Creando una Trayectoria Profesional en Seguridad Digital

Laboratorio 1: Fundamentos de la Ciberseguridad

Agosto, 2021

Índice

1. Laboratorio 1A

Acerca del Laboratorio 1A

Objetivos: *Entendiendo procesos, conexiones y usuarios.*

Requerimientos: Utilice la máquina con sistema operativo Kali Linux, si su host es el sistema Operativo Windows, realice también el punto 1.2 de este laboratorio.

1.1. Plataforma Linux

1. Inicie una ventana de la terminal (bash) del sistema operativo Kali Linux
2. Identifique los usuarios locales con el comando:

   $ **cat** /etc/passwd

3. Identifique las interfaces de red con o sin dirección IP asignada:

   $ ip link show

4. Identifique las direcciones IP asignadas a su equipo mediante el comando:

   $ sudo ifconfig

5. Identifique los los procesos activos, mediante el comando:

   $ **ps** –aux

6. Identifique las conexiones abiertas con el comando:

   $ netstat –anop

1.2. Plataforma Windows

1. Inicie una ventana de la terminal de DOS (cmd) (*Inicio* > *ejecutar* > *cmd.exe*)
2. Identifique los usuarios locales mediante el comando:

```
Microsoft Windows [Version 10.0.19042.867]
Copyright (c) 2020 Microsoft Corporation. All rights reserved.

net users
```

3. Identifique la dirección IP asignada a su equipo con el comando:

```
Microsoft Windows [Version 10.0.19042.867]
Copyright (c) 2020 Microsoft Corporation. All rights reserved.

ipconfig
```

4. Identifique la dirección los procesos activos mediante el comando:

```
Microsoft Windows [Version 10.0.19042.867]
Copyright (c) 2020 Microsoft Corporation. All rights reserved.

tasklist /v
```

5. Identifique las conexiones abiertas con el comando:

```
Microsoft Windows [Version 10.0.19042.867]
Copyright (c) 2020 Microsoft Corporation. All rights reserved.

netstat -ano
```

2. Laboratorio 1B

Acerca del Laboratorio 1B

Objetivos:*Interpretando el tráfico de la red.*

Requerimientos: Utilice la herramienta de análisis de protocolos de red Wireshark.

1. Inicie el analizador de protocolos Wireshark
2. Abra el archivo con capturas de tráfico de red `192.168.56.101.pcap` contenido en la carpeta compartida *Laboratorio 1*

   `File` > `Open` > `192.168.56.101.pcap`

3. Identifique el *saludo de tres vías del protocolo TCP* . Puede utilizar el siguiente filtro en Wireshark:

   ```
   tcp.flags.syn==1 or (tcp.seq==1 and tcp.ack==1 and tcp.len==0
   and tcp.analysis.initial_rtt)
   ```

4. Identifique las direcciones IP origen y destino de la conexión
5. Identifique los puertos TCP origen y destino de la conexión
   - Realice una lectura en formato `ASCII` del contenido de la comunicación
   - Sobre uno de los paquetes capturados, seleccione `Follow, TCP Stream` **¿Puede ver el contenido del paquete?**
6. Identifique el intercambio de llaves públicas del protocolo SSH
   - Sobre uno de los paquetes capturados, seleccione Follow, TCP Stream. **¿Puede ver el paquete cifrado?**
7. Realice una lectura del contenido de los paquetes filtrados en el protocolo TELNET Y HTTP
   - Puede utilizar el siguiente filtro para encontrar algún inicio de sesión mediante el protocolo HTTP mediante el método POST:

     `frame contains "user"` && `http.request.method == "POST"`

- Puede utilizar sl siguiente filtro para encontrar si el frame en la sección de datos (*data*) del protocolo TELNET contiene la palabra *bandera*:

  `telnet` && `frame contains "bandera"`

- **¿Puede identificar el contenido en texto plano?**
- **¿Puede localizar las banderas?**