**TLP: Amber | AMS | Evento de Seguridad | DSM | Múltiples Reconocimientos de Puertos**

Buena tarde;

Durante el monitoreo de la consola Deep Security se detectaron eventos de reconocimiento:

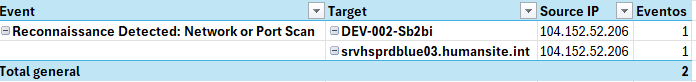
|  |  |
| --- | --- |
| **Equipos:** | * **DEV-002-Sb2bi** * **srvhsprdblue03.humansite.int** |
| **Source IP:** | * 104[.]152[.]52[.]206 * 104[.]152[.]52[.]206 |
| **Detección:** | Reconnaissance Detected: Network or Port Scan |
| **Eventos:** | 2 |

Un network scan (escaneo de red) es una técnica utilizada para identificar hosts activos y servicios en una red. El objetivo es detectar qué dispositivos están en línea, sus direcciones IP y qué servicios están disponibles en esos dispositivos. Puede realizarse utilizando varias herramientas de software y técnicas, como el ping sweep, el escaneo de puertos y el escaneo de subredes.

Por otro lado, un port scan (escaneo de puertos) es una técnica utilizada para identificar qué puertos están abiertos en un dispositivo. Puede indicar qué servicios están disponibles en el dispositivo y puede ser utilizado por atacantes para identificar posibles vulnerabilidades de seguridad que puedan ser explotadas.

Los equipos con las direcciones IP´s mencionadas están realizando un escaneo de la computadora o la red. Ha escaneado o intentado escanear un total de una computadora.

**Anexamos Evidencia:**



\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Equipos:** | * **.** **BLUESERVER02-DHL** * **Sb2bserverRE-QA** |
| **Source IP:** | * **47[.]238[.]231[.]72** * **47[.]238[.]231[.]72** |
| **Detección:** | * Reconnaissance Detected: Computer OS Fingerprint Probe |
| **Eventos:** | 2 |

Si un “hacker” puede determinar qué tipo de sistema operativo está ejecutando una computadora objetivo, puede trabajar para explotar las vulnerabilidades presentes en ese sistema operativo.

 OS Fingerprinting es utilizado por profesionales de seguridad y hackers para mapear redes remotas y determinar qué vulnerabilidades pueden estar presentes para explotar.

Los equipos con las direcciones IP´s mencionadas intentaron realizar una sonda de "huella digital" para identificar el sistema operativo

**Se anexa evidencia:**

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

|  |  |
| --- | --- |
| **Equipos:** | * AppserverRE * Sb2bSrvRecibo * SMTPSVRCFDINET[.]ams[.]local * DBserverRe-QA * srvhsprdblue03[.]humansite[.]int * Sb2bserverRE-QA * DbserverRecibo * DbserverDev * AppserverRE-QA * appserverDev * DEV-002-Sb2bi * smtpserverhs[.]ams[.]local * SMTPSERVERENL[.]ams[.]local |
| **Source IP:** | * 159[.]192[.]105[.]100 * 220[.]133[.]20[.]40 * 114[.]32[.]100[.]73 * 77[.]107[.]131[.]96 * 177[.]85[.]224[.]93 * 220[.]133[.]92[.]196 * 159[.]192[.]104[.]79 * 128[.]22[.]175[.]67 * 74[.]218[.]29[.]74 * 1[.]34[.]85[.]243 * 59[.]126[.]252[.]139 * 159[.]192[.]106[.]207 * 218[.]161[.]74[.]135 * 220[.]135[.]113[.]71 * 14[.]136[.]23[.]194 * 114[.]33[.]37[.]21 * 114[.]33[.]11[.]178 * 174[.]57[.]71[.]99 * 220[.]132[.]135[.]212 * 128[.]199[.]181[.]4 * 1[.]174[.]20[.]156 |
| **Detección:** | * Reconnaissance Detected: TCP SYNFIN Scan |
| **Eventos:** | 96 |

Los equipos con las direcciones previamente mencionadas enviaron un paquete con los indicadores TCP "SYN" y "FIN" establecidos, una combinación ilegal. Esto casi siempre significa que está realizando un escaneo "FIN" para determinar qué puertos están abiertos.

**Se anexa evidencia:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Reconnaissance Detected: TCP SYNFIN Scan** | **appserverDev** | 159[.]192[.]104[.]79 | 1 |
| 159[.]192[.]106[.]207 | 1 |
| 59[.]126[.]252[.]139 | 1 |
| 74[.]218[.]29[.]74 | 1 |
| **AppserverRE** | 1[.]174[.]20[.]156 | 1 |
| 114[.]32[.]100[.]73 | 1 |
| 159[.]192[.]104[.]79 | 1 |
| 159[.]192[.]105[.]100 | 4 |
| 159[.]192[.]106[.]207 | 1 |
| 177[.]85[.]224[.]93 | 1 |
| 77[.]107[.]131[.]96 | 2 |
| **AppserverRE-QA** | 1[.]34[.]85[.]243 | 1 |
| 128[.]22[.]175[.]67 | 2 |
| 14[.]136[.]23[.]194 | 1 |
| 159[.]192[.]105[.]100 | 1 |
| 159[.]192[.]106[.]207 | 2 |
| 177[.]85[.]224[.]93 | 2 |
| 220[.]135[.]113[.]71 | 1 |
| 77[.]107[.]131[.]96 | 1 |
| **DbserverDev** | 114[.]32[.]100[.]73 | 1 |
| 159[.]192[.]105[.]100 | 1 |
| 74[.]218[.]29[.]74 | 1 |
| **DbserverRecibo** | 1[.]34[.]85[.]243 | 1 |
| 128[.]22[.]175[.]67 | 3 |
| 159[.]192[.]105[.]100 | 3 |
| 177[.]85[.]224[.]93 | 1 |
| 59[.]126[.]252[.]139 | 1 |
| 74[.]218[.]29[.]74 | 1 |
| 77[.]107[.]131[.]96 | 2 |
| **DBserverRe-QA** | 114[.]33[.]11[.]178 | 1 |
| 114[.]33[.]37[.]21 | 1 |
| 159[.]192[.]105[.]100 | 1 |
| 177[.]85[.]224[.]93 | 2 |
| 77[.]107[.]131[.]96 | 1 |
| **DEV-002-Sb2bi** | 1[.]34[.]85[.]243 | 1 |
| 159[.]192[.]104[.]79 | 1 |
| 74[.]218[.]29[.]74 | 1 |
| **Sb2bserverRE-QA** | 114[.]32[.]100[.]73 | 1 |
| 128[.]199[.]181[.]4 | 1 |
| 128[.]22[.]175[.]67 | 3 |
| 159[.]192[.]104[.]79 | 1 |
| 159[.]192[.]105[.]100 | 2 |
| 159[.]192[.]106[.]207 | 1 |
| 177[.]85[.]224[.]93 | 2 |
| 220[.]135[.]113[.]71 | 1 |
| **Sb2bSrvRecibo** | 128[.]199[.]181[.]4 | 1 |
| 128[.]22[.]175[.]67 | 3 |
| 159[.]192[.]104[.]79 | 1 |
| 159[.]192[.]105[.]100 | 1 |
| 159[.]192[.]106[.]207 | 1 |
| 177[.]85[.]224[.]93 | 4 |
| 220[.]133[.]20[.]40 | 1 |
| 77[.]107[.]131[.]96 | 3 |
| **SMTPSERVERENL[.]ams[.]local** | 159[.]192[.]104[.]79 | 1 |
| 159[.]192[.]105[.]100 | 1 |
| 159[.]192[.]106[.]207 | 1 |
| 59[.]126[.]252[.]139 | 1 |
| **smtpserverhs[.]ams[.]local** | 159[.]192[.]106[.]207 | 1 |
| 174[.]57[.]71[.]99 | 1 |
| 218[.]161[.]74[.]135 | 1 |
| 74[.]218[.]29[.]74 | 1 |
| **SMTPSVRCFDINET[.]ams[.]local** | 114[.]32[.]100[.]73 | 1 |
| 159[.]192[.]104[.]79 | 1 |
| 218[.]161[.]74[.]135 | 1 |
| 220[.]133[.]92[.]196 | 1 |
| 220[.]135[.]113[.]71 | 1 |
| 59[.]126[.]252[.]139 | 1 |
| **srvhsprdblue03[.]humansite[.]int** | 1[.]34[.]85[.]243 | 1 |
| 159[.]192[.]106[.]207 | 1 |
| 218[.]161[.]74[.]135 | 1 |
| 220[.]132[.]135[.]212 | 1 |
| 220[.]133[.]92[.]196 | 1 |
| **Total general** |  |  | **96** |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Procedemos a validar la reputación de las IPs:**

Interfaz de usuario gráfica, Aplicación, Tabla

Descripción generada automáticamente

Las siguientes IPs se encuentran bloqueadas dentro de la solución:

* 128[.]199[.]181[.]4 Bloqueada
* 104[.]152[.]52[.]206 Bloqueada

**Recomendaciones:**

• Corroborar que las IP´s catalogadas como no maliciosas son válidas para ustedes

• Cerrar los puertos que no sean necesarios para su operación.

Quedamos atentos a sus comentarios.

Saludos Cordiales.