The Ethical Hacker's Command Handbook

Chapter 3 – Part 1: Searchsploit Fundamentals & Exploit Research

Enumeration tells you what exists. Research tells you what is known about it.

Learning Objectives

Understand Searchsploit, Exploit-DB, basic searches, version-specific research, CVE lookups, result interpretation, and responsible vulnerability research workflows.

What is Searchsploit?

Searchsploit is a command-line tool that searches a locally stored copy of Exploit-DB. It helps locate public exploit references for identified software. It does not scan or exploit targets.

What is Exploit-DB?

Exploit-DB is a public archive of exploit references, proof-of-concept code, and related information. Entries typically include a title, EDB-ID, platform, file path, and references.

searchsploit apache

Purpose: Search software

What it does: Find exploit references related to Apache.

When to use: After identifying Apache with Nmap.

Avoid when: Software is still unknown.

Memory Tip: Search software first.

searchsploit "Apache 2.4.49"

Purpose: Search by version

What it does: Narrow results using product and version.

When to use: Exact version identified.

Avoid when: Version unknown.

Memory Tip: Version = Better results.

searchsploit windows

Purpose: Search by operating system

What it does: Locate Windows-related entries.

When to use: After OS detection.

Avoid when: Searching for a specific application.

Memory Tip: OS-level research.

searchsploit samba

Purpose: Search by service

What it does: Research a detected service.

When to use: Service identified during enumeration.

Avoid when: Service not confirmed.

Memory Tip: One service at a time.

searchsploit CVE-2021-41773

Purpose: Search by CVE

What it does: Locate entries matching a known CVE.

When to use: You already know the CVE identifier.

Avoid when: CVE is unknown.

Memory Tip: CVE = Specific vulnerability.

Typical Workflow

Nmap Enumeration → Identify Software → Identify Version → Searchsploit → Review Exploit References → Verify Applicability → Document Findings

Reference Fields

Field	Meaning
Title	Exploit description
EDB-ID	Exploit-DB identifier
Platform	Target platform
Path	Local exploit file location

Practice Questions

1. What is Searchsploit?
2. How is Searchsploit different from Nmap?
3. Why search using software versions?
4. What does an EDB-ID represent?
5. Why should exploit references always be verified before drawing conclusions?

The Ethical Hacker's Command Handbook

Chapter 3 – Part 2: Advanced Searchsploit Searching & Filters

Good researchers don't search more—they search smarter.

Learning Objectives

Learn exact phrase searches, title-only searches, multiple keywords, exclusion filters, version-based searches, CVE lookups, and efficient exploit research workflows.

searchsploit "Apache 2.4.49"

Purpose: Exact phrase search

What it does: Searches for an exact product/version.

When to use: Known software version.

Avoid when: Version unknown.

Memory Tip: Quotes = Exact

searchsploit apache linux

Purpose: Multiple keywords

What it does: Narrows results using multiple terms.

When to use: Reducing broad result sets.

Avoid when: Single keyword is sufficient.

Memory Tip: Combine related terms

searchsploit -t apache

Purpose: Title-only search

What it does: Searches only exploit titles.

When to use: Finding exploits by product name.

Avoid when: Searching descriptions is needed.

Memory Tip: t = Title

searchsploit --case Apache

Purpose: Case-sensitive search

What it does: Matches exact capitalization.

When to use: Specific text matching.

Avoid when: General searches.

Memory Tip: Case matters

searchsploit apache --exclude="dos"

Purpose: Exclude results

What it does: Filters unwanted result categories.

When to use: Removing irrelevant DoS entries.

Avoid when: All results are useful.

Memory Tip: Exclude = Filter

searchsploit windows

Purpose: Platform search

What it does: Searches by operating system/platform.

When to use: After OS detection.

Avoid when: Application-specific searches.

Memory Tip: Platform-based research

searchsploit CVE-2021-41773

Purpose: CVE search

What it does: Finds entries matching a CVE.

When to use: Known vulnerability identifier.

Avoid when: CVE unknown.

Memory Tip: CVE = Specific issue

Research Workflow

Nmap → Identify Product → Identify Version → Exact Search → Apply Filters → Review References → Verify Applicability → Document Findings

Goal	Command
Basic search	searchsploit apache
Exact phrase	searchsploit "Apache 2.4.49"
Title only	searchsploit -t apache
Multiple keywords	searchsploit apache linux
Exclude results	searchsploit apache --exclude="dos"
Search CVE	searchsploit CVE-2021-41773
Platform	searchsploit windows

Practice Questions

1. Why use quotation marks in Searchsploit?

2. What does -t do?

3. Why search using software versions?

4. How does --exclude help?
5. Why should Searchsploit results always be verified?

The Ethical Hacker's Command Handbook

Chapter 3 – Part 3: Searchsploit Options (-m, -x, -p, -u, -w, -j)

Finding an exploit is only the beginning. Understanding it is the next step.

Learning Objectives

Learn how to copy, inspect, locate, update, reference, and export Searchsploit results using the most useful command-line options.

Option -m

Command: searchsploit -m 50383

What it does: Copies the selected exploit into your current directory.

When to use: When you need your own editable copy.

Avoid when: You only want to read it.

Memory Tip: m = Make a copy

Option -x

Command: searchsploit -x 50383

What it does: Displays exploit source code in the terminal.

When to use: Quickly reviewing exploit code.

Avoid when: You intend to modify the file.

Memory Tip: x = Examine

Option -p

Command: searchsploit -p 50383

What it does: Shows the full local path to the exploit.

When to use: Finding or documenting exploit locations.

Avoid when: You already know the path.

Memory Tip: p = Path

Option -u

Command: searchsploit -u

What it does: Updates the local Exploit-DB database.

When to use: Before a new assessment or after a long gap.

Avoid when: Offline or intentionally using a fixed snapshot.

Memory Tip: u = Update

Option -w

Command: searchsploit -w apache

What it does: Displays Exploit-DB web URLs.

When to use: Reading online references or sharing links.

Avoid when: You only need local information.

Memory Tip: w = Website

Option -j

Command: searchsploit -j apache

What it does: Outputs results in JSON format.

When to use: Automation, scripts, dashboards.

Avoid when: You only need human-readable output.

Memory Tip: j = JSON

Comparison Table

Option	Purpose	Memory Tip
-m	Copy exploit locally	Make copy
-x	View exploit	Examine
-p	Show path	Path
-u	Update database	Update
-w	Show web URL	Website
-j	JSON output	JSON

Typical Workflow

Search → View (-x) → Copy (-m) if needed → Record Path (-p) → Read Online References (-w) → Keep Database Updated (-u).

Practice Questions

1. What is the difference between -m and -x?
2. Why should you use -u regularly?
3. What does -p display?
4. When is JSON output useful?
5. Why avoid editing the original Exploit-DB files?

The Ethical Hacker's Command Handbook

Chapter 3 – Part 4: Reading, Understanding & Analyzing Exploit Code

Reading exploit code is a research skill that helps you understand vulnerabilities and assess risk.

Learning Objectives

Understand exploit headers, software versions, CVE references, programming languages, dependencies, configuration variables, main logic, and a structured analysis workflow.

Exploit Header

Review the title, author, publication date, EDB-ID, target software, affected version, platform, and CVE before reading the code.

Software Version

Always compare the exploit's target version with the version identified during enumeration.

CVE Reference

Use CVE identifiers to research advisories, affected versions, severity, and mitigations.

Imports & Dependencies

Identify required libraries, packages, or external tools needed by the exploit.

Configuration Variables

Understand expected inputs such as target address, port, timeout, or file path.

Main Logic

Read the overall workflow to understand what the exploit is designed to do.

Output Messages

Review status messages to understand the script's execution flow.

Exploit Analysis Workflow

Searchsploit → Read Header → Verify Software Version → Review CVE → Check Dependencies → Understand Variables → Read Main Logic → Review Output → Document Findings

Section	What to Review
Header	Target, version, platform, CVE
Dependencies	Required libraries and tools

Variables	Expected user inputs
Main Logic	Overall workflow
Output	Status and results

Practice Questions

1. Why should you read the exploit header first?
2. Why must software versions be verified?
3. What can imports and dependencies tell you?
4. What are configuration variables used for?
5. Why is understanding the exploit workflow important?

The Ethical Hacker's Command Handbook

Chapter 3 – Part 5: Exploit Validation & Research Workflow

Identify → Research → Verify → Document

Learning Objectives

Learn how to validate exploit applicability by comparing software versions, reviewing CVEs, consulting vendor advisories, evaluating exploit requirements, and documenting findings.

Why Validation Matters

A Searchsploit result is not proof that a system is vulnerable. Always verify the software version, patch level, platform, and exploit requirements.

Compare Versions

Match the product, major version, minor version, and patch version identified during enumeration with the exploit documentation.

Review CVEs

Use CVE references to understand affected versions, severity, references, and available mitigations.

Vendor Advisories

Consult official vendor documentation to confirm affected versions, patches, fixes, and workarounds.

Evaluate Requirements

Determine whether authentication, configuration, operating system, or other prerequisites are required.

Document Findings

Record evidence, software version, exploit reference, verification status, and recommendations.

Validation Workflow

Nmap → Identify Product → Identify Version → Searchsploit → Review Exploit → Review CVE → Vendor Advisory → Evaluate Requirements → Document Findings

Step	Purpose
Nmap	Identify software and version
Searchsploit	Locate public exploit references

CVE	Research vulnerability details
Vendor Advisory	Confirm affected versions and fixes
Documentation	Record evidence and conclusions

Practice Questions

1. Why isn't a Searchsploit result enough to confirm a vulnerability?
2. Why should vendor advisories be reviewed?
3. What exploit requirements should be checked?
4. What should a professional report include?
5. Why is exploit validation important?

The Ethical Hacker's Command Handbook

Chapter 3 – Part 6: Searchsploit Master Cheat Sheet & Interview Guide

The best researchers memorize the workflow, not every command.

Top Searchsploit Commands

Purpose	Command
Basic Search	searchsploit apache
Exact Version	searchsploit "Apache 2.4.49"
Title Only	searchsploit -t apache
Copy Exploit	searchsploit -m 50383
View Exploit	searchsploit -x 50383
Show Path	searchsploit -p 50383
Update Database	searchsploit -u
Web URL	searchsploit -w apache
JSON Output	searchsploit -j apache
Search CVE	searchsploit CVE-2021-41773

Professional Research Workflow

Identify Software → Identify Version → Searchsploit → Review Header → Review CVE → Vendor Advisory → Evaluate Requirements → Document Findings

Memory Tricks

• -m = Make a copy

• -x = Examine exploit

• -p = Path

• -u = Update database

• -w = Website

• -j = JSON

• -t = Title search

• Quotes = Exact phrase

Common Beginner Mistakes

• Searching without confirming software versions.

• Ignoring exploit headers.

• Assuming every result applies.

• Forgetting to update Exploit-DB.

• Editing original exploit files instead of copying them.

Interview Questions

1. What is Searchsploit?
2. What is the difference between -m and -x?
3. Why use -u?
4. Why verify versions before reporting vulnerabilities?
5. What is the recommended exploit research workflow?