NMAP NSE SCRIPTS BY CATEGORIES:

- **AUTH** – AUTHENTICATION BYPASS & CREDENTIAL BRUTE FORCE.
- **BROADCAST** – DISCOVER HOSTS BY BROADCASTING.
- **BRUTE** – BRUTE-FORCE PASSWORDS FOR SERVICES.
- **DEFAULT** – RUN WHEN -SC IS USED (SAFE, GENERAL INFO).
- **DISCOVERY** – HOST/SERVICE DISCOVERY.
- **DOS** – DENIAL OF SERVICE CHECKS.
- **EXPLOIT** – KNOWN VULNERABILITIES EXPLOITATION.
- **EXTERNAL** – QUERY EXTERNAL SERVICES/APIS.
- **FUZZER** – SEND UNEXPECTED INPUT TO DETECT BUGS.
- **INTRUSIVE** – MIGHT CRASH OR SLOW SERVICES.
- **MALWARE** – CHECK FOR INFECTIONS/BACKDOORS.
- **SAFE** – SCRIPTS THAT WON'T HARM TARGET.
- **VERSION** – IMPROVE VERSION DETECTION.
- **VULN** – CHECK FOR VULNERABILITIES.

1.) AUTHENTICATION/BRUTEFORCE CATEGORY

These scripts are used for authentication bypass testing, credential brute-forcing, and login enumeration on various services.

SCRIPTS	DESCRIPTION
ftp-brute	Performs brute-force password guessing against FTP servers. **Example**: nmap –script ftp-brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt,ftp-brute.timeout=10 <target> -p 21
http-auth	Tests HTTP server authentication methods. **Example**: nmap --script http-auth <target> -p 80,443
http-brute	Brute-forces HTTP authentication credentials. **Example**: nmap --script http-brute --script-args http-brute.path=/protected, userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt,http-brute.hostname=<target> -p 80,443
imap-brute	Brute-forces credentials on IMAP servers. Example: nmap --script imap-brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt <target> -p 143,993
ssh-brute	Brute-forces credentials on SSH servers. **Example**: nmap --script ssh-brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt,ssh-brute.timeout=10 <target> -p 22
mysql-brute	Performs brute-force password guessing on MySQL servers. **Example:** nmap --script mysql-brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt,mysql-brute.timeout=8 <target> -p 3306
mssql-brute	Performs brute-force password guessing on MS-SQL servers. **Example:** nmap --script ms-ssql --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt,ms-sql-brute.timeout=8 <target> -p 1443
pgsql-brute	Performs brute-force password guessing on PostGreSQL servers. **Example:** nmap --script mysql-brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt <target> -p 5432
pop3-brute	Brute-forces credentials on POP3 servers.

	Example: nmap --script pop3-brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt <target> -p 110,995
rdp-brute	Brute-forces credentials on Remote Desktop Protocol (RDP) services. **Example:** nmap --script rdp-brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt,rdp-brute.timeout=8 <target> -p 3389
smb-brute	Brute-forces credentials on SMB services. **Example:** nmap --script smb-brute brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt,smb-brute.timeout=10 <target> -p 445
telnet-brute	Brute-forces credentials on Telnet servers. **Example:** nmap --script telnet-brute --script-args userdb=/path/to/userlist.txt,passdb=/path/to/passlist.txt,telnet-brute.timeout=10 <target> -p 23
vnc-brute	Brute-forces VNC authentication. **Example:** nmap --script vnc-brute --script-args --script-args passdb=/path/to/passlist.txt <target> -p 5900

2.) BROADCAST CATEGORY

These scripts are used for **host discovery** by sending broadcast queries on a network. Useful for finding devices without scanning each IP individually.

SCRIPTS	DESCRIPTION
broadcast-dhcp-discover	Sends a DHCP request to discover DHCP servers. Great for finding rogue/hidden DHCP servers (no target needed) **Example:** nmap --script broadcast-dhcp-discover
broadcast-dns-service-discovery	It queries multicast DNS, Useful in networks with Apple devices, IoT, printers, etc. **Example:** nmap --script broadcast-dns-service-discovery <IP/subnet>
broadcast-netbios-master-browser	Lists Windows domains and workgroups, helps map SMB shares. **Example:** nmap --script broadcast-netbios-master-browser <IP/subnet>
broadcast-ping	Pings hosts in the local network using broadcast ICMP. **Example:** nmap --script broadcast-ping <IP/subnet>
broadcast-pppoe-discover	Finds PPPoE servers (mostly in ISP or DSL environments) **Example:** nmap --script broadcast-pppoe-discover <IP/subnet>
broadcast-rip-discover	Queries the Routing Information Protocol. Rare, but can reveal routers sharing routes over LAN. **Example:** nmap --script broadcast-rip-discover <IP/subnet>
broadcast-upnp-info	Finds smart TVs, cameras, IoT gadgets, routers. Dumps device type, firmware, and services. **Example:** nmap --script broadcast-upnp-info <IP/subnet>
broadcast-wsdd-discover	Discovers devices using Web Services Dynamic Discovery (WSDD). **Example:** nmap --script broadcast-wsdd-discover
Run All broadcast Scripts	nmap --script broadcast

Note: Broadcast scripts only work within the local subnet and do not cross routers.

3.) DEFAULT CATEGORY

These scripts run when you use -sC or --script=default in Nmap. They are safe, non-intrusive, and gather general information about the target.

SCRIPTS	DESCRIPTION
banner	Retrieves and displays service banners. **Example:** nmap -p 80,443 --script banner <target>
default (meta-script)	Runs a set of common and safe scripts to collect information. **Example:** nmap -sC <target>
http-title	Retrieves the title of the target web page. **Example** nmap -p 80,443 --script http-title <target>
http-server-header	Displays the server header from HTTP responses. **Example** nmap -p 80,443 --script http-server-header <target>
ssh-hostkey	Retrieves and displays the SSH host key. **Example:** nmap -p 22 --script ssh-hostkey <target>
ssl-cert	Retrieves and displays an SSL certificate. **Example:** nmap -p 443 --script ssl-cert <target>
ssl-enum-ciphers	Lists supported SSL/TLS ciphers. **Example:** nmap -p 443 --script ssl-enum-ciphers <target>
whois-domain	Performs a WHOIS lookup for the target domain. **Example** nmap --script whois-domain <target>
address-info	Displays detailed information about the target's IP address. **Example:** nmap --script address-info <target>
service-info	Displays detailed information about the detected service. **Example:** nmap -p <port> --script service-info <target>
Run All Default Scripts	nmap -sC <target> OR nmap --script=default <target>

4.) DOS CATEGORY

These scripts are used to test for Denial of Service vulnerabilities. **Use with caution** as they can disrupt target systems.

SCRIPTS	DESCRIPTION
dos-dnsmasq	Tests for DNSmasq DNS server DoS vulnerability (CVE-2017-14491). **Example:** nmap --script dos-dnsmasq -p 53 <target>
http-slowloris	Performs a Slowloris DoS attack against an HTTP server. **Example:** nmap --script http-slowloris -p 80 <target>
http-slowloris-check	Checks if a target is vulnerable to Slowloris without fully exploiting it. **Example:** nmap --script http-slowloris-check -p 80,443 <target>
http-slowpost	Sends HTTP POST requests very slowly to keep connections open. **Example:** nmap --script http-slowpost -p 80 <target>
ssl-dos	Tests SSL/TLS services for DoS vulnerabilities by initiating multiple handshakes. **Example:** nmap --script ssl-dos -p 443 <target>
Run All DoS Scripts	nmap --script dos <target>

5.) EXPLOIT CATEGORY

These scripts attempt to **actively exploit** known vulnerabilities (usually for verification or proof-of-concept). **Use only with explicit permission.**

SCRIPTS	DESCRIPTION
ftp-proftpd-backdoor	Exploits the ProFTPD 1.3.3c backdoor to execute commands. **Example** nmap -p 21 --script ftp-proftpd-backdoor <target>
irc-unrealircd-backdoor	Detects and can trigger the UnrealIRCd "AB" backdoor (trojaned source release). **Example:** nmap -p 6667 --script irc-unrealircd-backdoor <target>
http-shellshock	Tests and can exploit Shellshock (CVE-2014-6271) in CGI-enabled web servers. **Example:** nmap -p 80,443 --script http-shellshock --script-args uri=/cgi-bin/status,cmd='id' <target>
http-phpself-xss	Attempts to exploit reflected XSS via PHP_SELF in misconfigured apps. **Example:** nmap -p 80 --script http-phpself-xss <target>
http-stored-xss	Probes for and may attempt to demonstrate stored XSS conditions. **Example:** nmap -p 80 --script http-stored-xss <target>
http-cross-domain-policy	Reports/exposes overly-permissive Flash crossdomain.xml (can be abused by attackers). **Example:** nmap -p 80 --script http-cross-domain-policy <target>
http-unsafe-output-escaping	Detects pages that dangerously reflect unescaped user input (XSS risk) and may demonstrate payloads. **Example:** nmap -p 80 --script http-unsafe-output-escaping <target>
http-dombased-xss	Checks for DOM-based XSS patterns and may attempt proof-of-concept payload reflection. **Example:** nmap -p 80 --script http-dombased-xss <target>
http-passwd	Attempts to retrieve /etc/passwd via common web misconfigurations (e.g., old aliasing or path traversal). **Example:** nmap -p 80 --script http-passwd <target>
http-litespeed-sourcecode-download	Attempts to download source code from vulnerable LiteSpeed setups. nmap -p 80 --script http-litespeed-sourcecode-download <target>
Run All exploit Scripts	nmap --script exploit <target>

6.) EXTERNAL CATEGORY

Scripts in this category **query third-party/online services or APIs**. Running them may disclose your target IP/domain to those services. Use with permission.

SCRIPTS	DESCRIPTION
asn-query	Maps an IP to its Autonomous System (AS) number. **Example"** nmap --script asn-query <target>
dns-blacklist	Checks IPs against anti-spam/open-proxy DNSBLs. You can limit by service/category. **Example** nmap --script dns-blacklist <target> # Limit to proxy lists nmap --script dns-blacklist --script-args dns-blacklist.categories=PROXY <target> # Check a specific list nmap --script dns-blacklist --script-args dns-blacklist.services=zen.spamhaus.org <target>
dns-check-zone	Audits a zone for RFC1912/best-practice issues. **Example:** nmap --script dns-check-zone --script-args dns-check-zone.domain=example.com <dns-server>
dns-random-srcport / dns-random-txid	Tests DNS recursion randomness (source port / TXID) for cache-poisoning risk. **Example:** nmap -p53 --script dns-random-srcport,dns-random-txid <dns-server>
dns-zeustracker	Checks whether targets are listed in the (legacy) abuse.ch Zeus tracker. **Example** nmap --script dns-zeustracker <target>
hostmap-bfk	Finds hostnames pointing to the target IP via BFK DNS logger. **Example:** nmap --script hostmap-bfk <target>
hostmap-crtsh	Finds subdomains via Certificate Transparency logs (crt.sh). **Example:** nmap --script hostmap-crtsh --script-args hostmap-crtsh.domain=example.com <target>
hostmap-robtex	Discovers hostnames for an IP via Robtex. **Example:** nmap --script hostmap-robtex <target>
http-cross-domain-policy	Fetches /crossdomain.xml and /clientaccesspolicy.xml to spot overly-permissive trust. **Example:** nmap -p80,443 --script http-cross-domain-policy <target>
http-google-malware	Checks Google Safe Browsing for malware/phishing listings.

	Example: nmap -p80,443 --script http-google-malware <target>
http-icloud-findmyiphone / http-icloud-sendmsg	Queries Apple MobileMe/iCloud endpoints (requires valid Apple ID creds). **Example:** nmap --script http-icloud-findmyiphone --script-args appleid=user@apple.com,password=...' <target> nmap --script http-icloud-sendmsg --script-args appleid=user@apple.com,password=...,message='Hello' <target>
http-open-proxy	Detects open HTTP proxies. **Example:** nmap -p8080,3128,8000,80 --script http-open-proxy <target>
http-proxy-brute	Brute-forces proxy auth (still "external" because many checks hit public sites). **Example:** nmap -p3128,8080 --script http-proxy-brute <target>
http-robtex-reverse-ip / http-robtex-shared-ns	Reverse-IP & shared-NS lookups via Robtex. **Example:** nmap --script http-robtex-reverse-ip,http-robtex-shared-ns <target>
http-virustotal	Checks a file or hash against VirusTotal (API key required; rate-limited). **Example:** # Hash lookup nmap --script http-virustotal --script-args 'apikey=<VT_KEY>,resource=<md5_or_sha1_or_sha256>' <target> # File upload (where supported by script version) nmap --script http-virustotal --script-args 'apikey=<VT_KEY>,file=</path/to/file>' <target>
http-xssed	Searches the xssed.com database for stored XSS records. **Example:** nmap --script http-xssed --script-args http-xssed.search=example.com <target>
ip-geolocation-geoplugin / ip-geolocation-ipinfodb / ip-geolocation-maxmind	IP geolocation via GeoPlugin, IPInfoDB, or a local MaxMind DB; companion map renderers below. **Example:** nmap --script ip-geolocation-geoplugin <target> nmap --script ip-geolocation-ipinfodb --script-args ipinfodb.apikey=<KEY> <target> nmap --script ip-geolocation-maxmind --script-args maxminddb=/path/to/GeoLite2-City.mmdb <target>

ip-geolocation-map-bing / ip-geolocation-map-google	Renders a Bing/Google map from geolocation results stored in Nmap's registry. **Example:** nmap --script ip-geolocation-geoplugin,ip-geolocation-map-google <target>
shodan-api	Queries Shodan for target data (API key required). **Example:** nmap --script shodan-api --script-args shodan-api.apikey=<KEY> <target>
smtp-enum-users	Enumerates SMTP users via VRFY/EXPN/RCPT TO. **Example** nmap -p25,465,587 --script smtp-enum-users <target>
smtp-open-relay	Tests whether the SMTP server will relay mail. **Example:** nmap -p25,465,587 --script smtp-open-relay <target>
socks-open-proxy	Detects open SOCKS proxies. **Example:** nmap -p1080 --script socks-open-proxy <target>
targets-asn	Generates IP prefixes for a given ASN (feeds other scans). **Example** nmap --script targets-asn --script-args targets-asn.asn=AS15169
tor-consensus-checker	Checks whether a target is a known Tor node. **Example:** nmap --script tor-consensus-checker <target>
traceroute-geolocation	Runs traceroute and annotates hops with geolocation; can export KML. **Example:** nmap --traceroute --script traceroute-geolocation --script-args 'traceroute-geolocation.kml=out.kml' <target>
vulners	Uses the Vulners.com API to map discovered CPEs to CVEs & CVSS. **Example:** # Best with service/version detection to populate CPEs nmap -sV --script vulners <target>
whois-domain / whois-ip	WHOIS lookups for domains or IP allocations (RIRs). **Example:** nmap --script whois-domain --script-args whois-domain.target=example.com <target> nmap --script whois-ip <target>
Run all external scripts:	nmap --script external <target>

7.) FUZZER CATEGORY

The **Fuzzer** scripts are used for sending unexpected, random, or malformed inputs to services to test for vulnerabilities, crashes, or unexpected behaviors.

SCRIPTS	DESCRIPTION
dns-fuzz	Performs a brute force of hostnames using a fuzzing approach to discover DNS subdomains. **Example:** nmap --script dns-fuzz --script-args timelimit=30s <target>
ftp-fuzz	Sends random or malformed commands to an FTP server to test for crashes or unexpected behavior. **Example:** nmap -p 21 --script ftp-fuzz <target>
http-form-fuzzer	Sends fuzzed input to HTML forms to test for vulnerabilities like buffer overflows or improper handling. **Example:** nmap -p 80 --script http-form-fuzzer --script-args 'http-form-fuzzer.url=/login' <target>
rdp-fuzz	Fuzzes the RDP protocol to test for weaknesses or crash vulnerabilities. **Example:** nmap -p 3389 --script rdp-fuzz <target>
smtp-fuzz	Sends malformed or unexpected SMTP commands to test the mail server's handling. **Example:** nmap -p 25 --script smtp-fuzz <target>
snmp-fuzz	Sends fuzzed SNMP queries to test for vulnerabilities in SNMP services. **Example:** nmap -p 161 --script snmp-fuzz <target>
ssh2-enum-algos-fuzz	Fuzzes SSH encryption and authentication algorithm negotiation to find unsupported or buggy handling. **Example:** nmap -p 22 --script ssh2-enum-algos-fuzz <target>

8.) INTRUSIVE CATEGORY

These scripts may send unusual traffic, exploit vulnerabilities, or cause potential disruption. Use with permission.

SCRIPTS	DESCRIPTION
http-shellshock	Tests for Shellshock vulnerability on web servers using CGI. **Example:** nmap -p80,443 --script http-shellshock <target>
http-slowloris	Performs a Slowloris DoS attack to test server's resilience. **Example:** nmap -p80 --script http-slowloris <target>
http-sql-injection	Tests HTTP parameters for SQL injection vulnerabilities. **Example:** nmap -p80 --script http-sql-injection <target>
rdp-vuln-ms12-020	Checks for MS12-020 RDP vulnerability. **Example:** nmap -p3389 --script rdp-vuln-ms12-020 <target>
smb-double-pulsar-backdoor	Detects the DoublePulsar SMB backdoor. **Example:** nmap -p445 --script smb-double-pulsar-backdoor <target>
smtp-vuln-cve2010-4344	Tests Exim for CVE-2010-4344 heap overflow vulnerability. **Example:** nmap -p25 --script smtp-vuln-cve2010-4344 <target>

9.) MALWARE CATEGORY

Scripts in this category help detect possible malware infections or related indicators. These scripts can be intrusive and should be run with caution.

SCRIPTS	DESCRIPTION
malware-host	Checks a host against known malware-infected host databases. **Example**: nmap --script malware-host <target>
malware-check	Performs checks for signs of known malware infections on a system or network service. **Example**: nmap --script malware-check <target>
malware-http	Identifies web-based malware infections, suspicious patterns, or known malicious files served over HTTP. **Example**: nmap -p 80,443 --script malware-http <target
malware-botnet	Detects signs that a host is part of a botnet, using known C2 server indicators. **Example**: nmap --script malware-botnet <target>

Tip: When scanning for malware, run with higher verbosity (-v) and consider using --script-args if a script allows customization (e.g., specifying malware database paths).

10.) **SAFE CATEGORY**

Scripts in the **safe** category are considered non-intrusive and won't harm the target system. They usually gather general information or perform harmless checks.

SCRIPTS	DESCRIPTION
afp-ls	Lists files and directories on AFP (Apple Filing Protocol) shares. **Example**: nmap --script=safe,afp-ls -p 548 <target>
dns-brute	Performs DNS subdomain brute force in a safe manner. **Example**: nmap --script=safe,dns-brute <target>
ftp-anon	Checks if anonymous FTP login is allowed. **Example**: nmap --script=safe,ftp-anon -p 21 <target>
http-title	Retrieves the title of a web page. **Example**: nmap --script=safe,http-title -p 80,443 <target>
smb-os-discovery	Retrieves OS information from SMB services. **Example**: nmap --script=safe,smb-os-discovery -p 445 <target>
ssl-cert	Retrieves SSL certificate details. **Example**: nmap --script=safe,ssl-cert -p 443 <target>
whois-domain	Performs a WHOIS lookup for a domain. **Example**: nmap --script=safe,whois-domain <target>
snmp-info	Retrieves basic information from an SNMP service. **Example**: nmap --script=safe,snmp-info -p 161 <target>

Note: The safe category is also triggered automatically with -sC.
nmap -sC <target>

11.) SERVICE VERSION DETECTION CATEGORY

These scripts enhance or customize Nmap's built-in version detection by probing specific services and retrieving detailed version and banner information.

SCRIPTS	DESCRIPTION
dns-nsid	Retrieves Name Server Identifier (NSID) from DNS servers. **Example:** nmap --script dns-nsid <target>
http-server-header	Displays the Server header from HTTP responses. **Example:** nmap -p80,443 --script http-server-header <target>
memcached-version	Retrieves version information from Memcached services. **Example:** nmap -p11211 --script memcached-version <target>
smb-protocols	Detects supported SMB protocol versions. **Example:** nmap -p445 --script smb-protocols <target>
ssh2-enum-algos	Enumerates supported SSH algorithms. **Example:** nmap -p22 --script ssh2-enum-algos <target>
ssh-hostkey	Retrieves and displays the SSH host key fingerprint. **Example:** nmap -p22 --script ssh-hostkey <target>
ssl-cert	Retrieves the SSL certificate from an SSL/TLS service. **Example:** nmap -p443 --script ssl-cert <target>
ssl-enum-ciphers	Enumerates supported SSL/TLS ciphers. **Example** nmap -p443 --script ssl-enum-ciphers <target>
xmpp-info	Extracts version and feature info from XMPP servers. **Example:** nmap -p5222,5269 --script xmpp-info <target>

12.) VULN CATEGORY

Scripts in this category are used to scan for vulnerabilities on host/devices

SCRIPTS	DESCRIPTION
http-vuln-cve2014-3704	Checks for SQL injection in Drupal 7.x. **Example:** nmap --script http-vuln-cve2014-3704 -p 80 <target>
http-vuln-cve2015-1427	Checks for Elasticsearch Groovy sandbox bypass. **Example:** nmap --script http-vuln-cve2015-1427 -p 9200 <target>
smb-vuln-ms17-010	Detects MS17-010 (EternalBlue) vulnerability in SMBv1. **Example**: nmap --script smb-vuln-ms17-010 -p 445 <target>
ftp-vsftpd-backdoor	Detects a malicious backdoor in vsftpd 2.3.4. **Example:** nmap --script ftp-vsftpd-backdoor -p 21 <target>
ssl-ccs-injection	Detects the OpenSSL CCS injection vulnerability (CVE-2014-0224). **Example:** nmap --script ssl-ccs-injection -p 443 <target>
http-vuln-cve2017-5638	Checks for Apache Struts2 Jakarta Multipart parser RCE (CVE-2017-5638). **Example:** nmap --script http-vuln-cve2017-5638 -p 8080 <target>
mysql-vuln-cve2012-2122	Checks for MySQL authentication bypass vulnerability. **Example:** nmap --script mysql-vuln-cve2012-2122 -p 3306 <target>
vulners	Checks for latest CVE using Vulners NSE **Example** nmap -sV --script vulners <target> **#Combine with brute-force NSEs** nmap -sV --script "vulners,ftp-brute,ssh-brute" <target> **# Parse only CVEs (grep example)** nmap -sV --script vulners <target> | grep "CVE" **for Windows, replace grep with:** (| findstr “CVE”) **# Grep for latest CVEs (2023-2025)** nmap -sV --script vulners <target> | grep -E "CVE-(2023|2024|2025)" **for Windows, replace grep with:** (| findstr /R "CVE-2023 CVE-2024 CVE-2025") **# Show only critical (CVSS ≥ 9.0)**

	nmap -sV --script vulners <target> | grep -E "CVE-(2023|2024|2025)" | awk '$2 >= 9.0 {print $0}' **for Windows, replace grep with:** \| findstr /R "CVE-2023 CVE-2024 CVE-2025" \| powershell -Command "$input | ForEach-Object { if ($_ -match '\s9\.[0-9]') { $_ } }"

WHAT HAPPENS WHEN YOU RUN NMAP **-sS** ,**-sT** and **–sA** SCANS

Nmap -sS host : TCP SYN Scan (Half-open scan)

How it works:
Sends a TCP **SYN** packet to the target port.
If the port replies **SYN/ACK** → it's *open*.
If the port replies **RST** → it's *closed*.
Nmap **does not complete the handshake** , it sends an RST instead of ACK (half-open).

- **Advantages:**

Faster.
Stealthier — many services don't log incomplete handshakes.
Needs **root/admin privileges** to craft raw packets.

- **Use case:**

Quick, stealthy port scan for recon.

Nmap -sT host : TCP Connect Scan (Full-open scan)

How it works:
Uses the OS's normal connect() system call to complete the **full TCP handshake** (SYN → SYN/ACK → ACK).
The connection is actually established before closing.

- **Advantages:**

Works without special privileges (non-root).

- **Disadvantages:**

Slower.
Easier to detect/log because connections are completed.

- **Use case:**

When you don't have root/admin privileges.

Nmap -sA host : TCP ACK Scan

How it works:
Sends TCP **ACK** packets to the target port.
The goal isn't to find open ports but to determine **firewall filtering**:
No response → filtered by firewall.
RST → unfiltered.
Often used to map firewall rules.

- **Advantages:**

Good for detecting stateless firewall rules.

- **Use case:**

Firewall and packet-filtering reconnaissance.

Compiled by ISSAT, I
1024-Cybersecurity Services

X: https://x.com/1024Cyber

GitHub: https://github.com/1024Cyber

LinkedIn: https://www/linkedin.com/in/1024Cyber