Testing Framework and Penetration Testing

Instructor: C. Pu (Ph.D., Assistant Professor)

Lecture 02

puc@marshall.edu

Overview

- A typical testing framework for an organization.

- It can be seen as a *reference framework* that comprises techniques and tasks that are appropriate at various phases of the software development life cycle (SDLC).

- Companies and project teams can use this model to develop their own testing framework and to scope testing services from vendors.

- This framework should not be seen as prescriptive, but as a flexible approach that can be extended and molded to fit an organization's development process and culture.

Overview

- It is critical to understand why building an end-to-end testing framework is crucial to assessing and improving software security.

- In Writing Secure Code Howard and LeBlanc note that issuing a security bulletin costs Microsoft at least $100,000, and it costs their customers collectively far more than that to implement the security patches.

- They also note that the US government's CyberCrime web site (http://www.justice.gov/criminal/cybercrime/) details recent criminal cases and the loss to organizations.
  - Typical losses far exceed USD $100,000.

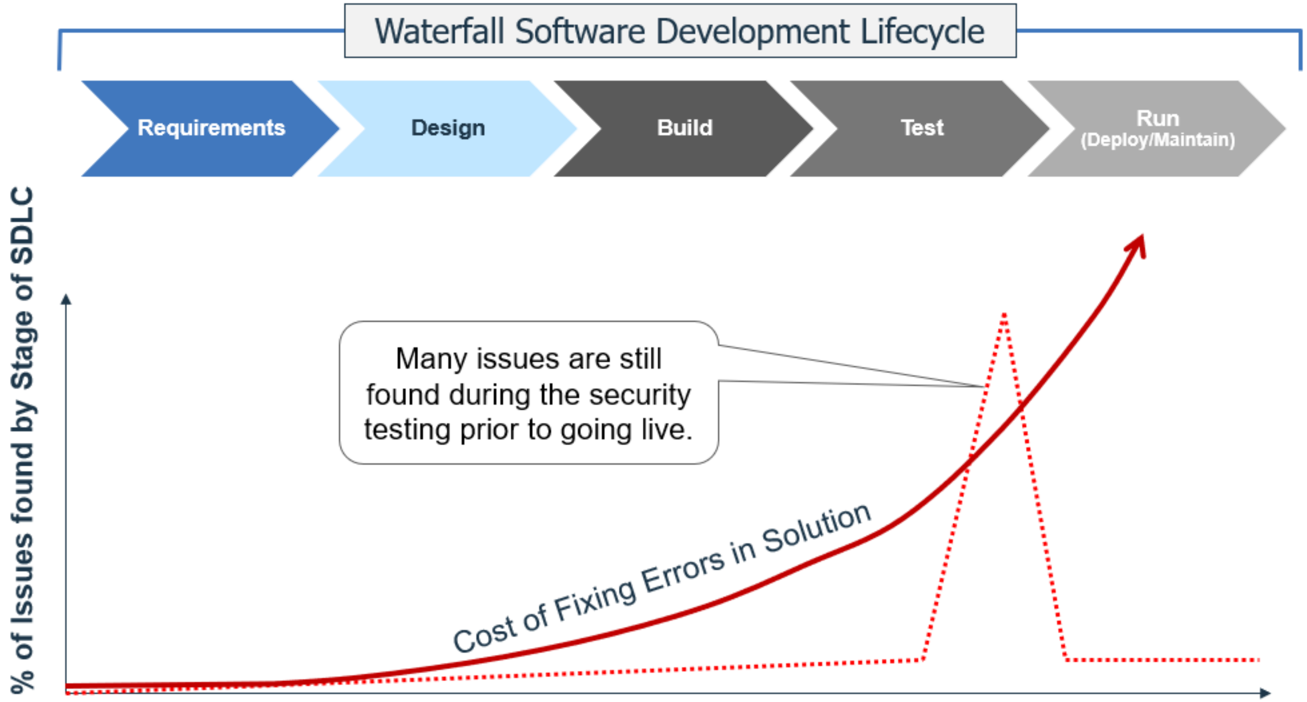
Overview

- With economics like this, it is little wonder why software vendors move from solely performing black box security testing, which can only be performed on applications that have already been developed, to concentrate on testing in the early cycles of application development such as definition, design, and development.

Overview

- Many security practitioners still see security testing in the realm of penetration testing.
- As discussed before, while penetration testing has a role to play, it is generally inefficient at finding bugs and relies excessively on the skill of the tester.
- It should only be considered as an implementation technique, or to raise awareness of production issues.
- To improve the security of applications, the security quality of the software must be improved.
- That means testing the security at the *definition*, *design*, *develop*, *deploy*, and *maintenance* stages, and not relying on the costly strategy of waiting until code is completely built.

Overview



Many issues are still found during the security testing prior to going live.

Overview

- The testing framework consists of the following activities that should take place:
  - Before development begins
  - During definition and design
  - During development
  - During deployment
  - Maintenance and operations

Defining Penetration Testing

- Being a pentester has become more important in today's world as organizations have had to take a more serious look at their security posture and how to improve it.

- Several high-profile incidents such as the ones involving retail giant Target and entertainment giant Sony have drawn attention to the need for better trained and more skilled security professionals who understand the weaknesses in systems and how to locate them.

Defining Penetration Testing

- Through a program that combines ***technological***, ***administrative***, and ***physical measures***, many organizations have learned to fend off their vulnerabilities.
  - ***Technology controls*** such as virtual private networks (VPNs), cryptographic protocols, intrusion detection systems (IDSs), intrusion prevention systems (IPSs), access control lists (ACLs), biometrics, smart cards, and other devices have helped security.
  - ***Administrative controls*** such as policies, procedures, and other rules have also been strengthened and implemented over the past decade.
  - ***Physical controls*** include devices such as cable locks, device locks, alarm systems, and other similar devices.

Defining Penetration Testing

- A penetration tester, or pentester, is employed by an organization either as an internal employee or as an external entity such as a contractor hired on a per-job or per-project basis.
- In either case, pentesters conduct a penetration test, meaning they survey, assess, and test the security of a given organization by using the same techniques, tactics, and tools that a malicious hacker would use.
  - The main differences between a malicious hacker and a pentester are *intent* and the *permission* that they get, both legal and otherwise, from the owner of the system that will be evaluated.
  - Additionally, pentesters are *never to reveal the results of a test* to anyone except those designated by the client.

Defining Penetration Testing

- As a safeguard for both parties, a ***nondisclosure agreement*** (***NDA***) is usually signed by both the hiring firm and the pentester.

- This protects company property and allows the pentester access to internal resources.

- Finally, the pentester works under contract for a company, and the contract specifies what is off-limits and what the pentester is expected to deliver at the end of the test.

- All of the contractual details depend on the specific needs of a given organization.

Defining Penetration Testing

- Some other commonly encountered terms for pentester are penetration tester, ethical hacker, and white-hat hacker.
- All three terms are correct and describe the same type of individual (though some may debate these apparent similarities in some cases).
- Typically the most commonly used name is pentester.
- EC-Council uses ethical hacker when referencing its own credential, the Certified Ethical Hacker.

Recognizing Your Opponents

- Script Kiddies
  - These hackers have limited or no training and know how to use basic tools or techniques.
  - They may not even understand any or all of what they are doing.

- White-Hat Hackers
  - These hackers think like the attacking party but work for the good guys.
  - They typically are characterized by having what is commonly considered to be a code of ethics that says they will cause no harm.
  - This group is also known as pentesters.

Recognizing Your Opponents

- Gray-Hat Hackers
  - These hackers straddle the line between the good and bad sides and have decided to reform and become the good side.
  - Once they are reformed, they may not be fully trusted, however.
  - Additionally, in the modern era of security these types of individuals also find and exploit vulnerabilities and provide their results to the vendor either for free or for some form of payment.

Recognizing Your Opponents

- Black-Hat Hackers
  - These hackers are the bad guys who operate on the wrong side of the law.
  - They may have an agenda or no agenda at all.
  - In most cases, black-hat hackers and outright criminal activity are not too far removed from one another.
- Cyberterrorists
  - Cyberterrorists are a new form of attacker that tries to knock out a target without regard to being stealthy.
  - The attacker essentially is not worried about getting caught or doing prison time to prove a point.

Confidentiality, Integrity, and Availability

- Any organization that is security minded is trying to maintain the CIA triad— or the core principles of ***confidentiality***, ***integrity***, and ***availability***.
- The following list describes the core concepts.
- You should keep these concepts in mind when performing the tasks and responsibilities of a pentester.

Confidentiality, Integrity, and Availability

- ***Confidentiality***
  - This refers to the safeguarding of information, keeping it away from those not otherwise authorized to possess it.
  - Examples of controls that preserve confidentiality are permissions and encryption.
- ***Integrity***
  - This deals with keeping information in a format that retains its original purposes, meaning that the data the receiver opens is the same the creator intended.
- ***Availability***
  - This deals with keeping information and resources available to those who need to use it.
  - Simply put, information or resources, no matter how safe, are not useful unless they are ready and available when called upon.

Confidentiality, Integrity, and Availability

- Anti-CIA
  - Improper Disclosure
    - This is the inadvertent, accidental, or malicious revealing or accessing of information or resources to an outside party.
    - Simply put, if you are not someone who is supposed to have access to an object, you should never have access to it.

Confidentiality, Integrity, and Availability

- Anti-CIA
  - Unauthorized Alteration
    - This is the counter to integrity as it deals with the unauthorized or other forms of modifying information.
    - This modification can be corruption, accidental access, or malicious in nature.

Confidentiality, Integrity, and Availability

- Anti-CIA
  - Disruption (aka Loss)
    - This means that access to information or resources has been lost when it otherwise should not have.
    - Essentially, information is useless if it is not there when it is needed.
    - While information or other resources can never be 100 percent available, some organizations spend the time and money to get 99.999 percent uptime, which averages about six minutes of downtime per year.

Broad Categories of Cybercrime

- Identity Theft
  - This is the stealing of information that would allow someone to assume the identity of another party for illegal purposes.
  - Typically this type of activity is done for financial gains such as opening credit card or bank accounts or in extreme cases to commit other crimes such as obtaining rental properties or other services.

Broad Categories of Cybercrime

- Theft of Service
  - Examples are the use of phone, Internet, or similar items without expressed or implied permission.
  - Examples of crimes or acts that fall under this category would be acts such as stealing passwords and exploiting vulnerabilities in a system.
  - Interestingly enough, in some situations just the theft of items such as passwords is enough to have committed a crime of this sort.
  - In some states, sharing an account on services such as Netflix with friends and family members can be considered theft of service and can be prosecuted.

Broad Categories of Cybercrime

- Network Intrusions or Unauthorized Access
  - This is one of the oldest and more common types of attacks.
  - It is not unheard of for this type of attack to lead into other attacks such as identity theft, theft of service, or any one of a countless other possibilities.
  - In theory, any access to a network that one has not been granted access to is enough to be considered a network intrusion; this would include using a Wi-Fi network or even logging into a guest account without permission.

Broad Categories of Cybercrime

- Posting and/or Transmitting Illegal Material
  - This has gotten to be a difficult problem to solve and deal with over the last decade.
  - Material that is considered illegal to distribute includes copyrighted materials, pirated software, and child pornography, to name a few.
  - The accessibility of technologies such as encryption, file sharing services, and ways to keep oneself anonymous has made these activities hard to stop.

Broad Categories of Cybercrime

- Fraud
  - This is the deception of another party or parties to illicit information or access typically for financial gain or to cause damage.

Broad Categories of Cybercrime

- Embezzlement
  - This is one form of financial fraud that involves theft or redirection of funds as a result of violating a position of trust.
  - The task has been made easier through the use of modern technology.

Broad Categories of Cybercrime

- Dumpster Diving
  - This is the oldest and simplest way to get and gather material that has been discarded or left in unsecured or unguarded receptacles.
  - Often, discarded data can be pieced together to reconstruct sensitive information.
  - While going through trash itself is not illegal, going through trash on private property is and could be prosecuted under trespassing laws as well as other portions of the law.

Broad Categories of Cybercrime

- Writing Malicious Code
  - This refers to items such as viruses, worms, spyware, adware, rootkits, and other types of malware.
  - Essentially this crime covers a type of software deliberately written to wreak havoc and destruction or disruption.

Broad Categories of Cybercrime

- Unauthorized Destruction or Alteration of Information
  - This covers the modifying, destroying, or tampering with information without appropriate permission.

Broad Categories of Cybercrime

- Denial-of-Service (DoS) and Distributed Denial-of-Service (DDoS) Attacks
  - These are both ways to overload a system's resources so it cannot provide the required services to legitimate users.
  - While the goals are the same, the terms DoS and DDoS actually describe two different forms of the attack.
  - DoS attacks are small scale, one-on-one attacks, whereas DDoS attacks are much larger in scale, with thousands of systems attacking a target.

Broad Categories of Cybercrime

- Cyberstalking
  - This is a relatively new crime on this list.
  - The attacker in this type of crime uses online resources and other means to gather information about an individual and uses this to track the person and, in some cases, try to meet these individuals in real life.
  - While some states, such as California, have put laws in place against stalking, which also cover crimes of the cyber variety, they are far from being universal.
  - In many cases, when the stalker crosses state lines during the commission of their crime, it becomes a question of which state or jurisdiction can prosecute.

Broad Categories of Cybercrime

- Cyberbullying
  - This is much like cyberstalking except in this activity individuals use technologies such as social media and other techniques to harass a victim.
  - While this type of crime may not seem like a big deal, it has been known to cause some individuals to commit suicide as a result of being bullied.

Broad Categories of Cybercrime

- Cyberterrorism
  - This, unfortunately, is a reality in today's world as hostile parties have realized that conventional warfare does not give them the same power as waging a battle in cyberspace.
  - It is worth nothing that a perpetrator conducting terrorism through cyberspace runs the very real risk that they can and will be expedited to the targeted country.

Broad Categories of Cybercrime

- To help understand the nature of cybercrime, it is first important to understand the three core forces that must be present for a crime, any crime, to be committed.

- These three items are:
  - Means or the ability to carry out their goals or aims, which in essence means that they have the skills and abilities needed to complete the job
  - Motive or the reason to be pursuing the given goal
  - Opportunity, the opening or weakness needed to carry out the threat at a given time