



Know your tools:
OpenSSH+Ansible
tips and tricks.

Dariusz Puchalak



Dariusz Puchalak

- 20+ lat Linux/Unix Sysadmin
- 9+ lat trener
- 2+ lat w OSEC

<http://www.OSEC.pl>

- Od 2009 na rynku
- doświadczona kadra (ACNI, RHCA)
- specjalizacja open-source
- subskrypcje, szkolenia, konsultacje



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.

Uwierzytelnianie == OpenSSH

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

Podnoszenie uprawnień.

become_method:

- sudo
- su
- pbrun
- pfexec
- doas
- dzdo
- ksu



Playbooks - demo



Roles == code reuse.



Variables



Conditionals





Windows - winrm

Ustawić zmienne:

ansible_hosts: windows

ansible_user: Administrator

ansible_password: Pa\$\$w0rd

ansible_port: 5986

ansible_connection: winrm

when using default WinRM self-signed certificates:

ansible_winrm_server_cert_validation: ignore



Vmware?



roles - ubiquity*

OpenSSH patterns

Host *.puchalak.???

IdentityFile ~/.ssh/id_puchalak

IdentitiesOnly yes

PreferredAuthentications publickey,password

Ansible patterns

```
~(web|db).*\.example\.com  
webservers[0:1]
```



O jeden host za daleko...

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).



Łączymy to co znamy.

Nowa jakość

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 192.168.1.125

ProxyCommand ssh pluton-remote nc %h %p

Host unison

HostName unison.net.puchalak

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

