

# CHEAT SHEET

### **Scanning Options**

Target network range: 10.10.10.0/24

Disables port scanning: -sn

Disables ICMP Echo Requests: -Pn

Disables DNS Resolution: -n

Performs the ping scan by using ICMP Echo Requests against the target: -PE

Shows all packets sent and received: --packet-trace

Displays the reason for a specific result: --reason

Disables ARP Ping Requests: --disable-arp-ping

Scans the specified top ports that have been defined as most frequent: --top-ports=<num>

Scan all ports: -p-

CHEAT SHEET

Scan all ports between 22 and 110: -p22-110

Scans only the specified ports 22 and 25: -p22, 25

Scans top 100 ports: -F

Performs an TCP SYN-Scan: -sS

Performs an TCP ACK-Scan: -sA

Performs an UDP Scan: -sU

Scans the discovered services for their versions: -sV

Perform a Script Scan with scripts that are categorized as "default": -sC

Performs a Script Scan by using the specified scripts: --script <script>

Performs an OS Detection Scan to determine the OS of the target: -0

Performs OS Detection, Service Detection, and traceroute scans: -A

Sets the number of random Decoys that will be used to scan the target: -D RND: 5



CHEAT SHEET

Specifies the network interface that is used for the scan: -e

Specifies the source IP address for the scan: -S 10.10.10.200

Specifies the source port for the scan: -g

DNS resolution is performed by using a specified name server:
--dns-server <ns>

### **Output Options**

Stores the results in all available formats starting with the name of "filename": -oA filename

Stores the results in normal format with the name "filename": -oN filename

Stores the results in "grepable" format with the name of "filename": -oG filename

Stores the results in XML format with the name of "filename": -oX filename

#### CHEAT SHEET

#### **Performance Options**

Sets the number of retries for scans of specific ports:

--max-retries < num>

Displays scan's status every 5 seconds:

--stats-every=5s

Displays verbose output during the scan:

-v/-vv

Sets the specified time value as initial RTT timeout:

--initial-rtt-timeout 50ms

Sets the specified time value as maximum RTT timeout:

--max-rtt-timeout 100ms

Sets the number of packets that will be sent simultaneously:

--min-rate 300

Specifies the specific timing template:

-T <0-5>

