# 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

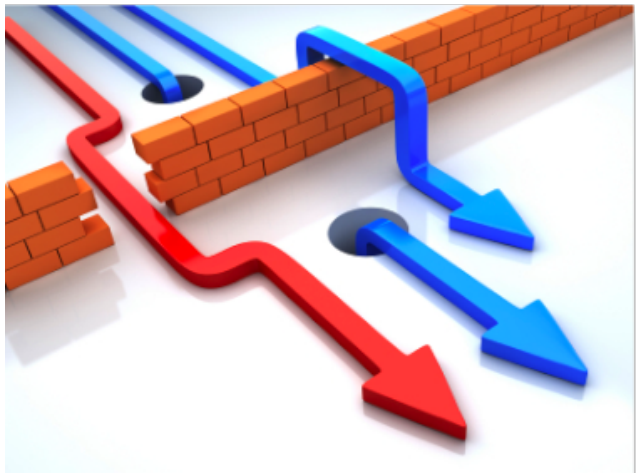
# Things we'll cover today

- 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

- Vulnerability scanners

# Terminology

- Vulnerability scanners
  - Automated tools to identify known flaws

# Terminology

- Vulnerability scanners
  - Automated tools to identify known flaws
  - First of all - fingerprinting target OS, also its services

# Terminology

- Vulnerability scanners
  - Automated tools to identify known flaws
  - First of all - fingerprinting target OS, also its services
  - Very important in the intelligence gathering step

# Terminology

- Vulnerability scanners
  - Automated tools to identify known flaws
  - First of all - fingerprinting target OS, also its services
  - Very important in the intelligence gathering step
  - Can provide comprehensive vulnerability reports, thus replacing some missing experience

# Terminology

- Vulnerability scanners
  - Automated tools to identify known flaws
  - First of all - fingerprinting target OS, also its services
  - Very important in the intelligence gathering step
  - Can provide comprehensive vulnerability reports, thus replacing some missing experience
  - e.g. Retina, Nessus, NeXpose, OpenVAS, Vega, etc

# PTES (Penetration Testing Execution Standard)

# PTES (Penetration Testing Execution Standard)

- Pre-engagement interactions. (...and coffee, probably)

# PTES (Penetration Testing Execution Standard)

- Pre-engagement interactions. (...and coffee, probably)
- Intelligence gathering. (passive & active)

# PTES (Penetration Testing Execution Standard)

- Pre-engagement interactions. (...and coffee, probably)
- Intelligence gathering. (passive & active)
- Threat modeling

# PTES (Penetration Testing Execution Standard)

- Pre-engagement interactions. (...and coffee, probably)
- Intelligence gathering. (passive & active)
- Threat modeling
- Vulnerability analysis

# PTES (Penetration Testing Execution Standard)

- Pre-engagement interactions. (...and coffee, probably)
- Intelligence gathering. (passive & active)
- Threat modeling
- Vulnerability analysis
- Exploitation

# PTES (Penetration Testing Execution Standard)

- Pre-engagement interactions. (...and coffee, probably)
- Intelligence gathering. (passive & active)
- Threat modeling
- Vulnerability analysis
- Exploitation
- Post exploitation

# PTES (Penetration Testing Execution Standard)

- Pre-engagement interactions. (...and coffee, probably)
- Intelligence gathering. (passive & active)
- Threat modeling
- Vulnerability analysis
- Exploitation
- Post exploitation
- Reporting

# Tools & utilities

# Tools & utilities

- Operating systems

# Tools & utilities

- Operating systems
  - Kali Linux (formerly BackTrack) - based on Debian
  - Pentoo - based on Gentoo
  - WHAX - based on Slackware

# Tools & utilities

- Operating systems
  - Kali Linux (formerly BackTrack) - based on Debian
  - Pentoo - based on Gentoo
  - WHAX - based on Slackware
- Frameworks

# Tools & utilities

- Operating systems
  - Kali Linux (formerly BackTrack) - based on Debian
  - Pentoo - based on Gentoo
  - WHAX - based on Slackware
- Frameworks
  - Metasploit
  - w3af

# Tools & utilities

- Operating systems
  - Kali Linux (formerly BackTrack) - based on Debian
  - Pentoo - based on Gentoo
  - WHAX - based on Slackware
- Frameworks
  - Metasploit
  - w3af
- Tools

# Tools & utilities

- Operating systems
  - Kali Linux (formerly BackTrack) - based on Debian
  - Pentoo - based on Gentoo
  - WHAX - based on Slackware
- Frameworks
  - Metasploit
  - w3af
- Tools
  - nmap, netcat, John the Ripper
  - tcpdump, Wireshark, upx, etc

# A few words on Metasploit

# A few words on Metasploit

- Written entirely in Ruby

# A few words on Metasploit

- Written entirely in Ruby
- Cross-platform

# A few words on Metasploit

- Written entirely in Ruby
- Cross-platform
- As of today, it contains about 1400 different exploits for Windows, Linux, OS X, iOS & Android, etc

# A few words on Metasploit

- Written entirely in Ruby
- Cross-platform
- As of today, it contains about 1400 different exploits for Windows, Linux, OS X, iOS & Android, etc
- Uses the modular approach, which makes possible combining different exploits with different payloads

# A few words on Metasploit

- Written entirely in Ruby
- Cross-platform
- As of today, it contains about 1400 different exploits for Windows, Linux, OS X, iOS & Android, etc
- Uses the modular approach, which makes possible combining different exploits with different payloads
- Highly extensible & reusable

# A few words on Metasploit

- Written entirely in Ruby
- Cross-platform
- As of today, it contains about 1400 different exploits for Windows, Linux, OS X, iOS & Android, etc
- Uses the modular approach, which makes possible combining different exploits with different payloads
- Highly extensible & reusable
- Has several useful interfaces (cli, console, armitage)

# A few words on Metasploit

- Written entirely in Ruby
- Cross-platform
- As of today, it contains about 1400 different exploits for Windows, Linux, OS X, iOS & Android, etc
- Uses the modular approach, which makes possible combining different exploits with different payloads
- Highly extensible & reusable
- Has several useful interfaces (cli, console, armitage)
- Free of charge, but commercial versions are also available

# References


- Kennedy D., OGorman J., Kearns D., Aharoni M. - Metasploit. The Penetration Testers Guide. (2011)
- Offensive Security - Metasploit Unleashed `http://www.offensive-security.com/metasploit-unleashed`
- Penetration Testing Execution Standard `http://www.pentest-standard.org/`
- Nmap `http://nmap.org/`
- Metasploit `http://www.metasploit.com/`

# Thanks for watching

"Try Harder" *Offensive Security*