TP Contôle R405

1 Consignes

- Tous documents autorisés.
- IA non autorisées
- Échanges interdits (portables rangés,montres connectées rangées, silence exigé. Si vous avez fini, merci de sortir en silence.)
- Un compte-rendu est à rendre sur Moodle. Il contiendra votre code et une "sortie" montrant son exécution réussi. La sortie doit faire apparaître l'heure et le nom de votre PC.

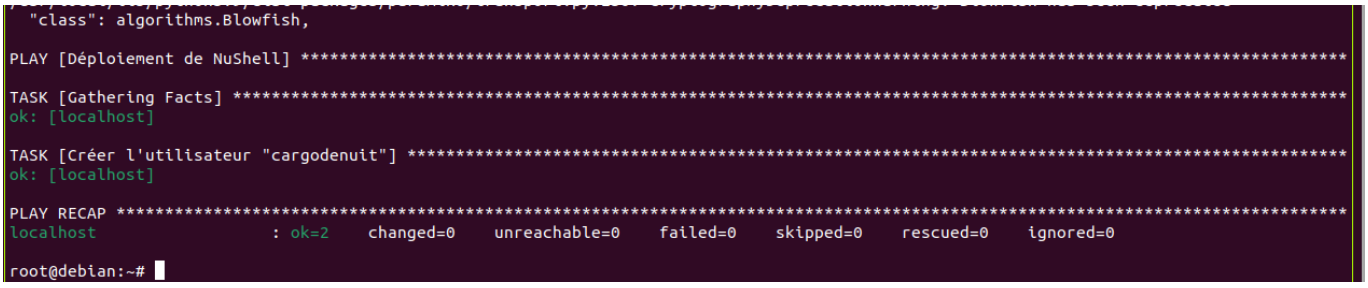
2 Création d'un playbook Ansible pour déployer des outils écrits en Rust comme NuShell

```
---
- name: Déploiement de NuShell
  hosts: localhost
  become: true

  tasks:
    - name: Créer l'utilisateur "cargodenuit"
      user:
        name: cargodenuit
        state: present
```

root@debian:~# id cargodenuit uid=1002(cargodenuit) gid=1002(cargodenuit) groupes=1002(cargodenuit)

root@debian:~# ls /home/ ansible/ bin/ cargodenuit/ student/ vagrant/



2.

```
---
- name: to nushell
  hosts: localhost
  become: yes
  become_user: cargodenuit

  tasks:
    - name: dl RUST
```

```
        get_url:
          url: https://sh.rustup.rs
          dest: /home/cargodenuit/rustup.sh
          mode: '0755'

      - name: exec RUST
        command: /home/cargodenuit/rustup.sh -y
        args:
          creates: /home/cargodenuit/.cargo/bin/rustup

      - name: add PATH
        lineinfile:
          dest: /home/cargodenuit/.bashrc
          line: 'export PATH="$HOME/.cargo/bin:$PATH"'
```

```
/usr/local/lib/python3.9/dist-packages/paramiko/transport.py:236: CryptographyDeprecationWarning: Blowfish has been deprecated
  "class": algorithms.Blowfish,
ansible-playbook [core 2.12.5]
  config file = /etc/ansible/ansible.cfg
  configured module search path = ['/root/.ansible/plugins/modules', '/usr/share/ansible/plugins/modules']
  ansible python module location = /usr/local/lib/python3.9/dist-packages/ansible
  ansible collection location = /root/.ansible/collections:/usr/share/ansible/collections
  executable location = /usr/local/bin/ansible-playbook
  python version = 3.9.2 (default, Feb 28 2021, 17:03:44) [GCC 10.2.1 20210110]
  jinja version = 2.11.3
  libyaml = True
Using /etc/ansible/ansible.cfg as config file
Skipping callback 'default', as we already have a stdout callback.
Skipping callback 'minimal', as we already have a stdout callback.
Skipping callback 'oneline', as we already have a stdout callback.

PLAYBOOK: exo2.yml *************************************************************************************************************************************
1 plays in exo2.yml

PLAY [to nushell] **************************************************************************************************************************************

TASK [Gathering Facts] *********************************************************************************************************************************
task path: /root/exo2.yml:2
ok: [localhost]
META: ran handlers

TASK [dl RUST] *****************************************************************************************************************************************
task path: /root/exo2.yml:8
changed: [localhost] => {"changed": true, "checksum_dest": null, "checksum_src": "72f55ae2b071e609af821a1b448d35525358d753", "dest": "/home
/cargodenuit/rustup.sh", "elapsed": 1, "gid": 1002, "group": "cargodenuit", "md5sum": "9457a47bb675d495b53d2ebbb757f63d", "mode": "0755", "
msg": "OK (23159 bytes)", "owner": "cargodenuit", "size": 23159, "src": "/home/cargodenuit/.ansible/tmp/ansible-moduletmp-1686235679.450435
6-e22ldii8/tmpathiq8a8", "state": "file", "status_code": 200, "uid": 1002, "url": "https://sh.rustup.rs"}

TASK [exec RUST] ***************************************************************************************************************************************
task path: /root/exo2.yml:14
ok: [localhost] => {"changed": false, "cmd": ["/home/cargodenuit/rustup.sh", "-y"], "delta": null, "end": null, "msg": "Did not run command
 since '/home/cargodenuit/.cargo/bin/rustup' exists", "rc": 0, "start": null, "stderr": "", "stderr_lines": [], "stdout": "skipped, since /
home/cargodenuit/.cargo/bin/rustup exists", "stdout_lines": ["skipped, since /home/cargodenuit/.cargo/bin/rustup exists"]}

TASK [add PATH] ****************************************************************************************************************************************
task path: /root/exo2.yml:19
ok: [localhost] => {"backup": "", "changed": false, "msg": ""}
META: ran handlers
META: ran handlers

PLAY RECAP *********************************************************************************************************************************************
localhost                  : ok=4    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

1.

```
---
- name: Deploie Nushell
  hosts: localhost
  vars:
    utilisateur: cargodenuit
  become: true
  become_user: "{{ utilisateur }}"
  tasks:
    - name: change le nom de mon pc
```

```
      command: hostnamectl set-hostname pc-julien

    - name: rust script
      get_url:
        url: https://sh.rustup.rs
        dest: /tmp/rustup.sh
        mode: '0755'

    - name: Installation de Rust
      shell: /tmp/rustup.sh -y
      args:
        executable: /bin/bash
```

4.

```
---
- name: Deploie Nushell
  hosts: localhost
  vars:
    utilisateur: cargodenuit
    chemin_cargo: /usr/bin/cargo
    chemin_nushell: /home/{{ utilisateur }}/.cargo/bin/nu
  become: true
  become_user: "{{ utilisateur }}"
  tasks:
    - name: Installation de NuShell
      environment:
        HOME: "/home/{{ utilisateur }}"
      shell: |
        {{ chemin_cargo }} install nu --root "{{ chemin_cargo }}"
        export PATH=$PATH:{{ chemin_nushell }}
        echo 'export PATH="$PATH:{{ chemin_nushell }}"' >> /home/{{
utilisateur }}/.bashrc
      args:
        executable: /bin/bash
```

Tentative update de cargo suite à un problème : cargo install cargo-update && cargo install-update -a

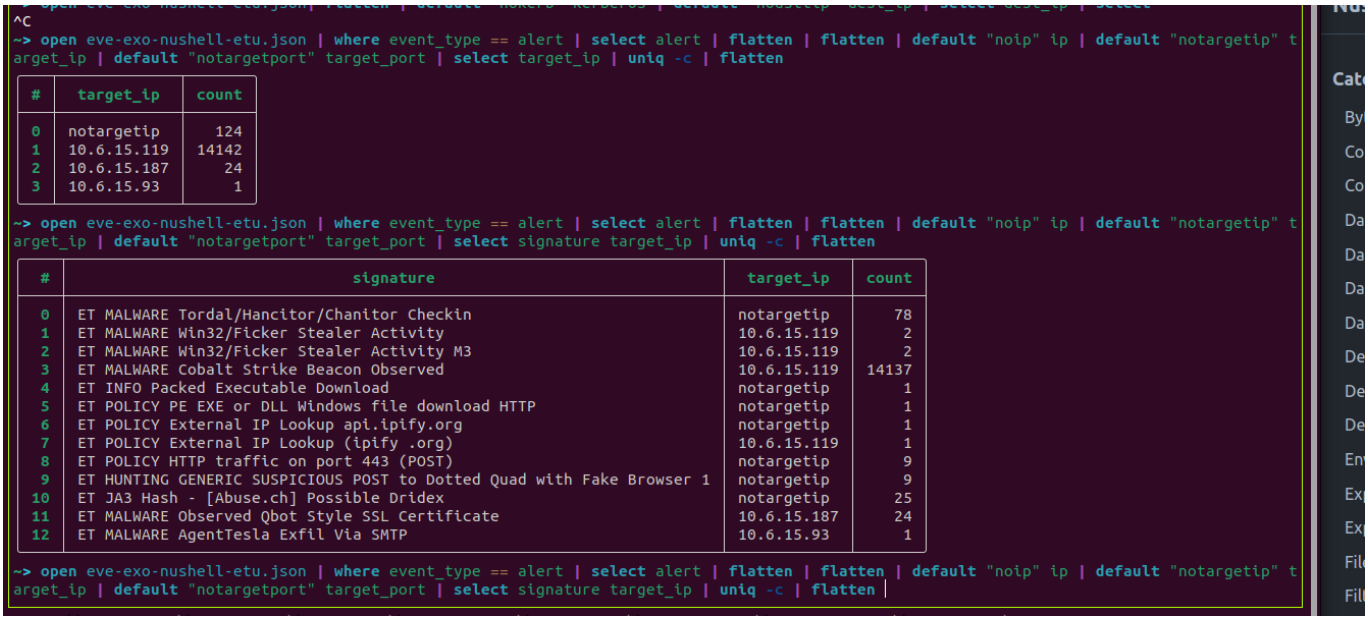
Apres plusieurs test toujour une erreur pour la 4.

3 Utilisation de NuShell dans le domaine de la cybersécurité

1. open eve-exo-nushell-etu.json | where event_type == alert | select alert | flatten | flatten | default "noip" ip | default "notargetip" target_ip | default "notargetport" target_port | select target_ip | uniq -c | flatten

2. open eve-exo-nushell-etu.json | where event_type == alert | select alert | flatten | flatten | default "noip" ip | default "notargetip" target_ip | default "notargetport" target_port | select signature target_ip | uniq -c | flatten

Réponse de la 1 et 2 :



```
^C
~> open eve-exo-nushell-etu.json | where event_type == alert | select alert | flatten | flatten | default "noip" ip | default "notargetip" t
arget_ip | default "notargetport" target_port | select target_ip | uniq -c | flatten
```

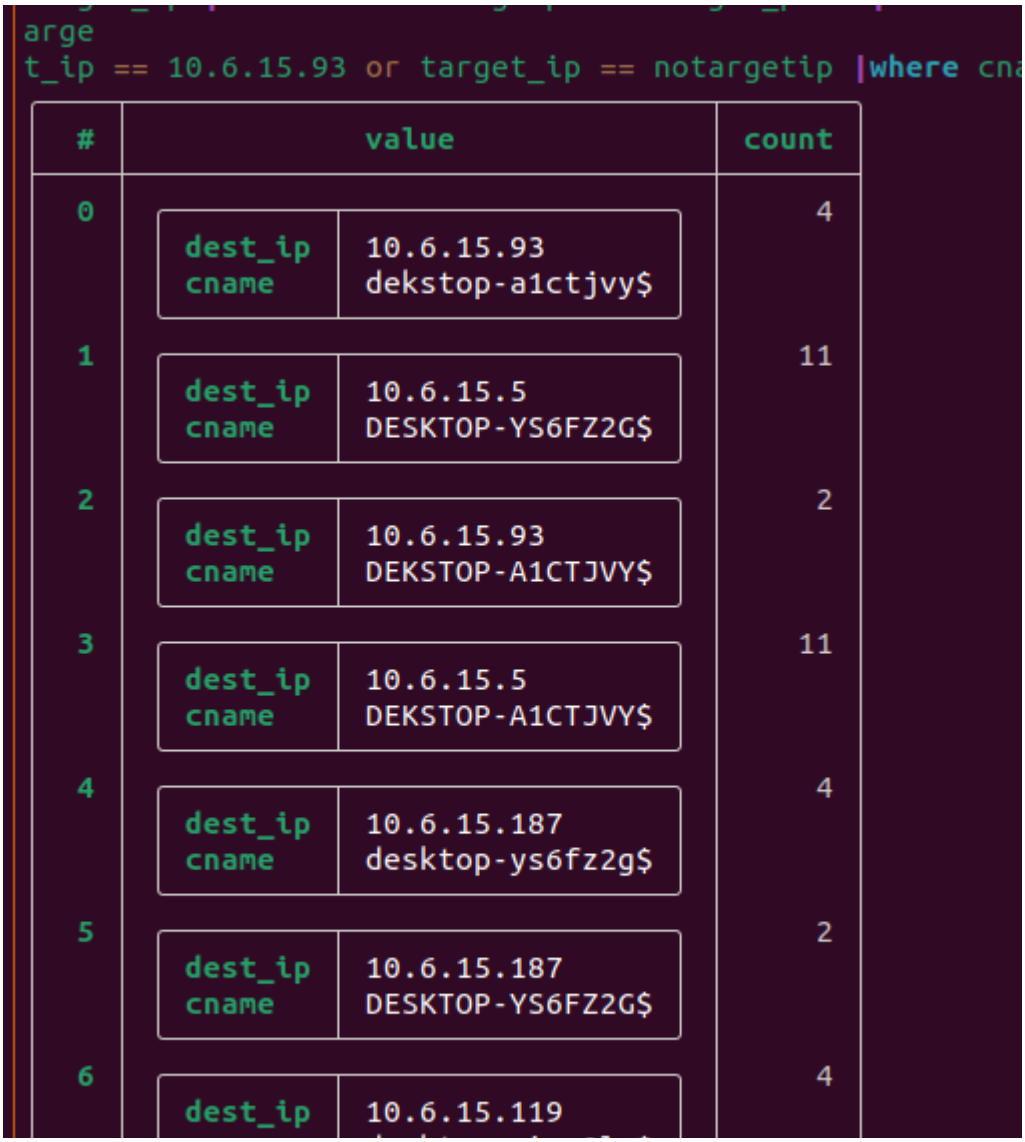
#	target_ip	count
0	notargetip	124
1	10.6.15.119	14142
2	10.6.15.187	24
3	10.6.15.93	1

```
~> open eve-exo-nushell-etu.json | where event_type == alert | select alert | flatten | flatten | default "noip" ip | default "notargetip" t
arget_ip | default "notargetport" target_port | select signature target_ip | uniq -c | flatten
```

#	signature	target_ip	count
0	ET MALWARE Tordal/Hancitor/Chanitor Checkin	notargetip	78
1	ET MALWARE Win32/Ficker Stealer Activity	10.6.15.119	2
2	ET MALWARE Win32/Ficker Stealer Activity M3	10.6.15.119	2
3	ET MALWARE Cobalt Strike Beacon Observed	10.6.15.119	14137
4	ET INFO Packed Executable Download	notargetip	1
5	ET POLICY PE EXE or DLL Windows file download HTTP	notargetip	1
6	ET POLICY External IP Lookup api.ipify.org	notargetip	1
7	ET POLICY External IP Lookup (ipify .org)	10.6.15.119	1
8	ET POLICY HTTP traffic on port 443 (POST)	notargetip	9
9	ET HUNTING GENERIC SUSPICIOUS POST to Dotted Quad with Fake Browser 1	notargetip	9
10	ET JA3 Hash - [Abuse.ch] Possible Dridex	notargetip	25
11	ET MALWARE Observed Qbot Style SSL Certificate	10.6.15.187	24
12	ET MALWARE AgentTesla Exfil Via SMTP	10.6.15.93	1

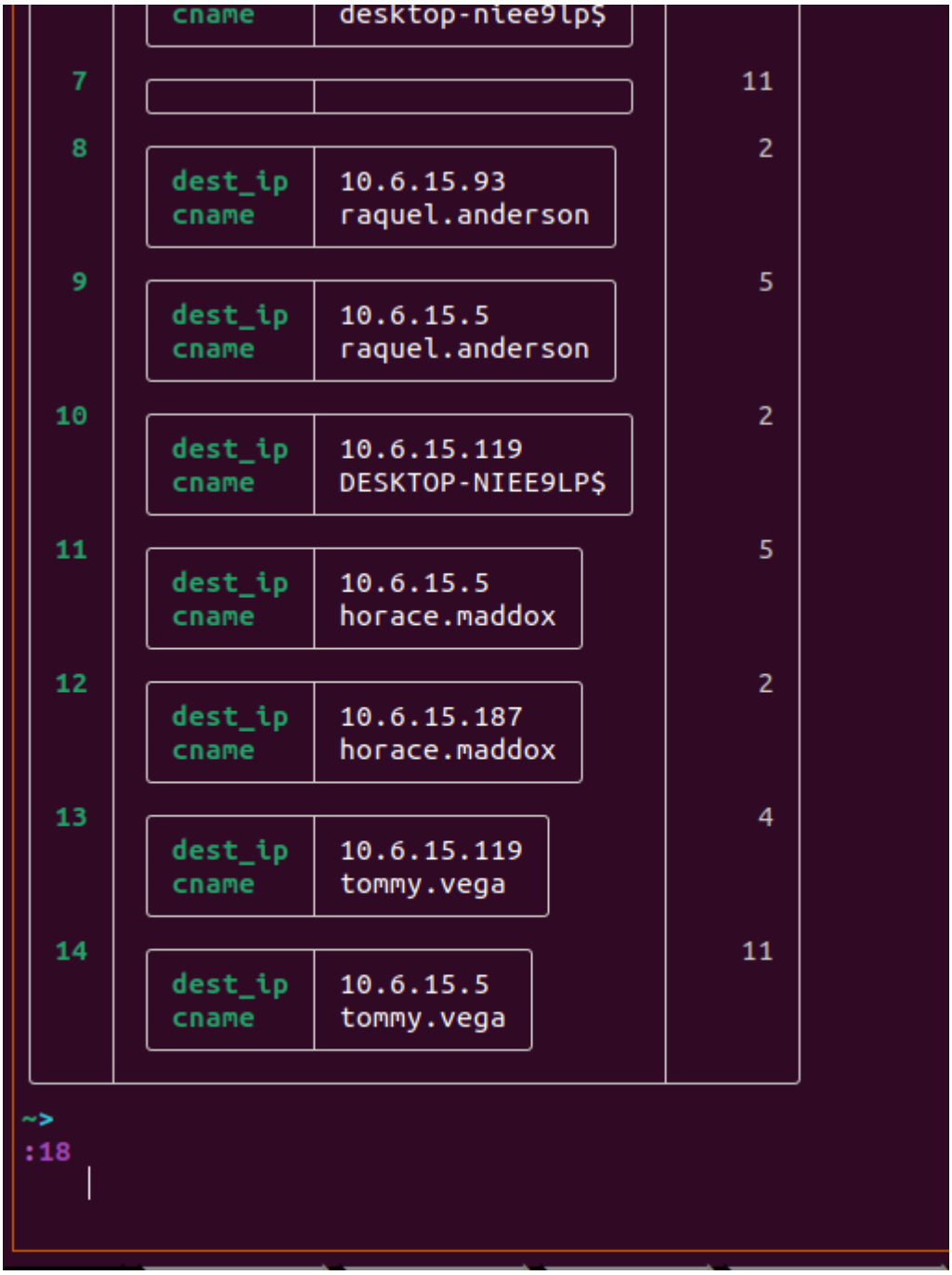
```
~> open eve-exo-nushell-etu.json | where event_type == alert | select alert | flatten | flatten | default "noip" ip | default "notargetip" t
arget_ip | default "notargetport" target_port | select signature target_ip | uniq -c | flatten
```

3. open $file | flatten | default "nokerb" kerberos| default "nodsttip" dest_ip|default "noip" ip | default "notargetip" target_ip | default "notargetport" target_port | default "nohost" cname| where target_ip == 10.6.15.119 or target_ip == 10.6.15.187 or target_ip == 10.6.15.93 or target_ip == notargetip |where cname != nohost and cname != |select dest_ip cname | uniq -c



```
arge
t_ip == 10.6.15.93 or target_ip == notargetip |where cna
```

#	value	count
0	dest_ip 10.6.15.93 cname dekstop-a1ctjvy$	4
1	dest_ip 10.6.15.5 cname DESKTOP-YS6FZ2G$	11
2	dest_ip 10.6.15.93 cname DEKSTOP-A1CTJVY$	2
3	dest_ip 10.6.15.5 cname DEKSTOP-A1CTJVY$	11
4	dest_ip 10.6.15.187 cname desktop-ys6fz2g$	4
5	dest_ip 10.6.15.187 cname DESKTOP-YS6FZ2G$	2
6	dest_ip 10.6.15.119	4


cname
desktop-niee9lp$
7
11
8
2
dest_ip
10.6.15.93
cname
raquel.anderson
9
5
dest_ip
10.6.15.5
cname
raquel.anderson
10
2
dest_ip
10.6.15.119
cname
DESKTOP-NIEE9LP$
11
5
dest_ip
10.6.15.5
cname
horace.maddox
12
2
dest_ip
10.6.15.187
cname
horace.maddox
13
4
dest_ip
10.6.15.119
cname
tommy.vega
14
11
dest_ip
10.6.15.5
cname
tommy.vega
~>
:18