Keywords: Nmap, Port Scan, Stealth Scan
Command: sudo nmap -sS target_IP
Functionality and Use Cases: This command is used to perform a TCP SYN scan, also known as a stealth scan. It's useful when you want to scan a target without making a full TCP connection.
Argument Description: -sS specifies the type of scan to be a TCP SYN scan.
Situations of Fail: This command may fail if the target system has firewall rules that block SYN packets.

Keywords: Nmap, Port Scan, Version Detection
Command: nmap -sV target_IP
Functionality and Use Cases: This command is used to determine the version of the services running on the target's open ports.
Argument Description: -sV enables version detection.
Situations of Fail: This command may fail if the service versions are configured to not respond to such probes.

Keywords: Nmap, Port Scan, Aggressive Scan
Command: nmap -A target_IP
Functionality and Use Cases: This command performs an aggressive scan which includes OS detection, version detection, script scanning, and traceroute.
Argument Description: -A enables aggressive scan options.
Situations of Fail: This command may fail if the target system has strong firewall rules or intrusion detection/prevention systems.

Keywords: Nmap, Port Scan, Timing Template
Command: nmap -T4 -sV target_IP
Functionality and Use Cases: This command is used to set the timing template to "aggressive". It speeds up the scan.
Argument Description: -T4 sets the timing template to "aggressive".
Situations of Fail: This command may fail if the network latency is high or the target system is heavily loaded.

Keywords: Nmap, Port Scan, OS Detection
Command: sudo nmap -O -sV target_IP
Functionality and Use Cases: This command is used to enable OS detection.
Argument Description: -O enables OS detection.
Situations of Fail: This command may fail if the target system is configured to not respond to such probes.

Keywords: Nmap, Port Scan, Ping Scan
Command: nmap -Pn -sV target_IP
Functionality and Use Cases: This command is used to skip the host discovery phase and directly scan the target.

Argument Description: -Pn skips host discovery.
Situations of Fail: This command may fail if the target system is offline or blocking all incoming packets.

Keywords: Nmap, Port Scan, Decoy Scan
Command: nmap -D RND:10 target_IP
Functionality and Use Cases: This command is used to perform a decoy scan, making it appear that the scan is coming from random IP addresses.
Argument Description: -D RND:10 generates 10 random decoy IP addresses.
Situations of Fail: This command may fail if the network's egress filtering is strict.

Keywords: Nmap, Port Scan, Script Scan
Command: nmap --script=default target_IP
Functionality and Use Cases: This command is used to perform a script scan using the default set of scripts.
Argument Description: --script=default specifies to use the default set of scripts.
Situations of Fail: This command may fail if the target system has strong firewall rules or intrusion detection/prevention systems.

Keywords: Nmap, Port Scan, Specific Ports
Command: nmap -p 80,443 -sV target_IP
Functionality and Use Cases: This command is used to scan specific ports (in this case, ports 80 and 443).
Argument Description: -p 80,443 specifies the ports to be scanned.
Situations of Fail: This command may fail if the specified ports are closed or filtered.

Keywords: Nmap, Port Scan, UDP Scan
Command: sudo nmap -sU target_IP
Functionality and Use Cases: This command is used to perform a UDP scan.
Argument Description: -sU specifies the type of scan to be a UDP scan.
Situations of Fail: This command may fail if the target system has firewall rules that block UDP packets.

Keywords: Nmap, Port Scan, TCP Connect Scan
Command: sudo nmap -sT target_IP
Functionality and Use Cases: This command is used to perform a TCP connect scan. It's useful when you can't send raw packets.
Argument Description: -sT specifies the type of scan to be a TCP connect scan.
Situations of Fail: This command may fail if the target system has firewall rules that block incoming TCP connections.

Keywords: Nmap, Port Scan, IP Protocol Scan
Command: sudo nmap -sO target_IP

Functionality and Use Cases: This command is used to determine which IP protocols (TCP, ICMP, IGMP, etc.) are supported by the target.
Argument Description: -sO specifies the type of scan to be an IP protocol scan.
Situations of Fail: This command may fail if the target system has firewall rules that block the IP protocols being probed.

Keywords: Nmap, Port Scan, Idle Scan
Command: sudo nmap -sI zombie_IP target_IP
Functionality and Use Cases: This command is used to perform an idle scan. It's useful when you want to scan a target while disguising the source of the scan.
Argument Description: -sI zombie_IP specifies the IP address of a "zombie" host to be used in the scan.
Situations of Fail: This command may fail if the "zombie" host is not truly idle or if it doesn't respond in the expected manner.

Keywords: Nmap, Port Scan, Fast Scan
Command: nmap -F target_IP
Functionality and Use Cases: This command is used to perform a fast scan, which scans fewer ports than a regular scan.
Argument Description: -F enables fast scan.
Situations of Fail: This command may fail if the most commonly open ports are not included in the fast scan.

Keywords: Nmap, Port Scan, Fragment Packets
Command: nmap -f target_IP
Functionality and Use Cases: This command is used to fragment the packets, making it harder for packet filters, intrusion detection systems, and other defenses to detect the scan.
Argument Description: -f enables packet fragmentation.
Situations of Fail: This command may fail if the network's egress filtering is strict.

Keywords: Nmap, Port Scan, Xmas Scan
Command: sudo nmap -sX target_IP
Functionality and Use Cases: This command is used to perform an Xmas scan, which sets the FIN, PSH, and URG flags, lighting up the packet like a Christmas tree.
Argument Description: -sX specifies the type of scan to be an Xmas scan.
Situations of Fail: This command may fail if the target system's TCP stack doesn't respond in the expected manner.

Keywords: Nmap, Port Scan, Null Scan
Command: sudo nmap -sN target_IP
Functionality and Use Cases: This command is used to perform a null scan, which sends packets with no flags set.
Argument Description: -sN specifies the type of scan to be a null scan.

Situations of Fail: This command may fail if the target system's TCP stack doesn't respond in the expected manner.

Keywords: Nmap, Port Scan, FIN Scan
Command: sudo nmap -sF target_IP
Functionality and Use Cases: This command is used to perform a FIN scan, which sends packets with only the FIN flag set.
Argument Description: -sF specifies the type of scan to be a FIN scan.
Situations of Fail: This command may fail if the target system's TCP stack doesn't respond in the expected manner.

Keywords: Nmap, Port Scan, ACK Scan
Command: nmap -sA target_IP
Functionality and Use Cases: This command is used to perform an ACK scan, which can be used to map out firewall rulesets.
Argument Description: -sA specifies the type of scan to be an ACK scan.
Situations of Fail: This command may fail if the target system's firewall doesn't respond in the expected manner.

Keywords: Nmap, Port Scan, Window Scan
Command: nmap -sW target_IP
Functionality and Use Cases: This command is used to perform a window scan, which can be used to infer the open state of a port without receiving any response.
Argument Description: -sW specifies the type of scan to be a window scan.
Situations of Fail: This command may fail if the target system's TCP stack doesn't respond in the expected manner.

Keywords: Nmap, Port Scan, Maimon Scan
Command: nmap -sM target_IP
Functionality and Use Cases: This command is used to perform a Maimon scan, which sends packets with the FIN and ACK flags set.
Argument Description: -sM specifies the type of scan to be a Maimon scan.
Situations of Fail: This command may fail if the target system's TCP stack doesn't respond in the expected manner.

Keywords: Nmap, Port Scan, Zombie Host
Command: nmap -sI zombie_IP:port target_IP
Functionality and Use Cases: This command is used to perform an idle scan using a specific zombie host and port.
Argument Description: -sI zombie_IP:port specifies the IP address and port of a "zombie" host to be used in the scan.
Situations of Fail: This command may fail if the "zombie" host is not truly idle or if it doesn't respond in the expected manner.

Keywords: Nmap, Port Scan, Timestamp Ping
Command: nmap -PP target_IP
Functionality and Use Cases: This command is used to perform a timestamp ping, which can be used to determine the uptime of the target.
Argument Description: -PP specifies the type of ping to be a timestamp ping.
Situations of Fail: This command may fail if the target system doesn't respond to timestamp requests.

Keywords: Nmap, Port Scan, Netmask Request Ping
Command: nmap -PM target_IP
Functionality and Use Cases: This command is used to perform a netmask request ping, which can be used to determine the subnet mask of the target.
Argument Description: -PM specifies the type of ping to be a netmask request ping.
Situations of Fail: This command may fail if the target system doesn't respond to netmask requests.

Keywords: Nmap, Port Scan, IP ID Sequence Generation
Command: nmap --randomize-hosts target_IP
Functionality and Use Cases: This command is used to randomize the order in which target hosts are scanned.
Argument Description: --randomize-hosts enables host randomization.
Situations of Fail: This command may fail if the number of target hosts is too large to be handled by Nmap.

Command: nmap -sS [target IP]
Argument Description: This command performs a SYN scan.
Usage: It is used to detect open ports without completing the TCP handshake, making it less likely to be detected by firewalls and IDS.
Situations of Fail: It may fail if the target system is configured to ignore SYN packets.

Command: nmap -sT [target IP]
Argument Description: This command performs a TCP connect scan.
Usage: It is used to detect open ports by completing the TCP handshake.
Situations of Fail: It may fail if the target system is configured to block new TCP connections.

Command: nmap -sU [target IP]
Argument Description: This command performs a UDP scan.
Usage: It is used to detect open UDP ports.
Situations of Fail: It may fail if the target system is configured to ignore UDP packets.

Command: nmap -sA [target IP]
Argument Description: This command performs an ACK scan.
Usage: It is used to detect firewalls and their rules.
Situations of Fail: It may fail if the target system is configured to ignore ACK packets.

Command: nmap -sN [target IP]
Argument Description: This command performs a Null scan.
Usage: It is used to detect open ports without sending any data.
Situations of Fail: It may fail if the target system is configured to ignore Null packets.

Command: nmap -sF [target IP]
Argument Description: This command performs a FIN scan.
Usage: It is used to detect open ports by sending a TCP packet with the FIN flag set.
Situations of Fail: It may fail if the target system is configured to ignore FIN packets.

Command: nmap -sX [target IP]
Argument Description: This command performs an Xmas scan.
Usage: It is used to detect open ports by sending a TCP packet with multiple flags set.
Situations of Fail: It may fail if the target system is configured to ignore Xmas packets.

Command: nmap -sI [target IP]
Argument Description: This command performs an Idle scan.
Usage: It is used to detect open ports without revealing the scanner's IP address.
Situations of Fail: It may fail if the target system is configured to ignore Idle packets.

Command: nmap -sV [target IP]
Argument Description: This command performs a version detection scan.
Usage: It is used to detect the version of services running on open ports.
Situations of Fail: It may fail if the target system is configured to block version detection scans.

Command: nmap -sC [target IP]
Argument Description: This command performs a script scan.
Usage: It is used to run scripts against open ports to gather more information.
Situations of Fail: It may fail if the target system is configured to block script scans.

Command: nmap -sR [target IP]
Argument Description: This command performs an RPC scan.
Usage: It is used to detect open RPC (Remote Procedure Call) services.
Situations of Fail: It may fail if the target system is configured to block RPC scans.

Command: nmap -sL [target IP]
Argument Description: This command performs a list scan.
Usage: It is used to list targets without scanning them.
Situations of Fail: It may fail if the target system is configured to block list scans.

Command: nmap -sP [target IP]
Argument Description: This command performs a ping scan.
Usage: It is used to detect if the target is up without scanning ports.

Situations of Fail: It may fail if the target system is configured to block ICMP requests.

Command: nmap -sZ [target IP]
Argument Description: This command performs a SCTP INIT scan.
Usage: It is used to detect open SCTP (Stream Control Transmission Protocol) ports.
Situations of Fail: It may fail if the target system is configured to block SCTP scans.

Command: nmap -sO [target IP]
Argument Description: This command performs an IP protocol scan.
Usage: It is used to detect supported IP protocols.
Situations of Fail: It may fail if the target system is configured to block IP protocol scans.

Command: nmap -sY [target IP]
Argument Description: This command performs a SCTP COOKIE ECHO scan.
Usage: It is used to detect open SCTP ports using COOKIE ECHO chunks.
Situations of Fail: It may fail if the target system is configured to block SCTP COOKIE ECHO scans.

Command: nmap -sM [target IP]
Argument Description: This command performs a SCTP address scan.
Usage: It is used to detect SCTP supported addresses.
Situations of Fail: It may fail if the target system is configured to block SCTP address scans.

Command: nmap -sW [target IP]
Argument Description: This command performs a Window scan.
Usage: It is used to detect open ports by examining the TCP window size.
Situations of Fail: It may fail if the target system is configured to block Window scans.

Command: nmap -sG [target IP]
Argument Description: This command performs a GGP scan.
Usage: It is used to detect open GGP (Gateway-to-Gateway Protocol) services.
Situations of Fail: It may fail if the target system is configured to block GGP scans.

Command: nmap -sH [target IP]
Argument Description: This command performs a HMP scan.
Usage: It is used to detect open HMP (Host Monitoring Protocol) services.
Situations of Fail: It may fail if the target system is configured to block HMP scans.

Command: nmap -sB [target IP]
Argument Description: This command performs a BGP scan.
Usage: It is used to detect open BGP (Border Gateway Protocol) services.
Situations of Fail: It may fail if the target system is configured to block BGP scans.

Command: nmap -sD [target IP]

Argument Description: This command performs a DCCP scan.
Usage: It is used to detect open DCCP (Datagram Congestion Control Protocol) services.
Situations of Fail: It may fail if the target system is configured to block DCCP scans.

Command: nmap -sE [target IP]
Argument Description: This command performs a EGP scan.
Usage: It is used to detect open EGP (Exterior Gateway Protocol) services.
Situations of Fail: It may fail if the target system is configured to block EGP scans.

Command: nmap -sI [target IP]
Argument Description: This command performs an IGMP scan.
Usage: It is used to detect open IGMP (Internet Group Management Protocol) services.
Situations of Fail: It may fail if the target system is configured to block IGMP scans.

Command: nmap -sJ [target IP]
Argument Description: This command performs a OSPFIGP scan.
Usage: It is used to detect open OSPFIGP (Open Shortest Path First Interior Gateway Protocol) services.
Situations of Fail: It may fail if the target system is configured to block OSPFIGP scans.

Command: nmap -sK [target IP]
Argument Description: This command performs a BBN-RCC-MON scan.
Usage: It is used to detect open BBN-RCC-MON services.
Situations of Fail: It may fail if the target system is configured to block BBN-RCC-MON scans.

Command: nmap -sL [target IP]
Argument Description: This command performs a CBT scan.
Usage: It is used to detect open CBT (Core Based Trees) services.
Situations of Fail: It may fail if the target system is configured to block CBT scans.

Command: nmap -sM [target IP]
Argument Description: This command performs a PIM scan.
Usage: It is used to detect open PIM (Protocol Independent Multicast) services.
Situations of Fail: It may fail if the target system is configured to block PIM scans.

Command: nmap -sN [target IP]
Argument Description: This command performs a PUP scan.
Usage: It is used to detect open PUP (PARC Universal Packet) services.
Situations of Fail: It may fail if the target system is configured to block PUP scans.

Command: nmap -sO [target IP]
Argument Description: This command performs a ARGUS scan.
Usage: It is used to detect open ARGUS services.
Situations of Fail: It may fail if the target system is configured to block ARGUS scans.

Keywords: Nmap, Vulnerability Scanning, Functionality, Port Scanning
Command: nmap -p 1-65535 -T4 -A -v [target IP]
Vulnerable Service Description: This command scans all ports to identify open ones, which could be vulnerable to attacks.
Usage: To identify all open ports on the target machine.
Situations of Fail: If the target machine has a firewall that blocks port scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Version Detection
Command: nmap -sV [target IP]
Vulnerable Service Description: This command identifies the version of the services running on the target machine.
Usage: To identify potentially outdated and vulnerable software versions.
Situations of Fail: If the target machine has a firewall that blocks version detection, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, OS Detection
Command: nmap -O [target IP]
Vulnerable Service Description: This command identifies the operating system of the target machine.
Usage: To identify potentially outdated and vulnerable operating systems.
Situations of Fail: If the target machine has a firewall that blocks OS detection, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script vuln [target IP]
Vulnerable Service Description: This command runs a script to identify known vulnerabilities on the target machine.
Usage: To identify known vulnerabilities that can be exploited.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Aggressive Scan
Command: nmap -A [target IP]
Vulnerable Service Description: This command performs an aggressive scan, which includes OS detection, version detection, script scanning, and traceroute.
Usage: To perform a comprehensive vulnerability scan.
Situations of Fail: If the target machine has a firewall that blocks aggressive scans, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Stealth Scan
Command: nmap -sS [target IP]

Vulnerable Service Description: This command performs a stealth scan, which is less likely to be detected by the target machine.
Usage: To perform a stealthy vulnerability scan.
Situations of Fail: If the target machine has a firewall that blocks stealth scans, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, UDP Scan
Command: nmap -sU [target IP]
Vulnerable Service Description: This command performs a UDP scan, which can identify open UDP ports that could be vulnerable to attacks.
Usage: To identify open UDP ports on the target machine.
Situations of Fail: If the target machine has a firewall that blocks UDP scans, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Ping Scan
Command: nmap -sn [target IP]
Vulnerable Service Description: This command performs a ping scan, which can identify if the target machine is up and running.
Usage: To identify if the target machine is up and running.
Situations of Fail: If the target machine has a firewall that blocks ping scans, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Timing Template
Command: nmap -T4 [target IP]
Vulnerable Service Description: This command sets the timing template to "aggressive", which speeds up the scan.
Usage: To speed up the vulnerability scan.
Situations of Fail: If the target machine has a firewall that blocks aggressive timing templates, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2014-3704 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2014-3704 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2014-3704 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script smb-vuln-ms17-010 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the MS17-010 vulnerability.
Usage: To identify if the target machine is vulnerable to the MS17-010 vulnerability.

Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2017-5638 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2017-5638 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2017-5638 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2017-1001000 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2017-1001000 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2017-1001000 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2018-11776 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2018-11776 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2018-11776 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2019-6340 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2019-6340 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2019-6340 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2020-0796 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2020-0796 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2020-0796 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2020-1938 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2020-1938 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2020-1938 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2020-3452 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2020-3452 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2020-3452 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2021-3156 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2021-3156 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2021-3156 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.

Keywords: Nmap, Vulnerability Scanning, Functionality, Script Scanning
Command: nmap --script http-vuln-cve2021-21985 [target IP]
Vulnerable Service Description: This command runs a script to identify if the target machine is vulnerable to the CVE-2021-21985 vulnerability.
Usage: To identify if the target machine is vulnerable to the CVE-2021-21985 vulnerability.
Situations of Fail: If the target machine has a firewall that blocks script scanning, this command will fail.