Pen Testing for DevSecOps

Challenges with Pentesting in DevSecOps

By embracing DevSecOps practices and integrating penetration testing into the development cycle, organizations can improve the effectiveness and efficiency of their security efforts, ultimately leading to better security outcomes

Lack of Expertise:	Penetration testers lack DevSecOps expertise in practices and tools, this may make DevSecOps tools integration with the development process challenging
Lack in communication	Communication barriers exist due to differing terminology and priorities. Different priorities and objectives between penetration testers and DevSecOps teams can also lead to communication breakdowns. This may lead to miscommunication, hold-ups, and exposed weaknesses
Lack of visibility:	Teams that engage in DevSecOps frequently operate in hectic settings and might not have the essential visibility into the systems and apps that are being tested. Because of this, penetration testers may find it challenging to carry out exhaustive testing
Technical Difficulties:	DevSecOps Tools, frameworks and lifecycle is exhaustive. For penetration testers who might not be acquainted with all of the tools and technologies in use, this could present technical difficulties
Time constraints:	Continuous testing is required by DevSecOps throughout the development lifecycle. There may be pressure on penetration testers to do their work quickly, which might result in mistakes and overlooked vulnerabilities

Vulnerability Scanning in CI/CD Pipeline

- Vulnerability scanning in CI/CD pipeline helps in early detection of vulnerabilities and security threats, unauthorized devices, and discover signs of a compromised system
- It helps in meeting compliance requirements such as HIPAA, PCI DSS, etc
- Conducting vulnerability scanning and adopting early preventive measures can help the organization in staying ahead of cybercriminals
- Common security vulnerabilities detected by vulnerability scanner in CI/CD pipeline:
- Cross-site scripting (XSS)
- SQL injection
- Command injection
- Path traversal
- Man-in-the-middle (MITM) attack
- Malicious code

Vulnerability Assessment and Remediation using AI

1.In DevSecOps, AI helps to improve vulnerability assessment and remediation in CI/CD pipeline by automating the detection, prioritization, and fixing of security vulnerabilities throughout the **software development lifecycle**

2.Automation and Efficiency: Traditional vulnerability management is labor-intensive and error-prone, while AI automates scanning, prioritization, and remediation, integrating smoothly into CI/CD pipelines for enhanced efficiency

3.Intelligent Prioritization: Manual methods can lead to inconsistent prioritization, whereas AI uses data-driven insights to ensure that critical vulnerabilities are addressed first within the CI/CD pipeline

4.Continuous Monitoring: Artificial Intelligence helps monitoring and detecting vulnerabilities in real-time throughout the CI/CD pipeline, ensuring continuous security

5.Advanced Analytics and Predictive Capabilities: AI provides advanced analytics and predictive capabilities which addresses potential vulnerabilities before they impact the pipeline

6.Adaptability and Self-Learning: AI keeps up with evolving threats and learns from new data, ensuring that CI/CD pipeline remain current and effective

Vulnerability Scanner Evaluation

While selecting a vulnerability scanner, the following technical aspects should be considered:

Test Coverage:	Ensure that the tool covers a wide range of security tests
Web Technology Coverage:	Ensure that the vulnerability scanning tool detects every form, page, and feature of the web application across various development stacks, frameworks, and deployment environments in order to manage vulnerabilities effectively
Ease of Use:	Ensure that all manual labor tasks to discover and detect threats are abstracted by the vulnerability scanning tool so that team focuses on value-added tasks
Speed and Quality:	Ensure that the vulnerability scanning tool quickly determines the functional health of all the application's resources and continuously updates the vulnerability inventory with low false positives
Compliance:	Ensure that the tool is meeting security in accordance with compliance standards such as HIPAA, GDPR, and ISO
Remediation Suggestions:	Ensure that the tool has automatic remediation feature for basic vulnerabilities and provides suggestions for more complicated issues

Terminology

▶**Ad hoc testing**: Testing carried out with no systematic approach or methodology. It is hoped that this book will steer you away from that.

▶**Black hat hacker**: A hacker who does break the law. This term is synonymous with cracker, but the term *black hat hacker* is far more common. Contrary to some media portrayals, a black hat is not necessarily any more skilled. Someone can break the law and still have only minimal skill.

▶**Cracker**: One who breaks into a system in order to do something malicious, illegal, or harmful. Synonymous with black hat hacker.

▶**Ethical hacking**: Someone who is using hacking techniques for legal and ethical purposes.

▶**Footprinting**: Scanning a target to learn about that target.

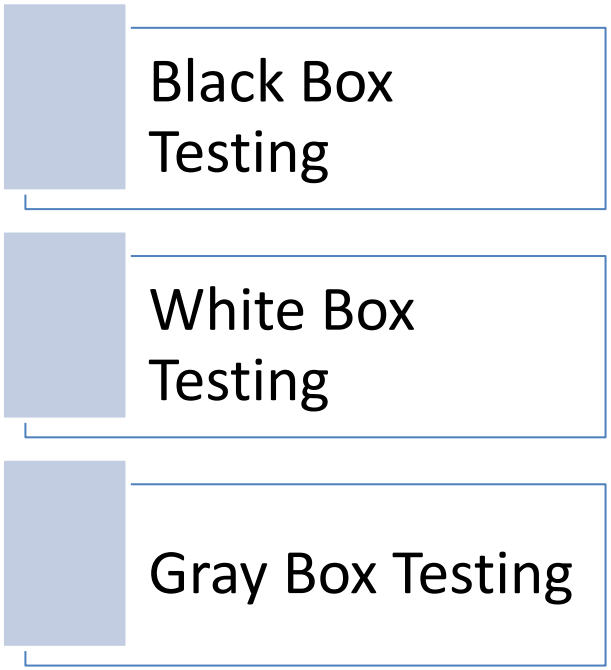
▶**Gray hat hacker**: A hacker who usually obeys the law but in some instances will cross the line into black hat hacking.

▶**Hacker**: One who tries to learn about a system by examining it in detail by reverse-engineering or probing the system. This is an important definition. Hackers, are not necessarily criminals. One can be a hacker and never break the law, nor do anything unethical.

▶**Script kiddy**: A slang term for an unskilled person who purports to be a skilled hacker. Some people download a tool or two, learn to use those, then consider themselves great hackers, when they are not.

▶**White hat hacker**: A hacker who does not break the law, often synonymous with ethical hacker. Essentially this is a person who uses hacking skills in a legal and ethical manner.

Testing Terms



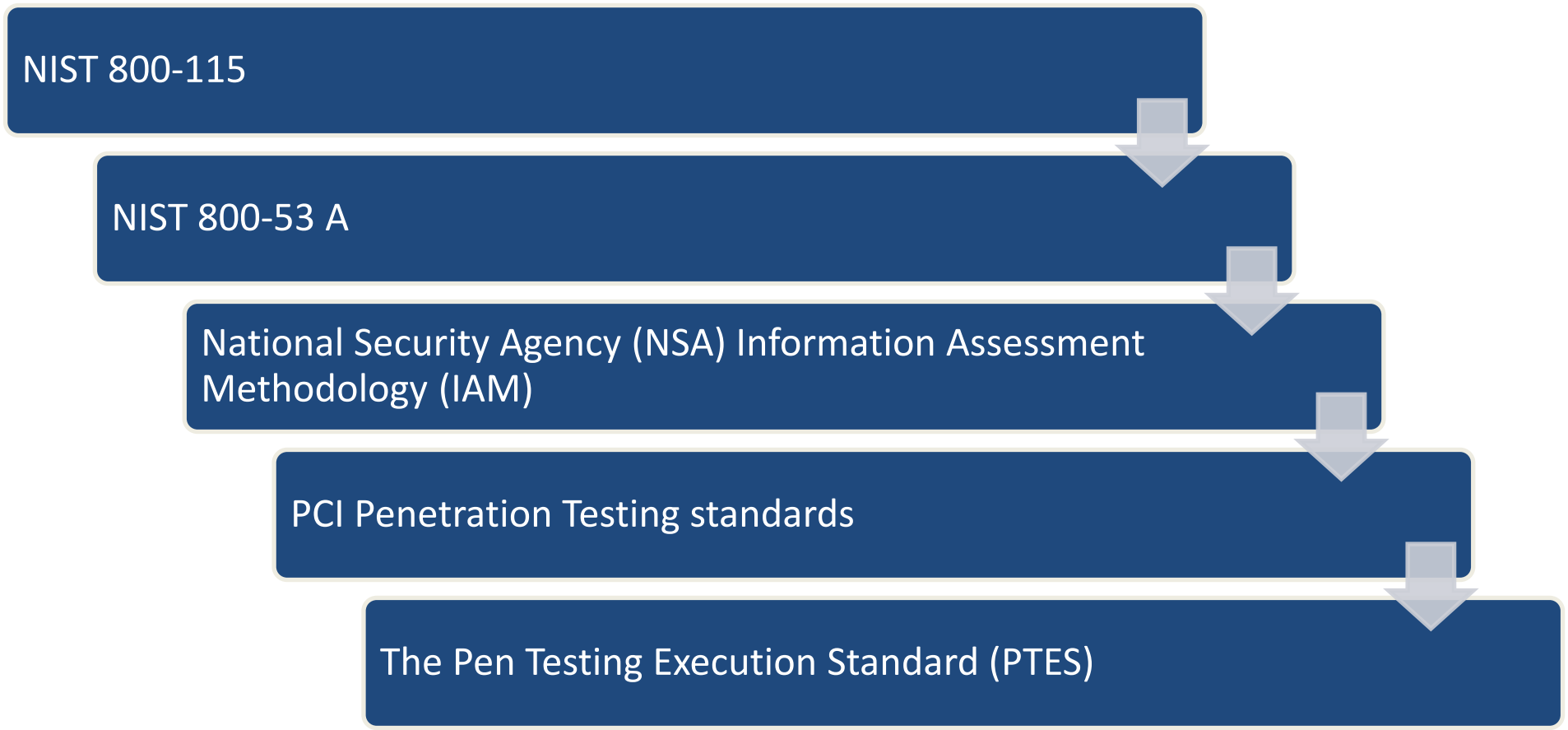
Note: White box is also known as clear box testing, glass box testing, transparent box testing, and structural testing

Quality of Security Testing

- False Positives
- False Negatives
- Incomplete

Reasons for false negatives

Security Standards to Know



NIST 800-115

NIST 800-115 describes security assessments and has four phases:

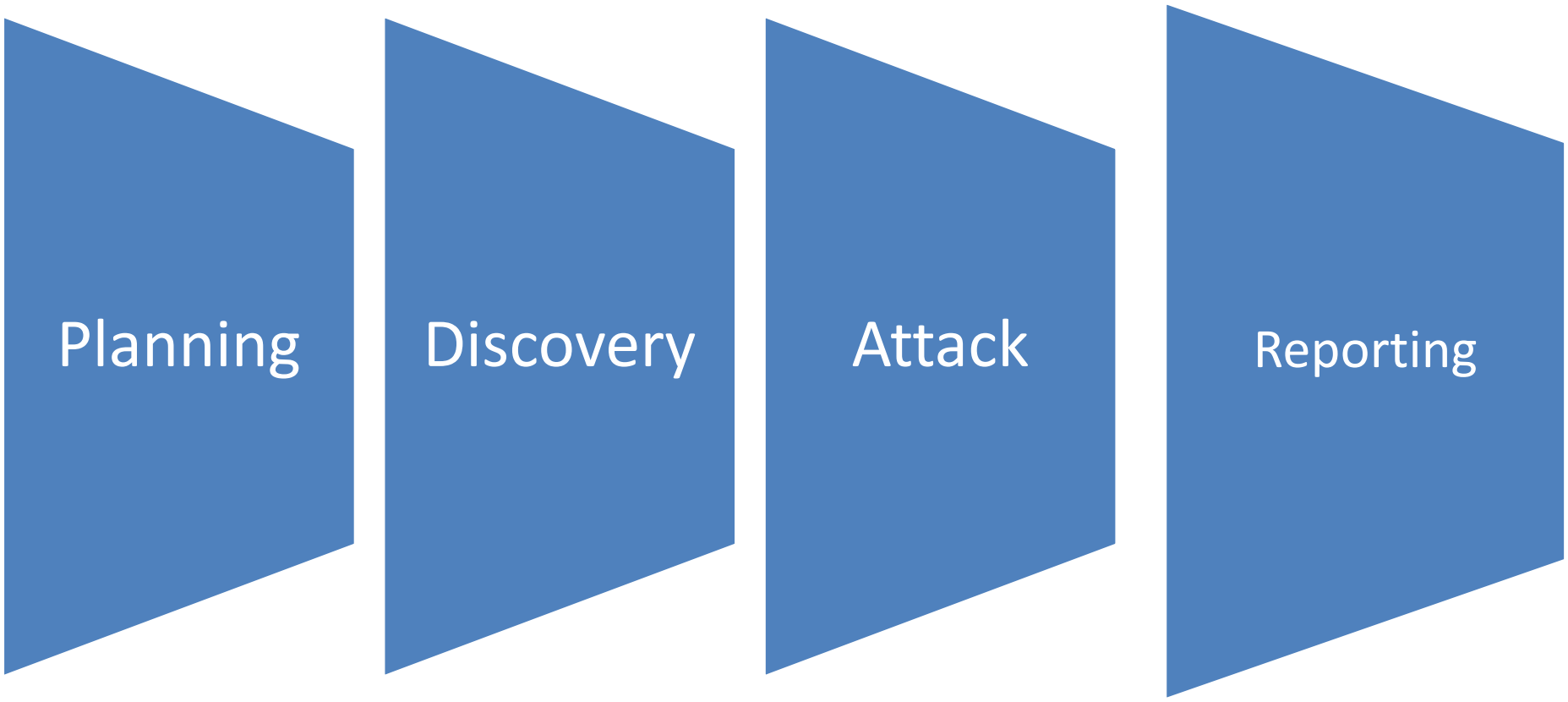


Image from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

NIST 800-115

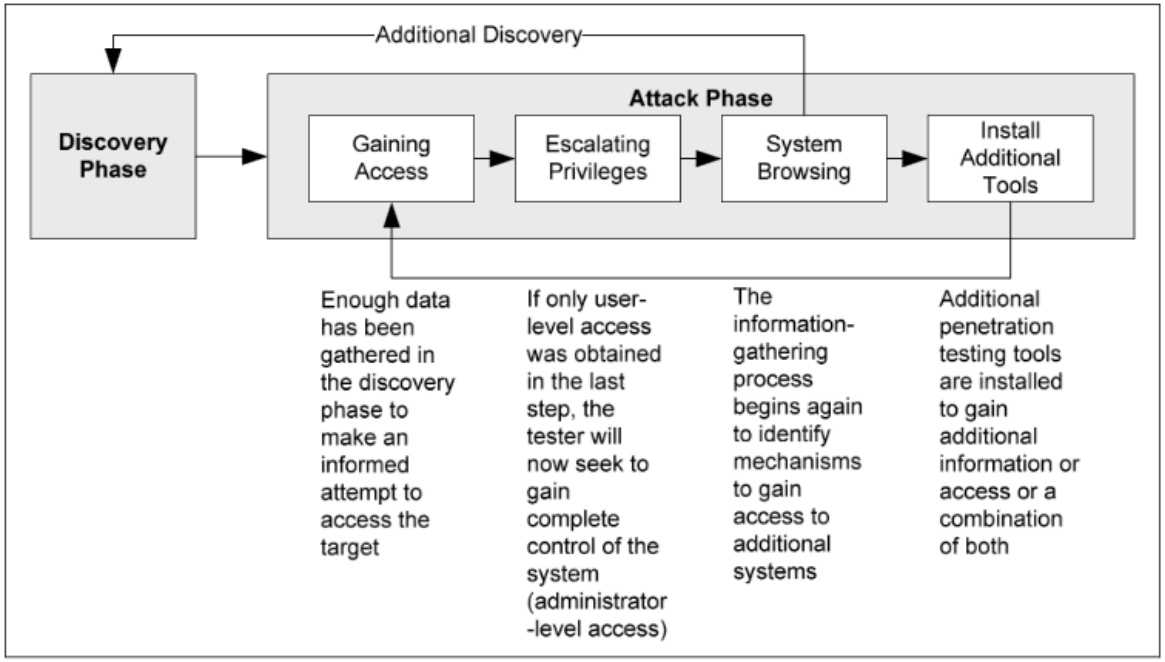
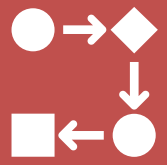


Figure 5-2. Attack Phase Steps with Loopback to Discovery Phase

NIST 800-115



Implement a repeatable and documented assessment methodology.

Determine the objectives of each security assessment, and tailor the approach accordingly.

Analyze findings, and develop risk mitigation techniques to address weaknesses.

NIST 800-115

Image from http://csrc.nist.gov/publications/nistpubs/800-115/SP800-115.pdf

Security Testing Technique	Security Testing Tool
Review	
Network Sniffing	Dsniff, Ettercap, Kismet, Mailsnarf, Msgsnarf, Ntop, Phoss, SinFP, SMB Sniffer, and Wireshark
File Integrity Checking	Autopsy, Foremost, RootkitHunter, and Sleuthkit
Target Identification and Analysis	
Application Security Testing	CIRT Fuzzer, Fuzzer 1.2, NetSed, Paros Proxy, and Peach
Network Discovery	Autonomous System Scanner, Ettercap, Firewalk, Netdiscover, Netenum, Netmask, Nmap, P0f, Tctrace, and Umit
Network Port and Service Identification	Amap, AutoScan, Netdiscover, Nmap, P0f, Umit, and UnicornScan
Vulnerability Scanning	Firewalk, GFI LANguard, Hydra, Metasploit, Nmap, Paros Proxy, Snort, and SuperScan
Wireless Scanning	Airsnarf, Airsnort, BdAddr, Bluesnarfer, Btscanner, FakeAP, GFI LANguard, Kismet, and WifiTAP
Target Vulnerability Validation	
Password Cracking	Hydra, John the Ripper, RainbowCrack, Rcrack, SIPcrack, SIPdump, TFTP-Brute, THC PPTP, VNCrack, and WebCrack
Remote Access Testing	IKEProbe, IKE-Scan, PSK-Crack, and VNC_bypauth
Penetration Testing	Driftnet, Dsniff, Ettercap, Kismet, Metasploit, Nmap, Ntop, SinFP, SMB Sniffer, and Wireshark

NIST 800-53 A

Guide for Assessing Security Controls in Federal Information Systems and Organizations

Assessments within the SDLC

Assessment Procedures

- Open Checklist Interactive Language

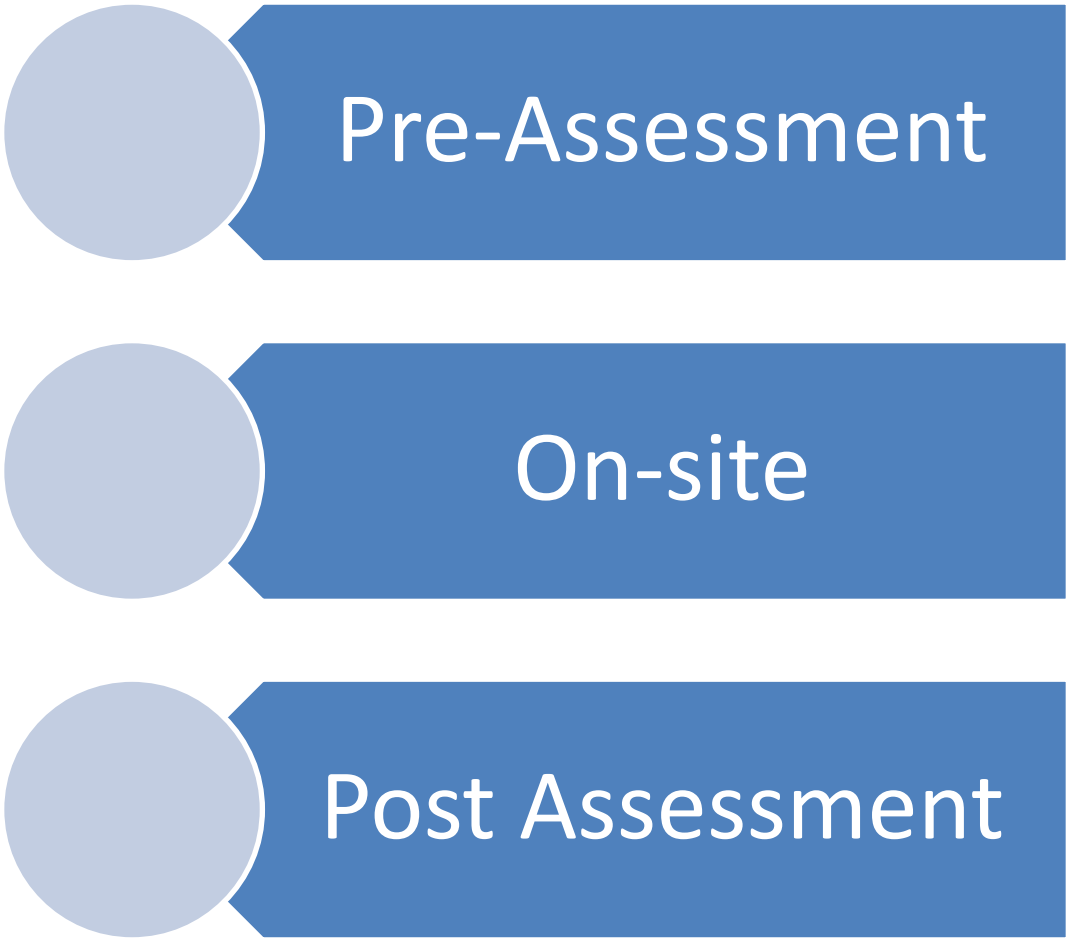
Preparing for Control Assessments

Developing Security Assessment Plans

Describes testing and evaluation procedures for the 17 required control families

http://csrc.nist.gov/publications/nistpubs/800-53A-rev1/sp800-53A-rev1-final.pdf

National Security Agency (NSA) Information Assessment Methodology (IAM)



http://www.sans.org/reading-room/whitepapers/auditing/application-nsa-infosec-assessment-methodology-1045
http://systemexperts.com/media/pdf/NSAIAM.pdf

NSA-IAM Overview

Pre-Assessment

- Determine and manage the customer's expectations
- Gain an understanding of the organization's information criticality
- Determine customer's goals and objectives
- Determine the system boundaries
- Coordinate with customer
- Request documentation

On-Site Assessment

- Conduct opening meeting
- Gather and validate system information (via interview, system demonstration, and document review)
- Analyze assessment information
- Develop initial recommendations
- Present out-brief

Post-Assessment

- Additional review of documentation
- Additional expertise (get help understanding what you learned)
- Report coordination (and writing)

See also http://www.isaca.org/Journal/archives/2007/Volume-2/Documents/jopdf0702-info-security-request.pdf

IAM

Information Criticality matrix

System Criticality matrices

Baseline INFOSEC evaluation areas

Technical Assessment Plan (TAP)

http://www.sans.org/reading-room/whitepapers/auditing/application-nsa-infosec-assessment-methodology-1045

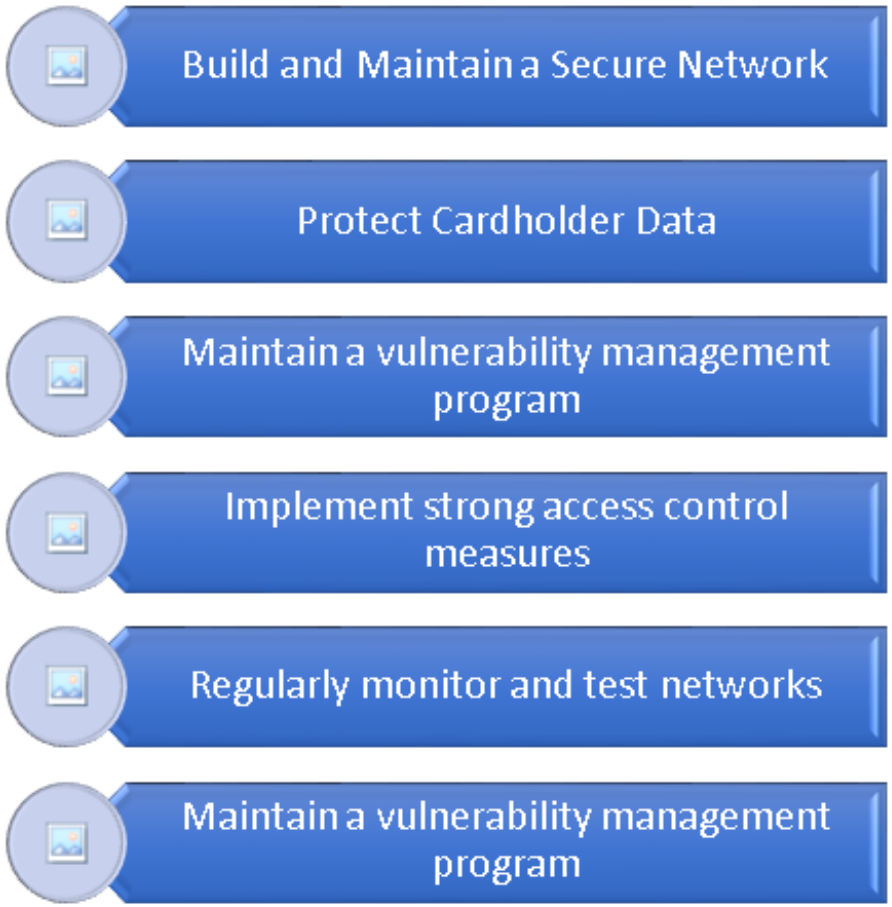
http://systemexperts.com/media/pdf/NSAIAM.pdf

PCI Penetration Testing standard

- Scope
- Qualifications of a Penetration tester
- Penetration Testing Components
- Methodology
- Pre-engagement
  - Pre-engagement includes scoping, documentations (network diagram, cardholder data flow diagram, etc.), rules of engagement, success criteria, review of past issues.
- The actual penetration test
- Post-Engagement
  - Remediation best practices, retest vulnerabilities, reporting and documentation standards.

https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

PCI Penetration Testing standard



PCI Penetration Testing standard

	Vulnerability Scan	Penetration Test
Purpose	Identify, rank, and report vulnerabilities that, if exploited, may result in an intentional or unintentional compromise of a system.	Identify ways to exploit vulnerabilities to circumvent or defeat the security features of system components.
When	At least quarterly or after significant changes.	At least annually and upon significant changes. (Refer to Section 2.6 of this document for information on significant changes.)
How	Typically a variety of automated tools combined with manual verification of identified issues.	A manual process that may include the use of vulnerability scanning or other automated tools, resulting in a comprehensive report.

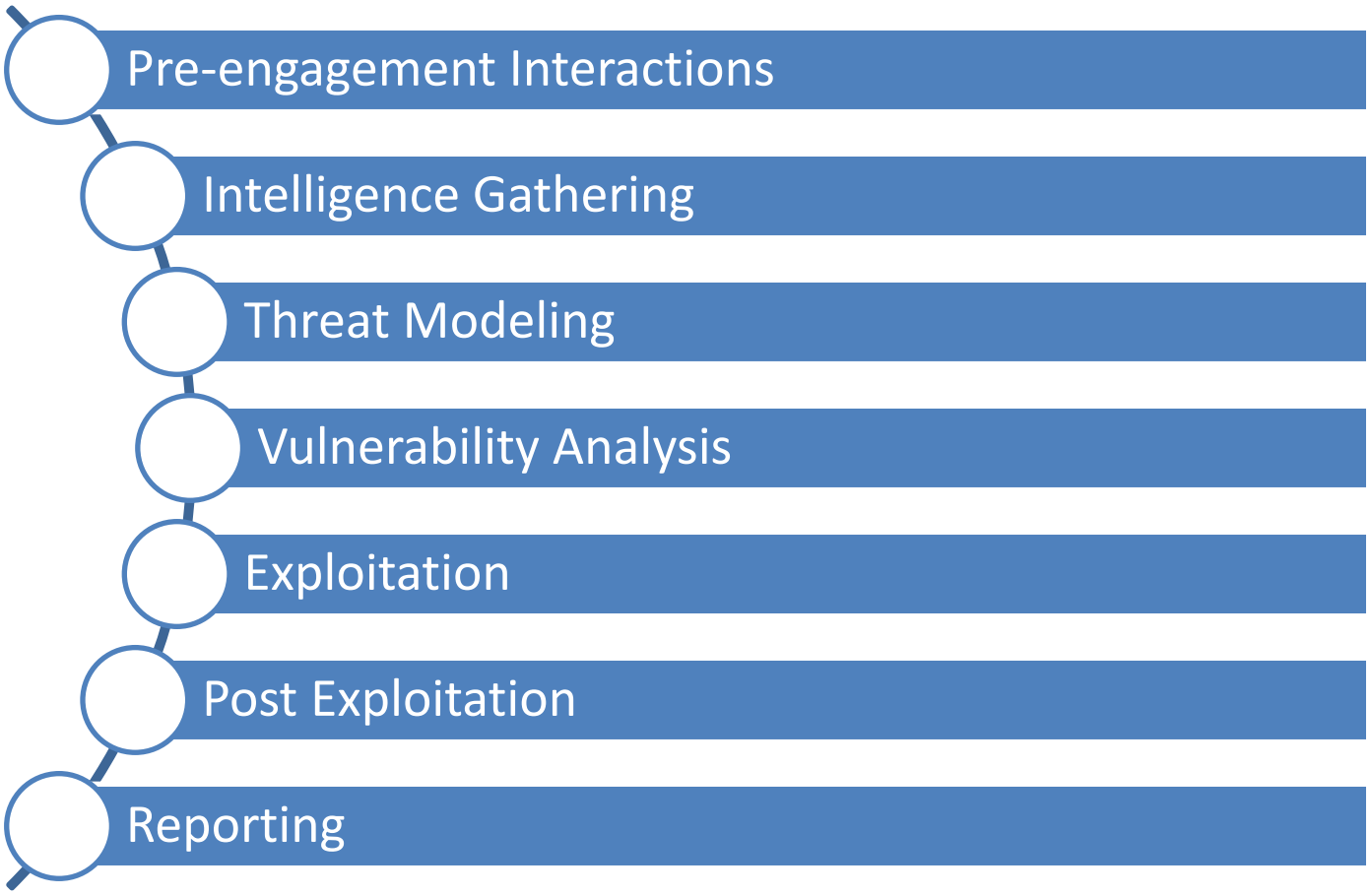
Chart from Penetration Testing Guidance
https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf

PCI Highlights

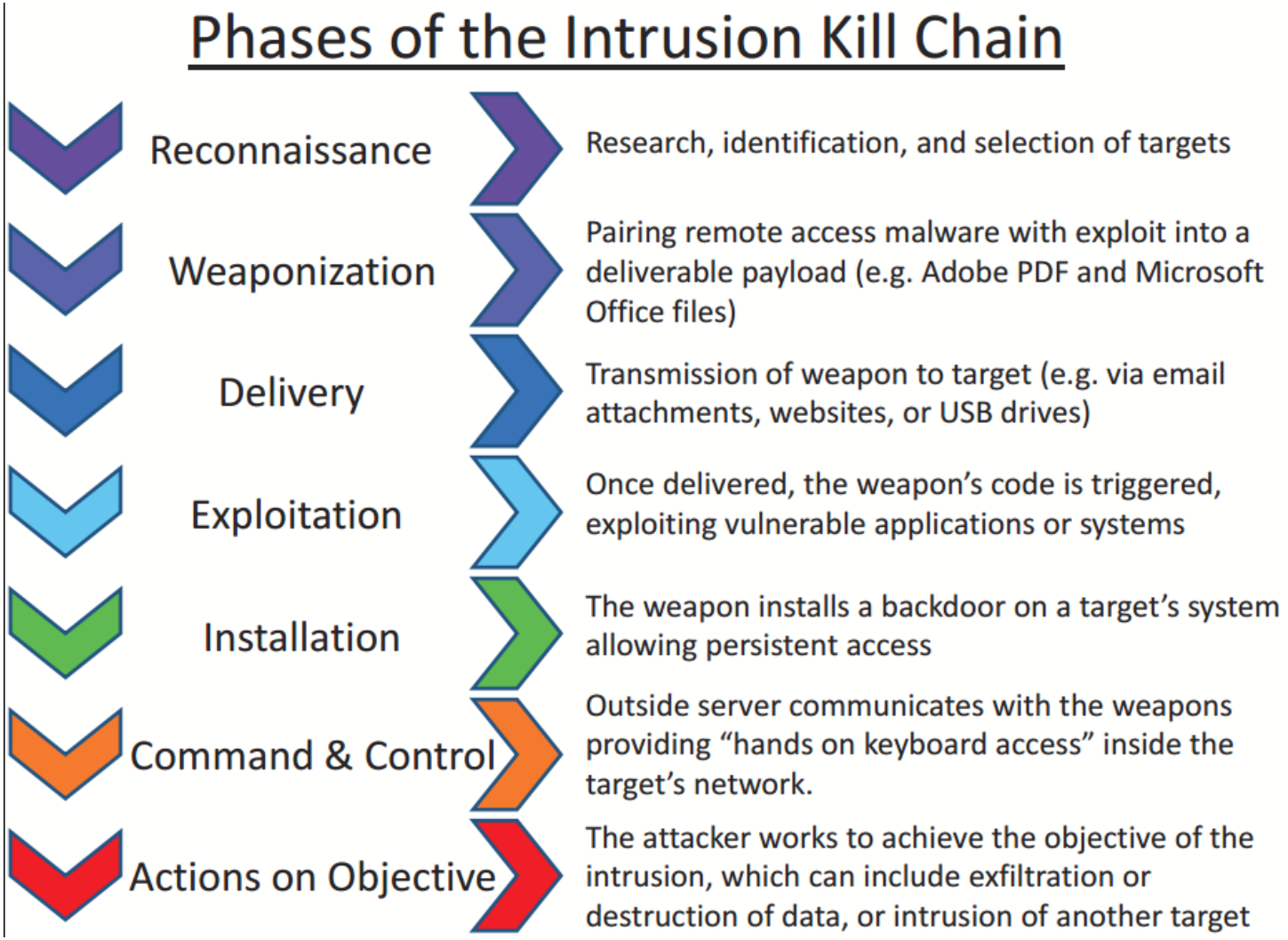
Pre-Engagement	Actual Test	Post-Engagement
• Scope • Documentation • Rules of engagement • Environment • Success Criteria • Past vulnerability scans	• Application Layer • Network Layer • Segmentation • How to handle card holder data • Post-exploitation	• Remediation • Retesting identified vulnerabilities • Cleaning Up • Reporting

PTES

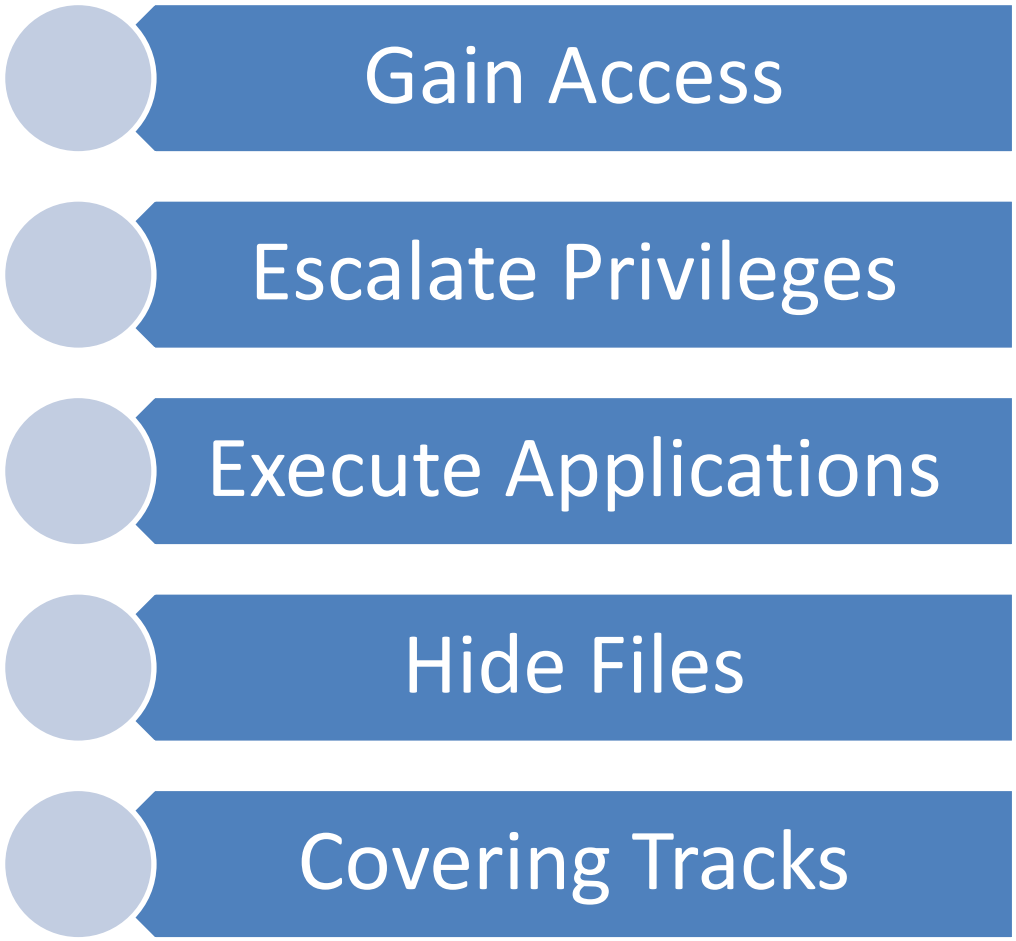
The Pen Testing Execution Standard (PTES, 2016) recommends seven stages



Cyber Kill Chain



CEH Lifecycle



What goes in a pen testing report

SANS has guidelines
http://www.sans.org/reading-room/whitepapers/bestprac/writing-penetration-testing-report-33343

InfoSec Institute has guidelines
http://resources.infosecinstitute.com/writing-penetration-testing-reports/

What goes in a pen testing report

The following is a general overview of what goes in a pen testing report

- Introduction
  - Tester name and contact information
  - What is being tested (Testing targets)
  - Why where those chosen?
- Executive summary
- Details
  - What methodology was used?
  - What tools where used?
  - What manual techniques where used?
  - Literally every test you did with screen shots and results.
- Exclusions
  - What was not tested and why
- Recommendations/Conclusions
  - What should be done to remediate discovered vulnerabilities
  - Are there other tests that should be done?

What goes in a pen testing report

The following are items that should permeate your report

- Why
  - Use footnotes to explain why a tool or technique was used.
  - Use footnotes to explain any details needed or to reference sources/standards
- Reference
  - Reference appropriate standards
    - PCI
    - HIPAA
    - NSA/IAM
    - Industry norms and recommendations

Remember you have to explain not only what you did but WHY you did it and what it means.

Vulnerability Scan v Pen Test vs Audit

Vulnerability Scan

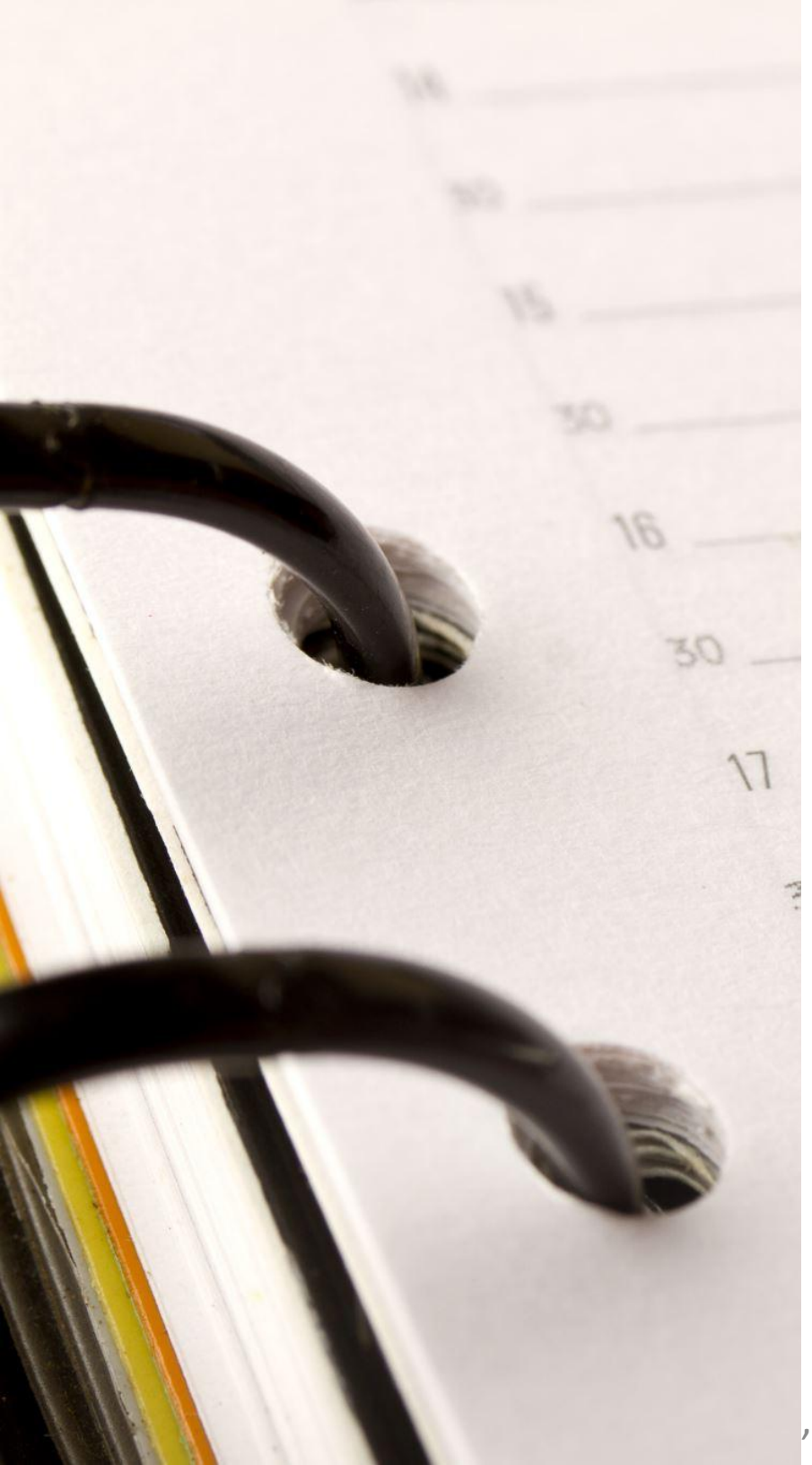
Uses tools to scan for known vulnerabilities

Pen Test

Actually attempts to break into the network

Audit

Checking logs, policies, looks for compliance to policies



Pen Testing

Who should do it?

- Outside parties?
- Inside staff?
- How to pick a good outside consultant
  - Experience
  - Training
  - Background checks
  - The report

Black box vs white box, when to use each technique.

What will a Pen Test accomplish?

FIND GAPS/FLAWS BEFORE SOMEONE ELSE DOES

VERIFY SECURITY MEASURES

DISCOVER GAPS IN SECURITY COMPLIANCE

Need for Bug Bounty Programs

With the introduction of DevSecOps methodology, organizations have been producing secure and robust software product fairly quickly

From the perspective of the developer and security team, the software product is secure; however, there could still be underlying vulnerabilities that can be exploited by an attacker

An interesting solution to this problem is a bug bounty program

Financial incentive is offered to ethical hackers who find and report security issues in the software product or applications

This will help the developer with discovery and remediation of unknown security issues in the application

Organizations can secure the application based on the reported vulnerabilities and suggested fixes by non-org\ security researchers

It also helps the organization in reducing data breaches

Vulnerability Scanning

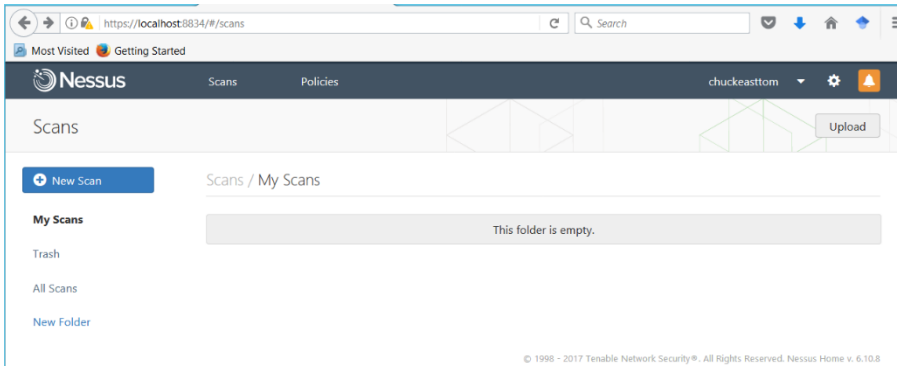
Must be routine. Depending on your environment that could be as long as annually, or as frequent as monthly.

Must use multiple tools. Nessus is a great place to start, but it is not the only tool. Other tools can include:

- Nmap for port scanning
- Vega
- Rapid 7 http://www.rapid7.com/products/nexpose/compare-downloads.jsp
- SAINT http://www.saintcorporation.com/solutions/vulnerabilityScan.html

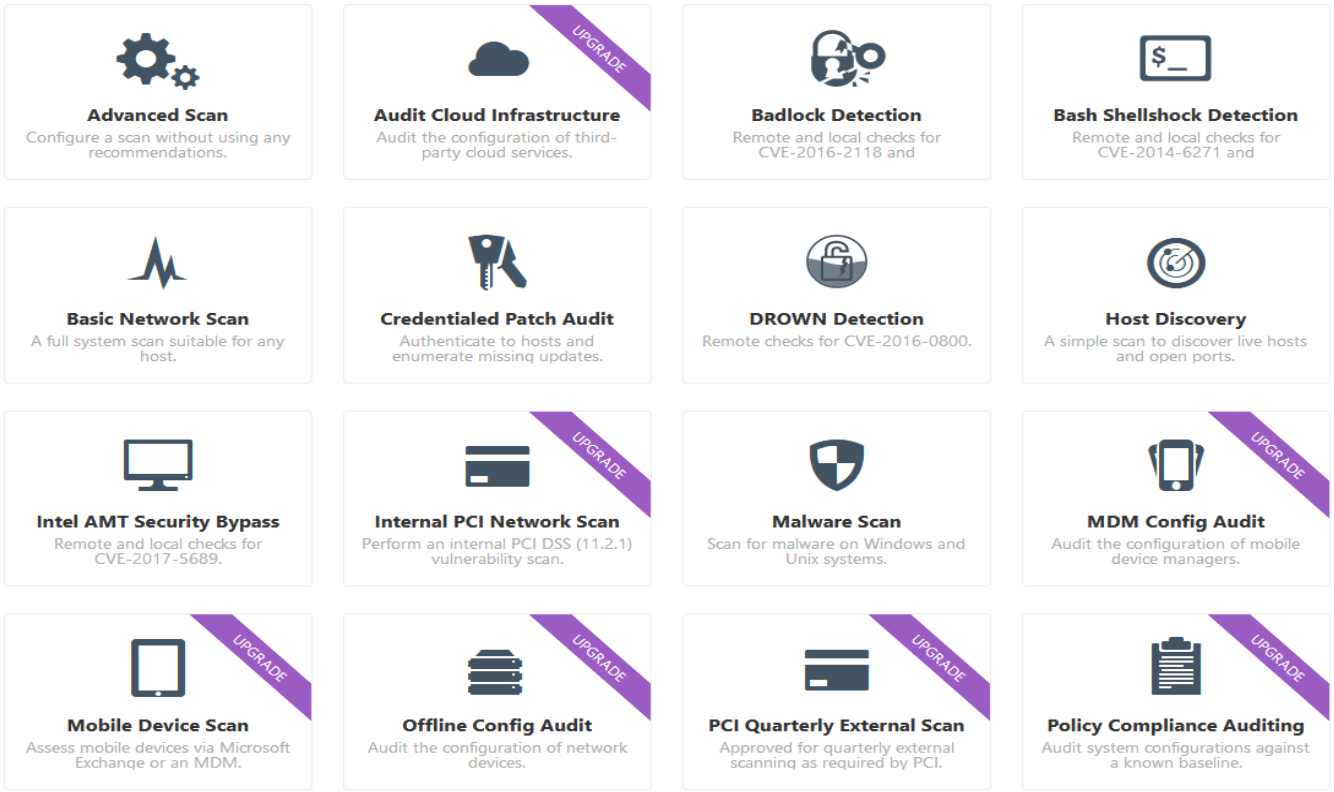
Vulnerability Scanners - Nessus

Nessus is a well-known vulnerability scanner. It has been used for many years. Unfortunately, it is not free. The license is over 2100 per year and can be obtained from https://www.tenable.com/ Its price has been a barrier for many penetration testers. The primary advantage of Nessus is that the vendor is constantly updating the vulnerabilities it can scan for..



Vulnerability Scanners - Nessus

The first step is to select New Scan. You then are given a number of options



Vulnerability Scanners - Others

Nexpose

This is another commercial product. It is from Rapid 7, the vendors who distribute Metasploit. You can find Nexpose at https://www.rapid7.com/products/nexpose/ There is a free trial version that you can download and experiment with. This tool is a Linux virtual machine and takes some effort to learn. Given that it is distributed by the same people who distribute Metasploit, it has received significant market attention.

SAINT

SAINT is a well-known vulnerability scanner. It is available at http://www.saintcorporation.com/. You can request a free trial version. It will scan the network for any TCP or UDP services, then scan those machines for any vulnerabilities. It uses Common Vulnerabilities and Exposures (CVE) as well as CERT advisories as references.

What should it consist of?

- Web testing
- Remote access testing
- Physical Penetration
- Social Engineering
- Phishing
- Virus

Tips for a successful pen test

Define your goals

Test should follow Risk Analysis

Formulate attacker profiles and test for those

Define the rules of engagement

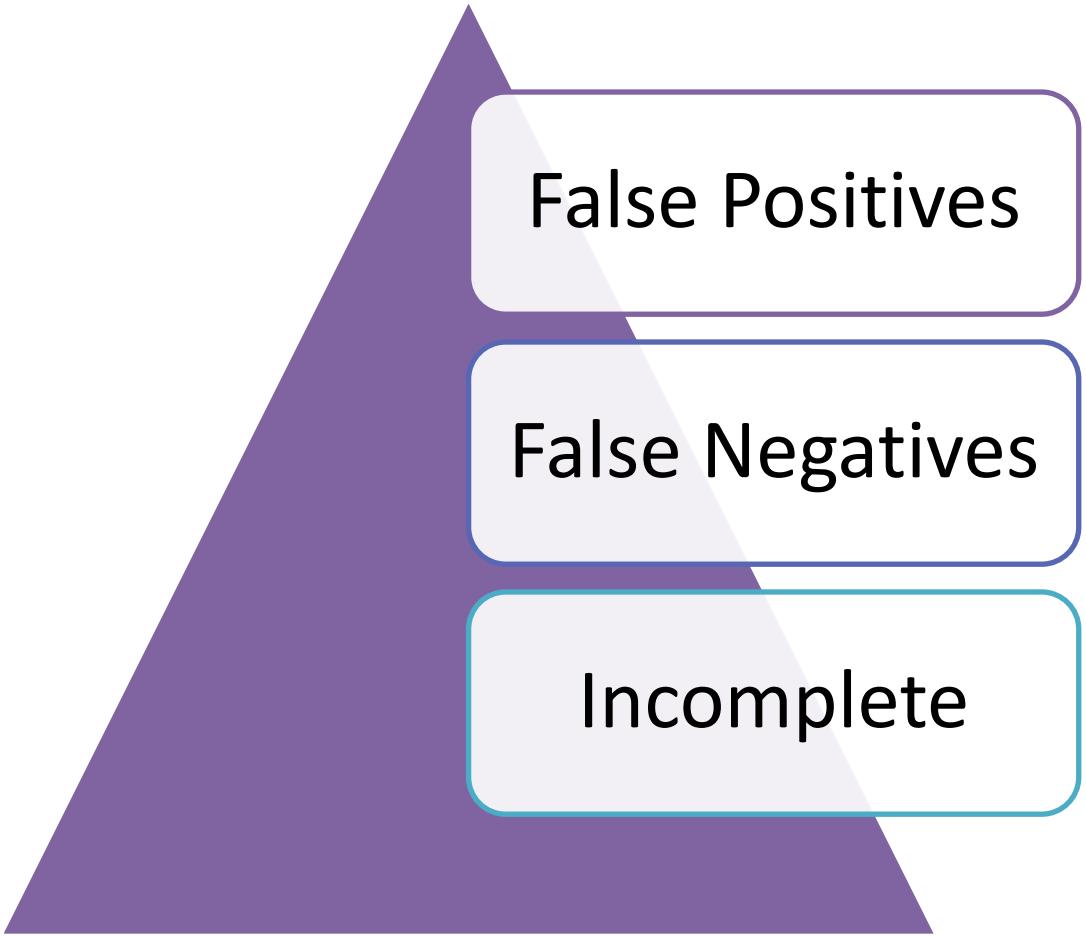
Detail what is expected, what is allowed, what is prohibited in advance.

It is often best to combine a vulnerability scan with a pen test, even if different parties perform each test.

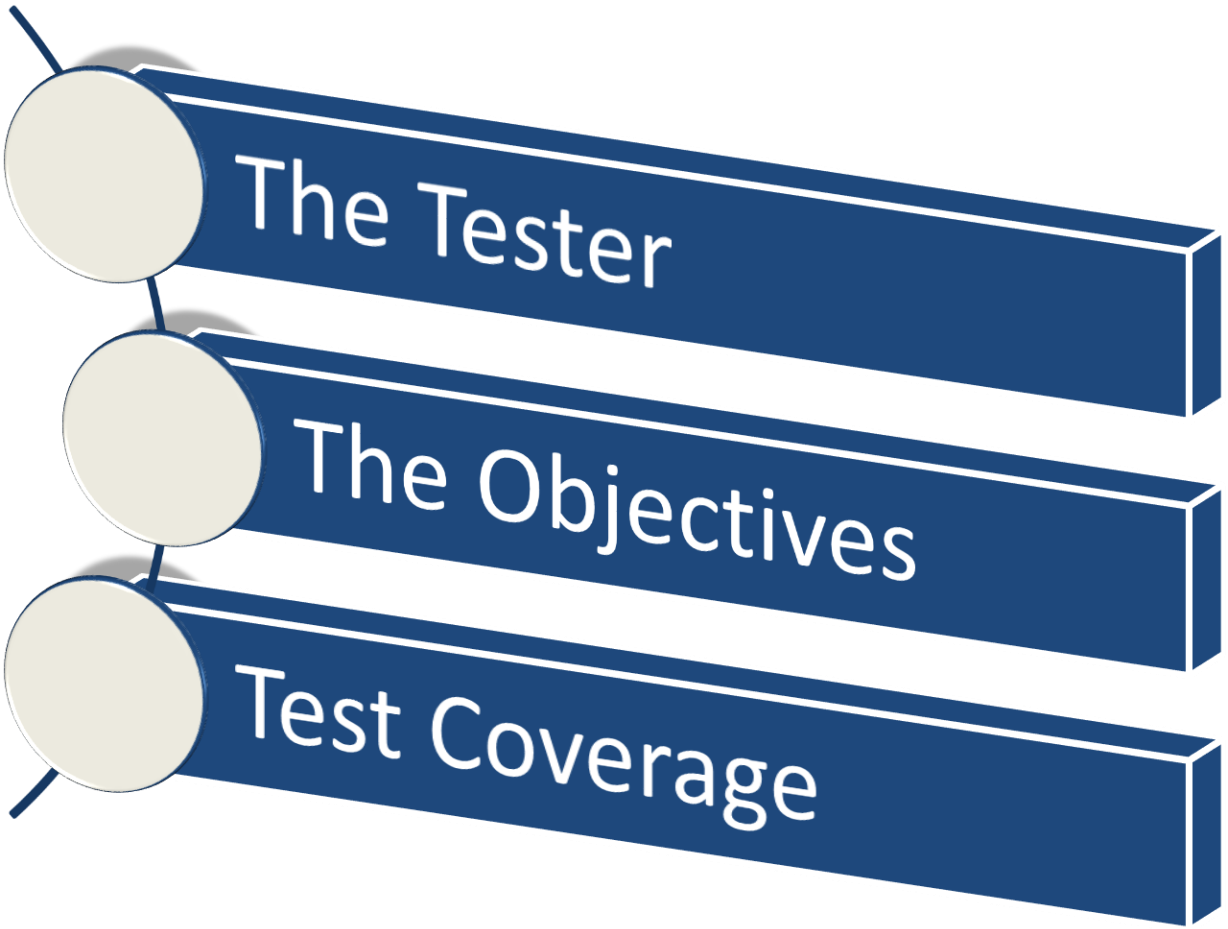
General Security Audit

- Review documents and policies
- Review accounts
- Review logs
- Review incident response reports
- Review incident response plans
- Network sniffing
- File integrity checking

Quality of Security Testing



Reasons for false negatives



Pre-test activites

- Risk assessment
- Setting clear goals
- Defining scope
- Know what is and is not being covered
- Plan tools and techniques

ISACA CISA Definition for Audit

"Systematic process by which a qualified, competent, independent team or person objectively obtains and evaluates evidence regarding assertions about a process for the purpose of forming an opinion about and reporting on the degree to which the assertion is implemented."

Auditor Qualifications

- **Independent:**
- **Professional Independence**: Auditor acts independent of group being audited
  - No friendships, dating, suggestive language, parties, lunches
- **Organizational Independence**: Auditor and his/her organization has no special interest in the audited organization
- **Qualified, Competent:**
- Adhere to Professional Ethics Standard
- ISACA standard and professional care
- Professional Competence
- Has skills/knowledge to complete task
- Continued professional training/education

Terms used in Audits

Control: The policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

IT Control Objective: A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.

Risk: The potential that a given threat will exploit vulnerabilities of an asset or group of assets to cause loss or damage to the assets.

Evidence: Evidence is any information used by the auditors whether the entity or data being audited follows the established audit criteria or objective.

IT Governance: A structure of relationships and processes to direct and control the enterprise in order to achieve the enterprise's goals by adding value while balancing risk versus return over IT and its processes

Control Self-Assessment (CSA

Control Assessment can be defined as a “management technique that assures stakeholders, customers and other parties that internal control system of the organization is reliable. It also ensures that employees are aware of the risks to the business and they conduct periodic, proactive reviews of control.

Substantive v Compliance Testing

Compliance Testing:

Are controls in place and consistently applied?

Access control

Program change control

Procedure documentation

Program documentation

Software license audits

System log reviews

Exception follow-ups

Substantive Testing:

Are transactions processed accurately?

Are data correct and accurate?

Double check processing

Calculation validation

Error checking

Operational documentation

If Compliance results are poor, Substantive testing should increase in type and sample number

Compliance Testing

Control: Is production software controlled?
Test: Are production executable files built from production source files?
Test: Were proper procedures followed in their release?

Control: Is Sales DB access constrained to Least Privilege?
Test: Are permissions allocated according to documentation?
Test: When sample persons access DB, can they access only what is allowed?

Substantive Testing

Audit: Is financial statement section related to sales accurate?

Test: Track processing of a sample transactions through the system, performing calculations manually

Test: Test error conditions

Audit: Is tape inventory correct?

Test: Search for sample days and verify complete documentation and tape completeness

Sampling

Statistical Sampling:
N% of all items randomly tested
Should represent population distribution
Variable Sampling: How accurate is the sample population in matching the full population?
Determine appropriateness of sampling: (e.g., $, weight, amount):
Sample average $24.50, Real average: $26.99
No statistical (or Judgment) Sampling:
Auditor justifies another distribution for sample selection
Which items are most risky?

Sampling

Tolerable Error Rate: The maximum allowable error rate (e.g., inappropriately documented changes)

Non-Statistical Sampling includes**:**
Discovery Sampling: A minimal testing model used when the expected occurrence rate is extremely low (e.g., find fraud, break laws)
Stop-or-Go Sampling: If the first 20 have zero errors, then stop. Else if the first 100 have < 10 errors, stop. Else…
Attribute Sampling: How many of X have Y attribute?
E.g. How many changes are appropriately documented?