Security in knowledge

SAST, DAST and Vulnerability Assessments, 1+1+1 = 4

Gordon MacKay

Digital Defense, Inc.

Chris Wysopal

Veracode

RSACONFERENCE2013

Session ID: **ASEC-W25**

Session Classification: Intermediate

AGENDA

- Risk Management Challenges
- Network Assessments – Assessing Risk Outside In
- Application Assessments – Assessing Risk Inside Out
- Combining Network and Application Assessments
- Ongoing Research and Development

THE RISK GAME – PLAY ALONG

What Picture Represents Most Risk?

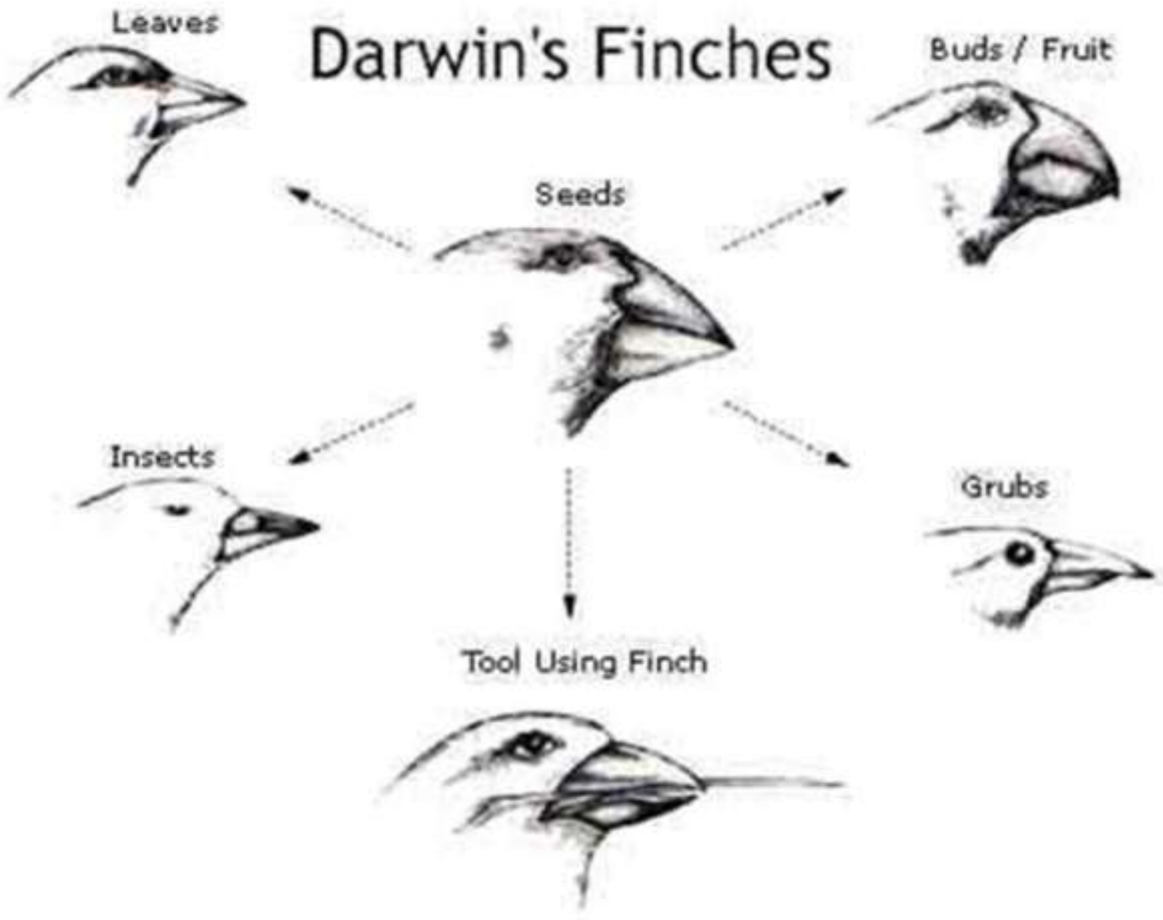
WHAT IS RISK?

- Risk is Relative to an Entity
- Risk Involves
  - An Entity with a Goal – Something to Gain/Lose
  - An Entity with Weaknesses/Disadvantages
  - An Environment Capable of Taking Advantage of Weaknesses

Risk = Threat x Vulnerability x Cost

ONE SOLUTION TO RISK

Evolution of Species



RISK MANAGEMENT CHALLENGES

- What is Value and Where is it Located?
- What are the Dangers to Organization’s Value?
- What are Weaknesses of Value Containers?
- What Risk Level is Acceptable?

Network Assessments – Outside In

- Automatically Inventory Containers
  - Attack Surface - Fully Visible, Camouflaged, Invisible
  - Location - Externally Internet facing versus deep within the Organization's Internal Network
  - Other Container Details

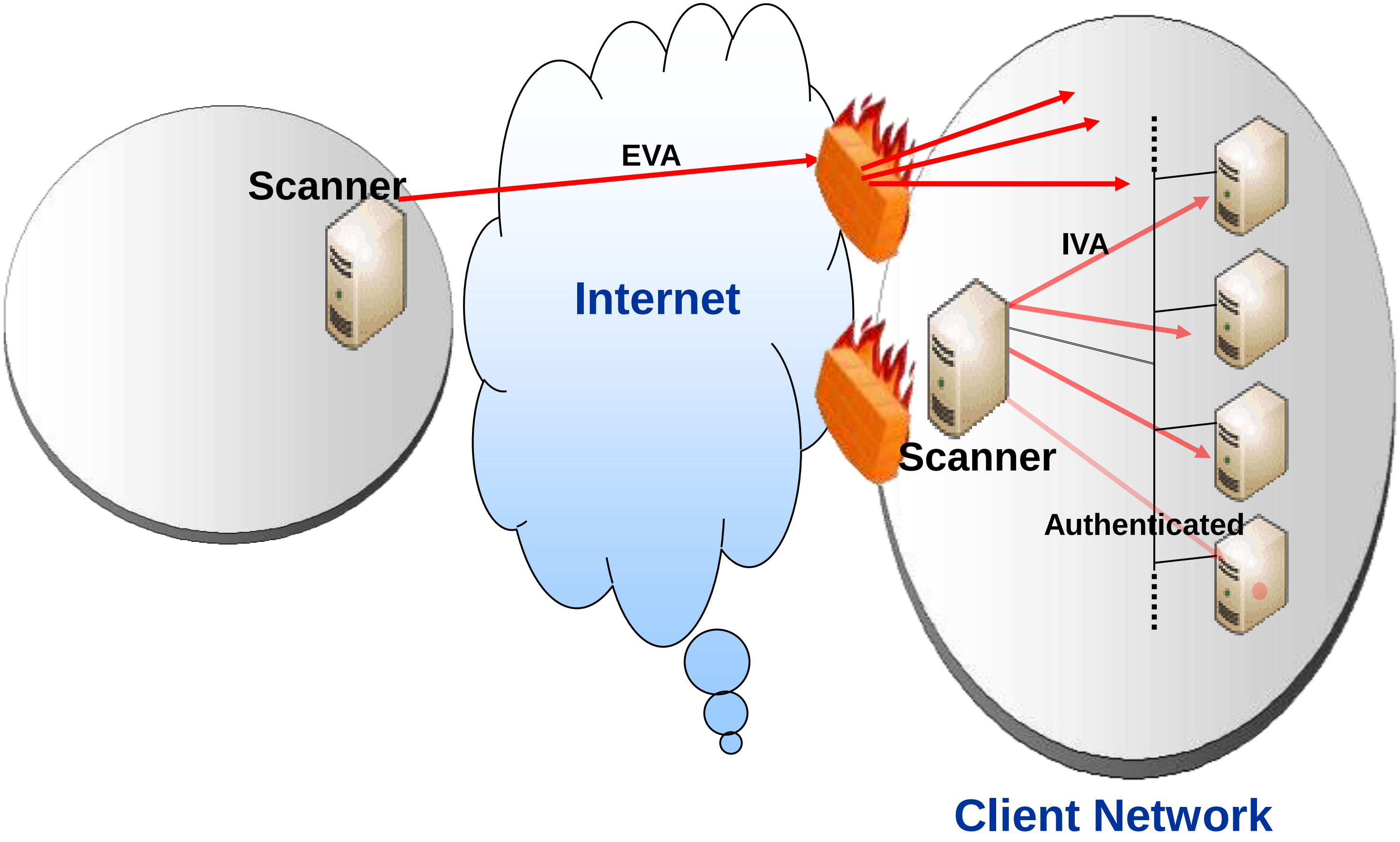
- Allow Mapping Assets to Containers

- Allow Value Assignments to Containers

- Assess Weaknesses of Containers

Network Assessments – Threat's Point of View

Vulnerability Paths



Network Assessment Strengths

- Hosts
- Network Map
- OS, Ports, Services, Applications
- Vulnerabilities within OSI Layer 2-7
- Misconfigurations
  - (e.g. Passwordless Protocols, Easily Guessable Passwords, SNMP configuration issues, much more)

Network Assessment Challenges

- Hidden Weaknesses (e.g. no or poor use of Encryption)
- Business Logic Issues
- Security Architecture Weaknesses

Endpoint Exposure

Applications

End points/OS

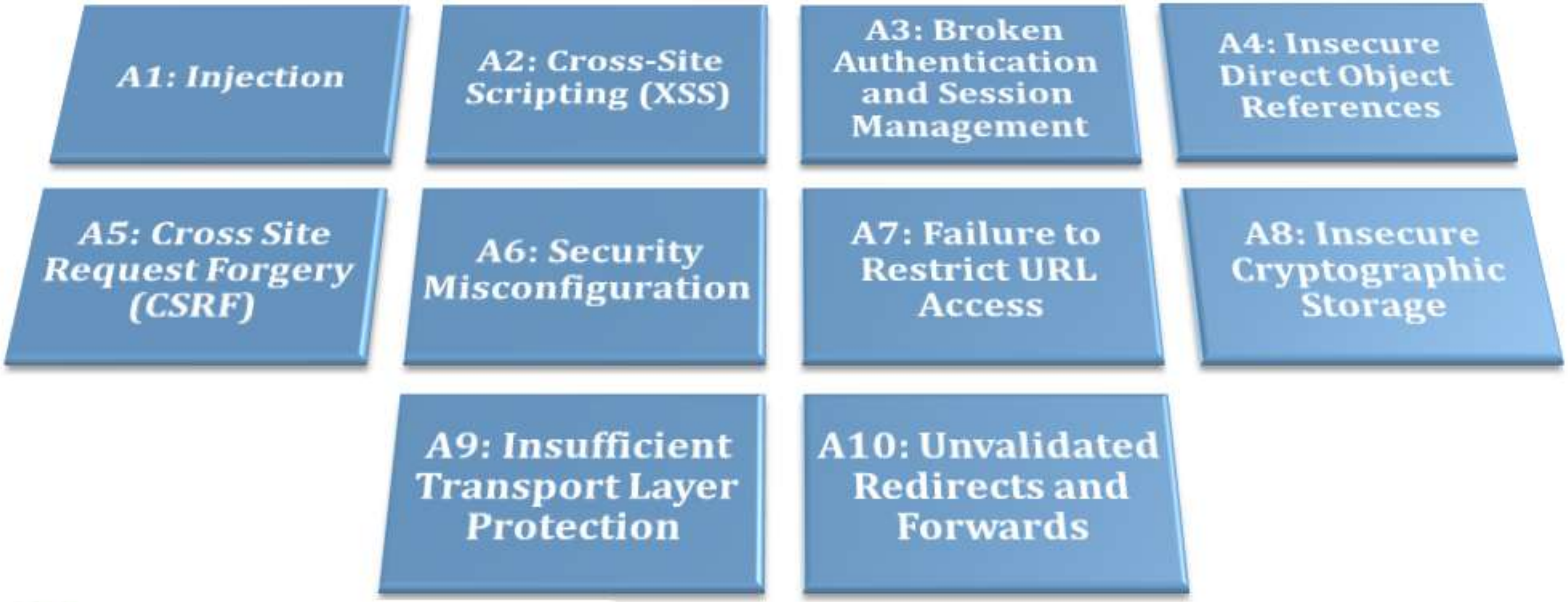
Network

Data

The Application layer is the most exposed to the attacker.

Even with hardened end points and networks vulnerabilities in applications can allow attackers to access data

OWASP TOP TEN



- A1: Injection
- A2: Cross-Site Scripting (XSS)
- A3: Broken Authentication and Session Management
- A4: Insecure Direct Object References
- A5: Cross Site Request Forgery (CSRF)
- A6: Security Misconfiguration
- A7: Failure to Restrict URL Access
- A8: Insecure Cryptographic Storage
- A9: Insufficient Transport Layer Protection
- A10: Unvalidated Redirects and Forwards

OWASP
The Open Web Application Security Project
http://www.owasp.org

http://www.owasp.org/index.php/Top_10

CWE & SANS Top 25

Insecure Interaction Between Components

- SQL Injection
- Command Injection
- XSS
- Unrestricted upload
- CSRF
- Open Redirect

Risky Resource Management

- Buffer Overflow
- Path Traversal
- Download of code with no check
- Untrusted inclusion
- Dangerous function
- Format String
- Integer Overflow

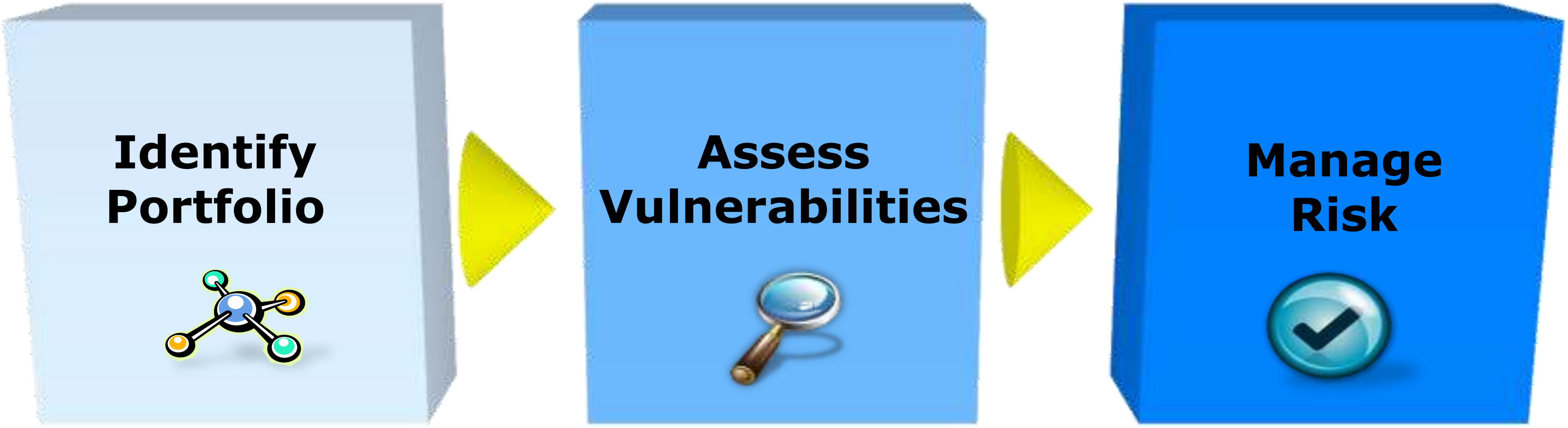
Porous Defenses

- Missing Authentication
- Missing Authorization
- Hard coded credentials
- Missing encryption
- Untrusted inputs in security decision
- Unnecessary Privileges
- Incorrect authorization
- Incorrect permission assignment
- Broken crypto
- No restriction of authorization attempts
- Use of one way hash with no salt

CWE & SANS Institute
TOP 25
MOST DANGEROUS SOFTWARE ERRORS

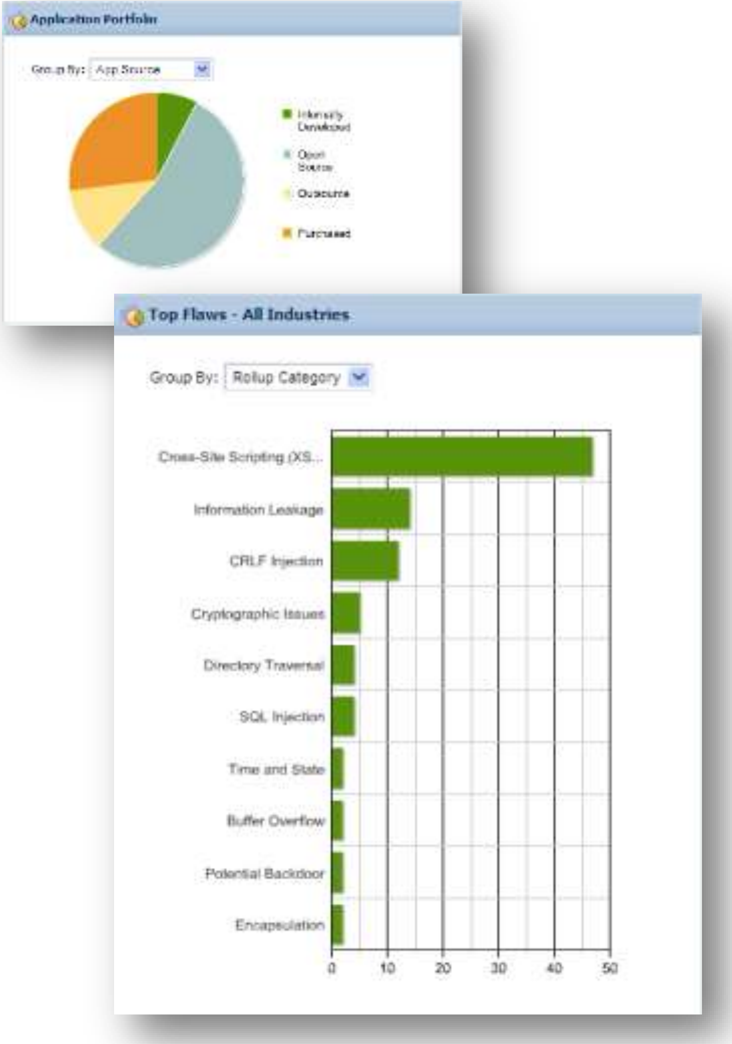
Application Security Program Elements

- From Risk Awareness to Risk Mitigation with an Application Security Program



IDENTIFY APPLICATION PORTFOLIO

- Get a handle on “application sprawl”
  - Involve business units, procurement and vendor management, and automated discovery
  - Consider regulatory impact, data leakage risk, operational risk
  - Create a policy



Application Portfolio

Group By: App Source

Top Flaws - All Industries

Group By: Rollup Category

ASSESS VULNERABILITIES

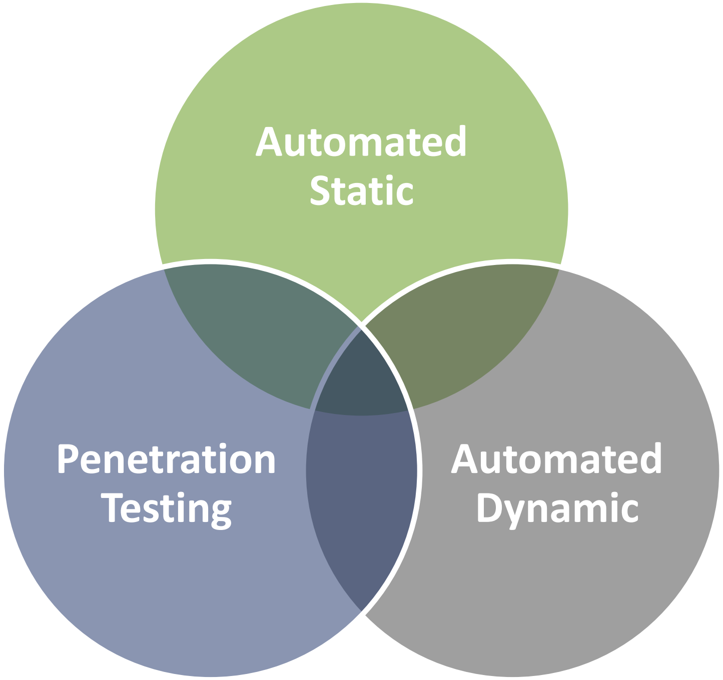
- Understand vulnerabilities in your application portfolio
  - Leverage automated analysis techniques
  - Static and dynamic scanning
  - Engage third-party vendors and service providers

Improving Coverage Of Vulnerability Classes

- Each testing technique has strengths and weaknesses

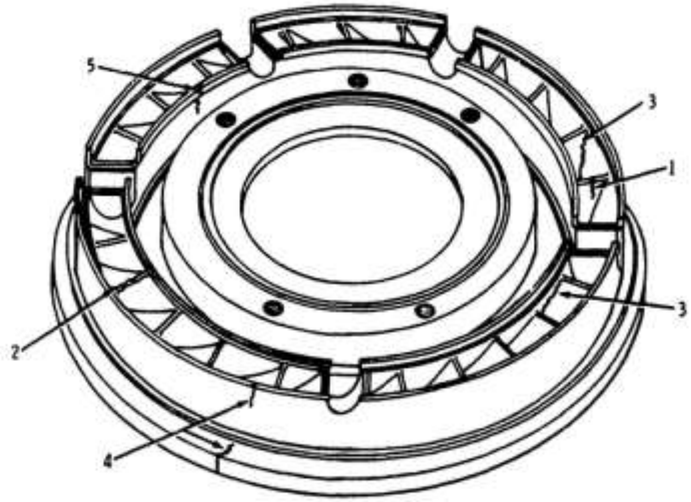
- A complete analysis includes:
  - Static analysis (i.e. White Box)
  - Dynamic analysis (i.e. Black Box)
  - Penetration testing

- Manual penetration testers can focus on vulnerabilities only humans can find



STATIC ANALYSIS

- Analysis of software performed without actually executing the program
- Full coverage of entire source or binary
- Not the “trial and error” of dynamic analysis
- Cannot see system configuration of deployment environment



DYNAMIC ANALYSIS

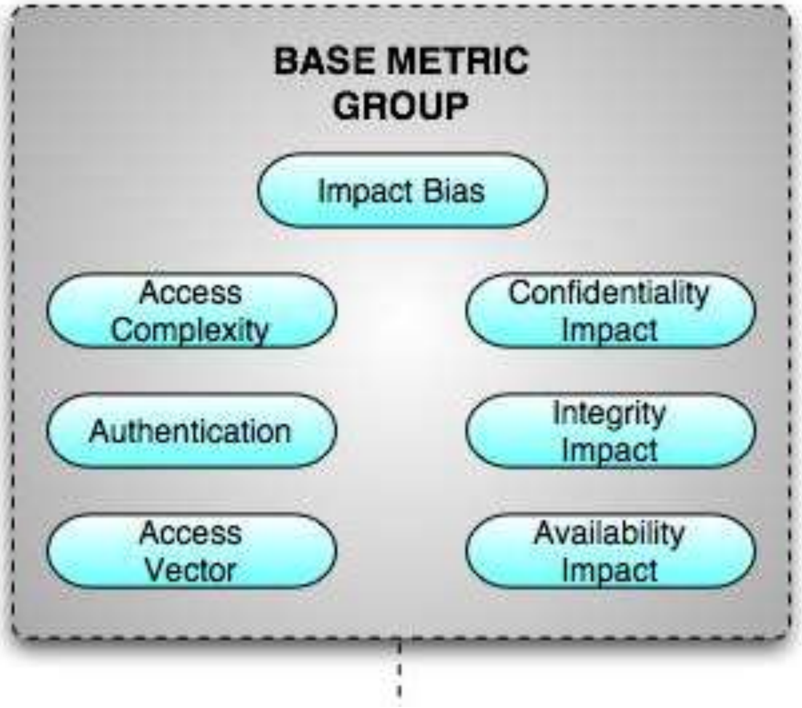
- Analysis of software performed against a running instance of the program
- Mimics how an attacker would attack the application
- Discovering vulnerabilities can take longer and coverage may be limited
- Exposes vulnerabilities in the deployment environment

Risk Management Evolution

- Managing risk is more than just a list of vulnerabilities

- How can this be combined with other risk information?
  - Asset criticality
  - Network location
  - Host vulnerabilities

- Combining application scan data with network scan data is a great start.



Combining APP Testing And Vuln Scanning

- Network vulnerability scanner knows where all the web applications are.

- It knows of any host vulnerabilities

- It may know about criticality of assets application has access to

- Application testing has knowledge of vulnerabilities that network vulnerability scanners don’t know about.

Evolving Towards Enterprise Security Intelligence

Vulnerability Management

Application Assessments

SUPER-POWERED RISK ASSESSMENTS

Network and Application Assessment

- Assessed applications mapped to network discovered containers provide increased environmental context

- Improved vulnerability class coverage

- More accurate risk assessments

Sample Assessed Application – WebGoat

- Installation and Deployment
  - Windows XP OS
  - Installed WebGoat 5.4 with Apache Tomcat 7.0.27
  - Additional Applications installed for remote management

- Assessments Performed
  - Veracode Static Analysis
  - Veracode Dynamic Analysis
  - Network Unauthenticated Vulnerability Assessment

WebGoat Veracode Assessment Findings

	Static	Dynamic
Very High		
OS Command Injection	2	1
High		
SQL Injection	21	1
Medium		
CRLF Injection	6	
Credential Management	2	
Cross-Site Scripting	117	10
Cryptographic Issues	1	
Directory Traversal	3	

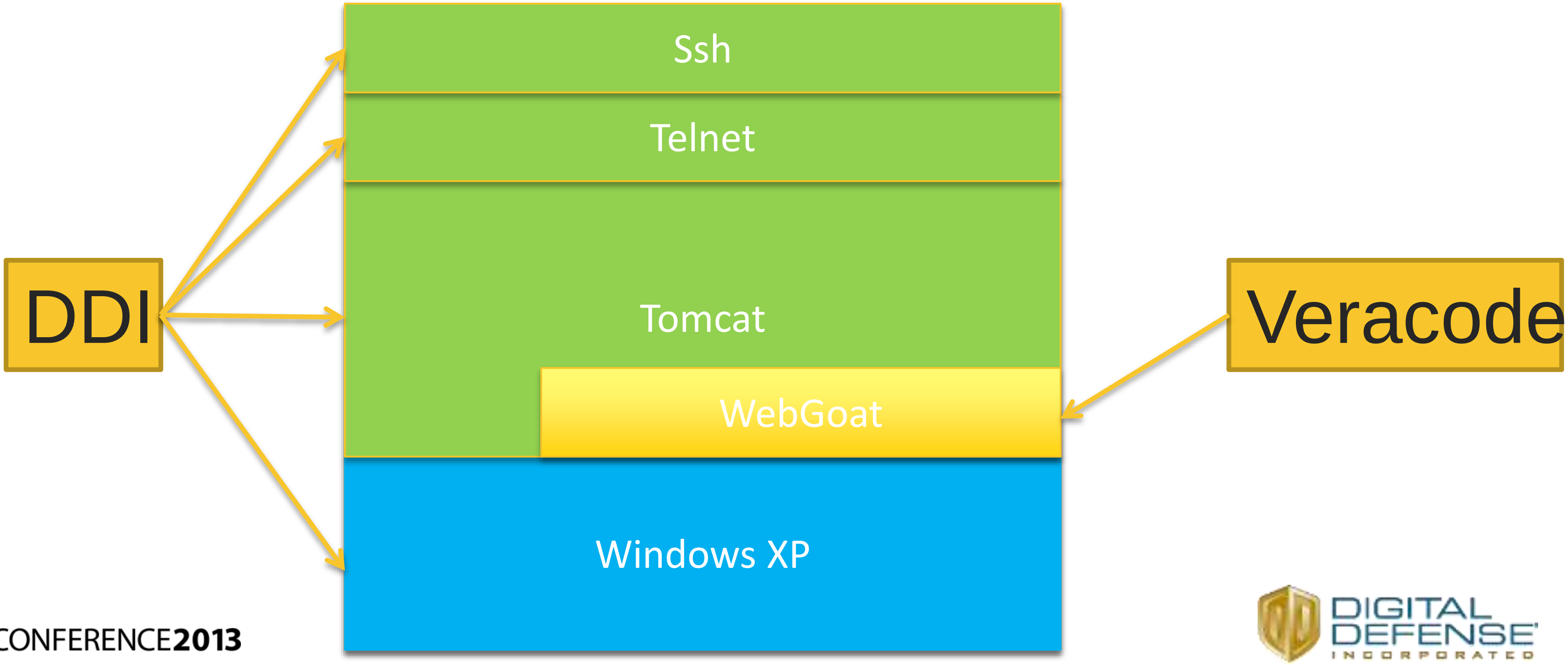
WebGoat DDI Assessment Findings

Unauthenticated Network Vulnerability Assessment
Critical (Compromised)
NetBIOS Shares: Win32/Rorpian Infected Files
High Risk Vulnerabilities
MS12-020 Remote Desktop Protocol Use-After-Free
MS08-067 Microsoft Windows Server Service Stack Overflow
FreeSSHd Authentication Bypass
High Risk Configuration Issues
Easily Guessable Telnet Credentials
Easily Guessable Password (SMB)
HTTP Easily Guessable Credentials (Tomcat Admin Interface)

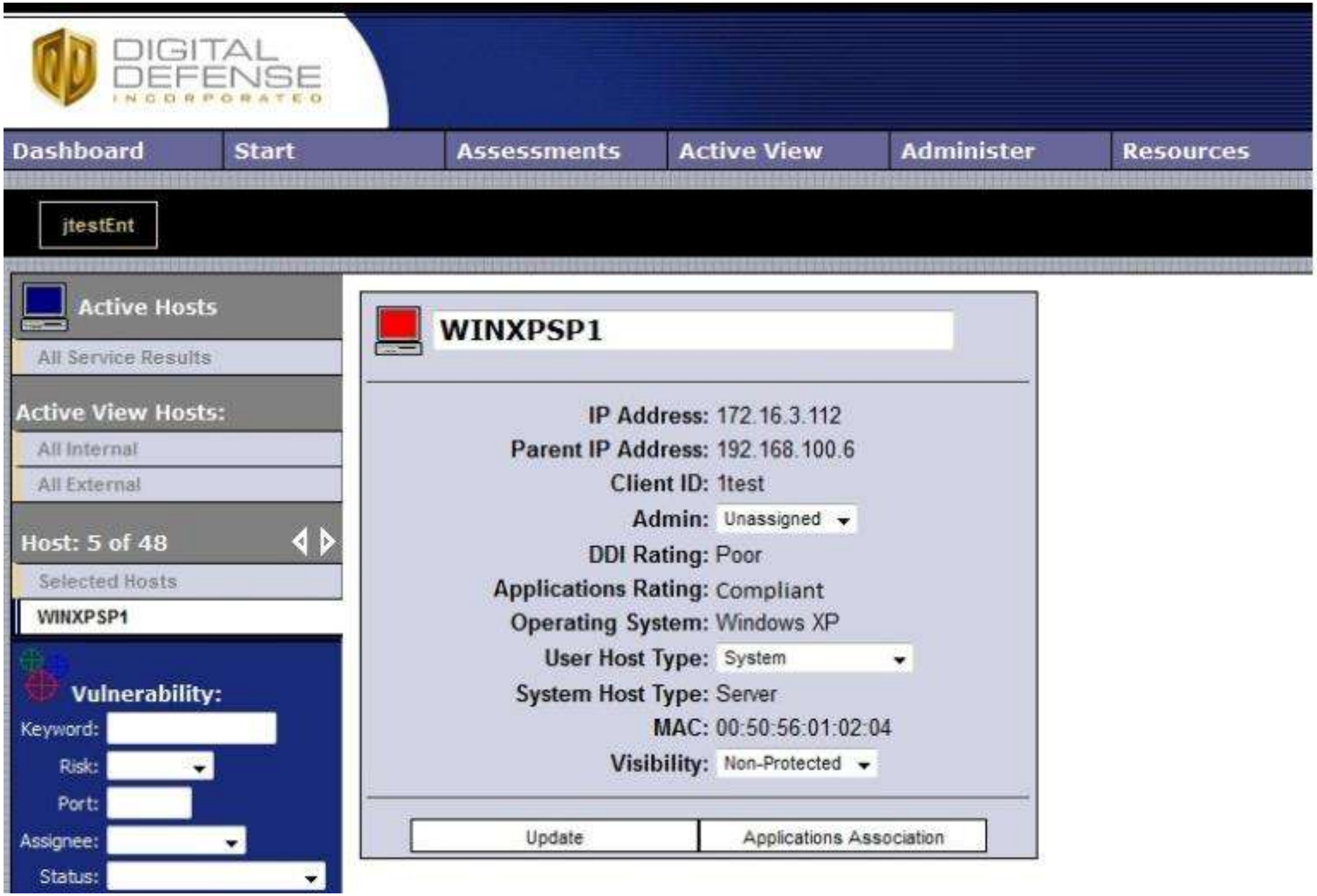
Combined Coverage

- DDI scans the attack surface exposed by the Ssh, telnet, and tomcat processes as well as Windows XP

- Veracode scans the attack surface exposed by the WebGoat application



Integration Sneak Peek



WINXPSP1

IP Address: 172.16.3.112
Parent IP Address: 192.168.100.6
Client ID: 1test
Admin: Unassigned
DDI Rating: Poor
Applications Rating: Compliant
Operating System: Windows XP
User Host Type: System
System Host Type: Server
MAC: 00:50:56:01:02:04
Visibility: Non-Protected

Summary

- Vulnerability scanning should include both host layer and application layer
- Vulnerability Silos impede understanding of overall security risk
- Map application layer vulnerabilities and host vulnerabilities over infrastructure to gain risk insight
- Come talk to us to find out our future research plans in this area.

QUESTIONS?

Contact

Gordon MacKay, Digital Defense Inc.
gordon.mackay@ddifrontline.com
@gord_mackay

Chris Wysopal, Veracode
cwysopal@veracode.com
@weldpond

Security in knowledge