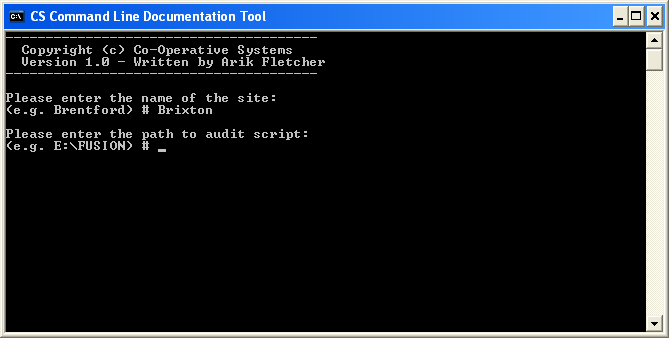
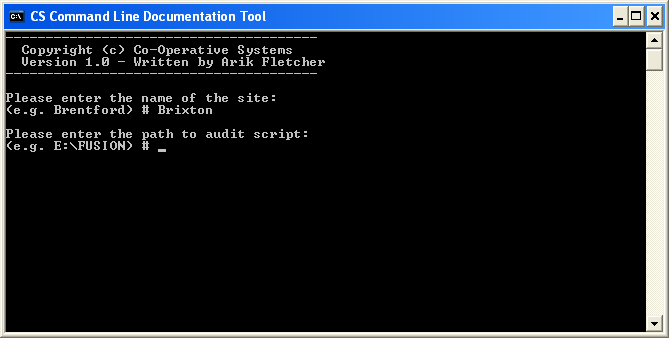
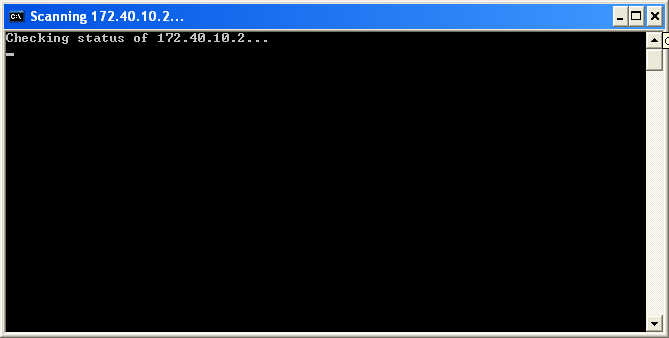
***NB: This tool will only work on networks that have all firewalls disabled; or have firewalls that permit remote File and Print sharing access and remote WMI access.***

1. Ensure that all PCs are switched on and are connected to the network.
2. Log into a networked **client PC** with **domain admin rights**
3. Extract the audit tool to a folder on the **local drive** (or a **USB drive**)-   
   this will consists of **1 folder and 2 files**:

|  |  |  |
| --- | --- | --- |
|  |  |  |
| ***VBS backend files*** | ***Audit frontend script*** | ***This readme file*** |

1. Once you have extracted the files, double click on the **audit.cmd** script file
2. Enter the name of the site you are auditing- e.g. **Brixton**:  
   *(Avoid spaces and special characters- i.e.* ***CentralLondon*** *instead of* ***Central London****)*  
     
   
3. Enter the full path to where you extracted theauditfiles- e.g. **C:\Audit***(Avoid spaces and special characters- quit and rename the folder if you’ve used any)*  
     
   
4. At this stage the tool will determine what the current IP range is and begin scanning each IP address within the range for active computers-   
     
   
5. As active hosts are identified the tool will create an XML document in the extracted tool folder under a site-named subfolder- e.g. **C:\Audit\Brixton**
6. Once the tool and all the documents have been created; zip up the audit folder and add it to your site report.