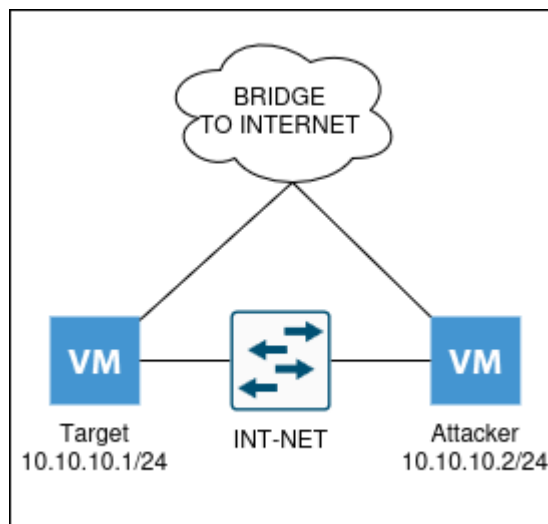


# Security: FTP Brute-force (Patator i CICFlowMeter)

## Schemat i opis środowiska testowego



Opis:

Środowisko składa się z dwóch maszyn wirtualnych (VM) działających na Ubuntu Server:

- Maszyna atakująca: uruchomiony program Patator do ataku brute-force na usługę FTP oraz tcpdump do przechwytywania ruchu.
- Maszyna ofiara: zainstalowany i skonfigurowany serwer FTP (vsftpd).
- Sieć: maszyny podłączone do tego samego switcha wirtualnego w Hyper-V.

Każda z Maszyn ma dysk o rozmiarze 8GB ([Wymagania minimalne ubuntu](#) mówią o minimalnie 5GB). Dyski są w formacie vhdx, wykorzystywanym przez hyper-v.

Dyski maszyn można pobrać z linka poniżej:

<https://1drv.ms/f/c/9dd28f74d9c48b45/EIEe6P0-WYpOmB3YukiRtzwBVGtNNW8QbW3jmy5V-9PWPQ?e=RLSO4>

Hasło do linka: Ostrowski19062025

## Oprogramowanie wykorzystane do wykonania eksperymentu

Komponent	Wersja	Nazwa
System operacyjny maszyn wirtualnych	24.04.2 LTS	Ubuntu Server
Hypervisor	Wersja: 10.0.26100.1882	Hyper-V
Serwer FTP	3.0.5	VSFTPD
Narzędzie ataku	1.0	Patator
Przechwytywanie ruchu	4.99.1	tcpdump

Komponent	Wersja	Nazwa
Analiza Ruchu	0.4.2	CICFlowMeter
Słownik do ataku	ok. 14 MB, 14344392 haseł	rockyou.txt

# Instalacja i konfiguracja

## Maszyna ofiara

```
administrator@target:~$ sudo apt update -y
[sudo] password for administrator:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
58 packages can be upgraded. Run 'apt list --upgradable' to see them.
administrator@target:~$ sudo apt install vsftpd -y
[LOGI Z INSTALACJI]
```

Zmiany w pliku konfiguracyjnym /etc/vsftpd.conf:

```
anonymous_enable=NO
local_enable=YES
write_enable=YES
listen=YES
listen_ipv6=NO
```

Tworzenie użytkownika FTP z hasłem a7s8d6a8s7d6a8s7d68s7:

```
administrator@target:~$ sudo adduser ftpuser
info: Adding user `ftpuser' ...
info: Selecting UID/GID from range 1000 to 59999 ...
info: Adding new group `ftpuser' (1001) ...
info: Adding new user `ftpuser' (1001) with group `ftpuser (1001)' ...
info: Creating home directory `/home/ftpuser' ...
info: Copying files from `/etc/skel' ...
New password:
Retype new password:
passwd: password updated successfully
Changing the user information for ftpuser
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
```

```
Other []:
Is the information correct? [Y/n] y
info: Adding new user `ftpuser' to supplemental / extra groups `users' ...
info: Adding user `ftpuser' to group `users' ...
administrator@target:~$
```

Restart usługi:

```
administrator@target:~$ sudo systemctl restart vsftpd
administrator@target:~$ sudo systemctl status vsftpd.service
● vsftpd.service - vsftpd FTP server
   Loaded: loaded (/usr/lib/systemd/system/vsftpd.service; enabled;
   preset: e>
   Active: active (running) since Thu 2025-06-19 15:00:47 UTC; 6s ago
   Process: 4065 ExecStartPre=/bin/mkdir -p /var/run/vsftpd/empty
   (code=exited>
   Main PID: 4068 (vsftpd)
     Tasks: 1 (limit: 4602)
    Memory: 704.0K (peak: 1.5M)
       CPU: 7ms
    CGroup: /system.slice/vsftpd.service
           └─4068 /usr/sbin/vsftpd /etc/vsftpd.conf

Jun 19 15:00:47 target systemd[1]: Starting vsftpd.service - vsftpd FTP
server.>
Jun 19 15:00:47 target systemd[1]: Started vsftpd.service - vsftpd FTP
server.
administrator@target:~$
```

## Maszyna atakująca

Instalacja Narzędzi:

```
administrator@attacker:~$ sudo apt update -y
[sudo] password for administrator:
Hit:1 http://security.ubuntu.com/ubuntu noble-security InRelease
Hit:2 http://archive.ubuntu.com/ubuntu noble InRelease
Hit:3 http://archive.ubuntu.com/ubuntu noble-updates InRelease
Hit:4 http://archive.ubuntu.com/ubuntu noble-backports InRelease
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
58 packages can be upgraded. Run 'apt list --upgradable' to see them.
administrator@attacker:~$ sudo apt install git python3-pip tcpdump -y
[TUTAJ LOGI Z INSTALACJI]
```

Przed instalacją patatora dodano repozytoria kali-linux do ubuntu.

Instalacja Patatora:

```
administrator@attacker:~$ sudo apt install patator -y  
[TUTAJ LOGI Z INSTALACJI]
```

Instalacja CICFlowMeter w wersji Python:

```
administrator@attacker:~/patator$ pip install cicflowmeter  
[TUTAJ LOGI Z INSTALACJI]
```

Pobranie słownika do ataku:

```
administrator@attacker:~$ wget  
https://github.com/danielmiessler/SecLists/raw/master/Passwords/Leaked-  
Databases/rockyou.txt.tar.gz  
--2025-06-19 15:19:13--  
https://github.com/danielmiessler/SecLists/raw/master/Passwords/Leaked-  
Databases/rockyou.txt.tar.gz  
Resolving github.com (github.com)... 140.82.121.3  
Connecting to github.com (github.com)|140.82.121.3|:443... connected.  
HTTP request sent, awaiting response... 302 Found  
Location:  
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/L  
eaked-Databases/rockyou.txt.tar.gz [following]  
--2025-06-19 15:19:14--  
https://raw.githubusercontent.com/danielmiessler/SecLists/master/Passwords/L  
eaked-Databases/rockyou.txt.tar.gz  
Resolving raw.githubusercontent.com (raw.githubusercontent.com)...  
185.199.109.133, 185.199.111.133, 185.199.110.133, ...  
Connecting to raw.githubusercontent.com  
(raw.githubusercontent.com)|185.199.109.133|:443... connected.  
HTTP request sent, awaiting response... 200 OK  
Length: 53291283 (51M) [application/octet-stream]  
Saving to: 'rockyou.txt.tar.gz'
```

```
rockyou.txt.tar.gz  
100%[=====]  
=====>] 50.82M 1.56MB/s in 32s
```

```
2025-06-19 15:19:48 (1.59 MB/s) - 'rockyou.txt.tar.gz' saved  
[53291283/53291283]
```

```
administrator@attacker:~$ tar -xzf rockyou.txt.tar.gz  
administrator@attacker:~$ wc -l rockyou.txt #liczba haseł około 14 milionów  
14344391 rockyou.txt  
administrator@attacker:~$ head rockyou.txt #pierwsze wpisy w pliku  
123456  
12345  
123456789  
password  
iloveyou  
princess
```

```
1234567
rockyou
12345678
abc123
```

## Test Komunikacji

Ping:

```
administrator@target:~$ ping 10.10.10.2
PING 10.10.10.2 (10.10.10.2) 56(84) bytes of data.
64 bytes from 10.10.10.2: icmp_seq=1 ttl=64 time=0.180 ms
64 bytes from 10.10.10.2: icmp_seq=2 ttl=64 time=0.229 ms
64 bytes from 10.10.10.2: icmp_seq=3 ttl=64 time=0.269 ms
64 bytes from 10.10.10.2: icmp_seq=4 ttl=64 time=0.286 ms
64 bytes from 10.10.10.2: icmp_seq=5 ttl=64 time=0.266 ms
64 bytes from 10.10.10.2: icmp_seq=6 ttl=64 time=0.293 ms
64 bytes from 10.10.10.2: icmp_seq=7 ttl=64 time=0.284 ms
^C
--- 10.10.10.2 ping statistics ---
7 packets transmitted, 7 received, 0% packet loss, time 6182ms
rtt min/avg/max/mdev = 0.180/0.258/0.293/0.037 ms
administrator@target:~$
```

FTP:

```
administrator@attacker:~$ ftp 10.10.10.1
Connected to 10.10.10.1.
220 (vsFTPd 3.0.5)
Name (10.10.10.1:administrator): ftpuser
331 Please specify the password.
Password:
230 Login successful.
Remote system type is UNIX.
Using binary mode to transfer files.
ftp> dir
229 Entering Extended Passive Mode (|||8296|)
150 Here comes the directory listing.
226 Directory send OK.
ftp>
```

## Przeprowadzenie Ataku

W jednej sesji terminala uruchomienie przechwytywania:

```
sudo tcpdump -i eth1 port 21 -w ftp_attack.pcap
```

W drugiej sesji terminala atak Patator:

```
administrator@attacker:~$ patator ftp_login host=10.10.10.1 user=ftpuser
password=FILE0 0=rockyou.txt -x ignore:mesg='Login incorrect' --rate-
limit=50
15:39:45 patator INFO - Starting Patator 1.0
(https://github.com/lanjelot/patator) with python-3.12.3 at 2025-06-19 15:39
UTC
15:39:45 patator INFO -
15:39:45 patator INFO - code size time | candidate
| num | mesg
15:39:45 patator INFO - -----
-----
15:40:38 patator INFO - 530 16 2.772 | 123456
| 1 | Login incorrect.
15:40:38 patator INFO - 530 16 2.778 | 12345
| 2 | Login incorrect.
15:40:38 patator INFO - 530 16 2.785 | 123456789
| 3 | Login incorrect.
15:40:38 patator INFO - 530 16 2.770 | password
| 4 | Login incorrect.
15:40:38 patator INFO - 530 16 2.770 | iloveyou
| 5 | Login incorrect.
15:40:38 patator INFO - 530 16 2.786 | princess
| 6 | Login incorrect.
15:40:38 patator INFO - 530 16 2.776 | 1234567
| 7 | Login incorrect.
15:40:38 patator INFO - 530 16 2.773 | rockyou
| 8 | Login incorrect.
15:40:38 patator INFO - 530 16 2.784 | 12345678
| 9 | Login incorrect.
15:40:38 patator INFO - 530 16 2.778 | abc123
| 10 | Login incorrect.
[TUTAJ CIĄGNIE SIĘ DALEJ]
```

- `--rate-limit=50`: ogranicza tempo ataku do 50 prób/sekundę (by nie przytłoczyć serwera)
- `rockyou.txt`: używa ogólnodostępnego słownika



W tym przypadku atak się nie powiedzie, ponieważ utworzone hasło nie znajduje się w `rockyou.txt` – i o to właśnie chodzi: chodzi o symulację nieudanego ataku, który będzie wyraźnie widoczny w ruchu.

# Efekty Ataku

## Po stronie atakującej

- Konsola Patatora wykaże tysiące nieudanych prób.
- Hasło nie zostanie złamane.
- Cały ruch jest zapisany w ftp\_attack.pcap.

## Po stronie serwera FTP

Fragment logu z /var/log/vsftpd.log:

```
administrator@target:~$ sudo tail -f /var/log/vsftpd.log
[sudo] password for administrator:
Thu Jun 19 15:27:39 2025 [pid 6752] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:27:50 2025 [pid 6751] [ftpuser] OK LOGIN: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7001] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7003] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7005] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7007] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7009] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7011] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7013] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7015] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7017] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:35 2025 [pid 7019] CONNECT: Client "10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7000] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7006] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7002] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7008] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7004] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7014] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7012] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7010] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7016] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
Thu Jun 19 15:40:37 2025 [pid 7018] [ftpuser] FAIL LOGIN: Client
"10.10.10.2"
```

```
Thu Jun 19 15:41:30 2025 [pid 7006] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7000] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7008] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7002] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7012] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7014] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7004] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7010] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7016] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:41:30 2025 [pid 7018] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7006] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7008] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7002] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7000] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7012] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7010] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7004] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7014] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7018] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
Thu Jun 19 15:42:23 2025 [pid 7016] [ftpuser] FAIL LOGIN: Client "10.10.10.2"  
[TUTAJ CIĄGNIE SIĘ DALEJ]
```

Pełna wersja logów do pobrania [vsftpd\\_copy.log](#)

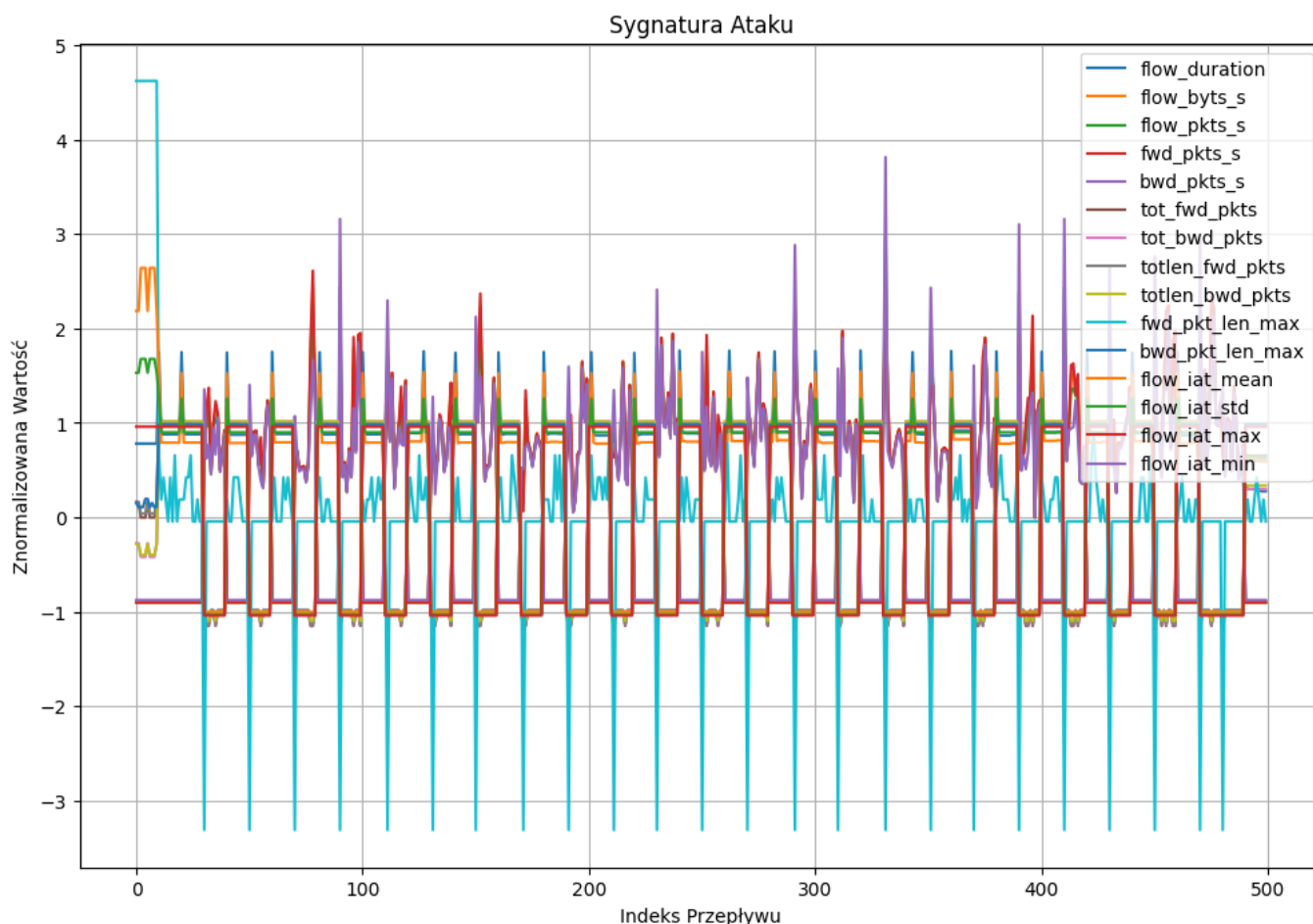
 Po 765 próbach (~122min) zatrzymano eksperyment

# Użycie CICFlowMeter (Python) i ekstrakcja cech

```
administrator@attacker:~$ cicflowmeter -f ftp_attack.pcap -c ftp_attack.csv
reading from file ftp_attack.pcap, link-type EN10MB (Ethernet), snapshot
length 262144
administrator@attacker:~$ ls -lah
total 186M
drwxr-x--- 7 administrator administrator 4.0K Jun 19 17:16 .
drwxr-xr-x 3 root root 4.0K Jun 19 15:07 ..
-rw----- 1 administrator administrator 1.1K Jun 19 15:25 .bash_history
-rw-r--r-- 1 administrator administrator 220 Mar 31 2024 .bash_logout
-rw-r--r-- 1 administrator administrator 3.7K Mar 31 2024 .bashrc
drwx----- 4 administrator administrator 4.0K Jun 19 17:15 .cache
drwx----- 2 administrator administrator 4.0K Jun 19 17:15 .config
-rw-rw-r-- 1 administrator administrator 263K Jun 19 17:16 ftp_attack.csv
-rw-r--r-- 1 tcpdump tcpdump 750K Jun 19 17:09 ftp_attack.pcap
drwxrwxr-x 7 administrator administrator 4.0K Jun 19 15:13 patator
-rw-r--r-- 1 administrator administrator 807 Mar 31 2024 .profile
-rw----- 1 administrator administrator 134M Sep 23 2015 rockyou.txt
-rw-rw-r-- 1 administrator administrator 51M Jun 19 15:19
rockyou.txt.tar.gz
drwx----- 2 administrator administrator 4.0K Jun 19 15:07 .ssh
-rw-r--r-- 1 administrator administrator 0 Jun 19 15:08
.sudo_as_admin_successful
drwxrwxr-x 6 administrator administrator 4.0K Jun 19 15:16 venv_patator
-rw-rw-r-- 1 administrator administrator 215 Jun 19 15:19 .wget-hsts
-rw----- 1 administrator administrator 108 Jun 19 15:25 .Xauthority
administrator@attacker:~$ cat ftp_attack.csv
src_ip,dst_ip,src_port,dst_port,protocol,timestamp,flow_duration,flow_byts_s
,flow_pkts_s,fwd_pkts_s,bwd_pkts_s,tot_fwd_pkts,tot_bwd_pkts,totlen_fwd_pkts
,totlen_bwd_pkts,fwd_pkt_len_max,fwd_pkt_len_min,fwd_pkt_len_mean,fwd_pkt_le
n_std,bwd_pkt_len_max,bwd_pkt_len_min,bwd_pkt_len_mean,bwd_pkt_len_std,pkt_l
en_max,pkt_len_min,pkt_len_mean,pkt_len_std,pkt_len_var,fwd_header_len,bwd_h
eader_len,fwd_seg_size_min,fwd_act_data_pkts,flow_iat_mean,flow_iat_max,flow
_iat_min,flow_iat_std,fwd_iat_tot,fwd_iat_max,fwd_iat_min,fwd_iat_mean,fwd_i
at_std,bwd_iat_tot,bwd_iat_max,bwd_iat_min,bwd_iat_mean,bwd_iat_std,fwd_psh_
flags,bwd_psh_flags,fwd_urg_flags,bwd_urg_flags,fin_flag_cnt,syn_flag_cnt,rs
t_flag_cnt,psh_flag_cnt,ack_flag_cnt,urg_flag_cnt,ece_flag_cnt,down_up_ratio
,pkt_size_avg,init_fwd_win_byts,init_bwd_win_byts,active_max,active_min,acti
ve_mean,active_std,idle_max,idle_min,idle_mean,idle_std,fwd_byts_b_avg,fwd_p
kts_b_avg,bwd_byts_b_avg,bwd_pkts_b_avg,fwd_blk_rate_avg,bwd_blk_rate_avg,fw
d_seg_size_avg,bwd_seg_size_avg,cwr_flag_count,subflow_fwd_pkts,subflow_bwd_
pkts,subflow_fwd_byts,subflow_bwd_byts
10.10.10.1,10.10.10.2,21,37852,6,2025-06-19
15:41:31,103.324816,12.12680601337824,0.1645296905246848,0.09678217089687341
,0.06774751962781139,10,7,736,517,100,54,73.6,15.226293048539425,81,66,73.85
714285714286,6.854166020511517,100,54,73.70588235294117,12.479464099930464,1
```



```
'totlen_bwd_pkts',  
    'fwd_pkt_len_max', 'bwd_pkt_len_max', 'flow_iat_mean',  
'flow_iat_std',  
    'flow_iat_max', 'flow_iat_min']  
df_selected = df[features]  
  
# Normalizacja danych (opcjonalnie)  
df_normalized = (df_selected - df_selected.mean()) / df_selected.std()  
  
# Wizualizacja  
plt.figure(figsize=(12, 8))  
for feature in df_normalized.columns:  
    plt.plot(df_normalized.index, df_normalized[feature],  
            label=feature)  
plt.title('Sygnatura Ataku')  
plt.xlabel('Indeks Przepływu')  
plt.ylabel('Znormalizowana Wartość')  
plt.legend()  
plt.grid(True)  
plt.show()
```



# Wnioski

- Skuteczność ataku brute-force zależy od słownika – jeśli hasło użytkownika nie jest w słowniku, atak się nie powiedzie, choć nadal generuje duży ruch i może zostać wykryty.
- Monitorowanie logów serwera FTP jest kluczowe – logi wyraźnie pokazują wielokrotne, nieudane próby logowania, co pozwala administratorowi wykryć próbę ataku.
- Przechwytywanie i analiza ruchu (tcpdump + CICFlowMeter) – umożliwiają szczegółową analizę zachowania sieci podczas ataku, co może być wykorzystane do budowy systemów wykrywania włamań (IDS).
- Ograniczenie szybkości ataku (-rate-limit=50) – jest istotne, aby nie przeciążyć serwera i lepiej symulować realistyczne warunki ataku.
- Silne, losowe hasło zabezpiecza konto – stosowanie silnych haseł, które nie występują w popularnych słownikach, jest podstawową ochroną przed atakami brute-force.
- Środowisko testowe oparte na VM i Hyper-V – pozwala na bezpieczne i kontrolowane przeprowadzanie eksperymentów bezpieczeństwa.