Comparison Analysis of Wireless Network Audits using Open Source tools

A Thesis submitted to the Department of Electronics and Electrical Engineering, BRAC University in partial fulfillment of the requirements for Bachelor of Science degree in Electronics and Communication Engineering

Nuzhat Nuary Islam

Fahmida Zareen

1st Sept,2014

Announcement

We do hereby announce that the thesis titled "Comparison Analysis of Wireless Network Audits using Open Source tools" submitted to the Department of Electrical and Electronics Engineering of BRAC University in partial fulfillment of the Bachelor of Science in Electronics and Communication Engineering. This work is our original work and was not submitted elsewhere for the award of any other degree or any other publication.

Date :

Supervisor

Sadia Hamid Kazi

Name :Nuzhat Nuary Islam

Student Id :10110019

Name :Fahmida Zareen

Student Id: 09210017

Acknowledgment

We are deeply obliged to our supervisor Ms. Sadia Hamid Kazi, Assistant Professor, BRAC University for her help, guidance, motivation, suggestion and encouragement throughout the course of this work. Moreover, we would like to thank Saidur Rahman for helping us to installation process of ubuntu , kismet and ettercap and Banking sectors monitoring pattern of Wi-Fi zone. Additionally , we would like to thank Naimul Aftab to help us to know about practical monitoring system of Wi-Fi zone of a RMG sector. Further, We would like to thank BRACU IT team to let us know their monitoring pattern of Wi-Fi zone. We are very grateful to have such a co-operation from all those people we have mentioned earlier.

Furthermore, we would like to thank our parents and our friends for supporting us.

Abstract

Wi-Fi, also spelled Wifi or WiFi, is a popular technology that allows an electronic device to exchange data or connect to the internet wirelessly using radio waves. WiFi has a lot of advantages, they are easy to set up and inexpensive. They're also unobtrusive. At the same time, a well-designed and secure installation of a WiFi network is not a trivial task. Many companies therefore need professional help to audit their WiFi deployments or pilots, and ensure that their use of this new technology is not done at the expense of security and performance. Many tools exist to enable security professionals to do Wi-Fi networks surveys, ranging from "Free" Open source tools, to sophisticated commercial products. Nowadays most of our industries are using wireless networks for communications, and security is a big issue here. But it has been seen that most of the industries do not monitor or audit their network, as the trend is that open source tools are not for professional purpose. And the professional and commercial audit tools are expensive for some of the industries in our country. But there are some of the open source tools for detecting, monitoring and penetrating which are very efficient, for example Wi-Fi networks are Kismet, NetStumbler ,Wireshark , WiFiFoFum , Aircrack and many more. The intention of this thesis is to do a comparison analysis of the top most open source audit tools and map them according to different industries of our country. The comparison analysis was done by practically installing the tools and using the tools to audit networks at different sites and then mapping the features to the requirements of the most popular sectors of industries of our country.

Table of Contents

Chapter- 1

Chapter 2

Chapter - 3

Chapter- 4

Chapter -5

Chapter-1

1. Introduction

1.1 Wi-Fi:

Wireless networking, frequently identified as Wi-Fi - is a technique of receiving broadband internet without wires. Wi-Fi allows us to connect a number of computers to the same broadband internet at a time. People have a laptop or any wifi supported gadget can be used within the coverage zone of wifi network. Extra phone lines or cables is not required if Wi-Fi is installed.[1]

1.2 How Wi-Fi works:

A wireless network uses radio waves, just like cell phones, televisions and radios do. In fact, communication transversely a wireless network is a lot like two-way radio communication. This is how it goes:

- ✓ Data translated by a computer's wireless adapter turn into a radio signal and transmitted through an antenna.
- ✓ A wireless router receives the signal and decodes it. The router sends the information to the Internet using a physical, wired Ethernet connection.

The process also works in overturn, with the router receiving information from the Internet, translating it into a radio signal and sending it to the computer's wireless adapter.

The radios used for Wi-Fi communication are very comparable to the radios used for walkie-talkies, cell phones and other devices. They can transmit and receive radio waves, and they can convert 1s and 0s into radio waves and convert the radio waves back into 1s and 0s. But Wi-Fi radios have a few distinguished differences from other radios:

- ➢ They broadcast at frequencies of 2.4 GHz or 5 GHz. This frequency is significantly higher than the frequencies used for cell phones, walkie-talkies and televisions. The higher frequency allows the signal to transmit more data.
- ➢ They utilize 802.11 networking standards, which come in more than a few flavors:
- ➢ **802.11a** transmits at 5 GHz and can move up to 54 megabits of data per second. It also uses **orthogonal frequency-division multiplexing** (OFDM), a more well-organized coding method that splits that radio signal into a number of sub-signals before they get in touch with a receiver. This significantly decreases interference.
- ➢ **802.11b** is the slowest and slightest costly standard. It's cost made it well-liked for a short time, but now it's becoming less common as faster standards become less expensive. 802.11b broadcasts in the 2.4 GHz frequency band of the radio spectrum. It can switch up

to 11 megabits of data per second. For increasing speed, it uses **complementary code keying (CCK**).

- **802.11g** transmits at 2.4 GHz like 802.11b, but it's a lot faster -- it can handle up to 54 megabits of data per second. 802.11g is faster because it uses the same OFDM coding as 802.11a.
- **802.11n** is the most widely available of the standards and is backward compatible with a, b and g. It significantly improved speed and range over its predecessors. For instance, although 802.11g theoretically moves 54 megabits of data per second, it only achieves real-world speeds of about 24 megabits of data per second because of network congestion. 802.11n, however, reportedly can achieve speeds as high as 140 megabits per second. 802.11n can transmit up to four streams of data, each at a maximum of 150 megabits per second, but most routers only allow for two or three streams.
- **802.11ac** is the newest standard as of early 2013. It has yet to be widely adopted, and is still in draft form at the **Institute of Electrical and Electronics Engineers (IEEE)**, but devices that support it are already on the market. 802.11ac is backward compatible with 802.11n (and therefore the others, too), with n on the 2.4 GHz band and ac on the 5 GHz band. It is less prone to interference and far faster than its predecessors, pushing a maximum of 450 megabits per second on a single stream, although real-world speeds may be lower. Like 802.11n, it allows for transmission on multiple spatial streams -- up to eight, optionally. It is sometimes called **5G Wi-Fi** because of its frequency band, sometimes **Gigabit Wi-Fi** because of its potential to exceed a gigabit per second on multiple streams and sometimes **Very High Throughput (VHT)** for the same reason.
- Other 802.11 standards focus on specific applications of wireless networks, like wide area networks (WANs) inside vehicles or technology that allows you to move from one wireless network to another seamlessly.
- Wi-Fi radios can transmit on any of three frequency bands. Or, they can "frequency hop" rapidly between the different bands. Frequency hopping helps reduce interference and lets multiple devices use the same wireless connection simultaneously. So long as they all have wireless adapters, several devices can use one router to connect to the Internet. This connection is convenient, virtually invisible and reliable enough; however, if the router fails or if too many people try to use high-bandwidth applications at the same time, users can experience interference or lose their connections. Although newer, faster standards like 802.11ac could help with that.

1.3 Structure of a Wireless Network:

It is easy to create Wi-Fi network with several computers and a wireless access point. Router is also needed to build a wireless network. This is a single unit that contains:

1. A port to connect with cable or DSL modem
2. A router

3. An Ethernet hub
4. A firewall
5. A wireless access point

A wireless router allows us to use wireless signals or Ethernet cables to connect computers and mobile devices to one another, to a printer and to the Internet. Most routers provide coverage for about 100 feet (30.5 meters) in all directions, although walls and doors can block the signal. If the home or the area where network will be set up is very large, it is important to buy reasonable priced range extenders or repeaters to increase working router's range.

As with wireless adapters, many routers can use more than one 802.11 standard. Normally, 802.11b routers are slightly less expensive than others, but because the standard is older, they're also slower than 802.11a, 802.11g, and 802.11n and 802.11ac routers. 802.11n routers are the most common.

Router will start work when it will be plugged in and it will start working at its default settings. Most routers let network administrator to use a Web interface to change routers internal settings. So, Administrator can select:

- **The name of the network, known as its service set identifier (SSID)**: The default setting is usually the manufacturer's name.
- **The channel that the router uses**: Most routers use channel 6 by default. If network builder live in an apartment and his neighbors are also using channel 6, he or she may experience interference. Switching to a different channel should eliminate the problem.
- **Router's security options**: Many routers use a standard, publicly available sign-on, so it's a good idea to set user's own username and password.

Security is an important part of a home wireless network, as well as public Wi-Fi hotspots. If an network administrator set his router to create an open hotspot, anyone who has a wireless card will be able to use his signal. Most people would rather keep strangers out of their network, though. Doing so requires the network administrator has to take few security precautions.

It's also vital to make sure security precautions are current. The Wired Equivalency Privacy (WEP) security measure was once the standard for WAN security. The idea behind WEP was to create a wireless security platform that would make any wireless network as secure as a traditional wired network. But hackers discovered susceptibility in the WEP approach, and currently it's easy to find applications and programs that can compromise a WAN running WEP security. It was succeeded by the first version of WiFi Protected Access (WPA), which uses Temporal Key Integrity Protocol (TKIP) encryption and is a step up from WEP, but is also no longer considered secure.

To keep network private, there are few methods available:

- **Wi-Fi protected Access version 2** (WPA2) is the successor to WEP and WPA, and is now the recommended security standard for Wi-Fi networks. It uses either TKIP or Advanced Encryption Standard (AES) encryption, depending upon what you choose at setup. AES is considered the most secure. As with WEP and the initial WPA, WPA2 security involves signing on with a password. Public hotspots are either open or use any of the available security protocols, including WEP, so use caution when connecting away from home. Wi-Fi Protected Setup (WPS), a feature that ties a hard-coded PIN to the router and makes setup easier, apparently creates a vulnerability that can be exploited by hackers, so you may want to turn off WPS if possible, or look into routers that do not have the feature.
- **Media Access Control** (MAC) address filtering is a little different from WEP, WPA or WPA2. It doesn't use a password to authenticate users -- it uses a computer's physical hardware. Each computer has its own unique MAC address. MAC address filtering allows only machines with specific MAC addresses to access the network. You must specify which addresses are allowed when you set up your router. If you buy a new computer or if visitors to your home want to use your network, you'll be required to add the new machines' MAC addresses to the list of approved addresses. The system isn't foolproof. A clever hacker can **spoof** a MAC address -- that is, copy a known MAC address to fool the network that the computer he or she is using belongs on the network.

Network administrator can also change other router settings to improve security. For instance, he or she can set it to block WAN requests to keep the router from responding to IP requests from remote users, set a limit to the number of devices that can connect the router and even disable remote administration so that only computers plugged directly into the router can change network settings. so, it is also important to change the Service Set Identifier (SSID), which is the network name, to something other than the default so that hackers can't immediately tell what router are using in this network. And selecting a strong password never hurts. [2]

1.4 Wi-Fi maintenance:

Wi-Fi is maintained by many applications and devices including video game consoles, home networks, PDAs, mobile phones, major operating systems, and other types of consumer electronics. Any products that are tested and approved as "Wi-Fi Certified" (a registered trademark) by the Wi-Fi Alliance are certified as interoperable with each other, even if they are from different manufacturers. For example, a user with a Wi-Fi Certified product can use any brand of access point with any other brand of client hardware that also is also "Wi-Fi Certified". Products that pass this certification are required to carry an identifying seal on their packaging that states "Wi-Fi Certified" and indicates the radio frequency band used (2.5GHz for 802.11b, 802.11g, or 802.11n, and 5GHz for 802.11a).[3]

1.5 Advantages of Wi-Fi:

Getting internet using less wire is one of the major plus sides of Wi-Fi. This is a wireless connection that can combine together multiple devices.

Wi-Fi network is particularly useful in cases where the wiring is not possible or even unacceptable. For example, it is often used in the halls of conferences and international exhibitions. It is ideal for buildings that are considered architectural monuments of history, as it excludes the wiring cables.

Wi-Fi networks are widely used to connect a variety of devices, not only between themselves but also to the Internet. And almost all modern laptops, tablets, and some mobile phones have this feature. It is very suitable and allows connecting to the internet almost anywhere, not just where the cables are laid.

Another advantage can be pretty easy to create a mesh Wi-Fi. To connect a new device to your network, simply turn on the Wi-Fi and do the simple setting in the software. In the case of wire technologies still need to pull the wire. Therefore, many modern offices are switching to this technology.

Consistency of Wi-Fi technology allows you to connect to the network in any country, although there are still little features of its application. All equipment with technology Wi-Fi certified and allows us to achieve high compatibility.

Fig 1.a: Wi-Fi network

1.6 Dis-advantages of Wi-Fi :

Significantly, it is particularly sensitive to electromagnetic radiation generated by household appliances. This mainly affects with speed of data transmission.
Despite the global standardization, many from different manufacturers are not fully compatible, which in turn affects the speed of communication.

Wi-Fi has a limited radius of action and it is suitable for home networking, which is more dependent on the environment. For example, a typical home router with Wi-Fi in the room has a range of up to 45 meters and up to 450 meters outside.

At high density Wi-Fi-points operating in the same or adjacent channels, they can interfere with each other. This affects the quality of the connection. This problem is common in apartment buildings, where many residents are using this technology. [4]

1.7 Wi-Fi security:

But with the rapid growth of Wi-Fi arises the number of hackers. The major concern of users at Wi-Fi hotspots is security. These types of wireless networks are primarily unsecure. This is because encryption methods such as WEP and WPA, which are usually used to protect private wireless networks, aren't implemented due to the complexities of supporting users. Moreover, using WEP or WPA means you'll have to advertise the "private" encryption key(s). So now there is no point in using encryption since the eavesdroppers will have the key(s) to quickly decode the Wi-Fi hotspot traffic.

Wi-Fi hotspots are usually susceptible to hackers. Once a free Wi-Fi hotspot is launched, suddenly a couple of more "free" Wi-Fi networks emerges that promise to allow you to access the Internet for free. Usually these happen to be fake Wi-Fi hotspots that invite you to get fooled into logging onto their networks. As you log in, your personal and sensitive data is stolen .Users that connect to these "free" networks are at great risk of experiencing a "channeling" attack. "Channeling" is a common practice used by hackers and identity thieves to conduct man-in-the-middle attacks, with the objective of stealing user names, passwords, and other sensitive data transmitted by the user and this is not a very tough job for the hacker.

Instructing the operating system to "remember" a particular network (or SSID) can be a fatal mistake. Now one of these fake Wi-Fi networks configure the name of their SSID as that of the one already given permission to, on a person's computer, the computer gets logged onto the network automatically, without the knowledge of the user.

By setting up an unauthorized access point in an airport lounge, hackers can easily trap passwords and other information without the user's knowledge.

Many Wi-Fi hotspot users don't understand the issues related to using public wireless networks, and so they don't take any steps to ensure their personal documents, privacy and identity are

safe. The same goes with the people installing the hotspots. They may not be aware of the issues they face, or the fact that they can take a few steps to help secure user access. [5]

Common attacks on wireless network are given below-

1.8 Attacks on Wi-Fi:

1. **Data Interception**: At present day, it is known that data sent over Wi-Fi can be captured by eavesdroppers – easily, within a few hundred feet; even farther with directional antennas. Fortunately, all Wi-Fi CERTIFIED products now support AES-CCMP data encryption and integrity. Unfortunately, there are still legacy products that only speak TKIP, and many WLANs are configured to accept both AES and TKIP. But TKIP is vulnerable to message integrity check (MIC) attacks that allow a limited set of spoofed frames to be injected – for example, ARP. Although resulting risks are modest, the writing is on the wall: The time has come to retire TKIP and require AES-CCMP.

2. **Denial of Service:** WLANs are characteristic ally vulnerable to DoS. Everyone segments the same unlicensed frequencies, making competition inevitable in populated areas. The good news: As enterprise WLANs migrate to 802.11n, they can use channels in the larger, less-crowded 5 GHz band, reducing "accidental DoS." Moreover, contemporary access points (APs) can auto-adjust channels to circumvent interference. But that still leaves DoS attacks: Phony messages sent to disconnect users, consume AP resources, and keep channels busy. To neutralize common DoS attack methods like Deauth Floods, look for newer products that support 802.11w management frame protection.

3. **Rogue APs***:* Business network saturation by unknown, unauthorized APs is another huge problem. Fortunately, most enterprise WLANs now uses legitimate APs to scan channels for possible rogues in their spare time. Unfortunately, verifying "true rogues" by tracing their wired network connectivity is a skill that ordinary WLAN gear has yet to perfect. Without accurate classification, automated rogue blocking is a risky proposition. To not just detect, but effectively mitigate rogue APs, deploy a Wireless IPS that can reliably differentiate between harmless neighbors, personal hotspots, and network-connected rogues that pose real danger, taking policy-based action to trace, block, and locate the latter.

4. **Wireless Intruders:** Wireless IPS products like Motorola AirDefense, AirMagnet, and AirTight can also detect malicious Wi-Fi clients operating in or near a business' airspace. However, truly effective defense requires up-to-date, properly deployed WIPS sensors. In particular, 802.11a/b/g sensors must be updated to monitor new 5 GHz channels (including 40 MHz channels), parse 802.11n protocols, and look for new 802.11n attacks. In addition, since 802.11n clients can connect from farther away, WIPS sensor placement must be reviewed to satisfy both detection and prevention needs.

5. **Mis-configured APs***:* Back when standalone APs were individually-managed, configuration errors posed a significant security threat. Today, most enterprise WLANs are centrally-managed, using coordinated updates and periodic audits to decrease TCO, improve reliability, and reduce risk. But 802.11n adds a slew of relatively complex configuration options, the consequences of which depend on (highly variable) Wi-Fi client capabilities. Arranging and breakdown for multi-media further complicates configuration. The solution: Combine sound, centralized management practices with 802.11n/WMM education and planning to reduce operator error.

6. **Ad Hocs and Soft APs***:* Wi-Fi laptops have long been able to establish peer-to-peer ad hoc connections that pose risk because they circumvent network security policies. Fortunately, ad hocs were so hard to configure so not many were encouraged to use them. Unfortunately, that barrier is being lifted by "soft APs" in Windows 7 and new laptops with Intel and Atheros Wi-Fi cards. Those virtual APs can provide easy, automated direct connections to other users, bypassing network security and routing traffic onto the enterprise network. Measures taken to hinder Ad Hocs may also prove useful against unauthorized Soft APs, such as IT-managed client settings and WIPS.

7. **Misbehaving Clients**: Clients that form unauthorized Wi-Fi connections of any type, whether accidentally or intentionally, put themselves and corporate data at risk. Some enterprises use Group Policy Objects to configure authorized Wi-Fi connections and prevent end-user changes. Others use host-resident agents and/or WIPS to monitor Wi-Fi client activity and disconnect high-risk connections. However, many businesses (especially SMBs) still depend on end-users to connect only to known, authorized wireless APs. Given pervasive deployment, longer reach, and broader consumer electronics integration, accidental or inappropriate Wi-Fi connections have never been easier

8. **Endpoint Attacks:** Now that over-the-air encryption and network-edge security have improved, attackers are concentrating Wi-Fi endpoints. Plentiful exploits have been published to take advantage of buggy Wi-Fi drivers, using buffer overflows to execute arbitrary commands – sometimes at ring 0 (high-privilege kernel mode). Automated attack tools like Metasploit can now be used to launch Wi-Fi endpoint exploits with minimal effort. Although vendors do (usually) patch these bugs once discovered, Wi-Fi driver updates are not distributed automatically with OS updates. To protect your workforce, track Wi-Fi endpoint vulnerabilities (for example, using WiFiDEnum) and keep your Wi-Fi drivers up-to-date.

9. **Evil Twin APs:** Fraudulent APs can easily advertise the same network name (SSID) as a legitimate hotspot or business WLAN, causing nearby Wi-Fi clients to connect to them. Evil Twins are easier-to-use hacker tools have increased your risk of running into one. Tools like Karmetasploit can now listen to nearby clients, discover SSIDs they're willing to connect to, and automatically start advertising those SSIDs. Once clients connect, DHCP and DNS are used to route client traffic through the Evil Twin, where local (phony) Web, mail, and file servers

execute man-in-the-middle attacks. The only effective defense against Evil Twins is server authentication, from 802.1X server validation to application server certificate verification.

10. **Wireless Phishing:** In addition to the above man-in-the-middle application attacks, hackers continue to develop new methods to trick Wi-Fi users. For instance, it's possible to poison Wi-Fi client Web browser caches, so long as the attacker can get into the middle of a past Web session – such as by using an Evil Twin at an open hotspot. Once poisoned, clients can be redirected to phishing sites long after leaving the hotspot, even when connected to a wired enterprise network. One technique for reducing this threat is to clear your browser's cache upon exit. Another possibility is to route all hotspot traffic (even public) through a trusted (authenticated) VPN gateway. [6]

To obtain awareness against these attacks in, there are few open source audit tools available to monitor and secure the Wi-Fi network. In this book, we will discuss about some of them and their features over wireless network.

1.9 Open Source Security Audit tools:

Improvement has been made in the security for Wi-Fi to a significant extent over the years. Today's enterprise WLANs can be made fairly immune to intrusion and misuse. However, end-to-end security still cannot be assumed; just enabling Wi-Fi encryption will not secure the applications running on the wireless network. Wi-Fi technologies, products, and attacks will continue to sprout. Security admin still need to keep updated on new threats, assess their business risk, and take appropriate action. Some Wi-Fi open source tools available for the safety of Wi-Fi zone are mentioned below-

Wireshark

Wireshark is a free and open-source packet analyzer. It is used for network troubleshooting, analysis, software and communications protocol development, and education. Originally named Ethereal, in May 2006 the project was renamed Wireshark due to trademark issues.

Wireshark is cross-platform, using the GTK+ widget toolkit to implement its user interface, and using pcap to capture packets; it runs on various Unix-like operating systems including Linux, Mac OS X, BSD, and Solaris, and on Microsoft Windows. There is also a terminal-based (non-GUI) version for Linux called TShark. Wireshark, and the other programs distributed with it such as TShark, are free software, released under the terms of the GNU General Public License.

Platform：Windows/Linux；License： GNU General Public License v3 [7]

Kismet

Linux fans know that Kismet is a Wi-Fi Swiss Army knife--it discovers APs and clients, captures Wi-Fi packets from local NICa or remote drones, and can generate alerts for fingerprinted recon activities. Kismet is a versatile client/server tool that can be paired with any RFMON-capable adapter--even on OS X or Cygwin. Using Kismet, one can identify discovered APs and clients which will help spot policy violations like mis-configured APs or misbehaving clients. [8]

Ettercap

Ettercap is a suite for man in the middle attacks on LAN. It features sniffing of live connections, content filtering on the fly and many other interesting tricks.

It supports active and passive dissection of many protocols (even ciphered ones) and includes many features for network and host analysis. These entire features are integrated with a easy-to-use and pleasureful ncurses/gtk interfaces.

Platform： Windows/Linux/BSD/MacOS, License: GNU General Public License

PRTG

PRTG is a open source network monitor where PRTG stands for Paessler Router Traffic Grapher. It is a network monitoring software from Paessler AG.PRTG runs on Windows and monitors network availability and network usage using SNMP, Packet Sniffing, WMI, IP SLAs and Netflow and various other protocols.

Platform : Windows, License :freeware/commercial

Nagios

Nagios is the definitive open source network monitoring solution. It can be used from simply checking to see if a network host is still up, all the way up to monitoring specific services on remote hosts, and even to trigger corrective action if a problem is detected. And tell you about all that by mail, phone, fax, pager, sirenes and flashing lights, and possibly also by carrier pigeon.

Platform : Linux, License : GPL v2

Easy-Creds

The easy-creds script is a bash script that leverages ettercap and other tools to obtain credentials during penetration testing.

Menu driven, it attack with basic ARP spoofing, one-way ARP spoofing and DHCP spoofing and the setup of a Fake AP.

Moreover, it has an SSLStrip log file parser that leverages a definition file to give one the compromised credentials and the site they have come from.

Platform： Linux； License: GNU General Public License v2

Aircrack-ng

Aircrack-ng is an 802.11 WEP and WPA-PSK keys cracking program that can recover keys once enough data packets have been captured. It implements the standard FMS attack along with some optimizations like KoreK attacks, as well as the all-new PTW attack, thus attack compared to other WEP cracking tools. In fact, Aircrack-ng is a set of tools for auditing wireless networks.

Platform: Windows/Linux ; License : GNU General Public License v2

Aircrax

It is easy to use wizard-like GUI tool to recover WEP/WPA keys using the aircrack-ngsuite. It is Written in C# using Mono, GTK#, and the Funkit library.

Platform :Windows/Linux ; License : GNU General Public License v3

Argus

Argus is a network Audit Record Generation and Utilization System tool. The Argus Project is focused on developing network activity audit strategies and prototype technology to support Network Operations, Performance and Security Management. If you look at packets to solve problems, or you need to know what is going on in your network you should find Argus a useful tool.

Platform: Windows/Linux ; License : GNU General Public License v2

Open AudIT

Open-AudIT is an application to let you know exactly what is on your network, how it is configured and when it changes. Open-AudIT will run on Windows and Linux systems. Essentially, Open-AudIT is a database of information that can be queried via a web interface. Data about the network is inserted via a Bash Script (Linux) or VBScript (Windows). The entire application is written in PHP, bash and vbscript. These are all 'scripting' languages - no compiling and human readable source code. Making changes and customizations is both quick and easy.

Platform: Windows/Linux ; License : GNU General Public License v2

Mitmjws

Mitmjws is a basic script to automate man-in-the-middle attacks. The script calls airbase, ettercap, sslstripper and driftnet, requires aircrack-ng with experimental software. So, before test this program, you need install all dependence tools and libraries. This project's source code is released under GNU General Public License v3 (GPLv3).

Platform: Windows/Linux/BSD/Mac OS; License: GNU General Public License-v3

Middler

The Middler is a Man in the Middle tool to demonstrate protocol middling attacks. Led by Jay Beale, the project involves a team of authors including InGuardians agents Justin Searle and

Matt Carpenter. The Middler is intended to man in the middle, or "middle" for short, every protocol for which we can create code.

In its first alpha release, a core built by Matt and Jay is released, with introductory plug-ins by Justin and InGuardians agent Tom Liston. It runs on Linux and Mac OS X, with most of the code functional on Windows. The current codebase is in the beta state, with a full release coming soon, with better documentation, easier installation, and even more plug-ins.

Platform: Windows/Linux/BSD/Mac OS; License: GNU General Public License v2

IPpon-mitm

Software updates apply patches or introduce new features to an application. In most cases, the update procedure is conducted in an insecure manner, exposing the updater to execution of malicious code or to manipulation of application data such as anti-virus signatures. This tool uses several techniques of update-exploitation attacks which leverages a man-in-the-middle technique, to build and inject a fake update reply or hijack an on-going update session.

Platform: Windows/Linux/BSD/Mac OS; License: GNU General Public License v2

AIMject

Man in the middle on AIM. Aimject facilitates man-in-the-middle attacks against AOL Instant Messenger's OSCAR protocol via a simple GTK interface. The features are: (1) sign-on/off detection; (2) message interception/decoding; (3) message injection into arbitrary conversations; (4) synchronization of AIM sequence numbers and fnac ids; (5) cloning of font styles/screen name formatting to avoid detection; (6) selective muting of conversation participants; (7) integrated ARP/DNS spoofing.

Platform: Windows/Linux/BSD/Mac OS; License: GNU General Public License v2

Andiparos

Andiparos is a fork of the famous Paros Proxy. It is an open source web application security assessment tool that gives penetration testers the ability to spider websites, analyze content, intercept and modify requests, etc. The advantage of Andiparos is mainly the support of Client Certificates on Smartcards. Moreover, it has several small interface enhancements, making the life easier for penetration testers...

Platform: Java

License: GNU General Public License v2[19]

Paros

A Java based HTTP/HTTPS proxy for assessing web application vulnerability. It supports editing/viewing HTTP messages on-the-fly. Other featuers include spiders, client certificate, and proxy-chaining, intelligent scanning for XSS and SQL injections etc. "Paros" for people who need to judge the security of their web applications. It is free of charge and completely written in Java. Through Paros's proxy nature, all HTTP and HTTPS data between server and client, including cookies and form fields, can be intercepted and modified.

Platform: Java;License: GNU Lesser General Public License v2.1

PktAnon

PKtAnon performs network trace anonymization. It is highly configurable and uses anonymization profiles. Anonymization profiles allow for mapping of arbitrary anonymization primitives to protocol attributes, thus providing high flexibility and easy usability. A great number of anonymization primitives and network protocols are supported and ready to use for online and offline anonymization.

Deep Network Analyzer

DNA is open, flexible and extensible deep network analyzer software server and software architecture for gathering and analyzing network packets, network sessions and applications protocols, passively off enterprise class networks.[9]

1.10 Methodology:

Open source tools have very easy installation process and configuration. Most of the open source tools have User manual guides which are available over their websites. So that, anyone can learn about using method of open source tools. Moreover, hackers are taking advantages of using open source tools as it is readily-accessible. Sometimes these open source tools can be used for ethical hacking. Additionally, ethical hacking means auditing or surveying any organizations wireless network by taking their permission. This audit can help a organization to learn more about their network condition.

We worked on public wi-fi hotspot to analyze few open source tools for testing their working method. We did not get any permission to work any private wi -fi network because it is very confidential and no organizations want to disclose their internal information with public wi-fi zone. When we implemented those open source tools, we saw that all the details about network interfaces are shown clearly. This information is very supportive for attackers to attack any wireless network .As general public do not aware of public wi-fi hotspot. We did survey in few organizations network pattern where they do not use any extra security tools for security concerns but use WPS for ensuring security.

In addition, we create a comparison list of popular five open source tools and further we categorized it for different sector's organizations. So that, IT team of different companies can know about these open source tools and can use it for their private and public wi-fi zone to save their network form unwanted hacking. By using these tools, network administrators can analyze their network and can update their network information rapidly.

Now, we are going to discuss about five open source tools working pattern, implementation procedure and their features in the below -

Chapter-2

2.1 WIRESHARK

The basic tool for observing the messages exchanged between executing protocol entities is called a **packet sniffer**. Packet sniffer captures ("sniffs") messages being received from computer; it will also typically store and/or display the contents of the various protocol fields in these captured messages. A packet sniffer itself is passive. It observes messages being sent and received by applications and protocols running on your computer, but never sends packets itself. Similarly, received packets are never explicitly addressed to the packet sniffer. Instead, a packet sniffer receives a copy of packets that are sent by application and protocols executing on machine.

Figure 2.a shows the structure of a packet sniffer. At the right of Figure 2.aare the protocols (in this case, Internet protocols) and applications (such as a web browser or ftp client) that normally run on your computer. The packet sniffer, shown within the dashed rectangle in Figure 3.a is an addition to the usual software in your computer, and consists of two parts. The **packet capture library** receives a copy of every link-layer frame that is sent from or received by your computer. The messages exchanged by higher layer protocols such as HTTP, FTP, TCP, UDP, DNS, or IP all are eventually encapsulated in link-layer frames that are transmitted over physical media such as an Ethernet cable. In Figure 2.a, the assumed physical media is an Ethernet, and so all upper layer protocols are eventually encapsulated within an Ethernet frame. Capturing all link-layer frames thus gives you all messages sent/received from/by all protocols and applications executing in your computer.

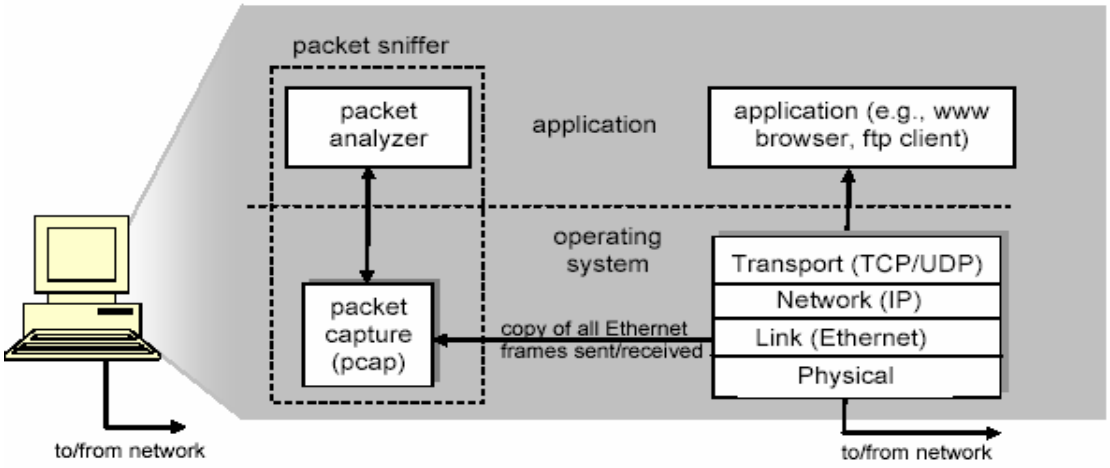


Figure 2.a : Packet sniffer structure

The second component of a packet sniffer is the **packet analyzer**, which displays the contents of all fields within a protocol message. In order to do so, the packet analyzer must "understand" the structure of all messages exchanged by protocols.[11]

There are many packet capturing and analyzing tools available in market but there is a tool wireshark that leads the rest. Wireshark is by far the best GUI based open source packet analyzer.

2.2 Ethereal and Wireshark

Because a command-line interface isn't everybody's idea of user friendliness, graphical solutions that also rely on the Libpcap library have been around for some time. One of these tools is Wireshark, which dates back to 2006. It was formerly known as Ethereal and is probably known to many administrators by that name. The tool was renamed when version 0.99.1 of Wireshark was released, because Ethereal developer Gerald Combs left Ethereal Software. He launched a successor project under the name of Wireshark with CACE Technologies, and this prompted Ethereal Software to discontinue the development of the predecessor product.

At present, Wireshark is mainly developed by the Wireshark community. Ethereal and Wireshark are genuine open source projects, although Ethereal is oriented to network analysis products by commercial vendors. Development milestones for Wireshark include version 1.0, which became available in March 2008, and the bug fix version 1.4, which became available in the summer of 2008. Both of these versions offered experimental support for Python scripts and the ability to right-click the packet details in the packet list to add protocol fields.

The release of Libpcap 1.0.0 added the ability to define the buffer size for recording and to view JPG files directly in Wireshark. Version 1.6 of Wireshark (which prompted me to write this article) was released in July 2011 and offers better support for large files of more than 2GB. It can also import text dumps in a similar style to text2pcap. The developers have also made the GUI more user-friendly so that adman's can hide columns while at the same time defining custom columns for the required fields.

The main feature of the new version is support for more than 30 new protocols including JSON, Wi-Fi P2P (Wi-Fi Direct), and Fiber Channel over Infinite Band. Also, Wireshark 1.6.0 can export SSL keys and SMB objects. Another new feature in Wireshark 1.6 is that the software displays VLAN tags (IEEE 802.1q) directly in the Ethernet II protocol tree.

2.3 What is Wireshark:

Wireshark is a tool that can capture network packets (both incoming and outgoing) and present them in a GUI providing detailed information about each packet captured. This tool is extremely helpful for network administrators to know details like which all computers are trying to communicate with a machine. Also, while debugging any connectivity related issue, the details provided by wireshark capture is very useful.

This tool is also used by protocol implementers to test whether a particular protocol packets are being correctively formed or not. Wireshark is also used in case of debugging by software developers in case they want to know how a packet arrived on wire and whether it was changed by an application or not?[12]

2.4 Practical outputs of using Wireshark:

Using Wireshark is not rocket science. A couple of configuration steps can help Wireshark to capture packets.

Here are the few steps to get your Wireshark up and capturing in a basic mode:

- Select the network interface on which we want to capture the packets. This can be done through **Capture->Interfaces** or can select the interface from the list as shown below. Please start this tool with administrator privileges otherwise you will not see any interface in the list.

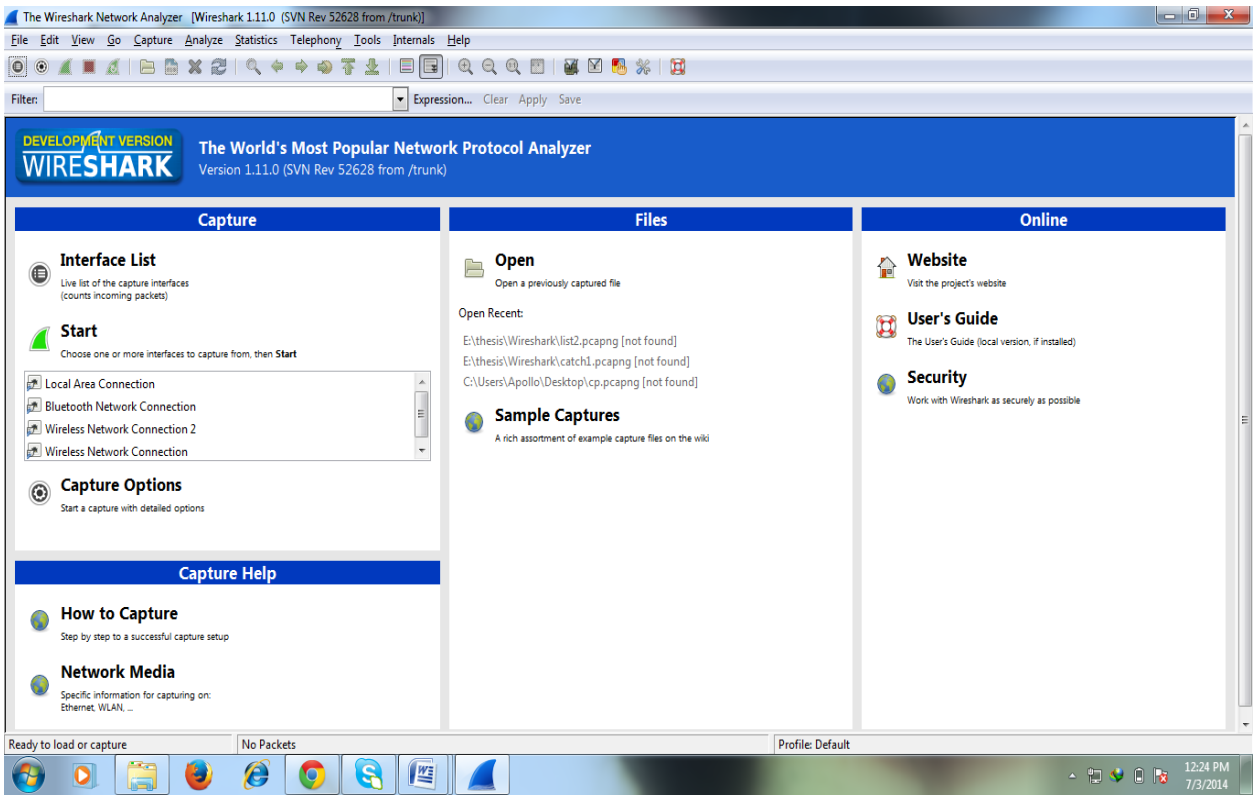


Figure2.b:wireshark home page

Once the interface is selected, Wireshark will start capturing all packets arriving and leaving the selected network interface.

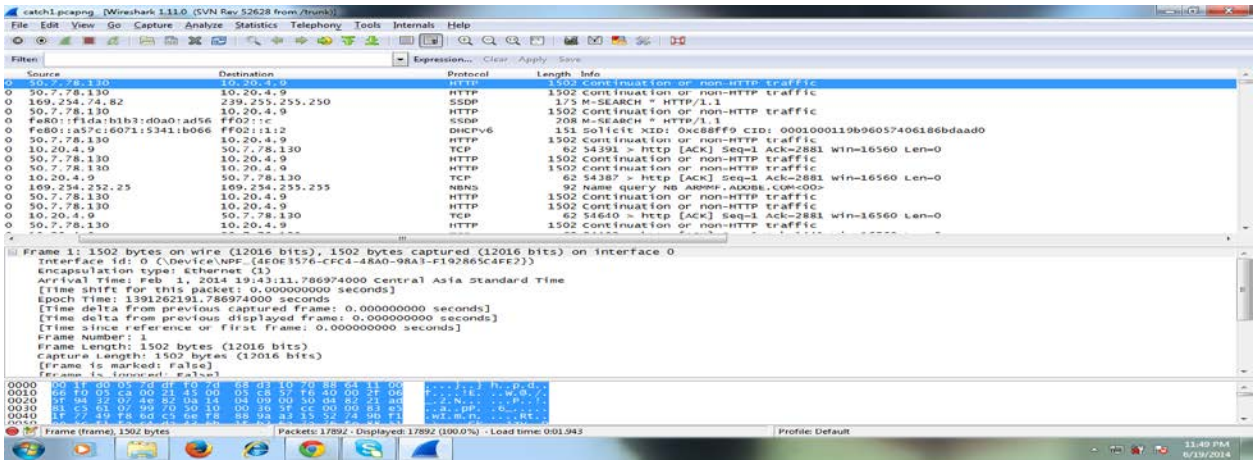


Figure 2.c: Live packet capture

If we click on any packet, we will see detailed information about that packet in the lower half of the Wireshark GUI.

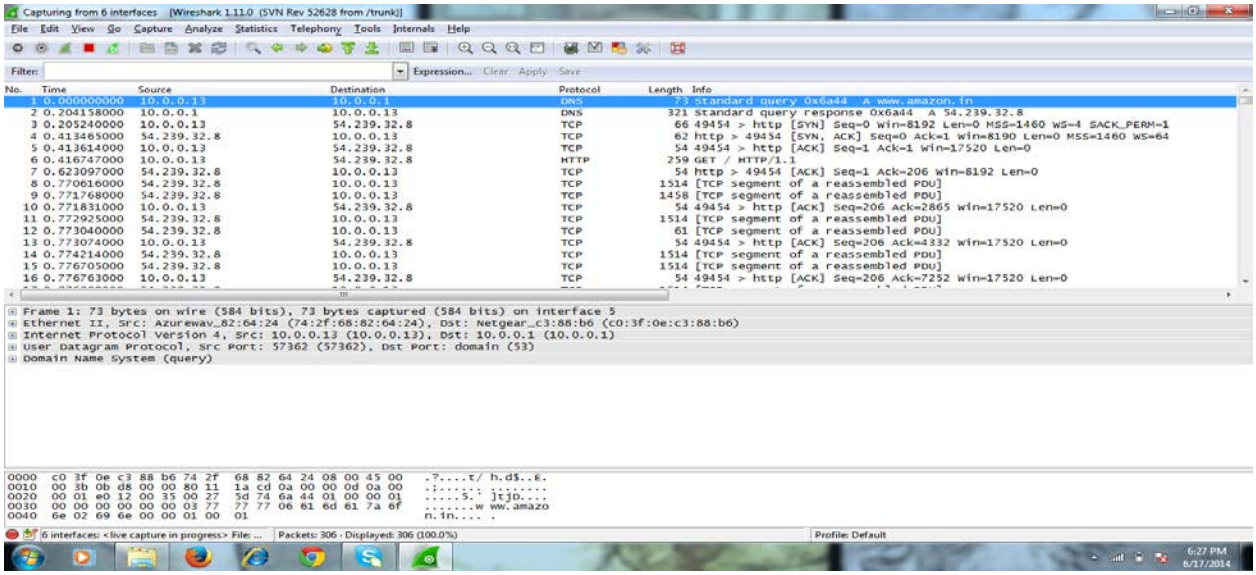


Figure 2.d: Details of packet

We can filter the packets based on various filters that are available with Wireshak. For example, if we want to highlight only TCP packets, just type **tcp** in the filter box and hit enter.

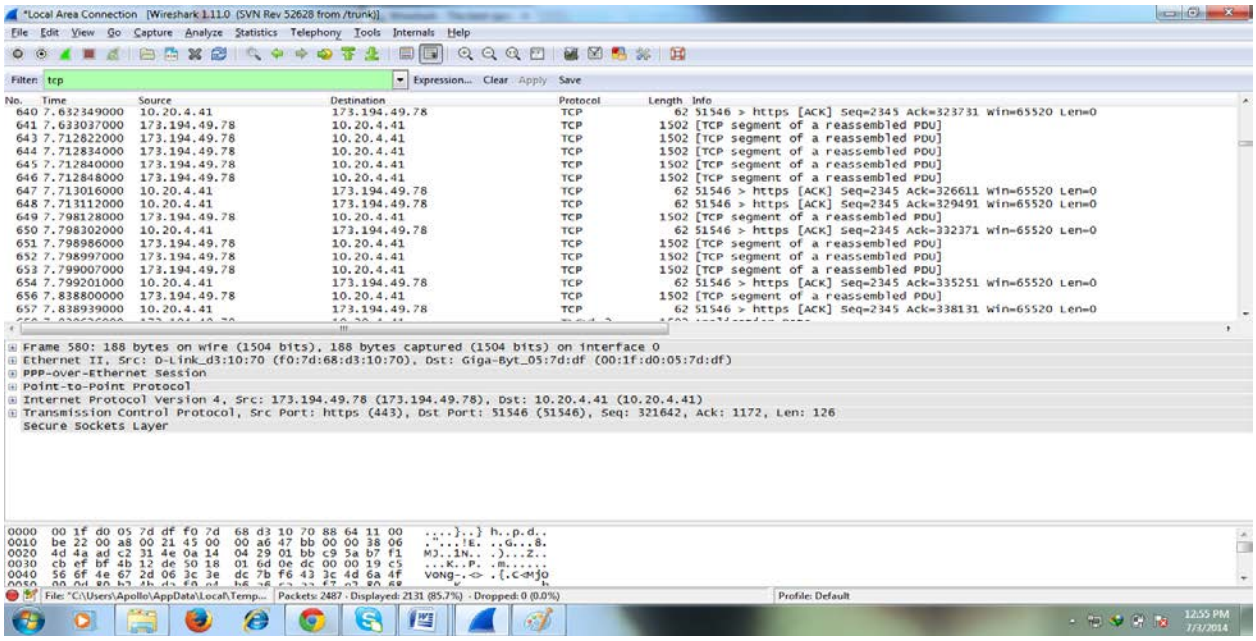


Figure 2.e: details of TCP packets

To stop the capture, need to hit the stop button present in GUI. Always stop Wireshark once we are done with capture otherwise it will keep capturing packets and will consume significant amount of system memory that may slow down the system.

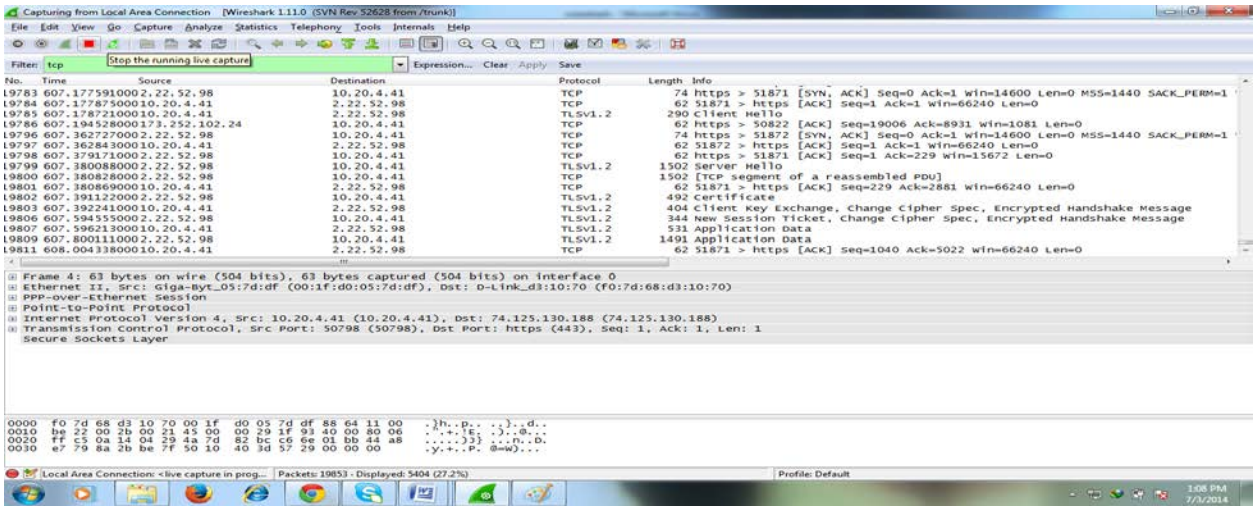


Figure 2.f: Stop option of wireshark

We can save the capture for future reference using **File->save**

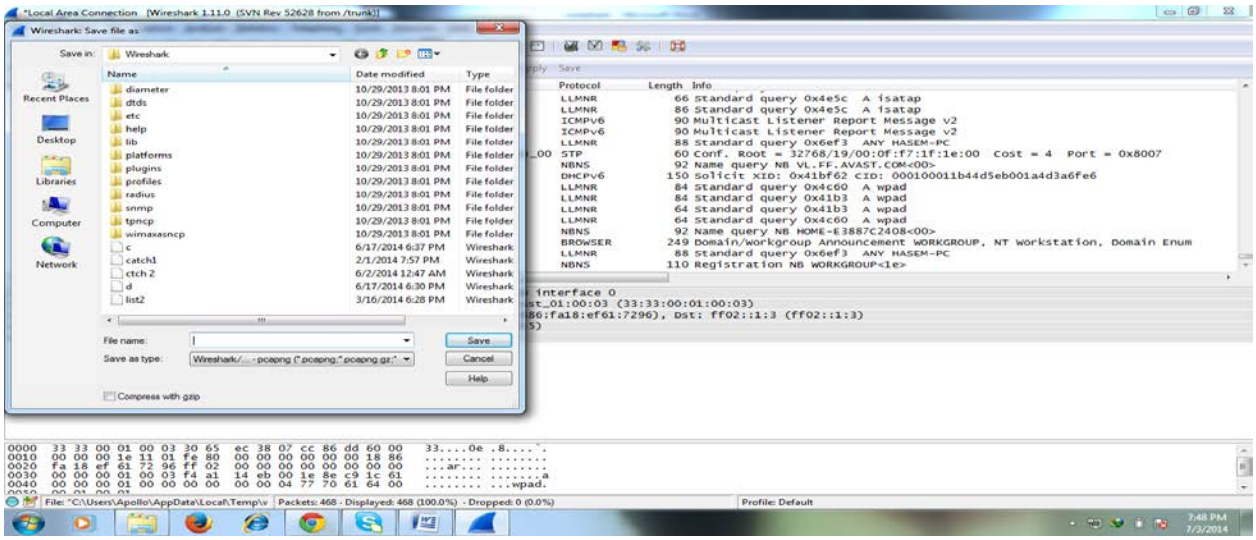


Figure 2.g: Save file

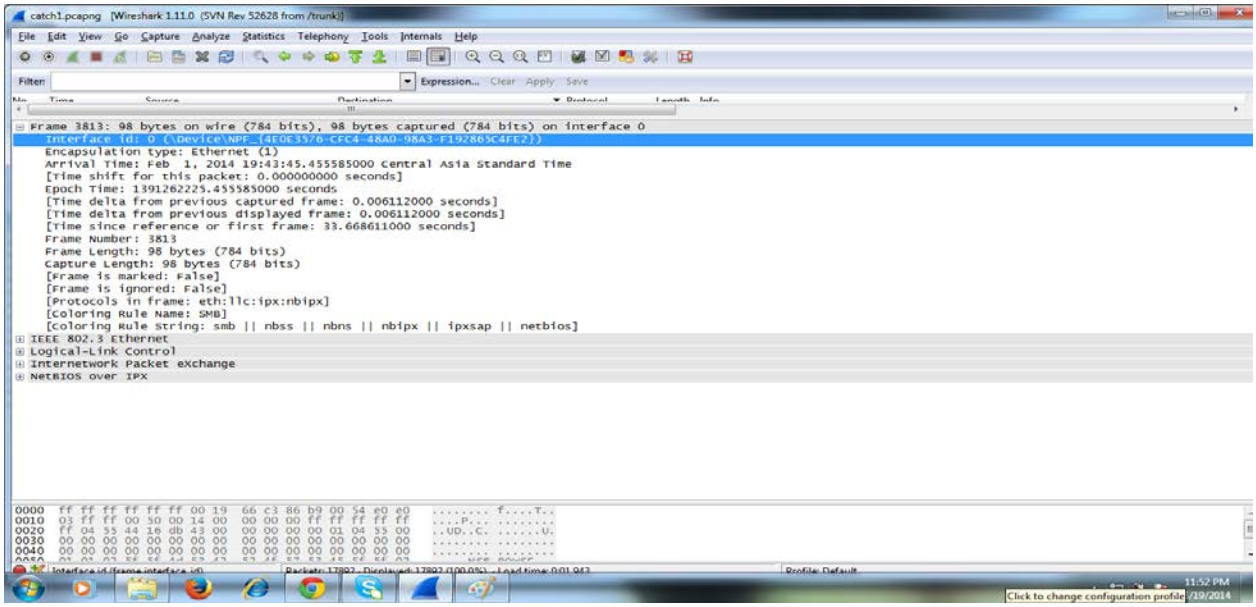


Figure 2.h: Frame details

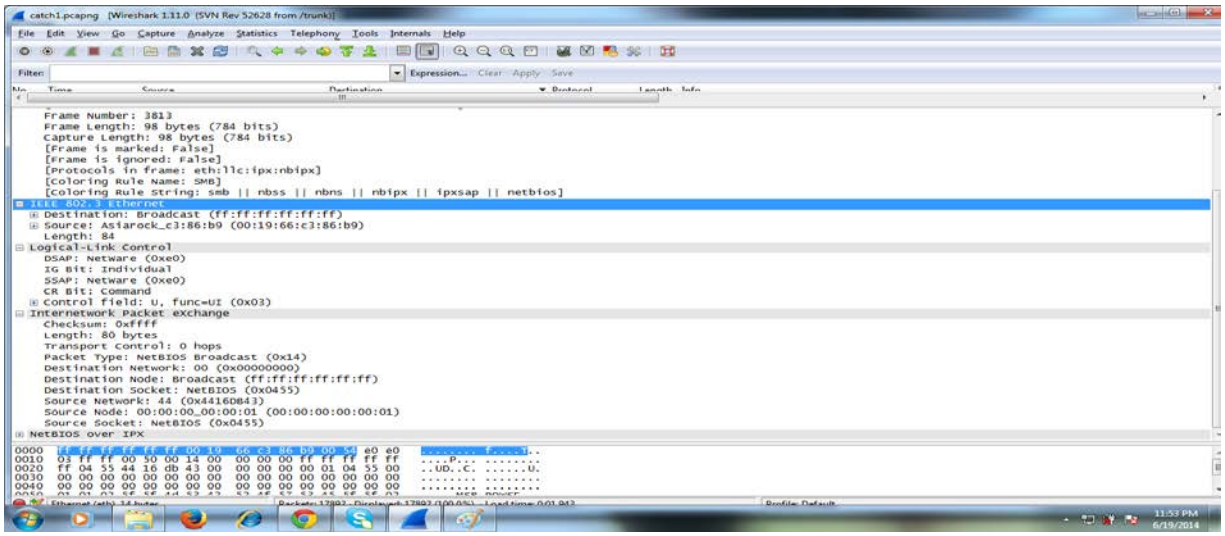


Figure 2.1: IEEE 803.3 Ethernet

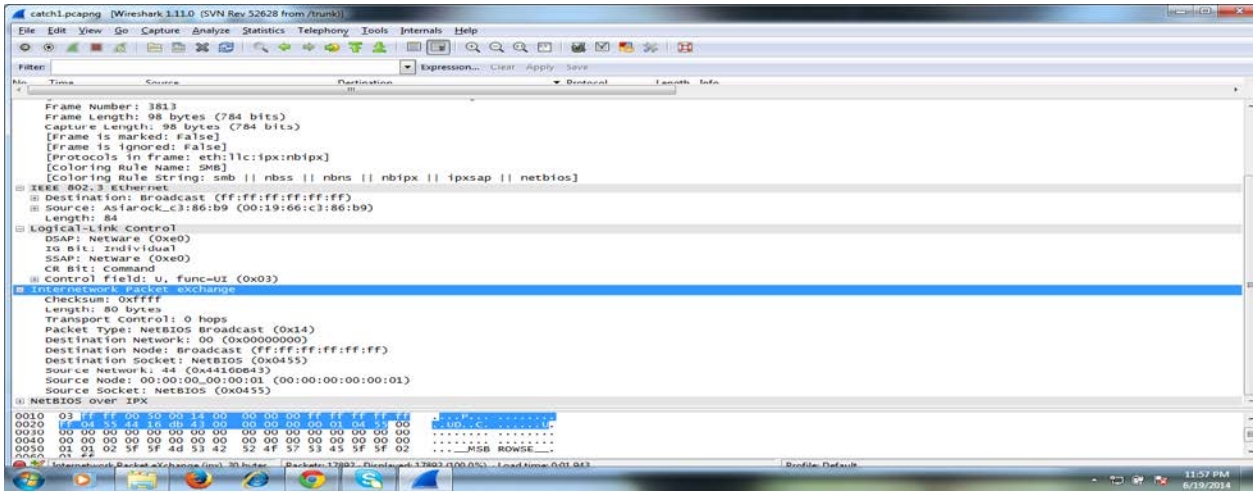


Figure 2.j: Internet packet Exchange

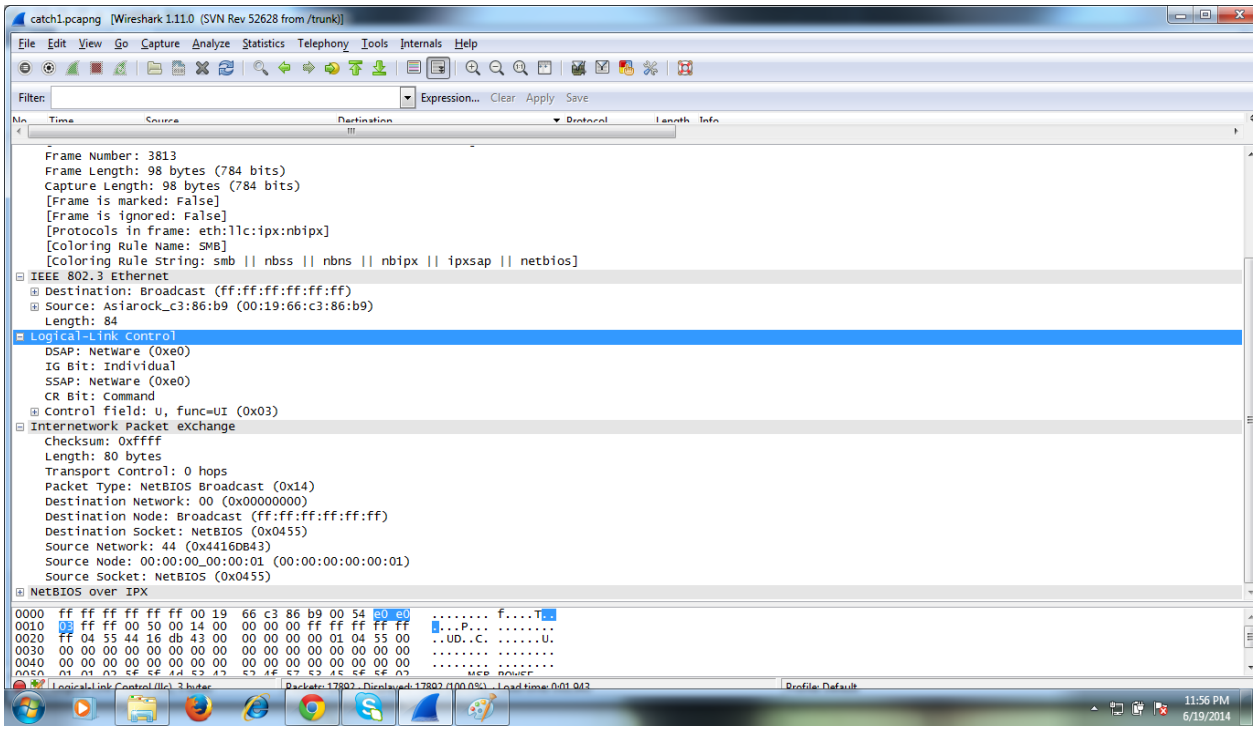


Figure 2.k: Logical-Link Control

So that, by following those steps, we can use Wireshark easily.[13]

2.5Protocol Analysis and Troubleshooting

A Protocol Analyzer

It is mostly a tool for seeing the bits and bytes flowing from end to end to a network in human understandable form. Without it, understanding a network communication exchange would be almost impossible. Network protocol is broken down into 7-layers. The part that WireShark deals with is layer 2 up to 7. Most well-known protocols can be decoded by WireShark.

Learn Network Protocols

One of the most obvious applications of WireShark is the ability to capture network traffic and look at it from the perspective of learning. For instance, if we are learning how the TCP protocol works, capture traffic from our own computer when we visit a web site. In the captured trace file, you will see every detail of the network communication exchange including the details of the well-known 3-way connection handshake.

Solve Network Problems

While "black box" method to network troubleshooting doesn't does not work, it is time to use WireShark. For example, at work, we had an issue where a computer was powerless to connect to a specific address on the Internet. We patterned the setup again. The Internet configuration

was OK because people can get to it from outside of our network, but from within out network, they could not reach this particular site. Normal troubleshooting method didn't change it. Using WireShark the network traffic being exchanged by our computer and the network could be captured. The capture revealed that our computer was getting a tcp check thus the connection would not go through. As it turns out, out company web filter was sending a TCP RESET to block us from reaching that particular site! Without WireShark, there was no way we could have figured this out. Solving network issues is probably the best use of WireShark. [14]

2.6 Wireshark Misconceptions

There is a combine misconception about wireshark to recognize what wireshark is not.

1. Wireshark is not a packet generator or packet dropper. It is only capture packets and analyze them. Through this, it is easy to configure some filters for wireshark to display only the packets but nothing can be done with actual packet.
2. Wireshark will never advise if any suspicious packets or mischievous connections. Thus, it cannot use as an alarm or notification for packets.[15]

Chapter - 3

3.1 KISMET

Kismet is an open source wireless network analyzer running under the Linux, UNIX and Mac OS X systems. It is able to detect any 802.11 a/b/g wireless networks around it. 802.11 a/b/g protocols are WLAN (Wireless Local Area Network) standards.

Kismet works with a lot of wireless cards supporting "monitor" mode. This mode captures packets without being able to associate in the same time with an access point and require privilege srights.

Kismet senses networks by passively sniffing providing it the advantages to discover the"hidden" wireless networks and being itself invisible.

Kismet can capture data which is not seen by other open source tools. The kismet program is composed by a server called "kismet_server" and a client "kismet_client" which can connect too many servers.

Kismet is able to produce several types of logs such as "dump", "csv" or "xml" files. Optionally, it can be related with a GPS device and the "gpsd" tool to draw the detected access points and wireless covering zones on maps such as the Google maps. "Sox" and "Festival" can also be used to play audio alarms for network events and speak out network summary on discovery.

Kismet is a passive sniffer which does not send any packets at all. Instead, Kismet works by putting the wireless client adapter into RF monitor mode. While in so-called “rfmon” mode, the wireless client is not (and cannot be) associated with any access point. Instead, it listens to all wireless traffic. Consequently, your wireless card cannot maintain a functional network connection while under Kismet control.
Users often report that Kismet finds more APs than other open source tools. Some network administrators configure their APs not to broadcast, or to “hide” their SSID. Kismet will detect hidden Aps, but without a network name. However, when a legitimate client associates with that AP, its real SSID is included in the initial handshake. Because Kismet sees all network management traffic, it will pick up these packets and discover the SSID which was supposedly “hidden.”[16]

3.2 Maintained Hardware

Kismet functions only work with network cards with drivers that support RF monitoring mode. In general, this comprises wireless cards based on the PRISM 2, 2.5, 3, and GT chipsets; older ORiNOCO cards without the HermesII chipset, such as the Orinoco Gold; and Atheros a/b/g chipsets.

In practice, there are many wireless cards on the market, and it is not always obvious whether there are supported drivers available. Some of the more popular supported wireless adapters include the ORiNOCO Gold, the original Apple Airport (not Extreme) card, and Intel Centrino. To further complicate things, drivers available for one platform, such as Linux, may not be available for another, such as OS X, even though Kismet itself is available for both. In general, Linux has the most supported drivers for Kismet. The Kismet Web site hosts a forum for discussion and questions about supported cards and driver availability.

3.3 Installing

Kismet is approved under the GNU General Public License. It is formally spread as a source package which you can compile for a variety of platforms, from Linux to OS X to BSD, if you're into that kind of thing.

The Kismet Web site also hands out pre-compiled binaries for Arm and MIPS platforms. These binaries allow running Kismet on small devices like the Sharp Zaurus Sl-6000L (using the Arm binary) or the venerable Linksys WRT54G router (using the MIPS binary).

Apple users can download pre-compiled Kismet for OS X from the KisMAC site, which includes a slick Aqua GUI.

Linux users who do not want to compile Kismet from source should check the sources for their supply.

Although Kismet uses a text-based interface, a window-based GUI called GKismet is available for Linux with Gnome libraries installed.'

Kismet is designed with client/server architecture. While most users run both the client and server on the same machine and simply use Kismet as a local application. Kismet clients can be used on remote systems. Such way, one or more remote machines can see real-time data from the machine hosting the Kismet server.

In a typical Linux install, the Kismet configuration files are found in /etc/kismet. This location may vary depending on platform.

Before running Kismet for the first time, it is need to edit the primary configuration file, kismet.conf.

Inside, the below file will be found

suiduser=your_username_here

The conventional wisdom is that user should set the above to a local user under which user'll run Kismet.We experienced it in Ubuntu and back track virshion 5 installed in Vmware, using the Kismet package provided by Ubuntu. We configured kismet as a root. It is need to tell Kismet which "source," or wireless adapter, to use. The basic syntax used in kismet.conf is:

source=type,interface,name

On my Ubuntu system with an Atheros-based Netgear WG511T card, my source configuration looks like this:

source=madwifi_ag,ath0,madwifi

Some alternative source lines for other cards include:

source=madwifi_b,ath0,madwifi

source=orinco,eth1,Orinoco

source=prism,wlan0,hostap

source=viha,en1,AirPort

The Kismet documentation contains a section called "Capture Sources," which includes a chart that lists the type and interface parameters for every supported chipset. The third parameter, name, can be set to anything you like for logging purposes.[17]

3.4 Running Kismet

Unless installing a window-based GUI for Kismet such as KisMAC or GKismet, this is a text-based application. In Linux system, we open a terminal window and launch Kismet as root for sniffing packets.

3.5 Further Fun

If anyone have a serial-based GPS receiver connected to a Kismet server, it is easy log and even map detected access points. You'll need GPSD, if it's not already installed, it is easy log and to provide communications between the receiver and Kismet.

Kismet can play and/or speak audible alerts, which is particularly helpful when detecting wireless networks from a moving vehicle. In the kismet.conf file, you can configure .wav format sounds for alerts, including new network detection, new WEP network, new network traffic, junk traffic, GPS lock and lost.

Using the text-to-speech software Festival, Kismet can also speak its findings using customizable templates available in kismet.conf. [18]

3.6 Features of Kismet:

- Ethereal/Tcpdump compatible data logging
- Airsnort compatible weak-iv packet logging
- Network IP range detection
- Built-in channel hopping and multi-card split channel hopping
- Hidden network SSID decloaking
- Graphical mapping of networks
- Client/Server architecture allows multiple clients to view a single
- Kismet server simultaneously
- Manufacturer and model identification of access points and clients
- Detection of known default access point configurations
- Runtime decoding of WEP packets for known networks
- Named pipe output for integration with other tools, such as a layer3 IDS
- like Snort
- Multiplexing of multiple simultaneous capture sources on a single Kismet
- instance
- Distributed remote drone sniffing
- XML output

3.7 General use of kismet

- War driving: Mobile detection of wireless networks, logging and mapping of network location, WEP, etc.
- Site survey: Monitoring and graphing signal strength and location.
- Distributed IDS: Multiple Remote Drone sniffers distributed throughout an installation monitored by a single server, possibly combined with a layer3 IDS like Snort.
- Rogue AP Detection: Stationary or mobile sniffers to enforce site policy against rogue access points.[19]

3.8 Practical result:

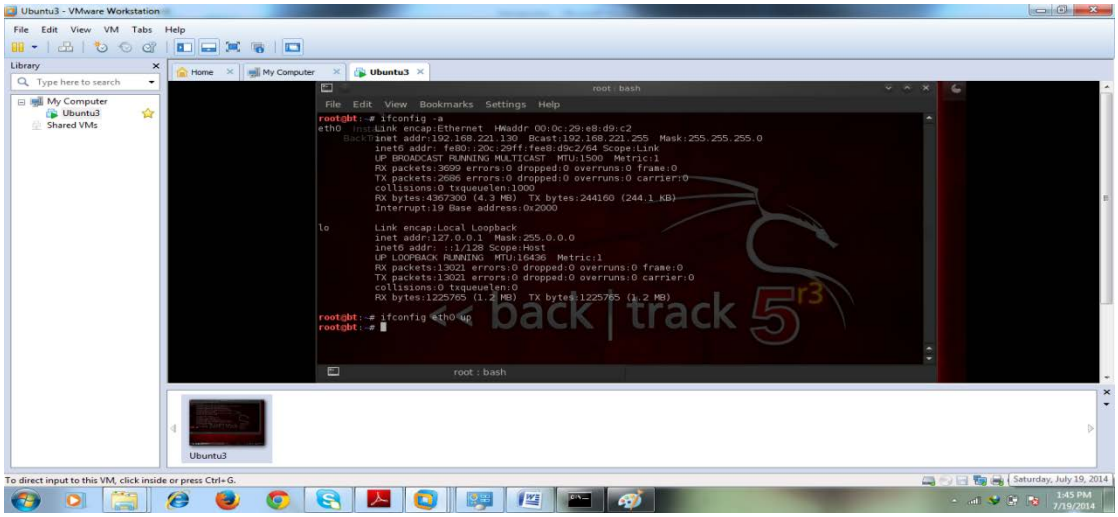


Figure 3.a: Kismet configuration (root server)

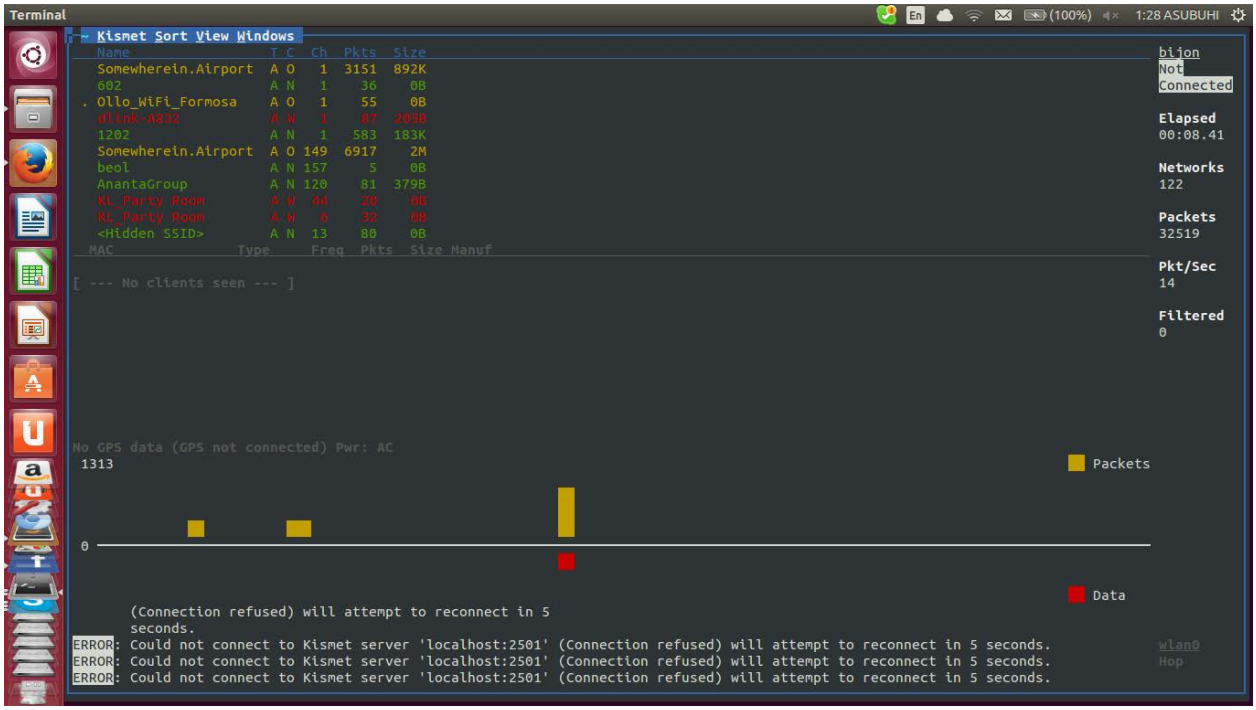


Figure 3.b: Kismet Startup with its channel

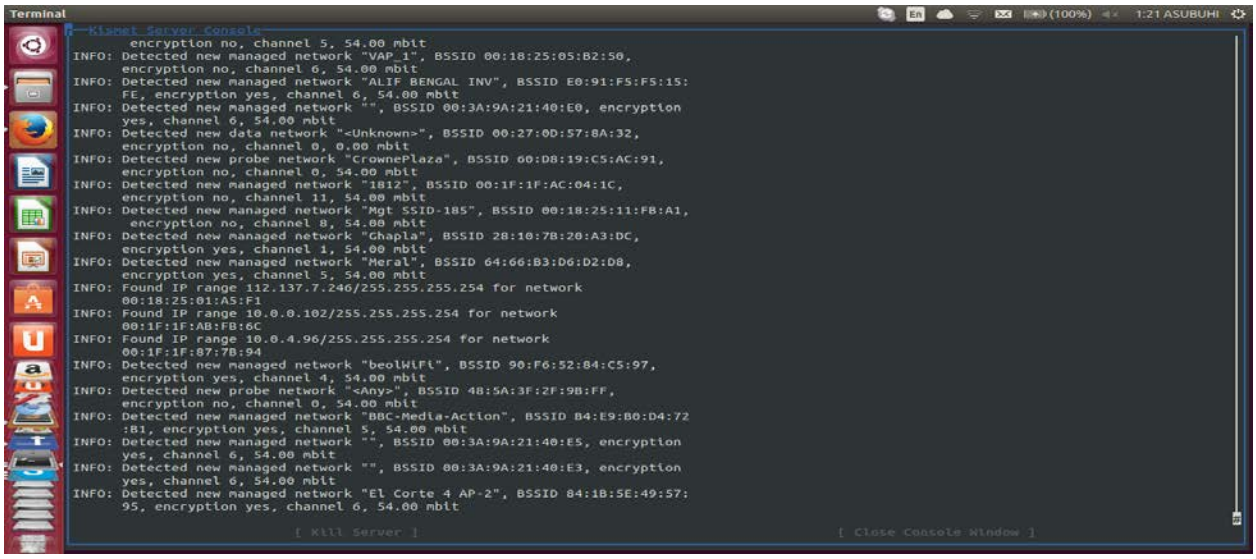


Figure 3.c: Hidden network interfaces

Chapter- 4

4.1 PRTG

PRTG is a user-friendly network monitoring software planned to provide real time statistics of every aspects governing within your network. It provides resource availability monitoring, bandwidth monitoring and usage monitoring

The PRTG Traffic Grapher is a Microsoft Windows software tool for monitoring and classifying traffic bandwidth use. It suggest a trouble-free, easy-to-learn interface and provides system administrators with live readings and long-term use trends for their network devices. The PRTG Traffic Grapher is most commonly used for bandwidth management, but its sensor technology can also be used to:

- Record the amount of data flowing in and out of Simple Network Management Protocol (SNMP)–enabled network components using the Internet MIB-2 standard
- Examine all data packets passing a computer's network interface card (packet sniffing)
- Incorporate bandwidth use data sent by Cisco routers using the NetFlow Version 5 protocol

The packet sniffer and NetFlow-based monitoring capabilities of the PRTG Traffic Grapher provide the capability to classify traffic by protocol, IP address, and MAC address.

Network and bandwidth monitoring data can be accessed through a Microsoft Windows GUI or through a web-based front end (Figure 4.a). The Microsoft Windows user interface provides easy access to data retrieval and configuration functions. In addition, an improved integrated web server is available to provide read-only remote access to collected data.

Monitoring results are presented in a variety of graphs and tables:

- Live data for the past 5 to 60 minutes
- 1- to 60-minute averages for up to 48 hours
- Hourly averages for up to 60 days
- Daily averages for up to 365 days
- Top talkers, top protocols, and top connections

Graphs are generated in real time for live reporting. The monitoring engine is capable of monitoring several thousand sensors. The six different live reporting views are:

- Data
- Events
- Sensors
- Custom
- Reports
- Browser

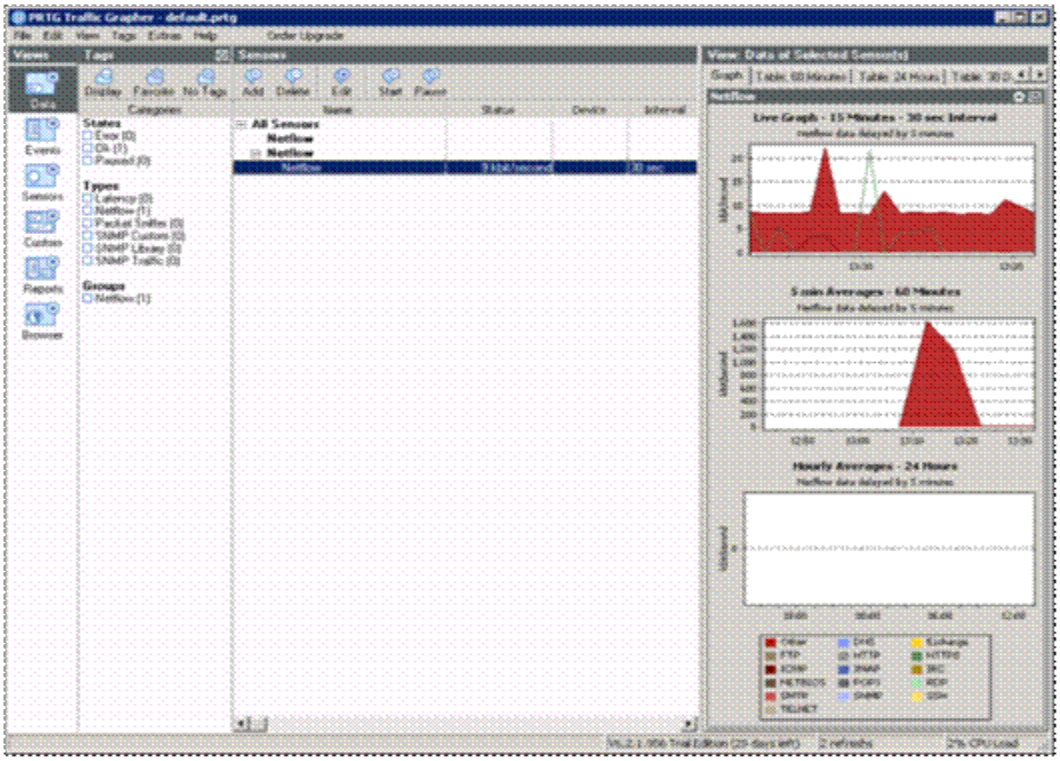


Figure 4.a: The PRTG Traffic Grapher User Interface

4.2 The PRTG Traffic Grapher User Interface

The software is available through various licensing options, for both freeware and commercial use. The freeware edition is free for personal and commercial use, but is limited to monitoring a maximum of 10 sensors (SNMP or packet sniffer–based only). To monitor more than 10 sensors or use NetFlow-based monitoring, a commercial edition must be purchased. Commercial editions offer additional features, which vary by edition:

- Monitoring of more devices and more ports and interfaces
- NetFlow collectors

A full-featured commercial version is available on a trial license for 30 days. Considering the time needed to execute a PoC effort, the 30-day trial is probably adequate if the PoC installation and tests are timed efficiently. A license can be obtained at http://www.paessler.com/prtg6/trial. Note that a commercial version is required to monitor NetFlow traffic.

In a NetFlow environment, the bandwidth use for all packets traversing a router can be monitored. For each flow of data, the router sends a NetFlow packet containing connection and bandwidth information to the monitoring system that is running the PRTG Traffic Grapher. In the PRTG Traffic Grapher, a NetFlow collector is configured to accept these packets and perform the accounting. The advantage of NetFlow is that it requires little additional CPU overhead on the router itself: 10,000 active flows create about a 7 percent additional CPU load; 45,000 active flows account for about a 20 percent additional load. In addition to configuring the monitoring system, it is necessary to configure the routers or switches to forward data to the collectors.

Deploying the PRTG Traffic Grapher for a Cisco WAAS Proof of Concept

The topology in Figure 4.b depicts the deployment of the PRTG Traffic Grapher and NetFlow for a Cisco WAAS PoC.[20]

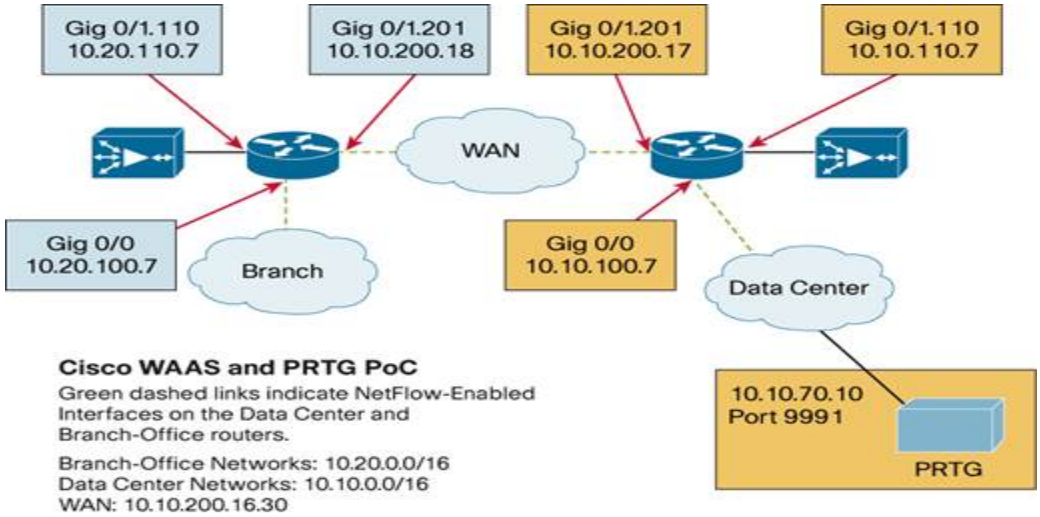


Figure 4.b: PoC Lab Topology

4.3 What is a Sensor?

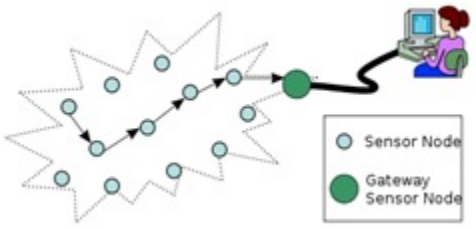


Figure 4.c: Sensor

Sensor uses for monitoring network in PRTG. Monitoring a device or service needs a sensor. The list of available sensor types is extensive covering everything from simple ping and port checks to HTTP, Web Service, SNMP, Windows/WMI, Linux/Unix/OS X, Virtual Server, Mail Servers, SQL, File, VoIP, QoS, and Hardware. The most interesting sensor type is the “Custom Sensor” type. If, for some reason, there is something we need to monitor that is not in their list of built-in sensors, it is here that we can create custom scripts or executables to do whatever we want.

There are two modes the scripts can run under: Standard and Advanced. Standard scripts support a single channel (or data point).

4.4 PRTG Probes

On a "probe", the sensors for a device perform the actual monitoring. The probe receives its configuration from the Core Server, runs the monitoring processes and delivers monitoring results back to the Core Server. A Core Server always has a local probe running on the same server. Additionally, a Core Server can manage an unlimited number of remote probes in order to achieve multiple location monitoring.

The authentic monitoring is performed by PRTG Probe processes which run on one or more computers. Through installation the self-styled "local probe" is automatically created by the system. In a single-probe installation, which is the default setup for all monitoring is performed by the local probe. Additionally, supposed "remote probes" must be created by the user. They are using SSL secured connections to the core and allow to securely monitoring services and systems inside remote networks which are not openly accessible or secured by firewalls. The following chart shows an example:

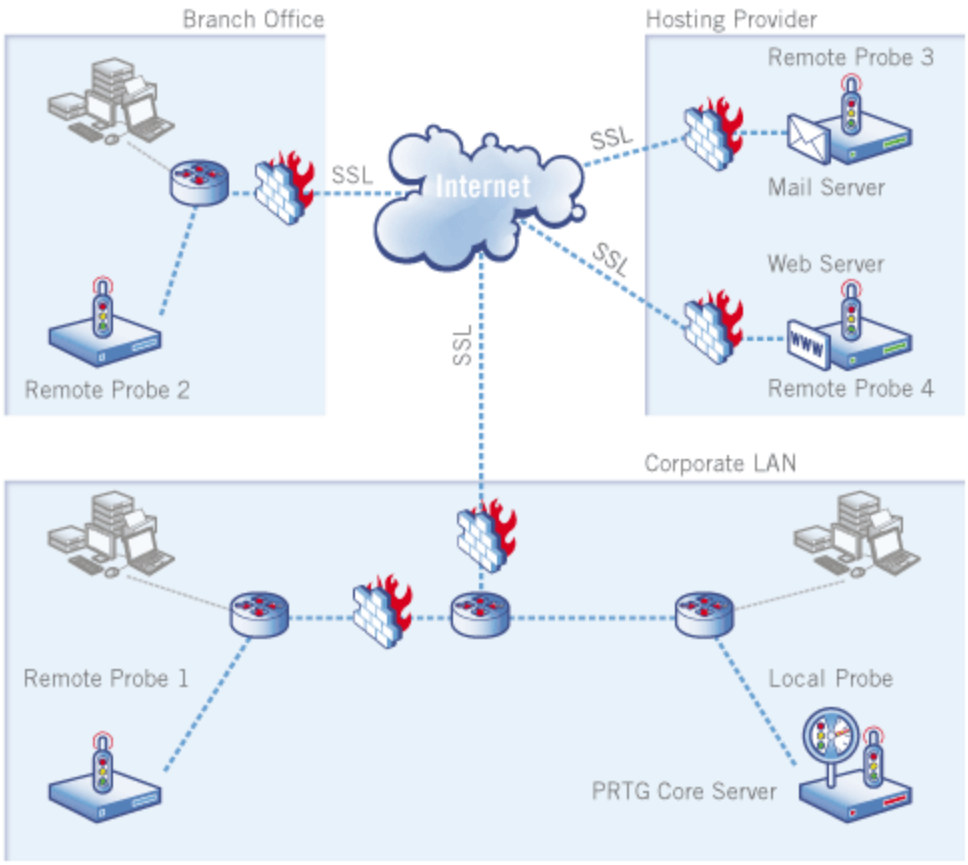


Figure 4.d: PRTG work pattern

4.5 PRTG API :

PRTG API helps us by giving a demo site setup, When we don't have any product installed in our PRTG monitoring system. The API covers following functional areas.

- Live data about properties, settings, and status information.
- Live Graphs are rendered as PNG files and can be used in other WebPages.
- Historic data can be downloaded for the historic monitoring for one sensor in XML or CSV format.
- Object Manipulation can be occurred in the system.

4.6 Flexible Alerting in PRTG:

In PRTG, alerting notification can be created for all users if they want to do something beyond their built-in support for Email, SMS/Pager, syslog, SNMP Traps, HTTP requests, Event log entries, alarm sound files and Amazon SNS.

4.7 Custom Alerting

PRTG allows its users to write their own custom programs that the notifications will run when a notification needs to occur. This is configured in the "Execute Program" section of the Notification configuration as shown below.[21]

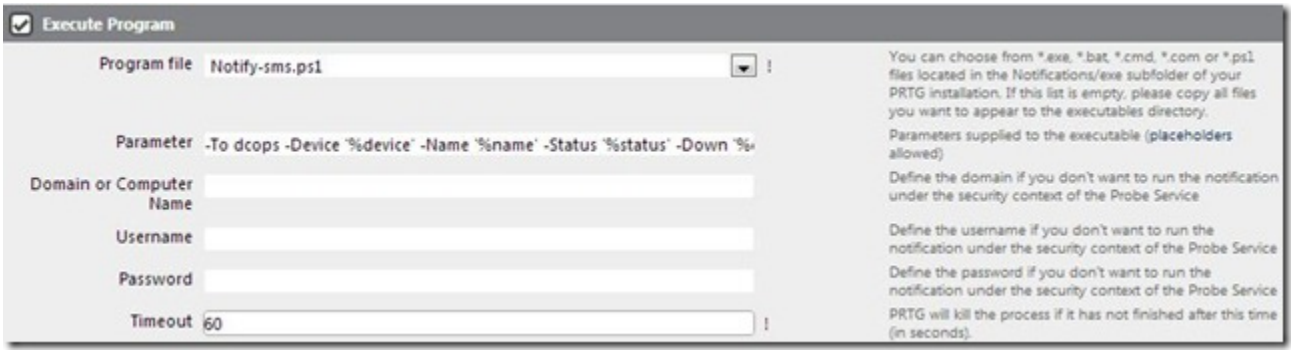


Figure 4.e: Execute Program

4.8 ERROR in PRTG

These are the common error messages displayed by PRTG sensors.

Error Message 1:

This particular error message describes that all DCOM communication protocols in the port are blocked over router. RPC server monitoring machine can be affected by

- firewall blockage
- domain policies blockages
- and running process

To avoid this error we need to

- Check the machine when it is powered on.
- Check the windows firewall of the monitored machine. If it is turned on, need to turn it off.
- Check for the domain policies governing the machine being monitored.

Error Message 2:

Access denied errors are generally caused by insufficient access permissions.
Solution:

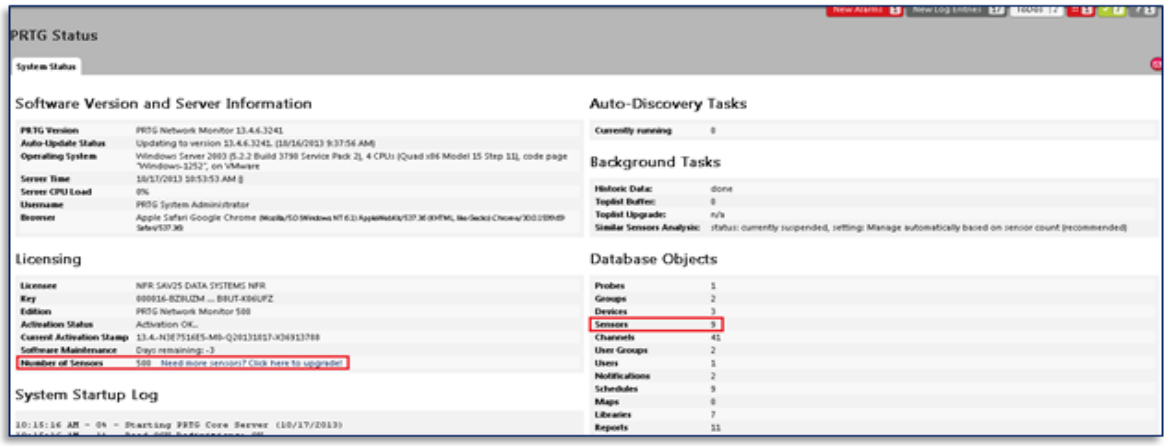
- Check for the Windows/SNMP identification under device settings. The computer name, username, and password should be correct.

Error Message 3:

The sensor is paused. When the sensor is paused, monitoring is disabled therefore no data will be acquired.
Solution:

- Restart the sensor

- If resuming the sensor didn't worked. Need to check license agreement; sensors are automatically paused when the maximum number of sensors allowed in license has been reached. To check for the total number of sensors allowed by the license and the total number of sensors used, navigate to:
  Setup > PRTG Status > System Status

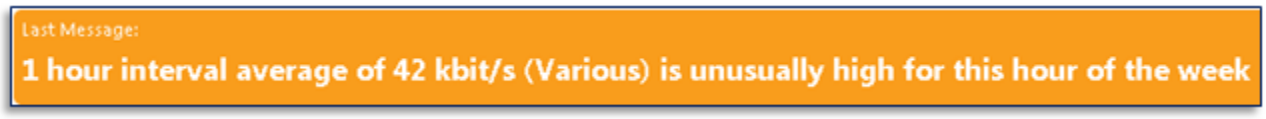


Error Message 4:

This error means no response to the ping attempt was received within a specified period of time. This error message is commonly displayed by ping sensors (ping, remote ping, multi-ping)
To avoid this error-

- Need to check for the physical connection of the device being monitored. Devices outside the network often show Request Timed Out errors.

Error Message 5:



Rather than an error message, this is actually a message signifying unusual state. When the sensor returns an unusual state, it means that the usage for a specific period of time exceeded that of the average consumption for the same period in previous days
To avoid this-

- Sensor will automatically return to normal state when conditions stabilize.
- Neglect this warning message if heavy traffic is expected.

4.9 MONITORING with PRTG:

PRTG is an open source tool for network assessment, so there should be some identifiable monitoring sensors to overview the network. Some of them is given below-

Firewall Monitoring:

PRTG Network Monitor provides a variety of sensors, for example SNMP, Netflow or Sensor, that makes monitoring any system's Firewall easy. To find out what is happening with one's internet connection at real time, **Firewall Monitoring** can be used. The firewall monitor of PRTG:

- Increases network security
- Shows outgoing and incoming traffic
- Easy to set up and configure
- Helps to Control Internet Usage.

Bandwidth Monitoring:

Bandwidth monitoring involves tracking the bandwidth usage of leased lines, network connections, network devices (routers, switches, etc.) and the like. This way, bandwidth monitoring software such as PRTG Network Monitor helps to monitor bandwidth-

- measure the actual amount of bandwidth being used (e.g. for billing purposes)
- proactively trace usage trends, bottlenecks, and connectivity errors
- make informed decisions on how to balance and route network traffic and decide what purchases are necessary to improve the flow of data within the network.
- Furthermore, a bandwidth monitoring software can also be used to alert administrators whether there are network load issues or breached bandwidth thresholds, etc.

Better network management is performed well by understanding bandwidth and resource consumption:

- Avoid bandwidth and server performance bottlenecks
- Find out what applications or what servers are using up your bandwidth
- Deliver better quality of service to your users by being proactive
- Reduce costs by buying bandwidth and hardware according to actual load

Netflow monitoring:

NetFlow monitoring shows:

- where bandwidth is used
- who is using it
- how it is being used
- why it is being used

It shows which specific applications are being used and how the usage might affect any network.

NetFlow monitoring is included in all PRTG Network Monitor licenses.
Cisco devices with NetFlow Support track the bandwidth usage of the network internally. The NetFlow protocol is supported by most Cisco routers and certain Cisco switches. These devices can be configured to send pre-aggregated data to the computer running a NetFlow monitor such as PRTG Network Monitor. Since the data is pre-aggregated, this is easier on the system than using the packet sniffer functionality. This makes NetFlow monitoring ideal for tracking bandwidth usage on high traffic networks.

Packet sniffing:

Packet sniffing is used within a network in order to capture and register data flows. Packet sniffing allows you to discern each individual packet and analyze its content based on predefined parameters. **Packet sniffing** allows for very detailed network monitoring and bandwidth usage analysis. However, a broader knowledge of networks and their inner functions is needed, in order to be able to recognize the relevance of the data being monitored.

Advantages of Packet Sniffing:

With addition to normal bandwidth monitoring capabilities based on SNMP, PRTG allows administrators to find out actual bandwidth usage based on multiple parameters, such as source and destination IP addresses, MAC addresses, port numbers, protocols, etc., using packet sniffing. Moreover, PRTG's packet sniffing functionality can be used to generate top lists, which enable administrators to recognize detailed usage trends, sources and destinations of individual communications via the network, as well as the details of the traffic flowing within said network.

Router Monitoring:

PRTG Network Monitor is a comprehensive network monitoring software with a wide range of router monitoring possibilities. Just choose one of the supported technologies, and you will be able to monitor router traffic and see network usage 24/7. If unusual behavior is detected, the software will alert you right away. This lets you troubleshoot problems before others are affected.

Usage Monitoring

To identify causes for bandwidth bottlenecks that are not caused by faulty systems Usage Monitoring is essential but an excessive bandwidth usage by single servers or users. Usage monitoring software such as PRTG Network Monitor analyzes the traffic in your network and provides you with detailed information on usage and activity. The results of the usage monitoring can be total bandwidth (e.g. flowing through a port of a switch) or drilled down to protocols.

Uptime Monitoring:

The term "uptime" is used to determine the time a computer system has been functional. In network terms it is defined by the availability of a server, device or site. In individual computer terms it is defined by the reliability and stability of the individual system. Networks require several reliable devices in order to work properly. **Uptime monitoring** software controls and monitors the availability of each single device and alerts the administrator when a system fails - usually through email or SMS. Uptime monitoring software can also be used to determine where issues may arise in future within a network and to proactively monitor the activity within said network, allowing administrators to balance loads or to consider purchasing options and plan upgrades. The simplest way is to use PING sensors at specified intervals. Good monitoring solutions offer many more sensor types for uptime monitoring so that services, websites, and applications can also be checked for uptime statistics.

Network Monitoring:

Network monitoring can be divided into two parts.

1. SQL Monitoring:

A good SQL Server solution offers the following benefits:

- Increased profits: no losses caused by undetected database failures.
- Improved customer satisfaction by providing reliable access to databases.
- This SQL Server monitoring solution installs easily and its usage is intuitive. Additional features like remote management (via web browser, Pocket pc, or Windows client) and notifications about SQL Server errors by email, ICQ, pager/SMS make the monitoring of SQL Servers easier.

2. Website Monitoring:

- Your website and network need to work well. Slow performance causes lost sales.
- Your network administrators need to know the status of all their websites to ensure that everything is working correctly.
- PRTG Network Monitor provides continuous website monitoring and automated alerts, not only if the website goes down, but also if it slows to respond.
- PRTG avoids losses caused by website failures and slow performance, and enhances customer satisfaction by ensuring 100% uptime with fast, reliable access to the website.

VoIP Network Monitoring:

- PRTG Network Monitor includes a powerful QoS ("Quality of Service") sensor. This sensor measures parameters such as:
- jitter,

- network latency
- packet loss
- PRTG allows you to see the quality of your VoIP connection at a glance and warns you when quality deteriorates. This is useful while troubleshooting the VoIP network even before users are affected by VoIP specific connection problems (echo, noise or breaks in the conversation). To set up VoIP network monitoring with QoS sensor, it is only required to put a remote probe on both ends of the connection and measure the connection quality between them. [22]

4.10 Practical Monitoring:

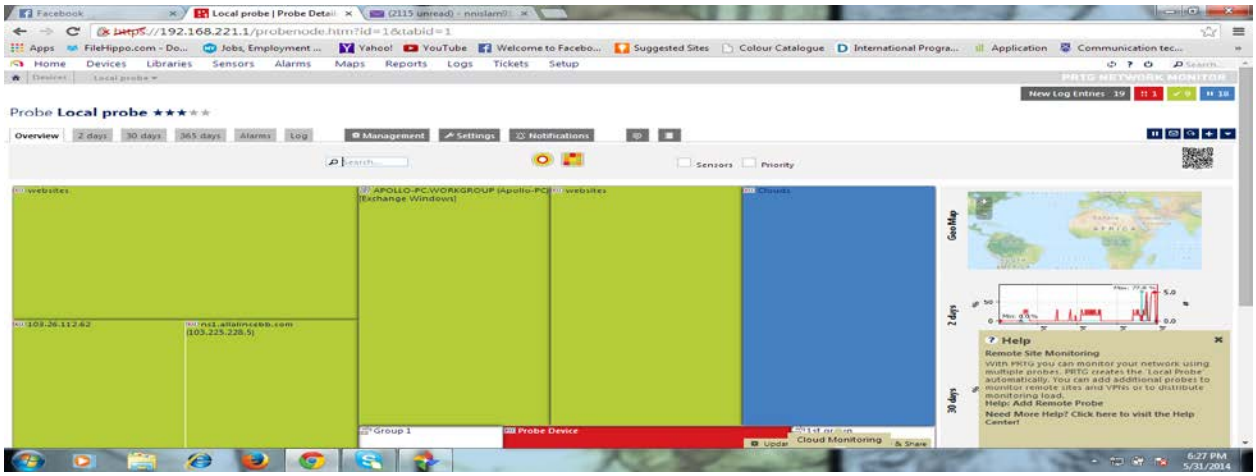


Figure 4.f: Total Local Probe

Figure 4.g: Local probe graph

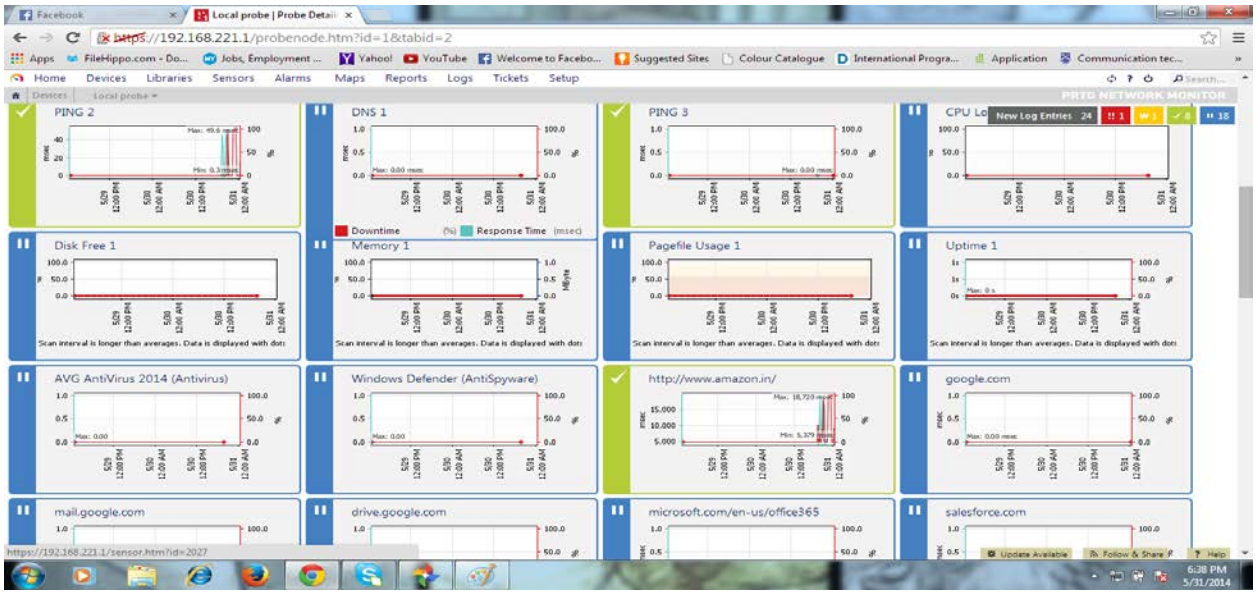


Figure 4.h: Entire local probe with all the sensors

Figure 4.i:sensor up with ok massage

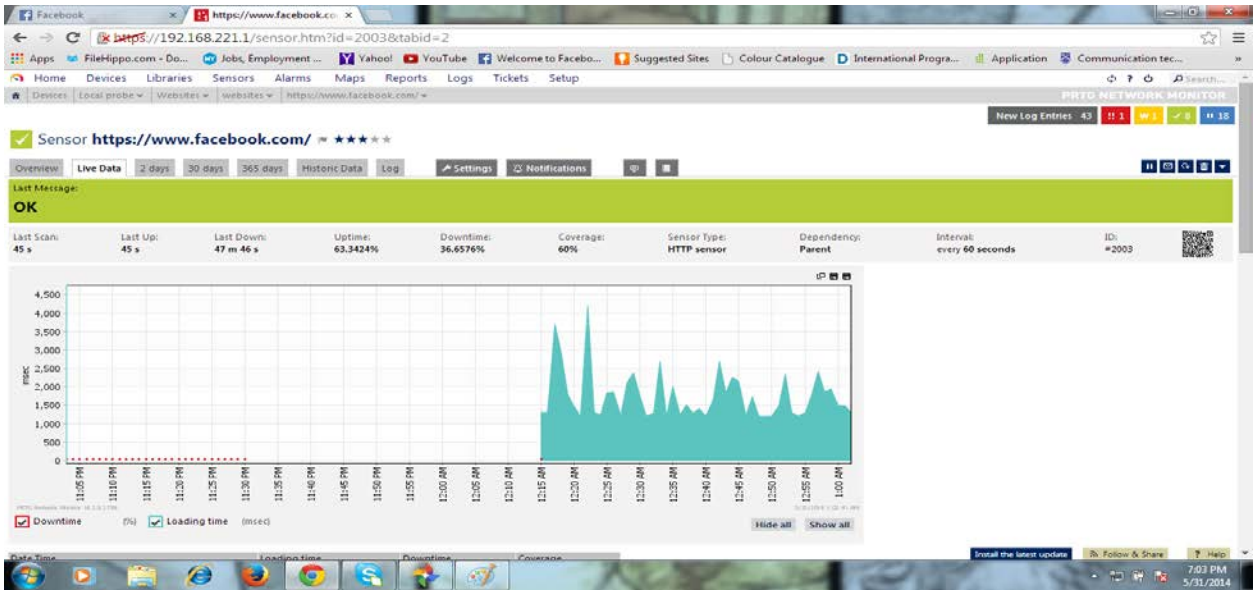


Figure 4.j: Ok massage

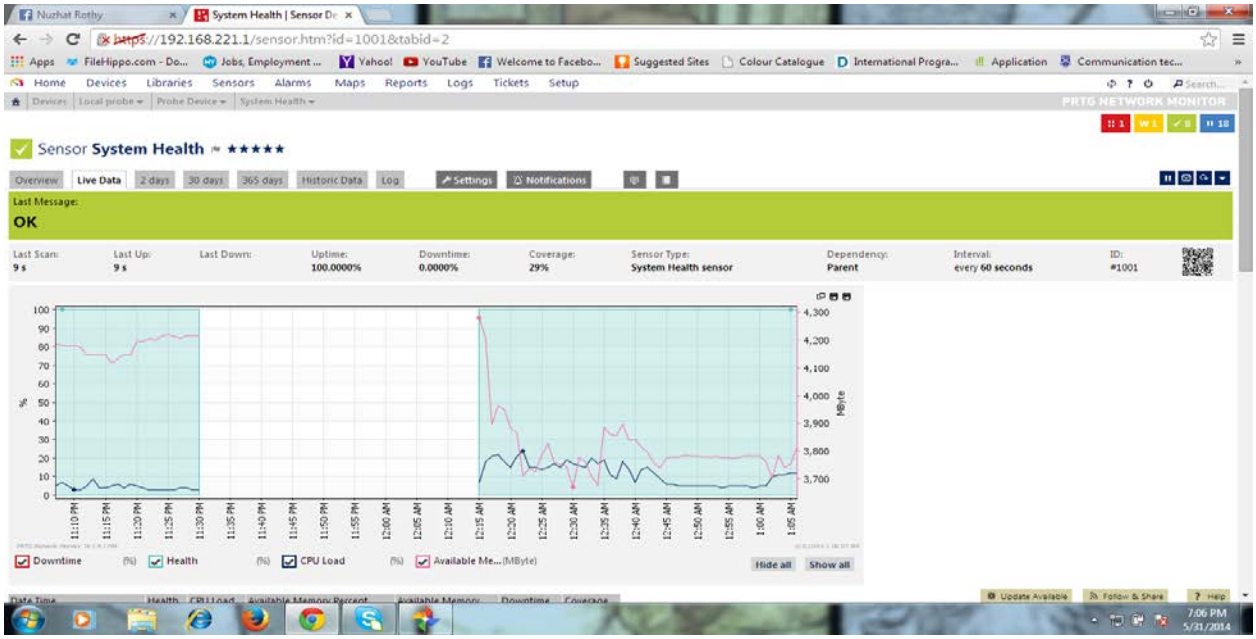


Figure 4.k: Ok massage with time difference

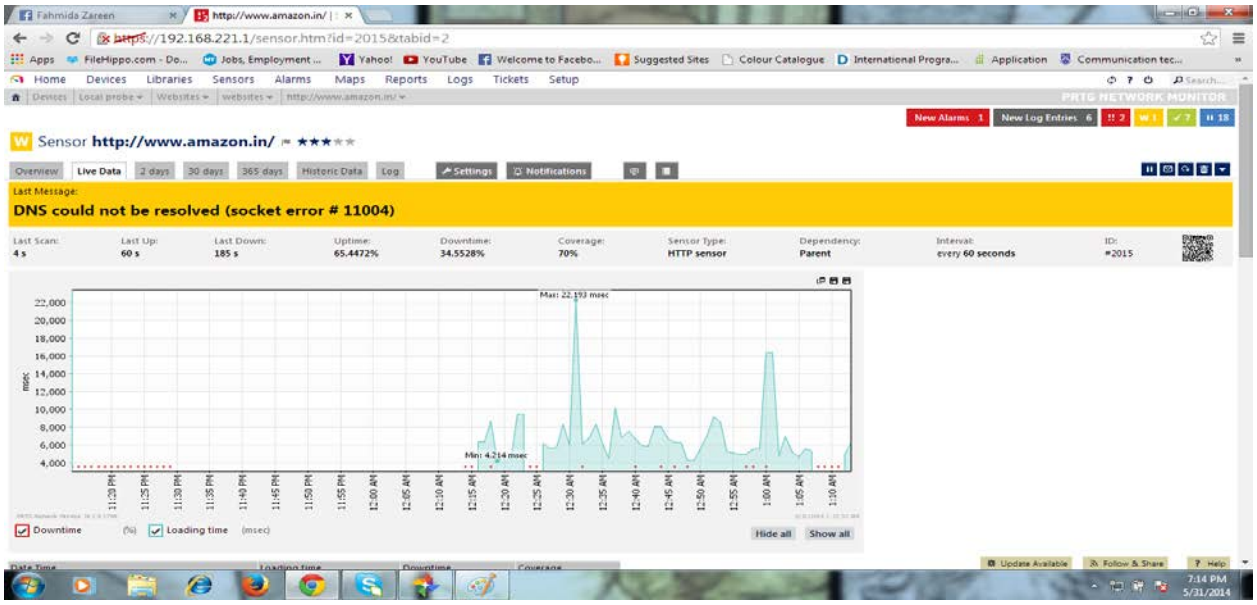


Figure 4.l: Error 1 where DNS could not be resolved

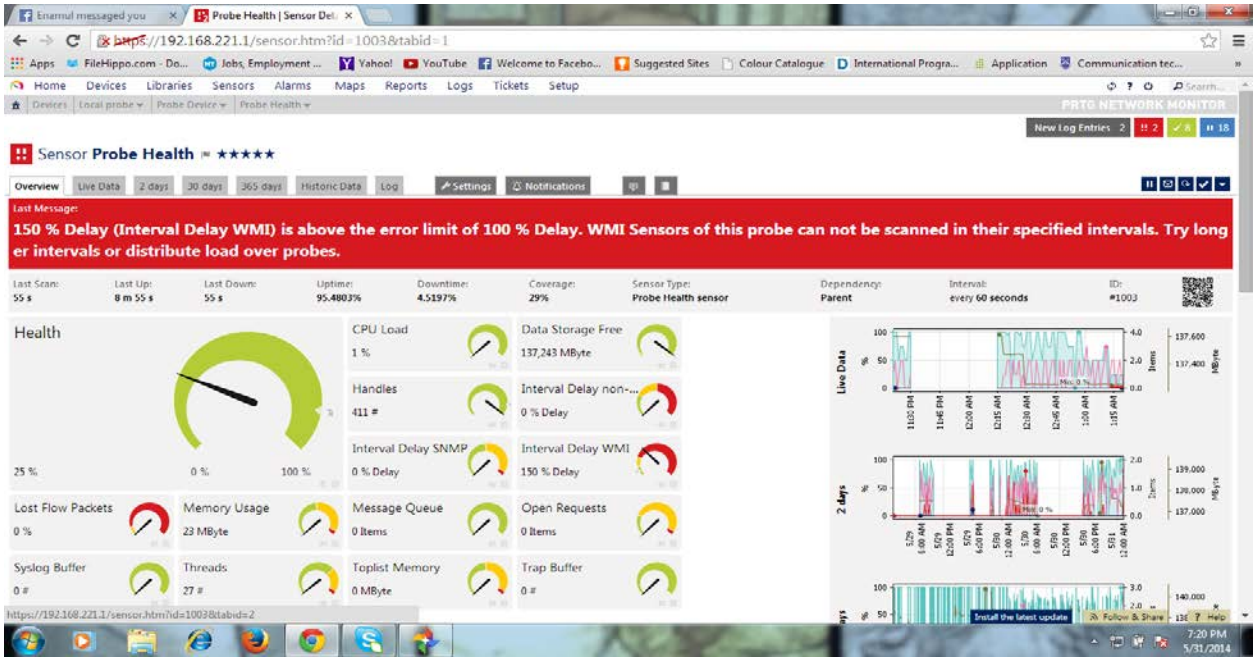


Figure 4.m: Error 2 with 150 percent delay where WMI sensors of this probe cannot scanned in their specified intervals

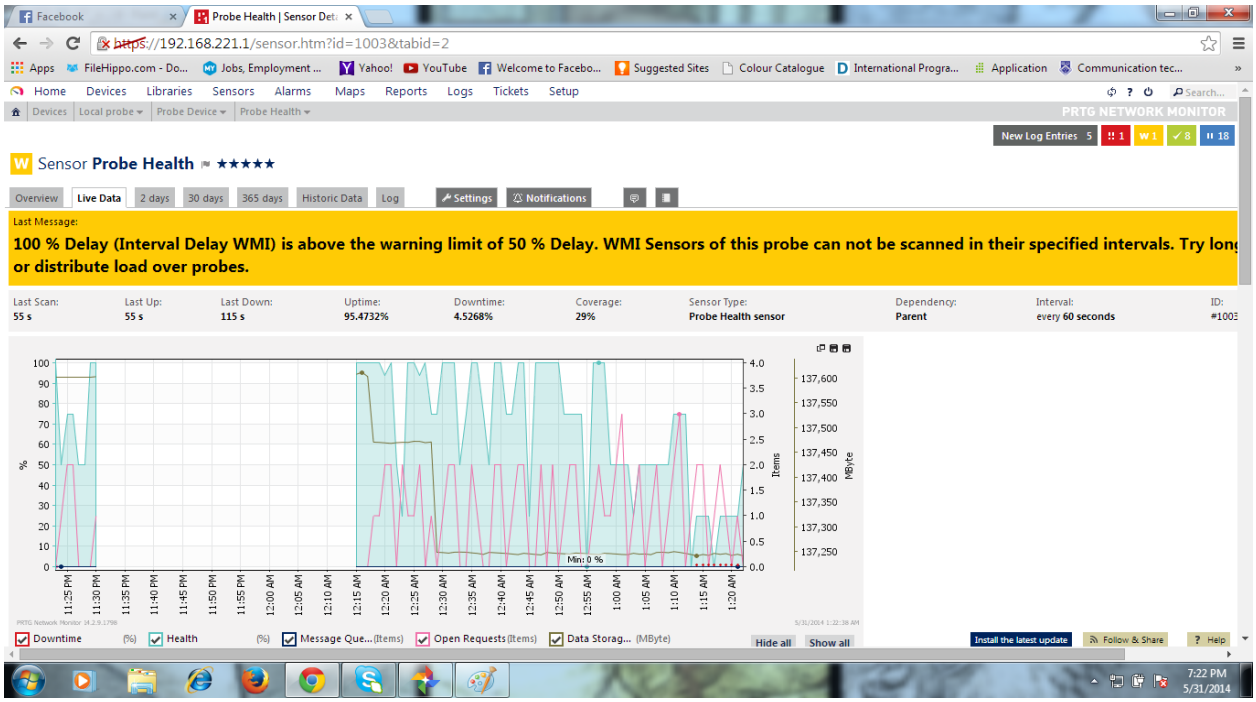
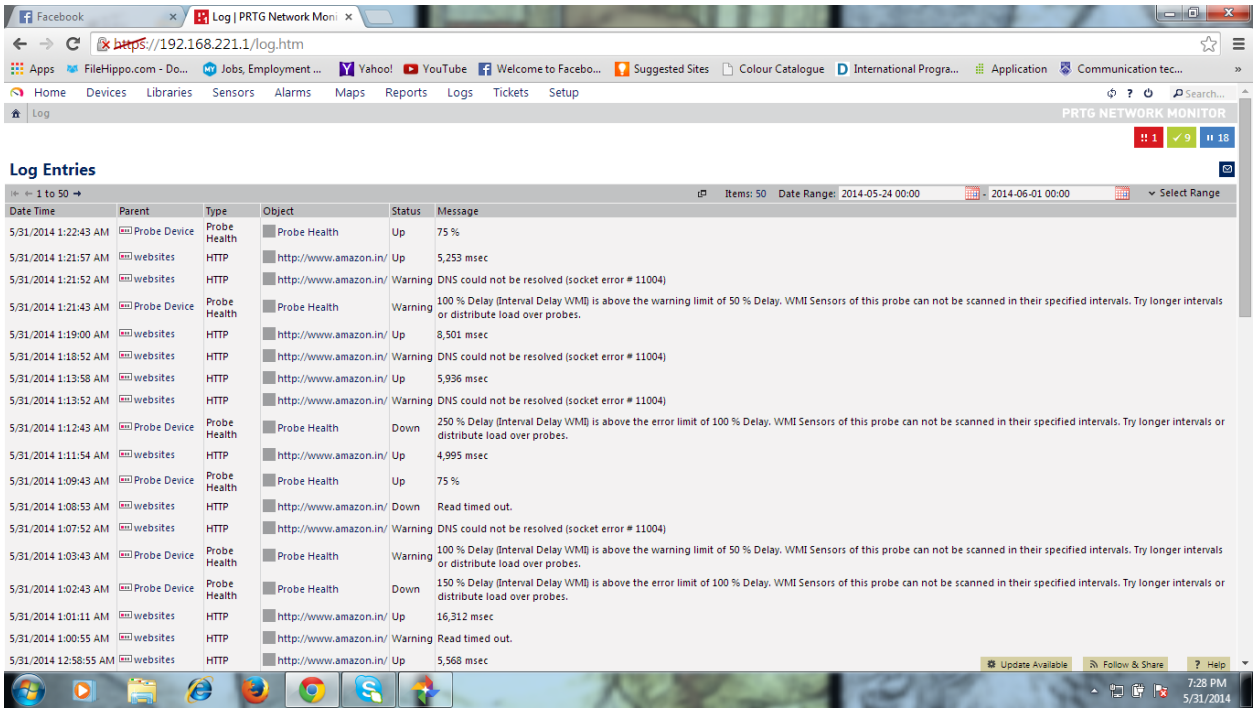


Figure 4.n: Error 3 100 percent delay where des 50 delay limit is 50 percent



Date Time	Parent	Type	Object	Status	Message
5/31/2014 1:22:43 AM	Probe Device	Probe Health	Probe Health	Up	75 %
5/31/2014 1:21:57 AM	websites	HTTP	http://www.amazon.in/	Up	5,253 msec
5/31/2014 1:21:52 AM	websites	HTTP	http://www.amazon.in/	Warning	DNS could not be resolved (socket error # 11004)
5/31/2014 1:21:43 AM	Probe Device	Probe Health	Probe Health	Warning	100 % Delay (Interval Delay WMI) is above the warning limit of 50 % Delay. WMI Sensors of this probe can not be scanned in their specified intervals. Try longer intervals or distribute load over probes.
5/31/2014 1:19:00 AM	websites	HTTP	http://www.amazon.in/	Up	8,501 msec
5/31/2014 1:18:52 AM	websites	HTTP	http://www.amazon.in/	Warning	DNS could not be resolved (socket error # 11004)
5/31/2014 1:13:58 AM	websites	HTTP	http://www.amazon.in/	Up	5,936 msec
5/31/2014 1:13:52 AM	websites	HTTP	http://www.amazon.in/	Warning	DNS could not be resolved (socket error # 11004)
5/31/2014 1:12:43 AM	Probe Device	Probe Health	Probe Health	Down	250 % Delay (Interval Delay WMI) is above the error limit of 100 % Delay. WMI Sensors of this probe can not be scanned in their specified intervals. Try longer intervals or distribute load over probes.
5/31/2014 1:11:54 AM	websites	HTTP	http://www.amazon.in/	Up	4,995 msec
5/31/2014 1:09:43 AM	Probe Device	Probe Health	Probe Health	Up	75 %
5/31/2014 1:08:53 AM	websites	HTTP	http://www.amazon.in/	Down	Read timed out.
5/31/2014 1:07:52 AM	websites	HTTP	http://www.amazon.in/	Warning	DNS could not be resolved (socket error # 11004)
5/31/2014 1:03:43 AM	Probe Device	Probe Health	Probe Health	Warning	100 % Delay (Interval Delay WMI) is above the warning limit of 50 % Delay. WMI Sensors of this probe can not be scanned in their specified intervals. Try longer intervals or distribute load over probes.
5/31/2014 1:02:43 AM	Probe Device	Probe Health	Probe Health	Down	150 % Delay (Interval Delay WMI) is above the error limit of 100 % Delay. WMI Sensors of this probe can not be scanned in their specified intervals. Try longer intervals or distribute load over probes.
5/31/2014 1:01:11 AM	websites	HTTP	http://www.amazon.in/	Up	16,312 msec
5/31/2014 1:00:55 AM	websites	HTTP	http://www.amazon.in/	Warning	Read timed out.
5/31/2014 12:58:55 AM	websites	HTTP	http://www.amazon.in/	Up	5,568 msec

Figure 4.o: Total Log entries in PRTG

Chapter -5

5.1 Nagios

Nagios is a powerful network, open computer system, enterprise-class host, service and infrastructure monitoring software application. Nagios offers monitoring and alerting services for servers, switches, applications, and services. It alerts the users when things go wrong and alerts them a second time when the problem has been resolved. Alerts can be delivered via email, SMS, or pager /(custom script).[23]

Nagios is a stable, scalable and extensible enterprise-class network and system monitoring tool which has the following functions:

- Monitoring of network services (SMTP, POP3, HTTP, NNTP, etc.).
- Monitoring of host resources (processor load, disk usage, etc.).
- Simple plug-in design that allows administrators to develop further service checks.
- Support for redundant Nagios servers.

A host can be reached only if a service is running on it. Therefore, everything in Nagios revolves around service checks. After all, no service can run without a host. If the host computer fails, it also cannot provide the desired service.

Things get slightly more complicated if a router, for example, is brought into play, which lies between users and the system providing services. If this fails, the desired service may still be running on the target host, but it is nevertheless no longer reachable for the user.

Nagios precisely informs the administrator of the failure of an important network component, instead of flooding the administrator with irrelevant error messages concerning services that cannot be reached.

Another important item is the *state* of a host or service. On one hand Nagios allows a much finer distinction than just "ok" or "not ok"; on the other hand the distinction between (*soft state*) and (*hard state*) means that the administrator does not have to deal with short-term disruptions that have long since disappeared by the time the administrator has received the information. These states also influence the intensity of the service checks.

How Nagios handles dependencies of hosts and services can be best illustrated with an example. Figure 5.a represents a small network in which the Domain Name Service on proxy is to be monitored.

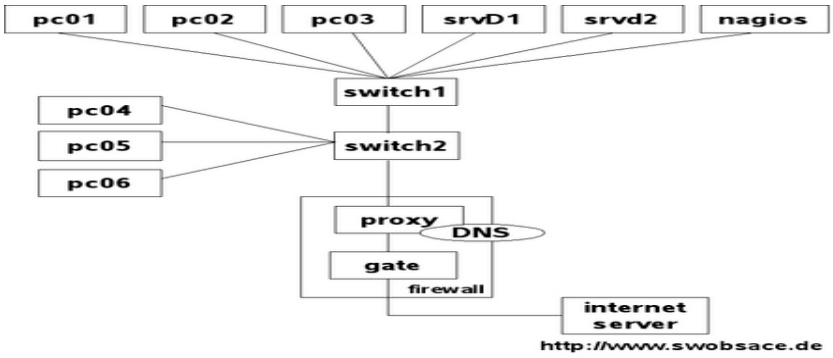


Figure 5.a: Topology of an example network

The service check always serves as the starting point for monitoring that is regularly performed by the system. As long as the service can be reached, Nagios takes no further steps; that is, it does not perform any host checks. For switch1, switch2, and proxy, such a check would be pointless anyway, because if the DNS service responds to proxy, then the hosts mentioned are automatically accessible.

If the name service fails, however, Nagios tests the computer involved with a host check, to see whether the service or the host is causing the problem. If proxy cannot be reached, Nagios might test the *parent* hosts entered in the configuration (Figure 5.b). With the parents host parameter, the administrator has a means available to provide Nagios with information on the network topology.

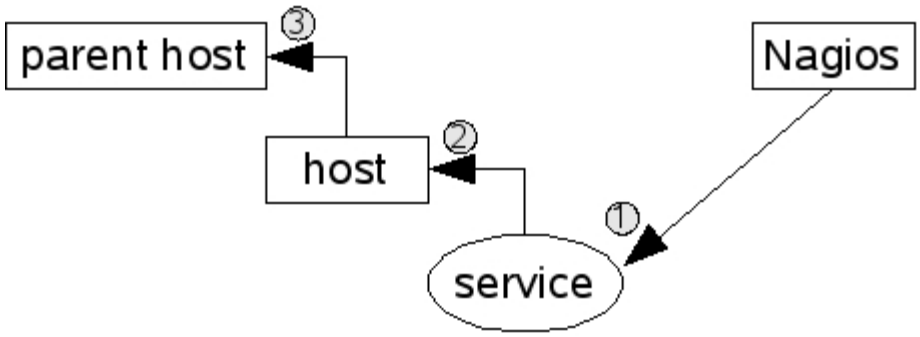


Figure 5.b: The order of tests performed after a service failure.

When doing this, the administrator only enters the direct neighbor computer for each host on the path to the Nagios server as the parent. Hosts that are allocated in the same network segment as the Nagios server itself are defined without a parent. For the network topology from Figure 5.b, the corresponding configuration (reduced to the host name and parent) appears as follows:

```
define host{
host_name  proxy
```

```
        ...

parents    switch2
}

define host{
host_name  switch2
  ...

parents    switch1
}

define host{
host_name  switch1
    ...
}
```

Switch1 is located in the same network segment as the Nagios server, so it is therefore not allocated a parent computer. What belongs to a network segment is a matter of opinion: if you interpret the switches as the segment limit, as is the case here, this has the advantage of being able to more closely isolate a disruption. But you can also take a different view and interpret an IP sub network as a segment. Then a router would form the segment limit; in this example, proxy would then count in the same network as the Nagios server. However, it would no longer be possible to distinguish between a failure of proxy and a failure of switch1 or switch2.

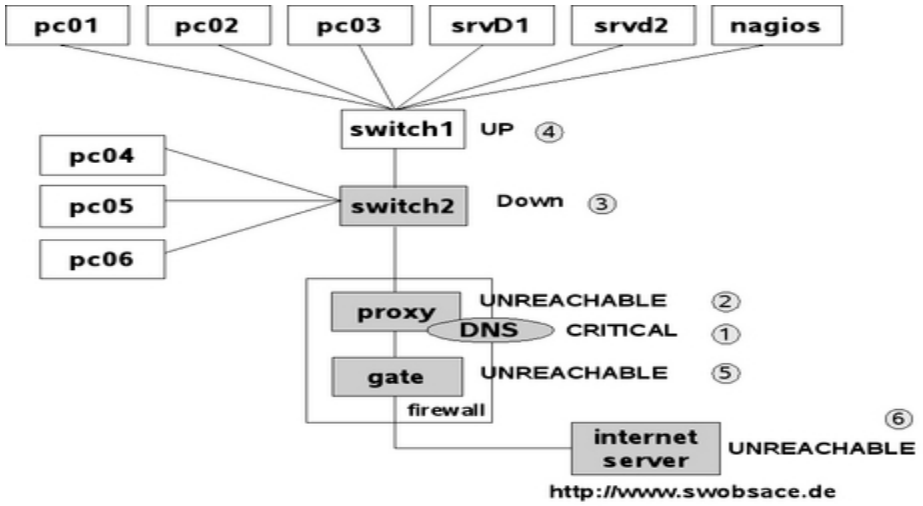


Figure 5.c: Classification of individual network nodes by Nagios.

If switch1 in the example fails, Figure 5.c shows the sequence in which Nagios proceeds: first the system, when checking the DNS service on proxy, determines that this service is no longer reachable (1). To differentiate, it now performs a host check to see what the state of the proxy computer is (2). Since proxy cannot be reached, but it has switch2 as a parent, Nagios also subjects switch2 to a host check (3). If this switch also cannot be reached, the system checks its parent, switch1 (4).

If Nagios can establish contact with switch1, the cause for the failure of the DNS service on proxy can be isolated to switch2. The system accordingly specifies the states of the host: switch1 is UP, switch2 DOWN; proxy, on the other hand, is UNREACHABLE. Through a suitable configuration of the Nagios messaging system.

In a further step, Nagios can determine other topology-specific failures in the network in the parent of gate, so gate is also represented as UNREACHABLE (5). Gate in turn also functions as a parent; the Internet server dependent on this is also classified as "UNREACHABLE".

This "intelligence", which distinguishes Nagios, helps the administrator all the more, the more hosts and services are dependent on a failed component. For a router in the backbone, on which hundreds of hosts and services are dependent, the system informs administrators of the specific disruption, instead of sending them hundreds of error messages that are not wrong in principle, but are not really of any help in trying to eliminate the disruption.

The parameter name parents can be explained by the fact that there are scenarios--such as in high availability environments--in which a host has two upstream routers that guarantee the Internet connection, for example

Forced Host Checks vs. Periodic Reach ability Tests:

Service checks are carried out regularly by Nagios, host checks only when needed. Although the check interval parameter provides a way of forcing regular host checks, there is no *real* reason to do this. There is one reason *not* to do this, however: continual host checks have a considerable influence on the performance of Nagios.

If administrator nevertheless want to regularly check the reach ability of a host, it is better to use a ping-based service check. At the same time he or she can obtain further information such as the response times or possible packet losses, which provides indirect clues about the network load or possible network problems. A host check, on the other hand, also issues an OK even if many packets go missing and the network performance is catastrophic. What is involved here--as the name "host check" implies--is only reach ability in principle and not the quality of the connection.[24]

5.2 States of Hosts and Services:

Nagios uses plug-in for the host and service checking for the network. They provide four different return values: O (OK), 1 (WARNING), 2 (CRITICAL), and 3 (UNKNOWN).
The return value UNKNOWN means that the running of the plug-in generally went wrong, perhaps because of wrong parameters. You can normally specify the situations in which the plug in issues a warning or a critical state when it is started.

Nagios determines the states of services and hosts from the return values of the plug-in. The states for services are the same as the return values OK, WARNING, CRITICAL and UNKNOWN. For the hosts the picture is slightly different: the UP state describes a reachable host, DOWN means that the computer is down, and UNREACHABLE refers to the state of non-reach ability, where Nagios cannot test whether the host is available or not, because a parent is down .

In addition to this, Nagios makes a distinction between two types of state: soft state and hard state. If a problem occurs for the first time (that is, if there was nothing wrong with the state of a service until now) then the program categorizes the new state initially as a soft state and repeats the test several times. It may be the case that the error state was just a one-off event that was eliminated a short while later. Only if the error continues to exist after multiple testing is it then categorized by Nagios as a hard state. Administrators are informed only of hard states, because messages involving short-term disruptions that disappear again immediately afterwards only add to an unnecessary flood of information.

In our example the chronological sequence of states of a service can be illustrated quite simply. A service with the following parameters is used for this purpose:

```
define service{
host_name               proxy
service_description     DNS
            ...

normal_check_interval   5
retry_check_interval    1
max_check_attempts      5

  ...
}
```

normal_check_interval specifies at what interval Nagios should check the corresponding service as long as the state is OK or if a hard state exists--in this case, every five minutes.

retry_check_interval defines the interval between two service checks during a soft state--one minute in the example. If a new error occurs, then Nagios will take a closer look at the service at shorter intervals.

max_check_attempts determines how often the service check is to be repeated after an error has first occurred. If max_check_attempts has been reached and if the error state continues, Nagios inspects the service again at the intervals specified in normal_check_interval.

Figure 5.d represents the chronological progression in graphic form: the illustration begins with an OK state (which is always a hard state). Normally Nagios will repeat the service check at five-minute intervals. After ten minutes an error occurs; the state changes to CRITICAL, but this is initially a soft state. At this point in time, Nagios has not yet issued any message.

Now the system checks the service at intervals specified in retry_check_interval, here this is every minute. After a total of five checks (max_check_attempts) with the same result, the state changes from soft to hard. Only now does Nagios inform the relevant people. The tests are now repeated at the intervals specified in normal_check_interval.

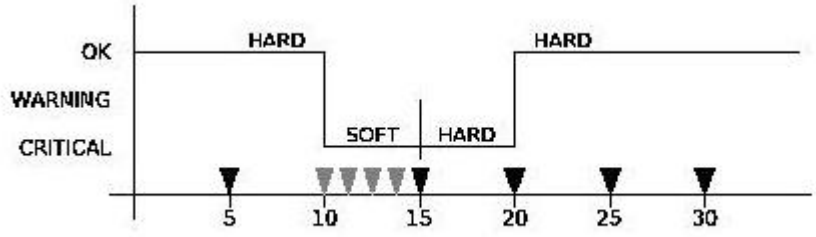


Figure 5.d: Example of the chronological progression of states in a monitored service

In the next test the service is again available; thus its state changes from CRITICAL to OK Since an OK state is always a hard state, this change is not subject to any tests by Nagios at shorter intervals.

The transition of the service to the OK state after an error in the hard state is referred to as a hard recovery. The system informs the administrators of this (if it is configured to do so) as well as of the change between various error-connected hard states (such as from WARNING to UNKNOWN). If the service recovers from an error soft state to the normal state (OK)--also called a soft recovery--the administrators will, however, not be notified.

Even if the messaging system leaves out soft states and switches back to soft states, it will still record such states in the Web interface and in the log files. In the Web front end, soft states can be identified by the fact that the value 2/5 is listed in the column Attempts, for example. This means that max_check_attempts expects five attempts, but only two have been carried out until now. With a hard state, max_check_attempts is listed twice at the corresponding position, which in the example is therefore 5/5.

More important for the administrator in the Web interface than the distinction of whether the state is still "soft" or already "hard", is the duration of the error state in the column Duration. From this a better judgment can be made of how large the overall problem may be.

For services that are not available because the host is down, the entry 1/5 in the column Attempts would appear, since Nagios does not repeat service checks until the entire host is reachable again. The failure of a computer can be more easily recognized by its color in the Web interface: the service overview in Figure6.e marks the failed host in red; if the computer is reachable, the background remains gray.[25]

5.3 Usefulness of Nagios:

- Plan for infrastructure upgrades before outdated systems cause failures
- Respond to issues at the first sign of a problem
- Automatically fix problems when they are detected
- Coordinate technical team responses
- Ensure any organization's SLAs are being met
- Ensure IT infrastructure outages have a minimal effect on their organization's bottom line
- Monitor entire infrastructure and business process of a network.[26]

5.4 For practical Monitoring system :

We followed this code which is given below-

```
define host{

use                 generic-host          ; Name of host template to use

host_namelocalhost

aliasLocalhost

address             127.0.0.1

    }
```

After using this we saw four states of nagios monitoring pattern OK, WARNING, CRITICAL, UNKNOWN.

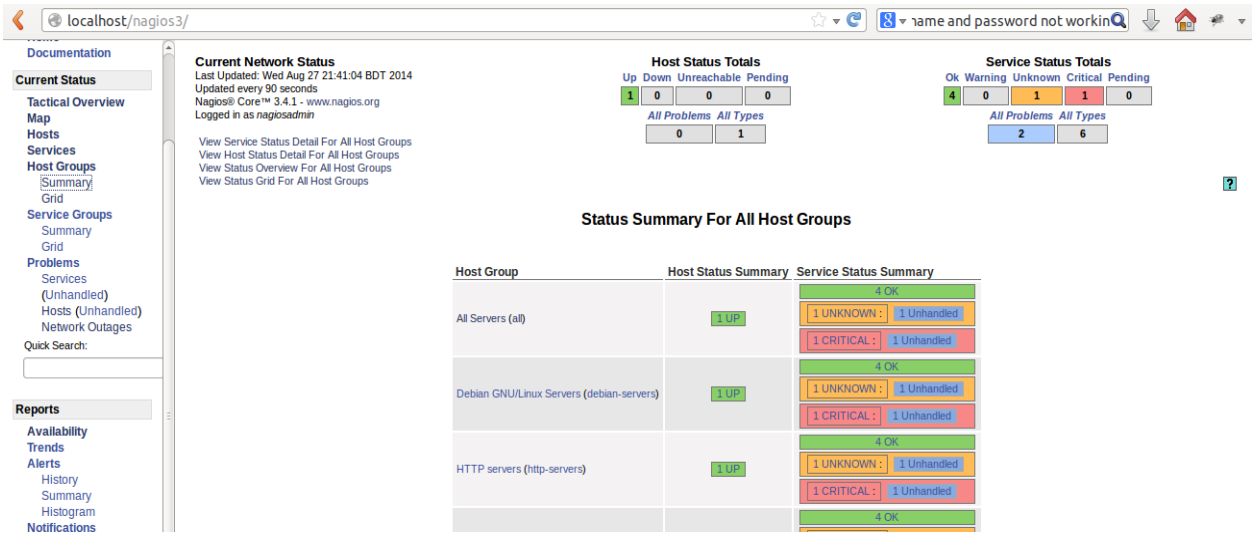


Figure 5.e : Status summery for all host

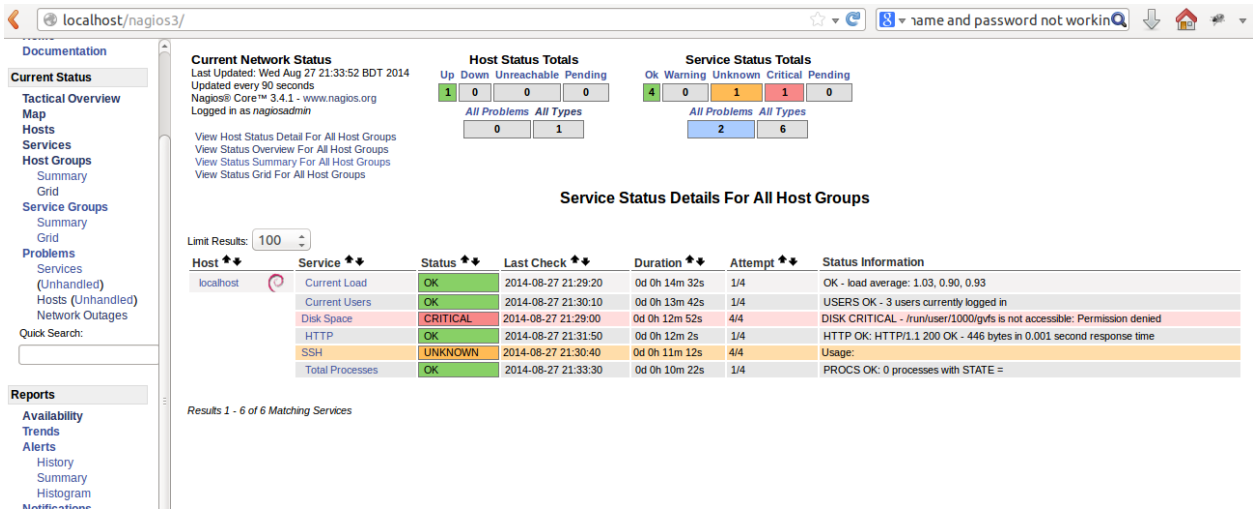


Figure 5.f : Service Status details for all host group

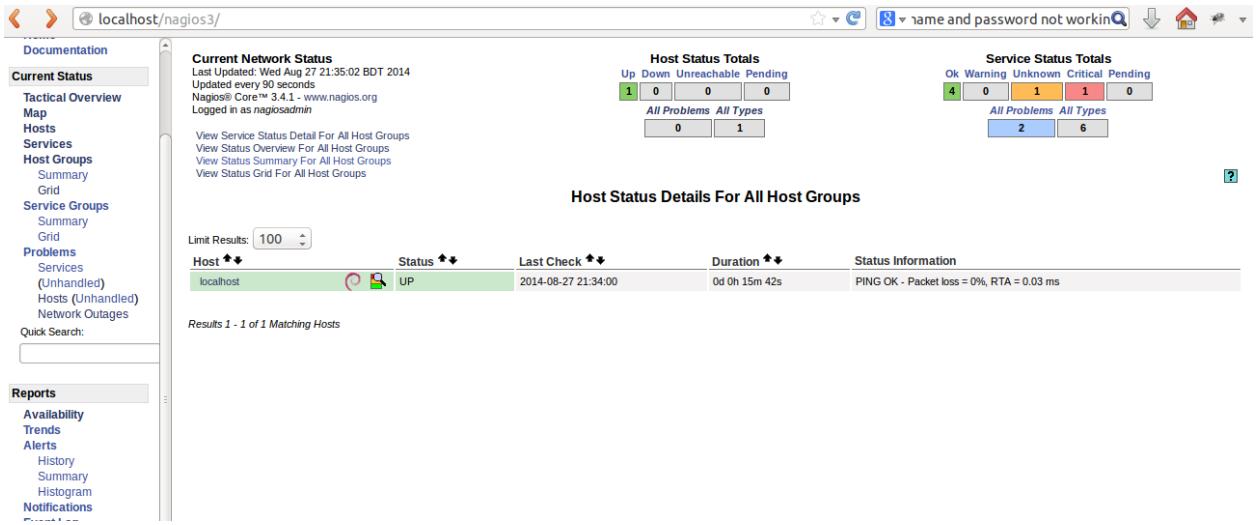


Figure 5.g : Host status summary

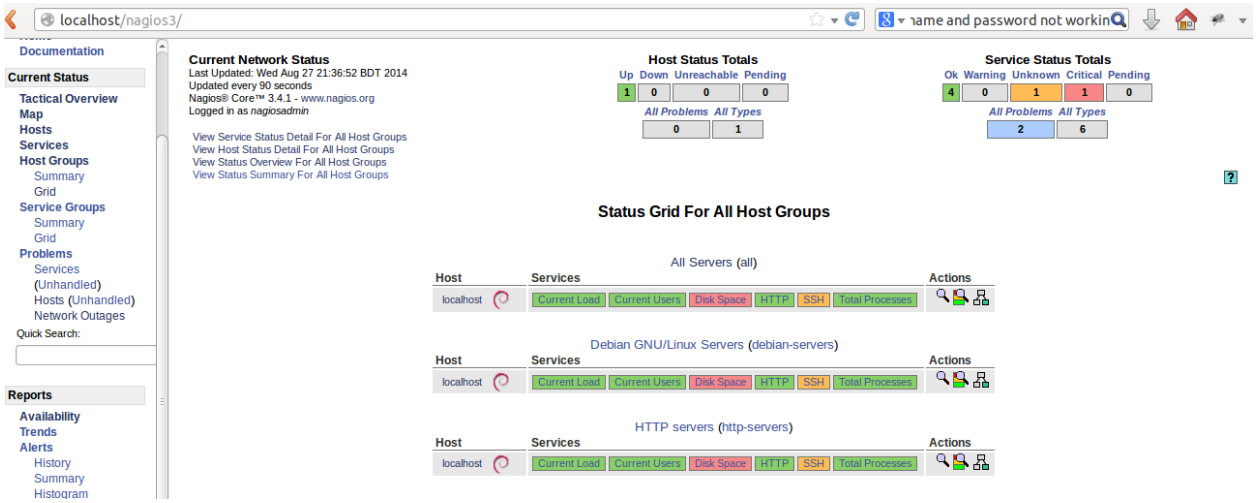


Figure 5.h: Status Grid for all host

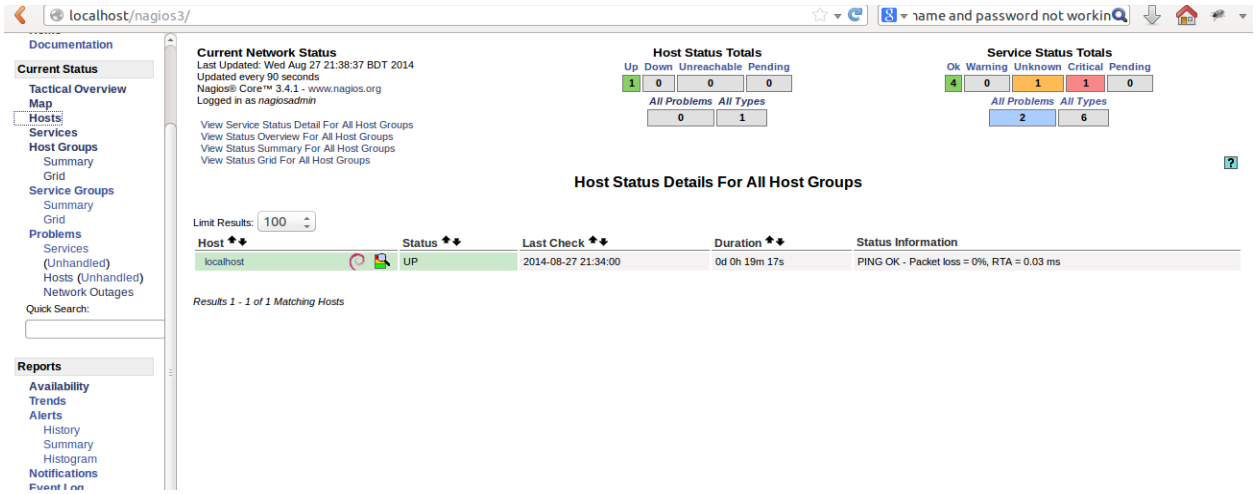


Figure 5.i : Host status details few seconds later

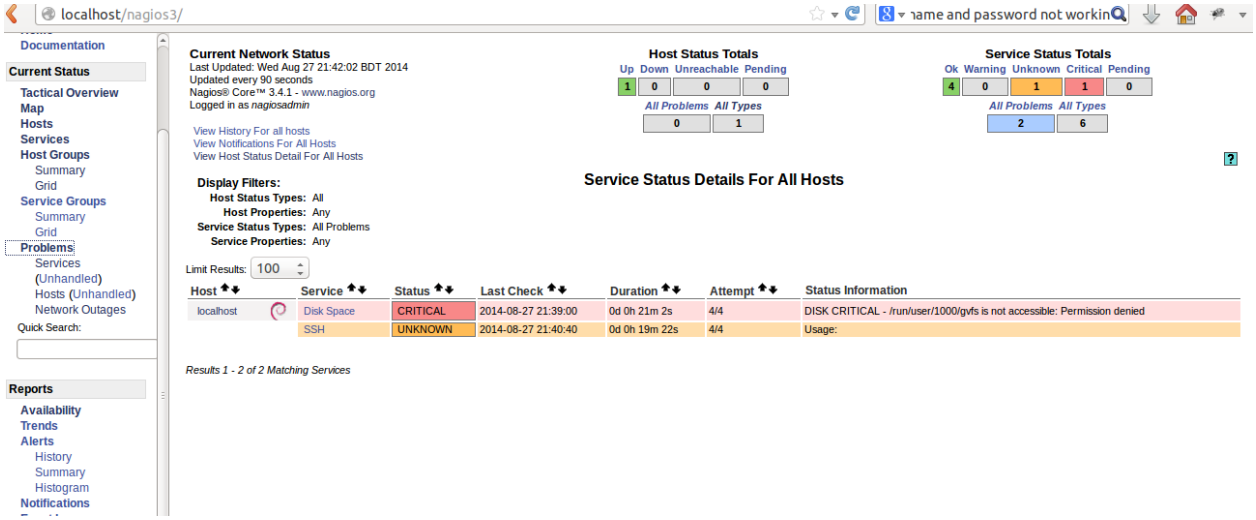


Figure 5.j: Service status details 1

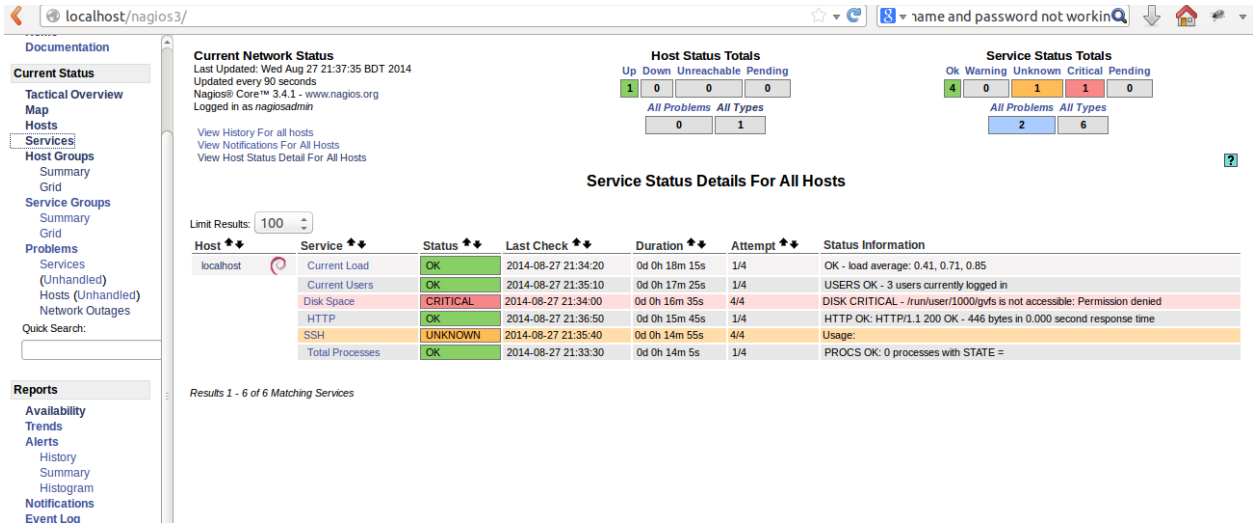


Figure 5.k: Service status details 2

Chapter-6

6.1 ETTERCAP

Ettercap stands for Ethernet Capture. Ettercap is a free and open source network security tool for man-in-the-middle attacks on LAN. It can be used for computer network protocol analysis and security auditing. It can be operated on various Unix-like operating system including Linux, Mac OS X, BSD and Solaris, and on Microsoft Windows. It is capable of intercepting traffic on a network segment, capturing passwords, and conducting active eavesdropping against a number of common protocols.

6.2 Ettercap working pattern:

Ettercap works by putting the network interface into promiscuous mode and by ARP poisoning the target machines. Thereby it can act as a 'man in the middle' and unleash various attacks on the victims. Ettercap has plug-in support so that the features can be extended by adding new plug-in. The attack comes when a machine asks the other ones to find the MAC address associated with an IP address. The pirate will answer to the caller with fake packets saying that the IP address is associated to its own MAC address and in this way, will "short-cut" the real IP - MAC association answer coming from another host. This attack is referred as ARP poisoning or **ARP spoofing** and is possible only if the pirate and the victims are inside the same broadcast domain which is defined on the host by an IP address and a Subnet mask, for example: 192.168.1.1 255.255.255.0

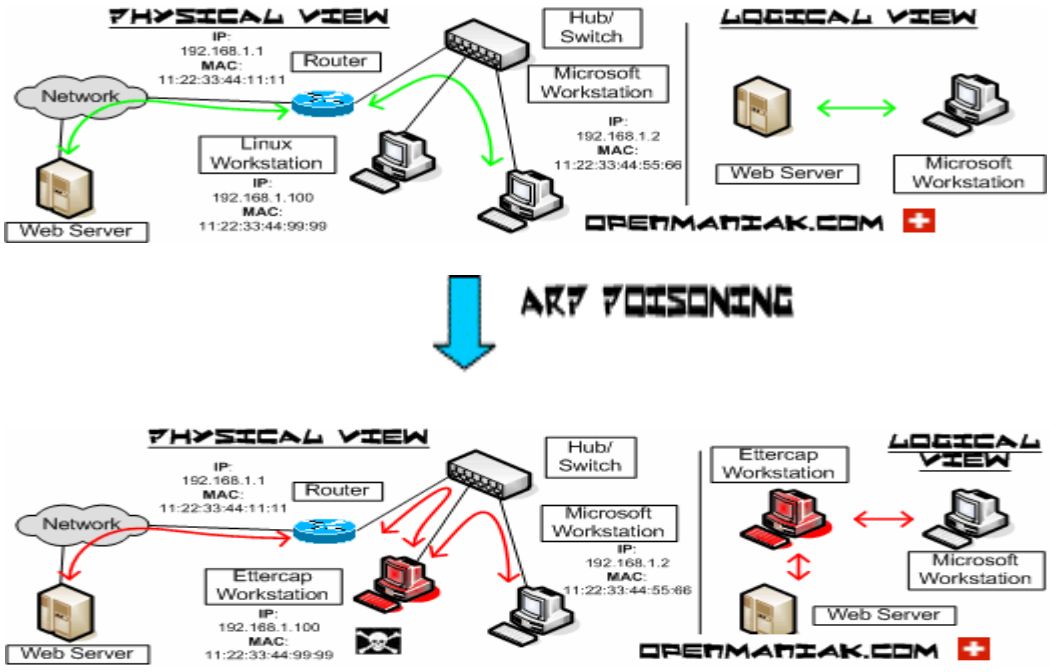


Figure 6.a : Ettercap ARP spoofing

In the case given earlier, a machine with IP 192.168.1.2 reaches internet resources from a local network. After the ARP poisoning attack, The Ettercap machine with IP 192.168.1.100is set as "man in the middle".

Man-in-the-middle attack

It is a form of active eavesdropping in which the attacker makes independent connections with the victims and relays messages between them, making them believe that they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all messages going between the two victims and inject new ones [27]

The Host list

Sending one ARP request for each ip in the LAN, it is possible to get the ARP request and then make the list of the hosts that are responding in the LAN. With this method, even windows host replies to the call-for-reply. Need to be very careful about class B (255.255.0.0) because ettercap will send 255*255 = 65025 ARP request.

Unified Sniffing

Ettercap NG uses sniffing method which is base for all the attacks occurring in network layer. The kernel IP forwarding is disabled and it is accomplished by ettercap. Some packets destination MAC addresses and attackers destination MAC addresses may same co- incidentally but with different IP addresses. Those packets can be re-broadcast to the wire and user may face man in the middle attack at that time.

Bridged Sniffing

In this method there are 2 interfaces may use to sniff packets and filtering them. This sniffing method is very stealthy as there is no way to detect someone in the middle. It’s called layer one attack. To avoid this attacks ettercap is working as inline IPS. [28]

ARP cache poisoning

ARP works basically on broadcast:

- when a machine connects to the network, it broadcasts its MAC address to the LAN (ethernet broadcast)
- When a machine needs to find a recipient (for a given IP), it sends a request using broadcast.

- When this learning process is over, the machine keeps the information in its ARP cache, that to save the network resources. The cache is a simple correspondence table of MAC / IP addresses.

we can check ARP cache with:

```
$ arp -a
```

Beyond its convenience, the big problem with broadcasting is that it does not authentication at all.

So, we can easily see how easy it is to corrupt an ARP cache with some forged packet. As the MAC address the only way to route date on an ethernet LAN, the potential impact of this attack is vast.

For best competence, the attacker will flood the targets with faked ARP responses at a high rate. That way, it gives little chance to a valid ARP record to survive long, as it will get quickly overwritten in the cache.

Nowadays, there are many convenient tools to drive this attack, like **Ettercap**.

We can start it in graphic mode:

```
$ ettercap -G
```

Got to the "*Sniff / United sniffing*" menu and select network interface:

Figure 6.b:Ettercap Input

"*Hosts / scan for hosts*" menu allow you to quickly visualize the machines of the LAN. Then, inthe "*Mitm*" (Man in the Middle) menu, choose "*Arp cache poisoning*"

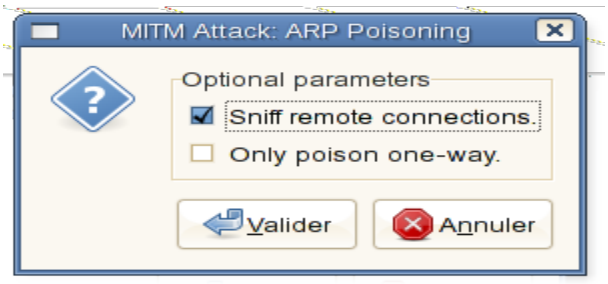


Figure 6.c : MITM Attack

Finally, “start / start sniffing” (default is all machines are targeted) :

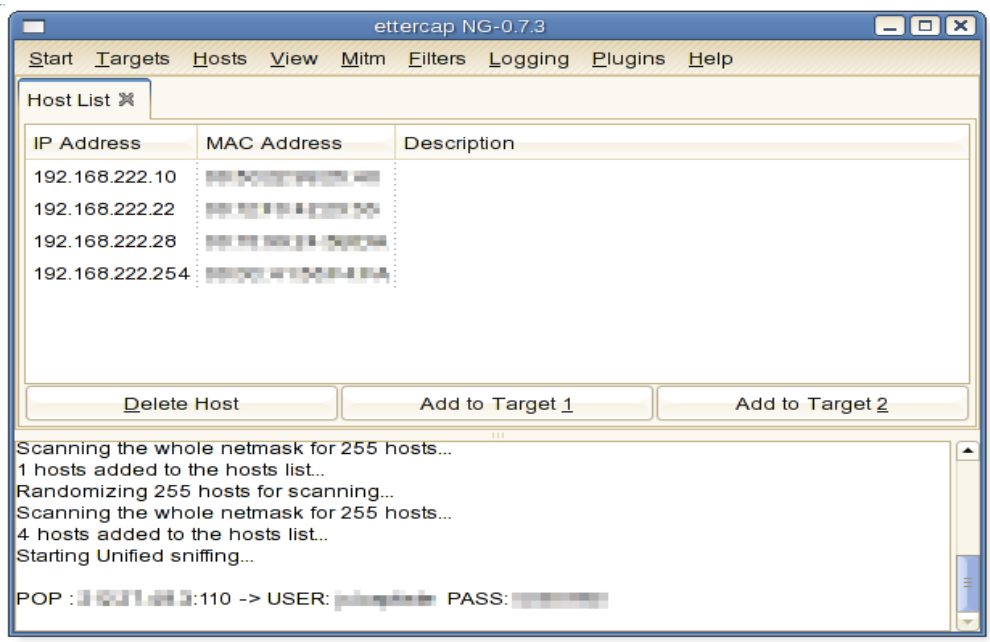


Figure 6.d: Sniffing

Immediately, Ettercap starts collecting data. Here some POP credentials can be read:

Several workaround can be set against this, though none is really satisfying:

1. Use static ARP entries for the LAN (arp -s 192.168.1.1 11-22-33-44-11-11) ; that is really not convenient, not scalable and unpractical for mobile devices ;
2. Some switches can detect MAC address changes and deactivate their port.
3. There are some tools to be set on a probe ; ARP watch for Linux checks the LAN and send an alert by mail or to syslog in case of malicious ARP events ;
4. More generic IDS / IPS like Snort should also be able to detect this attack ;

5. Radius / EAP hardware devices authentication is a more complex solution but the recommended one on large networks.[29]

To avoid ICMP poisoning, DHCP spoofing, port stealing, character injections,SSH1-man-in-the-middle, we need to use ettercap.

6.3 Ettercap features

Ettercap supports active and passive dissection of many protocols (including ciphered ones) and provides many features for network and host analysis. Ettercap offers four modes of operation:

- **IP-based**: packets are filtered based on IP source and destination.
- **MAC-based:** packets are filtered based on MAC address, useful for sniffing connections through a gateway.
- **ARP-based:** uses ARP poisoning to sniff on a switched LAN between two hosts (full-duplex).
- **Public ARP-based:** uses ARP poisoning to sniff on a switched LAN from a victim host to all other hosts (half-duplex).In addition, the software also offers the following features:

- **Character injection into an established connection**: characters can be injected into a server (emulating commands) or to a client (emulating replies) while maintaining a live connection.

- **SSH1 support**: the sniffing of a username and password, and even the data of an SSH1connection. Ettercap is the first software capable of sniffing an SSH connection in full duplex.

- **HTTPS support**: the sniffing of HTTP SSL secured data even when the connection is made through a proxy.
- **Remote traffic through a GRE tunnel**: the sniffing of remote traffic through a GRE tunnel from a remote Cisco router, and perform a man-in-the-middle attack on it.

- **Plug-in support:** creation of custom plug-ins using Ettercap's API.

- **Password collectors for**: TELNET, FTP, POP, IMAP, rlogin, SSH1, ICQ, SMB, MySQL ,HTTP, NNTP, X11, Napster, IRC, RIP, BGP, SOCKS 5, IMAP 4, VNC, LDAP, NFS, SNMP, Half-Life, Quake 3, MSN, YMSG

- **Packet filtering/dropping:** setting up a filter that searches for a particular string (or hexadecimal sequence) in the TCP or UDP payload and replaces it with a custom string/sequence of choice, or drops the entire packet.

- **OS fingerprinting:** determine the OS of the victim host and its network adapter.

- **Kill a connection:** killing connections of choice from the connections-list.
- **Passive scanning of the LAN**: retrieval of information. [30]

6.4 practical output :

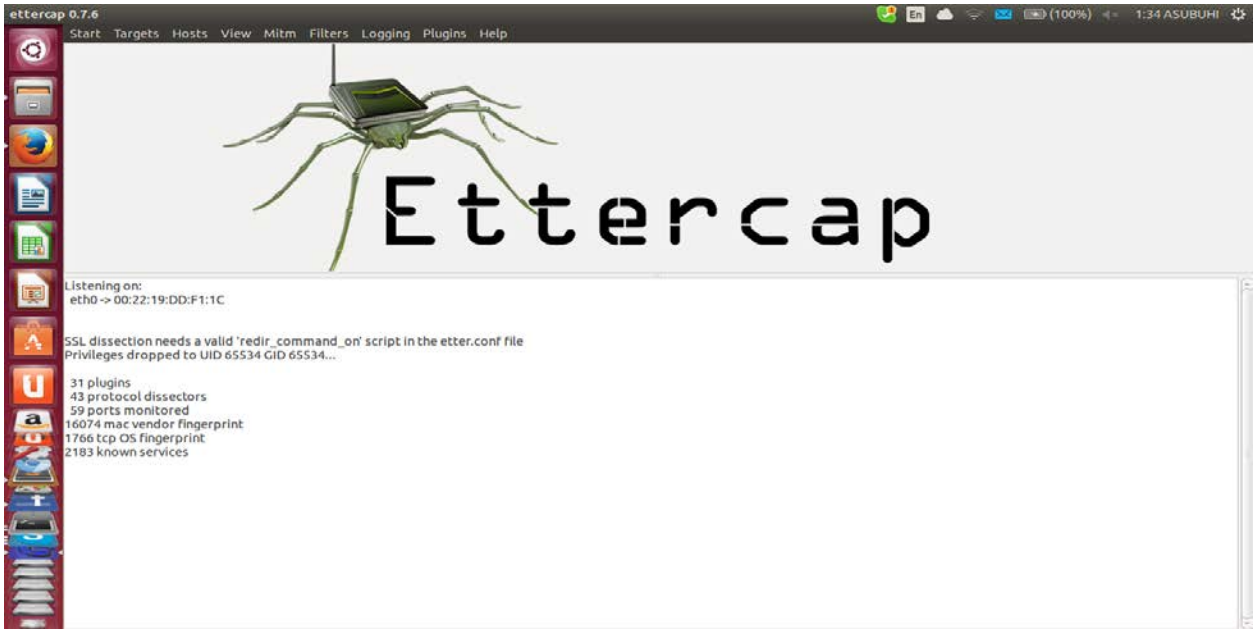


Figure 6.e:it shows-plug-in, protocol dissectors, Ports monitored, TCP OS fingerprints, MAC vendor fingerprints, known services.

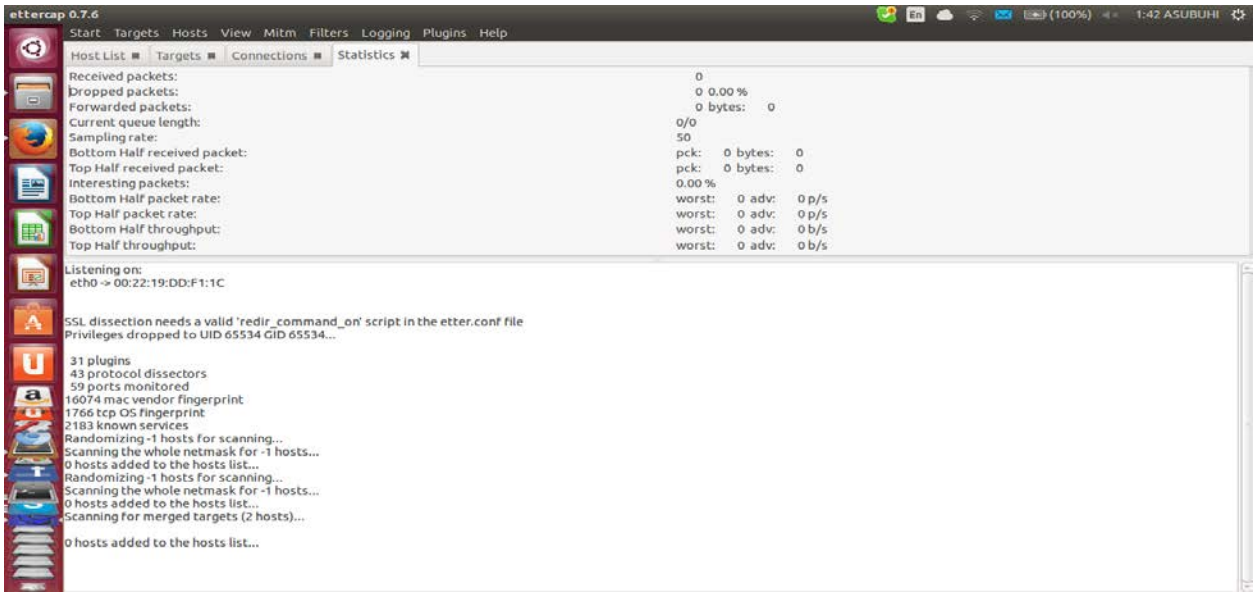


Figure 6.f: no host is added. it is only the monitoring pattern of ettercap.

Chapter-7

7.1 4 Critical Network Elements that Need for Monitoring

Businesses, depending on their size, purchase various networking infrastructure elements. Some of the basic network elements that need continuous monitoring are:

Email Servers: Every organization will have an Email server which distributes emails to all LAN users. If the email server fails, users are disconnected from the external world and key functions such as customer support have to face difficulties. IT Managers need to monitor their email servers for availability, mails in queue, size of mails received etc.

WAN links: Small Enterprises can save money by enhancing the WAN links. Oversubscribing can cost big bucks and under-subscribing deteriorates the network. Hence IT administrators should carefully balance the amount of work assigned in a particular period of time that is throughput, committed information rate (CIR) and burst rate with congestion, response time, and discards to optimize the link utilization. IT Managers should also find out who's using the most bandwidth to make necessary arrangements. Apart from bandwidth monitoring (discussed above), routers need to be monitored for availability and performance periodically. If a router fails it halts the entire LAN and hence IT Managers should set thresholds on various parameters on routers and attend problems immediately.

Business Applications :

- **Servers & Services**: Servers run critical applications and hence should be monitored for CPU, memory, disc space, services running on them (FTP, DNS, ECHO, IMAP, LDAP, TELNET, HTTP, POP, etc.) and their response time. Moreover the traffic utilization trends of these servers should also be monitored.
- **Server logs**: Small businesses running windows machines should also monitor the server logs for failed logon, account lockouts, bad passwords, failed attempts to secure files, security log tampering etc. Monitoring these logs gives detailed information on security loop holes existing inside the organization.
- **Applications, Databases, & Websites**: Small businesses run several mission critical applications, websites, and databases which need to be monitored periodically. Applications can be monitored for availability, response time etc. URLs should be monitored for availability.

LAN Infrastructure: LAN infrastructure devices such as switches, printers & wireless devices.

7.2 Top 3 Network Management Requirements For Small Networks

Small businesses have different network management needs and expectation because technical expertise and staff are limited. They want tools that are easy to install and use, are inexpensive, and feature rich.

- **Easy to install and use**: The network monitoring software should be intuitive enough to get started without reading that dry boring documentation.
- **Inexpensive** : The network monitoring software should be affordable.
- **Feature rich**: The network monitoring software should be able to monitor all your resources - both what you have today as well as what you might have tomorrow.[32]

7.3 Open Source Network Monitoring Software for Small Networks

Open Source offers many tools for various IT needs including network monitoring, bandwidth monitoring, network discovery etc. Most popular open source tools for network management are:

- **Nagios**: Network Monitoring Software
- **PRTG**: Traffic Monitoring Software
- **Kismet**: Wireless Monitoring Software
- **Wireshark**: network packet analyzer
- **Ettercap**: network security tool[31]

7.4 Secure Wi-Fi in Multi-Location Organizations

The number of retail stores, hotels, and public institutions, that consider WiFi hotspot access to be a critical network function, is increasing. , WiFi access is critical to these organizations' ability to run their business when it comes to enabling employee access to LAN applications, foster customer engagement, and support guest Internet access.

7.5 Requirements

To utilize Wi-Fi access efficiently, a multi-location organization must architect a solution that meets the following requirements:

- **Network Availability Within Budget** – increasingly newer multi-location organizations install Wi-Fi-only networks; no Ethernet cable is run. In these cases, the organization must consider the reliability of each location's connection to centralized resources, and architect a Wi-Fi infrastructure that fulfils requirements for network availability and reliability, while maintaining a low budget.

- **Flexible Security** – A common scenario on multi-location Wi-Fi networks is that different users have different access security requirements. Employees need 802.1X-based access – the industry standard for Wi-Fi security – while customers/guests are well-served by the use of a captive portal system with sign-on splash. A multi-location organization must ensure that its Wi-Fi infrastructure supports access by employees and guests, and configures the appropriate level of security for each.

- **Centralized Management, Distributed Deployment** – Most multi-location organizations choose not to staff each branch location with IT personnel. Therefore, a Wi-Fi infrastructure that can be centrally maintained from the headquarters location is crucial.

- **Seamless integration with a back-end data store-** Whether it be Active Directory, a simple SQL database or a self-registration or third-party guest management system, for administrative simplicity, the organization must ensure that its existing database of usernames and passwords can be extended to Wi-Fi access as well. [32]

Here we can see the condition for set up a successful Wi-Fi zone. For ensuring security in wireless network, we can use open source tools easily and open source tools can follow all the requirement which were given earlier. Some of open source tools comparison list shown below -

7.6 **Comparison chart of 5 open source tools -**

topic	Wireshark	Kismet	Ettercap	PRTG	Nagios
Platform	Windows\Linux	Linux\Windows\OSX\BSD	Windows\Linux\BSD\MacOS	Windows/Linux	Windows/Linux
License	GNU	GPL	GNU	Commercial/freeware	GPL v2
Software types	Network packet analyzer	Wireless monitoring software	Network security tool	Traffic monitoring software	Network monitoring software
Cost	Free	free	free	30 days free trial version but after that need to buy	Free for small environment but need to buy for large environment
Time	Less time consuming	Take more time then wirshark	Need time to detect attacker	Less time consuming	Time consuming
Installation process	Easy to install and available to download	Easy for Linux but little bit complex for windows and Vmware	Easy for Linux and MacOS but complex for windows	Easy for windows	Easy for Linux But need to download several part of nagios separately
File types	Link layer frame collector with all the protocols	Hidden SSID detector and detect all the packets with size	Network layer frame collector	SNMP ant netflow file collectors	SMTP,POP3,NNTP, HTTP etc.
Captured data	Live data capturing	Live and hidden data capture	Passive scanner	Passive and active scanner	Passive checker and instant remote host can capture
Security	Secured and configure some filters for packet s	More secured then wirshark and it is a client/server architecture	Security provider	Secured	Less secured then PRTG

Chart - 1

Still we are not using open source tools for our organization. we did review in specific area where they are depends on ISP provider and complex software applications.

7.7 Monitoring System in our few specific area

RMG Sector :

In RMG sector for most of the cases, network administrators are using software for analyzing their official Wi-Fi zone. Sometimes they are used to hire ASP provider to set up and monitoring Wi-Fi zone with their set up and monitoring equipments, which is costly as well. On the other hand, the organizations don't know the exact way to monitor their own Wi-Fi zone very safely and easily. But there are a few organizations available where the edge of Wi-Fi coverage area is small. Here, network administrator can identify their network manually. So, extra networking tool is not needed for these types of organization. We are focusing on multi locations organization where large amount of computers can be used in separate Wi-Fi area. In that case it is little bit tough to maintain the whole area within one infrastructure. Sometimes it gets very costly to maintain all the zone separately. Also there occurs some data connection problem or data congestion between source connection and data connection. To audit the entire network we need network audit tool. This way we can find out all the problems immediately and take proper steps to sort out all the problems.

Banking sector

Within the local banking sector, numerous company and client facing applications are hosted in a crossbreed or confidential Cloud, but are measured the dependability of the IT group for monitoring and investigation. This can present a confront to Network Engineers when they are tasked with temporary services to client complaint in a structure that is supported on mechanism, they cannot have right to use. In larger investment firms, after making vast investments in the network and application infrastructure to increase ultra-low latency in response time, IT budgets may be exhausted, making it hard to increase and improve inner systems. Important auditing and analysis tools may be cut from a financial plan, which binds the hands of engineers when a difficulty does arise.

With huge focus on security, IT organizations can take help of open source audit tools to ensure security within budget. Network engineers are using wi-fi security keys for protect their public network. But it is very difficult to ensure enough security in banking zone with wi-fi keys. So, it would be very helpful to use open source monitoring tools along with all the network and software applications.

Academic Sector :

In academic sector's Wi-Fi zone is monitored by software appliances and WPS method. We learned about this when we talked with the IT team of BRAC University. They don't use any kind off open source tools for auditing their network.

The principle of this thesis, in particular, is to introduce usefulness of open source tools in multi location organizations like RMG sector, Banking sector and academic sector. So that they can set up and audit their network by using open source tools. Open source tools are very easy to install, run and auditing Wi-Fi zone. Here we are proposed to use open source tools for auditing Wi-Fi area frequently. Since now a days, hacking is a common cyber attack, in most of the cases Wi-Fi network is protected by WPA 1 and WPA 2 which are very easy to attack. When we set up any Wi-Fi zone we are not monitoring it frequently so we are not aware about the current condition of our network and its security. If we use open source tools, it would be very easy to see all the details of Wi-Fi area like source, destination, frequency, nearby destination, affected or lost IP address etc.

Below we have enlisted the comparison between the open source tools which are applicable for some multi location organizations. User may choose a set of open source tools which we have given below. From the list 2 or 3 tools will b more efficient to audit a Wi-Fi network. Here we are giving some suggestions to the network administrator of the various sector where we have worked to analyze these set of open source tools.

7.8 In RMG - PRTG, Ettercap, Nagios can be more suitable to analyze wi fi network in RMG sector.

Topic	PRTG	Ettercap	Nagios
Based on	Sensor and probe based	IP based, Mac based, ARP based	Enterprise class host, service and infrastructure based
Monitoring protocols	SNMP and NetFLow	SSH1 and HTTP support but can collect password for any protcol	SSH1,HTTP,FTP,MySQL,PostgreSQL
Time needed	Need less time then nagios	Less time consuming	Time consuming
Cost	Free for 30 days trial version but after that need to buy license from Paessler	Free	Cost free for small area but for large area need to configure more nagios application to monitor network ,then it becomes costly
Types of services	Traffic monitoring within network and can give feedback about website with web grapher	Intercepting traffic on network segment and detect man in the middle attack	Work as graphic engine and update web interfaces ,identify remote host
Operating System	Easy for windows	Need Linux to use it	Easy to use but need linex OS
Type of tool	Traffic monitoring tool	Security ensured tool	Network monitoring

Chart - 2

7.9 In Bank - Ettercap, Kismets, Wireshark can be more suitable to analyze wi fi network in banking sector.

topic	Ettercap	kismet	wireshark
Types of tool	Network security tool	Wireless Network Analyzer	Network packet analyzer
Working pattern	Intercepting traffic on network segment and detect man in the middle attack	Work with multiple wireless card and sometimes it can be used for ethical hacking	Work for link layer protocol and public access point. So unwanted hacking can be reduced
Capture data	Can capture password for every protocol in network	Capture packet with any time and find hidden network with radio frequency	Capture live data and show each and every frame with details
Cost	Cost free	Cost free	Cost free
Operating system	linux	Need Linux OS	Linux \windows
Security	It ensures security to the network very strongly	More secured then wireshark	Used as secondary security tool
Time	Though it takes time to detect man in the middle attack in the network, it is very effective for network	Need more time than wireshark as it has more effect then wireshark	Less time consuming

Chart 3

7.10 In Academic sector - PRTG, Kismet, Wireshark, can be more suitable to analyze Wi-Fi network in academic sector.

topic	PRTG	Wireshark	Kismet
Analyzer types	Network Traffic Analyzer	Network packet analyzer	Wireless network analyzer
Monitoring style	Monitoring more devices and ports and interfaces	Work for link layer protocol and public access point. So unwanted hacking can be reduced	Work with multiple wireless card and sometimes it can be used for ethical hacking
Captured data	Capture live data for past 1 to 60 minutes and can continue further capture with data and graph	Capture live data and show each and every frame with details	Capture packet with any time and find hidden network with radio frequency
cost	Free for 30 days trial version but after that need to buy license from Paessler	Cost free	Cost free
Operating System	Easy for windows OS	Linux	Linux
Time	Less time consuming	Less time consuming	Need more time then wirshark as it has more effective value then wireshark
Protocol details	Netflow collectors	Live packet collectors with old and new protocols	Hidden interfaces and protocols can be collected

Chart -4

7.11 Conclusion

We tried our best to introduce about usefulness of some powerful open source tools for auditing wireless network. So that network administrator, IT administrator can use open source tools along with their manual process and software application for surveying wireless network and protect network from some unwanted hacking. Now-a-days, wi-fi becomes very common method of using broadband internet connection in multi-location business organizations. Most of the offices are sharing their information via wi fi connection. If WPS accessibility is enable then it may face some kind of virtual attack.

When we did our survey on RMG, Bank and Academic area we came to know that they are using manual process for monitoring wireless network. Basically, network administrator protect wireless network using all the security keys named WEP, WPA, WPA2. However, WPA2 is more secured then other keys, Additionally, WPA 2 can be break down easily, when WPS (Wi-Fi Protected Setup) remaining enable mood. So attacker may take 2- 14 hours to break it down. In that case if administrators are use open source tools along with WPS they might be able to know about current condition of wireless network. Earlier in this paper it was described that open source tools can capture live information and detect random interfaces with passwords. Few open source tools can capture past data as well. Therefore, these types of tools can help to reduce Wi-Fi attacks.

In RMG sector WPA2 can play a vital role to protect wireless network of that organization. However, they can use open source tools along with WPA2.It would be more secured for wireless network. As open source tools are not expensive, it can easily set into budget. When we did survey on Wi-Fi zone of different business organization, we categorized few tools for different sectors. From that analysis we proposed to RMG sector's network administrator to use at least two Open Source tools named PRTG and Ettercap for auditing their network. By using those tools they will be benefited and will be able to know the current condition of wireless network.

In banking sector, if IT department (Network Administrator) does not keep up with the current phase of network traffic, they may face some unwanted hacking. To get rid from these types of problem Open Source Audit tools need to be included as a part of security maintenance system. So, here we suggest using Ettercap and Kismet for auditing their network.

Open Source audit tools are also useful for auditing wireless network of academic sector like universities, colleges and schools. From our survey we suggest to all the network administrator of academic sectors to use PRTG and wireshark to monitor wi-fi zone. So that, they can know what is going on in their network. After that for ensuring security, they can take proper initiatives for wireless network.

7.12 References

1. What is wireless Internet .N. d. Web wise. Retrieved 01, 2014, from. http://www.bbc.co.uk/webwise/guides/about-wifi
2. V.w.Brain. M.Jhonson(2013, 08). How wi fi works. How stuff works. Retrieved 10, 2013, from http://computer.howstuffworks.com/wireless-network1.htm
3. Term of Wi-Fi. *Wi-Fi-support*. N.d. Retrieved 10, 2013, from. http://www.webopedia.com/TERM/W/Wi_Fi.htm
4. T.K. N.d. Advantage dis-advantages of Wi- Fi . Retrieved 11, 2013, from http://digitalwalt.com/wi-fi-advantages-disadvantages/
5. Security concern on Wi-Fi.2010, July 9.*airlink.in*. Retrieved 11, 2013, from http://airlink.in/blog/security-concerns-on-wifi-networks-how-do-we-overcome-them
6. P.Lisa (2010, 03). Top ten wi fi security threats. e *security planet*. Retrieved 11, 2013, from http://www.esecurityplanet.com/views/article.php/3869221/Top-Ten-WiFi-Security-Threats.htm
7. A.O.; G.R; J.B., (2007, 02). Wireshark. *http://en.wikipedia.org/wiki/Wireshark*. Retrieved 11, 2013, from https://www.google.com.bd/search?q=http://www.wireshark.org/&ie=utf-8&oe=utf-8&rls=org.mozilla:en-US:official&client=firefox-a&channel=sb&gws_rd=cr&ei=hYX9U9aZGJGIuASZ-YAw
8. Kismet.N.d.*dragorn@kismetwireless.net* . Retrieved 12, 2013, from http://www.kismetwireless.net/
9. Network Auditing. N.d Open foundry. Retrieved 01, 2014, from http://www.openfoundry.org/en/resourcecatalog/Security/Network-Auditing
10. L. E. (2003). Wireless network Audit using open source tools. Version no 1.0(assignment version no 1.4 b), a short tutorial, 3-25.
11. Wireshark tutorial. N.d.webhost.bridgew.edu. Retrieved 01, 2014, from http://webhost.bridgew.edu/sattar/CS430/HW/LABS/wireshark.htm
12. C.Himanshu (2012, 09). Wireshark the best open source tools. www.ibm.com. Retrieved 01, 2014, from https://www.ibm.com/developerworks/community/blogs/6e6f6d1b-95c3-46df-8a26-b7efd8ee4b57/entry/wireshark_the_best_open_source_network_packet_analyzer_part_i60?lang=e
13. J.F,K.w, K. (2007). Wirshark-lab: getting started. Version2
14. Using wireshark for network-trouble-shooting. N. d. jaspersoft.com. Retrieved 01, 2014, from http://community.jaspersoft.com/wiki/using-wireshark-network-troubleshooting
15. D.Thomas. N.d. Wireshark. Admin network and security. Retrieved 01, 2014, from http://www.admin-magazine.com/Articles/Wireshark
16. W.Aaron (2006, 03). Introduction to kismet. WI-FI PLANET. Retrieved 02, 2014, from http://www.wi-fiplanet.com/tutorials/article.php/359553
17. Uwe,G.Hans, D.Christien (1998). KISMET V.6.0.2. Virsion1.4,

18. C.Belisa (2008, 03). Kismet the easy tutorial. Open maniac. Retrieved 02, 2014, from http://openmaniak.com/kismet.php
19. Kismet (2007). Readme. Retrieved 02, 2014, from http://www.kismetwireless.net/documentation.shtml
20. Using PRTG (2005, 03). Cisco. Retrieved 02, 2014, from http://www.cisco.com/c/en/us/products/collateral/routers/wide-area-application-services-waas-software/white_paper_C11-582242.html
21. Architecture. PAESSLER. n. d. Retrieved 03, 2014, from http://www.paessler.com/manuals/prtg7/system_architecture
22. P.Joe (2012, 11). Monitoring your network with PRTG. Technical article. Retrieved 03, 2014, from https://devcentral.f5.com/articles/monitoring-your-network-with-prtg-api-automation#.U4s7Y9ySxFs
23. Nagios (2005, 10). Wiki. Retrieved 04, 2014, from http://en.wikipedia.org/wiki/Nagios
24. Philcore, (2005, 10). Using nagios to monitor network. Debian administration. Retrieved 03, 2014, from http://www.debianadministration.org/article/299/Using_Nagios_to_Monitor_Network
25. B. Wolfgang (2006). Nagios: System and monitoring (N.Ed.N.Vol. Chapter-8). Open source press, no starch press.
26. Nagios overview (2010, 05). Nagios. Retrieved 08, 2014, from http://www.nagios.org/about/overview
27. N.Duane (2004). An Ettercap Primer. GIAC Security essential certification, (option 1), 1.4b,
28. Ettercap. N.d. Github. Retrieved 07, 2014, from https://github.com/Ettercap/ettercap/blob/master/README
29. Introduction to network attack.(2008,10). Phocean.net. Retrieved 07, 2014, from http://www.phocean.net/2008/10/12/introduction-to-network-attacks-network-layer.html
30. Ettercap(2007). ARP spoofing and beyond, a short tutorial,
31. Free networking monitoring tools for small network n.d Mange engine, Opmaniak. Retrieved 07, 2014, from http://www.manageengine.com/network-monitoring/network-monitoring-tool.html
32. Secure Wi-Fi in multi-location Organizations. N.d. Cloudessa. Retrieved 07, 2014, from http://cloudessa.com/solutions/secure-wifi-in-multi-location-organizations/