Maximizing the ROI of your Pentest

SaintCon
October 2025

John, Mark, & Brian Hoopes

Agenda

- Why are you getting a pentest?
- What you can do to maximize value
  - Before the test
  - During the test
  - After the test
- How do you know if you got a good pentest?

Slides: https://www.merisec.com/blog

Know your Bias - Mark

- “Boutique” Pentester
- Application Penetration Tester (12 years)
  - Network Penetration Tester (6 years)
  - Secure Development Trainer
- Web Development Project Manager (5 years)
- Major Incident Manager, Web hosting operator (6 years)

Slides: https://www.merisec.com/blog

Know Your Bias - Brian

- Software Engineer (15 years)
  - Broadcast media websites
  - KSL Marketplace - growing development team from 1 developer to 25+
- CISO (5 years)
  - Focused on Security and Trust and Safety
  - Started Security “office”

My views are my own and not my employers.

deseret digital media

KSL.com

Know Your Bias - John

- Operations (5 years)
  - Mainframe
  - Network
  - Web Hosting
- Security Penetration Tester (25 years)
  - Focused on Application Security
  - Pivoted to Hardware / ATM / Automotive

My views are my own and not my employers.

Why get a pentest?

Required for Compliance

Understand your Security Posture

Required by a Customer

Test Your Procedures / Team

Measure Seccess of a Security Campaign

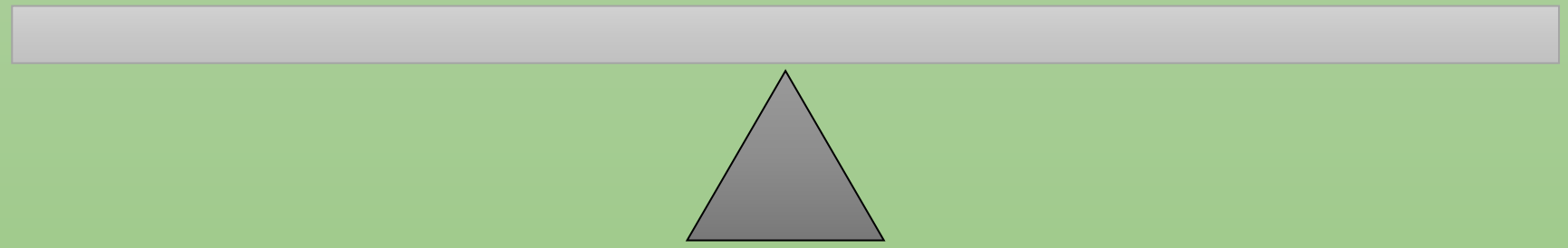
Due Diligence (M&A)

Preparing for Success

How much do you tell your pentester?

A REAL attacker won't have any starting information

A pentester's time is limited



Pentest Preparation Checklist

- ❑ Context
- ❑ Scope
  - ❑ Source Code
- ❑ Test Environment
- ❑ Roles / IDs
- ❑ Rules of Engagement
  - ❑ WAF

Set the Stage for the Pentester

What does your company do?

What value does the application provide?

Who are your users?

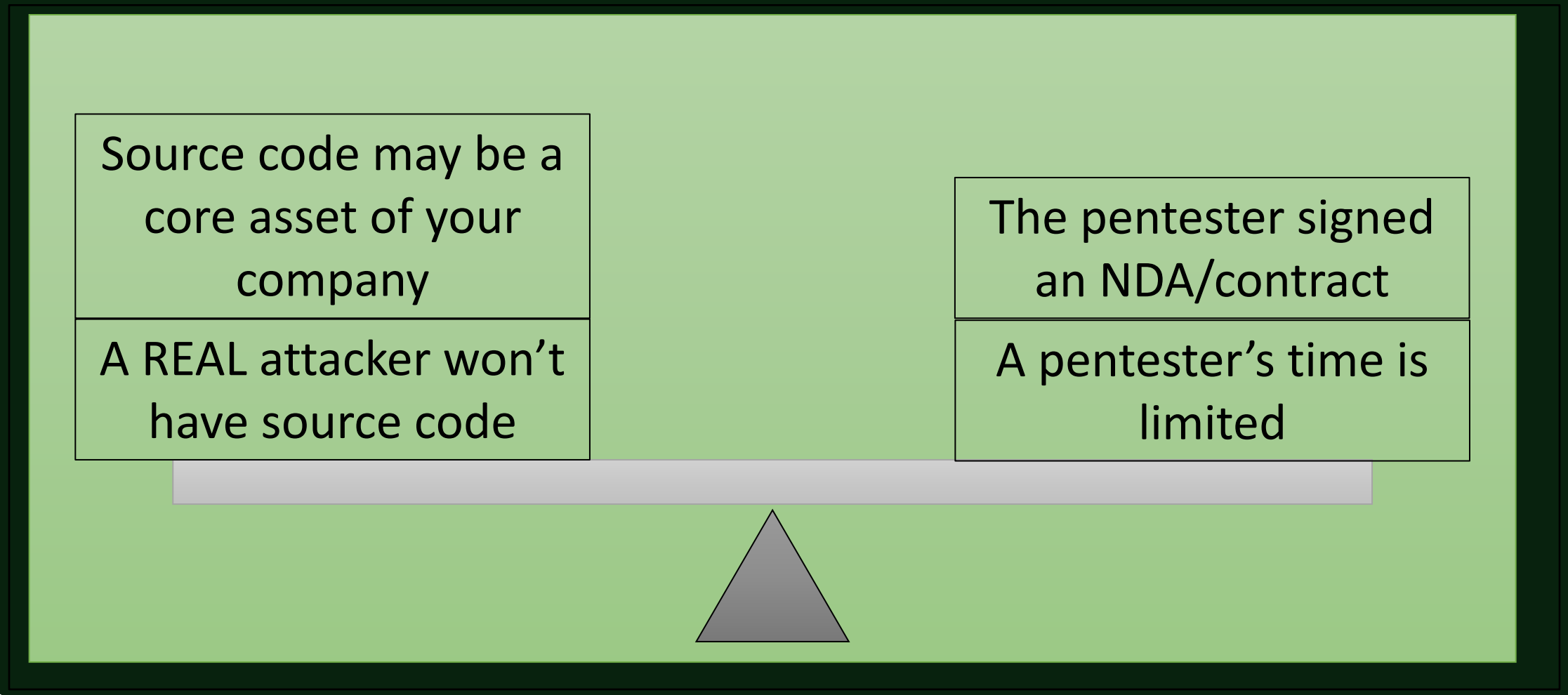
Why are you getting a pentest?

What risk in this environment keeps you up at night?

Defining the Scope

- External Network
  - A list of IP addresses, subnets, and/or domains to be tested
  - Direction to perform OSINT to discover IPs and assets
- Internal Network
  - Often presented in terms of network ranges
  - What is NOT in scope. Both techniques and specific devices
- Application
  - Web: Starting URL(s), in-scope/out-of-scope supporting services
- Clouds
  - Export a list of assigned IPs, but this can be ephemeral and is probably not contiguous
  - Other cloud resources

To give source code or not to give source code?



Testing in production?

Production

- Typically lower setup effort
- Represents the actual surface an attacker will go against
- Might impact clients
  - Sometimes attacks live-on past the pentest
- If there is a vulnerability, you may have just caused a data breach

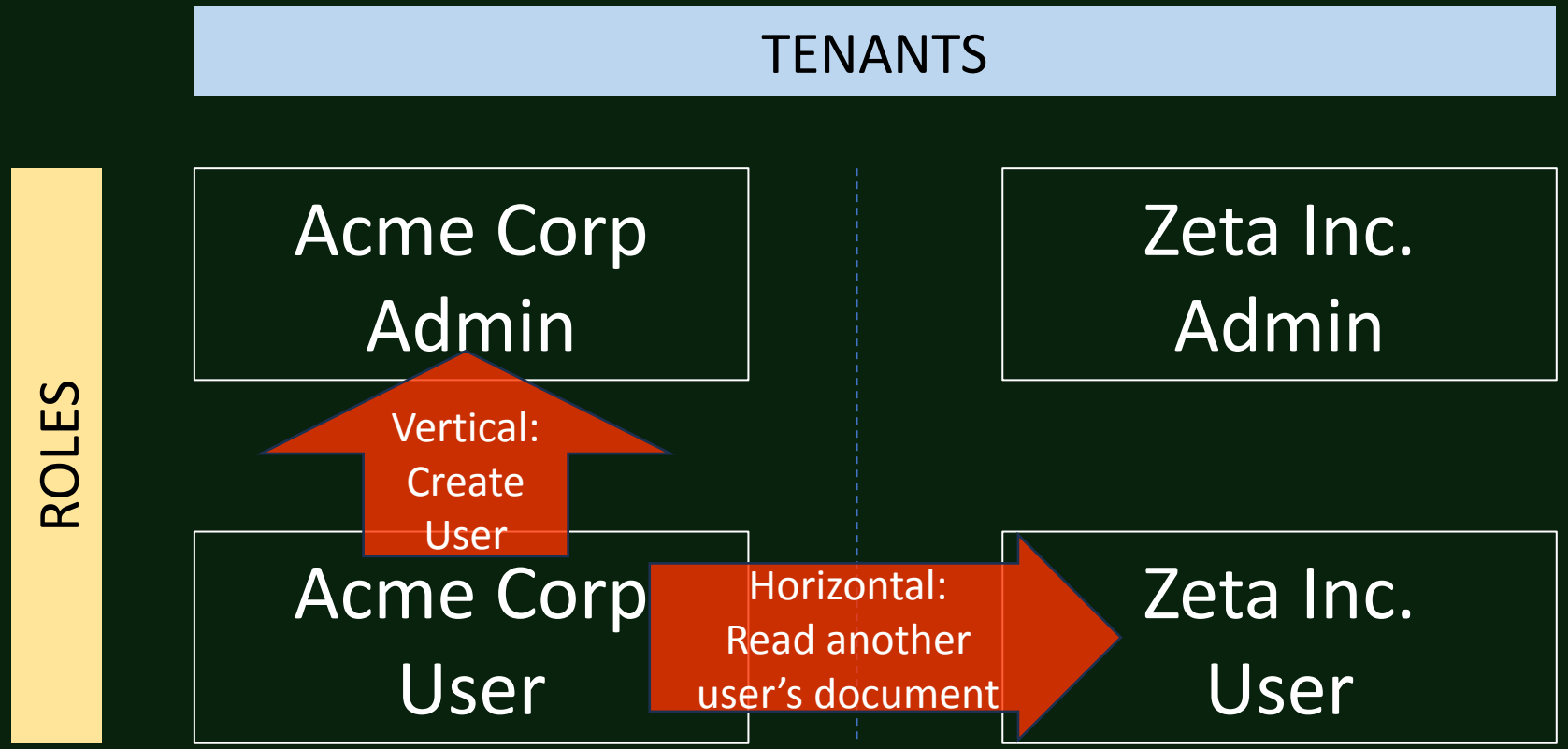
Test/UAT/Dev/etc.

- May require setting up network access (VPN) to access
- May require adding realistic data
- May occupy an environment normally used for other things

Pentest Preparation Checklist

- ✔ Context
- ✔ Scope
  - ✔ Source Code
- ✔ Test Environment
- ❑ Roles / IDs
- ❑ Rules of Engagement
  - ❑ WAF

Why to testers want so many IDs?

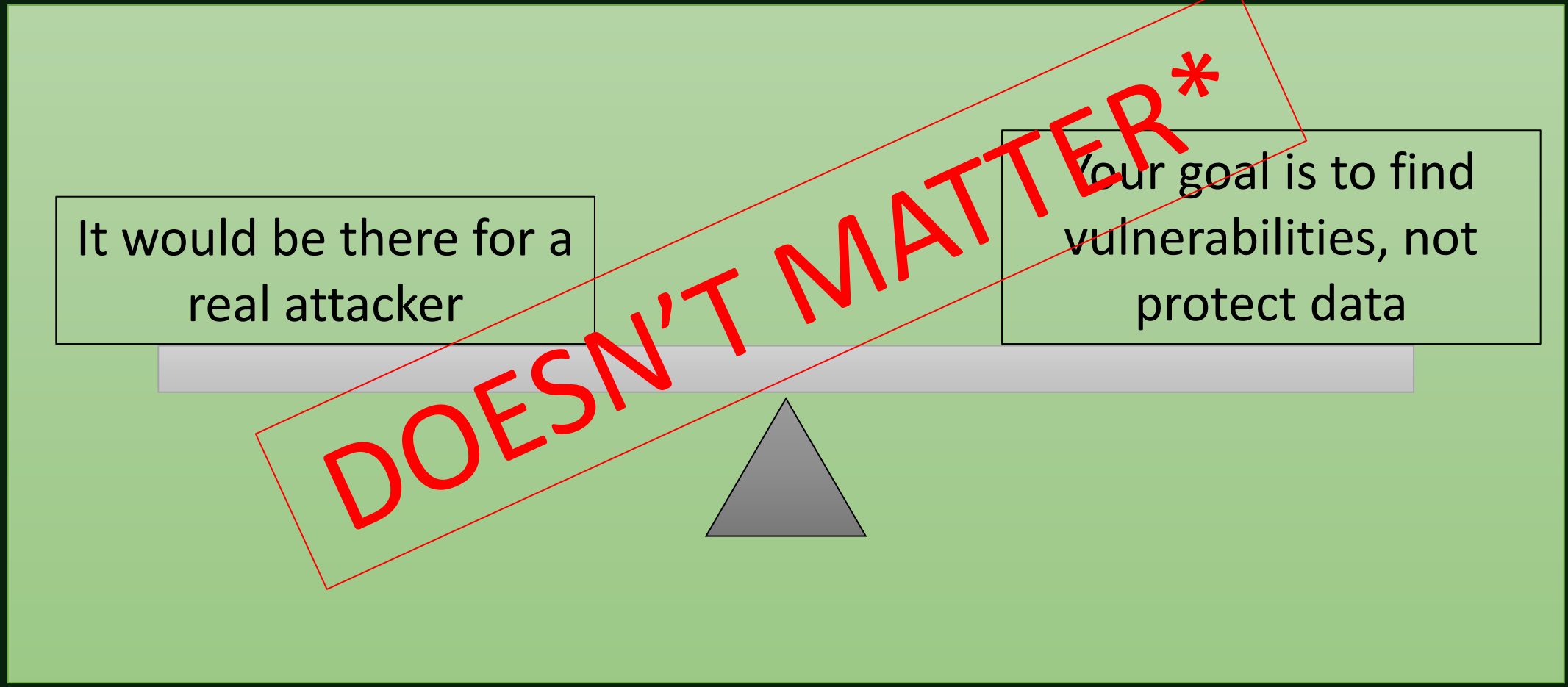


Rules of Engagement

Common Elements

- ❑ Time of day
- ❑ Out-of-scope servers / domain
  - ❑ 3rd Party
  - ❑ Temperamental
  - ❑ Soon to be out of service*
- ❑ Out-of-scope techniques
  - ❑ Denial of Service
  - ❑ Social Engineering
  - ❑ Password Cracking
- ❑ Sensitive Data Handling

Do you turn off your WAF?



Quick Example

Search

Capybara

NO DOCUMENTS FOUND

Search

Capybara” or “a”=“a

BLOCKED BY XYZ WAF

Search

Capybara” or “z”=“z

838 DOCUMENTS FOUND

Set the Stage for Your Team

A mandatory security review of our application will be taking place from April 1 to April 10. As a reminder, any high or critical findings discovered will need to be remediated before this version can be released.

To support our common goal of protecting client and company data, an independent security review will be performed from April 1 to April 10. We will prioritize fixing any high or critical findings before we put the code in production.

During the Test

Keep the Test Environment Available

Change the Test Environment

**Except to fix a critical vulnerability*

Expect Questions

How does the "[*name*]" feature work?

Should [*user role*] be able to [*modify object*]?

Is [server] in scope?

Exploiting this vulnerability might [*potential risk*]. Should I try it?

Expect Updates

Critical / High Finding Updates	• Typically delivered “immediately” after discovery • Should include vulnerability, impact, and replication steps • Should be delivered over a secure channel
Periodic Updates	• Typically delivered between daily and weekly • Should include a high-level description of what has been tested • May include outstanding questions or roadblocks
Testing Start / Stop Updates	• May be useful if a SOC is ignoring alerts

After the Test

Readout Calls – It's your dime

- Invite anyone who might have a question
  - The people who are going to have to fix the problem
  - Grumpy executive who thinks a problem is worse than it is
- Ask about what your tester has seen at similar companies
  - Resolution strategies, resolution timing, design decisions
- Report phrasing can be adjusted
- Report severities can be adjusted…sometimes

Requesting Finding Severity Changes

- Good Reasons
  - An external business process mitigates the impact
  - There is a control that blocks the attack path that was not part of the test
    - IF it can be tested now, otherwise it just gets added as a note in the finding

- Bad Reasons
  - We can’t pass compliance with anything higher than a medium severity
  - We can’t fix it within the deadline that comes with that severity
  - We couldn’t reproduce the exploit

How do you know if you got a good pentest?

- Communication with pentester
  - They should know specific details of your environment / application
- Level of detail in the report
  - Findings should describe specific features
  - Replication steps should be included (not just screenshots)
  - Recommendations should be tailored
  - If there are few findings, the report should describe the techniques used to test in more detail.

Sample Executive Summaries

“ Coyote Corp. conducted a security review of the Acme Corp. internal network between April 1 and April 10, 2025. No vulnerabilities were found. ”

vs

“ Roadrunner Inc. conducted a security review of the Acme Corp. internal network between April 1 and April 10, 2025. The network demonstrated strong security practice including patch management, egress filtering, and network segmentation. No vulnerabilities were found.

Roadrunner attempted to capture and replay Windows hashes observed on the network, however SMB Signing was required on all Windows systems, blocking this common attack. ”

Sample Finding

“ Cross-site Scripting occurs when unvalidated input is inserted into a webpage. Coyote Corp was able to save a malicious payload into the user profile page as seen in the screenshot below. ”

vs

“ JavaScript Injection (commonly known as Cross-site Scripting) occurs when user-controlled input is incorporated into a webpage without proper validation or encoding. Roadrunner was able to save a JavaScript payload in the “title” field of the user profile page, and that payload was executed on the user profile, user search, and user management pages (viewable only by the administrator).

To replicate the vulnerability follow these steps…”

Sample Replication Steps

“ Evidence
The screenshot below shows the Cross-site Scripting payload executing.”

vs

“ Replication Steps

1. Log in to the Acme site as a user in the “viewer” role.
2. Click on the profile picture in the top right and select “My Profile”
3. Click “Edit Profile” at the top of the page.
4. In the “Title” field, enter the following payload

“><img src=bad onerror=“alert(‘XSS in Title’)”><x a=“

…

”

Fix the concept not the instance

Conclusions

When to Pentest?

- As your one security investment
- When required by customer or compliance
- As the capstone to your security program

How Do You Know If You Got A Good Pentest?

- The report should contain specific details about your environment
- Failed attacks and strong controls should be included in the executive summary

How Do You Maximize the ROI Of Your Pentest?

- **Eliminate barriers between the pentester and the vulnerabilities**

Thank You!

Slides
https://www.merisec.com/blog

Mark Hoopes
mark@meristeminfosec.com
https://www.linkedin.com/in/markhoopes/

Brian Hoopes
brian.hoopes@gmail.com
https://www.linkedin.com/in/brian-hoopes/

John Hoopes
john@olympus.dyns.cx
https://www.linkedin.com/in/johnhoopes