THE BRIDGE

CYBER SECURITY

Enumeración en Linux

Manual

- **Enumerate Kernel version**
  - uname –a
- **Enumerate Sudo version**
  - sudo -V
- **Eumerate System users**
  - cat /etc/passwd |cut -d ":" -f 1
- **Eumerate System groups**
  - cat /etc/group |cut -d ":" -f 1
- **Eumerate Services**
  - netstat -anlp
  - netstat -ano
- **Enumerate root run binaries**
  - ps aux | grep root
- **Enumerate binary version**
  - dpkg -l
- **Enumerate shells**
  - cat /etc/shells
- **Enumerate current shell**
  - echo $SHELL

Manual

- **Enumerate Shell Version**
  - /bin/bash --version
- **Enumerate sudo rights and Enumerate not-reseted Env Variables**
  - sudo -l
- **Enumerate SUID - SGID executables**
  - find / -type f -a \(-perm -u+s -o -perm -g+s \) -exec ls -l {} \; 2> /dev/null
- **Enumerate Backups**
  - find /var /etc /bin /sbin /home /usr/local/bin /usr/local/sbin /usr/bin /usr/games /usr/sbin /root /tmp -type f \(-name "*backup*" -o -name "*\.bak" -o -name "*\.bck" -o -name "*\.bk" \) 2>/dev/null
- **Enumerate DBs**
  - find / -name '.db' -o -name '.sqlite' -o -name '*.sqlite3' 2>/dev/null

Manual

- **Enumerate root Crontab**
  - cat /etc/crontab | grep ‘root’
- **Enumerate Hidden Files**
  - find / -type f -iname ".*" -ls 2>/dev/null
- **Enumerate Programming Languages**
  - which python
  - which perl
  - which ruby
  - which lua0
- **Enumerate Environment**
  - env
- **Enumerate History command with pass**
  - history |grep -i -E '\-p|\-pass|\-password|*:*|*@*|passw'
- **GTFOBins** is a curated list of Unix binaries that can be used to bypass local security restrictions in misconfigured systems.
  - https://gtfobins.github.io/

Automatica

- **LinEnum**
  - Es un script de enumeración de Linux. Se ejecuta en el host de destino y busca muchos de los métodos comunes de escalada de privilegios o errores de configuración.
  - https://github.com/rebootuser/LinEnum

- **linux-smart-enumeration**
  - Este script mostrará información relevante sobre la seguridad del sistema Linux local, lo que ayudará a aumentar los privilegios.
  - https://github.com/diego-treitos/linux-smart-enumeration

- **LinPeas**
  - Es un script que busca posibles rutas para escalar privilegios en hosts Linux/Unix*/MacOS.
  - Las comprobaciones se explican en book.hacktricks.xyz.
  - https://github.com/carlospolop/PEASS-ng/tree/master/linPEAS

- **linux-exploit-suggester-2**
  - Cuando se ejecuta sin argumentos, el script realiza un 'uname -r' para obtener la versión de lanzamiento del sistema operativo Linux y devuelve una lista de posibles vulnerabilidades. Se incluyen enlaces a CVE y POC de explotación aplicables.
  - https://github.com/jondonas/linux-exploit-suggester-2


THE
BRIDGE