

# Wykrywanie zagrożeń i reakcja na incydenty

Laboratorium 8

Tomasz Jarząbek 272279

Wiktoria Migasiewicz 272177

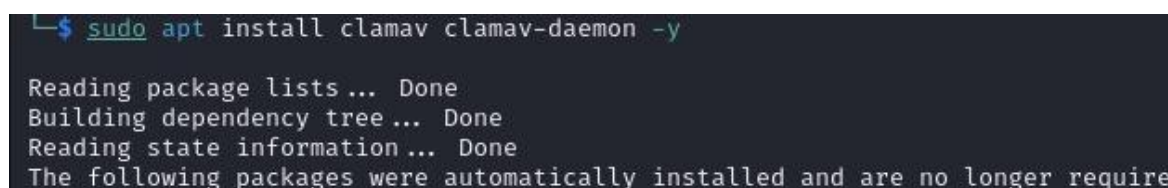
# 1. Wprowadzenie

Celem niniejszego ćwiczenia było praktyczne zapoznanie się z podstawowymi technikami wykrywania zagrożeń oraz reagowania na incydenty bezpieczeństwa w systemie Linux. W ramach zadań skonfigurowano środowisko testowe z wykorzystaniem maszyny wirtualnej z systemem Ubuntu, a następnie zainstalowano i skonfigurowano narzędzie antywirusowe ClamAV. Wykonano serię testów, w tym skanowanie plików testowych (np. EICAR), tworzenie własnych sygnatur oraz reguł YARA, a także aktywację ochrony w czasie rzeczywistym. Ćwiczenie miało na celu rozwinięcie umiejętności praktycznych w zakresie identyfikacji i analizy potencjalnych zagrożeń oraz automatyzacji działań defensywnych.

## 2. Realizacja ćwiczeń

### 2.1 Instalacja narzędzia ClamAV

Zainstalowano narzędzie ClamAV oraz zrestartowano usługi clamav-daemon oraz clamav-freshclam.



```
$ sudo apt install clamav clamav-daemon -y
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following packages were automatically installed and are no longer require
```

Rysunek 1. Proces instalacji narzędzia ClamAV



```
$ sudo systemctl restart clamav-daemon
sudo systemctl restart clamav-freshclam
```

Rysunek 2. Restart usług clamav-daemon oraz clamav-freshclam

### 2.2 Wstępny test pliku EICAR

Pobrano plik testowy EICAR TXT do folderu domyślnego – Downloads oraz uruchomiono skan narzędziem „clamscan” z opcją „multiscan” w lokalizacji domowej. Narzędzie ClamAV poprawnie zidentyfikowało zagrożenie



```
$ wget https://secure.eicar.org/eicar.com.txt -P ~/Downloads
--2025-05-17 16:07:55-- https://secure.eicar.org/eicar.com.txt
Resolving secure.eicar.org (secure.eicar.org)... 89.238.73.97, 2a00:1828:1000:2497::2
Connecting to secure.eicar.org (secure.eicar.org)|89.238.73.97|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 68 [text/plain]
Saving to: '/home/kali/Downloads/eicar.com.txt'

eicar.com.txt      100%[====>]          68  --.-KB/s   in 0s

2025-05-17 16:07:55 (149 MB/s) - '/home/kali/Downloads/eicar.com.txt' saved [68/68]
```

Rysunek 3. Proces pobierania pliku tekstowego EICAR

```

└─$ sudo clamscan --multiscan --fdpass /home/$(whoami)/Downloads
/home/kali/Downloads/eicar.com.txt: Win.Test.EICAR_HDB-1 FOUND

----- SCAN SUMMARY -----
Infected files: 1
Time: 0.028 sec (0 m 0 s)
Start Date: 2025:05:17 16:08:37
End Date: 2025:05:17 16:08:37

```

Rysunek 4. Proces uruchomienia narzędzia ClamAV

## 2.3 Wykrywanie sygnatury.

Utworzono plik testowy z przypadkową zawartością oraz wygenerowano sygnaturę SHA 256 dla tego pliku za pomocą narzędzia sigtool. Uruchomiono skan narzędziem clamscan w lokalizacji domowej, wczytując bazę utworzoną w poprzednim punkcie. Narzędzie ClamAV poprawnie zidentyfikowało zagrożenie.

```

(kali@kali)-[~]
└─$ echo "random content for testing" > ~/test.txt

```

Rysunek 5. Umieszczenie treści w pliku tekstowym

```

(kali@kali)-[~]
└─$ sigtool --sha256 ~/test.txt > ~/mydb.hdb

```

Rysunek 6. Wygenerowanie sygnatury dla pliku

```

(kali@kali)-[~]
└─$ clamscan --database=~/mydb.hdb ~/

Loading: 0s, ETA: 0s [=====] 1/1 sigs
Compiling: 0s, ETA: 0s [=====] 10/10 tasks

/home/kali/.face: OK
/home/kali/.vboxclient-display-svgx11-tty7-service.pid: OK
/home/kali/.bashrc: OK
/home/kali/.xsession-errors: OK
/home/kali/.vboxclient-draganddrop-tty7-control.pid: OK
/home/kali/.face.icon: Symbolic link
/home/kali/.profile: OK
/home/kali/.vboxclient-seamless-tty7-control.pid: OK
/home/kali/.Xauthority: OK
/home/kali/.vboxclient-hostversion-tty7-control.pid: OK
/home/kali/test.txt: test.txt.UNOFFICIAL FOUND
/home/kali/.dmrc: OK

```

Rysunek 7. Uruchomienie narzędzia clamscan

```

----- SCAN SUMMARY -----
Known viruses: 1
Engine version: 1.4.2
Scanned directories: 1
Scanned files: 24
Infected files: 1
Data scanned: 0.06 MB
Data read: 0.03 MB (ratio 1.88:1)
Time: 0.009 sec (0 m 0 s)
Start Date: 2025:05:17 17:37:25
End Date: 2025:05:17 17:37:25

```

Rysunek 8. Wynik skanu narzędziem clamscan

## 2.4 Wykrywanie pliku na podstawie reguły YARA

Utworzono regułę YARA i uruchomiono skan narzędziem clamscan wczytującym tę regułę. Narzędzie poprawnie zidentyfikowało zagrożenie.

```

GNU nano 7.2 /home/kali/yara_rules/teule.yar
rule TeuleRule {
  strings:
    $a = "random content for testing"
  condition:
    $a
}

```

Rysunek 9. Treść reguły YARA

```

(kali@kali)-[~/clamav/build]
$ clamscan --disable-cache --official-db-only=no --database=~/.empty_clamav_db --yara=~/.yara_rules/teule.yar ~/test.txt

Loading: 0s, ETA: 0s [=====] 1/1 sigs
Compiling: 0s, ETA: 0s [=====] 10/10 tasks

/home/kali/test.txt: OK

----- SCAN SUMMARY -----
Known viruses: 1
Engine version: 1.5.0-beta
Scanned directories: 0
Scanned files: 1
Infected files: 0
Data scanned: 0.00 MB
Data read: 0.00 MB (ratio 0.00:1)
Time: 0.012 sec (0 m 0 s)
Start Date: 2025:05:17 19:24:41
End Date: 2025:05:17 19:24:41

(kali@kali)-[~/clamav/build]
$

```

Rysunek 10. Uruchomienie narzędzia clamscan z regułą YARA

## 2.5 On-Access scanning

Sprawdzono działanie On-Access scanning, poprzez dodanie do pliku konfiguracyjnego clamd.conf opcji:

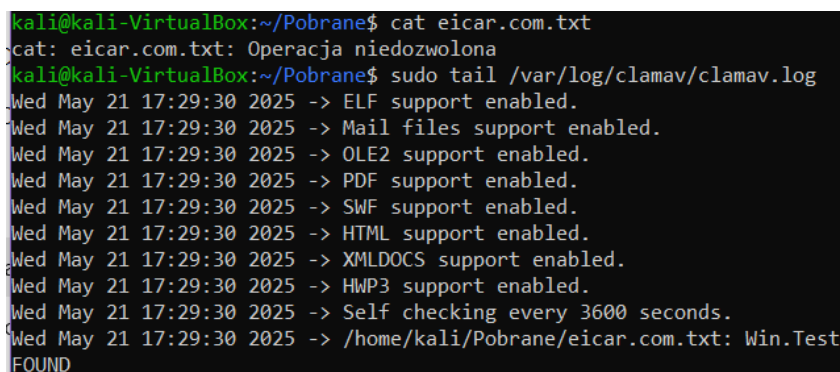
- *OnAccessIncludePath /home*
- *OnAccessExcludeUname clamav*
- *OnAccessPrevention yes*

Zrestartowano usługę „clamav-daemon” i uruchomiono proces On-Access scanning komendą *sudo clamavd -fdpass*. Następnie próbowano odczytać pobrany plik EICAR komendą „cat”, co dało poniższy efekt zamieszczony z fragmentu konsoli i na załączonym zrzucie ekranu. Również sprawdzono logi z „/var/log/clamav/clamav.log”.

```
kali@kali-VirtualBox:~/Pobrane$ cat eicar.com.txt
cat: eicar.com.txt: Operacja niedozwolona

kali@kali-VirtualBox:~/Pobrane$ sudo tail /var/log/clamav/clamav.log
Wed May 21 17:29:30 2025 -> ELF support enabled.
Wed May 21 17:29:30 2025 -> Mail files support enabled.
Wed May 21 17:29:30 2025 -> OLE2 support enabled.
Wed May 21 17:29:30 2025 -> PDF support enabled.
Wed May 21 17:29:30 2025 -> SWF support enabled.
Wed May 21 17:29:30 2025 -> HTML support enabled.
Wed May 21 17:29:30 2025 -> XMLDOCS support enabled.
Wed May 21 17:29:30 2025 -> HWP3 support enabled.
Wed May 21 17:29:30 2025 -> Self checking every 3600 seconds.
Wed May 21 17:29:30 2025 -> /home/kali/Pobrane/eicar.com.txt: Win.Test.EICAR_HDB-1(44d88612fea8a8f36de82e1278abb02f:68) FOUND

kali@kali-VirtualBox:~/Pobrane$
```



```
kali@kali-VirtualBox:~/Pobrane$ cat eicar.com.txt
cat: eicar.com.txt: Operacja niedozwolona
kali@kali-VirtualBox:~/Pobrane$ sudo tail /var/log/clamav/clamav.log
Wed May 21 17:29:30 2025 -> ELF support enabled.
Wed May 21 17:29:30 2025 -> Mail files support enabled.
Wed May 21 17:29:30 2025 -> OLE2 support enabled.
Wed May 21 17:29:30 2025 -> PDF support enabled.
Wed May 21 17:29:30 2025 -> SWF support enabled.
Wed May 21 17:29:30 2025 -> HTML support enabled.
Wed May 21 17:29:30 2025 -> XMLDOCS support enabled.
Wed May 21 17:29:30 2025 -> HWP3 support enabled.
Wed May 21 17:29:30 2025 -> Self checking every 3600 seconds.
Wed May 21 17:29:30 2025 -> /home/kali/Pobrane/eicar.com.txt: Win.Test.EICAR_HDB-1(44d88612fea8a8f36de82e1278abb02f:68) FOUND
FOUND
```

Rysunek 10. Próba uzyskania dostępu