Reporte Ejecutivo de Ciberseguridad: Análisis de Vulnerabilidad y Explotación en el Sistema "Under Pass"

---

1. Portada

- **Título del Reporte**: Análisis de Vulnerabilidad y Explotación en el Sistema "Under Pass"
- **Fecha**: 24 de Diciembre de 2024
- **Nombre de la Organización**: (N/A) - Proyecto Educativo
- **Autor(es)**: tellmefred

---

2. Resumen Ejecutivo

Este informe documenta el análisis y explotación de la máquina "Under Pass" de Hack The Box, un entorno diseñado para evaluar habilidades de enumeración, explotación y escalada de privilegios. A través de técnicas de reconocimiento de red, fuerza bruta y manipulación de servicios, se logró obtener acceso inicial y posteriormente escalar privilegios hasta obtener acceso root.

Este reporte detalla cada fase del proceso, proporciona un análisis técnico y recomienda medidas para mitigar riesgos similares en entornos reales.

---

3. Introducción

- **Contexto**: "Under Pass" es una máquina que simula vulnerabilidades comunes en sistemas Linux, enfocada en la explotación de servicios web y escalada de privilegios.
- **Propósito**: Identificar y explotar vulnerabilidades del sistema, reforzando habilidades en ciberseguridad.
- **Alcance**: El análisis cubre desde el reconocimiento inicial hasta la escalada de privilegios para obtener acceso root.
- **Metodología**: Se utilizaron herramientas de escaneo de red (`nmap`), fuerza bruta sobre hashes y explotación de servicios SNMP y SSH.

---

4. Estado Actual de la Ciberseguridad

- **Resumen de la Postura de Ciberseguridad**:
  La máquina "Under Pass" presentó vulnerabilidades explotables debido a:
  - Exposición de un servicio SNMP no seguro.
  - Uso de credenciales por defecto en la aplicación Daloradius.
  - Permisos inseguros en el servicio `mosh-server` para escalada de privilegios.
- **Sistemas y Datos Críticos**:
  - Servicio web Daloradius (puerto 80).
  - Servicio SSH (puerto 22).
  - Servicio SNMP (puerto 161).
  - Permisos `sudo` sobre `mosh-server`.

---

5. Evaluación de Vulnerabilidades y Explotación

Reconocimiento

1. **Escaneo de Red**:
   - Escaneo inicial con `nmap` reveló los puertos 22 (SSH) y 80 (HTTP).
   - Un escaneo de puertos UDP identificó el puerto **161 (SNMP)**.
2. **Enumeración SNMP**:
   - Se utilizó `snmpwalk` para enumerar información y se descubrió una referencia a **Daloradius**, un servidor de administración de redes.
   - Se identificó la ruta predeterminada del archivo `login.php` de Daloradius.
3. **Credenciales por Defecto**:
   - Consultando la documentación de Daloradius, se identificaron las credenciales por defecto, que permitieron el acceso al panel de administración.

Explotación

1. **Acceso Inicial**:
   - Se accedió al panel de Daloradius usando credenciales por defecto.
   - En la sección de usuarios, se encontró un hash de contraseña perteneciente a un usuario (`numme`).
   - Se realizó un ataque de fuerza bruta para descifrar el hash, obteniendo la contraseña en texto claro.
   - Con las credenciales obtenidas, se accedió al sistema mediante SSH y se capturó la flag de usuario (`user.txt`).

Escalada de Privilegios

1. **Permisos de Sudo**:
    - Se ejecutó `sudo -l` y se identificó que el usuario podía ejecutar `mosh-server` con privilegios de root.
    - Se consultó la documentación (`man`) de `mosh-server`, identificando un comando que permitió escalar privilegios y obtener acceso root.
    - Finalmente, se capturó la flag de root (`root.txt`).

---

6. Recomendaciones

1. **Fortalecimiento de SNMP**:
    - Deshabilitar SNMP si no es necesario o asegurar el servicio con autenticación fuerte.
    - Limitar el acceso a SNMP únicamente desde IPs autorizadas.
2. **Gestión de Credenciales**:
    - Cambiar todas las credenciales por defecto inmediatamente después de la instalación de cualquier aplicación o servicio.
    - Implementar autenticación multifactor (MFA) para servicios críticos.
3. **Seguridad de Servicios Sudo**:
    - Limitar el uso de `sudo` solo a comandos esenciales y revisar periódicamente los permisos.
    - Eliminar permisos de `sudo` para servicios como `mosh-server` que pueden ser explotados para escalar privilegios.
4. **Auditoría y Monitoreo**:
    - Implementar herramientas de monitoreo para detectar accesos no autorizados a servicios web y SSH.
    - Revisar periódicamente logs de SNMP, SSH y Daloradius para detectar actividad sospechosa.

---

7. Conclusión

El análisis de la máquina "Under Pass" demostró que la combinación de servicios mal configurados y credenciales por defecto representa un riesgo significativo para la seguridad del sistema. La implementación de las recomendaciones propuestas es esencial para mitigar estos riesgos y mejorar la seguridad general del entorno.

---

8. Anexos

- Escaneos de red (`nmap`) y resultados de enumeración SNMP.
- Capturas de pantalla del proceso de explotación y escalada de privilegios.
- Detalles técnicos sobre la explotación de Daloradius y `mosh-server`.