Безопасность рабочих мест на Linux в 2024 году

OSDAY-2024
Михаил Новоселов
m.novosyolov@rosalinux.ru

do1.nixtux.ru/
download/osday2024

Кто видел вирусы под Linux?

- У админов ПК в среднем мало опыта с Linux
- Есть привычка, что нужен антивирус
- Не только лишь каждый видел живого трояна под Линукс
- Просто подбери пароль — типичный метод взлома
- Эксплоиты для уязвимостей с Github не всегда просто скачать, собрать и запустить

А как в мире Windows?

- Надежная песочница в браузерах
- Обычно пользователь сам запускает вирус («Как вырастить чайный гриб.pdf.exe»)
- Много ПНП: установка браузеров, торрентокачалок и т. д. вместе с другим ПО
- Серьезное вредоносное ПО эксплуатирует уязвимости (пример — Stuxnet)
- Нельзя простым способом защитить систему от запуска вирусов по принципу белого списка

Про Stuxnet

do1.nixtux.ru/download/osday2024

Что у нас, в Linux

- Надежная песочница в браузерах
- chmod +x «Как вырастить чайный гриб.pdf.exe» нужно сделать вручную
- ПО обычно не ставится не из репозитория (и пропагандировать это вредно!) — нет рекламных обвесов в комплекте
- Уязвимости в обработчиках desktop-файлов, PDF и т. д., как и в Windows
- Можно простым способом защитить систему от запуска вирусов по принципу белого списка
- Информация с доступом у пользователя часто ценнее, чем root-доступ к системе

Начальник — секретарю:
— Катенька, дорогая, перепиши месячную отчетность нашим партнерам, они сейчас к тебе подойдут.

— Добрый день, это вам переписать отчетность?
— Добрый день, да, будьте так любезны, вот чистая дискета, можно на нее.
— Да, конечно.

Вставляет в дисковод. И....

```
# mkfs -t vfat -c /dev/fd0h1440
# mount -t vfat -o iocharset=koi8-r,codepage=866 /dev/fd0 /mnt/floppy
# find / -noleaf -type f -name Otchet_april. [a-zA-Z] -exec cp '{ }';
/mnt/floppy \;
# ls -la /mnt/floppy/Otchet_april. [a-z][A-Z] && sync && sleep 3
```

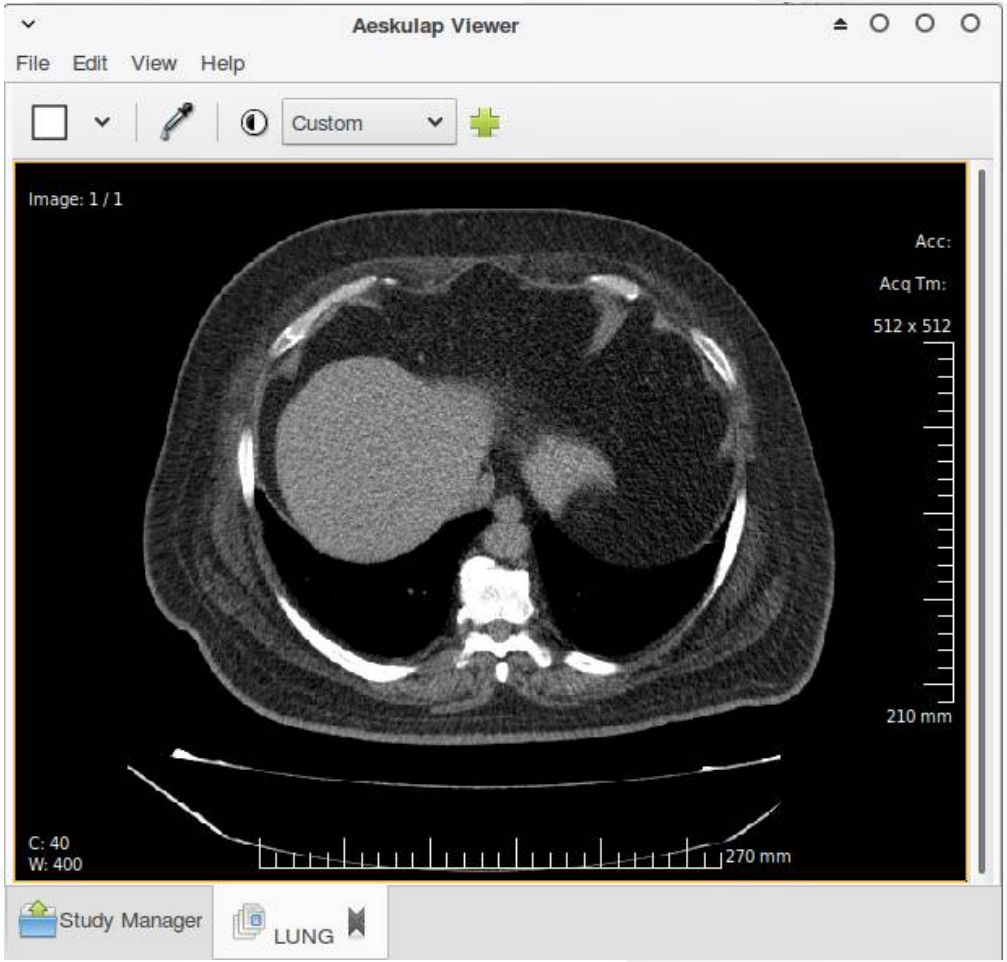
— Возьмите пожалуйста!
Партнёры:
— Нифига себе!!!
— Что такое?!... Я опять отмонтировать забыла?!

Разница Windows/Linux

- Windows: библиотеки у каждой программы с собой, надеяться на их обновление не приходится
- Windows: обновления ОС включают в себя новые шпионские модули и пр. хлам, ставятся долго, нудно и в неподходящий момент
- Linux: одна библиотека на всю систему (если ПО из репозитория)
- Linux: быстрые и безболезненные обновления (по крайней мере в Росе Хром/Fresh 🙃)
- На Linux проще нормально исправить уязвимость (технологический стек суверенен), чем затыкать её антивирусами, HIPS и пр.

Инструменты в Росе (Linux)

- Обновления библиотек и ядра ОС
- mount -o noexec
- IMA http://wiki.rosalab.ru/ru/index.php/IMA
- fapolicyd
- Landlock
- AltHa
- Отключаемость генераторов превью PDF, картинок и т. д.
- Набор пакетов с готовыми конфигами-харденингами sconfigs https://abf.io/import/sconfigs
- Большой набор свободных драйверов принтеров, ipp-usb
- Большой репозиторий



Набор пакетов с готовыми конфигами-харденингами **sconfigs**

sconfigs-basic-audit	Конфиг auditd с базовым набором правил
sconfigs-detailed-audit	Конфиг auditd с расширенным набором правил
sconfigs-disable-coredumps	Отключение сохранения «корок»
sconfigs-disable-filesystems-modules	Отключение ядерных модулей редких ФС
sconfigs-disable-network-modules	Отключение редко нужных сетевых модулей
sconfigs-disable-ipv6	Отключение IPv6
sconfigs-harden-kernel	Харденинги через sysctl
sconfigs-harden-network-settings	Харденинги через sysctl
sconfigs-login-warning	Страшная надпись при входе по SSH и в TTY
sconfigs-sshd	Харденинг openssh-server

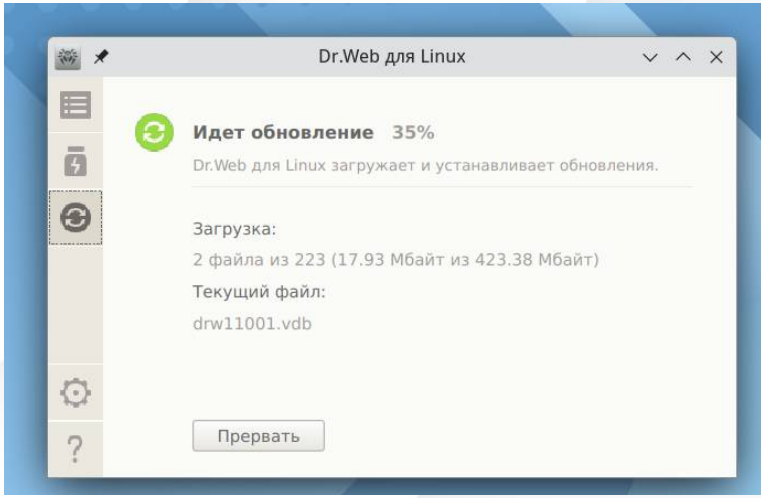
Эффекты от резидентного сигнатурного антивируса в Linux

POCA

```
user@rosa-qq8krq ~ $ grep -R . /proc/pressure
/proc/pressure/io:some avg10=29.31 avg60=9.99 avg300=5.00 total=80299593
/proc/pressure/io:full avg10=0.48 avg60=1.85 avg300=2.67 total=61062154
/proc/pressure/cpu:some avg10=64.28 avg60=21.22 avg300=7.59 total=53453855
/proc/pressure/cpu:full avg10=0.00 avg60=0.00 avg300=0.00 total=0
/proc/pressure/irq:full avg10=0.81 avg60=0.35 avg300=0.43 total=10346373
/proc/pressure/memory:some avg10=0.09 avg60=0.05 avg300=0.01 total=140286
/proc/pressure/memory:full avg10=0.09 avg60=0.05 avg300=0.01 total=107066
```

```
  0[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||96.8%] Tasks: 129, 263 thr, 1
  1[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||94.9%] Load average: 2.22 1.4
  2[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||96.8%] Uptime: 00:15:17
  3[||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||95.5%]
Mem[|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||1.60G/7.64G]
Swp[                                                                      0K/15.5G]

  Main   I/O
    PID USER       PRI  NI  VIRT   RES   SHR S  CPU%▽MEM%   TIME+  Command
  17009 root        20   0  253M 16128 12160 S  68.6  0.2  0:21.25 /opt/drweb.com/bin/drweb-filecheck.real
  19698 root        20   0  253M 16128 12160 R  60.3  0.2  0:19.19 /opt/drweb.com/bin/drweb-filecheck.real
  19956 root        20   0 4251M  494M  4480 S  30.8  6.3  0:03.56 /opt/drweb.com/bin/drweb-se.real
  19938 root        20   0 4251M  494M  4480 S  30.1  6.3  0:03.74 /opt/drweb.com/bin/drweb-se.real
  19939 root        20   0 4251M  494M  4480 R  30.1  6.3  0:03.67 /opt/drweb.com/bin/drweb-se.real
  19957 root        20   0 4251M  494M  4480 R  30.1  6.3  0:03.49 /opt/drweb.com/bin/drweb-se.real
  19936 root        20   0 4251M  494M  4480 S  29.5  6.3  0:03.40 /opt/drweb.com/bin/drweb-se.real
  19932 root        20   0 4251M  494M  4480 S  28.2  6.3  0:03.57 /opt/drweb.com/bin/drweb-se.real
  19934 root        20   0 4251M  494M  4480 S  28.2  6.3  0:03.80 /opt/drweb.com/bin/drweb-se.real
  19937 root        20   0 4251M  494M  4480 R  28.2  6.3  0:03.32 /opt/drweb.com/bin/drweb-se.real
  19940 root        20   0 4251M  494M  4480 S  28.2  6.3  0:03.47 /opt/drweb.com/bin/drweb-se.real
  19935 root        20   0 4251M  494M  4480 R  27.6  6.3  0:03.72 /opt/drweb.com/bin/drweb-se.real
  19941 root        20   0 4251M  494M  4480 R  27.6  6.3  0:03.39 /opt/drweb.com/bin/drweb-se.real
  19950 root        20   0 4251M  494M  4480 S  27.6  6.3  0:03.61 /opt/drweb.com/bin/drweb-se.real
  19933 root        20   0 4251M  494M  4480 R  26.9  6.3  0:03.49 /opt/drweb.com/bin/drweb-se.real
  19951 root        20   0 4251M  494M  4480 R  26.9  6.3  0:03.54 /opt/drweb.com/bin/drweb-se.real
  19953 root        20   0 4251M  494M  4480 R  26.3  6.3  0:03.68 /opt/drweb.com/bin/drweb-se.real
  19954 root        20   0 4251M  494M  4480 S  25.6  6.3  0:03.60 /opt/drweb.com/bin/drweb-se.real
  20295 user        20   0  713M 71880 60672 R  21.8  0.9  0:00.34 /usr/bin/spectacle
```



~90% (?) баз — вирусы для Windows

Польза и вред от антивируса в Linux в 2024 г.

- Создает новые дыры
- Греет воздух

- *Теоретически* может защитить, если обновится быстрее, чем ОС
- Или если есть анализ поведения программ

Безопасность рабочих мест на Linux в 2024 году

OSDAY-2024
Михаил Новоселов
m.novosyolov@rosalinux.ru

do1.nixtux.ru/
download/osday2024