

# Workshop Pentesting

---

7ª edição Comunica+  
24/10/2017

Pedro Queirós, Cybersecurity Engineer

**multicert**

Engineering for digital security



# Summary

---

- What is a pentest?
- Planning and preperation
- Information gathering
- Vulnerability detection
- Social Engineering
- Exploitation
- Analysis and reporting

# What is a pentest?

---

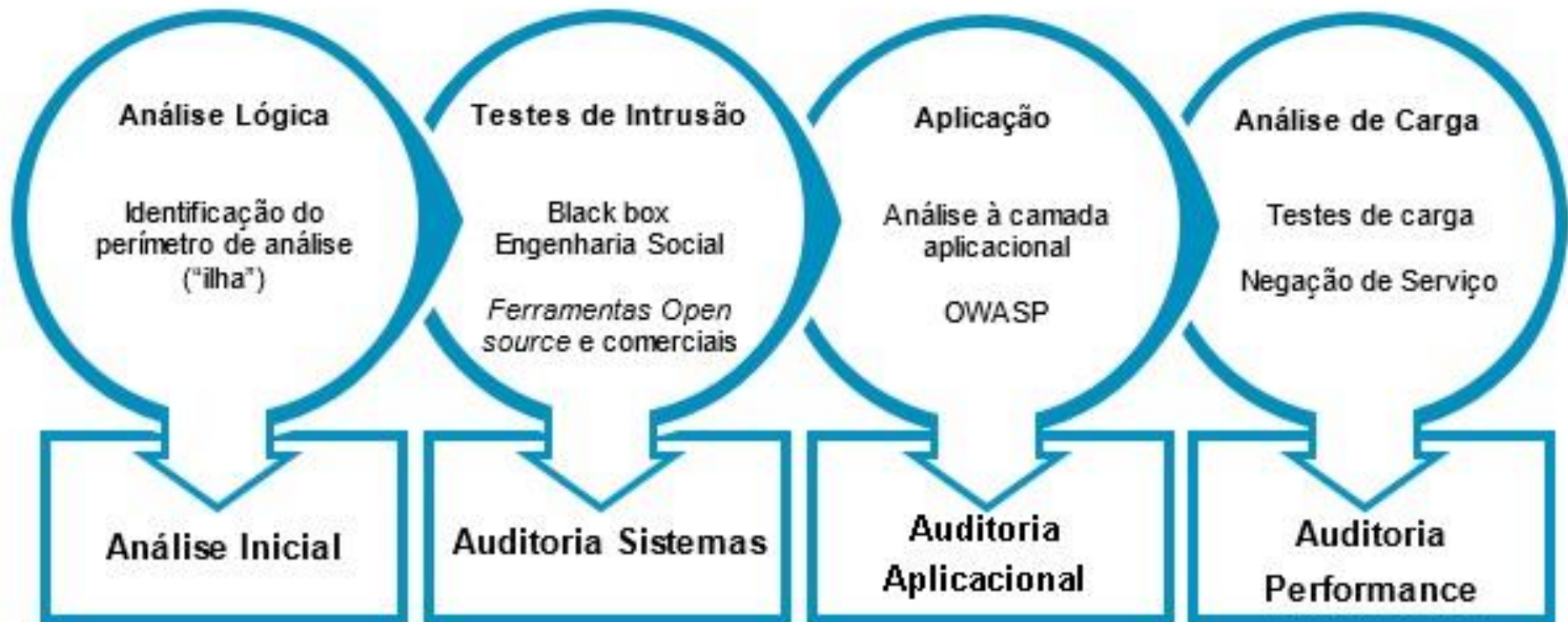
- Authorized simulated attack on a computer system.
- Primary goal focused on finding vulnerabilities that could be exploited.
- Inform the client about the vulnerabilities **along with recommended mitigation strategies.**

# What is a pentest?

---

- **White box**
  - Testers are given full disclosure about the network prior to the penetration testing. This will include IP addresses, source code, network protocols, diagrams, etc...
- **Black box**
  - Testers are given very little or no information prior to the penetration test.

# Planning and preperation



[https://www.owasp.org/index.php/Penetration\\_testing\\_methodologies](https://www.owasp.org/index.php/Penetration_testing_methodologies)

# Information gathering

---

- The first phase in security assessment.
- Focused on collecting as much information as possible about a target application
- Information Gathering is the most critical step of an application security test



# Information gathering

Área Cliente/Parceiro
Apoio a Cliente
Contactos
Loja Online
PT
EN

multicert
Produtos
Sectores e áreas de atuação
Sobre nós

You Tube
in

## engenheiro de software sênior (m/f)

Ao profissional selecionado ser-lhe-á dada a oportunidade de participar em projetos aliciantes com projeção nacional e internacional.

No âmbito destes projetos, deverá participar no processo de desenvolvimento de software em vigor na organização, observando as boas práticas instituídas, além de constituir um reforço da equipa de desenvolvimento.

### O que procuramos

- Licenciatura Pré-Bolonha ou Mestrado Pós-Bolonha em Eng<sup>a</sup> Informática, Eng<sup>a</sup> de Sistemas ou similar
- Competências técnicas decisivas: JSE/JEE, WebServices, SQL, XML, Arquiteturas de Software, UML
- Valoriza-se conhecimentos em: PKI, EJB/Hibernate, testes unitários (JUnit, TestNG), EIA, Linux, Jboss, Tomcat, Postgresql, SpringFramework, Ant, Maven, JavaScript, HTML5
- Capacidade de organização e resistência ao stress
- Elevada capacidade de aprendizagem
- Boa capacidade de comunicação e trabalho em equipa
- Forte sentido de responsabilidade e ética profissional
- Experiência mínima superior a 3 anos

# Information gathering

- Harvester

```
root@kali:~# theharvester -d hackingloops.com -b all -f vanshit
*****
* TheHarvester Ver. 2.2a *
* Coded by Christian Martorella *
* Edge-Security Research *
* cmartorella@edge-security.com *
*****

Full harvest..
[-] Searching in Google..
Searching 0 results...
Searching 100 results...
```

- Metagoofil

```
root@kali:~# metagoofil -d -t doc -l 200 -n 50 -o /root/
-f /root/file.html
[+] List of users found:
-----
Lydia Jallow
M. Renee Brown
Renee Brown Doug
```



# Information gathering

---

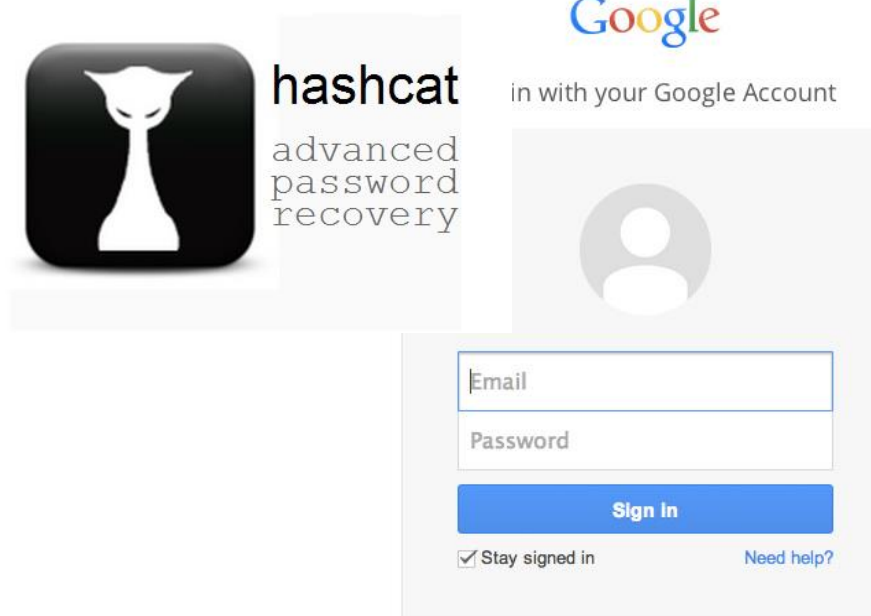
- Good old Google!!
  - `site:linkedin.com inurl:pub "at <organisation name>"`
  - `site:facebook.com "<search terms>"`
  - `site:twitter.com "<search terms>"`
- Dumpster diving



# Information gathering



';--have i been pwned?

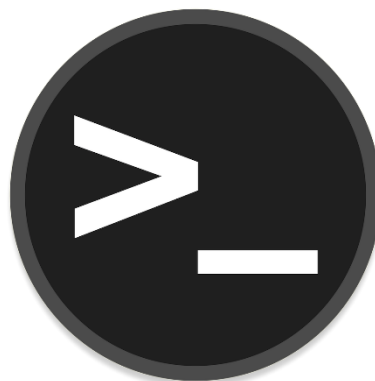


# Information gathering

---



# Vulnerability detection



When everything else fails



# Social engineering

“What I found personally to be true was that it's easier to manipulate people rather than technology” - *Kevin Mitnick*

“There is no technology today that cannot be defeated by social engineering.” - *Frank Abagnale*

## Social engineering types

- *Quid pro Quo*
- Phishing
- Baiting
- Pretext
- Diversion

# Social engineering

---



All i need is a USB flash drive...

“... I forgot my CV, but i have it here in this USB drive!”



# Social engineering

Humm... quem fez isto cometeu um erro n00b...  
Seguem contactos de quem criou o domínio:

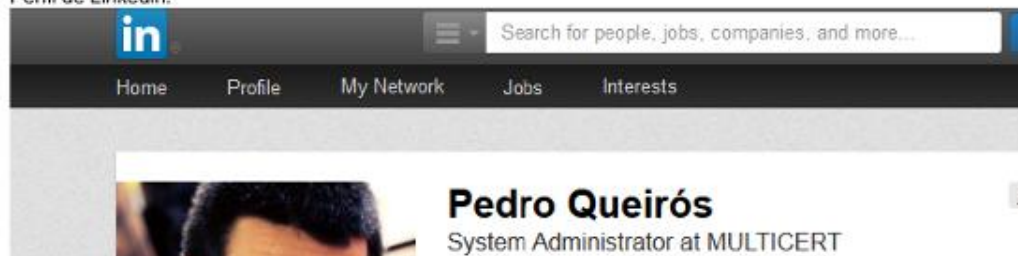
istrant Contact Information:

Name	Pedro Queiros
Organization	
Address	
City	
State / Province	--
Postal Code	
Country	PT
Phone	
Email	

Foto da casa dele..



Perfil de LinkedIn:



# Exploitation

---

- Focuses solely on establishing access to the client system, bypassing security restrictions.
- Identify the main entry point into the organization and to identify high value target assets

# Exploitation

---

- Physical Access
  - Attempting to circumvent physical security controls and gain unauthorized access.
- Proximity Access (WiFi)
  - Regardless of protocol, there are a number of attacks available for WEP, WPA, WPA2, EAP-FAST, EAP-LEAP, and other avenues
- Traffic Analysis
  - Identify what type of information is being sent and be able to understand and manipulate that traffic.

# Exploitation

---

Metasploit Framework, a tool for developing and executing exploit code against a remote target machine



# Exploitation

Metasploit Framework, a tool for developing and executing exploit code against a remote target machine

```
root@bt:/pentest/exploits/framework3# ./msfconsole

      o
      8      o  o
      8      8
ooYoYo. .oPYo. o8P .oPYo. .oPYo. .oPYo. 8 .oPYo. o8 o8P
8' 8 8 8oooo8 8 .oooo8 Yb.. 8 8 8 8 8 8 8
8 8 8 8. 8 8 8 'Yb. 8 8 8 8 8 8 8
8 8 8 `Yooo' 8 `YooP8 `YooP' 8YooP' 8 `YooP' 8 8
.....:8.....:
:8:
:

=[ metasploit v3.7.0-dev [core:3.7 api:1.0]
+ -- ==[ 675 exploits - 352 auxiliary
+ -- ==[ 217 payloads - 27 encoders - 8 nops
      =[ svn r12286 updated today (2011.04.09)

msf > █
```

# Analysis and Reporting

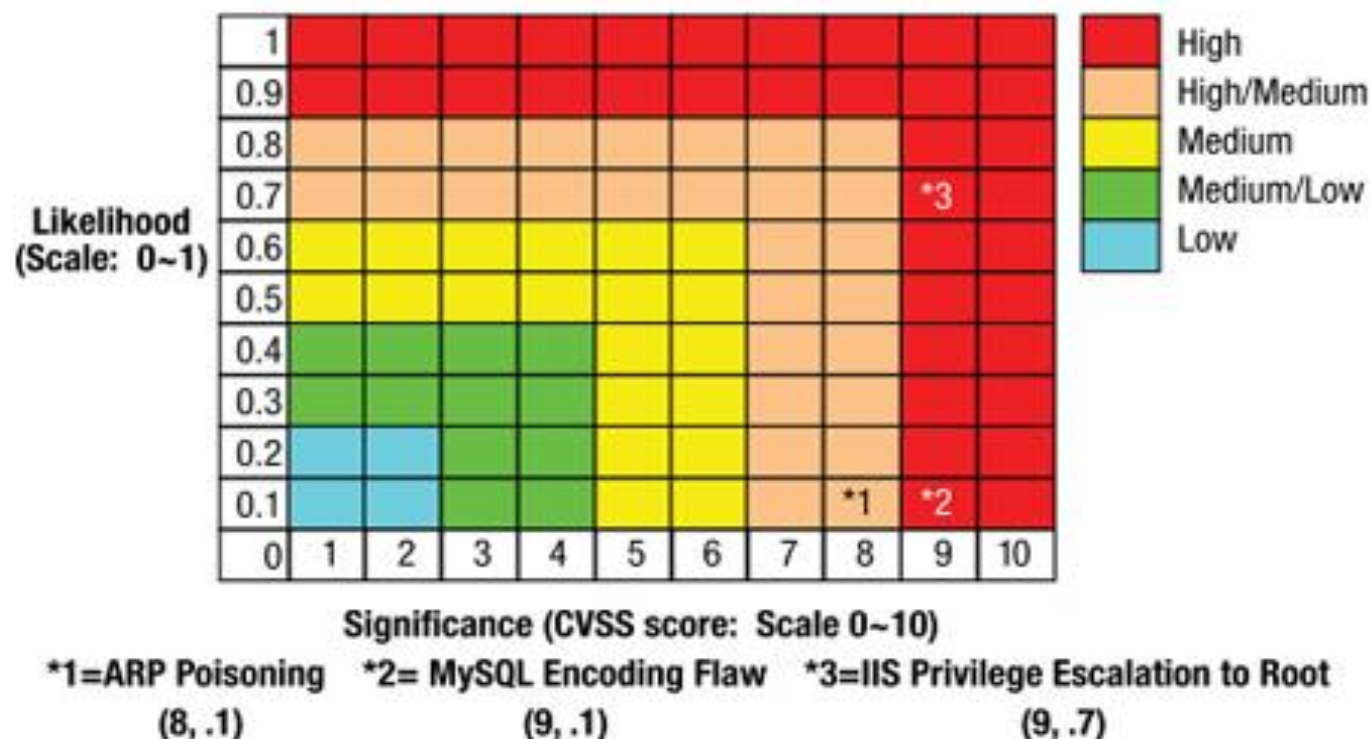
---





# Analysis and Reporting

- Should provide a high level of understanding.
- Structure should make it easy for a non technical user to understand what was done.
- Risk profile.



# Thank you!

## Questions?

Pedro Queirós  
pedro.queiros@multicert.com

**multicert**

Engineering for digital security

---

Lagoas Park, Edifício 3, Piso 3,  
2740-266 Porto Salvo  
Oeiras - Portugal  
Tel.: +351 217 123 010  
Fax: +351 217 123 011

Avenida Sidónio Pais, 379  
Edifício Hoechst B, Piso1, Sala 5  
4100-468 Porto - Portugal  
Tel.: +351 223 391 810  
Fax: +351 223 391 811

**[www.multicert.com](http://www.multicert.com)**