nmap switches cheat sheet

nmap switches cheat sheet is an essential resource for network administrators, cybersecurity professionals, and IT enthusiasts who rely on Nmap to perform network discovery and security auditing. This comprehensive guide provides an in-depth overview of the most commonly used Nmap switches, enabling users to execute efficient scans tailored to their specific needs. From basic host discovery to advanced port scanning techniques, understanding the various options and flags can dramatically improve the effectiveness and precision of network assessments. This article covers topics including scan types, host discovery options, port specification, output formatting, and advanced features such as script scanning and timing controls. Whether you are a beginner or an experienced user, this nmap switches cheat sheet will serve as a valuable reference for optimizing your scanning strategies. Following the introduction, a clear table of contents outlines the main sections covered in this guide.

Basic Scan Switches

Understanding the fundamental switches used for basic scans is crucial when starting with Nmap. These switches allow users to perform quick and effective scans to identify live hosts, open ports, and services running on a network. Basic scan switches are often the first step in network reconnaissance and help lay the groundwork for more detailed analysis.

Ping Scan

The **-sn** switch, formerly known as *-sP*, tells Nmap to perform a ping scan. This means Nmap will only check if the hosts are up without scanning any ports. It is useful for quickly identifying live devices on a network.

Simple TCP Connect Scan

The **-sT** switch enables a TCP connect scan, which attempts to complete the TCP three-way handshake with target ports. This scan type does not require special privileges and is useful for basic port scanning on networks where raw packet privileges are not available.

SYN Scan

The **-sS** switch initiates a SYN scan, also known as a half-open scan. This method sends SYN packets and analyzes responses without completing the TCP handshake, making it stealthier and faster than a full connect scan.

- **-sn**: Ping scan (host discovery only)
- **-sT**: TCP connect scan
- **-sS**: SYN scan (stealth scan)

Host Discovery Options

Host discovery switches help determine which hosts in a specified range are online and responsive. These options can be combined to improve accuracy and speed by using different protocols and techniques to elicit responses from target devices.

ICMP Echo Request

The **-PE** switch sends ICMP echo requests (pings) to probe hosts. Many devices respond to this type of ping, making it a standard method for host discovery.

TCP SYN and ACK Probes

Switches **-PS** and **-PA** send TCP SYN and ACK packets respectively to specified ports. These probes can bypass some firewalls that block ICMP traffic but allow TCP traffic, improving host discovery success.

ARP Ping

By default, on local networks, Nmap uses ARP requests for host discovery. The **-PR** switch explicitly enables ARP ping, which is highly reliable for detecting hosts on Ethernet networks.

- **-PE**: ICMP echo request
- **-PS[port]**: TCP SYN ping to specified port
- **-PA[port]**: TCP ACK ping to specified port
- **-PR**: ARP ping (local network only)

Port Specification and Scan Techniques

Port specification switches allow targeting specific ports or ranges to optimize scan results and reduce scanning time. Nmap offers multiple scan techniques suited for different environments and security requirements.

Port Range and List

The **-p** switch is used to specify ports explicitly. Users can define single ports, comma-separated lists, or ranges using hyphens. For example, *-p 22,80,443* scans ports 22, 80, and 443, while *-p 1-1000* scans the first 1000 ports.

UDP Scan

The **-sU** switch enables UDP port scanning. UDP scans are slower and less reliable but necessary for detecting services running over UDP, such as DNS or SNMP.

Version Detection

The **-sV** switch probes open ports to determine the version of the service running. This information is critical for vulnerability assessments and understanding the target environment.

- **-p**: Specify ports to scan
- **-sU**: UDP scan
- **-sV**: Service/version detection

Output and Reporting Switches

Output formatting switches help users save scan results in various formats for analysis, reporting, or archival purposes. Effective reporting is essential in professional environments to document findings and support decision-making.

Normal Output

The **-oN** switch saves scan results in a human-readable normal format, which is useful for quick reviews and sharing with non-technical stakeholders.

XML Output

The **-oX** switch exports results in XML format, suitable for automated processing or importing into other tools for further analysis.

Grepable Output

The **-oG** switch produces output designed for easy parsing with grep or other command-line tools, aiding in quick filtering and extraction of specific information.

- **-oN filename**: Normal output
- **-oX filename**: XML output
- **-oG filename**: Grepable output
- **-oA basename**: Saves all formats simultaneously

Advanced Scanning Features

Nmap includes advanced switches that enhance scanning capabilities, providing deeper insights and customized scanning strategies. These features are particularly valuable for security assessments and thorough network evaluations.

OS Detection

The **-O** switch enables operating system detection by analyzing TCP/IP stack responses. This helps identify the OS version and type running on target

hosts.

Traceroute

The **--traceroute** option traces the network path to the target, revealing intermediate hops and network topology. It can assist in understanding network infrastructure and potential points of vulnerability.

Decoy Scans

The **-D** switch performs decoy scans by sending packets from fake sources to confuse intrusion detection systems and obscure the origin of the scan.

- **-O**: OS detection
- **--traceroute**: Trace network path
- **-D decoy1,decoy2,...**: Decoy scanning

Timing and Performance Controls

Timing switches allow users to balance scan speed and stealthiness. Adjusting timing can help evade detection or complete scans faster, depending on the operational requirements and network conditions.

Timing Templates

Nmap provides predefined timing templates from **-T0** (paranoid) to **-T5** (insane), controlling delay between probes and parallelism.

Max Retries

The **--max-retries** switch limits the number of retransmissions for probes, affecting scan duration and reliability.

Host Timeout

The **--host-timeout** option sets a maximum time allowed for scanning a host before timing out, preventing scans from hanging indefinitely.

- **-T0 to -T5**: Timing templates from slowest to fastest
- **--max-retries**: Limit probe retransmissions
- **--host-timeout**: Maximum scan time per host

Script Scanning and NSE

Nmap’s scripting engine (NSE) dramatically extends its capabilities by allowing users to run custom scripts for vulnerability detection, malware scanning, and more. Understanding script-related switches is essential for leveraging this powerful feature.

Enable Scripts

The **--script** switch specifies which NSE scripts to run during a scan. Users can target specific scripts by name or use categories such as *default*, *vuln*, or *exploit*.

Script Arguments

The **--script-args** option passes arguments to scripts, allowing customization of script behavior, such as specifying usernames, passwords, or ports.

Script Output

Nmap includes script results in the standard output formats, making it easy to correlate script findings with port and host data.

- **--script=scriptname**: Run specific NSE scripts
- **--script-args=name=value**: Pass arguments to scripts
- **--script-trace**: Debug script execution

Frequently Asked Questions

What is an Nmap switches cheat sheet?

An Nmap switches cheat sheet is a concise reference guide that lists commonly used command-line options (switches) for the Nmap network scanning tool, helping users quickly remember and utilize various scanning techniques.

Which Nmap switch is used to perform a TCP SYN scan?

The switch '-sS' is used in Nmap to perform a TCP SYN scan, which is a stealthy scan that sends SYN packets to determine open ports without completing the TCP handshake.

How can I scan multiple IP addresses using Nmap switches?

You can scan multiple IP addresses by listing them separated by spaces, or by using IP ranges or CIDR notation, for example: 'nmap 192.168.1.1 192.168.1.2' or 'nmap 192.168.1.0/24'.

What switch do I use to enable verbose output in Nmap?

The '-v' switch enables verbose output in Nmap, providing more detailed information during the scan process.

How do I perform an OS detection scan with Nmap?

Use the '-O' switch to enable OS detection, which attempts to determine the operating system running on target hosts.

Which switch helps in scanning all ports with Nmap?

The '-p-' switch tells Nmap to scan all 65535 TCP ports instead of the default top 1000 ports.

How can I perform a UDP scan using Nmap switches?

The '-sU' switch is used to perform a UDP scan, which sends UDP packets to detect open UDP ports on the target.

What is the purpose of the '-A' switch in Nmap?

The '-A' switch enables aggressive scan options, including OS detection, version detection, script scanning, and traceroute, providing comprehensive information about the target.

How do I save scan results to a file using Nmap switches?

You can save scan results using output switches like '-oN' for normal output, '-oX' for XML, and '-oG' for grepable output. For example, 'nmap -oN scan.txt 192.168.1.1' saves the output to scan.txt.

Additional Resources

1. *Nmap Network Scanning: The Official Nmap Project Guide to Network Discovery and Security Scanning*
This comprehensive guide, authored by the creators of Nmap, covers all aspects of network scanning using Nmap. It provides detailed explanations of Nmap commands, switches, and options, making it an essential resource for both beginners and advanced users. The book includes practical examples and real-world scenarios to help readers master network discovery and security auditing.

2. *Nmap Cookbook: The Fat-free Guide to Network Discovery and Security Scanning*
The Nmap Cookbook is a practical collection of recipes that demonstrate the use of Nmap switches and features. Each recipe focuses on specific tasks such as scanning techniques, script usage, and output analysis. It’s ideal for system administrators and security professionals looking for quick, actionable tips on using Nmap effectively.

3. *Mastering Nmap: Network Security and Penetration Testing Techniques*
This book delves into advanced Nmap functionalities, including custom scripts, performance tuning, and evasion techniques. It explains how to leverage various switches to conduct thorough penetration tests and vulnerability assessments. Readers will benefit from detailed case studies and step-by-step walkthroughs.

4. *Nmap in the Enterprise: Practical Network Security Scanning for IT Professionals*
Focused on enterprise environments, this book explores how to integrate Nmap scanning into large-scale network security workflows. It highlights essential switches for scheduling, automation, and reporting. The book also covers best practices for minimizing network disruption while maximizing scan effectiveness.

5. *Effective Nmap Scripting: Automate Network Security Tasks with NSE*
This title concentrates on the Nmap Scripting Engine (NSE) and how to use its switches to automate complex scanning tasks. It provides a thorough introduction to writing and deploying custom scripts, enhancing Nmap's capabilities beyond standard scanning. Security analysts and developers will find this book incredibly useful for extending Nmap’s functionality.

6. *Nmap Essentials: Quick Reference for Network Scanning Commands and*

Switches
Designed as a quick reference guide, this book compiles all essential Nmap switches and command-line options in an easy-to-access format. It is perfect for users who need to quickly recall syntax and usage without sifting through lengthy documentation. The concise explanations and examples help users optimize their scanning strategies efficiently.

7. *Practical Nmap Strategies for Cybersecurity Professionals*
This book offers a strategic approach to using Nmap in cybersecurity operations. It emphasizes the importance of selecting the right switches for different security objectives such as reconnaissance, vulnerability detection, and compliance auditing. Readers gain insights into integrating Nmap with other security tools and frameworks.

8. *Nmap for Network Administrators: Troubleshooting and Security Scanning Made Simple*
Aimed at network administrators, this book simplifies the use of Nmap for routine network troubleshooting and security checks. It explains common switches that help identify network issues, open ports, and unauthorized services. The book also provides tips for generating clear scan reports to support network management.

9. *The Nmap Switches Cheat Sheet: A Handy Guide to Command-line Options*
This concise cheat sheet-style book is dedicated entirely to cataloging Nmap switches and their practical uses. It serves as a quick-access manual for both new and experienced Nmap users. With categorized sections and usage tips, it helps users navigate and apply Nmap commands with confidence and speed.

Nmap Switches Cheat Sheet