

# **Задание 1. Анализ возможных атак на Linux-системы и разработка методов защиты**

Step 1: Выбрать пять атак на Linux-системы из открытых источников, в особенности из [матрицы Mitre](#).

Step 2: Описать, в чём суть каждой атаки и из-за чего она происходит.

Step 3: Описать, как выявить и предотвратить каждую из атак.

Атака № 1: Spearphishing (через различные сервисы).

Суть: Атакующий под видом обычного пользователя или представителя какой-нибудь компании может отправить фишинговое сообщение жертве, через популярные сервисы, которыми пользуются огромное количество обычных пользователей. Тут используется тактика социальной инженерии, атакующий изучает интересы жертвы, на каких группах она сидит, с кем разговаривает и т.д.

Атакующий пишет любое сообщение, которое может заинтересовать жертву нажать на ссылку с malware, например: «Вы выиграли 50000 рублей, кликни сюда и заберите Ваш выигрыш». Если жертва нажмёт на ссылку, то на его устройство установится malware – и атакующий получит доступ к данным жертвы. Типы malware в сообщениях зависят от выбора атакующего: Одна жертва может быть doxxed, а у другой зашифроваться система.

Выявление и предотвращение: Для предотвращения spearphishing атаки, нужно воспользоваться антивирусом, в случае с интранетом компании — заблокировать сайты и некоторые службы, которые потенциально могут быть использованы для spearphishing. Также можно проводить обучение пользователей об отличии тактик социальной инженерии и сообщений spearphishing с вирусными ссылками. Для обнаружения подобных сообщений, необходимо смотреть журнал приложения, через который была совершена атака или мониторить интернет активность.

Атака № 2: Задача по расписанию.

Суть: Атакующий может использовать функцию расписания для повторяющегося исполнения вредоносного кода. Задача также может быть расписана в удаленной системе, предоставив необходимые аутентификационные данные. Во время расписания задачи на удаленной системе возможно потребует члена группы админ или привилегированная группа на удаленной системе.

Выявление и предотвращение: Необходимо сделать так, чтобы админы групп могли делать какие-либо изменения в задачах по расписанию. Необходимо мониторить исполняемые команды, только что созданные контейнеры, только что созданные файлы и изменения сделанные с ними, только что созданные процессы и только что созданные расписанные работы.

### Атака № 3: Перебор пароля или атака брутальной силы.

Суть: Для выявления пароля, чтобы войти в учётную запись пользователя, атакующий может использовать атаку брутальной силы или перебора пароля. Если пароля учётной записи простой, то атакующий сможет его быстро отгадать или скрипту для атаки брутальной силы нужно будет пару секунд или минут.

Иногда для перебора пароля необходимо использовать словарные файлы или для получения пароля достаточно просто получить его хэш, затем его декодировать или достаточно просто посмотреть на файлы, которые были скомпрометированы и находятся в открытом доступе, хотя они являются конфиденциальной информацией. Иногда такая атака используется, когда неизвестен не пароль ни его хэши.

Выявление и предотвращение: Нужно устанавливать политики паролей. В такой политике устанавливается минимальное количество символов необходимых для использования, не только буквы, но и цифры/символы/знаки и т. д. Пароль не должен быть простым, поскольку при использовании простого пароля, это удобно и пользователю и атакующему — он спокойно проникнет в систему. Пример того, какой пароль может подойти, а какой нет:

Пример: Такой не подойдёт вообще — «admin123».

Вот такой может подойти — «YPI,o^vanzy&ueaP" `8H` {P(».

Также нельзя использовать один и тот же пароль всё время, у каждого пароля должен быть свой срок годности. Когда срок годности пароля приближается к концу, то пользователю придёт уведомление о том, что пора поменять пароль — если пароль не будет изменён, то учётная запись будет заблокирована. В случае если пользователь захочет набрать истёкший пароль, но при этом он его не поменял, появится уведомление о том, что срок годности пароля истёк и что необходимо немедленно поменять пароль. Но срок годности пароля может быть и продлён.

Использовать мультифакторную аутентификацию (MFA) — кроме пароля, атакующему или владельцу учётной записи необходимо набрать ещё и одновременный код, когда пароль был набран правильно (это больше относится к 2FA), но для дополнительной аутентификации могут быть использованы и другие данные, например отпечаток пальца, лицо или штрих-код у карточки, которая есть только у владельца.

Блокировать аккаунты при определённом количестве неправильно набранного пароля — это зависит от конфигурации системы. Если атакующий не сможет правильно подобрать пароль или отгадать его определённое количество раз, то учётная запись временно блокируется и никто не сможет войти в данную учётную запись. При попытке войти на временно заблокированную учётную запись, владелец это заметит и быстро поменяет пароль.

Те учётные записи, которые подверглись утечке или атаке брутальной силы — их необходимо сбрасывать. Поскольку фактически такие учётные записи являются задними дверьми, атакующий имеет удаленный доступ ко внутренней системе.

#### Атака № 4: Дамп ОС данных.

Суть: Атакующий может за дампить полномочия, для получения данных для регистрации в учётную запись, обычно в виде хэша или текстового файла — те данные могут содержать данные об используемой OS и его приложения или ПО. Полномочие могут быть также использованы для получения другой информации, которая является тайной. Может использоваться как атакующими, так и тестировщиками для проверки на безопасность.

Выявление и предотвращение: Ограничить дублирование полномочий, через различные системы и учётные записи, научить пользователей и админов не пользоваться одним и тем же паролем на нескольких учётных записях, поскольку если будет скомпрометирован один пароль, то будут скомпрометированы все учётные записи с этим паролем.

Сделать так, чтобы учётные записи администратора сети имели уникальные пароли, среди всех систем сети.

Убедиться в том, чтобы backup был хорошо защищён — необходимо шифровать всю чувствительную информацию.

Вытаскивание паролей из памяти требуют привилегии корня. Поэтому лучше запрещать доступ к привилегированным учётным записям, для того чтобы предотвратить программы к доступу к такой чувствительной части памяти.

Для получения паролей и хешей хранящихся в памяти, процессы должны открывать maps файлы в /proc файловой системе, для анализа процесса. Данный файл хранится в директории /proc/<pid>/maps, когда <pid> директория является необыкновенным id процесса, которая была допрошена для такой аутентификации данных. Инструмент мониторинга AuditD, которые предустановлен во многих дистрибутивах, может использоваться для просмотра вражеских процессов, открывающие этот файл в файловой системе proc, поднимающий тревогу на id процесса, имя процесса и аргументы таких программ.

#### Атака № 5: Противник-по-середине (DHCP Spoofing) - ближе к Man-in-the-middle.

Суть: Атакующий может перенаправлять сетевой трафик на системы, принадлежащие атакующему, тем самым подменяя трафик протокола DHCP и действуя как вредоносный DHCP сервер на сети жертвы. При достижении позиции противник-по-середине, атакующий может собирать коммуникации сети, включая пройденные полномочия, особенно если они были отправлены через небезопасные, не зашифрованные протоколы. Это также может приводить к «Нюханию трафика» или «Манипуляции переданных данных».

Атакующий также может подменить в качестве мошеннического DHCP сервера на сети жертвы, через который легитимные хосты могут получать вредоносные конфигурации сети. Например, malware может действовать как DHCP сервер и предоставлять DNS сервера, принадлежащие атакующему на заражённые компьютеры. Через вредоносные конфигурации сети, атакующий может достичь позиции противник-по-середине, перенаправлять трафик клиента, через системы принадлежащие атакующему и собирать информацию с сети клиента.

## **Задание 2. Сбор информации о системе**

Step 1: Найти пароли и SSH-ключи в системе и сделать экранные выстрелы вывода команд.

Это небольшая часть из общего выведенного текста от данной команды.

```
kali@kali: ~/.ssh
File Actions Edit View Help
[(kali㉿kali)-[~/ssh]] $ chmod 700 ~/ssh
[(kali㉿kali)-[~/ssh]] $ touch ~/ssh/authorized_keys
[(kali㉿kali)-[~/ssh]] $ chmod 600 ~/ssh/authorized_keys
[(kali㉿kali)-[~/ssh]] $ cat ~/ssh/id_rsa.pub >> ~/ssh/authorized_keys
cat: /home/kali/.ssh/id_rsa.pub: No such file or directory
[(kali㉿kali)-[~/ssh]] $ touch ~/ssh/id_rsa.pub
[(kali㉿kali)-[~/ssh]] $ chmod 600 ~/ssh/id_rsa.pub
[(kali㉿kali)-[~/ssh]] $ cat ~/ssh/id_rsa.pub >> ~/ssh/authorized_keys
[(kali㉿kali)-[~/ssh]] $ find / -name "authorized_keys" 2> /dev/null
/home/kali/.ssh/authorized_keys
[(kali㉿kali)-[~/ssh]] $ sudo find / -name authorized_keys 2> /dev/null
/home/kali/.ssh/authorized_keys
[(kali㉿kali)-[~/ssh]] $
```

Здесь набрав данную команду, спам с сообщениями об отказе доступа — с sudo произошло что-то подобное (при альтернативной команде, ничего не показывало).

Step 2: Воспользоваться утилитой LinPEAS и найти уязвимые места в системе + описать три найденные уязвимости. В описании указать, что это за уязвимость, почему это опасно, как защититься.

The terminal window shows the following steps:

- curl -L https://github.com/carlosoplop/PEASS-ng/releases/latest/download/linpeas.sh
- linpeas-ng by carlosoplop
- Do you like PEASS?
- Get the latest version : <https://github.com/sponsors/carlosoplop>
- Follow on Twitter : [@book\\_hacktricks](#)
- Respect on HTB : [SirBroccoli](#)
- Thank you!
- Quick Start
- Find the latest versions of all the scripts and binaries in the releases page.
- ADVISORY: This script should be used for authorized penetration testing and/or educational purposes only. Any misuse of this software will not be the responsibility of the author or of any other collaborator. Use it at your own compute rs and/or with the computer owner's permission.
- Linux Privesc Checklist: <https://book.hacktricks.xyz/linux-hardening/linux-privilege-escalation-checklist>
- LEGEND:
  - Red: It's a PE vector
  - Yellow: You should take a look to it
  - LightCyan: Users with console

Скрипт запущен.

The terminal window shows the following steps:

- File Actions Edit View Help
- System Information
- Operative system
- Linux version 6.5.3-1kali2 (Debian 15.2.0-4) 13.2.0, GNU ld (GNU Binutils for Debian) 2.41 #1 SMP PREEMPT\_DYNAMIC Debian 6.5.3-1kali2 (2023-10-03)
- Distributor ID: Kali
- Description: Kali GNU/Linux Rolling
- Release: 2023.3
- Codename: kali-rolling
- Sudo version
- sudo version 1.9.14p2
- PATH
- /usr/local/bin:/usr/local/sbin:/usr/bin:/sbin:/usr/local/games:/usr/games
- Date & uptime
- Tue Oct 31 12:25:26 AM EDT 2023
- 00:23:26 up 12 min, 1 user, load average: 1.00, 1.05, 0.70
- Any sdv/disk\* disk in /dev? (limit 20)
- disk
- sda
- sda1
- sda2
- sda3
- sda5
- Unmounted file-system?
- Check if you can mount unmounted devices
- UUID=17d9e43-32a4-bbb4-8000-6e79c959efc5 / ext4 errors=remount-ro 0 1
- UUID=76b4380d-04c2-49ef-b5c3-50827c748b35a none swap sw 0 0
- /dev/sr0 /media/cdrom0 udf iso9660 user,noauto 0 0
- MacPEAS
- Environment
- Any private information inside environment variables?
- LESS\_TERMCAP\_M0=
- HISTFILESIZE=0
- POWERSHELL\_TELEMETRY\_OPTOUT=1
- LANGUAGE=en\_US.UTF-8
- TERM=xterm
- LESS\_TERMCAP\_ue=
- XDG\_SEAT=seat0
- DOTNET\_CLI\_TELEMETRY\_OPTOUT=1
- SESSION\_PID=1183
- XDG\_SESSION\_TYPE=x11
- SHLVL=1
- HOME=/home/kali
- USER=kali
- DESKTOP\_SESSION=lightdm-xsession
- GTK\_MODULES=glib:atk:bridge
- XDG\_SEAT\_PATH=/org/freedesktop/DisplayManager/Seat0

Вот некоторое содержимое из данного скрипта. Абсолютное большинство текста, которое может потребовать внимания — выделено красным. Под красным обозначено — Вы должны на это посмотреть.

```

File Actions Edit View Help
[+] [CVE-2022-2586] Searching Signature verification failed in dmesg
dmesg NOT Found
Details: https://book.hacktricks.xyz/linux-hardening/privilege-escalation#dmesg-signature-verification-failed
dmesg NOT Found

[+] [CVE-2022-2586] Executing Linux Exploit Suggester
https://github.com/zet-/linux-exploit-suggester 0mPEAS
[+] [CVE-2022-2586] rft_object UAF
Details: https://www.openwall.com/lists/oss-security/2022/08/29/5
Exposure: less probable
Tags: ubuntu-(20.04) [kernel:5.12.13]
Download URL: https://www.openwall.com/lists/oss-security/2022/08/29/5
Comments: kernel.unprivileged_usersns_clone=1 required (to obtain CAP_NET_ADMIN)

[+] [CVE-2021-4034] pwnkit
Details: https://www.qualys.com/2022/01/25/cve-2021-4034/pwnkit.txt
Exposure: less probable
Tags: ubuntu-10|11|12|13|14|15|16|17|18|19|20|21,debian=7|8|9|10|11,fedora,majaro
Download URL: https://codelead.github.com/berdav/CVE-2021-4034/zip/main

[+] [CVE-2021-3156] sudo Baron Samedi
Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: less probable
Tags: mint-19_ubuntu-18|20, debian=9
Download URL: https://codelead.github.com/blasty/CVE-2021-3156/zip/main

[+] [CVE-2021-22555] Netfilter heap out-of-bounds write
Details: https://www.qualys.com/2021/01/26/cve-2021-3156/baron-samedit-heap-based-overflow-sudo.txt
Exposure: less probable
Tags: centos-6|7|8,ubuntu-14|16|17|18|19|20, debian=9|10
Download URL: https://codelead.github.com/wrawit/CVE-2021-3156/zip/main

MacPEAS
[+] [CVE-2021-22555] Netfilter heap out-of-bounds write
Details: https://google.github.io/security-research/pocs/linux/cve-2021-22555/writeup.html
Exposure: less probable
Tags: ubuntu-20.04 [kernel:5.8.0-+]
Download URL: https://raw.githubusercontent.com/google/security-research/master/pocs/linux/cve-2021-22555/exploit.c
ext-url: https://raw.githubusercontent.com/tolses/kernel-exploits/master/CVE-2021-22555/exploit.c
Comments: in_tables kernel module must be loaded

```

```

File Actions Edit View Help
inet 127.0.0.1 netmask 255.0.0.0
inet br0 netmask 255.255.255.0 brd 192.168.1.1
inet br0:1 netmask 255.255.255.0 brd 192.168.1.1
loop txqueuelen 1000 queueing discipline pfifo_fast
RX packets 131 bytes 9095 (8.8 Kib)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 131 bytes 9095 (8.8 Kib)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

[+] Active Ports
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#open-ports
tcp 0 0 127.0.0.1:1883 0.0.0.0:*
LISTEN -
tcp 0 0 127.0.0.1:5432 0.0.0.0:*
LISTEN -
tcp6 0 0 ::1:5432 ::* LISTEN -
tcp6 0 0 ::1:1883 ::* LISTEN -

[+] Can I sniff with tcpdump?
tcpdump -i br0 -w /tmp/capture.pcap

[+] My user
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#users
uid=1000(kali) gid=1000(kali) groups=1000(kali),4(sudo),20(dialout),24(cdrom),25(floppy),27(sudo),29(audio),30(dip),44(video),46(plugdev),100(users),106(netdev),117(wireshark),120(bluetooth),138(scanner),141(vboxsf),142(kaboxer)

[+] Do I have PGP keys?
/usr/bin/gpg
netpgp Not Found
netpgp Not Found

[+] Checking 'sudo -l', '/etc/sudoers', and '/etc/sudoers.d'
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#sudo-and-suid
PEAS
Matching Defaults entries for kali on kali:
env_reset, mail_badpass, secure_path:/usr/local/bin:/usr/sbin:/usr/bin\:/sbin\:/bin, use_pty

User kali may run the following commands on kali:
(root) NOPASSWD: /usr/sbin/openvz
(ALL : ALL) ALL

[+] Quick Start
https://book.hacktricks.xyz/linux-hardening/privilege-escalation#reusing-sudo-tokens
Current user has .sudo_as_admin_successful file, so he can execute with sudo

[+] Checking Phexy policy
https://book.hacktricks.xyz/linux-hardening/privilege-escalation/interesting-groups-linux-pe-pe-method-2

[+] Supersusers
root:x:0:0:root:/root:/usr/bin/zsh

[+] Users with console

```

Среди возможных уязвимостей было только это, а всё остальное, что могло потребовать внимания — было красным. Если тут об уязвимостях, то максимум касаемо openvas, что пользователь kali может спокойно входить в Greenbone Security Assistant. Любой получивший доступ к данной учётной записи, сможет спокойно войти в GSA.

```

File Actions Edit View Help
-rw-r--r-- 1 root root 25 Feb  9 2023 /var/lib/dpkg/info/tightvncserver.conf
/etc/tightvncserver.conf
-rw-r--r-- 1 root root 32 Feb  9 2023 /var/lib/dpkg/info/xtightvncviewer.conf
/etc/xtightvncviewer.conf

-rw-r--r-- 1 root root 371 Oct  6 2022 /usr/share/legion/wordlists/vnc-betterdefaultpasslist.txt
123456
qazwsx
ADMIN
TOUCHLOW
Esteban
Esteban123
master
passwdf1
querty123
Administrator
rynpas

```

Только красное.

Step 4 and 5: Выгрузить список пользователей и групп в вашей системе + сохранить файл с выгрузкой результатов выполнения команд или сделать экранные выстрелы.

```
(kali㉿kali)-[~]
└─$ cat /etc/passwd
root:x:0:0:root:/root:/usr/bin/zsh
daemon:x:1:1:daemon:/usr/sbin/nologin
bin:x:2:2:bin:/bin:/usr/sbin/nologin
sys:x:3:3:sys:/dev:/usr/sbin/nologin
sync:x:4:65534:sync:/bin:/sync
games:x:5:60:games:/usr/games:/usr/sbin/nologin
man:x:6:12:man:/var/cache/man:/usr/sbin/nologin
lp:x:7:lp:/var/spool/lpd:/usr/sbin/nologin
mail:x:8:8:mail:/var/mail:/usr/sbin/nologin
news:x:9:9:news:/var/spool/news:/usr/sbin/nologin
uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin
proxy:x:13:13:proxy:/usr/sbin/nologin
www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin
backup:x:34:34:backup:/var/backups:/usr/sbin/nologin
list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin
ircd:x:39:39:ircd:/run/ircd:/usr/sbin/nologin
_apt:x:42:65534::/nonexistent:/usr/sbin/nologin
nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin
systemd-network:x:998:998:systemd Network Management:/:/usr/sbin/nologin
mysql:x:100:107:MySQL Server,,,:/nonexistent:/bin/false
tss:x:101:108:TPM software stack,,,:/var/lib/tpm:/bin/false
strongswan:x:102:65534::/var/lib/strongswan:/usr/sbin/nologin
systemd-timesync:x:997:997:systemd Time Synchronization:/:/usr/sbin/nologin
redsocks:x:103:109::/var/run/redsocks:/usr/sbin/nologin
rwhod:x:104:65534::/var/spool/rwho:/usr/sbin/nologin
iodine:x:105:65534::/run/iodine:/usr/sbin/nologin
messagebus:x:106:111::/nonexistent:/usr/sbin/nologin
miredo:x:107:65534::/var/run/miredo:/usr/sbin/nologin
redis:x:108:114::/var/lib/redis:/usr/sbin/nologin
usbxmux:x:109:46:usbxmux daemon,,,:/var/lib/usbxmux:/usr/sbin/nologin
mosquitto:x:110:116::/var/lib/mosquitto:/usr/sbin/nologin
tcpdump:x:111:118::/nonexistent:/usr/sbin/nologin
sshd:x:112:65534::/run/sshd:/usr/sbin/nologin
_rpc:x:113:65534::/run/rpcbind:/usr/sbin/nologin
dnsmasq:x:114:65534:dnsmasq,,,:/var/lib/misc:/usr/sbin/nologin
statd:x:115:65534::/var/lib/nfs:/usr/sbin/nologin
avahi:x:116:122:Avahi mDNS daemon,,,:/run/avahi-daemon:/usr/sbin/nologin
stunnel4:x:1996:996:stunnel service system account:/var/run/stunnel4:/usr/sbin/nologin
Debian-snmp:x:117:123::/var/lib/snmp:/bin/false
_gvm:x:118:124::/var/lib/openvms:/usr/sbin/nologin
speech-dispatcher:x:119:29:Speech Dispatcher,,,:/run/speech-dispatcher:/bin/false
sshh:x:120:125::/nonexistent:/usr/sbin/nologin
postgres:x:121:126:PostgreSQL administrator,,,:/var/lib/postgresql:/bin/bash
pulse:x:122:128:PulseAudio daemon,,,:/run/pulse:/usr/sbin/nologin
saned:x:123:131::/var/lib/saned:/usr/sbin/nologin
inetsim:x:124:132::/var/lib/inetsim:/usr/sbin/nologin
lightdm:x:125:133:Light Display Manager:/var/lib/lightdm:/bin/false
geoclue:x:126:134::/var/lib/geoclue:/usr/sbin/nologin
king-phisher:x:127:135::/var/lib/king-phisher:/usr/sbin/nologin
polkitd:x:994:994:polkitd:/nonexistent:/usr/sbin/nologin
rtkit:x:128:136:RealtimeKit,,,:/proc:/usr/sbin/nologin
colorl:x:129:137:colorl colour management daemon,,,:/var/lib/colorl:/usr/sbin/nologin
nm-openvpn:x:130:138:NetworkManager OpenVPN,,,:/var/lib/openvpn/chroot:/usr/sbin/nologin
nm-openconnect:x:131:139:NetworkManager OpenConnect plugin,,,:/var/lib/NetworkManager:/usr/sbin/nologin
kali:x:1000:1000:kali,,,:/home/kali:/usr/bin/zsh
_mta-sts:x:132:143::/var/lib/mta-sts:/usr/sbin/nologin
smmta:x:133:144:Mail Transfer Agent,,,:/var/lib/sendmail:/usr/sbin/nologin
smmsp:x:134:145:Mail Submission Program,,,:/var/lib/sendmail:/usr/sbin/nologin
_galeria:x:135:65534::/nonexistent:/usr/sbin/nologin
_gophish:x:136:146::/var/lib/gophish:/usr/sbin/nologin

(kali㉿kali)-[~]
```

Just execute `linpeas.sh` in a MacOs:

Quick Start

Find the latest versions of all the scripts

# From github  
curl -L https://github.com/carlosoplop/PEASS-ng/tree/master/linPEAS

Step 6: Выгрузить в файл список запущенных команд под обычной учётной записью (УЗ) и под УЗ корень. Сохранить выгруженный файл.

```
ubuntu@ubuntu:~$ cat ~.bash_history
./                                .bash_logout          .config/           .ssh/
..                                .bashrc             .local/            .sudo_as_admin_successful
.bash_history                     .cache/            .profile
ubuntu@ubuntu:~$ cat ~./.bash_history
ip ad
sudo apt install ssh
sudo systemctl enable ssh
sudo systemctl start ssh
sudo systemctl status ssh
clear
sudo tail -f /var/log/auth.log
ubuntu@ubuntu:~$
```

Тут список запущенных команд, сделанных обычным пользователем.

P.S. В Kali такой директории нет по умолчанию, поэтому пришлось показать на Ubuntu. Также здесь я не смог найти список команд, которые были совершены пользователем корень (или суперпользователь).

```
kali@kali: ~/.ssh
File Actions Edit View Help
[(kali㉿kali)-[~/ssh]]$ history kali
 1 sudo apt install isc-dhcp-server
 2 clear
 3 sudo nano /etc/default/isc-dhcp-server
 4 sudo nano /etc/dhcp/dhcpd.conf
 5 sudo apt install wpasupplicant wireless-tools
 6 iwlist wlan0 scan
 7 sudo nano /etc/network/interfaces
 8 sudo apt update
 9 sudo apt upgrade\
10 sudo apt upgrade
11 clear
12 sudo apt install apache2
13 cd /etc/apache2
14 ls -la\
15 ls -la
16 nano apache2.conf
17 sudo nano apache2.conf
18 clea
19 clear
20 apache2ctl -M
21 apache2ctl -m
22 sudo apache2ctl -M
23 clear
24 sudo a2enmod headers
25 sudo a2enmod rewrite
26 sudo a2enmod proxy
27 sudo a2enmod php8.2
28 systemctl restart apache2
29 cd /etc/apache2/sites-available
30 ls -la
31 sudo nano test.file.conf
32 a2ensite test.site
33 sudo nano test.file.conf
34 sudo a2ensite test.site
35 sudo nano cd /etc/hosts
36 sudo a2ensite test.site
37 sudo nano test.file.conf
38 ls -la
39 sudo nano test.file.conf
40 sudo a2ensite www.test.site
41 sudo a2ensite test.site
42 sudo a2ensite test.site.
43 sudo a2ensite test.site
44 sudo nano test.file.conf
45 openssl req -new -x509 -days 30 -keyout server.key -out -server.pem
46 clear
47 ls -la
48 nano -server.pem
49 nano server.key
50 cd /etc/ssl/certs
51
```

Альтернативно можно посмотреть историю всех команд активного пользователя (через команду history).

```
root@kali: /home/kali/.ssh
File Actions Edit View Help
[(root㉿kali)-[~/home/kali/.ssh]]# history
 1 cd /etc/apache2/sites-available
 2 ls -la
 3 nano test.file.conf
 4 a2ensite test.site
 5 nano test.file.conf
 6 a2ensite test.site
 7 mkdir -p /var/www/test.site/public_html
 8 chown -R $USER:$USER /var/www/test.site/public_html
 9 chmod -R 755 /var/www
10 nano test.file.conf
11 a2ensite test.site
12 nano /var/www/test.site/public_html/index.html
13 cp /var/www/test.site/public_html/index.html
14 clear
15 cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/test.site
16 cp /etc/apache2/sites-available/000-default.conf /etc/apache2/sites-available/test.site.conf
17 sudo nano /etc/apache2/sites-available/test.site.conf
18 clear
19 sudo a2ensite test.site
20 systemctl reload apache2
21 sudo a2dissite test.site
22 systemctl reload apache2
23 clear
24 cd ..
25 cd ..
26 clear
27 a2ensite test.site
28 systemctl reload apache2
29 systemctl start apache2
30 cd /etc/ssl/
31 ls -la
32 cd ..
33 ls -la
34 cd /etc/apache2/sites-available
35 ls -la
36 cd ..
37 cd sites-enabled
38 ls -la
39 nano test.site.conf
40 cd ..
41 cd sites-available
42 ls -la
43 nano test.site.conf
44 nano test.site
45 nano test.site.conf
46 nano test.file.conf
47 nano test.file
48 nano test.site
49 nano test.file
50 nano test.site
51 nano test.file
52 nano test.file.conf
```

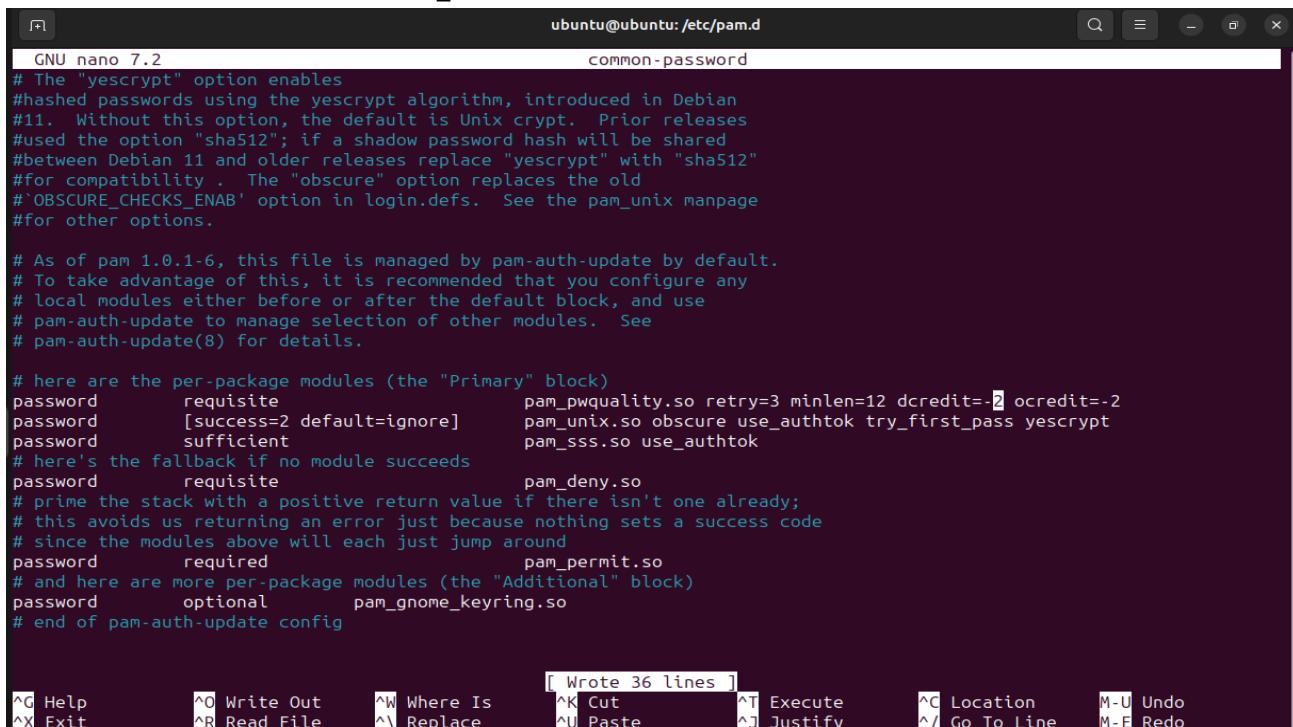
Тоже самое, но у пользователя корень (или суперпользователь).

Step 7: В журнале /var/log/auth.log найти события выполнения команд под УЗ sudo. Сделать экранный выстрел лога.

```
ubuntu@ubuntu:~  
ed for user gdm(uid=123) by (uid=0)  
2023-10-31T02:15:25.040306-05:00 ubuntu systemd-logind[828]: New session c1 of user gdm.  
2023-10-31T02:15:25.094981-05:00 ubuntu (systemd): pam_unix(systemd-user:session): session opened for user gdm(uid=123)  
by (uid=0)  
2023-10-31T02:15:29.555216-05:00 ubuntu polkitd[814]: Registered Authentication Agent for unix-session:c1 (system bus n  
ame :1.36 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)  
2023-10-31T02:15:50.624385-05:00 ubuntu gdm-password]: gkr-pam: unable to locate daemon control file  
2023-10-31T02:15:50.624577-05:00 ubuntu gdm-password]: gkr-pam: stashed password to try later in open session  
2023-10-31T02:15:50.647093-05:00 ubuntu gdm-password]: pam_env(gdm-password:session): deprecated reading of user enviro  
nment enabled  
2023-10-31T02:15:50.647228-05:00 ubuntu gdm-password]: pam_unix(gdm-password:session): session opened for user ubuntu(u  
id=1000) by (uid=0)  
2023-10-31T02:15:50.698408-05:00 ubuntu systemd-logind[828]: New session 2 of user ubuntu.  
2023-10-31T02:15:50.733121-05:00 ubuntu (systemd): pam_unix(systemd-user:session): session opened for user ubuntu(uid=1  
000) by (uid=0)  
2023-10-31T02:15:51.125252-05:00 ubuntu gdm-password]: gkr-pam: unlocked login keyring  
2023-10-31T02:15:51.636874-05:00 ubuntu gnome-keyring-daemon[1631]: The PKCS#11 component was already initialized  
2023-10-31T02:15:51.654578-05:00 ubuntu gnome-keyring-daemon[1813]: discover_other_daemon: 1  
2023-10-31T02:15:51.655863-05:00 ubuntu gnome-keyring-daemon[1812]: discover_other_daemon: 1  
2023-10-31T02:15:51.656296-05:00 ubuntu gnome-keyring-daemon[1631]: The Secret Service was already initialized  
2023-10-31T02:15:51.656975-05:00 ubuntu gnome-keyring-daemon[1814]: discover_other_daemon: 1  
2023-10-31T02:15:53.724692-05:00 ubuntu polkitd[814]: Registered Authentication Agent for unix-session:2 (system bus na  
me :1.77 [/usr/bin/gnome-shell], object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8)  
2023-10-31T02:15:57.879765-05:00 ubuntu gdm-launch-environment]: pam_unix(gdm-launch-environment:session): session clos  
ed for user gdm  
2023-10-31T02:15:57.892908-05:00 ubuntu systemd-logind[828]: Session c1 logged out. Waiting for processes to exit.  
2023-10-31T02:15:57.924207-05:00 ubuntu polkitd[814]: Unregistered Authentication Agent for unix-session:c1 (system bus  
name :1.36, object path /org/freedesktop/PolicyKit1/AuthenticationAgent, locale en_US.UTF-8) (disconnected from bus)  
2023-10-31T02:15:57.930497-05:00 ubuntu systemd-logind[828]: Removed session c1.  
2023-10-31T02:16:08.244081-05:00 ubuntu (sd-pam): pam_unix(systemd-user:session): session closed for user gdm  
2023-10-31T02:16:11.119333-05:00 ubuntu sudo:    ubuntu : TTY=pts/0 ; PWD=/home/ubuntu ; USER=root ; COMMAND=/usr/bin/ca  
t /var/log/auth.log  
2023-10-31T02:16:11.120446-05:00 ubuntu sudo: pam_unix(sudo:session): session opened for user root(uid=0) by (uid=1000)  
ubuntu@ubuntu:~$
```

Через выше введённую команду.

### Задание 3. Настройка систем безопасности Linux



```
GNU nano 7.2                                         common-password
# The "yescrypt" option enables
#hashed passwords using the yescrypt algorithm, introduced in Debian
#11. Without this option, the default is Unix crypt. Prior releases
#used the option "sha512"; if a shadow password hash will be shared
#between Debian 11 and older releases replace "yescrypt" with "sha512"
#for compatibility . The "obscure" option replaces the old
#'OBSCURE_CHECKS_ENAB' option in login.defs. See the pam_unix manpage
#for other options.

# 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_pwquality.so retry=3 minlen=12 dcredit=-2 ocredit=-2
password      [success=2 default=ignore]    pam_unix.so obscure use_authtok try_first_pass yescrypt
password      sufficient         pam_sss.so use_authtok
# 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
# and here are more per-package modules (the "Additional" block)
password      optional            pam_gnome_keyring.so
# end of pam-auth-update config

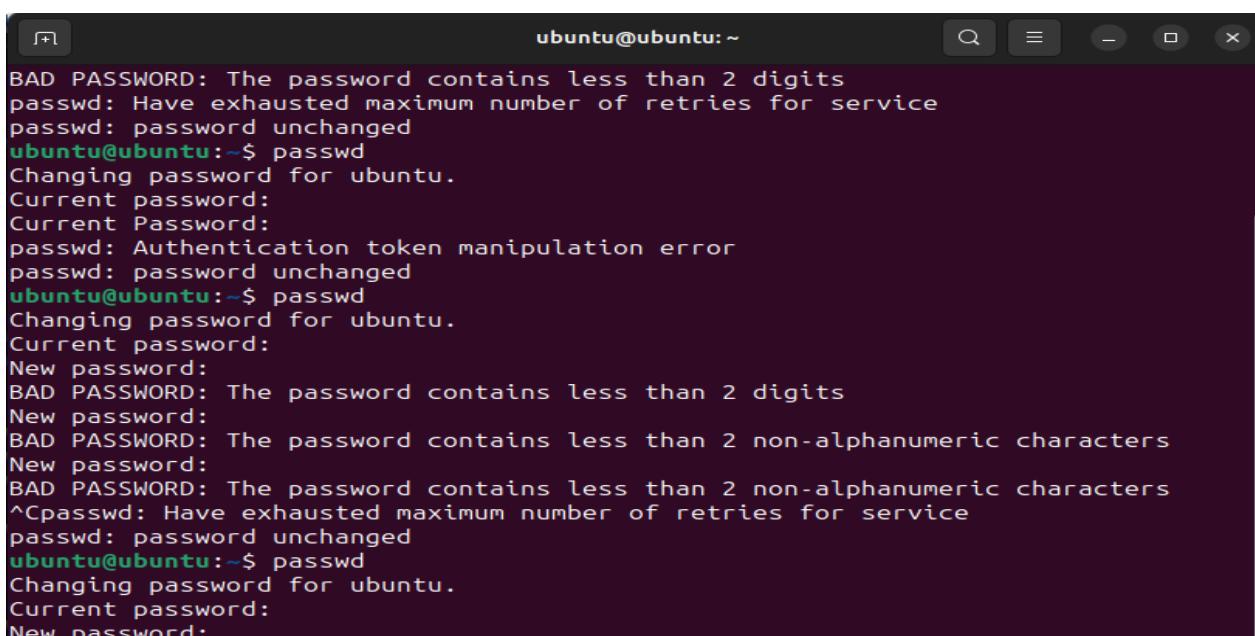
[ Wrote 36 lines ]
```

^G Help ^O Write Out ^W Where Is ^K Cut ^T Execute ^C Location M-U Undo  
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo

Step 1: Настроить критерии сложного пароля.

Я поменял немного данный файл для паролей, в дистрибутивах на основе RedHat он называется /etc/security/pwquality.conf. Тут мин. кол-во символов — 12, мин. кол-во цифр -2, мин. кол-во заглавных букв — 2.

Step 2: Проверить, что критерии работают и пользователь не может задать лёгкий пароль и сделать экранный выстрел результата.



```
ubuntu@ubuntu:~$ passwd
BAD PASSWORD: The password contains less than 2 digits
passwd: Have exhausted maximum number of retries for service
passwd: password unchanged
ubuntu@ubuntu:~$ passwd
Changing password for ubuntu.
Current password:
Current Password:
passwd: Authentication token manipulation error
passwd: password unchanged
ubuntu@ubuntu:~$ passwd
Changing password for ubuntu.
Current password:
New password:
BAD PASSWORD: The password contains less than 2 digits
New password:
BAD PASSWORD: The password contains less than 2 non-alphanumeric characters
New password:
BAD PASSWORD: The password contains less than 2 non-alphanumeric characters
^Cpasswd: Have exhausted maximum number of retries for service
passwd: password unchanged
ubuntu@ubuntu:~$ passwd
Changing password for ubuntu.
Current password:
New password:
```

Вот результат добавленных изменений. При пароле менее 12 символов, тоже об этом предупреждает.

Step 3: Добавить одно запрещающее правило через iptables и сделать скриншот. Описать, как работает правило.

```
ubuntu@ubuntu:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ubuntu@ubuntu:~$ sudo iptables -P INPUT DROP -p http --dport 80 -j ACCEPT
iptables v1.8.9 (nf_tables): unknown protocol "http" specified
Try 'iptables -h' or 'iptables --help' for more information.
ubuntu@ubuntu:~$ sudo iptables -A INPUT -p tcp --dport 80 -j DROP
ubuntu@ubuntu:~$ sudo iptables -L
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
DROP      tcp   --  anywhere            anywhere             tcp dpt:http
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ubuntu@ubuntu:~$
```

Тут я запретил проход незащищённого трафика, данное правило будет отбрасывать без уведомления весь http трафик.

Step 4: Установить утилиту Auditd и настройте через неё мониторинг файла /etc/sudoers.

```
ubuntu@ubuntu:~$ sudo apt install auditd
Display all 71611 possibilities? (y or n)
ubuntu@ubuntu:~$ sudo apt install auditd audiod
audiofile-tools audiolink    audiotools    audisdp-plugins auditd
ubuntu@ubuntu:~$ sudo apt install auditd audisdp-plugins
[sudo] password for ubuntu:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following additional packages will be installed:
  libauparse0
The following NEW packages will be installed:
  audisdp-plugins auditd libauparse0
0 upgraded, 3 newly installed, 0 to remove and 5 not upgraded.
Need to get 314 kB of archives.
After this operation, 1,012 kB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://ru.archive.ubuntu.com/ubuntu mantic/main amd64 libauparse0 amd64 1:3.1.1-1 [58.0 kB]
Get:2 http://ru.archive.ubuntu.com/ubuntu mantic/main amd64 auditd amd64 1:3.1.1-1 [217 kB]
Get:3 http://ru.archive.ubuntu.com/ubuntu mantic/universe amd64 audisdp-plugins amd64 1:3.1.1-1 [39.0 kB]
Fetched 314 kB in 1s (382 kB/s)
ubuntu@ubuntu:~$ sudo auditctl -l
No rules
ubuntu@ubuntu:~$ auditctl -a exit,always -F path=/etc/sudoers -F perm=wa
You must be root to run this program.
ubuntu@ubuntu:~$ sudo auditctl -a exit,always -F path=/etc/sudoers -F perm=wa
ubuntu@ubuntu:~$ sudo auditctl -l
-w /etc/sudoers -p wa
ubuntu@ubuntu:~$
```

Готово.

Step 5: Создать новую учётную запись в Linux, добавить её в sudoers.

The screenshot shows a terminal window titled "ubuntu@ubuntu:~". The command "nano /etc/sudoers" is running. The content of the file is displayed in blue and black text. A specific line, "test ALL=(ALL:ALL) ALL", is highlighted with a yellow background. The bottom of the screen shows the nano editor's menu bar with options like Help, Write Out, Where Is, Cut, Execute, Location, Undo, Exit, Read File, Replace, Paste, Justify, Go To Line, and Redo.

```
# Per-user preferences; root won't have sensible values for them.
#Defaults:%sudo env_keep += "EMAIL DEBEMAIL DEBFULLNAME"

# "sudo scp" or "sudo rsync" should be able to use your SSH agent.
#Defaults:%sudo env_keep += "SSH_AGENT_PID SSH_AUTH_SOCK"

# Ditto for GPG agent
#Defaults:%sudo env_keep += "GPG_AGENT_INFO"

# Host alias specification

# User alias specification

# Cmnd alias specification

# User privilege specification
root    ALL=(ALL:ALL) ALL
test    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:
@include /etc/sudoers.d
```

Добавил нового пользователя в файл sudoers.

Step 6: С помощью команды ausearch -f /etc/sudoers посмотреть вывод и сделать экранный выстрел.

The screenshot shows a terminal window titled "ubuntu@ubuntu:~". The command "sudo ausearch -f /etc/sudoers" is run. The output shows audit logs. One log entry is highlighted with a yellow background. The log entry details a process (audit) with various parameters like proctitle, msg, item, name, inode, dev, mode, uid, ogid, rdev, nametype, cap\_fp, cap\_fe, cap\_fver, cap\_frootid, and cwd.

```
time->Tue Oct 31 01:08:19 2023
type=PROCTITLE msg=audit(1698732499.818:179): proctitle=6E616E6F002F6574632F7375646F657273
type=PATH msg=audit(1698732499.818:179): item=1 name="/etc/sudoers" inode=3932600 dev=08:02 mode=0100440 uid=0 ogid=0
rdev=00:00 nametype=NORMAL cap_fp=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=PATH msg=audit(1698732499.818:179): item=0 name="/etc/" inode=3932161 dev=08:02 mode=040755 uid=0 ogid=0 rdev=00:00
nametype=PARENT cap_fp=0 cap_fe=0 cap_fver=0 cap_frootid=0
type=CWD msg=audit(1698732499.818:179): cwd="/home/ubuntu"
type=SYSCALL msg=audit(1698732499.818:179): arch=c000003e syscall=257 success=yes exit=3 a0=fffffff9c a1=562534bcb7f0 a2=241 a3=1b6 items=2 ppid=3704 pid=3705 auid=1000 uid=0 euid=0 suid=0 egid=0 sgid=0 tty=pts1 ses=3
comm="nano" exe="/usr/bin/nano" subj=unconfined key=(null)
ubuntu@ubuntu:~$
```

Вот что вышло у меня.