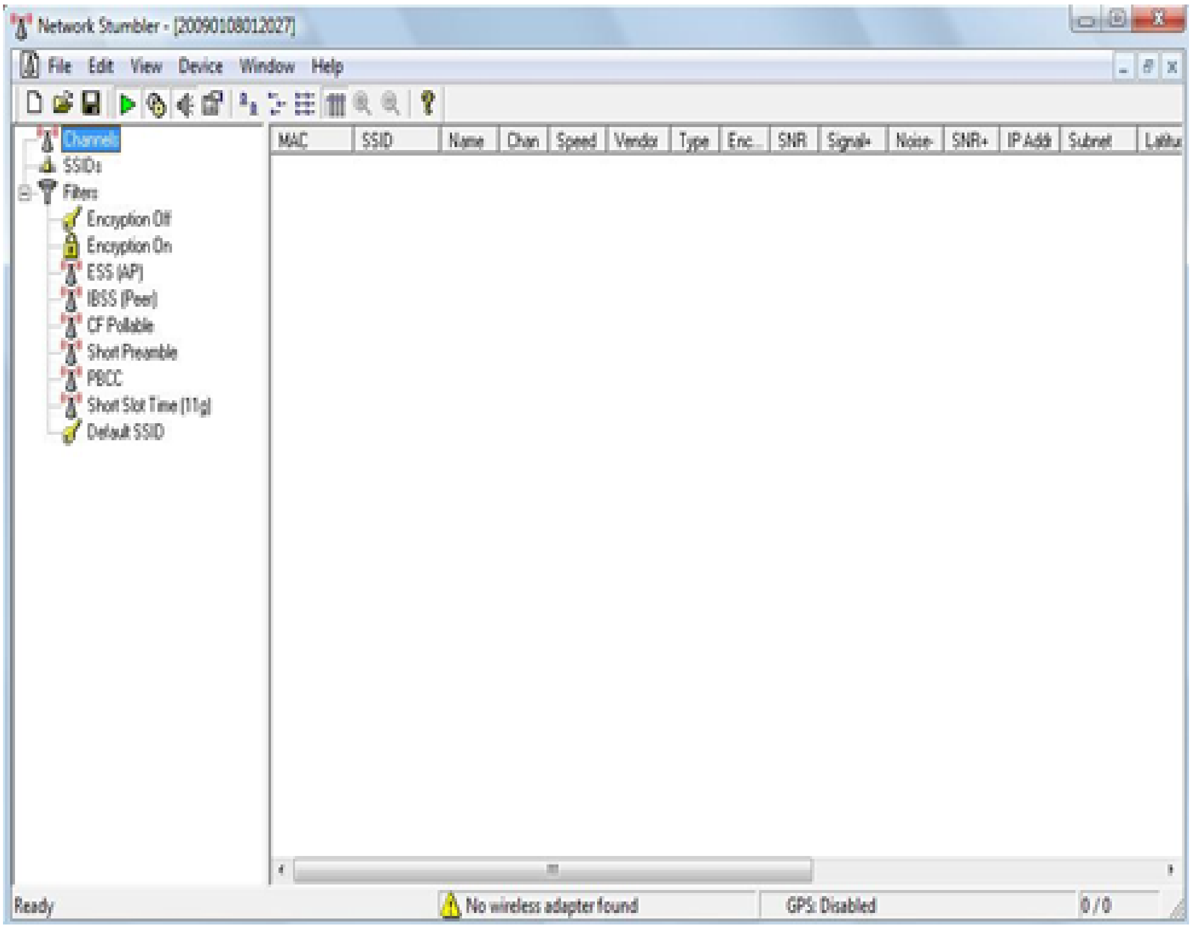
point (rogue) near the target wireless network or in a place where a victim may believe that wireless Internet is available.

5.4 Hacking Tool:

a. Netstumbler:

Netstumbler is a high level WLAN scanner. It operates by sending a steady stream of broadcast packets on all possible channels.[2]

Access Points (AP) respond to broadcast packets to verify their existence, even



Ready

No wireless adapter found

GPS: Disabled

0 / 0

Figure 5.3: Screenshort of Network Stumbler Tool

if beacons have been disabled. **NetStumbler displays:**

1. Signal Strength
2. MAC Address
3. SSID
4. Channel details

NetStumbler is a Windows-based war-driving tool that will detect wireless networks and mark their relative position with a GPS. NetStumbler uses an 802.11 Probe Request sent to the broadcast destination address, causing all access points in the area to issue 802.11 Probe Response containing network configuration information, such as their SSID and WEP status. When hooked up to a GPS, NetStumbler will record a GPS coordinate for the highest signal strength found for each access point. Using the network and GPS data, the user can create maps with tools such as Microsoft MapPoint.

NetStumbler supports the Hermes chipset cards on Windows 2000, the most popular being the Lucent (now Proxim) Orinoco branded cards. On Windows XP the NDIS 5.1 networking library has 802.11 capabilities itself, which allows NetStumbler to be used with most cards that support it. To use NetStumbler, the user inserts his wireless card and sets his SSID or network name to ANY. As discussed before, this instructs the driver to use a zero-length SSID in its Probe Requests, causing most access points to respond to Probe Requests along with their SSID or a zero-length SSID.

The probe requests are difficult to be detected as that from NetStumbler activity as NetStumbler utilizes the active scanning method described in the IEEE 802.11 specification without anomalous characteristics. Once an AP is discovered, NetStumbler will probe the AP for its information, often the same information stored in the SNMP MIB system.sysName.o parameter.

b. AiroPeek:

Airopeek is a comprehensive packet analyzer for IEEE 802.11 wireless LANs, supporting all higher level network protocols such as TCP/IP, Apple Talk, NetBUI and IPX [3]. In addition, AiroPeek quickly isolates security problems, fully decodes 802.11a and 802.11b WLAN protocols, and analyzes wireless network performance with accurate identification of signal strength, channel and data rates.

AiroPeek's customizable 3-pane view, allows the user to display a packet capture list, a single packet decode, as well as the hex view of raw data, altogether or in any combination. He can navigate through multiple selected packets to reconstruct the threads of network conversations. Multiple capture windows can be open simultaneously for easy comparison of packet views, protocol usage, or total traffic vs. traffic subsets.

AiroPeek supports Lucent and Cisco 802.11b cards and also has support for some of the newer 802.11a cards. AiroPeek NX is primarily designed for wireless network troubleshooting and analysis. AiroPeek NX supports channel scanning at a user-defined interval as well as decrypting traffic on the fly with a provided WEP key. AiroPeek NX's filtering is also configurable. AiroPeek NX also provides a useful Nodes view, which groups detected stations by their MAC address and will also show IP addresses and protocols observed for each.

AiroPeek NX has a new view called the SSID Tree, available on the Nodes Tab. The SSID Tree provides an intuitive, hierarchical view, displaying the relationship between WLAN ESSIDs, Access Points and their associated Stations. The SSID Tree also facilitates the auditing of Encryption and Authentication schemes in use.

AiroPeek can fully decode all 802.11 protocols, displaying management, control and data packets as well as all higher-level network protocols such as TCP/IP, AppleTalk, NetBEUI and IPX. AiroPeek tells you the status, length, and timestamp of a packet immediately, adding:

- The speed at which the packet was transmitted
- The channel number and radio frequency at which the packet was transmitted
- The signal strength of the transmission in which the packet was received.

c. Airsnort :

AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys [1]. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second.

AirSnort tool is a collection of the scripts and programs derived from the research conducted by Tim Newsham, the University of Maryland, and the University of California at Berkley. AirSnort is a wireless LAN (WLAN) tool which recovers encryption keys. AirSnort operates by passively monitoring transmissions, computing the encryption key when enough packets have been gathered. AirSnort requires approximately 5-10 million encrypted packets to be gathered. Once enough packets have been gathered, AirSnort can guess the encryption password in under a second. Weak IV's are collected and sorted according to which key byte they help to expose. A weak IV can assist in exposing only one key byte. When a sufficient number of weak IVs have been gathered for a particular key byte, statistical analysis will show a tendency towards a particular value for that key byte.

Each of the 256 possible values for a given key byte is scored as to their probability of being the correct value. The crack process makes a key guess based on the highest ranking values in the statistical analysis phase. The number of guesses that airsnort will make for each key byte is governed by the 'breadth' parameter in the preferences section of airsnort. This is because weak IVs are not distributed in a linear fashion across the entire IV space.

It has two modes. The monitor mode enables a wireless NIC to capture packets without associating with an access point or ad-hoc network. This is desirable when the user does not want to transmit any packets. In fact transmitting is sometimes not possible while in monitor mode (driver dependent). Another aspect of monitor mode is that the NIC does not consider whether the CRC values are correct for packets captured in monitor mode, as some packets may in fact be corrupted. Promiscuous mode allows the user to view all wireless packets on a network to which he is associated. The need to associate means that the user must have some means of authenticating himself with an access point. In promiscuous mode, packets are not seen until the user has associated. Not all wireless drivers support promiscuous mode.

Some of the other tools like Kismet, Wireshark and Backtrack OS are also used.

5.5 WEP Crack

WEP Crack is an open source tool for breaking 802.11 WEP secret keys. While Airsnort has captured the media attention, WEP Crack was the first publically available code that demonstrated the above attack.

The current tools are Perl based and are composed of the following scripts: · WeakIVGen.pl, prism-getIV.pl, WEPCrack.pl

5.6 Countermeasures for Securing Wi-Fi

The mentioned countermeasures are inrespective of operating systems Linux,Windows and MAC.The Countermeasures are tried in home and small business network where it can support up to sixteen clients.

- Don't Configured WIFI Router as Unsecured Connection, It can be misused by someone.

- Usually ISP configure your phone number/mobile number as default Network Key in Router. one should change it as soon as possible if so.

- If configured as Unsecured Connection then enable the logging system. This helps you to get MAC (Media Access Control) address of the machines which uses your wifi router.

- If Configured as Unsecured Connection then kindly install packet capturing software or WLAN analyzing software so that you can keep eye on machines which uses your wifi router.

- If configured as Unsecured Connection then bind your MAC address with the router. This will only allow your authenticated laptops to get connected to router.

- Protect Your SSIDS & Dont use WEP while isp configures ur router.

- Dont ever use viral networks like ”Free internet” Or ”wifi” Network because those networks are designed to steal your data from laptop.

- Maintain All types of Logs for atleast 6 months.First of all enable promiscuous mode(it is a configuration of a network card that makes the card pass all traffic it receives to the central processing unit rather than just frames address to it- a feature normally used for packet sniffing.) in the router.Create a virtual server from the control panel on the router where the logs will be stored.

Chapter 6

Secure file transfer model in LAN

The following are the main points which are covered in this model

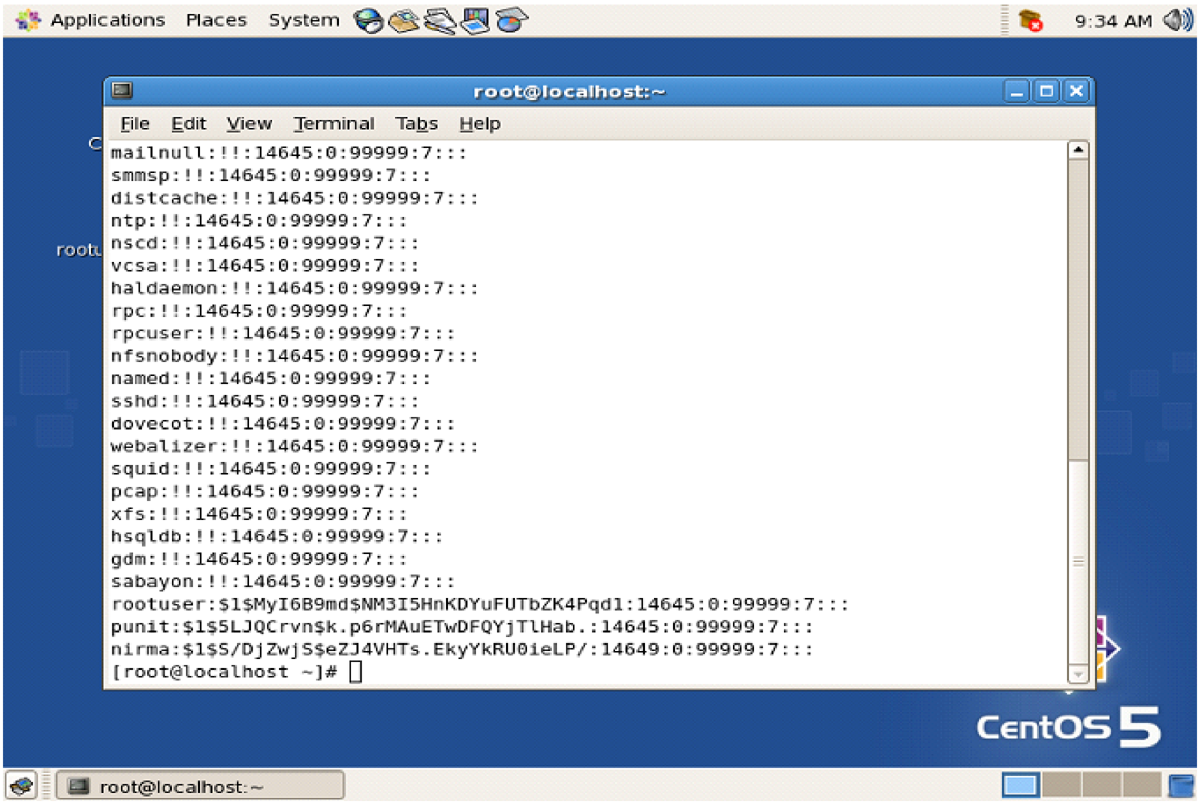
- Maintain log file
- Create privilege group
- Use LINUX server for more security
- Can be accessible by non linux users also (windows and MAC)

6.1 Introduction to the LINUX

LINUX is a multi user open source server operating system which is used for desktop and server. Some of the popular flavors of LINUX desktop are Ubuntu and Fedora , while the flavors used for the servers are CENTOS and Redhat.
LINUX is more secure due to some of the following reasons

- User can login to the shell if he knows username and password
- Password is encrypted with DES (data encryption standard) which accepts 64 bit input key and produces 104 bit hash value
- Three types of permissions to the file are Read , write and execute

- The figure shows how password is encrypted by MD5 (message digest 5 algorithm)



```
mailnull:!!:14645:0:99999:7:::
smmsp:!!:14645:0:99999:7:::
distcache:!!:14645:0:99999:7:::
ntp:!!:14645:0:99999:7:::
nscd:!!:14645:0:99999:7:::
vcsa:!!:14645:0:99999:7:::
haldaemon:!!:14645:0:99999:7:::
rpc:!!:14645:0:99999:7:::
rpcuser:!!:14645:0:99999:7:::
nfsnobody:!!:14645:0:99999:7:::
named:!!:14645:0:99999:7:::
sshd:!!:14645:0:99999:7:::
dovecot:!!:14645:0:99999:7:::
webalizer:!!:14645:0:99999:7:::
squid:!!:14645:0:99999:7:::
pcap:!!:14645:0:99999:7:::
xfs:!!:14645:0:99999:7:::
hsqldb:!!:14645:0:99999:7:::
gdm:!!:14645:0:99999:7:::
sabayon:!!:14645:0:99999:7:::
rootuser:$1$MyI6B9md$NM3I5HnKDYuFUTbZK4Pqd1:14645:0:99999:7:::
punit:$1$5LJQCrvn$k.p6rMAuETwDFQYjTlHab.:14645:0:99999:7:::
nirma:$1$S/DjZwjS$eZJ4VHTs.EkyYkRU0ieLP/:14649:0:99999:7:::
[root@localhost ~]# 
```

Figure 6.1: How password is encrypted with MD5

6.1.1 Secure file transfer model in Linux

For the project I have installed the VSFTPD (Very secure File Transfer Protocol Daemon) package which can be installed using the following command (yum install vsftpd) in the fedora terminal.

- The File Transfer Protocol's purpose is the platform independent data transfer of the internet, it is based on a server/client architecture.

- RFC 959 determins FTP to be split in two different channels, one serves for the data (TCP-port 20) and the other for the control (TCP-port 21).

- Over the control channel the two sides (server and client) exchange commands for the initiation of the data transfer

A FTP connection involves four steps:

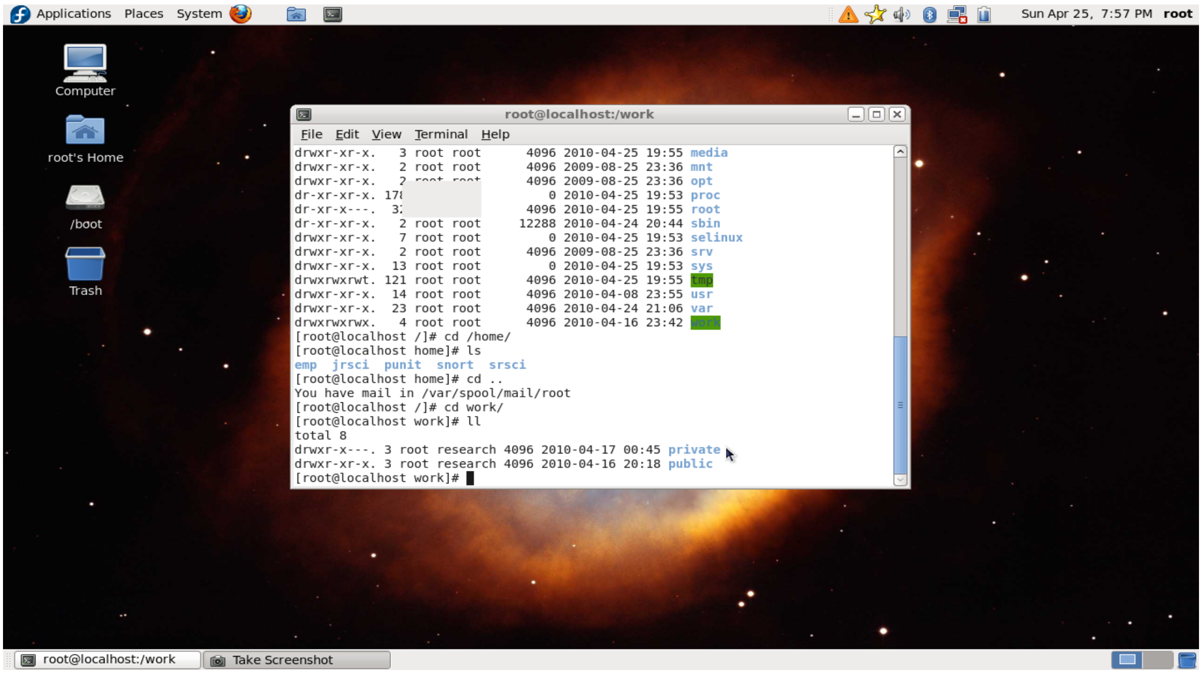
- User authentication
- Establishing the control channel
- Establishing the data channel
- Discontinuing the connection

One example is the fact that vsftpd is operated in chroot mode, which means a program (in this case vsftpd) is assigned a new root directory , it can no longer access programs or files outside of that directory - it is so to speak 'locked up'.

Should a FTP-server be compromised the potential attacker will be isolated from the rest of the system and extensive damage will be prevented. The following are the steps to create a ACL (access control list) based system:- Example is as below:-
Main folder is in /work,
There are two subfolders in work folder which are public and private public folder is used to publicly access three users jrsci,srsci,emp. Access rights of users are as below:- srsci → access, delete, modify
jrsci → acesss, modify but not delete
emp → access, but not delete or modify only readonly

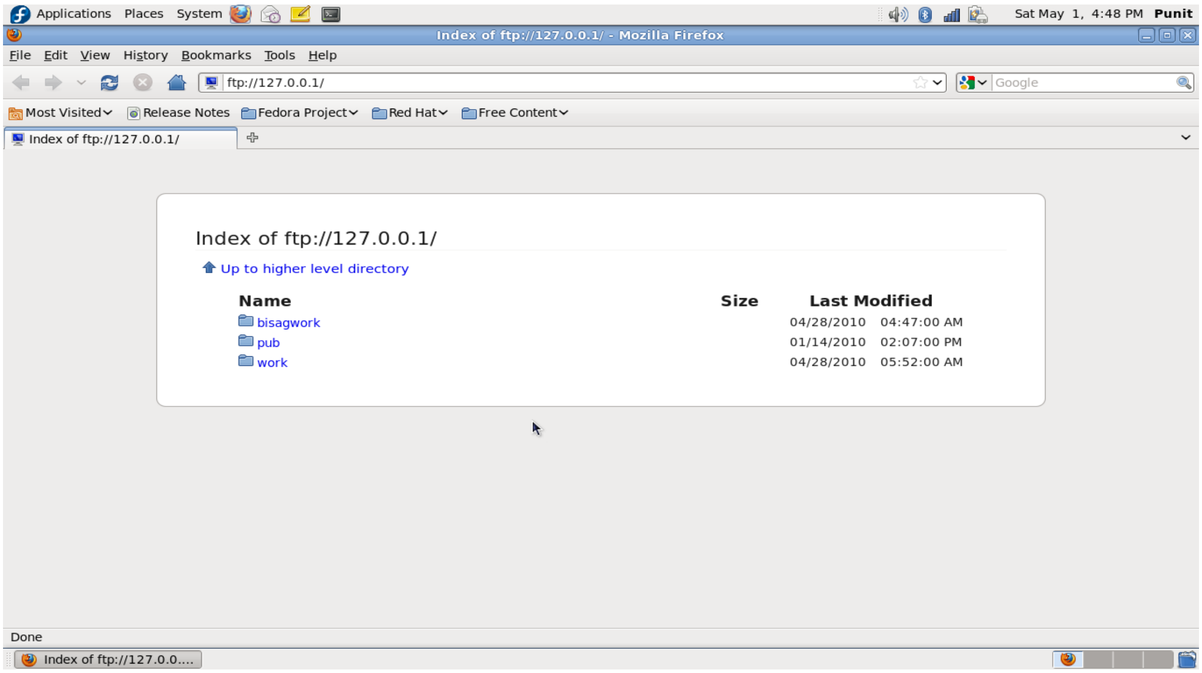
private folder is used only for private purpose for srsci, jrsci but not emp

srsci → full rights
jrsci → only readonly
emp → prohibited



```
drwxr-xr-x.   3 root root      4096 2010-04-25 19:55 media
drwxr-xr-x.   2 root root      4096 2009-08-25 23:36 mnt
drwxr-xr-x.   2                4096 2009-08-25 23:36 opt
dr-xr-xr-x. 17                    0 2010-04-25 19:53 proc
dr-xr-x---.  3                 4096 2010-04-25 19:55 root
dr-xr-xr-x.   2 root root     12288 2010-04-24 20:44 sbin
drwxr-xr-x.   7 root root         0 2010-04-25 19:53 selinux
drwxr-xr-x.   2 root root      4096 2009-08-25 23:36 srv
drwxr-xr-x.  13 root root         0 2010-04-25 19:53 sys
drwxrwxrwt. 121 root root      4096 2010-04-25 19:55 tmp
drwxr-xr-x.  14 root root      4096 2010-04-08 23:55 usr
drwxr-xr-x.  23 root root      4096 2010-04-24 21:06 var
drwxrwxrwx.   4 root root      4096 2010-04-16 23:42 work
[root@localhost /]# cd /home/
[root@localhost home]# ls
emp  jrsci  punit  snort  srsci
[root@localhost home]# cd ..
You have mail in /var/spool/mail/root
[root@localhost /]# cd work/
[root@localhost work]# ll
total 8
drwxr-x---. 3 root research 4096 2010-04-17 00:45 private
drwxr-xr-x. 3 root research 4096 2010-04-16 20:18 public
[root@localhost work]# █
```

Figure 6.2: Allocation of permission to the folder



Index of ftp://127.0.0.1/

Up to higher level directory

Name	Size	Last Modified
bisagwork		04/28/2010 04:47:00 AM
pub		01/14/2010 02:07:00 PM
work		04/28/2010 05:52:00 AM

Figure 6.3: Two folders in the work dictionary

Actual representation in the system

```
# cd /
# mkdir work
# chmod 777 work
# cd work
# mkdir public
# mkdir private
# chmod 755 public
# chmod 750 private
```

For the windows compatibility Sambha package is installed and configured in the LAN

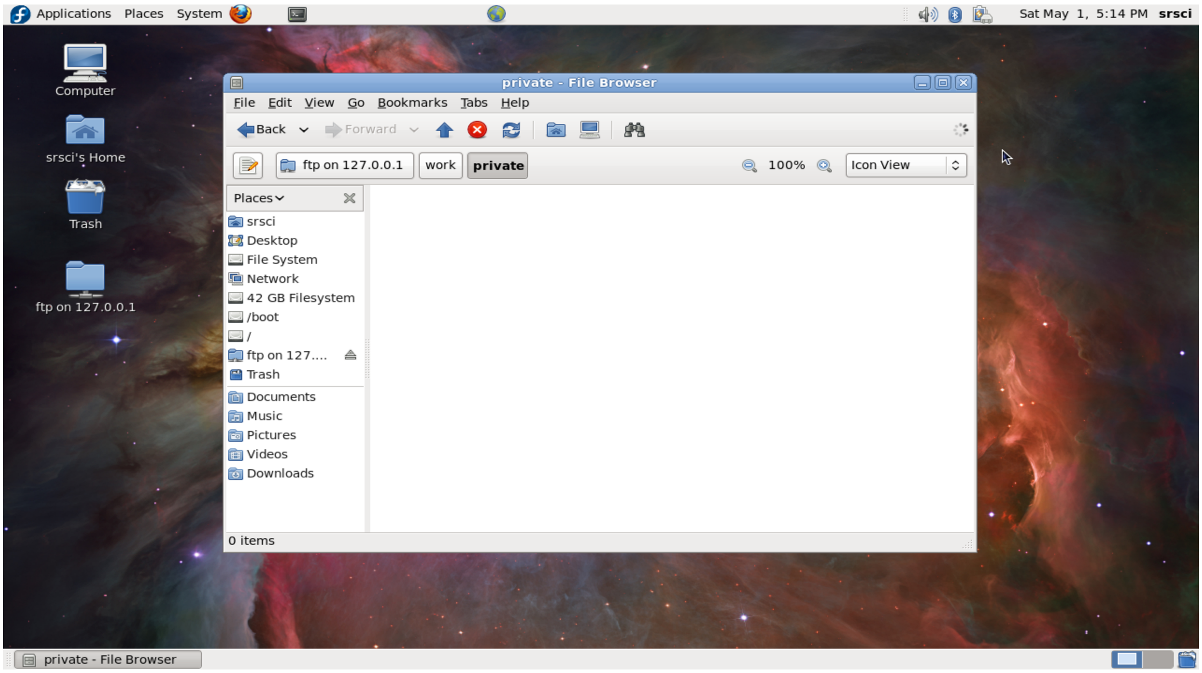


Figure 6.4: Shows srsci can access the private folder

Chapter 7

Intrusion Detection & Prevention System

7.1 Introduction to IDPS

- IDPS is security system that detects and prevents malicious activity from computers or networks.[5]

- Intrusion- Unauthorized access to computer system or network is treated as Intrusion activity

- Intruder- The victim who performed intrusion activity is called intruder

- Project IDPS basically provides the web interface to network administrator to provide security for network managed by Linux server from any unwanted malicious attacks which is actually intrusion.

- IDPS also provide the easily manageable site for managing network from anywhere in the world. IDPS works on Linux server but it can be access from any client machine

- snort_inline is open source tools which help to log packets into database.

- It helps to analysis real time network traffic and it helps to gather information from networks

7.2 Facilities provided in the system are as follows:-

- Existing system has the facility of authentication
- System provides the facility that define the group of alerts.
- Alerts can be move from one group to another group.
- System provides facility to create users as admin and sub-admin and also assign them different rights.
- System provides facility for admin for applying rule by selecting the category of rules. Admin can edit the rule by selecting the category of rules.
- System provides the facility to install IDPS on just clicking one button.
- Admin can edit the rule by selecting the category of rules.
- System provides the facility to install IDPS on just clicking one button.
- Admin don't require editing configuration file.
- System works on any platform.
- Easily configuration of IDPS.
- Any person other than admin can't do sql injection system has dynamic design and dynamic paging.
- Systems can exports alerts on local client side

7.3 Snort

Snort is a free and open source network intrusion prevention system (NIPS) and network intrusion detection system (NIDS) capable of performing packet logging and real-time traffic analysis on IP network.

It receives packets sent from Netfilter (iptables) firewall with the help of the libipq library, compares them with snort signature rules and tags them as drop if they match a rule, then finally sends them back to Netfilter (iptables) where the snort inline tagged packets are dropped[7].

Snort inline is basically a modified version of Snort that accepts packets from iptables and IPFW (IPFIREWALL) via libipq(linux) or divert sockets(FreeBSD), instead of libpcap. It then uses new rule types (drop, sdrop, reject) to tell iptables/IPFW whether the packet should be dropped, rejected, modified, or allowed to pass based on a snort rule set.

An IDS (Intrusion Detection System) logs an alert when a packet matches a signature rule but does not discard or even modify it. This is different with an IPS (Intrusion Prevention System) where a packet matching a signature rule is blocked or modified. The backend used is MYSQL and the frontend used is PHP.

7.4 Installation procedure and package requirements for the installation and working of snort in Linux

The lists of the packages needed are as follows:-[8]

- httpd php php-mysql
- iptables
- iptables-ipv6
- iptables-devel
- perl-DBI
- perl-DBD-MySQL
- mysql
- mysql-libs
- mysql-devel
- mysql-server pcre
- pcre-devel libdnet
- libdnet-devel
- libpcap
- libpcap-devel
- php-pear
- php-pear-Image-Color

- php-pear-Image-Canvas
- php-pear-Image-Graph
- libnet (*http : //www.packetfactory.net/libnet/dist/deprecated/libnet*−1.0.2*a.tar.gz*)
- snort_inline (*http : //snort_inline.sourceforge.net/download.html.*)

7.4.1 The steps to install snort are as follows :-

First of all open the terminal window ,type su - to login as the root user. Follow the mentioned steps:-

- # go to the file location using the cd command.
- # mkdir /etc/snort_inline
- # mkdir /etc/snort_inline/rules
- # mkdir /var/log/snort_inline
- # tar -xzf snort_inline-2.6.1.5.tar.gz
- # cd snort_inline-2.6.1.5
- # ./configure –with-mysql –enable_inline
- # make
- # make install
- # cp etc/* /etc/snort_inline/
- # vim /etc/snort_inline/snort_inline.conf
- Change RULE-PATH variable to var RULE-PATH /etc/snort_inline/rules
- After the line with ”output alert-fast: snort_inline-fast”, add following line...

- Output database: log, mysql, user=snort password=snort dbname=snort host=localhost
- # cp etc/classification.config /etc/snort_inline/rules
- # cp etc/reference.config /etc/snort_inline/rules
- # useradd snort; echo ”snort” — passwd –stdin snort;
- # chkconfig mysqld on
- # chkconfig httpd on
- # /etc/init.d/mysqld start
- # /etc/init.d/httpd start

7.4.2 Database Setting using MySQL (My Structured Query Language)

Following are the steps for database settings in MySQL[11]:-

- mysql -u root -p
- mysql> create database snort;
- mysql> set password for root@localhost=password('root password');
- mysql> grant insert,select on root.* to snort@localhost;
- mysql> set password for snort@locahost=password('snort user password');
- mysql> grant create,insert,update,select,delete on snort.* to snort@localhost;
- mysql> grant create,insert,update,select,delete on snort.* to snort;
- mysql> exit
- # mysql -u root -p < schemas/create-mysql snort

7.4.3 Steps to Block URL signatures

The steps to block a particular social networking website like www.orkut.com is shown below:-

- # vim /etc/snort_inline/rules/local.rules
- # write down the following rules.
- drop tcp \ HOME-NET any \ EXTERNAL-NET \ HTTP-PORTS (msg:"ORKUTBLOCKING";content:"www.orkut.com";reference:url,www.orkut.com; classtype:web-application-activity; sid:17740000; rev:4;)
- # vim /etc/snort_inline/snort_inline.conf
- # insert the following line
- #include $RULE-PATH/local rules

7.4.4 NetFilter's Description

NetFilter is a linux kernel module available since the kernel version 2.4. It provides three main functionalities.

- Packet filtering - Accepts or Drops packets.
- NAT - Changes the source or destination IP address of network packets.
- Packet Managing - Modifies packets (like for Quality of Service)

Iptables is a tool needed to configure Netfilter; it must be launched as root. Netfilter queues packets to snort_inline in the userspace with the help of the ip-queue kernel module and libipq. Then, if a packet matches a snort-inline attack signatue, it is tagged by libipq and comes back to NetFilter where it is dropped.
A packet is dropped if it matches an attack signature. Three options are available in this mode.

- Drop - Drops a packet, sends a reset back to the host, logs the events.
- Sdrop - Drops a packet, without sending a reset back to the host.
- Ignore - Drops a packet, sends a reset back to the host, does not log the event
- A packet is modified if it matches an attack signature.

7.4.5 Script configuration of the snort

```
# modprobe ip-queue
# lsmod | grep ip-queue
# iptables -A INPUT -s 127.0.0.1 -d 127.0.0.1 -i lo -j ACCEPT
# iptables -A OUTPUT -s 127.0.0.1 -d 127.0.0.1 -o lo -j ACCEPT
# iptables -A INPUT -j QUEUE
# iptables -A OUTPUT -j QUEUE
# iptables -A FORWARD -j QUEUE
# snort-inline -Q -v -c /etc/snort-inline/snort-inline.conf -l /var/log/snort-inline
```

7.4.6 Script configuration to check the log file

```
# tail -f /var/log/snort-inline/snort-inline-fast
# tail -f /var/log/snort-inline/snort-inline-full
```

7.4.7 BASE (Basic Analysis and Security Engine

The following steps are needed to install and configure BASE engine which is used to provide a graphical interface of the snort.[10] Download BASE engine (Basic Analysis and Security Engine) from the following web link

(http://sourceforge.net/project/showfiles.php?group-id=10338)

Install BASE using the following steps:- # cd /var/www/html

# tar -xzf base-1.4.0.tar.gz

# mv base-1.4 base

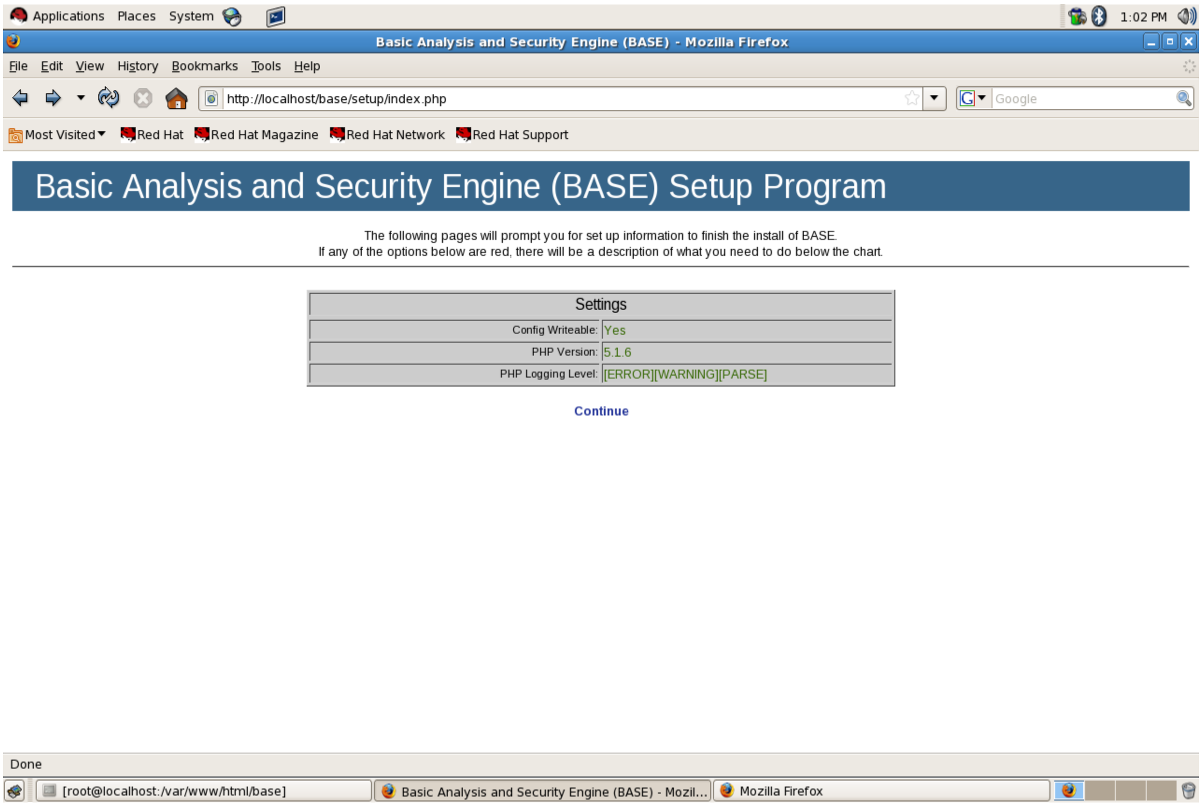
Download adodb from (http://easynews.dl.sourceforge.net/sourceforge/adodb/adodb480.tgz)

# tar -xzf adodb480.tgz

# mv adodb /var/www/html/base

After the above procedure I have followed the following steps

step 1:open browser and run: http://localhost/base


Applications Places System
1:02 PM
Basic Analysis and Security Engine (BASE) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/base/setup/index.php
Google
Most Visited
Red Hat
Red Hat Magazine
Red Hat Network
Red Hat Support
Done
[root@localhost:/var/www/html/base]
Basic Analysis and Security Engine (BASE) - Mozil...
Mozilla Firefox

Basic Analysis and Security Engine (BASE) Setup Program

The following pages will prompt you for set up information to finish the install of BASE.
If any of the options below are red, there will be a description of what you need to do below the chart.

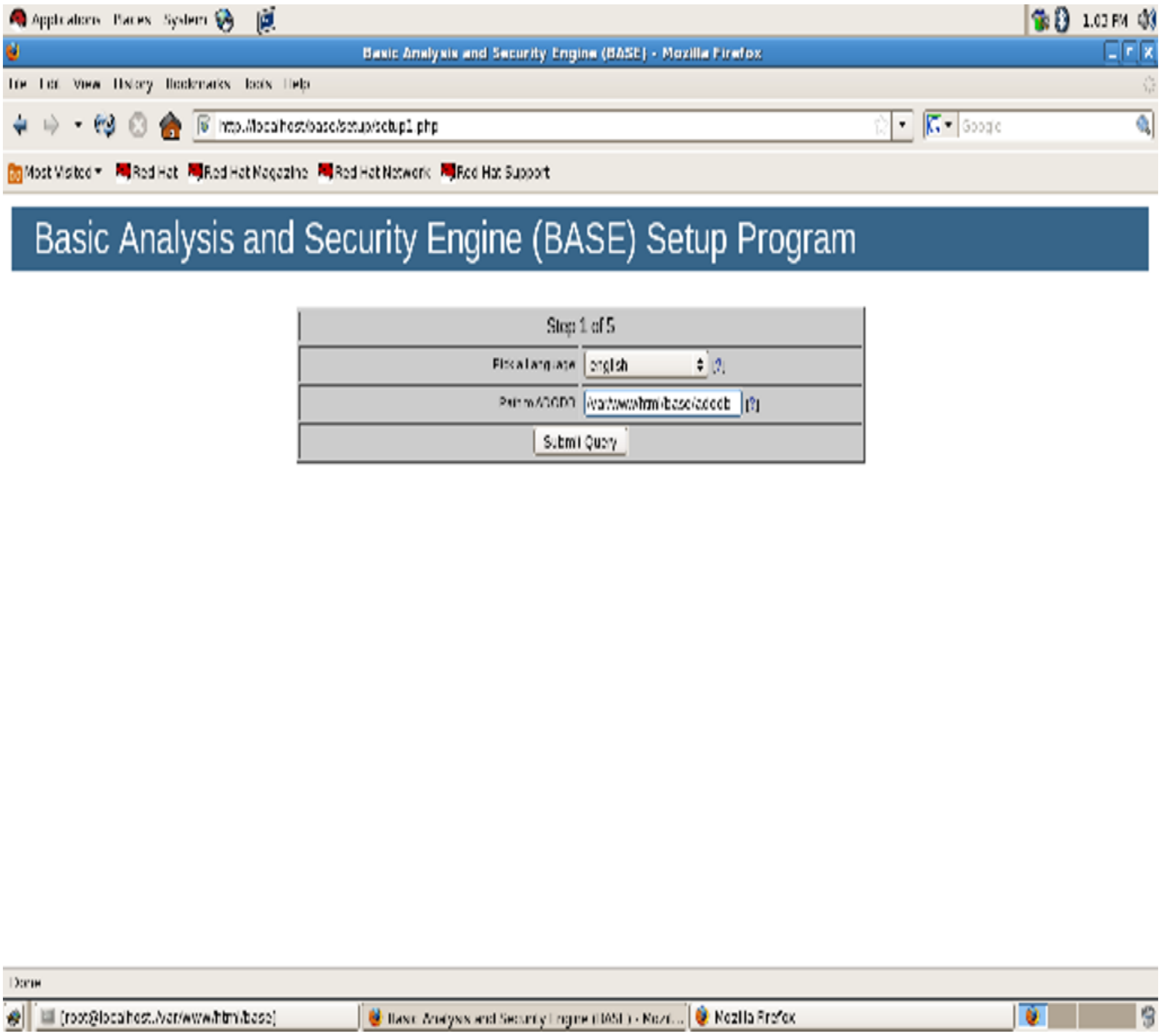
Settings	
Config Writeable:	Yes
PHP Version:	5.1.6
PHP Logging Level:	[ERROR][WARNING][PARSE]

Continue

Figure 7.1: Configuration of the BASE engine

Step 2: Language and path to adodb. In our case it is /var/www/html/base/adodb

In the Figure 7.2 it is shown that one has to select the language and give the path to the adodb. After giving the path one has to click on the submit query button .


Applications Places System
1:03 PM
Basic Analysis and Security Engine (BASE) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/base/setup/setup1.php
Google
Most Visited Red Hat Red Hat Magazine Red Hat Network Red Hat Support
Done
[root@localhost:/var/www/html/base]
Basic Analysis and Security Engine (BASE) - Mozi...
Mozilla Firefox

Basic Analysis and Security Engine (BASE) Setup Program

Step 1 of 5

Pick a Language: english [?]

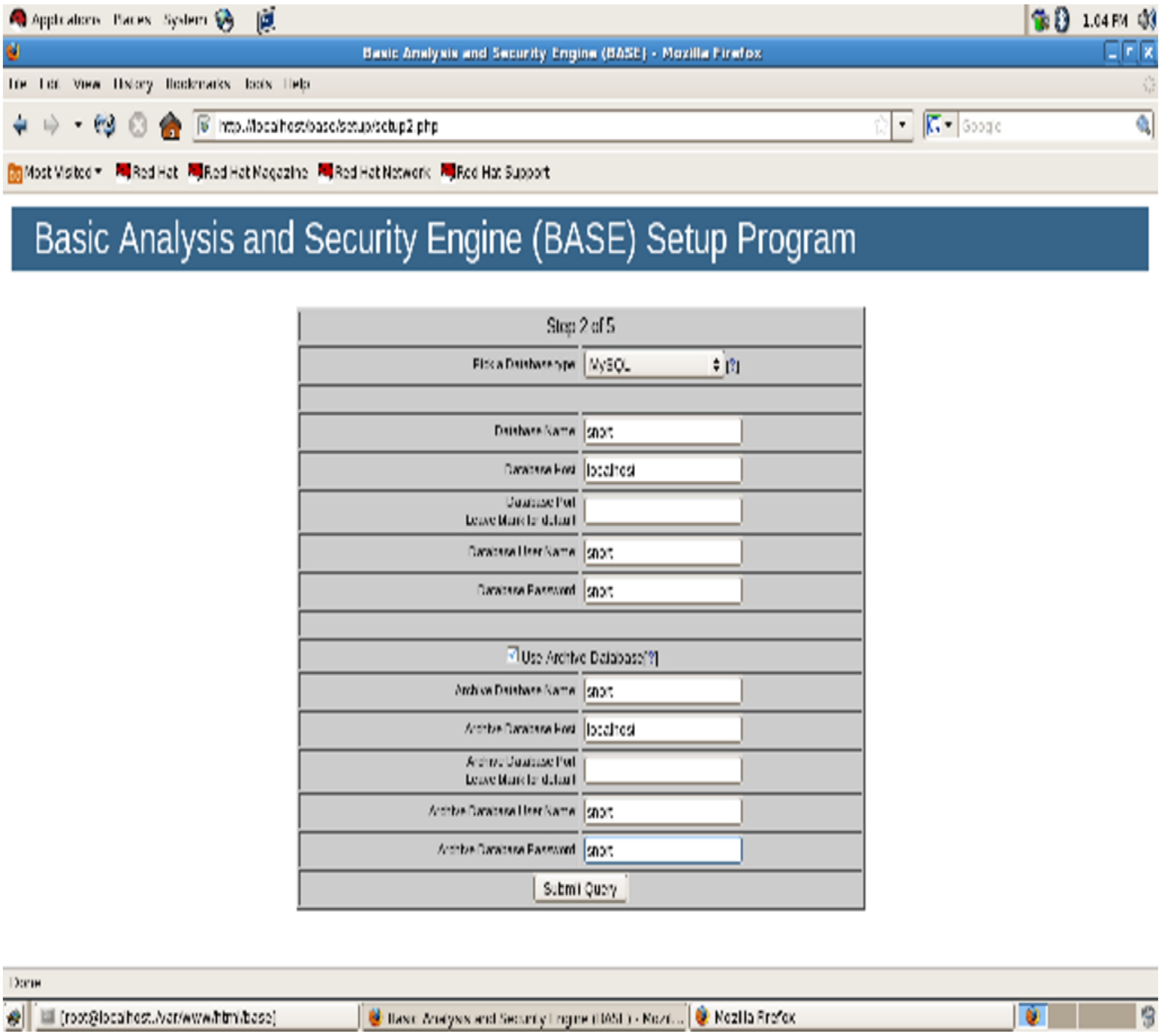
Path to ADODB: /var/www/html/base/adodb [?]

Submit Query

Figure 7.2: Configuration of the path

Step 3: MySQL Settings

In the Figure 7.3 it is shown the steps to configure the settings for the MySOL.



Applications Places System
1:04 PM
Basic Analysis and Security Engine (BASE) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/base/setup/setup2.php
Google
Most Visited
Red Hat
Red Hat Magazine
Red Hat Network
Red Hat Support
Done
[root@localhost:/var/www/html/base]
Basic Analysis and Security Engine (BASE) - Mozi...
Mozilla Firefox

Basic Analysis and Security Engine (BASE) Setup Program

Step 2 of 5

Pick a Database type	MySQL [?]
Database Name	snort
Database Host	localhost
Database Port Leave blank for default	
Database User Name	snort
Database Password	snort

☑ Use Archive Database[?]

Archive Database Name	snort
Archive Database Host	localhost
Archive Database Port Leave blank for default	
Archive Database User Name	snort
Archive Database Password	snort

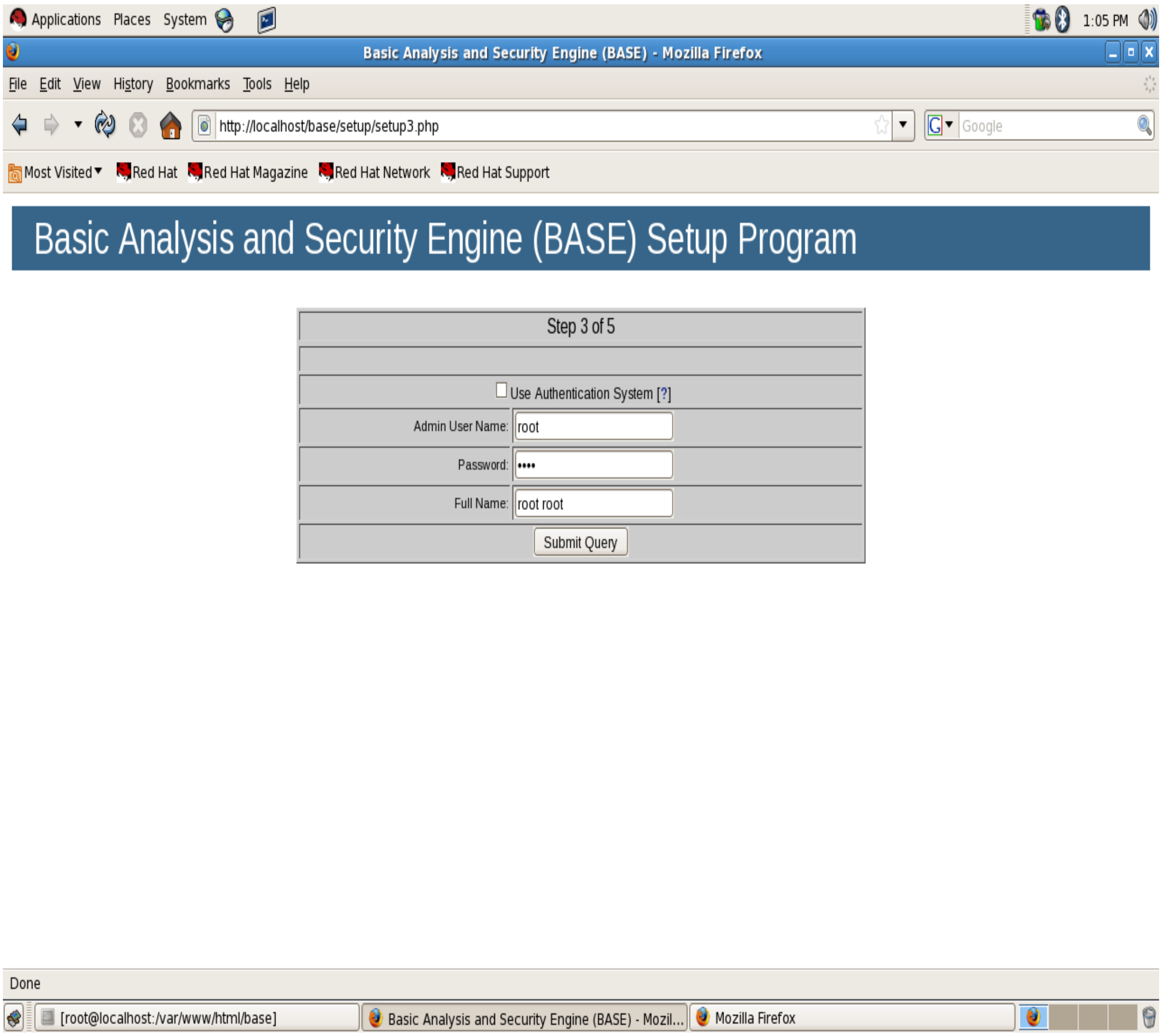
Submit Query

Figure 7.3: Settings for MySQL

Here one has to select the domain MySQL, give the database name as snort and give the database host name as localhost. Click on the use archive database and fill it in the same manner as mentioned above.

Step 4:Base Authentication System

In the Figure 7.4 it is shown that one has to assign a admin name, give a strong password and assign a full name. Here the admin name is root and the full name is root root.


Applications Places System
1:05 PM
Basic Analysis and Security Engine (BASE) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/base/setup/setup3.php
Google
Most Visited
Red Hat
Red Hat Magazine
Red Hat Network
Red Hat Support
Done
[root@localhost:/var/www/html/base]
Basic Analysis and Security Engine (BASE) - Mozil...
Mozilla Firefox

Basic Analysis and Security Engine (BASE) Setup Program

Step 3 of 5

□ Use Authentication System [?]

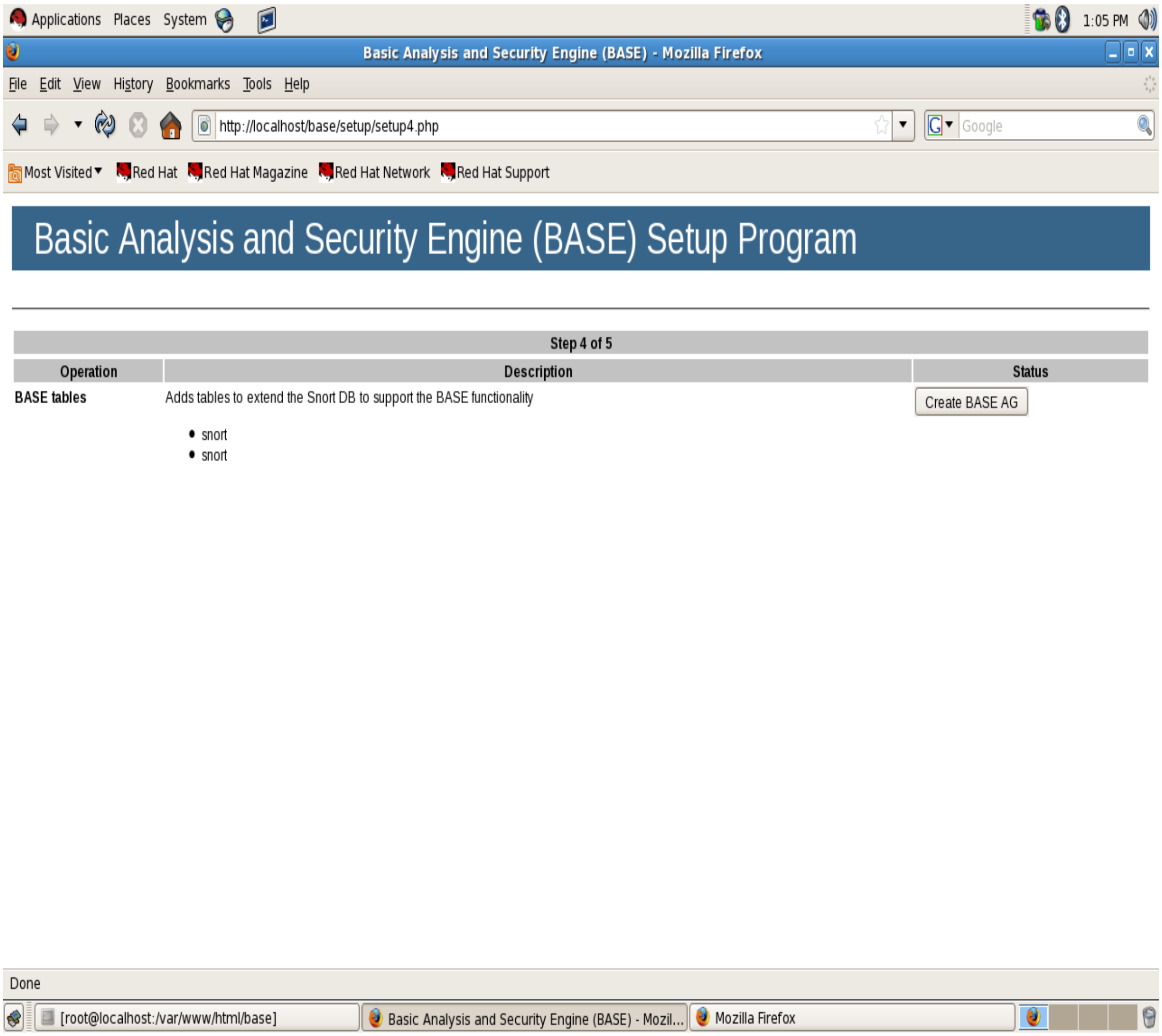
Admin User Name:	root
Password:	••••
Full Name:	root root

Submit Query

Figure 7.4: Authentication to the root

Step 5: Create the MySQL database and tables (click on create Base AG)

The Figure 7.5 shows the procedure to create MySQL database and tables. Simply click on the create BASE AG and proceed to the next step.


Applications Places System
1:05 PM
Basic Analysis and Security Engine (BASE) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/base/setup/setup4.php
Google
Most Visited
Red Hat
Red Hat Magazine
Red Hat Network
Red Hat Support
Done
[root@localhost:/var/www/html/base]
Basic Analysis and Security Engine (BASE) - Mozil...
Mozilla Firefox

Basic Analysis and Security Engine (BASE) Setup Program

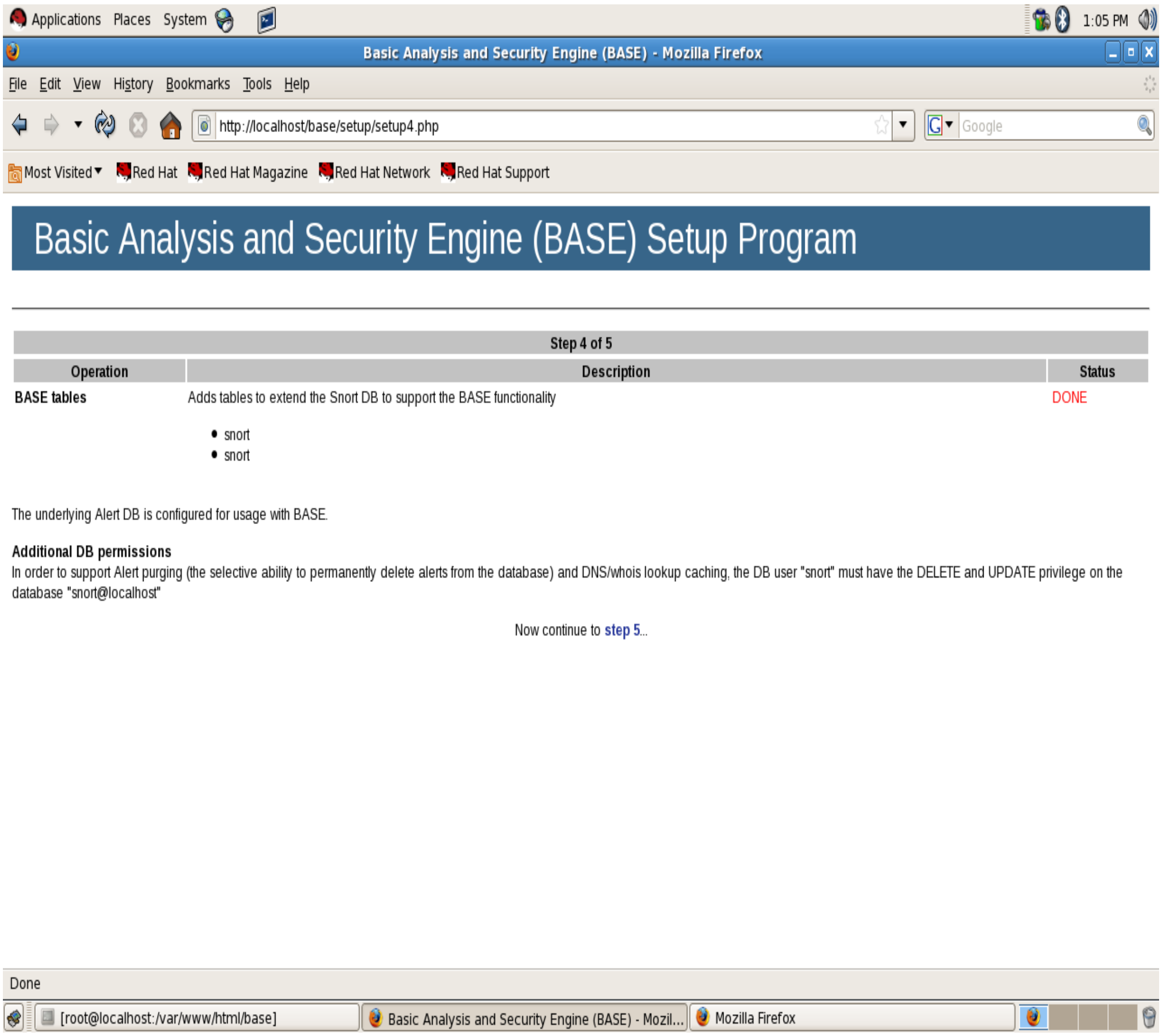
Step 4 of 5

Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality • snort • snort	Create BASE AG

Figure 7.5: Adding the MySQL database in BASE

Step 6: Add tables to extend snort DB to support BASE functionality

The Figure 7.6 shows the procedure to add the tables to extend snort DB to support the BASE functionality. One has to select the mentioned package and click done.


Applications Places System
1:05 PM
Basic Analysis and Security Engine (BASE) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/base/setup/setup4.php
Google
Most Visited
Red Hat
Red Hat Magazine
Red Hat Network
Red Hat Support
Done
[root@localhost:/var/www/html/base]
Basic Analysis and Security Engine (BASE) - Mozil...
Mozilla Firefox

Basic Analysis and Security Engine (BASE) Setup Program

Step 4 of 5

Operation	Description	Status
BASE tables	Adds tables to extend the Snort DB to support the BASE functionality • snort • snort	DONE

The underlying Alert DB is configured for usage with BASE.

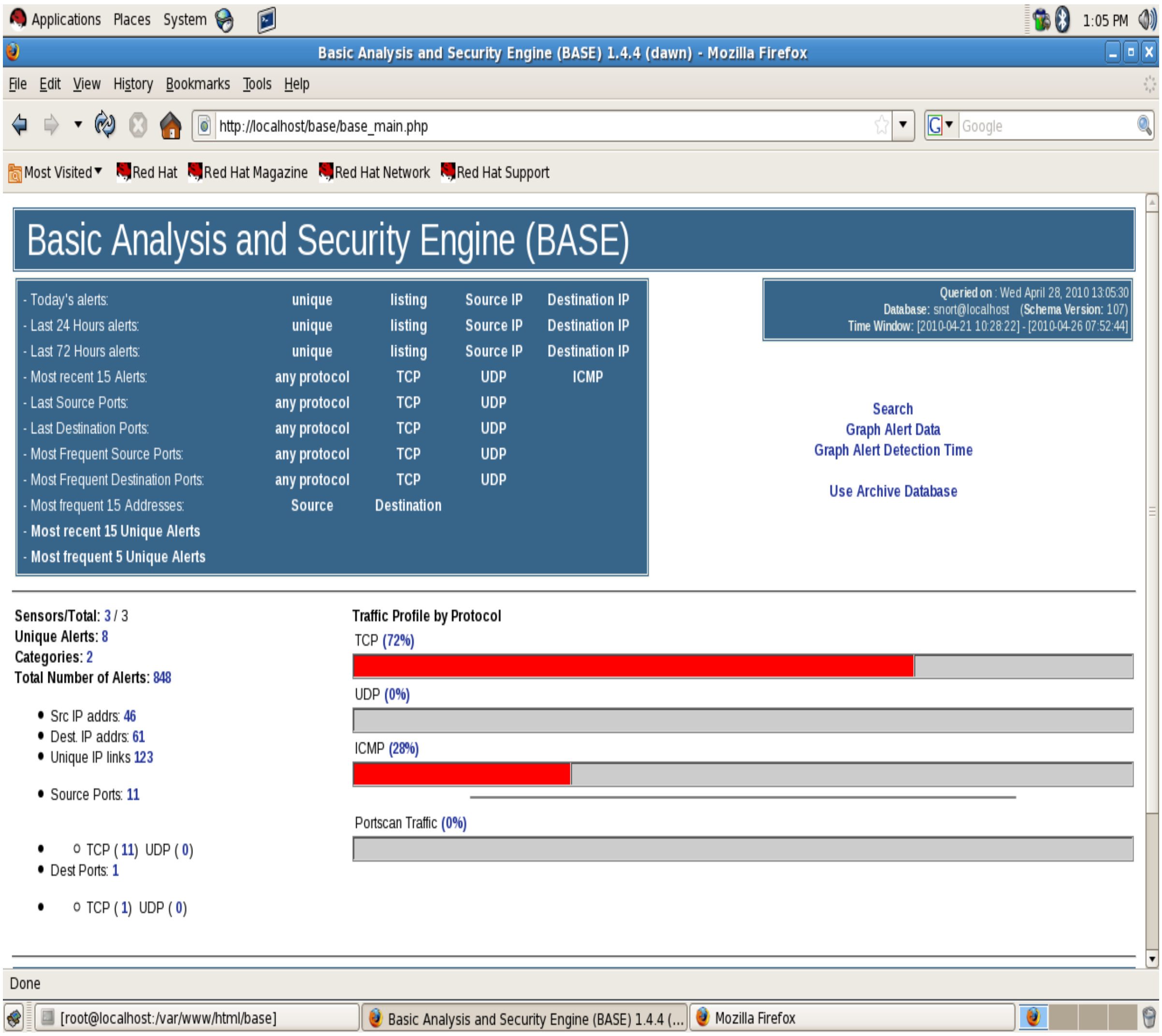
Additional DB permissions
In order to support Alert purging (the selective ability to permanently delete alerts from the database) and DNS/whois lookup caching, the DB user "snort" must have the DELETE and UPDATE privilege on the database "snort@localhost"

Now continue to step 5...

Figure 7.6: Adding other tables to extent BASE Functionality

Step 7:Final figure of the BASE engine configuration

The Figure 7.7 shows the working of the BASE system. It shows the unique alerts ,


Applications Places System
1:05 PM
Basic Analysis and Security Engine (BASE) 1.4.4 (dawn) - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/base/base_main.php
Google
Most Visited
Red Hat
Red Hat Magazine
Red Hat Network
Red Hat Support
Done
[root@localhost:/var/www/html/base]
Basic Analysis and Security Engine (BASE) 1.4.4 (...
Mozilla Firefox

Basic Analysis and Security Engine (BASE)

- Today's alerts:	unique	listing	Source IP	Destination IP
- Last 24 Hours alerts:	unique	listing	Source IP	Destination IP
- Last 72 Hours alerts:	unique	listing	Source IP	Destination IP
- Most recent 15 Alerts:	any protocol	TCP	UDP	ICMP
- Last Source Ports:	any protocol	TCP	UDP	
- Last Destination Ports:	any protocol	TCP	UDP	
- Most Frequent Source Ports:	any protocol	TCP	UDP	
- Most Frequent Destination Ports:	any protocol	TCP	UDP	
- Most frequent 15 Addresses:	Source	Destination		
- Most recent 15 Unique Alerts				
- Most frequent 5 Unique Alerts				

Queried on : Wed April 28, 2010 13:05:30
Database: snort@localhost (Schema Version: 107)
Time Window: [2010-04-21 10:28:22] - [2010-04-26 07:52:44]

Search
Graph Alert Data
Graph Alert Detection Time

Use Archive Database

Sensors/Total: 3 / 3
Unique Alerts: 8
Categories: 2
Total Number of Alerts: 848

- Src IP addrs: 46
- Dest. IP addrs: 61
- Unique IP links 123
- Source Ports: 11
- ○ TCP (11) UDP (0)
- Dest Ports: 1
- ○ TCP (1) UDP (0)

Traffic Profile by Protocol

TCP (72%)

UDP (0%)

ICMP (28%)

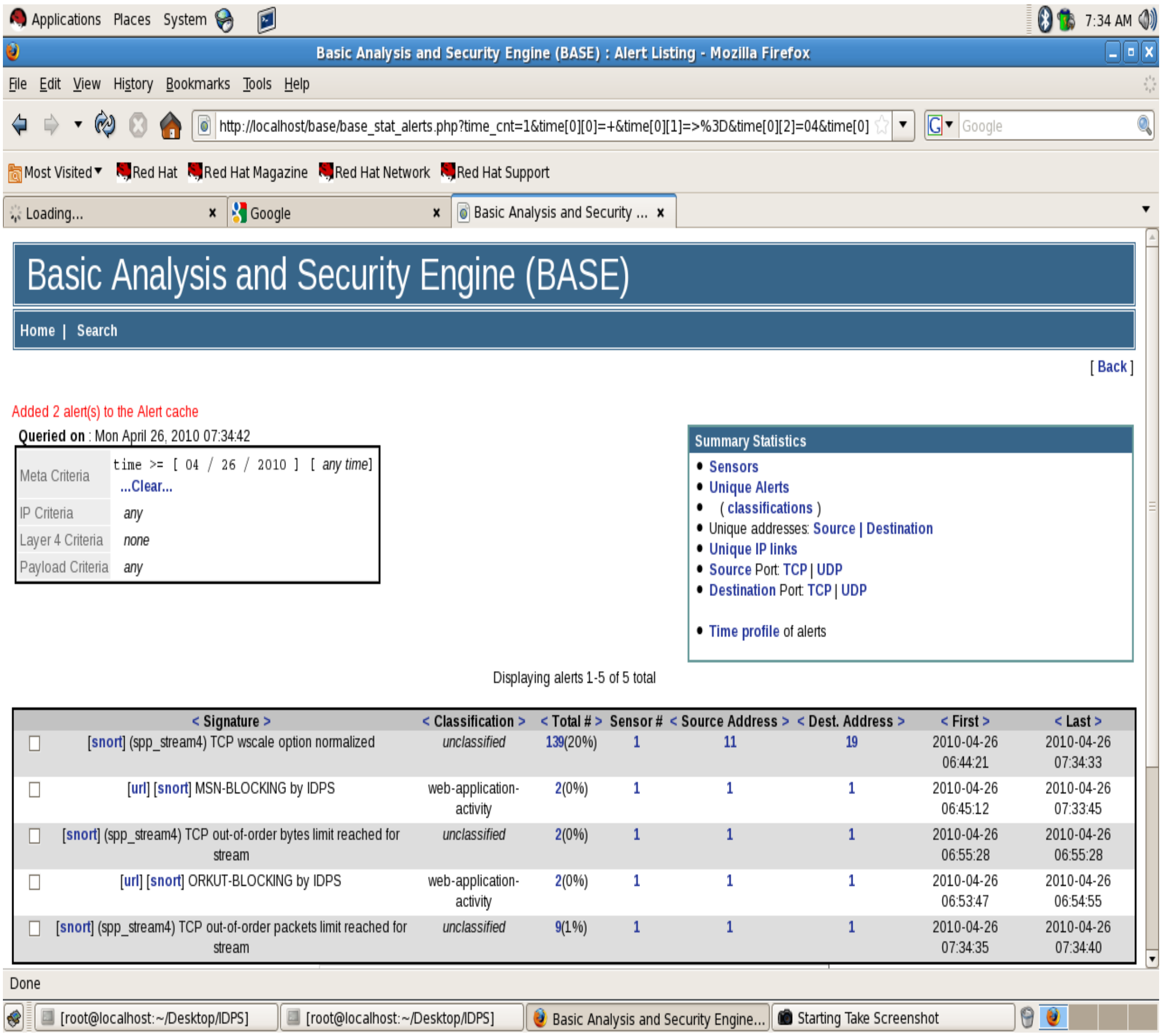
Portscan Traffic (0%)

Figure 7.7: Working of BASE

the TCP traffic the UDP traffic and the portscan traffic.

Step 8:Figure shows the working of the BASE engine

The Figure 7.8 shows the working of the BASE engine which shows the list of the website which has been blocked, the unique alerts with the source and destination IP address.


Applications Places System
7:34 AM
Basic Analysis and Security Engine (BASE) : Alert Listing - Mozilla Firefox
File Edit View History Bookmarks Tools Help
http://localhost/base/base_stat_alerts.php?time_cnt=1&time[0][0]=+&time[0][1]=>%3D&time[0][2]=04&time[0]
Google
Most Visited
Red Hat
Red Hat Magazine
Red Hat Network
Red Hat Support
Loading...
Google
Basic Analysis and Security ...
Done
[root@localhost:~/Desktop/IDPS]
[root@localhost:~/Desktop/IDPS]
Basic Analysis and Security Engine...
Starting Take Screenshot

Basic Analysis and Security Engine (BASE)

Home | Search

[Back]

Added 2 alert(s) to the Alert cache

Queried on : Mon April 26, 2010 07:34:42

Meta Criteria	time >= [04 / 26 / 2010] [*any time*] ...Clear...
IP Criteria	*any*
Layer 4 Criteria	*none*
Payload Criteria	*any*

Summary Statistics

- Sensors
- Unique Alerts
- (classifications)
- Unique addresses: Source | Destination
- Unique IP links
- Source Port: TCP | UDP
- Destination Port: TCP | UDP
- Time profile of alerts

Displaying alerts 1-5 of 5 total

	< Signature >	< Classification >	< Total # >	Sensor #	< Source Address >	< Dest. Address >	< First >	< Last >
□	[snort] (spp_stream4) TCP wscale option normalized	*unclassified*	139(20%)	1	11	19	2010-04-26 06:44:21	2010-04-26 07:34:33
□	[url] [snort] MSN-BLOCKING by IDPS	web-application-activity	2(0%)	1	1	1	2010-04-26 06:45:12	2010-04-26 07:33:45
□	[snort] (spp_stream4) TCP out-of-order bytes limit reached for stream	*unclassified*	2(0%)	1	1	1	2010-04-26 06:55:28	2010-04-26 06:55:28
□	[url] [snort] ORKUT-BLOCKING by IDPS	web-application-activity	2(0%)	1	1	1	2010-04-26 06:53:47	2010-04-26 06:54:55
□	[snort] (spp_stream4) TCP out-of-order packets limit reached for stream	*unclassified*	9(1%)	1	1	1	2010-04-26 07:34:35	2010-04-26 07:34:40

Figure 7.8: Working of BASE engine and testing

Chapter 8

Conclusion,Contribution and future Scope

8.1 Conclusion

The Snort has been installed and is working properly. The secure file transfer model allows only the srsci group to read , write and execute files whereas the jrsci group is allowed only to read the file from the server and the rest users are not allowed to read the files. The loopholes in the Wi-Fi are explained with the countermeasures to protect it . Study in the various field of network security has also been done.

8.2 Contribution

In the first part I have successfully studied the various technologies for network security, found the vulnerability in the network with the help of the available tools as explained, worked on the wireless security and described countermeasures to protect it. Whereas in the second part I have created a secure file transfer model in the Linux environment, also created an Intrusion Detection and Prevention system by installing and configuring the snort and giving graphical interface with the help of the BASE engine.

8.3 Future Scope

Wi-Fi and LAN security can be enhanced my adding some of the modules in the operating system used so that the data, which is a very important asset of the organization can be kept safe. Various loopholes can be searched and solutions to them have to be implemented. Moreover the interface and security measures have to be made simple in installation and use so that a new person can also easily use it and the forensic can be made easily.

Appendix A

List of Abbreviations

ARP/RARP	Address Resolution Protocol/Reverse Address
DCAP	Data Link Switching Client Access Proto
DHCP	Dynamic Host Configuration Protocol
DVMRP	Distance Vector Multicast Routing Protocol
ICMP/ICMPv6	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol version 4
IPv6	Internet Protocol version 6
MARS	Multicast Address Resolution Server
PIM	Protocol Independent Multicast-Sparse Mode (PIM-SM)
RIP2	Routing Information Protocol
RIPng for IPv6	Routing Information Protocol for IPv6
RSVP	Resource ReSerVation setup Protocol
VRRP	Virtual Router Redundancy Protocol
Mobile IP	Mobile IP Protocol
RUDP	Reliable UDP
TALI	Transport Adapter Layer Interface
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
XOT	X.25 over TCP
BGMP	Border Gateway Multicast Protocol
DIS	Distributed Interactive Simulation
DNS	Domain Name Service

ISAKMP/IKE	Internet Security Association and Key Management Protocol and Internet Key Exchange
iSCSI	Small Computer Systems Interface
LDAP	Lightweight Directory Access Protocol
MZAP	Multicast-Scope Zone Announcement Protocol
NetBIOS/IP	NetBIOS/IP for TCP/IP Environment
COPS	Common Open Policy Service
FANP	Flow Attribute Notification Protocol
Finger	User Information Protocol
FTP	File Transfer Protocol
HTTP	Hypertext Transfer Protocol
IMAP4	Internet Message Access Protocol rev 4
IMPPpre/IMPPmes	Instant Messaging and Presence Protocols
IPDC	IP Device Control
IRC	Internet Relay Chat Protocol
ISAKMP	Internet Message Access Protocol version 4rev1
NTP	Network Time Protocol
POP3	Post Office Protocol version 3
Radius	Remote Authentication Dial In User Service
RLOGIN	Remote Login
RTSP	Real-time Streaming Protocol
SCTP	Stream Control Transmision Protocol
S-HTTP	Secure Hypertext Transfer Protocol
SLP	Service Location Protocol
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SOCKS	Socket Secure (Server)
TACACS+	Terminal Access Controller Access Control System
TELNET	TCP/IP Terminal Emulation Protocol
TFTP	Trivial File Transfer Protocol
WCCP	Web Cache Coordination Protocol
BGP-4	Border Gateway Protocol
EGP	Exterior Gateway Protocol
EIGRP	Enhanced Interior Gateway Routing Protocol
HSRP	Cisco Hot Standby Router Protocol
IGRP	Interior Gateway Routing
NARP	NBMA Address Resolution Protocol
NHRP	Next Hop Resolution Protocol
OSPF	Open Shortest Path First
TRIP	Telephony Routing over IP
ATMP	Ascend Tunnel Management Protocol

References

[1] http://airsnort.shmoo.com.

[2] http://www.netstumbler.org.

[3] http://www.wildpackets.com.

[4] Network protocol analyzer,wwww.wireshark.com.

[5] *Network Technology using IDS.*

[6] www.kaspersky.com,www.jupiterworks.com.

[7] www.snort.org.

[8] www.sourceforge.org.

[9] Jun-Dian Lee and Chih-Peng Fan. Efficient low-latency rc4 architecture designs for ieee 802.11i wep/tkip. 2007.

[10] Tom Negrino. *JavaScript and Ajax for the Web.*

[11] Stephen Walther. *Introduction to PHP.* Prentice Hall, 2005.