Definitive Guide™ to *Next-Generation Vulnerability Management*

Leveraging Continuous Monitoring to Mitigate Threats and Simplify Compliance

Steve Piper, CISSP

FOREWORD BY:
Ron Gula

Compliments of:

tenable
network security

About Tenable Network Security

Tenable Network Security is relied upon by more than 20,000 organizations in over 100 countries — including the entire U.S. Department of Defense and many of the world's largest companies and governments — to stay ahead of emerging vulnerabilities, threats, and compliance-related risks. Its award-winning Nessus and SecurityCenter solutions have received the highest-possible rating in Gartner's MarketScope for Vulnerability Assessment, and Tenable's innovative Passive Vulnerability Scanner (PVS) and Log Correlation Engine (LCE) technologies afford its customers with unprecedented continuous monitoring capabilities and a compelling alternative to traditional bulky SIEM platforms. Tenable continues to set the standard for identifying vulnerabilities, preventing attacks, and helping its customers comply with a multitude of regulatory requirements. For more information, visit Tenable online at www.tenable.com.

SC MAGAZINE
AWARDS
2013
WINNER
Honored in the U.S.

Winner of the coveted
2013 SC Magazine Excellence Award
for Best Enterprise Security Solution

Definitive Guide™
to
Next-Generation Vulnerability Management

Steve Piper, CISSP

Foreword by Ron Gula

CYBEREDGE
PRESS

Definitive Guide™ to Next-Generation Vulnerability Management

Published by:
CyberEdge Group, LLC
1997 Annapolis Exchange Parkway
Suite 300
Annapolis, MD 21401
(800) 327-8711
www.cyber-edge.com

LIMIT OF LIABILITY/DISCLAIMER OF WARRANTY: THE PUBLISHER AND THE AUTHOR 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. THE ADVICE AND STRATEGIES CONTAINED HEREIN MAY NOT BE SUITABLE FOR EVERY SITUATION. 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.

For general information on CyberEdge Group research and marketing consulting services, or to create a custom *Definitive Guide* book for your organization, contact our sales department at 800-327-8711 or info@cyber-edge.com.

ISBN: 978-0-9888233-2-7 (paperback); ISBN: 978-0-9888233-3-4 (eBook)
Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

Publisher's Acknowledgements

CyberEdge Group thanks the following individuals for their respective contributions:

Editor: Susan Shuttleworth
Graphic Design: Debbi Stocco
Production Coordinator: Valerie Lowery
Special Help from Tenable: Jonathan Brody, Ron Gula, Manish Patel, Vatsal Sonecha, Ed Wong

Table of Contents

Foreword v

Introduction vii

Chapters at a Glance vii

Helpful Icons viii

Understanding Vulnerability Management 1

Exploring Vulnerabilities and Exploits 2

What is a Vulnerability? 3

Identifying vulnerabilities by CVE 3

Rating vulnerabilities by CVSS 5

Staying informed through Bugtraq 5

Common Vulnerability Sources 5

What is an Exploit? 6

Known versus zero-day exploits 7

Defining Vulnerability Management 7

The origins of VM 8

Emergence of continuous monitoring 9

Common Use Cases 10

Key Components 10

Active vulnerability scanners 10

Passive vulnerability scanners 11

Log correlation engines 11

Management console 12

Exploring Next-Generation Vulnerability Management 13

Standard Features 14

Policy templates 14

Interactive dashboards 15

Pre-built and custom reports 16

Daily security intelligence updates 17

Granular access control 17

Trouble ticketing 18

IPv6 support 18

Advanced Features 19

Passive vulnerability scanning 19

Log aggregation and correlation 20

Mobile device scanning 20

Virtualization platform scanning 20

Intelligent load balancing 21

Asset lists 21

Configuration auditing 22

Patch auditing 23

Remediation scanning 23

Malware detection 23

Management console tiering 24

Getting Started 25

10 Steps for Getting Started 25

Step 1: Determine what to scan 25

Step 2: Architect your solution 26

Step 3: Install your management console 28

Step 4: Deploy your active and passive scanners 28
Step 5: Assign user permissions 29
Step 6: Categorize your assets 29
Step 7: Construct vulnerability scanning policies 29
Step 8: Construct configuration auditing policies..................... 31
Step 9: Customize your dashboards 32
Step 10: Customize your reports...32

The Case for Continuous Monitoring 33

Defining Continuous Monitoring 34
Origins of Continuous Monitoring 34
Why periodic scanning isn't enough...35
Continuous Monitoring Use Cases 36
Prioritizing patching efforts..36
Identifying policy violations 36
Providing context for IPS and NGFW platforms.......................36
Monitoring web applications 37
Detecting internal threats 37

Achieving and Sustaining Regulatory Compliance.................39

Payment Card Industry Data Security Standard (PCI DSS)...................40
North American Electric Reliability Corporation (NERC) 43
Federal Information Security Management Act (FISMA)......................44

Integrating NGVM with Your Existing Infrastructure 47

Security Information and Event Management (SIEM) 48
Perimeter Security Defenses 49
Intrusion Prevention Systems (IPS)...49
Next-Generation Firewalls (NGFW)..50
Unified Threat Management (UTM) 50
Risk Management 50
Mobile Device Management (MDM)...50
Incident Management 51
Access Management 51
Patch Management 52
Penetration Testing 52

Selecting the Right VM Solution 53

Support for Continuous Monitoring 54
Flexible Deployment Options...55
Enterprise-class Scalability and Performance 56
Comprehensive Policy Coverage 57
Daily Security Intelligence Updates 57
Best-of-Breed Feature Set 57
Accuracy of Authenticated Scans 58
Broad Integration Support 59
Ease of Use..59
Superior Customer Service...60

Glossary 61

Foreword

Vulnerability management is the single best protection an organization can implement to reduce its network security risks. In my view, it's more important than any other network security technology because it improves the security posture of *all* network components — not just high-profile assets.

As our networks evolve in response to mobile computing, BYOD (bring your own device), social media, and cloud computing influences, so do the threats we face. Our cyber adversaries are bright, well-funded, and highly motivated. And with a new software vulnerability disclosed nearly once an hour, our network attack surfaces are only getting bigger.

As information security professionals, we live in a cat-and-mouse world. And it's clear the bad guys have the upper hand. If we stand a chance of defending our networks against today's sophisticated threat landscape, we must think differently.

I started my career as a vulnerability researcher and penetration tester for the U.S. National Security Agency (NSA). Like most pen testers, my team was consistently able to compromise our internal networks and identify both immediate and long-term security issues that were not being addressed. And unfortunately, repeat visits down the line didn't show much improvement.

As a point security measure, I realized that penetration testing didn't have a strategic impact on the NSA divisions we were helping. This influenced me a great deal when I wrote the Dragon intrusion detection system (IDS). Knowing how difficult it was for organizations to run a secure network, I wanted to develop a technology that detected bad guys with little-to-no human intervention. Dragon was very successful and detected lots of attacks, but the high volume of attacks allowed some attackers to fly under the radar. Attackers were now evading not only network IDS, but also firewalls and antivirus platforms.

So, when I co-founded Tenable Network Security in 2002, I had the mindset that there were no easy or quick solutions to solve our security problems. Only a well-run, carefully managed network could achieve security that is “obtainable and defendable,” which is the very meaning of the word *tenable*.

The key to a well-run network is the ability to measure security risks in real time. Over the last decade, Tenable has heavily invested in game-changing security innovations, including passive vulnerability assessment, log analysis, and advanced threat detection technologies that fuel our continuous monitoring solution. Today, our award-winning vulnerability management solution, called SecurityCenter Continuous View, has earned the trust of thousands of companies and government agencies around the world, including the entire U.S. Department of Defense.

The world knows Tenable for Nessus. But if you think that’s all we have to offer, it’s time to take a closer look.

This book is an excellent guide through the next generation of vulnerability management technology and provides a glimpse into the future of continuous monitoring. It outlines how the explosion of applications and network technologies is vastly outpacing our ability to defend them, and illustrates how a modern vulnerability management platform capable of 100 percent asset discovery can uncover vulnerabilities and security misconfigurations in real time — even within the latest mobile devices.

It’s time to shed your preconceived notions about vulnerability management and discover how continuous monitoring can take your network security strategy to a whole new level.

Welcome to the next generation of vulnerability management technology.

Ron Gula
Co-founder, CEO and CTO
Tenable Network Security

Introduction

Today's enterprise IT security teams face two seemingly insurmountable tasks — defending the organization from a deluge of sophisticated cyberthreats and demonstrating compliance with constantly evolving government and industry regulations. Fortunately, there is a new breed of security technology that can help your organization achieve both of these objectives. I'm talking, of course, about next-generation vulnerability management (NGVM).

Unlike traditional vulnerability management (VM) offerings that focus on periodic active scanning, NGVM equips IT organizations with a continuous monitoring solution needed to detect 100 percent of network assets — including the latest mobile devices — and defend them against software vulnerabilities, security misconfigurations, and now, cyberthreats. This arms today's enterprises with a new weapon to fight advanced persistent threats (APTs) and other sophisticated attacks. It also integrates with your infrastructure and management systems to provide relevant context for prioritized remediation.

If you're tasked with defending your network from cyberthreats and/or supporting regulatory compliance audits, this is one book you simply can't afford to miss.

Chapters at a Glance

Chapter 1, "Understanding Vulnerability Management," defines VM and distinguishes between vulnerabilities and exploits. In this chapter, I explore common VM uses cases and review key components of a modern VM solution.

Chapter 2, "Exploring Next-Generation Vulnerability Management," describes standard and advanced features found in best-of-breed NGVM solutions.

Chapter 3, "Getting Started," lists 10 steps to get your NGVM system up and running and provides helpful tips and tricks to maximize security effectiveness.

Chapter 4, "The Case for Continuous Monitoring," gets to the heart of today's enterprise-class NGVM solutions. Here you'll learn why active scanning alone is insufficient for mitigating cyberthreats and how to leverage continuous monitoring to improve your network's security posture.

Chapter 5, "Achieving and Sustaining Regulatory Compliance," reviews common government and industry regulatory frameworks and describes how VM can help enterprises support ongoing regulatory compliance audits.

Chapter 6, "Integrating NGVM with Your Existing Infrastructure," details the value of, and methodology for, integrating NGVM systems into your existing network and security infrastructure.

Chapter 7, "Selecting the Right NGVM Solution," provides guidance on what to look for — and what to avoid — when evaluating enterprise-class VM solutions.

Glossary provides handy definitions to key terminology (appearing in *italics*) used throughout this book.

Helpful Icons

TIP

Tips provide practical advice that you can apply in your own organization.

DON'T FORGET

When you see this icon, take note as the related content contains key information that you won't want to forget.

CAUTION

Proceed with caution because if you don't it may prove costly to you and your organization.

TECH TALK

Content associated with this icon is more technical in nature and is intended for IT practitioners.

ON THE WEB

Want to learn more? Follow the corresponding URL to discover additional content available on the Web.

Chapter 1

Understanding Vulnerability Management

In this chapter

- Define vulnerability management and distinguish between vulnerabilities and exploits
- Explore common vulnerability management use case
- Review the key components of a modern vulnerability management solution

"To err is human; to forgive, divine."

— Alexander Pope (1688-1744), English poet

Human errors made in the software development industry can, at times, result in the financial devastation of companies victimized by attackers who exploit these errors — commonly called *vulnerabilities*. As IT contends with thousands of new operating system and application vulnerabilities each year — by identifying, prioritizing, and then mitigating them — the use of *vulnerability management (VM)* products has become essential.

Before learning about the immense value that *next-generation vulnerability management (NGVM)* solutions deliver above and beyond typical VM offerings, it's best to cover the basics of vulnerability management. In this chapter, I define software vulnerabilities and depict common *exploits* (attacks) that target them. I then describe how organizations today are leveraging VM technology to their advantage and review the key components that comprise today's modern solutions.

TIP

If you're already familiar with the basics of VM, feel free to skip this chapter.

Exploring Vulnerabilities and Exploits

Despite what information security vendors might tell you, no single security product can make a network safe from all attacks. The best way to secure your network is by implementing a *defense-in-depth* strategy comprised of layered security defenses, with VM as its foundation.

To understand why VM (and NGVM) is so important, let's review the findings from Verizon's 2013 Data Breach Investigations Report (DBIR), which analyzed 621 confirmed data breaches that occurred in 2012.

- ☑ 92 percent were perpetrated by outsiders.
- ☑ 78 percent of initial intrusions were rated as low difficulty.
- ☑ 71 percent targeted user devices.

ON THE WEB

To download a free copy of Verizon's 2013 DBIR, connect to: http://www.verizonenterprise.com/DBIR/2013/.

Additionally, a white paper titled "Raising the Bar for Cybersecurity" (James A. Lewis, February 2013) published by the Center for Strategic & International Studies (CSIS) sheds even more light on the need for effective VM.

- ☑ 75 percent of attacks use publicly known vulnerabilities in commercial software that could be prevented by regular patching.
- ☑ 85 percent of breaches took months to be discovered; the average time is five months.
- ☑ 96 percent of successful breaches could have been avoided if the victim had put in place simple or intermediate controls.

The bottom line is that it shouldn't be so easy for hackers — especially given how far VM and complementary *patch management* (more on that later) solutions have come over the past decade. These solutions work in concert to help reduce your network's attack surface.

Before we proceed further, let's cover the fundamentals of VM technology, starting with defining the term *vulnerability*.

What is a Vulnerability?

In the context of information security, a *vulnerability* is a weakness that allows an attacker to gain unauthorized access to a computer host or device. To compromise a vulnerable system, three elements must exisit: a system flaw, an ability to access the flaw, and a capability to exploit the flaw.

DON'T FORGET

Most information security practitioners think of vulnerabilities in terms of operating system and application defects that enable attackers to remotely exploit systems, but vulnerabilities can also be caused by the organization itself through misconfigured security settings.

The *window of vulnerability* is the time span from the discovery of a software vulnerability (ideally by the vendor or a trustworthy vulnerability researcher) to its mitigation (fix) by deploying a software patch.

Vendors almost always wait to disclose software vulnerabilities to their users until they have published the corresponding *patches* (software updates that fix their vulnerabilities). That way, organizations have the opportunity to patch their systems before attackers can develop *exploits* to leverage the vulnerability.

Identifying vulnerabilities by CVE

Prior to 1999, information security tools that detected and/or mitigated software security vulnerabilities had no way to interoperate with each other, as there was no common way to identify or categorize vulnerabilities. But in 1999, that changed when MITRE Corporation — an American not-for-profit organization — compiled the first vulnerability database to assign a unique identifier to each vulnerability.

"Patch Tuesday"

The second Tuesday of each month is widely known as "Patch Tuesday" (or sometimes "Black Tuesday" or "Microsoft Tuesday"), as this is the day Microsoft releases the newest fixes for its Windows operating system and software applications. Microsoft introduced Patch Tuesday in 2003 in response to customer complaints about its practice of issuing patches sporadically throughout the year. The company chose Tuesday because it is not the first day of the week (which often falls on a holiday), but is early enough that organizations have time to apply the patches before the following weekend.

By delivering its patches only once per month — except for the occasional "out-of-band" disclosure for the most severe vulnerabilities — Microsoft enables organizations to plan in advance and install multiple patches on a single system with just one reboot.

The day following each Patch Tuesday is jokingly called "Exploit Wednesday," as attackers have had a full 24 hours to construct malware to exploit unpatched vulnerabilities associated with the prior day's disclosures.

All Microsoft security bulletins can be found by connecting to: http://technet.microsoft.com/en-us/security/bulletin.

MITRE's publicly available database – hosted by the U.S. National Vulnerability Database (NVD) in partnership with MITRE — contains a unique *CVE* (common vulnerability and exposures) identifier for each catalogued vulnerability. One example of the more than 56,000 unique vulnerabilities is CVE-2013-1288, where 2013 is the year the vulnerability was registered and 1288 is the number assigned by its corresponding CVE Numbering Authority (CNA). MITRE has granted CNA designations to more than a dozen software vendors, including Adobe, Apple, Cisco, Microsoft, Oracle, and Red Hat.

ON THE WEB

To query the NVD for CVEs by keyword search, connect to: http://web.nvd.nist.gov/view/vuln/search. For a complete list of CVE-compatible products, connect to: http://cve.mitre.org/compatible/compatible.html.

Thanks to MITRE Corporation and its CVE database, vulnerability management, patch management, intrusion prevention system (IPS), and next-generation firewall (NGFW) vendors can interoperate with each other through the common CVE framework.

Rating vulnerabilities by CVSS

In 2004, just five years following the launch of the CVE database, research conducted by the National Infrastructure Advisory Council led to the launch of *CVSS* (common vulnerability scoring system) — a free and open industry standard for assessing the severity of system vulnerabilities. Today, CVSS vulnerability ratings are under the custodianship of the Forum of Incident Response and Security Teams (FIRST).

DON'T FORGET

The current standard, CVSSv2, has been adopted by NVD as the primary method for quantifying the severity of vulnerabilities. CVSS scores range from 0 to 10 and fall into one of three classifications:

- ☑ Minor: 0 to 3.9
- ☑ Major: 4.0 to 6.9
- ☑ Critical: 7.0 to 10

Staying informed through Bugtraq

Bugtraq is an electronic mailing list dedicated to issues about information security. It was launched in 1993 and was originally hosted at Crimelab.com. Today, Bugtraq is maintained by SecurityFocus, an online computer security news portal that was acquired by Symantec in 2002.

ON THE WEB

SecurityFocus maintains its own vulnerability database and assigns a Bugtraq ID (BID) for select CVEs. To query Bugtraq vulnerabilities by vendor (or by CVE), connect to: http://www.securityfocus.com/vulnerabilities. Or to sign up for one of 14 Bugtraq mailing lists maintained by SecurityFocus, connect to: http://www.securityfocus.com.

Common Vulnerability Sources

There is a common misconception that Microsoft is the largest single source of software vulnerabilities. That may be because Microsoft vulnerabilities are the initial point of attack of so many high-profile *advanced persistent threats (APTs)*. Or it could be because of the regular attention Microsoft receives from its Patch Tuesday announcements.

In any case, Microsoft was associated with the fourth-largest number of vendor-related vulnerabilities, behind Oracle, Apple, and Mozilla, respectively. Table 1-1 provides a summary of vulnerabilities disclosed in 2012 from the 10 largest vendor sources.

Vendor	*Total Vulns.*	*Critical Vulns.*	*Major Vulns.*	*Minor Vulns.*
Oracle	424	76	238	110
Apple	270	141	115	14
Mozilla	195	118	72	5
Microsoft	169	117	48	4
IBM	154	42	94	18
Google	150	79	66	5
Adobe	137	127	10	0
Cicsco	134	85	45	4
HP	74	38	31	5
Apache	55	10	41	4

Table 1-1: Top 10 vendors by numbers of vulnerabilities reported in 2012.
Source: Data compiled from National Vulnerability Database.

What is an Exploit?

An *exploit* is a piece of software (malware), a chunk of data, or a sequence of commands that takes advantage of (or exploits) a security vulnerability to compromise or adversely affect a system.

TIP

A *remote exploit* takes advantage of the vulnerability of a targeted system without ever requiring local access to that system. In contrast, a *local exploit* needs local access to the vulnerable system and usually involves increasing the privileges of the user account running the exploit.

Attackers that use exploits often deliver them through social engineering attacks, including:

- ☑ *Spear phishing*
- ☑ *Whaling*
- ☑ *Baiting*
- ☑ *Water holing*
- ☑ *Search engine poisoning*

TIP

Consult the glossary at the end of this book for concise descriptions of these social engineering attacks.

Known versus zero-day exploits

The window of vulnerability is the time period extending from discovery of a software vulnerability to mitigation (fix) by deploying a software patch. Many vulnerabilities are discovered by the software vendors themselves or from outside (“white hat”) vulnerability researchers.

The worst-case scenario occurs when an ill-intentioned (“black hat”) hacker discovers a critical software vulnerability and uses it to his advantage by creating *zero-day exploits*. They’re called zero-day exploits because they are created before “day zero” of public awareness — and certainly before the vendor has issued a patch.

Defining Vulnerability Management

Let’s get to the heart of our topic by defining and discussing modern vulnerability management.

Vulnerability management is the cyclical practice of identifying, classifying, remediating, and mitigating software vulnerabilities and security misconfigurations. IT research firm Gartner estimates the size of the VM market in 2012 at $435 million (up from $390 million in 2011).

A full-featured VM (or NGVM) solution — working in concert with your existing security infrastructure (see Chapter 6) — can help IT continually answer the following five critical questions:

- ☑ Which systems are vulnerable?
- ☑ Which systems are out of compliance?
- ☑ Which systems are being attacked?
- ☑ Which systems have already been compromised?
- ☑ Which systems shoud we fix first?

TIP

The term *vulnerability management* refers to a complete VM (and NGVM) solution (equipped with scanners and a management console), while vulnerability assessment references vulnerability scanners.

Today's (basic) VM solutions provide the following capabilities:

- ☑ Active scanning to uncover known vulnerabilities
- ☑ Asset classification capabilities
- ☑ Centralized configuration of distributed active scanners
- ☑ Ability to map vulnerabilities to CVEs and Bugtraq IDs
- ☑ Remediation workflows describing how to mitigate each vulnerability
- ☑ Centralized administration with dashboards and reports

TIP

Most leading VM solutions go well beyond this minimum feature set, as I discuss in the "Advanced Features" section of the next chapter.

The origins of VM

The first widely used vulnerability assessment scanner, called Nessus, was created by a 17-year-old Frenchman named Renaud Deraison. It was launched as open source alpha code in April 1998 with just 50 plugins. (More on plugins in Chapter 2.) Over the past 15 years, use of Nessus has exploded and it is now the most widely used vulnerability assessment scanner in the world. Here are a few of the significant milestones in the evolution of Nessus:

- ☑ **April 1998** – Nessus alpha version is launched.
- ☑ **May 2000** – Nessus 1.0 is released.
- ☑ **September 2002** – Tenable is founded by Renaud Deraison, Ron Gula, and Jack Huffard.
- ☑ **January 2003** – Tenable launches management console to centrally manage multiple Nessus scanners.
- ☑ **September 2003** – Tenable introduces real-time passive vulnerability detection capability.
- ☑ **December 2005** – Tenable launches the first Nessus graphical user interface (GUI).
- ☑ **May 2008** – Nessus exceeds 5 million downloads.
- ☑ **December 2010** – Tenable launches Nessus Perimeter Service.
- ☑ **February 2013** – Tenable wins the prestigious SC Magazine Excellence Award for Best Enterprise Security Solution.

ON THE WEB

For a more comprehensive look at Nessus' 15-year history, connect to: http://www.tenable.com/nessus-15/.

Today, Nessus is the *de facto* standard for vulnerability assessment and is used by more than 20,000 Tenable customers in more than 100 countries. Renaud Deraison now serves as Chief Research Officer at Tenable.

Emergence of continuous monitoring

Continuous monitoring is arguably the most exciting development in the VM industry in the past decade. Rather than relying on periodic (usually quarterly) active scan results, organizations are implementing real-time passive vulnerability discovery solutions to strengthen their security posture and continually minimize their networks' attack surface.

TIP

This paradigm shift in the way organizations think about VM is so compelling that I've dedicated an entire chapter to this topic (see Chapter 4). But don't jump ahead just yet, as we've still got a lot of ground to cover.

Common Use Cases

When the VM industry was first conceived, there was just one primary use case — mitigating network vulnerabilities. Although it certainly continues to be a driving factor, mitigating vulnerabilities is now part of a much longer list of capabilities that includes:

- ☑ Auditing patch configurations
- ☑ Monitoring security configurations
- ☑ Identifying malware and malicious activities
- ☑ Securing mobile devices
- ☑ Securing virtual and cloud environments
- ☑ Sustaining regulatory compliance

TIP

For more information on how modern NGVM solutions address these use cases, turn to the "Advanced Features" section in Chapter 2.

Key Components

Although VM (and NGVM) products vary greatly, most leading vendors that focus on enterprise-class deployments offer four main solution components — active vulnerability scanners, passive vulnerability scanners, log correlation engines, and management consoles.

Active vulnerability scanners

An *active vulnerability scanner* (such as Nessus) is a software application designed to identify hosts connected to the network and assess their weaknesses by identifying operating system and application vulnerabilities and security misconfigurations.

DON'T FORGET

An active vulnerability scanner is sometimes compared to a network scanner (or port scanner), such as Nmap (www.nmap.org). Although both scanner types can identify hosts and host assets (such as operating systems, ports, protocols, and certain applications), only a vulnerability scanner can enumerate vulnerabilities and security misconfigurations.

Active vulnerability scanner software is usually installed by IT organizations on their own hardware. Leading VM providers support Microsoft Windows, Mac OS X, Linux, Free BSD, and Solaris platforms. Some even provide vulnerability scanners packaged as VMware virtual machines.

Vendor-hosted perimeter scanning service

Although most organizations host their own active vulnerability scanners, some prefer to leverage a VM vendor's hosted perimeter scanning service to scan Internet-facing hosts. Such offerings are delivered via a software-as-a-service (SaaS) model, where the scanning software (and management console) is hosted in the vendor's cloud.

Passive vulnerability scanners

A *passive vulnerability scanner* is an essential component of enterprise-class NGVM solutions because of the need for continuous monitoring. (More on continuous monitoring in Chapter 4.) Instead of actively scanning hosts on a periodic basis (often monthly or quarterly), passive vulnerability scanners merely listen to network traffic to identify and classify hosts and detect their vulnerabilities.

While a passive vulnerability scanner is not intended to replace an active scanner, it helps identify systems as soon as they connect to your network and extract basic vulnerability information based on the traffic they generate. A passive scan also provides network topology and monitors communications between hosts, identifies relationships, and looks for unusual connections to malicious sites and configuration changes indicative of malware or compliance violations.

As I discuss in Chapter 4, passive vulnerability scanners paint a much broader picture of the system vulnerabilities and security misconfigurations on your network. This also allows organizations to proactively prepare for audits or address security issues between monthly or quarterly active scans.

Log correlation engines

Better NGVM solutions provide a *log correlation engine* to extract log data from key infrastructure components, such as firewalls, intrusion detection and prevention systems

(IDS/IPS), DNS servers, DHCP servers, web proxies, and certain application logs. These logs provide powerful context for analyzing normal and anomalous traffic indicating abuse, errors, malicious activities, or unusual insider activity.

The ability to bond this data with vulnerability intelligence provides context for forensics and even asset discovery, and extends vulnerability analysis to systems that cannot be easily scanned or are not permitted to be scanned. Organizations can also leverage log correlation engines (typically built into the VM management console; see next section) to demonstrate compliance with many industry and government mandates that require system log aggregation.

TIP

In many instances, an NGVM vendor's log correlation engine may satisfy an organization's requirements for a log management or SIEM (security information and event management) solution.

Management console

The management console is the central nervous system of every VM (and NGVM) deployment. Installed and configured by the user on company-provided hardware, the management console is responsible for key VM (and NGVM) functions, including:

- ☑ Assigning granular user permissions
- ☑ Creating scanning policies
- ☑ Load balancing active scanning tasks
- ☑ Distributing daily software updates
- ☑ Aggregating scan results from active and passive vulnerability scanners
- ☑ Displaying real-time dashboards
- ☑ Generating alerts and custom reports

Now that you're grounded in the fundamentals of vulnerability management, turn to Chapter 2 to explore the standard and advanced features of leading NGVM solutions.

Chapter 2

Exploring Next-Generation Vulnerability Management

In this chapter

- Understand the differences between typical VM offerings and modern NGVM solutions
- Explore standard and advanced features found in best-of-breed NGVM solutions

Let's now explore common features that comprise today's modern NGVM solutions. But before we proceed, let's first contrast the key capabilities of typical VM offerings with modern NGVM solutions, as depicted in Table 2-1.

Key Capabilities	*VM*	*NGVM*
Centralized administration	✓	✓
Dashboards and reports	✓	✓
Active vulnerability scanning	✓	✓
Passive vulnerability scanning	✗	✓
Log aggregation and correlation	✗	✓
Mobile device scanning	✗	✓
Virtualization platform scanning	✗	✓
Intelligent scanner load balancing	✗	✓
Patch auditing	✗	✓
Malware detection	✗	✓

Table 2-1: Comparison of VM and NGVM solutions.

DON'T FORGET

Some VM vendors may claim to offer one or more of the NGVM capabilities depicted in Table 2-1, but unless they offer all of them, their offerings will fall short of expectations.

To explore the capabilities found in today's NGVM solutions, I separate NGVM features into two groups — standard features that you can expect to see in any VM and NGVM offering and advanced features you'll consistently find in best-of-breed NGVM solutions.

Standard Features

CAUTION

The features in this section are typical of a basic VM solution. If any are missing from a product that you're evaluating, carefully consider the implications to your overall security goals.

Policy templates

Whether you're motivated by regulatory compliance or reducing your network's attack surface, creating active scan policies is at the heart of a good VM solution. Today's VM/NGVM vendors make it easy by incorporating a library of scan policy templates into their offerings.

Regulatory compliance policy templates

Following is a sampling of common regulatory compliance templates you'll find in virtually any VM/NGVM solution:

- ☑ Payment Card Industry (PCI)
- ☑ Health Insurance Portability and Accountability Act (HIPAA)
- ☑ Federal Information Security Management Act (FISMA) with CyberScope application support
- ☑ Sarbanes-Oxley Act (SOX)
- ☑ North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP)
- ☑ Gramm-Leach-Bliley Act (GLBA)
- ☑ Defense Information Systems Agency (DISA)

IT security framework policy templates

The following IT security frameworks are used to help reduce your network's attack surface:

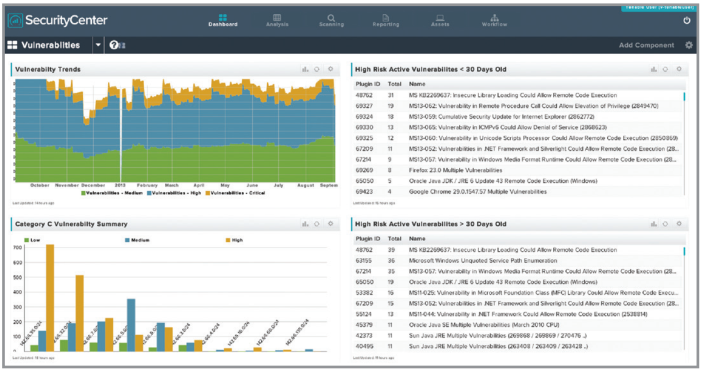
- ☑ SANS 20 Critical Security Controls (CSCs)
- ☑ Control Objectives for Information and Related Technology (COBIT)
- ☑ Center for Internet Security (CIS)
- ☑ NIST SP 800-53
- ☑ ISO 27001

Interactive dashboards

Organizations that acquire VM/NGVM solutions to reduce the likelihood of cyberthreats will find an interactive dashboard critical to this task. Unlike reports (see next section) that are generated periodically, the dashboard provides a real-time view of system vulnerabilities and security misconfigurations across the enterprise.

DON'T FORGET

A good dashboard (see Figure 2-1) should be highly interactive, enabling users to "drill down" into tables, charts, and graphs to uncover underlying data.



High Risk Active Vulnerabilites < 30 Days Old

Plugin ID	Total	Name
48762	31	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
69327	19	MS13-062: Vulnerability in Remote Procedure Call Could Allow Elevation of Privilege (2849470)
69324	18	MS13-059: Cumulative Security Update for Internet Explorer (2862772)
69330	13	MS13-065: Vulnerability in ICMPv6 Could Allow Denial of Service (2868623)
69325	12	MS13-060: Vulnerability in Unicode Scripts Processor Could Allow Remote Code Execution (2850869)
67209	11	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (28...
67214	9	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (28...
69269	8	Firefox 23.0 Multiple Vulnerabilities
65050	5	Oracle Java JDK / JRE 6 Update 43 Remote Code Execution (Windows)
69423	4	Google Chrome 29.0.1547.57 Multiple Vulnerabilities

Last Updated: 15 hours ago

High Risk Active Vulnerabilites > 30 Days Old

Plugin ID	Total	Name
48762	39	MS KB2269637: Insecure Library Loading Could Allow Remote Code Execution
63155	36	Microsoft Windows Unquoted Service Path Enumeration
67214	35	MS13-057: Vulnerability in Windows Media Format Runtime Could Allow Remote Code Execution (28...
65050	19	Oracle Java JDK / JRE 6 Update 43 Remote Code Execution (Windows)
53382	16	MS11-025: Vulnerability in Microsoft Foundation Class (MFC) Library Could Allow Remote Code Execu...
67209	15	MS13-052: Vulnerabilities in .NET Framework and Silverlight Could Allow Remote Code Execution (28...
55124	13	MS11-044: Vulnerability in .NET Framework Could Allow Remote Code Execution (2538814)
45379	11	Oracle Java SE Multiple Vulnerabilities (March 2010 CPU)
42373	11	Sun Java JRE Multiple Vulnerabilities (269868 / 269869 / 270476 ..)
40495	11	Sun Java JRE Multiple Vulnerabilities (263408 / 263409 / 263428 ..)

Last Updated: 11 hours ago

Figure 2-1: Sample dashboard

Better NGVM vendors provide customizable dashboard templates, making it easy to monitor areas of concern based on your role in the organization. Common dashboard templates include:

- ☑ Vulnerability metrics
- ☑ Accounts, authentication, and password audits
- ☑ Cyberthreats (APTs, exploits, botnets)
- ☑ Regulatory compliance (PCI, HIPAA, FISMA)
- ☑ Mobile device security

Pre-built and custom reports

Reporting is a critical function of any NGVM solution, enabling you to provide required information to internal and external regulatory compliance auditors and to satisfy the wide-ranging needs of IT security managers. Better NGVM management consoles include a report creation wizard that makes it easy to construct meaningful reports.

Most NGVM vendors give their customers a head start in creating reports by providing a library of dozens of pre-built report templates. Here is a small sampling of commonly available report templates:

- ☑ Regulatory compliance (PCI, HIPAA, FISMA, SOX)
- ☑ Vulnerability trending (by OS and application)
- ☑ Network service vulnerabilities
- ☑ Virtual computing vulnerabilities
- ☑ Web browser vulnerabilities
- ☑ Platform-specific vulnerabilities (Oracle, EMC, Cisco, Adobe, Microsoft SQL Server, Apache, Apple)
- ☑ Outstanding remediation tracking
- ☑ Consolidated report for missing patches

Daily security intelligence updates

Every VM vendor offers ongoing updates of vulnerability *plugins* (or *checks*), which enable the VM system to scan for new OS- and application-level vulnerabilities. Better NGVM providers also include additional sources of security intelligence, enabling their customers to uncover hidden threats including:

- ☑ IP, URL, and domain reputation feeds
- ☑ Botnet feeds
- ☑ Malware feeds

CAUTION

On average, 27 new operating system and application vulnerabilities are disclosed by researchers and vendors every day. Some VM vendors only update their plugins (or checks) once per week or a couple of times per month. Avoid these solutions at all costs. It's critically important that your vulnerability scanners remain up-to-date when performing active and passive scans.

Granular access control

In virtually every enterprise IT security organization today, the "principle of least privilege" prevails, meaning that IT users are only granted access to the systems and administrative privileges they need to do their jobs — nothing more.

NGVM systems support this practice by enabling administrators to granularly control access permissions to perform the following tasks:

- ☑ Administer user permissions
- ☑ Configure scan policies
- ☑ Create and modify dashboards and reports
- ☑ View scan results by network or asset list
- ☑ Modify system settings

Trouble ticketing

Most NGVM systems offer a basic trouble-ticketing component to assign vulnerability remediation (requests to remediate vulnerabilities by applying patches and/or correcting security misconfigurations) to IT security personnel. This capability enables managers to view a queue of requested vulnerability remediation tickets by system, by business unit, and even by user.

IPv6 support

Although only 1 percent of Internet traffic is transmitted using the IPv6 protocol (with the other 99 percent using IPv4), the ability to scan IPv6 hosts is a growing concern. When evaluating NGVM solutions, be sure to select one that can detect vulnerabilities within IPv6-only hosts and can passively identify these hosts (see the "Vulnerability assessment in an IPv6 world" sidebar). You may not appreciate it today, but you will in the years ahead.

Vulnerability assessment in an IPv6 world

IPv6 is the next-generation Internet protocol address standard intended to supplement, and eventually replace, the IPv4 protocol commonly used today. IPv6, which uses 128-bit addresses, was created in response to the rapid depletion of 32-bit IPv4 addresses. Although IPv4 accommodates 4.3 billion addresses, virtually all of them have already been allocated. IPv6, on the other hand, can accommodate 3.4 x 1038 addresses. Put another way, IPv6 allows every human on Earth to have trillions of IPv6 addresses!

Once IPv6 really takes off and IPv4 becomes a thing of the past (okay, many years from now), actively scanning a 48-bit IPv6 subnet would take about 69,000 years, assuming your scanners can handle a million hosts per second!

By incorporating an IPv6-capable passive vulnerability scanner into your NGVM solution, you are essentially future-proofing your NGVM investment, while identifying vulnerable hosts and security misconfigurations in between full active scans. IPv6-only hosts are identified and profiled as they naturally communicate over the network. Active scanners now know exactly which IPv6 hosts to scan when the time comes to do so.

Advanced Features

Now that you're grounded in the basics of VM features, let's pull back the layers of this proverbial onion and explore many of the advanced features you'll find in best-of-breed NGVM solutions.

Passive vulnerability scanning

As I discuss in Chapter 1, a passive vulnerability scanner is a network discovery and vulnerability analysis tool that delivers continuous, real-time network profiling. Rather than actively "probing" network hosts for vulnerabilities as active network scanners do, passive scanners merely "listen" to traffic to uncover security risks.

The benefits of adding passive vulnerability scanning to your NGVM solution are compelling. This technology:

- ☑ Alerts you to vulnerabilities and security misconfigurations in between periodic active scans
- ☑ Pinpoints potential insider threats undetected by your perimeter security defenses
- ☑ Provides an alternative to active scanning for mission-critical components, such as medical devices and industrial process controllers in SCADA environments
- ☑ Evaluates security risks of mobile devices
- ☑ Identifies new IPv6-only hosts
- ☑ Supports U.S. federal continuous monitoring guidelines (see Chapter 4 for more information)

DON'T FORGET

If you actively scan your network for vulnerabilities quarterly, you'll have an accurate snapshot four times per year. Passive vulnerability scanners keep you abreast of your network's security risks the other 361 days of the year.

Log aggregation and correlation

Also in Chapter 1, I discuss the benefits of incorporating log aggregation and correlation technology into your NGVM solution. Built right into the NGVM management console, this capability helps you to identify new hosts on network segments not monitored by passive vulnerability scanners or hosts that were not connected to the network during the last active network scan.

As new hosts are identified, they are grouped together in dynamic asset lists (see the "Asset lists" section ahead) and scanned by active scanners to detect system vulnerabilities and security misconfigurations.

Mobile device scanning

Today, mobile device management (MDM) vendors provide enterprises with critical capabilities to secure and monitor mobile devices such as smartphones, tablet computers, and mobile POS (point of sale) devices. MDM solutions can provision mobile devices, distribute applications, maintain security configurations, and secure data — but they can't monitor for mobile device vulnerabilities. That's where NGVM solutions come in, as they can:

- ☑ Enumerate iOS-, Android-, and Windows-based mobile devices that are accessing the network
- ☑ Detect known mobile device vulnerabilities
- ☑ Audit the efficacy of MDM controls
- ☑ Detect jailbroken smartphone devices

Virtualization platform scanning

Today's NGVM solutions incorporate special APIs enabling active scanners to authenticate privileged credentials when performing credentialed scans of virtualization platforms, such as VMware vSphere and vCenter. This helps to identify vulnerabilities and security misconfigurations within virtualization components. Most NGVM solutions contain special plugins (checks) specifically designed for this task.

Intelligent load balancing

No single active vulnerability scanner can handle the load of scanning all hosts on all network segments across the enterprise — at least not in a timely fashion. In fact, in larger, geographically dispersed enterprises, it's not uncommon to find dozens — or even hundreds — of vulnerability scanners in use.

Most leading NGVM solutions provide the means to aggregate the collective resources of vulnerability scanners by balancing their respective workloads to optimize efficiency and complete full network scans more quickly. However, some solutions require load balancing to be configured manually, and most vendors use a *round robin* (equal distribution) algorithm to distribute scanning assignments.

TIP

The optimal load-balancing solution requires no human intervention (beyond simply enabling the load-balancing feature) and considers the resource utilization of the scanners to avoid overloads. Intelligent load balancing can shorten a full enterprise network scan from weeks to days.

Asset lists

These days, *asset lists* have become a critical feature of the vulnerability management process (more on this in Chapter 3). But surprisingly, not all VM solutions incorporate them.

This term refers to the ability to categorize hosts (assets) into groups using predefined or user-defined tags (metadata) that enable NGVM users to construct policies, monitor dashboards, and create reports for only the hosts assigned to a given asset list. Assigning hosts to asset lists can be performed manually and/or dynamically (automatically). Common asset list tags include:

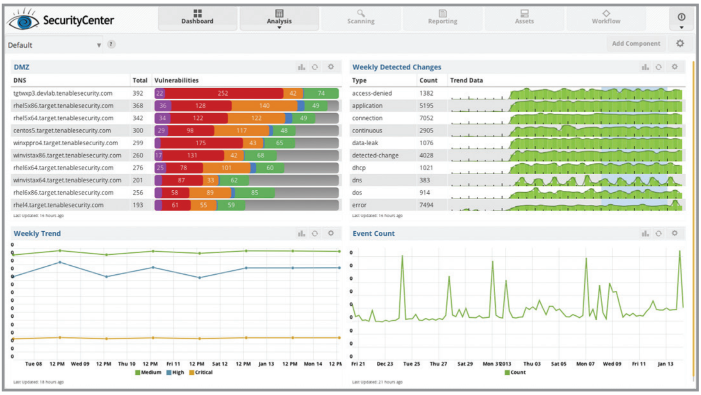
- ☑ Business criticality (low, medium, high)
- ☑ Geography (United States, Europe, Asia)
- ☑ Host type (desktop, server, mobile device)
- ☑ Business division (finance, sales, marketing)

Configuration auditing

Mitigating host vulnerabilities is certainly critical to reducing your network's attack surface, but it's only part of what a full-featured NGVM solution can do. Leading NGVM solutions can also assess the security configurations of your network hosts and devices against custom-created configuration assessment policies and predefined policies that align with common IT security frameworks.

With a configuration-auditing feature built into your NGVM solution, you can monitor the security configuration settings (see Figure 2-2) of a wide range of assets, including:

- ☑ Operating systems (Windows, Unix, Linux)
- ☑ Databases (Oracle, MySQL, IBM DB2, Informix)
- ☑ Applications (Apache, IIS, Exchange, SharePoint)
- ☑ Web browsers (Internet Explorer, Firefox, Safari)
- ☑ Antivirus software (McAfee, Symantec, Trend Micro)
- ☑ Network infrastructure (firewalls, routers, switches)
- ☑ Virtual infrastructure (VMware, Hyper-V)



DMZ

DNS	Total	Vulnerabilities
tgtwxp3.devlab.tenablesecurity.com	392	22 252 42 74
rhel5x86.target.tenablesecurity.com	368	36 128 140 49
rhel5x64.target.tenablesecurity.com	342	34 122 122 49
centos5.target.tenablesecurity.com	300	29 98 117 48
winxppro4.target.tenablesecurity.com	299	175 43 65
winvistax86.target.tenablesecurity.com	260	17 131 42 68
rhel6x64.target.tenablesecurity.com	276	25 78 101 60
winvistax64.target.tenablesecurity.com	201	87 33 62
rhel6x86.target.tenablesecurity.com	256	58 89 85
rhel4.target.tenablesecurity.com	193	61 55 59

Last Updated: 16 hours ago

Weekly Detected Changes

Type	Count	Trend Data
access-denied	1382	
application	5195	
connection	7052	
continuous	2905	
data-leak	1076	
detected-change	4028	
dhcp	1021	
dns	383	
dos	914	
error	7494	

Last Updated: 16 hours ago

Last Updated: 18 hours ago

Last Updated: 21 hours ago

Figure 2-2: Real-time view of security configuration errors.

Patch auditing

Patch auditing, a feature available only in a select few NGVM solutions, integrates patch scanning with patch management system information to eliminate time-consuming manual comparisons needed to resolve discrepancies between network security and IT operations teams on the patch status of IT assets. This integration compares the results of vulnerability scanning against the status of patch management systems to identify inconsistencies.

NGVM solutions that support patch auditing commonly integrate with popular patch (and endpoint) management solutions, including:

- ☑ Microsoft Windows Server Update Services (WSUS)
- ☑ Microsoft System Center Configuration Manager (SCCM)
- ☑ VMware Go (formerly Shavlik)
- ☑ IBM Tivoli Endpoint Manager (TEM)
- ☑ Red Hat Network Satellite

Remediation scanning

Once a vulnerability system has been patched or its security configuration error rectified, cautious NGVM users may wish to re-scan the host to gain an additional level of assurance that it is no longer vulnerable. This practice, called remediation scanning, can often be triggered by a single mouse click when viewing the attributes of a single host record. But some rudimentary VM solutions require a scan job just for that host be manually configured.

Remediation scanning saves valuable time throughout the day when NGVM users wish to validate host remediation.

Malware detection

Although typical signature-based perimeter security defenses — such as intrusion prevention systems (IPSs), next-generation firewalls (NGFWs), and secure web gateways

(SWGs) — are excellent at detecting known threats, they often miss new and emerging threats, threats contained within portable media devices, and threats that compromise mobile devices used outside the office.

TECH TALK

Today’s leading NGVM solutions offer an additional layer of cyberthreat defense by detecting threats missed by perimeter security defenses. They do so through the following methods:

- ☑ Using credentialed scans to determine if currently running processes match known malware signatures
- ☑ Identifying hosts listed in a known bot database
- ☑ Scanning web applications to determine if they’ve been accessed by known bad DNS names or URLs
- ☑ Inspecting hosts for signs of compromise or rootkits

Management console tiering

Large, geographically dispersed enterprises often implement multiple NGVM management consoles to delegate administrative control to local IT security teams. Each IT security team constructs its own scan policies, manages its own NGVM users, and monitors the results of active/passive vulnerability scans and configuration audits.

Such organizations also have a centralized security operations center (SOC) to monitor the security posture of the entire enterprise from one location. Management console tiering enables vulnerability and configuration-auditing data from multiple NGVM management consoles to be aggregated to a master console at the SOC.

Although it’s entirely possible to replicate ALL data from underlying management consoles to the master console, in practice only data relevant to critical systems is filtered to the master console, preserving bandwidth across regional offices and disk space on the master console.

Chapter 3

Getting Started

In this chapter

- Understand the steps involved in getting your NGVM system up and running
- Pick up tips and tricks to maximize the security effectiveness of your NGVM investment

Whether you're replacing your legacy VM system with a modern NGVM solution, or you're initiating a new vulnerability management program from scratch, this chapter provides 10 actionable steps for getting your new NGVM solution up and running.

TIP

For tips on selecting the right NGVM solution for your environment, jump to Chapter 7.

10 Steps for Getting Started

These 10 steps are listed in a logical, methodical order. For example, you shouldn't attempt to design a solution before you've determined exactly which assets you need to scan. However, two pairs of steps are completely interchangeable: Steps 7 and 8 (constructing vulnerability scanning and configuration auditing policies) and Steps 9 and 10 (customizing dashboards and reports).

Step 1: Determine what to scan

The first step in getting started is to identify the assets that you want to scan, as well as those you want to exclude from scanning. Most organizations start with servers and network devices as they are mission critical to company operations.

Examples of assets typically scanned are:

- ☑ File servers
- ☑ Databases
- ☑ Web servers
- ☑ SMTP/POP servers
- ☑ FTP servers
- ☑ Firewalls
- ☑ Switches
- ☑ Load balancers
- ☑ LDAP servers
- ☑ Wireless access points

TIP

When configuring your active scan policies (more on that in Step 7), you'll need to specify ranges of IP addresses or a collection of individual IP addresses for hosts that you want to scan. Many NGVM solutions offer lightweight "discovery scans" to catalog network assets before performing a full-network vulnerability scan. Discovery scans help you to make better-informed decisions regarding which hosts to include and exclude in your scanning policies.

CAUTION

Active vulnerability scanning can occasionally crash systems such as Voice over IP (VoIP) phone systems and printers. Be sure to note the IP addresses of hosts you want to exclude from your active scanning policies.

Step 2: Architect your solution

Once you know which hosts you need to scan, you'll need to answer a few more questions to properly design your solution:

- ☑ Where are the hosts to be scanned located?
- ☑ How frequently will active scans be performed?
- ☑ Does the organization want to detect network vulnerabilities (and potential rogue hosts) in between active scans?
- ☑ What third-party systems will your NGVM solution need to integrate with? (More on that in Chapter 6.)

By answering these key questions, you and your vendor will be in a better position to design your NGVM solution. You'll need to determine how many active scanners you'll require to accommodate your workload, where the scanners should be positioned, and what third-party systems you'll need to integrate with.

But, there's another important consideration to ponder. Today's NGVM vendors offer three types of solutions: software, hardware (appliances), and software-as-a-service (SaaS) offerings.

DON'T FORGET

Most enterprises choose a software-based NGVM solution for the flexibility it provides. NGVM software can be installed on the organization's platform of choice and can even be deployed within virtual machines.

Software-based solutions are ideal for scanning both internal and external hosts. However, some vendors also offer a SaaS-based perimeter scanning service for organizations that want to scan externally facing assets in their DMZ (to demonstrate PCI compliance, for example).

Don't get your head stuck in the cloud

Some vendors claim to offer a 100 percent SaaS-based VM solution. But don't be fooled! You still need to deploy on-premises appliances — hardware or virtual, often numbering in the dozens or sometimes hundreds — across the enterprise to scan internal hosts. Vulnerability data collected by these appliances is not processed locally. Rather, your sensitive internal vulnerability data is sent to the vendor's cloud for aggregation and analysis, along with data from all of their other customers, posing an extraordinary risk to enterprises if the cloud were to become compromised.

A SaaS-based deployment for internal scanning has other drawbacks, as well. Whenever an organization wants to deploy an additional scanner, it must contact the vendor to purchase (or lease) another physical appliance or acquire a license key for a virtual appliance, thus causing a procurement delay and increasing the cost of the deployment. Also, today's so-called SaaS-only offerings often fall short in the functionality enterprises demand, such as passive vulnerability scanning and granular access control.

SaaS-based VM solutions — or NGVM solutions, for that matter — may be adequate for scanning assets in your DMZ, but they often fall short when it comes to scanning your internal infrastructure.

Step 3: Install your management console

Before deploying your active and passive scanners, it's best to install your management console software. That way, when you bring new scanners online, they can instantly connect to your management console to receive security intelligence updates and network scanning instructions.

DON'T FORGET

Management consoles are typically deployed at an organization's headquarters or security operations center (SOC). But remember, better NGVM providers support distributed management architectures for larger, geographically dispersed organizations. You may want to deploy multiple management consoles — one per geographic location — and implement a master management console at the SOC to aggregate critical security events.

Step 4: Deploy your active and passive scanners

With your management console (or consoles) up and running, it's time to deploy your active and passive scanners.

Active vulnerability scanners are essentially nodes on the network that actively probe hosts and network devices (i.e., initiate network connections with them) in search of vulnerabilities and security misconfigurations. For best results, you should deploy at least one active scanner for each local area network (LAN), as scanning hosts on the other end of a wide area network (WAN) can significantly extend the time necessary to complete a full network scan.

Popular active scanners, such as Nessus, require as little as 2GB of available memory to operate, although 4GB of memory is recommended for scanning larger networks. Active scanners usually support a variety of Windows, Unix, and Linux platforms. They can run on your own approved hardware or within VMware or other virtual machines.

CAUTION

If using an active scanner to scan both internal and perimeter hosts, do not place the scanner behind a NAT (network address translation) device as scan results may be distorted and false positives or negatives can occur.

TECH TALK

Unlike active scanners, which generate network traffic to function, passive scanners merely “sniff” (inspect) network traffic. When deploying passive vulnerability scanners, you’ll want to connect them to the network in a way that enables them to listen to the largest possible amount of network traffic. To this end, I recommend that you either connect them to the SPAN port of your network switches or interface them with aggregation TAPs or network packet brokers (NPBs) so a single passive scanner can inspect traffic from many network segments simultaneously. Just be sure the network interface card (NIC) is fast enough to keep up with the cumulative speed of your aggregated network segments.

Step 5: Assign user permissions

As I mentioned in the “Granular access control” section in Chapter 2, most enterprise IT security organizations follow the principle of least privilege, where you assign the least number of access permissions needed for IT users to do their jobs. This practice is commonly followed when assigning user permissions within NGVM systems.

TIP

Invest the time up front to identify the many types of users who will need to interface with your NGVM solution. Document the access permissions associated with each role so you don’t need to reinvent the wheel each time you create a new NGVM system user account.

Step 6: Categorize your assets

Grouping hosts into asset lists is a relatively new innovation in the VM/NGVM industry. Instead of manually tracking (static) IP addresses of grouped hosts, each host is essentially assigned metadata — such as business criticality, geography, host type, and business division — making it much simpler to monitor groups of hosts. This will help later on when creating policies.

Step 7: Construct vulnerability scanning policies

Constructing effective vulnerability scanning policies is critical to the success of any NGVM deployment. In this step, I discuss the differences between authenticated and unauthenticated scans, considerations for determining active scan frequency, and typical configuration settings associated with your vulnerability scanning policies.

Authenticated versus unauthenticated scans

A vulnerability scanner can only gather a fraction of the details about a system without authenticating to it. A scan without pre-configured administrative credentials is called an *unauthenticated scan*. Such scans can enumerate operating systems, network ports open on the system, and services listening on ports, and vulnerabilities associated with them. But the accuracy and thoroughness of this data will be much lower than if the scanner had authenticated to the system.

Authenticated scans (or *credentialed scans*) provide deeper and more-accurate assessment of the target systems. By pre-configuring your active scanners with administrative credentials (preferably dedicated to the scanning process), you'll know exactly which systems are vulnerable and how to remediate them.

DON'T FORGET

Most organizations perform a mix of both authenticated and unauthenticated scans. Unauthenticated scans are particularly useful to uncover vulnerabilities within custom web applications.

Determining your active scan frequency

Enterprises typically conduct full network scans on a quarterly basis. More security-savvy organizations conduct them monthly, while less-security-conscious organizations conduct them annually. The frequency at which an organization scans may be motivated by industry and/or governmental regulatory compliance standards (see Chapter 5) or simply based on its ability to keep up with processing scan results and patching systems.

TIP

Most organizations configure their scanners to operate during off-peak hours, such as evenings, weekends, and holidays. This is because scanners generate traffic that could, in certain circumstances, degrade network performance. And there's always the off chance that a scanner could disrupt an active IT system.

Typical vulnerability scanning policy settings

Today's vulnerability scanners offer dozens of configuration options. Following is a list of the most common ones:

- ☑ Range of target system IP addresses and system ports
- ☑ Administrative credentials for authenticated scans
- ☑ Maximum number of simultaneous target systems that can be scanned by a single scanner
- ☑ Maximum number of simultaneous plugins (or checks) that can be run against a single target host
- ☑ SMTP settings to automatically email scan results to predetermined recipients
- ☑ Automatic plugin update frequency
- ☑ Use of IPv4 and/or IPv6 protocols for scanning

TIP

In preparation for your first active scan, I recommend you start small with an initial scanning policy for a small number of critical systems, and limit the scope of vulnerabilities to those with known exploits granting remote access. That way, you won't be overwhelmed with thousands of identified vulnerabilities in your first scan.

Step 8: Construct configuration auditing policies

Better NGVM solutions offer the ability to scan hosts and network devices for security misconfigurations that violate internal acceptable use policies (AUPs) and/or external compliance regulations. When configured properly, your NGVM system can detect a variety of misconfigurations:

- ☑ Unauthorized applications and protocols
- ☑ Unnecessarily opened ports
- ☑ Violations of minimum password strength
- ☑ Default accounts with default passwords

- ☑ Improper file and directory permissions
- ☑ Misconfigured encryption settings
- ☑ Use of default SSL certificates

Be sure to leverage your management console's library of policy templates for a head start in constructing effective configuration auditing policies.

Step 9: Customize your dashboards

In organizations that conduct frequent active scans and/or have implemented a real-time continuous monitoring solution, a customizable dashboard is the primary interface for security analysts to monitor security posture. A good dashboard should adapt to the needs of the user, rather than forcing the user to adapt to an inflexible dashboard. A good dashboard should also enable users to "drill down" into data displayed in intuitive charts, graphs, and tables, making it easy to find the data they're looking for.

TIP

Better NGVM providers offer a choice of multiple dashboard templates to accommodate any role within the organization.

Step 10: Customize your reports

While security analysts primarily interface with dashboards, IT security management and compliance auditors generally access the information they need through reports.

A good NGVM management console will offer a variety of pre-built reports. The reporting engine must enable users to customize reports to meet their specific needs.

Chapter 4

The Case for Continuous Monitoring

In this chapter

- Learn why active scanning alone is not sufficient for mitigating today's cyberthreats
- Discover how continuous monitoring can drastically improve your network's security posture

Imagine you're the head of security for a new bank. An obvious security precaution is to install closed-circuit television (CCTV) surveillance cameras at strategic points, including the main entrance and in front of each teller window. Now, further imagine that one of the CCTV vendors offered you an amazing discount, but his cameras only capture one still image every three months. Would you buy it? Of course not! To adequately protect your bank's assets, you must remain vigilant with a constant, 24 x 7 video feed.

Conducting just one full network scan per quarter is like taking one snapshot of your network every three months. It's certainly helpful to understand your security posture at a given moment, but as new vulnerabilities are disclosed virtually every hour of the day, it's critical to maintain a continuous view of your network's security posture — 24 x 7 x 365. Thus, continuous monitoring was born.

This chapter defines continuous monitoring, identifies its core components, and illustrates continuous monitoring use cases not possible with periodic scanning alone.

Defining Continuous Monitoring

Continuous monitoring, in the context of NGVM, is the process of constantly and persistently monitoring network assets (both known and unknown), vulnerabilities, and security configurations in an effort to reduce the network's attack surface and mitigate cyberthreats. Core components of a continuous monitoring solution include:

- ☑ **Active scanners** to establish a baseline of assets and scan for vulnerabilities and security misconfigurations
- ☑ **Passive scanners** to monitor for rogue hosts, detect suspicious network anomalies, and identify vulnerabilities and security misconfigurations in between full active network scans
- ☑ **Log aggregators** to compile logs from internal systems to identify new hosts on network segments not monitored by passive scanners
- ☑ **Management console** to aggregate vulnerability and security configuration intelligence and communicate results through dashboards and reports

DON'T FORGET

It should be obvious by now that the "secret sauce" of any continuous monitoring solution is the combination of passive vulnerability scanning and log aggregation and correlation. Without these critical capabilities, you've got just another VM solution.

CAUTION

An existing SIEM (security information and event management) platform, like those referenced in Chapter 6, cannot participate in a continuous monitoring solution as it's not designed to import host data into the NGVM management console. Better NGVM vendors offer a purpose-built log management / SIEM solution specifically designed to operate within an NGVM environment.

Origins of Continuous Monitoring

Continuous monitoring became mainstream in September 2011 when the National Institute of Standards and Technology (NIST) released Special Publication (SP) 800-137 — one of many NIST publications tied to FISMA compliance. NIST SP 800-137 is designed to assist federal organizations in developing a continuous monitoring strategy. It cites the following essential processes:

- ☑ Ongoing assessment of security controls
- ☑ Configuration management and change control
- ☑ Security impact analysis
- ☑ Security status reporting

Although the NIST publication was intended for consumption by U.S. federal agencies, the concept of continuous monitoring is spreading to security-conscious commercial organizations at a rapid pace.

ON THE WEB

To download NIST SP 800-137 or other NIST publications, connect to http://csrc.nist.gov/publications/PubsSPs.html.

CAUTION

Some vendors have interpreted continuous monitoring to mean more-frequent scanning (weekly or daily). Others have added the ability to run continuous active scans, where as soon as one scan finishes, another one starts in hopes of capturing new devices. In reality, this is not an adequate solution, but rather a problem resulting in substantial overhead and network impact.

An NGVM solution provides the flexibility to continually monitor for new assets and vulnerabilities in real time, offering the most complete visibility to assets and vulnerabilities.

Why periodic scanning isn’t enough

When you scan your network periodically — even monthly — at best your vulnerability intelligence is accurate 12 times per year.

If you’re motivated to invest in NGVM simply because you’re trying to tick a regulatory compliance checkbox, then jump to the next chapter. But if you’re serious about security, read on, because there are lots of ways that continuous monitoring can help.

Continuous Monitoring Use Cases

Continuous monitoring is a critical component of any sensible *defense-in-depth* (layers of security defenses) strategy. It provides enterprises new ways to reduce a network's attack surface while identifying threats that have slipped past traditional security defenses.

Prioritizing patching efforts

Although most enterprises regularly patch systems on 30-, 60-, or 90-day cycles, from time to time critical vulnerabilities occur that, if not immediately corrected, may expose the organization to extraordinary risk. As continuous monitoring provides 100 percent real-time asset discovery, IT can better prioritize both scheduled and out-of-band patching efforts to more efficiently and effectively reduce network security risks.

Identifying policy violations

Many enterprises document internal policies regarding approved system configurations and use of network resources, but few organizations have the means to monitor for policy compliance. Continuous monitoring can help organizations identify all sorts of policy violations, such as:

> ☑ Use of unauthorized client applications, such as Facebook, Twitter, FTP, Skype, iTunes, and more
>
> ☑ Use of expired SSL certificates
>
> ☑ Use of autocomplete for password fields
>
> ☑ Use of plain text password authentication
>
> ☑ Use of persistent cookies

Providing context for IPS and NGFW platforms

Most IPS and next-generation firewall (NGFW) solutions lack contextual awareness for analyzing security events and for tuning (optimizing) the threat detection policy. Here's how continuous monitoring can bridge that gap.

TECH TALK

Exporting endpoint and vulnerability intelligence to SIEMs and correlating it against threats detected by your IPS and NGFW devices helps prioritize security events so analysts can focus attention on those that really matter (e.g., the exploit matches the target operating system and that OS is vulnerable). This can reduce the number of actionable (or applicable) security events by more than 95 percent, saving tremendous time and resources.

In addition, tuning the threat-detection policy (i.e., selecting applicable threat signatures) of your IPS or NGFW accomplishes two objectives: (1) ensuring you have the appropriate signatures to protect your network's assets; and (2) optimizing the number of signatures enabled to maximize the performance of your network security devices. If you enable all of your threat-detection signatures, your IPS or NGFW may slow to a crawl.

Monitoring web applications

Large enterprises commonly deploy custom web applications. Although these are web services, they don't always run on common HTTP ports, such as ports 80 and 443, causing organizations to miss auditing many of their critical assets.

Continuous monitoring secures custom web applications by identifying risks within HTTP and HTTP services (regardless of port), SSL certificates, and potentially insecure or hostile web content.

Detecting internal threats

Beyond detecting system vulnerabilities and security misconfigurations, leading NGVM platforms capable of continuous monitoring are useful for identifying threats emanating from within the network, such as:

☑ Detecting rogue hosts planted on the inside

☑ Detecting unusual encrypted sessions

☑ Detecting non-standard VPN clients

☑ Detecting hosts connecting to known-bad websites

U.S. Department of Defense arms itself with continuous monitoring

The Defense Information Systems Agency (DISA) is a U.S. Department of Defense (DoD) combat support agency that provides IT and communications support to the President, Vice President, Secretary of Defense, and military services. Recently, DISA evaluated leading VM solutions to serve as the foundation for its new Assured Compliance Assessment Solution (ACAS). DISA established ACAS to replace the outdated Secure Configuration Compliance Validation Initiative (SCCVI) suite of software, which lacked a continuous monitoring capability — now a key component for FISMA compliance.

DISA evaluated several leading VM solutions against the following technical objectives:

- Support enterprise-wide VM deployment across the DoD, with the ability to tier system management
- Provide fast and accurate enterprise-wide network security assessment
- Implement real-time risk assessment across DoD networks to provide situational awareness and enable informed risk-based management decisions consistent with federal guidelines for continuous monitoring

After conducting a series of on-site evaluations, DISA concluded that only one vendor offered a solution that met all of its criteria — Tenable Network Security (www.tenable.com). Tenable's award-winning SecurityCenter platform incorporates Nessus Vulnerability Scanner and Passive Vulnerability Scanner (PVS) software as part of its highly scalable NGVM continuous monitoring solution.

Since Tenable SecurityCenter is 100 percent software based, the DoD can roll out new instances without the need to procure and install hardware appliances. Tenable's automated load-balancing capability makes supporting the DoD's largest networks a cinch. And no other NGVM offering can match Tenable's unique management console tiering ability, which allows DISA to aggregate security data in one central location in support of its mission.

To learn more about ACAS and DISA's use of Tenable SecurityCenter as its foundation for continuous monitoring, connect to: http://www.disa.mil/Services/Information-Assurance/SCM/ACAS.

Chapter 5

Achieving and Sustaining Regulatory Compliance

In this chapter

- Review common government and industry regulatory frameworks required for today's enterprises
- Learn how NGVM can help enterprises achieve and sustain regulatory compliance

IT organizations spend millions of dollars trying to meet the requirements of, and demonstrate ongoing compliance with, industry and government regulations pertaining to information security. Continuous monitoring aids these compliance initiatives by proactively identifying issues prior to an audit. Log analysis further helps by isolating recurring security issues and providing proof of compliance.

CAUTION

Vendors that separate compliance and vulnerability management capabilities into separate modules prolong regulatory compliance processes. These solutions should be highly integrated. A unified NGVM system, for example, can enable a user to trace the root cause of a compliance issue to an unpatched system compromised by a botnet. Such automated insight is nearly impossible with separate VM and compliance functions.

In this chapter, I discuss how VM — and to a larger extent, NGVM — plays an important role in helping IT organizations achieve and sustain compliance with four of the most common regulations facing enterprises today.

Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS (or just PCI, for short) was established in 2004 by the five founding brands of the PCI Security Standards Council: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, and Visa, Inc. The objective of PCI is to increase controls on credit card data to reduce organizations' exposure to credit card theft.

ON THE WEB

PCI DSS v2.0 is comprised of 12 high-level requirements and 221 sub-requirements. You can access all PCI documentation at http://www.pcisecuritystandards.org. PCI DSS v3.0 is expected in November 2013. No changes regarding vulnerability assessments are anticipated.

The process of validating PCI compliance varies based on an organization's annual credit card transaction volume. Merchants that process more than 6 million Visa and/or MasterCard transactions or more than 2.5 million American Express transactions annually (categorized as level 1 merchants) must hire a PCI Security Standards Council-approved qualified security assessor (QSA) to conduct an annual report on compliance (ROC). Merchants that process fewer credit card transactions annually (level 2, 3 and 4 merchants) may demonstrate compliance by completing a self-assessment questionnaire (SAQ).

TECH TALK

Some credit card companies, such as Visa, permit level 1 merchants to facilitate annual ROC reports using internal employees certified by the PCI Security Standards Council as internal security assessors (ISAs), providing the ROC report is signed by an officer of the company prior to submission. This is an alternative to using external QSAs.

ON THE WEB

Regardless of whether an organization submits a ROC or an SAQ to demonstrate compliance, it must use a VM (or NGVM) solution from an approved scanning vendor (ASV) to conduct quarterly vulnerability scans of the organization's Internet-facing systems. To determine whether a VM (or NGVM) vendor is an ASV, connect to: https://www.pcisecuritystandards.org/approved_companies_providers/approved_scanning_vendors.php.

Although PCI isn't law, credit card companies enforce compliance by imposing contractual penalties and sanctions, including revocation of a merchant's right to process credit card transactions.

VM (and certainly NGVM) plays a significant role in demonstrating PCI compliance. In fact, you can't achieve PCI compliance without a VM solution from an ASV. Table 5-1 lists several of the high-level PCI requirements (paraphrased for brevity) that a VM (or NGVM) solution can help satisfy.

Req.	*PCI DSS 2.0 Standard*
1.4	Install personal firewall software on mobile devices with Internet connectivity
2.1	Always change vendor-supplied defaults before installing a system on the network
2.2	Develop industry-accepted configuration standards for all system components
2.3	Encrypt all non-console administrative access
4.1	Use strong cryptography and security protocols to safeguard sensitive cardholder data
5.1	Deploy anti-virus (AV) software on all systems
5.2	Ensure that all AV mechanisms are current
6.1	Ensure that all system components are protected from known vulnerabilities
6.2	Establish a process to identify and assign a risk ranking to newly discovered vulnerabilities
6.6	For public-facing Web applications, address new threats and vulnerabilities on an ongoing basis
11.1	Test for the presence of wireless access points
11.2	Run internal and external network vulnerability scans at least quarterly and after any significant change to the network

Table 5-1: Sample PCI requirements satisfied by VM

Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is maintained by the U.S. Department of Health & Human Services (www.hhs.gov). Designed to protect the confidentiality and integrity of patient health information (PHI), HIPAA had only a muted effect on the security industry until 2009, when the Health Information Technology for Economic and Clinical Health Act (HITECH) imposed mandatory audits and fines for noncompliance.

Penalties for noncompliance range from $100 to $50,000 per violation (up to $1.5 million in a calendar year), depending on whether the violation relates to willful neglect. Also, personnel who knowingly disclose PHI face a prison sentence of up to 10 years.

As with PCI, VM technology is essential for HIPAA compliance. Table 5-2 summarizes the high-level sections of HIPAA satisfied, in whole or in part, by VM capabilities.

Section	*Topic*
§ 164.308(a)(1)	Security Management Process
§ 164.308(a)(4)	Information Access Management
§ 164.308(a)(5)	Security Awareness Training
§ 164.308(a)(6)	Security Incident Procedures
§ 164.310(c)	Workstation Security
§ 164.310(d)(2)	Device and Media Controls
§ 164.312(a)(1)	Access Control
§ 164.312(b)	Audit Control
§ 164.312(c)	Integrity
§ 164.312(e)	Transmission Security

Table 5-2: HIPAA requirements addressed by VM

ON THE WEB

For more information about HIPAA, connect to: http://www.hhs.gov/ocr/privacy/index.html.

North American Electric Reliability Corporation (NERC)

The North American Electric Reliability Corporation (NERC; www.nerc.com) is a not-for-profit organization with a mission to “ensure the reliability of the North American bulk power system.” It encompasses the interconnected SCADA power grids of the United States, Canada, and a portion of Baja California, Mexico. (See the “Special considerations for SCADA networks” sidebar for more information on SCADA.)

Following the passage of the Energy Policy Act of 2005, funding for an “Electric Reliability Organization” was approved by the U.S. government (and later Canada) to develop and enforce cybersecurity compliance standards for organizations contributing to the U.S. power grid. In 2006, NERC applied for and was granted this designation. That same year, NERC introduced its Critical Infrastructure Protection (CIP) Reliability Standards, labeled CIP-002 through CIP-009. In 2009, it approved version 2 of these standards and began auditing Registered Entities for compliance.

As of June 30, 2010, all Registered Entities must prove “auditable compliance” with all eight categories of CIP controls on a semi-annual basis. Failure to meet any one standard may result in financial penalties of up to $1 million per day, depending on risk and severity.

Of the eight categories of CIP controls, six have components related to VM:

☑ **CIP-002:** Critical Cyber Asset Identification

☑ **CIP-003:** Security Management Controls

☑ **CIP-005:** Electronic Security Perimeter(s)

☑ **CIP-007:** Systems Security Management

☑ **CIP-008:** Incident Reporting and Response Planning

☑ **CIP-009:** Recovery Plans for Critical Cyber Assets

ON THE WEB

For more information on NERC standards, connect to: http://www.nerc.com/pa/Stand/Pages/default.aspx.

Special considerations for SCADA networks

SCADA (supervisory control and data acquisition) is a term used for computer-controlled systems that monitor and control industrial processes that exist in the physical world. Examples of SCADA systems include power generation, oil refining, water treatment systems, and manufacturing.

From a technology point of view, SCADA networks (that run over routed protocols like IP) are just like any other network. They have various nodes that communicate over various protocols. They are subject to the same sorts of attacks as traditional computer networks. And SCADA manufacturers make the same programming mistakes (causing exploitable vulnerabilities) that Microsoft, Adobe, and other software vendors make.

But SCADA systems are also unique in that aggressive port scanning by typical vulnerability scanners can negatively affect their performance. Vulnerability scans have been responsible for crashing SCADA devices, disrupting processes, and causing erroneous displays in control centers.

To uncover vulnerabilities on SCADA networks without disrupting performance, special precautions must be taken. First, only use active vulnerability scanners that have SCADA plugins (or checks) specifically designed to identify popular SCADA systems, services, and protocols (such as DNP3, ICCP, and MODBUS) and identify their inherent vulnerabilities — all without adversely affecting performance or availability. Second, leverage passive vulnerability scanners — also equipped with SCADA plugins — to monitor systems in between periodic active scans.

Maintaining the integrity and availability of SCADA systems is serious business. In some environments, it can mean the difference between life and death. If you're responsible for securing a SCADA environment, take the time to sit down with prospective NGVM vendors to thoroughly understand their SCADA scanning abilities.

Federal Information Security Management Act (FISMA)

The Federal Information Security Management Act of 2002 (FISMA) assigns certain responsibilities to U.S. government agencies to ensure the confidentiality, integrity, and availability of federal government data. The act requires program officials to conduct annual reviews of information security programs. However, as of September 2012, the Office of Management and Budget (OMB) requires monthly data feeds to be sent to its new CyberScope application portal (see "CyberScope targets FISMA reporting" sidebar).

Several publications from the National Institute of Standards and Technology (NIST) provide guidance on FISMA compliance, including the use of Security Content Automation Protocol (SCAP)-compliant VM solutions to facilitate FISMA reporting. The following four publications are particularly relevant to VM (and NGVM) solutions:

- ☑ **NIST 800-37:** Guide for Applying the Risk Management Framework to Federal Information Systems
- ☑ **NIST 800-53:** Recommended Security Controls for Federal Information Systems and Organizations
- ☑ **NIST 800-128:** Guide for Security-Focused Configuration Management of Information Systems
- ☑ **NIST 800-137:** Information Security Continuous Monitoring for Federal Information Systems

ON THE WEB

To view the full text of FISMA regulations, connect to: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf. To access NIST 800-series Special Publications (related to information security), connect to: http://csrc.nist.gov/publications/PubsSPs.html.

CyberScope targets FISMA reporting

The U.S. Department of Homeland Security, in conjunction with the U.S. Department of Justice, has developed a web-based application (launched by the OMB) called "CyberScope" to standardize manual and automated data inputs for FISMA compliance reporting. FISMA reporting used to take place annually, but with CyberScope that requirement is now monthly.

NIST has assisted by providing data models within CyberScope that leverage existing SCAP (pronounced "ess-cap") primitives (developed by the National Vulnerability Database, or NVD), including:

- ▶ Common Vulnerabilities and Exposures (CVE)
- ▶ Common Vulnerability Scoring System (CVSS)
- ▶ Common Configuration Enumeration (CCE)
- ▶ Common Platform Enumeration (CPE)

All U.S. federal agencies subject to FISMA must select VM products capable of processing CyberScope-compliant data feeds. Such products must also be designated by NIST as SCAP validated. For a list of SCAP-validated VM products, connect to: http://nvd.nist.gov/scapproducts.cfm.

McKesson prescribes NGVM solution for regulatory compliance

McKesson Corporation, ranked 14th on the 2013 FORTUNE 500 list, is a healthcare services and information technology company dedicated to making the business of healthcare run better. McKesson employs over 32,500 workers in more than 50 locations around the globe. The company partners with hospitals, physician offices, and pharmaceutical companies to improve their financial, operational, and clinical performance with solutions that include pharmaceutical supply management, healthcare information technology, and business and clinical services.

Like most large enterprises, McKesson struggled with the day-to-day challenges of mitigating network vulnerabilities while demonstrating regulatory compliance. Unlike most organizations that are only subject to one or two regulations, McKesson faces five — HIPAA, PCI, Sarbanes-Oxley (SOX), HITRUST (Health Information Trust Alliance), and FISMA.

Rather than relying on multiple vulnerability scanners with varying capabilities, McKesson's CISO decided it was time to standardize on one enterprise-class NGVM solution — one that not only offered best-in-class vulnerability detection, but also automated compliance reporting for all five regulations affecting the business.

After a thorough investigation and multiple on-site product evaluations, McKesson selected Tenable SecurityCenter (www.tenable.com). McKesson chose the Tenable solution because of its massive library of 50,000+ Nessus vulnerability plugins, passive vulnerability scanning capability in support of continuous monitoring, automated scanner load balancing capability that accelerates full network scans, and daily security intelligence updates. Plus, Tenable offers a library of compliance policy templates, dashboards, and reports that is second to none.

Since deploying Tenable SecurityCenter, McKesson's IT security staff has drastically reduced its regulatory compliance efforts while gaining deeper insight into network vulnerabilities and security misconfigurations.

Chapter 6

Integrating NGVM with Your Existing Infrastructure

In this chapter

- Understand the value of integrating NGVM into your existing network and security infrastructure
- Learn the fundamentals of integrating NGVM systems with popular third-party products

In today's complex and ever-changing cyberthreat environment, you need all the help you can get to stay ahead of the bad guys. A well-coordinated defense-in-depth strategy is your best bet to avert successful attacks. But if the pieces of your security defense puzzle don't fit well together, cyberthreats will almost certainly slip through the cracks.

NGVM is the cornerstone of an effective cybersecurity program. Since *advanced persistent threats (APTs)* and other targeted attacks penetrate your network by exploiting an underlying system vulnerability, mitigating those vulnerabilities in the first place is a huge step in fighting advanced threats.

In this chapter, I identify the most common network and security infrastructure platforms appropriate for NGVM integration. Along with identifying sample vendors in each product category, I describe common third-party integration techniques and the resulting benefits from multi-product integration.

Security Information and Event Management (SIEM)

A SIEM (pronounced “sim”) is often described as a “single pane of glass” for monitoring security events across an entire enterprise. Security analysts in enterprise SOCs usually often monitor SIEM consoles more than the consoles of all other security products combined.

SIEMs are designed to aggregate data (usually log data) from dozens of sources, including virtually all of your network security products, plus many of your network infrastructure systems. A SIEM is equipped with dozens of rules to correlate disparate sources of information and uncover hidden threats. It also aggregates security alerts from your various security products so analysts have one dashboard to monitor to gauge the security posture of the organization.

An NGVM platform can export all — or just a subset — of the vulnerability data it collects to your SIEM of choice through automated syslog uploads at pre-defined intervals or in real time by using the NGVM vendor’s API. NGVM solutions benefit SIEMs by forwarding security and compliance intelligence not only from active vulnerability scanners, but also integrated passive vulnerability scanners and log correlation engines.

DON’T FORGET

As I reference in Chapter 4, leading NGVM vendors offer SIEM / log correlation engine solutions that are tightly integrated with the NGVM management console. Although these solutions are intended to identify new hosts as part of a continuous monitoring solution, they may also satisfy an organization’s larger need for full-fledged SIEM functionality. Typical SIEM offerings from NGVM vendors provide log aggregation and normalization, full-text search, correlation rules, flow analysis, forensics support, and more. So if you’re in the market for both NGVM and SIEM solutions, evaluate NGVM platforms first. Your NGVM vendor just might have the SIEM you’re looking for.

Sample vendors: HP (ArcSight), IBM (QRadar), LogRhythm, Novell (Sentinel), RSA (enVision), Splunk, and Symantec (SMS)

Perimeter Security Defenses

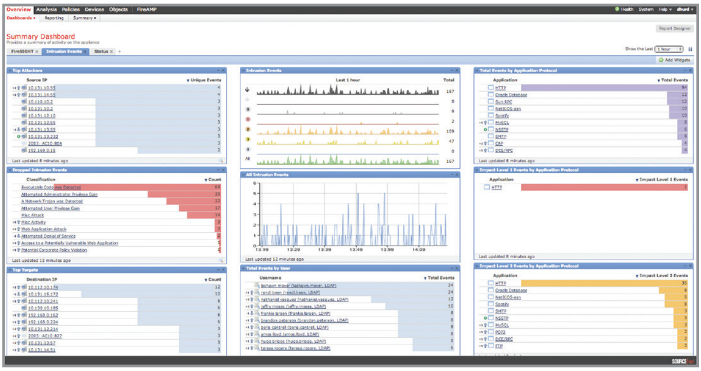
Traditional perimeter security defenses leverage threat-detection signatures (or rules) to detect known exploits. These devices are highly accurate at identifying threats; however, they may generate thousands of security events daily. Prioritizing security events to determine which ones really matter can be a time-consuming, painstaking process.

"Tuning" these devices by selecting signatures that are relevant to your environment is also a cumbersome process. If you enable too many signatures, the performance of your security device is diminished. Conversely, enabling too few signatures puts your organization at risk.

NGVM platforms provide rich intelligence to perimeter security defenses so security analysts can prioritize security events and optimize the detection policies of these devices. Examples of such perimeter security defenses follow.

Intrusion Prevention Systems (IPS)

An inline IPS (or passive IDS) is a security device that sits right behind the firewall to detect a myriad of cyberthreats. Some IPS solutions, such as Sourcefire (see Figure 6-1), offer automated threat-to-target correlation within their own management consoles, leveraging real-time vulnerability intelligence imported from NGVM solutions.



Summary Dashboard
Provides a summary of activity on the appliance

Top Attackers

Source IP	Unique Events
10.131.10.55	4
10.131.14.55	4
10.110.10.2	3
10.131.10.2	3
10.131.12.10	3
10.131.12.55	3
10.131.13.55	3
10.131.13.222	3
2003::AC10:80A	3
192.168.0.15	2

Last updated 8 minutes ago

Intrusion Events

Last 1 hour	Total
↓	167
	0
0	9
1	2
2	109
3	47
4	0
All	167

Total Events by Application Protocol

Application	Total Events
HTTP	94
Oracle Database	12
Sun RPC	12
NetBIOS-ssn	10
Spotify	10
MySQL	6
NSSTP	6
SMTP	6
CAP	4
DCE/RPC	4

Last updated 8 minutes ago

Dropped Intrusion Events

Classification	Count
Executable Code was Detected	69
Attempted Administrator Privilege Gain	30
A Network Trojan was Detected	22
Attempted User Privilege Gain	17
Misc Attack	14
Misc Activity	3
Web Application Attack	3
Attempted Denial of Service	2
Access to a Potentially Vulnerable Web Application	1
Potential Corporate Policy Violation	1

Last updated 12 minutes ago

All Intrusion Events

Last updated 12 minutes ago

Impact Level 1 Events by Application Protocol

Application	Impact Level 1 Events
HTTP	1

Last updated 8 minutes ago

Top Targets

Destination IP	Count
10.112.10.174	12
10.131.15.172	10
10.112.10.241	6
10.130.10.185	6
192.168.0.162	6
192.168.0.224	6
10.131.12.214	3
2003::AC10:827	3
10.131.13.57	3
10.131.14.51	3

Total Events by User

Username	Total Events
lashawn mover (lashawn.mover, LDAP)	24
randi bean (randi.bean, LDAP)	24
nathaniel vasquez (nathaniel.vasquez, LDAP)	12
jeffry moses (jeffry.moses, LDAP)	10
frankie larsen (frankie.larsen, LDAP)	8
brandon peterson (brandon.peterson, LDAP)	8
boris cantrell (boris.cantrell, LDAP)	8
amos lloyd (amos.lloyd, LDAP)	8
hugo briggs (hugo.briggs, LDAP)	6
teresa rogers (teresa.rogers, LDAP)	6

Impact Level 2 Events by Application Protocol

Application	Impact Level 2 Events
HTTP	35
Oracle Database	6
NetBIOS-ssn	5
Spotify	5
SMTP	3
NSSTP	3
MySQL	3
POP3	2
DCE/RPC	2
FTP	2

Figure 6-1: Sourcefire dashboard displays correlated intrusion events by severity

Sample vendors: Check Point, Cisco, HP, IBM, Juniper, McAfee, and Sourcefire

Next-Generation Firewalls (NGFW)

An NGFW is a multi-function perimeter security device that incorporates three main security components — firewall, IPS, and application control. Some NGFW vendors also offer URL filtering and on-board SSL decryption.

Sample vendors: Check Point, McAfee (Stonesoft), Palo Alto Networks, and Sourcefire

Unified Threat Management (UTM)

A UTM is also a multi-function perimeter security device that is primarily used by small-to-midsize organizations. Like an NGFW, UTMs incorporate firewall, IPS, and application control functions, but may also include antivirus, antispam, data loss prevention (DLP), and other capabilities.

Sample vendors: Check Point, Dell SonicWALL, Fortinet, Sophos (Astaro), and WatchGuard

Risk Management

NGVM integration with a variety of risk management products helps automate key functions of the risk management process — including asset discovery and vulnerability assessment — into one consolidated view. The combined solution affords enterprises the ability to model their network topology, gauge network vulnerability status, and determine which vulnerable systems can actually be accessed.

Sample vendors: Core Security, Firemon, RedSeal, Risk I/O, and RSA Archer Technologies

Mobile Device Management (MDM)

Mobile devices are now a pervasive part of the enterprise IT landscape, driven in part by company-approved *BYOD* (bring your own device) initiatives. Although the proliferation of smartphones and tablets has dramatically increased employee productivity and responsiveness, inherent vulnerabilities within mobile device operating systems and applications introduce new risks that most organizations are ill-equipped to mitigate.

Thankfully, NGVM vendors are now expanding their vulnerability coverage to uncover both vulnerabilities and security misconfigurations within network-connected mobile devices. Some have also begun to integrate their products with mobile device management (MDM) solutions to monitor these devices even when active and passive vulnerability scanning is not possible. NGVM/MDM integration delivers the following benefits:

- ☑ Enumerate iOS, Android, and Windows mobile devices accessing the corporate network
- ☑ Detect known mobile vulnerabilities, including out-of-date OS versions
- ☑ Provide detailed mobile device information, including serial number, model, version, timestamp of last connection, and user
- ☑ Discover jailbroken iOS devices

Sample vendors: AirWatch, Apple (Profile Manager), Citrix (XenMobile), Fiberlink, Good Technology, Microsoft (ActiveSync), MobileIron, and SAP (Afaria)

Incident Management

Although most NGVM solutions offer a built-in incident management (ticketing) capability, many enterprises prefer to leverage their existing incident management platform for receiving, prioritizing, and assigning critical security events.

Some NGVM solutions integrate with external incident management applications by way of an API, while others simply generate automated emails to be received and processed by the incident management system.

Sample vendors: BMC (Remedy), CA, HP, and IBM

Access Management

In Chapter 3, I describe the immense value that authenticated scans deliver compared to unauthenticated scans. But, of course, one of the challenges of authenticated scans is safely managing administrative credentials configured within the NGVM management console.

To mitigate this concern, some enterprises are turning to access management vendors for the answer. These vendors offer robust password vault solutions that centrally manage and encrypt administrative passwords. This helps mitigate the risk of stolen credentials, which especially concerns customers leveraging SaaS-based VM solutions.

Sample vendors: Cyber-Ark and Thycotic

Patch Management

Better NGVM systems enable users to audit the efficacy of their patch management solutions. Active vulnerability scanners scan the environment for vulnerabilities and then correlate discovered vulnerabilities with those reportedly patched by the patch management system. This quickly identifies inconsistencies that may result.

TECH TALK

To configure patch auditing, patch management system credentials are entered into the NGVM management console and special Patch Management Windows Auditing Conflicts plugins are used by the scanners.

Sample vendors: IBM (TEM), Microsoft (WSUS and SCCM), VMware (Go), and Red Hat (Network Satellite)

Penetration Testing

“Pen tests” attempt to compromise systems by simulating the actions of an attacker. Experienced NGVM users often turn to penetration testing to better understand their risk. Integrating vulnerability scanning results into the pen testing console better equips the pen tester to identify the cost and consequences of exposure.

Sample vendors: Core Security and Immunity

Chapter 7

Selecting the Right VM Solution

In this chapter

- Recognize telltale signs of inferior vulnerability management offerings
- Know what to look for when evaluating enterprise-class VM solutions

Like most information security products, no two VM solutions are alike. Some focus purely on single-scanner vulnerability assessment (i.e., no management console or scanner load balancing) for small to medium-size businesses, while others offer full-featured, continuous monitoring for the enterprise.

Selecting the right VM solution is a critical decision for any enterprise — especially given the volume and sophistication of today's cyberthreats. In this chapter, I provide 10 criteria to consider when evaluating VM solutions — some related to the product and some to the provider. But before I describe what you should look for, I'd like to take a few moments to educate you about what to avoid:

- ☑ Avoid solutions that don't offer a passive vulnerability scanner or log correlation engine for continuous monitoring.
- ☑ Stay away from solutions that only issue security intelligence updates (with new plugins) weekly rather than daily.
- ☑ Bypass solutions that require a degree in rocket science to use.

☑ Steer clear of solutions that offer little to no integration with your existing security infrastructure.

☑ Rule out solutions that take several days (or possibly weeks) to complete one full network scan.

☑ Be wary of so-called SaaS-only solutions that require you to lease the vendor's scanner hardware appliances, inhibiting your ability to deploy new scanners at will.

TIP

IT researcher Gartner publishes an annual report called "MarketScope for Vulnerability Assessment." In it, Gartner rates more than 10 leading VM vendors on a five-point scale, as follows (from worst to best): Strong Negative, Caution, Promising, Positive, and Strong Positive. When creating a shortlist of VM vendors to consider, start with those designated by Gartner as "Strong Positive." You'll be glad you did.

Let's now review the 10 most important criteria to consider when shopping for an enterprise-class VM solution.

Support for Continuous Monitoring

DON'T FORGET

If I had to pick one attribute of an enterprise-class VM solution that, frankly, is a "showstopper" if missing, it would be continuous monitoring. That's why I dedicated an entire chapter to this important topic.

TIP

For a refresher on the components and value of continuous monitoring, flip back to Chapter 4.

Without continuous monitoring, visibility into vulnerabilities and security misconfigurations of your mission-critical systems will only be accurate once every month, quarter, or year, depending on your active scanning frequency. You might be satisfying the "meets minimum" requirement of PCI, HIPAA, or other industry regulation, but you certainly won't be improving your network's security posture. And you won't be leveraging your VM investment to its fullest potential.

CAUTION

Beware of VM vendors that tout a continuous monitoring capability without a passive vulnerability scanner or log correlation engine in their product portfolio. These vendors may offer a feature that automatically triggers the next active scan immediately following completion of the last active scan. Although increasing the frequency of active scanning is good, it pales in comparison to what organizations can uncover with real-time passive vulnerability scanning — especially since active scans usually take place at night when laptops and other mobile devices aren't connected to the network.

Flexible Deployment Options

Enterprises like choices. Some prefer to deploy vulnerability scanner software on vendor-provided hardware appliances. Others (most, actually) prefer to distribute scanner software on their own company-approved hardware platforms and operating systems, or as pre-packaged VMware virtual appliances. Still others prefer to leverage cloud-based scanning solutions for scanning perimeter assets.

Regardless of your preferred scanner platform — vendor-provided or homegrown — it's best to select a VM provider that supports all of the aforementioned scanner delivery options. You may prefer one scanner delivery model at headquarters and another for smaller branch offices. Or you simply might change your mind down the road.

DON'T FORGET

One advantage of software-only scanners (that you deploy on your own hardware and operating system) is that usually the VM vendor licenses its software based on monitored IP addresses, thus providing scanner software at no charge. The benefit here is that you can deploy five scanners or 500 scanners without paying an additional penny. This affords you the freedom to design a solution that is right for your environment without having to worry about how many scanner software licenses to purchase.

CAUTION

One more thing: beware of so-called SaaS-based VM solutions that tout their 100 percent cloud-based deployment model. This is a fallacy. To scan internal hosts, they typically lease you hardware appliances or virtual appliances — charging you for each one. This limits your flexibility when you decide at a moment's notice that you need another scanner, as you must go through the purchasing process to procure an additional physical or virtual appliance from your VM provider.

Enterprise-class Scalability and Performance

The performance and scalability of VM solutions vary drastically from one provider to the next. There are two considerations here: the performance of an individual scanner and the scalability of a cluster of scanners.

The ratio of monitored IPs to active scanner varies by organization and, frankly, has a lot to do with the organization's targeted active scan frequency. The faster a scanner completes its assigned scan jobs (as configured in the management console), the better it is for the organization. Some scanners can scan a 1,000-node Microsoft Windows network segment in a single day, while others take a week or longer. The only way to determine this for yourself is to put competing scanners to the test during an evaluation phase.

Although the performance of each scanner is important, so is the scalability of the full VM solution. Most VM providers offer a basic, "round robin" load-balancing capability, where assigned hosts are equally distributed among active scanners. There are two problems with this approach. First, it assumes that the hardware specifications of each scanner are equal, and second, it assumes that scanning each host takes an identical amount of time. The best load-balancing approach is intelligent, where the VM management console constantly monitors the CPU and memory usage of each scanner to intelligently distribute the workload so the full network scan is completed in the least amount of time.

Comprehensive Policy Coverage

A good VM provider makes it easy for organizations to track mandated compliance with industry and government regulations and voluntary compliance with IT security frameworks — although many of these frameworks are referenced by compliance regulations.

At a minimum, a robust VM platform should provide customizable dashboards and reports that support the following:

- ☑ **Regulations:** PCI, HIPAA, FISMA (with CyberScope support), NERC, GLBA (Gramm-Leach-Bliley Act)
- ☑ **IT security frameworks:** SANS 20 Critical Security Controls, Center for Internet Security (CIS) Configuration Benchmarks, NIST 800-53

Daily Security Intelligence Updates

As I mention in Chapter 2, software vendors disclose an average of 27 new operating system and application vulnerabilities every day. And new malware is created virtually every minute of the day.

DON'T FORGET

If your VM vendor publishes security intelligence updates on a weekly — rather than a daily — basis, there's a good chance your scanners lack the ability to detect the latest vulnerabilities when conducting a full network scan. And with so many APTs exploiting recently disclosed vulnerabilities, this is a chance you simply can't afford to take.

Best-of-Breed Feature Set

VM is not new. In fact, it's been around for decades. VM vendors have had many years to equip enterprises with the features they need to uncover vulnerabilities and security misconfigurations while maintaining regulatory compliance.

So be sure to select a VM solution that incorporates most, if not all, of the following features:

☑ Customizable, interactive (not static) dashboards

☑ Library of pre-built reports

☑ Granular access control

☑ Passive vulnerability scanning

☑ Log correlation engine

☑ Scanning of mobile devices (smartphones and tablets)

☑ Automated, intelligent load balancing

☑ Customizable asset lists

☑ Security configuration auditing

☑ Patch auditing

☑ Remediation scanning

☑ Management console tiering

☑ Malware detection

A select few VM solutions have recently added malware detection capabilities to supplement IPS, NGFW, and advanced threat protection systems. Although not core to the function of VM, malware detection does offer an additional layer of defense — especially for threats hand-carried through the office front door on laptop hard drives and portable USB drives, which bypass your traditional perimeter defenses.

Accuracy of Authenticated Scans

There are two attributes that determine the accuracy of authenticated scans — the quantity and quality of plugins (checks). Some scanners offer only 10,000 or 20,000 plugins, while leading scanners come equipped with 50,000 or more.

But offering the most plugins doesn't guarantee vulnerability-detection accuracy. Vendors must thoroughly test their plugins before they are published to minimize the potential of false positives (reported vulnerabilities that do not exist) and false negatives (missed vulnerabilities).

Broad Integration Support

Another important concept to which I dedicate an entire chapter is VM integration support. The best security solutions share intelligence with and/or receive intelligence from other security solutions.

If you missed it, Chapter 6 describes ways that VM can interoperate with a variety of IT systems, including:

- ☑ Security information and event management (SIEM)
- ☑ Intrusion prevention systems (IPS)
- ☑ Next-generation firewall (NGFW)
- ☑ Unified threat management (UTM)
- ☑ Risk management
- ☑ Mobile device management
- ☑ Incident management
- ☑ Access management
- ☑ Patch management
- ☑ Penetration testing

CAUTION

If you're considering a VM vendor that offers few ways to integrate with your existing IT infrastructure, it's a telltale sign of a rudimentary VM solution. It's definitely time to move on.

Ease of Use

The best VM products are feature rich but also easy to use. Although you probably won't become fluent in every feature on the first day, the product should be easy to learn and offer comprehensive, well-written documentation to walk you through more-difficult concepts.

A security product could have every feature you could ever wish for. But if it's too difficult to use, your team is unlikely to embrace it.

Superior Customer Service

Selecting a VM vendor is just as important as selecting a VM solution. When evaluating competing offerings, be sure to consider the customer support provided by each vendor.

TIP

Even if you don't come across any difficulties during your product evaluations, make up a few reasons to call and email each vendor's customer support department. Gauge how quickly they respond to your inquiries and how thoroughly they answer your questions.

Clemson University graduates to a better VM solution

Clemson University is a major science and engineering research institution with nearly 20,000 students and 1,200 faculty and staff. Clemson's IT security team is responsible for the compliance, policy setting, and protection of more than 80,000 registered devices connected to its network, which spans 46 counties across South Carolina.

In addition to housing sensitive student, faculty, and financial transaction information, the university serves as the data hub for a crucial state medical device service. Needless to say, the security of Clemson's data is critical.

The university has a small yet dedicated IT security team. One of its responsibilities is to support five full compliance audits per year, including PCI and HIPAA. As completing full network scans took far too long with existing scanners, and generating compliance reports was a manual, tedious process, the Director of Security Infrastructure felt it was time to look for a more robust VM solution.

After evaluating a half-dozen VM products, Clemson selected Tenable SecurityCenter (www.tenable.com), including its highly regarded Nessus vulnerability scanners. Now Clemson's IT security team has a library of dashboards and reports to simplify compliance auditing, and full network scans are completed in less than half the time they took before. As an added bonus, Clemson discovered SecurityCenter's ability to audit system patches, which the team deploys on a 30-day cycle, providing the organization with an additional level of confidence.

Supporting compliance audits used to be a multi-day process for Clemson's IT security team. Now they can deliver audit results on the same day.

Glossary

active vulnerability scanner: A software application, such as Nessus, designed to assess computers and network infrastructure devices for vulnerabilities and security misconfigurations by actively probing them.

advanced persistent threat (APT): A sophisticated cyber attack that exploits vulnerabilities to gain network access and remain undetected for extended periods of time.

asset list: A grouping of network hosts that share a common attribute, such as business criticality, geography, or host type. Assets lists are used to configure scanning policies, monitor dashboards, and generate reports.

authenticated scan: A network scan from an active vulnerability scanner configured with administrative credentials, making it possible to uncover all potential vulnerabilities and security misconfigurations. Also known as a credentialed scan.

baiting: A social-engineering attack in which a media device (e.g., USB flash drive) with malware-infected files is deliberately left in proximity to a targeted organization.

blended threat: A cyber attack incorporating a combination of threats exploiting network vulnerabilities.

bot: An infected computer (usually an endpoint device) commandeered by a command and control (CnC) server.

buffer overflow attack: A cyber attack accomplished by placing more data into the buffer of a web-based application than it's configured to hold, enabling the attacker to run custom code (often with the escalated privileges granted to the vulnerable application or network service).

BYOD (bring your own device): A security trend related to organizations' allowing employees to use personally owned devices to access company applications and data.

continuous monitoring: Leveraging a combination of active and passive scanning techniques to perform 100 percent asset discovery and continuously monitor a network for vulnerabilities and security misconfigurations.

CVE (common vulnerabilities and exposures): Unique identifiers assigned and maintained by MITRE Corporation for publicly known information security vulnerabilities.

CVSS (common vulnerability scoring system): Open industry standard under the custodianship of the Forum of Incident Response and Security Teams (FIRST) for assessing the severity of vulnerabilities. CVSS scores are incorporated into CVE descriptions. (See CVE.)

defense-in-depth strategy: Leveraging multiple layers of security defenses so that a threat missed by one layer of security may be caught by another.

exploit: A piece of software (malware), a chunk of data, or a sequence of commands that takes advantage (or exploits) a security vulnerability to compromise a host. (See local exploit, remote exploit.)

false negative: In the context of VM, failure to report a vulnerability or security misconfiguration that is present.

false positive: In the context of VM, falsely reporting the presence of a vulnerability or security misconfiguration.

intrusion protection system (IPS): An inline (active) signature-based threat-detection device that monitors the network and blocks known cyber attacks upon detection.

local exploit: An exploit that needs prior access to the vulnerable system to increase account privileges. (See exploit.)

log correlation engine: NGVM system component responsible for aggregating log data from network segments not monitored by a passive vulnerability scanner in an effort to identify new hosts.

malware: Malicious software created to infiltrate or disrupt computer networks to gain access to confidential data or adversely affect availability of IT services. (See worm, virus, Trojan.)

passive vulnerability scanner: A software application, such as Tenable PVS, designed to assess computers and network infrastructure devices for vulnerabilities and security misconfigurations by passively profiling traffic generated by them.

patch: A vendor-supplied software update to correct vulnerabilities in operating systems and applications. (See patch management.)

patch management: The cyclical process of acquiring, testing, and installing patches to administered computer systems in a coordinated effort to mitigate vulnerabilities. (See patch.)

Patch Tuesday: The second Tuesday of each month, when Microsoft releases security patches to correct vulnerabilities within its operating system and application products.

phishing: The act of sending seemingly innocuous emails to large numbers of individuals. By falsely claiming to be a legitimate entity, the sender attempts to scam users into surrendering private information. (See spear phishing.)

plugins: Audit instructions used by active and passive vulnerability scanners to check for system vulnerabilities and security misconfigurations. Also known as checks.

remote exploit: An exploit that does not need prior access to the vulnerable system to increase account privileges. (See exploit.)

search engine poisoning: Creating seemingly innocuous yet malicious websites optimized with key words to appear high up in search engine results in an effort to infect connecting computers with malware.

spear phishing: A phishing attempt directed toward individuals within a targeted organization, often to initiate an APT against that organization. (See phishing, APT.)

SQL injection attack: A cyber attack against a database-driven web application during which the attacker executes unauthorized SQL commands to exploit insecure code.

Trojan: Malware that masquerades as a legitimate application or file with the ultimate purpose of granting a hacker unauthorized access to a computer.

unauthenticated scan: A network scan from an active vulnerability scanner not configured with administrative credentials, thus limiting the vulnerabilities and security misconfigurations able to be detected in comparison to an authenticated scan. (See authenticated scan.)

virus: A malicious computer program commonly attached to legitimate executables and files that is designed to spread from one computer to another to disrupt their operation.

vulnerability: A weakness (i.e., bug) in a host's operating system or application that can be exploited by an attacker in an effort to compromise a computer network. (See vulnerability management.)

vulnerability management: The cyclical practice of identifying, classifying, remediating, and mitigating software vulnerabilities and security misconfigurations. (See vulnerability.)

water holing: Compromising a website with malware likely to be visited by a particular target group, rather than attacking the target group directly.

whaling: A spear phishing attack directed at senior executives and other high-profile employees of a targeted organization. (See spear phishing.)

window of vulnerability: The time span from discovery through mitigation of a software vulnerability. During this period, unpatched hosts are particularly vulnerable to attack.

worm: A form of malware that exploits system vulnerabilities to propagate itself to other hosts.

zero-day threat: A cyber attack that exploits an unknown (or unreported) OS or application vulnerability before the availability of a corresponding patch.

Discover how next-generation vulnerability management (NGVM) solutions equipped with continuous monitoring can improve your security posture and simplify compliance.

Think you know vulnerability management? Think again. A new breed of technology has emerged, enabling enterprises to continuously monitor their networks for vulnerabilities, security misconfigurations, and now cyberthreats — all while supporting company BYOD initiatives and sustaining regulatory compliance. If you're tasked with securing your network and/or supporting compliance audits, this is one book you can't afford to miss.

- Understanding vulnerability management — start with the basics by understanding vulnerabilities and exploits
- Getting started — learn how to get your NGVM system up and running
- Making the case for continuous monitoring — discover why active scanning alone is insufficient for mitigating cyberthreats
- Sustaining regulatory compliance — work smarter to achieve and sustain compliance with government and/or industry regulations
- Integrating with your infrastructure — understand why and how to integrate NGVM with your existing infrastructure
- Selecting the right NGVM solution — know exactly what to look for, and what to avoid, when evaluating NGVM solutions

About the Author

Steve Piper is an information security author, consultant, analyst, and speaker with more than 20 years of IT experience. He has authored numerous award-winning books on cybersecurity, networking, and Big Data. Steve holds a CISSP security certification from ISC2 and BS and MBA degrees from George Mason University. Follow Steve on Twitter at @StevePiper or learn more at www.stevepiper.com.

CYBEREDGE PRESS

Not for resale

ISBN 978-0-9888233-2-7

9 780988 823327