FYP DOCUMENT

SECURE NETWORK INFRASTRUCTURE

USING MOBILE AGENT

ADVISOR:

Dr. Aawis Shibli

CO-ADVISORS:

Mr. Qasim Rajpoot

TEAM MEMBERS:

Saqib Khan	2007-NUST-BIT-139
Mudasser Mahmood	2007-NUST-BIT-30

DATED:

20-Jun-2011

DEDICATION

To Allah the Almighty & To my Parents and Faculty

CERTIFICATE OF APPROVAL

It is certified that the contents and form of thesis entitled "Secure Network Infrastructure using mobile agent" submitted by Saqib khan (2007-NUST-BIT-139) & Mudasser Mahmood (2007-NUST-BIT-30) have been found satisfactory for the requirement of the degree.

Advisor:	Dr. Awais Shibli	**Signature:** __________________
Co-Advisor:	Mr. Qasim Rajpoot	**Signature:** __________________

Table of Contents

Chapter 01

1. INTRODUCTION

Mobile agents are a recent network computing paradigm compared with the used approach to remote computing, based on a client-server model. Mobile agents are self-contained software modules and data that can be launched by a human user and then, they autonomously migrate through the network. They visit remote hosts, perform there their tasks; migrate to the next host, eventually returning to the management station, where their actions were initiated. A mobile agent is a paradigm shift in the world of remote computing and networks.

Mobile agents have two basic properties autonomous operations and mobility. Because of these two properties it is expected that network security system based on mobile agents will be better and more effective than security technologies used in current networks. Besides basic capabilities, to travel through the networks and perform their tasks, agents can also perform very complex and sophisticated functions. With regard to mobility research issues two kinds of code of mobility are to be outlined .One is known as strong mobility and second one is called weak mobility

An active agent is migrated on the network then it comes on the remote host, these all functionalities are achieved using object serialization. After the entire agent launches and run it on the remote host and gather the results of network monitoring and analysis on the remote host. Our application the activity watcher not only gathers the information like the recent items accessed on the remote host but also the network monitoring which all comes in the watching the activities on the network**.** The initialization of the network scanners is performed on the remote host by the administrator and these scanners on their own behalf collect information on the remote host of network monitoring and then launching activity watcher application on this system and merge to with the system. The main functionalities of the activity watcher application are returning the browser cookies, running processes, software installed and .exe files. When the code of activity watcher application is merged with the system and then agent creator will write a code and this particular application shall do its services. This all process shall be secure and reliable and the transfer of mobile agent, migrating through network will be the main objective to be achievedfiltering of information, distributed over the LAN.

1.1.Scope

The scope of the mobile agents' infrastructure is to perform tasks across different networks. In order to accomplish complex network tasks mobile agents must be prepared in the form of teams and their actions must be maintained by various particular components in the networking environment. Such method represents a complex Mobile Agents System (MAS), comprising several different types of components. These components perform their functionality and, combined together, they represent the complete infrastructure for management and execution of mobile agents. Mobile agents' tasks must be organized in a secure manner and in a trusted way while communicating with other agents may be static or any remote independent agent. It will be compatible that it shall easily adopt according to the agent owner approach and techniques used. Retrieval from the database server shall be quite efficient and trusted. The actions performed by the mobile agents will be according to the different assurance levels to be discussed later. It will be based on the different assurance levels like high, medium and low.

1.2.Glossary

Term	Definition
MAS	Mobile agents systems/servers
PKI	Public key infrastructure
Html	Hypertext markup language
MAS	Mobile Agent System
UDDI	Universal Description, Discovery and Integration
KDS	Key distribution server
SRS	Software Requirements Specification
IDPS	Intrusion detection and prevention system
NIDS	Network intrusion detection system

1.3. References

[IEEE] The applicable IEEE standards are published in "IEEE Standards Collection," 2001 edition.

[Reaves SPMP] "Software Project Management Plan Jacksonville State University Computing and Information Sciences

MagicNet systems developed by the KTH Sweden under assistance of Mr. .Awais Shibli

Research paper IEEE standard Shibli_Paper_4_Korea_AL on infrastructure of trusted mobile agents' technology.

1.4.Document overview

Firstly this document is about the introduction of the mobile agents and then use cases and the designing of the infrastructure and mobile agents systems discussed. After the literature study has been given and then methodology adopted to accomplish the project. Different assurance levels are discussed which can be performed based on strategy used. The discussion on the results and conclusion to be made.

2. LITERATURE REVIEW

The overall description of the project and the literature review is discussed in this section, The principles, functions and topology of standardized infrastructure for security services are based on the technologies like for instance PKI and secure XML/Web federation, various secure network protocols, and other security standards. Large-scale intrusion detection and prevention systems, based on secure mobile agents and various security services in a networking environment, can best be provided by such a network security infrastructure. We have identified the following core components of our security infrastructure for mobile agents, classified in two groups:

2.1.Components for Deployment and Execution of Mobile Agents

The most important component of the MAS is mobile agents. Mobile agents are self-contained software modules with additional configuration and security credentials and accumulated data baggage. They roam a network, moving autonomously from one server to another, perform their designated tasks, and finally, eventually, return to their agents' management station.

Besides their code, mobile agents also have associated *credentials*, comprising header and trailer information, that describe the type and other attributes of an agent, a *baggage,* that agents have created and accumulated during their activities at various hosts, and finally *Routing information* for traversing the network.

Security infrastructure for mobile agents system also offers services for mobile agents to collaborate with each other in order to execute security and administrative functions in the network.

This means that we have also addressed security problems for agents' collaboration. In order words, our infrastructure also provides strong safety for agents' communication messages.

2.2. Phases of the mobile agents systems

The different phases of the mobile agents that how agents are created, adopted and assigned privileges, deployed and executed. (Courtesy from MagicNet systems).

MagicNet system into four functional phases: a) *Trusted Mobile Agents Creation and Validation Phase*: when agents are being created, validated and appraised; b) *Mobile Agents Acquisition Phase*, when agents are published and adopted; c) *Mobile Agents Deployment Phase,* when agents are retrieved, users are authenticated and XACML polices are created for specific local domains, and d) *Mobile Agents Execution Phase*, which contains runtime components (physical network) for agents. Agents traverse the network and perform their tasks during execution phase shows different phases and information flow. Information objects in these phases are in fact mobile agents. Mobile agents' development starts in the first phase i.e. "trusted mobile agents' creation and validation phase″. The outputs of the first phase serve as inputs for the next phase, and so on. Each phase provides input to the subsequent phase. Finally, mobile agents execute in a network during "*mobile agents execution phase*". In each of these four phases, the functionalities in each particular phase are discussed in the following section in the form of bullets:

1) Trusted Mobile Agents Creation and Validation Phase
    a. Agent Creation
    b. Agent Trust Appraisal
    c. Agent Privileges Assignment
2) Mobile Agents Adoption Phase
    a. Agent Publication
    b. Agent Retrieval
3) Mobile Agents Deployment Phase
    a. Agent Code Authentication
    b. Agent Owner Authentication
    c. Agent Launching
4) Mobile Agents Execution Phase
    a. Agent Hosting and Execution
    b. Agent Return

c. Agent Transfer

2.3.Securities of mobile agent systems

Since mobile agents roam and execute through an entire network, it is important to provide strong protection of agents and all their resources. At the same time, it is equally important to protect agent's platforms against malicious agents. We have applied various standard security mechanisms and services in order to protect mobile agents, their baggage, communication messages, control structures and platforms against various accidental and intentional threats. In that context, security services for secure computing and secure handling of data applied to mobile agents systems have also been addressed. Our system provides mobile agents system security services, such as confidentiality and integrity of resources, access control to resources, authentication and authorization of users and other active components, protection and non- repudiation of transactions, etc.

Therefore, our mobile agents system is very secure and all its components and resources are strongly protected. We provide protection of mobile agents' code and data using cryptography. Our system provides also an effective solution to perform computing with the encrypted code of mobile agents. This feature provides protection against reverse engineering and allows preservation of code correctness in spite of malware, worms, or viruses

3. ARCHITECTURE

3.1.Block Diagram

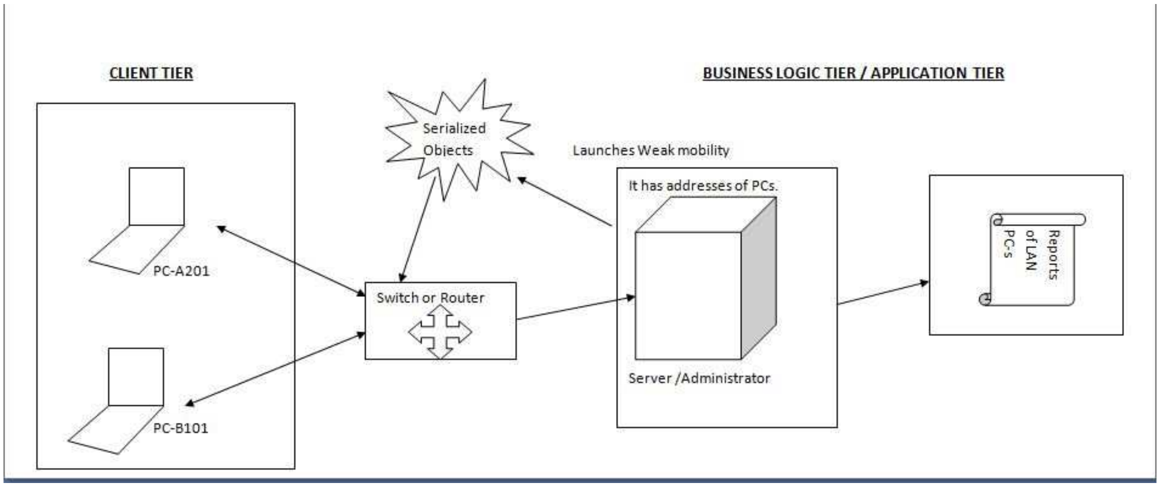


Figure: 3.1

When the agent is migrated on the network then it comes on the remote host, these all functionalities are achieved using object serialization. After the entire agent launches and run it on the remote host and gather the results of network monitoring and analysis on the remote host. Our application the activity watcher not only gathers the information like the recent items accessed on the remote host but also the network monitoring which all comes in the watching the activities on the network**.** The initialization of the network scanners is performed on the remote host by the administrator and these scanners on their own behalf collect information on the remote host of network monitoring and then launching activity watcher application on this system and merge to with the system. The main functionalities of the activity watcher application are returning the browser cookies, running processes, software installed and .exe files. When the code of activity watcher application is merged with the system and then agent creator will write a code and this particular application shall do its services. This all process shall be secure and reliable and the transfer of mobile agent, migrating through network will be the main objective to be achieved.

3.2.Overview of System Design

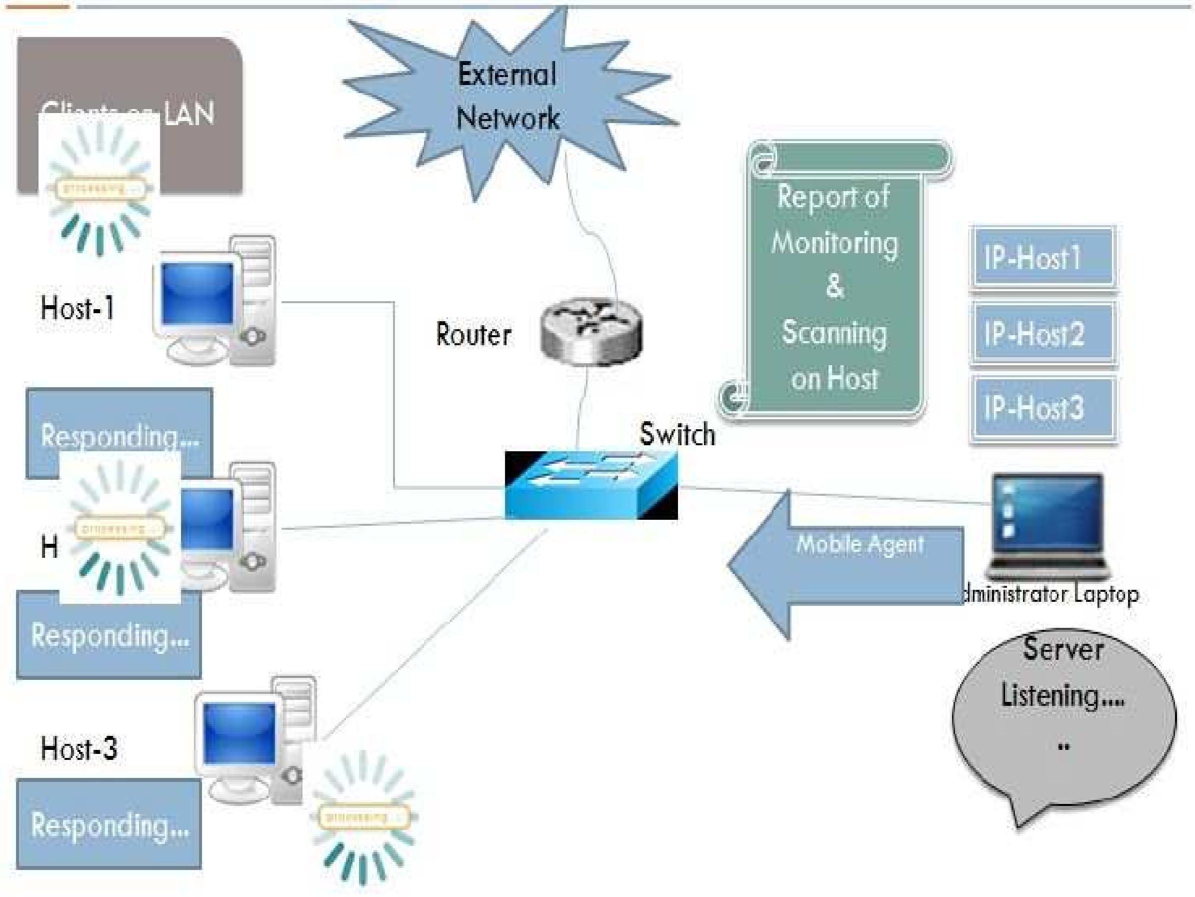


Figure: 3.2

3.3.Use cases

3.3.1. Mobile agent's creation and launch on network

Mobile agents are created specifically on the server by the agent owner, agent owner write the code of mobile agent called as the mobile agent code. This functionality is achieved by the method of object serialization and then lanuched on the server from where mobile agent migrate across the network and launch on the remote host where it performs the operation of network monitoring using different scaners and return the result.

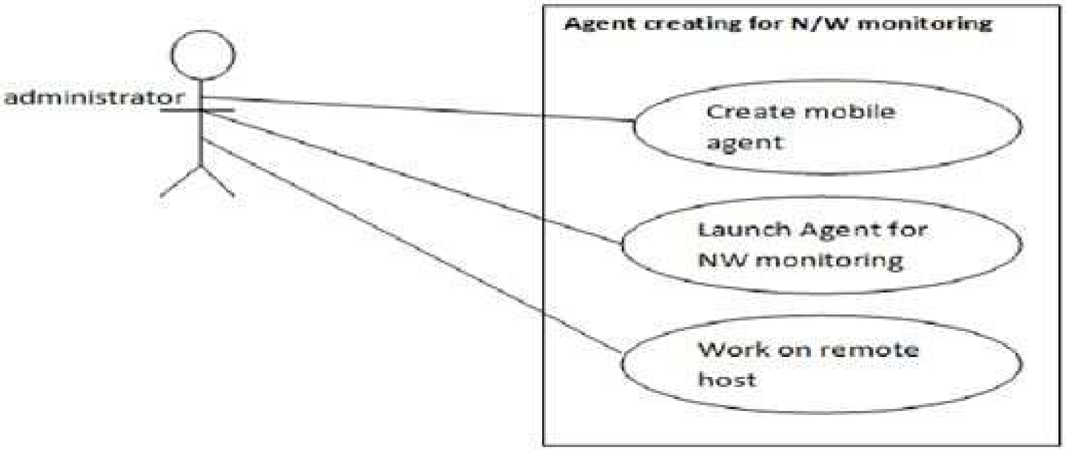

administrator
Agent creating for N/W monitoring
Create mobile agent
Launch Agent for NW monitoring
Work on remote host

Figure: 3.3.1

3.3.2. Network Monitoring using Nessus

Nessus is a powerful, cross-platform network scanner that does many things. And of those many things Nessus do, most people prefer to employ its power as a network vulnerability scanner. And Nessus does that very well. But Nessus doesn't have to be limited to network security. Of the many features Nessus has, the one I tend to use the most is network mapping. By using Nessus to scan your network, you can save the results, giving you an outstanding map of your current network.

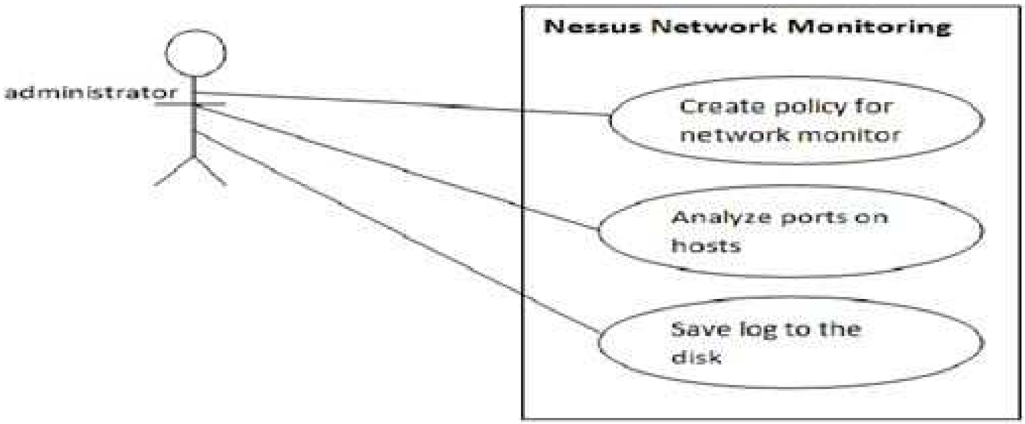


Figure: 3.3.2

3.3.3. Network Monitoring using Wireshark

With the Wireshark network analyzer, networking pros can address a wide range of monitoring for functions that range from bandwidth optimization and application analysis to troubleshooting and network security. Wireshark is an open source network monitoring tool, so networking pros can tailor the tool to their exact needs. And those needs can range from basic traffic transmission testing to intrusion prevention, analysis of bandwidth usage, application security testing and identification of faulty configurations.

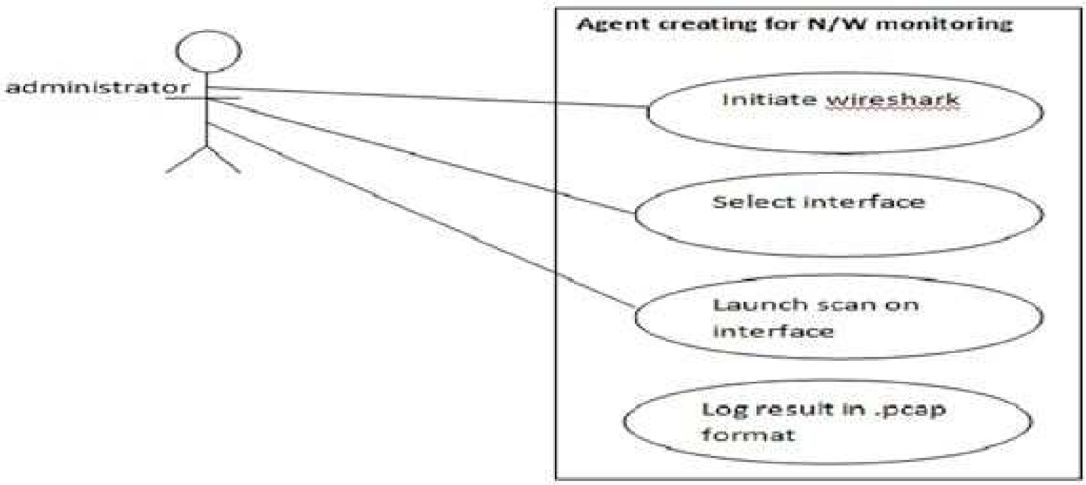


Figure:3.3.3

3.3.4. Network Monitoring using Nmap

Nmap ("Network Mapper") is an open source tool for network exploration and security auditing. It was designed to rapidly scan large networks, although it works fine against single hosts. Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

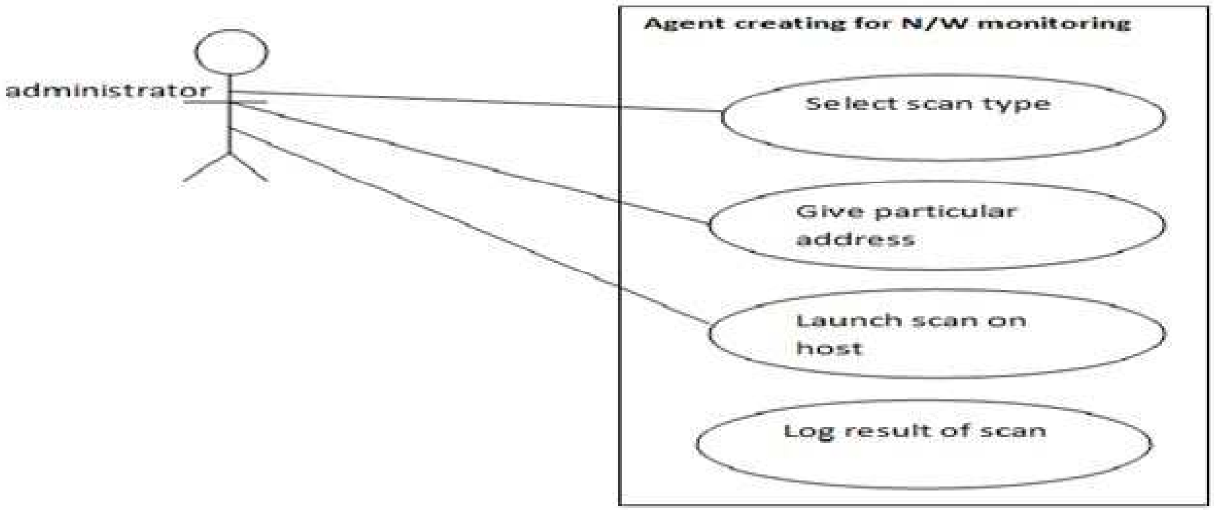


Figure:3.3.4

3.3.5. Activity watcher

Once an infrastructure is built which is secure and trustworthy, then we can launch on any service or activity in that infrastructure, for instance an activity watcher is an application which is migrated and launched on this infrastructure and it gives us all the processes and .exe files, cookies and recent data used.

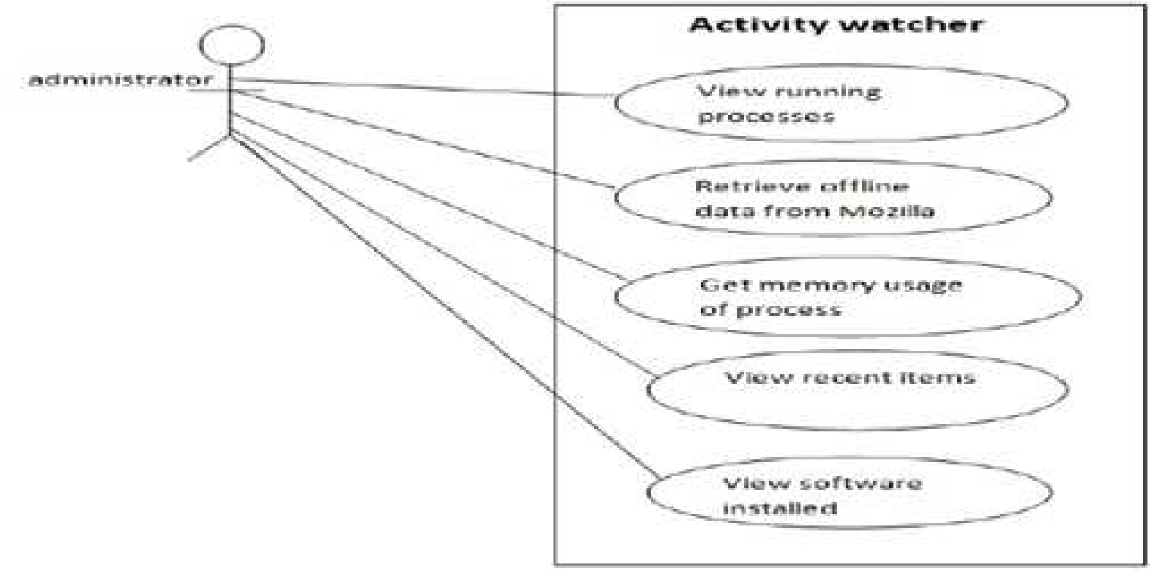


Figure: 3.3.5

3.3.6. Snort NIDS (network intrusion detection system)

Snort is an open source network intrusion detection and prevention system which was developed by the "Sourcefire". Snort is well known tool to analyze the network traffic and define rules and standards that what rules are defined in the network. Snort works on command line options and it can be configured in three modes: sniffer mode, packet logger mode and NIDS mode. But we shall be configuring snort in NIDS mode. In this mode, we will define some rules and standards and then configure it. It will then itself analyze the traffic and match with the defined rules and standards and record the particular packets and show the output or generate any message to the administrator.

3.4.Requirement specifications

3.4.1. Functional Requirements

Use Case Name:	Agent creation for Network Monitoring
Priority	Essential
Trigger	Menu selection
Precondition	Sever is connected to the machines over the network -LAN
Basic Path	1. Client or Administrator sends the request for analyzing the traffic over the network or for machines security. 2. Server generates the object serialization in order to achieve the weak mobility to perform the required tasks.
Post condition	Report will be sent to administrator
Exception Path	If there is a connection failure the Server returns to the wait state

Use Case Name:	Nessus for Network Monitoring
Priority	Essential
Trigger	Menu selection
Precondition	Nessus (network security tool) must be configured Policies must be updated and Sever is connected to the machines over the network –LAN
Basic Path	1. Client o Administrator sends the request for analyzing the traffic over the network or for machines security. 2. Server check the policies in the look up table of Nessus and using Object serialization , ports on remote machine will be analyzed
Alternate Path	N/A
Post condition	Logs will be saved on disk and sent to administrator
Exception Path	If there is a connection failure the Server returns to the wait state

Use Case Name:	Wire shark for Network Monitoring
Priority	Essential
Trigger	Menu selection
Precondition	Wire shark (network security tool) must be configured Interfaces must be known and Sever is connected to the machines over the network –LAN
Basic Path	1. Client o Administrator sends the request for analyzing the traffic over the network or for machines security. 2. Server checks interface which has been selected and using Object serialization and launch scan on interface
Alternate Path	N/A
Post condition	Logs will be saved on disk in .pcap format and sent to administrator
Exception Path	If there is a connection failure the Server returns to the wait state

Use Case Name:	Activity Watcher
Priority	Essential
Trigger	Menu selection
Precondition	Sever is connected to the machines over the network –LAN All tools especially network security tools must be configured
Basic Path	1. Client o Administrator sends the request for analyzing the traffic over the network or for machines security. 2. Server checks the following condition: • View current live Process • View Mozilla data and history • Check memory usage by processes • View Recent items • View the installed software which has been selected and using Object serialization and launch scan on interface
Post condition	Logs will be saved on disk and sent to administrator
Exception Path	If there is a connection failure the Server returns to the wait state

3.4.2. Non-functional requirements

There are requirements that are not functional in nature. Specifically, these are the application must be compatible with Microsoft windows only and both the Mozilla firefox and Internet Explorer web browsers are being used for network security tools.

3.5.Sequence Diagram:

This functionality is achieved by the method of object serialization and then lanuched on the server from where mobile agent migrate across the network and launch on the remote host where it performs the operation of network monitoring using different scaners and return the result.

Mobile agent's creation and launch on network

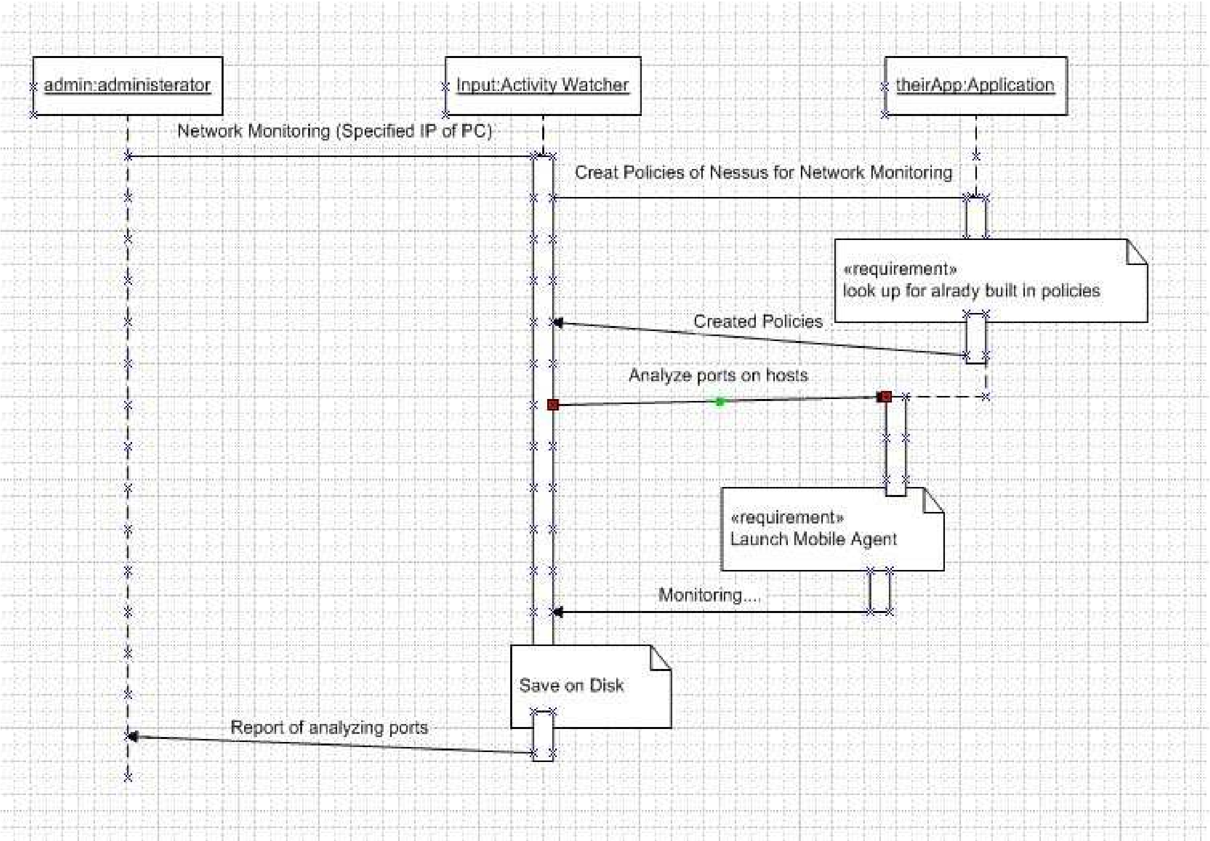


Figure: 3.5.1

By using Nessus to scan your network, you can save the results, giving you an outstanding map of your current network. It's an easy way to keep track of how many systems you have, what systems are deployed, what current IP addresses each system is assigned, and what ports are open on each system

Network Monitoring using Nessus

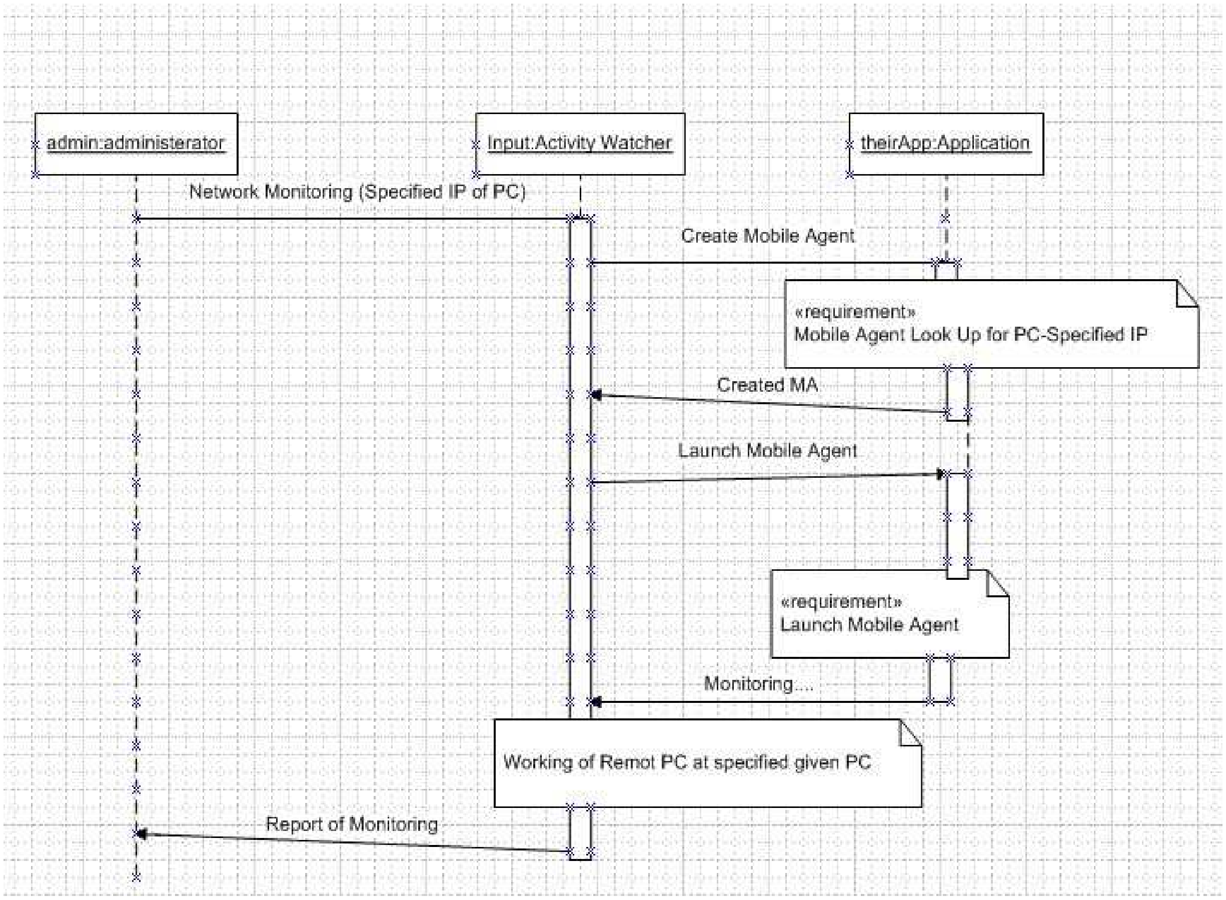


Figure:3.5.2

Wireshark is an open source network monitoring tool, so networking pros can tailor the tool to their exact needs. And those needs can range from basic traffic transmission testing to intrusion prevention, analysis of bandwidth usage, application security testing and identification of faulty configurations.

Activity watcher

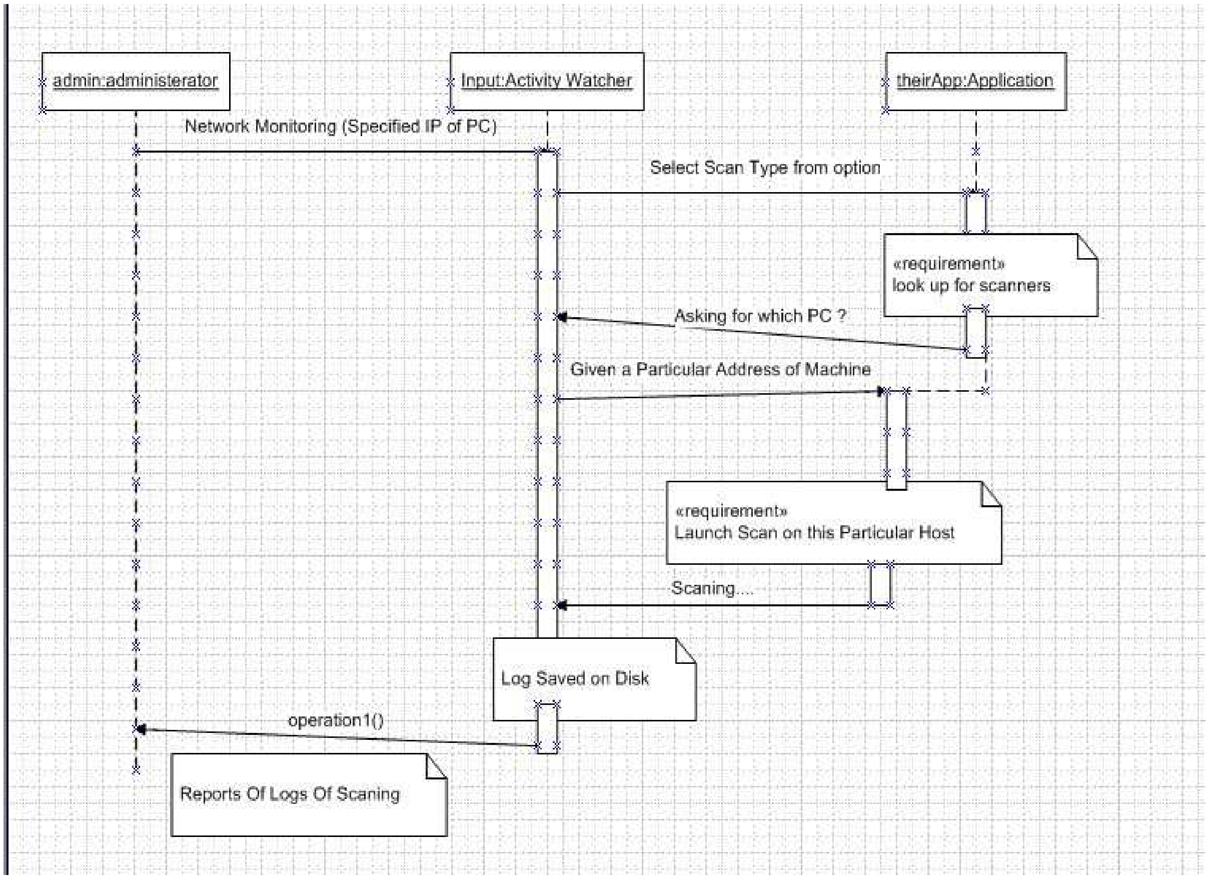


Figure: 3.5.3

It will then itself analyze the traffic and match with the defined rules and standards and record the particular packets and show the output or generate any message to the administrator.

Network Monitoring using Wireshark

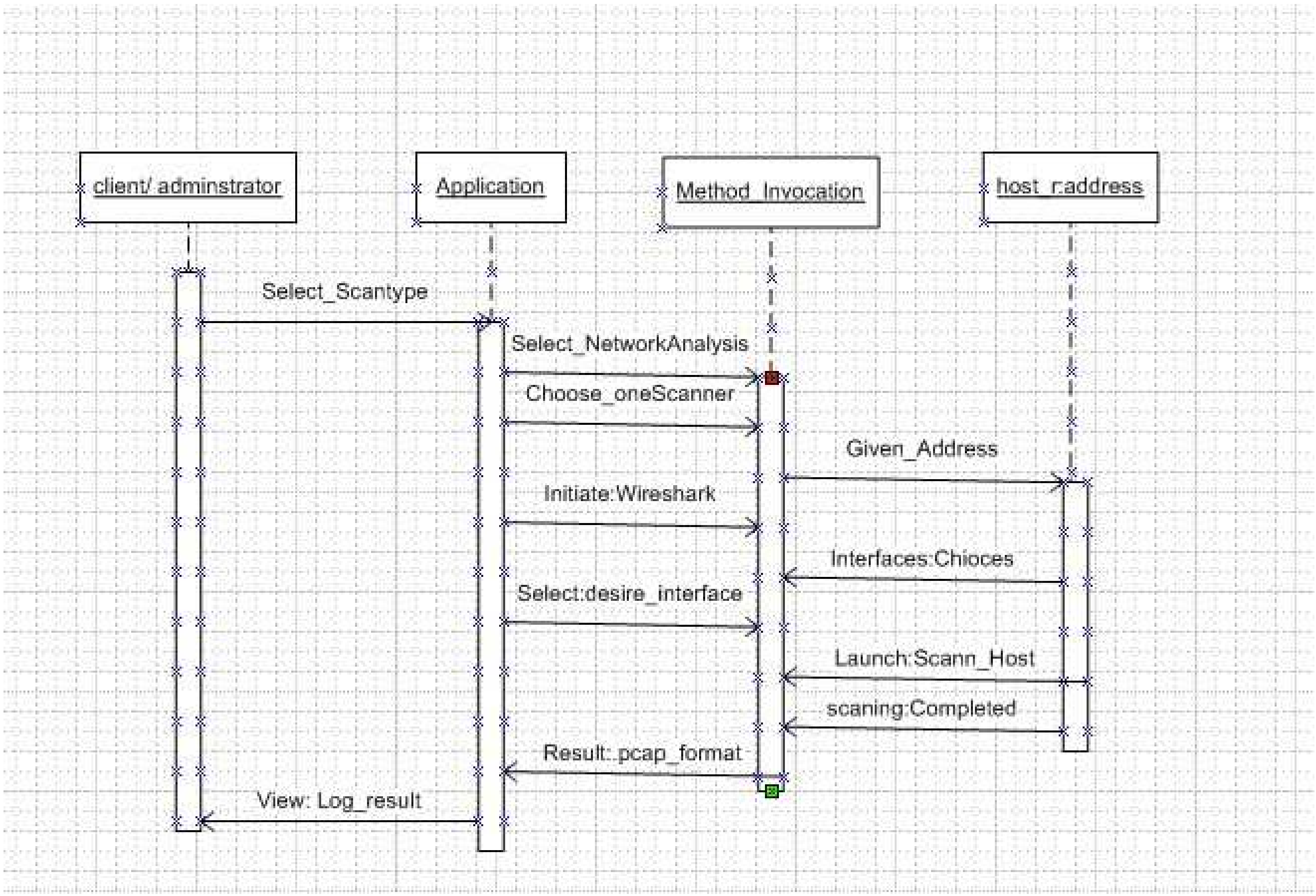


Figure: 3.5.4

Nmap uses raw IP packets in novel ways to determine what hosts are available on the network, what services (application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. While Nmap is commonly used for security audits, many systems and network administrators find it useful for routine tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime.

Network Monitoring using Nmap

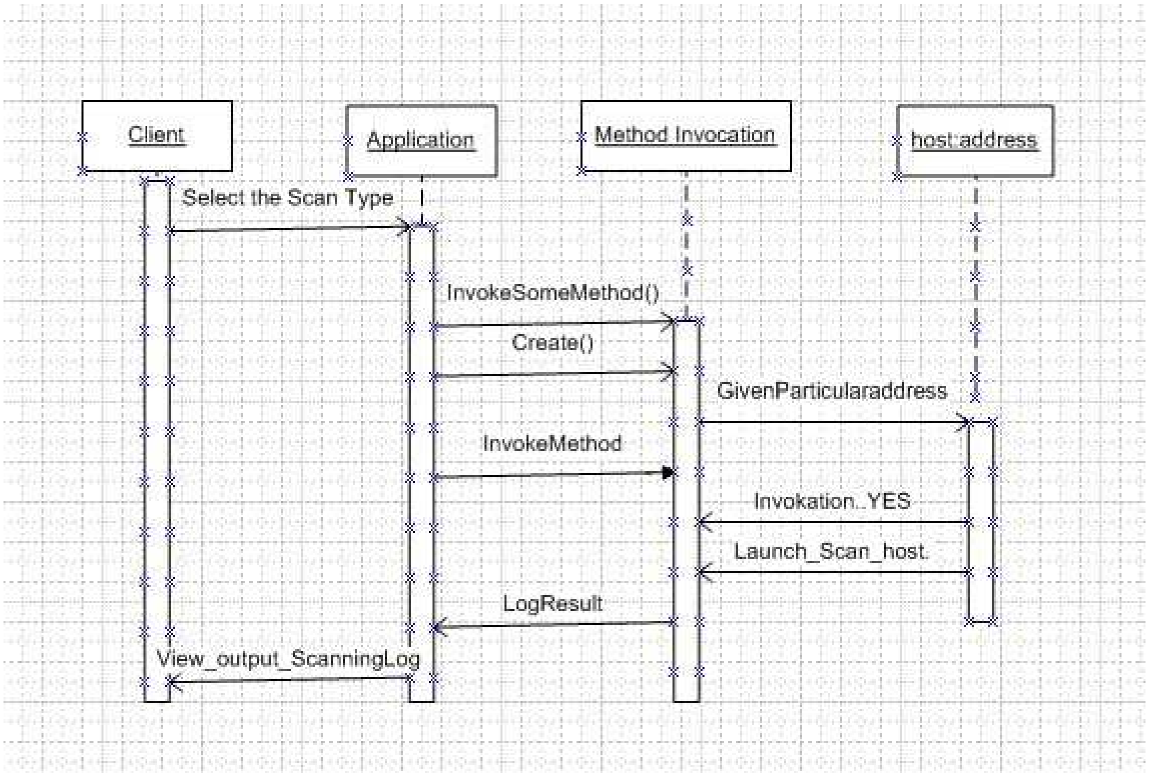


Figure: 3.5.5

Once an infrastructure is built which is secure and trustworthy, then we can launch on any service or activity in that infrastructure, for instance an activity watcher is an application which is migrated and launched on this infrastructure and it gives us all the processes and .exe files, cookies and recent data used.

Snort NIDS (network intrusion detection system)

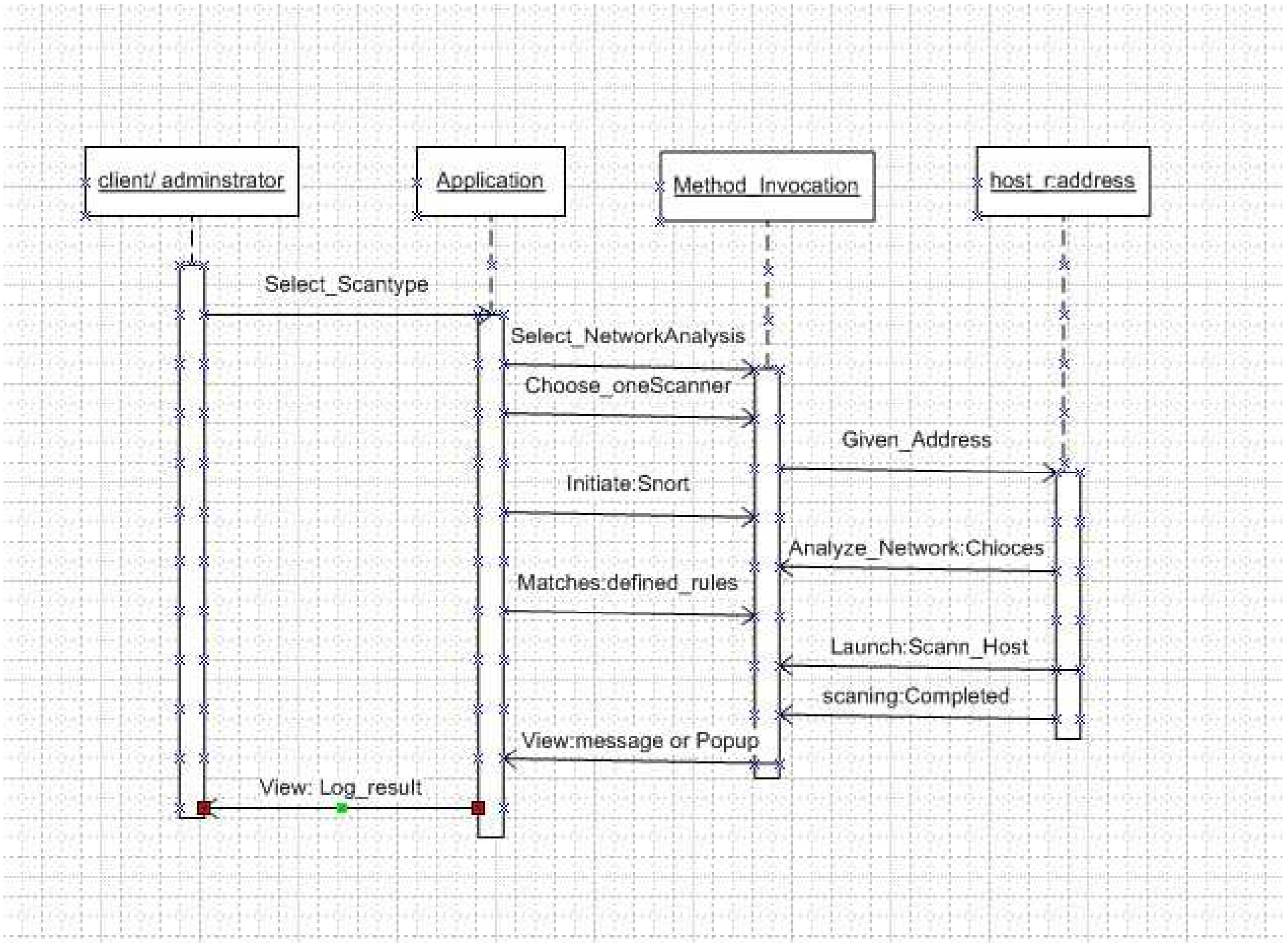


Figure: 3.5.6

3.6.Flow Chart:

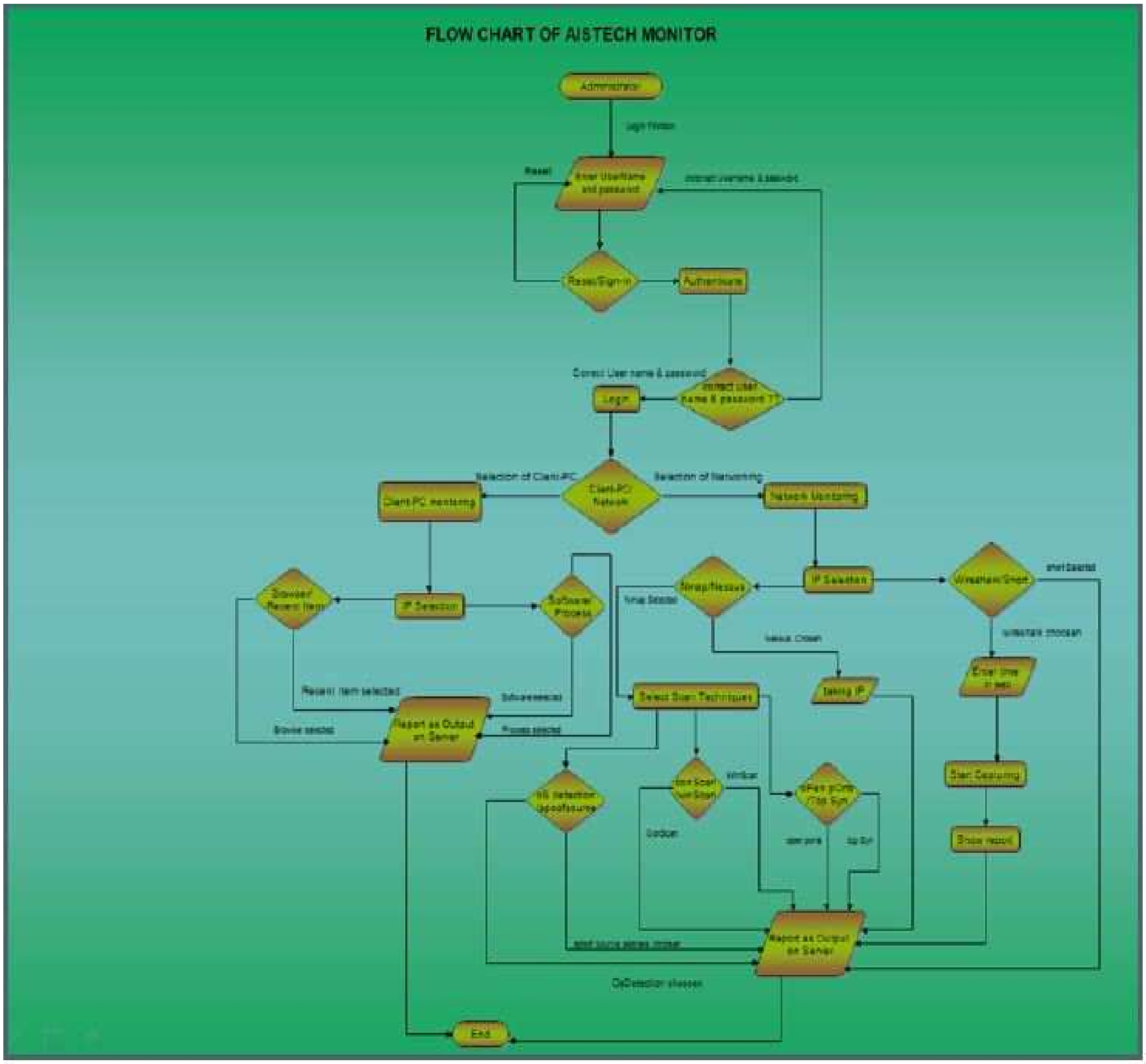


Figure: 3.6

Chapter 04

4. METHODOLOGY

The methodology and how this project will work are discussed in this section. To build a secure network infrastructure by achieving weak mobility, we have to use the object serialization methods of java over the network sockets. After all, application that we have built named "activity watcher" is launched on this infrastructure and it shall migrate to the network and perform its particular tasks and functionalities discussed in the functional requirement section above. We shall also configure Snort which is an intrusion detection system (IDS) and will be merged with this infrastructure.

To create a secure infrastructure for the mobile agents we have to follow following five services which are provided by the system architecture.

4.1.Achieving weak mobility using object serialization

In this service a code is created and assigned specification of their functions and services. In this service we achieved the weak mobility of agent sing object serialization in java. In fact weak mobility of agent means that, agent cannot save its state and next time it has no strength of retaining its original state and execution flow stops and following is the fragmentation of code using weak mobility.

```
void main(String args[]) {
... // some instructions
go(“NewNode”, “NewMethod”);
// not reached
} //end of main
void NewMethod() {
// the execution restarts HERE
...
} //end of NewMethod
```

On a Pc of LAN, a code of weak mobility launches on the network using network socket programming and it retrieve local information, installed software, memory usage and browser’s history to administrator

4.2.Launch of agents on network

At the end, when all issues are resolved and services are taken place then final step on the server is to launch the agent so it should migrate on the network and run on the remote host in that particular network.

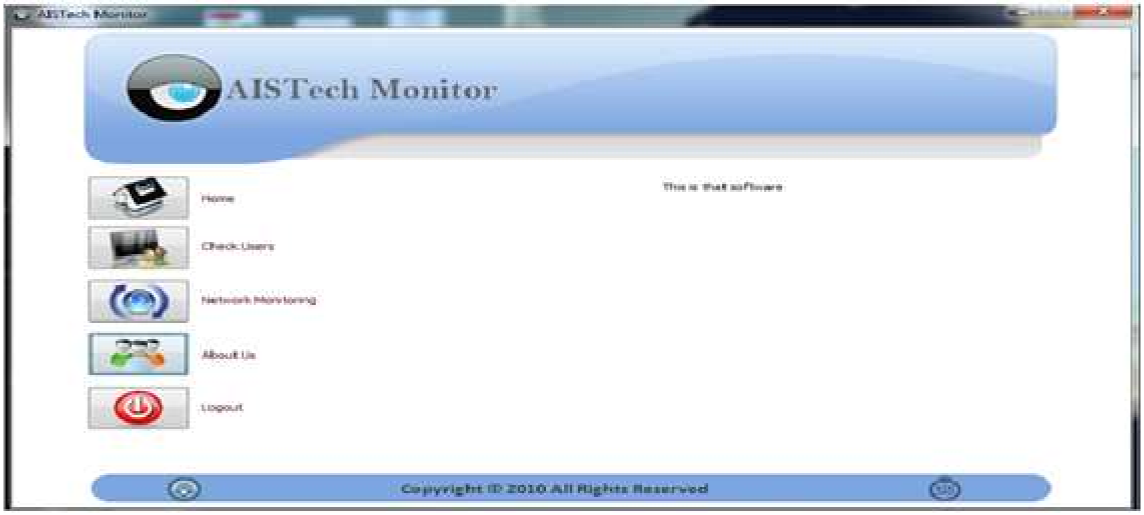
4.3.Run network security scanner on host

When the agent is migrated on the network then it comes on the remote host, these all functionalities are achieved using object serialization. After the entire agent launches and run it on the remote host and gather the results of network monitoring and analysis on the remote host.

4.4.Activity watcher

Our application the activity watcher not only gathers the information like the recent items accessed on the remote host but also the network monitoring which all comes in the watching the activities on the network**.** The initialization of the network scanners is performed on the remote host by the administrator and these scanners on their own behalf collect information on the remote host of network monitoring and then launching activity watcher application on this system and merge to with the system. The main functionalities of the activity watcher application are returning the browser cookies, running processes, software installed and .exe files. When the code of activity watcher application is merged with the system and then agent creator will write a code and this particular application shall do its services. This all process shall be secure and reliable and the transfer of mobile agent, migrating through network will be the main objective to be achieved.

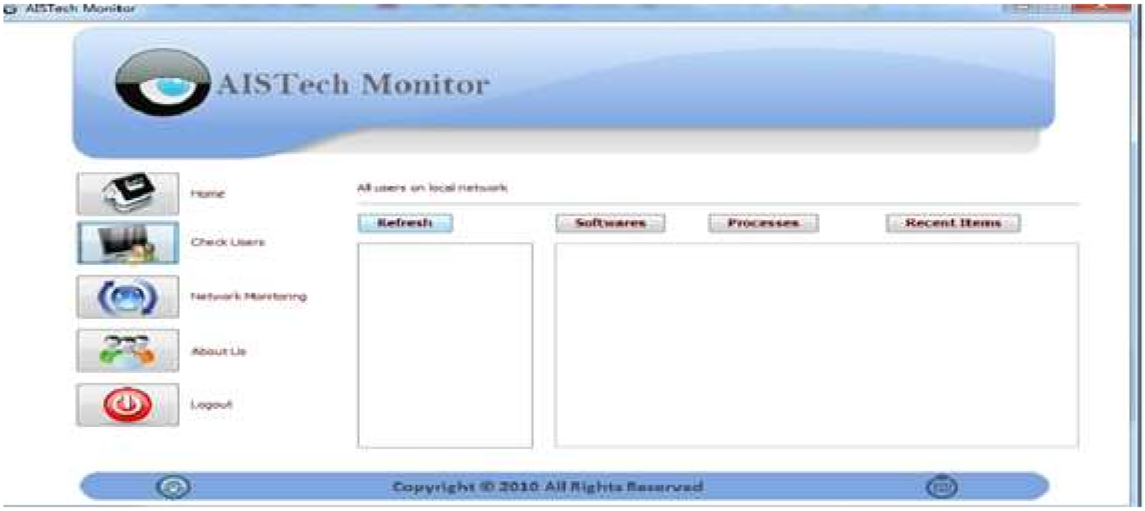
The main interfaces of AISTech monitor (Activity watcher application)



This is that software

Figure:4.4.0

The main interfaces of AISTech monitor (Activity watcher application)



All users on local network

Figure: 4.4.1

5. CONCLUSION

5.1.Problems and challenges:

- Configuration of Network Scanners
- Implementing Network Scanners and launching on client machine
- Integration of network scanners
- Agents communication

5.2.Achieved targets

All objectives have achieved in "AISTech Monitor"

- Background study of mobile agents
- Activity watcher application for LAN-PCs
- Network security scanners configuration
- Integrating modules
- Reports generation

6. APPENDEX

6.1.Network Scanners:

There are a number of network scanners, which are helpful for the work of network administrator. These are very useful for the monitoring of network traffic, ports analysis on network, the vulnerabilities on any host in the network etc.

We have worked on four network scanners in our project, which are rated the top 4 network scanners which include; Nessus, nmap, snort and Wireshark. The tutorials included for each of the network scanners is as under:

- Installation of network scanners:
- Installation of Nessus network scanner

Introduction:

This document is about the installation and configuration of Tenable Network Security's Nessus. How did I use the Nessus_4.4 as a network scanner in the network? Please do share your comments and suggestions about this basic tutorial on Muddasser.mahmood@seecs.edu.pk.

What is Nessus?

Tenable Network Security's Nessus is a vulnerability scanner is a world leader in active scanners, featuring high-speed discovery, configuration auditing, and asset profiling, sensitive data discovery and vulnerability analysis of security posture. Nessus scanners can be distributed throughout an entire enterprise, inside DMZs and across physically separate networks. Tenable Network Security, Inc. is the author and manager of the Nessus Security Scanner. In addition to constantly improving the Nessus engine, Tenable writes most of the plug-in available to the scanner, as well as compliance checks and a

wide variety of audit policies. (http://www.tenable.com/products/nessus)

The main features of Nessus are as under:

- High speed scanning: scan the entire network in no time and fast.
- Agent less audits: it tests the patches, configurations and content.

- In-depth assessments: it keenly tests the network devices, systems, and application.

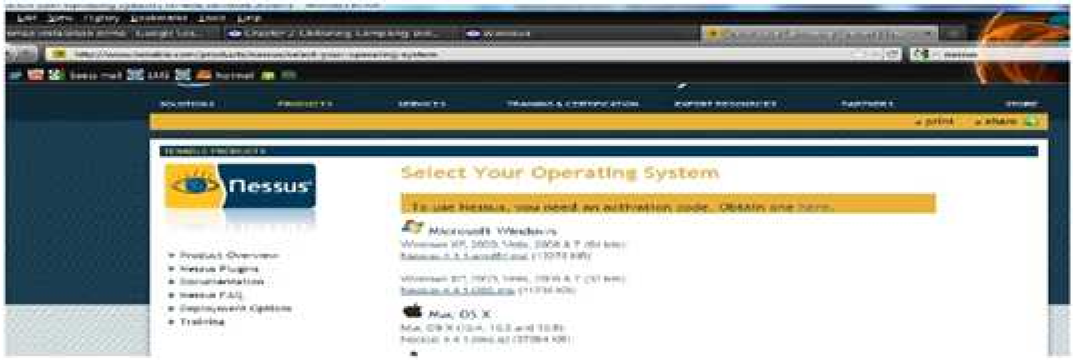
Prerequisites

Though Nessus installation and configuration can be done on multiple platforms like, windows, UNIX, Suse, RedHat, Solaris, and Debian 5, but I have installed and configured it on Windows 7 Professional. System prerequisites are as under to install Nessus.

- Tenable recommends a minimum of 1 GB of memory to operate Nessus. To conduct larger scans of multiple networks, at least 2 GB of memory is recommended, but it may require up to 4 GB.
- A Pentium 3 processor running at 2 GHz or higher is recommended. When running on Mac OS X, a dual-core Intel® processor running at 2 GHz or higher is recommended.

6.1.1. Steps to install Nessus

First of all, you need to download Nessus 4.2.2 and Nessus can be installed various OS such as Microsoft Windows, Mac OS, Linux, FreeBSD, and Solaris. In this example, I have installed it in Windows 7.



Select Your Operating System

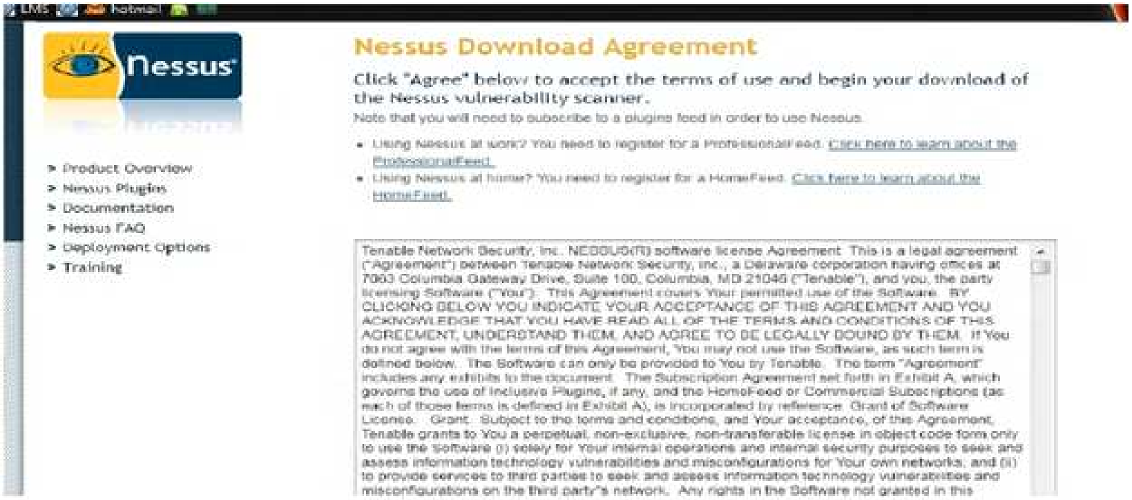
To use Nessus, you need an activation code. Obtain one here.

Microsoft Windows

Mac OS X

Figure: 6.1.1

After you select the correct operating system version it will show a up page of software license agreement. In order to download Nessus you need to click on the "I Accept" Button in order to continue further.



Nessus Download Agreement

Click "Agree" below to accept the terms of use and begin your download of the Nessus vulnerability scanner.

Note that you will need to subscribe to a plugins feed in order to use Nessus.

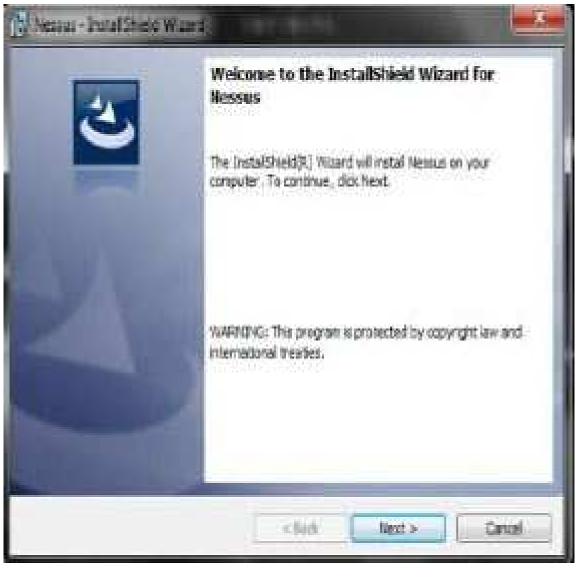
- Using Nessus at work? You need to register for a ProfessionalFeed. Click here to learn about the ProfessionalFeed.
- Using Nessus at home? You need to register for a HomeFeed. Click here to learn about the HomeFeed.

Tenable Network Security, Inc. NESSUS(R) software license Agreement. This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM. If You do not agree with the terms of this Agreement, You may not use the Software, as such term is defined below. The Software can only be provided to You by Tenable. The term "Agreement" includes any exhibits to the document. The Subscription Agreement set forth in Exhibit A, which governs the use of Inclusive Plugins, if any, and the HomeFeed or Commercial Subscriptions (as each of those terms is defined in Exhibit A), is incorporated by reference. Grant of Software License. Grant. Subject to the terms and conditions, and Your acceptance, of this Agreement, Tenable grants to You a perpetual, non-exclusive, non-transferable license in object code form only to use the Software (i) solely for Your internal operations and internal security purposes to seek and assess information technology vulnerabilities and misconfigurations for Your own networks, and (ii) to provide services to third parties to seek and assess information technology vulnerabilities and misconfigurations on the third party"s network. Any rights in the Software not granted in this

Figure: 6.6.2

On screenshot below is where you select which type of processor and operating system that you plan to install it at. Once you have downloaded Nessus, it's time to install Nessus on your machine by double- clicking on the icon to run set up of Nessus downloaded in your directory. Steps involved in installing Nessus on windows 7 are as under:

- Once the setup loaded click "Next"



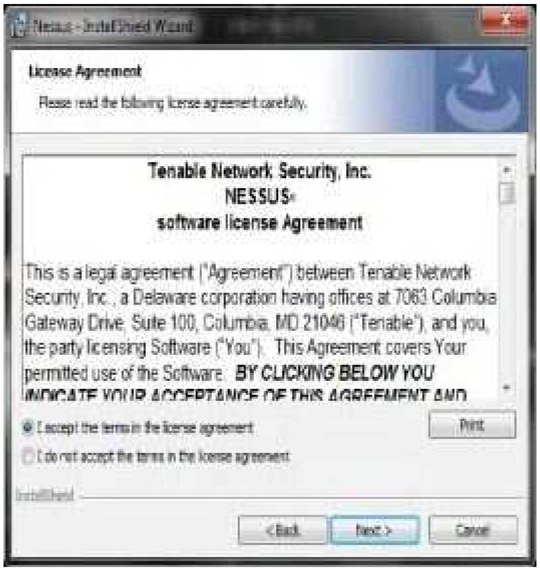
Welcome to the InstallShield Wizard for Nessus

The InstallShield(R) Wizard will install Nessus on your computer. To continue, click Next.

WARNING: This program is protected by copyright law and international treaties.

Figure:6.6.3

- The next screen is the software agreement read the agreement and click on "I accept the terms in the license agreement" in order to continue. After you have agreed click “next”



License Agreement

Please read the following license agreement carefully.

Tenable Network Security, Inc.
NESSUS®
software license Agreement

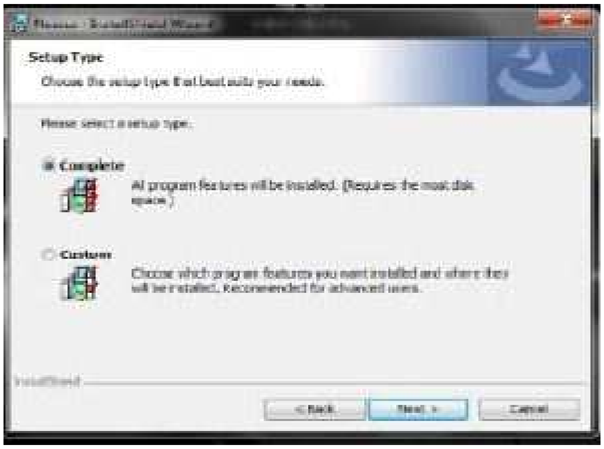
This is a legal agreement ("Agreement") between Tenable Network Security, Inc., a Delaware corporation having offices at 7063 Columbia Gateway Drive, Suite 100, Columbia, MD 21046 ("Tenable"), and you, the party licensing Software ("You"). This Agreement covers Your permitted use of the Software. ***BY CLICKING BELOW YOU INDICATE YOUR ACCEPTANCE OF THIS AGREEMENT AND***

● I accept the terms in the license agreement

○ I do not accept the terms in the license agreement

Figure: 6.6.4

- The next screen show where you want to install Nessus. By default it is set to install in the program files in C: \ drive. Press "Next" to continue
- Choose "Complete" in order to receive all functions of the program can click "Next" to continue.



Nessus - InstallShield Wizard

Setup Type

Choose the setup type that best suits your needs.

Please select a setup type.

● Complete

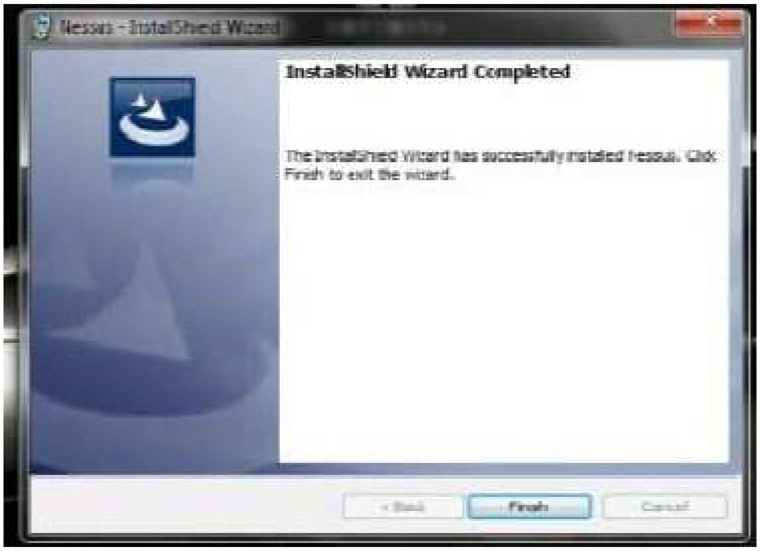
All program features will be installed. (Requires the most disk space.)

○ Custom

Choose which program features you want installed and where they will be installed. Recommended for advanced users.

Figure: 6.6.5

- Now you're ready to install click "Install" to continue. Click "Finish" to close the setup and you're done.



Nessus - InstallShield Wizard

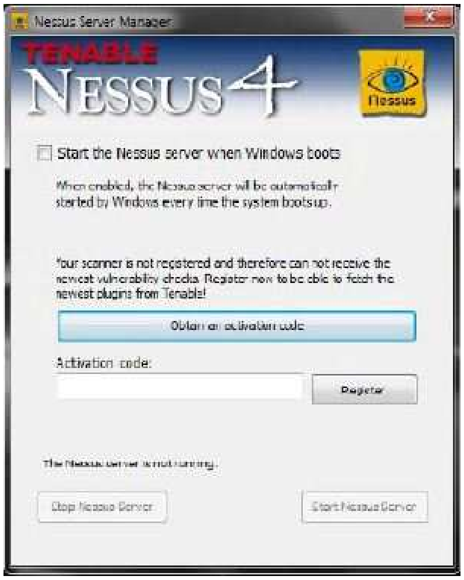
InstallShield Wizard Completed

The InstallShield Wizard has successfully installed Nessus. Click Finish to exit the wizard.

Figure:6.6.6

- You should make sure that you look two icons on your desktop: one is Nessus server manager and other is Nessus client.

- First Uncheck the "Start the Nessus server when Windows Boots" if you do not Nessus to start when you turn on your computer. In to use Nessus to the fullest you need have to an activation code. Just Click on the button that says "Obtain an activation code" it will open your web browser.



□ Start the Nessus server when Windows boots

When enabled, the Nessus server will be automatically started by Windows every time the system boots up.

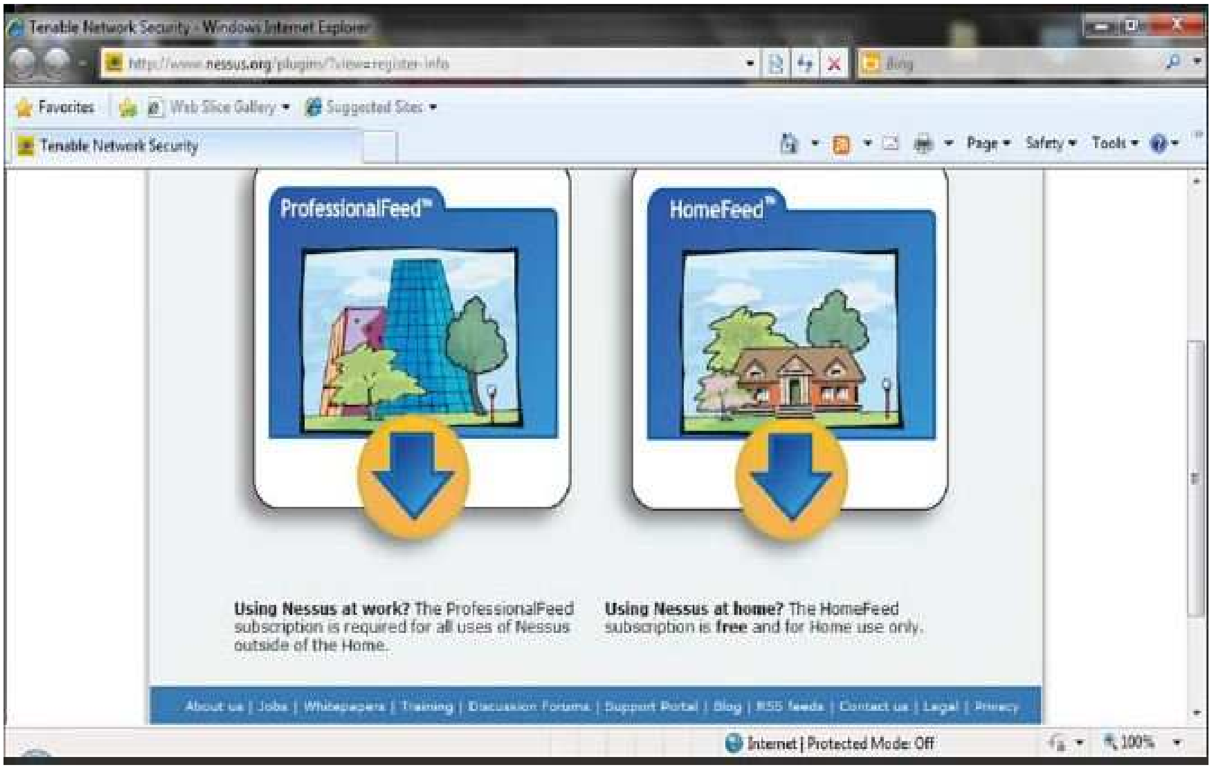
Your scanner is not registered and therefore can not receive the newest vulnerability checks. Register now to be able to fetch the newest plugins from Tenable!

Activation code:

The Nessus server is not running.

Figure:6.6.7

There are two types of subscriptions. There is the Professional Feed and Home Feed. Commercial organizations that use the Nessus vulnerability scanner must purchase a Professional Feed subscription to scan their network, obtain support, updates to their database of vulnerability checks and compliance auditing.


Tenable Network Security - Windows Internet Explorer
http://www.nessus.org/plugins/?view=register-info
Bing
Favorites
Web Slice Gallery
Suggested Sites
Tenable Network Security
Page
Safety
Tools
ProfessionalFeed™
HomeFeed™

Using Nessus at work? The ProfessionalFeed subscription is required for all uses of Nessus outside of the Home.

Using Nessus at home? The HomeFeed subscription is **free** and for Home use only.

About us | Jobs | Whitepapers | Training | Discussion Forums | Support Portal | Blog | RSS feeds | Contact us | Legal | Privacy
Internet | Protected Mode: Off
100%

Figure:6.6.8

The ProfessionalFeed receive immediate access to:

The newest Nessus plugins as soon as they are released. Perform an unlimited amount of complete PCI-DSS compliance audits. Perform web application audits of custom and embedded applications to test for cross site scripting, SQL injection. Conduct operating system, application and SQL database configuration audits against CERT, CIS, DISA STIGs, GLBA, HIPAA, NIST SCAP FDCC, NSA and PCI standards. Conduct content audits such as adult content, personally identifiable information (credit cards, SSN, etc.) corporate spreadsheets, and much more. SCADA vulnerability checks to detect and audit

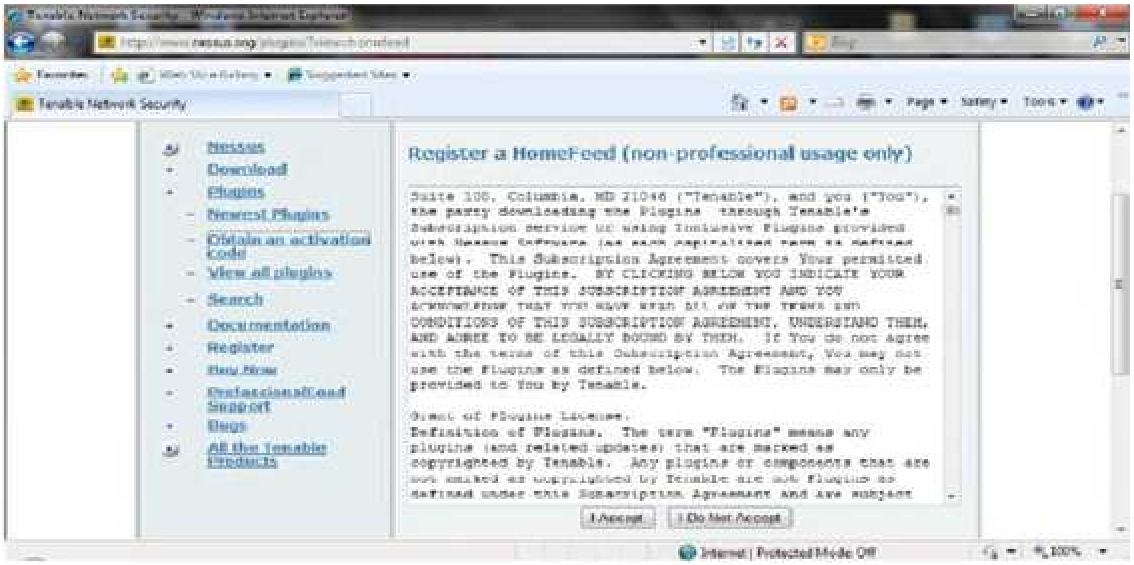
Control System devices. Each ProfessionalFeed costs $1,200 per year per Nessus scanner and can be purchased from a Authorized ProfessionalFeed Partners or Tenable's online Store. Hardware appliance options are also available (Only available in the US).

The HomeFeed receive immediate access to:

The HomeFeed subscription is available for home use **ONLY**. The HomeFeed Subscription is a non-commercial subscription that permits you to use the plugins in conjunction with Registered Scanners for your personal use solely to detect vulnerabilities only on your own personal system (or for your own personal network) that you use for non-commercial purposes or on the personal system (or for the personal network) of another natural person in a non-commercial arrangement. You are not eligible to subscribe to the HomeFeed Subscription if you are a corporation, a governmental entity or any other form of organization. You may not subscribe to the HomeFeed Subscription to use the Plugins on a computer owned by your employer or otherwise use the Plugins for the benefit of or to perform any services for any corporation, governmental entity or any other form of organization.

Obtain activation code and activate Nessus:

Steps involved are:

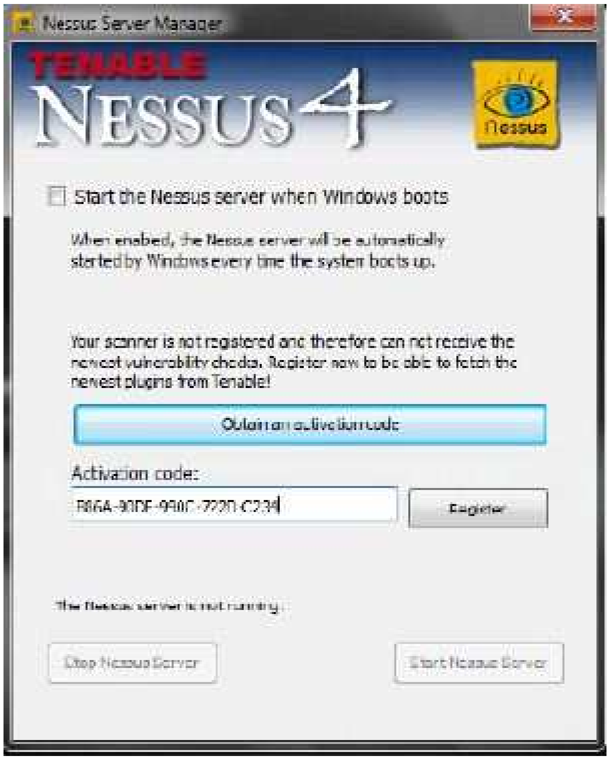


Register a HomeFeed (non-professional usage only)

```
Suite 100, Columbia, MD 21046 ("Tenable"), and you ("You"),
the party downloading the Plugins through Tenable's
Subscription service or using Inclusive Plugins provided
with Nessus Software (as each capitalized term is defined
below). This Subscription Agreement covers Your permitted
use of the Plugins. BY CLICKING BELOW YOU INDICATE YOUR
ACCEPTANCE OF THIS SUBSCRIPTION AGREEMENT AND YOU
ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND
CONDITIONS OF THIS SUBSCRIPTION AGREEMENT, UNDERSTAND THEM,
AND AGREE TO BE LEGALLY BOUND BY THEM. If You do not agree
with the terms of this Subscription Agreement, You may not
use the Plugins as defined below. The Plugins may only be
provided to You by Tenable.

Grant of Plugins License.
Definition of Plugins. The term "Plugins" means any
plugins (and related updates) that are marked as
copyrighted by Tenable. Any plugins or components that are
not marked as copyrighted by Tenable are not Plugins as
defined under this Subscription Agreement and are subject
```

Figure:6.6.9



□ Start the Nessus server when Windows boots

When enabled, the Nessus server will be automatically started by Windows every time the system boots up.

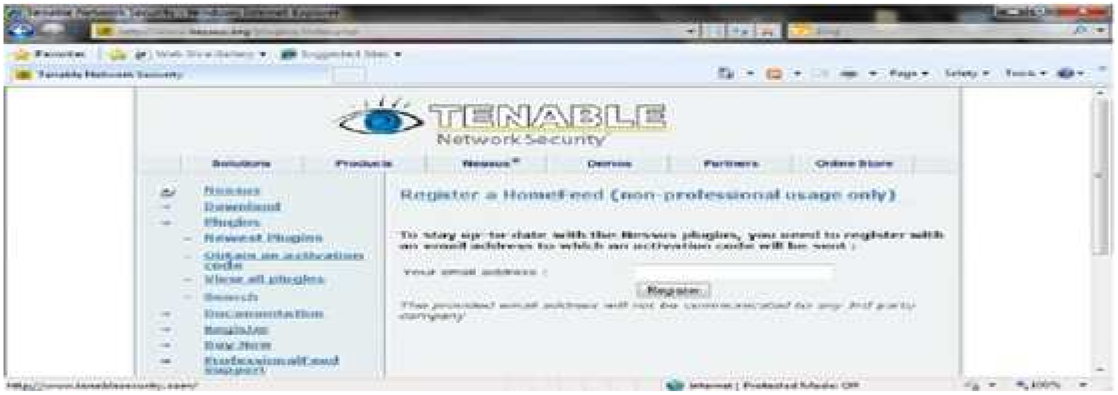
Your scanner is not registered and therefore can not receive the newest vulnerability checks. Register now to be able to fetch the newest plugins from Tenable!

Activation code: B86A-30DF-990C-722D-C234

The Nessus server is not running.

Figure:6.7.0

- Type your e-mail address in order for Nessus to send you an activation code.



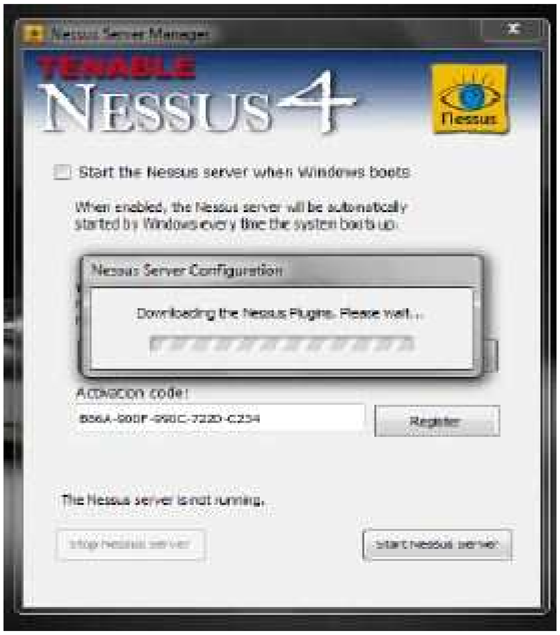
Register a HomeFeed (non-professional usage only)

To stay up-to-date with the Nessus plugins, you need to register with an email address to which an activation code will be sent :

Your email address :

The provided email address will not be communicated to any 3rd party company

- Once you have submitted your e-mail you will receive an e-mail containing the activation code. Also, in the e-mail will contain on how to insert the code on Microsoft Windows
- Go back to the "Nessus Server Manager" insert your activation code and click on "Register". It is going to activate Nessus and also download the latest plugins and process is going to take about 15 to 30 mins.



Nessus Server Manager

□ Start the Nessus server when Windows boots

When enabled, the Nessus server will be automatically started by Windows every time the system boots up.

Nessus Server Configuration

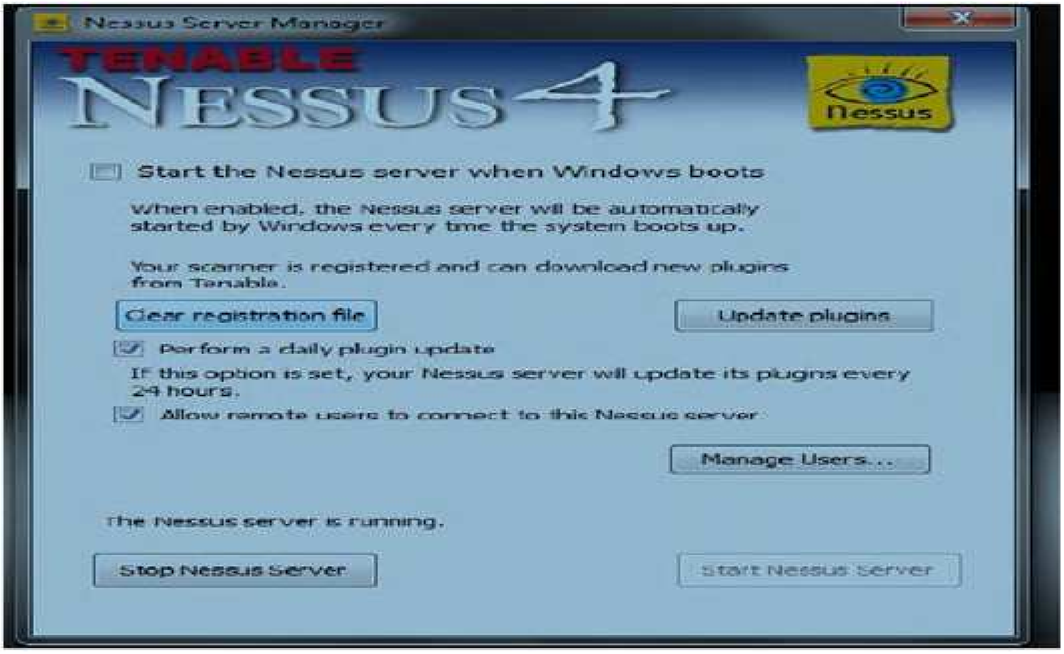
Downloading the Nessus Plugins. Please wait...

Activation code: B86A-900F-990C-722D-C234

The Nessus server is not running.

Figure: 6.7.1

- You're almost done there are two check boxes. If the "Perform a daily plugin update" check then Nessus will update its plugins every 24 hours. If the "Allow remote users to connect to this Nessus server" check then other computers on the network can type your IP Address on their own computer and login from there.



Nessus Server Manager

□ Start the Nessus server when Windows boots

When enabled, the Nessus server will be automatically started by Windows every time the system boots up.

Your scanner is registered and can download new plugins from Tenable.

☑ Perform a daily plugin update

If this option is set, your Nessus server will update its plugins every 24 hours.

☑ Allow remote users to connect to this Nessus server

The Nessus server is running.

Figure:6.7.2

- The screenshot show current user accounts:
  - The "edit" button is to modify users
  - The "plus (+)" button is for adding new users.
  - The "minus (-)" button is to remove users.

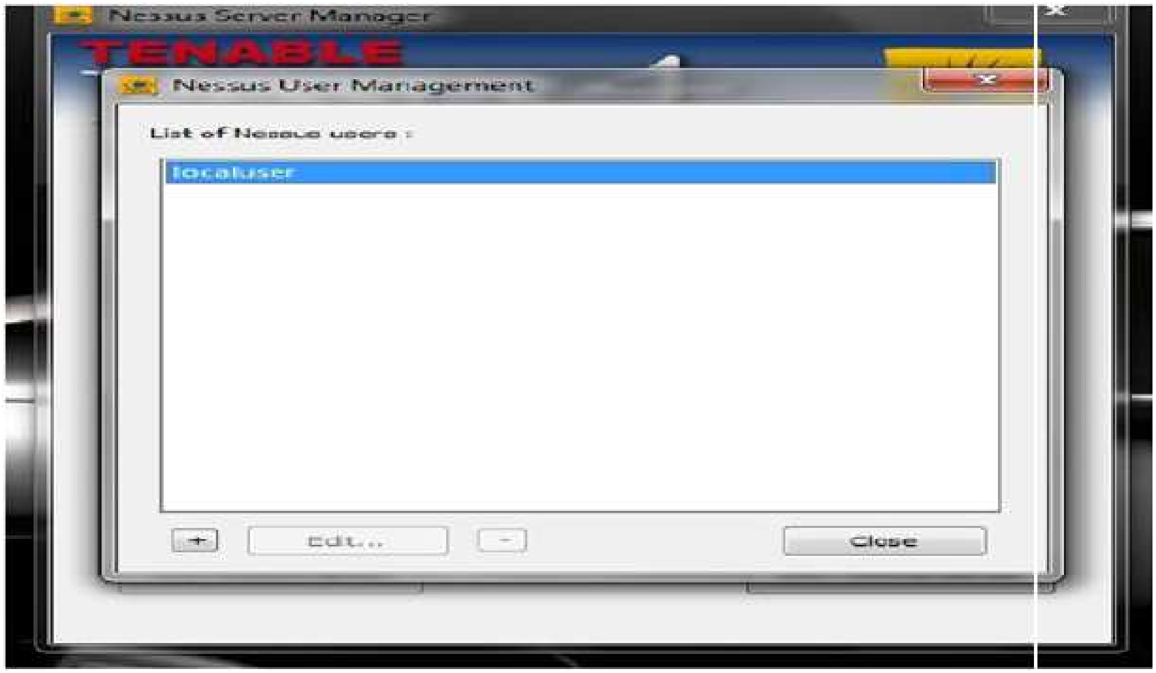


Figure:6.7.3

- Now you're ready to use Nessus let's begin. Click on "Nessus Client" icon. Nessus is a web application that runs on your web browser. The security certificate is going to appear just click on "Continue to this website (not recommended)". Accept the certificate and then it takes time to initialize Nessus
- This is you're login interface enter your Nessus credentials.

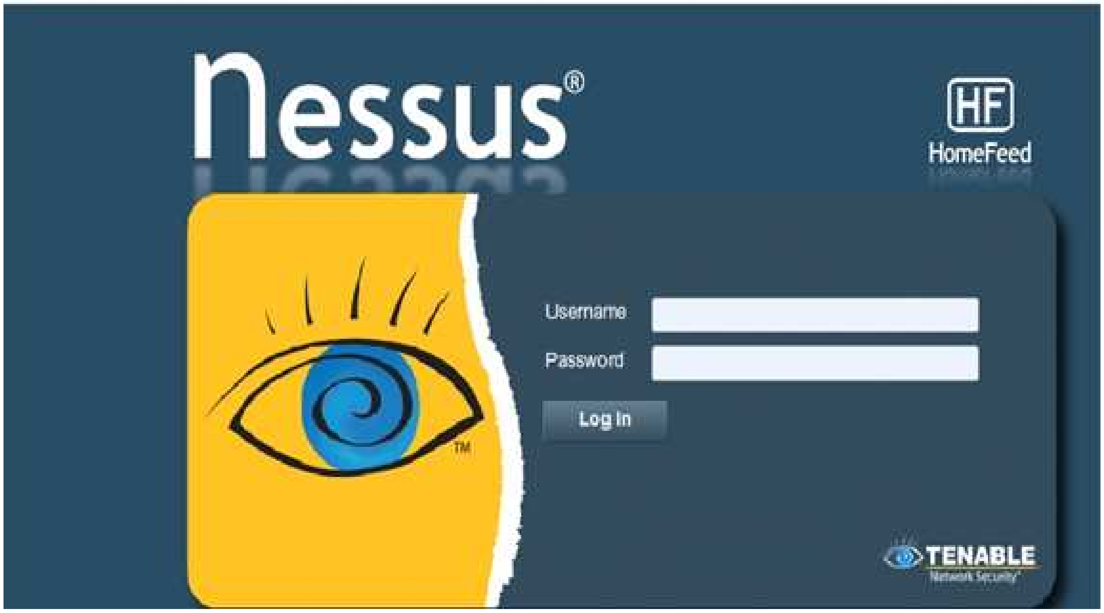
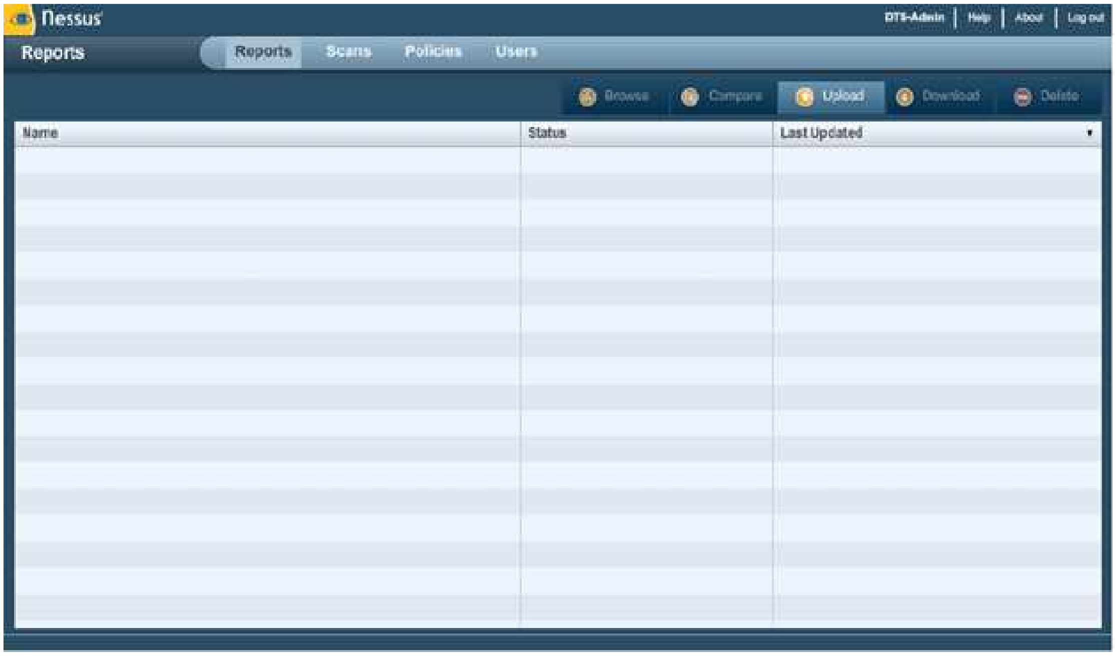


Figure:6.7.4

- By default it is going to load the "Reports". The "Reports" tab is where indicates either the penetration is running or it’s done.



Name	Status	Last Updated

Figure: 6.7.5

- To run a test you need to create a policy. Click on the "Policies" tab and click on the "Add" Button.

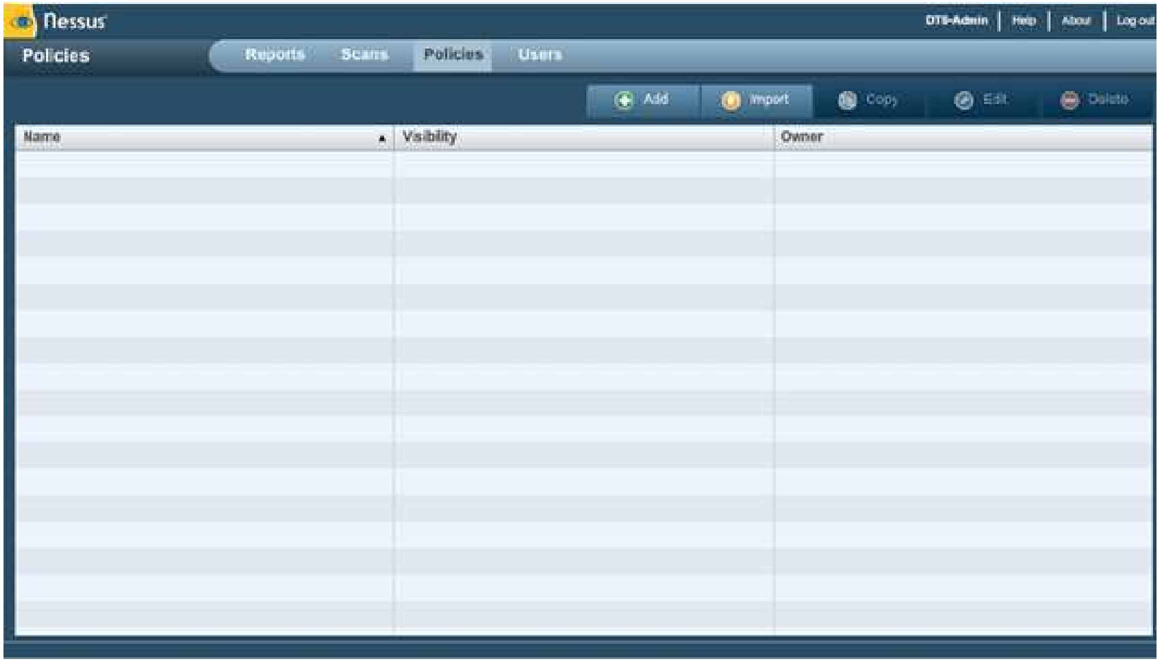
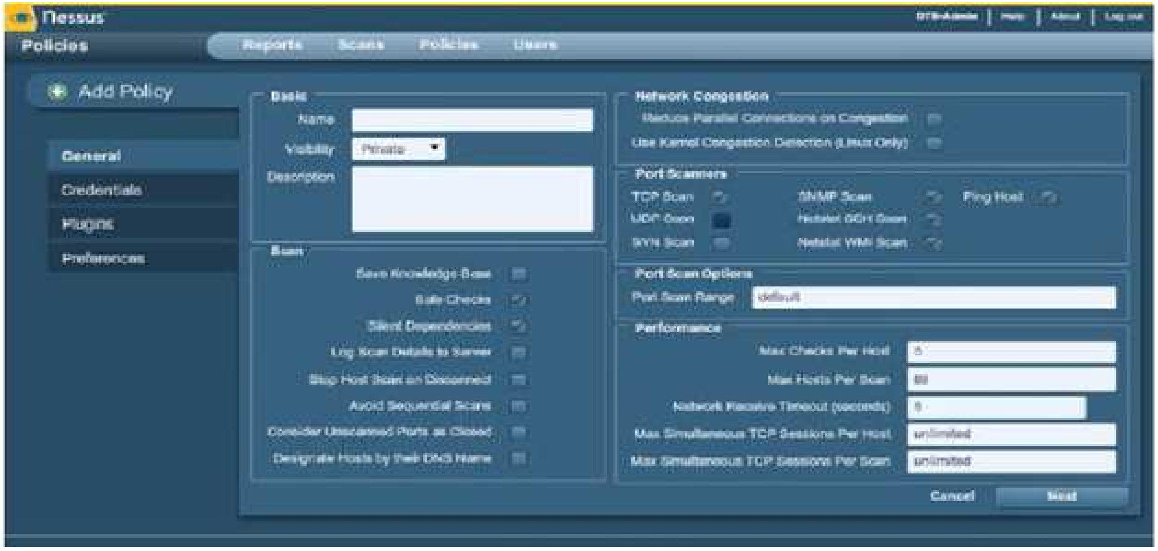


Figure:6.7.6

- On General Tab is where you name your policy and if you want to make your policy shared or private. Also, this is where you configure Nessus on how it behaves.



Basic

Name

Visibility: Private

Description

Scan

Save Knowledge Base □

Safe Checks ☑

Silent Dependencies ☑

Log Scan Details to Server □

Stop Host Scan on Disconnect □

Avoid Sequential Scans □

Consider Unscanned Ports as Closed □

Designate Hosts by their DNS Name □

Network Congestion

Reduce Parallel Connections on Congestion □

Use Kernel Congestion Detection (Linux Only) □

Port Scanners

TCP Scan ☑ SNMP Scan ☑ Ping Host ☑

UDP Scan □ Netstat SSH Scan ☑

SYN Scan □ Netstat WMI Scan ☑

Port Scan Options

Port Scan Range: default

Performance

Max Checks Per Host: 5

Max Hosts Per Scan: 80

Network Receive Timeout (seconds): 5

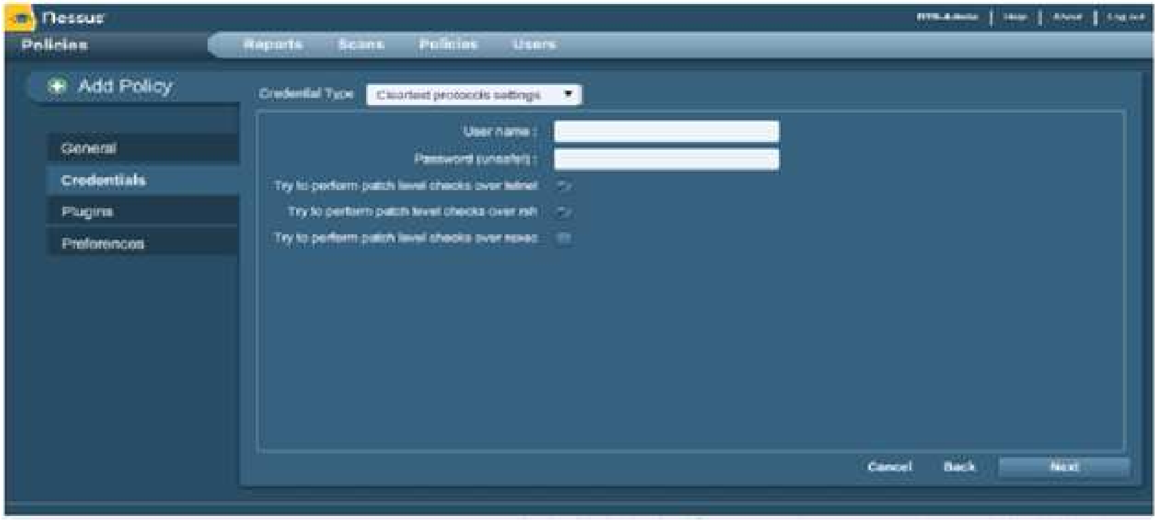
Max Simultaneous TCP Sessions Per Host: unlimited

Max Simultaneous TCP Sessions Per Scan: unlimited

Figure:6.7.7

- On the Credentials tab this is where enter any user name and password that you want to test such as Linux machine.

- On the Plug-ins tab is where you want to enable or disable test.



Credential Type: Cleartext protocols settings

User name :

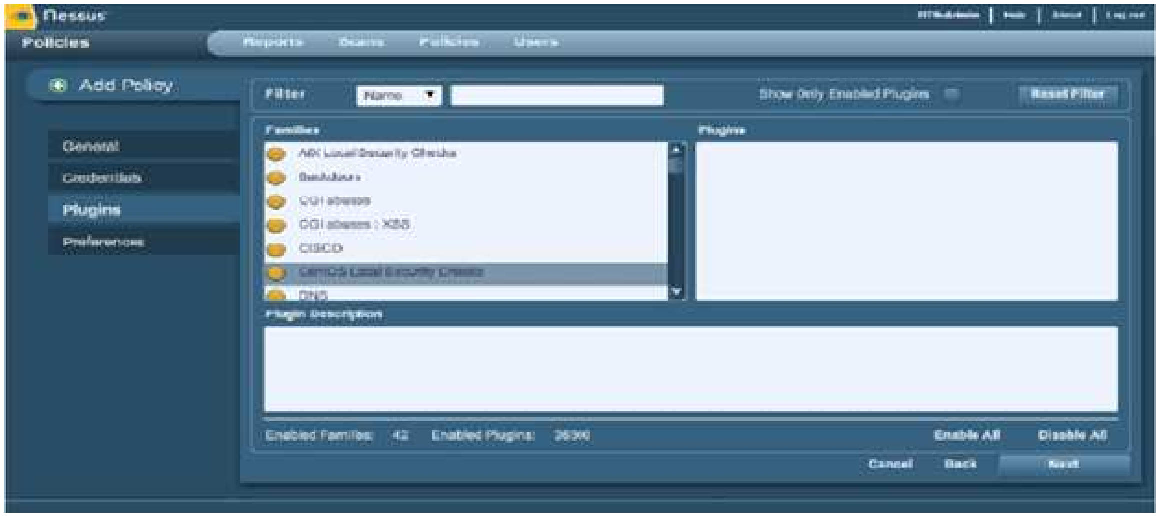
Password (unsafe) :

Try to perform patch level checks over telnet ☐

Try to perform patch level checks over rsh ☐

Try to perform patch level checks over rexec ☐

Figure:6.7.8



Filter: Name

Show Only Enabled Plugins ☐

AIX Local Security Checks

Backdoors

CGI abuses

CGI abuses : XSS

CISCO

CentOS Local Security Checks

DNS

Enabled Families: 42 Enabled Plugins: 36300

Figure:6.7.9

- The Preferences tab includes means for granular control over scan settings. Selecting an item from the drop-down menu will display further configuration items for the selected category.

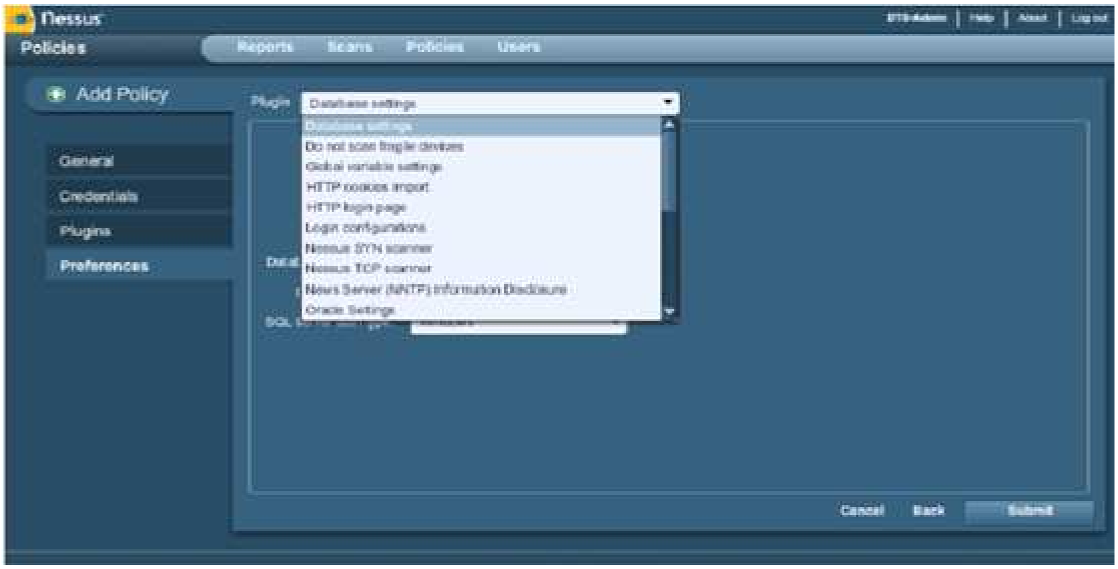


Figure:6.8.0

- Click on "Submit" button to save your policy and now you're ready to scan your network. You must read the user guide to properly configure the network scan and also it going much more detail on what every drop down option does.

  http://www.nessus.org/documentation/nessus_4.2_user_guide.pdf

6.2.Installation of Nmap security scanner:

Introduction:

This document is about the installation and configuration of Nmap network security scanner. How did I use the Nmap 5.51 as a network scanner in the network? Please do share your comments and suggestions about this basic tutorial on

Muddasser.mahmood@seecs.edu.pk.

What is NMAP?

Nmap ("Network Mapper") is a free of charge and open source (license) utility for network searching or security auditing. Many systems and network administrators also find it useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. It is very powerful, easy, popular and flexible tool. Nmap uses raw IP packets in novel ways to resolve what hosts are available on the network, what services application name and version) those hosts are offering, what operating systems (and OS versions) they are running, what type of packet filters/firewalls are in use, and dozens of other characteristics. It was designed to rapidly scan large networks, but works fine against single hosts. Nmap runs on all major computer operating systems. The main features of the Nmap security scanner are as under:

- Host discovery: Nmap is useful for discovery of in-use IP addresses and determine which hosts are up and which hosts are down by sending some "echo request".
- Port Scanning: it is quite helpful in determining open ports; open ports are the ports where services are representing listening services. Port scanning mechanism is used to check the compliance to policy: no web servers on the desktop, usually port scanning tells the port name, number and the associated services on that port with the help of Nmap.
- Nmap OS identification: Nmap assist in attempting the OS versions of the scanned systems or hosts. It requires discovering one open port and one closed port, after that observe the responses to packets sent from the open and the closed ports.

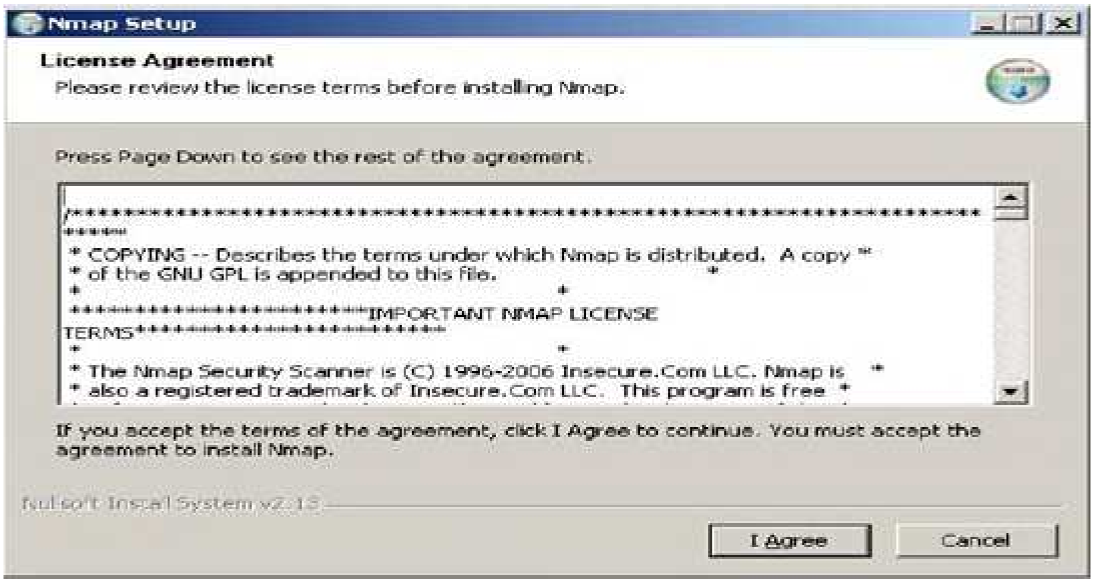
Prerequisites

It was written by security consultant, Fyodor. Nmap is basically designed for the larger networks, but works fine with the single host also. Nmap runs on all major computer operating systems, and official binary packages are available for Linux, Windows, and Mac OS X. In addition to the classic command- line Nmap executable, the Nmap suite includes an advanced GUI and results viewer (Zenmap), a flexible data transfer.

Steps to install Nmap:

We have installed Nmap on the windows machine, Nmap runs on all versions of Windows since NT, including 2K, XP, Vista, Windows 7, and Server 2003/2008. Installation of the Nmap is very easy and straight forward. Steps involved are following:

- First of all, download the installer file from the link http://nmap.org/download.html
- Double click the installer file. Accept the license agreement by clicking on the "I agree" button.



License Agreement

Please review the license terms before installing Nmap.

Press Page Down to see the rest of the agreement.

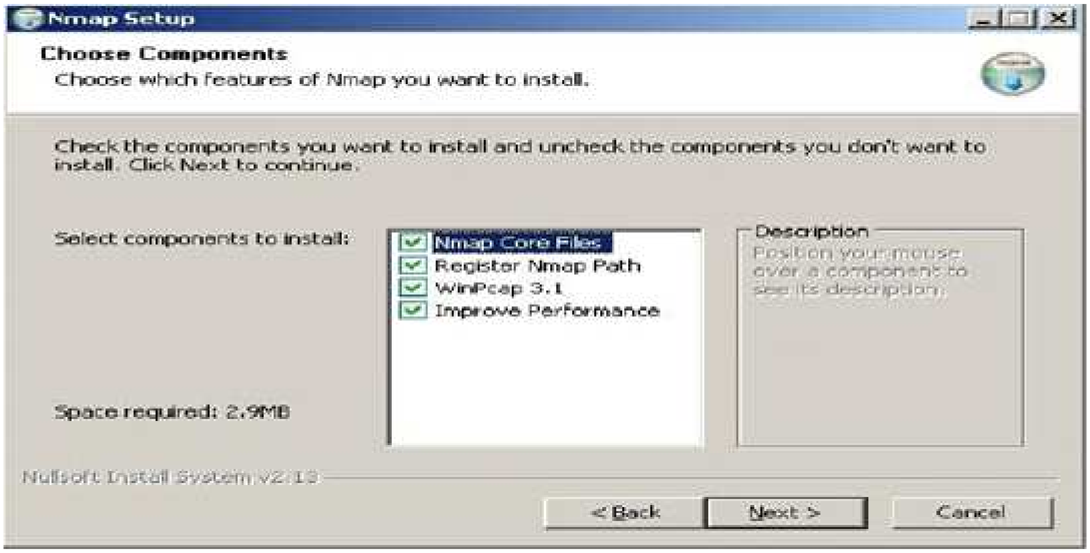
```
/***************************************************************************
*****
 * COPYING -- Describes the terms under which Nmap is distributed.  A copy *
 * of the GNU GPL is appended to this file.                        *
 *                                                  *
 ***************************IMPORTANT NMAP LICENSE
TERMS***************************
 *                                                  *
 * The Nmap Security Scanner is (C) 1996-2006 Insecure.Com LLC. Nmap is    *
 * also a registered trademark of Insecure.Com LLC.  This program is free  *
```

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install Nmap.

Nullsoft Install System v2.13

Figure: 6.8.1

- Accept the defaults on the Choose Components dialog box. Click the 'Next' button.


Nmap Setup
Choose Components
Choose which features of Nmap you want to install.

Check the components you want to install and uncheck the components you don't want to install. Click Next to continue.

Select components to install:

☑ Nmap Core Files
☑ Register Nmap Path
☑ WinPcap 3.1
☑ Improve Performance

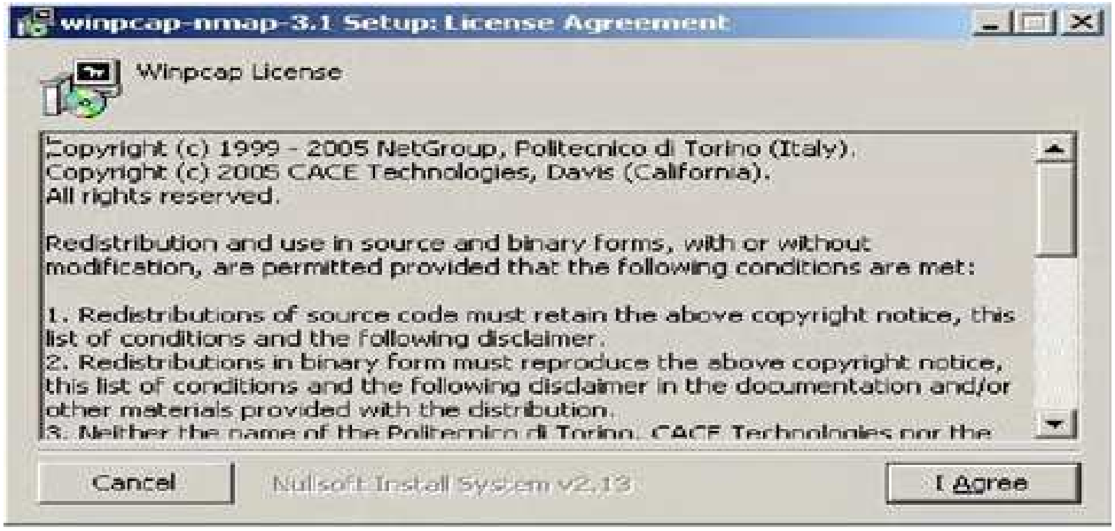
Description
Position your mouse over a component to see its description.

Space required: 2.9MB

Nullsoft Install System v2.13
< Back
Next >
Cancel

Figure:6.8.2

- Choose an installation directory (or accept the default). Click the 'Install' button. Installation of NMAP will proceed.
- Winpcap is required component of NMAP. Its installation will start during the install if NMAP. Read the license agreement and click the 'I Agree' button.



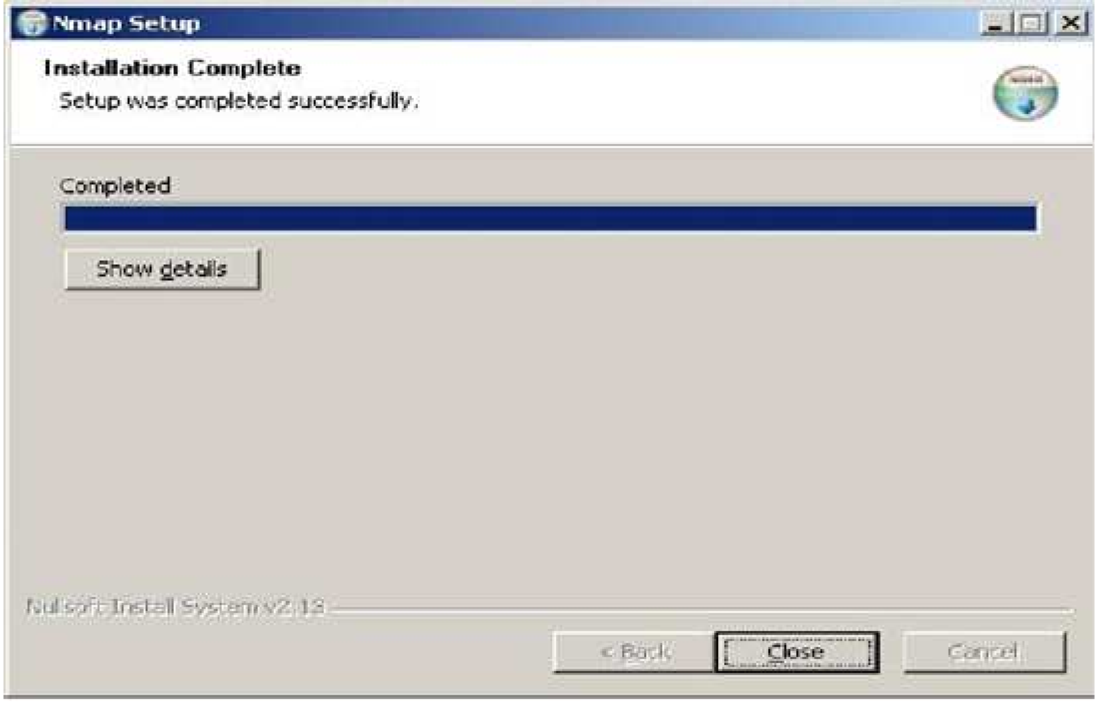
Copyright (c) 1999 - 2005 NetGroup, Politecnico di Torino (Italy).
Copyright (c) 2005 CACE Technologies, Davis (California).
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the Politecnico di Torino, CACE Technologies nor the

Figure:6.8.3

- Select an installation directory (or accept the default). Click the 'Install' button.
- The installation of Winpcap will now proceed. Click the 'Close' button on the Winpcap completed dialog box.



Nmap Setup

Installation Complete

Setup was completed successfully.

Completed

Nullsoft Install System v2.13

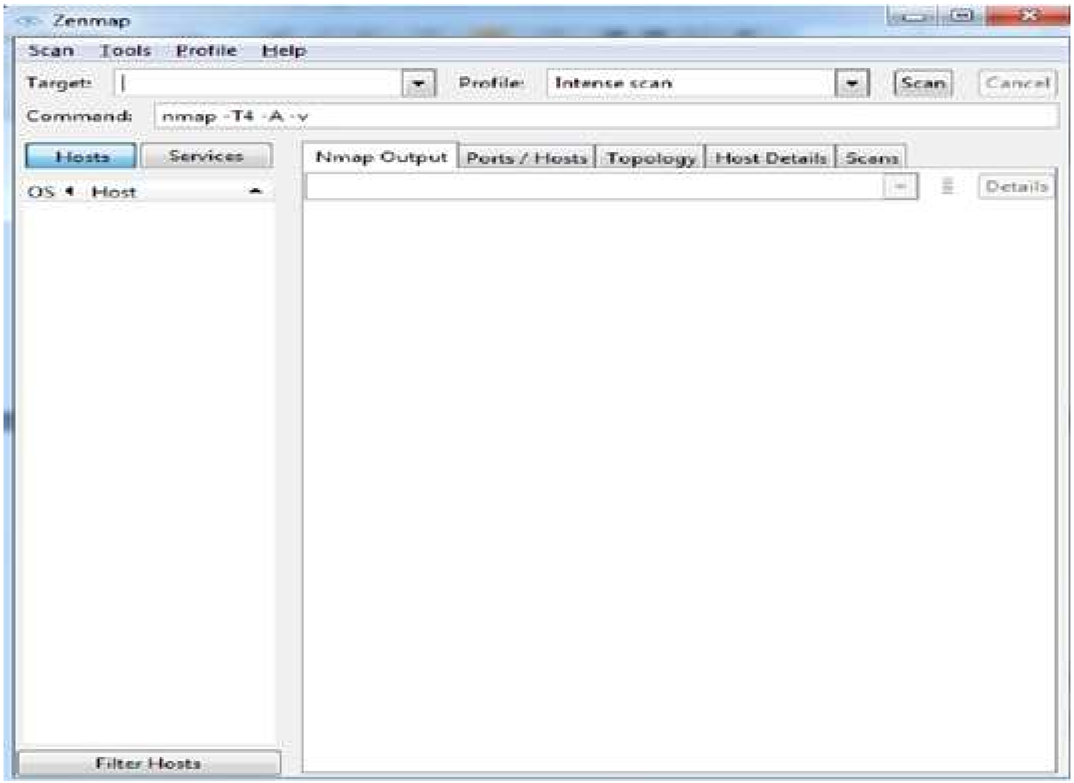
Figure:6.8.4

- Click the 'Close' button on the NMAP completed dialog box.

Running NMAP on Windows

Steps involved in running Nmap GUI interface named as Zenmap are as under:

- First of all double click the icon of the Nmap Zenmap GUI present on the desktop. When Nmap is opened, the following screen is showed.



Profile: Intense scan

Command: nmap -T4 -A -v

Figure:6.8.5

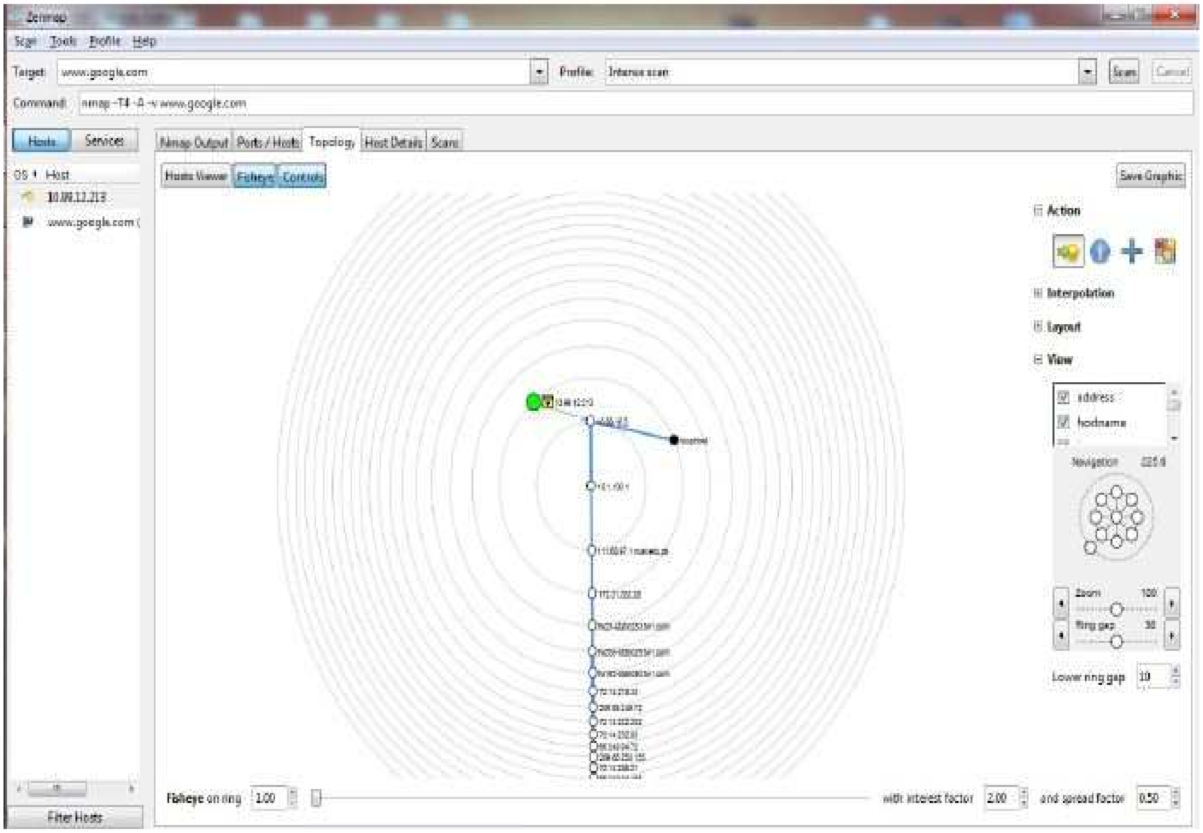
In the above screen, Write the target name or set of targets like 192.168.1.1(it is a single IP address) or 10.3.51.0/24(by giving set of IP addresses like to watch 255 address here it shall scan). In the profile option write the type of scan like intense scan, UDP scan, TCP scan etc. We can also give command here, if anyone is good enough with the commands.

In the Nmap output tab, the results are shown, where in the ports/hosts tab ports or the hosts are shown and in the topology tab, topology for the scanned result. Details of the hosts are shown in Host Details tab. In the left pane, we can scan or filter the hosts by clicking on the filter hosts button

We can scan by services by clicking on the services button in the left panel as shown in the above screen

Example:

We are going to scan a particular IP address; it is a sort of port scanning and wants also check if this host is up or down. The command for the above task is as under: nmap -T4 -A -v 10.99.12.213. The screen shot for the above command is as under:



Target: www.google.com

Profile: Intense scan

Command: nmap -T4 -A -v www.google.com

Figure:6.8.6

Where to Get More Information

Anyone interested for the further tasks and help regarding the Nmap, and then I have not even scratched the surface on this topic. However, I hope that this introduction will pique the curiosity of anyone who has either never heard of port scanning or have never used the technique. Use the following resources to learn more about NMAP and port scanning in general

Installation and configuration of snort network scanner:

For snort tutorial and help visit the following link:

http://www.snort.org/assets/151/Installing_Snort_2.8.6.1_on_Windows_7.pdf