RouterSpace - 10.10.11.148

Tabla de contenido

Tabla de contenido

Enumeración

Como paso inicial en nuestra ruta, realizaremos una enumeración del objetivo para poder detectar vectores de ataque y así idear un plan o estrategia para lograr vulnerar esta máquina como tal. Veremos tecnologías web, puertos, servicios y sus versiones, campos de ataque y más.

Puertos

Con ayuda de Nmap (nuestra favorita, o lo es en mi caso), vamos a enumerar las entradas del servidor y visualizar si alguna de estas es vulnerable debido a su versión o servicio expuesto de esta, con el fin de detectar vectores de ataque.

```
PORT      STATE    SERVICE VERSION
22/tcp    open     ssh     (protocol 2.0)
80/tcp    open     http
```

Aggressive OS guesses: Linux 4.15 - 5.6 (92%), Linux 5.0 (92%), Linux 5.0 - 5.4 (91%), Linux 5.3 - 5.4 (91%), Linux 2.6.32 (91%), Linux 5.0 - 5.3 (90%), Crestron XPanel control system (90%), Linux 5.4 (89%), ASUS RT-N56U WAP (Linux 3.4) (87%), Linux 3.1 (87%)
No exact OS matches for host (test conditions non-ideal).

Web

El servicio web cuenta con algunos campos muy básicos, uno de ellos es un campo de texto y el otro una caja de selección.

Infraestructura del objetivo:
• **Servidor:** N/A

• **Lenguaje de programación:** Html, Java
• **Framework:** N/A
• **Librerías:** Jquery
• **SO:** Linux/Android

Explotación

Descubrimiento:
Se obtiene una aplicación para celular android (APK), con ella se procede a instalat un emulador de android apra visualizar la aplicación y poder ver su funcionamiento, después de ello se procede a revisar si la aplicación realiza conexiones con el exterior. Al visualizar esto, se procede a jugar con la petición.

Vulnerabilidad detectada:
Se detecta una inyección de comandos a traves del API descubierta.

Descripción:
Un ataque de inyección de comandos, que también se conoce como Command Injection, es básicamente cuando un atacante inyecta código para ejecutar comandos en un sistema. Se aprovecha siempre de alguna vulnerabilidad existente y sin que la víctima sea consciente de ello. De esta forma va a lograr el control del servidor y poder utilizarlo como si fueran un usuario legítimo.

Exploit:
No se usa un exploit como tal, se utilizan una serie de comandos para vulnerar a la víctima.

Ataque:
Al detectarse la brecha se procede a realizar los siguientes comandos para entrar al sevidor de la víctima:
• Como no fue posible establecer una conexión inversa, se procede a usar otra técnica.
• Creamos una llave ssh con ssh-keygen
• Copiamos la llave en la petición para explotar la inyección de comandos.
• Añadimos el comando echo “llave ssh rsa” > /home/paul/.ssh/authorized_keys
• Nos conectamos por medio de ssh paul@routerspace.htb

Enumeración Interna

Debemos realizar una enumeración interna para poder visualizar nuestros posibles vectores para escalar privilegios y obtener un usuario privilegiado.

A continuación, veremos los comandos y su respuesta:

Hostname:
Arquitectura: x64
SO: Android

Escalada de privilegios

Descubrimiento:
Usando linPeas detectamos una serie de brechas, como la versión del kernel junto con esto una

serie de exploit's que nos pueden ayudar a escalar privilegios.

Vulnerabilidad detectada:
[CVE-2021-3156] sudo Baron Samedit

Descripción:

Exploit:
Es posible encontrarlo en la siguiente ubicación https://github.com/worawit/CVE-2021-3156

Ataque:
Se procede a ejecutar el exploit detectado y hemos ganado

Credenciales/Usuarios detectados

Durante la explotación, ya sea inicial, intermedia o final, es posible acceder a información sensible sobre algunos usuarios, dicha información será almacenada y guardada para un posterior movimiento.

Credenciales

En el archivo config.php se encuentra

Hash

Hash del usuario que maneja el recurso compartido (SMB)
•

Usuarios

Usuarios detectados con pocos privilegios:

Usuarios detectados:
paul