Blue Team Cheat Sheet

**Connecting to Servers**

Use the following command to access Linux servers through a GUI interface:  
rdesktop -g 1280x1024 -u [user] [ip]  
For Windows servers use:  
xfreerdp /u:[user] /v:[ip] /size:1280x1024 /cert:ignore

**CySec Servers on the Network**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Purpose | IP | Open Ports | Running Services |
| Webserver | Holds the webpage for the CySec company that customers use to log in |  |  |  |
| Database Server | Maintains the user login DB for the webserver, and the confidential customer data from CySec customers |  |  |  |
| Domain Controller | Runs the LDAP used for Windows authentication, and controls DNS (not really) |  |  |  |
| Fileserver | Houses the CySec company share and vital worker data that is used daily |  |  |  |
| Elastic Server | Analysis server capturing all network traffic and funneling it to Elastic |  |  |  |

**Credential Information**

ALL ACCOUNTS WITH 'GOLD' IN THEM ARE OUT OF SCOPE! DO NOT EDIT THEM OR DELETE THEM. DO NOT CREATE FAKE GOLD ACCOUNTS.

* username: gold1 password: 135thCSC\_gold  
  username: gold2 password: 135thCSC\_gold

**Known CySec login credentials:**

* administrator (Administrator | 135thCSC\_defaultadmin) (DOMAIN CONTROLLER)
* Enterprise Admin (enteradmin | 135thCSC\_enter) (FILESERVER, WEBSERVER, DATABASESERVER)
* Domain Admin (domadmin | 135thCSC\_dom) (FILESERVER, DATABASESERVER, DOMAIN CONTROLLER)
* Security Admin (secadmin | 135thCSC\_sec) (ELASTIC SERVER)
* Joe Glow (jglow | 135thCSC\_glow)
* Kim Early (kearly | 135thCSC\_early)