Хакимуллин Рустем Рафаилевич, 11-901

ЛАБОРАТОРНАЯ РАБОТА №1. LIME И VOLATILITY. ФОРЕНЗИКА.

Шаблон для упражнения:

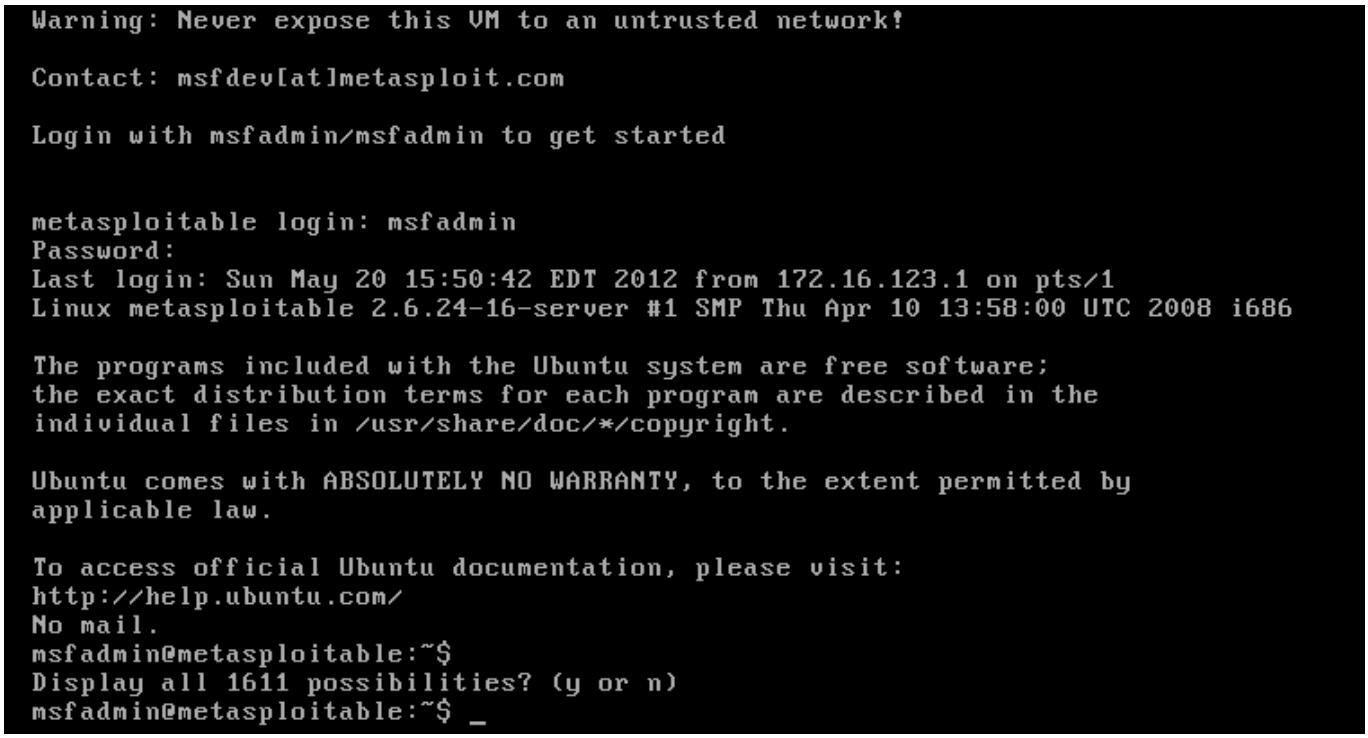
- Цель
- Ситуация
- Алгоритм
- Результат

Содержание:

Создание виртуальной машины Metasploitable

1.2.1. Вход в Metasploitable

- Цель: Создать и войти в виртуальную
- Ситуация: есть образ машины и VirtualBox
- Алгоритм:
    1. Создаем машину в VirtualBox
    2. Выбираем нужный образ машины
- Результат: можем работать с виртуальной машиной



Смена пароля для пользователя msfadmin

- Цель: изменить пароль пользователя
- Ситуация: имеем дефолтные данные пользователя
- Алгоритм:
    1. `sudo su-`
    2. вводим старый пароль
    3. вводим новый пароль

- Результат: пароль изменён

```
msfadmin@metasploitable:~$ sudo su -
[sudo] password for msfadmin:
Sorry, try again.
[sudo] password for msfadmin:
root@metasploitable:~# passwd
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
root@metasploitable:~#
```

Обновление библиотек

- Цель: Изменить репозитории
- Ситуация: есть дефолтные репозитории
- Алгоритм:

Создание backup-файла репозиториев - Переходим в папку /etc/apt
Сохраняем резервную копию списка репозиториев с помощью команды `sudo cp sources.list sources.list.BKP`
Просмотрим с помощью `ls -l sources.list*`

```
root@metasploitable:~# cd /etc/apt
root@metasploitable:/etc/apt# cp sources.list.sources.list.BKP
cp: missing destination file operand after `sources.list.sources.list.BKP'
Try `cp --help' for more information.
root@metasploitable:/etc/apt# cp sources.list sources.list.BKP
root@metasploitable:/etc/apt# ls -l sources.list*
-rw-r--r-- 1 root root 3152 2010-04-16 02:06 sources.list
-rw-r--r-- 1 root root    0 2010-03-16 19:01 sources.list~
-rw-r--r-- 1 root root 3152 2022-04-20 17:47 sources.list.BKP

sources.list.d:
total 0
```

Просмотр списка репозиториев - Смотрим репозитории, которые есть на данный момент с помощью команды `grep -v “^#” sources.list | head -20:`

```
root@metasploitable:/etc/apt# grep -v "^#" sources.list | head -20

deb http://us.archive.ubuntu.com/ubuntu/ hardy main restricted
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy main restricted

deb http://us.archive.ubuntu.com/ubuntu/ hardy-updates main restricted
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy-updates main restricted

deb http://us.archive.ubuntu.com/ubuntu/ hardy universe
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy universe
deb http://us.archive.ubuntu.com/ubuntu/ hardy-updates universe
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy-updates universe

deb http://us.archive.ubuntu.com/ubuntu/ hardy multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy multiverse
deb http://us.archive.ubuntu.com/ubuntu/ hardy-updates multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy-updates multiverse

deb http://us.archive.ubuntu.com/ubuntu/ hardy-backports main restricted univers
e multiverse
deb-src http://us.archive.ubuntu.com/ubuntu/ hardy-backports main restricted uni
verse multiverse
```

Замена репозиториев командой `sed -i 's/http:\/\/us.archive.ubuntu.com/http:\/\/old-releases.ubuntu.com/g' sources.list`

```
root@metasploitable:/etc/apt# grep -v "^#" sources.list | head -20

deb http://old-releases.ubuntu.com/ubuntu/ hardy main restricted
deb-src http://old-releases.ubuntu.com/ubuntu/ hardy main restricted

deb http://old-releases.ubuntu.com/ubuntu/ hardy-updates main restricted
deb-src http://old-releases.ubuntu.com/ubuntu/ hardy-updates main restricted

deb http://old-releases.ubuntu.com/ubuntu/ hardy universe
deb-src http://old-releases.ubuntu.com/ubuntu/ hardy universe
deb http://old-releases.ubuntu.com/ubuntu/ hardy-updates universe
deb-src http://old-releases.ubuntu.com/ubuntu/ hardy-updates universe

deb http://old-releases.ubuntu.com/ubuntu/ hardy multiverse
deb-src http://old-releases.ubuntu.com/ubuntu/ hardy multiverse
deb http://old-releases.ubuntu.com/ubuntu/ hardy-updates multiverse
deb-src http://old-releases.ubuntu.com/ubuntu/ hardy-updates multiverse

deb http://old-releases.ubuntu.com/ubuntu/ hardy-backports main restricted unive
rse multiverse
deb-src http://old-releases.ubuntu.com/ubuntu/ hardy-backports main restricted u
niverse multiverse

root@metasploitable:/etc/apt# sed -i 's/http:\/\/us.archive.ubuntu.com/http:\/\/
old-releases.ubuntu.com/g' sources.list
```

1.3.4. Обновить список репозиториев для менеджера пакетов apt

```
W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/restri
cted/binary-i386/Packages.gz  404 Not Found [IP: 185.125.190.36 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/main/s
ource/Sources.gz  404 Not Found [IP: 185.125.190.36 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/restri
cted/source/Sources.gz  404 Not Found [IP: 185.125.190.36 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/univer
se/binary-i386/Packages.gz  404 Not Found [IP: 185.125.190.36 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/univer
se/source/Sources.gz  404 Not Found [IP: 185.125.190.36 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/multiv
erse/binary-i386/Packages.gz  404 Not Found [IP: 185.125.190.36 80]

W: Failed to fetch http://security.ubuntu.com/ubuntu/dists/hardy-security/multiv
erse/source/Sources.gz  404 Not Found [IP: 185.125.190.36 80]

E: Some index files failed to download, they have been ignored, or old ones used
 instead.
root@metasploitable:/etc/apt#
```

Установка заголовочных файлов ядра с помощью команды `sudo apt-get install linux-headers-2.6.24-16-server`

```
Reading state information... Done
The following extra packages will be installed:
  linux-headers-2.6.24-16
The following NEW packages will be installed:
  linux-headers-2.6.24-16 linux-headers-2.6.24-16-server
0 upgraded, 2 newly installed, 0 to remove and 154 not upgraded.
Need to get 8773kB of archives.
After this operation, 68.3MB of additional disk space will be used.
Do you want to continue [Y/n]? y
Get:1 http://old-releases.ubuntu.com hardy/main linux-headers-2.6.24-16 2.6.24-1
6.30 [8129kB]
Get:2 http://old-releases.ubuntu.com hardy/main linux-headers-2.6.24-16-server 2
.6.24-16.30 [644kB]
Fetched 8773kB in 20s (429kB/s)
Selecting previously deselected package linux-headers-2.6.24-16.
(Reading database ... 37635 files and directories currently installed.)
Unpacking linux-headers-2.6.24-16 (from .../linux-headers-2.6.24-16_2.6.24-16.30
_all.deb) ...
Selecting previously deselected package linux-headers-2.6.24-16-server.
Unpacking linux-headers-2.6.24-16-server (from .../linux-headers-2.6.24-16-serve
r_2.6.24-16.30_i386.deb) ...
Setting up linux-headers-2.6.24-16 (2.6.24-16.30) ...
Setting up linux-headers-2.6.24-16-server (2.6.24-16.30) ...
```

Установка утилиты Zip с помощью команды `sudo apt-get install zip`

```
root@metasploitable:/etc/apt# apt-get install zip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  zip
0 upgraded, 1 newly installed, 0 to remove and 154 not upgraded.
Need to get 106kB of archives.
After this operation, 254kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com hardy/main zip 2.32-1 [106kB]
Fetched 106kB in 0s (128kB/s)
Selecting previously deselected package zip.
(Reading database ... 52382 files and directories currently installed.)
Unpacking zip (from .../archives/zip_2.32-1_i386.deb) ...
Setting up zip (2.32-1) ...
root@metasploitable:/etc/apt#
```

- Результат: обновлены библиотеки и установлены новые

Установка LiME

- Цель: установить LiME
- Ситуация: LiME не поставлен
- Алгоритм:
    1. Скачиваем архив с помощью команды `wget http://www.computersecuritystudent.com/DOWNLOADS/lime-forensics-1.1-r17.tar.gz`
    2. Распаковываем с помощью команды `tar zxvf lime*.tar.gz`
    3. Переходим в корень с помощью команды `cd src/`
    4. Собираем с помощью команды `make`
- Результат: LiME установлен

```
root@metasploitable:/var/tmp# cd src
root@metasploitable:/var/tmp/src# make
make -C /lib/modules/2.6.24-16-server/build M=/var/tmp/src modules
make[1]: Entering directory `/usr/src/linux-headers-2.6.24-16-server'
  CC [M]  /var/tmp/src/tcp.o
  CC [M]  /var/tmp/src/disk.o
  CC [M]  /var/tmp/src/main.o
  LD [M]  /var/tmp/src/lime.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /var/tmp/src/lime.mod.o
  LD [M]  /var/tmp/src/lime.ko
make[1]: Leaving directory `/usr/src/linux-headers-2.6.24-16-server'
strip --strip-unneeded lime.ko
mv lime.ko lime-2.6.24-16-server.ko
make tidy
make[1]: Entering directory `/var/tmp/src'
rm -f *.o *.mod.c Module.symvers Module.markers modules.order \.*.o.cmd \.*.ko.c
md \.*.o.d
rm -rf \.tmp_versions
make[1]: Leaving directory `/var/tmp/src'
root@metasploitable:/var/tmp/src# ls
disk.c                    lime.h  Makefile         tcp.c
lime-2.6.24-16-server.ko  main.c  Makefile.sample
root@metasploitable:/var/tmp/src#
```

Установка вспомогательных библиотек

- Цель: установить библиотеки
- Ситуация: нет необходимых библиотек
- Алгоритм:
  Установили заголовочные файлы библиотеки libelf командой
  `apt-get install libelfg0-dev`

```
root@metasploitable:/var/tmp/src# apt-get install libelfg0-dev
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following NEW packages will be installed:
  libelfg0-dev
0 upgraded, 1 newly installed, 0 to remove and 154 not upgraded.
Need to get 60.1kB of archives.
After this operation, 258kB of additional disk space will be used.
Get:1 http://old-releases.ubuntu.com hardy/main libelfg0-dev 0.8.6-4 [60.1kB]
Fetched 60.1kB in 0s (154kB/s)
Selecting previously deselected package libelfg0-dev.
(Reading database ... 52397 files and directories currently installed.)
Unpacking libelfg0-dev (from .../libelfg0-dev_0.8.6-4_i386.deb) ...
Setting up libelfg0-dev (0.8.6-4) ...

root@metasploitable:/var/tmp/src# _
```

Распаковка архива командой `tar zxfv libdwarf-20140208.tar.gz`

```
root@metasploitable:/var/tmp# wget http://www.computersecuritystudent.com/SECURI
TY_TOOLS/METASPLOITABLE/EXPLOIT/lesson1/libdwarf-20140208.tar.gz
--18:50:26--  http://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITAB
LE/EXPLOIT/lesson1/libdwarf-20140208.tar.gz
           => `libdwarf-20140208.tar.gz'
Resolving www.computersecuritystudent.com... 108.210.130.146
Connecting to www.computersecuritystudent.com|108.210.130.146|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1,718,546 (1.6M) [application/x-gzip]

100%[====================================>] 1,718,546    382.69K/s    ETA 00:00

18:50:31 (347.14 KB/s) - `libdwarf-20140208.tar.gz' saved [1718546/1718546]
```

сборка командой `make`

```
tatic_vars.o print_static_vars.cc
g++  -g -O2 -I. -I. -I./../libdwarf -DCONFPREFIX=/usr/local/lib    -c -o print_s
trings.o print_strings.cc
g++  -g -O2 -I. -I. -I./../libdwarf -DCONFPREFIX=/usr/local/lib    -c -o print_t
ypes.o print_types.cc
g++  -g -O2 -I. -I. -I./../libdwarf -DCONFPREFIX=/usr/local/lib    -c -o print_w
eaknames.o print_weaknames.cc
g++  -g -O2 -I. -I. -I./../libdwarf -DCONFPREFIX=/usr/local/lib    -c -o strstrn
ocase.o strstrnocase.cc
g++  -g -O2 -I. -I. -I./../libdwarf -DCONFPREFIX=/usr/local/lib    -c -o uri.o u
ri.cc
g++  -g -O2 -I. -I. -I./../libdwarf -DCONFPREFIX=/usr/local/lib  -o dwarfdump ch
eckutil.o dwarfdump.o dwconf.o print_abbrevs.o print_aranges.o print_die.o print
_frames.o print_lines.o print_locs.o print_macros.o print_pubnames.o print_range
s.o print_reloc.o print_sections.o print_static_funcs.o print_static_vars.o prin
t_strings.o print_types.o print_weaknames.o strstrnocase.o uri.o naming.o common
.o  tag_common.o    -L../libdwarf -ldwarf -lelf
make[1]: Leaving directory `/var/tmp/dwarf-20140208/dwarfdump2'



root@metasploitable:/var/tmp/dwarf-20140208# cp dwarfdump/dwarfdump /usr/bin
root@metasploitable:/var/tmp/dwarf-20140208#
```

скопировали собранный файл в папку исполняемых файлов командой `cp dwarfdump/dwarfdump /usr/bin`

```
root@metasploitable:/var/tmp/dwarf-20140208# ls /usr/bin/dwarfdump
/usr/bin/dwarfdump
```

- Результат: библиотеки установлены и находятся в usr/bin

Скачивание, настройка и установка фреймворка Volatility

- Цель: скачать Volatility
- Ситуация: Volatility не установлен

- Алгоритм: Скачали архив с исходными кодами с помощью команды `wget http://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITABLE/EXPLOIT/lesson1/volatility-2.3.1.tar.gz`

```
root@metasploitable:/var/tmp# wget http://www.computersecuritystudent.com/SECURI
TY_TOOLS/METASPLOITABLE/EXPLOIT/lesson1/volatility-2.3.1.tar.gz
--19:24:25--  http://www.computersecuritystudent.com/SECURITY_TOOLS/METASPLOITAB
LE/EXPLOIT/lesson1/volatility-2.3.1.tar.gz
           => `volatility-2.3.1.tar.gz'
Resolving www.computersecuritystudent.com... 108.210.130.146
Connecting to www.computersecuritystudent.com|108.210.130.146|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 1,764,063 (1.7M) [application/x-gzip]

100%[====================================>] 1,764,063    374.77K/s    ETA 00:00

19:24:30 (332.39 KB/s) - `volatility-2.3.1.tar.gz' saved [1764063/1764063]
```

распаковка

```
volatility-2.3.1/CREDITS.txt
volatility-2.3.1/resources/
volatility-2.3.1/resources/volatility.ico
volatility-2.3.1/resources/volatility.svg
volatility-2.3.1/tools/
volatility-2.3.1/tools/linux/
volatility-2.3.1/tools/linux/Makefile
volatility-2.3.1/tools/linux/module.c
volatility-2.3.1/tools/linux/pmem/
volatility-2.3.1/tools/linux/pmem/Makefile
volatility-2.3.1/tools/linux/pmem/pmem.c
volatility-2.3.1/tools/vtype_diff.py
volatility-2.3.1/tools/mac/
volatility-2.3.1/tools/mac/convert.py
volatility-2.3.1/vol.py
volatility-2.3.1/pyinstaller/
volatility-2.3.1/pyinstaller/hook-distorm3.py
volatility-2.3.1/pyinstaller/hook-volatility.py
volatility-2.3.1/pyinstaller.spec
volatility-2.3.1/volatility.egg-info/
volatility-2.3.1/volatility.egg-info/SOURCES.txt
volatility-2.3.1/volatility.egg-info/dependency_links.txt
volatility-2.3.1/volatility.egg-info/top_level.txt
volatility-2.3.1/volatility.egg-info/PKG-INFO
root@metasploitable:/var/tmp# _
```

Сборка командой `make`

```
root@metasploitable:/var/tmp# cd volatility-2.3.1/tools/linux/
root@metasploitable:/var/tmp/volatility-2.3.1/tools/linux# make
make -C //lib/modules/2.6.24-16-server/build CONFIG_DEBUG_INFO=y M=/var/tmp/vola
tility-2.3.1/tools/linux modules
make[1]: Entering directory `/usr/src/linux-headers-2.6.24-16-server'
  CC [M]  /var/tmp/volatility-2.3.1/tools/linux/module.o
  Building modules, stage 2.
  MODPOST 1 modules
  CC      /var/tmp/volatility-2.3.1/tools/linux/module.mod.o
  LD [M]  /var/tmp/volatility-2.3.1/tools/linux/module.ko
make[1]: Leaving directory `/usr/src/linux-headers-2.6.24-16-server'
dwarfdump -di module.ko > module.dwarf
make -C //lib/modules/2.6.24-16-server/build M=/var/tmp/volatility-2.3.1/tools/l
inux clean
make[1]: Entering directory `/usr/src/linux-headers-2.6.24-16-server'
  CLEAN   /var/tmp/volatility-2.3.1/tools/linux/.tmp_versions
  CLEAN   /var/tmp/volatility-2.3.1/tools/linux/Module.symvers
make[1]: Leaving directory `/usr/src/linux-headers-2.6.24-16-server'
root@metasploitable:/var/tmp/volatility-2.3.1/tools/linux#
```

```
root@metasploitable:/var/tmp/volatility-2.3.1/tools/linux# ls -l module.dwarf
-rw-r--r-- 1 root root 1051355 2022-04-20 19:26 module.dwarf
```

Создание пользователя

```
root@metasploitable:/# zip /var/www/UBUNTU-MSF804.zip /var/tmp/volatility-2.3.1/
tools/linux/module.dwarf /boot/System.map-2.6.24-16-server
  adding: var/tmp/volatility-2.3.1/tools/linux/module.dwarf (deflated 90%)
  adding: boot/System.map-2.6.24-16-server (deflated 74%)
root@metasploitable:/# ls -l /var/www/UBUNTU-MSF804.zip
-rw-r--r-- 1 root root 345639 2022-04-20 19:38 /var/www/UBUNTU-MSF804.zip
```

Результат: Volatility установлен, профиль создан

Форензика

- Цель: создать дамп оперативной памяти и посмотреть её
- Ситуация: Нет дампа оперативной памяти
- Алгоритм: Создаём дамп с помощью команды `sudo insmod lime-2.6.24-16-server.ko "path=/var/tmp/src/mem.img format=lime"`

```
root@metasploitable:/# cd /var/tmp/src/
root@metasploitable:/var/tmp/src# insmod lime-2.6.24-16-server.ko  "path=/var/tm
p/src/mem.img format=lime"
```

Копируем ранее созданный профиль Volatility

`cd /var/tmp/volatility-2.3.1;` mkdir ./volatility/profiles

`cp /var/www/UBUNTU-MSF804.zip /var/tmp/volatility-2.3.1./volatility/profiles/;` vol.py --plugins=/var/tmp/volatility-2.3.1./volatility/profiles/ --info | grep –i profile | grep –i linux;`

необходим Python более старой версии, установлен более новый, не работает

- Результат: проделана только первая часть работы (дамп оперативной памяти), далее не получилось просмотреть из-за версии Pythona

Оформление результатов