Desafío 18

Nombre: Matias O. Riedel

**Objetivo**

Realizar pruebas sobre sistemas informáticos simulando la actuación de un atacante malintencionado para identificar y resolver vulnerabilidades antes de que sean explotadas. El objeto de estudio es el sitio <http://vulnweb.com/>.

**1. Google: Identificación de sitios web hospedados en**[**http://vulnweb.com**](http://vulnweb.com/)

Para este caso procedemos a ejecutar el siguiente comando en nuestro navegador ‘site:vulnweb.com -www’

Donde podremos visualizar los demas sitios que hospedados por la pagina en si

Texto

Descripción generada automáticamente

Links de los sitios:

<http://rest.vulnweb.com>

<http://testphp.vulnweb.com/pictures/>

<http://testhtml5.vulnweb.com/report>

<http://testasp.vulnweb.com/Search.asp>

**2. DIG & WHOIS: Información del Dominio**

Ahora procederemos a obtener información del dominio anteriormente mencionado ‘http://vulnweb.com/’

Para eso procederemos a ingresar a nuestro terminal de nuestro Linux y ejecutaremos el siguiente comando para obtener información del dominio

Donde nos devolverá lo siguiente:  
  
root@svr-lab:/# whois vulnweb.com

Domain Name: VULNWEB.COM

Registry Domain ID: 1602006391\_DOMAIN\_COM-VRSN

Registrar WHOIS Server: whois.eurodns.com

Registrar URL: http://www.EuroDNS.com

Updated Date: 2023-05-26T07:56:15Z

Creation Date: 2010-06-14T07:50:29Z

Registry Expiry Date: 2025-06-14T07:50:29Z

Registrar: EuroDNS S.A.

Registrar IANA ID: 1052

Registrar Abuse Contact Email: legalservices@eurodns.com

Registrar Abuse Contact Phone: +352.27220150

Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited

Name Server: NS1.EURODNS.COM

Name Server: NS2.EURODNS.COM

Name Server: NS3.EURODNS.COM

Name Server: NS4.EURODNS.COM

DNSSEC: unsigned

The Registry database contains ONLY .COM, .NET, .EDU domains and

Registrars.

Domain Name: vulnweb.com

Registry Domain ID: D16000066-COM

Registrar WHOIS Server: whois.eurodns.com

Registrar URL: http://www.eurodns.com

Updated Date: 2023-05-26T10:04:20Z

Creation Date: 2010-06-14T00:00:00Z

Registrar Registration Expiration Date: 2025-06-13T00:00:00Z

Registrar: Eurodns S.A.

Registrar IANA ID: 1052

Registrar Abuse Contact Email: legalservices@eurodns.com

Registrar Abuse Contact Phone: +352.27220150

Domain Status: clientTransferProhibited http://www.icann.org/epp#clientTransferProhibited

Registry Registrant ID:

Registrant Name: Acunetix Acunetix

Registrant Organization: Acunetix Ltd

Registrant Street: 3rd Floor,, J&C Building,, Road Town

Registrant City: Tortola

Registrant State/Province:

Registrant Postal Code: VG1110

Registrant Country: VG

Registrant Phone: +1.23456789

Registrant Fax:

Registrant Email: administrator@acunetix.com

Registry Admin ID:

Admin Name: Acunetix Acunetix

Admin Organization: Acunetix Ltd

Admin Street: 3rd Floor,, J&C Building,, Road Town

Admin City: Tortola

Admin State/Province:

Admin Postal Code: VG1110

Admin Country: VG

Admin Phone: +1.23456789

Admin Fax:

Admin Email: administrator@acunetix.com

Registry Tech ID:

Tech Name: Acunetix Acunetix

Tech Organization: Acunetix Ltd

Tech Street: 3rd Floor,, J&C Building,, Road Town

Tech City: Tortola

Tech State/Province:

Tech Postal Code: VG1110

Tech Country: VG

Tech Phone: +1.23456789

Tech Fax:

Tech Email: administrator@acunetix.com

Name Server: ns1.eurodns.com

Name Server: ns2.eurodns.com

Name Server: ns3.eurodns.com

Name Server: ns4.eurodns.com

DNSSEC: unsigned

Ahora también usaremos el comando ‘dig vulnweb.com’ donde vamos a pretender obtener direcciones ip del dominio principal, donde cuando lo ejecutemos en nuestra terminal obtendremos la siguiente información:

Texto

Descripción generada automáticamente

**3. Identificación de IPs**

Para este paso procederemos a utilizar nuevamente el mismo comando ‘dig’ para identificar las ips de los demas sitios hospedados por el mismo sitio.

Rest.vulnweb.com

Texto

Descripción generada automáticamente

testphp.vulnweb.com

Texto

Descripción generada automáticamente

testhtml5.vulnweb.com

Texto

Descripción generada automáticamente

testasp.vulnweb.comTexto

Descripción generada automáticamente

**4. GEOIP: Geolocalización de las direcciones IP**

Ahora procederemos a Geolocalizar las direcciones IP de cada uno de los sitios analizados, para esto utilizaremos el comando ‘geoiplookup’

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente

**5. NMAP/SHODAN: Identificación de servicios y puertos abiertos**

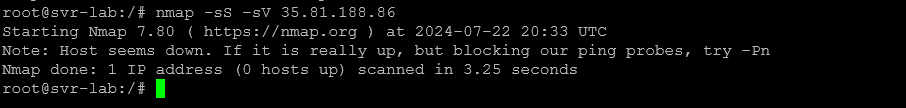
Ahora mismo procederemos a analizar los servicios y puertos abiertos de cada uno de las ips. Para realizar esto lo haremos de la siguiente manera ‘nmap -sS -sV [ip]’

Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente



Procederemos a instalar el siguiente aplicativo shodan para poder escanear nuestras ips de los servidores

Instalaremos nuestras dependencias  
‘sudo apt-get update’

‘sudo apt-get install python3 python3-pip -y’

Instalamos con el siguiente comando

‘pip3 install shodan’

‘shodan init YOUR\_API\_KEY’ (Aca utilizaremos la apikey de nuestro perfil de shodan)



Una vez validado procedemos a ejecutar el siguiente comando con nuestro comando ‘shodan host {ip}’ de la siguiente manera.



Texto

Descripción generada automáticamente

Texto

Descripción generada automáticamente con confianza media