UNIVERSITY of WASHINGTON

For Zoom: If your name does not show your first and last name, please rename yourself from the participants screen with your first and last name.

Be sure to complete the poll to receive attendance credit for the class session.

Hacking 310

Lesson 01: Pentesting Process

Course Overview

Hacking 310 is the first of three courses for the Ethical Hacking certificate.

Objectives for Hacking 310:

- Describe the various types of penetration tests and ethical hacking;
- Recognize the limitations of penetration testing and ethical hacking;
- Identify several free testing methodologies;
- Demonstrate the overall process and rules of engagement of a penetration test;
- Demonstrate reconnaissance by using Nmap, DNS lookups, Maltego, search engine vulnerability (finding tools);
- Demonstrate network-based exploitation using tools such as Metasploit to compromise vulnerable systems, basics of pivoting, and pilfering;
- Describe the common web vulnerabilities; and
- Exploit common application vulnerabilities and flaws.

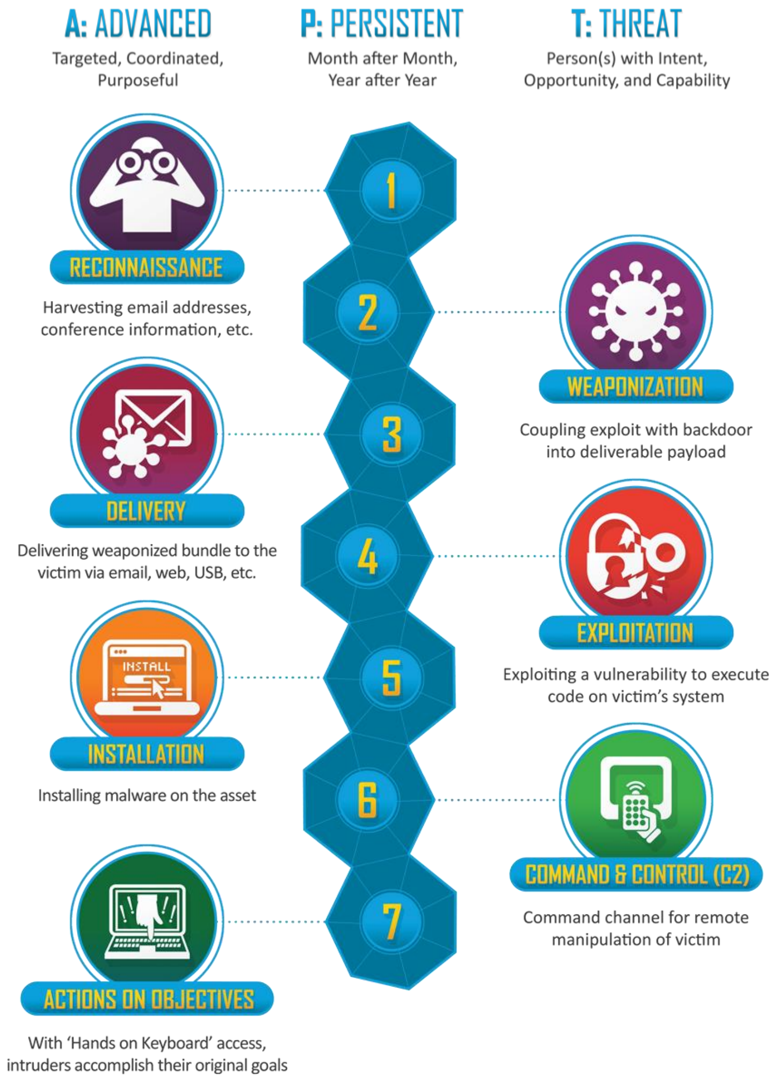
Introduction

- Who am I?
  - James Walker
- Ways to contact me?
  - Preferred - Canvas Online Learning System Messaging
  - UW Email: jaywalk@uw.edu
  - SMS/Phone: 801-419-6359
- Class Format
  - Weekly Lectures: Monday 6PM – 9PM PST
  - Grades
    - Weekly Homework – Canvas Online Learning System
    - Weekly Participation – Don’t miss more than 4 lecture sessions
  - **If you have an extenuating circumstance, please let me know in advance; exceptions will be approved on a case-by-case basis**

Learning Objectives

- What is Penetration Testing?
- What is Ethical Hacking?
- Types of Penetration Tests
- Red/Blue Teams
- Phases of a Penetration Test
- Setting up a Penetration Testing environment

Lockheed Martin Corp: Cyber Kill Chain



A: ADVANCED
Targeted, Coordinated, Purposeful

P: PERSISTENT
Month after Month, Year after Year

T: THREAT
Person(s) with Intent, Opportunity, and Capability

1. **RECONNAISSANCE**
Harvesting email addresses, conference information, etc.

2. **WEAPONIZATION**
Coupling exploit with backdoor into deliverable payload

3. **DELIVERY**
Delivering weaponized bundle to the victim via email, web, USB, etc.

4. **EXPLOITATION**
Exploiting a vulnerability to execute code on victim's system

5. **INSTALLATION**
Installing malware on the asset

6. **COMMAND & CONTROL (C2)**
Command channel for remote manipulation of victim

7. **ACTIONS ON OBJECTIVES**
With 'Hands on Keyboard' access, intruders accomplish their original goals

Figure © Lockheed Martin Corporation:

https://www.lockheedmartin.com/us/what-we-do/aerospace-defense/cyber/cyber-kill-chain.html

Penetration Testing

- What is pentesting?
    - Security assessment
    - Black/White/Gray box testing
- What is ethical hacking?
    - Hacking is about learning how things work
    - Hollywood & misconceptions
    - Informal security assessments and responsible disclosure
    - Bug bounty
    - Red/Blue/Purple team

Phases of a Penetration Test

- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Intelligence Gathering

- What is it?
- Target selection
- OSINT
- Covert gathering
- Foot printing
- Identifying Protection Mechanisms

Threat Modeling

- What is it?
- Business asset analysis
- Business process analysis
- Threat agents / threat communities analysis
- Threat capability analysis
- Comparable targets

Vulnerability Analysis

- What is it?
- Testing
- Active
- Passive
- Validation
- Research

Exploitation

- What is it?
- Countermeasures
- Evasion
- Precision Strike
- Customized Exploitation
- Pivoting
- Escalation
- Objectives

Post Exploitation

- We have success, what now?
- Rules of Engagement
- Persistence
- Infrastructure Analysis
- Pillaging
- Exfiltration
- Cleanup

Reporting

- Last but not least, arguably the most important step, the deliverable the client is paying for
- Notes, notes, more notes, also did I mention take notes
- Screenshots are great proof too

Preparing Your Pentesting Platform

- Home lab & setup, if you want
- Student lab environment
  - Windows VM
  - Kali Linux VM
- Tools used in this course:
  - Kali Linux
    - Nmap
    - Wireshark
    - Maltego
    - Ettercap
    - OWASP ZAP
    - Standard Unix/Linux utils:
      - Nslookup
      - Whois
      - Netstat
      - Bash Primer: http://linuxcommand.org/lc3_learning_the_shell.php
  - VMWare vSphere via Web Browser