

Engagement Results Charts

To help Demo Client understand the severity of the threats identified during testing, vPenTest Partner has included an over-all summary chart below that displays a comparison of the report findings as well as the vulnerabilities that were discovered.

Internal Network Security Assessment Results

PenTest Findings

The following chart displays the overall severity of the report findings that were documented as part of the penetration testing efforts.



As part of the penetration test, vPenTest Partner also performed a vulnerability assessment to provide additional value and insight as to the vulnerabilities that were identified by our vulnerability scanner. This vulnerability scan included the discovery of common security vulnerabilities that are publicly documented with Common Vulnerabilities and Exposures (CVE) scores.

VULNERABILITY ASSESSMENT FINDINGS

129 TOTAL



Discovered Threats

DISCOVERED THREATS	THREAT SEVERITY RANKINGS	
Internal Network Security Assessment (12)		
IPv6 DNS Spoofing		Critical
Link-Local Multicast Name Resolution (LLMNR) Spoofing		Critical
Outdated Microsoft Windows Systems		Critical
Password Document Stored in Network Share		High
Anonymous FTP Enabled		Medium
Insecure Protocol - FTP		Medium
Insecure Protocol - Telnet		Medium
LDAP Permits Anonymous Bind Access		Medium