Nmap :

**Aggressive Scan**

1. nmap -A -T4 -p- --script=auth,broadcast,brute,default,discovery,dos,exploit,external,fuzzer,intrusive,malware,safe,version,vuln target.com

**Script Scan**

|  |  |  |
| --- | --- | --- |
| **Category** | **Parameter to Use** | **Description** |
| auth | --script=auth | Handles authentication protocols (SSH, HTTP, etc.) |
| broadcast | --script=broadcast | Uses broadcast/multicast to discover LAN devices |
| brute | --script=brute | Performs brute-force login attempts |
| default | --script=default | Default scripts run with -sC or -A |
| discovery | --script=discovery | Helps uncover hosts and services |
| dos | --script=dos | Checks for denial-of-service vulnerabilities |
| exploit | --script=exploit | Exploits specific vulnerabilities (⚠️ use with care) |
| external | --script=external | Queries external resources (WHOIS, GeoIP, etc.) |
| fuzzer | --script=fuzzer | Sends unusual inputs to test system behavior |
| intrusive | --script=intrusive | May trigger detection or instability (⚠️ aggressive) |
| malware | --script=malware | Detects malware infections and indicators |
| safe | --script=safe | Gentle scripts, won't disrupt targets |
| version | --script=version | Enhances service/version detection |
| vuln | --script=vuln | Tests for known CVEs and security flaws |

**Nmap Scan result**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Test Category** | **Script / Technique** | **Target Port / Service** | **Result / Finding** | **Severity / Risk** |
| OS Detection | -O (OS fingerprinting) | N/A | OS Detected: Linux 4.X (90% confidence) | Low |
| Version Detection | -sV | 22 (SSH) | OpenSSH 7.6 detected | Informational |
| Script Scan | --script=default | 80 (HTTP) | HTTP Server header: Apache 2.4.29 | Informational |
| Vulnerability Detection | --script=vuln | 445 (SMB) | **CVE-2017-0144 (EternalBlue)** vulnerable | High |
| Auth Methods Enumeration | --script=auth | 22 (SSH) | Password auth enabled | Medium |
| Brute-force Check | --script=ftp-brute | 21 (FTP) | No valid credentials found | Low |
| Malware Check | --script=http-malware-host | 80 (HTTP) | No signs of malware detected | Informational |
| Broadcast Discovery | --script=broadcast-dhcp-discover | N/A | DHCP server found: 192.168.1.1 | Low |
| Traceroute | --traceroute | N/A | 8 hops to target, no anomalies | Informational |
| DNS Resolution | Reverse Lookup | Target IP | Resolved to example.com | Low |

**Nmap Scan Type**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Scan Type** | **Nmap Flag** | **Purpose** | **Result / Outcome** | **Notes** |
| **TCP Connect Scan** | -sT | Full TCP handshake scan to detect open ports | Open ports found: 22, 80, 443 | No root privileges required |
| **SYN (Stealth) Scan** | -sS | Half-open TCP scan to avoid detection | Same open ports detected | More stealthy, requires root |
| **UDP Scan** | -sU | Scans UDP ports | Port 161 open (SNMP), others filtered | May be slow due to no responses |
| **Version Detection** | -sV | Identifies service versions | Apache 2.4.29, OpenSSH 7.9, vsftpd 3.0.3 | Useful for vuln matching |
| **OS Detection** | -O | Attempts to determine operating system | Linux 4.X (89% accuracy) | Depends on open/filtered ports |
| **Aggressive Scan** | -A | Combines OS, version, script, and traceroute | Deep fingerprinting and vulns found | Noisy and high-impact |
| **All Ports Scan** | -p- | Scans all 65,535 TCP ports | Additional services found on 8080, 8443 | Longer scan time |
| **Default Script Scan** | -sC | Runs default NSE scripts | Output includes SSL certs, HTTP headers, etc. | Equivalent to --script=default |
| **Traceroute** | --traceroute | Maps path packets take to host | 12 hops, latency peaked at 142ms | Helps with network mapping |