

RETEX PENTEST

Vous prendrez bien un peu de Guacamole ?



Slides !



[https://blog.volker-carstein.com/barbhack 2024 retex pentest slides.pdf](https://blog.volker-carstein.com/barbhack%202024%20retex%20pentest%20slides.pdf)

Briefing

- I. Contexte de la mission
- II. Partie Active Directory
- III. Guacamole et “O-day”
- IV. Photoshop pour passer Domain Admin
- V. Un peu de persistance



Who am I ?



Volker Carstein (@volker_carstein)

- Pentester le jour, jack of all trades la nuit
- Work @ Bsecure, freelance @ Parabellum Services
- Ingénierie sociale, OSINT et sécurité offensive (préférence pour l'Active Directory)
- Speaker @ LeHack, Barbhack, Insomni'hack, SecSea, etc

I - Contexte de la mission



Salade de concombre, melon et tofu au basilic

<https://vegan-pratique.fr/recettes/salade-de-concombre-melon-et-tofu-au-basilic/>

I - Contexte de la mission

- Mission de pentest interne chez Bsecure
- Active Directory + réseau local
- Une semaine de pentest à deux
- **Pas de compte fourni**
 - Accès via VPN au réseau interne



II - Partie Active Directory



Pad Thai

<https://vegan-pratique.fr/recettes/pad-thai/>

II - Partie Active Directory

Comment avoir un compte ?

- [ASREProast](#) ? Non car pas de compte pour query les comptes vulnérables
- [MiTM/Coerce + relay](#) ? Pas possible à cause du VPN utilisé
- Solution : **OSINT** et **password spray**

II - Partie Active Directory

- OSINT
 - Récupérer une liste d'employés
 - Connaître/deviner le format du username
 - Ici, guess à partir du format de l'adresse mail de notre contact client
 - Se constituer une wordlist



II - Partie Active Directory

- **Spray & pray**
 - **Mots de passe classiques à spray**
 - **NomDuClient + Année (+ ou - 1)**
 - **VilleDuSiègeClient + Numéro département**
 - **Attention au lockout ! 5 essais max dans ce cas là**
 - **netexec goes brrrrr**



II - Partie Active Directory

```
SMB 10.3 445 .com\ .com\ GON_FAILURE
SMB 10.3 445 .com\ .com\ S_LOGON_FAILURE
SMB 10.3 445 .com\ .com\ ATUS_LOGON_FAILURE
SMB 10.3 445 .com\ .com\ GON_FAILURE
SMB 10.3 445 .com\ .com\ TATUS_LOGON_FAILURE
SMB 10.3 445 .com\ .com\ TUS_LOGON_FAILURE
SMB 10.3 445 .com\ .com\ N_FAILURE
SMB 10.3 445 .com\ .com\ FAILURE
SMB 10.3 445 .com\ .com\ JRE
SMB 10.3 445 .com\ .com\ LURE
SMB 10.3 445 .com\ .com\ JRE
SMB 10.3 445 .com\ .com\ JRE
SMB 10.3 445 .com\ .com\ LUF
SMB 10.3 445 .com\ .com\ E
SMB 10.3 445 .com\ .com\ ILLU
SMB 10.3 445 .com\ .com\ ST
SMB 10.3 445 .com\ .com\ JRE
SMB 10.3 445 .com\ .com\ JRE
SMB 10.3 445 .com\ .com\ JRE
SMB 10.3 445 .com\ .com\ JRE
```

[+] .com\ .com\ 2024

Compte obtenu avec NomDuClient + Année



II - Partie Active Directory

Maintenant qu'on a un compte, explorons le champ des possibles :

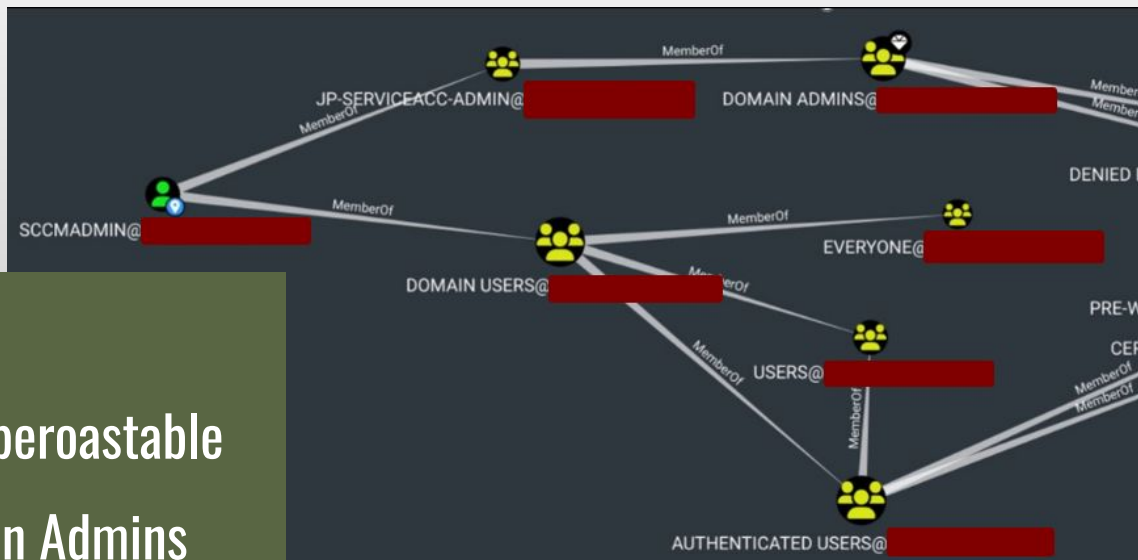
- Bloodhound pour avoir de l'info
- [Check des délégations Kerberos](#) : rien
- [ASREProast](#) : rien
- [sAMAccountName spoofing](#) : nope
- [ADCS](#) : rien
- [SCCM](#) : rien
- [Shares sur le réseau](#) : 2 nouveaux comptes !



II - Partie Active Directory

Kerberoast

- Compte SCCMADMIN kerberoastable
- Membre du groupe Domain Admins
- Free win ?



II - Partie Active Directory


Kerberoast

- Wordlist avec [LDAPWordlistHarvester](#)
- + la liste de règle : [clem9669 large.rule](#)
- Hashcat et c'est parti !

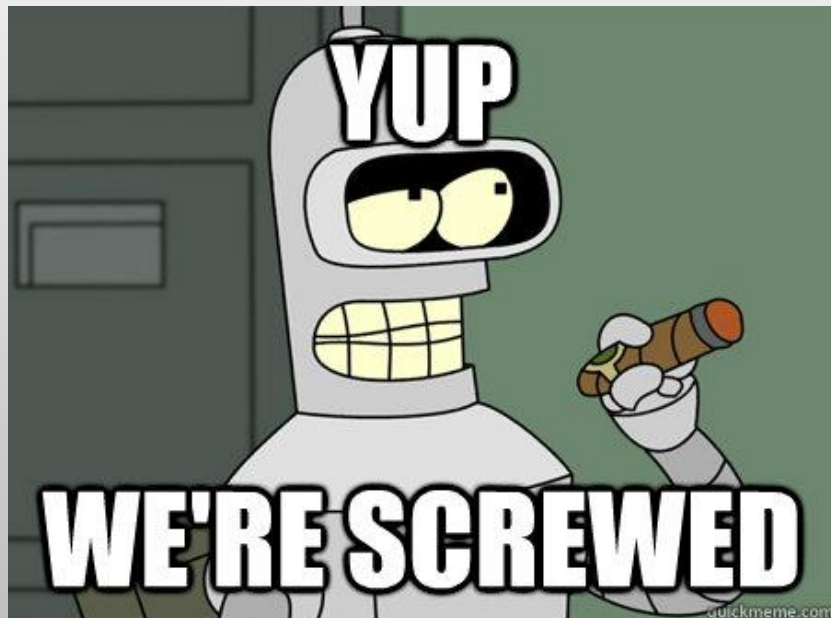
II - Partie Active Directory

Kerberoast

- Wordlist avec [LDAPWordlistHarvester](#)
- + la liste de règle : [clem9669 large.rule](#)
- Hashcat et c'est parti !

	Hashcat lancé pour crack le compte Kerberoastable
	Moitié des hashes testés : rien
	Status..:Exhausted Recovered....:0/1

II - Partie Active Directory



III - Guacamole et “0-day”



Guacamole (pas le software)

<https://francevegetalienne.fr/plats-du-monde-aims-en-france/2018/7/26/guacamole-vgtali-en-vegan>

III - Guacamole et “0-day”

On fouille le reste de l’interne

- Services d’administration (SSH, RDP, etc.)
- Services web divers
 - Wallix, Wazuh, Prometheus, Semaphore, etc.
 - Et un en particulier, **Guacamole**



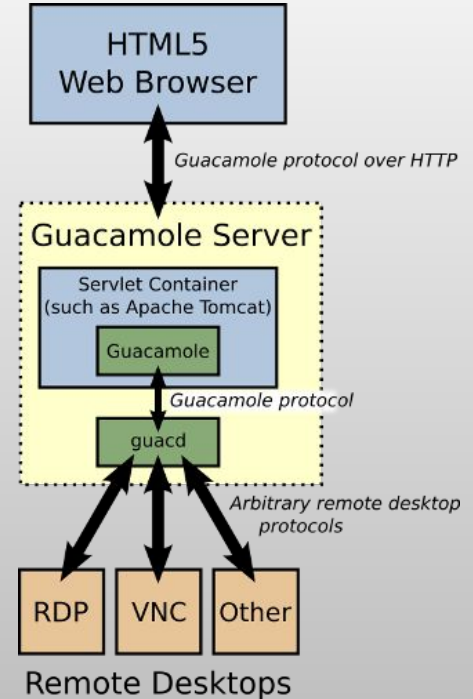
III - Guacamole et “0-day”



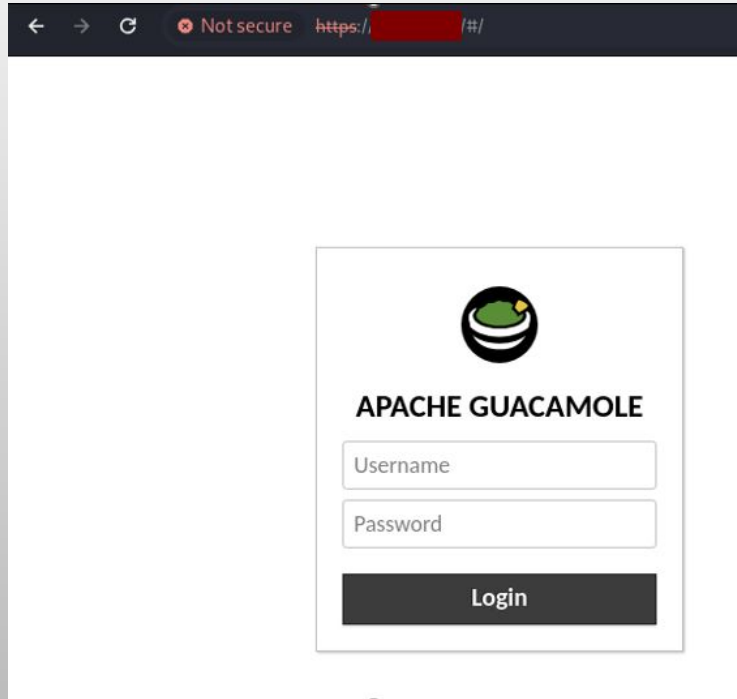
Apache Guacamole

Full à jour, version 1.5.5

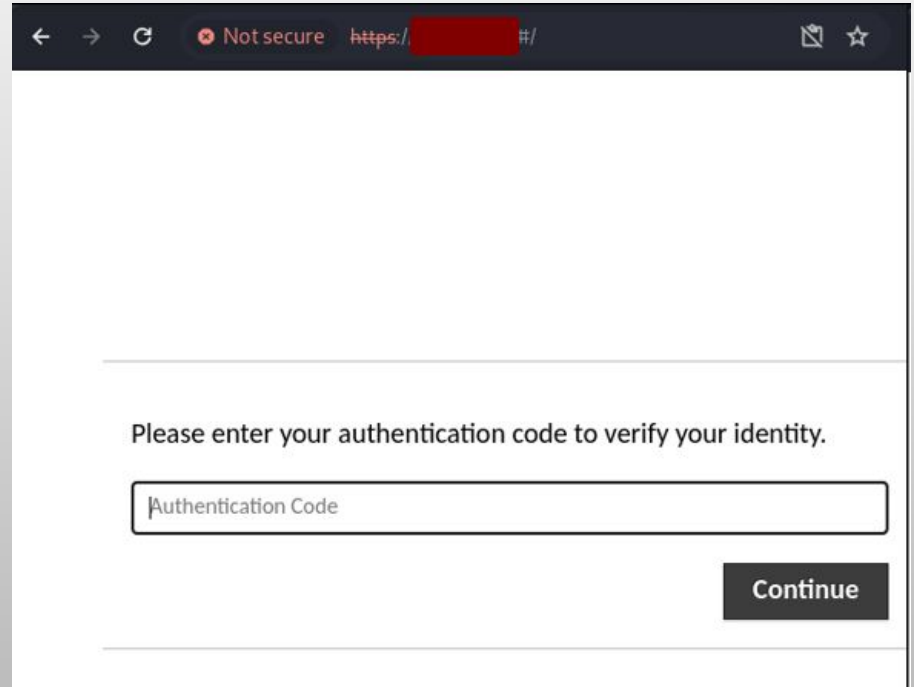
Apache Guacamole is a [free and open-source](#), [cross-platform](#), clientless [remote desktop gateway](#) maintained by the [Apache Software Foundation](#). It allows users to control [remote computers](#) or [virtual machines](#) via a [web browser](#), and allows administrators to dictate how and whether users can connect using an extensible [authentication](#) and [authorization](#) system. Destination machines can be kept isolated behind Guacamole and need not be reachable over the [internet](#).



III - Guacamole et “0-day”



III - Guacamole et “0-day”



III - Guacamole et "0-day"

? **Payload sets**

You can define one or more payload sets. The number of payload set Positions tab. Various payload types are available for each payload in different ways.

Payload set: Payload count: 1,000,000

Payload type: Request count: 1,000,000

? **Payload settings [Numbers]**

This payload type generates numeric payloads within a given range

Number range

Type: Sequential Random

From:

To:

Step:

How many:

Number format

Base: Decimal Hex

Min integer digits:

Max integer digits:

Min fraction digits:

Max fraction digits:

Examples

000001

654321

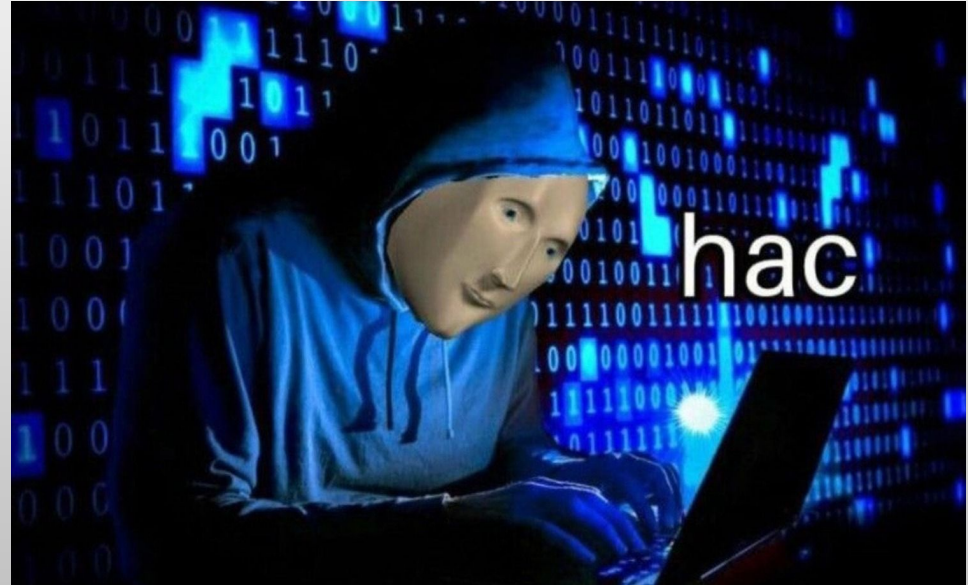
- 10^6 possibilités
- Soit wordlist à la main
- Soit celle-ci : [6 digit mix.txt](#)
 - Pas besoin du random sur celle là car déjà shuffle



III - Guacamole et "0-day"

Request	Payload	Status code	Respon...	Error	Time
9	624839	200	158		
10	780722	200	3		
11	676061	200	5		
12	663001	200	2		
13	515850	200	2		
14	082035	200	4		
15	195490	200	5		
16	650284	200	5		
17	365833	200	3		
18	727349	200	6		
19	220630	200	2		
20	865964	200	5		
21	094302	200	2		
22	313797	200	3		
23	483973	200	3		
24	627298	200	3		
25	914331	200	2		
26	403926	200	4		
27	978594	200	5		
28	793032	200	4		
29	746219	200	3		
30	363186	200	7		

Request	Response	
Request	Response	
Pretty	Raw	Hex
1 GET / HTTP/2		
2 Host: blog.volker-carstein.com		
3 Sec-Ch-Ua: "Chromium";v="127", "NotA;Brand";v="99"		
4 Sec-Ch-Ua-Mobile: ?0		
5 Sec-Ch-Ua-Platform: "Linux"		
6 Accept-Language: fr-FR		
7 Upgrade-Insecure-Requests: 1		
8 User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/127.0.6533.100 Safari/537.36		
9 Accept:		
10 text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;q=0.7		
11 gnd-exchange;v=b3;q=0.7		
12 Sec-Fetch-Site: none		
13 Sec-Fetch-Mode: navigate		
14 Sec-Fetch-User: ?1		
15 Sec-Fetch-Dest: document		
16 Accept-Encoding: gzip, deflate, br		
17 Priority: u=0, i		
18 Connection: keep-alive		
19 Content-Length: 48		
20		
21 username=guacamini&password=guacamini&otp=205913		



III - Guacamole et “0-day”

C'est une vuln, mais en fait non

Subject: Bypass 2FA on Guacamole 1.5.5
To: <security@guacamole.apache.org>

Hi everyone,

I was able to bypass the 2FA by simply bruteforcing it during a pentest.
The default configuration for 2FA is 6 digits, which can be bruteforced with 10 request per seconds in less than 24 hours.

Below is a sample of an authentication request (the guac-totp parameter was bruteforced) :

```
POST /api/tokens HTTP/1.1
Host: localhost
Content-Length: 54
Accept: application/json, text/plain, */*
Content-Type: application/x-www-form-urlencoded
Sec-Ch-Ua-Mobile: ?0
User-Agent: XXX
Connection: keep-alive

username=XXXXXX&password=YYYYY&guac-totp=123456
```

This issue mainly comes from the fact that there is no authentication failure limitation.

Do you need more information about this vulnerability ?

Regards,

De: [REDACTED] <[REDACTED]@apache.org>
Subject: Re: Bypass 2FA on Guacamole 1.5.5
To: [REDACTED] <[REDACTED]@bsecure.fr>
Cc: <security@guacamole.apache.org>

[REDACTED]

Thank you for reaching out privately via our security@ list - we greatly appreciate researchers that follow responsible disclosure practices.

Overall, rate limiting is an aspect of security that Guacamole has historically excluded from the scope of its own security model in favor of external solutions like "fail2ban" that can provide this at the firewall level:

<https://github.com/fail2ban/fail2ban>

The lack of internal rate limiting within Guacamole is not a vulnerability in itself, however the benefit for adding our own rate limiting as an alternative is understood and has already been implemented for our upcoming 1.6.0 release:

<https://issues.apache.org/jira/browse/GUACAMOLE-990> ("Enforce rate limit within TOTP")

III - Guacamole et “0-day”

C'est une vuln, mais en fait non

If you are concerned about more sophisticated and distributed attacks with respect to your own deployment of **Guacamole**, I think you would need to look into deploying and configuring something like a WAF.

TLDR :
Mettre un fail2ban/WAF et/ou
attendre la 1.6.0

- > It could be a good idea to make the totp 8 digits long instead of 6.
- > What do you think ?
- >

You can always override the defaults as needed, but be cautious:

The defaults were chosen because they are the most widely supported combination of values. There are popular TOTP applications out there (like Google Authenticator) that will silently ignore some TOTP parameters. If you use such an authenticator and happen to choose options that they don't support, they will appear to successfully scan the QR code yet generate invalid codes.

You need to make sure that any TOTP authenticator application(s) you will be using support your desired parameters before overriding them.

IV - Photoshop pour passer Domain Admin



Lasagnes vegan

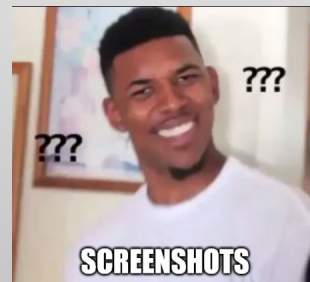
<https://vegan-pratique.fr/recettes/lasagnes-a-bolognaise/>

IV - Photoshop pour passer Domain Admin

- Session admin Guacamole obtenue
- Accès à une session déjà en cours sur une machine de CI/CD
 - Fouiller le plus vite possible pour trouver des choses
 - L'idéal serait de se maintenir un accès
- Loot récupéré :
 - **Screenshots** de tickets Kerberos
 - **Screenshots** d'une clé privée
- L'admin revient après 15 min et ferme sa session pour la journée

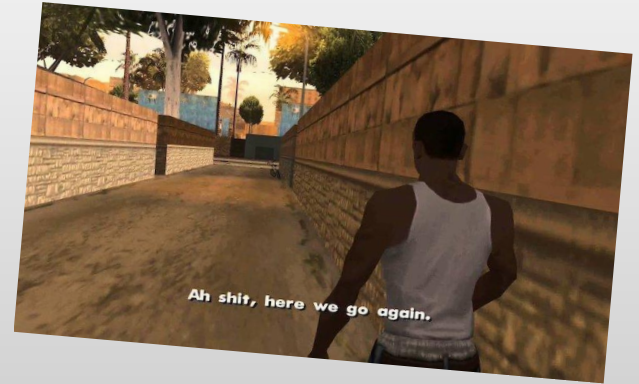
IV - Photoshop pour passer Domain Admin

- Session admin Guacamole obtenue
- Accès à une session déjà en cours sur une machine de CI/CD
 - Fouiller le plus vite possible pour trouver des choses
 - L'idéal serait de se maintenir un accès
- Loot récupéré :
 - **Screenshots** de tickets Kerberos
 - **Screenshots** d'une clé privée
- L'admin revient après 15 min et ferme sa session pour la journée



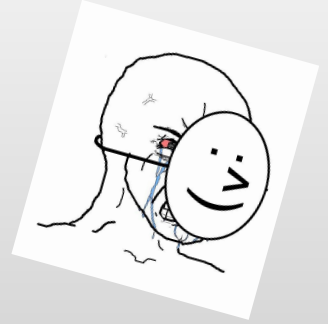
IV - Photoshop pour passer Domain Admin

- Jeudi soir, 18-19h environ
- Les tickets Kerberos vont expirer dans la nuit
- Un des tickets est pour un compte domain admin
- La clé privée devrait nous permettre également des choses intéressantes
- From screenshots de tickets/clé to DA ?



IV - Photoshop pour passer Domain Admin

- Solution simple : OCR
 - Pour un screenshot de base64 pris à travers un navigateur + bureau distant Guacamole -> **c'est non**
- On s'arme de courage et on recopie à la main le ticket puis on vérifie avec `describeTicket.py`
- Comment corriger les confusions subtiles ? `l / 1 / l`, `o / 0`, etc



IV - Photoshop pour passer Domain Admin

- **Technique de masquage avec Photoshop**

(ou autre logiciel avec gestion de calques transparents)

- Screenshot “objectif” et screenshot “recopié” sur un calque chacun
- Un des screenshots en semi-transparent et d’une autre couleur
- Alignement ligne par ligne pour minimiser l’erreur
- Dès qu’un écart apparaît, on corrige sur la copie de travail du texte recopié



IV - Photoshop pour passer Domain Admin

```
-----BEGIN OPENSSH PRIVATE KEY-----  
b3B1bnNzaC1rZXktdjEAAAABAg5vbmUAAAABbm9uZQAAAAAAAAABAAAAB1wAAAAdzc2gtcn  
NhAAAAAwEAAQAAAQAEakVJ3pj7snJNfiL0cwoJ82pEYDbQpX0Dsei8hCAHQ02B3U55fidPa  
mNhQ1LxL2QLzr04A8X/Q8+cYbjCB1C7Jcx70r1Eua1k45Xa2YeF+oHYr1p31Cf0yZdP9fU  
0tChHEeuRAa3IDdhXVfW5y79um40AYYACJwLZcyr6nn1LXLsZ1BVB0X+vNtua2sSf/b+Wi  
N1NPAkHr2t+ge0tv0lQKXuMgyI67pLd+PNrxcYvjgy0CLA1a+yGMve/6gSGRnZUR5S2JI7  
UU1vFGNKwqQw/1sSdw0H9UoALvcvmp/f1B8//a1Qk1JhIdGxGUzmnBVDeJK94XBk4fEpBN  
Gg7UJ+jWzejyA4RVGDjGmXz1SEFIr5I1YWteflxh2DKQNpQjYthIZQLNT0gs0mfmErOzD  
yH4171bCBfQV/28t+su80Lwe7EV1wJki0+WNuQS5SHeygQqUTKUeYeVlk8ii+aWtpRx1Jh  
Dc+plP6yT/3XNBznfDJAASW8jrl1SYCE6CRx+pxxAAAFiNmch6VznYerAAAAB3NzaC1yc2
```

NB: Pour les plus pirates d'entre vous, notez que cette clé a été générée pour Barbhack a titre d'exemple (#SaxX )

IV - Photoshop pour passer Domain Admin

- Ticket pour DA reconstruit, clé privée reconstruite
- Le compte ne peut pas [DCSync](#)
 - Création d'un compte machine via [PTT](#)
 - [Ajout des droits de DCSync](#)
 - [DCSync](#), dump du hash de krbtgt
 - Win, at last



V - Un peu de persistance



Mousse au chocolat

<https://www.sweetandsour.fr/gourmandise-2/mousse-au-chocolat-vegan-au-blender-sans-aquafaba/>

V - Un peu de persistance

- 2 techniques mises en place (outre la création de compte + droits pour DCSync)
 - [Delegation to KRBTGT](#)
 - Backdoor via [AdminSDHolder](#)
- + le dump de krbtgt qui permet de [forger des tickets](#) (et donc de persister)

V - Un peu de persistance

Delegation to KRBTGT

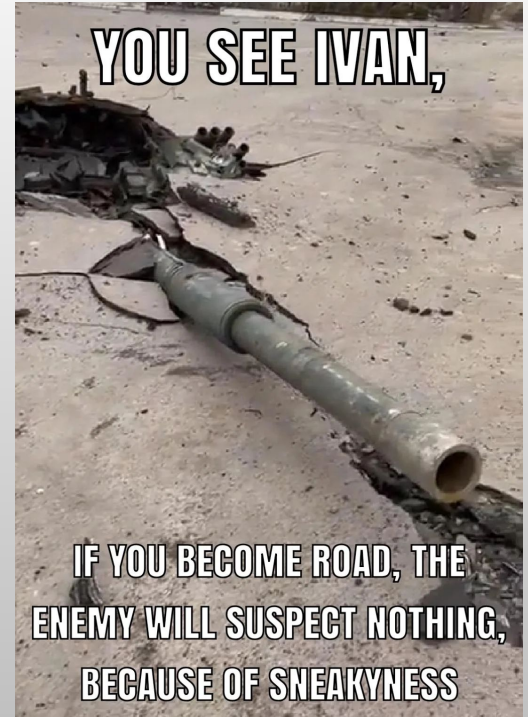
- Abus de Resource-Based Constraint Delegation (RBCD)
- Configurer l'attribut `ms-DS-Allowed-To-Act-On-Behalf-Of-Other-Identity` du compte `krbtgt` pour permettre à un compte contrôlé de demander des tickets "en tant que"
- S4U pour obtenir un ST vers `krbtgt` en tant que compte privilégié
 - ST vers `krbtgt` = TGT
- Pass the ticket, profit



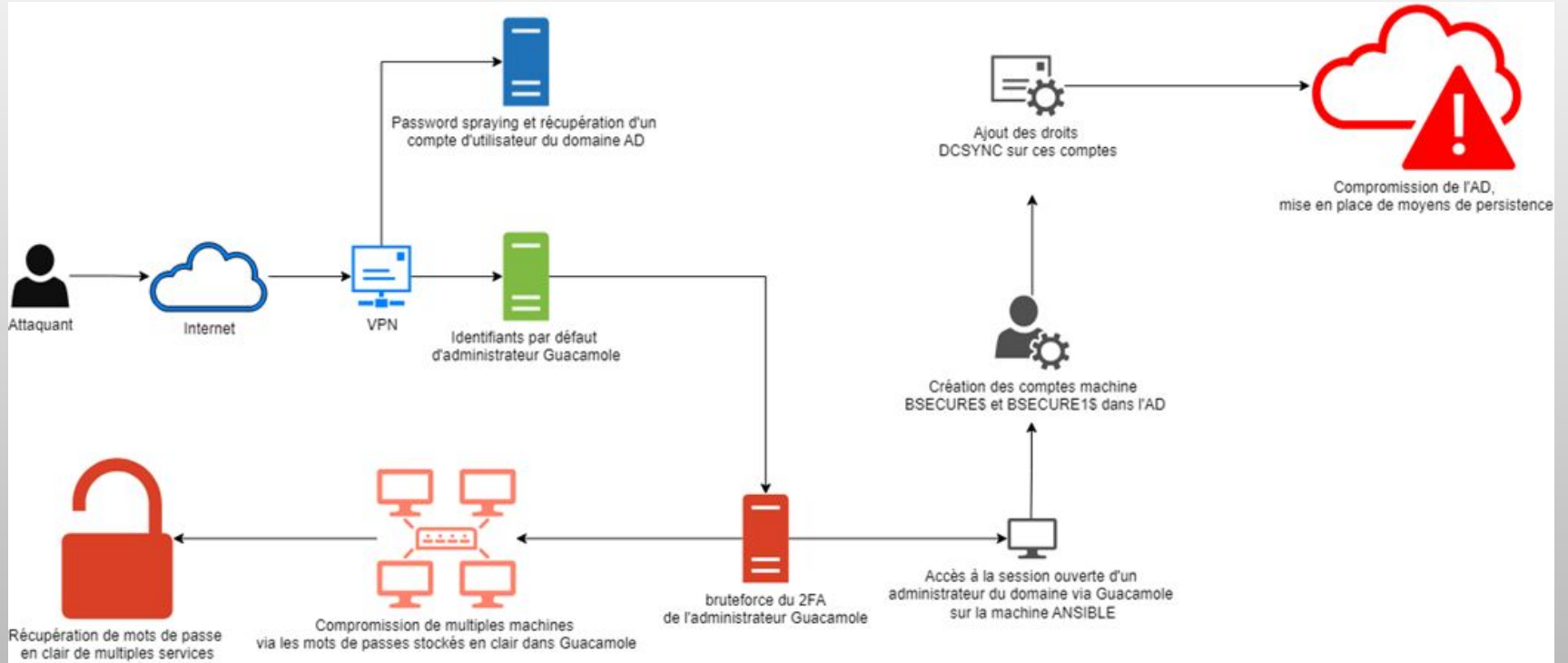
V - Un peu de persistance

Backdoor via [AdminSDHolder](#)

- Compte dont la DACL sert de template
- DACL répliquée toutes les 60 min sur les objets protégés
- Ajouter des droits (ex: FullControl), laisser propagate
- Profit !



Conclusion



Conclusion

- Les OTP c'est pas la panacée, un peu de périmétrique ça fait pas de mal
- Quand la porte est fermée, on passe par la fenêtre
- Démarrer sans compte c'est challenge
- Il suffit d'une erreur pour rentrer (exemple: mot de passe par défaut)
- Try hard à faire des trucs de singes, parfois ça marche
- C'était tendu, mais fun !

Thank you !

