

Prueba número 3

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 o PDF.
- Plazo: 1 semana
- Entrega por mail: jaime.gomezg@usm.cl

Pregunta 1 (25 puntos):

Realice la creación de un malware troyano, utilizando la aplicación putty como contenedor, luego realice el análisis utilizando Virustotal y evidencie el resultado.

Pregunta 2 (25 puntos):

Obtenga las contraseñas cuyos digest están listados a continuación utilizando la herramienta john the Ripper.

25f9e794323b453885f5181f1b624d0b

5f4dcc3b5aa765d61d8327deb882cf99

d8578edf8458ce06fbc5bb76a58c5ca4

e99a18c428cb38d5f260853678922e03

098f6bcd4621d373cade4e832627b4f6

Dados estos dos archivos de contraseña y usuarios de un sistema Linux, debe encontrar las contraseñas de los 5 usuarios.

<u>Usuarios:</u>

user1:x:1001:1001::/home/user1:/bin/sh

user2:x:1002:1002::/home/user2:/bin/sh

user3:x:1003:1003::/home/user3:/bin/sh

user4:x:1004:1004::/home/user4:/bin/sh

user5:x:1005:1005::/home/user5:/bin/sh

Contraseñas:

user1:\$6\$BuN/EYaVqwxKgtDH\$/kwRUUkQYuPA3Bx7jj.g39vWBqYNl4YjSwyQsQfgSEltrV0Fp1kA.H9n6710G80AbHjP9h8QZitVFKbk9bgBM0:18451:0:99999:7:::

user2:\$6\$PR1FnaiRT8i9nlo2\$JkUrtvR9PmA2lbYqGM5ECjM/vqYvsueSeOWl0.YCqEbWuqxJkhZ6qdY CSG4wkkM5h3SFzi0lYyyhYJ8zeiRVB0:18451:0:99999:7:::

user3:\$6\$/DUAkOu1b/By05o8\$2JTlzyJGjD/Sg048Xdjqsv5/59VSE2T8tWGlPCLMGHreixsFcOYqutrxMfau7zY5jNfAddTbqg8O78bq.GrN00:18451:0:99999:7:::

user4:\$6\$vQjkPAsNW4wB6hDS\$XJDnC/uufKzWPItTt4djZ6DWgsXxAlVISxcvm9xmgvnz2JoZQqlOMbcLhpKfpSQDnf9cvlURklwFn5n7t70k31:18451:0:99999:7:::

user5:\$6\$Q41qgfZpYqdadbrT\$2vHKOfqBJsueNvvWeDBEYoKkh0dHQEZ.vo9tu3ANfMZUu2F8JaYzbn D4erFcpi8.uKXlQk1tV7gmNk2/HteYf1:18451:0:99999:7:::

Pregunta 3 (25 puntos):

El siguiente archivo fue obtenido a través de una captura de autenticación a un sistema SMB de Microsoft, debe encontrar la contraseña del usuario.

mssal-

Pregunta 4 (25 puntos):

Realice la creación de un túnel HTTP utilizando la aplicación reDuh y genere algún tipo de tráfico encapsulado y evidencia la captura de tráfico solamente de paquetes HTTP