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

Gordon MacKay
Digital Defense, Inc.

Chris Wysopal
Veracode
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
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

\[
\text{Risk} = \text{Threat} \times \text{Vulnerability} \times \text{Cost}
\]
ONE SOLUTION TO RISK

Evolution of Species

Darwin's Finches

Leaves → Darwin's Finches

Buds / Fruit → Darwin's Finches

Seeds → Darwin's Finches

Insects → Darwin's Finches

Grubs → Darwin's Finches

Tool Using Finch
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

Scanner

EVA

Internet

Scanner

Authenticated

Client Network
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
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.
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
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
ASSESS VULNERABILITIES

- Understand vulnerabilities in your application portfolio
  - Leverage automated analysis techniques

- Static and dynamic scanning

- Engage third-party vendors and service providers
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
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.
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
<table>
<thead>
<tr>
<th></th>
<th>Static</th>
<th>Dynamic</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Very High</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>OS Command Injection</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td><strong>High</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SQL Injection</td>
<td>21</td>
<td>1</td>
</tr>
<tr>
<td><strong>Medium</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>CRLF Injection</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>Credential Management</td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>Cross-Site Scripting</td>
<td>117</td>
<td>10</td>
</tr>
<tr>
<td>Cryptographic Issues</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>Directory Traversal</td>
<td>3</td>
<td></td>
</tr>
</tbody>
</table>
# 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
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