Penetration Testing

A brief introduction to Penetration Testing

Sergiu Terman

CVUT

June 14, 2014

Things we'll cover today

Things we'll cover today

- What is a pentest

Things we'll cover today

- What is a pentest
- Terminology

Things we'll cover today

- What is a pentest
- Terminology
- Penetration Test Execution Standards

Things we'll cover today

- What is a pentest
- Terminology
- Penetration Test Execution Standards
- Tools & utilities

Penetration Test (pentest)

- Attacking a computer system to find its vulnerabilities
- Many times resumes to gaining access to the system

Why need for a pentest?

Why need for a pentest?

- Its one of the most effective ways to identify weaknesses

Why need for a pentest?

- Its one of the most effective ways to identify weaknesses
- A pentester has to think like a real world (black hat) cracker, so a pentest could reflect the real life behaviour of an assault

Why need for a pentest?

- Its one of the most effective ways to identify weaknesses
- A pentester has to think like a real world (black hat) cracker, so a pentest could reflect the real life behaviour of an assault

Why need for a pentest?

- Its one of the most effective ways to identify weaknesses
- A pentester has to think like a real world (black hat) cracker, so a pentest could reflect the real life behaviour of an assault
- He has to discover means in which a cracker might compromise the security and deliver damage to the organization

Types of pentests

Types of pentests

- Overt pentest: (also called white box)

Types of pentests

- Overt pentest: (also called white box)
  - The pentester has insider knowledge: the system, its infrastructure, etc. (used when time is limited.)

Types of pentests

- Overt pentest: (also called white box)
  - The pentester has insider knowledge: the system, its infrastructure, etc. (used when time is limited.)
- Covert pentest (also called black box)

Types of pentests

- Overt pentest: (also called white box)
  - The pentester has insider knowledge: the system, its infrastructure, etc. (used when time is limited.)
- Covert pentest (also called black box)
  - The pentester has basic or no information whatsoever, except the company name

Terminology

Terminology

- Exploit
  - Taking advantage of a flaw within the attacked target. (i.e. SQL injection, configuration errors.)

Terminology

- Exploit
  - Taking advantage of a flaw within the attacked target. (i.e. SQL injection, configuration errors.)
- Payload
  - Code to be executed on the attacked target. (i.e. and usually a reverse shell or bind shell.)

Terminology

- Exploit
  - Taking advantage of a flaw within the attacked target. (i.e. SQL injection, configuration errors.)
- Payload
  - Code to be executed on the attacked target. (i.e. and usually a reverse shell or bind shell.)
- Shellcode
  - A piece of code to be run after exploitation, typically written in machine code, usually spawns a shell (hence the name)

Terminology

- SERGIU TERMAN <3