

CIP-005-1 Electronic Security Perimeter(s)

R2 Electronic Access Controls

R2.1 Access Control

R2.1.1 Access This Computer from the Network

This test determines if the SeNetworkLogonRight right is assigned to Administrators, Authenticated Users, and Enterprise Domain Controller accounts. This right gives users the ability to access resources on the Windows system from anywhere on the system's network.

Passed

100 %

List contained the required items: BUILTIN\Administrators, BUILTIN\Users. Full list on this machine: Everyone, BUILTIN\Administrators, BUILTIN\Users, BUILTIN\Backup Operators

R2.1.2 Act as Part of the Operating System

This test determines whether the list of users or groups permitted to 'Act as Part of the Operating System' is empty. This setting ensures that users are restricted only to those permissions explicitly set forth in their roles (i.e. avoids veiled privilege elevation).

Passed

100 %

List contained the required items: . Full list on this machine:

R2.1.3 Allow Log on Locally

This test verifies that only authorized users can log on at the console of the system. This configuration helps to prevent unauthorized users from accessing the system from the console.

Failed

0 %

Items shouldn't be present: Guest, BUILTIN\Users

List should only contain: BUILTIN\Administrators, BUILTIN\Backup Operators, but actually contained: Guest, BUILTIN\Administrators, BUILTIN\Users, BUILTIN\Backup Operators

R2.2 Ports and Services

R2.2.1 HTTP SSL Disabled

This test determines if the HTTP SSL Service is disabled on a Windows system. This service enables Secure Socket Layer (SSL) encryption of the HTTP protocol via Internet Information Services (IIS). Disabling unnecessary services running on a system is a security best practice that helps limit avenues of attack.

Passed

100 %

