Penetration Testing

ICSS - DSV

Kerem Kocaer

bitsec

2010/04/14

1 EHLO

Kerem is:

- a graduate from ICSS
- a security consultant at Bitsec Consulting AB
- a security enthusiast

Kerem works with:

- **administrative security**
  security standards and frameworks, security requirements, policies, guidelines, etc…
- **technical security**
  penetration tests, vulnerability analysis, security review of products, infrastructures, web applications, etc..

2 AGENDA / GOALS

Today, we shall:

- define what a pentest is and is not
- discuss if / why one would need a pentest
- look at the different types of pentests
- go through the steps of a pentest
- experiment
- have fun

3 WHAT IS A PENETRATION TEST

- *"a method of **evaluating the security** of a computer system or network by **simulating an attack** from a malicious source"* – wikipedia

- Common confusion
  - **Vulnerability assessment:** scanning for vulnerabilities and filtering out false positives
  - **Penetration testing:** scanning for vulnerabilities and exploiting them

- **Goal:** Demonstrate how to bypass security controls.
- Simulating a real attack involves exploiting vulnerabilities to demonstrate that the security mechanisms actually fail.
- Penetration tests can involve "dangerous" attacks that can disrupt availability.
- Both provide a picture of the current state of security.

4 WHY WOULD YOU DO A PENTEST?

- Discover technical weaknesses and vulnerabilities before the bad guys
- Prove to Management that security should be taken seriously
- Test the effectiveness of current security mechanisms, see if they fulfill the requirements
- Discover problems in internal policies and procedures (when it comes to security administration), system administration, incident management, log management, etc...
- Reduce attack vectors
- Obtain higher assurance by continuously testing your systems

4 WHY WOULD YOU DO A PENTEST?

The Big Picture: Vuln. Assessments and Pen. Tests are …

- **compliance** requirements
  - ISO 27001 Req 15:2:2: Technical Compliance Checking
    "Information systems shall be regularly checked for compliance with security implementation standards."
  - PCI DSS Req 11: Regularly test systems and processes
    "Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification."
  - LGA Compliance Audit Questionnaire, Question 12.2.2
    - *"Has an external assessment of the Gaming System(s) vulnerabilities been conducted?"*
    - *"Is there an internal audit process to assess the level of technical compliance with operating procedures?"*

4 WHY WOULD YOU DO A PENTEST?

The Big Picture: Vuln. Assessments and Pen. Tests are …

- **risk analysis** activities
  - OCTAVE Phase 2: Identify Infrastructure Vulnerabilities
    "the outputs of Phase 2 document the present state of the computing infrastructure with respect to technological weaknesses that could be exploited by human threat actors."

4 WHY WOULD YOU DO A PENTEST?

The Big Picture: Vuln. Assessments and Pen. Tests are …

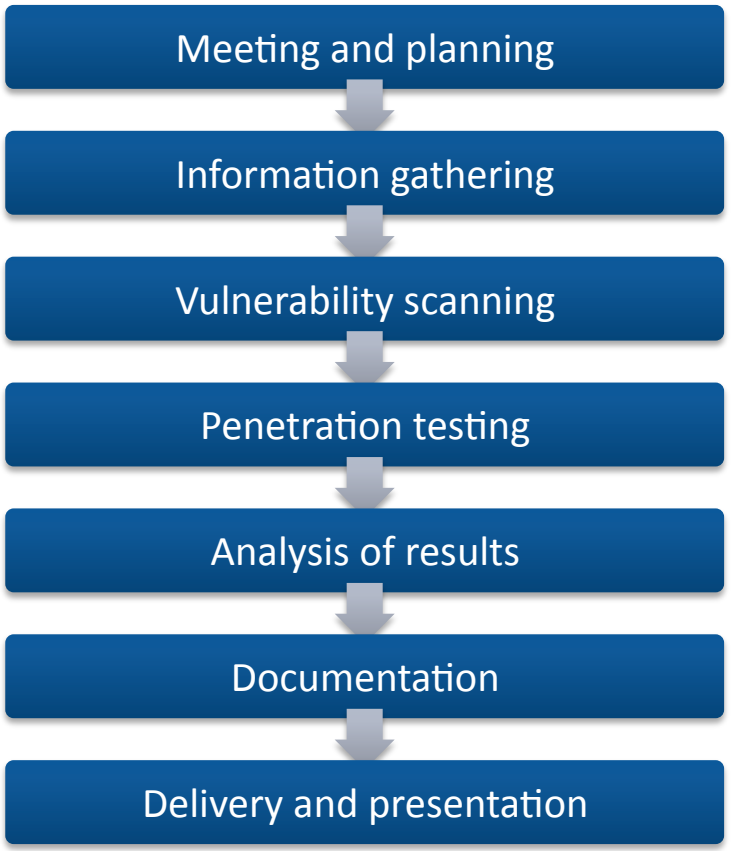
- **Common Criteria** security assurance components
  - CC Part 3 – Class AVA: Vulnerability Assessment
    "The evaluator shall conduct penetration testing, based on the identified potential vulnerabilities, to determine that the TOE is resistant to attacks performed by an attacker possessing Basic attack potential."

5 TYPES OF PENETRATION TESTS

- Black-box / Gray-box / White-box
- Destructive / Non-destructive
- Internal / External
- Target / environment
  - Infrastructure / Network
  - A single machine
  - Web application
- Wireless
- Social engineering

6 METHODOLOGY

A typical penetration testing project



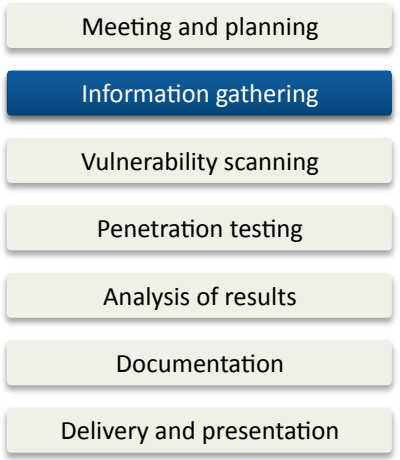
6.1 Meeting and planning

- **What type of penetration testing?**
  - Black-box or white-box?
  - External or internal?
  - To DoS or not to DoS?
  - Can I exploit humans?
- **What's the target?**
  - How many IPs?
  - Firewalls, IDSs, IPSs, ?
- **What are the objectives?**
- **What is the primary goal?**
- **Project planning**
  - How many hours?
  - How many consultants?
  - How much time for each step?
- **Coordinate with customer**

6.2 Information gathering

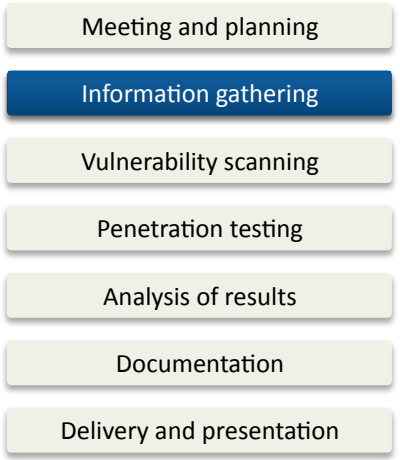
- **Goal:** Gather "enough" information about the target

- **Ask** the customer (previous phase)
- **Read** documentation and diagrams
- **Passive information gathering**
  - Internet service registration / WHOIS
  - Domain Name System
  - Website (public docs, robots.txt, error messages, ...)
  - Search engines
  - Emails
  - Online analysis websites (netcraft, archive)
  - Tools
    - Maltego
    - Metagoofil
    - Traceroute
    - ...
  - Passive sniffing (if hub)



6.2 Information gathering

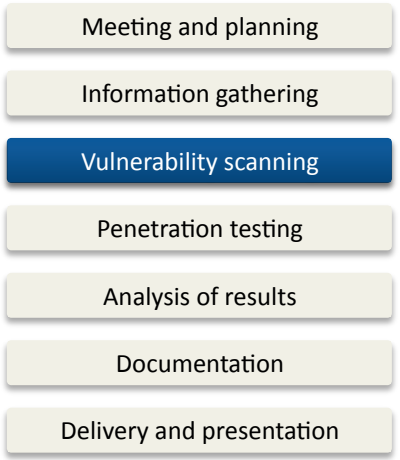
- **Active information gathering**
  - Spider
  - Check live systems – Host enumeration
  - Check open ports
  - Banner grab
  - Fingerprinting
  - OS detection
  - Network mapping – including FW, routers, etc.
  - Active sniffing – ARP poisoning – Switched environment
  - Social engineering



6.3 Vulnerability scanning

- **Goal:** Identify vulnerabilities that can potentially be exploited, based on information gathered in the previous phase

- **Manual search**
  - CVE database (nvd.nist.gov)
  - Security Focus (www.securityfocus.com)
  - Mailing lists such as Bugtraq / Full Disclosure (Insecure.org)
  - Google ...
- **Automated tools, such as:**
  - Nessus
  - Qualys
  - (Core Impact)
- **In web applications:**
  - WebInspect
  - Paros / Burpsuite / WebScarab
  - Fuzzing
  - Nikto

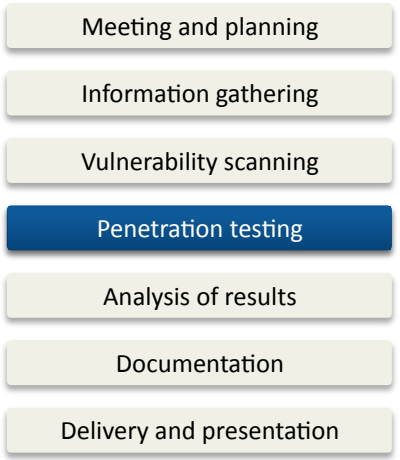


6.4 Penetration testing

- **Time to have some fun…**

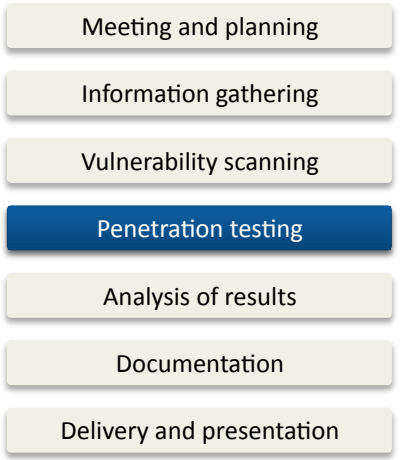
- **Goal:** Exploiting the vulnerabilities that were previously identified, in order to:
  - get access to the target machine,
  - retrieve confidential information,
  - render service unavailable,
  - launch further attacks, etc…

- **Steps:**
  - Penetrate
  - Escalate privilege
  - Maintain access
  - Clean up



6.4 Penetration testing

- **Penetrate!**
  - Web search & compile
  - Core Impact-like solutions
  - Metasploit
- **Escalate!**
  - Crack admin/root password, with
  - Rainbow tables
  - Dictionnary attack
  - Brute-force
- **Maintain!**
  - Rootkits
  - Trojans
- **Clean up!**
  - Disable auditing
  - Clean logs



6.4 Penetration testing

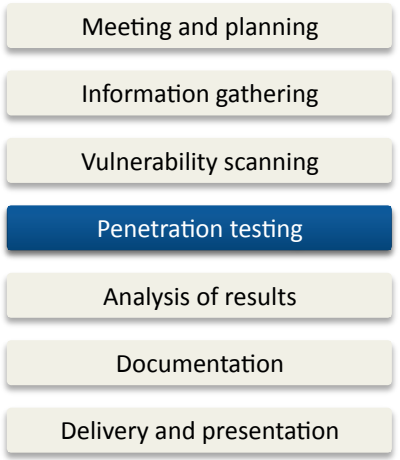
- **Denial of Service**

- **Goal:** Make a resource unavailable to its intended users
- **Warning:** Be sure the customer is cool with that!

- Some scans and exploits can cause DoS. Include or exclude them according to the agreement with the customer.

- **DoS attacks**
  - Smurf
  - Fraggle
  - SYN flood
  - Teardrop
  - Ping of Death
  - ..

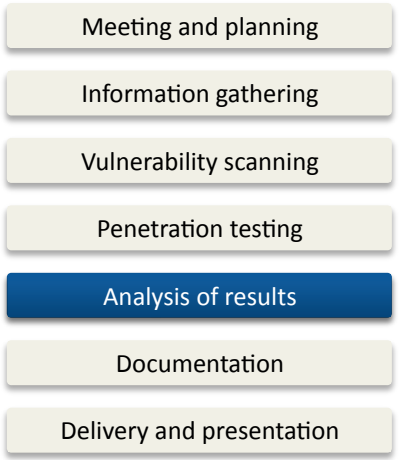
- **DDoS !**



6.5 Analysis of results

- Since we're the good guys, we don't go further than proving that the vulnerabilities are exploitable

- **Steps:**
  - Stop
  - Take a deep breath
  - Analyse what a malicious hacker could do with the identified exploit(s)
  - Check if the project goals are met
  - Proceed to documentation



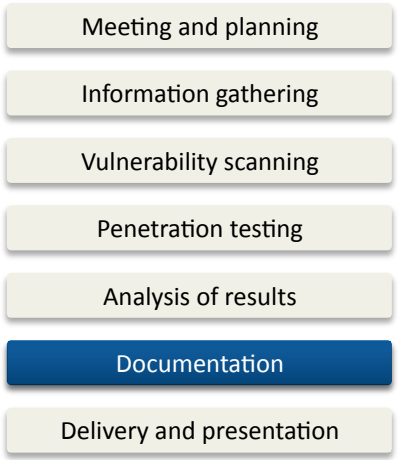
6.6 Documentation

- Probably the most boring but the most important step
- Do not underestimate the time needed for documentation

- **Goal:** Classify and report identified risks

- **Classification:**
  - High risk
  - Medium risk
  - Low risk
  - Information

- **Important sections:**
  - Executive summary
  - Purpose, scope, limitations
  - Risks, weaknesses, vulnerabilities
  - Risk remediation, recommentations
  - Appendices with logs and screenshots



6.7 Delivery and presentation

- Present the results during a meeting with the customer
- Adjust the level of technical detail according to the audience
- Answer questions
- Receive feedback

7 SOCIAL ENGINEERING

- What's the weakest link?

- Feelings
- Phishing

- *Demo: nasty PDF*

8 WIRELESS

- A whole big topic of its own,
  - WEP
  - WPA/2
  - Wardriving

- *Demo: nasty AP*

9 TOOLS

- To start with, you can play with:
  - BackTrack
  - Nmap
  - Nessus
  - Metasploit
  - WebScarab
  - Wireshark
- You can practice with:
  - De-ICE PenTest Discs
  - Metasploit Unleashed
  - WebGoat
  - HackThisSite
  - Hax.tor.hu
  - Damn Vulnerable Linux / WebApp

- Build your own lab..
- Test your own network..

10 RESOURCES

- Check these websites:
  - milw0rm
  - Security Focus
  - insecure.org
  - packetstormsecurity.org
  - InfoSecNews (maillist / RSS)
  - OWASP
  - Dark Reading
  - Blogs

QUESTIONS