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

        - 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	https://tinyurl.com/z6yl32k
CyberChef	https://tinyurl.com/h8hf4uc
Swaks	https://tinyurl.com/ytqrw96w

Information Gathering

Name	URL
Nmap	https://tinyurl.com/9og4655

Vulnerability Analysis

Name	URL
nikto	https://tinyurl.com/pu28ujz
Sparta	https://tinyurl.com/n24hfeb

Web Application Analysis

Name	URL
ffuf	https://tinyurl.com/2e5nyvw8
fpmvuln	https://tinyurl.com/ys38zw8w
Gobuster	https://tinyurl.com/y2bqjxcj
JSON Web Tokens	https://tinyurl.com/y3xmvqup

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

Password Attacks

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

pypykatz	https://tinyurl.com/yxp3rds4
RsaCtfTool	https://tinyurl.com/ybvm97ey
SprayingToolkit	https://tinyurl.com/2yzbkw8x

Reverse Engineering

Name	URL
AvalonialLSpy	https://tinyurl.com/ywez6rvy
binwalk	https://tinyurl.com/ycgf2rn2
cutter	https://tinyurl.com/ypy6duxm
dnSpy	https://tinyurl.com/y7k9r2zy
GEF	https://tinyurl.com/nmtak2c
ghidra	https://tinyurl.com/y5ojpa5p
ImHex	https://tinyurl.com/y32bgpm9
JD-GUI	https://tinyurl.com/yo3wyung
peda	https://tinyurl.com/ohx63nb
pwndbg	https://tinyurl.com/z5np3re
Radare2	https://tinyurl.com/y3tvmeoq

Exploitation Tools

Name	URL
Evil-WinRM	https://tinyurl.com/yyj7vkrg
ImageTragick	https://tinyurl.com/ycm9mqcs
Metasploit	https://tinyurl.com/d3kqjuo
MSL / Polyglot Attack	https://tinyurl.com/y3qzu9oa

Post Exploitation

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