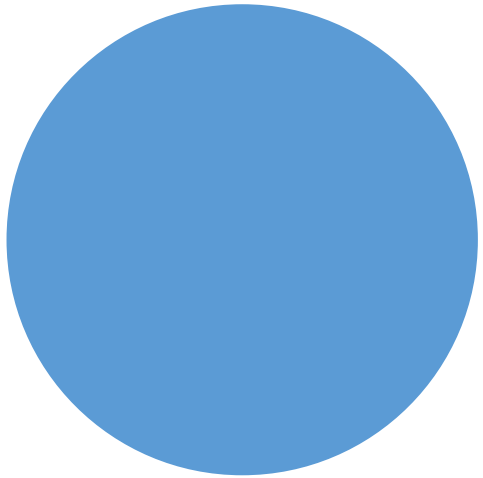
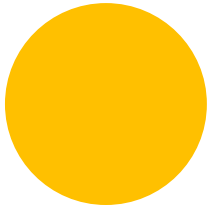
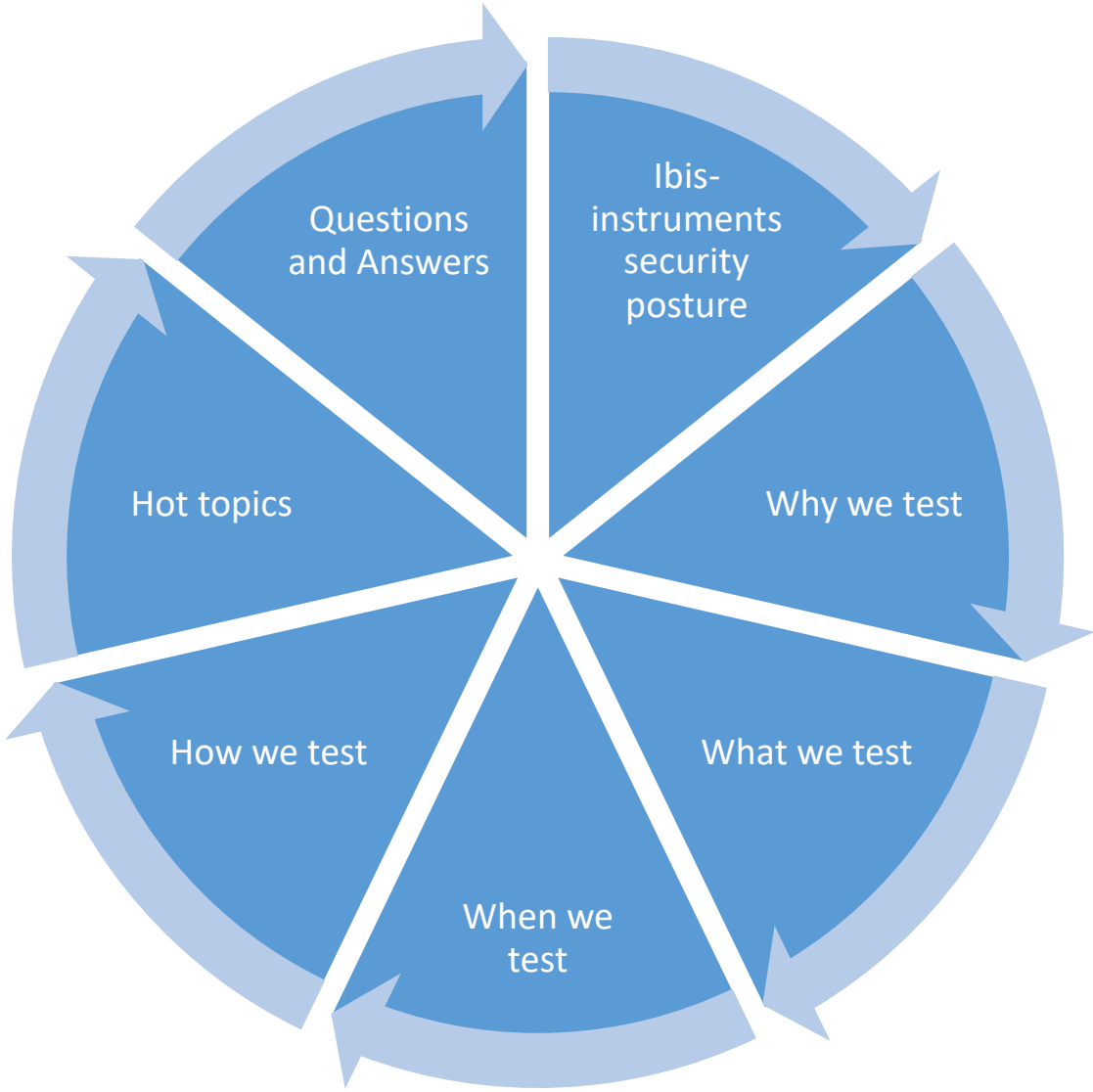



Vulnerability and penetration testing

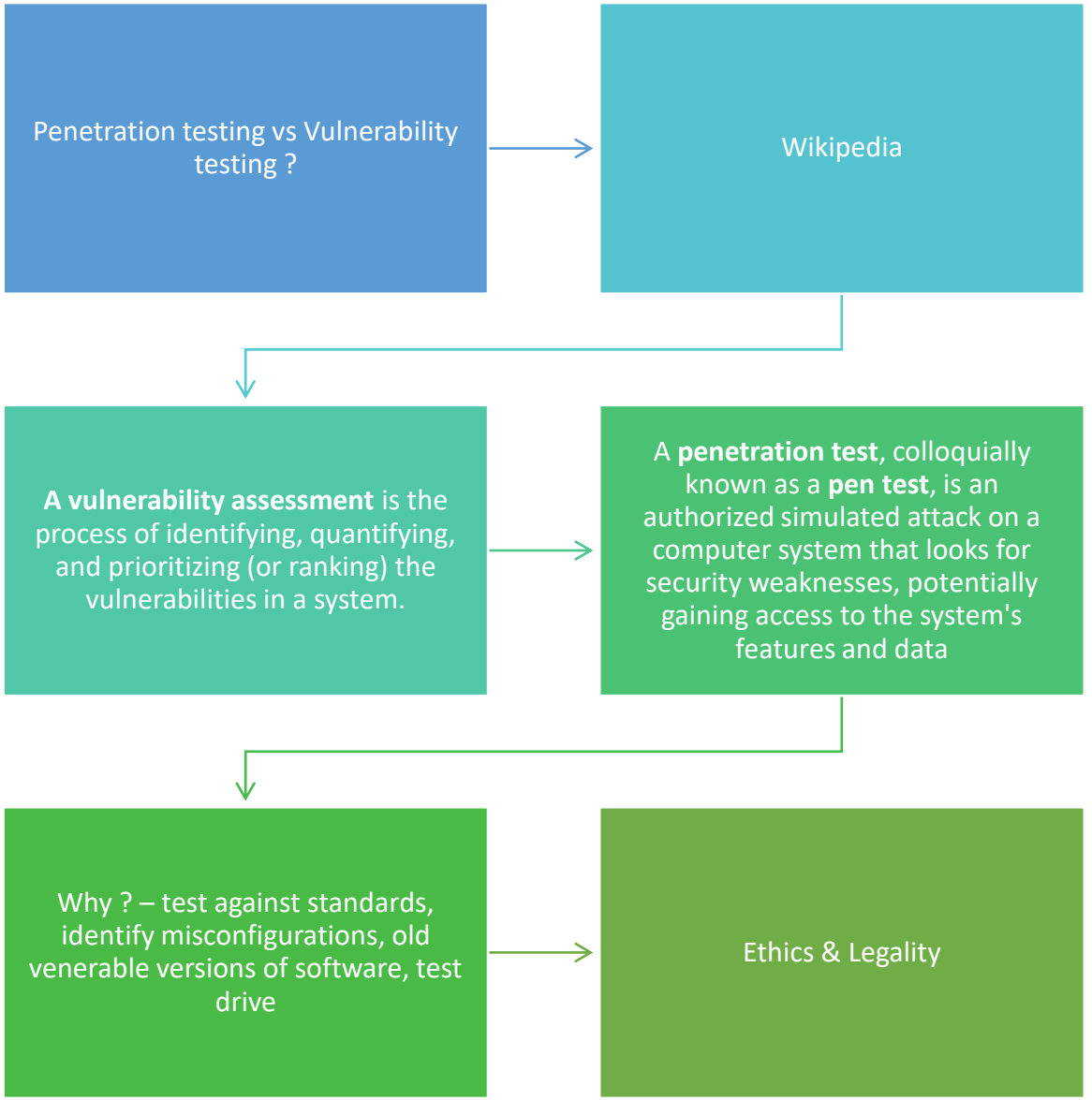
Predrag Skundric

September 2017

Presentation topics



Definition


Penetration testing vs Vulnerability testing ?
Wikipedia
A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system.
A penetration test, colloquially known as a pen test, is an authorized simulated attack on a computer system that looks for security weaknesses, potentially gaining access to the system's features and data
Why ? – test against standards, identify misconfigurations, old venerable versions of software, test drive
Ethics & Legality

Why testing

Preventing financial loss through fraud (hackers, extortionists and disgruntled employees) or through lost revenue due to unreliable business systems and processes.

Proving due diligence and compliance to your industry regulators, customers and shareholders. Non-compliance can result in your organisation losing business, receiving heavy fines, gathering bad PR or ultimately failing. Protecting your brand by avoiding loss of consumer confidence and business reputation.

vulnerability testing helps shape information security strategy through identifying vulnerabilities and quantifying their impact and likelihood so that they can be managed proactively; budget can be allocated and corrective measures implemented.

In order to be compliance with Law regulations and relevant standards related to information security (ISO 27001, PCI DSS, ISO 31000 etc.)

Process of vulnerability testing

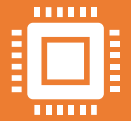
- **Defining Goals& Objectives: -** Defines goals and objectives of Vulnerability Analysis
- **Defining Scope**: - While performing the Assessment and Test, Scope of the Assignment needs to be clearly defined.
- **Defining type of testing:**

  a) Black Box Testing: - Testing from an external network with no prior knowledge of the internal network and systems.

  b) Grey Box Testing: - Testing from either external or internal networks, with the knowledge of internal network and system. It's the combination of both Black Box Testing and White Box Testing.

  c) White Box Testing: - Testing within the internal network with the knowledge of internal network and system. Also known as Internal Testing.

Process of vulnerability testing - continued



Information Gathering: - Obtaining as much information about IT environment such as Networks, IP Address, Operating System Version, etc. It's applicable to all the three types of Scopes such as Black Box Testing, Grey Box Testing and White Box Testing

Vulnerability Detection: -In this process, vulnerability scanners are used, it will scan the IT environment and will identify the vulnerabilities.

Providing report about vulnerabilities to customer

Information Analysis and Planning: - It will analyze the identified vulnerabilities, to devise a plan for penetrating into the network and systems.

What we can test

- Perimeter network
- Windows based environments
- Unix/Linux based environments
- Databases (Oracle, SQL etc.)
- Applications
- Patch management systems etc.

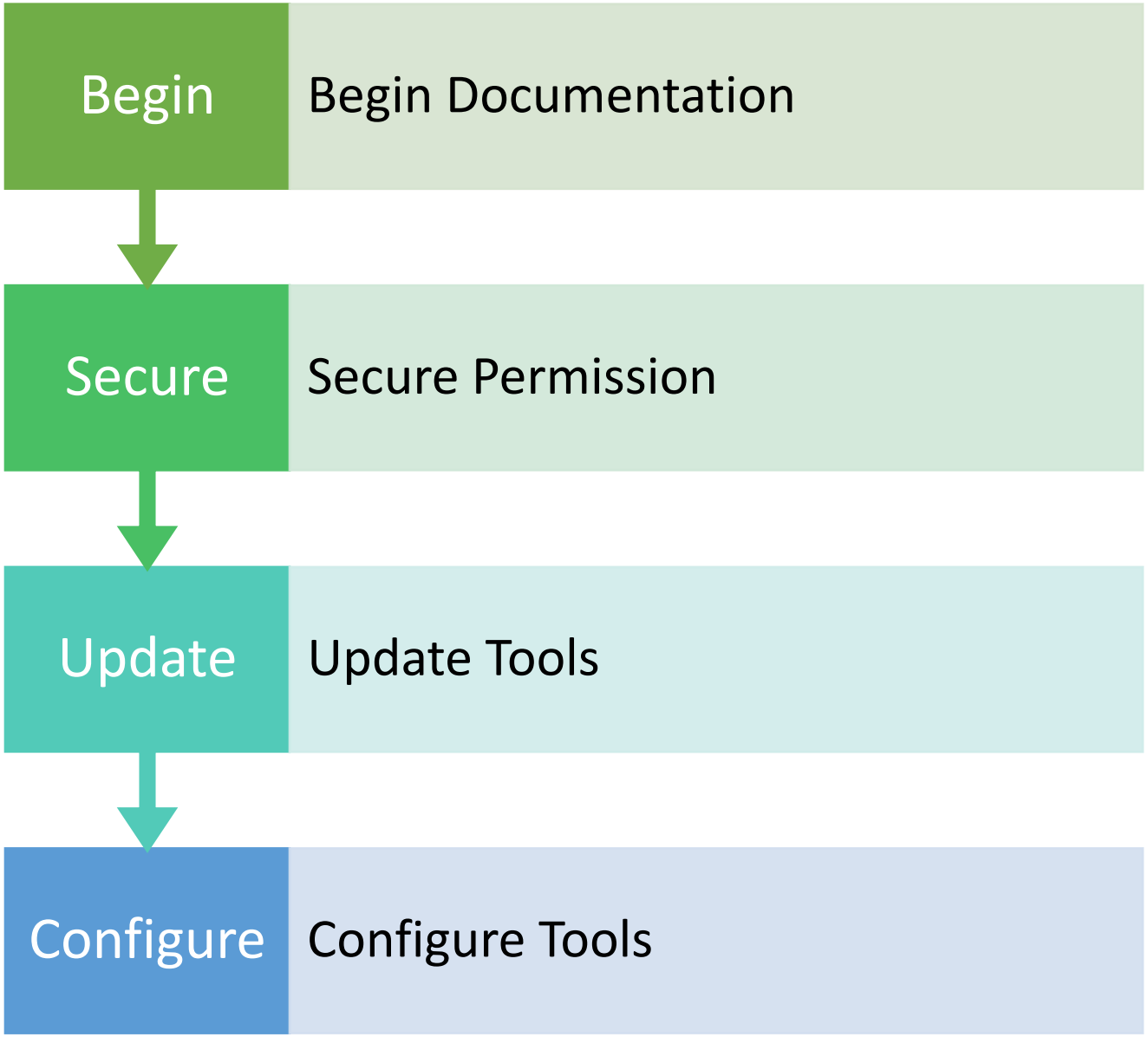
When to test

- Before posting system into production, best practice is during development phase
- On regular basis for critical systems recommendation is to test every three months and for other systems twice per year
- When significant changes on IT infrastructure are made
- Penetration tests should be made once per year or in case of significant changes on perimeter networks

Vulnerability Methodology

- Phases:
- Setup
- Test execution
- Vulnerability Analysis
- Reporting
- Remediation

Setup phase


Begin
Begin Documentation
Secure
Secure Permission
Update
Update Tools
Configure
Configure Tools

Test execution phase

Run the Tools

If applicable for one detected vulnerability try to provide confirmation from another one

Vulnerability Analysis phase

Defining and classifying network or System resources.

Assigning priority to the resource(Ex: - High, Medium, Low)

Identifying potential threats to each resource.

Developing a strategy to deal with the most prioritize problems first.

Defining and implementing ways to minimize the consequences if an attack occurs.

Reporting phase

Create report draft which will be sent to management for verification

Sending report document to customer in order to be adopted or to provide correction feedback

Remediation phase

Customer need to implement changes in order to fix findings provided within vulnerability/penetration test report

Verification of implemented changes

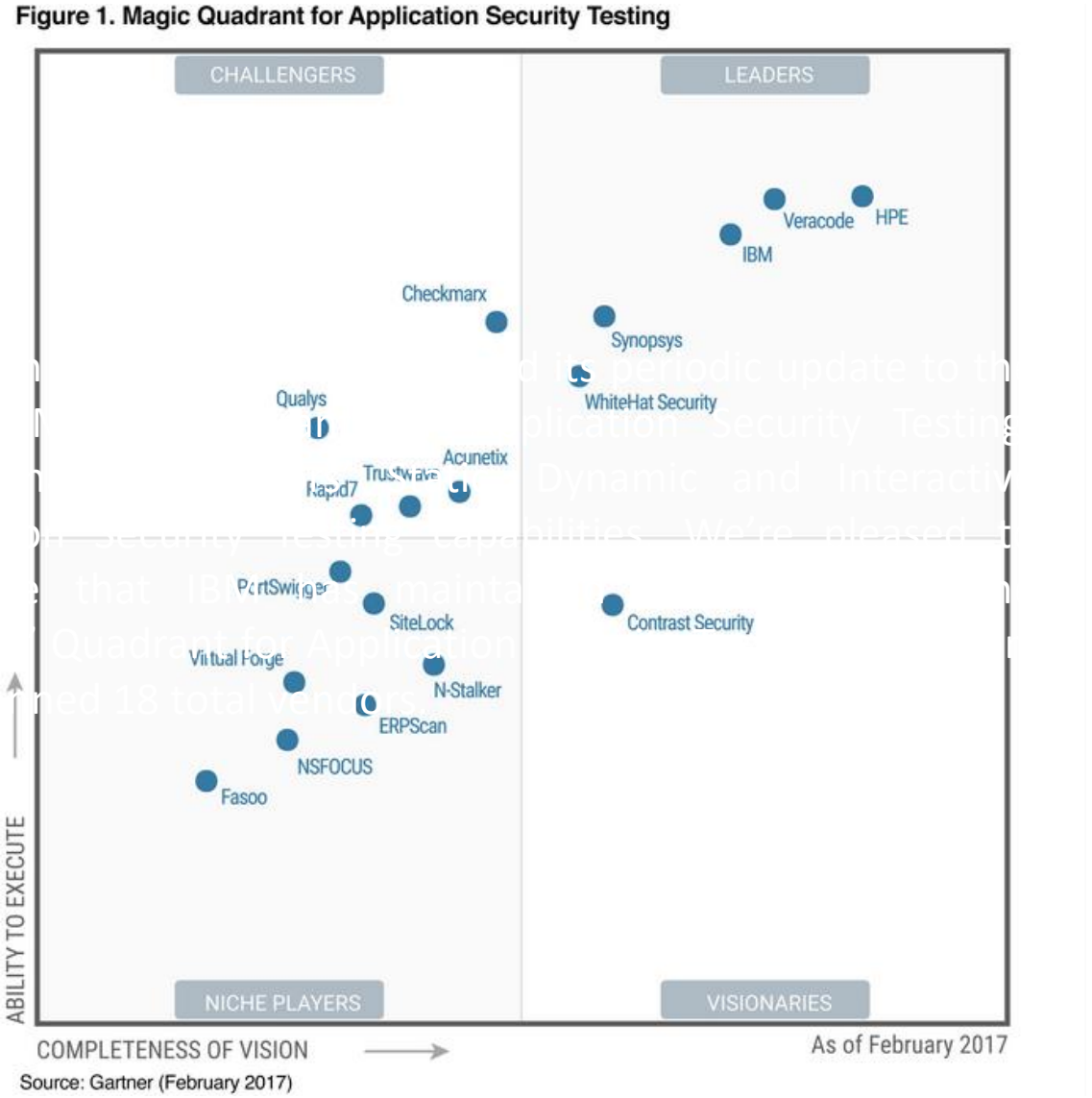
Test performing tools

Open Source

Licensed (Commercial tools)

Additional information

- https://securityintelligence.com/ibm-retains-leadership-position-in-2017-gartner-magic-quadrant-for-application-security-testing/



Questions and answers?