Pen Testing: Planning, Scoping, and Recon

Penetration Testing – Getting Started

Alexander Tushinsky

Cybersecurity & Software Development Consultant

@ltmodcs alextushinsky.com

Overview

- Project Management
- Effective Notes

Project Management

Penetration Testing Engagement

- What do we do first?

Project Management Tasks

- Goals and objectives
- Scope of work
- Budgets
- Schedule
- Communications plan
- Deliverables

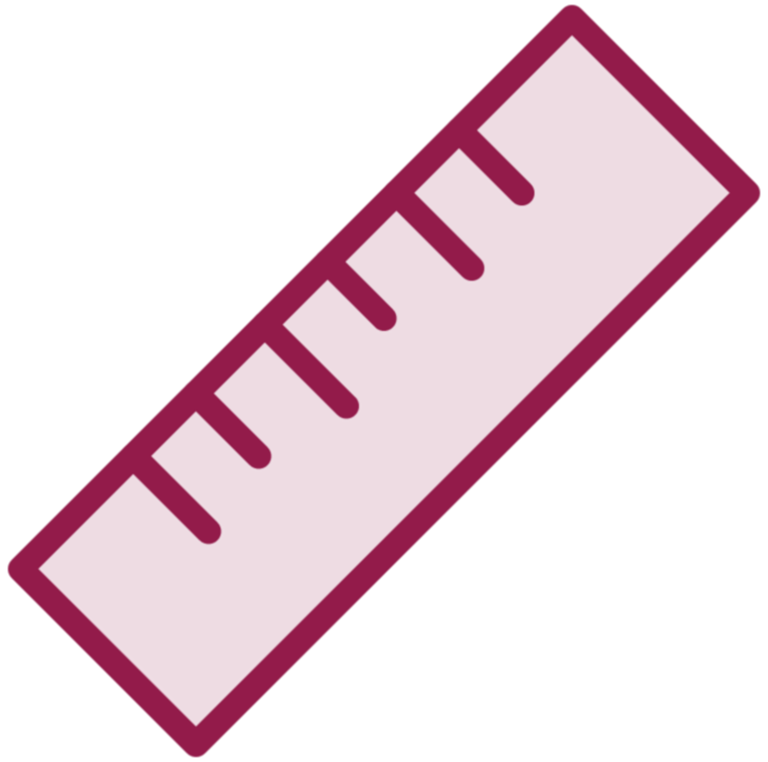
Goals

- An achievable outcome
- Should be SMART
  - Specific
  - Measurable
  - Achievable
  - Realistic
  - Time-bound

Identify vulnerabilities in Application X that permit a non-administrative account to access personally identifiable information in software release version 3.01.

Objectives

- How we achieve our goal
- Actionable steps
- Determine the types of attacks that mitigate the risk identified by the goal



Scope of Work

- Identify resources and end-points that will be targeted
- What is out of scope?
- Destructive attacks
- Working on the scope directly impacts your statement of work

Budget

- Based on the scope
- Based on your rates
- Scope may change as a result

Schedule

- Availability of environment / end-points
- Availability of company resources
- Agreed upon timeframes for attack
- Your availability
- Budget and scope play are considered as well
- Part of Rules of Engagement document

Communications Plan

- Point of contact for support
- Escalation path for reporting critical issues
- Where to report illegal activity
- Who gets the final report?
- Two-way street

Deliverables

- List of artifacts that meet project goals
- Supporting documentation
- Debriefing sessions
- Remediation and re-testing

Taking Good Notes

Project Note Taking

- Clear and concise phrases
- Write the notes based on your understanding of what was said
- Use heading, bullets, or numbered lists to create sections
- Underline or “star” items of importance

Pen Test Note Taking

- Evidence
- Steps to recreate the attack
- Organize by tools used
  - Capture commands/scripts used
  - Any significant results
  - Screenshots
  - Video

Confidentiality

- Notes you take demonstrate vulnerabilities
- Must be encrypted, if kept online
- Can only be shared within the scope of the signed Non-disclosure agreement

Note Requirements

- Digital (preferred)
- Hierarchical
- Searchable
- Support for multiple media types
- Access from anywhere
- Secure

Notes Applications

- Cherry Tree
- Trilium Notes
- Microsoft OneNote
- Many, many others, including Typora, Trilium, Joplin, and KeepNote

Demo

Note Taking Applications

- Cherry Tree
- Microsoft OneNote