*DEPARTMENT OF INFORMATION TECHNOLOGY* Experiment No.2

|  |  |
| --- | --- |
| Semester | T.E. Semester VI – Information Technology |
| Subject | System and web security |
| Subject Professor In-charge | Prof. Chintan Shah. |
| Assisting Teachers | Prof. Mohit Gujar |
| Laboratory | L007 |

|  |  |  |
| --- | --- | --- |
| Student Name | Ashutosh Engavle | |
| Roll Number | 15101B0042 | |
| Grade and Subject Teacher’s Signature |  |  |

|  |  |  |
| --- | --- | --- |
| Experiment Number | 2 | |
| Experiment Title | NMAP Network Mapper Tool | |
| Resources / Apparatus Required | Hardware:  Monitor,Printer,Mouse | Software:  Windows |
| Objectives  (Skill Set / Knowledge Tested / Imparted) | NMAP Network Mapper Tool | |
| Theory of Operation | 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.  Nmap features include:   * Host discovery – Identifying hosts on a network. For example, listing the hosts that respond to TCP and/or ICMP requests or have a particular port open. * Port scanning – Enumerating the open ports on target hosts. * Version detection – Interrogating network services on remote devices to determine application name and version number. * OS detection – Determining the operating system and hardware characteristics of network devices. * Scriptable interaction with the target – using Nmap Scripting Engine (NSE) and Lua programming language. * Nmap can provide further information on targets, including reverse DNS names, device types, and MAC addresses.   Zenmap is the official graphical user interface (GUI) for the Nmap Security Scanner.  It is a multi-platform, free and open-source application designed to make Nmap easy for beginners to use while providing advanced features for experienced Nmap users.  Frequently used scans can be saved as profiles to make them easy to run repeatedly. A command creator allows interactive creation of Nmap command lines.  Scan results can be saved and viewed later. Saved scans can be compared with one another to see how they differ. The results of recent scans are stored in a searchable database. | |
| Code & Output: | #1: Scan a single host or an IP address (IPv4)    #2: Scan multiple IP address or subnet (IPv4)    #3: Read list of hosts/networks from a file (IPv4)  The -iL option allows you to read the list of target systems using a text file. This is useful to scan a large number of hosts/networks.    #4: Scan a network and find out which servers and devices are up and running:    #5: Fast scan    #6: Display the reason a port is in a particular state    #7: Only show open (or possibly open) ports    #8: Show host interfaces and routes  This is useful for debugging (ip command or route command or netstat command like output using nmap)    #9: Scan Specific Ports    #10: The fastest way to scan all devices/computers for open ports ever    Zenmap: | |
| Conclusion: | Thus we have studied NMAP Network Mapper Tool | |