# Executive Summary

The purpose of this vulnerability scan is to gather data on Windows and Linux Operating systems, as well as user accounts in the **“ClientDomains”** domain in the 10.10.1.1/24 subnet. Of the hosts identified, 30 user accounts and 30 systems were found to be active and were scanned.

# Scan Results

Results from the raw scan will be provided upon delivery.

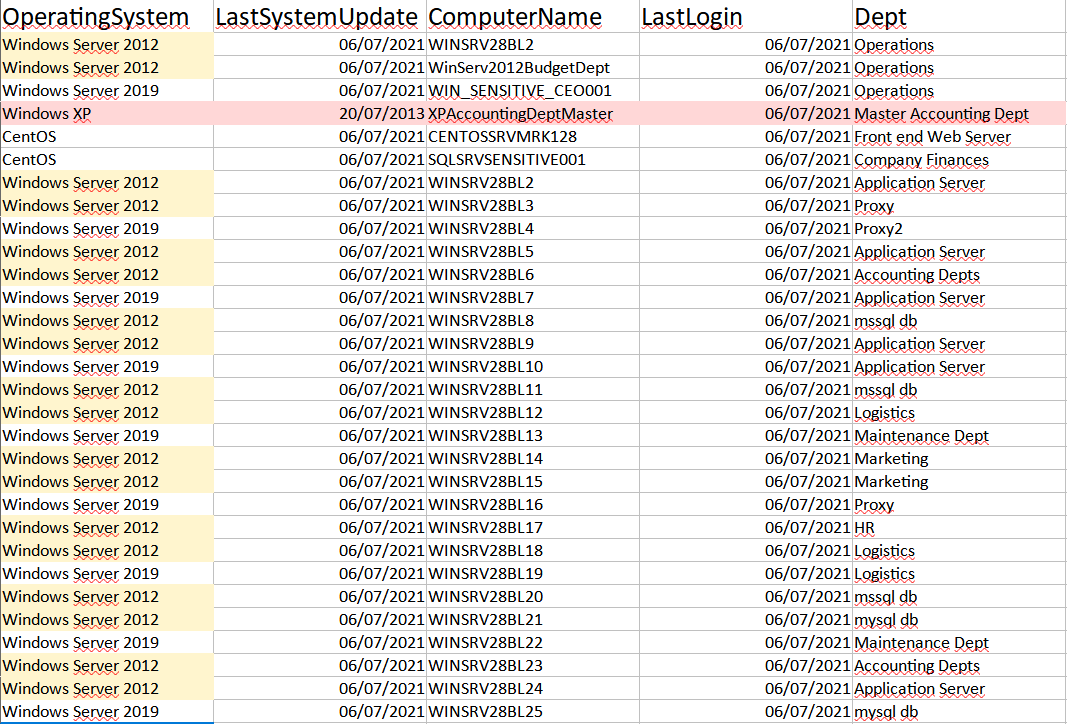
# Findings (2-3 sentences)

Accounts  
There are 10 not-compliant accounts. Furthermore, after reviewing departments and permissions, it should be noted that user Ted L White works in the Marketing Department, but holds permissions for Executives, Admins, and Domain Admins Group.  
Finally, there are three accounts that have not had a password change since 2009.

Systems  
Server “XPAccountingDeptMaster” has not been updated since 2013.

Remediation (2-3 sentences)  
The remediation section should include the following key terms highlighted below.  
Accounts  
It is recommended to rotate passwords for the ALL users. Doing so will put the organization at 100% compliant with password policy. In addition, Ted White’s permissions should be reviewed for accuracy.  
Systems  
Server “XPAccountingDeptMaster” is running on an obsolete operating system, putting the  
organization at high risk. Recommend migrating to an up-to-date server and discontinue server  
“XPAccountingDeptMaster”. ]

We recommend upgrading all the 18 systems running Windows Server 2012 to a newer version such as Windows Server 2019]



The red highlighted line is the non compliant. The yellow ones are the old versions of windows server.