

MSP Vendor PCI Compliance Feedback

Tenable Network Security, Inc

Background

- Ron Gula, CTO & Co-Founder Tenable Network Security
- Nessus is used by many MSPs for their remote/internal scanning including PCI scanning
- Informally polled a variety of ASVs and QSVs that use Nessus

Switching from v1 to v2

- Simply by re-scanning a system, customers get different results
 - Sometimes better
 - Sometimes worse
- Some MSPs did a cold switch, others gave preview scans, .etc
- Nessus uses CVSSv2 from NIST which accounts for Denial of Service whereas PCI vendors try to automate that out.

“Secret” Vulnerabilities and Targets

- Many MSPs going through certification are frustrated with the testing methodology.
- When something is missed, the diagnostics of figuring out if it was your scanner, your network, or even the targets can be difficult.
- Compare this to something like the SANS Top 20, DOD’s IAVA program or NIST SCAP guides where the list is openly publicized within a community.

ASVs not doing Patch Auditing

- There is a general feeling that the more you test, the more you find which increases support costs.
- Many merchants use XP or devices that there are no readily non-agent methods to assess the security off