Breakout 1 and Unix 1 Solution

Breakout 1

Notepad shortcut on the desktop when you RDP into the system. Open this up and type in the following into it and save it as a ".bat" file.

```
ftp.exe
```

Execute the created file - you can run system commands by appending "!" in front of a command.

1. Asked to read a specific registry key value, this can be done using the ftp.exe binary opened using reg query command.

```
!reg query <registry key>
!reg query HKEY_CLASSES_ROOT\exefile\shell\open\command
!reg query HKCR\exefile\shell\open\command
```

2. Tells you about a service running that is running as an admin user which can be exploited to open the final trophy file. It first asks you the username of the account running the service. Number of ways to do this (wmic, net services etc) however the easiest is to run Task Manager from the ftp.exe binary we already have open.

```
!taskmgr.exe

When it opens review the running processes and you can see the user its running as
(backum<random-numbers>).
```

3. The backup agent is running in the bottom right taskbar. You can right click then open the Help option, which loads Notepad under the backup user account. You can the go File -> Open to open the trophy file.

Unix 1

Serviceman

1. Entry point is an XDMCP service running on UDP port 177. Note there are no other services accessible remotely so this is the only service you will see open.
2. Need to connect and get a trophy file from a banner with a user list:

```
Xephyr -query 10.10.10.10 -screen 800x600 :1
OR
MobaXterm
```

3. This will disclose a list of username on the system. One of the users passwords is trivial i.e. username as password or "password". Believed that the last user is the way in.
4. And the other one had Apache running under sudo, so you can do 'httpd –f /etc/shadow –t' and get it to read shadow as a configuration file which spits out the top line.

```
httpd –f /etc/shadow –t
```

Or Nessus will get you screenshot.
+ brute force users, last user permitted access with the same password as username.