# Offensive Computer Security: Summary 1

David De Lille

February 20, 2015

## 1 Risk

Risk = Threat x Vulnerability

> "Risk is a function of the likelihood of a given thread-source's exercising a particular potential vulnerability, and the resulting impact of that adverse event on the organisation."

Threat: consequences of bad thing happening
Vulnerability: probability of bad thing happening

## 2 Hacking versus Penetration testing

The difference is: permission. Penetration testing without permission is illegal.

## 3 History of Disclosure

### 3.0 No disclosure [1950-1988]

### 3.1 Mailing lists [1988-1993]

Security is only discussed on invite-only mailing lists. Security researchers seen as evil, and vendors don't care. Mailing lists were easily leaked. Everything is buy-at-your-own-risk.

### 3.2 Full Disclosure [1993-2002]

This was a (controversial) reaction to vendors being unwilling to solve security problems, in order to force them to act. Researchers would disclose security problems to everyone (good and bad). The result was a constant a race between exploiters and patchers. This is still a problem for start-ups that don't have the resources for specialized security personnel. It didn't reduce the amount of attacks.

### 3.3 Responsible Disclosure [2002-2010]

Process submitted to IETF. Similar to Full Disclosure, but researchers should wait to release info until the vendor can patch the problem. The problem was that this places the responsibility to fix the problem on the researcher, rather than the vendor.

### 3.4 Coordinated Vulnerability Disclosure [2010-present]

Vendors promise not to sue researchers, and accept responsibility for the problems. Vendorsec mailing lists were attempted, but were again broken/leaked.
Delayed disclosure = give vendor a certain amount of time to patch before doing full disclosure. Abused by researchers at conferences to gain glory.
Bug bounties are programs offered by certain companies that grant cash rewards for discovering bugs.

## 4 Penetration testing cycle


(Note: cycle can restarted at any point.)

## 4.0 Prior

Discuss the details of the engagement with the client:

- what: which targets, what is off limits, what kind of threat model (e.g. insider threat, ex-employee), BYOD?
- how: physical access?, social engineering?, covert/overt?
- when: timeline of the pentest
- report: what kind of report are they expecting?

## 4.1 Reconnaissance

Gathering intelligence on the target(s). Two types of intel: OSINT and HUMINT.

OSINT (open source intelligence):

- search engines: URLs, filetypes, devices (http://www.shodanhq.com/)
- company website
- public records
- social media
- way-back-machine

HUMINT (human intelligence):

- phone
- physical access

## 4.2 Scanning and Enumeration

The goal is to identify the **attack surface**, by scanning ways to get in and finding new ways. Jump back to Reconnaissance step if needed. Finally, find vulnerabilities in the attack surface.

## 4.3 Gain access

Exploit vulnerabilities to break in:

- Social Engineering (easiest way by far)
- web app exploitation
- pivoting from 3rd party
- network app exploitation
- malicious USB
- etc

### 4.4 Privilege Escalation

Increase capabilities by:

- password cracking
- SUID exploits
- sandbox escape
- keylogging
- social engineering
- etc

### 4.5 Maintain access and Post Exploitation

Complete the actual goal of attack, which can include:

- going after money/data/users/intellectual property
- installing a backdoor
- expanding control (e.g. passwords, pivoting to 3rd party)
- erasing logs

## 5 Threat models

- Attacker centric: what are his goals and how can he achieve them
- Software centric: design review (step through and evaluate each part)
- Asset centric: start from pot o' gold

## 6 Categories of Threats

- Advanced Persistent Threat (APT): most powerful hackers (potentially state-funded)
- Hacktivism: LulzSec, Anonymous, etc.
- Commodity threats: as capable as hactivists, but fewer in numbers

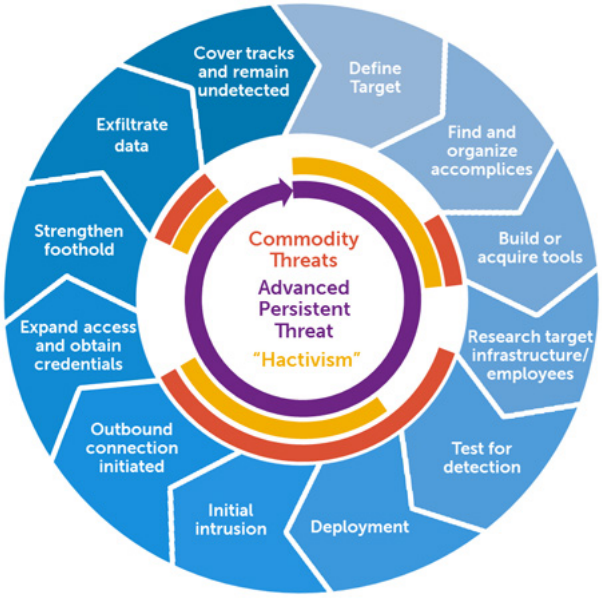


Figure 1: Attacker life cycle

# 7 Attacker goals

What are the bad guys after:

- money/data/users/intellectual property
- critical infrastructure
- enemies/political dissidents
- credit cards/financial data
- password (hashes)
- sabotage
- pivoting to 3rd party
- long term backdoors
- 4 teh lulz

## 8 Asymmetric advantage attacker

Attackers only need to find one hole; defenders need to stop everything.

Bad guys also have distinct advantages over pentesters:

- can be completely anonymous (proxy, spoofing)
- attack BYOD/significant other
- attack partners
- blackmail, $5 wrench
- widely available crime kits
- can break laws

## 9 Other Notes

- Physical access = game over
- Its important to know how to communicate security