


# Limit access to Script Tools

## CSC 4: Controlled Use of Administrative Privileges

Binary	Functions	Type
<a href="#">Atbroker.exe</a>	Execute	Binaries
<a href="#">Bash.exe</a>	Execute AWL bypass	Binaries
<a href="#">Bitsadmin.exe</a>	Alternate data streams Download Copy Execute	Binaries
<a href="#">Certutil.exe</a>	Download Alternate data streams Encode Decode	Binaries
<a href="#">Cmd.exe</a>	Alternate data streams	Binaries
<a href="#">Cmdkey.exe</a>	Credentials	Binaries
<a href="#">Cmstp.exe</a>	Execute AWL bypass	Binaries
<a href="#">Control.exe</a>	Alternate data streams	Binaries
<a href="#">Csc.exe</a>	Compile	Binaries
<a href="#">Cscript.exe</a>	Alternate data streams	Binaries
<a href="#">Dfsvc.exe</a>	AWL bypass	Binaries
<a href="#">Diskshadow.exe</a>	Dump Execute	Binaries
<a href="#">Dnscmd.exe</a>	Execute	Binaries



Credit to LOLBAS Living Off The Land Binaries And Scripts - (LOLBins and LOLScripts)

# How is this thing configured?

## CSC 5: Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

### Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers

**Establish, implement, and actively manage (track, report on, correct) the security configuration of mobile devices, laptops, servers, and workstations using a rigorous configuration management and change control process in order to prevent attackers from exploiting vulnerable services and settings.**

Establish Secure Configurations	Maintain documented security configuration standards for all authorized operating systems and software.
Maintain Secure Images	Maintain secure images or templates for all systems in the enterprise based on the organization's approved configuration standards. Any new system deployment or existing system that becomes compromised should be imaged using one of those images or templates.
Securely Store Master Images	Store the master images and templates on securely configured servers, validated with integrity monitoring tools, to ensure that only authorized changes to the images are possible.
Deploy System Configuration Management Tools	Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.
Implement Automated Configuration Monitoring Systems	Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.

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