Universidad Nacional del Sur

Proyecto Final de Carrera
Ingeniería en Computación

Seguridad en redes LAN: utilizando docker para mejorar la infraestructura.

Salvador Catalfamo

Bahía Blanca – Argentina
2020

Universidad Nacional del Sur

Proyecto Final de Carrera
Ingeniería en Computación

Seguridad en redes LAN: utilizando docker para mejorar la infraestructura.

Salvador Catalfamo

Bahía Blanca – Argentina
2020

Resumen

A lo largo de la carrera, hemos visto como las organizaciones abordan los temas de seguridad en sus sistemas informáticos. Mayormente, se concentran en los equipos que están expuestos a la red pública, dejando de lado los que se encuentran aislados de la misma. Erróneamente, muchas veces se piensa que es suficiente, sin embargo, puede traer graves inconvenientes. Es por eso que realizaremos un estudio teórico/práctico sobre las consecuencias de la navegación en redes internas sin ningún tipo de cifrado de datos ni certificaciones.

Palabras Clave:

Seguridad e Infraestructura

Docker

Linux

Kali

Máquinas Virtuales

Índice general

1. Introducción **1**

1.1. Objetivos 1

1.2. Plan de tesis y principales contribuciones 1

1.3. Trabajos previos relacionados 1

2. (Ajustar) ¿Qué circula por una red interna? **1**

2.1. Introducción 2

2.2. Proocolos asociados a la web 2

2.2.1. ¿Que es el protocolo HTTP? 2

2.2.2. Métodos del protocolo HTTP 2

2.2.3. HTTPS con SSL 2

2.3. Protocolos asociados al Correo electrónico (explicacion de todo lo que hace un servidor de correo, y sus protocolos) 2

2.3.1. ¿Que es el protocolo SMTP? 2

2.3.2. Recorrido completo de un mail 2

2.3.3. SMTP con SSL 2

2.4. Protocolos asociados a la consulta de un sitio (DNS) 2

2.4.1. ¿Que es el protocolo DNS? 2

2.4.2. Recorrido completo de un mail 2

2.4.3. SMTP con SSL 2

3. (Nuevo) Herramientas a Utilizar **1**

3.1. El problema de los protocolos http y smtp 2

3.2. Conceptos básicos 2

3.2.1. Snoofing 2

3.2.2. Spoofing . . . 2
3.2.3. Arp attack . . . 2
3.3. Herramientas utilizadas . . . 2
3.3.1. Kali Linux . . . 2
3.3.2. Ettrcap . . . 2
3.3.3. Wireshark . . . 2
3.4. Casos de estudio . . . 2
3.4.1. Caso de estudio: Sniffing de la red para obtener credenciales . . . 2
3.4.2. Caso de estudio: Sniffing de la red para obtener mails internos/externos . . . 2

4. Casos de estudio (Explotaciones y soluciones) 1
4.1. (Seccion va para Herramientas utilizadas)Conceptos básicos . . . 2
4.1.1. Virtualización . . . 2
4.1.1.1. Máquinas virtuales . . . 2
4.1.1.2. Máquinas Docker . . . 2
4.1.2. Certificación SSL . . . 2
4.1.2.1. En qué consiste una Certificación SSL . . . 2
4.1.2.2. Challenges en una Certificación . . . 2
4.2. Mejorando la seguridad en la navegación - Alternativas . . . 2
4.2.1. Self-signed Certificates . . . 2
4.2.2. Internal CA . . . 2
4.2.3. Estrategia utilizadas, ojala que con let's encrypt . . . 2
4.3. Estrategia . . . 2
4.4. CertBot para redes internas . . . 2
4.5. Mejorando la seguridad en los servidores de correo . . . 2

5. Conclusiones y Resultados Obtenidos 3

A. Glosario 5
A.1. Terminología . . . 5
A.2. Simbología . . . 5

Capítulo 1

Introducción

1.1. Objetivos

- item 1
- item 2

```
 Este es un bien ambiente para
poner codigo
```

En [5] se [1] ve...

casa

casa

`casa`

casa

casa

1.2. Plan de tesis y principales contribuciones

1.3. Trabajos previos relacionados

[1] Esta es una nota al pie

Figura 1.1: Esta es la figura del escudo de la uns

Capítulo 2

(Ajustar) ¿Qué circula por una red interna?

2.1. Introducción

2.2. Proocolos asociados a la web

2.2.1. ¿Que es el protocolo HTTP?

2.2.2. Métodos del protocolo HTTP

2.2.3. HTTPS con SSL

2.3. Protocolos asociados al Correo electrónico (explicacion de todo lo que hace un servidor de correo, y sus protocolos)

2.3.1. ¿Que es el protocolo SMTP?

2.3.2. Recorrido completo de un mail

2.3.3. SMTP con SSL

2.4. Protocolos asociados a la consulta de un sitio (DNS)

2.4.1. ¿Que es el protocolo DNS?

2.4.2. Recorrido completo de un mail

Capítulo 3

(Nuevo) Herramientas a Utilizar

En éste capítulo se verá por qué los protocolos http y smtp son inseguros, introducción al snnifin, spoofing, arp attack

3.1. El problema de los protocolos http y smtp

3.2. Conceptos básicos

3.2.1. Snoofing

3.2.2. Spoofing

3.2.3. Arp attack

3.3. Herramientas utilizadas

3.3.1. Kali Linux

3.3.2. Ettrcap

3.3.3. Wireshark

3.4. Casos de estudio

3.4.1. Caso de estudio: Sniffing de la red para obtener credenciales

3.4.2. Caso de estudio: Sniffing de la red para obtener mails internos/externos

Capítulo 4

Casos de estudio (Explotaciones y soluciones)

4.1. (Seccion va para Herramientas utilizadas)Conceptos básicos

4.1.1. Virtualización

4.1.1.1. Máquinas virtuales

4.1.1.2. Máquinas Docker

4.1.2. Certificación SSL

4.1.2.1. En qué consiste una Certificación SSL

4.1.2.2. Challenges en una Certificación

4.2. Mejorando la seguridad en la navegación - Alternativas

4.2.1. Self-signed Certificates

4.2.2. Internal CA

4.2.3. Estrategia utilizadas, ojala que con let's encrypt

4.3. Estrategia

4.4. CertBot para redes internas

Capítulo 5

Conclusiones y Resultados Obtenidos

Apéndice A

Glosario

A.1. Terminología

Término en inglés	**Traducción utilizada**
argument	argumento
argumentative system	sistema argumentativo
assumption	suposición
atom	átomo
backing	fundamentos
blocking defeater	derrotador de bloqueo
burden of proof	peso de la prueba
claim	afirmación

A.2. Simbología

Símbolo	**Página**	**Significado**
$\neg h$	103	negación fuerte del átomo h

Bibliografía

[1] Bondarenko, A., Dung, P. M., Kowalski, R., and Toni, F. An abstract argumentation–theoretic approach to default reasoning. *Artificial Intelligence 93*, 1–2 (1997), 63–101.

[2] Capobianco, M. El Rol de las Bases de Dialéctica en la Argumentación Rebatible. tesis de licenciatura, July 1999.

[3] Capobianco, M., Chesñevar, C. I., and Simari, G. R. An argumentative formalism for implementing rational agents. In *Proceedings del 2do Workshop en Agentes y Sistemas Inteligentes (WASI), 7mo Congreso Argentino de Ciencias de la Computación (CACIC)* (El Calafate, Santa Cruz, Oct. 2001), Universidad Nacional de la Patagonia Austral, pp. 1051–1062.

[4] Chesñevar, C. I. *Formalización de los Procesos de Argumentación Rebatible como Sistemas Deductivos Etiquetados*. PhD thesis, Departamento de Ciencias de la Computación, Universidad Nacional del Sur, Bahía Blanca, Argentina, Jan. 2001.

[5] Davis, R. E. *Truth, Deduction, and Computation*. Computer Science Press, 1989.

[6] García, A. J. La Programación en Lógica Rebatible: su definición teórica y computacional. Master's thesis, Departamento de Ciencias de la Computación, Universidad Nacional del Sur, Bahía Blanca, Argentina, July 1997.

[7] Haenni, R. Modeling uncertainty with propositional assumption-based systems. In *Applications of uncertainty formalisms*, A. Hunter and S. Parsons, Eds. Springer-Verlag, 1998, pp. 446–470.