Cheatsheet Workshop Penetration Testing
von Korbinian Bauer am 10.07.2025

Kali Linux

Kali Linux ist eine auf Debian basierende Linux Distribution, die speziell für Penetrationstests und Sicherheitsanalysen entwickelt wurde.

Benutzer: kali

Passwort: kali

Befehl	**Beschreibung**
cd	Verzeichnis wechseln
ls	Inhalt eines Verzeichnisses anzeigen
cat	Inhalt einer Datei anzeigen
ip addr (ip a)	Zeigt IP-Adressen und Netzwerkschnittstellen
ifconfig	Zeigt Netzwerkinterfaces und IP-Adressen
history	Zeigt zuletzt genutzte Befehle
pwd	Aktuelles Verzeichnis anzeigen
whoami	Aktuellen Benutzer anzeigen
find	Dateien und Verzeichnisse suchen
grep	Textmuster in Dateien suchen
man	Handbuchseite zu einem Befehl anzeigen
sudo su	Root-Shell starten (alle Befehle mit Root-Rechten)
python3 <python_script>	Python-Skript ausführen

Google Dorking

Befehl	Beschreibung	Beispiel
site:	Nur auf bestimmter Domain suchen	site:example.com
filetype:	Nach Dateitypen suchen	filetype:pdf
ext:	Alternative zu filetype:	ext:xls
inurl:	Begriff in URL suchen	inurl:admin
intitle:	Begriff im Seitentitel suchen	intitle:"index of"
intext:	Begriff im Seiteninhalt suchen	intext:"confidential"
allinurl:	Alle Begriffe in URL	allinurl:admin login
allintitle:	Alle Begriffe im Titel	allintitle:index of
allintext:	Alle Begriffe im Text	allintext:username password
cache:	Zeigt Googles Cache-Version	cache:example.com
related:	Ähnliche Seiten finden	related:example.com
link:	Zeigt Seiten, die verlinken (veraltet)	link:example.com
"..."	Exakte Wortgruppe suchen	"login password file"
-	Begriff ausschließen	login -facebook

theHarvester

OSINT-Tool zur Sammlung von Informationen wie E-Mail-Adressen, Subdomains und Usernames aus öffentlich zugänglichen Quellen (Suchmaschinen, Shodan, Hunter, etc.).

theHarvester -d [DOMAIN] -b [DATENQUELLE] [OPTIONEN]

Option	Bedeutung
-l	Limit der Suchergebnisse
-f	Speichert Ergebnis als HTML/XML-Datei
-v	Ausführliche Ausgabe (verbose)

NMAP

Befehl	Beschreibung
nmap -sn <IP/Netz>	Ping Sweep – Welche Hosts sind online? (ohne Portscan)
nmap -PR <IP/Netz>	ARP-Scan – Erkenne Geräte im lokalen Netzwerk (Layer 2)
nmap -sS <IP>	TCP SYN-Scan (Stealth) – Schneller & unauffälliger Portscan
nmap -sT <IP>	TCP Connect – Standard-Portscan (sichtbarer Verbindungsaufbau)
nmap -sU <IP>	UDP-Scan – Erkennt offene UDP-Ports (langsamer)
nmap -p 22,80,443 <IP>	Scan nur bestimmte Ports (hier: SSH, HTTP, HTTPS)
nmap -p- <IP>	Scan **alle** 65535 TCP-Ports
nmap -sV <IP>	Service-/Versionsscan – Welche Dienste & Versionen laufen?
nmap -O <IP>	Betriebssystemerkennung (OS-Fingerprint)
nmap -A <IP>	Aggressiv: Scan mit -sV, -O, Traceroute und mehr
nmap -T4 <IP>	Timing-Option für schnelleren Scan (Wert 0–5; 3 = Standard 4 = schnell, 5 = riskant)
nmap -Pn <IP>	Kein Ping vor dem Scan – nützlich bei Firewalls, die ICMP blocken
nmap -v <IP>	Mehr Details während des Scans (verbose mode)
nmap -oN scan.txt <IP>	Ausgabe in Datei speichern (normaler Text)
nmap -oX scan.xml <IP>	Ausgabe als XML (z.B. für Weiterverarbeitung)
nmap --top-ports 100 <IP>	Scan der 100 häufigsten Ports

NMAP in Metasploit

Befehl	Beschreibung
msfconsole	Startet Metasploit
workspace	Zeigt aktuelle Workspaces
workspace -a <name>	Neuen Workspace hinzufügen
workspace -d <name>	Workspace löschen
workspace -r <name>	Bestehenden Workspace umbenennen
workspace <name>	Zu einem Workspace wechseln
workspace -h	Hilfe zu Workspace-Befehlen anzeigen
hosts	Zeigt alle Hosts im aktuellen Workspace
services	Zeigt gefundene Dienste
db_nmap	Nmap Befehle wie gewohnt

Im Fall von: Database not connected

sudo service postgresql start

sudo msfdb init

Netexec – SMB-Recon

Vielseitiges Post-Exploitation-Tool zur automatisierten Netzwerkerkundung und Ausnutzung von Windows-Umgebungen.

Kategorie	Befehl	Beschreibung
Scan & Recon	netexec smb 192.168.56.0/24	SMB-Dienste im Subnetz erkennen
	netexec smb 192.168.56.101	Einzelnes Ziel prüfen
Authentifizierung	netexec smb <ip> -u "" -p ""	Null-Session (leerer Benutzer & Passwort) testen
	netexec smb <ip> -u user -p pass	Authentifizierung mit Benutzer & Passwort
	netexec smb <ip> -U users.txt -P passwords.txt	Bruteforce mit User- und Passwortlisten
Freigaben	netexec smb <ip> -u user -p pass --shares	SMB-Shares anzeigen
	netexec smb <ip> -u user -p pass --list	Dateien in allen erreichbaren Shares auflisten
	netexec smb <ip> -u user -p pass --list <share>	Dateien in bestimmtem Share anzeigen
Benutzerinfos	netexec smb <ip> -u user -p pass --users	Lokale Benutzer auflisten (wenn möglich)
	netexec smb <ip> -u user -p pass --groups	Lokale Gruppen auflisten
RCE / Admin	netexec smb <ip> -u admin -p pass --exec "whoami"	Remote-Befehl ausführen (wenn Admin-Rechte vorhanden)
Weitere Infos	netexec smb <ip> --pass-pol	Passwort-Richtlinie anzeigen
	netexec smb <ip> --sessions	Aktive SMB-Sessions anzeigen
	netexec smb <ip> --loggedon-users	Angemeldete Benutzer anzeigen (nur Windows + Admin)

SMB-Client

Kommandozeilenprogramm, das Zugriff auf freigegebene SMB/CIFS-Ressourcen (wie Windows-Shares) bietet, ähnlich wie ein FTP-Client

Kategorie	Befehl	Beschreibung
Dateien übertragen	smbclient //<ip>/<share> -N	Auf Share zugreifen ohne Passwort
	get <filename> (innerhalb smbclient)	Datei herunterladen

OpenVas (Vulnerability Scanner)

Freies (Community Edition), leistungsfähiges Framework zur automatisierten Sicherheitsprüfung und Schwachstellenanalyse von IT-Systemen.

Befehl	Beschreibung
sudo gvm-start	Startet den Scanner und Webinterface
https://localhost:9392	OpenVas aufrufen

Anmeldung: Anmeldedaten liegen als Datei auf dem Desktop

Workflow:

Ziel (Target) konfigurieren

Im Webinterface (GVM GUI):

1. **Configuration > Targets > New Target**
2. **Name**: z. B. „Target1“
3. **Hosts**: IP-Adresse oder Hostname (z. B. 192.168.1.10)
4. Portlist auswählen oder benutzerdefiniert
5. Speichern

Scan-Task erstellen und konfigurieren

1. **Scans > Tasks > New Task**
2. **Name**: z. B. „Scan1“
3. **Scan Config**: z. B. „Full and fast“
4. **Target**: Das eben erstellte Ziel auswählen
5. Speichern

Scan ausführen

1. Unter **Tasks** auf die play taste neben deinem Task klicken

Ergebnisse anzeigen

1. **Scans > Reports**
2. Bericht öffnen → zeigt Schwachstellen, CVSS-Bewertung, Hinweise zur Behebung
3. Optional: Filter nach Schweregrad, Hosts, CVE etc.

Burp Suite

Leistungsstarkes Werkzeug zur Sicherheitsanalyse von Webanwendungen – ideal für das Abfangen, Manipulieren und Testen von HTTP(S)-Verkehr.

Burp Suite starten

- Einfach die Burp Suite Community Edition starten.
- **Temporary Project** auswählen → **Start Burp**.

Vorgefertigten Burp-Browser nutzen

Klicke im Proxy-Tab > Open Browser

Ein Chromium-basierter, vorkonfigurierter Burp-Browser öffnet sich – alles, was du darin aufrufst, wird automatisch über den Burp-Proxy geleitet

Öffne die gewünschte Webseite (http://localhost:3000)

Proxy-Tab nutzen – Requests abfangen

- Gehe zu **Proxy > Intercept**.
- Stelle: **„Intercept is ON“**
- HTTP-Request vom Browser wird im Proxy abgefangen.
- **Send to Repeater** = zur manuellen Manipulation

Repeater-Tab – Manuelle Anfrage testen

- Gehe zu **Repeater-Tab**.
- Der Request von Proxy wird dort angezeigt.
- Du kannst:
    - **Header / Body** bearbeiten
    - Anfrage mit **„Send“** erneut senden
    - Antwort analysieren

Nikto

Open-Source-Webscanner, der bekannte Schwachstellen, veraltete Software, gefährliche Dateien, Konfigurationsprobleme und mehr aufdeckt.

nikto -h <Ziel>

Option	Beschreibung
-h	Zielhost (IP, Domain oder URL)
-p <Port>	Zielport (Standard: 80)
-Tuning <Codes>	Scan-Typen einschränken (s. unten)
-ssl	HTTPS erzwingen (auch: -443)

Code	Scan-Typ
0	Alle Scans (Standard)
1	Server-Fehlkonfiguration
2	Standard-Dateien
3	Sicherheitslücken (z. B. XSS)
4	Ausforschende Tests (z. B. Banner)
5	Fehlerhafte Programme
6	Admin-Seiten
7	Ausforschende Tests
8	Inhalt (z. B. Verzeichnisse)
9	Webserver-Spezifisch

Metasploit

Leistungsstarkes Framework zur Durchführung von Penetrationstests, mit dem Sicherheitslücken gesucht, ausgenutzt und dokumentiert werden können.

Grundlagen

Befehl	Beschreibung
msfconsole	**Starte Metasploit**
help	**Zeigt Hilfebefehle an**
exit	**Beende Metasploit**
back	**Zurück ins Hauptmenü**

Modul-Recherche & Auswahl

Befehl	Beschreibung
search <Stichwort>	**Suche nach Exploits, Payloads oder Aux-Modulen**
info <Modul>	**Zeigt Detailinfos zu einem Modul**
use <Modul>	**Modul auswählen (z. B. Exploit oder Auxiliary)**

Konfiguration von Ziel und Optionen

Befehl	Bedeutung (einfach erklärt)
set RHOSTS <Ziel-IP>	Wo das Zielsystem erreichbar ist
set LHOST <deine-IP>	Wohin sich das Ziel zurückmelden soll
set RPORT <Port>	Über welchen Dienst das Ziel angesprochen wird
set LPORT <Port>	Wo du auf die Rückverbindung wartest
set TARGETURI <Pfad>	Welcher genaue Ort in der Webanwendung angegriffen wird
show options	Zeigt alle benötigten und optionalen Einstellungen

Payload-Management

Befehl	Beschreibung
set PAYLOAD <Payload>	Payload setzen (z. B. reverse shell)
show payloads	Verfügbare Payloads anzeigen

Exploit-Ausführung & Zielprüfung

Befehl	Beschreibung
check	**Prüft, ob Ziel verwundbar ist**
exploit oder run	**Führt das Modul aus**

Session-Management

Befehl	Beschreibung
sessions	Zeigt aktive Sessions
sessions -i <ID>	Interaktion mit einer Session
background	Session in den Hintergrund
kill <ID>	Beendet eine Session