Module 8 (Penetration Test Report)

• At the end of this module, you should have a good idea of the structure of a reasonable penetration test report and also understand a little bit about evaluating risks using the MS DREAD model.
Penetration Test Report Structure*

- Executive Summary
- Technical Report
  - Intro
  - Information Gathering
  - Vulnerability Assessment
  - Exploitation/Vulnerability Confirmation
  - Risk/Exposure
  - Conclusion

Executive Summary

- Background
- Overall Posture
- Risk Ranking/Profile
- General Findings
- Recommendation Summary
- Strategic Roadmap
Technical Report
Intelligence Gathering

• Passive Intelligence
  – (Open Source Intelligence or OSINT see thegrugq)

• Active Intelligence
  – Infrastructure mapping, port scanning (footprinting)

• Corporate Intelligence
  – Information about corporate structure (identify sources)

• Personnel Intelligence
  – Information mapping users to the client organization
Technical Report
Vulnerability Assessment

• Vulnerability Classification Levels
• Technical Vulnerabilities
  - OSI Layer Vulns
  - Scanner-identified
  - Manually-identified
  - Overall Exposure
• Logical Vulnerabilities (see http://bit.ly/147Vpf1)
  - NON OSI Vuln
  - Type of vuln
  - How/Where it is found
• Exposure
• Summary of Results
Technical Report
Exploitation/Vulnerability Confirmation

• Exploitation Timeline
• Targets selected for Exploitation
• Exploitation Activities
• Indirect Attack
  – Phishing
  – Clientside
  – Browser
• Post-Exploitation Activities
Technical Report
Risk/Exposure

- Evaluate incident frequency
- Estimate loss magnitude per incidence
- Derive Risk
Technical Report
Conclusion

- Recap all elements of the report.
- Support growth of client's security posture.
- Give positive support and guidance to enable progress in security program.
MS Risk Model DREAD
(Visual Studio Security Push)

• DREAD: Evaluate each 0-10
  - Damage Potential
  - Reproducibility
  - Exploitability
  - Affected Users
  - Discoverability

• \((D + R + E + A + D)/5 = \text{DREAD Score}\)

• Don't just accept the score as fact, understand what it is and figure out how to explain it.