**A). What is Nmap?**

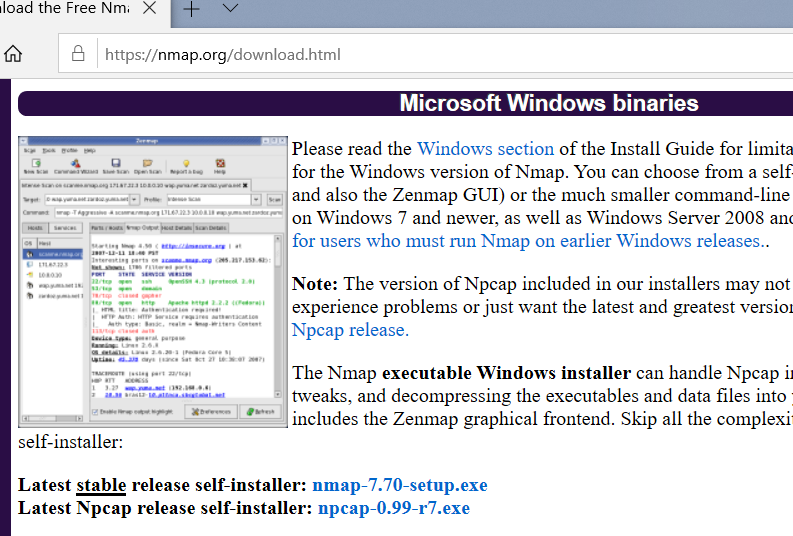
Nmap (Network Mapper) is a free and open source utility for network discovery and security auditing. It’s useful for tasks such as network inventory, managing service upgrade schedules, and monitoring host or service uptime. Nmap uses raw IP packets in novel ways to determine what hosts are available 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.

It was designed to rapidly scan large networks but works fine against single hosts. 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, redirection, and debugging tool (Ncat), a utility for comparing scan results (Ndiff), and a packet generation and response analysis tool (Nping).

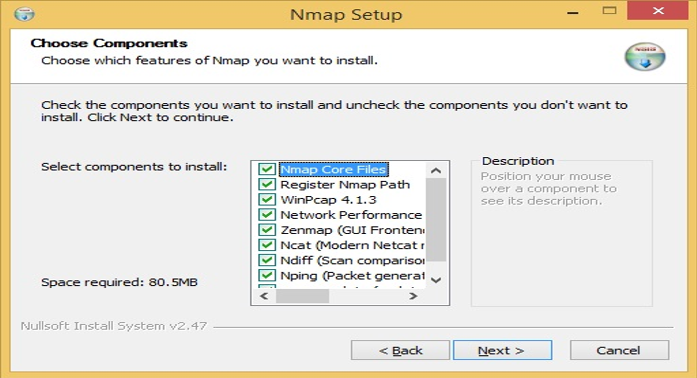
Nmap was named “Security Product of the Year” by Linux Journal, Info World, LinuxQuestions.Org, and Codetalker Digest. It was even featured in twelve movies, including The Matrix Reloaded, Die Hard 4, Girl With the Dragon Tattoo, and The Bourne Ultimatum.

Here are the steps to install NMAP on Windows:

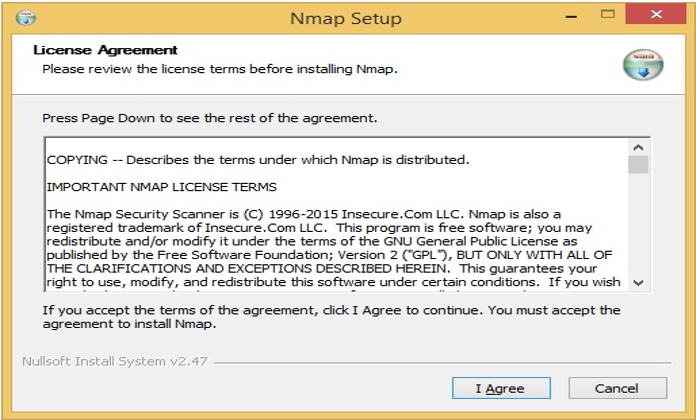
1. Browse to <https://nmap.org/download.html> and download the latest self-installer:



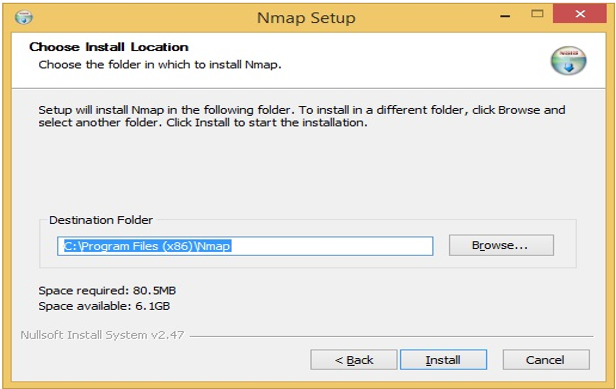
1. Choose the components to install. By default, the **Zenmap GUI** will be installed:



1. Run the downloaded **.exe** file. In the window that opens, accept the license terms:



1. Select the install location and click **Install**:



1. The installation should be completed in a couple of minutes.

**B). Study how to use the NMAP Security Scanner.**

Solution:

Following are some of the commands which are commonly used in NMAP:

* **Auth:** Use to test whether you can bypass authentication mechanism
* **Broadcast:** Use to find other hosts on the network and automatically add them to scanning que.
* **Brute:** Use for brute password guessing.
* **Discovery:** Use to discover more about the network.
* **Dos:** Use to test whether a target is vulnerable to DoS
* **Exploit:** Use to actively exploit a vulnerability
* **Fuzzer:** Use to test how server responds to unexpected or randomized fields in packets and determine other potential vulnerabilities
* **Intrusive:** Use to perform more intense scans that pose a much higher risk of being detected by admins.
* **Malware:** Use to test target for presence of malware
* **Safe:** Use to perform general network security scan that's less likely to alarm remote administrators
* **Vuln:** Use to find vulnerabilities on the target

**C) Study and implement the iptables:**

Solution:

### 1. View / List All iptables Rules

When you want to check what rules are in iptables, use –list option as shown below.

# iptables --list

### Example 1: Iptables list output showing no rules

# iptables --listChain INPUT (policy ACCEPT)target prot opt source destination Chain FORWARD (policy ACCEPT)target prot opt source destination Chain OUTPUT (policy ACCEPT)target prot opt source destination

The above output shows chain headers. As you see, there are no rules in it.

### Example 2: Iptables list output showing some rules

When there is a rule to disable ping reply, you have the iptables list output as like the following. You can see the rule in the OUTPUT chain.

# iptables --listChain INPUT (policy ACCEPT)target prot opt source destination Chain FORWARD (policy ACCEPT)target prot opt source destination Chain OUTPUT (policy ACCEPT)target prot opt source destinationDROP icmp -- anywhere anywhere icmp echo-request

### 2. Delete iptables Rules using flush option

When you want to delete all the rules, use the flush option as shown below.

# iptables --flush

After doing this, your iptables will become empty, and the “iptables –list” output will look like what is shown in the example 1.

You can also delete (flush) a particular iptable chain by giving the chain name as an argument as shown below.

# iptables --flush OUTPUT

**To implement the iptables (firewall) in Linux & Fedora is:**

# iptables –A INPUT –j DROP

It will implement the firewall and no ping request from the other PC's will come to your PC.

To see the detail list of iptables the command is:

# iptables –L

To delete or remove the iptables the command is

# iptables -F

To INSTALL NMAP in Fedora the command is:

# apt –get nmap –v