

Compliments of  **QUALYS®**
CONTINUOUS SECURITY

2nd Edition

Vulnerability Management

FOR
DUMMIES®
A Wiley Brand

**Making
Everything
Easier!™**

FREE eTips at dummies.com®

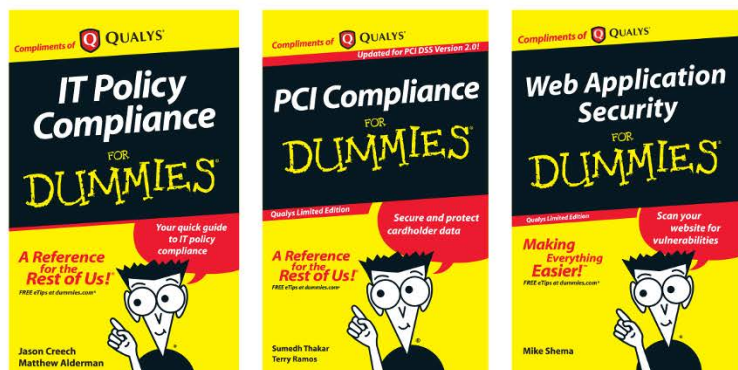


Check out our other “For Dummies” books:

IT Policy Compliance For Dummies

PCI Compliance For Dummies

Web Application Security For Dummies



Visit qualys.com/dummies to get your copy.

Vulnerability Management

FOR
DUMMIES®
A Wiley Brand

2nd Edition

by Wolfgang Kandek

FOR
DUMMIES®
A Wiley Brand

Vulnerability Management For Dummies®, 2nd Edition

Published by
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
England

For details on how to create a custom *For Dummies* book for your business or organisation, contact CorporateDevelopment@wiley.com. For information about licensing the *For Dummies* brand for products or services, contact BrandedRights&Licenses@Wiley.com.

Visit our Home Page on www.customdummies.com

Copyright © 2015 by John Wiley & Sons Ltd, Chichester, West Sussex, England

All Rights Reserved. No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or by any means, electronic, mechanical, photocopying, recording, scanning or otherwise, except under the terms of the Copyright, Designs and Patents Act 1988 or under the terms of a licence issued by the Copyright Licensing Agency Ltd, 90 Tottenham Court Road, London, W1T 4LP, UK, without the permission in writing of the Publisher. Requests to the Publisher for permission should be addressed to the Permissions Department, John Wiley & Sons, Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, England, or emailed to permreq@wiley.com, or faxed to (44) 1243 770620.

Trademarks: Wiley, the Wiley Publishing logo, For Dummies, the Dummies Man logo, A Reference for the Rest of Us!, The Dummies Way, Dummies Daily, The Fun and Easy Way, Dummies.com and related trade dress are trademarks or registered trademarks of John Wiley & Sons, Inc. and/or its affiliates in the United States and other countries, and may not be used without written permission. All other trademarks are the property of their respective owners. Wiley Publishing, Inc., is not associated with any product or vendor mentioned in this book.

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER, THE AUTHOR, AND ANYONE ELSE INVOLVED IN PREPARING THIS WORK MAKE NO REPRESENTATIONS OR WARRANTIES WITH RESPECT TO THE ACCURACY OR COMPLETENESS OF THE CONTENTS OF THIS WORK AND SPECIFICALLY DISCLAIM ALL WARRANTIES, INCLUDING WITHOUT LIMITATION WARRANTIES OF FITNESS FOR A PARTICULAR PURPOSE. NO WARRANTY MAY BE CREATED OR EXTENDED BY SALES OR PROMOTIONAL MATERIALS. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. THIS WORK IS SOLD WITH THE UNDERSTANDING THAT THE PUBLISHER IS NOT ENGAGED IN RENDERING LEGAL, ACCOUNTING, OR OTHER PROFESSIONAL SERVICES. IF PROFESSIONAL ASSISTANCE IS REQUIRED, THE SERVICES OF A COMPETENT PROFESSIONAL PERSON SHOULD BE SOUGHT. NEITHER THE PUBLISHER NOR THE AUTHOR SHALL BE LIABLE FOR DAMAGES ARISING HEREFROM. THE FACT THAT AN ORGANIZATION OR WEBSITE IS REFERRED TO IN THIS WORK AS A CITATION AND/OR A POTENTIAL SOURCE OF FURTHER INFORMATION DOES NOT MEAN THAT THE AUTHOR OR THE PUBLISHER ENDORSES THE INFORMATION THE ORGANIZATION OR WEBSITE MAY PROVIDE OR RECOMMENDATIONS IT MAY MAKE. FURTHER, READERS SHOULD BE AWARE THAT INTERNET WEBSITES LISTED IN THIS WORK MAY HAVE CHANGED OR DISAPPEARED BETWEEN WHEN THIS WORK WAS WRITTEN AND WHEN IT IS READ.

Wiley also publishes its books in a variety of electronic formats. Some content that appears in print may not be available in electronic books.

ISBN: 978-1-119-13150-2 (pbk); ISBN: 978-1-119-05829-8 (ebk); ISBN: 978-1-119-13151-9 (ebk)

10 9 8 7 6 5 4 3 2 1

Introduction

W

elcome to *Vulnerability Management For Dummies*!

Businesses use the Internet as a vital global resource for huge benefits in linking workers, suppliers and customers. However, connecting with the global Internet exposes your company network to many threats. Savvy criminals can use the Internet to break into your network, sneak malware onto your computers, extract proprietary information and abuse your IT resources. New computers joining the Internet get probed by attackers within an hour of connection and if left unprotected fall victim to attacks within 24 hours.

You can prevent most of these attacks by using a vulnerability management (VM) program. VM enables you to continuously monitor your network infrastructure, and by using a VM program you can stay several steps ahead of the attackers and protect your business resources.

About This Book

This book simply explains what you can do to automatically manage vulnerabilities and how to select the right tools to keep your network safe from attack.

Foolish Assumptions

In writing this book, we've assumed that you:

- ✓ Are somewhat familiar with information technology and networking.
- ✓ Want to understand the risks of networking and buggy software.
- ✓ Are thinking about using a vulnerability management application to improve your network security.

After reading this book you'll know more about how to do vulnerability management.

How This Book is Organized

This book is divided into six succinct parts:

- ✓ **Part I: Understanding the Need for Vulnerability Management.** Start here if you need a primer.
- ✓ **Part II: Doing Vulnerability Management.** Take a walk through the essential, best-practice steps of successful vulnerability management.
- ✓ **Part III: Considering Your Options for Continuous Vulnerability Management.** Here, you can gain an understanding of the pros and cons of different options for automating vulnerability management.
- ✓ **Part IV: Using Qualys VM: Continuous Vulnerability Management.** Meet Qualys VM – the effective cloud-based way to automate the vulnerability management process for continuous security.
- ✓ **Part V: Embracing Continuous Monitoring.** Leverage vulnerability management to continuously monitor risks and immediately respond to urgent attacks.
- ✓ **Part VI: Ten Best Practice Checks for Doing Continuous Vulnerability Management.** Follow these to help ensure your success with VM!

Dip in and out of this book as you wish; go to any part that interests you immediately or read it from cover to cover.

Icons Used in This Book



We highlight crucial text for you with the following icons:

This icon targets hints and shortcuts to help you get the best from vulnerability management solutions.



Memorize these pearls of wisdom, and remember how much better it is to read them here than to have your boss give a know-it-all lecture.



The bomb means ‘whoops’. It signals common errors that happen all the time. Avoid these at all cost.



You can skip information next to this icon if you’re not into it. Don’t worry – you don’t have to be a security whiz or hot rod programmer to do vulnerability management.

Where to Go from Here

Check out the headings and start reading wherever it makes sense for you. This book is written with a sequential logic, but if you feel a need to express your inner Spock you can start anywhere to extract good stuff.

If you want a hands-on demo or a trial version of Qualys VM – our featured vulnerability management solution – visit www.qualys.com.

Part I

Understanding the Need for Vulnerability Management

In This Part

- ▶ Understanding the threat posed by cyber criminals
- ▶ Reviewing the sources of software vulnerabilities
- ▶ Surveying international trends in vulnerabilities
- ▶ Defining vulnerability management as the way to remove risks

To a cyber criminal, vulnerabilities on a network are high-value assets. These vulnerabilities can be targeted for exploitation, which results in unauthorized access to the network. Once inside, cyber criminals look for personal information, credit card and health accounts, plus business secrets, intellectual property and, in short, anything that they can sell on the black market. In addition, the exploited computer is now a beachhead for further attacks into your network and it becomes part of a platform that attacks the network of other organizations.

Security researchers are continually discovering flaws in software, faulty configurations of applications and IT gear, and (dare we say?) good old human error – problems that lead to new vulnerabilities appearing on a daily basis. Whatever their source, vulnerabilities don't go away by themselves. Their detection, removal and control require *vulnerability management* (or *VM*) – the continuous use of specialized security tools and workflow that proactively help eliminate exploitable risks.

Who's at Risk?

Every single business with an Internet connection is at risk due to network vulnerabilities. Whether you're a small business, a multinational corporation or a government, it makes no difference – you're at risk.

The challenge for every business, then, is to maintain a safe, open, and interconnected network, making it easy to exchange information with customers, suppliers and business partners around the world.

Unfortunately, making this information both highly available and secure is hard work. Malware, such as Trojan horses and viruses, constantly threaten the theft of information and disruption of business operations. Moreover, the constant rate of new vulnerabilities discovered each day – and the speed with which new exploits are created – make this challenge even steeper.

The solution is to immunize your network from security threats by eliminating their origin: vulnerabilities.

How Vulnerabilities Expose Your Network to Danger

Vulnerabilities have plagued operating systems and software applications since the earliest days of computing. Successful exploits of vulnerabilities used to be rare and were often attributed to pranksters. In the last few years, however, criminal attackers have realized the monetary payback of cyber crime, and now you read about successful attacks made via the Internet almost every day.

The universal connectivity provided by this global pathway gives hackers and criminals easy access to your network and its computing resources – and they don't waste much time in getting started. When your computers are running without current security updates, they are *immediately* vulnerable to a variety of exploits. For example, a University of Michigan study, *How Vulnerable are Unprotected Machines on the Internet?*, found that servers with open ports and

other vulnerabilities were scanned by attackers within about 23 minutes of being attached to the Internet and vulnerability probes started in 56 minutes. The average time to the first exploit being made was less than 19 hours. Any business that doesn't proactively identify and fix vulnerabilities is susceptible to abuse and information theft.

Where do vulnerabilities come from?



Programming mistakes, or *bugs*, cause most vulnerabilities in software. For example, a common mistake – which happens in the memory management area of programs – is data blocks still being used after they've been declared free by other parts of the programs. When this 'use-after-free' programming mistake is found by attackers, they can often exploit it and gain control over the computer.

Computer scientists estimate that every thousand lines of software code in well-managed software products contain about one bug, with that number rising to 25 per thousand for unscrutinized code. Modern software projects typically have millions of lines of code. An operating system like Windows 7, for example, has 40 million lines of code, a Microsoft Office application between 30 and 50 million and popular Internet browsers between five and 10 million. It's no surprise, therefore, to see regular announcements of new vulnerabilities, with related patches and workarounds.

Attackers do not develop exploits for all vulnerabilities that are published, but they do constantly scrutinize critical vulnerabilities in widely installed software packages. To give you an idea of the attackers' reach, consider Microsoft; the organization has determined that between 10 and 25 per cent of the vulnerabilities it publishes are exploited within the first 30 days of publication.

The best way to counter this threat is to quickly identify and eliminate all vulnerabilities – and on a continuous basis. For example, Microsoft and Adobe release advisories and patches on the second Tuesday of each month – commonly called *Patch Tuesday* – whereas Oracle releases vulnerability patches on a quarterly schedule. Many of the newer software projects,

such as Google Chrome and programs in the Android, iOS and Windows appstores, have moved to continuous release cycles.



Careless programmers aren't the only source of vulnerabilities, though. A study by Hewlett-Packard Co. found that 80 per cent of applications contain vulnerabilities exposed by incorrect configuration. For example, improper configuration of security applications, such as a firewall, may allow attackers to slip through ports that should be closed. Likewise, mobile device users may use an unauthorized or even a malware-infested website without going through the corporate virtual private network (VPN), perhaps because the official VPN is a bother when you want to surf Facebook, eBay or Craig's List ads. Letting your security guard down like this exposes devices and your network to attacks. Even just clicking on an email attachment or website link infected with malware can be enough to trigger an attack.

The exploitation of vulnerabilities via the Internet is a huge problem that requires immediate proactive control and management. That's why companies need to use VM – to proactively detect and eliminate vulnerabilities in order to reduce overall security risk and prevent exposure.

Looking more closely at attack trends

Data breach disclosures in the news have documented the unauthorized exposure of millions of confidential consumer records worldwide. The resulting damage to a breached organization's reputation can be significant, causing customers to take their business elsewhere. Such damage is adequate proof why organizations must do more to protect their networks from attack.



A dramatic change in the security threat landscape is raising the bar still further for organizations, both large and small, who want to actively minimize successful attacks on their vulnerabilities. Recent data show that attacks are no longer restricted to traditional types of generic viruses, worms, Trojans and other single-vector attacks. Over the last few years, a fundamental change in the nature of attacks made

reveals a movement away from nuisance and destructive attacks towards more stealthy, hard-to-detect activity motivated by financial gain. This type of attack has the following five characteristics:

- ✓ Increased professionalism and commercialization of malicious activities, allowing non-technical criminals to enter the market.
- ✓ Attacks that are increasingly tailored for specific regions and interest groups.
- ✓ Increasing numbers of multi-staged attacks.
- ✓ Attackers that target victims by first exploiting trusted entities.
- ✓ Increasing numbers of attacks against browser vulnerabilities, mirroring the rise in browser usage in people's day-to-day activities.

A recent *Verizon Data Breach Investigations Report* studied 63,000 confirmed security incidents. The report found that within 18 business sectors, confirmed data loss was especially high in accommodation, finance and retail businesses, and had a clear focus on financial gain. The Ponemon Institute found that the average cost of a data breach is \$5.4 million for an organization, or \$188 per record. For a large organization, losses can be astronomical, and the 2013 breach of 140 million customer financial records at Target Corporation cost the organization about \$148 million.



Because the fallout from cyber attacks poses such serious financial risk, your organization needs to stop malware and other attacks by deploying layers of security technology. The Council on CyberSecurity (www.counciloncybersecurity.org) promotes a blueprint for an intuitive approach to the problem with its *Critical Security Controls*. Traditional security technology such as anti-virus/anti-spyware software, firewall, intrusion detection/prevention, VPN and encryption are part of that blueprint, yet while they're effective in their own spheres of purpose, none of these measures perform the most fundamental of all security measures: the continuous management of your hardware and software assets, their configurations and vulnerabilities. According to the Council and its case studies, the returns of implementing a security program that focuses

on knowing one's environment and quickly fixing detected vulnerabilities are over 90 per cent, so the value of effective VM is clear.

Detecting and Removing Vulnerabilities

VM has evolved from simply running a scanner on an application, computer or network to detect common weaknesses. Scanning remains an essential element of VM, but continuous VM now includes other technologies and workflow that contribute to the bigger picture required for controlling and removing vulnerabilities.

The primary objectives of VM are to:

- ✓ Maintain a database of the computers and devices of your network – your *hardware assets*.
- ✓ Compile a list of installed software – your *software assets*.
- ✓ Change a software configuration to make it less susceptible to attack.
- ✓ Identify and fix faults in the installed software that affect security.
- ✓ Alert to additions of new devices, ports or software to the databases to allow an analysis of the changed attack surface and to detect successful attacks.
- ✓ Indicate the most effective workflow for patching and updating your devices to thwart attacks (such as malware, bots and so on).
- ✓ Enable the effective mitigation and management of security risks.
- ✓ Document the state of security for audit and compliance with laws, regulations and business policy.
- ✓ Continuously repeat the preceding steps so as to ensure the ongoing protection of your network security.

Consistent, ongoing execution of VM is difficult, if not impossible to do on a manual basis. You have simply too many 'moving parts' to juggle and act on in a timely and cost-effective manner.

Repetitive tasks that regularly cycle through all devices are enormously time consuming and an inefficient use of IT and network staff time. For this reason, organizations need to automate and simplify as much as they can for each element of the VM process, which we cover in Part II.

VM can automatically document regulatory compliance

A major benefit of VM is the built-in reports provided by VM software. Some of these reports are good enough for documentation demanded by auditors checking for regulatory compliance. Security is a growing requirement for financial transactions, health care information, and information used in many other forms of business automation solutions.

Legal network security requirements are seen in a growing number of government and industry-specific regulations for safeguarding the confidentiality, integrity and availability of electronic data from information security breaches. Organizations that don't fully comply and stay up-to-date with security regulations face serious potential consequences and including fines, civil and sometimes criminal penalties. Part III tells you more about VM and compliance.

As you find out more about VM in this book, keep related regulations for

compliance in the back of your mind – especially as they relate to your company. The regulations may specify use of certain VM-related processes or technologies. VM-related technologies provide reports such as those from scanning and patch management systems. The network and IT departments use these reports to document network security audits and remediation, including detailed, prioritized lists of existing vulnerabilities related to severity of risk, and verification of vulnerabilities that were fixed with patches or work-arounds.

The most important idea about compliance is that VM can automate much of what used to be an expensive, time-consuming manual process. Getting the right VM solution can not only *protect* your network and data – it can also *save you money* by automating daily chores for VM! Any business can easily automate VM.

Getting Ready to Do VM

As you get ready to do VM, be sure to organize your priorities for security. This includes determining everything that needs protection, including servers, network services, applications and endpoints. In the past, this process was a manual one that required an enormous effort to organize details and keep the information current. Luckily, new software tools can now automate this process, saving you time, improving accuracy and lowering the total cost of ownership (see Part II).

Part II

Doing Vulnerability Management

In This Part

- ▶ Discovering and categorizing assets for VM
 - ▶ Scanning systems for vulnerabilities
 - ▶ Prioritizing assets by business risk
 - ▶ Remediating vulnerabilities
 - ▶ Informing the security team, auditors and management with reports
 - ▶ Continuously repeating these steps for ongoing security
 - ▶ Adopting the right solution
-

In practice, *vulnerability management (VM)* means systematically and continuously finding and eliminating vulnerabilities in your computer systems. Many of the steps or processes involved in VM use technology; other steps need IT staff to implement patches, software updates and follow-ups. The integration of these processes produces stronger computer security and protection of your organization's systems and data.

This Part walks you through six steps for laying the foundation of a successful VM program.

Step 1: Scoping Your Systems to Identify Your Inventory



In order to find vulnerabilities, you must first understand what *assets* (such as servers, desktops, copiers and mobile devices) are running on your network. This involves uncovering forgotten devices. You also need to identify the people who are responsible for maintaining these assets (the *owners*).

The main purpose of *scoping*, also called *asset discovery*, is to organize your computer systems according to the role they play in your business, to establish an evaluation baseline. Usually, the scoping process begins automatically at the start of a VM scan. During scoping, the VM technology solution creates a database of all computer systems and network devices with an Internet Protocol (IP) address that are attached to your network. Figure 2-1 shows a network map created with information from an asset database.



Scoping starts with a vulnerability scan – usually done by directing the scanner at a particular Internet Protocol address or range of addresses, so it's useful to organize your database by IPs.

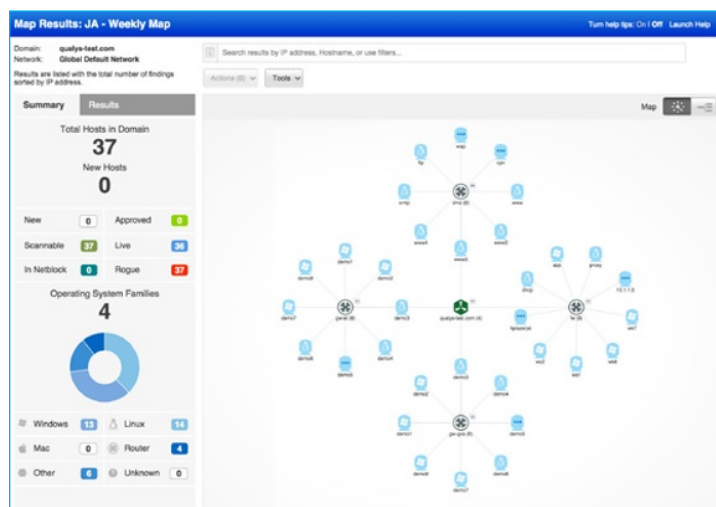
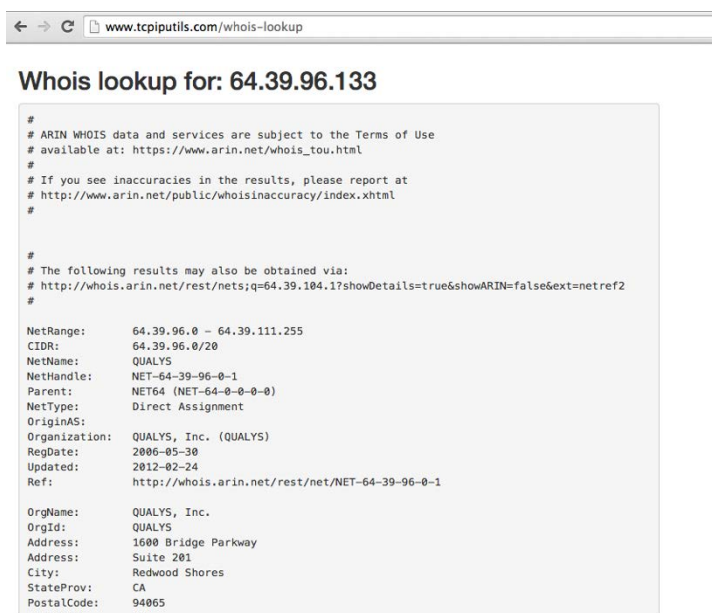


Figure 2-1: A network map identifies and shows the logical relationship between all the assets on a network.

Beginning with a limited set of your computer systems to test drive this scoping process is a helpful step. Often, starting with your organization's Internet-facing systems makes the most sense. Your Internet perimeter is usually well defined in terms of IP addresses and system ownership, and the computer systems exposed to the Internet are the ones upon which attackers first focus their attention. Consequently, these systems are the ones that you want to look at first.

When you do so, record the IP address ranges that make up your publicly visible Internet perimeter and their corresponding system and business owners. Your website can give you an initial starting point, as it will return an IP address allocated to your company. You can use this IP address to perform further research. For example: 'whois 64.39.96.133' will inform you that Qualys owns the IP address range 64.39.96.0 – 64.39.111.255. Figure 2-2 provides an example.



```
#
# ARIN WHOIS data and services are subject to the Terms of Use
# available at: https://www.arin.net/whois_tou.html
#
# If you see inaccuracies in the results, please report at
# http://www.arin.net/public/whoisinaccuracy/index.xhtml
#

#
# The following results may also be obtained via:
# http://whois.arin.net/rest/nets;q=64.39.104.1?showDetails=true&showARIN=false&ext=netref2
#

NetRange: 64.39.96.0 - 64.39.111.255
CIDR: 64.39.96.0/20
NetName: QUALYS
NetHandle: NET-64-39-96-0-1
Parent: NET64 (NET-64-0-0-0-0)
NetType: Direct Assignment
OriginAS:
Organization: QUALYS, Inc. (QUALYS)
RegDate: 2006-05-30
Updated: 2012-02-24
Ref: http://whois.arin.net/rest/net/NET-64-39-96-0-1

OrgName: QUALYS, Inc.
OrgId: QUALYS
Address: 1600 Bridge Parkway
Address: Suite 201
City: Redwood Shores
StateProv: CA
PostalCode: 94065
Country: US
```

Figure 2-2: Identifying device ownership for IP addresses.

eBay case study



Industry: Technology

Headquarters: San Jose, California, USA

Locations: Worldwide

Major Brands: eBay, PayPal, Shopping.com

Employees: 34,000+

Annual Revenue: USD\$15.2+ billion

Stock Symbol: EBAY (NASDAQ)

'Qualys VM has made the job of auditing our network much easier. We used to have to dig through results and do a lot of manual analysis to get meaningful reports, and those were inconsistent. Qualys takes care of that nightmare.' – Senior Manager, Information Security

Objectives:

- ✓ Reliably identify network vulnerabilities across the global network.
- ✓ Audit the network security of business partners and help those partners to quickly remediate vulnerabilities and eliminate risks.
- ✓ Rollout an automated solution that would find the most recent vulnerabilities without requiring

constant and time-consuming staff research.

- ✓ Provide senior management with the ability to audit and review the security 'posture' (industry term for 'status') at any time.

Results:

- ✓ After a careful market evaluation, eBay selected Qualys VM for both network-perimeter scanning and auditing vulnerabilities on the network within the corporate firewall, and on partner networks.
- ✓ eBay now has a default vulnerability management standard to evaluate security throughout both eBay's and partner networks.
- ✓ Simplified reporting gives senior executives a concise, real-time view into the company's security risks. Qualys VM enables eBay execs to measure the changes in those risks as they implement security measures.

See www.qualys.com/customers/ for more info and other case studies.

Step 2: Assessing Your Security Status



Assessment is done with vulnerability scanning and is the foundational process for finding and fixing the vulnerabilities in your computer systems. You can perform an assessment via vulnerability scanning in two ways:

- ✓ A one-off scan that gives you a snapshot of the security status of your computer systems at a particular moment in time.
- ✓ A scan that runs repeatedly on a periodic basis (say daily or weekly), allowing you to track the speed of applying patches and software updates and to assess how your security status is improving. This level of assessment provides you with more information that is useful for effective VM.

In both cases, making a scan involves two steps:

- 1. The scanner uses its library of vulnerabilities to test and analyze computer systems, services and applications for known security holes.**
- 2. A post-scan report organizes and prioritizes the actual vulnerabilities and gives you information for applying patches and updates.**

How often should you scan?

Asset inventory, configuration and vulnerability data gathered by your scanner is the raw fuel for continuous monitoring of computer security. Without fresh data, monitoring is not continuous, and your computer systems will be at risk. Therefore, for best results, Qualys suggests that you scan your important computer systems daily and your strategic, high-value assets multiple times daily – or better still, *continuously*.

A scanning tool such as Qualys VM allows you to continuously and automatically scan any asset in your network. As a result, the vulnerability scanning data you obtain will truly be up to date. This enables you to use that data with an add-on tool, like Qualys Continuous Monitoring, as a real-time component of keeping your computer systems safe from exploits.

Launching a scan

You can usually schedule a vulnerability scan to run repeatedly or run it on demand. Your scan request needs to specify the particular computer systems or network devices that you want to check for vulnerabilities, typically as a combination of IP addresses, ranges of IP addresses and asset groups. The scan is then initiated by your VM application. Figure 2-3 shows a scan created to launch repeatedly every week.

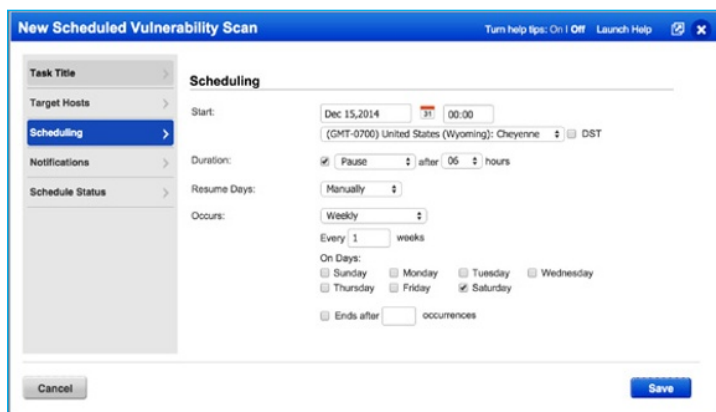


Figure 2-3: Creating a scheduled scan.



Before you launch a scan, it makes sense to inform the parties responsible for the systems you're scanning. System owners might have local or network security mechanisms installed that block vulnerability scans. In these cases, ask them to 'whitelist' the IP addresses of your scanner and VM scanning solution to avoid unnecessary alerts and provide you with better results.

Reviewing options for scanning tools

Your choice of scanning technology is an important element of an effective VM implementation. You have many options. All use a vulnerability database of known risks, but these databases vary in coverage, effective quality and frequency of receiving vulnerability updates. Traditionally, locally installed scanners require software applications that you install and

maintain. These can tie up significant time and resources – plus, they carry typical operational overhead.



By contrast, software applications from a cloud provider may also be used. These applications are hosted by a vendor and used by businesses with a web browser over the Internet. This delivery model, called *Software as a Service (SaaS)*, is commonly used for a variety of applications – including VM. A cloud-based VM solution provides the ability to perform the scans on demand over the Internet. You simply log in to your account and manage everything online.

Cloud-based VM works without special software and is always up to date with the most recent and comprehensive set of vulnerability signatures. As a result, you don't have to worry about updates to scanning technology because they're automatically applied within the VM system. Better yet, cloud-based VM requires no system or database administrators from your side, which frees you to focus your resources on

Public enemy #1: Open system administration channels

Organizations of all sizes appreciate the power of remote system administration. Productivity and response is accelerated when administrators can address problems from home during service outages, or work from a hotel or hotspot while traveling. But this convenience also increases the network 'attack surface' by opening additional entry slots via the Internet. As a consequence, attackers are also making use of these remote access channels. They either launch 'brute force' attacks against these channels (where they continuously guess the password until the correct one is found) or they use stolen or cracked credentials to gain access

to the exposed computer systems. Remote access allows attackers to use these openings as beachheads to access other devices on the internal network. This attack mechanism was recently highlighted by the US-CERT in an official alert responding to the Backoff Point-of-Sale malware in US-CERT TA14-212A.

Vulnerability management solutions can help to identify your open system administration channels and alert you in case a new channel is detected. Scanning your Internet perimeter for systems that allow remote system administration is a key step to preventing attacks.

analyzing and remediating vulnerabilities. We describe the benefits of using the cloud for VM in more detail in Part III.

Knowing what to scan

The simple answer to the question of what to scan is pretty much anything that is connected to your organization's network.



You can scan by broad functional classifications – such as Internet-facing servers, workstations, network devices and printers – or by areas of responsibility in departments such as Finance, HR or Legal.

Mobile computing

Many organizations have shifted a large percentage of workstations from fixed desktop computers to portable notebook computers for more productivity and flexibility.

This flexibility presents a serious challenge for VM scanning: How can you scan a machine that is sporadically connected to your organization's network? One way is to intercept machines when they access the virtual private network (VPN) server and catch them with a traditional remote VM scan. But this approach is getting harder to execute because many organizations no longer require VPNs to perform remote work. Instead, e-mail and other applications are increasingly used through the Internet with Software-as-a-Service (SaaS).



The best solution for mobile is an agent-based approach, where locally installed small-footprint software provides all the information necessary to evaluate the security state of the machine. An agent tuned for VM information gathering can be non-intrusive without affecting functions of the operating system and applications – with a near-zero effect on processing, memory and network bandwidth.

Non-intrusiveness and ease-of-installation are key factors for deployment and acceptance by mobile users. The other hurdle is winning acceptance by IT staff because they will scrutinize requests for additional agents, and insist the agents provide clear value without negatively affecting IT infrastructure.



When you evaluate agent-based technologies for mobile VM scanning, consider:

- ✓ **Integration of results:** Results from agent-based scans and normal VM scans must provide the same data and are used in the same reporting, ticketing and asset management systems.
- ✓ **Always-on:** Agents should transmit results continuously, as soon as they are connected to the Internet, without need for a VPN network.
- ✓ **Minimal footprint:** The need for zero impact on the target machine favors an approach where no VM scan is run directly on the notebook computer. Instead, data on the state of security changes is collected and transferred to an Internet-facing system for evaluation of vulnerability signatures.
- ✓ **Update speed:** Signatures for normal and agent-based scans should be the same, or released in a way that prevents result skew.

With agent-based scanning, you'll be able to provide 100 per cent coverage of your installed infrastructure.

Virtualization

For servers, virtualization has led to similar gains in flexibility. With virtualization technology, a server can be set up on demand, often within a few minutes. Generic virtualization service providers now provide the ability to host these servers with geographical options worldwide. However, while virtual server infrastructure has become more agile and efficient, virtual servers are also harder to track – especially for VM.

In order to properly address scanning virtualized servers in your VM program, evaluate:



- ✓ **Virtual scanners:** Scan engines are available for your virtualization platforms, allowing you to seamlessly integrate the scanner into your virtualization setup.
- ✓ **Monitoring:** In virtual environments, the creation of new servers tends to be dynamic. This is especially true for virtualization service providers and may result in the creation of new server networks. The downside for you is that your virtual servers on these networks are not



automatically scanned by many VM solutions. Be sure your VM solution provides monitoring capability to automatically scan virtual servers. This requirement is mandatory!

- ✓ **Authorization:** Service providers frequently restrict scanning to pre-approved hosts. Acquiring this approval will introduce an additional request/wait step in executing your VM program. Look for pre-approved scanning solutions to eliminate this manual and time-consuming requirement.

Step 3: Prioritizing and Working With Your Scan Results



Research has shown that between 10 per cent and 40 per cent of all vulnerabilities are exploited by attackers, as shown in Figure 2-4 (for Microsoft application and operating system vulnerabilities during the last five years). Findings such as this make clear how crucial it is to fix vulnerabilities in your systems.

Fixing all vulnerabilities at once, however, is practically impossible. In fact, in large organizations, the amount of vulnerability data can be overwhelming if you don't properly

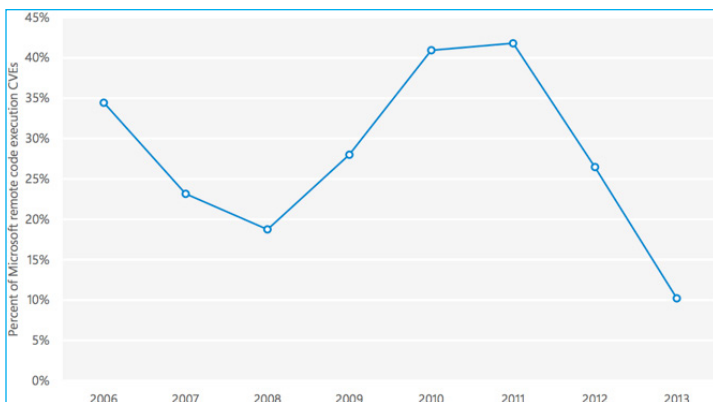


Figure 2-4: Percentage of Microsoft remote code execution vulnerabilities with known exploits.

categorize, segment and prioritize it in a meaningful fashion. A functional VM workflow allows you to automatically rank vulnerabilities to determine the most critical issues that could impact the most critical systems.



Your VM system should be able to indicate the most efficient patch for you to apply to a vulnerability. Smart VM systems know which patches are cumulative and contain or supersede older patches. The VM system will automatically take that data into account when listing the most important vulnerabilities to fix. This capability can improve your effectiveness in patching by 10 times or more!



Organizations can optimize their patching workflow by addressing vulnerabilities that have known associated exploits. Look for a VM system that allows you to filter your detected vulnerabilities by the following categories:

- ✓ Exploits in use in the wild (ExploitKits and zero-days)
- ✓ Commercial Exploit tools (Canvas, Core, Metasploit)
- ✓ Proof of Concepts (Exploit DB)

These categories are ordered from highest-risk reduction (first ✓) to medium- (second ✓) and lowest- (third ✓) risk reduction. As you begin doing VM, focus on vulnerabilities that are listed in the 'ExploitKit' category in order to achieve maximum and rapid impact on reducing risk of exploits in your network environment. Figure 2-5 shows this option selected in Qualys VM.

Tagging your assets

Managing your inventory of network assets is equally important as discovering what's out there! To do this flexibly and efficiently, choose a VM solution that includes a handy feature called 'asset tagging.' A *tagging system* allows you to organize your assets into logically similar groups, such as by device type, similar busi-

ness impacts or organizational characteristics.

Your VM solution should provide a way to easily assign and modify *tags*, which assign one or more labels to each asset, much like you might organize emails with an application like Google Gmail and other similar email systems. Tags let you organize

(continued)

(continued)

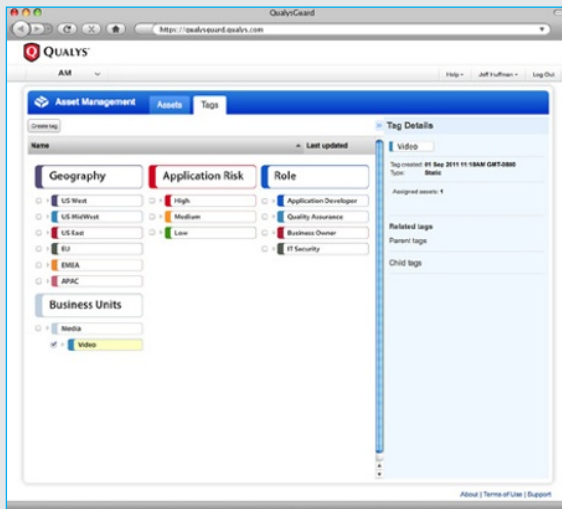
assets for scanning, reporting and remediation in a variety of ways, including:

- ✓ Manually assigning assets to groups.
- ✓ Automatically grouping assets according to attributes such as IP address or DNS name.
- ✓ Dynamically ‘tagging’ assets according to customizable rules.

Asset tagging shows its power and utility when used in conjunction with rule definitions. For example, assets tagged with ‘Internet facing’

are all systems that have IPs with routable IP addresses (in other words, not RFC 1918 private IPs: 10.x.x.x or 192.168.x.x); ‘web servers’ are systems that have port 80 or 443 open; and ‘Windows servers’ are all systems with Operating System Windows Server 2003, 2008 or 2012. The figure shows asset tags applied to a variety of custom attributes and sub-attributes.

With asset tagging, your IT, security and compliance teams are informed quickly and effectively about the issues they need to know about most!



The result of combining filtering capability to scan for ExploitKit-only vulnerabilities with the business-related tags enables true risk-based prioritization (see Figure 2-5). This functionality enables your security staff to focus on identifying critical data and systems most likely to be exploited by an attack.

Search

User Configuration: ☐ Disabled ☐ Edited

Category: ☐ NOT All

Patch Solution: ☐ Patch Available ☐ Trend Micro Virtual Patch Available ☐ No Patch Solution

CVE ID: ☐ NOT

Exploitability: ExploitKits ×

Associated Malware: All

Vendor Reference: ☐ NOT

CVSS Base Score: (or greater)

CVSS Temporal Score: (or greater)

Search

Figure 2-5: Selecting ExploitKits to scan for 'high exploitability' vulnerabilities.

Knowing what to look for in scan results

Scan results need to be:

- ✓ Comprehensive.
- ✓ Specific – especially with respect to data about the detection of the vulnerability and provision of instructions for remediation.
- ✓ Free of *false positive* (vulnerability wrongly detected) or *false negative* (vulnerability present but not detected) scan results.
- ✓ Easy to understand.



False positives in particular are toxic to VM programs because they drown the scan results with vulnerabilities that don't match what's in your IT asset inventory. Chasing down false positives is a waste of time. Likewise, a false negative may occur when the VM solution fails to detect a vulnerability that actually exists in your network. These occasions are less

visible, yet not knowing about the vulnerability places your network at serious risk of exploitation by hackers.

Improving the odds for good scan results



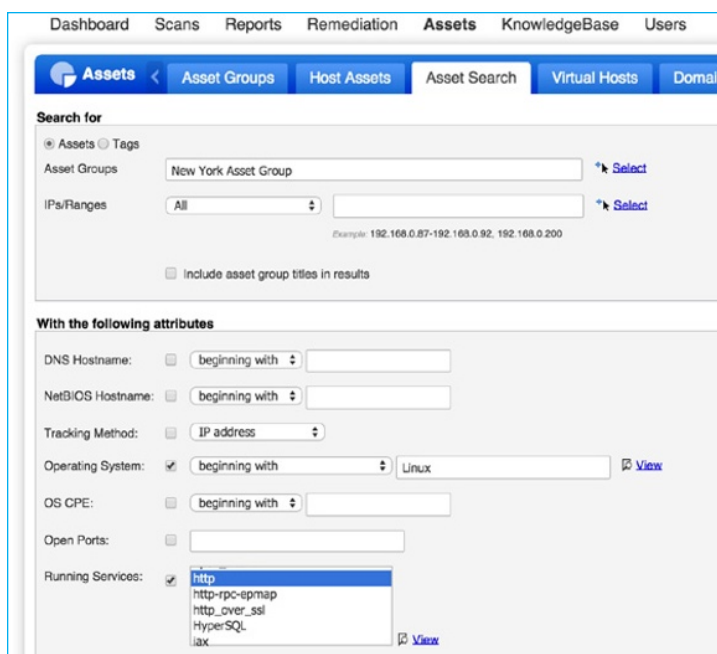
Substantial industry- and government-driven efforts are aimed at collecting data about computer system vulnerabilities. The VM solution you choose should incorporate as many of the findings as possible to tap the collective wisdom of vulnerability researchers.

To keep up with the pace of vulnerability announcements, take a look at:

- ✓ The Common Vulnerabilities and Exposures (CVE) website at www.cve.mitre.org.
- ✓ The National Institute of Standards and Technology's National Vulnerability Database at <http://nvd.nist.gov>. The NIST database takes CVE to the next level by adding standardized CVSS severity scores and detailed information for each of its vulnerabilities.
- ✓ The United States Computer Emergency Readiness Team (CERT) Vulnerability Notes Database at www.kb.cert.org/vuls/.
- ✓ The Exploit DB database that collects Proof of Concepts for vulnerability exploits at www.exploit-db.com/.
- ✓ A particular vulnerability management vendor's own knowledgebase gleaned from its ongoing research and development efforts.



Often, you can judge the impact of a new vulnerability by performing searches on your scan results. Imagine, for example, a new vulnerability is announced for the Apache webserver under Linux. You can get a first estimate of your affected machine by searching your assets for all Linux servers that have the HTTP service. Figure 2-6 shows such a search for IPs called 'New York Asset Group,' and within that group, all Linux hosts running the HTTP service.



Dashboard Scans Reports Remediation **Assets** KnowledgeBase Users

Assets < Asset Groups Host Assets Asset Search Virtual Hosts Domains

Search for

☒ Assets ☐ Tags

Asset Groups: * Select

IPs/Ranges: * Select

Example: 192.168.0.87-192.168.0.92, 192.168.0.200

☐ Include asset group titles in results

With the following attributes

DNS Hostname: ☐ beginning with

NetBIOS Hostname: ☐ beginning with

Tracking Method: ☐ IP address

Operating System: ☒ beginning with View

OS CPE: ☐ beginning with

Open Ports: ☐

Running Services: ☒
http-rpc-epmap
http_over_ssl
HyperSQL
IAX View

Figure 2-6: Asset search for New York servers with HTTP.

The result of good scanning is accurate, up-to-date and concise vulnerability information that you can trust and apply to the assets on your organization's network.

Thinking like a hacker

The VM solution you select needs to allow your security team to 'think like a hacker' as it uses the scanning technology to identify and fix vulnerabilities inside and outside the firewall.

To duplicate a hacker's workflow, each scan should work from the outside, looking in. The implication

for a scanner is that it's deployed outside the firewall and audits all of an organization's hosts facing the Internet. Naturally, the scanner's platform also needs protection from attacks via the Internet, so be sure to account for this safety factor as you choose a solution.

(continued)

(continued)

The VM solution needs to operate by the same steps used as a hacker, including:

1. **Gathering information** and finding out as much about a host as possible without visiting or connecting to it, with techniques such as whois, DNS and IP assignments.
2. **Discovering** and identifying hosts in the target subnet, including topology, firewalls and other devices.
3. **Scanning** and finding out the potential targets and vulnerabilities associated with hardware, software and their open ports via network scanning and port scanning.
4. **Verification** and confirming the vulnerabilities to achieve the goal of a successful exploit.

Employing technologies to improve scanning



Look for scanners that use a variety of active operating system (OS) discovery techniques, such as banner grabbing and binary grabbing, OS specific protocols and TCP (transmission control protocol)/IP stack fingerprinting (determines operating system used by a remote target), and passive techniques such as packet spoofing (concealing or forging identity with a fake source IP address). Fingerprinting entails careful inspection for subtle variations in implementation of RFC (request for comments) standards. A service discovery engine detects backdoors, Trojans and worms by checking TCP and UDP (user datagram protocol) services, including those on non-default ports and with fake banners. A similar discovery process is used to fingerprint HTTP applications by leveraging software's version ID, service pack ID and installed patches. A good scanner will correlate OS and HTTP fingerprint tests to quickly find true vulnerabilities and minimize false positives.

Step 4: Fixing Vulnerabilities

Fixing vulnerabilities is another core discipline of vulnerability management. Such is the importance of this step that the risks of getting it wrong or avoiding it can have huge implications for an organization.

Traditional manual processes for finding flaws, suggesting patches and other remediation actions are far too slow, error-prone and ultimately too expensive to be used efficiently. Also, the high cost of patching coupled with the high volume of flaws detected in software applications sometimes encourages organizations to delay remediation. This may cause an organization to delay updates even for critical patches or large, highly tested updates such as service packs. Unfortunately, delay causes a ‘technical debt’ in the software systems, which is a fatal strategy. As an example of technical debt, recall the recent case of Windows XP. Organizations that did not prepare for its end-of-life in 2014 and failed to replace the aging operating system are now faced with immense problems. On one hand, the technical debt is so high that an upgrade to a supported system requires a major change in underlying hardware, technology and user interface. The alternative is to pay Microsoft top dollar for each necessary patch and continue using an operating system that can be easily invaded by any moderately skilled attacker.



So, fixing vulnerabilities is essential. Fortunately, mature software vendors fix flaws in their products on a regular basis and perform extensive testing on the new versions. Operating system, Internet browser and standard application updates should thus be transparent to your business and cause no interruption in your workflow. This tendency has accelerated in recent years, especially on mobile platforms. Thanks to ubiquitous connectivity, the industry is moving to ‘silent updates’ such as with Google Chrome, the Windows App store and the new Windows 10.

If you have special configurations that are not covered by the software vendor’s testing, or applications that are custom written, it makes sense to perform your own pre-testing on patches before applying them to live systems.



Pre-testing patches

Follow these tips for pre-testing:

- ✓ Ensure the testing takes place in your organization’s unique environment. Most problems with patches are due to third-party applications or modifications to default configuration settings.

- ✓ Verify the integrity of the patches by comparing checksums with the information provided by the software vendors.
- ✓ Check that the patch corrects the vulnerability without affecting applications and operations of the business process.



Managing patching

Follow these tips for patching:

- ✓ Remediate vulnerabilities as quickly as possible and minimize risk by applying the patches in the priority we outline in Step 3.
- ✓ Adopt automated patch management and software distribution solutions – these are crucial for all but the smallest environments in streamlining the patching process and keeping costs to a minimum. The rollback capability included in such tools can restore software to a previous state and ensures that organizations use appropriate software versions efficiently.
- ✓ Integrate patch management with other automated VM processes. For example, Qualys VM provides one-click links to vulnerability patches, fixes and workarounds to use during this phase of workflow.

Using a VM solution that does ‘patch packaging’



Software vendors usually group fixes for multiple vulnerabilities into a single patch, called *patch packaging*. It is important for your workflow to choose a comprehensive VM solution that can integrate patch packaging on two critical levels. The first includes vulnerabilities identified by Common Vulnerabilities and Exposures (CVE) number (for example CVE-2014-2799); the other includes vulnerabilities identified by a vendor’s patch ID number (for example, Microsoft’s MS14-052, which contains 37 CVEs). These distinctions avoid potential confusion between your security and operations staff, for both tend to think differently about patches. Security staff often focus on CVE and operations staff often think about security in terms of particular vendors’ patches.

In addition to patch packaging, software vendors usually provide cumulative patches, which means the newest version contains all previous patches. Again, it is important that your tool has knowledge of these *supersedes* and indicates the best patch to apply in a given situation. This capability avoids overwhelming operations staff with tens or hundreds of work items when a handful are adequate. An example of a patch report with supersedes is shown in Figure 2-7.

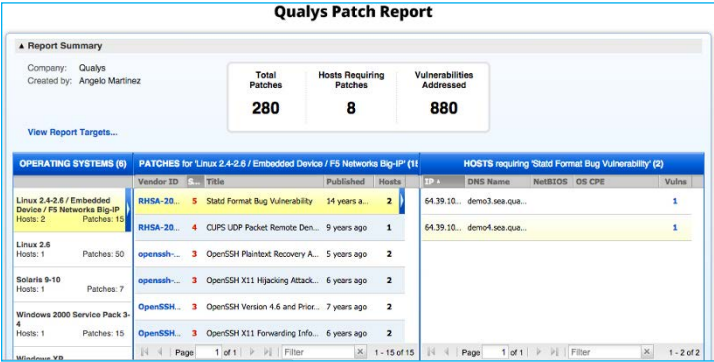


Figure 2-7: Patch report ranks patches by ‘supersedes’.

Olympus Europa case study



Industry: Manufacturing
Headquarters: Hamburg, Germany
Locations: Europe
Employees: 4,700

‘For me, the Qualys VM platform is simultaneously also the central data basis for communicating with the management. The reports

contain all of the essential points and are readily comprehensible, so they strengthen our executives’ commitment to IT-security-related issues.’ – Specialist Responsible for IT Auditing

Objectives:
Due to a huge distributed IT architecture, Olympus Europa sought to

(continued)

(continued)

automate its manual vulnerability audit and remediation efforts, and centrally unify all phases of these processes for policy and regulatory compliance.

Results:

- ✓ Qualys VM enables Olympus Europa to automate existing test schemata and to integrate them into the vulnerability remediation workflow.
- ✓ The Qualys API enables integration with other software solutions.

✓ The Qualys Cloud Platform makes it simple to centrally control and use the Qualys VM scanner in the various business groups.

✓ Reporting from the Qualys platform enables communication between the specialists responsible for IT security and the company's business executives, and enables policy and regulatory compliance.

See www.qualys.com/customers/ for more info and other case studies.

Step 5: Staying Informed

The VM solution you adopt should keep you fully informed of your company's network security state. Your trusted informant will be the built-in reports and dashboards that allow you to customize the type and presentation of vulnerability information exactly as you need it. Reports will inform a variety of stakeholders, including first responders and specialists in network operations, security operations and IT operations; people responsible for patching and IT configuration updates; IT department managers and directors; chief information security officers; compliance officers; auditors; and corporate executives.

Examples of typical reports, such as those shown in Figure 2-8, include:

- ✓ **Dashboard**, which provides an 'at-a-glance' summary of network vulnerabilities and remediation status.
- ✓ **Vulnerability summary**, which lists all vulnerabilities on the network by priority.
- ✓ **Threat analysis**, which details specific threats to each device on the network and enables drill-down review of specific issues.



Figure 2-8: An array of VM reports will enable effective network security.

- ✓ **Patch report**, which shows the status of patching, which devices remain unpatched by priority, and who is responsible for remediation.
- ✓ **SSL certificate management**, which ensures the correct certificates are in use and notifies when renewals are due.
- ✓ **Compliance reports** as documentation for auditors, notification of compliance status for executives, and as a 'to-do' list for operations staff.

The most useful reporting capabilities for operations staff are the ability to understand what vulnerabilities need fixing, and how to accomplish that task.

Getting familiar with the elements of scan reports

A VM system should allow for both detailed and summary reporting. Detailed reports (such as the example in Figure 2-9) are geared towards your technical staff and provide information at the lowest level: severity of the vulnerabilities, vulnerability detection details and remediation steps that aid IT administrators in their task of addressing the vulnerabilities.

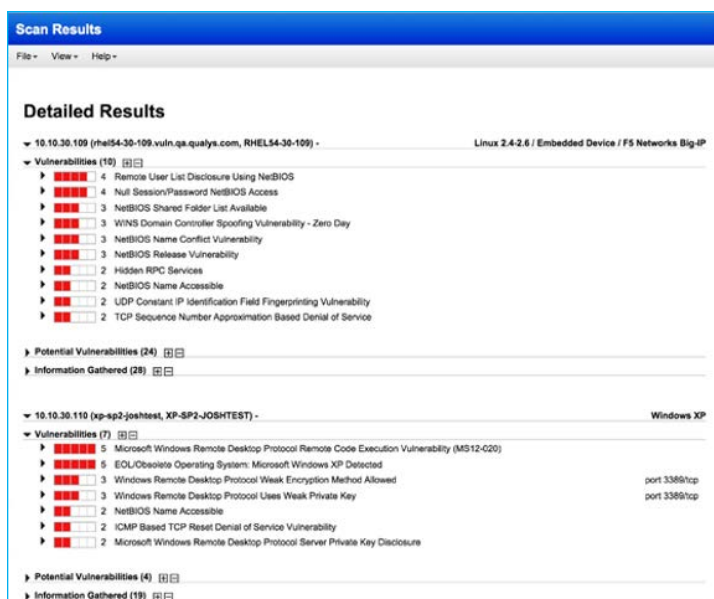


Figure 2-9: Scan report of vulnerabilities identified on the network.

Summary reports, on the other hand, provide information of a higher level – for example, on all systems with a certain tag. Scorecard reports are particularly useful in gathering high-level status data that can be presented to your executives; see Figure 2-10 for an example.

Benefitting from built-in trouble ticketing



As you examine initial vulnerability reports, it's useful for the VM system to let you instantly assign a *trouble ticket* – a kind of tracking system for problems – to a particular vulnerability to help speed remediation workflow.

Trouble ticketing enables organizations – especially larger organizations – to automatically distribute and assign vulnerability remediation actions to certain individuals or groups. For example, you can have all critically-rated web server risks directed to the web IT security manager and all lower-level risks assigned to other personnel. A continuous monitoring system, such as Qualys Continuous Monitoring, integrates VM reporting such

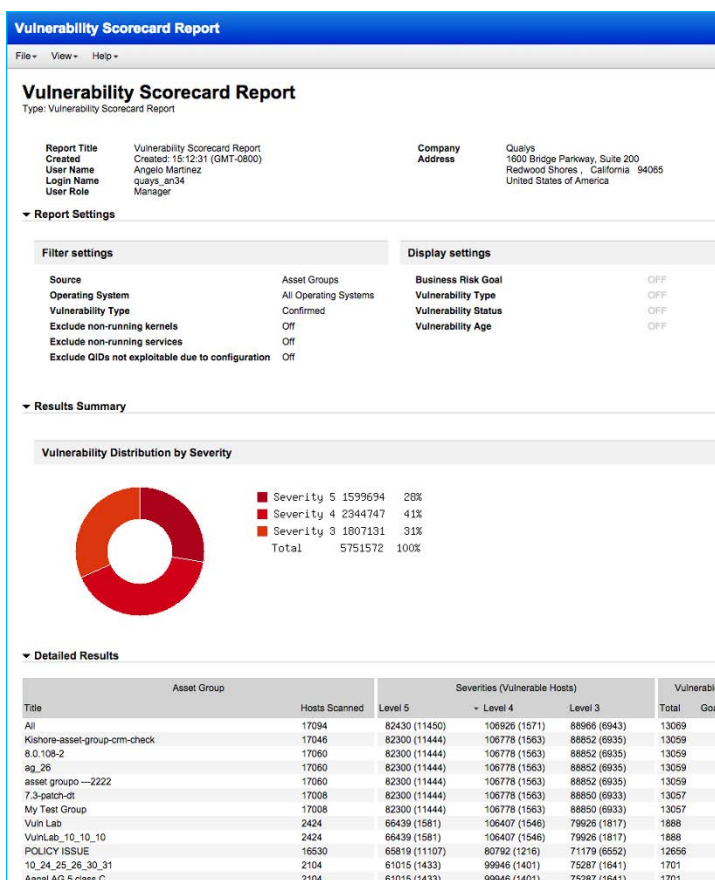


Figure 2-10: A vulnerability scorecard report gives quick security state summary.

that high priority alerts are instantly sent to appropriate first responders for immediate remediation. An example of trouble ticketing assignment is shown in Figure 2-11.



Ensure your VM solution enables the IT security team to analyze remediation trends, including long-term trends in open- and closed-ticket status (that is, solved and unsolved problems). This ability facilitates progress tracking and easy analysis of other security metrics you may have in place.

Figure 2-12 shows an example of ticket status tracking and reporting.

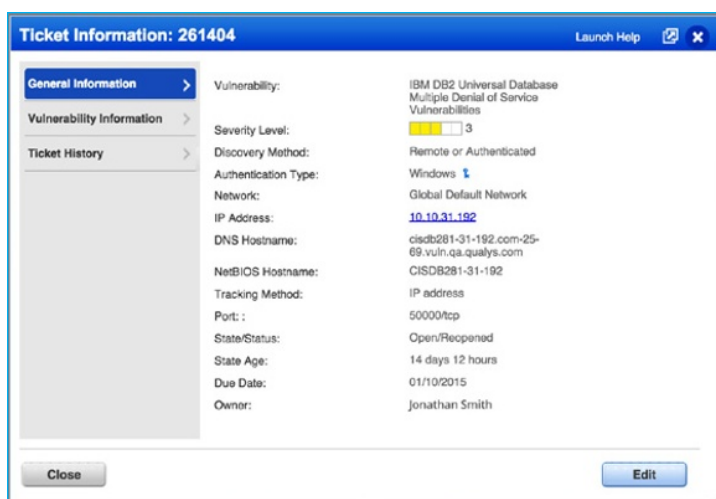


Figure 2-11: One-click assignment of a vulnerability trouble ticket.

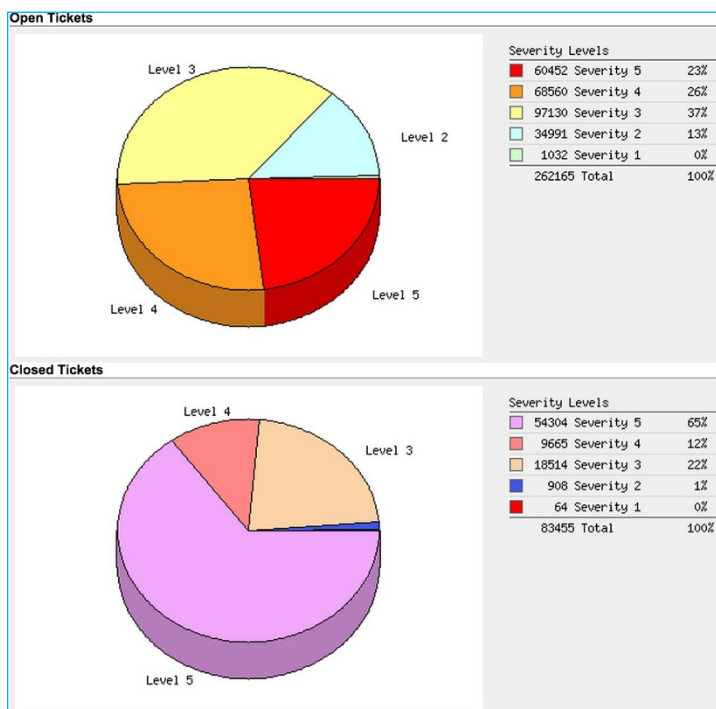


Figure 2-12: Trouble ticket report by severity level.



You can use the notification options of your VM system to keep you apprised of new vulnerabilities as they are published. Modern VM systems allow you to define search criteria to filter for the new vulnerabilities that apply to your installed infrastructure. Look for a system that allows you to define multiple profiles so that the vulnerabilities in question can be sent to the relevant teams – for example, all Windows systems to the operating system team and all Microsoft Office and Adobe application vulnerabilities to the applications team.

Fifth Third Bank case study



Industry: Financial Services

Headquarters: Cincinnati, Ohio, USA

Business: Diversified financial services company

Locations: Operates 15 affiliates with 1,300 full-service banking centers throughout the United States

Employees: 21,000+

Annual Revenue: USD\$6.6+ billion

Total Assets: USD\$303 billion in managed assets

'It's not about being secure the day the auditors show up. It's about being secure and compliant every month, week, day and hour. And Qualys VM helps us to achieve and demonstrate that continuous level of

security and compliance.' – Manager of Information Security Vulnerability Management Team

Objectives:

- ✓ Fifth Third's vulnerability management team, dedicated to keeping 5,000 servers and 30,000 desktops secure, needed to move away from manual-based scanners that only allowed the team to run ad-hoc scans, and lacked the ability to centrally manage vulnerability data or trend the bank's risk management progress over time.
- ✓ The organization wanted to attain more accurate scan results and organize data by business units, system platforms and any other way needed.

(continued)

*(continued)***Results:**

- ✓ Fifth Third has 20 Qualys VM appliances deployed that continuously audit more than 30,000 specific IP addresses automatically throughout the bank's infrastructure.
- ✓ Via Qualys VM's ability to assign highly-specific asset tags (which quantifies monetary value of an asset based on business purpose), the bank can now examine and report its vulnerability

information in any way it needs. The bank can break down its reporting by machine types, business units and many other ways.

- ✓ Fifth Third has improved efficiency via the use of Qualys VM's API to automate report distribution to all IT managers, systems administrators and others.

See www.qualys.com/customers/ for more info and other case studies.

Step 6: Repeating – and Reporting – Continuously

Lest you think the tasks of VM are now done, think again! Continuous VM means the preceding five steps actually are an ongoing process. A continuous loop of VM is necessary for three reasons.



First, in years past, the enterprise network was static and rarely changed. Now, however, corporate and government networks are distributed, complex and highly dynamic with independent operational teams managing and changing configurations to firewalls, routers, switches, load balancers, hosts, applications and other systems. With the consumerization of IT and programs like bring your own device (BYOD), networks now include not just company-owned devices but devices belonging to individuals who don't always follow the same rigid patching and security practices. This presents a significant opportunity for cybercriminals to exploit newly introduced vulnerabilities and infiltrate networks in between scans.



Second, new vulnerabilities in software for devices and applications are discovered every day, which is another source of threats that can exploit operational configurations changing by the minute.

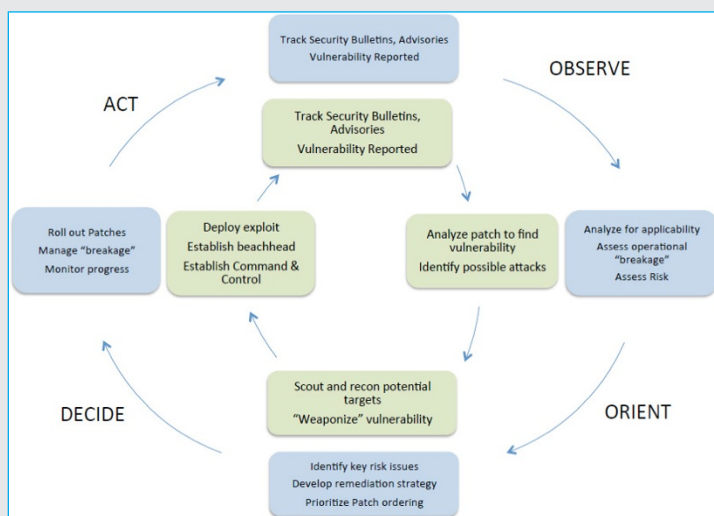
Repeat after me: “OODA”

Here’s a mantra that can help keep cyber criminals away. *OODA* is short for observe, orient, decide and act. The phrase was created by US Air Force Colonel John Boyd and it relates to a strategic approach to combat operations. This four-part process is often called the ‘OODA Loop’ because it is meant to be repeated over and over again.

The OODA concept is applicable to VM because just as a fighter pilot needs to observe, orient, decide and act while fighting the enemy, so do

you as you fight enemy attackers who attempt to break into your network and steal your vital data. Just as the military does OODA in a continuous loop, so do you, but with the steps for VM described in this Part. OODA is an easy way to remember the critical aspect: *repetition*.

Success requires you to complete the loop faster than attackers. The following diagram relates OODA to the steps for VM. Follow these steps continuously, and may the Force be with you!



Third, attackers are leveraging the power of cloud and parallel computing to continuously scan and attack vulnerabilities within your networks and systems, often at speeds that surpass your ability to react. In this new age of cyber crime, it is truly a race to the finish line to see who can identify and patch vulnerabilities quickest.



By continuously doing the steps for VM, your company can keep abreast of new vulnerabilities and immediately take steps to protect the security of your network. Continuous scans are also an important way to ensure the success of your security team's remediation efforts.



For example, after applying a patch or completing the remediation process, be sure to rescan critical assets, as shown in Figure 2-13. This step verifies that the fix worked and that it doesn't cause other network devices, services or applications to malfunction or be exposed to other vulnerabilities.

Reporting compliance with laws and regulations



You've heard all the acronyms: PCI DSS, HIPAA, GLBA, SB 1386, SOX, FISMA, Basel II, COBIT and many more. These are laws, regulations and frameworks that tell a broad range of organizations and disciplines that they must secure personally identifiable information stored in or transferred out of

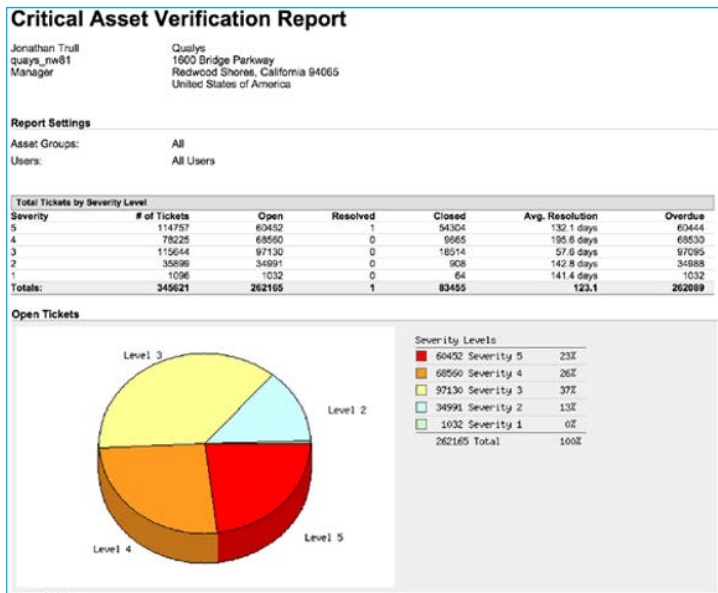


Figure 2-13: VM report on vulnerabilities for critical assets.

Business processes that use data with personally identifiable information are, by nature, IT-intensive. So be prepared for the auditors who'll want to see documentation describing security policies and controls. The auditors will also want to examine documentation that verifies compliance with specific requirements of all relevant laws and regulations. Preparing reports customized to those requirements is where you could spend a substantial amount of time. But guess what? This is where your VM solution can pay off in a big way.

Data used in standard VM reports, such as listing vulnerabilities, severity levels, assets affected, remediation status and history can also be used to satisfy many reporting requirements for security provisions of laws and regulations. Existing reports may suffice, but do check with your VM solution provider to enquire about custom report templates. Some providers offer templates for major laws and regulations that completely automate the process of creating documentation for compliance. Figure 2-14 shows an example of compliance documentation.

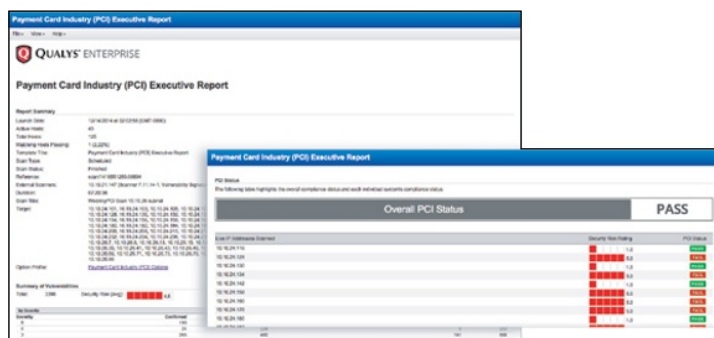


Figure 2-14: A VM report documenting compliance with PCI DSS standard.

Reporting compliance with internal policies

As a bonus, some VM solutions also provide customization features for reports that verify unique internal policy

requirements for an organization. For example, Qualys VM has reports for many laws and regulations, and provides simple customization features for documenting compliance with your business policy, as shown in Figure 2-15. Qualys also offers extensions like these with add-on services such as Qualys Policy Compliance (PC), Qualys Payment Card Industry (PCI) and Qualys Web Application Security (WAS). Either way, a robust reporting capability will reward your efforts at VM with accessible evidence of security and protection. The customization, scope and precision of VM reports also helps to make your IT security department look good to executives running the company.

The Equitable Bank case study



Industry: Financial Services

Headquarters: Southeastern Wisconsin, USA

Business: Provides commercial and consumer banking, finance and mortgage services

Size: USD \$20 million annual revenue, 7 locations

'Qualys VM is wonderful technology. It helps you to quickly determine which vulnerabilities are high-risk and which ones aren't as urgent. For banks, that risk assessment aspect of it is really important.' – VP and IT Officer

Objectives:

- ✓ To find a way to manage growing IT risks and escalating state and

federal regulatory mandates as the community bank grew.

- ✓ To achieve these goals without substantial cost or resource and deployment burdens.

Results:

- ✓ Qualys VM helps The Equitable Bank to automate the full continuous cycle of vulnerability management to protect its network and operations from the latest security threats. Automation has helped the bank achieve its risk management and resource objectives.
- ✓ Qualys Express allows The Equitable Bank to document and submit proof of network security policy compliance to auditors and regulators.

See www.qualys.com/customers/ for more info and other case studies.



Figure 2-15: A security compliance report for financial systems.

Time to Choose a Solution for VM

After reviewing the steps to VM in the preceding sections comes the time to choose a solution that can:

- ✓ Map your network and all its devices.
- ✓ Accurately and efficiently scan for the largest potential number of vulnerabilities.
- ✓ Clearly and comprehensively report scanning results.
- ✓ Shepherd the remediation process, whether through use of the VM ticketing system or integration with your IT organization's system.
- ✓ Test and confirm that vulnerabilities are fixed.
- ✓ Automatically produce accurate, comprehensive and detailed reports and dashboards to verify compliance with internal policies, and legally mandated regulations for security.

- ✓ Help you automatically repeat these steps as part of a continuous, ongoing process to ensure network security.
- ✓ Ultimately, keep you and your security team one step ahead of the bad guys who are constantly looking for vulnerabilities to exploit!

Part III

Considering Your Options for Continuous Vulnerability Management

.....

In This Part

- ▶ Choosing the best path for eliminating vulnerabilities
 - ▶ Paying a consultant for vulnerability assessments
 - ▶ Running open source or commercial VM software yourself
 - ▶ Using a cloud-based VM solution
 - ▶ Comparing the attributes of cloud and traditional VM software
-

Vulnerability management (VM) is critical for every business to prevent mass and targeted attacks that take advantage of weaknesses in your computing infrastructure. VM also helps to demonstrate compliance of your security requirements to auditors.

The steps of VM are fundamental, but so are the ways in which you implement solutions to meet operational requirements. This Part provides preparatory ideas for choosing and implementing continuous VM solutions.

Choosing the Best Path to Eliminate Vulnerabilities

The choice of what solution you implement for VM will directly affect your company's actual state of security and

compliance. As you weigh options for each step of VM, consider these tips:



- ✓ **Automate as much as you can.** Many of the steps to VM are repetitive and applied to all networked devices in the enterprise. Manually doing these tasks consumes an enormous amount of time and resources. Regulatory requirements may require your company to extend VM to suppliers, business partners and channel representatives. There's no way you'll have enough budget and people on staff to do all these steps manually. Automation is a must – not only for affordability and economies of scale, but also to ensure that VM is done in a rapid, systematic and comprehensive manner and that the steps are repeated in a continuous process.

People skilled in security are a scarce resource and shouldn't be tied up in doing manual tasks that can easily be automated; use them when their expertise *cannot* be automated. Examples include deciding the priority of patches and negotiating the proper window to apply those patches. Automated VM can be run with minimal staff involvement, even in large organizations!



- ✓ **Use solid, safe technology.** VM is concerned with preserving the safety and security of your data, applications and network. Don't skimp on the technology required to do the job right. And be especially careful about implementing experimental, unproven solutions into your VM system. When it comes to your business network, systems and data, safer is better than sorry. Stick with VM technology that has a solid track record and wide use in the community.



- ✓ **Chose a solution that grows with your business.** Change is the only certain aspect of business, so check out a proposed VM solution's ability to scale as your organization's requirements grow more complex and demanding. It's one thing to secure a few machines or a small department; it's another to coordinate VM with multiple departments, divisions, business units, and independent business partners – domestic and global.

With that, the following sections look at a few options for implementing a continuous VM solution.

Option: Paying a Consultant

Consultants are a great resource to assist you in protecting your network and are experts in identifying weaknesses. However, there's a big difference between continuous VM and simply identifying issues or proving there are weaknesses. Many consultants perform what's called *vulnerability assessment*, which means they try to find vulnerabilities and prioritize their ranking. A couple of comprehensive vulnerability assessments per year might cost tens or even hundreds of thousands of dollars. A vulnerability assessment test captures in-depth vulnerability information at a single point in time. The results of this test might be adequate for specific compliance instances with a regulation, but providing ongoing, reliable security is a different matter.



The shelf life of a point-in-time vulnerability assessment is fleeting:

- ✓ Results are valid only until the environment changes or until new threats arise – which is daily!
- ✓ Results are accurate for a day at best. In typical companies, administrators reconfigure networks and devices every day. Also, new vulnerabilities are found daily and vulnerability assessments are quickly outdated. If you want VM to help strengthen security, it's more appropriate to do consistent, daily scans.
- ✓ Regular assessments quickly become too expensive to outsource for manual processing by vulnerability assessments testing consultants.



Continuous VM is relatively easy when you use an automated solution, so you may want to aim additional resources on fixing any issues detected. Remediation of vulnerabilities can often be time consuming, so consultants can provide great value in assisting you in this complex task.

Penetration testing vs. vulnerability assessments

Penetration testing, or pen testing, takes vulnerability testing one step further. After scanning for vulnerabilities, a consultant also exploits them to gain access to a machine. In this way, pen tests can be useful in demonstrating that vulnerabilities create real weakness in your corporate infrastructure, allowing an attacker to install malware and steal internal, proprietary information.

Carry out pen testing after implementing a vulnerability management program. The Council on CyberSecurity recommends pen testing as Priority 18, whereas vulnerability management is listed as Priority 4. Ask pen testers for yourself; most will agree that if you already have a VM program, using a pen test is of very limited value.

Option: Run Software Yourself

Software-based solutions enable you to install software for vulnerability management on your internal network and run them yourself. Software can automate many of the processes for needed continuous VM. However, running your own VM system software carries the usual price tag of having to manage and secure another software system. You have to operate and maintain a full hardware and software stack on multiple machines in between everything else on the usual IT and security person's daily list of things to do.

Tasks for running and maintaining VM software include:

- ✓ Buying and maintaining the servers and infrastructure to reliably run the VM software applications.
- ✓ Ensuring the VM applications and infrastructure are always 100 per cent secure and performing at peak operational efficiency.
- ✓ Integrating the required data exchange between component software used for VM solutions.
- ✓ Keeping software maintenance up-to-date with the latest updates and patches from each vendor.
- ✓ And, of course, continuously responding to alerts and managing the vulnerabilities spotted by your system.

Do-it-yourselfers have two choices. You can download Open Source software or buy commercial solutions.

Open Source software: Often free, but not cheap

Open Source software is developed in an open, collaborative manner. The software is often free, and users are able to use, change, or improve it, and share it. However, two considerations about Open Source software need to be taken into account for VM:



- ✓ **Open Source software may be free but it's not inexpensive.** Open Source software carries the same operational costs as commercial software. Be ready to pay for equipment space, rack and air conditioning, system administration, deployment and configuration, maintenance and patching (if and when they arrive from community developers), backup and restore, redundancy, failover and uninterrupted power, audit logs, provision for VM application security and maintenance, capacity planning and event monitoring. The list goes on!
- ✓ **Training and support is skimpy.** Your security staff must know how to operate tools and capabilities of VM – and how to quickly eradicate vulnerabilities found on the network. With Open Source software, it's rare to find packaged training and support information together from Open Source forums on the Internet. While many experts collaborate on sharing their tips, it helps to know the people who program the software because they're often the only source of information – especially for Open Source modules or plug-ins that may not work as described. When you rely on Open Source for VM, gurus are essential for handling technical aspects of the job.

Commercial software: Initial cost plus maintenance

The other option for running VM software yourself is to use commercial software. Most of us automatically think

of commercial software as a 'safe' option, and it usually constitutes the bulk of installed applications. But commercial software has its drawbacks, so consider these points:



- ✓ **Commercial software costs real money.** You have to buy it, and that requires budget, process and paperwork to convince the boss to sign the purchase order.
- ✓ **You must pay every year for the right to receive updates and support.** Updates are crucial for the security of any software products but doubly so for continuous VM, which depends on daily updates for accurate assessments.
- ✓ **Maintenance brings higher assurance, but you still need to check for yourself.** A commercial venture should be developing the VM software with industry standards for software assurance and security. Ask your vendors about how they do this. On the other hand, mistakes are virtually assured in any software application so you must regularly and rapidly install updates and new patches. Find out how that process works and how you'll have to integrate it with your internal process for updates and patching. Check on the provider's training and support programs to ensure that your security staff will be able to deploy and use the solution.
- ✓ **Commercial software costs the same to run as Open Source solutions.** Be ready to pay for the same long list of things that you'd have to pay for with Open Source.

Option: Use a Cloud Solution



Cloud-based solutions have become a mainstream way to use software solutions and many organizations follow a 'cloud-first' policy. They know firsthand the advantages that come with cloud applications – such as fast implementation, low maintenance and pay-as-you-go – which offer the best solution for solving their business problems.

Cloud-based solutions can take many forms; they typically focus on infrastructure, platform or entire applications. The applications-focused model is called Software-as-a-Service (SaaS) and has been proven successful in many areas such

as sales automation, email and security. With SaaS, vendors have specialized teams that operate entire applications for you. These applications run in a multi-tenant architecture that is always updated and offers plenty of computing capacity to spare. Users access the application with a browser over the Internet.

A variety of cloud applications include customer relations management, office productivity, human resources, videoconferencing and accounting. A cloud provider handles all the technical ‘heavy lifting’ of infrastructure behind the application and you can use it right away without requiring special technical expertise or training to deploy and use it. No gurus needed either!

Qualys was the first company to offer VM as a cloud solution and is the global leader in providing continuous security with its cloud service called Qualys VM. Qualys VM provides vulnerability management, policy compliance and other security services with the Qualys Cloud Suite and a platform performing more than one billion scans and audits per year for thousands of customers around the globe.

Comparing Cloud to Traditional Software for Continuous VM

Organizations can deploy VM in several ways. Some do it themselves by purchasing, deploying and managing software-based VM products. Some hire consultants to do vulnerability assessments, who often use the same software-based products that hiring organizations could run themselves. A growing number are turning to a proven alternative: doing continuous VM with a cloud solution.



As you choose a VM solution, weigh the pros and cons of each against four key factors: Design, Deployment, Management, and Compliance. Each of these plays a crucial role in determining successful deployment of VM.

Design: Assessing risk from the outside, looking in

Software-based solutions are installed by users on their enterprise network and operated manually. This is a familiar process but using software-based solutions for VM has huge drawbacks:



- ✓ Software-based solutions don't provide an outsider's view of network vulnerabilities, especially for devices on the perimeter.
- ✓ Installation options are either on the non-routable private side of the network or on the public-facing Internet side. Behind-the-firewall deployments are unable to process exploits such as transmission of incorrectly formatted data packets so their scans generate many false positives and false negatives. Products deployed outside the firewall are subject to attacks and compromise. Secure communications of scan assessments are questionable.

With a cloud solution, however, the application is installed and operated by a trusted third party and has scanner appliances connected on the organization's network and at secure external facilities. The latter option enables the cloud VM solution to mimic the perspective of a hacker during the network audit process and from the outside, looking in. Scan data from inside the firewall is generated from the hardened scanner appliances and sent to the cloud platform where it is integrated with the external audit data.

Deployment: Keeping operational burdens to a minimum



When organizations deploy software-based solutions, they need to provide servers to run the VM application. For large enterprises, this may require servers in multiple data centers worldwide, so deployment can consume a lot of time as IT staff rolls out the required infrastructure and network engineers configure communication paths in their firewalls.

Smooth integration of these resources with enterprise management platforms is often challenging, if not impossible.

A cloud solution, however, has many operational advantages:

- ✓ Cloud is already ‘up and running’ so deployment is instant, no matter how many sites need VM, and no matter where they are in the world.
- ✓ Cloud covers mobile workstations with Internet-connected agents that provide continuous visibility.
- ✓ Cloud is inherently scalable and immediately begins working for the largest enterprise.
- ✓ Cloud solutions typically provide an API allowing for simple integration with enterprise network management platforms.

Management: For an effective, low-cost solution

Software-based solutions require substantial overheads for VM. In large-scale deployments, scan results are dispersed across multiple network segments and devices, so collating for an enterprise-wide view of vulnerabilities is a long manual process. Software updates and patches must be applied on every distributed node, which also require hardware maintenance and backup.



VM with a cloud solution, however, eliminates all these issues:

- ✓ Secure cloud hosting means that updates are automatic and instant for the entire enterprise.
- ✓ Enterprise-wide collation of vulnerability data is automatic.
- ✓ The total cost of ownership (TCO) is lower with cloud due to the elimination of manual deployment, management and reporting.

Compliance: Audits and reports for a variety of policies and regulations

Demonstrating compliance with software-based solutions is difficult. In addition to manually collating reports, the data is ‘owned’ by the user and so is subject to extra scrutiny and skepticism by auditors. By contrast, fully automated cloud vulnerability reporting is trusted by auditors because it’s collected and held by a secure third party. Cloud provides tamper-proof capability by enforcing access to VM functionality and reporting based on a user’s operational role in an organization. This role-based capability further protects the integrity of VM results for verification of compliance.

Part IV

Using Qualys VM: Continuous Vulnerability Management

In This Part

- ▶ Providing continuous VM with the cloud
 - ▶ Speeding follow-through with prioritized remediation
 - ▶ Automating document compliance
 - ▶ Keeping costs to a minimum
 - ▶ Trying Qualys VM for free
-

The growing deluge of documented data breaches has spurred a considerable amount of rethinking within computer security circles. Virtually all industry analysts now agree that computer security should be based on multiple layers and that fast remediation of exploitable vulnerabilities is of critical importance. The independent Council on CyberSecurity's *Critical Security Controls* recommends that to be successful a security strategy should involve accurately configuring software applications, rapidly patching software vulnerabilities and keeping software updated. This is where Qualys comes in.

Qualys VM is a cloud-based continuous vulnerability management (VM) solution, part of the Qualys Cloud Suite – a scalable security platform that offers other solutions in relevant fields, such as PCI, Web Application Security, Policy Compliance, Malware detection and more. It plays a vital role in computer security and supports related requirements in compliance management.

Discovering Continuous VM

Whereas non-cloud-based VM involves acquiring, installing, supporting and maintaining a software-based solution, cloud-based continuous VM brings in a trusted third party, such as Qualys VM.

Industry experts define VM to include the following criteria. Continuous VM should:



- ✓ Identify both external and internal weaknesses.
- ✓ Automatically scan using a continually updated database of known attacks.
- ✓ Be highly accurate, essentially eliminating false positives and false negatives – and be non-intrusive.
- ✓ Use inference-based scanning to ensure that only applicable vulnerabilities are tested for each scan.
- ✓ Generate concise, actionable, customizable reports, including vulnerability prioritization using severity levels and trend analysis.
- ✓ Provide tested remedies and workarounds for cases where no remedy as yet exists.
- ✓ Provide distributed scanning capabilities with consolidated reporting and centralized management capabilities.
- ✓ Offer both authenticated (credential-based) and simple non-authenticated techniques for scanning.
- ✓ Provide user access management to restrict users' roles and privileges to their function in the organization and network responsibility.
- ✓ Supply workflow capabilities for prioritizing and tracking remediation efforts.
- ✓ Enable customers to build compliance reporting.
- ✓ Integrate seamlessly with customers' Security Information & Event Management (SIEM), Intrusion Detection System (IDS), patch management and help desk systems.
- ✓ Automatically execute the steps of VM in a continuous, ongoing process.

That's a lot of requirements, but Qualys VM meets every one of them with its cloud architecture and easy-to-use user interface.

Accessing Qualys VM

Users access Qualys VM by simply logging in via a web browser. By using this standard approach to access its web service-based delivery architecture, Qualys VM users can immediately use the service and audit the security of their external and internal networks. Continuous VM services with Qualys VM are available 24x7 to all subscribers worldwide.



With Qualys VM you can schedule scans to occur automatically, including selected scan targets, start time, duration and occurrence frequency.

Continuous VM features in Qualys VM provide a broad array of capabilities for finding and eliminating network vulnerabilities. Qualys VM:

- ✓ Discovers all systems attached to your network.
- ✓ Identifies and analyzes vulnerabilities on all discovered systems.
- ✓ Reports findings of discovery and vulnerability analysis.
- ✓ Shepherds the vulnerability remediation process.
- ✓ Confirms that remedies or workarounds have been applied.
- ✓ Provides documentation to verify security compliance.
- ✓ Automatically repeats the VM-for-continuous-protection steps.
- ✓ Alerts on variances from expected configurations in vulnerabilities, exposed services, installed software and certificates.

Elements of Qualys VM's architecture in the Qualys Cloud Platform (which you can see in Figure 4-1) include a KnowledgeBase, Security Operations Centers, Internet scanners, scanner appliances and a secure web interface.

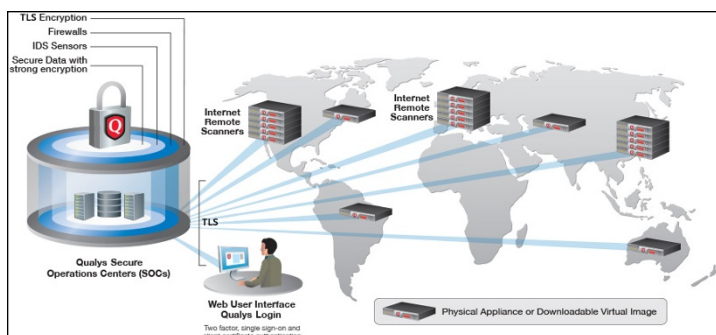


Figure 4-1: Qualys VM's cloud-based architecture.

KnowledgeBase

The core of Qualys VM is its KnowledgeBase. KnowledgeBase contains the intelligence that powers the Qualys VM continuous vulnerability management service. It's updated daily with signatures for new vulnerabilities, validated patches, exploit usage indicators and other data that continuously improves its effectiveness.

Security Operations Centers



The KnowledgeBase resides inside Qualys Security Operations Centers (SOCs), which provide secure storage and processing of vulnerability data on an n-tiered architecture of load-balanced application servers. That's computer-speak for the ability to expand processing power to meet customer demand simply by adding more servers. All computers and racked equipment are isolated from other systems in a locked vault.

Internet scanners



Qualys VM Internet scanners carry out perimeter scanning for customers. These remote scanners begin by building an inventory of protocols found on each machine undergoing an audit. After discovering the protocols, the scanner detects which ports are attached to services, such as web servers, databases and e-mail servers. At that point, the scanners initiate an *inference-based* vulnerability assessment, based on vulnerabilities that could actually be present (due to operating system and configurations) to quickly identify true vulnerabilities and minimize false positives.

Scanner appliances

To map domains and scan IPs behind the firewall, Qualys VM Scanner Appliances are installed by customers. These are either virtual or physical devices that install within a matter of minutes, gather security audit data inside the firewall and communicate securely with Qualys SOC's. These appliances use a hardened operating-system kernel designed to withstand attacks. In addition, they contain no services or *daemons* (background software processes) that are exposed to the network. These devices poll the SOC's for software updates and new vulnerability signatures, and process job requests.

Secure web interface

Users interact with Qualys VM through its secure web interface. Any standard web browser permits users to navigate the Qualys VM user interface, launch scans, examine audit report data and manage the account. Secure communications are assured via HTTPS encryption. All vulnerability information, as well as report data, is encrypted with unique customer keys to guarantee that your information remains confidential and makes the vulnerability information unreadable by anyone other than those with proper customer authorization.

Prioritizing Remediation to Guide and Speed Up Staff Follow-Through

Qualys VM provides a remediation ticketing capability similar to trouble tickets created by a support call center. As the security manager, you can control the priority-driven policies for these tickets and automatically assign responsibility for fixing them. Qualys VM notes when tickets have been created, and tracks all remediation changes in subsequent scans. The automation of these processes can dramatically speed remediation of vulnerabilities.



Reports from Qualys VM automatically identify and rank vulnerabilities with the Qualys VM Scanning Engine. This engine assigns one of five severity levels to define the urgency associated with remediating each vulnerability. Rankings are based

on a variety of industry standards such as CVE and NIST. These levels are:

- **Level 1 (minimal):** Information can be collected.
- **Level 2 (medium):** Sensitive information can be collected, such as precise version and release numbers of software running on the target machine.
- **Level 3 (serious):** Indications that threats such as directory browsing, denial of service or partial read of limited files have been detected.
- **Level 4 (critical):** Red-flag indications that file theft, potential backdoors or readable user lists present on target machines have been discovered.
- **Level 5 (urgent):** Backdoor software has been detected, or read-and-write access on files, remote execution or other activities are present.

Details for each vulnerability are displayed in a report, as shown in Figure 4-2:

Qualys VM also provides an Executive Report, which summarizes the status of repair for all vulnerabilities.

Detailed Results

10.10.30.100 (10.10.30.100) vuln.qualys.com, RHLS4-30-100) Linux 2.4-2.6 / Embedded Device / FS Networks BigIP

Vulnerabilities (19)

4 Remote User List Disclosure Using NetBIOS

QID: 40033 **Category:** Information gathering **CVSS Base:** 5 **CVSS Temporal:** 4.5

Vendor Reference: CVE-2009-5009

Regnum ID: 809

Service Modified: 01/01/2014

User Modified: -

Edited: No

PCI Vult: Yes

Ticket State: -

THREAT:
A null session connection to the IPCS share was successful. NetBIOS access can be obtained with any authenticated account on the host. Therefore unauthorized users can steal the remote user list. This kind of attack is commonly exploited by users with weak passwords, such as the GUEST account.
Please note that the QID is passed when Qualys is able to enumerate the user-list of a target via the 'net' API functions (in which case QID 79003 is posted as well), or when Qualys is able to 'brute-force' known SIDs via LocalLookupids (in which case only QID 40033 is posted).
While both techniques use anonymous NetBIOS sessions, we are unaware of a system-level fix for LocalLookupids, as Microsoft considers this to be requisite functionality.

IMPACT:
By exploiting this vulnerability, unauthorized users can launch brute force password attacks and other intrusive attacks based on collected information. Employees, customer, and partner information may be gathered. Spawning the user list is also possible.

SOLUTION:
It is recommended that you disable null sessions.

Before editing any configuration file in a production environment, the changes should be well tested in a rehearsal environment.

Read the Microsoft documents called [How to Use the RestrictAnonymous Security Value](#) and [Restricting Anonymous Access](#) for more information. If this vulnerability was discovered on a domain controller, please note that some of the recommended settings may not have any effect. Read the Microsoft article [Deprecation of Certain Permissions Choices](#) for more information regarding Pre-Windows 2000 Compatible Access.

For Windows NT, setting this registry value limits only certain interfaces to this data. It is not possible to completely eliminate this vulnerability through a registry setting.

There is another interesting Microsoft document called [Local Lookupids](#) about Windows security policies settings for local policies.

Windows XP onwards Microsoft has added more granular control to the anonymous user access by adding a group of more DWORD registry values in the same key location as RestrictAnonymous.

RestrictAnonymousdirm = 1 to restrict share information access. RestrictAnonymousdirm = 1 to prevent enumeration of SAM accounts (User Accounts) and EnumerateUsersAnonymous = 1 to prevent null sessions from having any rights. Setting the RestrictAnonymous value to 1 restricts null session access to unauthorized users to all server pipes and shares except those listed in the NullSessionPipes and NullSessionShares entries. Additionally set HKLM\LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters, NullSessionPipes and NullSessionShares, to a null string.

For Samba servers there is no direct way of disabling null session access. A workaround is to specify a non existing UNIX account in global section of Samba config file, guest account = NON EXISTING USER.

Adding 'restrict anonymous = 2' in smb.conf can help resolve the issue.

Figure 4-2: Qualys VM individual vulnerability report.

Automating Compliance Documents for Auditors



One area that distinguishes Qualys VM from other VM solutions is its very flexible, comprehensive and intelligent reporting capability. Most other solutions produce rigid reports that reflect, one-for-one, whatever data they gathered during a scan. Few, if any, mechanisms can filter, regroup or synthesize the data into higher levels of information abstraction. Qualys VM reports, however, are like quality business intelligence reporting and come with filtering and sorting that enables you to view data any way you want.

Components of Qualys VM reporting are:

- ✓ **Network assets** (IPs and/or asset groups) included in the report.
- ✓ **Graphs and charts** showing overall summaries and network security status.
- ✓ **Trending analysis** for a given network.
- ✓ **Vulnerability data** with detailed specificity.
- ✓ **Filtering and sorting options** to provide other flexible ways to view your network's data.

The Qualys VM Dashboard provides an instant one-page snapshot of your network's overall security position, as you can see in Figure 4-3.

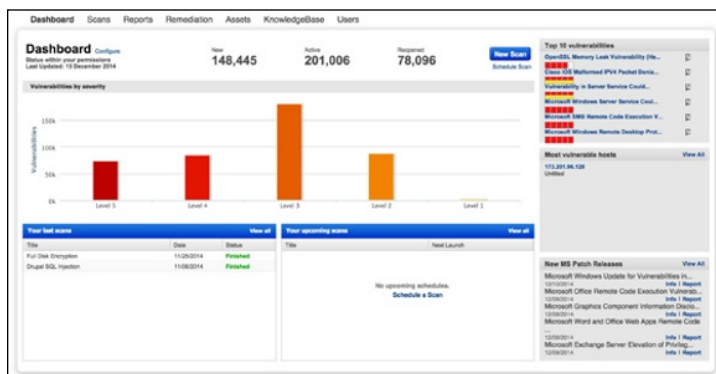


Figure 4-3: Qualys VM Dashboard.

The Dashboard is a portal to more detailed reports that describe each aspect of VM processes. Qualys VM provides a range of report templates that automatically present VM data and information synthesis typically required by an IT organization for vulnerability remediation. You can easily customize the templates to display specialized reports, formats (such as HTML, XML and PDF) and associated distribution to appropriate staff members, executives and auditors.

For example, customizable templates automatically generate reports such as:

- ✓ Unremediated vulnerabilities with the highest level of severity.
- ✓ Rogue devices discovered on the network.
- ✓ Technical compliance with a specific regulation, such as requirements of PCI DSS.
- ✓ Trouble-ticket status for a particular department or business process, such as a financial reporting system or an order processing system.
- ✓ Trend analysis for use in job performance appraisals of network security staff.

Ease of integrations

Qualys' open, XML-based application programming interface (API) platform is unique in the security industry. The APIs programmatically expose core Qualys VM capabilities, including scan, map, scheduler, ticketing, account management and references. This allows Qualys VM to easily interface with other security and network management applications.

In addition to viewing reports with Qualys' web-based interface, as a customer you can manually or programmatically export your vulnerability data and scan results/reports in XML format using Qualys VM's open,

published API specifications. These capabilities are used in a number of current and in-process third-party integrations, including support for the leading firewall and intrusion detection system (IDS) providers.

Qualys VM's IDS integrations enable enterprises to automatically correlate ongoing attacks with actual target host vulnerabilities, reducing false alarms.

Qualys VM also integrates with vulnerability remediation systems and help-desk solutions to automatically trigger the assignment and tracking of remediation.

Keeping the Costs Down



Qualys VM is cost-effective thanks to automation, which saves both small- and medium-sized businesses and large, multinational organizations a huge amount of time compared to the manual execution of continuous processes for VM. Qualys VM's secure architecture is updated daily with new vulnerability audits, and quarterly with new product features. All updates are done seamlessly to subscribers. The costs of ownership are assumed by Qualys and distributed across a large subscriber base. Users benefit from an immediately deployable VM capability at a far lower cost compared to using an internal, software-based solution.

Contrasting cloud-based audits against costly vulnerability assessments

Vulnerability assessment is the term for computer security auditing performed by outside consultants. Essentially, the consultant identifies vulnerabilities and prioritizes them for your organization. While a vulnerability assessment captures vulnerability information at a single point in time, however, its shelf life is fleeting and the results are valid only until the environment changes or until new threats arise. In short, vulnerability assessments are literally valid for just days. With network administrators reconfiguring networks and devices daily, and vulnerabilities emerging at the rate of 25+ per week, computer security requires frequent, continuous assessment.



Another computer security discipline called *penetration testing* is a supplement to VM. Penetration testing executes an attack against found vulnerabilities and gives computer security teams a change to exercise their defensive and detection capabilities. The Council on CyberSecurity, a non-profit standards organization with a strong bias towards practical solutions, ranks pen testing at number 18 in its Top 20 cybersecurity activities and VM is ranked number four. Talk to pen testers about their services and they will confirm that it makes little sense to test the security of an

organization while known, exploitable vulnerabilities exist in its infrastructure.

Cloud-based vulnerability assessments are the ideal supplement to or replacement for penetration tests. Qualys VM provides subscribers with unlimited assessments – daily if required – at a fraction of the cost of one penetration test. Differential reporting and trend analysis is automatically included so you can measure your security improvements over time.

Helping to continuously monitor your network perimeter

The automation of Qualys VM provides your company with continuous VM. This capability is automatically integrated with another offering from Qualys, called Qualys Continuous Monitoring (CM).

Qualys CM is a broader service that provides your company with a comprehensive, always-on view of potential security holes affecting the entire enterprise network perimeter, empowering you to immediately identify and proactively address potential vulnerabilities before they turn into breaches. Built on the Qualys Cloud Platform, Qualys CM uses its elastic scanning capacity to dynamically scale to networks of any size and scope. The key benefit is first responders on operational teams are alerted as soon as an unauthorized change is detected. (See the ‘Qualys Cloud Suite’ sidebar for more information about Qualys CM and other Qualys services and Part V for an in-depth look at how CM boosts the odds of protecting your IT environment from attacks.)

Counting the Qualys VM subscriber benefits

Qualys VM is designed to operate effectively on diverse networks of any size. It’s the first scalable, cost-effective SaaS application providing proactive security audits inside and outside the firewall.

Qualys VM enables total control over the security audit and VM process, including:

- ✓ Easy deployment with the Qualys VM cloud architecture.
- ✓ Ability to easily manage continuous VM, no matter how large your network may be.
- ✓ A fully-automated, always-updated solution that eliminates traditional labor-intensive operations, saving time and simplifying large-scale VM.
- ✓ Rapid identification and visualization of network assets.
- ✓ Accurate vulnerability detection that eliminates the time-consuming, manual work of verifying results and consolidating data.
- ✓ Accessible VM service to authorized users from anywhere on the globe.

Trying Out the Free Trial and Four-Step VM Program

Now that you're familiar with the basics of VM, it's time to do it for real. You can benefit from a free, seven-day trial of Qualys VM. All you need to use it is a web browser. Go to www.qualys.com/freetrial and get started!

After registering, you receive an e-mail with a secure link to your user name, password and initial login URL. After checking the terms and conditions, you see a welcome screen that looks like Figure 4-4:

The welcome window guides you through the essential VM steps for auditing your external network (perimeter). You need a brief set-up to use Qualys VM. First time through, keep it simple and enter your network's top-level domain ID. Later, you may want to try domains, asset groups and related business units to experience the full power of Qualys VM.

Step 1: Mapping your network

After you've set up Qualys VM, go to the section called Map, click on 'Start a Map' and do it! This automatically analyses

your network and generates data for all devices attached to the IP or range of IPs that you stated in set-up.

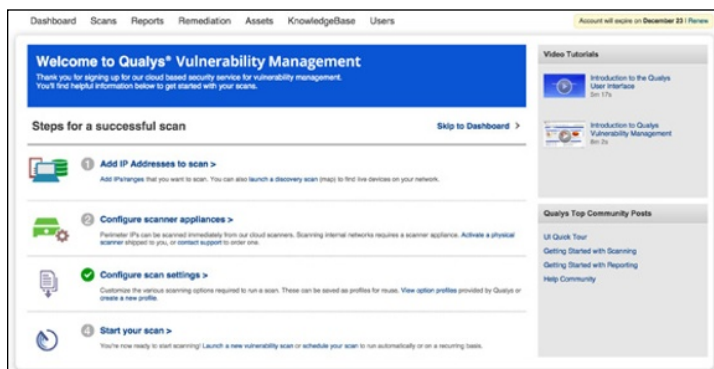


Figure 4-4: The Qualys VM welcome screen.

Step 2: Scanning your network

Once the map is created, you can scan all devices on your entire network or a designated subset of those devices. To do this, go to the section called Scan, click on 'Start a Scan' and do it!

Step 3: Generating scan reports

Reports are the key deliverable of Qualys VM, and are the best and most comprehensive in the industry. To automatically generate reports, go to the section called Report. First, tell Qualys VM what kind of reports you want for Scans and Maps. Next, click on 'Run Reports'. That's it.

As you familiarize yourself with the easy-to-use interface of Qualys VM, you may want to explore generating various other reports and trying more comprehensive Qualys VM functionality.

Step 4: Remediating risks

This step is where your work begins as you need to implement fixes for issues detected. Don't worry – Qualys VM can

guide you through the remediation process. When it tells you about vulnerabilities, Qualys VM also provides hotlinks to remediation patches, fixes and workarounds. It tells you what to fix first based on business priorities and severity levels. And, by rescanning, Qualys VM can verify that these vulnerabilities have been properly corrected.

Congratulations! You're now ready to reap the benefits of VM for a secure, protected network. Going on to use Qualys VM on a regular basis will help to ensure maximum safety and security of your network, applications and data.

If you have any questions, contact Qualys at www.qualys.com and we'll be happy to respond.

The Qualys Cloud Suite

The Qualys Cloud Suite provides a broad range of cloud-based security and compliance solutions for organizations of all sizes.

Network security

VM – Qualys Vulnerability Management (the theme of this book) is a cloud service that gives you immediate, global visibility into where your IT systems might be vulnerable to the latest Internet threats and enables you to protect against them. It helps you to continuously secure your IT infrastructure and comply with internal policies and external regulations.

Perimeter monitoring

CM – Qualys Continuous Monitoring is a next-generation cloud service that gives you the ability to identify threats and unexpected changes in your Internet perimeter before they turn into breaches. With it, you can track what happens within

Internet-facing devices throughout your 'demilitarized zones' (DMZs) and cloud environments anywhere in the world. CM brings a new approach to VM and network security, enabling you to immediately identify and proactively address potential problems such as unexpected hosts/OSes, expiring secure sockets layer (SSL) / transport layer security (TLS) certificates, inadvertently open ports, severe vulnerabilities and undesired software.

Compliance

PC – Qualys Policy Compliance is a cloud service that performs automated security configuration assessments on IT systems throughout your network. It helps you to reduce risk and continuously comply with internal policies and external regulations.

PCI – Qualys PCI Compliance provides businesses, online merchants and Member Service Providers the

(continued)

(continued)

easiest, most cost-efficient and highly-automated way to achieve compliance with the Payment Card Industry Data Security Standard. Known as PCI DSS, the standard provides organizations with the guidance they need to ensure that payment cardholder information is kept secure from possible security breaches.

Web application security

WAS – Qualys Web Application Scanning is a cloud service that accurately and efficiently tests your web applications no matter where they are – on internal networks, hosted on the Internet or in cloud platforms such as Amazon. Qualys WAS allows organizations to proactively scan their websites for malware, providing automated alerts and in-depth reporting to enable prompt identification and eradication of malware. It enables organizations to protect their customers from malware infections and safeguard their brand reputations. Relied on by leading companies with some of the most demanding web apps in the world, Qualys WAS will help you safeguard your apps, whether you have just a few or thousands.

WAF – Qualys Web Application Firewall is a next-generation cloud service that brings an unparalleled combination of scalability and simplicity to web app security. Its automated, adaptive approach lets you

quickly and more efficiently block attacks on web server vulnerabilities and app security defects, prevent disclosure of sensitive information and control where and when your applications are accessed.

Q – Qualys SECURE Seal enables businesses of all sizes to scan their websites for the presence of malware, network and web application vulnerabilities, and SSL certificate validation. Once a website passes these four comprehensive security scans, the Qualys SECURE Seal service generates a Qualys SECURE Seal for the merchant to display on their website, demonstrating to online customers that the company is maintaining a rigorous and proactive security program.

Desktop/Browser Security

Qualys BrowserCheck is a fast way to check if your browser and plugins are up to date with the latest security patches. Qualys BrowserCheck is a free service offered as a Personal Edition for individuals and Business Edition for an organization.

Qualys Top 4 Security Controls is a free service that lets you verify if your Windows PCs are implementing the Top 4 security controls noted by the Council on CyberSecurity: application whitelisting, application patching, OS patching and minimization of administrative privileges.

Part V

Embracing Continuous Monitoring

In This Part

- ▶ Distinguishing the relationship between VM and CM
 - ▶ Perusing examples of some results of using Qualys CM
 - ▶ Forging an always-on approach to security with Qualys CM
-

Misconfigurations and new vulnerabilities appear on a daily basis – and may immediately expose a computer or network device to attacks. These dangers make the job of defending networks an urgent priority for organizations.

In a perfect world, your network would have an always-on, continuous dashboard of your global perimeter to handle this responsibility and network security controls that have the ability to automatically identify and alert on any attack, prevent operational interruptions and protect the confidentiality, integrity and availability of critical applications and data. Achieving this state is the Holy Grail of security; continuous monitoring (CM) – which will detect threat actors who can launch sophisticated attacks from any global location at any time – is a vital step toward accomplishing this goal.

This Part describes the need for CM and offers a blueprint for creating a continuous security practice. As a result as implementing it, CM will give your organization the most comprehensive view of its global perimeter and empower you to proactively identify and address potential threats enabled by vulnerabilities in software or weak system configurations.

Understanding Continuous Monitoring and Vulnerability Management

Qualys Continuous Monitoring provides organizations with a comprehensive, always-on view of potential security holes, empowering them to immediately identify and proactively address potential vulnerabilities before they are exploited into breaches. Built on the Qualys Cloud Platform, Qualys CM uses its elastic scanning capacity to dynamically scale to networks of any size and scope.



The key benefit of Qualys CM is that it instantly alerts first responders on operational teams as soon as an unauthorized change is detected.

A deep, symbiotic relationship exists between continuous vigilance and alerting aspects of Qualys CM and the assessment and remediation aspects of Qualys Vulnerability Management (VM). Cyber threats may consist of software-borne threats, such as exploits that install worms, viruses and ‘drive-by’ infections from malware on websites; they also may target internal issues such as those related to bad configurations of your IT environment. Responding to threats from both scenarios requires the integration of continuous monitoring *plus* assessment and remediation.

The whole idea of continuous monitoring hinges on the availability of timely, accurate data about your IT environment, including information about changes to systems and configurations that expose new vulnerabilities. These data are automatically collected and analyzed during scans. CM is the next step of immediately putting this information into the hands of first responders for judgment and action.

Transforming the old model



Qualys CM transforms the old scanning-and-report driven process by parsing scan results by your criteria and automatically alerting appropriate first responders with specific information tailored for the respective assets assigned to

their responsibility. The old way entailed passing a big, often arcane report through a bureaucracy of managers, supervisors and technicians. As a result, the velocity of remediation was often way behind the threats that were appearing by the minute.



In contrast, Qualys CM sends ‘Twitter-like’ bursts of essential information quickly into the hands of the right people for immediate and targeted action. This service accelerates the ability of first responders to stay ahead of threats to the most important assets. Qualys CM lets you granularly control the intervals and targets of notification.

Scanning frequently: making CM effective



The frequency of vulnerability scanning is what fuels the effectiveness of alerts by Qualys CM. For example, if you scan once a quarter or even once a month, having the ability to ‘continuously monitor’ data from those scans is hardly up-to-date when vulnerabilities change by the minute on a giant, fluid attack surface. Given the continuous change in threats, Qualys suggests scanning your network at least daily, and *continuously* for critical, high-priority assets. As a result, vulnerability scanning data will truly be up-to-date, which enables Qualys CM to be a useful and vital component of keeping your network safe from exploits.

Critical Security Controls and continuous monitoring

The Council on CyberSecurity offers explicit guidance on continuous monitoring in its *Critical Security Controls*. The CSCs (formerly known as the ‘SANS 20 Critical Controls’) are a prioritized, risk-based approach to cyber security. They are the result of a consensus process that involved

a wide variety of cyber security professionals from government and industry who were asked: ‘In practice, what works and where do you start?’ The CSCs are a blueprint for helping you to secure your computer systems from risk.

(continued)

(continued)

For continuous monitoring, the *Critical Security Controls* recommend that you:

- ✓ **Scan** and perform automatic vulnerability scans, on a weekly basis, or more frequently.
- ✓ **Measure alerts and effectiveness** in minutes.
- ✓ **Discover** and identify unauthorized hosts within 24 hours.

- ✓ **Patch** critical systems within 48 hours.

Qualys is a founding member and active participant in developing CSCs. To learn more, visit <http://www.counciloncybersecurity.org/critical-controls/>.

Identifying the Capabilities of Qualys Continuous Monitoring



Qualys CM helps you follow the guidance of the *Critical Security Controls* (see the ‘*Critical Security Controls* and continuous monitoring’ sidebar) by providing you with the ability to:

- ✓ Integrate data from Qualys VM scans, which are done periodically (by schedule) for vulnerabilities on all network-connected systems.
- ✓ Scan on demand for ad-hoc checks or for specific vulnerabilities such as ‘forbidden ports’, which is recommended by CSC 4.
- ✓ Scan continuously for mission-critical systems and sub-networks.
- ✓ Receive reports on vulnerabilities in patch-centric views using ‘supersede’ information to help boost efficiency in scanning and remediation.
- ✓ Inspect reports that integrate Common Vulnerabilities and Exposures (CVE) and Common Vulnerability Scoring System (CVSS) standards for flexible analysis of results.
- ✓ Track remediation with an internal ticket system that provides visibility and control for ensuring the safety of vital systems and networks.

- ✓ Receive immediate notification of vulnerabilities and remediation paths to first responders. (For an example, see Figure 5-1).

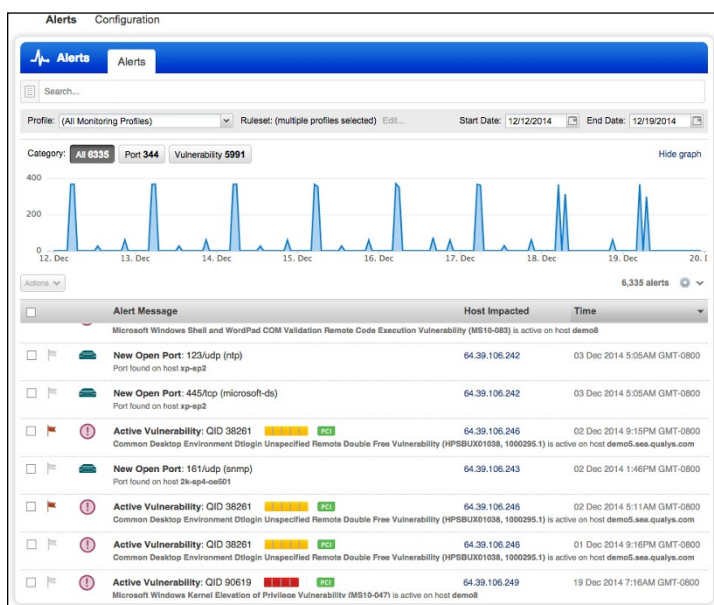


Figure 5-1: Qualys CM alerts let first responders instantly drill down to details such as new open ports, ports closed or ports changed.

Viewing Examples of Results Using Qualys Continuous Monitoring



Alerts sent by Qualys CM to first responders specify changes in an organization's attack surface that may result in a compromise of asset security. Examples of typical significant events include:

- ✓ **New vulnerability found:** Alerts are sent based on severity level of the vulnerability and the affected host. You can also specify alerts for specific vulnerabilities. For example, even though patches were published for the infamous Heartbleed Bug, this vulnerability continues

to appear due to deployment of hosts infected by bad images used for configuration. Specifying a rule that searches for 'QID 42430' will immediately identify the presence of this vulnerability, and Qualys CM will notify first responders accordingly.

- ✔ **New host:** A new host appearing on your network is a significant event. For example, you could specify a rule permitting hosts in the 'demilitarized zone' (DMZ) to only run Linux, and follow a certain naming convention. Qualys CM will immediately detect hosts with variations from the rule and notify first responders accordingly.
- ✔ **New open port:** A host may have been securely configured in the past, but a port deliberately or accidentally opened is an event that exposes the machine to attack. Qualys CM notes this event and alerts first responders accordingly. Rules specified with Qualys CM can monitor granular port-related criteria such as having more ports open in addition to port 80.
- ✔ **New software installed:** Qualys CM can send an alert if a host has new software installed (including an upgrade or downgrade), or is running a version of software that is out-of-date and/or unpatched. This capability is enabled by configuring Qualys VM to do authenticated scanning, which logs the scanner into the host as if it were an authorized user of the machine.
- ✔ **Changes in a SSL certificate:** Usually these alerts are related to multiple hosts. Granular alert criteria may include certificates that are new (even though they may be valid and not expired). This event is important because it detects when someone may have swapped in a valid certificate, but not the certificate that should be used for a particular host. For example, if your organization only buys certificates from Verisign, a rule specifying that will automatically detect an invalid certificate purchased elsewhere, such as from GoDaddy. You can reuse Rule Sets, such as those governing results described in the preceding bullets, as often as you like, thus simplifying administration and your use of Qualys CM.



You can combine multiple rules to give even more advanced functionality. For example, you could enforce a host with port 80 open to run a Windows operating system. Finally, the all-in-one Guided Search Box feature in Qualys CM helps users to quickly locate and analyze detailed event information.



With capabilities like these, CM is a critical approach for ensuring the ongoing protection of your network's perimeter. Qualys CM provides an always-on, comprehensive view of your perimeter with integrated alerts so you can act quickly to address potential threats when changes occur in your network environment.

Part VI

Ten Best Practice Checks for Doing Continuous Vulnerability Management

.....

In This Part

- ▶ Checking everything to ensure you're protected
 - ▶ Producing technical, management, and compliance reports
 - ▶ Patching and tracking
-

The ten checks for doing continuous vulnerability management (VM) in this Part reflect the variety of security measures that are required to effectively identify and eliminate weaknesses on your network. These checks form an aggressive plan for removing vulnerabilities in key resources before attackers can exploit your network.

Discover Your Network Assets

You can't measure risk if you don't know what you have on your network. Discovering your assets helps you to determine the areas that are most susceptible to attacks, and network mapping automatically detects all networked devices. VM gives you the capability to do a full network discovery of your network assets on a global scale.

Prioritize and Classify Your Assets

Most organizations have five to 20 categories of network assets whose classification is determined by value to the overall business. Tier the hierarchy of assets by value to the business. For example, critical databases, financial systems and other important business assets should be ranked in a higher category than clerical desktops, non-production servers and remote laptops. Classify asset priority based on the value to the business and do not give critical assets a lower categorization due to presumptions about their safety.

Assess Vulnerabilities with Comprehensive Scans

Run comprehensive and accurate scans on your assets, starting with the most important ones. Doing so will give you full visibility of the level of risk associated with your assets. Intelligent scanning rapidly finds vulnerabilities on your network – automatically or on demand. You can scan lower categories of assets less frequently.

Perform Vulnerability Management both Inside and Outside the DMZ

Be comprehensive about your network auditing. Therefore, perform VM both on your ‘demilitarized zone’ (DMZ, or the external network boundary) and on your internal systems. That’s the only way to achieve optimal security protection. Hackers’ exploits are crafty and will otherwise breach your network, so make sure you guard and check everything.

Remediate by Prioritizing Patching Efforts

Prioritize application of patches, starting with the most critical vulnerabilities on the most important assets, and proceed to the less critical ones. Get in the habit of setting (and exceeding!) performance goals to reduce the level of critical vulnerabilities in the network.

Track Remediation Progress

Automatic generation of trouble tickets enables you to track each remediation step and to measure progress over time. If you have a larger organization, using a ticketing system will speed remediation, save you time, enable you to compare performance of distributed teams and provide recognition to leaders and followers. Peer pressure will encourage security teams to share experiences of actions, leading to a more rapid reduction in vulnerabilities.

Inform the Technical Staff with Detailed VM Reports

Vulnerability reports should be comprehensive, with full instructions on how to remediate vulnerabilities. Customizable reports are also desirable, allowing technical staff to view data in the desired context while reducing information overload.

Inform Management about VM

Use gathered metrics from scans to communicate the status of network security to senior management. Lines of business managers can understand the trend of vulnerabilities and the efforts of the security team to minimize risks to the enterprise. Use actual performance measurements to educate your executive management team and show the value of VM in maintaining business continuity, reducing risks and maintaining a secure infrastructure.

Inform Auditors for Policy Compliance

VM delivers trusted, third-party auditing and reporting which meets compliance needs of the Health Insurance Portability and Accountability Act (HIPAA), Gramm–Leach–Bliley Act (GLBA), California Senate Bill 1386, Sarbanes–Oxley Act (SOX), Basel II and the Payment Card Industry Data Security Standard (PCI DSS). You can use reports from VM solutions to document the state of security over time on systems in scope for compliance.

Continuously Repeat the VM Process on a Regular Basis

VM is not a one-time effort. Best VM practices suggest regular, continuous scanning and remediation to proactively guard against internal and external threats and ensure compliance. Scan critical systems continuously and less critical assets daily to detect the latest vulnerabilities.

Qualys is the leading provider of continuous vulnerability management & compliance solutions

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud security and compliance solutions, with over 7,700 customers in more than 100 countries, including a majority of each of the Forbes Global 100 and Fortune 100. The Qualys Cloud Platform and integrated suite of solutions help organizations to simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance and protection for IT systems and Web applications. Customers use Qualys to perform more than 1 billion security audits annually, helping them protect their IT infrastructures from cyber attacks.

Qualys Awards

Qualys is overwhelmingly recognized as the leader in its space. Qualys has won awards ranging from Best Vulnerability Management Solution, Best Security Product, Best Security Company, Best Network Protection Service and much more!



Successfully learn how to do continuous vulnerability management and protect your network!

Vulnerability management may seem like a daunting task. This book is a quick guide to understanding how to protect your network and data with continuous VM – from learning about risks to networks to selecting a solution that discovers vulnerabilities and quickly remediates them. This book also tells you about the industry's leading VM solution – Qualys VM. No matter what your level of knowledge about security, *Vulnerability Management For Dummies* is a simple way to learn how to control the risks that affect every network.

Full details about Qualys' solutions are available at www.qualys.com.

- *Learn why organizations need to do continuous VM — discover how VM protects your network*
- *Get the best VM solution for your business — rapidly set your company on the path to stronger security*
- *Follow our four-step program for VM — successfully manage and eliminate vulnerabilities*

Qualys, Inc. is a pioneer and leading provider of cloud security and compliance solutions, overwhelmingly recognized as the leader in its space. Customers use Qualys to perform more than 1 billion security audits annually, helping them protect their IT infrastructures from cyber attacks.



Open the book and find:

- Why organizations need VM
- Options for VM
- How to do continuous VM
- How to get the best VM solution from Qualys
- A four-step program for VM

Go to Dummies.com
for videos, step-by-step examples,
how-to articles, or to shop!

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley's ebook EULA.