Red Team

Spring 2018

Format

- Hands-on Assignments
- Knowledge Sharing
- Accelerated Learning

Accelerated Learning

- Quick onboarding
- Resources for newcomers
- Overview of fundamentals
- Focus on

3 Tiers

🍎 Tier 1 – aka lil rojos

💯 Tier 2 – aka Spicy bois

🔥 Tier 3 – aka Fuego

🍎 Tier 1 - aka lil rojos

- Set up a virtual environment
- Run Kali Linux as a VM
- Complete overthewire.org Bandit Labs
- 3 weeks

VirtualBox

vmware

💯 Tier 2 – aka Spicy bois

metasploit®

- Set up virtual lab
- Run Metasploitable2 & Kali
- Pentest & Document 5 exploits (including 2 web)
- 3 weeks

🔥 Tier 3 – aka Fuego

- Vulnhub
- Hackthebox (if you're l33t)
- Pentest & Document

Documentation

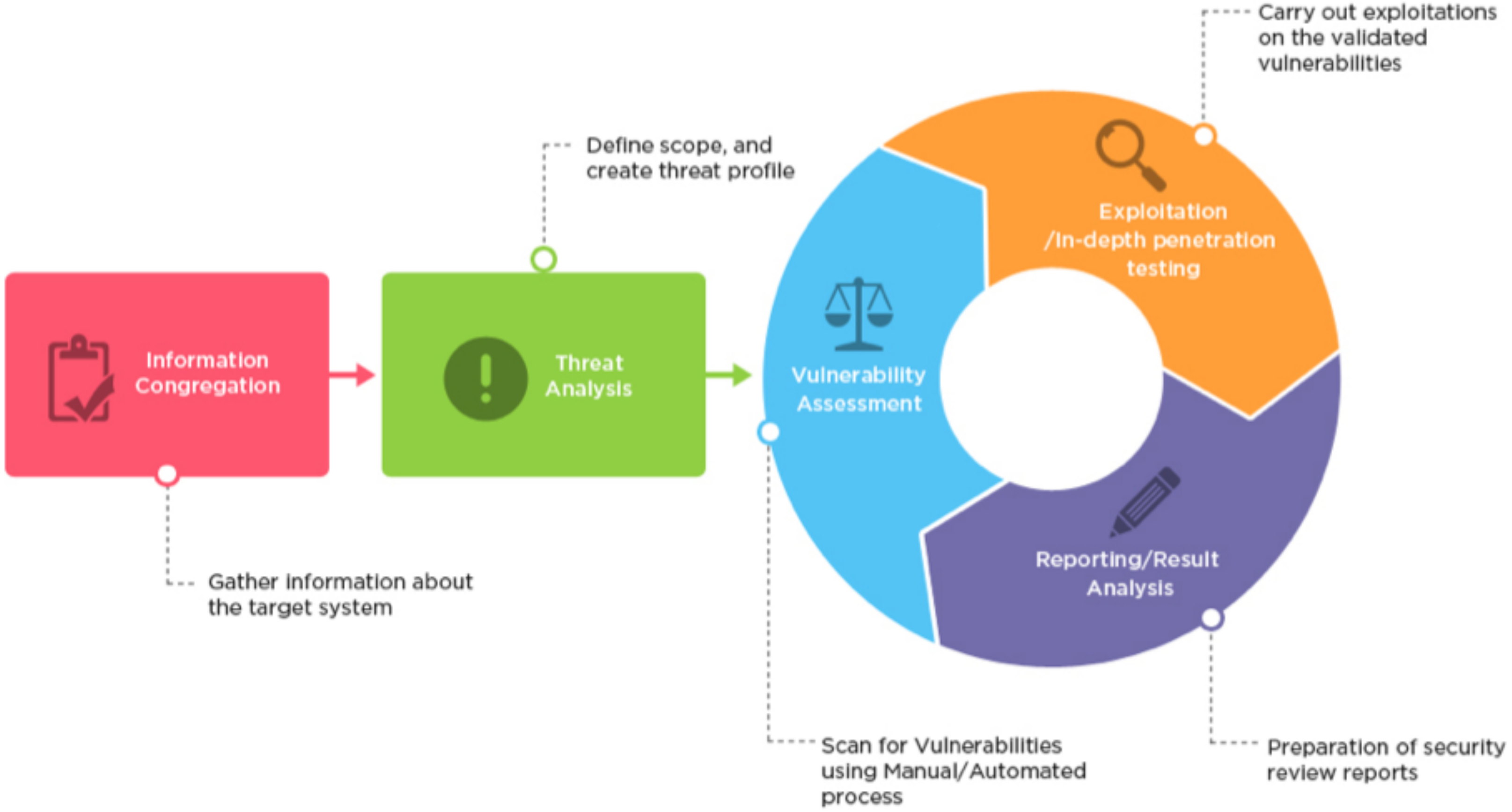
- Essential part of every penetration test

- All steps leading to a successful attack get thoroughly documented; this ensures everything can be reconstructed in detail afterwards

- At the end of an engagement, documentation is used as the basis for an individual report

- Reports make findings understandable to technical admins as well as management

Pentest Lifecycle



Information Congregation

Threat Analysis

Vulnerability Assessment

Exploitation /In-depth penetration testing

Reporting/Result Analysis

Gather information about the target system

Define scope, and create threat profile

Scan for Vulnerabilities using Manual/Automated process

Carry out exploitations on the validated vulnerabilities

Preparation of security review reports

Attack Lifecycle

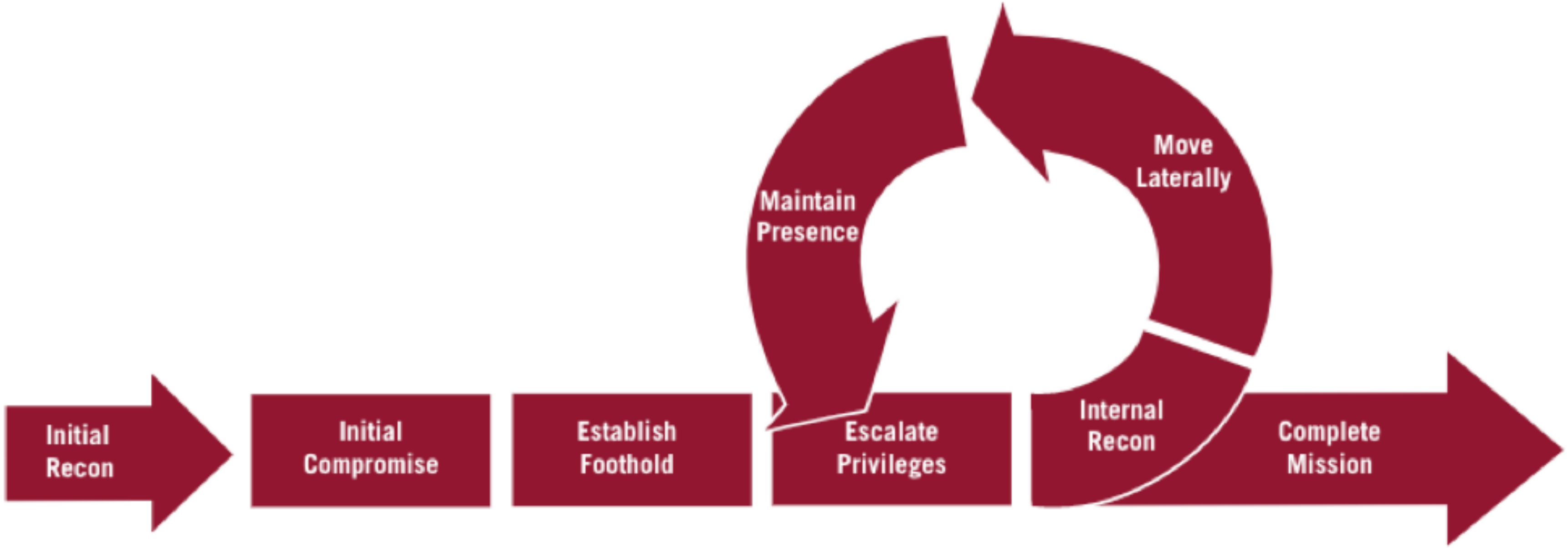


FIGURE 14: Mandiant's Attack Lifecycle Model

Knowledge Sharing

- Weekly presentations by Tiers 2 & 3
  - Executive Summary
  - Technical Details
  - Proof Of Concept

- Reports will be uploaded to Red Team's GitHub

Red Team Engagements