1000 - Get-$pwnd: Attacking Battle-Hardened Windows Server

Saturday at 10:00 in Track 3
20 minutes | Demo, Tool
Lee Holmes*Principal Security Architect, Microsoft*

Windows Server has introduced major advances in remote management hardening in recent years through
PowerShell Just Enough Administration ("JEA"). When set up correctly, hardened JEA endpoints can provide
a formidable barrier for attackers: whitelisted commands, with no administrative access to the underlying
operating system.

In this presentation, watch as we show how to systematically destroy these hardened endpoints by exploiting
insecure coding practices and administrative complexity.
Lee Holmes
Lee Holmes is the lead security architect of Microsoft's Azure Management group, covering Azure Stack,
System Center, and Operations Management Suite. He is author of the Windows PowerShell Cookbook,
and an original member of the PowerShell development team.

#defcon25/by_track/track3/saturday #defcon25/By_Day/_saturday