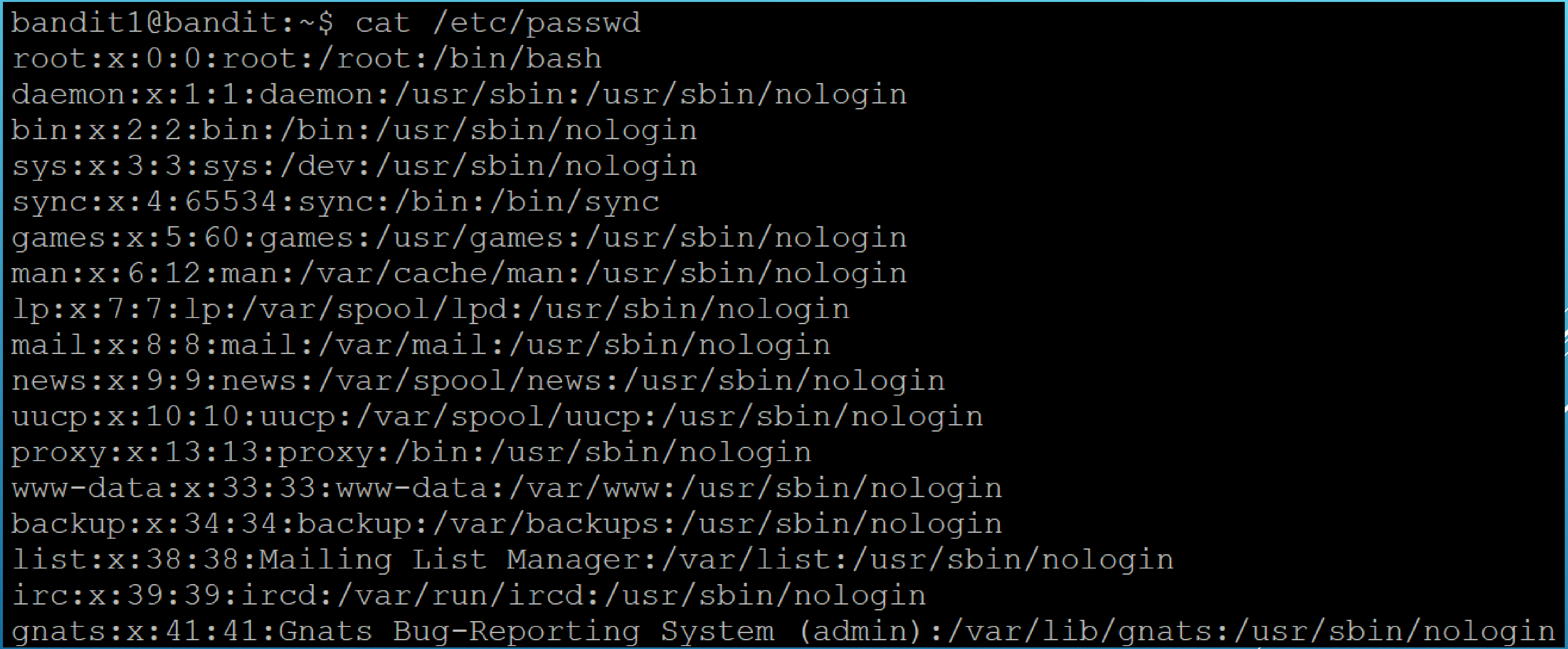
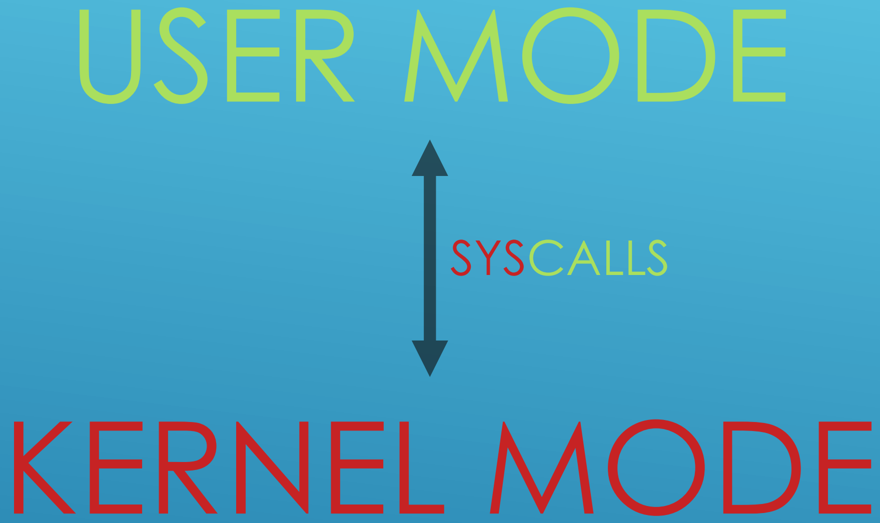
ESKALACJA UPRAWNIEŃ: PODSTAWY

Mawekl



```
bandit1@bandit:~$ cat /etc/passwd
root:x:0:0:root:/root:/bin/bash
daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/bin/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/bin:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin
gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin
```

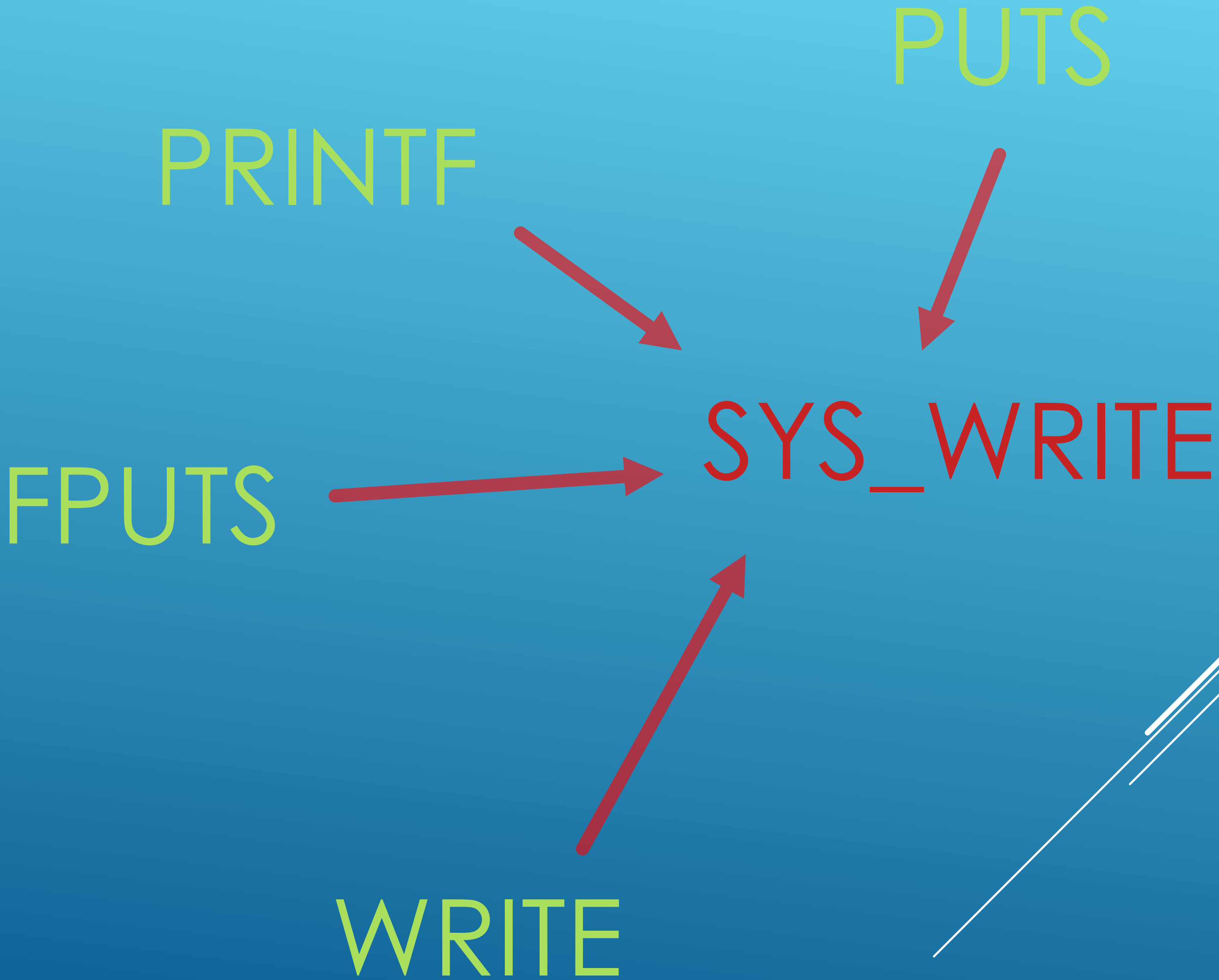
ATTACK SURFACES:
- KERNEL
- SET-UID, SET-GID



USER MODE

SYSCALLS

KERNEL MODE



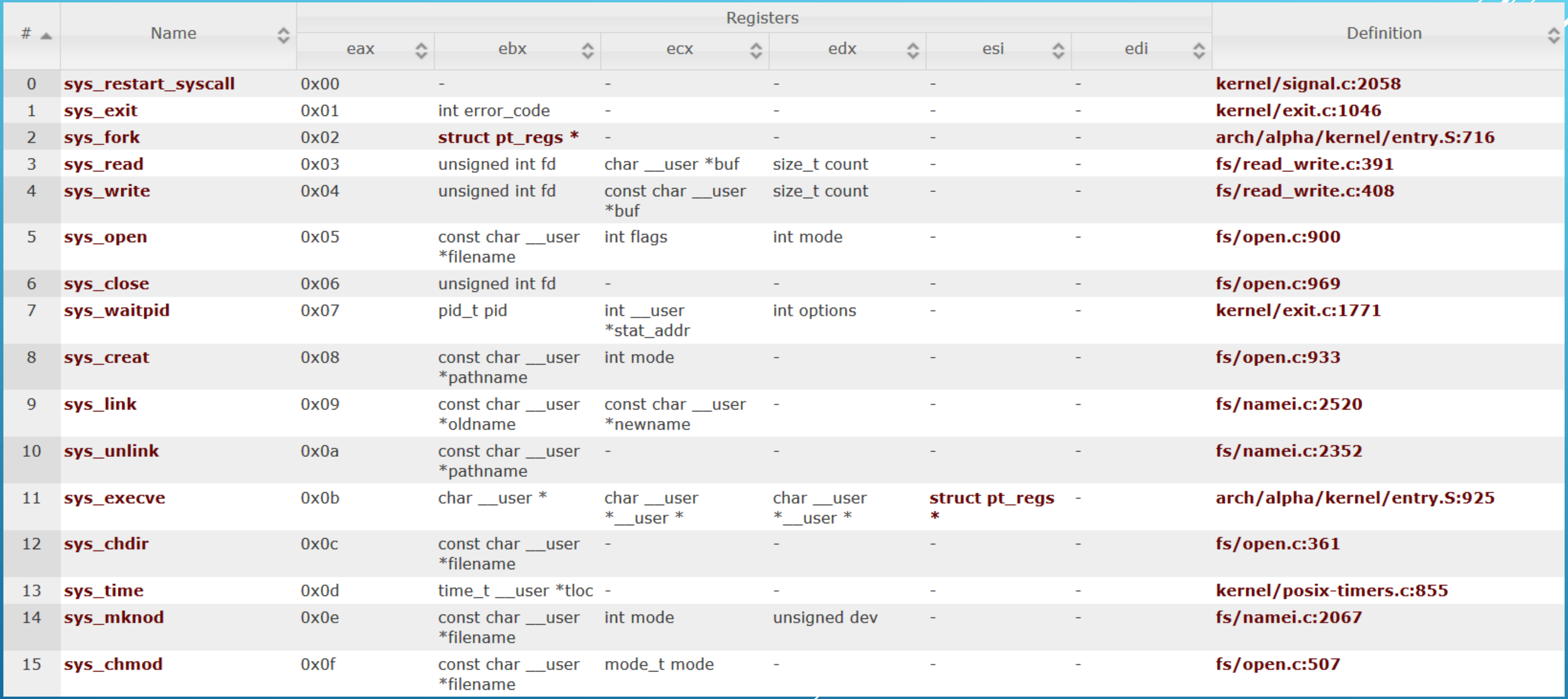
PUTS

PRINTF

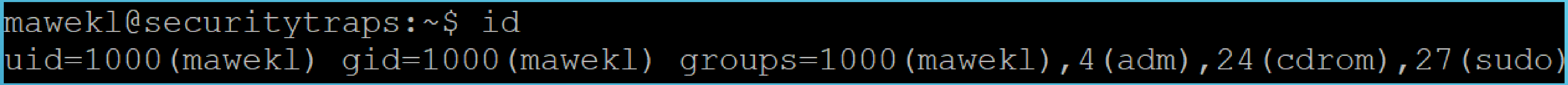
SYS_WRITE

FPUTS

WRITE



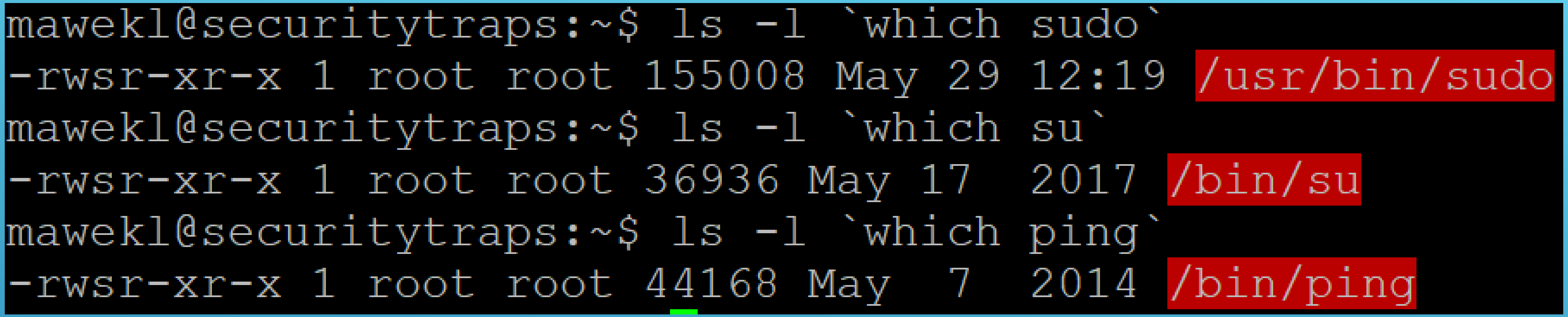
#	Name	Registers						Definition
		eax	ebx	ecx	edx	esi	edi	
0	**sys_restart_syscall**	0x00	-	-	-	-	-	**kernel/signal.c:2058**
1	**sys_exit**	0x01	int error_code	-	-	-	-	**kernel/exit.c:1046**
2	**sys_fork**	0x02	**struct pt_regs ***	-	-	-	-	**arch/alpha/kernel/entry.S:716**
3	**sys_read**	0x03	unsigned int fd	char __user *buf	size_t count	-	-	**fs/read_write.c:391**
4	**sys_write**	0x04	unsigned int fd	const char __user *buf	size_t count	-	-	**fs/read_write.c:408**
5	**sys_open**	0x05	const char __user *filename	int flags	int mode	-	-	**fs/open.c:900**
6	**sys_close**	0x06	unsigned int fd	-	-	-	-	**fs/open.c:969**
7	**sys_waitpid**	0x07	pid_t pid	int __user *stat_addr	int options	-	-	**kernel/exit.c:1771**
8	**sys_creat**	0x08	const char __user *pathname	int mode	-	-	-	**fs/open.c:933**
9	**sys_link**	0x09	const char __user *oldname	const char __user *newname	-	-	-	**fs/namei.c:2520**
10	**sys_unlink**	0x0a	const char __user *pathname	-	-	-	-	**fs/namei.c:2352**
11	**sys_execve**	0x0b	char __user *	char __user *__user *	char __user *__user *	**struct pt_regs ***	-	**arch/alpha/kernel/entry.S:925**
12	**sys_chdir**	0x0c	const char __user *filename	-	-	-	-	**fs/open.c:361**
13	**sys_time**	0x0d	time_t __user *tloc	-	-	-	-	**kernel/posix-timers.c:855**
14	**sys_mknod**	0x0e	const char __user *filename	int mode	unsigned dev	-	-	**fs/namei.c:2067**
15	**sys_chmod**	0x0f	const char __user *filename	mode_t mode	-	-	-	**fs/open.c:507**



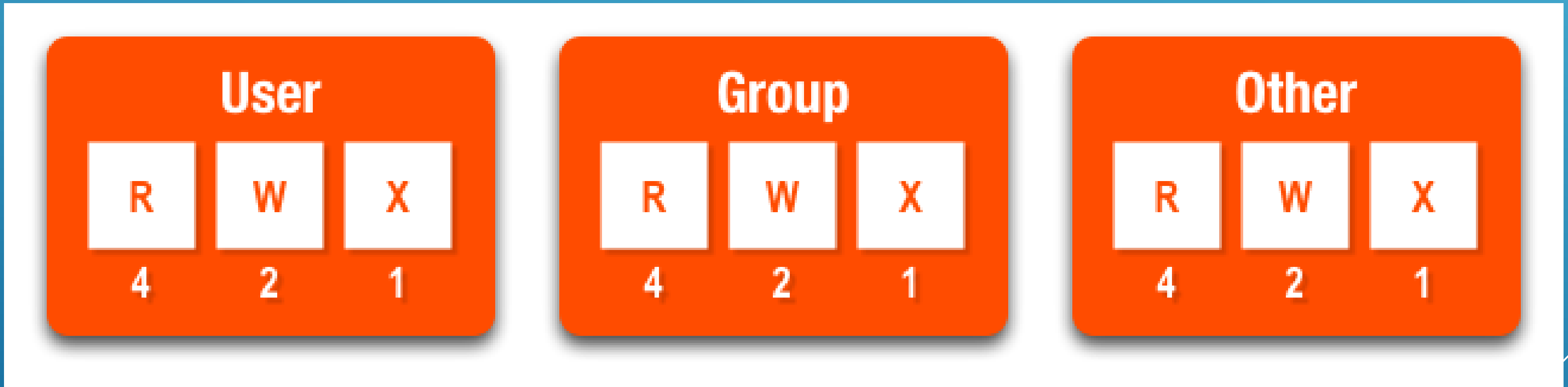
```
mawekl@securitytraps:~$ id
uid=1000(mawekl) gid=1000(mawekl) groups=1000(mawekl),4(adm),24(cdrom),27(sudo)
```

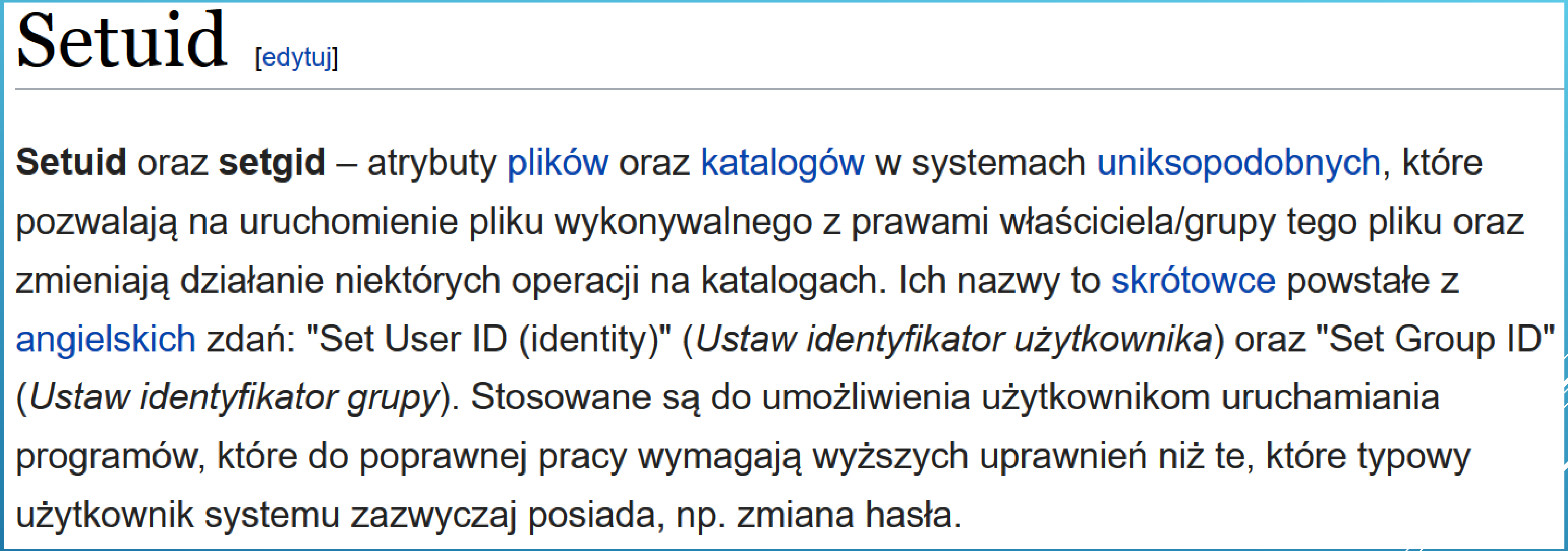
Real UID
Effective UID
Saved UID

Real GID
Effective GID
Saved GID



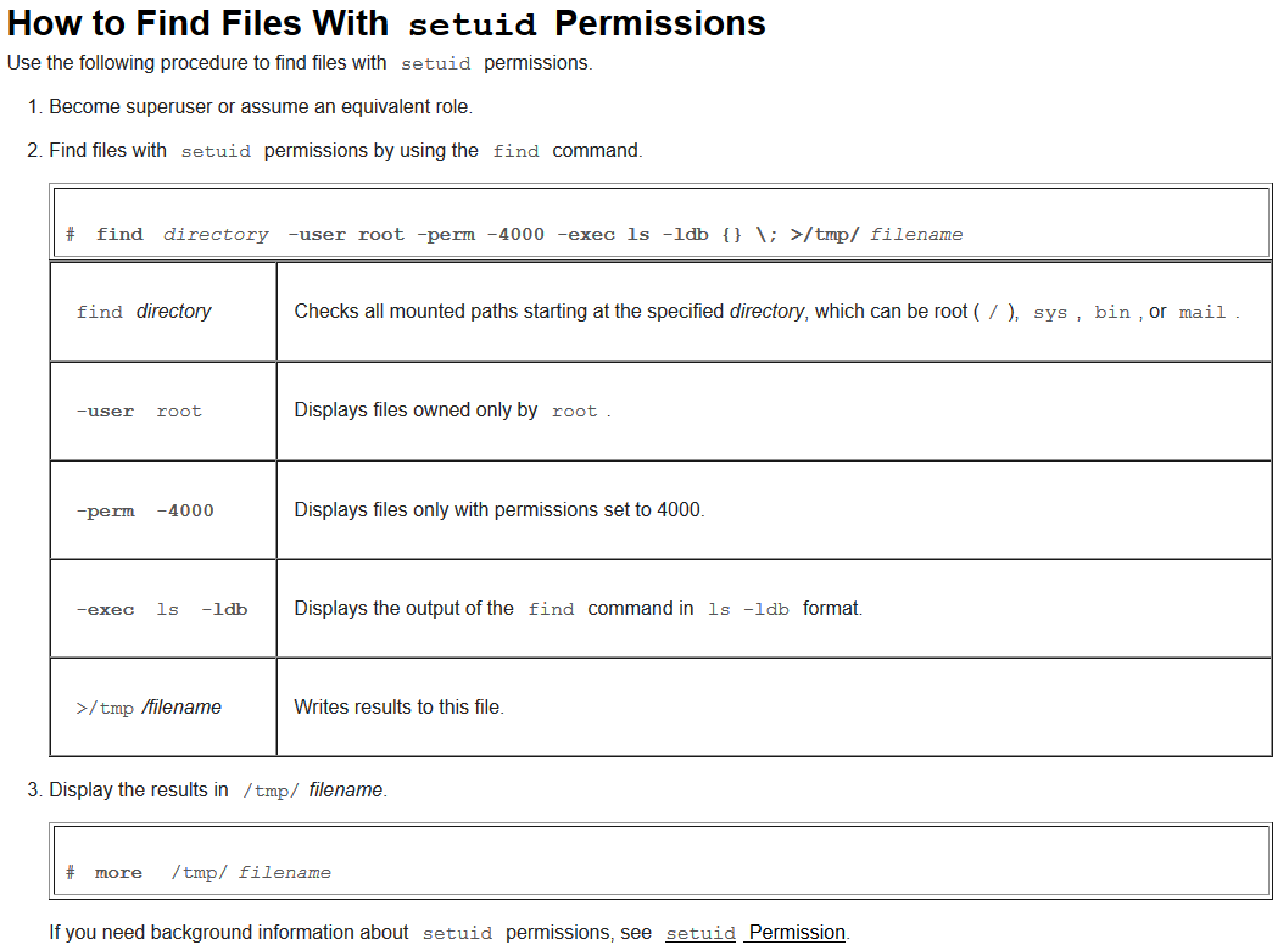
```
mawekl@securitytraps:~$ ls -l `which sudo`
-rwsr-xr-x 1 root root 155008 May 29 12:19 /usr/bin/sudo
mawekl@securitytraps:~$ ls -l `which su`
-rwsr-xr-x 1 root root 36936 May 17  2017 /bin/su
mawekl@securitytraps:~$ ls -l `which ping`
-rwsr-xr-x 1 root root 44168 May  7  2014 /bin/ping
```





Setuid [edytuj]

Setuid oraz **setgid** – atrybuty plików oraz katalogów w systemach uniksopodobnych, które pozwalają na uruchomienie pliku wykonywalnego z prawami właściciela/grupy tego pliku oraz zmieniają działanie niektórych operacji na katalogach. Ich nazwy to skrótowce powstałe z angielskich zdań: "Set User ID (identity)" (*Ustaw identyfikator użytkownika*) oraz "Set Group ID" (*Ustaw identyfikator grupy*). Stosowane są do umożliwienia użytkownikom uruchamiania programów, które do poprawnej pracy wymagają wyższych uprawnień niż te, które typowy użytkownik systemu zazwyczaj posiada, np. zmiana hasła.



How to Find Files With `setuid` Permissions

Use the following procedure to find files with `setuid` permissions.

1. Become superuser or assume an equivalent role.
2. Find files with `setuid` permissions by using the `find` command.

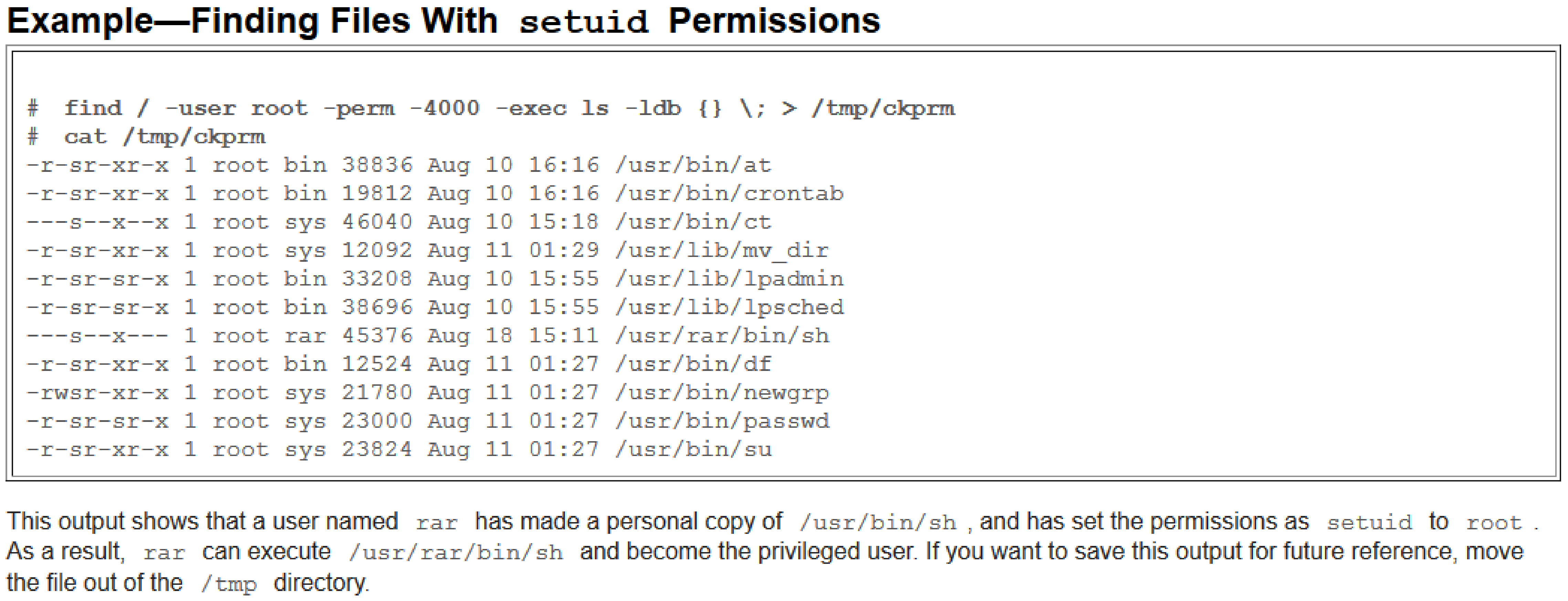
```
# find directory -user root -perm -4000 -exec ls -ldb {} \; >/tmp/ filename
```

`find` *directory*	Checks all mounted paths starting at the specified *directory*, which can be root (`/`), `sys` , `bin` , or `mail` .
`-user root`	Displays files owned only by `root` .
`-perm -4000`	Displays files only with permissions set to 4000.
`-exec ls -ldb`	Displays the output of the `find` command in `ls -ldb` format.
`>/tmp` */filename*	Writes results to this file.

3. Display the results in `/tmp/` *filename*.

```
# more /tmp/ filename
```

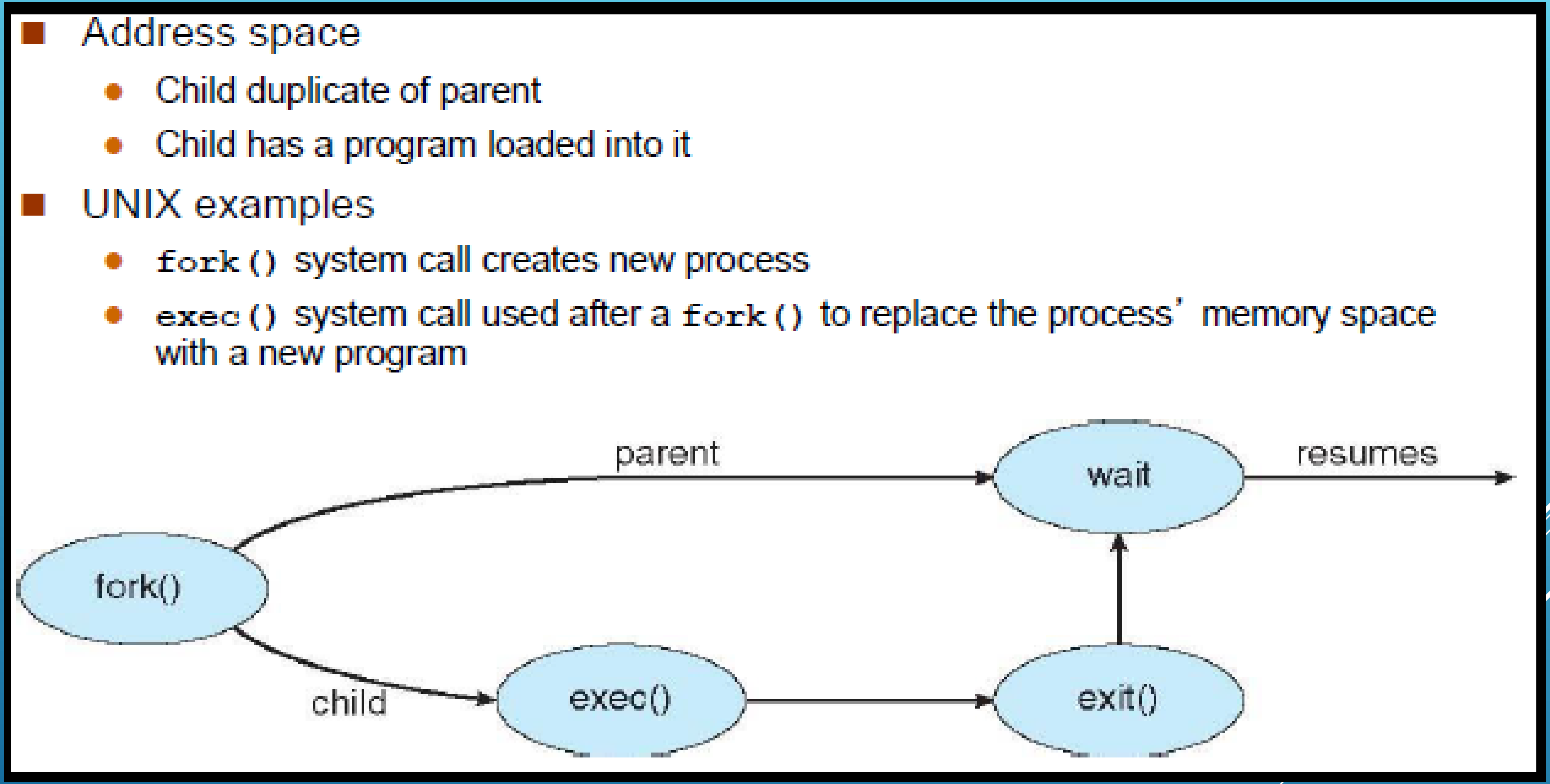
If you need background information about `setuid` permissions, see `setuid` Permission.



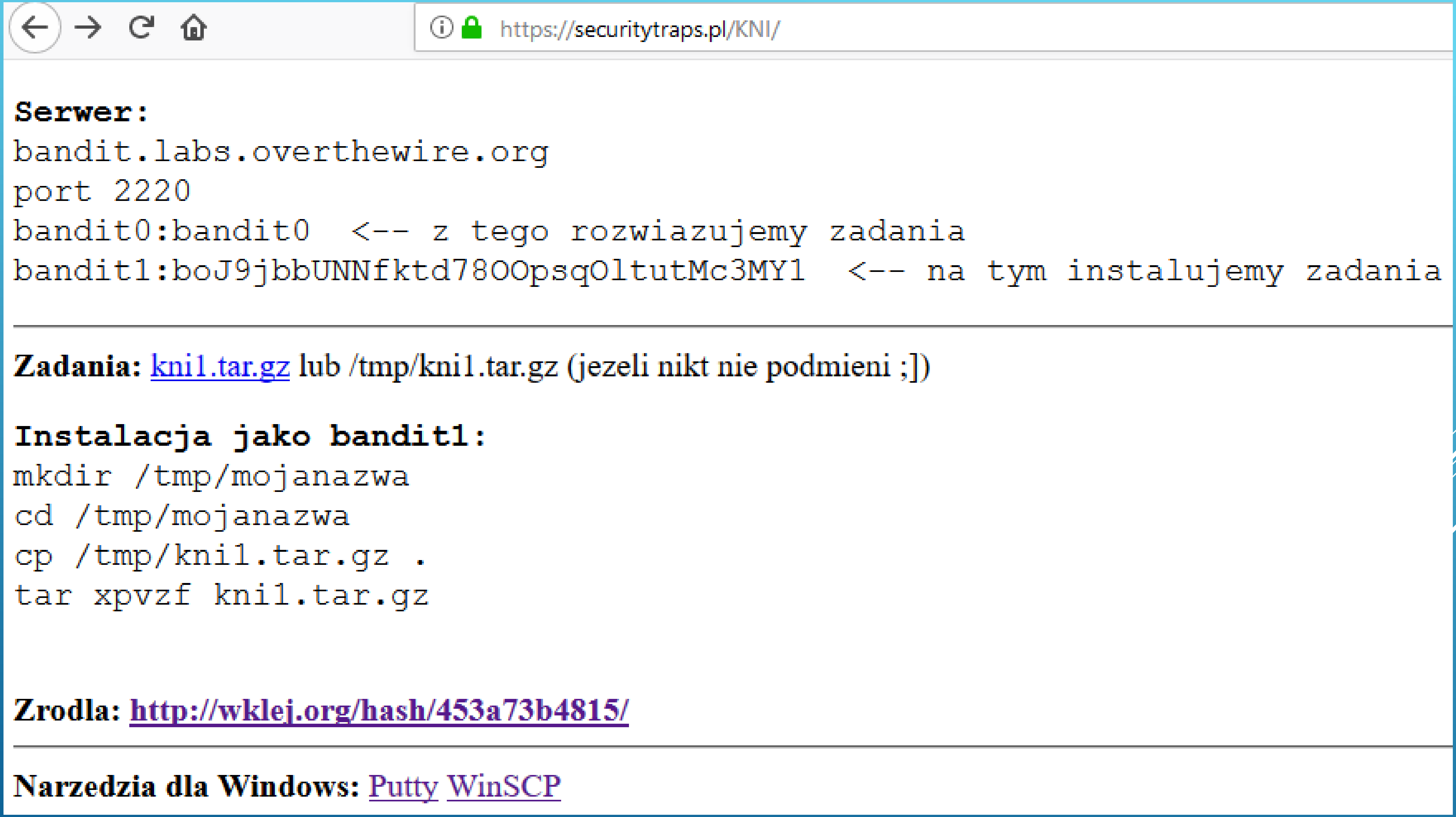
Example—Finding Files With setuid Permissions

```
#  find / -user root -perm -4000 -exec ls -ldb {} \; > /tmp/ckprm
#  cat /tmp/ckprm
-r-sr-xr-x 1 root bin 38836 Aug 10 16:16 /usr/bin/at
-r-sr-xr-x 1 root bin 19812 Aug 10 16:16 /usr/bin/crontab
---s--x--x 1 root sys 46040 Aug 10 15:18 /usr/bin/ct
-r-sr-xr-x 1 root sys 12092 Aug 11 01:29 /usr/lib/mv_dir
-r-sr-sr-x 1 root bin 33208 Aug 10 15:55 /usr/lib/lpadmin
-r-sr-sr-x 1 root bin 38696 Aug 10 15:55 /usr/lib/lpsched
---s--x--- 1 root rar 45376 Aug 18 15:11 /usr/rar/bin/sh
-r-sr-xr-x 1 root bin 12524 Aug 11 01:27 /usr/bin/df
-rwsr-xr-x 1 root sys 21780 Aug 11 01:27 /usr/bin/newgrp
-r-sr-sr-x 1 root sys 23000 Aug 11 01:27 /usr/bin/passwd
-r-sr-xr-x 1 root sys 23824 Aug 11 01:27 /usr/bin/su
```

This output shows that a user named `rar` has made a personal copy of `/usr/bin/sh` , and has set the permissions as `setuid` to `root` . As a result, `rar` can execute `/usr/rar/bin/sh` and become the privileged user. If you want to save this output for future reference, move the file out of the `/tmp` directory.



- Address space
  - Child duplicate of parent
  - Child has a program loaded into it
- UNIX examples
  - `fork()` system call creates new process
  - `exec()` system call used after a `fork()` to replace the process' memory space with a new program



Serwer:

```
bandit.labs.overthewire.org
port 2220
bandit0:bandit0  <-- z tego rozwiazujemy zadania
bandit1:boJ9jbbUNNfktd78OOpsqOltutMc3MY1  <-- na tym instalujemy zadania
```

Zadania: kni1.tar.gz lub /tmp/kni1.tar.gz (jezeli nikt nie podmieni ;])

Instalacja jako bandit1:

```
mkdir /tmp/mojanazwa
cd /tmp/mojanazwa
cp /tmp/kni1.tar.gz .
tar xpvzf kni1.tar.gz
```

Zrodla: http://wklej.org/hash/453a73b4815/

Narzedzia dla Windows: Putty WinSCP