Trabajo Práctico N°5

Sniffing

1. Instalar el sniffer Snort (www.snort.org).

Hecho. Hubo que realizar algunas adaptaciones para poder ejecutarlo en entorno Windows. Se adjuntan archivos modificados/agregados en https://github.com/poximan/ARS/tree/master/tp5/Snort.

2. Buscar en internet un formulario en un sitio seguro (https) y realizar el análisis de paquetes

("sniffear") del envío de los datos del formulario. Localizar el contenido de los distintos campos y explicar lo encontrado.

Se probó con https://bancainternet.bancocredicoop.coop/bcclbi/. La ip tomada al momento del test fue 200.47.24.9.

No se encontró ningún campo, esta todo cifrado. Lo único fue la referencia a la url, porque va plana.

Se adjunta volcado de trafico (ver pto2-dump-seg.txt).

3. Realizar el análisis de paquetes ("sniffear") del envío de los datos del formulario del sitio http://www.geonames.org/login. Localizar el contenido de los distintos campos y explicar lo encontrado.

Se probó la url sugerida. La ip tomada al momento del test fue 188.40.62.8.

Se encontraron los datos de formulario de login planos. No hay nada cifrado. Mi prueba fue usuario → "nuevo-usuario" y contraseña → "nueva-contraseña".

Se adjunta volcado de trafico (ver pto3-dump-noseg.txt).

4. Realizar el análisis de paquetes ("sniffear") del envío de los datos del formulario del sitio http://www.apps.jsf2.com/xhtml/post-form.html. Localizar el contenido de los distintos campos y explicar lo encontrado.

Se trata de un formulario malicioso que habilita el protocolo SSDP para descubrir servicios de red. Es independiente en cuando a que no necesita asistencia de un servidor remoto. Ademas en la base del protocolo UpnP. Al habilitar este protocolo, se esta generando un ataque de reflexión SSDP, que habilita a un atacante externo a obtener y redireccionar las respuestas, generando un DDoS.

El trafico generado se compone de tramas UDP (ver pto4-dump-post.txt).

5. Realizar el análisis de paquetes ("sniffear") mientras:

    1. La PC recibe comandos ping de otra PC.

```
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
WARNING: No preprocessors configured for policy 0.
06/07-19:07:04.344901 D0:57:7B:17:53:C7 -> 10:7D:1A:3E:CA:2D type:0x800 len:0x62
192.168.18.121 -> 192.168.18.119 ICMP TTL:64 TOS:0x0 ID:251 IpLen:20 DgmLen:84 DF
Type:8  Code:0  ID:4854   Seq:132  ECHO
7F AC 19 5B 00 00 00 00 78 89 06 00 00 00 00 00  ...[....x.......
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                          01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
06/07-19:07:04.345126 10:7D:1A:3E:CA:2D -> D0:57:7B:17:53:C7 type:0x800 len:0x62
192.168.18.119 -> 192.168.18.121 ICMP TTL:128 TOS:0x0 ID:24952 IpLen:20 DgmLen:84
Type:0  Code:0  ID:4854  Seq:132  ECHO REPLY
7F AC 19 5B 00 00 00 00 78 89 06 00 00 00 00 00  ...[....x.......
10 11 12 13 14 15 16 17 18 19 1A 1B 1C 1D 1E 1F  ................
20 21 22 23 24 25 26 27 28 29 2A 2B 2C 2D 2E 2F   !"#$%&'()*+,-./
30 31 32 33 34 35 36 37                          01234567
=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+=+
```

    2. La PC realiza comandos ping a otra PC.

=+

06/07-19:14:48.405752 10:7D:1A:3E:CA:2D -> D0:57:7B:17:53:C7 type:0x800 len:0x4A

192.168.18.119 -> 192.168.18.121 ICMP TTL:128 TOS:0x0 ID:25239 IpLen:20 DgmLen:60

Type:8 Code:0 ID:1   Seq:343 ECHO

61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop

71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi

=+

WARNING: No preprocessors configured for policy 0.

06/07-19:14:48.444304 D0:57:7B:17:53:C7 -> 10:7D:1A:3E:CA:2D type:0x800 len:0x4A

192.168.18.121 -> 192.168.18.119 ICMP TTL:64 TOS:0x0 ID:3308 IpLen:20 DgmLen:60

Type:0 Code:0 ID:1 Seq:343 ECHO REPLY

61 62 63 64 65 66 67 68 69 6A 6B 6C 6D 6E 6F 70 abcdefghijklmnop

71 72 73 74 75 76 77 61 62 63 64 65 66 67 68 69 qrstuvwabcdefghi

=+

Localizar los paquetes relacionados con los comandos ping y explicar.

Los tipos para ECHO ping y ECHO REPLY ping están cruzados. Cuando localhost ejecuta ping, genera ECHO y recibe ECHO REPLY.

Cuando el equipo remoto ejecuta ping, localhost recibe ECHO y genera ECHO REPLY.

6. Explique para qué se puede utilizar el modo Network Intrusion Detection System (NIDS) de snort.

Para detectar intrusos en la red, anomalías o riesgos como ataques de denegación de servicio, consulta cíclica de puertos o intentos de entrar a un equipo. Por definición, snord observa el tráfico en la red analizando paquetes, entonces usarlo para implementar NDIS implica buscar patrones sospechosos durante el análisis de trafico.

En caso de detectar un ataque, puede tomar medidas protectoras.

7. Explique por qué es inseguro utilizar hubs en una red.

Porque replican todo el trafico en todos los puertos conectados. Trabaja por inundación enviando contenido potencialmente sensible a destinatarios no deseados por el remitente. En este sentido, el peor caso para un switch -que es cuando hace broadcast- es mas protectivo porque no inunda la red con el mensaje del remitente, sino con un paquete especial para aprendizaje de la topología. Una vez localizado el puerto de reenvío, despacha el mensaje del remitente.

8. ¿Es posible realizar un análisis de paquetes (“sniffing”) de un switch?

Es posible, pero en forma pasiva solo podría escucharse el propio trafico de esa boca. En caso de tener acceso administrador al switch, podrían programarse reenvios de paquetes destinados a otras bocas. En este ultimo caso la “observación” de paquetes sería mas provechosa.

En caso que el switch no permita este tipo de servicios (el reenvio), no tendría sentido monitorearlo.