Red Team Cheat Sheet

**Red Team Resources**

Beacons and other scripts are located on the Desktop of your jumpboxes.

**Beacon Notes**

* Remember to edit your beacon scripts with your jumpboxes' IP address.
* Remember to start your beacon receiving server. Navigate to the beacon folder on your desktop in the terminal. Run the command: >flask run <

**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 | 172.31.135.8 | 80 | Apache 2 |
| Database Server | Maintains the user login DB for the webserver, and the confidential customer data from CySec customers | 172.31.135.4 | 3306 | MySQL |
| Domain Controller | Runs the LDAP used for Windows authentication, and controls DNS (not really) | 172.31.135.3 | 3389, 53 | LDAP, DNS |
| Fileserver | Houses the CySec company share and vital worker data that is used daily | 172.31.135.5 | 139 | smbd |
| Elastic Server | Analysis server capturing all network traffic and funneling it to Elastic | 172.31.135.6 | 9200, 5601 | Elastic, Kibana |

**Known Compromises**

* Database Server: Weak authentication setup for MySQL. Default passwords have not been changed.
* Webserver: If logged into the website with an admin account, SQL injection can be used to grab all the login data.
* Domain Controller: Poor GPO setup, allowing non-domain users to create and edit users.
* Fileserver: Poor authentication setup. The smbd service is open to guest and can be mounted and edited from any machine.

**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)