How to Use the NET Command on a Security Test (1)

To find out who you are on a Microsoft Windows machine you can use the following commands: **whoami**, or **query user** at the command line. The Microsoft Windows **net** command is a powerful post exploitation tools that allows us to perform a wide variety of functions. Using the **net** command, we can enumerate local users as follows:

```
C:\> net user
User Accounts for \\TRAININGWKSTN01
-------------------------------------------------------------------------------
Administrator        Andrew Blyth          Arthur Pendragon        Iain Sutherland
```

In the above we can see a number of local accounts on the target machine. If the machine is part of a domain then we can use the net command to query the users in that domain via the following.

```
C:\> net user /domain
User Accounts for \\TRAININGWKSTN01
-------------------------------------------------------------------------------
Administrator        Andrew Blyth          Campbell Murray.        Huw Read
```

The above lists the users that exist with the domain and thus these users can log onto any computer within that domain. We can tell what domain computer is in via the following command.

```
C:\> systeminfo | findstr /B "Domain"
Domain:                 training.merimetso.net
```

The above command new tells us that the computer system that is giving is a command prompt is part of the domain `training.merimetso.net`. If you want to find the list of local groups on the machine, then you can use the following command:

```
C:\> net localgroup
```

Once we have identified the lists of local groups then we query the local group to identify all users in the group

```
C:\> net localgroup Administrators
```

If we are on a domain controller (DC) then we can use the following command to list the groups

```
C:\> net group
User Accounts for \\TRAININGWKSTN01
-------------------------------------------------------------------------------
* Domain Admins
```

In the above we can see all of the groups that exist on the domain controller. We can also use the net command to identify all of the users within a specific group via the following command. In the following command we can see that three users are part of the **Domain Admins** group.

```
C:\> net group "Domain Admins"
Group Name.          Domain Admins
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Administrator                      Andrew Blyth.                    Huw Read
```

We can find out information about a specific user and what groups they are a member of using the following command. If you run the following command on a None domain controller then it will just list the local groups that you are a member of and for the global groups, it will display "***None**".

```
C:\> net user "Andrew Blyth"
. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .
Local Group Membership       *Administrators         *Users
Global Group Membership      *Domain Admins          *Domain Users       *Users
```

We can use the net command to change a user password if we have sufficient privileges via the following command. The ability to reset password and add users to groups is dependent on the set of privileges that we have. We can identify the privileges that we have via the "**whoami /priv**" command

```
C:\> net user "Andrew Blyth" "MyN3wPa55w0rd"
```

We can also add a user to a local group via the following command.

```
C:\> net localgroup Administrators "Andrew Blyth" /add
```

To add a user to a domain group then we can use the following command. But to execute this command you must be on a domain controller.

```
C:\> net group "Domain Admins" "Andrew Blyth" /add
```

All of the above command allow is to profile a system and escalate privileges where possible