**Experiment No.: Date:**

**Title:** To study Network Audit

**Program Statement:** To perform Network Audit using Namp and Zenmap

**Learning Objectives:** At the end of this experiment, students will be able to:

* Learn the basics of network audit
* Use different network auditing tools that are available in the Linux and Windows environments to obtain network auditing parameters

**Pre-requisite:** Basic networking models TCP/IP and OSI, Network

**Apparatus:** Workstations installed with

Ubuntu or Windows, Nmap latest version, Zenmap latest version

**Theory:-**

Network auditing works through a systematic process where a computer network is analyzed for:

* Security
* Implementation of control
* Availability
* Management
* Performance

The data is gathered, vulnerabilities and threats are identified, and a formal audit report is sent to network administrators.

It is generally done by an information system auditor, network analyst/auditor or any other individual with a network management and/or security background. It uses both manual and automated techniques to gather data and review network posture. It reviews:

* Each node of a network
* Network control and security processes
* Network monitoring processes
* Other data

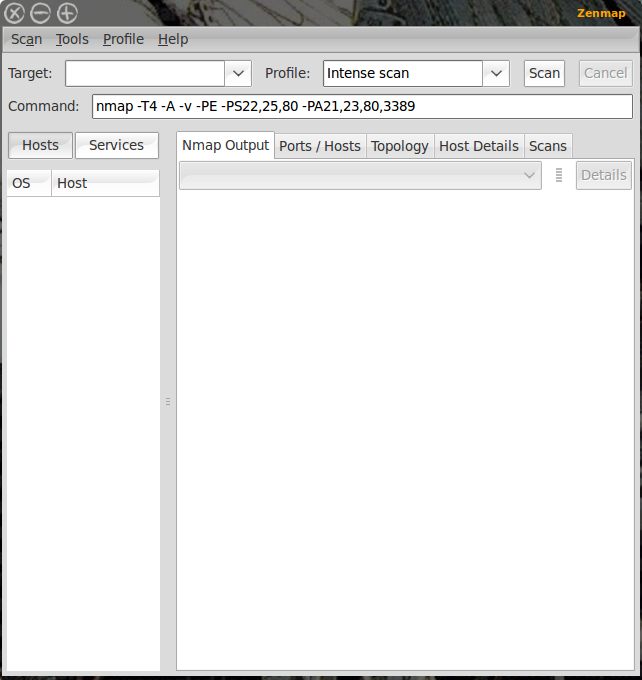
Although a network audit may focus more on network control and security, it also reviews processes and measures that ensure network availability, performance and quality of service.

Auditing a small network is not a difficult task for smaller network. But for large networks , a network administrator need to make use of one of the de facto standard open source network auditing tools – Zenmap which is the graphical front end for the very popular Nmap command line tool. It gives an interactive graphical map of any network. The purpose of Zenmap is not to replace Nmap, but to make Nmap more useful*.*

**Procedure:-**

1. **Installation:-** Nmap.Org is the official source for downloading Nmap source code and binaries for Nmap and Zenmap. Source code is distributed in bzip2 and gzip compressed tar files, and binaries are available for Linux (RPM format), Windows (NSIS executable installer) and Mac OS X (.dmg disk image). The Nmap executable Windows installer can handle WinPcap installation, registry performance tweaks, and decompressing the executables and data files into your preferred location. It also includes the Zenmap graphical frontend. Skip all the complexity of the Windows zip files with a self-installer:

Run latest release self-installer :nmap-7.01-setup.exe.

[](http://www.linux.com/images/stories/zenmap_main.png)

**Figure 1 :- GUI**

1. After opening the GUI Zenmap, network audit can be started. The first step is decide the network whose audit is to be done .Enter the IP address e.g192.168.33.110 of it in the Target section for scanning the network. If entire network is to be scanned then enter 192.168.33.\* in the Target section . Then select the profile as intense scan and click the scan button and the scan will begin. All discovered addresses will begin filling up the left plane and scan out will fill up the right plane. Let the scan complete before you click on different tabs in the right plane which are explained as below:-

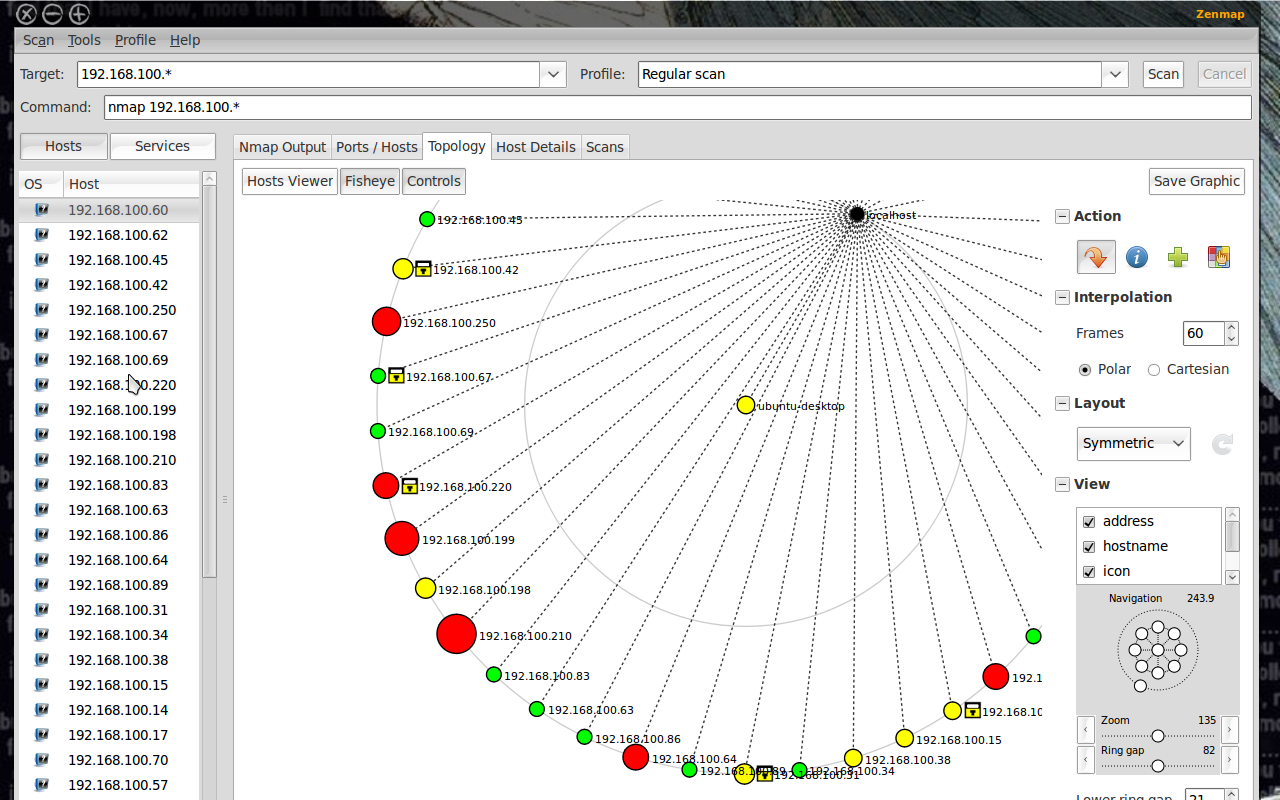
**Namp Output**:- This is the default tab and shows the output of the command

**Ports/Hosts:-** This tab shows what ports are open on what port

**Topology:**-This tab is very important for audit since this shows actual topology of your network. The layout of your network will displayed in the graphical form

**Host Details:-** This tab will give you specific information of a host which is selected from left plane where all of the IP addresses and host names are displayed

**Scans:-** This tab lists all of the scans which you have executed



**Figure 2 :- Topology**

1. **Topology:**- This is going to be one of the important tool in your audit. On clicking on this you can see a blob of red, green and yellow circles with their IP addresses. The ring gap can be enlarged by using zoom option from controls. You can add/remove various details by expanding the View section (click the ‘+’ sign next to view) and check the details (which are listed below)you want to see:-

Address, Hostname, Icon, Latency, Ring, Region, Slow In/Out

Size and colour of circles in the map also signifies number of open ports on that particular host.

Green circle:- < 3 open ports

Yellow Circle:- 3 to 6 open ports

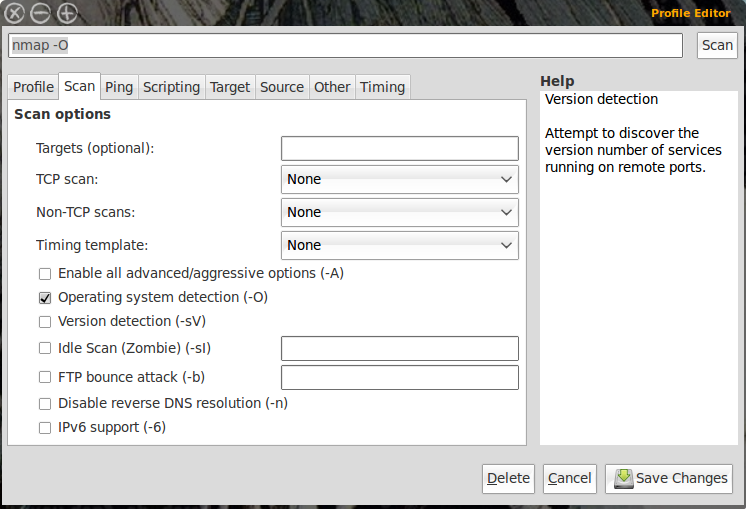
Red Circle:- > 6 open ports

Square without ‘T’ symbol:- For router / switch or wireless access point

Square with ‘T’ symbol:- A host with some ports filtered

This map is interactive; a host can be selected and can be made focal point of map.

1. **Scan Profile**:- As mentioned, you can use the default scanning profiles, or you can create your own. To do this click **Profile** and then select either New Profile or Command or Edit Current Profile. If you only want to make a minor change you can select a specific profile and then edit that profile. In my scan above I added Operating System information. To do that selects a scan profile and then click **Profile > Edit Current Profile**. In this new window click on the Scan tab and then check the OS option and then click Save Changes to finish up. If you make a change to a profile you will need to re-run the scan to get the desired results.



**Figure4:- Scan Profile**

**Conclusion:-**

Write conclusion with the help of following questions:-

1. Which network information do you get from Zenmap?
2. How does Nmap help network engineer /administrator?