



# OSCP Cheat Sheet

commit activity 15/month

contributors 3

Commands, Payloads and Resources for the OffSec Certified Professional Certification (OSCP).

Since this little project get's more and more attention, I decided to update it as often as possible to focus more helpful and absolutely necessary commands for the exam. Feel free to submit a pull request or reach out to me on [Twitter](#) for suggestions.

Every help or hint is appreciated!

**DISCLAIMER:** A guy on Twitter got a point. Automatic exploitation tools like `sqlmap` are prohibited to use in the exam. The same goes for the automatic exploitation functionality of `LinPEAS`. I am not keeping track of current guidelines related to those tools. For that I want to point out that I am not responsible if anybody uses a tool without double checking the latest exam restrictions and fails the exam. Inform yourself before taking the exam!

I removed `sqlmap` because of the reasons above but `Metasploit` is still part of the guide because you can use it for one specific module. Thank you **Muztahidul Tanim** for making me aware and to [Yeeb](#) for the resources.

Here are the link to the [OSCP Exam Guide](#) and the discussion about [LinPEAS](#). I hope this helps.

**END NOTE:** This repository will also try to cover as much as possible of the tools required for the proving grounds boxes.

Thank you for reading.

## Table of Contents

---

- [Basics](#)
- [Information Gathering](#)
- [Vulnerability Analysis](#)
- [Web Application Analysis](#)
- [Password Attacks](#)
- [Reverse Engineering](#)
- [Exploitation Tools](#)
- [Post Exploitation](#)
- [Exploit Databases](#)
- [CVEs](#)
- [Payloads](#)
- [Wordlists](#)
- [Social Media Resources](#)
- [Commands](#)
  - [Basics](#)
    - [curl](#)
    - [Chisel](#)
    - [File Transfer](#)
    - [FTP](#)
    - [Kerberos](#)
    - [Ligolo-ng](#)

- Linux
- Microsoft Windows
- PHP Webserver
- Ping
- Python Webserver
- RDP
- showmount
- smbclient
- socat
- SSH
- Time and Date
- Tmux
- Upgrading Shells
- VirtualBox
- virtualenv
- Information Gathering
  - memcached
  - NetBIOS
  - Nmap
  - Port Scanning
  - snmpwalk
- Web Application Analysis
  - Burp Suite
  - cadaver
  - Cross-Site Scripting (XSS)
  - ffuf
  - Gobuster
  - GitTools
  - Local File Inclusion (LFI)
  - PDF PHP Inclusion
  - PHP Upload Filter Bypasses
  - PHP Filter Chain Generator
  - PHP Generic Gadget Chains (PHPGGC)

- Server-Side Request Forgery (SSRF)
- Server-Side Template Injection (SSTI)
- Upload Vulnerabilities
- wfuzz
- WPScan
- XML External Entity (XXE)
- Database Analysis
  - MongoDB
  - MSSQL
  - MySQL
  - NoSQL Injection
  - PostgreSQL
  - Redis
  - sqlcmd
  - SQL Injection
  - SQL Truncation Attack
  - sqlite3
  - sqsh
- Password Attacks
  - CrackMapExec
  - fcrack
  - hashcat
  - Hydra
  - John
  - Kerbrute
  - LaZagne
  - mimikatz
  - pypykatz
- Exploitation Tools
  - ImageTragick
  - MSL / Polyglot Attack
  - Metasploit
- Post Exploitation

- [Active Directory Certificate Services \(AD CS\)](#)
- [ADCSTemplate](#)
- [BloodHound](#)
- [BloodHound Python](#)
- [bloodyAD](#)
- [Certify](#)
- [Certipy](#)
- [enum4linux-ng](#)
- [Evil-WinRM](#)
- [Impacket](#)
- [JAWS](#)
- [Kerberos](#)
- [ldapsearch](#)
- [Linux](#)
- [Microsoft Windows](#)
- [PassTheCert](#)
- [PKINITtools](#)
- [Port Scanning](#)
- [powercat](#)
- [Powermad](#)
- [PowerShell](#)
- [pwncat](#)
- [rpcclient](#)
- [Rubeus](#)
- [RunasCs](#)
- [smbpasswd](#)
- [winexe](#)
- [CVE](#)
  - [CVE-2014-6271: Shellshock RCE PoC](#)
  - [CVE-2016-1531: exim LPE](#)
  - [CVE-2019-14287: Sudo Bypass](#)
  - [CVE-2020-1472: ZeroLogon PE](#)
  - [CVE-2021-3156: Sudo / sudoedit LPE](#)

- CVE-2021-44228: Log4Shell RCE (0-day)
- CVE-2022-0847: Dirty Pipe LPE
- CVE-2022-22963: Spring4Shell RCE (0-day)
- CVE-2022-30190: MS-MSDT Follina RCE
- CVE-2022-31214: Firejail LPE
- CVE-2023-21746: Windows NTLM EoP LocalPotato LPE
- CVE-2023-22809: Sudo Bypass
- CVE-2023-23397: Microsoft Outlook (Click-to-Run) PE (0-day) (PowerShell Implementation)
- CVE-2023-32629, CVE-2023-2640: GameOverlay Ubuntu Kernel Exploit LPE (0-day)
- CVE-2023-4911: Looney Tunables LPE
- GodPotato LPE
- Juicy Potato LPE
- JuicyPotatoNG LPE
- MySQL 4.x/5.0 User-Defined Function (UDF) Dynamic Library (2) LPE
- PrintSpoofer LPE
- SharpEfsPotato LPE
- Shocker Container Escape
- Payloads
  - Donut
  - Exiftool
  - GhostScript
  - nishang
  - Reverse Shells
  - ScareCrow
  - Shikata Ga Nai
  - Web Shells
  - ysoserial
- Templates
  - ASPX Web Shell
  - Bad YAML
  - Exploit Skeleton Python Script

- [JSON POST Rrequest](#)
- [Python Pickle RCE](#)
- [Python Redirect for SSRF](#)
- [Python Web Request](#)
- [XML External Entity \(XXE\)](#)

## Basics

Name	URL
Chisel	<a href="https://tinyurl.com/z6yl32k">https://tinyurl.com/z6yl32k</a>
CyberChef	<a href="https://tinyurl.com/h8hf4uc">https://tinyurl.com/h8hf4uc</a>
Swaks	<a href="https://tinyurl.com/ytqrw96w">https://tinyurl.com/ytqrw96w</a>

## Information Gathering

Name	URL
Nmap	<a href="https://tinyurl.com/9og4655">https://tinyurl.com/9og4655</a>

## Vulnerability Analysis

Name	URL
nikto	<a href="https://tinyurl.com/pu28ujz">https://tinyurl.com/pu28ujz</a>
Sparta	<a href="https://tinyurl.com/n24hfeb">https://tinyurl.com/n24hfeb</a>

## Web Application Analysis

Name	URL
ffuf	<a href="https://tinyurl.com/2e5nyvw8">https://tinyurl.com/2e5nyvw8</a>
fpmvuln	<a href="https://tinyurl.com/ys38zw8w">https://tinyurl.com/ys38zw8w</a>
Gobuster	<a href="https://tinyurl.com/y2bqjxcj">https://tinyurl.com/y2bqjxcj</a>
JSON Web Tokens	<a href="https://tinyurl.com/y3xmvqup">https://tinyurl.com/y3xmvqup</a>

JWT_Tool	<a href="https://tinyurl.com/2ry85jf7">https://tinyurl.com/2ry85jf7</a>
Leaky Paths	<a href="https://tinyurl.com/yman7qqf">https://tinyurl.com/yman7qqf</a>
PayloadsAllTheThings	<a href="https://tinyurl.com/y4ezgl4c">https://tinyurl.com/y4ezgl4c</a>
PHP Filter Chain Generator	<a href="https://tinyurl.com/yv3gjun7">https://tinyurl.com/yv3gjun7</a>
PHPGGC	<a href="https://tinyurl.com/yaz8sz94">https://tinyurl.com/yaz8sz94</a>
Spose	<a href="https://tinyurl.com/ynlscezd">https://tinyurl.com/ynlscezd</a>
Wfuzz	<a href="https://tinyurl.com/psuc9d9">https://tinyurl.com/psuc9d9</a>
WhatWeb	<a href="https://tinyurl.com/7u2t8h9">https://tinyurl.com/7u2t8h9</a>
WPScan	<a href="https://tinyurl.com/kc9zypf">https://tinyurl.com/kc9zypf</a>
ysoserial	<a href="https://tinyurl.com/q4x2gct">https://tinyurl.com/q4x2gct</a>

## Password Attacks

Name	URL
CrackMapExec	<a href="https://tinyurl.com/ngzqxs2">https://tinyurl.com/ngzqxs2</a>
Default Credentials Cheat Sheet	<a href="https://tinyurl.com/2mbz9hdk">https://tinyurl.com/2mbz9hdk</a>
Firefox Decrypt	<a href="https://tinyurl.com/y5dzosvz">https://tinyurl.com/y5dzosvz</a>
hashcat	<a href="https://tinyurl.com/ytbkp2hp">https://tinyurl.com/ytbkp2hp</a>
Hydra	<a href="https://tinyurl.com/podb3lg">https://tinyurl.com/podb3lg</a>
John	<a href="https://tinyurl.com/2yquyysj">https://tinyurl.com/2yquyysj</a>
keepass-dump-masterkey	<a href="https://tinyurl.com/ypwg5xh2">https://tinyurl.com/ypwg5xh2</a>
KeePwn	<a href="https://tinyurl.com/yq8uco5o">https://tinyurl.com/yq8uco5o</a>
Kerbrute	<a href="https://tinyurl.com/y66kz8ad">https://tinyurl.com/y66kz8ad</a>
LaZagne	<a href="https://tinyurl.com/m9k4zzr">https://tinyurl.com/m9k4zzr</a>
mimikatz	<a href="https://tinyurl.com/qdf539r">https://tinyurl.com/qdf539r</a>
Patator	<a href="https://tinyurl.com/onz6ly9">https://tinyurl.com/onz6ly9</a>



pypykatz	<a href="https://tinyurl.com/yxp3rds4">https://tinyurl.com/yxp3rds4</a>
RsaCtfTool	<a href="https://tinyurl.com/ybvm97ey">https://tinyurl.com/ybvm97ey</a>
SprayingToolkit	<a href="https://tinyurl.com/2yzbkw8x">https://tinyurl.com/2yzbkw8x</a>

## Reverse Engineering

Name	URL
AvaloniaLSpy	<a href="https://tinyurl.com/ywez6rvy">https://tinyurl.com/ywez6rvy</a>
binwalk	<a href="https://tinyurl.com/ycgf2rn2">https://tinyurl.com/ycgf2rn2</a>
cutter	<a href="https://tinyurl.com/ypy6duxm">https://tinyurl.com/ypy6duxm</a>
dnSpy	<a href="https://tinyurl.com/y7k9r2zy">https://tinyurl.com/y7k9r2zy</a>
GEF	<a href="https://tinyurl.com/nmtak2c">https://tinyurl.com/nmtak2c</a>
ghidra	<a href="https://tinyurl.com/y5ojpa5p">https://tinyurl.com/y5ojpa5p</a>
ImHex	<a href="https://tinyurl.com/y32bgpm9">https://tinyurl.com/y32bgpm9</a>
JD-GUI	<a href="https://tinyurl.com/yo3wyung">https://tinyurl.com/yo3wyung</a>
peda	<a href="https://tinyurl.com/ohx63nb">https://tinyurl.com/ohx63nb</a>
pwndbg	<a href="https://tinyurl.com/z5np3re">https://tinyurl.com/z5np3re</a>
Radare2	<a href="https://tinyurl.com/y3tvmeoq">https://tinyurl.com/y3tvmeoq</a>

## Exploitation Tools

Name	URL
Evil-WinRM	<a href="https://tinyurl.com/yyj7vkrq">https://tinyurl.com/yyj7vkrq</a>
ImageTragick	<a href="https://tinyurl.com/ycm9mqcs">https://tinyurl.com/ycm9mqcs</a>
Metasploit	<a href="https://tinyurl.com/d3kqjuo">https://tinyurl.com/d3kqjuo</a>
MSL / Polyglot Attack	<a href="https://tinyurl.com/y3qzu9oa">https://tinyurl.com/y3qzu9oa</a>

## Post Exploitation

Name	URL
ADCSKiller - An ADCS Exploitation Automation Tool	<a href="https://tinyurl.com/2xa2la3z">https://tinyurl.com/2xa2la3z</a>
ADCSTemplate	<a href="https://tinyurl.com/yp89grdv">https://tinyurl.com/yp89grdv</a>
BloodHound Docker	<a href="https://tinyurl.com/ypzjy87j">https://tinyurl.com/ypzjy87j</a>
BloodHound	<a href="https://tinyurl.com/y2s37jeg">https://tinyurl.com/y2s37jeg</a>
BloodHound	<a href="https://tinyurl.com/ymc3svna">https://tinyurl.com/ymc3svna</a>
BloodHound Python	<a href="https://tinyurl.com/ybsrj8pt">https://tinyurl.com/ybsrj8pt</a>
Certify	<a href="https://tinyurl.com/267b27re">https://tinyurl.com/267b27re</a>
Certipy	<a href="https://tinyurl.com/2c3ltmmt">https://tinyurl.com/2c3ltmmt</a>
enum4linux-ng	<a href="https://tinyurl.com/ymbmo3kr">https://tinyurl.com/ymbmo3kr</a>
Ghostpack-CompiledBinaries	<a href="https://tinyurl.com/ym88zaxv">https://tinyurl.com/ym88zaxv</a>
GTFOBins	<a href="https://tinyurl.com/yccgv6ks">https://tinyurl.com/yccgv6ks</a>
Impacket	<a href="https://tinyurl.com/243wq45x">https://tinyurl.com/243wq45x</a>
Impacket Static Binaries	<a href="https://tinyurl.com/ya5yzamu">https://tinyurl.com/ya5yzamu</a>
JAWS	<a href="https://tinyurl.com/223k2krg">https://tinyurl.com/223k2krg</a>
KrbRelay	<a href="https://tinyurl.com/yw8bodx9">https://tinyurl.com/yw8bodx9</a>
KrbRelayUp	<a href="https://tinyurl.com/2746ujpv">https://tinyurl.com/2746ujpv</a>
Krbrelayx	<a href="https://tinyurl.com/2bk3fjy5">https://tinyurl.com/2bk3fjy5</a>
LAPSDumper	<a href="https://tinyurl.com/287cdjlq">https://tinyurl.com/287cdjlq</a>
LES	<a href="https://tinyurl.com/yszucubjb">https://tinyurl.com/yszucubjb</a>
LinEnum	<a href="https://tinyurl.com/lxhk642">https://tinyurl.com/lxhk642</a>
LOLBAS	<a href="https://tinyurl.com/ypalagrk">https://tinyurl.com/ypalagrk</a>
Isassy	<a href="https://tinyurl.com/ygbh2wp6">https://tinyurl.com/ygbh2wp6</a>