

Wykrywanie zagrożeń i reakcja na incydenty

Laboratorium 1

Tomasz Jarząbek 272279
Wiktoria Migasiewicz 272177

16.03.2025

Spis treści

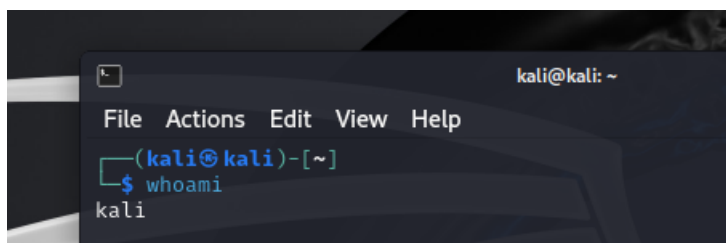
1	Wprowadzenie	3
2	Instalacja Kali Linux	3
3	Wykonane komendy	3
3.1	Procesy	3
3.2	Aplikacje	4
3.3	Otwarte porty	6
3.3.1	Netstat	6
3.3.2	Nmap	7
3.4	Pliki	7
3.5	Komendy	8
3.6	Cron	8
3.7	Logi	9
3.8	Kernel	10
3.9	Parametry Hardware'owe	10
3.10	Parametry sieciowe	11

1 Wprowadzenie

Celem niniejszego ćwiczenia było przeanalizowanie różnych technik systemu Linux, które służą do administracji systemu i jednocześnie są bardzo przydatne w wykrywaniu wszelakich podatności lub śladów działań złośliwych programów. Do analizy wykorzystano system operacyjny Kali Linux, który również został zainstalowany na potrzeby ćwiczenia, oraz pewne wbudowane, lub nie, narzędzia, takie np. vsftpd, netstat.

2 Instalacja Kali Linux

Ćwiczenie rozpoczęto od zainstalowania Systemu Operacyjnego Kali Linux, za pomocą gotowego obrazu lub przy pomocy Hypervisora typu II, np. VirtualBox na systemie Windows. Instalacja przebiegła pomyślnie, użytkownik nazywa się *kali*.

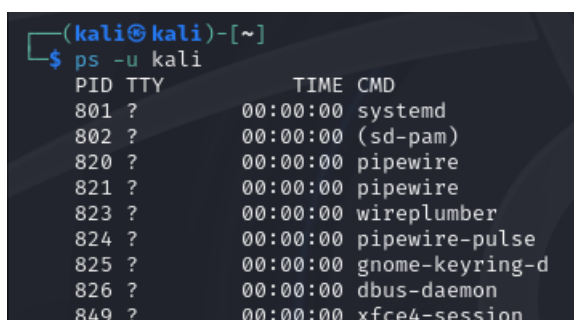


Rysunek 1: Zainstalowany Kali Linux wraz z użytkownikiem Kali.

3 Wykonane komendy

3.1 Procesy

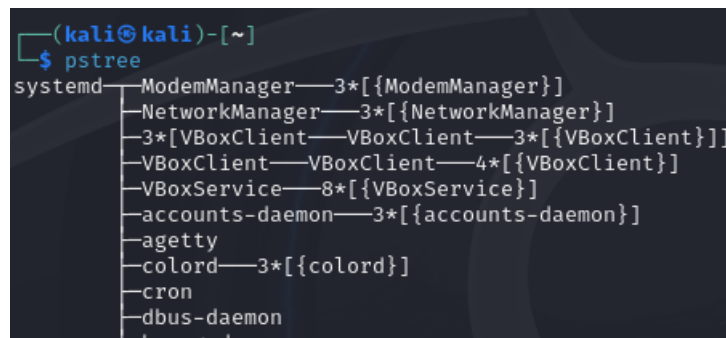
Najpierw, wyświetlono listę procesów użytkownika **kali**. Zrobiono to komendą, która wraz z wynikiem została zaprezentowana poniżej:



Rysunek 2: Lista procesów dla użytkownika Kali.

Następnie wyszukano i wyświetlono drzewo procesów i zidentyfikowano, które procesy zostały uru-

chomione w oparciu o proces rodzica *systemd*. Dodatkowo zainicjowany został *systemd* przez rodzica *systemd*.



Rysunek 3: Drzewo procesów.

Znalezione procesy wypisano poniżej:

- ModemManager
- NetworkManager
- VBoxClient (kilka instancji)
- VBoxService
- accounts-daemon
- agetty
- colord
- cron
- dbus-daemon
- haveged
- lightdm
- polkitd
- qterminal
- rtkit-daemon
- ssh-agent
- systemd-journal
- systemd-logind
- systemd-udev
- udisksd
- upowerd

3.2 Aplikacje

Polecenie:

Proszę wyświetlić listę zainstalowanych aplikacji, a później odszukać wersję serwera ssh (openssh-server).

Wykorzystana komenda:

`dpkg -list`

Wynik:

```
(kali@kali)~$ dpkg --get-configuration | grep -E "(Wtyczki|Pakety)"
```

```
Wybór:U-nieznany/I-instalacja/R-usunięcie/P-wyczyszczenie/H-zatrzymanie  
Stan:N-brak/I-zainstalowany/C-skongigrowany/U-rozpakovany/  
// F-część, skonfigurowany/H-część, zainstalowany/W-wyżw. czek./T-wyżw. zap.  
|| Błądy(brak)/R-do pon. inst. (duże litery w "Stan" i "Błędy"-problemy)  
// Nazwa Wersja  
---  
7zip 24.08+dfsg-1  
accountsservice 23.13.9-7  
acl 2.3.2-2+b1  
adduser 3.137  
adwaita-icon-theme 47.0-2  
aircrack-ng 1.1:7+git20230807.4bf83f1a-2  
alsa-topology-conf 1.2.5.1-3  
alsa-ucm-conf 1.2.12-1  
amass 4.2.0-0kali1  
amass-common 4.2.0-0kali1  
amd64-microcode 3.20240820.1  
apache2 2.4.62-3  
apache2-bin 2.4.62-3  
apache2-data 2.4.62-3  
apache2-utils 2.4.62-3  
apparmor 3.1.7-1+b3  
apt 2.9.10+kali1  
apt-file 3.3  
apt-utils 2.9.10+kali1
```

Rysunek 4: Wynik działania `dpkg -list`.

Polecenie `dpkg -list` (lub skrót `dpkg -l`) wypisuje listę wszystkich pakietów zainstalowanych w systemie, ich wersje i krótki opis.

Wykorzystana komenda:

```
dpkg -l | grep openssh-server
```

Wynik:

```

(kali@kali)~$ dpkg -l grep openssh-server
Wybór:U=nieznany/I=instalacja/R=usunięcie/P=wyczyszczenie/H=zatrzymanie
| Stan:N=brak/I=zainstalowany/C=skonfigurowany/U=rozpakowany/
| / F=częśc. skonfigurowany/H=częśc. zainstalowany/W=wyzw. czek./T=wyzw. zap.
|| Błędy?(=brak)/R=do pon. inst. (duże litery w "Stan" i "Błędy"=problemy)
|| / Nazwa Wersja Architektura Opis
+++-----+-----+-----+-----+
ii grep 3.11-4 amd64 GNU grep, egrep and fgrep
ii openssh-server 1:9.9p1-3 amd64 secure shell (SSH) server, for
lines 1-8/8 (END)

```

Rysunek 5: Wynik komendy grep w openssh.

dpkg -l pokazuje listę pakietów, ale grep openssh-server filtruje wynik, pozostawiając jedynie informacje o pakiecie openssh-server, w tym jego wersję.

Polecenie:

Proszę w oparciu o pliki „dpkg.log”, „dpkg.log.1” itd. zidentyfikować datę instalacji usługi vsftpd.

Wykorzystana komenda:

```
grep "vsftpd"/var/log/dpkg.log* | grep "install" Wynik:
```

```
(kali㉿kali)-[~]
$ grep "vsftpd" /var/log/dpkg.log* | grep "install"
2025-03-13 19:30:23 install vsftpd:amd64 <none> 3.0.5-0.1
2025-03-13 19:30:23 status half-installed vsftpd:amd64 3.0.5-0.1
2025-03-13 19:30:25 status installed vsftpd:amd64 3.0.5-0.1
```

Rysunek 6: Wynik komendy `grep` w szukaniu daty instalacji `vsftpd`.

Pliki `/var/log/dpkg.log*` zawierają historię instalacji pakietów. `grep "vsftpd"` wyszukuje wpisy dotyczące pakietu `vsftpd`, a `grep "install"` ogranicza wyniki do operacji instalacji.

Zidentyfikowana data instalacji usługi `vsftpd` to 13.03.2025.

3.3 Otwarte porty

3.3.1 Netstat

Odwiedzono w przeglądarce internetowej stronę **exploit-db.com**, a następnie przeszukano otwarte i nasłuchujące porty UDP i TCP w celu analizy połączenia z odwiedzaną witryną. W tym celu, najpierw zidentyfikowano adres IP strony przy pomocy narzędzia **nslookup**, co podało wynik pokazany poniżej:

```
(kali@kali)-[~]
$ nslookup exploit-db.com
Server:      192.168.100.1
Address:     192.168.100.1#53

Non-authoritative answer:
Name:   exploit-db.com
Address: 192.124.249.13
```

Rysunek 7: Wynik działania `nslookup` na `exploit-db.com`.

Następnie, w trybie administratora, przeanalizowano nasłuchujące porty z pomocą narzędzia **netstat**. Wydano komendę z flagami filtrującymi interesujące nas informacje.

```
(kali@kali)-[~]
$ sudo netstat -tunp
Active Internet connections (w/o servers)

```

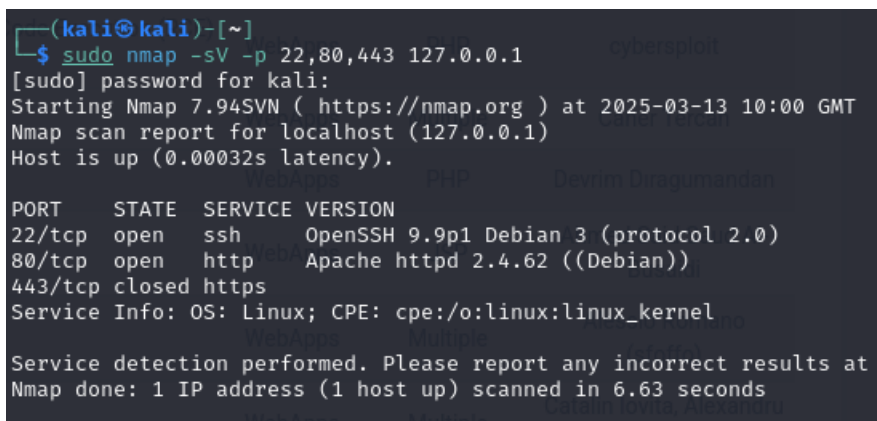
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name
tcp	0	0	10.0.2.15:54038	104.81.99.158:443	ESTABLISHED	15041/firefox-esr
tcp	0	0	10.0.2.15:50370	192.124.249.13:443	ESTABLISHED	15041/firefox-esr
tcp	0	0	10.0.2.15:35454	34.107.243.93:443	ESTABLISHED	15041/firefox-esr
tcp	0	0	10.0.2.15:54042	104.81.99.158:443	ESTABLISHED	15041/firefox-esr
tcp	0	0	10.0.2.15:40502	96.16.54.201:443	ESTABLISHED	15041/firefox-esr
tcp	0	0	10.0.2.15:43362	142.250.186.206:443	ESTABLISHED	15041/firefox-esr
tcp	0	0	10.0.2.15:57074	142.250.186.195:443	ESTABLISHED	15041/firefox-esr
tcp	0	0	10.0.2.15:53708	96.16.54.137:443	ESTABLISHED	15041/firefox-esr
udp	0	0	10.0.2.15:68	10.0.2.2:67	ESTABLISHED	619/NetworkManager

Rysunek 8: Wynik działania `nslookup` na `exploit-db.com`.

Jak widać, ustalone jest połączenie ze stroną internetową na porcie 50370 i używany jest protokół HTTPS. Program, który otworzył połączenie, to Firefox (PID 15041).

3.3.2 Nmap

Przy pomocy narzędzia Nmap zidentyfikowano również wersje uruchomionych przez systemctl usług ssh i apache2. Pierwszy z nich nasłuchuje na porcie 22, a drugi na 80 i 443. Zatem po sprawdzeniu przez **systemctl status** i potwierdzenie, że procesy działają, polecenie poniżej zwróciło nam wersje obu z nich:



```
(kali㉿kali)-[~]
└─$ sudo nmap -sV -p 22,80,443 127.0.0.1
[sudo] password for kali:
Starting Nmap 7.94SVN ( https://nmap.org ) at 2025-03-13 10:00 GMT
Nmap scan report for localhost (127.0.0.1)
Host is up (0.00032s latency).

PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 9.9p1 Debian 3 (protocol 2.0)
80/tcp    open  http     Apache httpd 2.4.62 ((Debian))
443/tcp   closed https
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel

Service detection performed. Please report any incorrect results at
Nmap done: 1 IP address (1 host up) scanned in 6.63 seconds
```

Rysunek 9: Wersje usług SSH i apache2.

3.4 Pliki

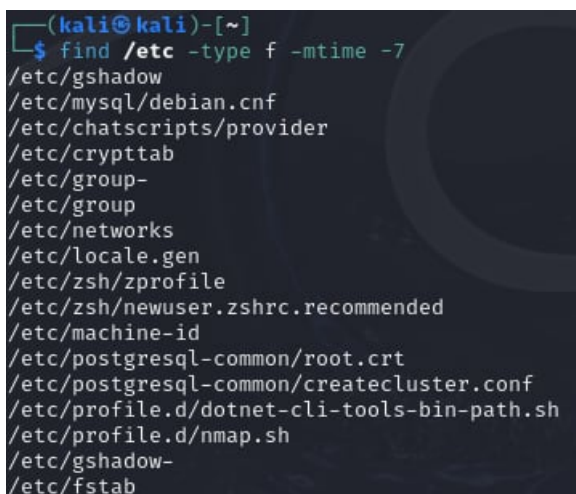
Polecenie:

Proszę odnaleźć pliki zmodyfikowane w ciągu ostatnich 7 dni w katalogu „/etc”.

Wykorzystana komenda:

```
find /etc -type f -mtime -7
```

Wynik:



```
(kali㉿kali)-[~]
└─$ find /etc -type f -mtime -7
/etc/gshadow
/etc/mysql/debian.cnf
/etc/chatscripts/provider
/etc/crypttab
/etc/group-
/etc/group
/etc/networks
/etc/locale.gen
/etc/zsh/zprofile
/etc/zsh/newuser.zshrc.recommended
/etc/machine-id
/etc/postgresql-common/root.crt
/etc/postgresql-common/createcluster.conf
/etc/profile.d/dotnet-cli-tools-bin-path.sh
/etc/profile.d/nmap.sh
/etc/gshadow-
/etc/fstab
```

Rysunek 10: Wynik szukania plików modyfikowanych.

`find /etc` przeszukuje katalog `/etc`, `-type f` ogranicza wynik do plików, a `-mtime -7` zwraca tylko te,

które były modyfikowane w ciągu ostatnich 7 dni.

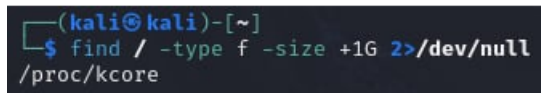
Polecenie:

Proszę odnaleźć pliki większe, niż 1GB w katalogu „/”.

Wykorzystana komenda:

`find / -type f -size +1G 2>/dev/null`

Wynik:



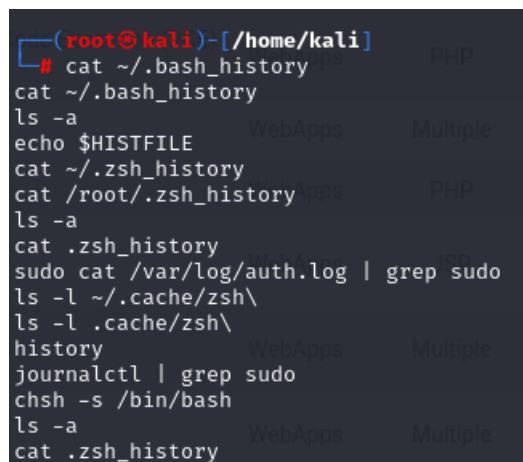
```
(kali@kali)-[~]  
$ find / -type f -size +1G 2>/dev/null  
/proc/kcore
```

Rysunek 11: Pliki większe niż 1 GB.

`find /` przeszukuje cały system, `-type f` ogranicza wyszukiwanie do plików, `-size +1G` zwraca tylko pliki większe niż 1GB, a `2>/dev/null` usuwa błędy dotyczące braku dostępu.

3.5 Komendy

Onaleziono listę wykonanych komend przez użytkownika root w pliku `.zsh_history`, a ku wygodzie przeniesiono powłokę na basha i historia zawierana jest w pliku `.bash_history`.



```
(root@kali)-[/home/kali]  
# cat ~/.bash_history  
cat ~/.bash_history  
ls -a  
echo $HISTFILE  
cat ~/.zsh_history  
cat /root/.zsh_history  
ls -a  
cat .zsh_history  
sudo cat /var/log/auth.log | grep sudo  
ls -l ~/.cache/zsh/  
ls -l .cache/zsh/  
history  
journalctl | grep sudo  
chsh -s /bin/bash  
ls -a  
cat .zsh_history
```

Rysunek 12: Lista historii komend wydawanych przez root-a.

3.6 Cron

Cron

Polecenie:

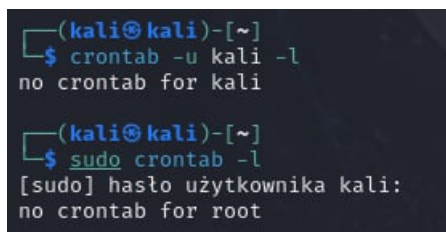
Proszę zidentyfikować listę wpisów w cronie użytkowników kali oraz root.

Wykorzystana komenda:


```
crontab -u kali -l
```

```
sudo crontab -l
```

Wynik:



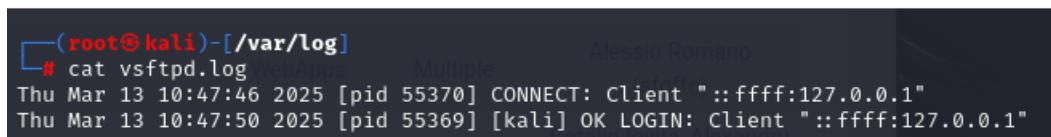
```
(kali@kali)-[~]  
$ crontab -u kali -l  
no crontab for kali  
  
(kali@kali)-[~]  
$ sudo crontab -l  
[sudo] hasło użytkownika kali:  
no crontab for root
```

Rysunek 13: Wynik szukania listy wpisów w Cronie dla kali i root.

`crontab -u kali -l` wyświetla harmonogram zadań użytkownika kali. `sudo crontab -l` pokazuje harmonogram dla użytkownika root.

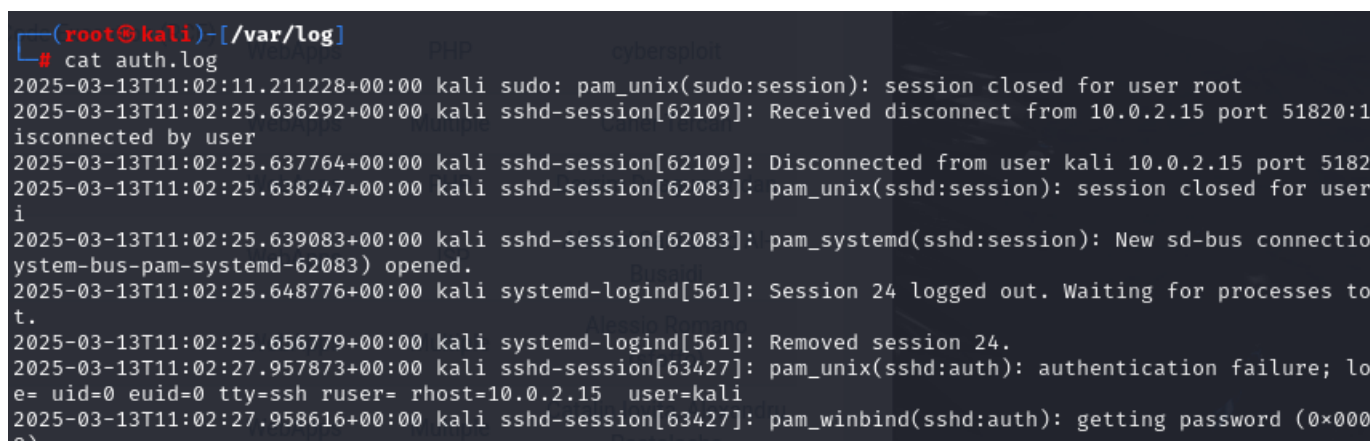
3.7 Logi

W celu sprawdzenia działania zapisywania logów, przetestowano logowanie do usługi FTP oraz SSH. W celu uzyskania logów SSH zainstalowano *rsyslog*. Po upewnieniu się za pomocą `systemctl`, że usługi są włączone i zalogowaniu się na localhosta, sprawdzono, odpowiednio, **vsftpd.log** i **auth.log**.



```
(root@kali)-[/var/log]  
# cat vsftpd.log  
Thu Mar 13 10:47:46 2025 [pid 55370] CONNECT: Client "::ffff:127.0.0.1"  
Thu Mar 13 10:47:50 2025 [pid 55369] [kali] OK LOGIN: Client "::ffff:127.0.0.1"
```

Rysunek 14: Logi dla FTP.



```
(root@kali)-[/var/log]  
# cat auth.log  
2025-03-13T11:02:11.211228+00:00 kali sudo: pam_unix(sudo:session): session closed for user root  
2025-03-13T11:02:25.636292+00:00 kali sshd-session[62109]: Received disconnect from 10.0.2.15 port 51820:1  
isconnected by user  
2025-03-13T11:02:25.637764+00:00 kali sshd-session[62109]: Disconnected from user kali 10.0.2.15 port 5182  
2025-03-13T11:02:25.638247+00:00 kali sshd-session[62083]: pam_unix(sshd:session): session closed for user  
i  
2025-03-13T11:02:25.639083+00:00 kali sshd-session[62083]: pam_systemd(sshd:session): New sd-bus connectio  
system-bus-pam-systemd-62083) opened.  
2025-03-13T11:02:25.648776+00:00 kali systemd-logind[561]: Session 24 logged out. Waiting for processes to  
t.  
2025-03-13T11:02:25.656779+00:00 kali systemd-logind[561]: Removed session 24.  
2025-03-13T11:02:27.957873+00:00 kali sshd-session[63427]: pam_unix(sshd:auth): authentication failure; lo  
e= uid=0 euid=0 tty=ssh ruser= rhost=10.0.2.15 user=kali  
2025-03-13T11:02:27.958616+00:00 kali sshd-session[63427]: pam_winbind(sshd:auth): getting password (0x000  
a)
```

Rysunek 15: Logi dla SSH.

3.8 Kernel

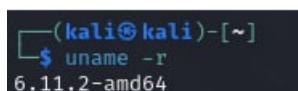
Polecenie:

Proszę wyświetlić wersję kernela.

Wykorzystana komenda:

```
uname -r
```

Wynik:



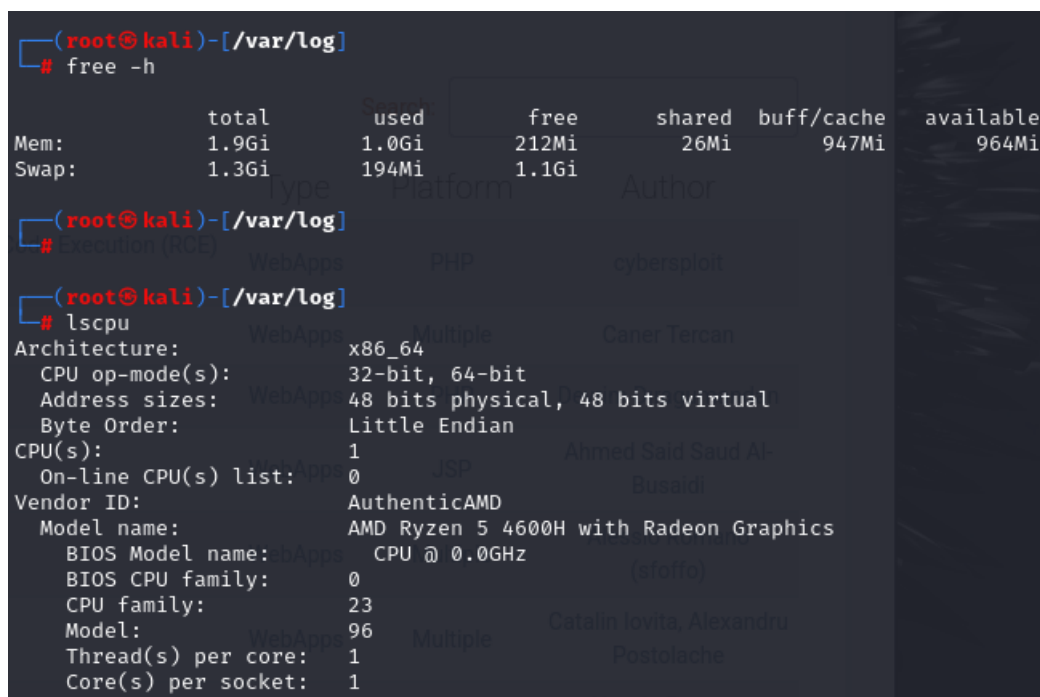
```
(kali㉿kali)-[~]  
$ uname -r  
6.11.2-amd64
```

Rysunek 16: Wynik komendy `uname -r`.

`uname -r` wyświetla aktualnie używaną wersję jądra systemu Linux.

3.9 Parametry Hardware'owe

Aby zobaczyć ilość dostępnego RAMu, liczby wirtualnych procesorów i ich taktowanie oraz łączny rozmiar dysku, wprowadzone zostały komendy, które wraz z wynikami, zamieszczone zostały poniżej:



```
(root㉿kali)-[/var/log]  
# free -h  


|       | total | used  | free  | shared | buff/cache | available |
|-------|-------|-------|-------|--------|------------|-----------|
| Mem:  | 1.9Gi | 1.0Gi | 212Mi | 26Mi   | 947Mi      | 964Mi     |
| Swap: | 1.3Gi | 194Mi | 1.1Gi |        |            |           |

  
(root㉿kali)-[/var/log]  
# lscpu  
Architecture: x86_64  
CPU op-mode(s): 32-bit, 64-bit  
Address sizes: 48 bits physical, 48 bits virtual  
Byte Order: Little Endian  
CPU(s): 1  
On-line CPU(s) list: 0  
Vendor ID: AuthenticAMD  
Model name: AMD Ryzen 5 4600H with Radeon Graphics  
BIOS Model name: bApps CPU @ 0.0GHz  
BIOS CPU family: 0  
CPU family: 23  
Model: 96  
Thread(s) per core: 1  
Core(s) per socket: 1
```

Rysunek 17: RAM oraz część wyniku dot. procesorów.

```
(root@kali)-[/var/log]
# df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            926M    0  926M   0% /dev
tmpfs           198M 1020K  197M   1% /run
/dev/sda1       24G   14G   8.2G  63% /
tmpfs           988M   4.0K  988M   1% /dev/shm
tmpfs           5.0M    0   5.0M   0% /run/lock
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-journald.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-udev-load-credentials.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev-early.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-sysctl.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-sysusers.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-tmpfiles-setup-dev.service
tmpfs           988M   2.1M  986M   1% /tmp
tmpfs           1.0M    0   1.0M   0% /run/credentials/systemd-tmpfiles-setup.service
tmpfs           1.0M    0   1.0M   0% /run/credentials/getty@tty1.service
tmpfs           198M  116K  198M   1% /run/user/1000
```

Rysunek 18: Dostępna pamięć dyskowa.

3.10 Parametry sieciowe

Polecenie:

Proszę uzyskać adres IP

Wykorzystana komenda:

ip a

Wynik:

```
(kali@kali)-[~]
$ ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host noprefixroute
        valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc fq_codel state UP group default qlen 1000
    link/ether 08:00:27:72:1f:70 brd ff:ff:ff:ff:ff:ff
    inet 192.168.100.16/24 brd 192.168.100.255 scope global dynamic noprefixroute eth0
        valid_lft 85866sec preferred_lft 85866sec
    inet6 fe80::a00:27ff:fe72:1f70/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

Rysunek 19: Wynik komendy ip a.

ip a (lub ip addr show) wyświetla listę interfejsów sieciowych wraz z przypisanymi im adresami IP.

Polecenie:

Proszę uzyskać listę serwerów DNS

Wykorzystana komenda:

`cat /etc/resolv.conf`

Wynik:



```
(kali㉿kali)-[~]  
$ cat /etc/resolv.conf  
# Generated by NetworkManager  
nameserver 192.168.100.1  
nameserver fe80::1%eth0
```

Rysunek 20: Wynik szukania serwerów DNS.

Plik `/etc/resolv.conf` przechowuje listę serwerów DNS skonfigurowanych w systemie.

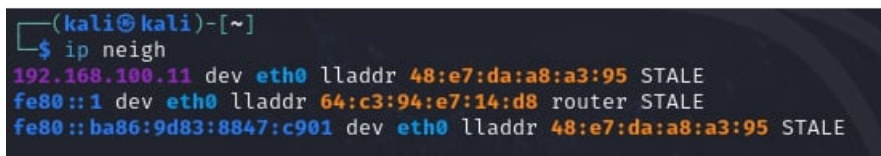
Polecenie:

Proszę uzyskać tablicę translacji adresów IP na adresy MAC

Wykorzystana komenda:

`ip neigh`

Wynik:



```
(kali㉿kali)-[~]  
$ ip neigh  
192.168.100.1 dev eth0 lladdr 48:e7:da:a8:a3:95 STALE  
fe80::1 dev eth0 lladdr 64:c3:94:e7:14:d8 router STALE  
fe80::ba86:9d83:8847:c901 dev eth0 lladdr 48:e7:da:a8:a3:95 STALE
```

Rysunek 21: Wynik komendy `ip neigh`.

`ip neigh` (lub `ip neighbor show`) wyświetla tablicę ARP, czyli mapowanie adresów IP na adresy MAC w lokalnej sieci.

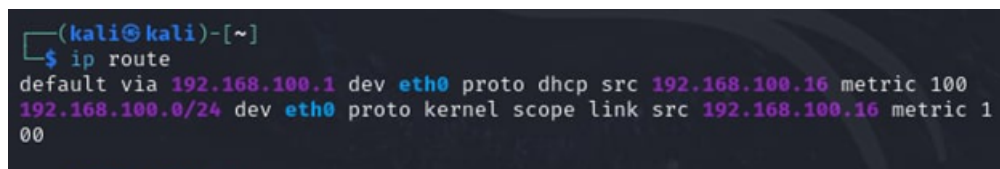
Polecenie:

Proszę uzyskać tablicę routingu

Wykorzystana komenda:

`ip route`

Wynik:



```
(kali㉿kali)-[~]  
$ ip route  
default via 192.168.100.1 dev eth0 proto dhcp src 192.168.100.16 metric 100  
192.168.100.0/24 dev eth0 proto kernel scope link src 192.168.100.16 metric 100
```

Rysunek 22: Wynik komendy `ip route`.

`ip route` pokazuje tablicę routingu, czyli trasowanie pakietów w systemie. Alternatywnie można użyć `route -n`.