ENGENSEC
Educating the Next generation experts in Cyber Security

Tempus

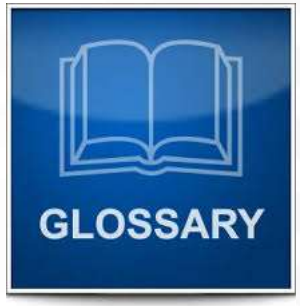
The project has been funded by the European Commission. The Education, Audiovisual and Culture Executive program (EACEA), TEMPUS IV. The content of this presentation reflects the opinion of the author.

Module 1. Introduction to the penetration testing

Penetration testing course

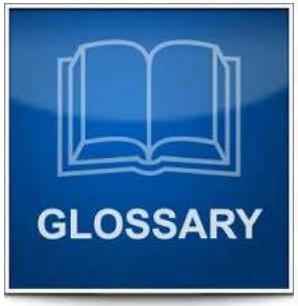
Some terms used by hackers

- Threat
- Asset
- Vulnerability
- Control
- Risk



Basic security terms

- Exploit
- Payload
- Zero day
- Advanced persistent threat
- Watering hole



Types of hackers

White

Grey

Black

What does real hacker do?

What we can take for our purposes?

- Model of hacker
- Methods
- Objectives
- Tools

Model of the hacker

- Knowledge of hacking methods
- Knowledge of hacking tools
- Black market connections
- Ability to develop exploits and hack tools
- Ability to search for zero-day vulnerabilities

What does ethical hacker use?

- Knowledge of hacking methods
- Knowledge of hacking tools
- Black market connections
- Ability to develop exploits and hack tools
- Ability to search for zero-day vulnerabilities

Objectives

Administrative access to main systems

Access to the specific information (for example, salaries of top-managers)

Ethical hacking set of tools

OR

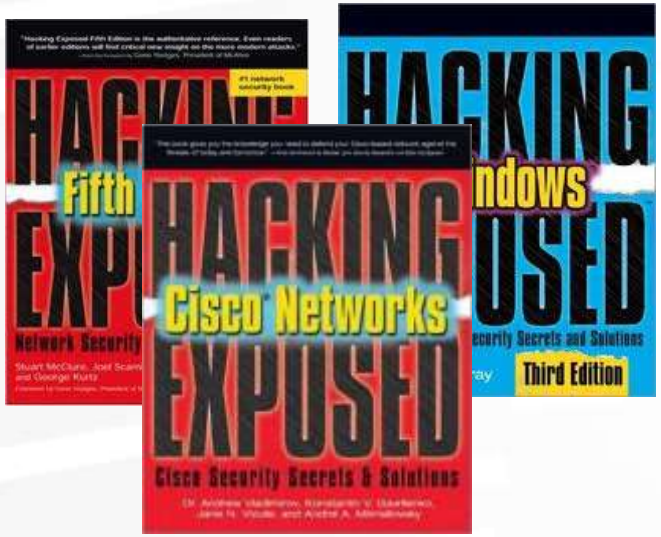
Linux
Windows + Hack tools installed

Live CD or Live USB:
Linux + Hack tools
Example: Kali Linux

Hack tools

- Standard network utilities for work with DNS, whois, ICMP, etc.
- Port scanners
- Vulnerability scanners
- Swiss knife: Netcat
- Exploit frameworks
- …

Methodologies



Security testing approaches

Classical penetration test

Automated vulnerability assessment

Configuration review

Combined approach

Classical penetration test

- Imitation of real hacking – we look for some critical vulnerabilities which could lead to gain access to the system or specific data.
- More art than audit. Quality is dependent upon level of penetration tester
- Usual result: couple critical vulnerabilities which were exploited
- High risk of system crash during the exploitation

Vulnerability assessment

- Use of vulnerability scanners
- Quality is dependent upon used tool
- Usual result: a lot of vulnerabilities of different criticality level
- Medium risk of system crash during the exploitation

Configuration review

- Check of system settings against special checklists (NIST, Center of Internet Security).
- Usual result: many vulnerabilities of different criticality level
- Low risk of system crash during the exploitation

Checklists for configuration review

http://benchmarks.cisecurity.org/downloads/

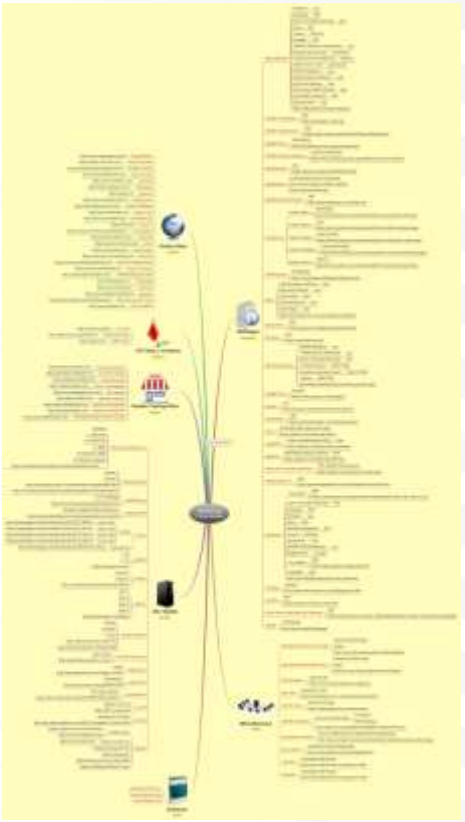
http://web.nvd.nist.gov/view/ncp/information

Penetration testing project management

- Agree list of IP addresses with client: critical/non-critical
- Approach negotiation
- Getting approvals from involved third parties (network providers, hosting providers, etc)
- Communication with client's IT-security officer during exploitation
- Reporting

Home hacking laboratory

- Online sites
- Operating systems with vulnerable software installed
- Special developed web-applications



Mindmap with such things: http://www.amanhardikar.com/mindmaps/Practice.html

Kali Linux


KALI LINUX
Boot menu
Live (686-pae)
Live (686-pae failsafe)
Live (forensic mode)
Install
Graphical install
Install with speech synthesis
Press ENTER to boot or TAB to edit a menu entry

Key important audit principle

Not documented – not done

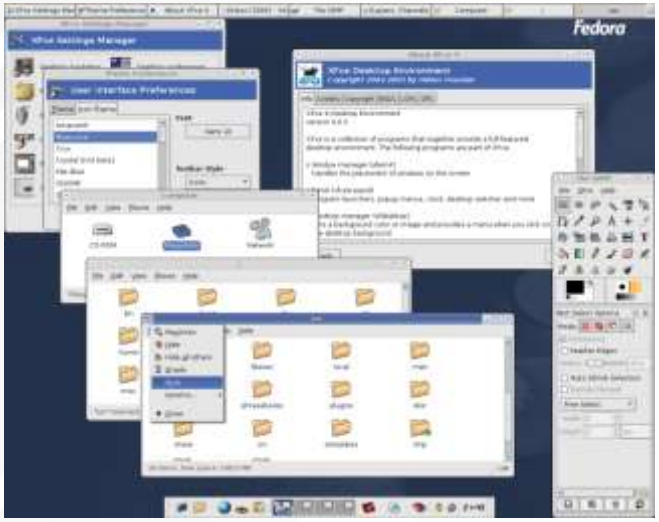
Different types of audit reports

1. Successful attack scenario. It's useful if the main objective of the testing was to demonstrate the possibility of system hacking.
2. Finding – Risk – Recommendation. It's useful if the main objective was to discover maximum vulnerabilities for remediation.

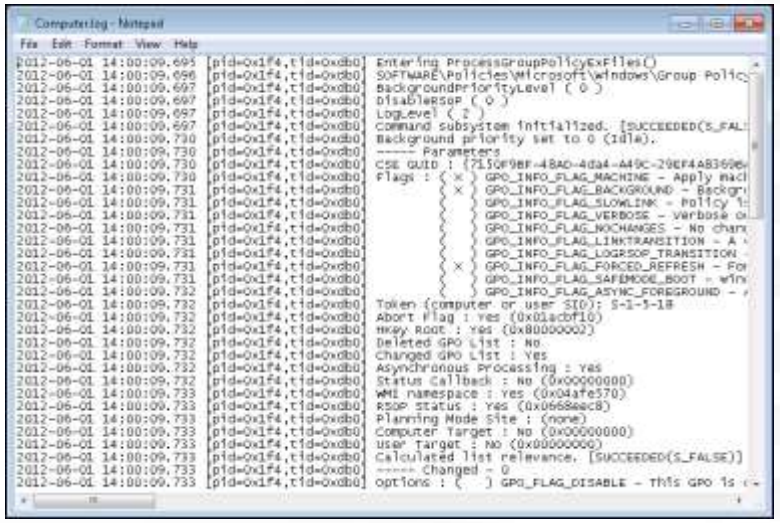
Documenting during the testing

- Objectives:
  - Proof of conducting particular test
  - Evidence of possibility of vulnerability exploitation
  - Information collection for further analysis.

Usual types of evidences



Screenshots



Utility logs

Main documenting problem

We have to link particular IP address and information from reports of different hack tools.

111.222.333.444

Port scanner: open ports, versions of network services

Vulnerability scanner: discovered vulnerabilities

Tool for password bruteforcing: cracked passwords

Exploitation framework: Was exploitation successful?

Best documenting tools ;)

LibreOffice
The Document Foundation