

< Teach
Me
Skills />

Безопасность Linux, Mac

Вопросы по предыдущим темам или ДЗ

Mini-quizе по прошлым темам:

1. Как используется реестр при загрузке ОС?
2. Что такое служба Windows?
3. Какие 3 основных компонента Kerberos?
4. Как можно настроить общую политику безопасности на нескольких компьютерах Windows?
5. Почему нельзя запустить dll двойным кликом?
6. Зачем выносить драйвера и остальной код за пределы ядра?

Mini-quizе по новой теме:

1. Что такое UID?
2. Что значит rwx?
3. Для чего существует POSIX?
4. Для чего применяется IPTABLES?
5. Что такое sudo?
6. Как вы думаете, как можно отслеживать безопасность в ОС Linux?

План занятия

1. Изучим историю unix систем
2. Узнаем как был создан linux
3. Разберемся как работает ядро
4. Узнаем о POSIX
5. Посмотрим как происходит загрузка
6. Разберемся в chmod
7. Изучим Iptables
8. Изучим механизмы обеспечения безопасности OSX
9. Сравним ОС по качеству защищенности



PDP-7 - ЭВМ

Uniplexed Information and Computing Service (**UNICS**) □ **UNIX**

Multiplexed Information and Computer Services (**MULTICS**)

UNIX -

семейство переносимых, многозадачных и многопользовательских ОС, которые основаны на AT&T Unix



Первые версии Unix были написаны на ассемблере.

В **69** году Томпсон и Ритчи разработали язык Би.

В **72** году была выпущена вторая редакция Unix, переписанная на языке Би.

В **73** годы на основе Би был разработан компилируемый язык, получивший название С.

В **80** AT&T запретили реализовывать **UNIX**
AT&T – передали исходные коды **Berkley**

Развитие UNIX-BASED

[GNU](#) (*GNU's **N**GNU **o**t **U**NIX*) — свободная Unix-like операционная система, разрабатываемая Проектом GNU.



Особенности Unix-Like

Монолитное ядро – Unix, Linux
Командная строка в пространстве
запускаемого процесса

[Подробная информация](#)

Микроядро – OSX

Linux использует **монолитное ядро**, которое потребляет больше ресурсов, в то время как Windows использует **гибридное ядро**, которое занимает меньше места, но при этом снижает эффективность работы системы, в отличие от Linux.

В Microsoft Windows файлы хранятся в каталогах/папках на разных дисках. В Linux файлы и папки, начиная с корневого каталога, упорядочены в виде древовидной структуры, разветвляясь на различные подкаталоги.

[Inter Process Communication \(IPC\)](#)



Особенности Unix-Like#2

Модули ядра и загрузка подгружаемых модулей.

Философия Unix

1. красиво — небольшое
2. каждая программа делает что-то одно, но хорошо
3. храните данные в простых текстовых файлах
4. пишите программы, которые бы работали вместе
5. правило ясности: ясность лучше заумности

POSIX - переносимый интерфейс операционных систем

Стандарты, описывающие интерфейсы между операционной системой и программой API, библиотеку языка C и набор приложений и их интерфейсов. Создан для обеспечения совместимости UNIX-LIKE операционных систем

CAT

CHMOD

CP

CUT

GREP

HEAD

LS

MAKE

MKDIR

OD

PASTE

PR

RM

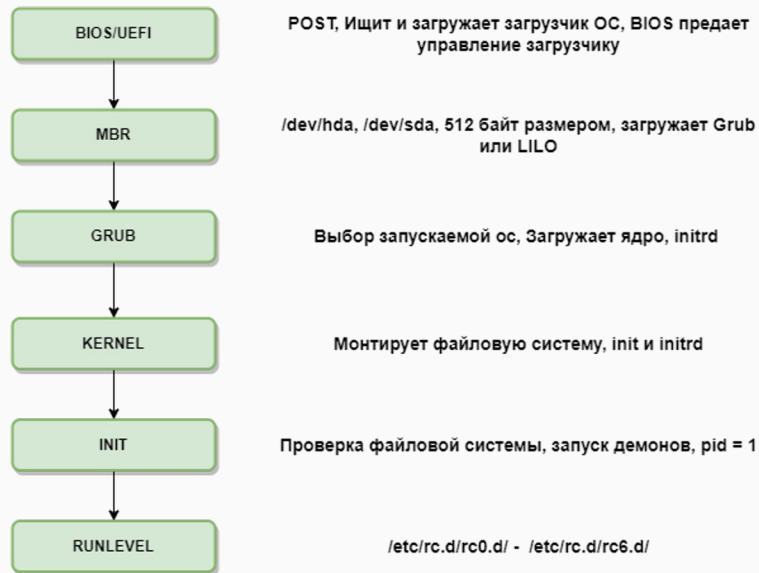
RMDIR

SORT

TAIL

TR

Загрузка UNIX-LIKE



level 0 - завершает работу системы

level 1 - однопользовательский режим работы. Чаще всего используется в целях обслуживания и выполнения других административных задач.

level 2 - многопользовательский режим работы без демонов.

level 3 - многопользовательский режим с поддержкой сети, но без графического интерфейса.

level 4 - не используется.

level 5 - запускается графический интерфейс.

level 6 - перезагружает систему.

[6 шагов загрузки ОС](#)

CHMOD

Rwx – символьное обозначение прав доступа

Модификаторы доступа

двоичная	символьная	права на файл	права на каталог
000	---	нет	нет
001	--x	выполнение	чтение свойств файлов
010	-w-	запись	нет
011	-wx	запись и выполнение	всё, кроме получения имени файлов
100	r--	чтение	чтение имён файлов
101	r-x	чтение и выполнение	доступ на чтение файлов/их свойств
110	rw-	чтение и запись	чтение имён файлов
111	rxw	все права	все права

- r (читать) заменяют на 4;
- w (запись) заменяют на 2;
- x (исполнение) заменяют на 1;
- 0 означает – ничего не делать (то, что в буквенной записи обозначается дефисом).
- 7 (rwx) = 4 + 2 + 1 (полные права);
- 5 (r-x) = 4 + 0 + 1 (чтение и выполнение);
- 6 (rw-) = 4 + 2 + 0 (чтение и запись);
- 4 (r--) = 4 + 0 + 0 (только чтение);
- и т.д.

Chmod 777 (u, g, o)

u - владелец файла

o - все остальные пользователи

g - группа файла

```
zaira@Zaira:~/freeCodeCamp$ ls -l
total 3856
-rw-r--r-- 1 zaira zaira 89 Apr 5 20:46 CODE_OF_CONDUCT.md
-rw-r--r-- 1 zaira zaira 210 Apr 5 20:46 CONTRIBUTING.md
-rw-r--r-- 1 zaira zaira 1513 Apr 5 20:46 LICENSE.md
-rw-r--r-- 1 zaira zaira 19933 Apr 5 20:46 README.md
drwxr-xr-x 4 zaira zaira 4096 Apr 6 22:45 api-server
-rw-r--r-- 1 zaira zaira 67 Apr 5 20:46 babel.config.js
drwxr-xr-x 10 zaira zaira 4096 Apr 6 22:55 client
drwxr-xr-x 5 zaira zaira 4096 Apr 6 22:54 config
```

MODE

OWNER

GROUP

SIZE

MODIFICATION

DATE

FILE/FOLDER NAME

CHOWN

chown — UNIX-утилита, изменяющая владельца и/или группу для указанных файлов.

groupadd **опции** **имя_группы**

groupadd **group1**

chown **пользователь** **опции** **/путь/к/файлу**
-R

chown **root** **./books**

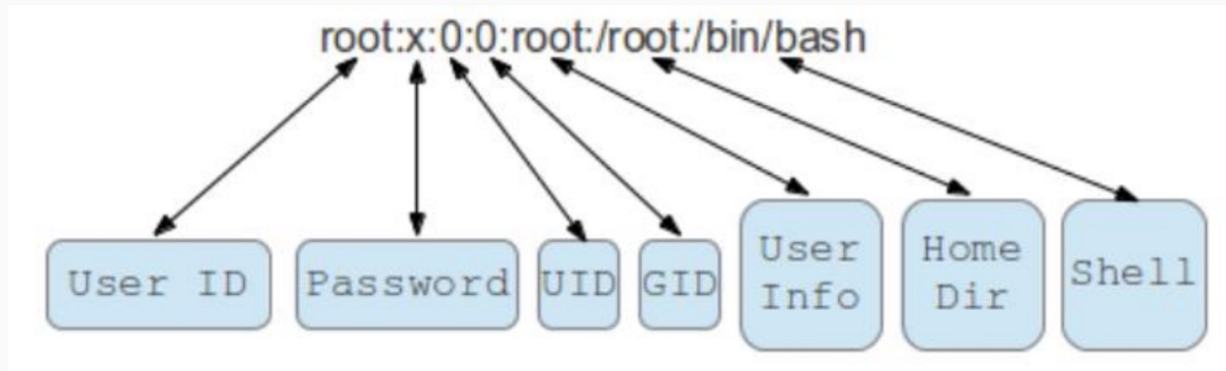
chown **root:root** **./books**

chown **root:root** **-R** **./books**

Пароли | Пользователи

Есть root ... и все остальные:

- root – id 0, может все!
- У обычных пользователей UID начинается с 500 или 1000, они не могут нанести серьезный вред



SUID bit – позволяет выполнение программы с правами хозяина файла.

Это – ключевой механизм повышения прав в Unix-системах.

Особенности SUID-программ в стандартных конфигурациях Linux:

- Работают с полномочиями пользователя root
- Используются для выполнения безопасных привилегированных операций.
- Используются для штатной смены идентификаторов пользователя: su, sudo, pkexec
- Программы учитывают идентификатор запустившего их пользователя и различные файлы конфигурации

SUID можно установить на копию /bin/sh для получения возможности выполнять команды с правами root без использования su/sudo.

При запуске шелла нужно использовать опцию -p, иначе effective uid будет сброшен.

```
# cp /bin/sh /bin/suid_sh  
# chmod u+s /bin/suid_sh  
$ /bin/suid_sh -p
```

Пароли | Пользователи

/etc/sudoers – файл с настройками sudo Редактирование в visudo

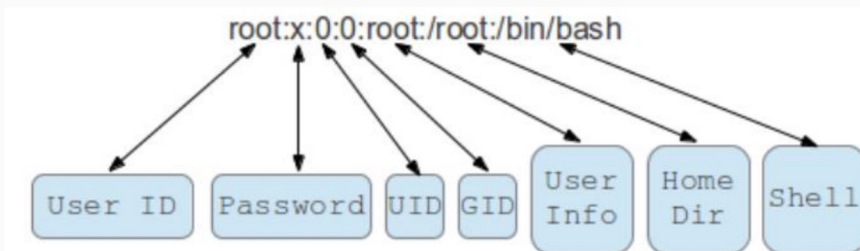
- `root ALL=(ALL:ALL) ALL` Первое поле показывает имя пользователя, которое правило будет применять к (`root`).
- `root ALL=(ALL:ALL) ALL` Первое "ALL" означает, что данное правило применяется ко всем хостам.
- `root ALL=(ALL:ALL) ALL` Данное "ALL" означает, что пользователь `root` может запускать команды от лица всех пользователей.
- `root ALL=(ALL:ALL) ALL` Данное "ALL" означает, что пользователь `root` может запускать команды от лица всех групп.
- `root ALL=(ALL:ALL) ALL` Последнее "ALL" означает, что данные правила применяются всем командам.

```
# This file MUST be edited with the 'visudo' command as root.
#
# Please consider adding local content in /etc/sudoers.d/ instead of
# directly modifying this file.
#
# See the man page for details on how to write a sudoers file.
#
Defaults        env_reset
Defaults        mail_badpass
Defaults        secure_path="/usr/local/sbin:/usr/local/bin:/usr/sbin:/usr/bin:/sbin:/bin:/snap/bin"
#
# Host alias specification
#
# User alias specification
#
# Cmnd alias specification
#
# User privilege specification
root    ALL=(ALL:ALL) ALL
#
# Members of the admin group may gain root privileges
%admin   ALL=(ALL) ALL
#
# Allow members of group sudo to execute any command
%sudo   ALL=(ALL:ALL) ALL
#
# See sudoers(5) for more information on "#include" directives:
#includedir /etc/sudoers.d
```

Список учетных записей пользователей хранятся в:

/etc/passwd

Формат:



Пароли | Пользователи

/etc/shadow – хэши паролей пользователей

```
smithj:Ep6mckrOLChF.:10063:0:99999:7:::
```

Как и в файле passwd, каждое поле в файле shadow отделяется двоеточием:

1. Username, до 8 символов. Совпадает с username в файле /etc/passwd.
2. Пароль, 13 символов (зашифрованный). Пустая запись (то есть, ::) показывает, что для входа пароль не нужен (обычно идея плохая), и запись ``*'' (то есть, :*) показывает, что вход заблокирован.
3. Количество дней (с 1 января 1970), когда пароль был сменен в последний раз.
4. Число дней до смены пароля (0 показывает, что он может быть сменен всегда).
5. Число дней, после которых пароль *должен* быть сменен (99999 показывает, что пользователь может не менять пароль фактически никогда).
6. Число дней, в течение которых пользователь получает предупреждения о необходимости пароль сменить (7 для полной недели).
7. Число дней после окончания действия пароля, когда еще можно работать. Если пароль не сменить, после данного срока он выдохнется, и аккаунт будет заблокирован.
8. Число дней, начиная с 1 января 1970, после которых пароль будет заблокирован.
9. Резервировано для возможного будущего использования.

Cron

Cron – это классический Unix-daemon, использующийся для периодического выполнения заданий в определенное время.

Особенности:

- Задания хранятся в специальных файлах в определенном формате.
- Поддерживается возможность запуска заданий от имени разных пользователей
- Системные задания кладутся в /etc/crontab
- Задания пользователей – в /var/spool/cron/crontabs

* * * * * <username> command(s)

- crontab -l - настройки для текущего пользователя
- crontab -e - редактирование

Crontab Structure	
* * * * * Command	
=Minute	(0 – 59)
=Hour	(0 – 23)
=Day of Month	(1 – 31)
=Month	(1 – 12 or Jan - Dec)
=Day of Week	(0 – 6 or Sun - Sat)

Cron

В чем ошибка?!

```
root@kali: /home/kali
File Actions Edit View Help
ls -alh /etc
total 1.4M
drwxr-xr-x 164 root root 12K Jun 19 18:22 .
drwxr-xr-x 19 root root 36K Jun 19 16:17 ..
-rw-r--r-- 1 root root 3.2K May 12 11:10 adduser.conf
-rw-r--r-- 1 root root 3.1K May 12 11:10 adduser.conf.dpkg-save
-rw-r--r-- 1 root root 44 May 12 11:52 adjtime
drwxr-xr-x 3 root root 4.0K May 12 11:12 alsa
drwxr-xr-x 2 root root 20K May 12 11:29 alternatives
drwxr-xr-x 8 root root 4.0K May 12 11:26 apache2
drwxr-xr-x 2 root root 4.0K May 12 11:10 apparmor
drwxr-xr-x 9 root root 4.0K May 12 11:27 apparmor.d
drwxr-xr-x 8 root root 4.0K May 12 11:52 apt
drwxr-xr-x 3 root root 4.0K May 12 11:22 avahi
-rwxrwxrwx 1 root root 32 Jun 15 17:10 backup.sh
-rw-r--r-- 1 root root 2.0K May 1 15:36 bash.bashrc
-rw-r--r-- 1 root root 45 Jan 24 2020 bash_completion
drwxr-xr-x 2 root root 4.0K May 12 11:24 bash_completion.d
-rw-r--r-- 1 root root 367 Jul 29 2019 bindresvport.blacklist
drwxr-xr-x 2 root root 4.0K Mar 15 07:03 binfmt.d
drwxr-xr-x 2 root root 4.0K May 12 11:21 bluetooth
drwxr-xr-x 3 root root 4.0K May 12 11:12 ca-certificates
-rw-r--r-- 1 root root 5.4K May 12 11:19 ca-certificates.conf
drwxr-s 2 root dip 4.0K May 12 11:19 chatscripts
drwxr-xr-x 2 root root 4.0K May 12 11:23 cifs-utils
drwxr-xr-x 3 root root 4.0K May 12 11:14 cloud
drwx 3 root root 4.0K Jun 14 16:27 cni

kali@kali: ~
File Actions Edit View Help
crontab: installing new crontab
# crontab -l
# Edit this file to introduce tasks to be run by cron.
#
# Each task to run has to be defined through a single line
# indicating with different fields when the task will be run
# and what command to run for the task
#
# To define the time you can provide concrete values for
# minute (m), hour (h), day of month (dom), month (mon),
# and day of week (dow) or use '*' in these fields (for 'any').
#
# Notice that tasks will be started based on the cron's system
# daemon's notion of time and timezones.
#
# Output of the crontab jobs (including errors) is sent through
# email to the user the crontab file belongs to (unless redirected).
#
# For example, you can run a backup of all your user accounts
# at 5 a.m every week with:
# 0 5 * * 1 tar -zcf /var/backups/home.tgz /home/
#
# For more information see the manual pages of crontab(5) and cron(8)
#
# m h dom mon dow command
* * * * * /etc/backup.sh
```

SELinux — это система принудительного контроля доступа, реализованная на уровне ядра.

1. Метки безопасности:

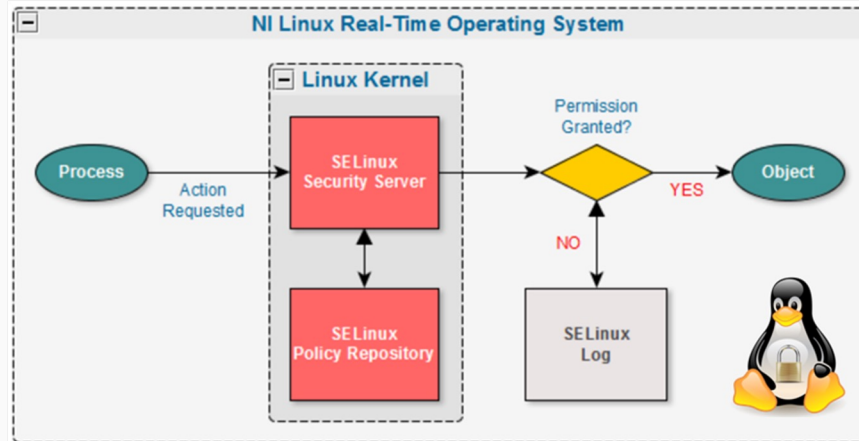
Каждый процесс, файл и объект в системе помечается меткой безопасности.

2. Политики безопасности:

SELinux использует набор политик безопасности, которые указывают, какие действия разрешены или запрещены

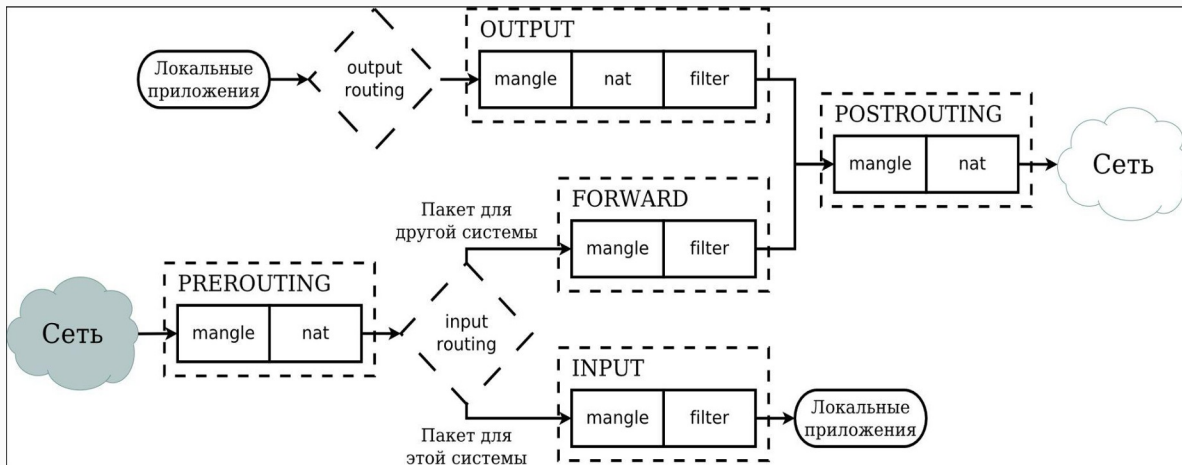
3. Принудительный контроль доступа:

SELinux принимает решения о доступе к ресурсам на основе политик безопасности и меток безопасности.



IpTables

IpTables - iptables — утилита командной строки, для управления работой межсетевого экрана **netfilter**



1.INPUT - эта цепочка применяется к пакетам, которые предназначены для самой системы.

2.FORWARD - эта цепочка применяется к пакетам, которые проходят через систему.

3.OUTPUT - эта цепочка применяется к пакетам, которые исходят из системы.

ACCEPT - разрешить прохождение пакета дальше по цепочке правил.

DROP - удалить пакет.

REJECT - отклонить пакет, и сообщить отправителю, что пакет был отклонен.

LOG - сделать запись о пакете в лог файл.

QUEUE - отправить пакет пользовательскому приложению.

IpTables#2

Блокировка IP-адреса

Чтобы заблокировать весь трафик от определенного IP-адреса, вы можете использовать следующую команду:

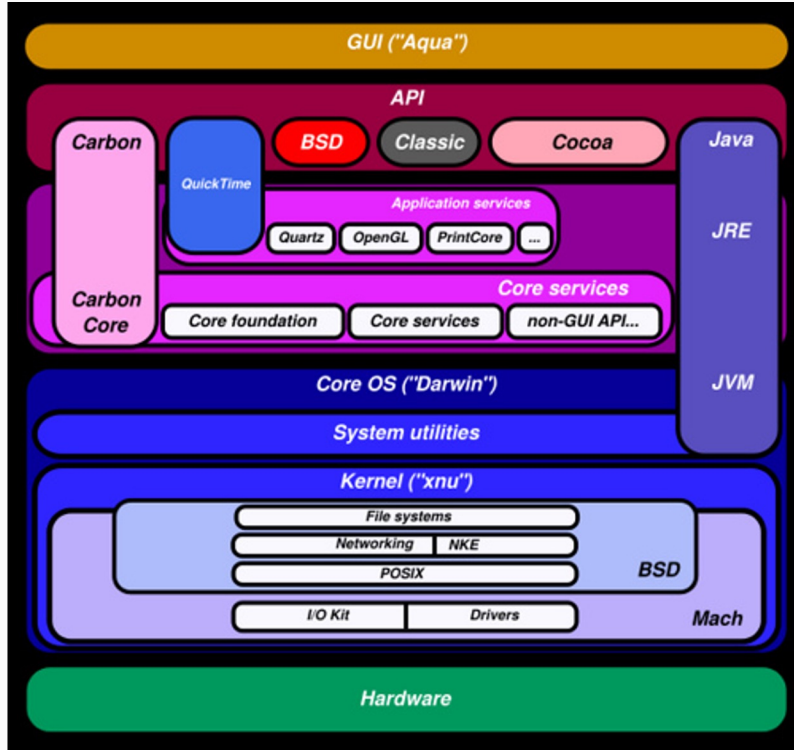
```
iptables -A INPUT -s 192.168.0.100 -j DROP
```

[Примеры правил](#)

- A** - добавить правило в цепочку;
- C** - проверить все правила;
- D** - удалить правило;
- I** - вставить правило с нужным номером;
- L** - вывести все правила в текущей цепочке;
- S** - вывести все правила;
- F** - очистить все правила;
- N** - создать цепочку;
- X** - удалить цепочку;
- P** - установить действие по умолчанию.

- p** - указать протокол, один из tcp, udp, udplite, icmp, icmpv6, esp, ah, sctp, mh;
- s** - указать ip адрес устройства-отправителя пакета;
- d** - указать ip адрес получателя;
- i** - входной сетевой интерфейс;
- o** - исходящий сетевой интерфейс;
- j** - выбрать действие, если правило подошло.

Ядро OSX



Ядра - XNU, MACH

Основные нюансы OsX

1. Гибридность
2. Драйвера и службы
3. Безопасность
4. Управление памятью
5. Системные вызовы
6. Многозадачность и планирование задач

Безопасность OSX



File Quarantine – запрашивает подтверждение на запуск не подписанного файла.

GateKeeper – Отправляет в карантин не подписанные файлы.

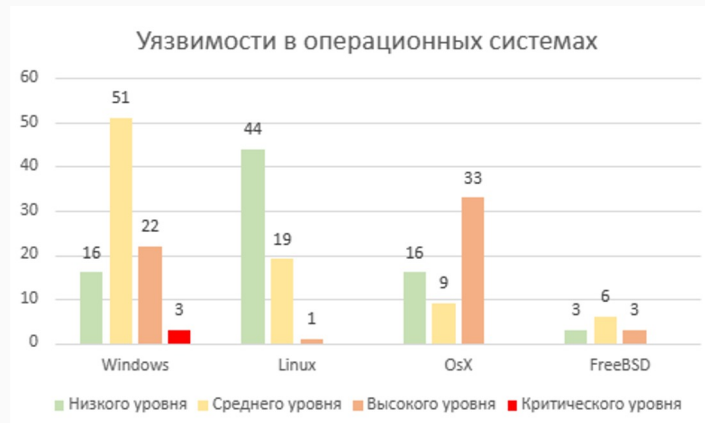
Xprotect – статический поиск IOC

TCC – БД с информацией о разрешениях доступа

MRT – Статический поиск определенных файлов и директорий

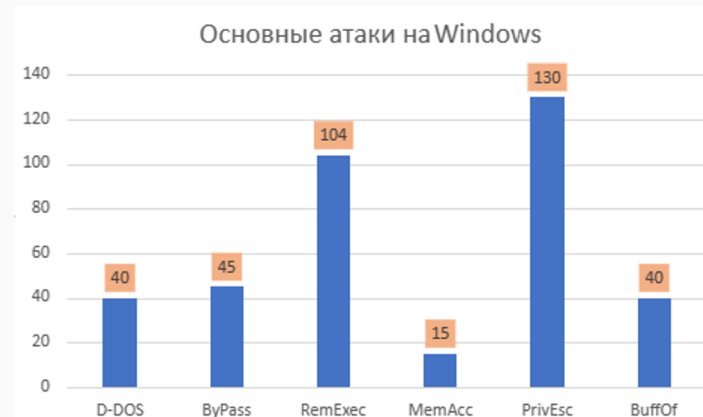
XPR – Проводит сканирование системы на наличие ВПО, и при необходимости «лечит» машину.

Сравнение OSX, Linux, Windows



Основные атаки на OSX:

1. Trojan
2. AdWare



Основные атаки на Linux:

1. Ransomware
2. Miners
3. Exploits
4. Trojan

Инструкция по настройке ОС Linux



Настройка устройства. BIOS и TPM.

1. Уникальный пароль на BIOS

1. Зайти в BIOS устройства в зависимости от производителя (кнопка F2/Del/ESC при запуске).
2. В большинстве случаев пароль на BIOS задается на вкладке Security.
3. На каждом устройстве задать уникальный пароль и записать в хранилище.

Пароль должен быть не менее 10 символов и содержать спец.символы и цифры.

2. Выставить режим загрузки UEFI

1. Зайти в BIOS → вкладка Boot → пункт Boot Mode → выставить значение «UEFI».

3. Установлена опция «Secure Boot» и отключены все лишние варианты загрузки

1. Зайти в BIOS → вкладка Security → пункт Secure Boot → выставить значение Enabled.

На моделях Asus ExpertBook при настройке SecureBoot в разделе Key Management нажать Reset To Setup Mode. При этом ключи ниже должны удалиться.

На вкладке Boot - выставить для всех пунктов загрузки устройства на «Disable». кроме загрузки с жесткого диска (если такой пункт есть).

Отключать USB Boot надо после установки ОС, если используется загрузочная флэшка.

4. Обязательная активация чипа TPM (при наличии)

1. Для проверки работы чипа зайти в ОС - запустить Выполнить - набрать «tpm.msc». Убедиться, что чип используется и проверить версию спецификации (желательная версия 2.0 и новее).
2. Если чип выключен необходимо включить его через BIOS. Расположение может отличаться от версий BIOS, производителя устройства и чипсета. Чаще всего расположен в разделах «Security» или «Advanced».

Установка новой ОС с форматированием дисков и настройкой шифрования

Ubuntu

1. Загрузите систему для установки, когда откроется окно тип установки:
2. Выбираете → Дополнительные возможности → Использовать LVM при новой установке → отметить Зашифровать новую установку
3. Введите пароль (ключ безопасности) для шифрования диска, рекомендуется локальная резервная копия у ИТ в спец.программе)

Данный пароль так же придется вводить пользователю при включении и перезагрузке устройства. Поэтому рекомендации тут иные чем для других паролей: 10 символов и использование только букв (любого регистра) и цифр.

4. После этого продолжаете установку системы
5. Уникальный пользователь и пароль на УЗ администратора
 1. (root - запрещён, указываем admin-minsk или admin-spb (в зависимости от офиса), рекомендуется локальная резервная копия у ИТ).
 2. Имя устройства формата **it<minsk,spb><инвентарный номер>** (пример: itminsk103306)

Настройка выполнения парольной политики

Ubuntu

Инструкция по настройке указана ниже

[Настройка парольной политики](#)

1. Установите модуль Cracklib PAM

```
sudo apt-get install libpam-cracklib
```

1. Откройте файл конфигурации

```
sudo vim /etc/pam.d/common-password
```

и внесите изменения

Запрещение использования старых паролей

Найдите следующую конфигурацию и добавьте **remember=5** Указывая на то, что 5 паролей, которые запрещены, и пароль, используемый для использования, будет сохранен `/etc/security/opasswd`

```
# As of pam 1.0.1-6, this file is managed by pam-auth-update by default.
# To take advantage of this, it is recommended that you configure any
# local modules either before or after the default block, and use
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password    requisite                       pam_cracklib.so retry=3 minlen=8 difok=3
password    [success=1 default=ignore]     pam_unix.so obscure use_authtok try_first_pass sha512 remember=5
# here's the fallback if no module succeeds
password    requisite                       pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
password    required                       pam_permit.so
```

Установите максимальную длину пароля

Найдите следующую конфигурацию и по умолчанию minlen=8 Изменить minlen=10 Указывает на то, что кратчайшая длина пароля должна быть 10

```
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password    requisite          pam_cracklib.so retry=3 minlen=10 difok=3
password    [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512 remember=5
# here's the fallback if no module succeeds
password    requisite          pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
```

Установите сложность пароля

Найдите следующую конфигурацию, добавьте его ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1 Он указывает на то, что пароль должен содержать, по меньшей мере, одну заглавную букву (UCredit), строчную букву (lcredit), dcredit и пунктуацию (ocredit), который может быть изменен в соответствии с потребностями

```
# pam-auth-update to manage selection of other modules. See
# pam-auth-update(8) for details.

# here are the per-package modules (the "Primary" block)
password    requisite          pam_cracklib.so retry=3 minlen=10 difok=3 ucredit=-1 lcredit=-1 dcredit=-1 ocredit=-1
password    [success=1 default=ignore] pam_unix.so obscure use_authtok try_first_pass sha512 remember=5
# here's the fallback if no module succeeds
password    requisite          pam_deny.so
# prime the stack with a positive return value if there isn't one already;
# this avoids us returning an error just because nothing sets a success code
# since the modules above will each just jump around
```


Откройте файл конфигурации и установите дату истечения срока действий пароля

```
sudo vi /etc/login.defs
```

```
PASS_MAX_DAYS 90
```

```
PASS_MIN_DAYS 0
```

```
PASS_WARN_AGE 5
```

```
# PASS_MIN_DAYS Minimum number of da
# PASS_WARN_AGE Number of days warn
#
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_WARN_AGE 7

#
# Min/max values for automatic uid selection
```

Установка антивируса

1. Дистрибутив и инструкцию вы должны составить для своих сотрудников



Настройка SSH-сервера

1. Установка SSH

```
sudo apt-get install ssh
```

2. Запуск сервиса

```
sudo systemctl start ssh
```

3. Добавление сервиса в автозагрузку

```
sudo systemctl enable ssh
```

4. Проверить статус работы сервиса

```
sudo systemctl status sshd
```

5. Создание резервной копии конфига

```
sudo cp /etc/ssh/sshd_config  
/etc/ssh/sshd_config.factory-  
defaults
```

6. Копирование открытых ключей (ИТ и ИБ) с ПК администраторов на ПК пользователя (ключи предварительно необходимо скачать с данной страницы - [SSH-ключи \(ИБ и ИТ\)](#))

```
ssh-copy-id -i <path-to-key> <admin account>@<new-pc-ip>  
пример: ssh-copy-id -i path/to/name.pub admin-  
msk@10.1.1.47
```

7. Команда для редактирования конфига

```
sudo nano /etc/ssh/sshd_config
```

8. Настроенный файл конфигурации - (отправлю в чат) можно скопировать напрямую на ПК пользователя или скопировать-вставить настройки в конфигурационный файл

9. Перезагрузить сервис для применение изменений

```
sudo systemctl restart ssh
```

Установка и настройка файервола

Ubuntu

1. Команда для установки

```
apt install ufw
```

2. Включить файервол

```
ufw enable
```

3. Задать правила для настройки файервола

```
ufw default allow incoming
```

```
ufw logging high
```

4. Перезагрузить файервол для применения изменений

```
ufw reload
```

5. Проверить работу файервола

```
ufw status verbose
```

Rules example:

```
sudo ufw deny from 203.0.113.0/24 # block subnet
```

```
sudo ufw deny in on eth0 from 203.0.113.100
```

```
sudo ufw allow from 192.168.100.0/24
```

```
sudo ufw delete allow from 192.168.100.1
```

```
sudo ufw status numbered
```

```
sudo ufw delete 1
```

```
sudo ufw app list
```

```
sudo ufw allow OpenSSH
```

```
sudo ufw allow from 203.0.113.0/24 proto tcp to any port 22
```

```
sudo ufw allow http
```

```
sudo ufw allow proto tcp from any to any port 80,443
```

Настройка безопасности операционной системы

Скачать данный скрипт (отправлю в чат)
на ПК пользователя, запустить от имени
администратора

```
./security_linux_ubuntu.sh
```

Спасибо за внимание!