



# Corporate Policy Requirements

VULNERABILITY MANAGEMENT

# Corporate Policy Requirements

- Laws and regulations that require vulnerability management programs (like PCI DSS, and FISMA) don't apply to all companies
- But...vulnerability management is still very important to them as a key component to security
- Therefore...organizations can (and do) require scanning under their own corporate policies



# Scan Targets

- What systems do you want to be covered by your scans?
- Do you scan all systems or just *critical* assets?
- Scanning tools like *QualysGuard* can be used to build your asset inventory automatically
- Admins then take that information and classify the systems as critical or non-critical



# QualysGuard Vulnerability Scanner

QualysGuard® Vulnerability Management - Dashboard

https://qualysguard.qualys.com/

John Doe (jdoe\_un) | Log Out

## QUALYSGUARD® VULNERABILITY MANAGEMENT

New ▾ Search View ▾ Setup ▾ Help ▾

**Navigation**

- Dashboard
- Map
- Scan
- Schedule
- Report
- Exceptions
- Remediation
- Asset Search
- Risk Analysis

**Tools**

- Asset Groups
- Report Templates
- User Accounts
- Option Profiles
- Scanner Appliances
- Host Assets
- Domain Assets
- Remediation Policy
- Authentication
- Business Units
- Virtual Hosts
- KnowledgeBase
- Policies
- Controls
- Activity Log

**Dashboard**

**Vulnerabilities by Severity Level**

Severity Level	Count	Notes
100 Serverity 1	+9	
84 Serverity 2	+7	
73 Serverity 3	+10	
31 Serverity 4	+4	
10 Serverity 5	+4	
Total	298	+34

**Vulnerabilities by Status**

Status	Percentage
Active	46%
Re-opened	5%
Fixed	10%
New	34%

**Open Tickets by Severity Level**

Severity Level	Count	Notes
Active	298	
Fixed	86	
Re-Opened	18	
Total	436	

**Top 10 Tickets**

Ticket #	Hostname	IP Address	Due Date	Owner
00023	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
00101	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
00115	fridge.qa.qualys.com	10.10.10.1	12/13/2004	Charlie Patton (quays_cp)
00234	freezer.qa.qualys.com	10.10.10.2	12/15/2004	Willie Brown (quays_wb)
00098	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (quays_sh)
00103	icebox.qa.qualys.com	10.10.10.23	12/15/2004	Son House (quays_sh)
00222	freezer.qa.qualys.com	10.10.10.2	12/16/2004	Willie Brown (quays_wb)
00200	dairy.qa.qualys.com	10.10.1.54	12/16/2004	Robert Johnson (quays_rj)
00212	fridge.qa.qualys.com	10.10.10.1	12/16/2004	Charlie Patton (quays_cp)
00010	icebox.qa.qualys.com	10.10.10.23	12/20/2004	Son House (quays_sh)

**Qualys Top 10 Vulnerabilities**

QID	Hostname
124895	Microsoft Phone Book Service Buffer Overflow Vulnerability
254780	Microsoft Windock Weak Mutex Permission Vulnerability
431289	Microsoft NTLMSSP Code Execution Vulnerability
457890	Microsoft WebDAV Service Provider Scripts Levy Vulnerability
053422	'ResetBrowser Frame' and 'HostAnnouncement Frame'
725403	Microsoft Multipli LPC and LPC Ports Vulnerabilities
223495	Remote Registry Access Authentication Vulnerability
257348	Microsoft Recycle Bin Creation Vulnerability
562344	Microsoft RDISK Registry Enumeration Vulnerability
345809	Microsoft Malformed RTF Control Word Vulnerability

**Most Vulnerable Hosts**

DNS Hostname	NetBIOS Hostname	IP Address	Asset Group	Last Scan Date	Business Impact	Security Risk	Business Risk
fridge.qa.qualys.com	ABC-Comp-local	10.10.10.1	Windows NT Machines, Marketing	07/15/2004	High	5	64
crisper.qa.qualys.com	BCC-Comp-local	10.10.10.2	Windows NT Machines, Marketing	07/15/2004	High	4	36
freezer.qa.qualys.com	CDE-Comp-local	10.10.10.23	Linux 2.4, Dev	06/22/2004	High	4	36
icebox.qa.qualys.com	DEF-Comp-local	192.168.1.45	Marketing	08/01/2004	High	4	36
dairy.qa.qualys.com	EFG-Comp-local	10.10.1.54	Mail Servers	08/01/2004	Medium	3	9



# Scan Frequency

- How often do we scan the systems?
- Schedule determined by your goals to meet security, compliance, or other business requirements
- Automated email reports or alerts can be configured, as well
- For example, the Nessus scanner allows you to setup daily, weekly, monthly, or other scheduled scans by date/time



# Tenable's Nessus Vulnerability Scanner

Nessus - Windows Internet Explorer  
https://localhost:8834/flash.html Certificate Error Bing

File Edit View Favorites Tools Help  
Favorites Suggested Sites Get more Add-ons

Nessus Reports Reports Mobile Scans Policies Users Configuration user Help About Log out

Keene\_policy Vulnerability Summary | Host Summary  
Completed: Feb 9, 2015 15:32 (1 Error)  
Download Report Remove Vulnerability | Audit Trail

Filters No Filters + Add Filter Clear Filters

Plugin ID	Count
11808	1
11835	1
12054	1
12209	1
22194	1
34477	1
35362	1
22034	1
26920	1
57608	1
11219	5
10736	4
11011	2
10111	1

Host Port  
10.3.1.6 445 / tcp

Plugin ID: 34477 Port / Service: cifs (445/tcp) Severity: Critical  
Plugin Name: MS08-067: Microsoft Windows Server Service Crafted RPC Request Han...

CPE  
cpe:/o:microsoft:windows

CVE  
[CVE-2008-4250](#)

BID  
[31874](#)

Cross-References  
[OSVDB:49243](#)  
JAVA:2008-A-0081  
MSFT:MS08-067  
CWE:94

Plugin Publication Date: 2008/10/23  
Plugin Last Modification Date: 2012/09/14

Done Local intranet | Protected Mode: Off 100%



# Scan Frequency Considerations

- Organizational risk appetite
  - How much time between a new threat and a scan?
- Regulatory requirements
  - Do you fall under FISMA or PCI DSS?
- Technical constraints
  - Network may not support scanning everything
- Business constraints
  - Do you have to avoid high business activity times?
- Licensing limitations
  - Scanners can control how many concurrent scans can be performed through licensing



# Best Practices For a New Program

- Start small
  - Start with a small section of the network's assets
- Expand slowly
  - Gradually add more scope to your scans
- Prevent overwhelming the enterprise systems and your system administration team

