JASON DION
TRAINING THE CYBER SECURITY WORKFORCE

Penetration Testing

THREAT MANAGEMENT

Penetration Testing (PenTest)

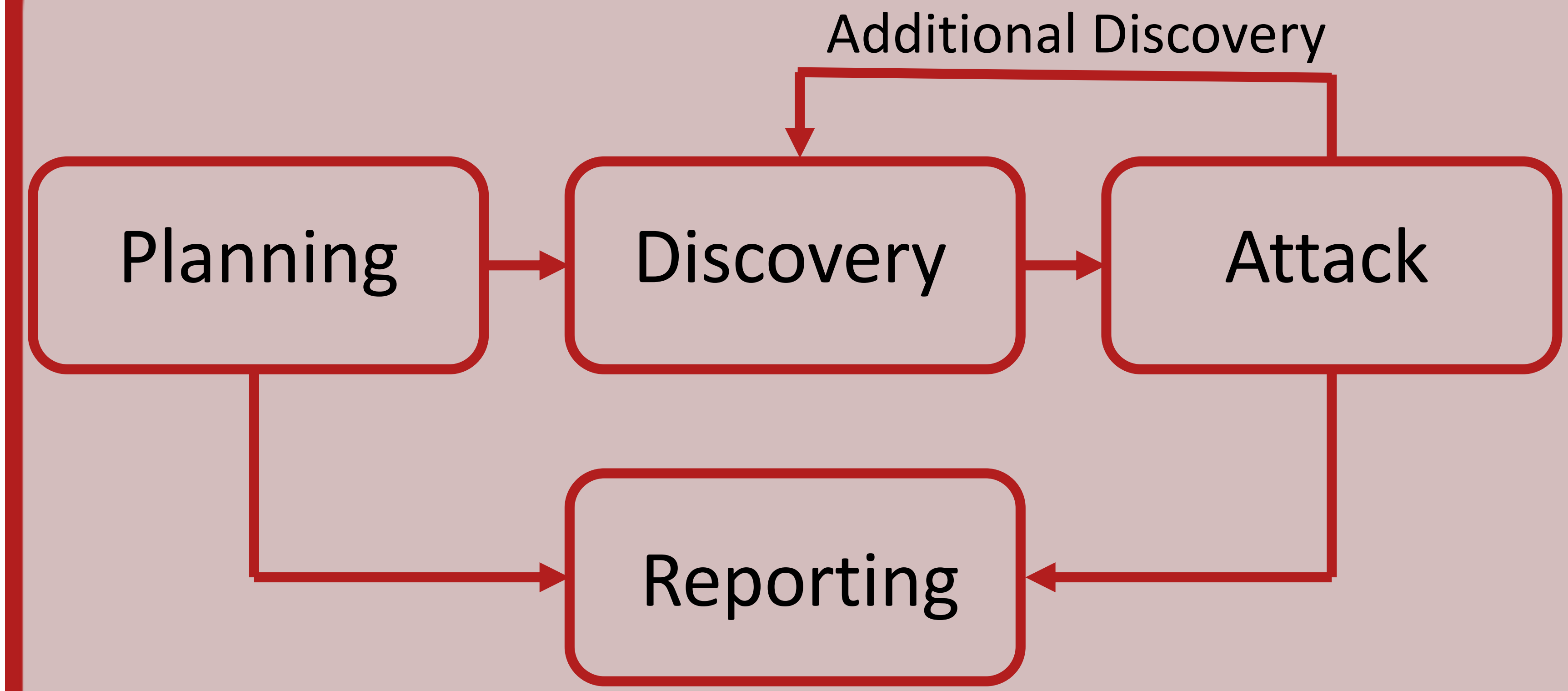
- Penetration testers simulate a cyber attack against your organization’s resources using the same information, tools, and techniques available to an attacker

- Goal:
  - To gain access to your systems and report the findings to management

Who can do the PenTest?

- Can be performed by internal staff or external consultants
- Requires highly skilled individuals
- Tests are very time consuming and costly

Phases of a PenTest



NIST SP 800-115 (Technical Guide to Information Security Testing and Assessment) divides PenTests into four phases

Planning

- An important phase of a PenTest
- No technical work is performed
- Timing, Scope, and Authorization is gained during the Planning Phase
- You should NEVER conduct a PenTest without authorization…it's illegal!

Discovery

- Testers conduct reconnaissance and gather as much information on the network, system, users, and applications

- Examples:
  - Open source research
  - Port scanning
  - Enumeration
  - Vulnerability scanning
  - Web application scanning

Execute the Attack

- Seeks to bypass the security controls and gain access to the system

- Attack Phase (aka Exploitation)
    - Gaining Access
    - Escalating Privileges
    - System Browsing
        - May refer back to discovery phase again
    - Installing Additional Tools

Source: NIST SP 800-115

Reporting

- Testers should prepare a detailed report after the test
- Contains results of the PenTest, describing their successful attacks and suggestions on how to fix them
- Should be prioritized based on the risk posed by each vulnerability exploited