TASK-1

Open port found:-

PORT	STATE	SERVICE	VERSION
135/tcp	open	msrpc	Microsoft Windows RPC
139/tcp	open	netbios-ssn	Microsoft Windows netbios-ssn
445/tcp	open	microsoft-ds?	
16992/tcp	open	http	Intel Small Business Technology Platform 11.8.97.4739

Potential security risk from open ports:-

Port 135/tcp – msrpc (Microsoft Windows RPC):- Attackers can gather detailed information about services, users, shares, and domain configuration. Vulnerable to known Windows RPC exploits like **MS03-026** (Blaster worm).

Port 139/tcp – netbios-ssn (NetBIOS Session Service):- Allows enumeration of **usernames**, **shared folders**, **OS version**, and **domain names** using tools. Susceptible to **NTLM relay**, **pass-the-hash**, and **SMB spoofing** attacks.

Port 445/tcp – microsoft-ds (SMB over TCP):- Vulnerable to **EternalBlue (MS17-010)** → Used in WannaCry ransomware. SMBv1 protocol is insecure and used in worm-based attacks
.
Port 16992/tcp – http (Intel Small Business Technology Platform):- Vulnerabilities in AMT could allow **unauthenticated remote access** to control or spy on the device. Runs **below OS level**, immune to OS firewalls and most antivirus. Can be used for **firmware-level backdoors**..

Starting Nmap 7.97 (https://nmap.org) at 2025-08-04 19:52 +0530 NSE: Loaded 158 scripts for scanning. NSE: Script Pre-scanning. Initiating NSE at 19:52 Completed NSE at 19:52, 0.00s elapsed Initiating NSE at 19:52 Completed NSE at 19:52, 0.00s elapsed Initiating NSE at 19:52 Completed NSE at 19:52, 0.00s elapsed Initiating Ping Scan at 19:53 Scanning 256 hosts [4 ports/host] Ping Scan Timing: About 29.35% done; ETC: 19:54 (0:01:15 remaining) Ping Scan Timing: About 57.96% done; ETC: 19:54 (0:00:44 remaining) Completed Ping Scan at 19:54, 105.44s elapsed (256 total hosts) Initiating Parallel DNS resolution of 256 hosts. at 19:54 Completed Parallel DNS resolution of 256 hosts. at 19:55, 43.93s elapsed Nmap scan report for 192.168.1.0 [host down] Nmap scan report for 192.168.1.1 [host down] Nmap scan report for 192.168.1.2 [host down] Nmap scan report for 192.168.1.3 [host down] Nmap scan report for 192.168.1.4 [host down] Nmap scan report for 192.168.1.5 [host down] Nmap scan report for 192.168.1.6 [host down] Nmap scan report for 192.168.1.7 [host down] Nmap scan report for 192.168.1.8 [host down] Nmap scan report for 192.168.1.9 [host down] Nmap scan report for 192.168.1.10 [host down] Nmap scan report for 192.168.1.11 [host down] Nmap scan report for 192.168.1.12 [host down] Nmap scan report for 192.168.1.13 [host down] Nmap scan report for 192.168.1.14 [host down] Nmap scan report for 192.168.1.15 [host down] Nmap scan report for 192.168.1.16 [host down] Nmap scan report for 192.168.1.17 [host down] Nmap scan report for 192.168.1.18 [host down] Nmap scan report for 192.168.1.19 [host down] Nmap scan report for 192.168.1.20 [host down] Nmap scan report for 192.168.1.21 [host down] Nmap scan report for 192.168.1.22 [host down] Nmap scan report for 192.168.1.23 [host down] Nmap scan report for 192.168.1.24 [host down] Nmap scan report for 192.168.1.25 [host down] Nmap scan report for 192.168.1.26 [host down] Nmap scan report for 192.168.1.27 [host down] Nmap scan report for 192.168.1.28 [host down] Nmap scan report for 192.168.1.29 [host down] Nmap scan report for 192.168.1.30 [host down] Nmap scan report for 192.168.1.31 [host down] Nmap scan report for 192.168.1.32 [host down] Nmap scan report for 192.168.1.33 [host down] Nmap scan report for 192.168.1.34 [host down] Nmap scan report for 192.168.1.35 [host down] Nmap scan report for 192.168.1.36 [host down] Nmap scan report for 192.168.1.37 [host down] Nmap scan report for 192.168.1.38 [host down] Nmap scan report for 192.168.1.39 [host down] Nmap scan report for 192.168.1.40 [host down] Nmap scan report for 192.168.1.41 [host down] Nmap scan report for 192.168.1.42 [host down] Nmap scan report for

192.168.1.43 [host down] Nmap scan report for 192.168.1.44 [host down] Nmap scan report for
192.168.1.45 [host down] Nmap scan report for 192.168.1.46 [host down] Nmap scan report for
192.168.1.47 [host down] Nmap scan report for 192.168.1.48 [host down] Nmap scan report for
192.168.1.49 [host down] Nmap scan report for 192.168.1.50 [host down] Nmap scan report for
192.168.1.51 [host down] Nmap scan report for 192.168.1.52 [host down] Nmap scan report for
192.168.1.53 [host down] Nmap scan report for 192.168.1.54 [host down] Nmap scan report for
192.168.1.55 [host down] Nmap scan report for 192.168.1.56 [host down] Nmap scan report for
192.168.1.57 [host down] Nmap scan report for 192.168.1.58 [host down] Nmap scan report for
192.168.1.59 [host down] Nmap scan report for 192.168.1.60 [host down] Nmap scan report for
192.168.1.61 [host down] Nmap scan report for 192.168.1.62 [host down] Nmap scan report for
192.168.1.63 [host down] Nmap scan report for 192.168.1.64 [host down] Nmap scan report for
192.168.1.65 [host down] Nmap scan report for 192.168.1.66 [host down] Nmap scan report for
192.168.1.67 [host down] Nmap scan report for 192.168.1.68 [host down] Nmap scan report for
192.168.1.69 [host down] Nmap scan report for 192.168.1.70 [host down] Nmap scan report for
192.168.1.71 [host down] Nmap scan report for 192.168.1.72 [host down] Nmap scan report for
192.168.1.73 [host down] Nmap scan report for 192.168.1.74 [host down] Nmap scan report for
192.168.1.75 [host down] Nmap scan report for 192.168.1.76 [host down] Nmap scan report for
192.168.1.77 [host down] Nmap scan report for 192.168.1.78 [host down] Nmap scan report for
192.168.1.79 [host down] Nmap scan report for 192.168.1.80 [host down] Nmap scan report for
192.168.1.81 [host down] Nmap scan report for 192.168.1.82 [host down] Nmap scan report for
192.168.1.83 [host down] Nmap scan report for 192.168.1.84 [host down] Nmap scan report for
192.168.1.85 [host down] Nmap scan report for 192.168.1.86 [host down] Nmap scan report for
192.168.1.87 [host down] Nmap scan report for 192.168.1.88 [host down] Nmap scan report for
192.168.1.89 [host down] Nmap scan report for 192.168.1.90 [host down] Nmap scan report for
192.168.1.91 [host down] Nmap scan report for 192.168.1.92 [host down] Nmap scan report for
192.168.1.93 [host down] Nmap scan report for 192.168.1.94 [host down] Nmap scan report for
192.168.1.95 [host down] Nmap scan report for 192.168.1.96 [host down] Nmap scan report for
192.168.1.97 [host down] Nmap scan report for 192.168.1.98 [host down] Nmap scan report for
192.168.1.99 [host down] Nmap scan report for 192.168.1.100 [host down] Nmap scan report for
192.168.1.101 [host down] Nmap scan report for 192.168.1.102 [host down] Nmap scan report for
192.168.1.103 [host down] Nmap scan report for 192.168.1.104 [host down] Nmap scan report for
192.168.1.105 [host down] Nmap scan report for 192.168.1.106 [host down] Nmap scan report for
192.168.1.107 [host down] Nmap scan report for 192.168.1.108 [host down] Nmap scan report for
192.168.1.109 [host down] Nmap scan report for 192.168.1.110 [host down] Nmap scan report for
192.168.1.111 [host down] Nmap scan report for 192.168.1.112 [host down] Nmap scan report for
192.168.1.113 [host down] Nmap scan report for 192.168.1.114 [host down] Nmap scan report for
192.168.1.115 [host down] Nmap scan report for 192.168.1.116 [host down] Nmap scan report for
192.168.1.117 [host down] Nmap scan report for 192.168.1.118 [host down] Nmap scan report for
192.168.1.119 [host down] Nmap scan report for 192.168.1.120 [host down] Nmap scan report for
192.168.1.121 [host down] Nmap scan report for 192.168.1.122 [host down] Nmap scan report for
192.168.1.123 [host down] Nmap scan report for 192.168.1.124 [host down] Nmap scan report for
192.168.1.125 [host down] Nmap scan report for 192.168.1.126 [host down] Nmap scan report for
192.168.1.127 [host down] Nmap scan report for 192.168.1.128 [host down] Nmap scan report for
192.168.1.129 [host down] Nmap scan report for 192.168.1.130 [host down] Nmap scan report for
192.168.1.131 [host down] Nmap scan report for 192.168.1.132 [host down] Nmap scan report for
192.168.1.133 [host down] Nmap scan report for 192.168.1.134 [host down] Nmap scan report for
192.168.1.135 [host down] Nmap scan report for 192.168.1.136 [host down] Nmap scan report for
192.168.1.137 [host down] Nmap scan report for 192.168.1.138 [host down] Nmap scan report for
192.168.1.139 [host down] Nmap scan report for 192.168.1.140 [host down] Nmap scan report for
192.168.1.141 [host down] Nmap scan report for 192.168.1.142 [host down] Nmap scan report for
192.168.1.143 [host down] Nmap scan report for 192.168.1.144 [host down] Nmap scan report for
192.168.1.145 [host down] Nmap scan report for 192.168.1.146 [host down] Nmap scan report for
192.168.1.147 [host down] Nmap scan report for 192.168.1.148 [host down] Nmap scan report for
192.168.1.149 [host down] Nmap scan report for 192.168.1.150 [host down] Nmap scan report for
192.168.1.151 [host down] Nmap scan report for 192.168.1.152 [host down] Nmap scan report for
192.168.1.153 [host down] Nmap scan report for 192.168.1.154 [host down] Nmap scan report for
192.168.1.155 [host down] Nmap scan report for 192.168.1.156 [host down] Nmap scan report for
192.168.1.157 [host down] Nmap scan report for 192.168.1.158 [host down] Nmap scan report for
192.168.1.159 [host down] Nmap scan report for 192.168.1.160 [host down] Nmap scan report for
192.168.1.161 [host down] Nmap scan report for 192.168.1.162 [host down] Nmap scan report for

192.168.1.163 [host down] Nmap scan report for 192.168.1.164 [host down] Nmap scan report for 192.168.1.165 [host down] Nmap scan report for 192.168.1.166 [host down] Nmap scan report for 192.168.1.167 [host down] Nmap scan report for 192.168.1.168 [host down] Nmap scan report for 192.168.1.169 [host down] Nmap scan report for 192.168.1.170 [host down] Nmap scan report for 192.168.1.171 [host down] Nmap scan report for 192.168.1.172 [host down] Nmap scan report for 192.168.1.173 [host down] Nmap scan report for 192.168.1.174 [host down] Nmap scan report for 192.168.1.175 [host down] Nmap scan report for 192.168.1.176 [host down] Nmap scan report for 192.168.1.177 [host down] Nmap scan report for 192.168.1.178 [host down] Nmap scan report for 192.168.1.179 [host down] Nmap scan report for 192.168.1.180 [host down] Nmap scan report for 192.168.1.181 [host down] Nmap scan report for 192.168.1.182 [host down] Nmap scan report for 192.168.1.183 [host down] Nmap scan report for 192.168.1.184 [host down] Nmap scan report for 192.168.1.185 [host down] Nmap scan report for 192.168.1.186 [host down] Nmap scan report for 192.168.1.187 [host down] Nmap scan report for 192.168.1.188 [host down] Nmap scan report for 192.168.1.189 [host down] Nmap scan report for 192.168.1.190 [host down] Nmap scan report for 192.168.1.191 [host down] Nmap scan report for 192.168.1.192 [host down] Nmap scan report for 192.168.1.193 [host down] Nmap scan report for 192.168.1.194 [host down] Nmap scan report for 192.168.1.195 [host down] Nmap scan report for 192.168.1.196 [host down] Nmap scan report for 192.168.1.197 [host down] Nmap scan report for 192.168.1.198 [host down] Nmap scan report for 192.168.1.199 [host down] Nmap scan report for 192.168.1.200 [host down] Nmap scan report for 192.168.1.201 [host down] Nmap scan report for 192.168.1.202 [host down] Nmap scan report for 192.168.1.203 [host down] Nmap scan report for 192.168.1.204 [host down] Nmap scan report for 192.168.1.205 [host down] Nmap scan report for 192.168.1.206 [host down] Nmap scan report for 192.168.1.207 [host down] Nmap scan report for 192.168.1.208 [host down] Nmap scan report for 192.168.1.209 [host down] Nmap scan report for 192.168.1.210 [host down] Nmap scan report for 192.168.1.211 [host down] Nmap scan report for 192.168.1.212 [host down] Nmap scan report for 192.168.1.213 [host down] Nmap scan report for 192.168.1.214 [host down] Nmap scan report for 192.168.1.215 [host down] Nmap scan report for 192.168.1.216 [host down] Nmap scan report for 192.168.1.217 [host down] Nmap scan report for 192.168.1.218 [host down] Nmap scan report for 192.168.1.219 [host down] Nmap scan report for 192.168.1.220 [host down] Nmap scan report for 192.168.1.221 [host down] Nmap scan report for 192.168.1.222 [host down] Nmap scan report for 192.168.1.223 [host down] Nmap scan report for 192.168.1.224 [host down] Nmap scan report for 192.168.1.225 [host down] Nmap scan report for 192.168.1.226 [host down] Nmap scan report for 192.168.1.227 [host down] Nmap scan report for 192.168.1.228 [host down] Nmap scan report for 192.168.1.229 [host down] Nmap scan report for 192.168.1.230 [host down] Nmap scan report for 192.168.1.231 [host down] Nmap scan report for 192.168.1.232 [host down] Nmap scan report for 192.168.1.233 [host down] Nmap scan report for 192.168.1.234 [host down] Nmap scan report for 192.168.1.235 [host down] Nmap scan report for 192.168.1.236 [host down] Nmap scan report for 192.168.1.237 [host down] Nmap scan report for 192.168.1.238 [host down] Nmap scan report for 192.168.1.239 [host down] Nmap scan report for 192.168.1.240 [host down] Nmap scan report for 192.168.1.241 [host down] Nmap scan report for 192.168.1.242 [host down] Nmap scan report for 192.168.1.243 [host down] Nmap scan report for 192.168.1.244 [host down] Nmap scan report for 192.168.1.245 [host down] Nmap scan report for 192.168.1.246 [host down] Nmap scan report for 192.168.1.247 [host down] Nmap scan report for 192.168.1.248 [host down] Nmap scan report for 192.168.1.249 [host down] Nmap scan report for 192.168.1.250 [host down] Nmap scan report for 192.168.1.251 [host down] Nmap scan report for 192.168.1.252 [host down] Nmap scan report for 192.168.1.253 [host down] Nmap scan report for 192.168.1.254 [host down] Nmap scan report for 192.168.1.255 [host down] NSE: Script Post-scanning. Initiating NSE at 19:55 Completed NSE at 19:55, 0.00s elapsed Initiating NSE at 19:55 Completed NSE at 19:55, 0.00s elapsed Initiating NSE at 19:55 Completed NSE at 19:55, 0.00s elapsed Read data files from: C:\Program Files (x86)\Nmap Nmap done: 256 IP addresses (0 hosts up) scanned in 160.25 seconds Raw packets sent: 2049 (77.852KB) | Rcvd: 8 (502B)