

Actividad práctica número 4:

Formato: Individual

Asignatura: Seguridad de Sistemas

Objetivo: conocer las técnicas para realizar enumeración de sistemas

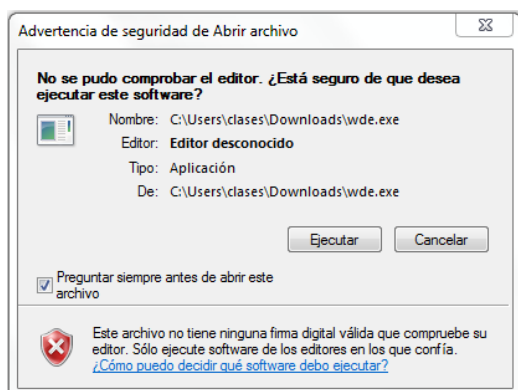
Título: Enumeración de Sistemas Operativos y Aplicaciones web

A.- Web Data Extractor

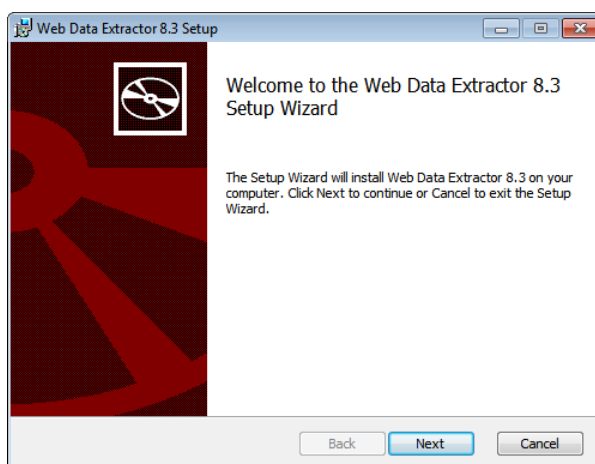
1.- Baje la aplicación Web Data Extractor en su computador Windows 7 desde el siguiente link

<http://www.webextractor.com/download.htm>

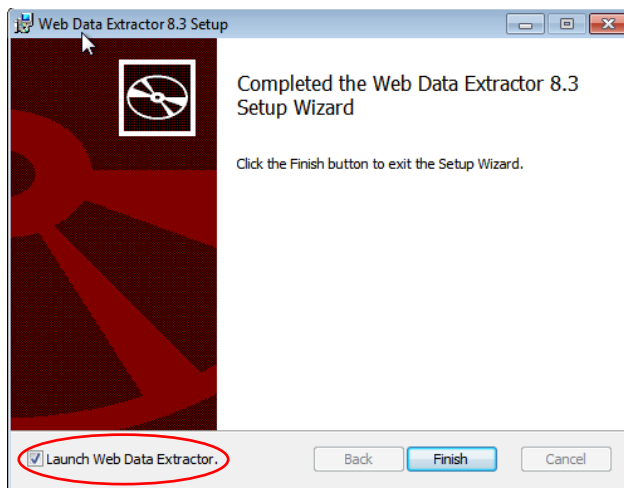
2.- Instale la aplicación en su computador



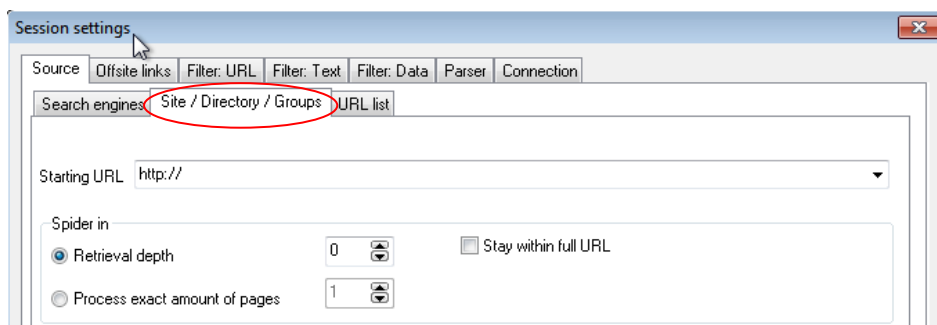
3.- Finalice la instalación



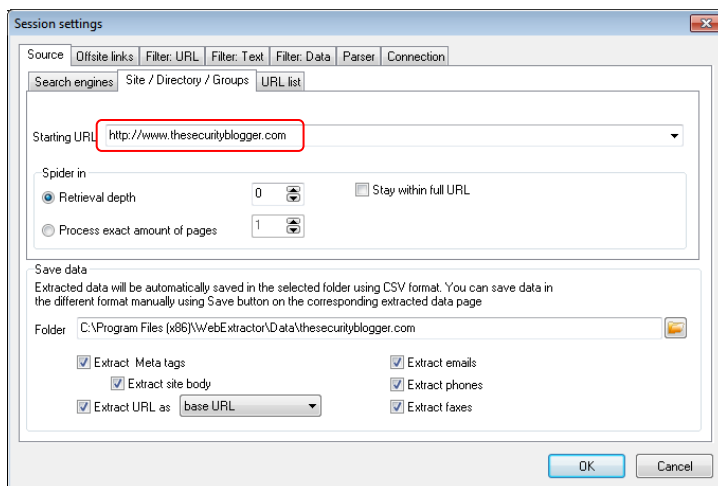
4.- Ejecute la aplicación una vez finalizada la instalación



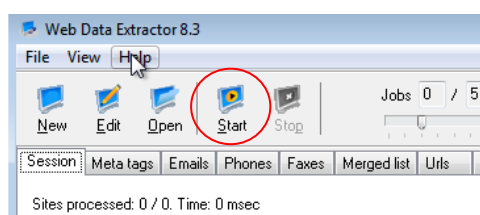
5.- Haga click en “New” y vaya a la opción “Site /Directory / Group”



6.- Ingrese la URL mostrada en la figura y haga click en OK




7.- A continuación haga click en “Start”



8.- Revise la conexión que realiza la herramienta para obtener información

Session			Meta tags (25)	Emails	Phones	Faxes	Merged list	Urls (333)	Inactive sites
Site processed: 0 / 1. Time: 2:02 min			URL processed		25				
			Traffic received		2,32 Mb				
URL			Size		State				
http://www.thesecurityblogger.com/?paged=2			Unknown		Connected.				
http://www.thesecurityblogger.com/?tag=aamir			Unknown		Connected.				
http://www.thesecurityblogger.com/?tag=aamir-lakhani			Unknown		Connected.				

9.- Una vez finalizado el test, revise la información en la opción “Mega Tags”

Session		Meta tags (57)	Emails	Phones	Faxes	Merged list	Urls (544)	Inactive sites	
<div></div>									
URL	Title		Keywords		Description		Host	Domain	Page size
http://www.thesecurityblogger.com/?p=156							http://www.thesi.com		951
http://www.thesecurityblogger.com/?p=247							http://www.thesi.com		951
http://www.thesecurityblogger.com/?p=332							http://www.thesi.com		951
http://www.thesecurityblogger.com/?p=431	Juniper Networks sells Junos Pulse to Siris C		juniper,junos pulse,		Juniper Networks sells Junos Pu		http://www.thesi.com		33910

Responda:

¿Qué tipo de información obtuvo?

10.- Repita la operación utilizando las siguientes URL:

www.altoromutual.com

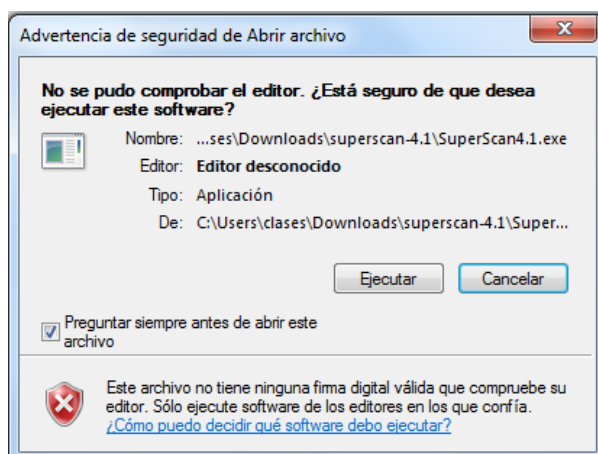
www.redusers.com

B.- SuperScan de McAfee

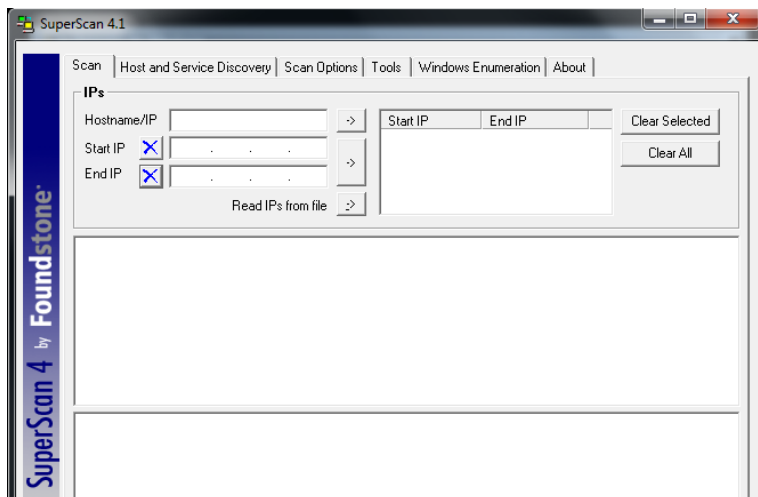
1.- Baje la aplicación SuperScan de McAfee de la siguiente dirección, en su computador con Windows 7.

<http://www.mcafee.com/us/downloads/free-tools/superscan.aspx>

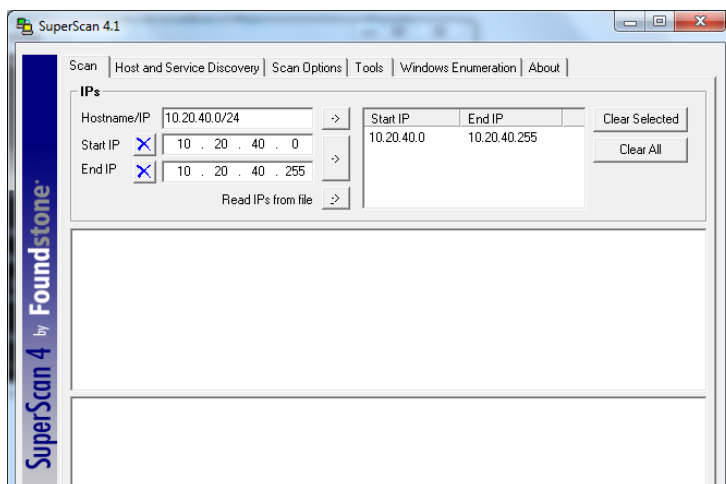
2.- Instale la aplicación en su estación de trabajo



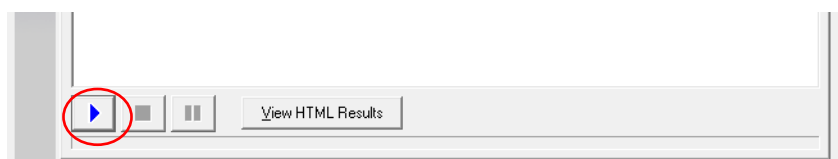
3.- Una vez finalizada la instalación, ejecútela con privilegios de Administrador



4.- Configure la aplicación para realizar un “scan” a la red local, según el ejemplo mostrado

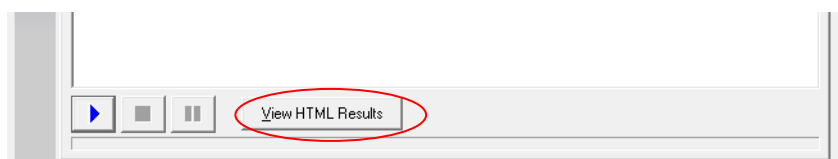


5.- Inicie el “scan” con la opción mostrada en la figura



¿Qué obtuvo como resultado?

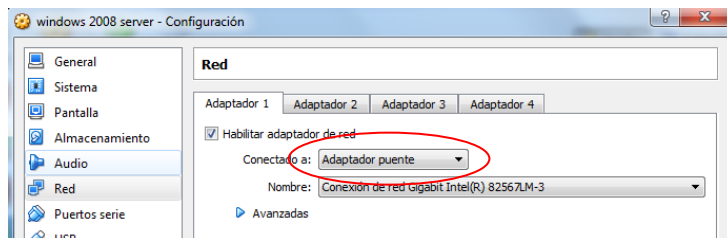
6.- Realice un reporte con la opción “View HTML Results”



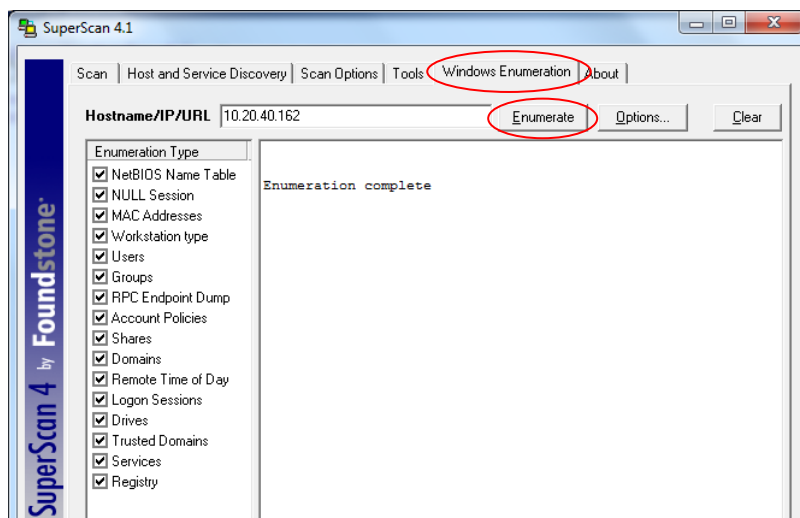
7.- Analice el reporte obtenido y comente con su compañero

IP	10.20.40.196
Hostname	lpc1210340.duoc.acad
Netbios Name	LC12IP2PROF
Workgroup/Domain	WORKGROUP
UDP Ports (1)	
137	NETBIOS Name Service
UDP Port	Banner
137	MAC Address: 00:21:86:F4:F7:B2
NETBIOS Name Service	NIC Vendor : Unknown
	Netbios Name Table (4 names)
	LC12IP2PROF 00 UNIQUE Workstation service name
	WORKGROUP 00 GROUP Workstation service name
	LC12IP2PROF 20 UNIQUE Server services name
	WORKGROUP 1E GROUP Group name
Total hosts discovered	1
Total open TCP ports	0
Total open UDP ports	1

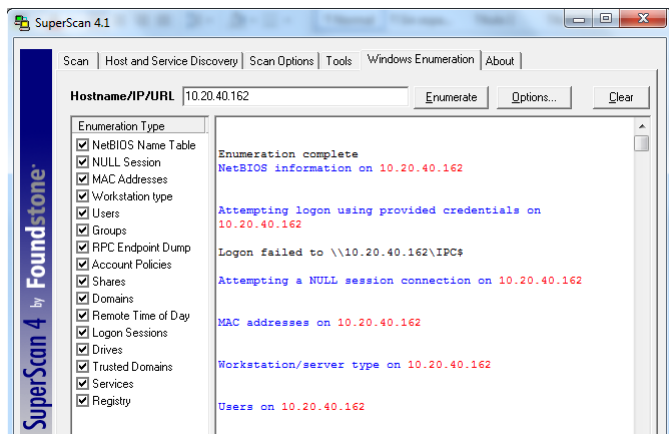
8.- Levante su servidor Windows 2008 con la interfaz de red en modo puente



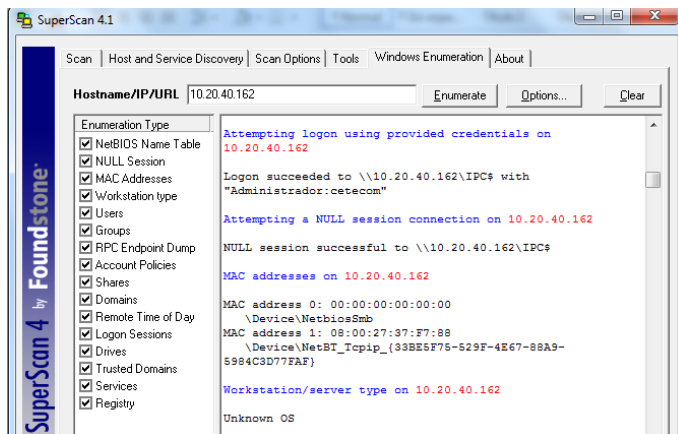
9.- Configure la opción de “Windows Enumeration” con la dirección IP de su servidor Windows 2008 y ejecute la opción “Enumerate”



10.- Observe el resultado y describa lo que pudo obtener como información

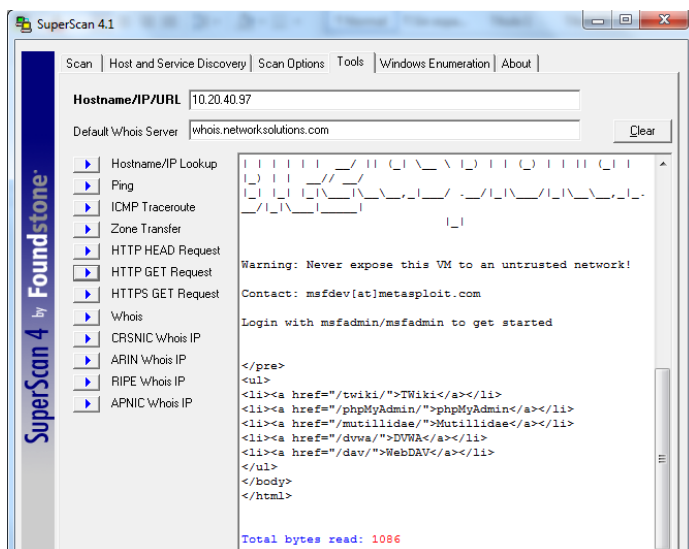


11.- A continuación baje el servicio firewall de su Windows 2008 Server y repita la operación



¿Qué diferencias observa respecto del caso anterior?

12.- A continuación, levante la máquina virtual de Metasploitable en modo puente y ejecute las herramientas de la opción “Tools”



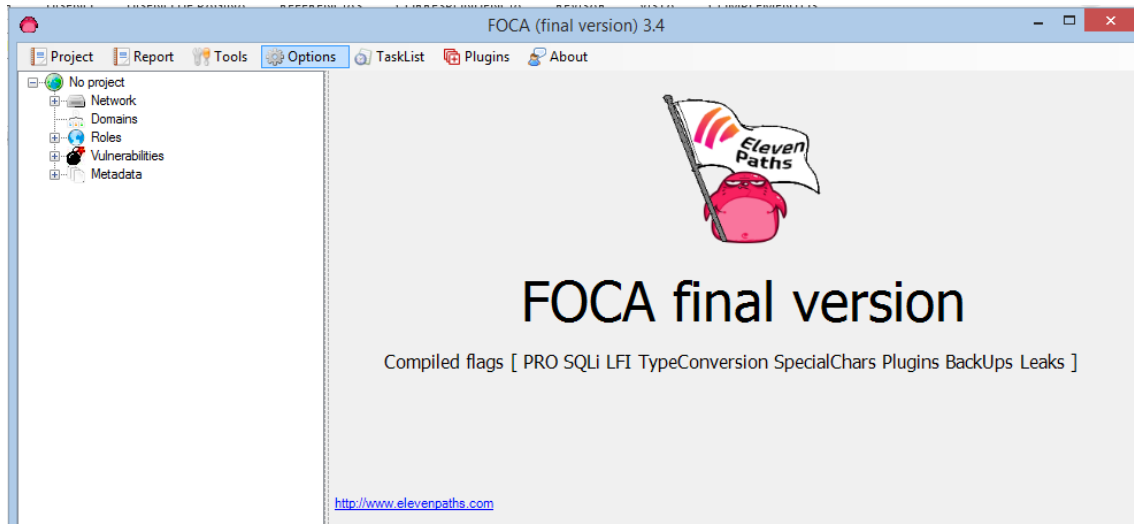
Observe la información obtenida en cada una de ellas

C.- FOCA de Informática 64

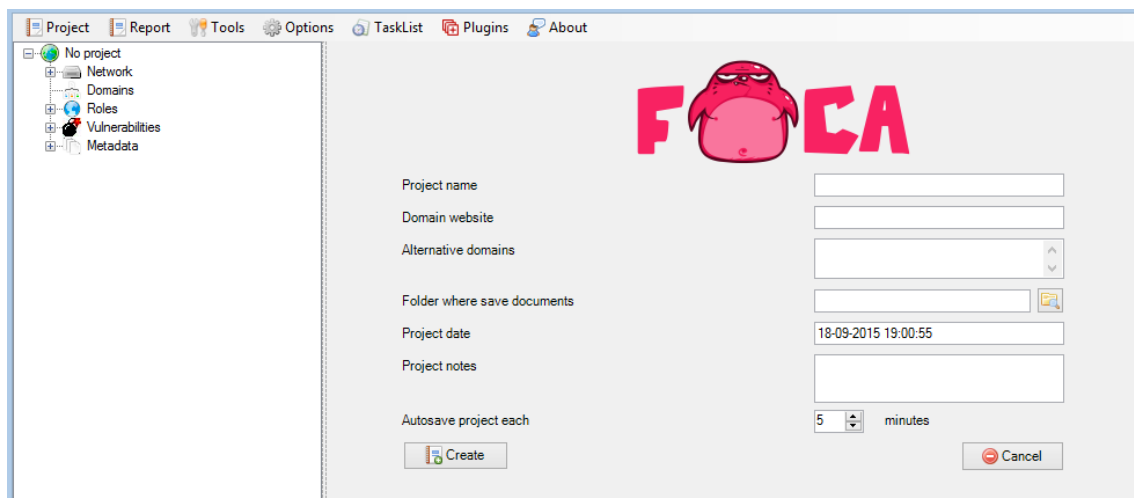
1.- Baje e instale la herramienta FOCA desde la siguiente dirección:

<https://www.elevenpaths.com/es/labstools/foca-2/index.html>

2.- Una vez instalada, ejecute la aplicación:



3.- Seleccione la opción Project > New Project del menú principal



4.- Ingrese los datos del proyecto siguiendo el ejemplo mostrado y haga click en la opción "Create"

The screenshot shows the FOCA application interface. On the left is a sidebar with a tree view containing: No project, Network, Domains, Roles, Vulnerabilities, and Metadata. The main area has the FOCA logo at the top. Below it is a form with the following fields: Project name (filled with "Mi primer proyecto FOCA"), Domain website (filled with "www.redusers.com"), Alternative domains (empty), Folder where save documents (empty), Project date (filled with "18-09-2015 19:00:55"), Project notes (empty), and Autosave project each (set to "5 minutes"). At the bottom of the form is a "Create" button, which is highlighted with a red rectangle. A "Cancel" button is also present.

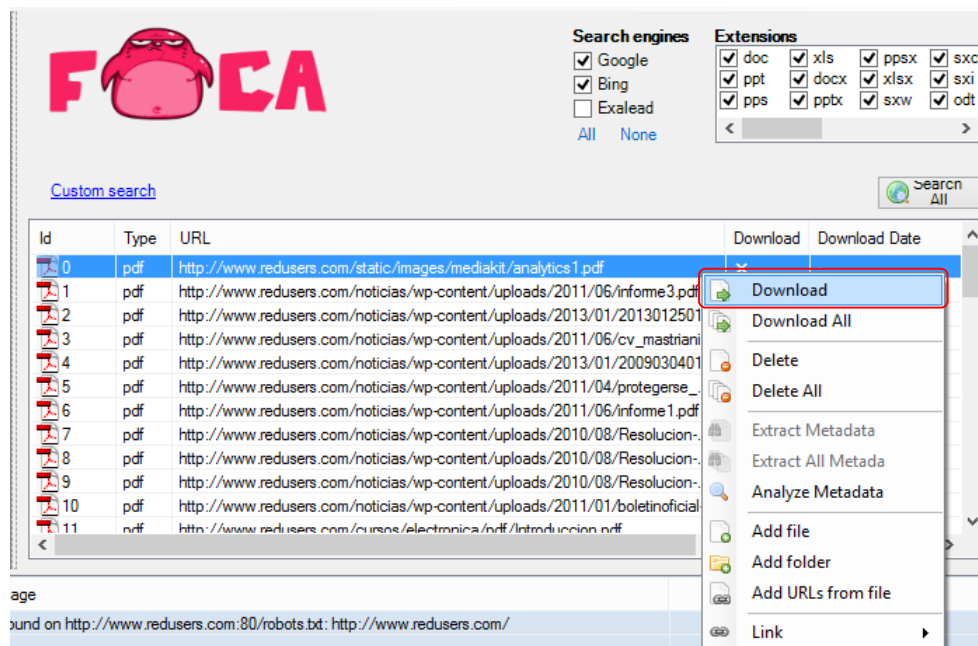
5.- Grabe el proyecto con el nombre que desee

The screenshot shows the FOCA application interface after the project has been created. The sidebar now shows "Mi primer proyecto FOCA" selected. The main area displays the FOCA logo and a "Search engines" section with checkboxes for Google, Bing, and Exalead. Below this is a "Custom search" link and a table with columns: Id, Type, URL, Download, and Download Date. A modal dialog box is open in the center, titled "Mi primer proyecto FOCA - FOCA (final version) 3.4". It contains an information icon and the text "Project saved successfully!". There is an "Aceptar" button at the bottom right of the dialog.

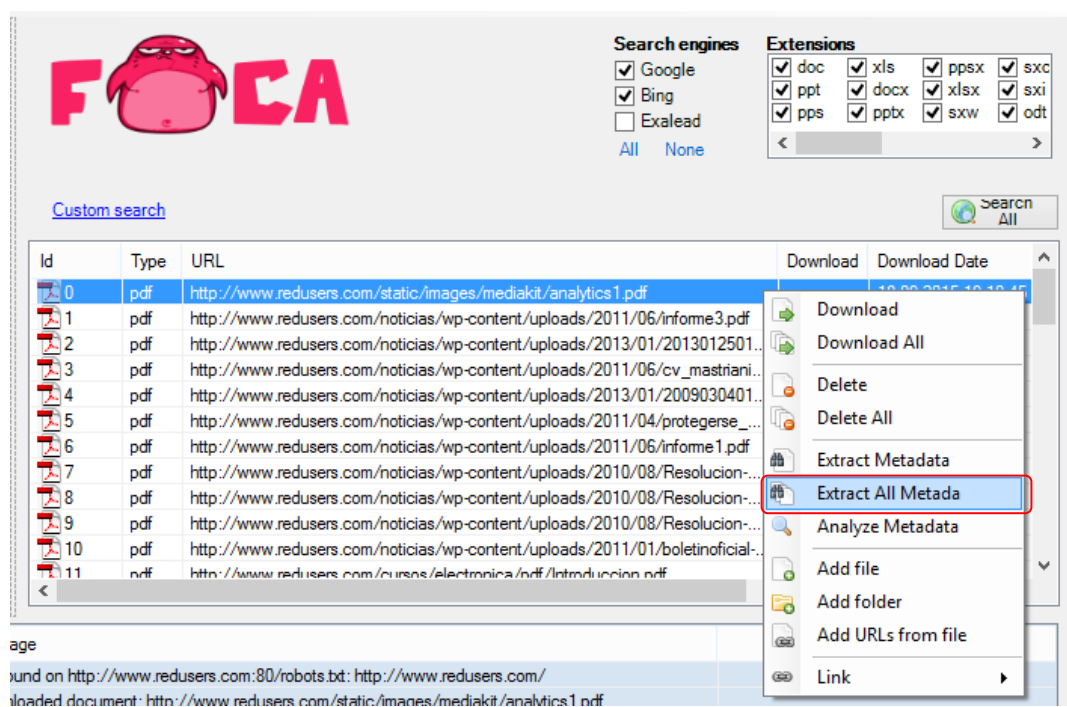
6.- Seleccione la opción "Search All" para iniciar la búsqueda de los documentos en el sitio seleccionado

The screenshot shows the FOCA application interface with the "Search All" button highlighted by a red rectangle. The sidebar is empty. The main area displays the FOCA logo, "Search engines" (Google, Bing, Exalead), and "Extensions" (doc, xls, ppsx, sxc, ppt, docx,xlsx, sxi,pps, pptx, sxw, odt). Below these is a "Custom search" link and a table with columns: Id, Type, URL, Download, Download Date, Size, and Analyzed. The "Search All" button is located at the bottom right of the main area.

7.- Una vez que haya finalizado el proceso de búsqueda de documentos, seleccione uno, haga click derecho > “Download” para bajar el documento seleccionado



8.- Una vez finalizado, haga click derecho > Extract All Meta Data, para obtener los metadatos del documento seleccionado



9.- Seleccione el documento en el menú de la izquierda para visualizar los metadatos

Attribute	Value
File Information	
URL	http://www.redusers.com/static/images/mediakit/analytics1.pdf
Local path	C:\Users\lgomez\AppData\Local\Temp\analytics1 (1).pdf
Download	Yes
Analyzed	Yes
Download date	18-09-2015 19:10:45
Size	102.88 KB
Dates	
Creation date	03-08-2009 12:44:05
Modified date	04-08-2009 11:22:06
Other Metadata	
Application	iText 2.1.3 (by lowagie.com)
Application	Google Analytics
Subject	RedUSERS
Title	Dashboard
Software	
iText 2.1.3 (by lowagie.com)	
Google Analytics	

Responda lo siguiente:

¿Cuál fue la fecha de creación del documento? _____

¿Cuándo fue modificado por última vez? _____

¿Quién fue el autor del documento? _____

¿Con que aplicación fue creado? _____

D.- Enumeración Linux interna

1.- Conéctese a la maquina Metasploitable2 vía ssh

```
root@kali:~# ssh msfadmin@10.0.2.130
The authenticity of host '10.0.2.130 (10.0.2.130)' can't be established.
RSA key fingerprint is SHA256:BQHm5EoHX9GciOLuVscegPXLQ0suPs+E9d/rrJB84rk.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.0.2.130' (RSA) to the list of known hosts.
msfadmin@10.0.2.130's password:
Linux metasploitable 2.6.24-16-server #1 SMP Thu Apr 10 13:58:00 UTC 2008 i686

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

Ubuntu comes with ABSOLUTELY NO WARRANTY, to the extent permitted by
applicable law.

To access official Ubuntu documentation, please visit:
http://help.ubuntu.com/
No mail.
Last login: Wed May 27 17:40:18 2020
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

msfadmin@metasploitable:~$
```

2.- Baje la aplicación LinEnum desde github

```
root@kali:~# git clone https://github.com/rebootuser/LinEnum.git
Cloning into 'LinEnum' ...
remote: Enumerating objects: 234, done.
remote: Total 234 (delta 0), reused 0 (delta 0), pack-reused 234
Receiving objects: 100% (234/234), 125.89 KiB | 575.00 KiB/s, done.
Resolving deltas: 100% (123/123), done.
root@kali:~#
```

3.- Conéctese al directorio de la aplicación LinEnum

```
root@kali:~# cd LinEnum/
root@kali:~/LinEnum# ls -l
total 68
-rw-r--r-- 1 root root 4972 May 27 22:11 CHANGELOG.md
-rw-r--r-- 1 root root 658 May 27 22:11 CONTRIBUTORS.md
-rw-r--r-- 1 root root 1067 May 27 22:11 LICENSE
-rwxr-xr-x 1 root root 46631 May 27 22:11 LinEnum.sh
-rw-r--r-- 1 root root 3829 May 27 22:11 README.md
root@kali:~/LinEnum#
```

4.- Levante un servidor web para la publicación del archivo LinEnum.sh

```
root@kali:~/LinEnum# python -m SimpleHTTPServer 80
Serving HTTP on 0.0.0.0 port 80 ...

```

5.- Baje la aplicación LinEnum a la máquina target en el directorio /tmp

```
msfadmin@metasploitable:~$ cd /tmp
msfadmin@metasploitable:/tmp$ wget http://10.0.2.125/LinEnum.sh
--18:20:02--  http://10.0.2.125/LinEnum.sh
          => `LinEnum.sh'
Connecting to 10.0.2.125:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 46,631 (46K) [text/x-sh]

100%[=====

18:20:02 (476.82 MB/s) - `LinEnum.sh' saved [46631/46631]

msfadmin@metasploitable:/tmp$
```

6.- Agregue permiso de ejecución al archivo LinEnum.sh

```
msfadmin@metasploitable:/tmp$ ls -l
total 48
-rw----- 1 tomcat55 nogroup      0 2020-05-27 17:40 4484.jsvc_up
-rw-r--r-- 1 msfadmin msfadmin 46631 2020-05-27 18:11 LinEnum.sh
msfadmin@metasploitable:/tmp$ chmod +x LinEnum.sh
msfadmin@metasploitable:/tmp$ ls -l
total 48
-rw----- 1 tomcat55 nogroup      0 2020-05-27 17:40 4484.jsvc_up
-rwxr-xr-x 1 msfadmin msfadmin 46631 2020-05-27 18:11 LinEnum.sh
msfadmin@metasploitable:/tmp$
```

7.- Ejecute la aplicación LinEnum.sh

```
msfadmin@metasploitable:/tmp$ ./LinEnum.sh

#####
# Local Linux Enumeration & Privilege Escalation Script #
#####
# www.rebootuser.com
# version 0.982

[-] Debug Info
[+] Thorough tests = Disabled
```

8.- Revise el reporte generado por la herramienta

E.- Enumeración de servicios externos

1.- Inicie su máquina Metasploitable II con la interfaz en modo Red NAT

2.- Edite el archivo /etc/samba/smb.conf

```
GNU nano 5.4 /etc/samba/smb.conf
#   behaviour of Samba but the option is considered important
#   enough to be mentioned here
#
# NOTE: Whenever you modify this file you should run the command
# "testparm" to check that you have not made any basic syntactic
# errors.
#===== Global Settings =====
[global]
## Browsing/Identification ###
```

3.- Agregue la siguiente entrada bajo el parámetro [global]

```
[global]
## Browsing/Identification ###
# Change this to the workgroup/NT-domain name your Samba server will part of
workgroup = WORKGROUP
client min protocol = CORE
client max protocol = SMB3
```

4.- A continuación, grabe el archivo.

5.- Ejecute el comando siguiente para realizar la enumeración

```
# enum4linux 10.0.2.8
Starting enum4linux v0.8.9 ( http://labs.portcullis.co.uk/application/enum4linux/ )

=====
| Target Information |
=====
Target ..... 10.0.2.8
RID Range ..... 500-550,1000-1050
Username ..... ''
Password ..... ''
Known Usernames .. administrator, guest, krbtgt, domain admins, root, bin, none
```

6.- Revise el listado de usuarios

```
=====
| Users on 10.0.2.8 |
=====
index: 0x1 RID: 0x3f2 acb: 0x00000011 Account: games Name: games Desc: (null)
index: 0x2 RID: 0x1f5 acb: 0x00000011 Account: nobody Name: nobody Desc: (null)
index: 0x3 RID: 0x4ba acb: 0x00000011 Account: bind Name: (null) Desc: (null)
index: 0x4 RID: 0x402 acb: 0x00000011 Account: proxy Name: proxy Desc: (null)
index: 0x5 RID: 0x4b4 acb: 0x00000011 Account: syslog Name: (null) Desc: (null)
index: 0x6 RID: 0xbba acb: 0x00000010 Account: user Name: just a user,111,, Desc: (null)
index: 0x7 RID: 0x42a acb: 0x00000011 Account: www-data Name: www-data Desc: (null)
index: 0x8 RID: 0x3e8 acb: 0x00000011 Account: root Name: root Desc: (null)
index: 0x9 RID: 0x3fa acb: 0x00000011 Account: news Name: news Desc: (null)
index: 0xa RID: 0x4c0 acb: 0x00000011 Account: postgres Name: PostgreSQL administrator,,,
```

7.- Revise los recursos compartidos

Share Enumeration on 10.0.2.8		
Sharename	Type	Comment
print\$	Disk	Printer Drivers
tmp	Disk	oh noes!
opt	Disk	
IPC\$	IPC	IPC Service (metasploitable server (Samba 3.0.20-Debian))
ADMIN\$	IPC	IPC Service (metasploitable server (Samba 3.0.20-Debian))
Reconnecting with SMB1 for workgroup listing.		