Reporting

Penetration Testing Execution Standard (PTES)

1. Pre-engagement Interactions
2. Intelligence Gathering / Reconnaissance
3. Threat Modeling
4. Vulnerability Analysis
5. Exploitation
6. Post-Exploitation
7. **Reporting**

www.pentest-standard.org

Why Write a Report?

- How else will the company know what you found?
- How else will the company know how to fix things?
- How else will managers AND technical folks understand what you did?

What Should a Report Do

- Convey your findings to the customer
  - How you got in
  - What you were able to obtain
  - How they can remediate

Think About Your Audience!

- Managers and Executives will read the report
  - Make sure they can understand it
- The technical frontline workers will read the report
  - Make sure they get the juicy details
  - They'll be the ones actually fixing the vulnerabilities you discovered

Components of a Report

- Executive Summary
- Methodology
- Strengths and Weaknesses
- Remediation Details

Executive Summary

- You'll typically write this last.
- How would you explain the results of the test to an Executive you ran into in the elevator?
- High level findings
- High level recommendations

Executive Summary – Likely Components

- **Scope of Work** – IPs tested, type of testing, etc.
- **Project Objectives** – The goal of the test, linking to the organization's objectives
- **Assumption** – Any assumptions the tester made?
- **Timeline** –Start and end dates
- **Summary of Findings** - High level view, discovered risks based on priorities
- **Summary of Recommendation** – Based on the risks, high level recommendations

Methodology

- How was the test conducted?
- Risk rating methodology
- Tools you used

Findings – Strengths and Weaknesses

- Provide detailed information on each finding
  - Make sure high level execs can still understand what’s going on, but include the juicy details so the IT staff can fix.
- Describe the issue and impact of the issue for each finding
- Be sure to include recommendations on how to mitigate or patch each vulnerability!!!
- Good place to use any graphics if you have any

Example Attacks

- Tell the customer how you got in
  - Allows them to replicate, and test their fixes
  - Allows them to validate your work
- Better credibility for you

Appendices

- This is where you’ll include ALL of the details.
- Detailed spreadsheet of each vulnerability
- Lists specific hostnames, IPs that are affected
- Low level technical details on how to remediate, if necessary

Sample Report

- https://www.offensive-security.com/reports/sample-penetration-testing-report.pdf

Take Notes!

- When writing the report, you'll wish you would've taken better notes during the technical portion of the test
  - Detailed Notes
  - Screenshots
  - Logging your activities

Closing Thoughts

- GOOD WRITING IS KEY
  - Grammar
  - Spelling
  - This will keep or kill your credibility
- Have your reports peer-reviewed
  - Someone that understands the technical
  - Someone that’s good at English and writing