Contents

1 Cuestionario

Pregunta 1
Menciona los tipos de protocolos de red

Respuesta:

- **Protocolos de comunicación**
  Son los que se encargan de establecer y gestionar las conexiones entre diferentes dispositivos.
  - TCP/IP
  - FTP
  - SSH
  - HTTP
- **Protocolos de transporte**
  Son los encargados de transportar datos entre dispositivos.
  - TCP
  - UDP
- **Protocolos de aplicación**
  Son aquellos que se utilizan para aplicaciones específicas, como el uso de redes sociales y el envio de correos electrónicos.
  - SMTP
  - POP3
  - IMAP
  - DNS
- **Protocolos de enrutamiento**
  Aquellos utilizados para dirigir los paquetes de datos a través de la red.
  - OSPF
  - RIP
  - BGP
- **Protocolos de seguridad**
  Son los encargados de proteger la información transmitida en la red.
  - SSL/TLS

  - IPsec
  - SSH

- **Protocolos de gestión**
  Utilizados para administrar y monitorear dispositivos de red.
  - SNMP
  - NetFlow

Pregunta 2
Respecto a tu pregunta anterior ¿Cómo funcionan? ¿Para qué sirven?

Respuesta:

Resuelto en la respuesta anterior.

Pregunta 3
¿Qué es un sniffer?

Respuesta:
Se puede defininir como un software el cual está diseñado específicamente para redes, con el proposito de capturar y analizar los paquetes que se envían y reciben.
El *sniffer* sería capáz de detectar qué estamos visitando, qué información enviamos, etc. De esta forma nuestra privacidad podría verse comprometida.

Pregunta 4
OSINT, ¿Qué es? ¿Para qué sirve?

Respuesta:
Open Source INTelligence

Es el conjunto de técnicas y herramientas para recopilar información pública, analizar los datos y correlacionarlos convirtiéndolos en conocimiento útil.

Su utlidad se basa en conseguir toda la información disponible en cualquier fuente pública sobre una empresa, persona física o cualquier otra cosa sobre la que queremos recopilar información para realizar una investigación, y haciendo que todo el conjunto de datos se convierta en inteligencia que nos sirva para ser más eficaces a la hora de querer obtener un resultado.

Pregunta 5
Investiga los 5 OSINT más usados.

Respuesta:

1. ***Google***
2. ***Redes sociales***
   - Facebook
   - Twitter
   - Linkedln
   - Instagram
3. ***Wayback Machine***
   Es un servicio y una base de datos que contiene copias de una gran cantidad de páginas de Internet, con esto se pueden consultsr diferentes versiones de páginas de Internet.

4. ***Maltego***
   Es una herramienta de visualización de datos que permite establecer relaciones y conexiones entre personas, organizaciones y otras entidades.

5. ***Shodan***
   Es un motor de busqueda que registra información sobre dispositivos conectados a Internet, como servidores, routers, cámaras web, etc.

Pregunta 6
¿Por qué el eslabón más débil de seguridad es el humano?

Respuesta:
Esto se debe al hecho de que el ser humano no es perfecto y es facilmente influenciable.//

Teniendo como consencuencias que seamos propensos a cometer errores y ser manipulados y engañados. Lo cual, en materia de seguridad, puede llegar a tener repercuciones como caer en estafas o extersiones. Dando un ejemplo más a fin, tomemos como ejemplo el phising o cuando compartimos contraseñas de redes sociales, cuentas de banco o del trabajo a personas sin pensar en las consecuencias que esto podría llegar a tener. Y esto más que nada es dado a que los humanos somos seres sentimentales y nuevamente, muy influenciables de lo que sucede en nuestro entorno.

Pregunta 7
¿Qué acciones haces para protegerte de ciberataques?

Respuesta:
Actualmente, ambos integrantes del equipo no estabamos al corriente en todos las posibles maneras en las que nuestra seguridad infórmatica puede llegar a ser perturbada. Por lo que en estos mommentos creemos que la acción más "segura" que usamos es la autenticación por 2 pasos.

Pregunta 8
¿Crees que tus métodos preventivos son suficientes?

Respuesta:
No, tal vez la autetenrticación por 2 pasos hoy en día es un buen mecanismo, pero creemos que podemos hacer más para proteger nuestra información.

2 Reporte Script

2.1 Requisitos

Pregunta
¿Qué problema queremos resolver o qué queremos saber? ¿Qué información necesitamos? ¿Para qué?

Nos interesa, mediante los protocolos con los que funciona internet y ciertas herramientas (*software*) ya existentes, poder sacar la mayor información de como funcionan ciertos sistemas (*objetivos*), en especifíco recopilar como es que se comunican en internet o que servicios/procesos están en constante ejecución, ya sea que cierto sistema operativo o algúna aplicación tenga falla y tratar de identificar en que sentido el sistema es vulnerable.

2.2 Indentificación de fuentes de información?

Pregunta
¿Qué fuentes nos pueden aportar información valiosa y veraz?

Creemos que lo valioso depende de las habilidades y conocimiento de uno, sí sabemos que en cierto puerto se ejecuta algún proceso con alguna vulnerabilidad entonces podriamos atacar, o si por otro lado el protocolo que usa una red nos permite identificarnos como un tercero. De donde nos podemos agarrar para recopilar es de las herramientas ya creadas que permiten el paso de mensajes en el sistema web actual, así mismo tambíen las personas pueden ser una fuente de información, ya sea que ellos la posean y la compartan o tengan credenciales para algún sistema con las cuales se podría obtener.

Sabemos que las herramientas que permiten el paso de mensajes son veraces pues permiten un correcto funcionamiento del internet, las personas podrian serlo o no, al igual que una base de datos. En un principo la base no deberia tener error o información basura, pero con gente capacitada quizá sea un cebo, es así que creemos que se puede confiar en herramientas/software/información que es de dominio público y tienen algún funcionamiento en la sociedad. Las vulnerabilidades que buscamos se auxilian de esta información, habilidades y experiencia.

2.3 Adquisición

Pregunta
Etapa de obtención de la información. Explicación script.

Para el *script*, nos ayudamos en los comandos de linux compartidos por Ximena.

2.4 Procesamiento

Pregunta
Dar formato a toda la información "en bruto" obtenida en la anterior fase. En caso de querer obtener más información explicar el posible uso de la misma, así como su relevancia.

2.5 Análisis

Pregunta
Generar datos de inteligencia a partir de todos los datos obtenidos, encontrando relaciones entre estos que nos permitan llegar a conclusiones (vulnerabilidades).

2.6 Presentación

Pregunta
Darle a la información y conclusiones un formato en el que se pueda comprender de manera eficaz y sencilla presentando así tus propias propuestas de ataque.

References

[1] https://autmix.com/blog/que-es-protocolo-red

[2] https://derechodelared.com/osint/