Curso	CURSO HACKING ÉTICO
MODULO 2	Recolección de Información
Título	Recolección de información
Nombre	EducaIT

Objetivos

En esta práctica debes poner en marcha las técnicas descritas en los videos y contenido teórico para obtener la información que se te pide.

Recuerda que la fase de recolección de información es muy importante cuando se trata de auditorias de “CAJA NEGRA” o “CAJA GRIS”, donde no disponemos de mucha información, o nula según el caso sobre los objetivos que queremos adudiar.

Enunciado

1. Utilizando las técnicas descritas en los videos, obtén la máxima información sobre los archivos de Zona de los dominios:

   - hackthissite.org
   - hack.me
   - casareal.es
   - mytcpip.com
   - educait.es

   Adjunta en la respuesta la siguiente información de cada uno de dichos dominios, si existe… Intenta utilizar comandos Shell como nslookup o dig, o páginas Web que te dan dicha información:

   - Registros NS
   - Registros MX
   - Registros tipo Address
   - Registro SPF
   - Registro DMARC
   - Registro DMARC
   - Versión del servidor de correo
   - Ubicación física de la página Web (datacenter, lo que seas capaz de averiguar)

2. De los dominios anteriores intenta sacar el mayor número de direcciones de correo posible.

3. Prueba los siguientes Google Dorks y expón de forma justificada al menos 5 resultados que puedan comprometer la seguridad de algún Site en función de los resultados devueltos al ejecutar los siguientes Dorks:

```
inurl:/login/index.jsp -site:hertz.*
intitle:"Index of" inurl:wp-json/oembed
intitle:"Index of" phpmyadmin
intitle:"Index of" wp-admin
intitle:index.of.?.sql
inurl: /filemanager/dialog.php
s3 site:amazonaws.com filetype:log
```

```
inurl:cgi/login.pl
inurl:zoom.us/j and intext:scheduled for
site:*/auth intitle:login
nurl: admin/login.aspx    Pages Containing Login Portals
"Index of" inurl:webalizer
"Index of" inurl:phpmyadmin
"Index of" inurl:htdocs inurl:xampp
s3 site:amazonaws.com intext:dhcp filetype:txt inurl:apollo
inurl:/index.aspx/login
filetype:log inurl:password.log
filetype:mbx mbx intext:Subject
filetype:mdb inurl:users.mdb
site:amazonaws.com inurl:login.php
intitle:"IIS Windows Server" -inurl:"IIS Windows Server"
intitle:"Apache2 Ubuntu Default Page: It works"
inurl:/filedown.php?file=
inurl:Dashboard.jspa intext:"Atlassian Jira Project Management Software"
inurl:app/kibana intext:Loading Kibana
site:https://docs.google.com/spreadsheets edit
inurl:8443 AND -intitle:8443 AND -intext:8443 prohibited|restricted|unauthorized
intitle:"index of" unattend.xml
inurl:/admin/index.php
inurl:bc.googleusercontent.com intitle:index of
inurl:office365 AND intitle:"Sign In | Login | Portal"
intext:"@gmail.com" AND intext:"@yahoo.com" filetype:sql
intitle:OmniDB intext:"user. pwd. Sign in."
intitle:"qBittorrent Web UI" inurl:8080
site:com inurl:jboss filetype:log -github.com
intitle:"index of" ".cpanel/caches/config/"
inurl:'/scopia/entry/index.jsp'
nurl:/index.aspx/login
intitle: "index of" "./" "./bitcoin"
inurl:/portal/apis/fileExplorer/
intitle:"index of" "/aws.s3/"
intitle:"index of" hosts.csv | firewalls.csv | linux.csv | windows.csv
intitle:Test Page for the Nginx HTTP Server on Fedora
inurl:_cpanel/forgotpwd
intitle:"index of /" intext:/backup
intitle:"Swagger UI - " + "Show/Hide"
site:drive.google.com /preview intext:movie inurl:flv | wmv | mp4 -pdf -edit -view
intext:"class JConfig {" inurl:configuration.php
"index of" "database.sql.zip"
```

Resultado

Dar respuesta a cada una de las preguntas planteadas. Añade siempre que sea posible el método o comandos utilizados para obtener las respuestas.