Practica 2: CSIRTs Parte 2

Nota: Buscar en la plataforma CTFd los archivos referenciados por los distintos ejercicios.

Análisis de encabezados

Ejercicio 05

Analice los encabezados del mensaje **mail_1.eml** y responda:

a) ¿Quién es el destinatario del mensaje?
b) ¿Cuál es el servidor de mail utilizado para recepcionar los mails de ese dominio?
c) Identifique en los headers la dirección IP que se conectó al servidor SMTP del destinatario para enviar el mensaje.
d) Si quisiera notificar al responsable del servidor desde el cuál se envió el mensaje, ¿cuál sería el punto de contacto adecuado para contactar al responsable?

Ejercicio 06

Analice los encabezados del mensaje **mail_2.eml** y responda:

a) ¿Quién es el destinatario del mensaje?
b) ¿Cuál es el servidor de mail utilizado para recepcionar los mails de ese dominio?
c) Identifique en los headers la dirección IP que se conectó al servidor SMTP del destinatario para enviar el mensaje.
d) Si quisiera notificar al responsable del servidor desde el cuál se envió el mensaje, ¿cuál sería el punto de contacto adecuado para contactar al responsable?

GESTION DE INCIDENTES

El objetivo es experimentar con las tareas que Ud. realizaría si trabajara en un CSIRT.
En caso de ser necesario, considere que su **comunidad objetivo** es:

```
El bloque IP 163.10.0.0/16
El dominio *.unlp.edu.ar
```

Nota: tenga en cuenta que todas las situaciones planteadas, aunque estén basadas en la realidad, son hipotéticas y no contienen datos reales sobre el origen o el destino de incidentes.

Ejercicio 07

El administrador de una red de investigación de la UNLP nos solicitó ayuda porque lo notificaron en varias oportunidades que llegan mails desde la cuenta admin@bankination.ctf.cert.unlp.edu.ar con estafas.

El administrador analizó los logs del servidor y asegura que los mensajes de mail no salieron de ahí. La semana pasada le informaron que vieron esos mails provenientes de otras cuentas del dominio, incluso algunas que no existen como **ic@bankination.ctf.unlp.edu.ar**.

Analiza la información dada para encontrar una posible causa del comportamiento observado de forma tal de poder recomendar buenas prácticas para que solucione el problema.

Ejercicio 08

Analizando los siguientes LOGS de un servidor interno que expone el puerto SSH a Internet para que el administrador se conecte desde la casa, responda:

```
# grep sshd.\*Failed /var/log/auth.log
Aug 18 23:08:26 sshd[768]: Failed password for root from 91.205.189.15 port 38156 ssh2
Aug 18 23:08:30 sshd[770]: Failed password for nobody from 91.205.189.15 port 38556 ssh2
Aug 18 23:08:34 sshd[772]: Failed password for invalid user asterisk from 91.205.189.15 port 38864 ssh2
Aug 18 23:08:38 sshd[774]: Failed password for invalid user sjobeck from 91.205.189.15 port 39157 ssh2
Aug 18 23:08:42 sshd[776]: Failed password for root from 91.205.189.15 port 39467 ssh2
```

a. ¿De qué tipo de incidente se trata?
b. Dirección de correo a la que se debería reportar la actividad maliciosa
c. Recomendaciones que se le podrían dar al administrador del servidor atacado.

Ejercicio 09

Monitoreando el tráfico de red, vi algo extraño. Uno de los servidores de la Universidad estaba haciendo muchos pings a una IP desconocida. Parte de este tráfico de red fue capturado en la captura llamada **tráfico raro.pcapng**. Se cree que se trata de un canal encubierto[1][2].

[1] Covert Channel - https://www.sans.org/reading-room/whitepapers/detection/covert-channels-33413
[2] Canal encubierto - https://es.wikipedia.org/wiki/Canal_encubierto

Ejercicio 10

Alguien me comentó que vió algo raro en uno de los protocolos de esta captura. No me llegó a mostrar nada, se tenía que ir... Me dijo que seguramente era un canal encubierto porque le pareció que usaban de una forma anormal uno de los protocolos…
Fijate por favor, no quiero molestarlo otra vez y tener que devolverle un favor.

Ejercicio 11

Un empleado de una de las facultades de la UNLP, informó sobre algo extraño. Dice que le hackearon la PC. Sospecha de un técnico que hace unos días fue a realizar unos arreglos y se olvidó de un pendrive raro que tiene un sticker que dice: rubber ducky. En el pendrive había un archivo extraño. ¿Puedes analizar este archivo para entender lo que pasó?