Security Assessments and Penetration Testing

CS-3113: PRINCIPLES OF CYBER SECURITY

BENJAMIN R. ANDERSON

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

Security Tests*: Verify that a control is functioning properly. These tests include automated scans, tool-assisted penetration tests, and manual attempts to undermine security.*

- *Should take place on a regular schedule, with attention paid to each of the key security controls protecting an organization.*

Security Assessments*: Comprehensive reviews of the security of a system, application, or other tested environment.*

- *Security assessments normally include the use of security testing tools but go beyond automated scanning and manual penetration tests.*
- *They also include a thoughtful review of the threat environment, current and future risks, and the value of the targeted environment.*

Security Audits*: Use many of the same techniques followed during security assessments but must be performed by independent auditors.*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

***Risk**: The possibility or likelihood [probability] that a threat will exploit a vulnerability to cause harm to an asset and the severity of damage that could result.*

- *The more likely it is that a threat event will occur, the greater the risk.*
- *The greater the amount of harm that could result if a threat is realized, the greater the risk.*
- `risk = threat * vulnerability`
- `risk = probability of harm * severity of harm`

When a risk is realized, a threat agent, threat actor, or threat event has taken advantage of a vulnerability and caused harm to or disclosure of one or more assets.

***Asset**: Anything used in a business process or task. If an organization relies on a person, place, or thing, whether tangible [*ex. People, trade secret, proprietary information, property*] or intangible [*ex. Public goodwill, reputation*], then it is an asset*

Definitions

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

Safeguards: *A safeguard, security control, protection mechanism, or countermeasure is anything that removes or reduces a vulnerability or protects against one or more specific threats.*

- *Also known as* ***Risk Response***

Attack: *The intentional attempted exploitation of a vulnerability by a threat agent to cause damage, loss, or disclose of assets.*

Breach: *A breach, intrusion, or penetration is the occurrence of a security mechanism being bypassed or thwarted by a threat agent. A breach is a successful attack.*

Risk Management*: A detailed process of identifying factors that could damage or disclose assets, evaluating those factors in light of asset value and countermeasure cost, and implementing cost-effective solutions for mitigating or reducing risk.*

Managing Risk

From: *An Introduction to Information System Risk Management*, Steve Elky, SANS, 2006:

- https://www.sans.org/white-papers/1204/
- *It is vital to manage risks to systems. Understanding risk, and in particular, understanding the specific risks to a system allow the system owner to protect the information system commensurate with its value to the organization. The fact is that all organizations have limited resources and risk can never be reduced to zero. So, understanding risk, especially the magnitude of the risk, allows organizations to prioritize scarce resources.*
- *Quantitative risk assessment draws upon methodologies used by financial institutions and insurance companies. By assigning values to information, systems, business processes, recovery costs, etc., impact, and therefore risk, can be measured in terms of direct and indirect costs.*
- *The results of qualitative risk assessments are inherently more difficult to concisely communicate to management. Qualitative risk assessments typically give risk results of "High", "Moderate" and "Low".*

Managing Risk

Watch: *Risk Assessment – CompTIA Security+ SsY0-501 – 5.3* by Professor Messer

- https://www.youtube.com/watch?v=WanKqjP0pfA

Pay attention to how risk is evaluated, qualitative risk assessment, quantitative risk analysis

Also: How to calculate Annualize Loss Expectancy (ALE):

- ALE = Single Loss Expectancy (SLE) * Annualized Rate of Occurrence (ARO)
- `ALE = SLE * ARO`
- We also have ALE = Asset Value (AV) * Exposure Factor (EF) * ARO
- `ALE = AV * EF * ARO`
- For example, imagine a flood will do $2 million in damage to a building, and that is expected every 50 years, we have:
  - `ALE = $2 million * 0.02 = $40,000`
- Or, if it is expected that a lightning strike will burn out half of the 50 workstations in a facility ($100k in workstations) because there are 2 separate circuits, and a lightning strike is expected once every 20 years, we have:
  - `ALE = $100k (AV) * 50% (EF) * 0.05 (ARO) = $2,500`

Managing Risk

Once a risk is identified, it needs to have a response

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

***Risk Mitigation (Reducing Risk)**: the implementation of safeguards, security controls, and countermeasures to reduce and/or eliminate vulnerabilities or block threats.*

- *Ex: Deploying firewalls*

***Risk Assignment (Transferring Risk)**: The placement of the responsibility of loss due to a risk onto another entity or organization.*

- *Ex: Purchasing insurance*

***Risk Deterrence**: The process of implementing deterrents to would-be violators of security and policy. The goal is to convince a threat agent not to attack.*

- *Ex: Implementing auditing, adding security cameras, etc.*

Managing Risk

Once a risk is identified, it needs to have a response (Cont’d)

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

Risk Avoidance*: The process of selecting alternate options or activities that have less associated risk than the default, common, expedient, or cheap option.*

- *Ex: Locate a business in Arizona instead of Florida to avoid hurricanes.*

Risk Acceptance*: The result after a cost/benefit analysis shows countermeasure costs would outweigh the possible cost of loss due to a risk.*

- [Ex: Accepting a certain amount of risk for driving a car]

Risk Rejection*: An unacceptable possible response to risk is to reject risk or ignore risk.*

- *Rejecting or ignoring risk may be considered negligence in court.*

Risk Analysis: Qualitative

Qualitative assessments are usually based on scenarios and not concrete values like the cost to replace a facility, system, intellectual property, or other asset

Note: It isn't always possible to have a quantitative assessment since some things can't be precisely calculated

- For example, what is the cost in public goodwill for losing 50,000 customer records? Or, the cost to a law firm's reputation of having their emails made public?

To handle these situations, a "scenario-based assessment" is often used

- This is where scenarios are given to a group of assessors and the threats are put on a relative scale like HIGH, MODERATE, LOW
- Ex: What is the threat from having our emails released?
- These scenarios are then evaluated using brainstorming, surveys, feedback from subject matter experts, etc.

Note: You will see the weaknesses in the sample report provided in the course project uses High, Moderate, and Low

Risk Analysis: Quantitative

From the *Certified Information Systems Security Professional Official Study Guide, Ninth Edition* by Chapple, Stewart, and Gibson (OSG):

The major steps or phases in quantitative risk analysis are as follows:

1. *Inventory assets, and assign a value (asset value [AV])*
2. *Research each asset, and produce a list of all possible threats to each individual asset. This results in asset-threat pairings.*
3. *For each asset-threat pairing, calculate the exposure factor (EF).*
4. *Calculate the single loss expectancy (SLE) for each asset-threat pairing.*
5. *Perform a threat analysis to calculate the likelihood of each threat being realized within a single year – that is, the annualized rate of occurrence (ARO).*
6. *Derive the overall loss potential for each threat by calculating the annualized loss expectancy (ALE)*
7. *Research countermeasures for each threat, and then calculate the changes to ARO, EF, ALE based on an applied countermeasure.*
8. *Perform a cost/benefit analysis of each countermeasure for each threat for each asset. Select the most appropriate response to each threat.*

Criticality Analysis

One item that may not be captured in the quantitative risk analysis is the criticality of an asset

- This is done in Phase 1: Inventory assets, and assign a value (asset value [AV])

An asset may not be that expensive, but it is critical for business operations

- ***Mission Related***: A workstation that controls your company's production line is more critical than a workstation used for updating social media
  - Both may have the same SLE, but one is more important

To do a criticality analysis:

- Understand which assets are critical
- Describe the asset
  - Location, type, etc.
- Rank the systems in some way
  - This can be numerical – most important, second most important, etc.
  - Relative:
    - No business without these assets; Greatly reduced without these assets
    - Business can continue for 0 hours without Asset A; for 24 hours without Asset B; until payroll end date without Asset C

Business Continuity Plan

Read: *Understanding security risk management: Criticality categories* by Susan Snedaker

- https://www.techtarget.com/searchitchannel/feature/Understanding-security-risk-management-Criticality-categories

From the article:

- *You can develop any category system that works for you but as with all rating systems, be sure the categories are clearly defined and that there is a shared understanding of the proper use and scope of each. Here is one commonly used rating system for assessing criticality:*
  - *Category 1: Critical Functions—Mission-Critical*
  - *Category 2: Essential Functions—Vital*
  - *Category 3: Necessary Functions—Important*
  - *Category 4: Desirable Functions—Minor*
- *Obviously, your business continuity plan will focus the most time and resources on analyzing the critical functions first, essential functions second. It's possible you will delay dealing with necessary and desirable functions until later stages of your business recovery. Many companies identify these four areas and set timelines for when each of these categories will be functional following a business disruption. Let's look at each category in more detail. You can use these category descriptions as-is or you can tweak them to meet your company's unique needs.*

Risk Assessment

Read/View: Risk Assessment Presentation by mmagario

- Slides 1-20
- https://www.slideshare.net/mmagario/risk-assessment-presentation-24896874

Key items from the Presentation:

- Threats can involve threat actors (people) but not everything that can affect an asset is a threat actor
  - Ex: Tornado or earthquake

Hazard

- *Natural*
- *Manmade*
- *Unintentional*
- *Safety*
- *Security*
- *Disasters*
- *Political/Military*
- *Environmental or Behavioral*

Threat

- *Manmade*
- *Intentional*
- *With Malice*
- *Terrorists*
- *Petty or Economic Criminals*
- *Subversives*

From: Risk Assessment Presentation by mmagario, https://www.slideshare.net/mmagario/risk-assessment-presentation-24896874

Risk Assessment

Consequence Analysis:

- How to determine the consequences from a hazard or successful threat to your system?
- This allows you to identify the various consequences should there be an event or breach that affects your organization

Consequence Analysis

- *Losses*
  - *Human Life*
  - *Property*
  - *Proprietary Information*
  - *Reputation*
- *Impact*
  - *Environmental*
  - *Economical*

From: Risk Assessment Presentation by mmagario, https://www.slideshare.net/mmagario/risk-assessment-presentation-24896874

Risk Assessment

Vulnerability Analysis

- The presentation provided 3 steps in this analysis
- Other methods contain up to 10 steps
- Can be modified for different industries, security needs, and situations

Vulnerability Analysis:

- *3 Distinct Steps*
  - *Define*
  - *Evaluate*
  - *Identify*

Define:

- What is the asset?

Evaluate:

- How is it used?
- What is the scope of the system?
- What are the components and dependencies?

Identify:

- What are the known security gaps or problems that currently exist with the system and/or its environment?

From: Risk Assessment Presentation by mmagario, https://www.slideshare.net/mmagario/risk-assessment-presentation-24896874

Risk Assessment

Probability Assessment:

- What is the probability of:
  - Your personal information being compromised in the next year?
  - Being affected by ransomware this month?
- These are hard questions, without solid answers
- Often, these numbers change with a new vulnerability
- People often disagree on the probability of an event happening

Probability Assessment:

- *View point dependent*
- *Based on attractiveness*
- *Historic Data*
- *Statistics*

Notes:

- The number a person assigns to a probability is highly dependent on their viewpoint and their background
- The probability a vulnerability will be exploited could easily vary depending on what information is processed on the system
  - For example, a financial system is a high-value target
  - Accurate historical data and statistical values may not exist or have large gaps
  - Data is becoming a bit better as insurance companies are analyzing information for providing cyber insurance

From: Risk Assessment Presentation by mmagario, https://www.slideshare.net/mmagario/risk-assessment-presentation-24896874

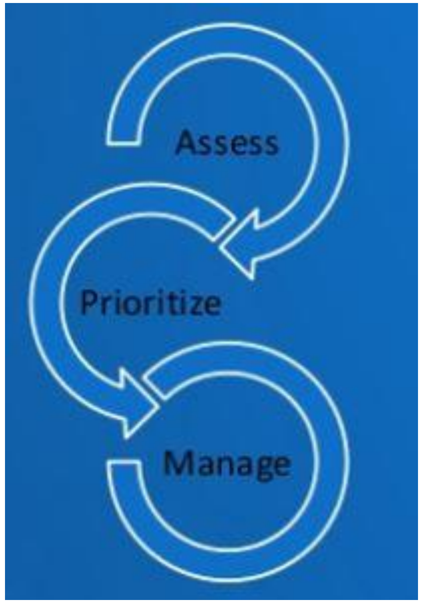
Risk Assessment

Quantitative risk analysis is much easier to manage

- However, a number is only as good as the input values

Risk:

- *Assessment*
- *Prioritization*
- *Management*



From: Risk Assessment Presentation by mmagario, https://www.slideshare.net/mmagario/risk-assessment-presentation-24896874

Risk Assessment

Mitigations:

- This is how you address the different risks
- Basically, how are the risks minimized (while also being cost effective)

Countermeasures:

- *Mitigation Opportunities*
  - *Safety*
  - *Security*
  - *Enforcement*
  - *Costs*
- ***Notes***:
  - Safety is usually the highest priority for mitigating risks
  - We can develop policies that address security risks – for example, require a two-person rule where no single person is allowed to perform an operation.
  - An organization also has to ensure the policies and mitigation strategies are used!
  - With finite resources, mitigations must be prioritized to those the biggest benefit – within time/budget constraints

From: Risk Assessment Presentation by mmagario, https://www.slideshare.net/mmagario/risk-assessment-presentation-24896874

Ethical Hacking

Read: Explore The 5 Phases of Ethical Hacking by Shivam Arora:

- https://www.simplilearn.com/phases-of-ethical-hacking-article
- You are responsible for knowing the 5 phases (reconnaissance, scanning, gain access, maintain access, cover tracks) and their descriptions

Penetration Testing

There are a lot of different definitions of Penetration Testing or Pentesting

Read: *What is penetration testing?* From Cloudflare

- https://www.cloudflare.com/learning/security/glossary/what-is-penetration-testing/
- Their definition:
  - *Penetration testing (or pen testing) is a security exercise where a cyber-security expert attempts to find and exploit vulnerabilities in a computer system. The purpose of this simulated attack is to identify any weak spots in a system's defenses which attackers could take advantage of.*
- You are responsible for being able to identify the definition, and the types of pen tests (open-box, closed-box, covert, external, internal)

Penetration Testing

Red Teaming is a set of activities that can include penetration testing

- Sandia National Laboratories identifies 8 types of red teaming – one of which is penetration testing

Read/Watch: *RT4PM*, Sandia National Laboratories

- https://casa.sandia.gov/rt4pm/
- *Red Teaming Quick Reference Sheet*, Sandia National Laboratories
- https://www.sandia.gov/app/uploads/sites/87/2021/08/2017-09-13_RT4PM_QRS_SAN2017-9535-TR.pdf
- The video and the quick reference sheet (QRS) will give you an idea of how pentesting fits into the overall system lifecycle, and what security needs it can meet
- The QRS also contains information on Penetration Testing, including a definition, considerations, deliverables, cost factors, and where it best fits in the overall system lifecycle

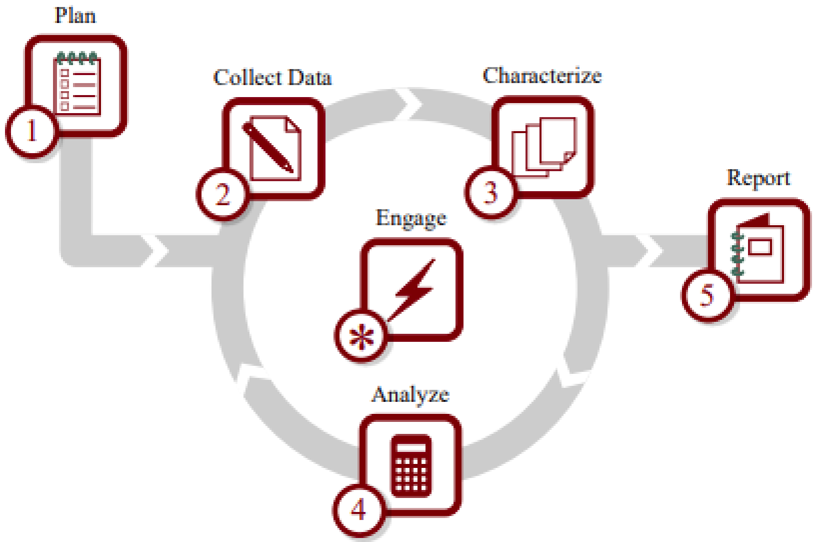
Penetration Testing

Read: *IDART™ Quick Reference Sheet*, Sandia National Laboratories

- ***Remember***: Pentesting is one of the kinds of red teaming you can do
- https://www.sandia.gov/app/uploads/sites/87/2021/08/2017-09-13_IDART_QRS_SAND2017-9579-TR.pdf
- You are responsible for knowing the phases of the assessment and the objective of each phase
  - Also pay special attention to the note about creating a Rules of Engagement

Note: I was a team lead for IDART (renamed CASA) for over 10 years

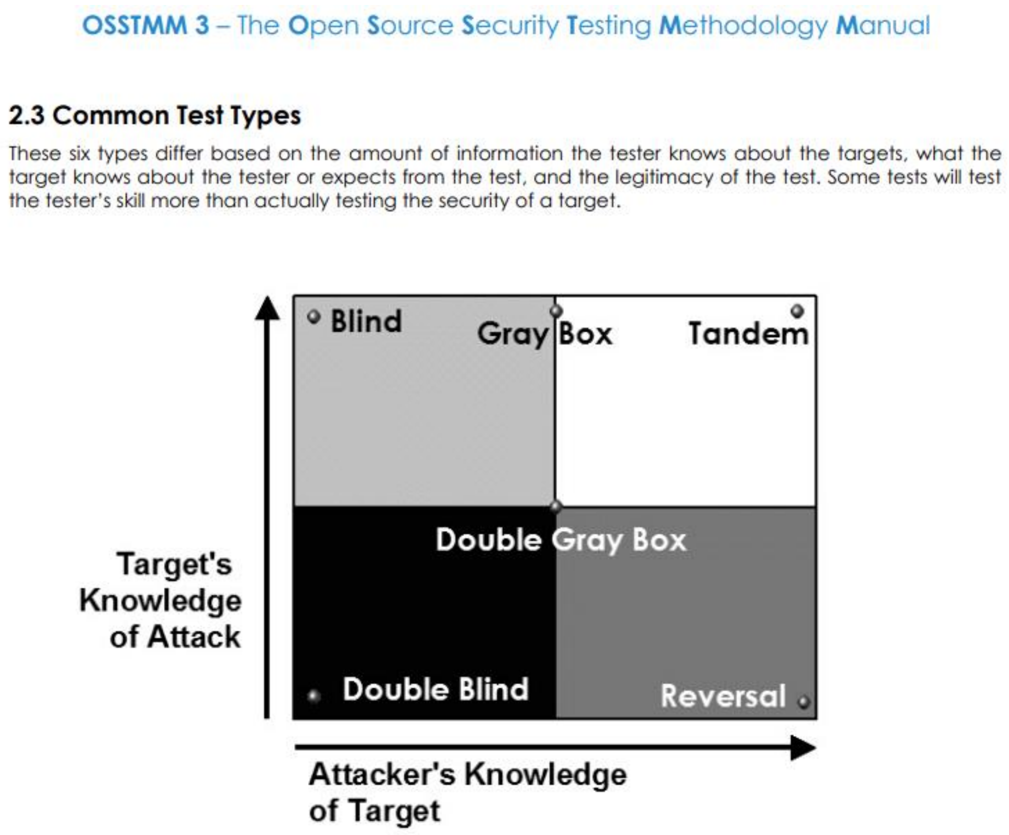
- If you have questions about it, let me know!



Types of Security Testing

Some types of security testing:

- Network scanning
- Vulnerability scanning
- Internal audits
- Wireless surveys (wardriving)
- Penetration testing
- Red teaming
- Phishing



OSSTMM 3 – The Open Source Security Testing Methodology Manual

2.3 Common Test Types

These six types differ based on the amount of information the tester knows about the targets, what the target knows about the tester or expects from the test, and the legitimacy of the test. Some tests will test the tester's skill more than actually testing the security of a target.

Blind
Gray Box
Tandem
Double Gray Box
Double Blind
Reversal
Target's Knowledge of Attack
Attacker's Knowledge of Target

Image from: OSSTMM 3, https://www.isecom.org/OSSTMM.3.pdf

Types of Penetration Tests

Some ways of differentiating tests is how much information the attacker has

- Black Box: No knowledge
- Gray Box: Some knowledge
- White Box: Full knowledge

In red teaming, there is the concept of "cooperation"

- If the administrators or users of a target system are actively helping the red team, it can save a lot of time and effort – which means it is less expensive
- May not give an accurate rating for what an attacker could actually do – but it does help discover what they could *possibly* do

There is also the idea of an external vs. internal test

- This is simply where the pentest team starts
- However, if you consider that phishing – especially spearphishing – is successful against at least *some* employees, that distinction is less meaningful

An internal test can also be conducted starting with credentials for a possible insider threat

- The pentest team could be given the credentials for a regular user, a user with elevated privileges, or an administrator
- This would give an idea of the damage that could be caused by the insider threat

Legal Issues

The reason to make note of the Rules of Engagement (RoE) in the previous slide is because it is very easy to run into legal trouble

Without proper authorization – from the system owner – you may be committing a computer crime

Some professionals haven’t been careful about their RoE

Read: *Arrested Development: Coalfire Pentesters 'Exonerated,' Charges Dismissed*, SecureWorld News Team, SecureWorld

- https://www.secureworld.io/industry-news/pentester-case-update-charges-dropped
- Charges were dropped, but that is a LOT of stress!

The RoE is your contract on what you are allowed to do – and what you aren’t

- Some consider it their “get out of jail free card”
- Make sure you follow it rigorously – it isn’t just a “guideline”
- I also recommend you include a process to update the RoE if you discover something during the assessment

Vulnerability Assessment

From Wikipedia, Vulnerability Assessment (computing):

- https://en.wikipedia.org/wiki/Vulnerability_assessment_(computing)
- ***Vulnerability assessment*** *is a process of defining, identifying and classifying the security holes in information technology systems. An attacker can exploit a vulnerability to violate the security of a system.*
- ***Purpose****: The primary purpose of the assessment is to find the vulnerabilities in the system, but the assessment report conveys to stakeholders that the system is secured from these vulnerabilities.*

One vulnerability scanner is Nessus by Tenable, Inc.

- To see what a vulnerability scanner looks like, read through the Nessus Professional demo pages:
  - https://www.tenable.com/products/nessus/demo

A limitation of vulnerability assessments (and any security assessment) is you only see the vulnerabilities for a snapshot in time

- If the system is updated, modified, or reconfigured, the assessment results may no longer be valid

Vulnerability Assessment vs. Pentest

While they are similar, these are two different activities

A vulnerability assessment is a scan of a system, network, website, application, or enterprise to identify, quantify, and prioritize vulnerabilities in a system

A penetration test is evaluating the security of a system by simulating an attack from a malicious source. The pentest team may use vulnerabilities, but may exploit other issues

- They could guess passwords for users, or use compromised credentials
- Could use system functionality in unexpected ways
- Exploit misconfigurations
- Use social engineering to obtain information

However, vulnerability assessments (such as a scan by Nessus) can be automated

Kali Linux

From Marvel's Spider-man: "With great power must also come… great responsibility!"

From: Kali.org:

- *Kali Linux is an open-source, Debian-based Linux distribution geared towards various information security tasks, such as Penetration Testing, Security Research, Computer Forensics and Reverse Engineering.*

Kali is the Linux distribution used by most industry professionals for their assessment work

The website has documentation on the various tools – and YouTube is loaded with guides and tutorials on using Kali and its tools

However, please keep in mind that Kali is a powerful tool – so you need to be responsible!

- Don't scan or touch any system you don't own
- If you use a system you own, make sure it is backed up – and you can restore that backup!

Learn responsibly!