

Ablauf Pentest

1. Identifizieren von Zielen
2. Auffinden von Services bzw. offenen Ports
3. Identifizieren von vorhandenen Schwachstellen innerhalb des Services
4. Versuch erkannte Schwachstellen auszunutzen
5. Privilege Escalation (falls nötig)
6. Dokumentation

netdiscover

- Passive scanning ohne aktiven Eingriff in das Netzwerk
- <ip> Scan nach aktiven Hosts (beisp. 192.168.0.0/24, 192.168.0.1-255)
- i (Interface, beisp. eth0, wlan0...)

nmap

Scantypen

- sn Ping Scan
- sS Syn-Scan
- sT Connect Scan

Optionen

- i Interface (eth0, eth1, wlan0...)
- Pn Alle Hosts als online behandeln
- T <1-5> Geschwindigkeit bzw. Timeout

1 - lange Timeoutzeit

5 - kurze Timeoutzeit

Port

- p Portangabe (80,444 , 0-80)
- F Fastscan

Output

- oA Ausgabe in alle Formate
- oX XML Output
- oG "grep"barer Output
- oN Normaler Output

Metasploit

msfconsole

- search Suchen nach einer CVE Nummer
- show options Anzeigen der Einstellungen

use Auswählen eines Exploits exploit/..

run / exploit Ausführen der gewählten Aktionen

set ...

...PAYLOAD Auswahl der Payload

...RHOST Remote Host (target)

...LHOST Local Host (attacker)

...RPORT Remote Port (target)

...LPORT Local Port (attacker)



By **leostark**
cheatography.com/leostark/

Not published yet.
 Last updated 3rd June, 2019.
 Page 1 of 1.

Sponsored by **CrosswordCheats.com**
 Learn to solve cryptic crosswords!
<http://crosswordcheats.com>