

# Transferir Archivos a un Sistema Comprometido

## Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Jueves 2 de Julio del 2015

# Presentación

Alonso Eduardo Caballero Quezada es Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling.

Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de doce años de experiencia en el área y desde hace ocho años labora como Consultor e Instructor Independiente en las áreas de Hacking Ético & Informática Forense. Perteneció por muchos años al grupo internacional de Seguridad RareGaZz e integra actualmente el Grupo Peruano de Seguridad PeruSEC. Ha dictado cursos presenciales y virtuales en Ecuador, España, Bolivia y Perú, presentándose también constantemente en exposiciones enfocadas a Hacking Ético, Informática Forense, GNU/Linux y Software Libre.



@Alonso\_ReYDeS



www.facebook.com/alonsoreydes



pe.linkedin.com/in/alonsocaballeroquezada/



# Transferencia de Archivos

La fase de post explotación se refiere a las acciones realizadas por un atacante malicioso, quien ya tiene algún tipo de control en el objetivo de evaluación, después de haber explotado satisfactoriamente alguna vulnerabilidad.

Estas acciones pueden incluir el subir archivos y herramientas hacia la máquina objetivo, intentar elevar o incrementar privilegios, expandir el control hacia otros objetivos de evaluación, instalar puertas traseras, o borrar evidencia del ataque, entre otras acciones.

Una de las primeras y principales acciones es subir archivos los cuales ayudarán a los procesos de post explotación. Entre estos se incluyen

- Códigos compilados de exploits

- Códigos de exploits,

- Herramientas para escanear

- Puertas traseras

- Rootkits

- Otros archivos útiles.

# Métodos para Transferir Archivos

Una de las principales limitaciones cuando se intenta subir archivos hacia el objetivo de evaluación comprometido, es la limitación impuesta a únicamente utilizar las herramientas disponible en el objetivo.

En los entornos GNU/Linux o similares, frecuentemente se pueden encontrar herramientas previamente instaladas en el sistema operativo, como netcat, wget o curl, lo cual facilita la descarga de archivos desde sistemas remotos. Sin embargo en Sistemas Windows, el proceso no podría ser tan sencillo.

Entre las principales métodos para transferir archivos se tienen.

Subir archivos utilizando TFTP

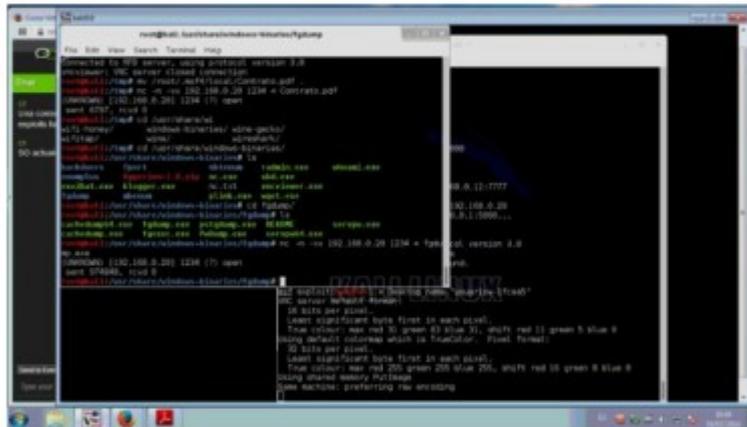
Subir archivos utilizando FTP

Utilizar debug.exe para transferir archivos

Subir archivos utilizando Meterpreter

## Curso Virtual de Hacking Ético

### 2015



#### Grupo Sábado:

4, 11, 18 y 25 de Julio del 2015  
De 9:00am a 12:45pm (UTC -05:00)

#### Grupo Domingo:

5, 12, 19 y 26 de Julio del 2015  
De 9:00am a 12:45pm (UTC -05:00)

Este curso virtual ha sido dictado a participantes residentes en los siguientes países:



Más Información: [http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Etico](http://www.reydes.com/d/?q=Curso_de_Hacking_Etico)  
E-mail: [caballero.alonso@gmail.com](mailto:caballero.alonso@gmail.com) / Sitio Web: <http://www.reydes.com>

# Cursos Virtuales

Todos los Cursos Virtuales dictados están disponibles en Video.

Curso Virtual de Hacking Ético

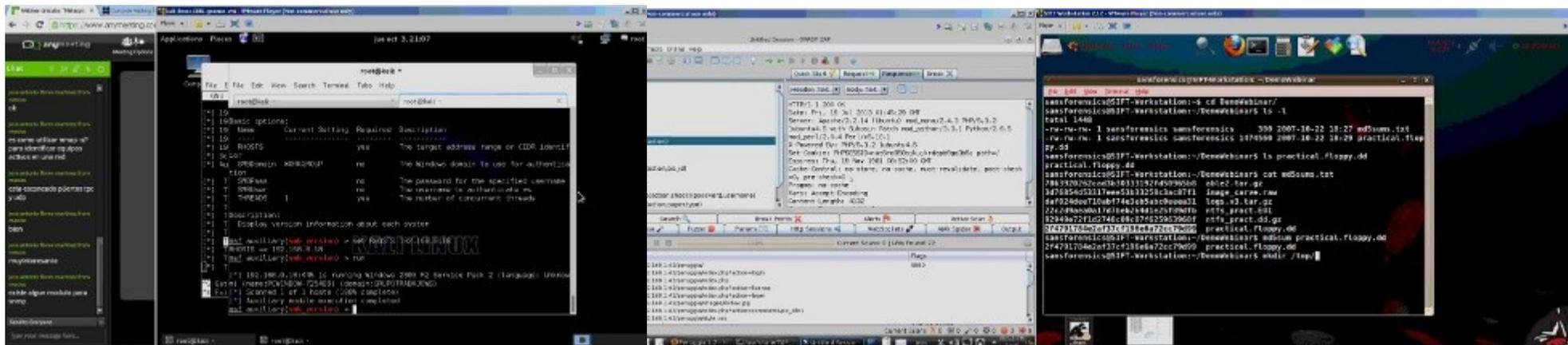
[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Etico](http://www.reydes.com/d/?q=Curso_de_Hacking_Etico)

Curso Virtual de Hacking Aplicaciones Web

[http://www.reydes.com/d/?q=Curso\\_de\\_Hacking\\_Aplicaciones\\_Web](http://www.reydes.com/d/?q=Curso_de_Hacking_Aplicaciones_Web)

Curso Virtual de Informática Forense

[http://www.reydes.com/d/?q=Curso\\_de\\_Informatica\\_Forense](http://www.reydes.com/d/?q=Curso_de_Informatica_Forense)



# Más Contenidos

Videos de 28 Webinars Gratuitos sobre Hacking Ético, Hacking Aplicaciones Web e Informática Forense.

<http://www.reydes.com/d/?q=videos>

Diapositivas utilizadas en los Webinars Gratuitos.

<http://www.reydes.com/d/?q=node/3>

Artículos y documentos publicados

<http://www.reydes.com/d/?q=node/2>

Mi Blog sobre temas de mi interés.

<http://www.reydes.com/d/?q=blog/1>

Alonso Caballero Quezada / ReYDeS Documentos Eventos Cursos Blog Contacto

Servicio Independiente de Hacking Ético

**Presentación**

**Alonso Eduardo Caballero Quezada** es Brainbench Certified Network Security (Master), Computer Forensics (U.S.) & Linux Administration (General), IT Masters Certificate of Achievement en Network Security Administrator, Hacking Countermeasures, Cisco CCNA Security, Information Security Incident Handling y Miembro de Open Web Application Security Project (OWASP). Ha sido Instructor en el OWASP LATAM Tour Lima, Perú del año 2014, y Conferencista en PERUHACK 2014. Cuenta con más de once años de experiencia en el área y desde hace siete años labora como Consultor e Instructor Independiente en las áreas de Hacking

**Cursos**

- Curso de Hacking Ético
- Curso de Hacking Aplicaciones Web
- Curso de Informática Forense
- Curso de Hacking con Kali Linux
- Curso Forense de Autopsy 3

**Mi Blog**

- Crear una Puerta Trasera Persistente utilizando Meterpreter
- Trazado de Rutas en Paralelo utilizando Scapy
- Automatizar un Ataque MITM para Recolectar Credenciales utilizando Subterfuge

# Demostraciones

```
root@kali: /usr/share/windows-b...
File Edit View Search Terminal Help
this option is mostly only use
prefix lines you send with you
-H on/off highlight incoming data with a
sequence (for e.g. chatting).
-V print version banner and exit
bug report and send bug report
unix-like OS specific options:
-s invoke a shell, nothing else.
a root shell
-w n "immobility timeout" in seconds
and program execution (the -e
-D on/off fork and run in background (da
root@kali: /usr/share/windows-binaries# sbd -k
Microsoft Windows [Version 5.2.3790]
(C) Copyright 1985-2003 Microsoft Corp.

C:\>set
set
ALLUSERSPROFILE=C:\Documents and Settings\All U
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Archivos de programa\Arch
COMPUTERNAME=PCWINDOW-7254B9
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO

root@kali: ~
File Edit View Search Terminal Help
-e 5c80
0CCE:5C80 00.
00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5C88 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5C90 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5C98 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CA0 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CA8 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CB0 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CB8 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CC0 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CC8 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CD0 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CD8 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CE0 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CE8 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CF0 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5CF8 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00 00.00
0CCE:5D00 00. 00. 00.
-e 5d00
0CCE:5D00 00.
EC 00.e 00.ac
-r cx
CX 0000
:5c00
-w
Escribiendo 05C00 bytes
-q

C:\>copy 1.dll klogger.exe
copy 1.dll klogger.exe
1 archivos copiados.
```

# Transferir Archivos a un Sistema Comprometido

## Webinar Gratuito

Alonso Eduardo Caballero Quezada

Consultor en Hacking Ético, Informática Forense & GNU/Linux

Sitio Web: <http://www.ReYDeS.com>

e-mail: [ReYDeS@gmail.com](mailto:ReYDeS@gmail.com)

Jueves 2 de Julio del 2015