IS2545, LECTURE 19: Penetration Testing

Bill Laboon

Remember that security testing is different…

- It is different from other kinds of testing in that you have an actual, thinking adversary.
- Oftentimes, the best way to prevent these adversaries from compromising your systems is to have you or someone else attempt to compromise it first (and report back an assessment).

Penetration Test

- An attack on a computer system looking for security weaknesses, from the perspective of a malicious adversary (“black hat”)
- aka “pen test”

Terminology: Black Hat, White Hat, Grey Hat

- **Black Hat** – Someone who attacks a computer system for personal gain or “the lolz” (the joy of mischief)
- **White Hat** – Someone who tests the security systems on an authorized basis (aka red team, tiger team)
- **Grey Hat** – Someone who violates laws or standards, but is otherwise a white hat hacker

Real World Example

- You are hired to try to gain access to the 40th floor of the Cathedral of Learning.
- What could you try?

Remember the People Element

- *"Users are a vulnerability that can never be patched.“*
  -Georgia Weidman
- *"People are prone to taking mental shortcuts. They may know that they shouldn't give out certain information, but the fear of not being nice, the fear of appearing ignorant, the fear of a perceived authority figure - all these are triggers, which can be used by a social engineer to convince a person to override established security procedures."*
  -Kevin Mitnick
- The weakest element is often the human element.

Technical and Social Aspects

- There are lots of possible technical vulnerabilities, as well, which *can* be fixed – but often are not.
- Technical vulnerabilities can often be done much more quickly, and may allow more chances of success on an absolute basis.

Pen Testing Is Big Business!

- Penetration ("pen") testing and security research has become much more mainstream in recent years.
- Bug bounties (https://www.facebook.com/BugBounty)
- Pwn2own
- zero-day markets
- Companies, e.g. Bulb Security, Offensive Security
- State actors (e.g. Stuxnet, Equation Group)
- Conferences (Black Hat, DefCon)

Penetration Testing Framework

- Pre-engagement Interactions
- Intelligence Gathering
- Threat Modeling
- Vulnerability Analysis
- Exploitation
- Post Exploitation
- Reporting

Pre-Engagement Interactions

- Discuss with stakeholders
- Determine what is in- and out-of-bounds
- Determine scope
- Determine reporting standards
- Determine schedule
- Get everything in writing!

Information Gathering

- Uncover information (OSINT - open-source intelligence) on target
- There is often more out there than you think!
- What are some places you might find OSINT on me?

Threat Modeling

- Determine what assets exist and what their value would be to an attacker
- What aspects of the InfoSec triad would be deleterious if violated?
  - *Confidentiality*
  - *Integrity*
  - *Availability*

Vulnerability Analysis

- Determine vulnerabilities that may exist on target systems
- Can be done with automated tools (e.g. nmap, metasploit, WireShark) or manually
- Possible Vulnerabilities: buffer overflows, SQL injection, XSS, etc. as discussed in last lecture

Exploitation

- Exploit vulnerabilities found in previous stage
- The first "action" phase
- Example:
  - You find out that a Windows domain server is running unpatched software which you know contains a privilege escalation bug (vulnerability analysis phase).
  - You write some software which takes advantage of this vulnerability and run it, giving you admin access (exploitation phase).

Post-Exploitation

- Once access is achieved, determine what information/damage can be done.
- Example: with admin access on domain server, I now have access to all other machines on that domain, including payroll and CRM servers.

Reporting

- Informing the stakeholders of the target what vulnerabilities exist, how they can be exploited, and the damage that can be caused when they are exploited.

Remember

- The goal is not exploitation for exploitation's sake.
- The goal is to:
  - determine what business value would be lost if an actual adversary was able to do the things that you have done.
  - determine ways to prevent this from happening by actual adversaries.