



Know your tools: Ansible + OpenSSH

Dariusz Puchalak



Ansible

Ansible

- silnik do automatyzacji systemów IT.
- konfiguracja
- wdrożenia
- zmiany

Małe wymagania.

- Python 2.x (ale niedługo 3.x)
- SSH
- Brak agentów.

Komunikacja - SSH

- Tak samo jak administrator (od strony sieciowej nic się nie zmienia!)
- Natywny bardzo mocny mechanizm (OpenSSH)
- Bezagentowy.



OpenSSH

Uwierzytelnianie == OpenSSH

- password,
- hostbased,
- publickey,
- Keyboard-interactive
- PAM
- keyboard-interactive:pam



Ansible + OpenSSH

OpenSSH patterns

Host *.puchalak.???

IdentityFile ~/.ssh/id_puchalak

IdentitiesOnly yes

PreferredAuthentications publickey,password

Ansible patterns

```
~(web|db).*\.example\.com
```

```
webservers[0:1]
```

Połączenie przez komputer pośredni

```
.ssh/config
```

```
...
```

```
Host hostB
```

```
    ProxyCommand ssh hostA nc %h %p
```

```
    HostName 10.1.8.31
```

```
Host hostA
```

```
    HostName 172.16.48.10
```

```
...
```

```
bash$ ssh hostB
```

Połączenie przez proxy WWW

Gdy trzeba się uwierzytelnić do serwera proxy:

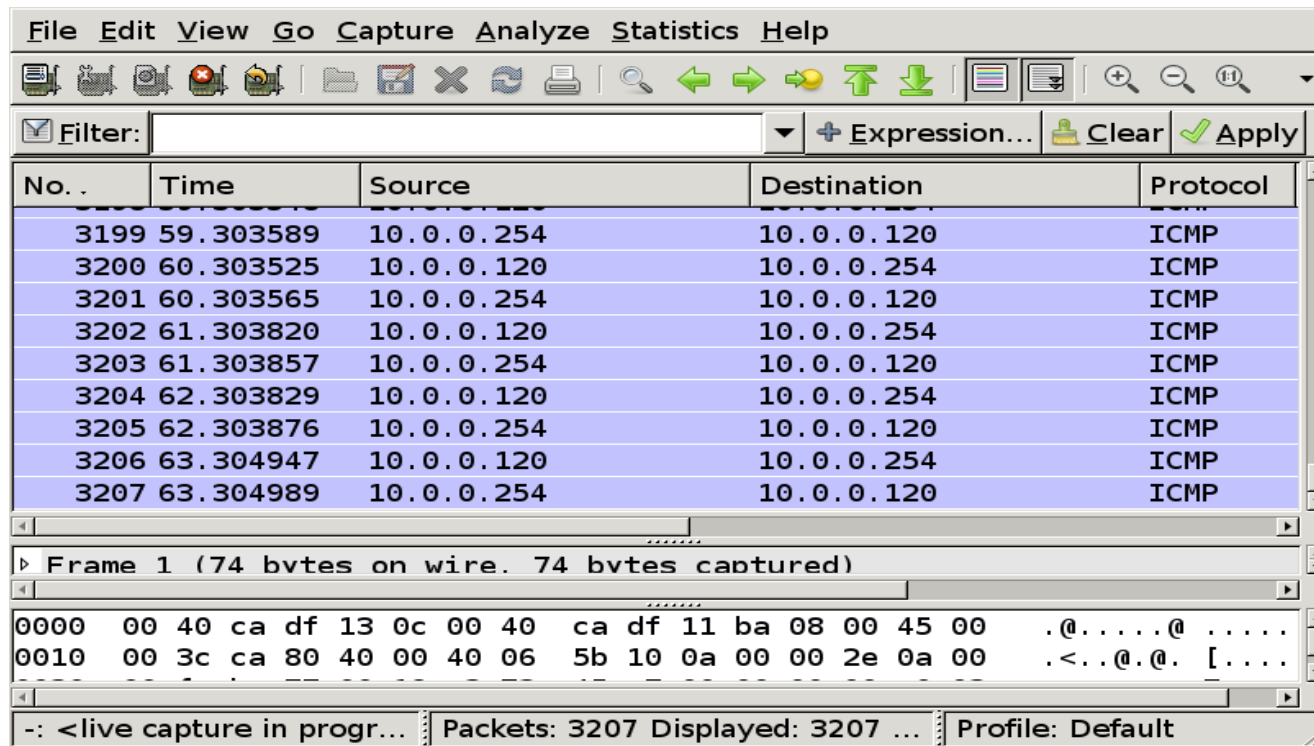
```
ProxyCommand nc -X connect -x  
192.168.1.1:8080 %h %p
```

```
netcat -X proxy_protocol
```

Supported protocols are ... “connect” (HTTPS proxy).

Zdalne przechwytywanie ruchu sieciowego.

```
ssh root@10.0.0.254 "tcpdump -l -n -s 0 -w - not port 22" | wireshark -i -
```



The screenshot shows the Wireshark interface with a packet capture of ICMP traffic. The main display area shows a list of 10 packets, all of which are ICMP. The source and destination IP addresses alternate between 10.0.0.254 and 10.0.0.120. The status bar at the bottom indicates that 3207 packets were captured and all 3207 are displayed.

No. .	Time	Source	Destination	Protocol
3199	59.303589	10.0.0.254	10.0.0.120	ICMP
3200	60.303525	10.0.0.120	10.0.0.254	ICMP
3201	60.303565	10.0.0.254	10.0.0.120	ICMP
3202	61.303820	10.0.0.120	10.0.0.254	ICMP
3203	61.303857	10.0.0.254	10.0.0.120	ICMP
3204	62.303829	10.0.0.120	10.0.0.254	ICMP
3205	62.303876	10.0.0.254	10.0.0.120	ICMP
3206	63.304947	10.0.0.120	10.0.0.254	ICMP
3207	63.304989	10.0.0.254	10.0.0.120	ICMP

Frame 1 (74 bytes on wire (74 bytes captured) on interface eth0):

```
0000  00 40 ca df 13 0c 00 40  ca df 11 ba 08 00 45 00  .@.....@ .....
0010  00 3c ca 80 40 00 40 06  5b 10 0a 00 00 2e 0a 00  .<..@.@. [...
```

-: <live capture in progr... | Packets: 3207 Displayed: 3207 ... | Profile: Default

Opcje

OpenSSH w wersji 6.7 posiada 42 przełączniki dostępne z linii poleceń.

Jak się w tym wszystkim połączyć?

\$HOME/.ssh/config

Host router

Hostname 192.168.1.1

Port 2022

User root

Ciphers aes256-cbc

MACs hmac-sha1

LocalForward

```
$HOME/.ssh/config
```

```
Host corp-remote
```

```
    HostName XXX.corp.pl
```

```
    LocalForward 1100 mail.int.corp:110
```

```
    LocalForward 1025 mail.int.corp:25
```

```
    LocalForward 1143 mail.int.corp:143
```

```
$ ssh corp-remote
```

```
Klient poczty skonfigurowany na:
```

```
POP3 localhost:1100
```

```
IMAP localhost:1143
```

```
SMTP localhost:1025
```


RemoteForward

RemoteForward 65020 127.0.0.1:22

Własny serwer proxy

DynamicForward 1080

Socks4/Socks5 proxy on localhost:1080

ssh remote.site.pl

Go to any site with „your address is” and you are connected from:

remote.site.pl

OpenSSH dla kolegów/koleżanek/...

GatewayPorts yes

GatewayPorts clientspecified

...

RemoteForward przecieki.pl:2080 internal.corp.pl:80

...

GatewayPorts no

RemoteForward [localhost]:2080

LocalForward [localhost]:1080

DynamicForward [localhost:1080

RDP w tunelu SSH

Host Live

Hostname 192.168.100.250

User puchalakd

LocalForward 3137 localhost:3389

PermitLocalCommand yes

LocalCommand rdesktop -c -xm -D -K -z -u puchalakd
-p TAJNEHASŁO -k pl -g 1024x768 localhost:3137 &

ProxyCommand ssh posrednik nc %h %p sleep 1

ConnectTimeout 10

Nowa jakość

Host unison

User puchalakd

Match Host unison exec "host -t A unison.net.puchalak"

HostName unison.net.puchalak

Host unison

HostName 192.168.1.125

ProxyCommand ssh pluton-remote nc %h %p

Nowa jakość

```
* * * * * flock -w 0 -n /root/.call.back ssh -i /root/.call.back  
-o BatchMode=yes -o ExitOnForwardFailure=yes -o  
StrictHostKeyChecking=no -R 12345:localhost:22  
puchalakd@somewhere.internet || exit 0
```

Host private.behind.nat

HostName 127.0.0.1

Port 12345

ProxyCommand ssh pluton-remote nc %h %p

Tylko jedno połączenie

Host *

ControlMaster auto

ControlPath ~/.ssh/ControlPath/%C

ControlPersist yes

SSHFS

Network filesystem using SSH
(Needs FUSE)

SSHFS

```
sshfs mirror:/mnt ~/mnt/
```

```
mirror:/mnt 6801418 4945780 1855639 73% /home/.../mnt
```



Ansible

ansible uruchamianie jednorazowo

```
ansible -m setup HOST
```

```
ansible -m raw -a 'apt-get install python-apt' -u root  
ovh
```

```
ansible -m service -u rootdp -a 'state=restarted  
name=sshd' ovh
```

```
ansible-doc -l | less
```

```
ansible-doc -m service
```



Łączymy to co znamy.



Pytania?
Dariusz.Puchalak@osec.pl