Descobrindo Hashes

+ Aqui cabe verificar a diferença entre hashs ntlm e lm.
→ O lm só era usado até o Windows XP, e pode ser identificado pela presença de aad3b435b51404ee

+ Para quebrar a senha hash lm, devemos setar uma wordlist e usar o john

```
john --format-lm --wordlist=/usr/share/wordlists/rockyou.txt hashxp
```

→ se n passarmos a wordlist, ele usará a wordlist default
→ hashxp é o arquivo que contém o hash

+ Para quebrar senhas ntlm,

```
john --format-nt --wordlist=/usr/share/wordlists/rockyou.txt hash10
```