Informe Ethical Hacking

Snifer@L4b's

JOSE MORUNO CADIMA, Snifer@L4b's

13 de marzo de 2021

Índice general

1 Informe Ethical Hacking Markdown *sniferl4bs.com*

1.1. Introducción

Se realizo la prueba de ethical Hacking al sitio web **www.sniferl4bs.com** con el fin de identificar las vulnerabilidades en el sitio web como en el servidor…

> **ATENCIÓN:** El contenido del presente documento tiene como fin de mostrar como se puede armar un reporte de Pentesting de manera rápida desde Markdown

1.2. Objectivo

Identificar vulnerabilidades.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."

2 Informe Ejecutivo

Se identifico que los servicios expuestos durante la prueba de pentesting cuentan con multiples vulnerabilidades.

2.1. Recomendaciones

Se recomienda realizar un soporte adecuado identificando los subdominios expuestos entre los cuales se identifico que es posible realizar un domain takeover por que los mismos se encuentran vulnerables a continuación se detalla.

Figura 2.1

3 Metodologias utilizadas

- OWASP
- ROADMAP WEB PENTESTING
- Mobile Security Project

4 Enumeración

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."

4.1. Pruebas realizadas

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum."

4.1.1. Datos identificados

4.1.1.0.1. Usuarios

- Usuarios de TI
    - Snifer
    - Gabo
- Administradores de dominios
    - Pepito

4.1.1.0.2. Credenciales

1. Passw0rd!
2. Hack3d!
3. sniferl4bs.com
4. myp4ssw0rd!

> EJEMPLO DE LISTAS

4.1.1.0.3. Servicios

Sitio web	Dirección IP	Puertos
Raspbian	0.0.0.0	
sniferl4bs.com	127.0.0.1	**TCP**: 22, 3389 **UDP**: 22,161

4.1.2. Subdominios identificados

Los subdominios identificados son los siguientes

```
http://20.sniferl4bs.com:80
http://biblioteca.sniferl4bs.com:80
http://craftbooks.sniferl4bs.com:80
http://ctf.sniferl4bs.com:80
http://ebp6l88ugt-r4gd.sniferl4bs.com:80
http://firefoxos.sniferl4bs.com:80
http://gxdy-sprtzop17j-a.sniferl4bs.com:80
http://nba.sniferl4bs.com:80
http://nz.sniferl4bs.com:80
http://pentest.sniferl4bs.com:80
http://rasperry.sniferl4bs.com:80
http://sniferl4bs.com:80
https://t.co:443
http://t.co:80
http://videoteca.sniferl4bs.com:80
http://vip4.sniferl4bs.com:80
https://www.sniferl4bs.com:443
http://www.sniferl4bs.com:80
```

Solución:

La solución es solucionar el problema.

4.1.2.1. Escalamiento de privilegios

Se accedio por el servicio SSH expuesto en el dominio vip4.sniferl4bs.com con las credenciales por defecto *admin:admin*

Mayor detalle tecnico ver los ANEXOS.

5 ANEXOS

5.1. ANEXO I - Recomendaciones

Subsanar las vulnerabilidades.

5.2. ANEXO II - Herramientas utilizadas

Nombre	Version	Descripción
Custom Tool	1.0.0	Aplicación para enumerar
Herramienta II	4.8.9	*Aplicación para explotar*