

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
1.1.1. objetivos principales	1
1.1.1.1. particulares	1
1.2. Plan de tesis y principales contribuciones	2
1.3. Trabajos previos relacionados	2
2. ¿Qué circula por una red interna?	1
2.1. Introducción	1
2.2. Protocolo HTTP/HTTPS	1
2.2.1. ¿Que es el protocolo HTTP?	1
2.2.2. Métodos del protocolo HTTP	1
2.2.3. HTTPS con SSL	1
2.3. Protocolo SMTP/SMTPS	1
2.3.1. ¿Que es el protocolo SMTP?	1
2.3.2. Recorrido completo de un mail	1
2.3.3. SMTP con SSL	1
3. Descripción del problema	1
3.1. El problema de los protocolos http y smtp	1
3.2. Conceptos básicos	1
3.2.1. Snoofing	1
3.2.2. Spoofing	1
3.2.3. Arp attack	1
3.3. Caso de estudio: Sniffing de la red para obtener credenciales	1

3.4. Caso de estudio: Sniffing de la red para obtener mails internos/externos	1
4. Implementación de la solución propuesta	1
4.1. Estrategia	2
4.2. Conceptos básicos	2
4.2.1. Virtualización	2
4.2.1.1. Máquinas virtuales	2
4.2.1.2. Máquinas Docker	2
4.2.2. Certificación SSL	2
4.3. Herramientas utilizadas	2
4.3.0.1. Kali Linux	2
4.3.0.2. Etmcap	2
4.3.0.3. Wireshark	2
4.4. Mejorando la seguridad en la navegación	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

1.1.1. objetivos principales

1.1.1.1. particulares

¹Esta es una nota al pie

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

1.2. Plan de tesis y principales contribuciones

1.3. Trabajos previos relacionados

Capítulo 2

¿Qué circula por una red interna?

2.1. Introducción

2.2. Protocolo HTTP/HTTPS

2.2.1. ¿Que es el protocolo HTTP?

2.2.2. Métodos del protocolo HTTP

2.2.3. HTTPS con SSL

2.3. Protocolo SMTP/SMTPS

2.3.1. ¿Que es el protocolo SMTP?

2.3.2. Recorrido completo de un mail

2.3.3. SMTP con SSL

Capítulo 3

Descripción del problema

En éste capítulo se verá por qué los protocolos http y smtp son inseguros, introducción al snifin, 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. Caso de estudio: Sniffing de la red para obtener credenciales

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

Capítulo 4

Implementación de la solución propuesta

4.1. Estrategia

4.2. Conceptos básicos

4.2.1. Virtualización

4.2.1.1. Máquinas virtuales

4.2.1.2. Máquinas Docker

4.2.2. Certificación SSL

4.3. Herramientas utilizadas

4.3.0.1. Kali Linux

4.3.0.2. Ettercap

4.3.0.3. Wireshark

4.4. Mejorando la seguridad en la navegación

4.5. Mejorando la seguridad en los servidores de correo

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.