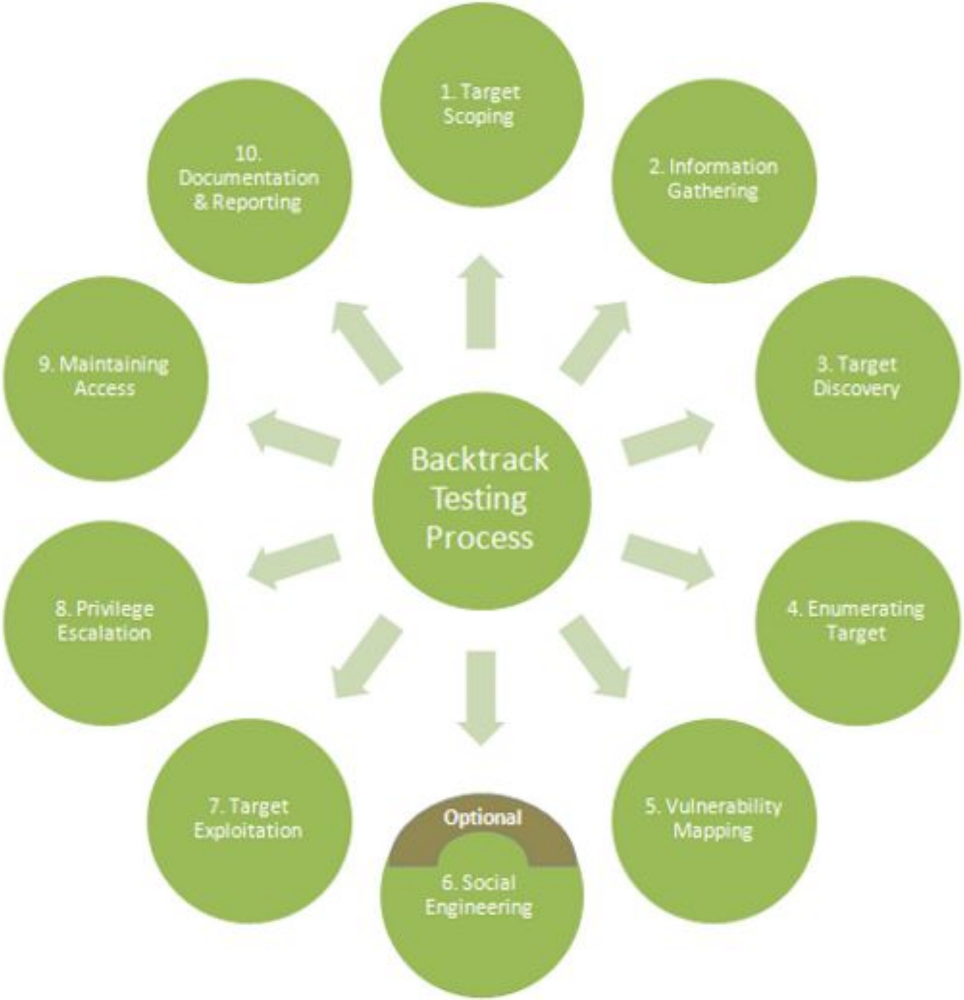
Web Pentest 101

from abrasax to /dev/null

0x01: Pentest Introduction

By the attacker side

- The pentest concept
- The practice
  - Enumeration
  - Exploitation
    - Web hacking
  - Priv Escalation
- Hands on



Backtrack Testing Process

1. Target Scoping

2. Information Gathering

3. Target Discovery

4. Enumerating Target

5. Vulnerability Mapping

Optional

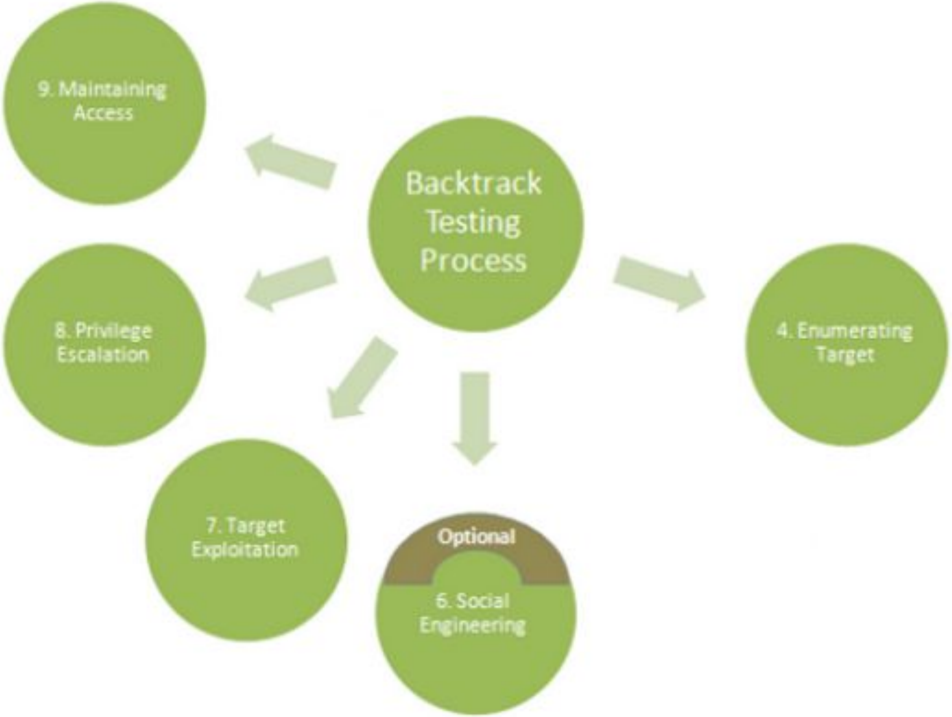
6. Social Engineering

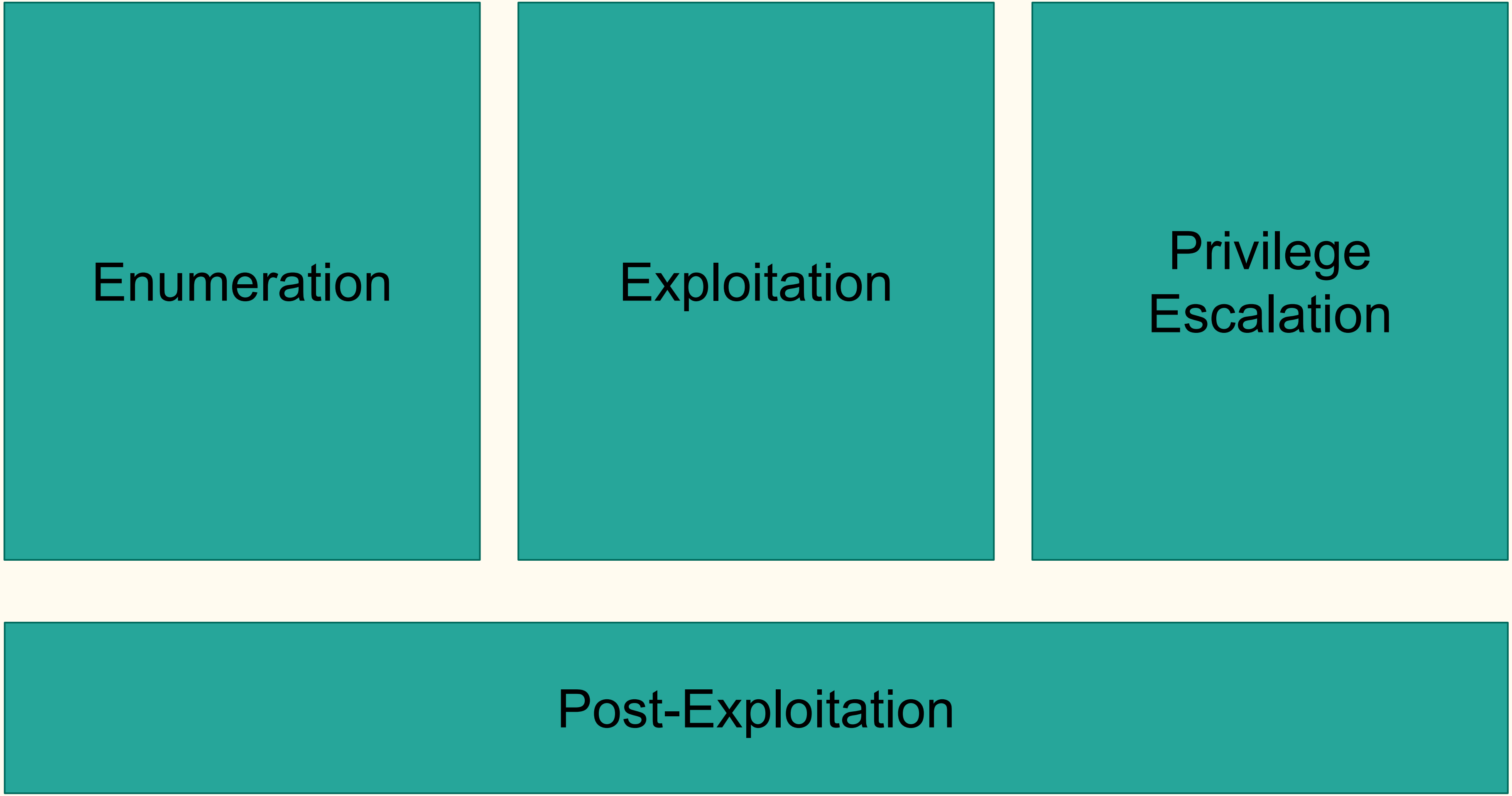
7. Target Exploitation

8. Privilege Escalation

9. Maintaining Access

10. Documentation & Reporting


Backtrack Testing Process
9. Maintaining Access
8. Privilege Escalation
7. Target Exploitation
Optional
6. Social Engineering
4. Enumerating Target

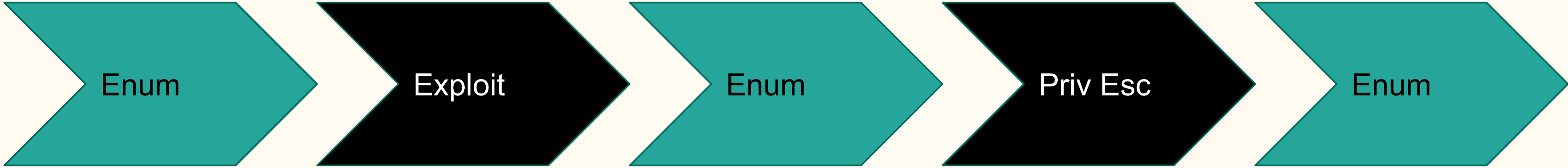


Enumeration

Exploitation

Privilege Escalation

Post-Exploitation



Enum

Exploit

Enum

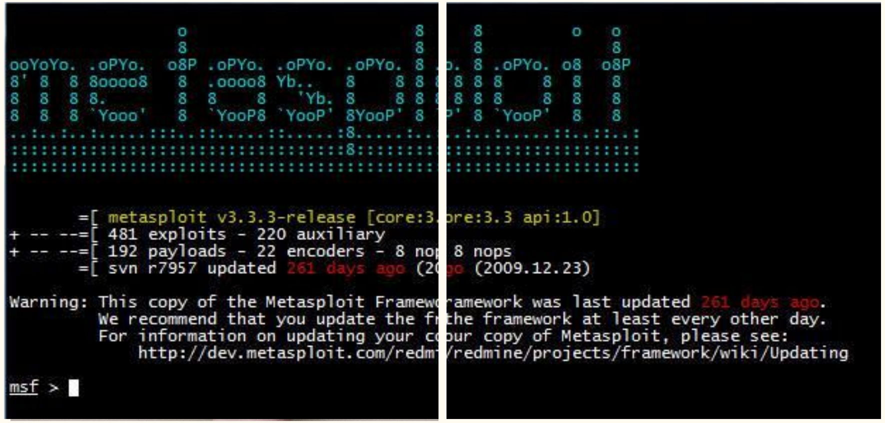
Priv Esc

Enum

Enumeration

Enumeration

1. *Look around Ted, you're all alone.*
    a. Nmap
    b. Netdiscover
2. Toc. Toc. Who's there?
    a. Nmap
3. I wanna know you better.
    a. Dirsearch / dirb / gobuster
    b. Wpscan

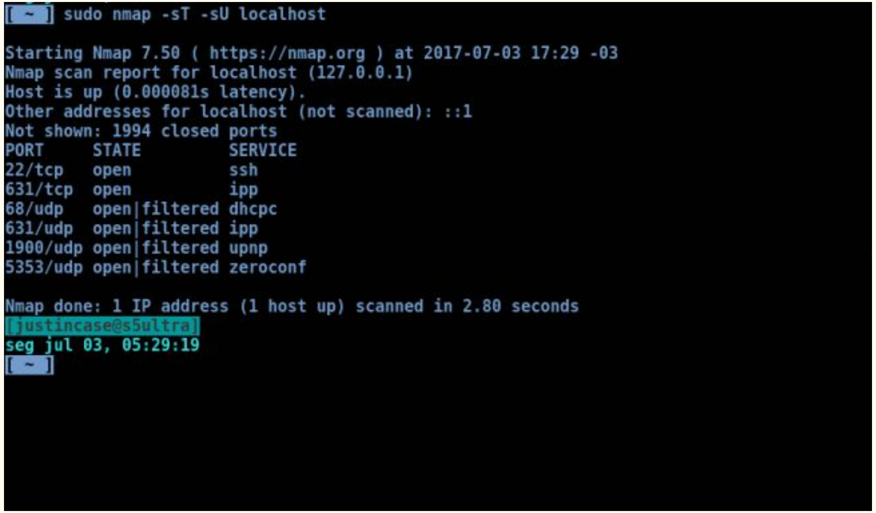


```
                 o                       8     8          o   o
                 8                       8     8              8
ooYoYo. .oPYo.  o8P .oPYo. .oPYo. .oPYo. 8 .o. 8 .oPYo. o8   o8P
8' 8  8 8oooo8   8  .oooo8 Yb..   8    8 8 8 8 8 8    8  8    8
8  8  8 8.       8  8    8   'Yb. 8    8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


       =[ metasploit v3.3.3-release [core:3.ore:3.3 api:1.0]
+ -- --=[ 481 exploits - 220 auxiliary
+ -- --=[ 192 payloads - 22 encoders - 8 no 8 nops
       =[ svn r7957 updated 261 days ago (2go (2009.12.23)

Warning: This copy of the Metasploit Framewramework was last updated 261 days ago.
         We recommend that you update the frthe framework at least every other day.
         For information on updating your coour copy of Metasploit, please see:
             http://dev.metasploit.com/redm/redmine/projects/framework/wiki/Updating

msf >
```



```
[ ~ ] sudo nmap -sT -sU localhost

Starting Nmap 7.50 ( https://nmap.org ) at 2017-07-03 17:29 -03
Nmap scan report for localhost (127.0.0.1)
Host is up (0.000081s latency).
Other addresses for localhost (not scanned): ::1
Not shown: 1994 closed ports
PORT     STATE         SERVICE
22/tcp   open          ssh
631/tcp  open          ipp
68/udp   open|filtered dhcpc
631/udp  open|filtered ipp
1900/udp open|filtered upnp
5353/udp open|filtered zeroconf

Nmap done: 1 IP address (1 host up) scanned in 2.80 seconds
[justincase@s5ultra]
seg jul 03, 05:29:19
[ ~ ]
```

Exploitation

Back to theory

Understanding about web attacks

Web attacks

Different types of web attacks

- There is different kind of attacks
- The most basically happens when you find sensitive data exposed, like files that anyone can read with passwords exposed
- Some sites also display their source code in errors, and you can read the code and look for attacks
- But the most important source of web attacks are inputs. Remember when we studied GET and POST? These parameters sometimes are expected to be a specifically kind of data, like a number, and if you change the number to a letter, the system don’t know what to do
- The web hacking is almost about exploit this unexpected behavior that the programer didn’t analyze

Local File Inclusion

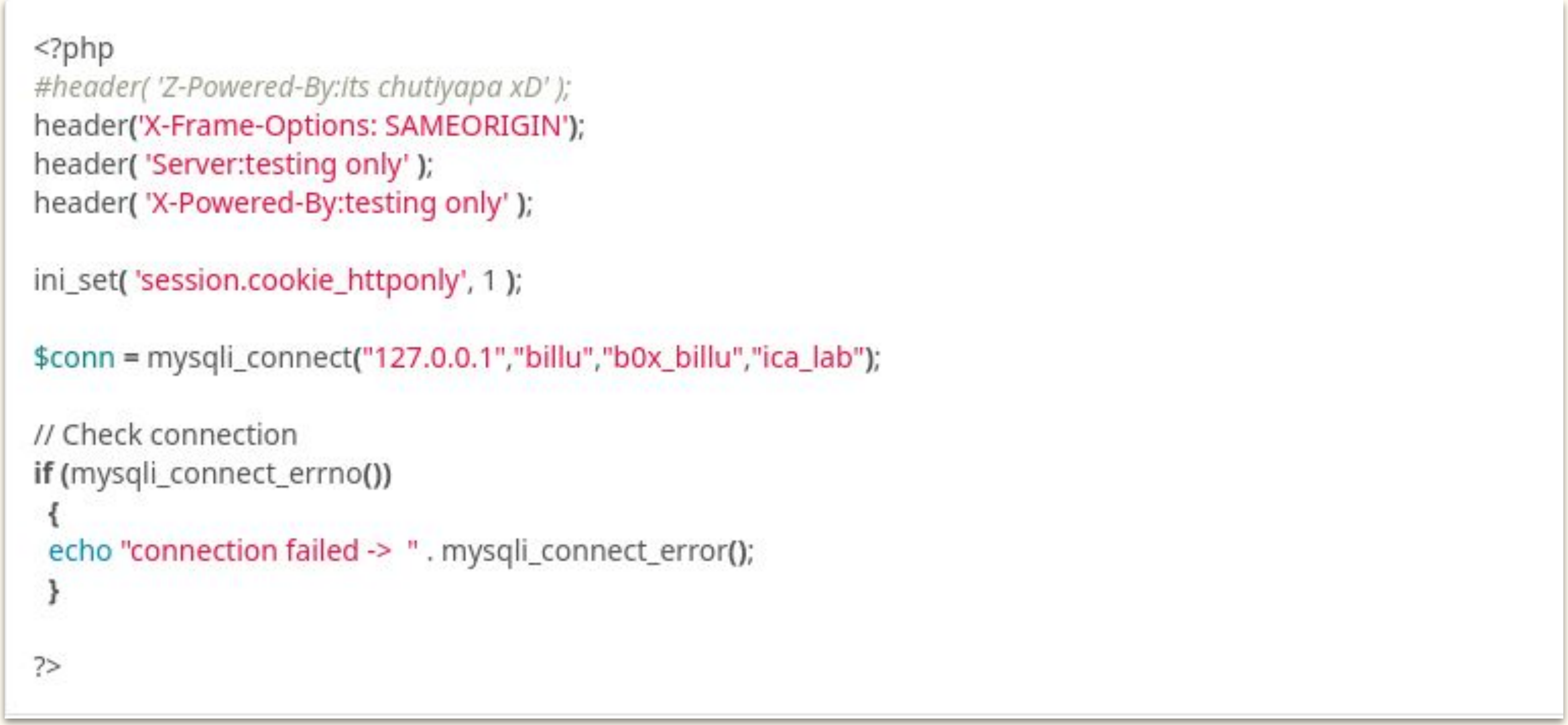
Local File Inclusion (LFI)

All the files are stored in the system, the initial page is by standard index.php

The PHP allows the programmer to show other files inside the actual one. The LFI vulnerability happens when a user can abuse this feature to choose which file will be printed in the page, choosing sensitive files and getting secret information

Files that users shouldn’t see:

- /etc/passwd
- /etc/shadow
- /proc/self/environ
- /var/www/phpmy/config.inc.php
  - Postman
- /proc/version
- /var/log/apache/access.log
- /var/log/sshd.log
- /var/log/mail



```php
<?php
#header( 'Z-Powered-By:its chutiyapa xD' );
header('X-Frame-Options: SAMEORIGIN');
header( 'Server:testing only' );
header( 'X-Powered-By:testing only' );

ini_set( 'session.cookie_httponly', 1 );

$conn = mysqli_connect("127.0.0.1","billu","b0x_billu","ica_lab");

// Check connection
if (mysqli_connect_errno())
 {
 echo "connection failed ->  " . mysqli_connect_error();
 }

?>
```

What can we do?

Look for more vulnerabilities

Back to enumeration

What can we try:

- Shell upload
- find RCE
- Look for others vulnerabilities
- Vulnerable version of a service
- Enumeration

Sobre esse desafio:

- Exploit: https://www.exploit-db.com/exploits/37292/
- Billu Box: https://www.vulnhub.com/entry/billu-b0x,188/
- Walkthrough: https://mrh4sh.github.io/billu-b0x-solution

When Hacking Get Serious: HackTheBox

More information:

- Matheus Vrech
- Telegram e Twitter: @vrechson
- Email: abrasax@cocaine.ninja
- POMBO:
- Grupo do Telegram: @pomboufscar
- Canal do Telegram: @pombocorreio
- Github: https://github.com/pombo-ctf