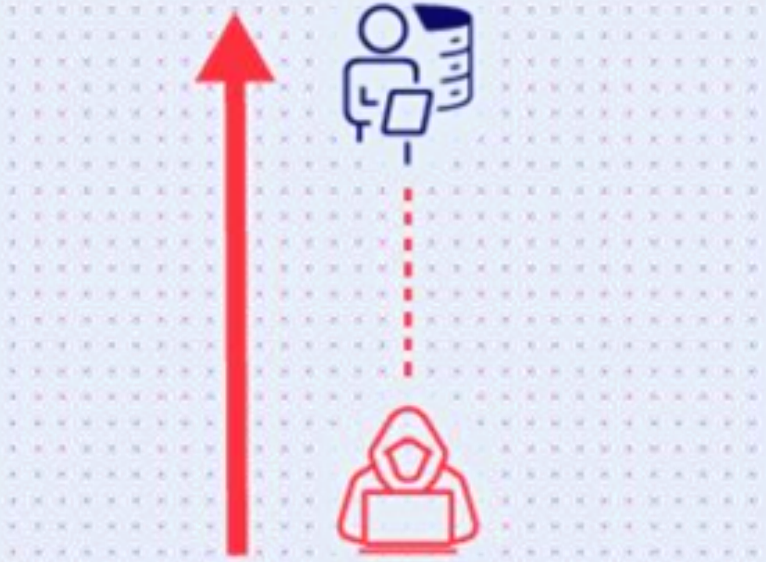
Escalada de privilegios en sistemas Linux: de usuario básico a root

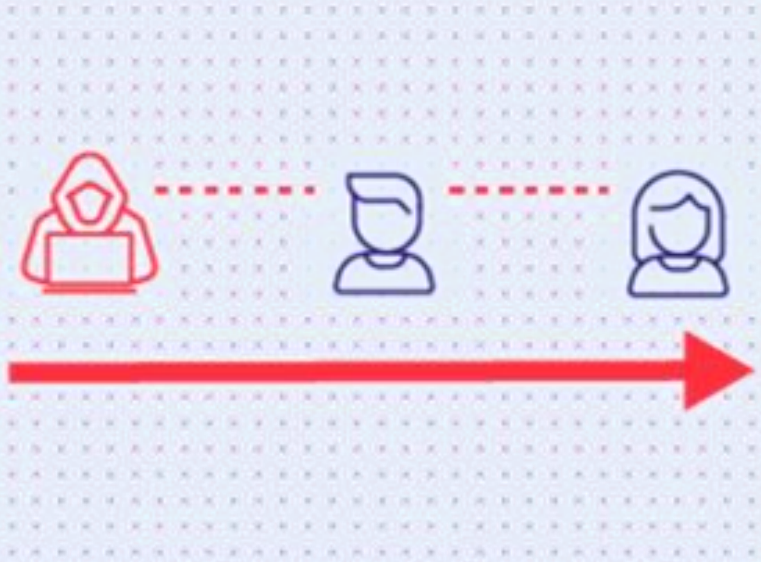
Types of Privilege Escalation

Vertical Privilege Escalation



Attackers elevate from **standard** user to **admin or root** by exploiting vulnerabilities, gaining full control to modify settings and access sensitive data.

Horizontal Privilege Escalation



Attackers stay at the **same privilege level** but access other users' data or resources due to weak access controls or session management flaws.

Hybrid Privilege Escalation

In complex environments like hybrid clouds, attackers exploit misconfigurations and weak IAM policies to escalate **privileges across on-premises and cloud systems**.

Privilege Escalation Attack Vectors

cymulate

1

Malware

Gather information about the target.

2

Vulnerabilities

Exploiting system flaws helps attackers bypass security and gain admin access.

3

Social Engineering

Phishing tricks users into revealing credentials or installing malware for system access.

4

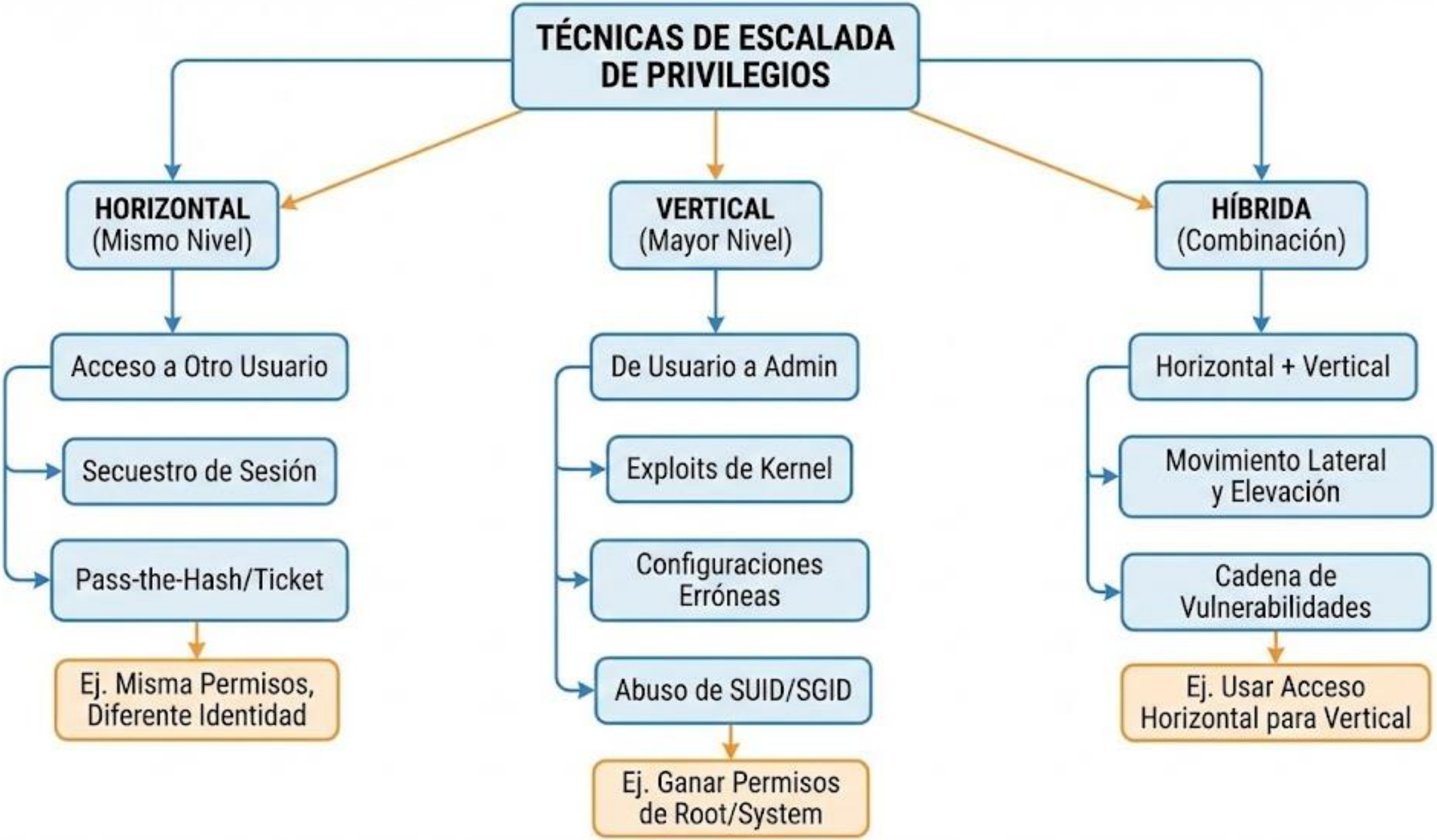
Misconfigurations

Weak settings, open ports, and permissive policies allow attackers to exploit systems.

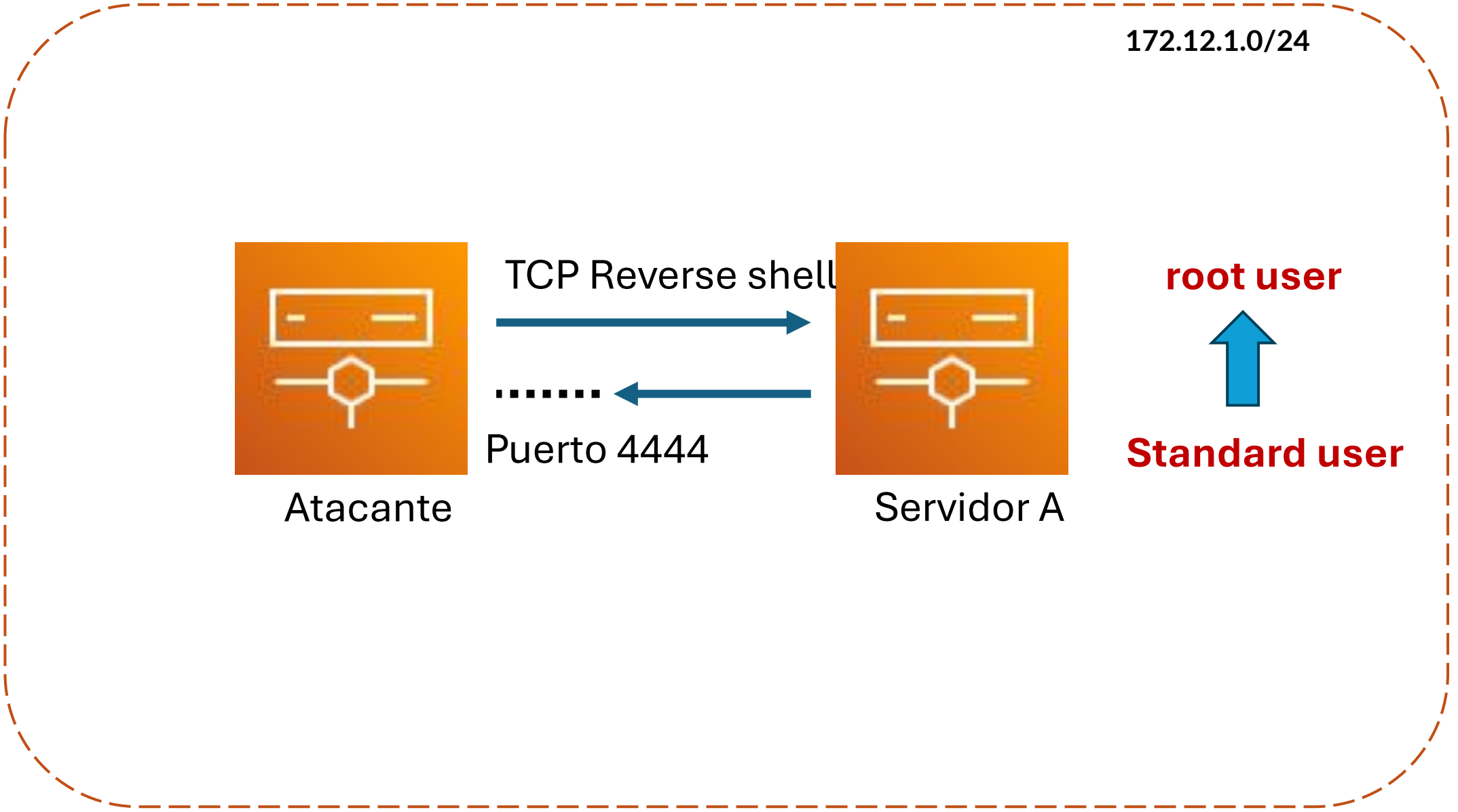
5

Credential Exploitation

Weak passwords and reused credentials enable attackers to escalate access.


TÉCNICAS DE ESCALADA DE PRIVILEGIOS
HORIZONTAL (Mismo Nivel)
VERTICAL (Mayor Nivel)
HÍBRIDA (Combinación)
Acceso a Otro Usuario
Secuestro de Sesión
Pass-the-Hash/Ticket
Ej. Misma Permisos, Diferente Identidad
De Usuario a Admin
Exploits de Kernel
Configuraciones Erróneas
Abuso de SUID/SGID
Ej. Ganar Permisos de Root/System
Horizontal + Vertical
Movimiento Lateral y Elevación
Cadena de Vulnerabilidades
Ej. Usar Acceso Horizontal para Vertical

Laboratorio & Herramientas


172.12.1.0/24
TCP Reverse shell
Puerto 4444
Atacante
Servidor A
root user
Standard user

Técnicas

"GTFOBins" (Uso indebido de awk)

En lugar de invocar directamente un shell (que podría monitorizarse mediante el registro de la línea de comandos), podemos utilizar los binarios estándar del sistema que permiten la ejecución de comandos. awk es un candidato ideal, ya que está instalado en casi todos los sistemas Linux.

awk procesa texto, pero también cuenta con una función system() que puede ejecutar comandos del sistema operativo. Como ejecutamos awk con sudo, el comando dentro de system() se ejecuta como root.

Técnicas

Método 2: Crear una puerta trasera "SUID“

Este método es útil porque crea una forma permanente de convertirse en root, la cual persiste incluso si el administrador elimina sus privilegios de sudo posteriormente.

Copiar el shell del sistema (/bin/bash) a una ubicación oculta y estableceremos el bit SUID (Establecer ID de usuario). Este bit le indica a Linux: "Cuando se ejecute este archivo, ejecútelo con los permisos de su propietario (root)", independientemente de quién lo esté ejecutando.

Técnicas

Método 3: Shadow

Manipulación directa de archivos de autenticación del sistema operativo mediante Shadow cat/tee.

Descifrado de contraseñas o creación de usuarios ocultos.

Recomendaciones para remediación o prevención

- Principio del mínimo privilegio
- Separación de funciones
-Aplicación de parches y gestión de vulnerabilidades
- Utilizar sistemas de gestión de secretos seguros para credenciales
- Habilitar la detección de escalada de privilegios en tiempo real