



# INSTITUTO TECNOLÓGICO DE MORELIA

Ingeniería en Sistemas Computacionales

Hardening de Servidores

## Práctica 1

### Sistemas Operativos Servidores

ALUMNO:

**Rogelio Cristian Punzo Castro**

**21120245**

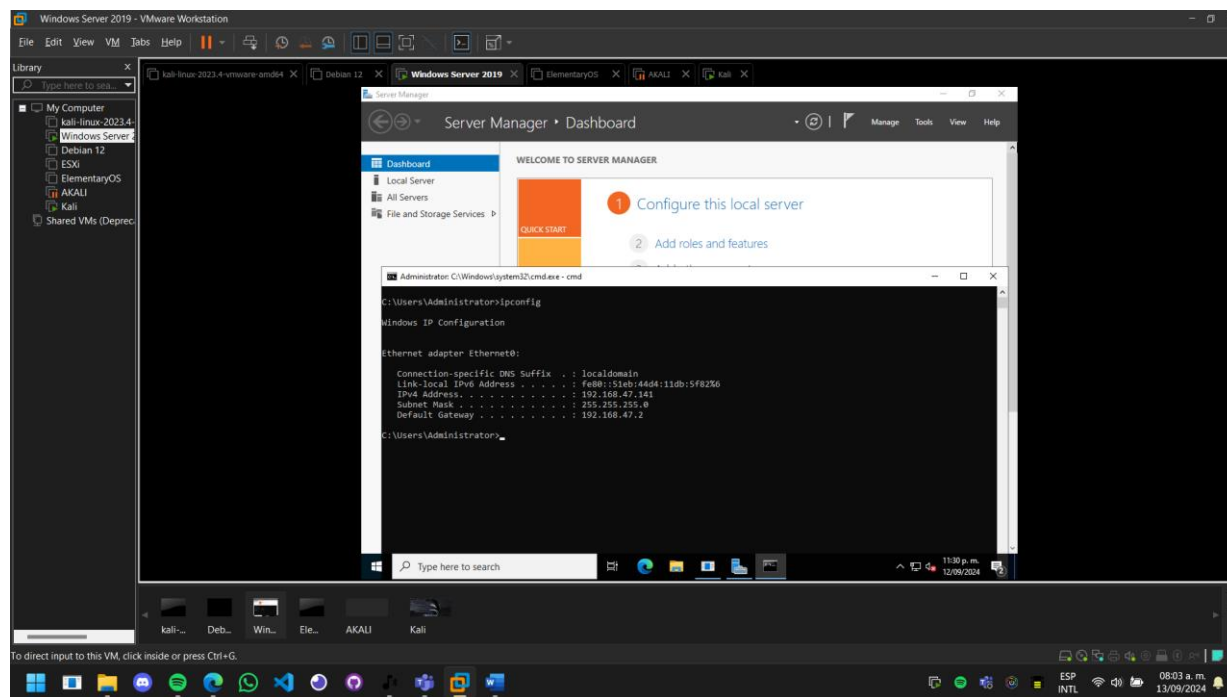
PROFESOR:

**Juan Jesús Ruiz Lagunas**

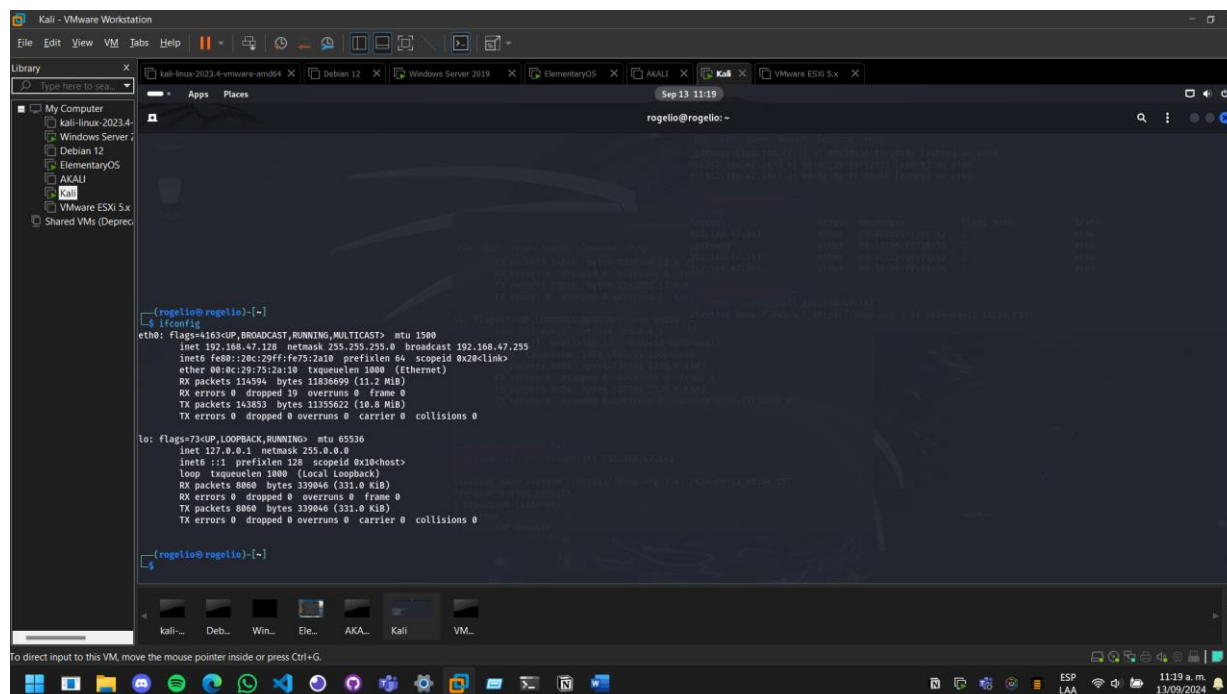
MORELIA, MICHOACÁN

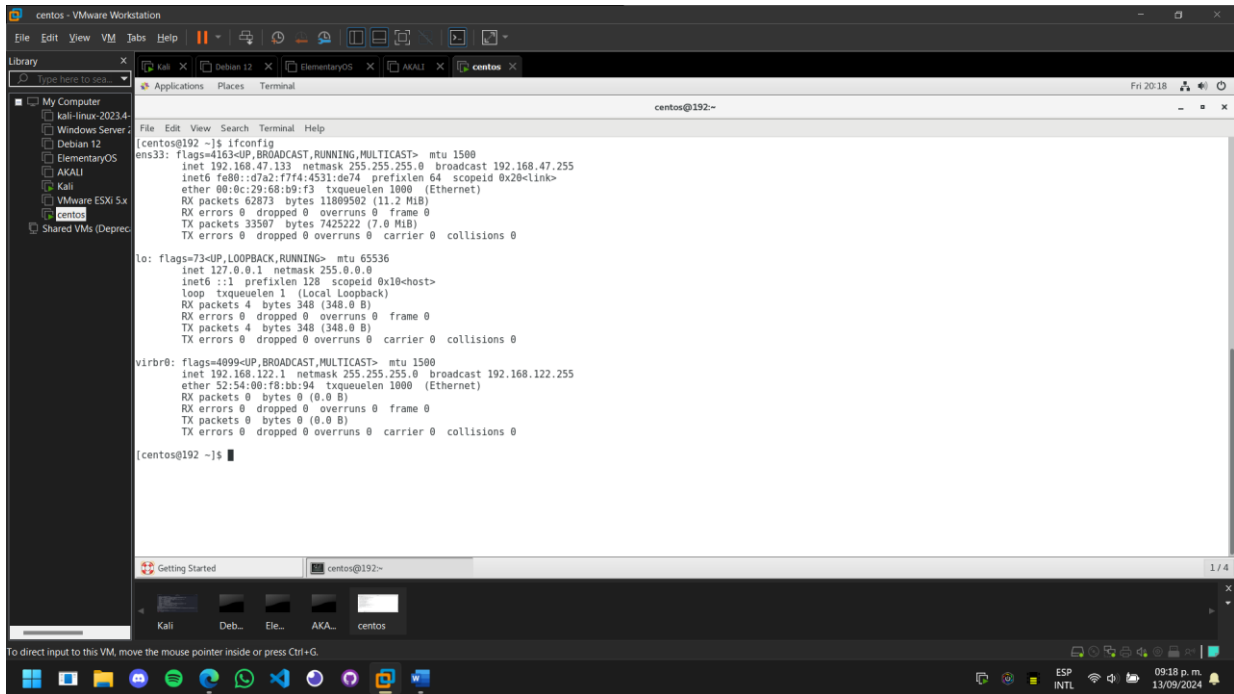
**(13 de Septiembre 2024)**

## Windows Server 192.168.47.141



## Kali Linux 192.168.47.128



**CentOS 192.168.47.133**

```
[centos@192 ~]$ ifconfig
ens33: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
    inet 192.168.47.133  netmask 255.255.255.0  broadcast 192.168.47.255
    inet6 fe80::d7a2:f7f4:4531:de74  prefixlen 64  scopeid 0x20<link>
    ether 00:0c:29:68:b9:f3  txqueuelen 1000  (Ethernet)
    RX packets 62873  bytes 11809582 (11.2 MiB)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 33587  bytes 7425222 (7.0 MiB)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

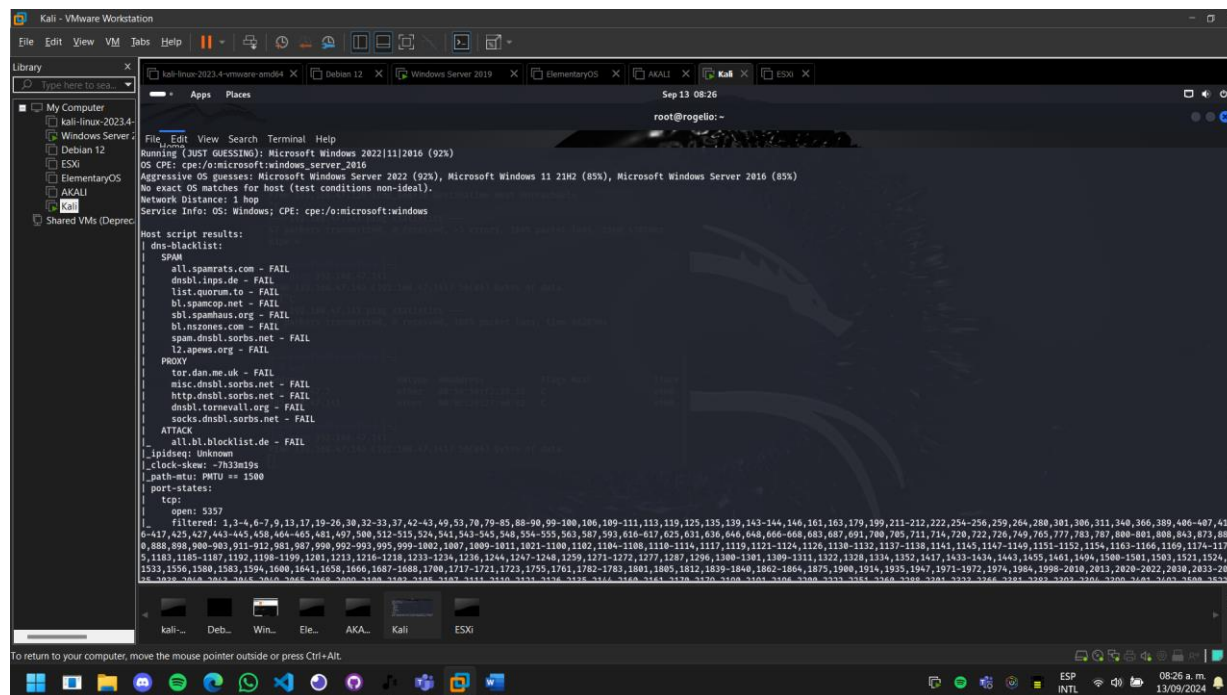
lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
    inet 127.0.0.1  netmask 255.0.0.0
    inet6 ::1  prefixlen 128  scopeid 0x10<host>
    loop txqueuelen 1  (Local Loopback)
    RX packets 4  bytes 348 (348.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 4  bytes 348 (348.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

virbr0: flags=4099<UP,BROADCAST,MULTICAST>  mtu 1500
    inet 192.168.122.1  netmask 255.255.255.0  broadcast 192.168.122.255
    ether 52:54:00:f8:bb:94  txqueuelen 1000  (Ethernet)
    RX packets 0  bytes 0 (0.0 B)
    RX errors 0  dropped 0  overruns 0  frame 0
    TX packets 0  bytes 0 (0.0 B)
    TX errors 0  dropped 0  overruns 0  carrier 0  collisions 0

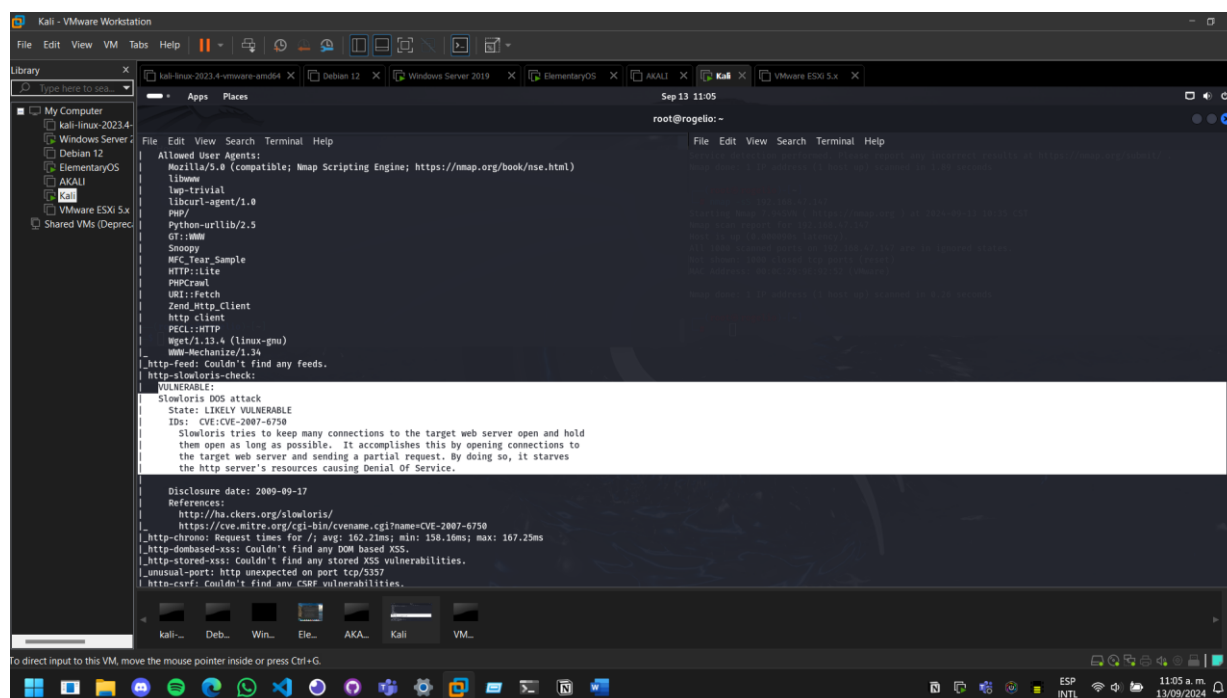
[centos@192 ~]$
```

## Relación de vulnerabilidades

### Windows Server 2019



**Puerto 5357/tcp:** Este puerto está abierto y ejecuta el servicio HTTP usando Microsoft HTTPAPI httpd 2.0 (SSDP/UPnP).



Se indicó que el servidor HTTP podría ser vulnerable a un ataque:

### Slowloris (CVE-2007-6750):

Slowloris es un ataque de denegación de servicio (DoS) dirigido a servidores web. Este ataque explota la forma en que muchos servidores manejan conexiones HTTP incompletas. El atacante envía múltiples solicitudes HTTP parciales que no se completan, lo que consume los recursos del servidor sin requerir mucho ancho de banda por parte del atacante.

Funcionamiento del ataque:

- Apertura de múltiples conexiones HTTP: El atacante establece múltiples conexiones con el servidor, pero no las completa.
- Envía cabeceras HTTP incompletas: Slowloris envía cabeceras HTTP muy lentamente, manteniendo las conexiones abiertas el mayor tiempo posible sin enviarlas por completo.
- Evita el timeout: Al enviar pequeños fragmentos de las cabeceras HTTP en intervalos regulares, el atacante evita que el servidor cierre las conexiones por timeout.
- Agotamiento de recursos: Al mantener abiertas muchas conexiones simultáneas y sin completarlas, el servidor queda incapaz de gestionar nuevas conexiones legítimas, ya que sus recursos se agotan.

Afecta principalmente a:

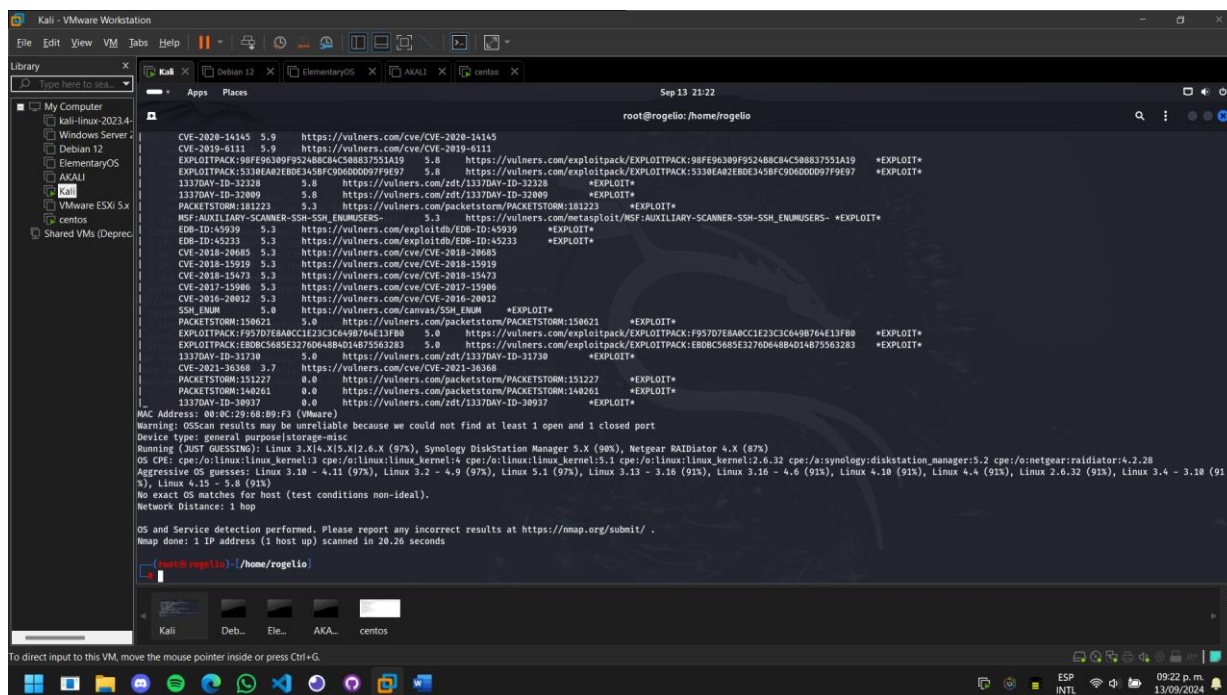
- Servidores web que manejan múltiples conexiones HTTP, como Apache.
- Servidores que no tienen medidas contra conexiones HTTP incompletas.

## CentOS 7

```

root@kali: /home/rogelio
root@rogelio: /home/rogelio
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-09-13 21:15 CST
Nmap scan report for 192.168.47.133 (192.168.47.133)
Host is up (0.00056s latency).
Not shown: 999 filtered tcp ports (no-response), 10 filtered tcp ports (host-prohibited)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 7.4 (protocol 2.0)
vulners:
cve/2020-15778 7.8 https://vulners.com/cve/CVE-2020-15778
SSV:92579 7.5 https://vulners.com/seebug/SSV:92579 *EXPLOIT*
PACKETSTORM:172661 7.5 https://vulners.com/packetstorm/PACKETSTORM:172661 *EXPLOIT*
F907918D-AE88-5384-86CF-3AF8523F3807 7.5 https://vulners.com/githubexploit/F907918D-AE88-5384-86CF-3AF8523F3807 *EXPLOIT*
1337DAY-ID-26576 7.5 https://vulners.com/zdt/1337DAY-ID-26576 *EXPLOIT*
CVE-2021-41617 7.8 https://vulners.com/cve/CVE-2021-41617
E0B-ID-46516 6.8 https://vulners.com/exploitdb/E0B-ID-46516 *EXPLOIT*
E0B-ID-46193 6.8 https://vulners.com/exploitdb/E0B-ID-46193 *EXPLOIT*
CVE-2019-6110 6.8 https://vulners.com/cve/CVE-2019-6110
CVE-2019-6109 6.8 https://vulners.com/cve/CVE-2019-6109
C94132FD-1FA5-5142-8AEE-8DAF45EEFE3 6.8 https://vulners.com/githubexploit/C94132FD-1FA5-5142-8AEE-8DAF45EEFE3 *EXPLOIT*
102130BE-F683-588B-8603-353173626207 6.8 https://vulners.com/githubexploit/102130BE-F683-588B-8603-353173626207 *EXPLOIT*
CVE-2023-51385 6.5 https://vulners.com/cve/CVE-2023-51385
CVE-2023-48795 5.9 https://vulners.com/cve/CVE-2023-48795
CVE-2020-16145 5.9 https://vulners.com/cve/CVE-2020-16145
CVE-2019-6111 5.9 https://vulners.com/cve/CVE-2019-6111
EXPLOITPACK:98FE96389F952488C84C308B37551A19 5.8 https://vulners.com/exploitpack/EXPLOITPACK:98FE96389F952488C84C308B37551A19 *EXPLOIT*
EXPLOITPACK:53338E2A82EBC3458FC9D6000097F9E97 5.8 https://vulners.com/exploitpack/EXPLOITPACK:53338E2A82EBC3458FC9D6000097F9E97 *EXPLOIT*
1337DAY-ID-32328 5.8 https://vulners.com/zdt/1337DAY-ID-32328 *EXPLOIT*
1337DAY-ID-32089 5.8 https://vulners.com/zdt/1337DAY-ID-32089 *EXPLOIT*
PACKETSTORM:181223 5.3 https://vulners.com/packetstorm/PACKETSTORM:181223 *EXPLOIT*

```



### Vulnerabilidades Críticas (Severidad > 9):

- CVE-2023-38408 (Severidad: 9.8):** Vulnerabilidad de ejecución remota de código en OpenSSH que permite a un atacante ejecutar código arbitrario en el servidor mediante un túnel SSH.
  - Permite a un atacante tomar control total del sistema afectado.
- 95499236-C9FE-56A6-9D7D-E943A24B633A (Severidad: 10.0):** Exploit que aprovecha una vulnerabilidad crítica en OpenSSH.
  - Posible ejecución de código remoto y control del sistema.
- 2C119FFA-ECE0-5E14-A4A4-354A2C38071A (Severidad: 10.0):** Otro exploit crítico para OpenSSH, específicamente diseñado para vulnerabilidades de ejecución de código.
  - Ejecución remota de código, escalamiento de privilegios.
- B8190CDB-3EB9-5631-9828-8064A1575B23 (Severidad: 9.8):** Vulnerabilidad que explota la ejecución de comandos arbitrarios a través del servicio SSH.
  - Control completo sobre el servidor afectado.
- 8FC9C5AB-3968-5F3C-825E-E8DB5379A623 (Severidad: 9.8):** Permite la ejecución de código a través de un exploit en OpenSSH.
  - Control total del sistema por parte de atacantes remotos.

- **8AD01159-548E-546E-AA87-2DE89F3927EC (Severidad: 9.8):** Similar a las anteriores, esta vulnerabilidad permite ejecutar comandos arbitrarios.
  - Pone en riesgo la integridad del sistema, permitiendo control total.
- **5E696\8B4-DBD6-57FA-BF6E-D9B2219DB27A (Severidad: 9.8):** Exploit de OpenSSH que facilita la ejecución de código remoto.
  - Da acceso completo al sistema para ejecutar comandos con privilegios elevados.

#### **Vulnerabilidades Altas (Severidad entre 7.0 y 9.8):**

- **CVE-2020-15778 (Severidad: 7.8):** Vulnerabilidad en OpenSSH en la función "scp" que permite a un atacante remoto ejecutar comandos arbitrarios en la máquina del cliente al transferir archivos.
  - Afecta la transferencia segura de archivos, comprometiendo la máquina del cliente.
- **SSV:92579 (Severidad: 7.5):** Exploit de OpenSSH que puede ser utilizado para acceder y manipular archivos de configuración.
  - Acceso no autorizado a configuraciones críticas del servidor.
- **PACKETSTORM:173661 (Severidad: 7.5):** Exploit que permite la enumeración de usuarios SSH y la ejecución de código.
  - Riesgo de fuga de información y control del sistema.
- **F0979183-AE88-53B4-86CF-3AF0523F3807 (Severidad: 7.5):** Exploit que aprovecha vulnerabilidades de OpenSSH para ejecutar código arbitrario.
  - Escalamiento de privilegios y acceso a información confidencial.
- **1337DAY-ID-26576 (Severidad: 7.5):** Vulnerabilidad explotable a través de OpenSSH para acceder a credenciales y ejecutar comandos arbitrarios.
  - Da control sobre el servidor y compromete la autenticación SSH.
- **CVE-2021-41617 (Severidad: 7.0):** Vulnerabilidad de condición de carrera en OpenSSH que puede permitir la manipulación de procesos.
  - Permite a un atacante ejecutar operaciones indebidas escalando privilegios.



## Conclusiones

Las vulnerabilidades de severidad alta y crítica representan riesgos significativos para la estabilidad y seguridad de un servidor, especialmente si están expuestas en un entorno de producción. Las medidas de mitigación incluyen la actualización de software vulnerable, configuración adecuada de servicios, y la implementación de controles adicionales como firewalls y autenticación multifactor, por otro lado, en cuanto se detecte alguna vulnerabilidad, esta debe ser atendida de inmediato para evitar compromisos serios en la seguridad del sistema. La mayoría de las vulnerabilidades que fueron detectadas en CentOS por ejemplo, permiten la ejecución de código remoto y, en algunos casos, el control completo del sistema afectado. Debido al potencial peligro que esto significa para cualquier sistema está claro que es esencial aplicar parches de seguridad, así como realizar escaneos periódicos y asegurar el servidor con medidas adicionales como la desactivación de protocolos vulnerables y el uso de autenticación más robusta.