RAPID7

NEXPOSE ENTERPRISE

METASPLOIT PRO

Effective Vulnerability Management and validation

March 2015

Q-EAST SOFTWARE
Smart Systems Management

nexpose® metasploit®

KEY SECURITY CHALLENGES

Common Challenges Organizations Experience

Key Security Challenges

- Visibility gaps of security risks to business
- Information overload inhibits decision making
- Difficulty in communicating remediation
- Security programs are too tactical
- Hard to show security adds value
- Costly compliance requirements

Patch ALL THE THINGS!

verizon

2014 DATA BREACH INVESTIGATIONS REPORT

Patch ALL THE THINGS

Exploiting browser, OS, and other third-party software (e.g., Flash and Java) vulnerabilities to infect end-user systems is a common initial step for attackers. Keeping everything up to date will make that step a lot harder to take.

nexpose®

metasploit®

RAPID7 SOLUTIONS

Nexpose Vulnerability Management

Know Your Network

Manage Risk Effectively

Simplify Your Compliance

nexpose®

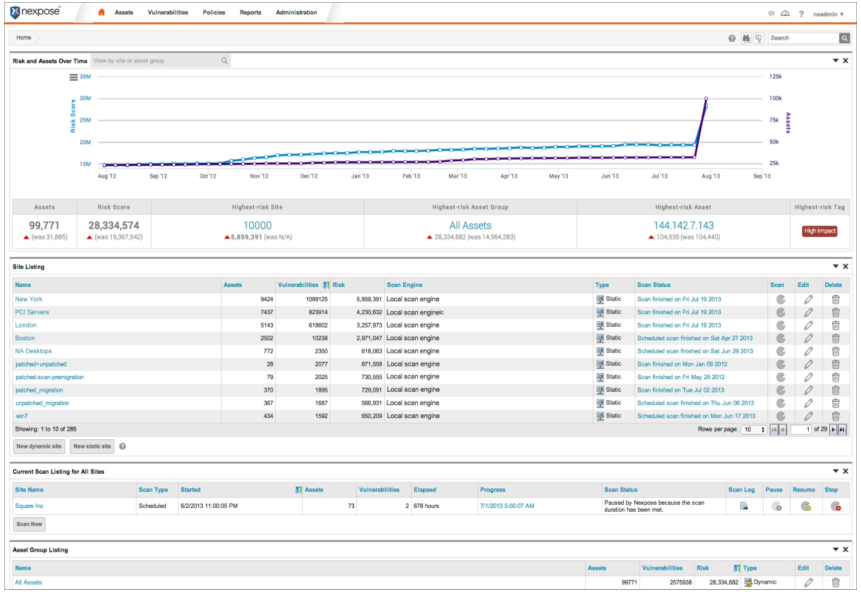
KNOW YOUR NETWORK

Before you can manage risk you need to find it

Efficient Security Assessment

Single Security Scan

- Simple setup & configuration
- Unified scanning
  - OS, Applications, Services, Web, Database, and configurations
- Consolidated reporting



Assets	Risk Score	Highest-risk Site	Highest-risk Asset Group	Highest-risk Asset	Highest-risk Tag
99,771 ▲ (was 31,885)	28,334,574 ▲ (was 19,367,542)	10000 ▲5,859,391 (was N/A)	All Assets ▲ 28,334,682 (was 14,964,283)	144.142.7.143 ▲ 104,535 (was 104,440)	High Impact

Site Listing

Name	Assets	Vulnerabilities	Risk	Scan Engine	Type	Scan Status	Scan	Edit	Delete
New York	9424	1089125	5,859,391	Local scan engine	Static	Scan finished on Fri Jul 19 2013	◎	✎	🗑
PCI Servers	7437	823914	4,230,632	Local scan engineIc	Static	Scan finished on Fri Jul 19 2013	◎	✎	🗑
London	5143	618602	3,257,973	Local scan engine	Static	Scan finished on Fri Jul 19 2013	◎	✎	🗑
Boston	2502	10238	2,971,047	Local scan engine	Static	Scheduled scan finished on Sat Apr 27 2013	◎	✎	🗑
NA Desktops	772	2350	618,063	Local scan engine	Static	Scheduled scan finished on Sat Jun 29 2013	◎	✎	🗑
patched+unpatched	28	2077	871,558	Local scan engine	Static	Scan finished on Mon Jan 09 2012	◎	✎	🗑
patched-scan-premigration	79	2025	730,555	Local scan engine	Static	Scan finished on Fri May 25 2012	◎	✎	🗑
patched_migration	370	1895	729,091	Local scan engine	Static	Scan finished on Tue Jul 02 2013	◎	✎	🗑
unpatched_migration	367	1687	566,931	Local scan engine	Static	Scheduled scan finished on Thu Jun 06 2013	◎	✎	🗑
win7	434	1592	650,209	Local scan engine	Static	Scheduled scan finished on Mon Jun 17 2013	◎	✎	🗑

Showing: 1 to 10 of 285 Rows per page: 10 1 of 29

New dynamic site New static site

Current Scan Listing for All Sites

Site Name	Scan Type	Started	Assets	Vulnerabilities	Elapsed	Progress	Scan Status	Scan Log	Pause	Resume	Stop
Square Inc	Scheduled	6/2/2013 11:00:05 PM	73	2	678 hours	7/1/2013 5:00:07 AM	Paused by Nexpose because the scan duration has been met.				

Scan Now

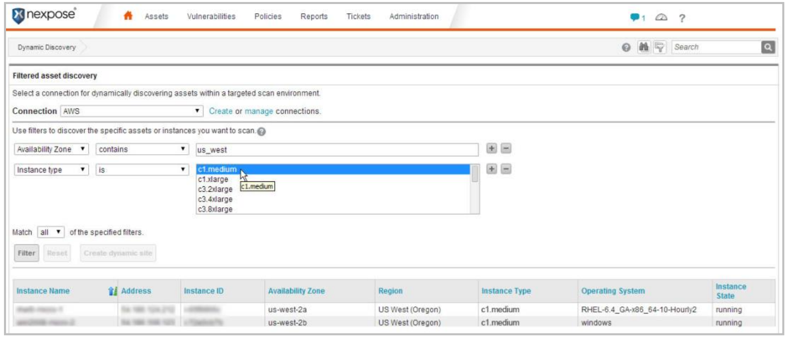
Asset Group Listing

Name	Assets	Vulnerabilities	Risk	Type	Edit	Delete
All Assets	99771	2575938	28,334,682	Dynamic	✎	🗑

Across Modern Networks

- Physical, virtual, and cloud
- Real-time discovery
- Expert scanning system

Comprehensive Visibility



Filtered asset discovery

Select a connection for dynamically discovering assets within a targeted scan environment.

Connection AWS ▾ Create or manage connections.

Use filters to discover the specific assets or instances you want to scan.

Availability Zone ▾ contains ▾ us_west

Instance type ▾ is ▾ c1.medium, c1.xlarge, c3.2xlarge, c3.4xlarge, c3.8xlarge

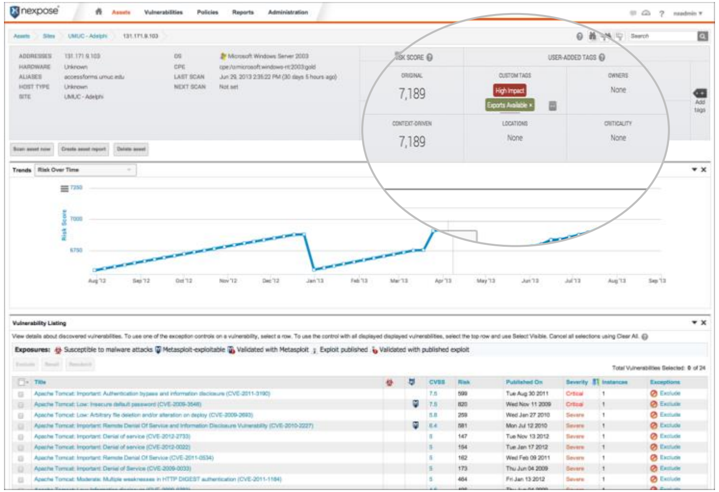
Match all ▾ of the specified filters.

Instance Name	Address	Instance ID	Availability Zone	Region	Instance Type	Operating System	Instance State
[redacted]	[redacted]	[redacted]	us-west-2a	US West (Oregon)	c1.medium	RHEL-6.4_GA-x86_64-10-Hourly2	running
[redacted]	[redacted]	[redacted]	us-west-2b	US West (Oregon)	c1.medium	windows	running

Understand Business Context

- Automatic classification
- Identify important systems
- Assign remediation owners

RealContext™



ADDRESSES	131.171.9.103	OS	Microsoft Windows Server 2003
HARDWARE	Unknown	CPE	cpe:/o:microsoft:windows-nt:2003:gold
ALIASES	accessforms.umuc.edu	LAST SCAN	Jun 29, 2013 2:35:22 PM (30 days 5 hours ago)
HOST TYPE	Unknown	NEXT SCAN	Not set
SITE	UMUC - Adelphi		

RISK SCORE

ORIGINAL: 7,189

CONTEXT-DRIVEN: 7,189

USER-ADDED TAGS

CUSTOM TAGS: High Impact, Exports Available

OWNERS: None

LOCATIONS: None

CRITICALITY: None

Vulnerability Listing

View details about discovered vulnerabilities. To use one of the exception controls on a vulnerability, select a row. To use the control with all displayed displayed vulnerabilities, select the top row and use Select Visible. Cancel all selections using Clear All.

Exposures: Susceptible to malware attacks Metasploit-exploitable Validated with Metasploit Exploit published Validated with published exploit

Total Vulnerabilities Selected: 0 of 24

□	Title			CVSS	Risk	Published On	Severity	Instances	Exceptions
□	Apache Tomcat: Important: Authentication bypass and information disclosure (CVE-2011-3190)			7.5	599	Tue Aug 30 2011	Critical	1	Exclude
□	Apache Tomcat: Low: Insecure default password (CVE-2009-3548)		●	7.5	820	Wed Nov 11 2009	Critical	1	Exclude
□	Apache Tomcat: Low: Arbitrary file deletion and/or alteration on deploy (CVE-2009-2693)			5.8	259	Wed Jan 27 2010	Severe	1	Exclude
□	Apache Tomcat: Important: Remote Denial Of Service and Information Disclosure Vulnerability (CVE-2010-2227)		●	6.4	581	Mon Jul 12 2010	Severe	1	Exclude
□	Apache Tomcat: Important: Denial of service (CVE-2012-2733)			5	147	Tue Nov 13 2012	Severe	1	Exclude
□	Apache Tomcat: Important: Denial of service (CVE-2012-0022)			5	154	Tue Jan 17 2012	Severe	1	Exclude
□	Apache Tomcat: Important: Remote Denial Of Service (CVE-2011-0534)			5	162	Wed Feb 09 2011	Severe	1	Exclude
□	Apache Tomcat: Important: Denial of Service (CVE-2009-0033)			5	173	Thu Jun 04 2009	Severe	1	Exclude
□	Apache Tomcat: Moderate: Multiple weaknesses in HTTP DIGEST authentication (CVE-2011-1184)			5	464	Fri Jan 13 2012	Severe	1	Exclude

nexpose®

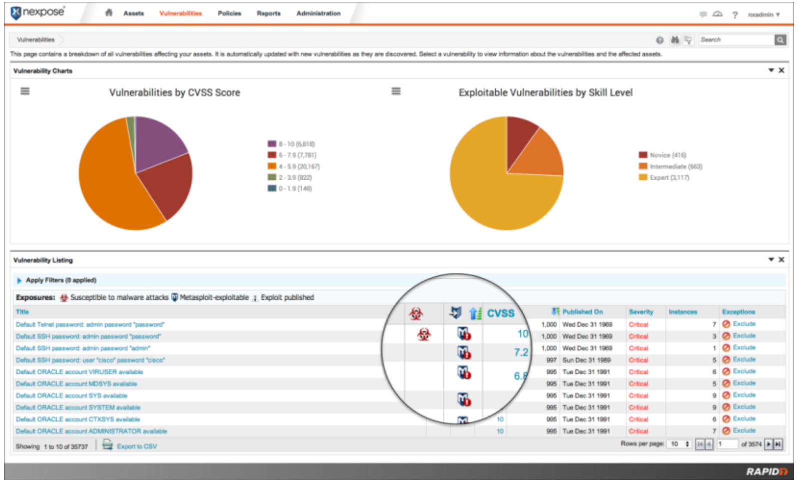
MANAGE RISK EFFECTIVELY

Not all risk is created equal and shouldn’t be treated the same

Vulnerability Validation

Validate with Metasploit PRO

- Safely exploit vulnerabilities
- Focus on proven risks
- Closed-loop remediation



This page contains a breakdown of all vulnerabilities affecting your assets. It is automatically updated with new vulnerabilities as they are discovered. Select a vulnerability to view information about the vulnerabilities and the affected assets.

Vulnerability Charts

Vulnerability Listing

Apply Filters (0 applied)

Exposures: ☣ Susceptible to malware attacks Ⓜ Metasploit-exploitable ⇣ Exploit published

Title	☣	Ⓜ	CVSS		Published On	Severity	Instances	Exceptions
Default Telnet password: admin password "password"	☣	Ⓜ	10	1,000	Wed Dec 31 1969	Critical	7	Exclude
Default SSH password: admin password "password"		Ⓜ	7.2	1,000	Wed Dec 31 1969	Critical	3	Exclude
Default SSH password: admin password "admin"		Ⓜ	6.8	1,000	Wed Dec 31 1969	Critical	1	Exclude
Default SSH password: user "cisco" password "cisco"		Ⓜ		997	Sun Dec 31 1989	Critical	5	Exclude
Default ORACLE account VIRUSER available				995	Tue Dec 31 1991	Critical	6	Exclude
Default ORACLE account MDSYS available				995	Tue Dec 31 1991	Critical	5	Exclude
Default ORACLE account SYS available				995	Tue Dec 31 1991	Critical	9	Exclude
Default ORACLE account SYSTEM available				995	Tue Dec 31 1991	Critical	9	Exclude
Default ORACLE account CTXSYS available			10	995	Tue Dec 31 1991	Critical	6	Exclude
Default ORACLE account ADMINISTRATOR available			10	995	Tue Dec 31 1991	Critical	7	Exclude

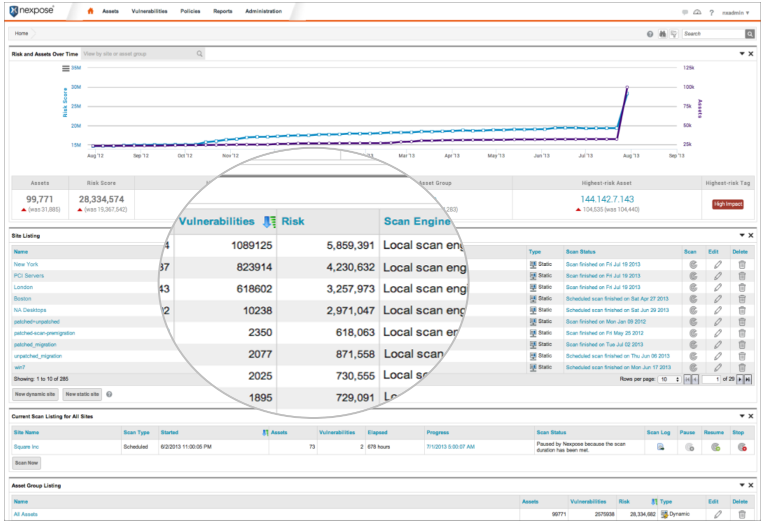
Showing 1 to 10 of 35737 | Export to CSV

Rows per page: 10 | 1 of 3574

Advanced Vulnerability Prioritization

- Threat-driven risk algorithm
- Granular risk scoring
- Use RealContext™ to increase risk score

RealRisk™



Assets	Risk Score	Asset Group	Highest-risk Asset	Highest-risk Tag
99,771 (was 31,885)	28,334,574 (was 19,367,542)	,283)	144.142.7.143 104,535 (was 104,440)	High Impact

Site Listing

Vulnerabilities	Risk	Scan Engine
1089125	5,859,391	Local scan en
823914	4,230,632	Local scan eng
618602	3,257,973	Local scan eng
10238	2,971,047	Local scan eng
2350	618,063	Local scan er
2077	871,558	Local scan
2025	730,555	Local sc
1895	729,091	Lc

Name	Type	Scan Status
New York	Static	Scan finished on Fri Jul 19 2013
PCI Servers	Static	Scan finished on Fri Jul 19 2013
London	Static	Scan finished on Fri Jul 19 2013
Boston	Static	Scheduled scan finished on Sat Apr 27 2013
NA Desktops	Static	Scheduled scan finished on Sat Jun 29 2013
patched+unpatched	Static	Scan finished on Mon Jan 09 2012
patched-scan-premigration	Static	Scan finished on Fri May 25 2012
patched_migration	Static	Scan finished on Tue Jul 02 2013
unpatched_migration	Static	Scheduled scan finished on Thu Jun 06 2013
win7	Static	Scheduled scan finished on Mon Jun 17 2013

Showing: 1 to 10 of 285

Rows per page: 10 | 1 of 29

New dynamic site | New static site

Current Scan Listing for All Sites

Site Name	Scan Type	Started	Assets	Vulnerabilities	Elapsed	Progress	Scan Status
Square Inc	Scheduled	6/2/2013 11:00:05 PM	73	2	678 hours	7/1/2013 5:00:07 AM	Paused by Nexpose because the scan duration has been met.

Scan Now

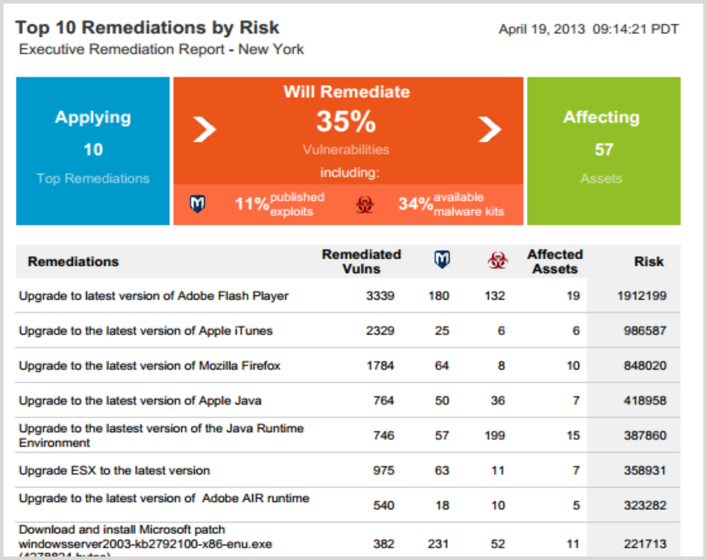
Asset Group Listing

Name	Assets	Vulnerabilities	Risk	Type
All Assets	99771	2575938	28,334,682	Dynamic

Risk Remediation Planning

- Actionable impactful decisions
- Short targeted reports
- Step-by-steps instructions

Top Remediations



Top 10 Remediations by Risk April 19, 2013 09:14:21 PDT

Executive Remediation Report - New York

Applying 10 Top Remediations › Will Remediate 35% Vulnerabilities including: M 11% published exploits ☣ 34% available malware kits › Affecting 57 Assets

Remediations	Remediated Vulns	M	☣	Affected Assets	Risk
Upgrade to latest version of Adobe Flash Player	3339	180	132	19	1912199
Upgrade to the latest version of Apple iTunes	2329	25	6	6	986587
Upgrade to the latest version of Mozilla Firefox	1784	64	8	10	848020
Upgrade to the latest version of Apple Java	764	50	36	7	418958
Upgrade to the lastest version of the Java Runtime Environment	746	57	199	15	387860
Upgrade ESX to the latest version	975	63	11	7	358931
Upgrade to the latest version of Adobe AIR runtime	540	18	10	5	323282
Download and install Microsoft patch windowsserver2003-kb2792100-x86-enu.exe (4278824 bytes)	382	231	52	11	221713

nexpose®

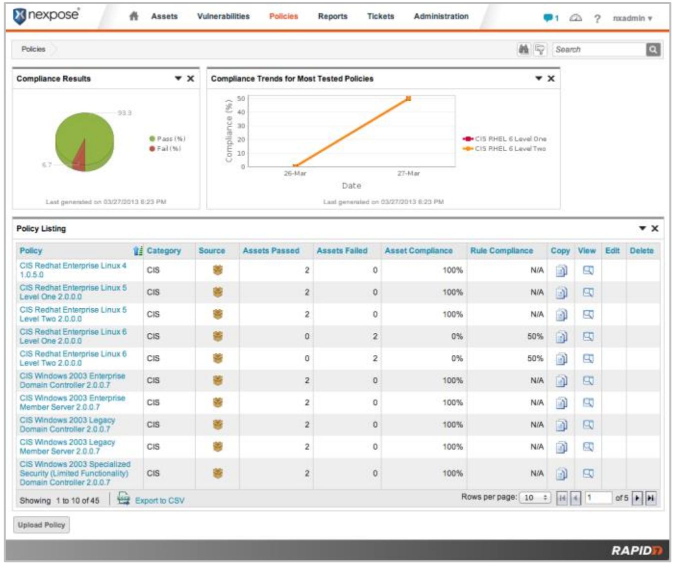
SIMPLIFY YOUR COMPLIANCE

Don’t spend too much time showing and improving compliance

Unified Security & Compliance

- Single assessment scan
- Customizable policies
- Consolidated reporting

Policy Manager



Policy	Category	Source	Assets Passed	Assets Failed	Asset Compliance	Rule Compliance	Copy	View	Edit	Delete
CIS Redhat Enterprise Linux 4 1.0.5.0	CIS		2	0	100%	N/A				
CIS Redhat Enterprise Linux 5 Level One 2.0.0.0	CIS		2	0	100%	N/A				
CIS Redhat Enterprise Linux 5 Level Two 2.0.0.0	CIS		2	0	100%	N/A				
CIS Redhat Enterprise Linux 6 Level One 2.0.0.0	CIS		0	2	0%	50%				
CIS Redhat Enterprise Linux 6 Level Two 2.0.0.0	CIS		0	2	0%	50%				
CIS Windows 2003 Enterprise Domain Controller 2.0.0.7	CIS		2	0	100%	N/A				
CIS Windows 2003 Enterprise Member Server 2.0.0.7	CIS		2	0	100%	N/A				
CIS Windows 2003 Legacy Domain Controller 2.0.0.7	CIS		2	0	100%	N/A				
CIS Windows 2003 Legacy Member Server 2.0.0.7	CIS		2	0	100%	N/A				
CIS Windows 2003 Specialized Security (Limited Functionality) Domain Controller 2.0.0.7	CIS		2	0	100%	N/A				

Showing 1 to 10 of 45 | Export to CSV

Rows per page: 10 | 1 of 5

RAPID7

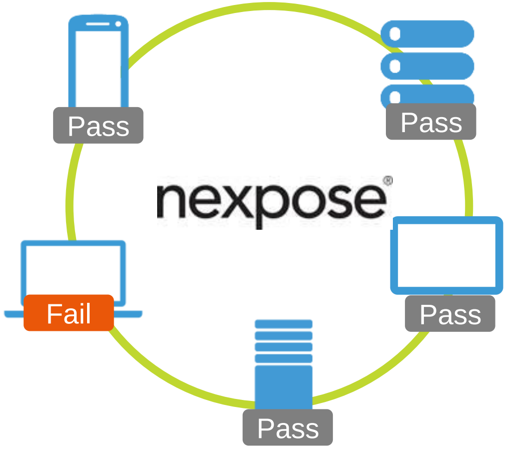
Q-EAST SOFTWARE
Smart Systems Management

Compliance Auditing & Reporting

- Customizable Audit Reports
- PCI Compliance Reports

Policy Scanning & Reporting

PCI HIPAA SOX NERC 🔒 COMPLAINT



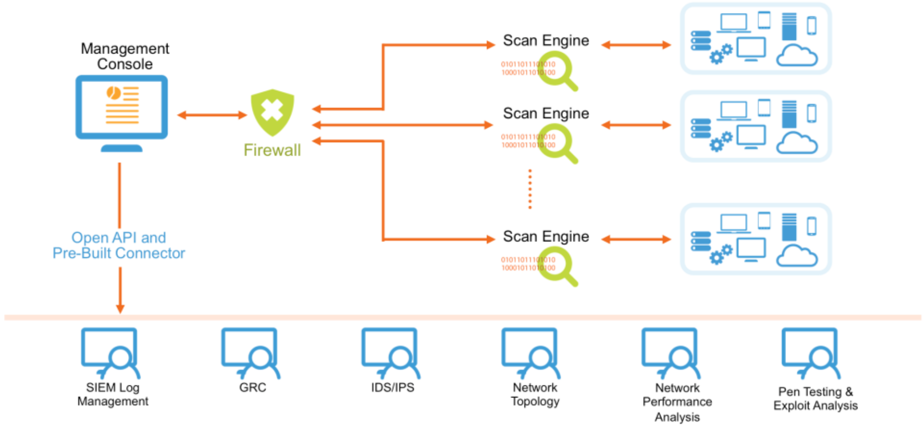
nexpose®

ARCHITECTURE

Flexible and Scalable Architecture

- Multiple deployment options
- Agentless scanning
- Scale with scan engines
- OpenAPI™ for integrations

Enterprise Architecture



metasploit®

INCREASE YOUR PRODUCTIVITY ON PENETRATION TESTS

We’re Not Always Covering the Basics

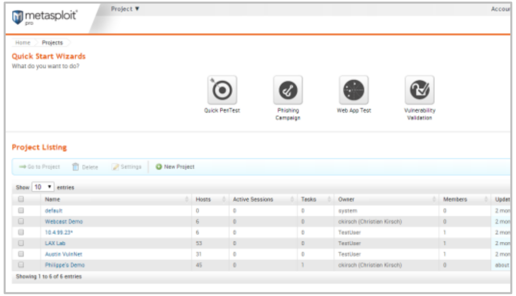
62%

2013 had
62% more data breaches
than 2012

Source: Symantec Internet Security Threat Report metasploit®

Test Your Defenses More Efficiently

Penetration Testing



Quick Start Wizards

What do you want to do?

Project Listing

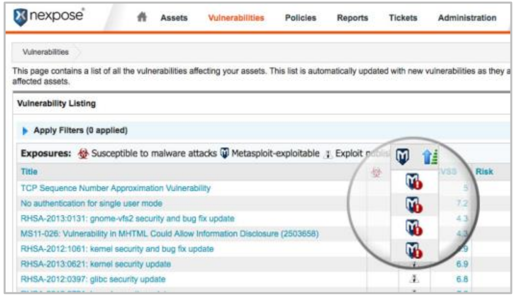
Show 10 ▼ entries

□	Name	Hosts	Active Sessions	Tasks	Owner	Members	Updat
□	default	0	0	0	system	0	2 mon
□	Webcast Demo	6	0	0	ckirsch (Christien Kirsch)	0	2 mon
□	10.4.99.23*	6	0	0	TestUser	1	2 mon
□	LAX Lab	53	0	0	TestUser	1	2 mon
□	Austin VulnNet	31	0	0	TestUser	1	2 mon
□	Philippe's Demo	45	0	1	ckirsch (Christien Kirsch)	0	about

Showing 1 to 6 of 6 entries

- Simulate a real-world attack to test your defenses
- Conduct penetration tests 45% faster

Vulnerability Validation



Vulnerabilities

This page contains a list of all the vulnerabilities affecting your assets. This list is automatically updated with new vulnerabilities as they a affected assets.

Vulnerability Listing

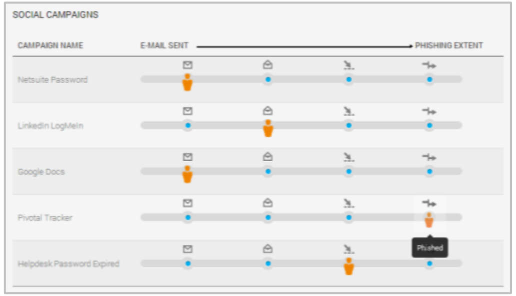
Apply Filters (0 applied)

Exposures: Susceptible to malware attacks Metasploit-exploitable Exploit publis

Title	CVSS	Risk
TCP Sequence Number Approximation Vulnerability	5	
No authentication for single user mode	7.2	
RHSA-2013:0131: gnome-vfs2 security and bug fix update	4.3	
MS11-026: Vulnerability in MHTML Could Allow Information Disclosure (2503658)	4.3	
RHSA-2012:1061: kernel security and bug fix update	6.9	
RHSA-2013:0621: kernel security update	6.9	
RHSA-2012:0397: glibc security update	6.8	

- Validate vulnerabilities to demonstrate risk
- Close-loop integration with Nexpose for remediation

Phishing Simulation


SOCIAL CAMPAIGNS

CAMPAIGN NAME — E-MAIL SENT → PHISHING EXTENT

Netsuite Password

LinkedIn LogMeIn

Google Docs

Pivotal Tracker

Helpdesk Password Expired

- Validate vulnerabilities to demonstrate risk
- Close-loop integration with Nexpose for remediation

Where Penetration Testers Should Spend their Time

- Simulating an attacker by identifying and exploiting the most likely attack vectors
- Moving laterally across the network
- Compromising the security assessment “goal”
- Testing the effectiveness of people, processes and defensive technologies
- Analyzing gaps in the security program
- Providing insights on how to mitigate risk

Where Penetration Testers Actually Spend their Time

- Scripting their own solution to automate your standard workflows
- Tracking assessment data and correlating different sources
- Reporting on findings with manual or home-grown solution
- Developing custom payloads and obfuscators to evade anti-virus solutions

The Challenge: Productivity of Open Source Solutions

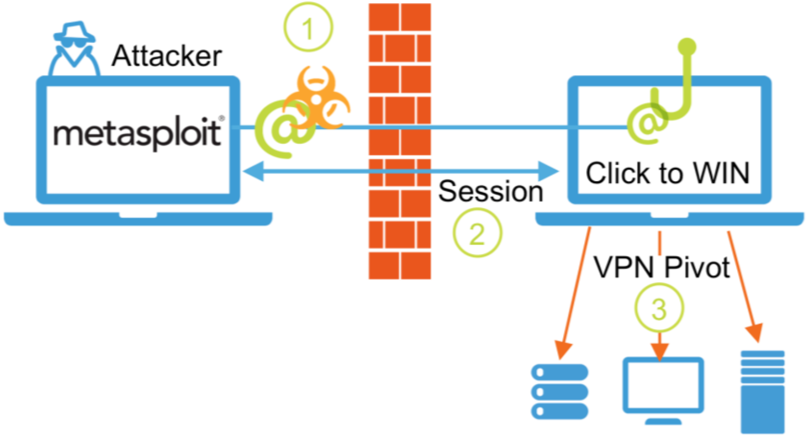
Open source security tools are great for innovation but not for productivity.

Manage Data and Automate Workflows

- Data management for large projects
  - Metasploit Pro supports 1,000s of hosts
  - Annotate, tag, sort, group and find
- You decide, Metasploit automates
  - **Wizards:** Standard workflows, e.g. quick pentests, web app tests, phishing simulation
  - **Task Chains:** Custom workflows, e.g. your preferred “opening moves” on an engagement
  - **MetaModules:** Discrete tasks, e.g. testing a credential across all services on a network

Evade Anti-Virus, Bypass Firewalls, Take Control

- Evade anti-virus with Dynamic Payloads
  - Evades all top 10 AV solutions by default
- Get past IPS with stage encoding and manipulating the transport layer
- Get around firewalls using VPN pivoting
  - Full local access to local networks through compromised hosts
- Take control of compromised machines
  - Choose from over 200 post-exploitation modules to be run when session is created



VPN Pivoting gives you full local network access through a compromised machine

Automatically Generate Reports of Key Findings

- Reports take up to 30% of an assessment
  - Automatically record actions and findings
  - Generate reports
  - Technical, management and compliance report
- Help with regulatory compliance
  - Metasploit Pro helps comply with PCI DSS, HIPAA, FISMA and SOX

nexpose®

PRIORITIZE AND DEMONSTRATE RISK WITH CLOSED-LOOP VULNERABILITY VALIDATION

Security Professionals Often Face These Questions

IT Operations asks

- Is the vulnerability “real” and not a false positive?
- What’s the impact of the vulnerability?
- What vulnerabilities should be patched first, given our limited resources?

Auditors ask

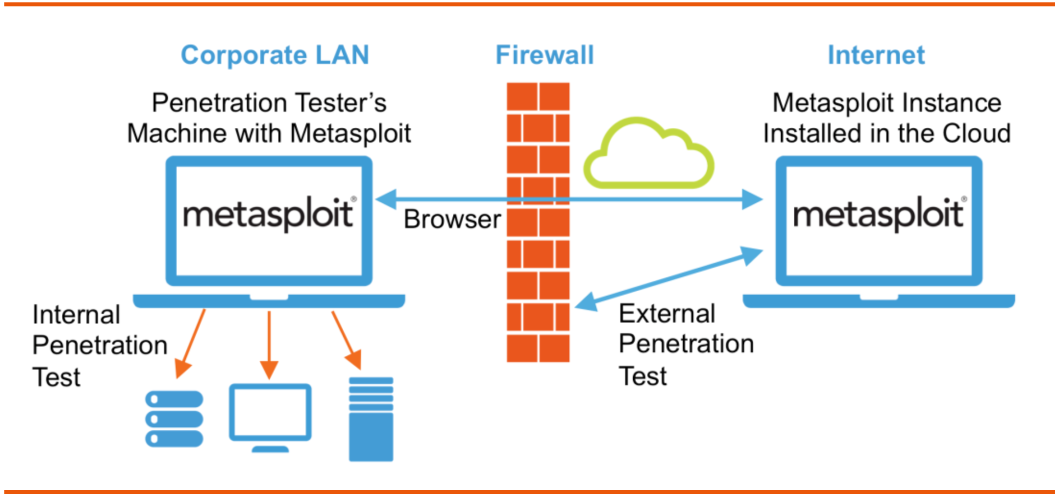
- Show me that you successfully remediated the vulnerability?
- Can you prove that your compensating control actually mitigates the risk?

Prioritize Vulnerabilities and Demonstrate Risk

- Metasploit validates vulnerabilities to demonstrate risk and prioritize remediation
  - Eliminate false positives and vulnerabilities with compensating controls
- Validated vulnerabilities are pushed back to Nexpose for closed-loop reporting
  - Report on validated vulnerabilities
- Tip: Agree on SLA with IT operations to remediate validated vulnerabilities

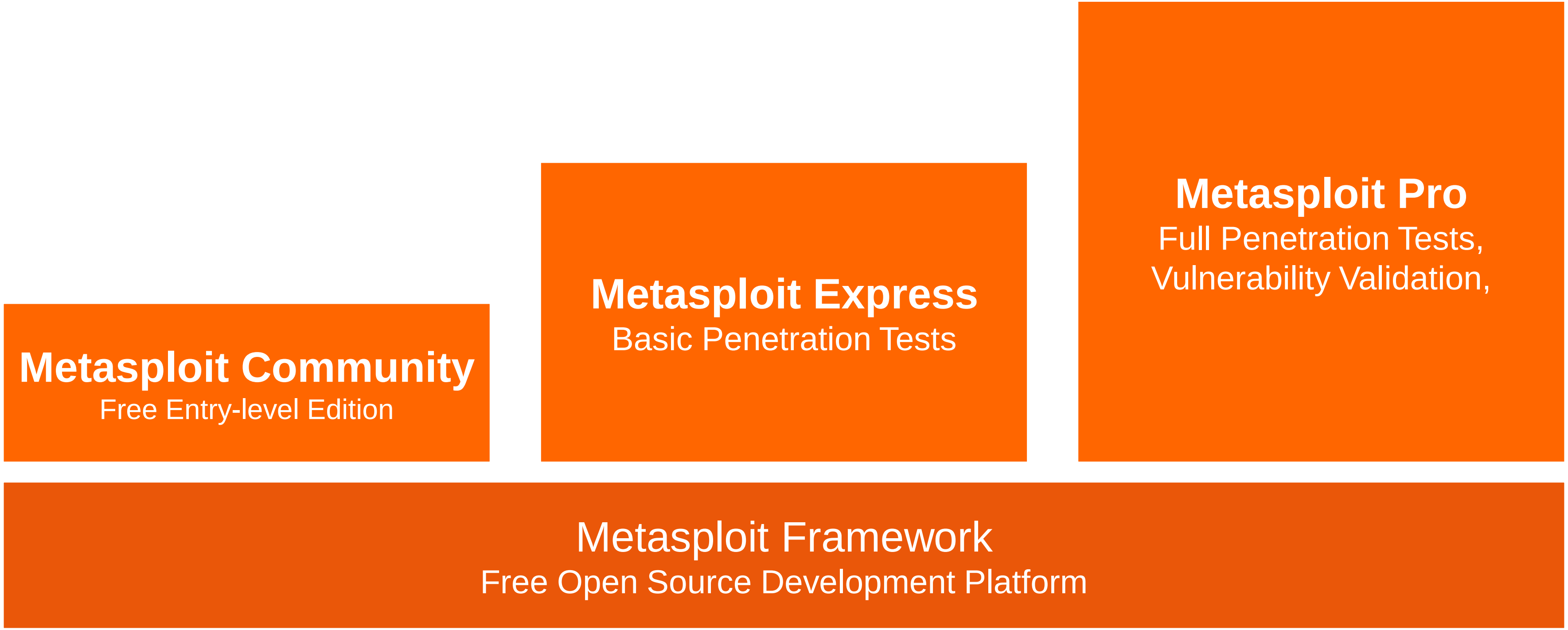
Metasploit Pro’s Deployment Options

- Web-based user interface
- API integrations
- 10+ installations per named-user
- Enterprise-level support



Corporate LAN
Firewall
Internet
Penetration Tester’s Machine with Metasploit
metasploit
Browser
Metasploit Instance Installed in the Cloud
metasploit
Internal Penetration Test
External Penetration Test

Metasploit Editions - Overview



Metasploit Pro
Full Penetration Tests,
Vulnerability Validation,

Metasploit Express
Basic Penetration Tests

Metasploit Community
Free Entry-level Edition

Metasploit Framework
Free Open Source Development Platform

nexpose®

metasploit®

QUESTIONS?

VLAD.GLADIN@QEAST.RO