Cybersécurité
& Tests d'intrusion

20/05/2021
Thomas ROUSSEAU
thomas.rousseau@wavestone.com

/me

Thomas ROUSSEAU

Cybersecurity consultant @ WAVESTONE

Former dev @ autolib'

Former student @ TELECOM Paris

Disclaimer

Loi Godfrain (1988) relative à la fraude informatique / Article 323-1

	Intrusion non-autorisée, peu importe l'objectif	2 ans	60 000 €
	Altération au système et/ou atteinte au système	3 ans	100 000 €
	Données personnelles en jeu	5 ans	150 000 €

Auditeur / Pentester
Get paid to hack

Bug Bounty
Get paid to hack (freelance edition)

Challenges
~~Do not~~ try this at home !

DEFENSIVE  *OFFENSIVE*

Vulnerability hunting

Phishing

Red-Team

Blue-Team

Purple-Team

Application penetration testing

Threat hunting

Reverse Engineering

Internal penetration testing

Vishing

Forensic

Incident response

Internet exposure assessment

Bug Bounty

IAM

Organizational review

OSINT

Physical security testing

Audit outils aéroportuaires

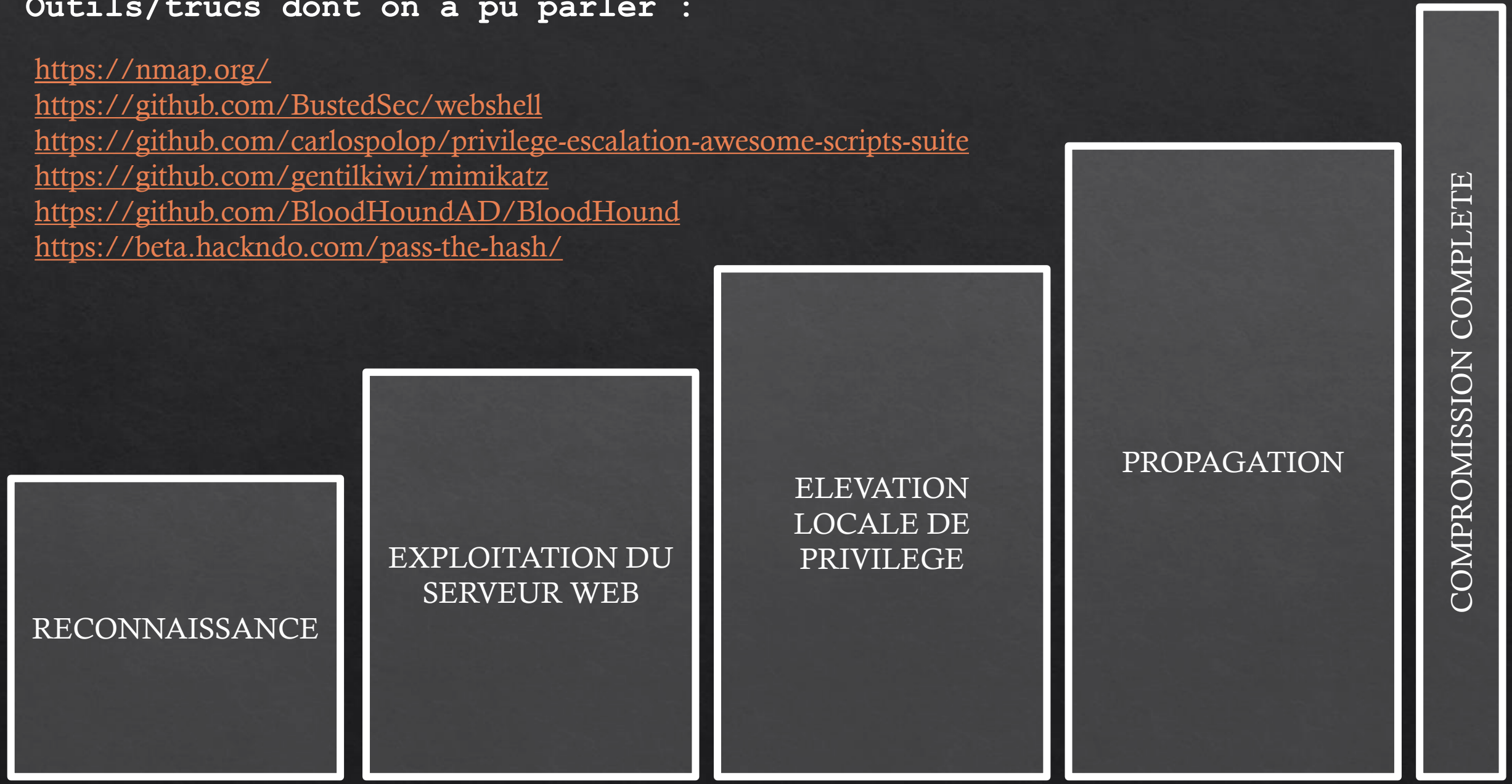
Campagne de phishing

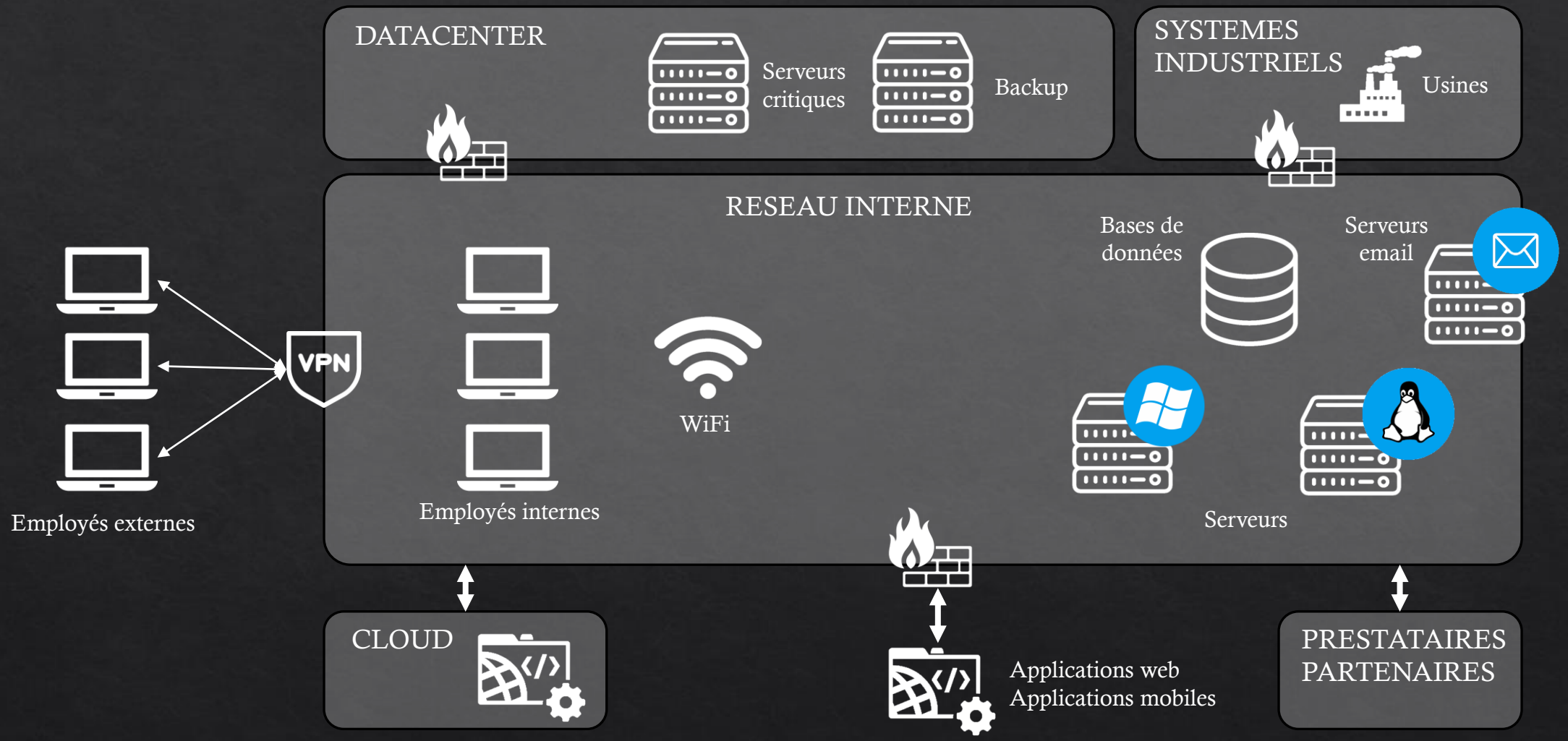
Red Team mondial

Audit d'application web e-commerce

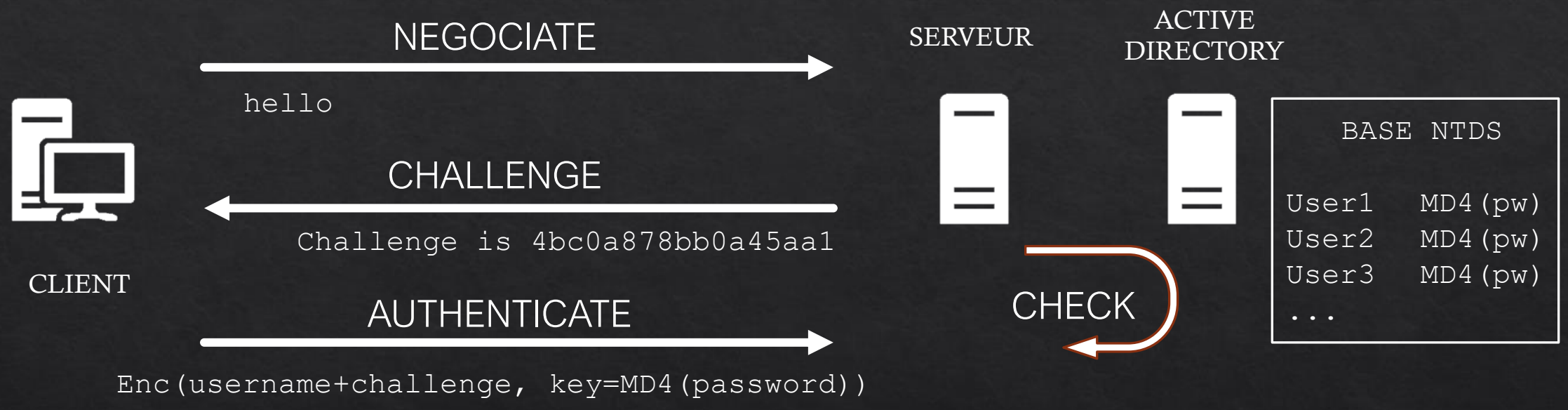
Outils/trucs dont on a pu parler :

https://nmap.org/
https://github.com/BustedSec/webshell
https://github.com/carlospolop/privilege-escalation-awesome-scripts-suite
https://github.com/gentilkiwi/mimikatz
https://github.com/BloodHoundAD/BloodHound
https://beta.hackndo.com/pass-the-hash/




DATACENTER
Serveurs critiques
Backup
SYSTEMES INDUSTRIELS
Usines
RESEAU INTERNE
Bases de données
Serveurs email
VPN
WiFi
Employés externes
Employés internes
Serveurs
CLOUD
Applications web
Applications mobiles
PRESTATAIRES PARTENAIRES

Authentification NTLM



Pass-The-Hash

Où trouver ces hash NTLM ?

Serveurs Windows

UTILISATEURS LOCAUX

Base SAM (fichiers)
Necessite d'être administrateur

Contrôleurs de domaine

TOUS LES UTILISATEURS (LOCAL=DOMAINE)

Base NTDS (fichiers)
Necessite d'être Admin de Domaine

UTILISATEURS DE DOMAINE

Mémoire du processus LSASS
Necessite d'être administrateur

```
cme smb -u Administrator -d the-best-dom.net -h <HASH NTLM> --lsa <TARGETS>

cme smb -u Administrator -d the-best-dom.net -h <HASH NTLM> --ntds <DC>
```

Conférences

Defcon

Hack in Paris

The Hack

Black Hat

Cyber Defense Summit

Blogs

https://pentestlab.blog/
https://krebsonsecurity.com/
http://pentestmonkey.net/
https://book.hacktricks.xyz/
https://adsecurity.org/

Plateformes

http://flaws.cloud/
https://w3challs.com/
https://www.hackthebox.eu/
https://tryhackme.com/

Questions ?