**Compte Rendu TP2 : Hardening OS**

*Partie I*

**1.Anatomy of a program**

*FILE*

Commande ls :

**file /usr/bin/ls**

**/usr/bin/ls: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=1afdd52081d4b8b631f2986e26e69e0b275e159c, for GNU/Linux 3.2.0, stripped**

Commande ip :

**file /usr/sbin/ip**

**/usr/sbin/ip: ELF 64-bit LSB pie executable, x86-64, version 1 (SYSV), dynamically linked, interpreter /lib64/ld-linux-x86-64.so.2, BuildID[sha1]=77a2f5899f0529f27d87bb29c6b84c535739e1c7, for GNU/Linux 3.2.0, stripped**

Fichier mp3 :

**file song.mp3**

**song.mp3: Audio file with ID3 version 2.3.0, contains:MPEG ADTS, layer III, v1, 320 kbps, 44.1 kHz, JntStereo**

*READELF*

Adresse de commencement : **readelf -S /usr/bin/ls**

La partie .texte commence : **0000000000004d50**

*LDD*

**ldd /usr/bin/ls**

**alinux-vdso.so.1 (0x00007fffac5ef000)**

**libselinux.so.1 => /lib64/libselinux.so.1 (0x00007f8f77e64000)**

**libcap.so.2 => /lib64/libcap.so.2 (0x00007f8f77e5a000)**

**libc.so.6 => /lib64/libc.so.6 (0x00007f8f77c00000)**

**libpcre2-8.so.0 => /lib64/libpcre2-8.so.0 (0x00007f8f77b64000)**

**/lib64/ld-linux-x86-64.so.2 (0x00007f8f77ebb000)**

Glibc **: /lib64/libc.so.6 (0x00007f8f77c00000)**

**2.Syscalls basics**

**A.syscalls** :

Lire un fichier stocké sur un disque :

**|%rax|name|utility|**

**|:-:|:-:|:-|**

|0| **: read|lire des fichiers stockés sur un disque|**

|1| **: write|ecrire dans un fichier stocké sur disque|**

|59| **: execve|executer des processes/programmes|**

|57| **: fork|créér un nouveau process|**

**B.objdump :**

Afficher contenu de la section .text : **objdump -s -j .text /usr/bin/ls -d**

Instruction call :

**objdump -s -j .text /usr/bin/ls -d | grep "call"**

**171e8: e8 03 fe ff ff callq 16ff0 <\_obstack\_memory\_used@@Base+0x66e0>**

**16974: e8 07 e0 fe ff callq 4980 <memset@plt>**

**16826: e8 45 e2 fe ff callq 4a70 <memcpy@plt>**

**10819: e8 32 b9 ff ff callq c150 <\_\_sprintf\_chk@plt+0x7410>**

**108a4: ff d0 callq \*%rax**

**108cd: ff d0 callq \*%rax**

**1098e: e8 7d 40 ff ff callq 4a10 <strcmp@plt>**

Instruction syscall : **objdump -s -j .text /usr/bin/ls -d | grep "syscall"**

Aucune information retournée, ainsi on en déduit qu’il n’y a pas de syscall dans la commande « ls »

Instruction syscall dans Glibc : **objdump -s -d -j .text /usr/lib64/libc.so.6**

Instruction syscall qui exécute le syscall open :

**objdump -s -d -j .text /usr/lib64/libc.so.6 | grep "syscall" -B 3**

**127e95: b8 03 00 00 00 mov $0x3,%eax**

**127e9a: 8b 7d a0 mov -0x60(%rbp),%edi**

**127e9d: 0f 05 syscall**

Syscall appelle la variable contenant la valeur 3, qui est l'instruction syscall "**open**".

*Partie II : OBSERVE*

**1.strace**

strace de ls :

**strace ls dossier\_de\_tp**

puis 🡪 syscall écriture du résultat :

**write(1, "tp\_exemple tp\_leo1"..., 53tp\_exemple fichier\_tp**

**) = 53**

strace de cat :

**strace cat dossier\_de\_tp/fichier\_\_tp**

**openat(AT\_FDCWD, "dossier\_de\_tp/fichier\_tp", O\_RDONLY) = 3**

puis 🡪 ecriture des résultats dans le terminal

**write(1, "strace de cat\n", 10des cats**

**) = 10**

strace de curl efrei.fr : **strace -c curl efrei.fr**

**2.sysdig**

sysdig pour ls : **sysdig proc.name=ls**

puis 🡪 on tape ls dans un second terminal

**2039 18:10:34.403327526 0 ls (6317.6317) < write res=31 data=fichier\_tp**

sysdig pour cat :

**sysdig proc.name=cat**

puis 🡪 syscall demande l'ouverture du fichier

**1070 18:20:07.408883391 0 cat (6363.6363) < openat fd=3(<f>/home/LucasM/dossier\_de\_tp/fichier\_tp) dirfd=-100(AT\_FDCWD) name=dossier\_de\_tp/fichier\_tp(/home/LucasM/dossier\_de\_tp/fichier\_tp) flags=1(O\_RDONLY) mode=0 dev=FD00 ino=215897**

Enfin 🡪 syscall ecrit le contenu du fichier dans le terminal

**1082 18:20:07.409164408 0 cat (6363.6363) < write res=10 data=des CATS.**

sysdig pour tracer les syscall de mon utilisateur : **sysdig user.name=LucasM**

**2.NGINX Tracing**

Sysdig sur NGINX : **sysdig proc.name=nginx**

Puis 🡪 lancer le service nginx manuellement dans un terminal

**/usr/sbin/nginx**

Syscalls repérés lors du sysdig de nginx **: epoll\_wait accept4 recvfrom close switch epoll\_ctl setsockopt write sendfile writev fstat newfstatat openat**

**3.NGINX Hardening**

On ajoute la ligne trouvée précédemment dans la configuration du service :

**[Service]**

**SystemCallFilter=epoll\_wait accept4 recvfrom close switch epoll\_ctl setsockopt write sendfile writev fstat newfstatat openat**

*Partie IV*

**1.Test**

Ouverture du port pour le fonctionnement de l'app **: sudo firewall-cmd --zone=public --add-port=13337/tcp --permanent**

Fichier calculatrice.service :

**[unit]**

**Description=Calc nc eval**

**[Service]**

**ExecStart=/usr/bin/python3 /opt/calc.py**

**Restart=always**