# Project C – Ethical Hacking

By: Malcolm Brown

# Executive Summary

- Install a network upgrade for the client.
- Determine the vulnerabilities on the server.
- Exploit the vulnerabilities.

# Production Server Vulnerabilities

- There are several vulnerabilities on the production server.
- To name a few; vsFTPd version 2.3.4 backdoor, SSL/TLS MITM vulnerability (CCS Injection), and Port 23 or telnet.

# Production Server Exploits

- Port 21 is the control port for FTP; information is sent using cleartext making it easy to exploit.
- Port 1099/Java RMI is a mechanism that allows an object that exists in one Java virtual machine to access and call methods that are contained in another Java virtual machine

# Webserver Vulnerabilities

- While checking the webserver for vulnerabilities I discovered quite a few but just to name some.
- Port 80
- Port 5432
- Port 139

# Webserver Exploits

- Port 5432/PostGres is an open source database which can be found mostly in Linux operating systems.
- Port 139 or NetBIOS is a protocol used for file and print sharing under all current versions of Windows

# Recommendations

- Use File Transfer Protocol Secure (FTPS)
- Upgrade and update software regularly
- Maintain a Secure Firewall
- Use Private Networks and VPNs

Appreciate your time

Any Questions