**TLP: Amber | Evento\_de\_Seguridad | GAP | DSM |**

**Multiples\_Reconocimientos\_de\_Puertos**

**TLP: Amber | Evento\_de\_Seguridad | AMS | DSM |**

**Multiples\_Reconocimientos\_de\_Puertos**

**TLP: Amber | Evento\_de\_Seguridad | GPV | DSM |**

**Multiples\_Reconocimientos\_de\_Puertos**

* **Poner Target en Valores de la Tabla Dinámica**

Buena tarde,

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

|  |  |
| --- | --- |
| **Equipos:** | * GDLNVR7 * PVR-WIN-NAS |
| **Source IP:** | * 10[.]219[.]200[.]12 * 10[.]219[.]200[.]11 * 10[.]223[.]127[.]11 * 10[.]223[.]201[.]161 * 23[.]215[.]40[.]237 |
| **Detección:** | Reconnaissance Detected: Network or Port Scan |
| **Eventos:** | 1 |

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:

|  |  |  |  |
| --- | --- | --- | --- |
| **Event** | **Target** | **IP Source** | **Eventos** |
| Reconnaissance Detected: Network or Port Scan | GDLNVR7 | 10[.]223[.]127[.]11 | 1 |
| 10[.]223[.]201[.]161 | 1 |
| 23[.]215[.]40[.]237 | 1 |
| PVR-WIN-NAS | 10[.]219[.]200[.]11 | 8 |
| 10[.]219[.]200[.]12 | 9 |
| **Total general** |  |  | **20** |

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

**Procedemos a validar la reputación de las IPs que no son internas, siendo las restantes internas no son catalogadas como maliciosas.** D

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.