Вводная лекция

CTF

Jeopardy (task-based)	Attack-Defense

1. **Reverse**
2. **PWN**
3. **WEB**
4. **Cryptography**
5. Misc
6. Forensics
7. Network
8. Steganography
9. PPC

http://ctftime.org/ - Все CTFы

https://kmb.ufoctf.ru/ - Краткий экскурс

Что нужно для CTF?

1. Умение гуглить
2. Упорство
3. Желание и свободное время
4. Компания единомышленников (Желательно)
5. Умение писать на каком-либо языке программирования (Python, Ruby)

Что даёт CTF?

1. Удовольствие от решенных тасков.
2. Практический опыт в ИБ

LINUX

Некоторые дистрибутивы

Хакерские:

1. Kali Linux
2. Black Arch

Обычные:

1. Ubuntu https://www.ubuntu.com/
2. Linux Mint
3. Arch

Вход в систему

```
        insmod ext2
        set root='hd0,msdos1'
        if [ x$feature_platform_search_hint = xy ]; then
          search --no-floppy --fs-uuid --set=root --hint-bios=hd0,msdos1\
 --hint-efi=hd0,msdos1 --hint-baremetal=ahci0,msdos1  ceed44b7-f29d-4dba\
-b8fc-2f155975b299
        else
          search --no-floppy --fs-uuid --set=root ceed44b7-f29d-4dba-b8f\
c-2f155975b299
        fi
        echo        'Loading Linux 4.9.0-4-amd64 ...'
        linux        /boot/vmlinuz-4.9.0-4-amd64 root=/dev/sda1 ro  quie\
t
        echo        'Loading initial ramdisk ...'
        initrd        /boot/initrd.img-4.9.0-4-amd64
```

rw init=/bin/bash

```
-b8fc-2f155975b299
        else
          search --no-floppy --fs-uuid --set=root ceed44b7-f29d-4dba-b8f\
c-2f155975b299
        fi
        echo        'Loading Linux 4.9.0-4-amd64 ...'
        linux        /boot/vmlinuz-4.9.0-4-amd64 root=/dev/sda1 rw init=\
/bin/bash
        echo        'Loading initial ramdisk ...'
        initrd        /boot/initrd.img-4.9.0-4-amd64
```

Некоторые команды и утилиты

Commands	Description
rm	Удаление файла
cp	Копирование файла
mv	Перемещение файла
pwd	Вывод текущей директории
uname	Вывод сведений о системе
whoami	Вывод текущего пользователя
cat	Вывод файла
nano, pico	Редакторы
ls	Вывод списка файлов в директории
file	Получение информации о файле
passwd	Смена пароля пользователя
chmod	Смена прав на файл
cd	Перемещение между директориями

Некоторые команды и утилиты

Commands	Description
top	Вывод списка процессов
kill	Завершение процесса
pidof	Получение айди процесса
mount/umount	Монтирование внешнего носителя
mkdir	Создание директории
grep	Поиск по регулярному выражению
find	Поиск файлов
ssh	Подключение по ssh
ifconfig	Вывод информации о сетевых интерфейсах
python	Запуск интерпретатора python’a
ping	Проверка целостности сетей
gcc	Компилятор C/C++
apt[-*]	Установка и обновление программных пакетов

Некоторые команды и утилиты

Commands	Description
sudo	Выполнение команды от суперпользователя root
wget	Скачивание файла по ссылке
strings	Вывод печатных строк файла
xxd	Хексовый дамп файла
gdb	Отладчик
curl	Выполнение запросов
nc	Подключение по сокету
./	Запуск исполняемого файла
clear	Очистка экрана
…	…
…	Многие, многие другие…

Все еще о командах

Если не знаете, что делает <команда> и какие флаги у неё есть:

1. man <команда>
2. <команда> -h или <команда> --help (работает не всегда)
3. google: “<команда> example”

Полезные мелочи

Hotkeys	
Стрелка вверх↑	Возвращение к предыдущей команде
Стрелка вниз↓	Возвращение к следующей команде
tab	Дописывание команды за вас ☺
home	Ставит курсор в начало строки
end	Ставит курсор в конец строки
shift+pgUp	Скролл вверх
shift+pgDown	Скролл вниз
shift+insert	Вставка в терминал (работает не всегда и не везде)
ctrl+l	Очистка экрана

Перенаправление ввода/вывода

“>” Перенаправление вывода в файл

“|” Перенаправление вывода другой команде/утилите

Примеры:

python –c “print –c ‘A’*100” > 123.txt – выполнит функцию print на питоне и запишет вывод в файл 123.txt

cat 123.txt | grep “123” –выводит содержимое 123.txt и ищет подстроку “123”

cat /etc/passwd | more – поэкранный вывод содержимого /etc/passwd

Ссылка на вики

Конец

По всем вопросам обращайтесь в telegram:

@f0reXwQw

@rarerarerare