How to Use the NET Command on a Security Test (2)

We can use the net command to explore what files and folders are being from a target system. First let us check the DNS name of the target.

```
C:\> nslookup ws2003-01.dev.snowcapcyber.co.uk
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Name:        ws2003-01.dev.snowcapcyber.co.uk
Address:     172.16.2.100
```

First lets is look at all of the options that the **net use** command gives us.

```
C:\> net use /?
NET USE [devicename | *] [\\computername\sharename[\volume] [password | *]]
         [/USER:[domainname\]username]
         [/USER:[dotted domain name\]username]
         [/USER:[username@dotted domain name]
```

We begin by querying the target system to see what it is exporting. This command will either succeed or return an error message. In the following example, it will return an error message and I will demonstrate how to fix this problem.

```
C:\> net view \\172.16.2.100 /ALL
System error 53 has occurred

The network path was not found
```

We can fix this error via establishing an IPC null share with the target system, as follows. Please not that this is an anonymous share as you are providing no username and no password.

```
C:\> net use \\172.62.2.100\ipc$ “” /user:””

The command completed successfully.
```

So, we can now re-execute our initial query and we should see the list fi all folders shared on the network from the target machine. Please note that when specifying a target machine can make use of its IP address, or its Domain Name (FQDN) or its NetBIOS name.

```
C:\> net view \\ws2003-01.dev.snowcapcyber.co.uk /ALL
Shared resources on \\
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Data                 Disk     Data Folder
Presentations        Disk     Corporate Presentations
```

If you have sufficient domain/local privileges, then you can access the share as follows, and you will be able to specify the mount point were the disk/folder will be mounted on the local system

```
C:\> net use z: \\172.16.2.100\Presentations
The command completed successfully.
```

If not, then you will be required to provide a username and as password as follows.

```
C:\> net use z: \\172.16.2.100\Presentations “MyPa55w0rd” /user:”Andrew Blyth”

The command completed successfully.
```

You can also a access provide a username as password via interacting with the command line command as follows:

```
C:\> net use z: \\172.16.2.100\Presentations
Enter the username for ‘172.16.2.100’: administrator@dev.snowcapcyber.co.uk
Enter the password for ‘172.16.2.100’’: **********

The command completed successfully.
```

We can then see what we have successfully mount and where via the “**net use**” command.

```
C:\> net use z: \\172.16.2.100
Status          Local       Remote                   Networks
-------------------------------------------------------------------------------
OK              Z:          \\172.16.2.100\Data      Microsoft Windows Network
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
```

You can also delete shares that are mounted. So, in the following we are deleting a share that is mounted as disk **Z:** using the “**net use Z: /delete**” command.