TRIPWIRE® SECURESCAN

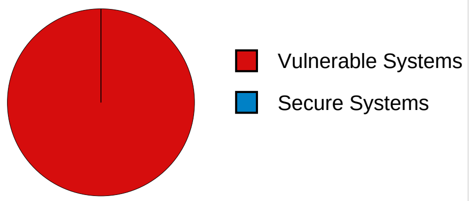
Company: VSE International
Contact: VSE International

Informational Report

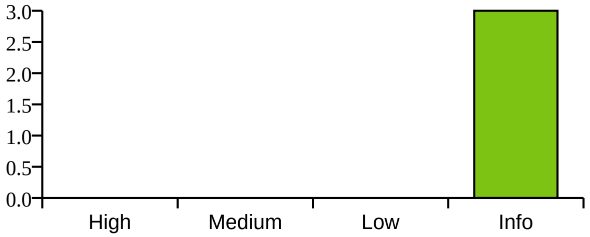
Assessment Summary

- Devices Discovered: **1**
- Devices with Vulnerabilities: **1**
- Total Items Detected: **3**
- Patch Priority Vulnerabilities: **0**
- Date scan completed: **2015-04-19**

Vulnerabilities by System

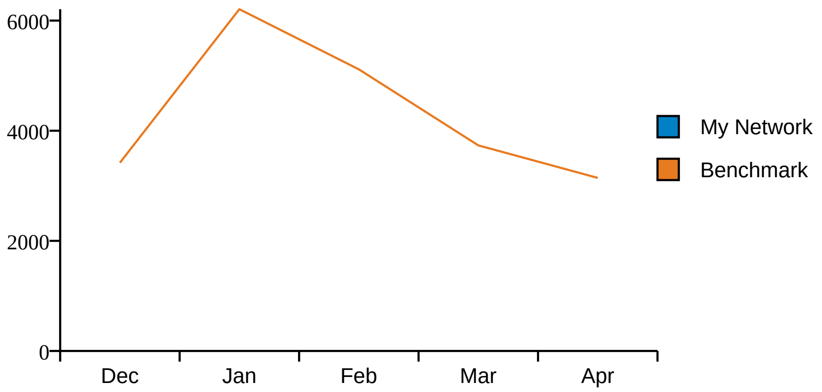


Vulnerabilities by Severity



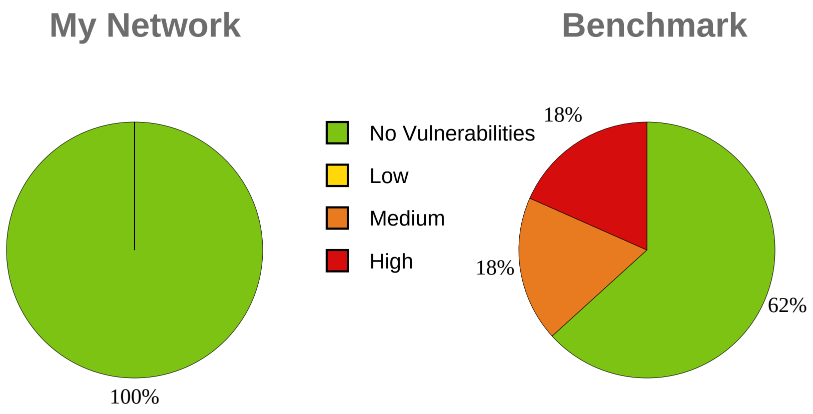
Benchmarks

Average Risk Score



This scorecard shows average risk score for all hosts in my environment, compared with the Tripwire Benchmark. The higher the value, the greater the risk.

Systems by Vulnerability Severity



Systems by Vulnerability Severity counts the percentage of systems with one or more vulnerabilities detected, by severity level.

Top Vulnerabilities

These are the top vulnerabilities on your network, ranked by aggregate risk.

Rank	Vulnerability Information
1	NetBIOS Name Table: Details Affected Systems: TOMAS-PC
2	HTTP Available: Details Affected Systems: TOMAS-PC
3	IP Addresses Enumerated Via NetBIOS: Details Affected Systems: TOMAS-PC

Solution Details

192.168.0.103 TOMAS-PC Windows 5.x

Risk Score: 0 Items Detected: 3 Patch Priority: 0 Low Confidence: 0 Informational: 3

Credentials Not Provided

Solution Details for TOMAS-PC (192.168.0.103) Windows 5.x:

Severity	Vulnerability	Ports	Score	Impact	Solution
INFO	IP Addresses Enumerated Via NetBIOS (Tripwire ID: 28951)	UDP/137	0	An attacker might learn about your computer and network to help with a future attack.	Restrict access within a broadcast domain to trusted hosts only.
INFO	HTTP Available (Tripwire ID: 1343)	TCP/2869	0	An attacker might learn about your computer and network to help with a future attack.	HTTP should be disabled if it is not necessary for the planned operations of the server.
INFO	NetBIOS Name Table (Tripwire ID: 552)	UDP/137	0	An attacker might learn about your computer and network to help with a future attack.	System administrators should prevent remote users from accessing the NetBIOS Name Table. This can be accomplished by implementing packet filters on UDP port 137.

Application Details for TOMAS-PC (192.168.0.103) Windows 5.x:

Name	Description	Port
IPv4 Layer 4	Generic Layer 3 / Layer 4 RAW socket access.	IP
VMware Authentication Daemon	The VMware Authentication Daemon authenticates remote users who connect to a server using the VMware Management Interface or the VMware Remote Console.	TCP/902
Windows UPnP	Windows UPnP	UDP/1900
UPnP Discovered Application	UPnP Discovered Application	UDP/1900
Windows NetBIOS Name Service	Windows NetBIOS-NS daemon.	UDP/137
HTTP-Based Application	A web-based application or web-application development software.	TCP/2869
UPnP HTTP	UPnP HTTP daemon.	TCP/2869

Appendices

Host Configuration Data for TOMAS-PC (192.168.0.103) Windows 5.x:

Name: Nmap OS String
Source: TCP

Name: UPnP Server Banner
Source: UDP

Port 1900: Microsoft-Windows-NT/5.1 UPnP/1.0 UPnP-Device-Host/1.0

Name: WDRT_Access
Source: TCP

WDRT_SMB_AUTH_SUCCESS : False, WDRT_SMB_REGISTRY_ACCESS : False, WDRT_SMB_FILE_ACCESS : False, WDRT_RPC_AUTH_SUCCESS : False, WDRT_WMI_AUTH_SUCCESS : False, WDRT_HOST_IS_64BIT : False,

Name: IP Addresses via NETBIOS
Source: UDP

192.168.110.1\\, 192.168.237.1\\, 192.168.0.103\\, 169.254.1.1

Name: MAC Address
Source: UDP

e8:de:27:10:72:5e

Name: NetBIOS Group Name
Source: UDP

WORKGROUP

Name: NetBIOS Hostname
Source: UDP

TOMAS-PC

Vulnerability Instance Data for TOMAS-PC (192.168.0.103) Windows 5.x:

No items to report