

## Privileged Command Management Module

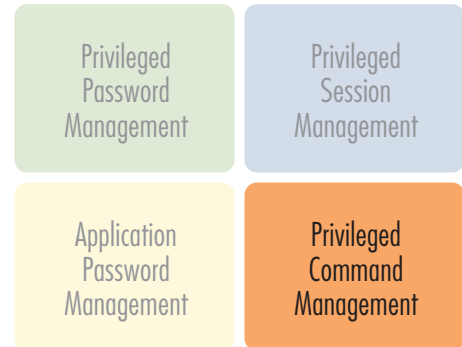
**e-DMZ Security's Privileged Command Management (PCM),** part of the TPAM Suite of privileged user and access control solutions, provides secure delegated administrative privileges across both Unix/Linux and Windows hosts. With PCM, daily administrative tasks such as performing system back-ups, managing system resources, users or access to programs can be delegated to specific authorized users and controlled to the specific command or program they are granted access.

As companies continue to streamline operations, they are forced to do more with less internal resources and/or look towards outsourcing as a cost-effective augmentation to limited and strained internal resources. For these reasons and more, demand to provide delegated privilege access continues to grow.

**Superuser Privilege Delegation:** Control the task or program environment privileged users have access to on a session by session basis. Across both Unix/Linux and Windows target hosts, with PCM you can grant users access to administrative accounts (root, administrator) or elevated privilege accounts and limit the task or program environment they can execute from that account. PCM dynamically establishes command specific sessions to back-end hosts. Once the user exits or otherwise leaves the authorized command/task/program, they are automatically logged out and the session is terminated.

**Proxy & Record Access:** PCM works through the TPAM Privileged Session Management (PSM) module to provide full session proxy, session recording and DVR-style session playback. With no direct access, your hosts are protected from local viruses or other concerns. Session recording provides an unmatched security and compliance audit. *See PCM brochure for more details.*

**Auto-Login:** Working in conjunction with PSM, command limited sessions can be configured for either interactive or automatic login. Auto-login enhances security and compliance by never exposing the account credential to the user. Optional full password management, including change controls, can be added via the Privileged Password Management (PPM) module. *See PPM brochure for more details*



### PCM Highlights:

- Delegated Privileged Access
- Limit Unix and Windows tasks/commands
- Limit Script/program access
- Session Proxy
- Auto-login
- Session recording, archive and replay<sup>1</sup>
- Optional full password management and control<sup>2</sup>

<sup>1</sup> Provided through PSM module as a prerequisite for PCM    <sup>2</sup> Provided with the addition of PPM module.

## Simple Command Creation

Through the Privileged Command interface, you can easily add the Unix/Linux or Windows commands that you would like to limit user access. These can be simple commands, scripts or program executables.

## Command Limited Access

Once commands are created, they are simply associated with the system/account from which the command will be executed. By granting users session request authorization to the system/account/command, the user session will be limited to the specific execution environment dictated by the command.

In the example screen shot, an authorized user session is limited to the Windows task manager. They are granted access to the back-end Windows resource, but their execution environment is limited to task manager functions. They have no START menu or other access beyond task manager. Once they exit the task manager environment, the session is immediately terminated.

## Full Session Recording and Archive

The PCM module works in conjunction with the privileged session management module, all the audit and session control features of PSM are available to command limited sessions. These include auto-login (no password exposure) and full session recording, archive and DVR-like playback.

### Privileged Command Management Tool

Select a Command to manage.

Command	Command Text	Description
WinPerfMon	mmc perfmon.msc /s	Windows performance monitor example
Windows Task Manager	taskmgr.exe	Windows Task Manager example
top	top -d 2	top command example
Password Change Menu	<pre>while [ 1 -eq 1 ]; do clear; echo '=PSW Menu='; echo 'Enter user or X'; read a; if [ \$a == "X" ]; then exit 0; else /bin/grep -w \$a /etc/passwd &gt;/dev/null; if [ \$? -ne 0 ]; then echo \$a 'does not exist'; else sudo /usr/bin/passwd \$a; fi; sleep 2; done</pre>	Menu for changing passwords on Unix
Menu Example	<pre>while [ 1 -eq 1 ]; do clear; echo '===='; echo '1. top'; echo '2. ls'; echo '3. exit'; echo '===='; read a; case \$a in (1) /usr/bin/top -d 2; continue;; (2) /bin/ls; read any; continue;; (3) clear; break; continue;; esac; done</pre>	Simple menu example
Computer Management	mmc compmgmt.msc /s	Computer Management Console example

### EGP Session

