Are those things exploitable?

CSC 3: Continuous Vulnerability Management

Continuous Vulnerability Management **Continuously acquire, assess, and take action on new information in order to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.**	
Run Automated Vulnerability Scanning Tools	Utilize an up-to-date Security Content Automation Protocol (SCAP) compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.
Perform Authenticated Vulnerability Scanning	Perform authenticated vulnerability scanning with agents running locally on each system or with remote scanners that are configured with elevated rights on the system being tested.
Protect Dedicated Assessment Accounts	Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses.
Deploy Automated Operating System Patch Management Tools	Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.
Deploy Automated Software Patch Management Tools	Deploy automated software update tools in order to ensure that third-party software on all systems is running the most recent security updates provided by the software vendor.
Compare Back-to-Back Vulnerability Scans	Regularly compare the results from consecutive vulnerability scans to verify that vulnerabilities have been remediated in a timely manner.
Utilize a Risk-Rating Process	Utilize a risk-rating process to prioritize the remediation of discovered vulnerabilities.

http://www.cisecurity.org/controls/

Who *really* needs admin rights?

CSC 4: Controlled Use of Administrative Privileges

Controlled Use of Administrative Privileges **The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.**	
Maintain Inventory of Administrative Accounts	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.
Change Default Passwords	Before deploying any new asset, change all default passwords to have values consistent with administrative level accounts.
Ensure the Use of Dedicated Administrative Accounts	Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.
Use Unique Passwords	Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.
Use Multi-Factor Authentication for All Administrative Access	Use multi-factor authentication and encrypted channels for all administrative account access.
Use Dedicated Workstations For All	Ensure administrators use a dedicated machine for all administrative tasks or tasks requiring administrative access. This machine will be segmented from the organization's primary network and not be allowed Internet access. This machine will not be used for reading e-mail, composing documents, or browsing the Internet.
Limit Access to Script Tools	**Limit access to scripting tools (such as Microsoft® PowerShell and Python) to only administrative or development users with the need to access those capabilities.**
Log and Alert on Unsuccessful Administrative Account Login	Configure systems to issue a log entry and alert on unsuccessful logins to an administrative account.

http://www.cisecurity.org/controls/