



Prueba número 1

Asignatura: Seguridad de Sistemas

Instrucciones:

- Trabajo individual
- Se realizará por encargo, es decir los estudiantes realizan el trabajo en sus dependencias y entregan un informe con el resultado en un archivo Word.
- Plazo: 1 semana
- Entrega por mail: jaime.gomezg@usm.cl

Pregunta 1 (10 puntos):

Obtenga el “Hosting History” de los siguientes sitios web”.

- <https://www.marca.com/>
- <http://www.lun.com/>
- <https://www.webscantest.com/>
- <http://testphp.vulnweb.com>
- <https://www.usm.cl/>

Pregunta 2 (10 puntos):

Obtenga la categoría de seguridad SSL/TLS de los siguientes sitios:

www.bci.cl

banco.italu.cl

www.marca.com

www.usm.cl

Pregunta 3 (5 puntos):

Obtenga el listado de direcciones de correo disponibles desde el dominio “usm.cl”

Pregunta 4 (10 puntos):

Valide si los siguientes dominios tienen habilitado DNSSec en sus servidores DNS

- microsoft.com
- nis.cl
- usm.cl
- csirt.gob.cl
- nic.cl

Pregunta 5 (20 puntos):

Utilizando workspace con Metasploit obtenga el listado de todos los servicios y sus versiones de las máquinas Metasploitable III y Windows 7, además del sistema operativo.

https://drive.google.com/drive/folders/1O60quNmDxD2l2REDXPg_etCLgbluJ9m6?usp=sharing

<https://developer.microsoft.com/en-us/microsoft-edge/tools/vms/>

Luego realice las siguientes búsquedas:

- Listar todos los servicios web
- Listar los servidores con el puerto 445 abierto
- Listar todos los servidores Apache

Pregunta 6 (20 puntos):

Obtenga la versión del servidor web y del lenguaje de los siguientes sitios web

- <http://webscantest.com/>
- <http://testphp.vulnweb.com/>
- <http://testasp.vulnweb.com/>
- <http://rest.vulnweb.com/>
- <https://altoromutual.com/>

Además, valide si están protegidos por WAF

Pregunta 7 (15 puntos):

Realice la enumeración interna de la máquina Metasploitable III (Linux) utilizando la herramienta Linenum y obtenga lo siguiente:

- Versión del Sistema Operativo
- Listado de usuarios
- Listado de servicios TCP
- Listado de archivos con suid habilitado
- Comandos que puede ejecutar el usuario vagrant utilizando sudo

Pregunta 8 (10 puntos):

Habilite la configuración SNMP en su máquina Windows 10, realice la enumeración de dicho protocolo y obtenga los siguientes datos:

- Listado de usuarios
- Listado de rutas
- Listado de servicios TCP
- Configuración del disco duro
- Listado de aplicaciones instaladas