Paweł Rajba
pawel@cs.uni.wroc.pl
http://itcourses.eu/

Application Security
Verification

Agenda

- Introduction & terminology
- Why penetration tests?
- Type of test & methodology
- Overview for the application part
- Review of tools and frameworks
- Vulnerable applications
- WebGoat

Introduction & terminology

- Vulnerability scan
  - Review a vulnerabilities, potentials „ways" used by hacker
- Vulnerability management
  - Managing vulnerabilities, deciding what to do and how to prioritize
- Penetration test a.k.a. pentest
  - Attacking a system in order to see if it is possible to break into
  - May test different areas of environment: IDS, IPS, WAF, OS, App
    - Usually we consider **infrastructure part** and **application part**
  - Pentest requires permission from the system owner (!)
- Exploit
  - A piece of software that take advantage from a vulnerability
  - Usually deliver a payload to a target system
- Payload
  - A piece of software that grants access to the system after it has been exploited

Example

- Example 1
  - Vulnerability
    - Buffer overflow
  - Exploit
    - A memory address
  - Payload
    - A code to executed
- Example 2
  - Vulnerability
    - SQL Injection
  - Payload which can be used to exploit vulnerability
    - Prepared SQL statement

Why penetration tests?

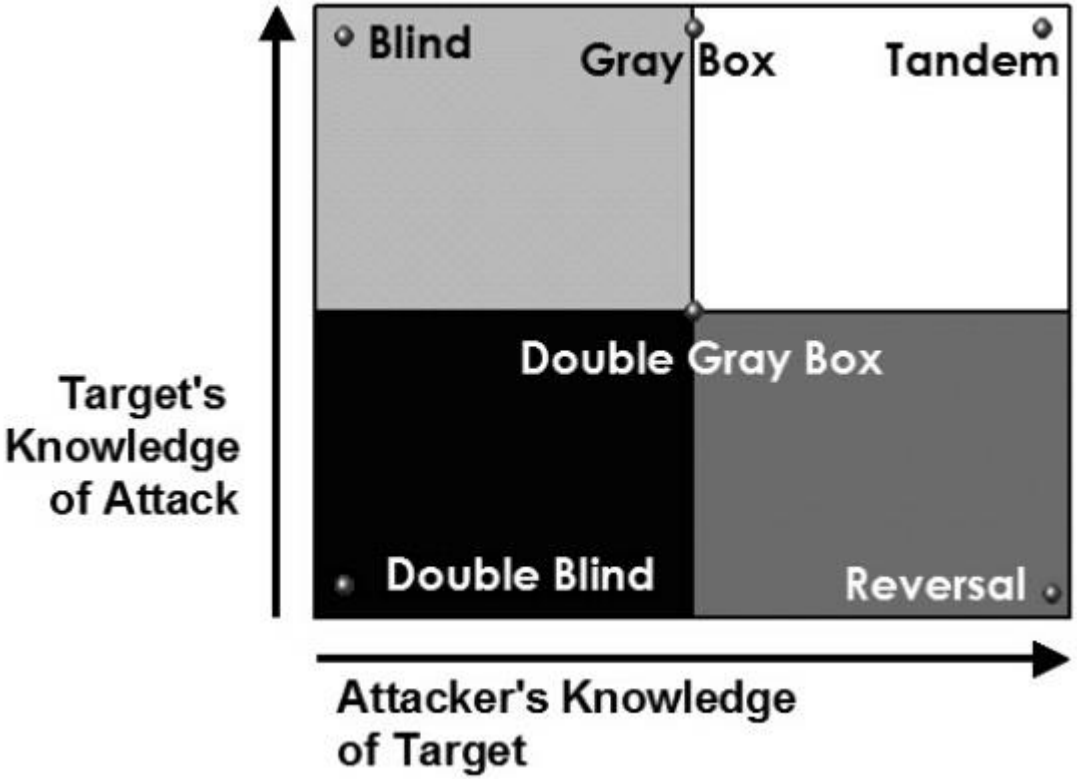
- Why to perform a penetration test
  - Prevent a data breach – find weakness and make system tight and better protected
  - Test security controls like firewalls, WAFs, IDSs, etc.
  - Ensure security level before put to production
  - Find areas where to put effort and money in future development
  - Compliance with certifications or other regulations
    - E.g. PCI DSS (https://www.pcisecuritystandards.org/)

Type of tests & methodologies

- Usually we consider 2 types of tests
  - Black box
  - White box
    - But it is not so easy…
- There are a lot of methodologies and implied types
  - OWASP Web Application Penetration Testing (Testing Guide)
  - Web Application Security Consortium Threat Classification (WASC-TC)
  - Penetration Testing Execution Standard (PTES)
  - Open Source Security Testing Methodology Manual (OSSTMM)
    - Read more: http://sekurak.pl/czego-ucza-metodologie-testow-penetracyjnych-cz-2/
      - Let's see this document

Type of tests & methodologies

- So, according to the OSSTMM we have the following quadrant:



Pentesting methodology

https://sekurak.pl/czego-ucza-metodologie-testow-penetracyjnych-cz-1/

Pentesting methodology

- Target Scoping
  - Define scope, methodology (black vs. white), who will know
- Informaction Gathering
  - Passive Info Gathering, from public sources: web browser, DNS, ...
- Target Discovery
  - Semi-passive info gathering
  - Active registration, starting to discover target, identifying networks, operating systems
- Enumerating Target
  - Scanning ports, IDS/IPS discovery, active search
- Vulnerability Mapping
  - Searching for vulnerabilities in common vulnerabilities databases, performing scans (blackbox, whitebox)
- Social Engineering (optional)
- Target Exploitation
- Privilege Escalation
- Maintaing Access (backdoors, cleaning after hack)
- Documentation and Reporting

https://sekurak.pl/czego-ucza-metodologie-testow-penetracyjnych-cz-1/

Overview for application part

- Main steps from application part perspective
  - Step 1
    - Initial activities
    - Test environment
  - Step 2
    - Automated scanning
  - Step 3
    - Verification of discovered vulnerabilities
    - False positive elimination
  - Step 4
    - Business Logic testing
    - Advanced manual exploitation
  - Step 5
    - Reporting
    - Mitigation plan

What if you have a lot of apps?

- Automation
- Applications Vulnerability Scans
  - HP Fortify, IBM AppScan
- Source code scan
  - During typing vs. during building
  - How it works?
- Potential scenario

Review of tools and frameworks

- A lot of rankings
  - http://projects.webappsec.org/w/page/13246988/Web%20Application%20Security%20Scanner%20List
  - https://www.owasp.org/index.php/Category:Vulnerability_Scanning_Tools
  - http://sectools.org/tag/web-scanners/
- Some more popular solutions
  - Metasploit, Burpsuit, Acunetix, HP WebInspect, IBM AppScan, Retina, QualysGuard, Arachni Scanner
- How to evaluate product? Short guide
  - http://projects.webappsec.org/w/page/13246986/Web%20Application%20Security%20Scanner%20Evaluation%20Criteria
- VERY IMPORTANT: Magic Quadrant from Gartner
  - http://securityintelligence.com/gartner-magic-quadrant-for-application-security-testing-2013/#.U44T5vl_sTs

Vulnerable applications

- Metasploitable
  - The whole virtual machine
  - Indended to test Metasploit, but can be used for other purposes
  - Available at:
    - https://information.rapid7.com/metasploitable-download.html
- OWASP Broken Web Applications Project
  - Another virtual machine
  - Available at:
    - https://www.owasp.org/index.php/OWASP_Broken_Web_Applications_Project
- Gruyere – application from Google University
  - Vulnerable application with exercises attached
  - Available at:
    - http://google-gruyere.appspot.com/

WebGoat

- A project from OWASP
- A set of exercises for playing with hacking
- Very good to understand weaknesses of apps
- Home page of the project
  - https://www.owasp.org/index.php/Category:OWASP_WebGoat_Project
- Bundled version
  - https://webgoat.googlecode.com/files/WebGoat-5.4-OWASP_Standard_Win32.zip
- In order to start:
  - Run webgoat
  - Go to http://localhost/WebGoat/attack
  - Put guest/guest credentials

ASVS

- Application Security Verification Standard
  - https://www.owasp.org/index.php/Category:OWASP_Application_Security_Verification_Standard_Project
- A checklist to verify a system
- A good starting point to develop your own „checklist”

References

- More references
  - Video about Arachni
    - http://www.securitytube.net/video/7024
  - Short introduction to penetration tests
    - https://community.rapid7.com/docs/DOC-2248
  - Introduction to Metasploit
    - http://www.irongeek.com/i.php?page=videos/metasploit-class