RETEX PENTEST

Vous prendrez bien un peu de Guacamole ?

31/08/2024

@volker_carstein

Slides !

https://blog.volkercarstein.com/barbhack_2024_retex_pentest_slides.pdf

@volker_carstein

Briefing

I. Contexte de la mission
II. Partie Active Directory
III. Guacamole et “0-day”
IV. Photoshop pour passer Domain Admin
V. Un peu de persistance

@volker_carstein

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 Thaï

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 ! Par défaut, 5 essais max
  - netexec goes brrrrr

II - Partie Active Directory

```
SMB  10.  445  [-]  .com\  GON_FAILURE
SMB  10.  445  [-]  .com\  S_LOGON_FAILURE
SMB  10.  445  [-]  .com\  ATUS_LOGON_FAILURE
SMB  10.  445  [-]  .com\  GON_FAILURE
SMB  10.  445  [-]  .com\  TATUS_LOGON_FAILURE
SMB  10.  445  [-]  .com\  TUS_LOGON_FAILURE
SMB  10.  445  [-]  .com\  N_FAILURE
SMB  10.  445  [+]  .com\  [redacted]:[redacted]2024
SMB  10.  445  [-]  .com\  ILURE
SMB  10.  445  [-]  .com\  URE
SMB  10.  445  [-]  .com\  LURE
SMB  10.  445  [-]  .com\  URE
SMB  10.  445  [-]  .com\  LU
SMB  10.  445  [-]  .com\  E
SMB  10.  445  [-]  .com\  ILL
SMB  10.  445  [-]  .com\  LU
SMB  10.  445  [-]  .com\  ST
SMB  10.  445  [-]  .com\  URE
SMB  10.  445  [-]  .com\  RE
SMB  10.  445  [-]  .com\  URE
```

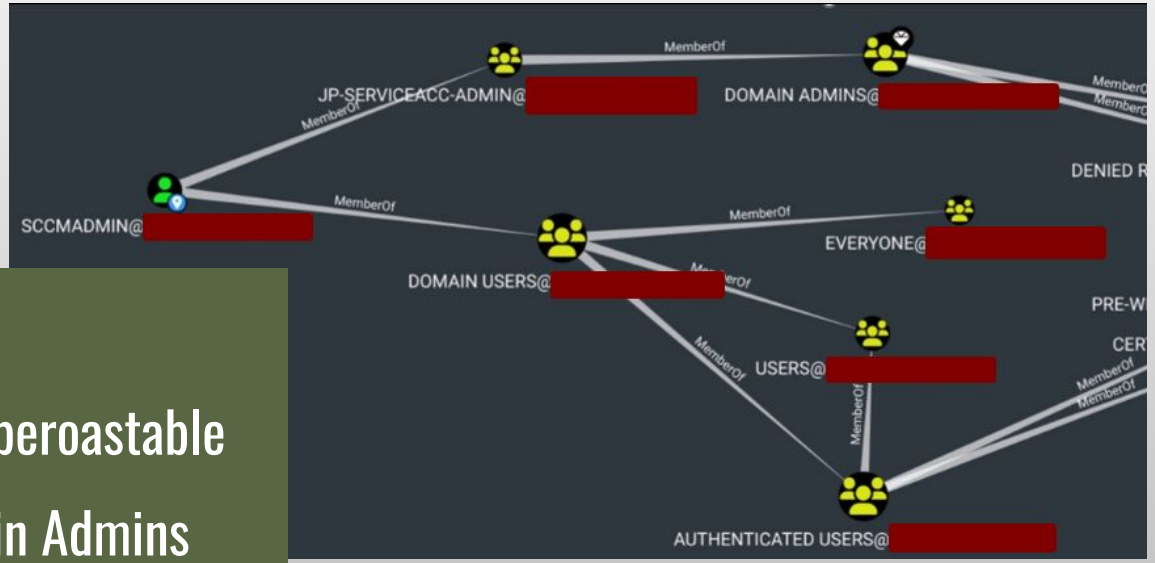
Compte obtenu avec NomDuClient + Année

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

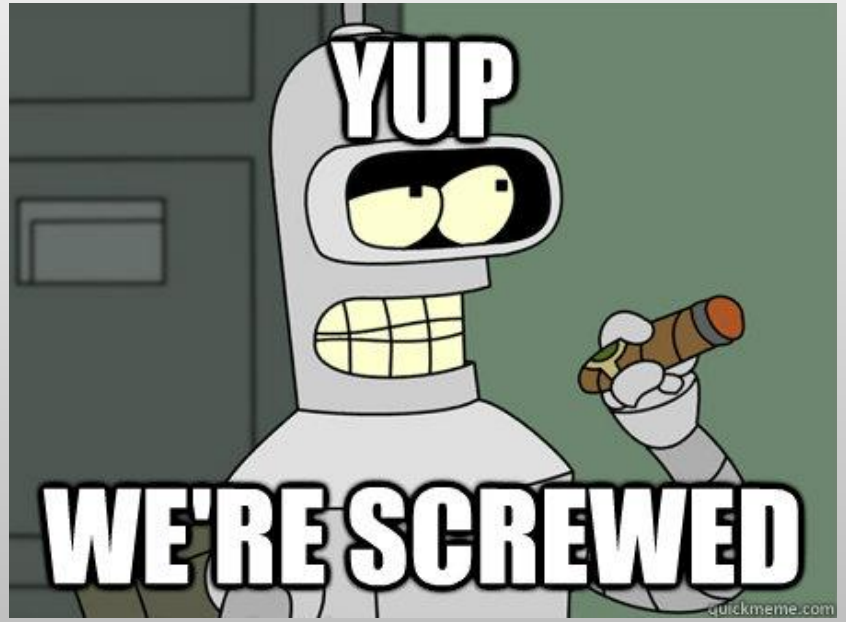
- Wordlist avec LDAPWordlistHarverster
- + la liste de règle : clem9669_large.rule
- Hashcat et c'est parti !

II - Partie Active Directory

Kerberoast

- Wordlist avec LDAPWordlistHarverster
- + la liste de règle : clem9669_large.rule
- Hashcat et c'est parti !

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-vgtalien-vegan

@volker_carstein

III - Guacamole et “0-day”

On fouille le reste de l’interne

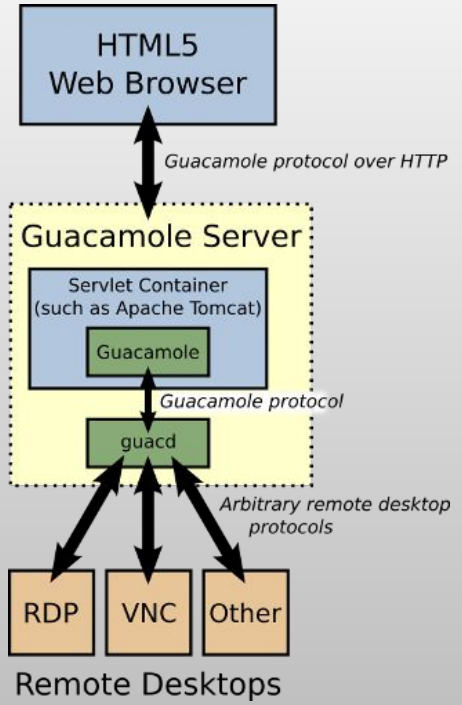
- Services d’administration (SSH, RDP, etc.)
- Services web divers
  - Wallix, Wazuh, Prometheus, Semaphore, etc.
  - Et un en particulier, **Guacamole**

III - Guacamole et “0-day”

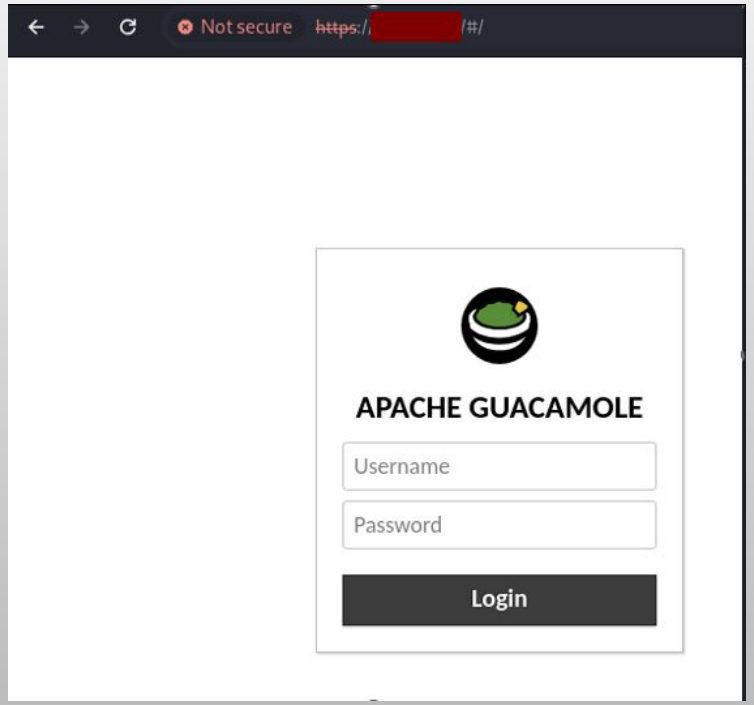
Apache Guacamole

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.

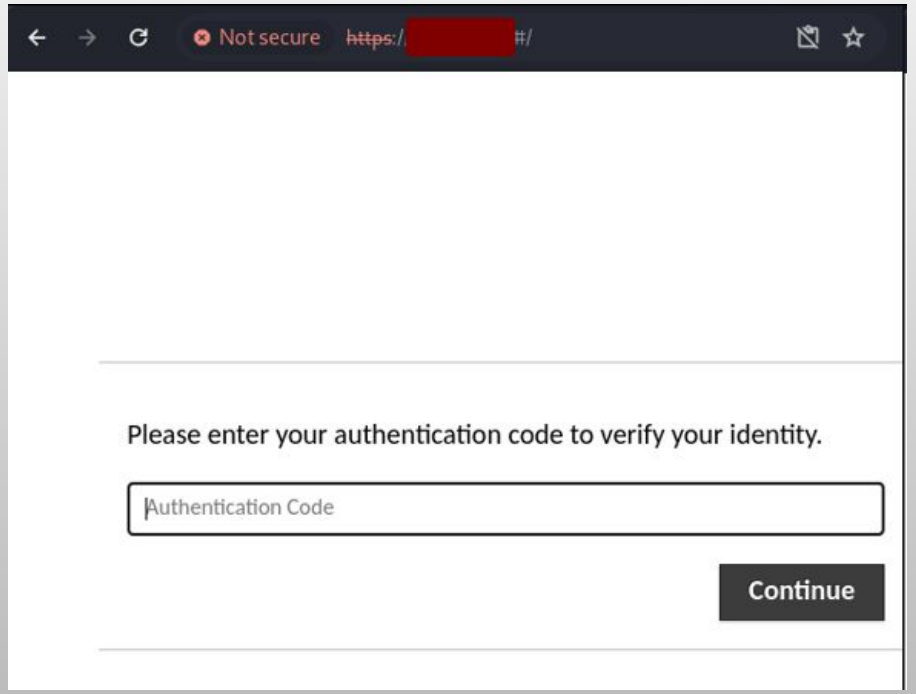


III - Guacamole et “0-day”



@volker_carstein

III - Guacamole et “0-day”



@volker_carstein

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 payloa
in different ways.

Payload set: 1 — Payload count: 1,000,000

Payload type: Numbers — Request count: 1,000,000

Payload settings [Numbers]

This payload type generates numeric payloads within a given range

Number range

Type: ○ Sequential ◉ Random

From: 000000

To: 999999

Step: 1

How many: 1000000

Number format

Base: ◉ Decimal ○ Hex

Min integer digits: 6

Max integer digits: 6

Min fraction digits: 0

Max fraction digits: 0

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

@volker_carstein

III - Guacamole et “0-day”

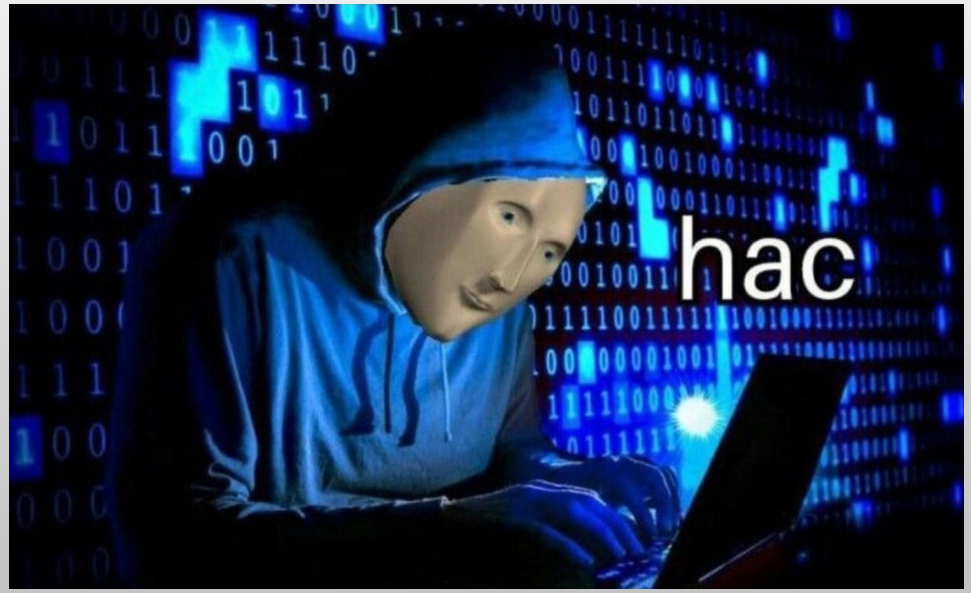
Request	Payload	Status code	Respon...	Error	Timeo
9	624839	200	158		
10	780722	200	3		
11	676061	200	5		
12	663001	200	2		
13	515850	200	2		
14	082035	200	4		
15	195490	200	5		
16	650284	200	5		
17	365833	200	3		
18	727349	200	6		
19	220630	200	2		
20	865964	200	5		
21	094302	200	2		
22	313797	200	3		
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

Pretty Raw Hex

```
GET / HTTP/2
Host: blog.volkercarstein.com
Sec-Ch-Ua: "Chromium";v="127", "Not)A;Brand";v="99"
Sec-Ch-Ua-Mobile: ?0
Sec-Ch-Ua-Platform: "Linux"
Accept-Language: fr-FR
Upgrade-Insecure-Requests: 1
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
Accept:
text/html,application/xhtml+xml,application/xml;q=0.9,image/avif,image/webp,image/apng,*/*;
gned-exchange;v=b3;q=0.7
Sec-Fetch-Site: none
Sec-Fetch-Mode: navigate
Sec-Fetch-User: ?1
Sec-Fetch-Dest: document
Accept-Encoding: gzip, deflate, br
Priority: u=0, i
Connection: keep-alive
Content-Length: 48

username=guacadmin&password=guacadmin&otp=205915
```



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.

Bellow 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>
[redacted]
Subject: Re: Bypass 2FA on Guacamole 1.5.5
To: [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.

@volker_carstein

IV - Photoshop pour passer Domain Admin

Lasagnes vegan

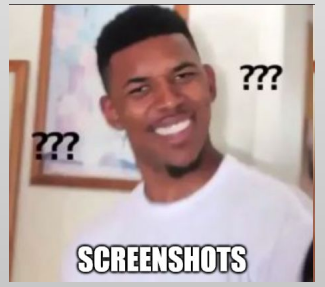
https://vegan-pratique.fr/recettes/lasagnes-a-bolognaise/

IV - Photoshop pour passer Domain Admin

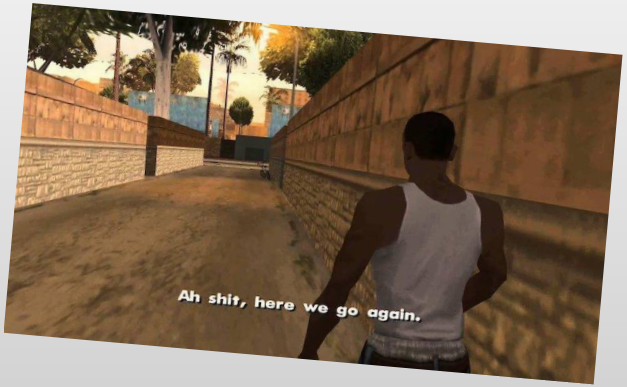
- Session admin Guacamole obtenue
- Accès à une session déjà en cours sur une machine de CI/CD
  - Fouiller le plus vite possible pour trouver des choses
  - L'idéal serait de se maintenir un accès
- Loot récupéré :
  - **Screenshots** de tickets Kerberos
  - **Screenshots** d'une clé privée
- L'admin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



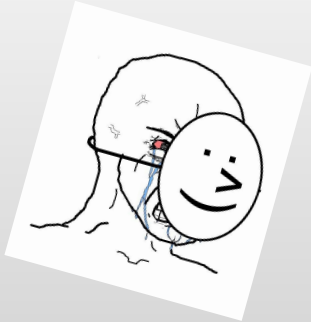
IV - Photoshop pour passer Domain Admin



- 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 / I, O / 0, etc



@volker_carstein

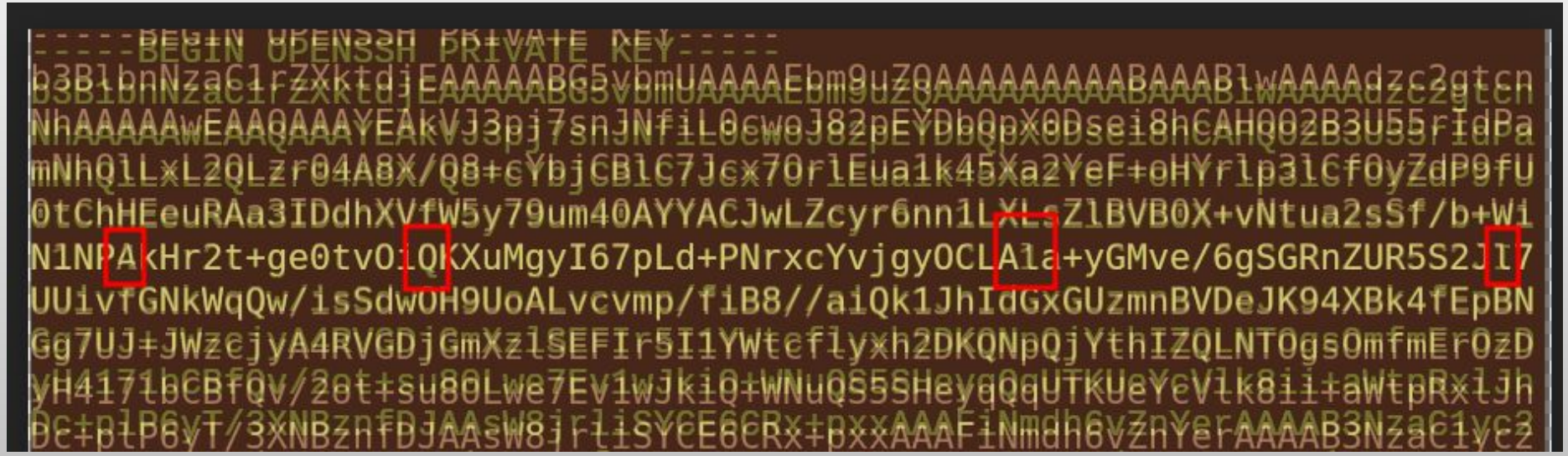
IV - Photoshop pour passer Domain Admin

- **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



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

@volker_carstein

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

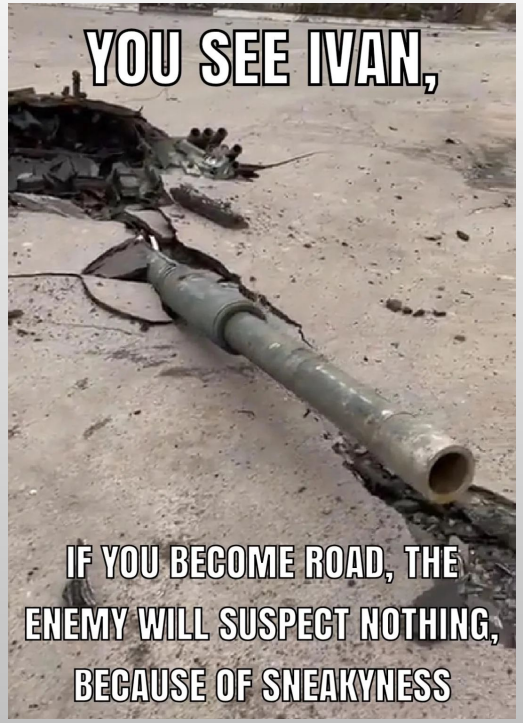
- Abus de Resource-Based Constraint Delegation (RBCD)
- Configurer l'attribut ms-DS-Allowed-To-Act-On-Behalf-Of-Other-Identity
  du compte krbtgt pour permettre à un compte contrôlé de demander des tickets "en tant que"
- S4U pour obtenir un ST vers krbtgt en tant que compte privilégié
    - ST vers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

@volker_carstein

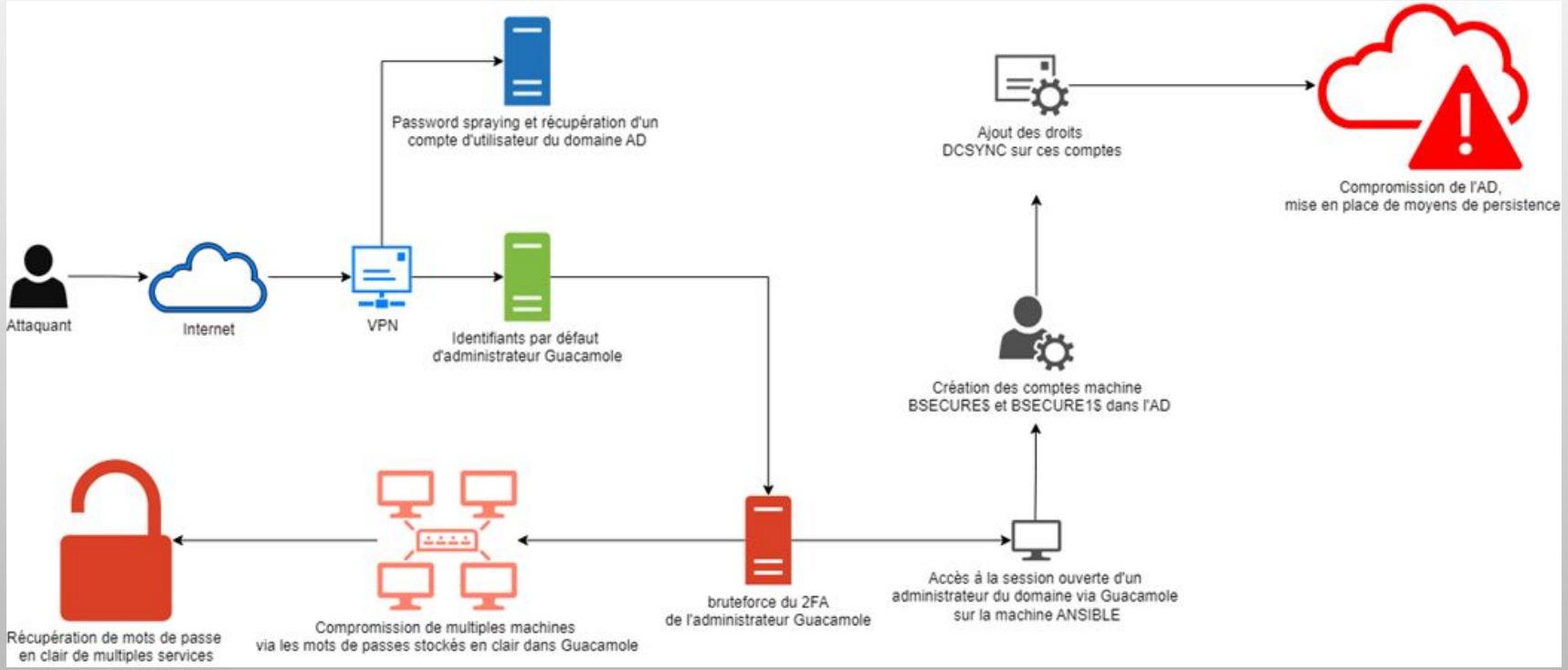
V - Un peu de persistance

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


Password spraying et récupération d'un compte d'utilisateur du domaine AD
Ajout des droits DCSYNC sur ces comptes
Compromission de l'AD, mise en place de moyens de persistence
Attaquant
Internet
VPN
Identifiants par défaut d'administrateur Guacamole
Création des comptes machine BSECURE$ et BSECURE1$ dans l'AD
Récupération de mots de passe en clair de multiples services
Compromission de multiples machines via les mots de passes stockés en clair dans Guacamole
bruteforce du 2FA de l'administrateur Guacamole
Accès à la session ouverte d'un administrateur du domaine via Guacamole sur la machine ANSIBLE

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 !

@volker_carstein

Thank you !

@volker_carstein