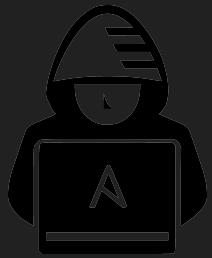
Hacking
Ansible vault password

Pierre Blanc
pierre@redhat.com



Agenda

- Mise en garde
- Ansible vault
- Approche
- Analyse
- Conclusion

Mise en garde

Ce contenu est fourni à des fins éducatives uniquement. Il ne doit en aucun cas être utilisé pour effectuer des activités illégales, y compris le piratage ou l'accès non autorisé à des données. L'objectif principal de cette présentation est de sensibiliser et d'informer sur les techniques de sécurité informatique afin d'améliorer la protection des utilisateurs légitimes. L'auteur et les intervenants déclinent toute responsabilité quant à l'utilisation abusive ou illégale des connaissances acquises à partir de ce contenu. Il est fortement recommandé de respecter les lois et réglementations en vigueur dans votre pays et d'obtenir l'autorisation appropriée avant d'entreprendre toute activité liée à la sécurité informatique.

Ansible Vault

Grandes lignes

Chiffrer les fichiers ansible
Fait partie d'Ansible
Première release v1.5.0 - Feb 18, 2014
Chiffrement symétrique fort

Ansible Vault

Chiffrement

AES 256bits
AES supporte les clés 128, 192 ou **256** bits
NSA l'utilise pour les documents **"TOP SECRET"**
Utilisation d'un sel

Ansible Vault

Contenu

```
$ANSIBLE_VAULT;1.1;AES256
6130313232316162333330393266363565363934396537663938616566643835633138303663663
3235616336376632303966613661366334316163396662650a306333663434323632623733303532
3333643035393164303836396465373534386530393766353137376438333036336165633732623 9
3337373866643734630a316431373431383466303530626338363430306363353035393934666335
3839353936343866313638353464353533373265336566346466353739336334303638643334356 5
6162323965396532393939623133331613864656435623735616264396666666435633535643736 61
3935613736316636366330376632616635626466353832303466643466323535356353163366133
3666663066616232386166653838323631623961653034616665363830363135366535343162636 5
3738
```

Ansible Vault

Salt

```
$ cat show_salt.py
#!/usr/bin/env python3
import sys

with open(str(sys.argv[1])) as f:
    data = ''.join(f.read().splitlines()[1:])

print(bytes.fromhex(data).decode().splitlines()[0])
```

Approche

- Existence de failles
  - Pas de CVE actuellement exploitable.
  - Garder ses systèmes à jour.
- Crackage
  - Bruteforce

Approche

Avec une RTX 4090 - MD5

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	1 secs
7	Instantly	Instantly	6 secs	21 secs	50 secs
8	Instantly	1 secs	5 mins	22 mins	59 mins
9	Instantly	33 secs	5 hours	23 hours	3 days
10	Instantly	14 mins	1 weeks	2 months	7 months
11	1 secs	6 hours	1 years	10 years	38 years
12	6 secs	7 days	76 years	623 years	2k years
13	1 mins	6 months	3k years	38k years	187k years
14	10 mins	12 years	204k years	2m years	13m years
15	2 hours	324 years	10m years	148m years	917m years
16	17 hours	8k years	552m years	9bn years	64bn years
17	1 weeks	219k years	28bn years	571bn years	4tn years
18	2 months	5m years	1tn years	35tn years	314tn years

Source: https://www.hivesystems.io/blog/are-your-passwords-in-the-green?utm_source=header

Approche

Outils

Des projets open source
- John
- hashcat

Attaque par bruteforce
CPU et GPU

- Incremental
- Dictionnaires
- Avec règles

Approche

Exécution

```
$ /usr/share/john/ansible2john.py play.yaml > play.in
$ hashcat -m 16900 -o play.out play.in passwords.txt -r rules/d3ad0ne.rule
```

Approche

Benchmarks

$ hashcat -m 16900 -O -b -D 1,2

11th Gen Intel(R) Core(TM) i7-11850H @ 2.50GHz

Intel CPU

Speed.....: 26.1 kH/s

Intel integrated GPU

Speed.....: 7.4 kH/s

GTX 1080

Sped.....: 138.7 kH/s

RTX2080 Super

Speed.....: 237.7 kH/s

MD5: 4130.7 MH/s

Approche

Benchmarks

RTX 4090

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	1 secs
7	Instantly	Instantly	6 secs	21 secs	50 secs
8	Instantly	1 secs	5 mins	22 mins	59 mins
9	Instantly	33 secs	5 hours	23 hours	3 days
10	Instantly	14 mins	1 weeks	2 months	7 months
11	1 secs	6 hours	1 years	10 years	38 years
12	6 secs	7 days	76 years	623 years	2k years
13	1 mins	6 months	3k years	38k years	187k years
14	10 mins	12 years	204k years	2m years	13m years
15	2 hours	324 years	10m years	148m years	917m years
16	17 hours	8k years	552m years	9bn years	64bn years
17	1 weeks	219k years	28bn years	571bn years	4tn years
18	2 months	5m years	1tn years	35tn years	314tn years

ChatGPT Hardware

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	Instantly	Instantly	Instantly
8	Instantly	Instantly	Instantly	Instantly	1 secs
9	Instantly	Instantly	4 secs	21 secs	1 mins
10	Instantly	Instantly	4 mins	22 mins	1 hours
11	Instantly	6 secs	3 hours	22 hours	4 days
12	Instantly	2 mins	7 days	2 months	8 months
13	Instantly	1 hours	12 months	10 years	47 years
14	Instantly	1 days	52 years	608 years	3k years
15	2 secs	4 weeks	2k years	37k years	232k years
16	15 secs	2 years	140k years	2m years	16m years
17	3 mins	56 years	7m years	144m years	1bn years
18	26 mins	1k years	378m years	8bn years	79bn years

Source:https://www.hivesystems.io

Analyse

- Suivre les bonnes pratiques liées aux mots de passe
- Le bruteforce de plus en plus efficace
- Attention aux données en ligne
- Mettre en place des ACL sur les fichiers de mots de passe pour restreindre l'accès.
- La mise à jour de mots de passe peut être fastidieuse, **automatisez la !**

Conclusion

Pas de CVE exploitable.

Mettre en place des ACL sur les fichiers de mots de passe pour restreindre l'accès, attention au publication externe.

Effectuer régulièrement une mise à jour des mots de passe et mettre en place un processus automatisé.

Utiliser des mots de passe longs et complexes ne faisant pas partie d’un dictionnaire.

Merci