Red Team
au service du
Blue Team

par Martin Dubé

2019-04-08

Desjardins

Avertissement!

Les opinions exprimées dans cette présentation sont les miennes et pas nécessairement celles de mon employeur.

msf> sessions -l

- Intro
- Perception d’un Red Teamer
- Pistes de solutions
- Conclusion

Qui est derrière le Hoodie?

- Fier membre de l'équipe ETTIC (*Ethical Hackers*) chez Desjardins
  - Chef d'une pratique de *Red Team*
  - Réaliser des simulations d'adversaires **patients**
  - Mettre en place des terrains d'entraînements pour les équipes
  - Certifications: OSCE, OSCP, GREM, GCIH, GSEC
- *Challenge Designer* à NorthSec
  - Évènement de sécurité à Montréal de >1000 participants
  - CTF de 600 personnes *on-site*
- 10 ans de consultation
  - [2014-2018] GoSecure
    - Team Lead (1 ans)
    - Pentester (2 ans)
    - Spécialiste Checkpoint (2 ans)
  - [2009-2014] CGI
    - Analyste en sécurité (2 ans)
    - Analyste en TI (3 ans)
- [2010-2016] Impliqué dans le Hackfest
  - 5 ans membre du CA
  - 7 ans comme *Challenge Designer*
- Dec-Bac en Informatique

Définition

Blue Team

- Équipe qui défend son organisation contre des attaques
- Près des opérations
- Exclu:
  - Architecte
  - Analyste
  - Accompagnement de projet

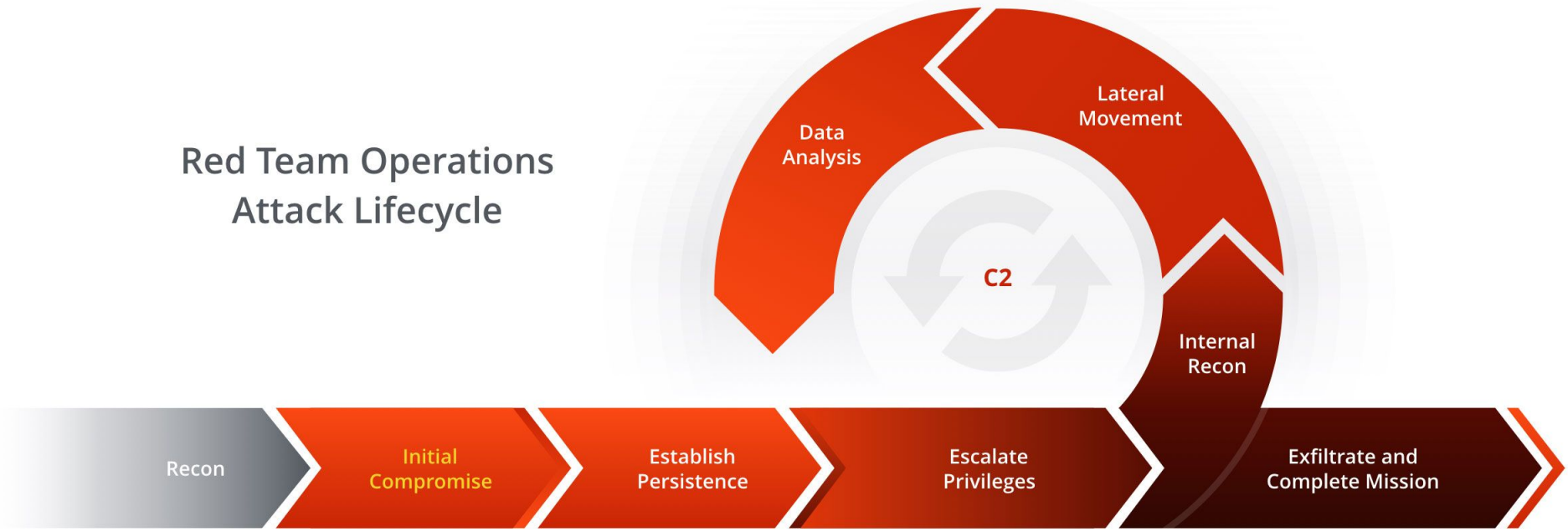
Red Team

- Équipe qui réalise des simulations d'adversaires
- Se démarque des *Pentesters*:
  - Scénarios
  - Objectifs
  - Détection > Mitigation
  - Un Blue Team est requis

Perception d’un Red Teamer

Bienvenue dans mon monde :)

Cyber Kill Chain



- Chaque phase est une opportunité de **mitiger** des attaques
- Chaque phase est une opportunité de **détecter** des attaques
- Objectif du **Blue Team**: rendre difficile le passage à la prochaine étape
- Objectif du **Red Team**: avancer dans le processus en mimiquant des comportements normaux d'utilisateurs

Source: https://github.com/infosecn1nja/Red-Teaming-Toolkit

Reconnaissance

- Fuite d'information
  - Collection #1 (772M)
  - MySpace (359M)
  - Linkedin (164M)
  - Source: https://haveibeenpwned.com/
  - Dropbox (67M)
  - LastFM (43M)
  - Et 7 milliards d'autres...
- Réseaux sociaux
  - Employés et leur titres sur Linkedin
  - Facebook
- Offres d'emplois
  - Recherche d'un spécialiste pour un produit précis
- Documentation publique ou semi-publique
  - Demande de Proposition (*RFP*) / Appel d'offre (AO)
- Site web de la compagnie
  - Adresses de courriels pour *phishing*
  - Exemple de documents aux couleurs de l'entreprise (utile pour *spear phishing*).

Accès Initiale

- Spear Phishing
  - “Bonjour Mr. le recruteur, voici mon CV.”
- Phishing
  - “Votre mot de passe doit être changé sur le site https://evil-cie.com”
- Intrusion d’un appareil dans le réseau
  - Raspberry Pi, Packet Squirrel
- Clé USB
  - Stocker un *malware et inviter une personne à l’exécuter*
  - *Simuler un clavier/sourie (Rubber Ducky)*
  - *Simuler une interface réseau (Lan Turtle)*
- Appel téléphonique
  - Inviter un employé à exécuter un programme malicieux
- *Password Spraying*
  - *Sites web en 1FA (Portails, Extranet, Accès VPN)*
- *Wi-Fi*
  - *Clé WPA2 Faible*
  - *Protocole d’authentification faible (PEAP -> MSCHAPv2)*

Persistence

- Privilèges utilisateur
  - Clé de registre
  - Répertoire de démarrage
  - Tâches planifiés
  - Profiles Powershell
- Privilèges administrateur
  - Services Windows
  - WMI
- Maintenir l'accès à long terme
  - Vol de mot de passe
  - Vol de *NTLM hash*
  - *Silver Tickets*
  - *Golden Tickets*

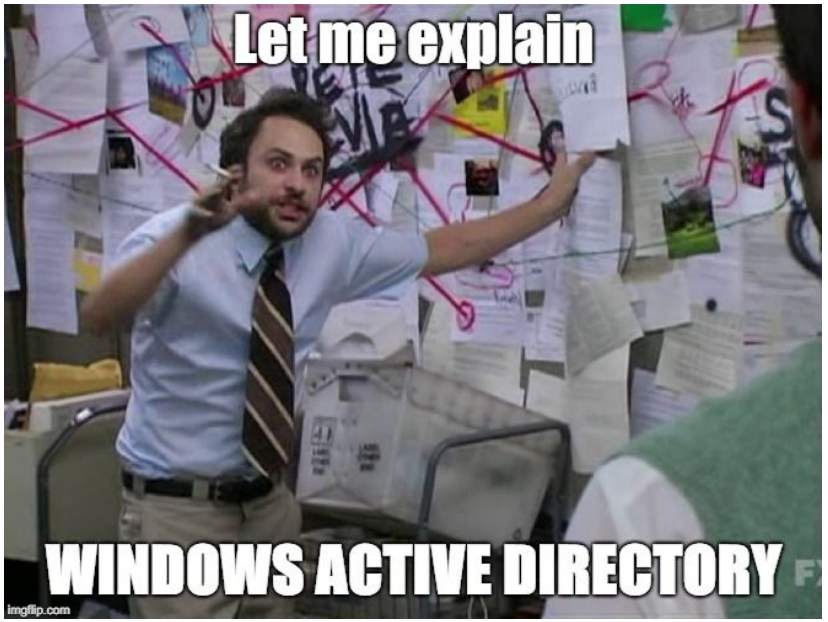
Escalation de Privilèges

- Privilèges utilisateur
  - Mot de passe
    - Dans des fichiers texte sur le poste
    - Dans des fichiers texte sur le réseau
    - Dans keepass avec un *Master password* faible
    - Dans les courriels
    - Mot de passe dans le champ Description de l'AD
  - Service qui s'exécute avec des droits élevés
  - Tâche planifié qui s'exécute avec des droits élevés
  - WSUS en HTTP
    - Permet d'être système sur n'importe quel machine du sous-réseau de l'attaquant (https://github.com/ctxis/wsuspect-proxy)

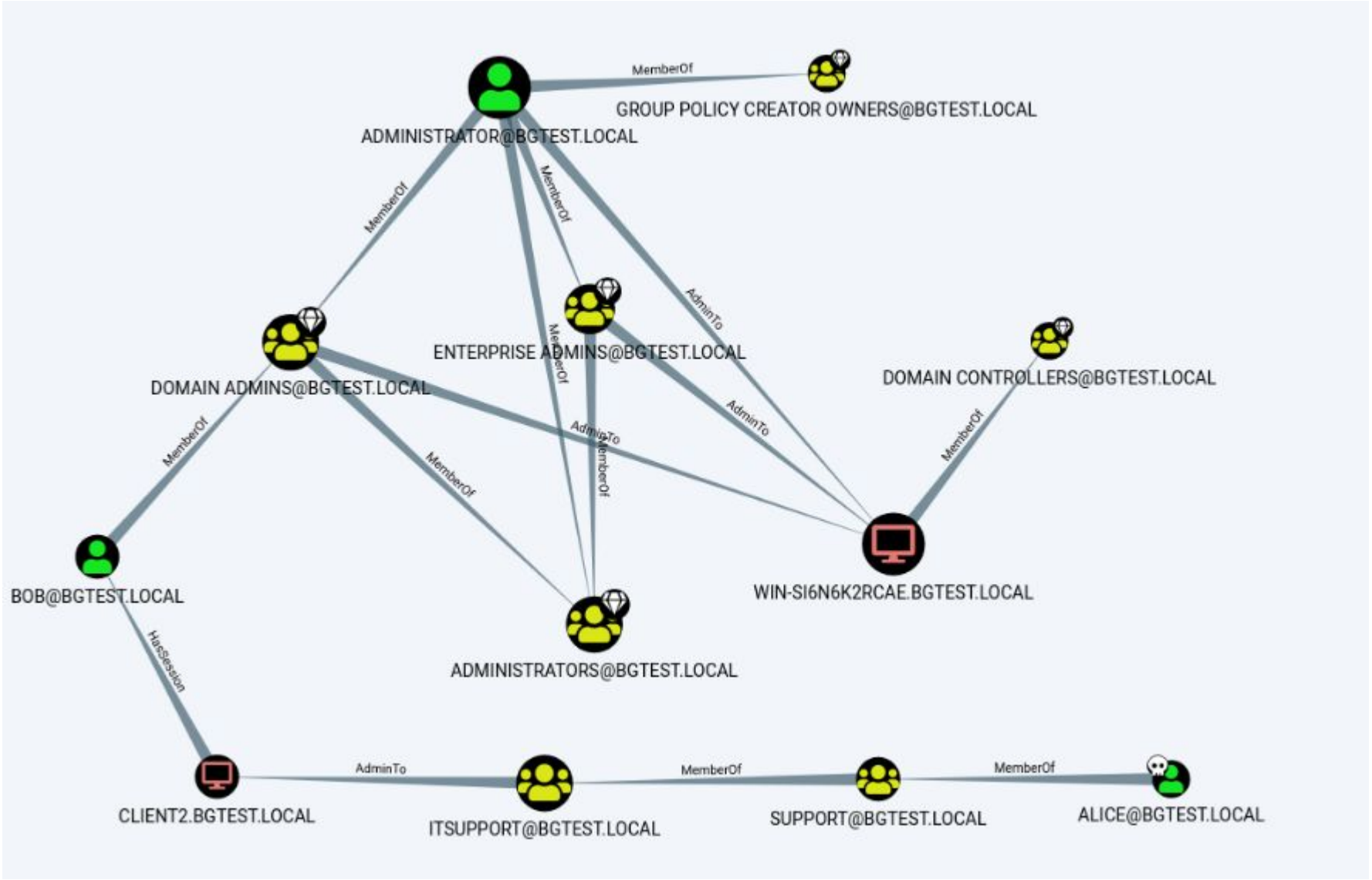
- Privilèges administrateur
  - 1001 techniques pour outrepasser UAC
  - .\mimikatz.exe
    - Récupérer des mots de passes en mémoire
    - Récupérer des *NTLM hash* en mémoire
    - Vol de tickets
    - DCSync

Reconnaissance Interne

- Active Directory est un annuaire qui se veut **accessible** par définition
  - Les GPO sont accessible par tous les utilisateurs authentifiés
    - \\domaine.com\SYSVOL
    - Group Policy Preferences (GPP)
    - Autre configuration sur les postes tel que le pare-feu, politique de sécurité
  - Énumération de tous les comptes et groupes
    - En particulier les comptes Domain Admin
  - Kerberoast
    - Récupérer des hash cassable
    - Récupérer des URL sensible
  - Délégation Kerberos
- Énumération sur le réseau
  - Politiques de mot de passe
  - Partage réseau
  - Service Windows (WinRM, SMB, RPC)
  - Qui est connecté où?
- Chemin vers *Domain Admin*
  - Bloodhound



Reconnaissance Interne (Bloodhound)



Déplacement Latéraux

- Un vaste éventail de protocoles
  - File Sharing (LLMNR, NetBios, SMB, iWARP)
  - Remote Assistance (PNRP, SSDP, TCP)
  - Remote Desktop (TCP, UDP, TCP-WS, TCP-WSS)
  - Remote Scheduled Tasks Management (RPC)
  - Remote Service Management (NP, RPC)
  - Windows Management Instrumentation (ASync, DCOM, WMI)
  - Windows Remote Management (HTTP, HTTPS)
- Avec le pare-feu Windows activé, **presque aucun de ces service est ouvert par défaut**
- La plupart supportent pass-the-hash ou pass-the-ticket

- Si un attaquant peut le faire, un *cryptolocker* peut aussi.

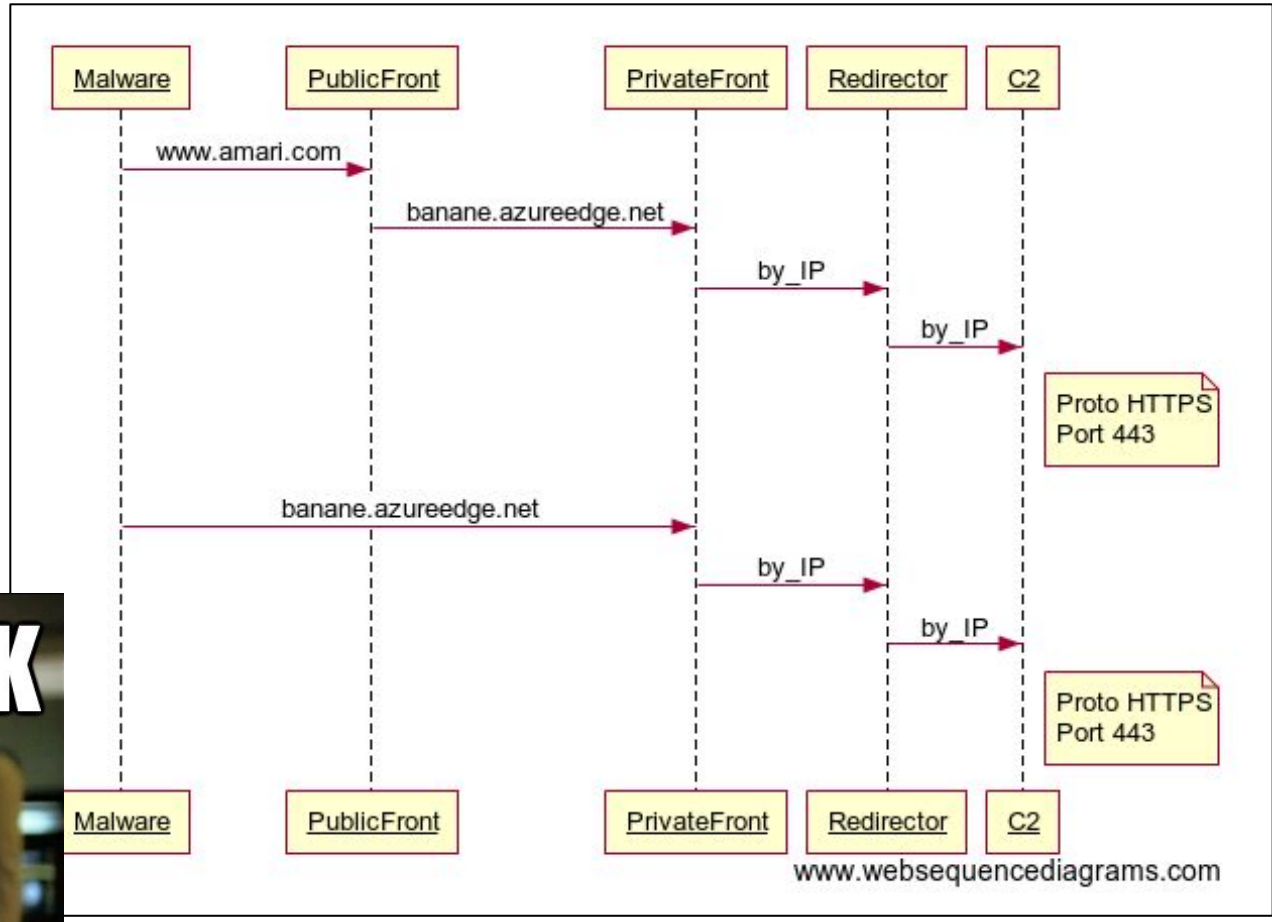
Exfiltration des données

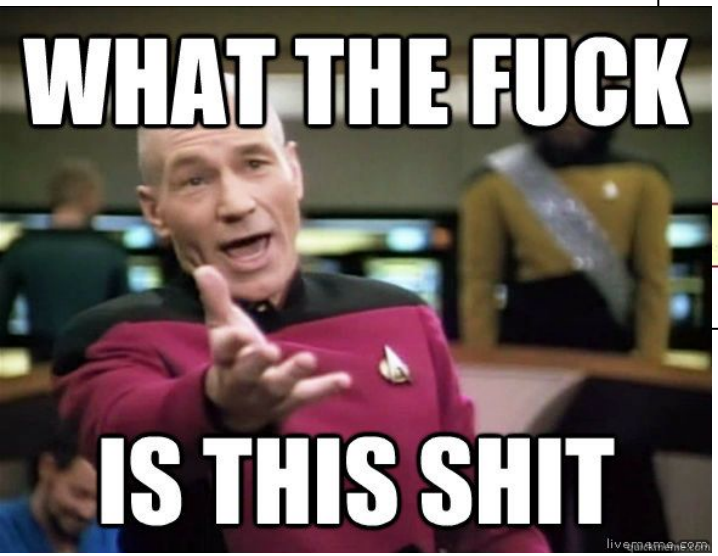
- Internet
  - Site web de l'attaquant: Webdav, Page de téléchargement
  - Site web publique: Google Drive, Dropbox, Amazon, Azure
  - Protocoles sécurisés: HTTPS, FTPS, SSH
- 3g / LTE
- Wi-Fi
- Clé USB

Et si on parlait de *Domain Fronting*

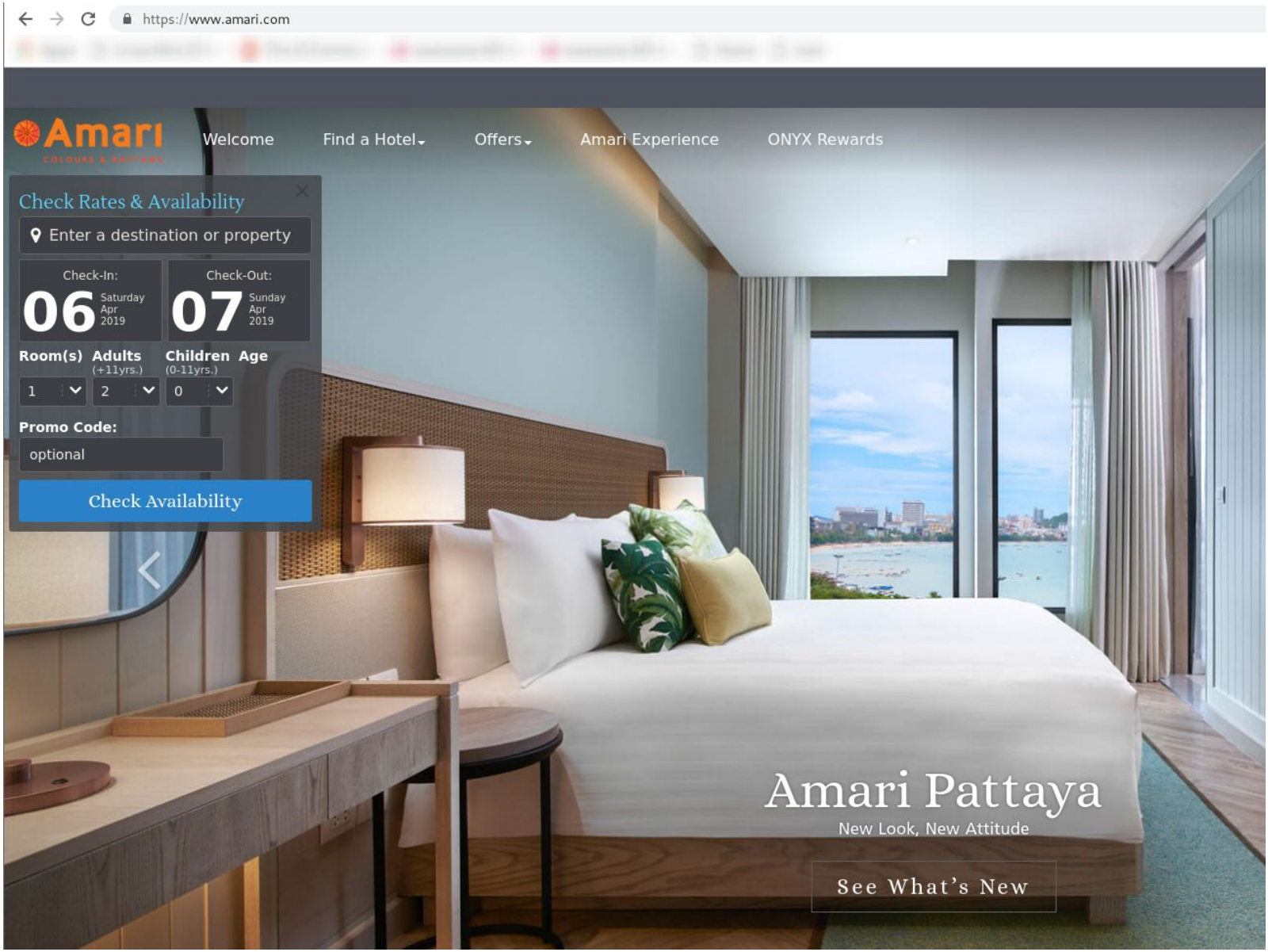
- Azure
  - ~400 domaines publique
  - Choix du préfix azuredge.net
- Amazon
  - ~90 000 domaines
  - Préfix aléatoire cloudfront.net
- Plusieurs autres:

  https://github.com/vysecurity/DomainFrontingLists





Aperçu de https://www.amari.com



Bref, Red et Blue ne s’affrontent pas à arme égale...

Modded: Lipo Battery

Réalité des 2 équipes

Blue Team	*Red Team*
▪ Doit couvrir **tous** les vecteurs ▪ Les outils sont dispendieux et fermé (pas accès au code source) ▪ Corriger une vulnérabilité prend entre 1 jour et 6 mois	▪ A besoin d'exploiter **un** vecteur ▪ Les outils sont gratuit et souvent libre de droit ▪ Identifier et divulguer une vulnérabilité prend entre 1h et 1 semaine

~200 techniques d'attaques à mitiger/détecter

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	SID-History Injection	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Scheduled Task	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	HISTCONTROL						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Hidden Files and Directories						
	Source	LSASS Driver	Sudo Caching	Hidden Users						
	Space after Filename	Launch Agent	Sudo	Hidden Window						

Source: https://attack.mitre.org/

~12 techniques d'attaques pour "gagner"

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command and Control
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	BITS Jobs	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Compiled HTML File	AppCert DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory Discovery	Exploitation of Remote Services	Data Staged	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Control Panel Items	AppInit DLLs	Application Shimming	CMSTP	Credentials in Files	Network Service Scanning	Logon Scripts	Data from Information Repositories	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History	Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Local System	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through API	Authentication Package	DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data from Network Shared Drive	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Execution through Module Load	BITS Jobs	Dylib Hijacking	Compiled HTML File	Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Data from Removable Media	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Exploitation for Client Execution	Bootkit	Exploitation for Privilege Escalation	Component Firmware	Hooking	Peripheral Device Discovery	Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	Graphical User Interface	Browser Extensions	Extra Window Memory Injection	Component Object Model Hijacking	Input Capture	Permission Groups Discovery	Remote Services	Input Capture		Multi-Stage Channels
	InstallUtil	Change Default File Association	File System Permissions Weakness	Control Panel Items	Input Prompt	Process Discovery	Replication Through Removable Media	Man in the Browser		Multi-hop Proxy
	LSASS Driver	Component Firmware	Hooking	DCShadow	Kerberoasting	Query Registry	SSH Hijacking	Screen Capture		Multiband Communication
	Launchctl	Component Object Model Hijacking	Image File Execution Options Injection	DLL Search Order Hijacking	Keychain	Remote System Discovery	Shared Webroot	Video Capture		Multilayer Encryption
	Local Job Scheduling	Create Account	Launch Daemon	DLL Side-Loading	LLMNR/NBT-NS Poisoning	Security Software Discovery	Taint Shared Content			Port Knocking
	Mshta	DLL Search Order Hijacking	New Service	Deobfuscate/Decode Files or Information	Network Sniffing	System Information Discovery	Third-party Software			Remote Access Tools
	PowerShell	Dylib Hijacking	Path Interception	Disabling Security Tools	Password Filter DLL	System Network Configuration Discovery	Windows Admin Shares			Remote File Copy
	Regsvcs/Regasm	External Remote Services	Plist Modification	Exploitation for Defense Evasion	Private Keys	System Network Connections Discovery	Windows Remote Management			Standard Application Layer Protocol
	Regsvr32	File System Permissions Weakness	Port Monitors	Extra Window Memory Injection	Securityd Memory	System Owner/User Discovery				Standard Cryptographic Protocol
	Rundll32	Hidden Files and Directories	Process Injection	File Deletion	Two-Factor Authentication Interception	System Service Discovery				Standard Non-Application Layer Protocol
	Scheduled Task	Hooking	SID-History Injection	File Permissions Modification		System Time Discovery				Uncommonly Used Port
	Scripting	Hypervisor	Scheduled Task	File System Logical Offsets						Web Service
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Gatekeeper Bypass						
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	HISTCONTROL						
	Signed Script Proxy Execution	LC_LOAD_DYLIB Addition	Startup Items	Hidden Files and Directories						
	Source	LSASS Driver	Sudo Caching	Hidden Users						
	Space after Filename	Launch Agent	Sudo	Hidden Window						

Source: https://attack.mitre.org/

Pistes de solutions

Trucs pour niveler le terrain de jeu

Le **comment** est aussi important que le **quoi**.

Solution #1 - Impliquer la sécurité offensive

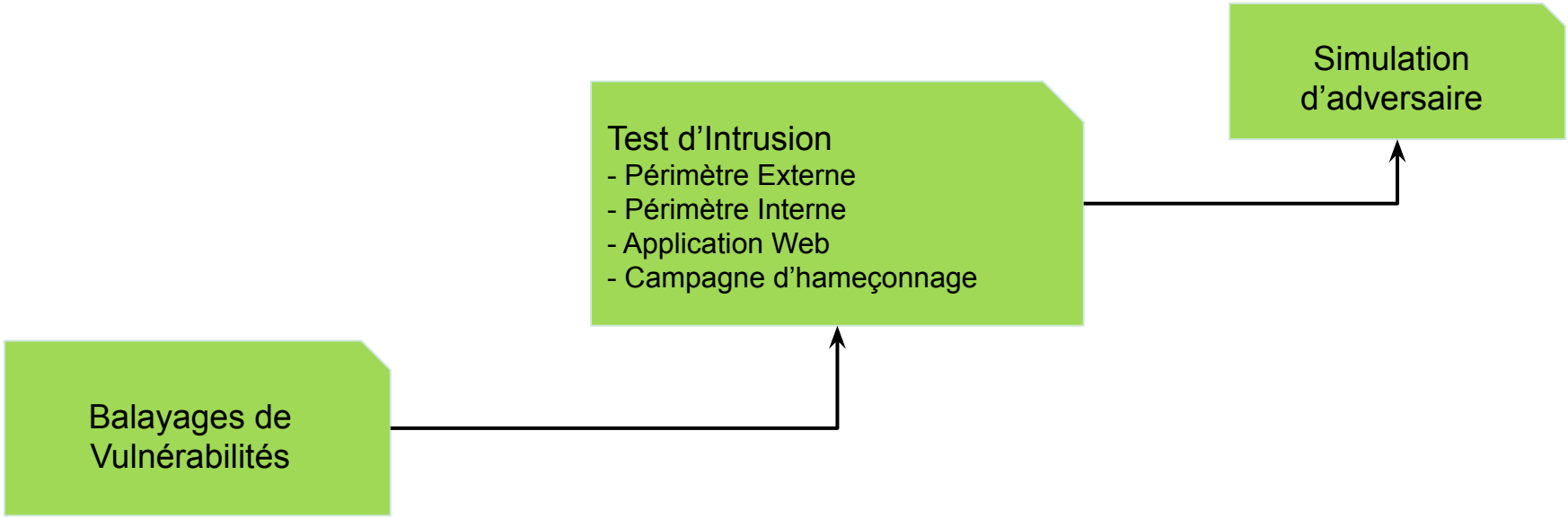
Quoi	Comment
❑ Balayage de Vulnérabilités	▪ Authentifié? Tous les ports? Tous les modules?
❑ Test d'intrusion	▪ Scope limité? Combien de temps?
❑ Anti-Virus	▪ Déployé partout? Activé partout? Alertes centralisés?
❑ Pare-feu sur les postes	▪ Activé inbound? Activé outbound?

Solution #1 - Impliquer la sécurité offensive

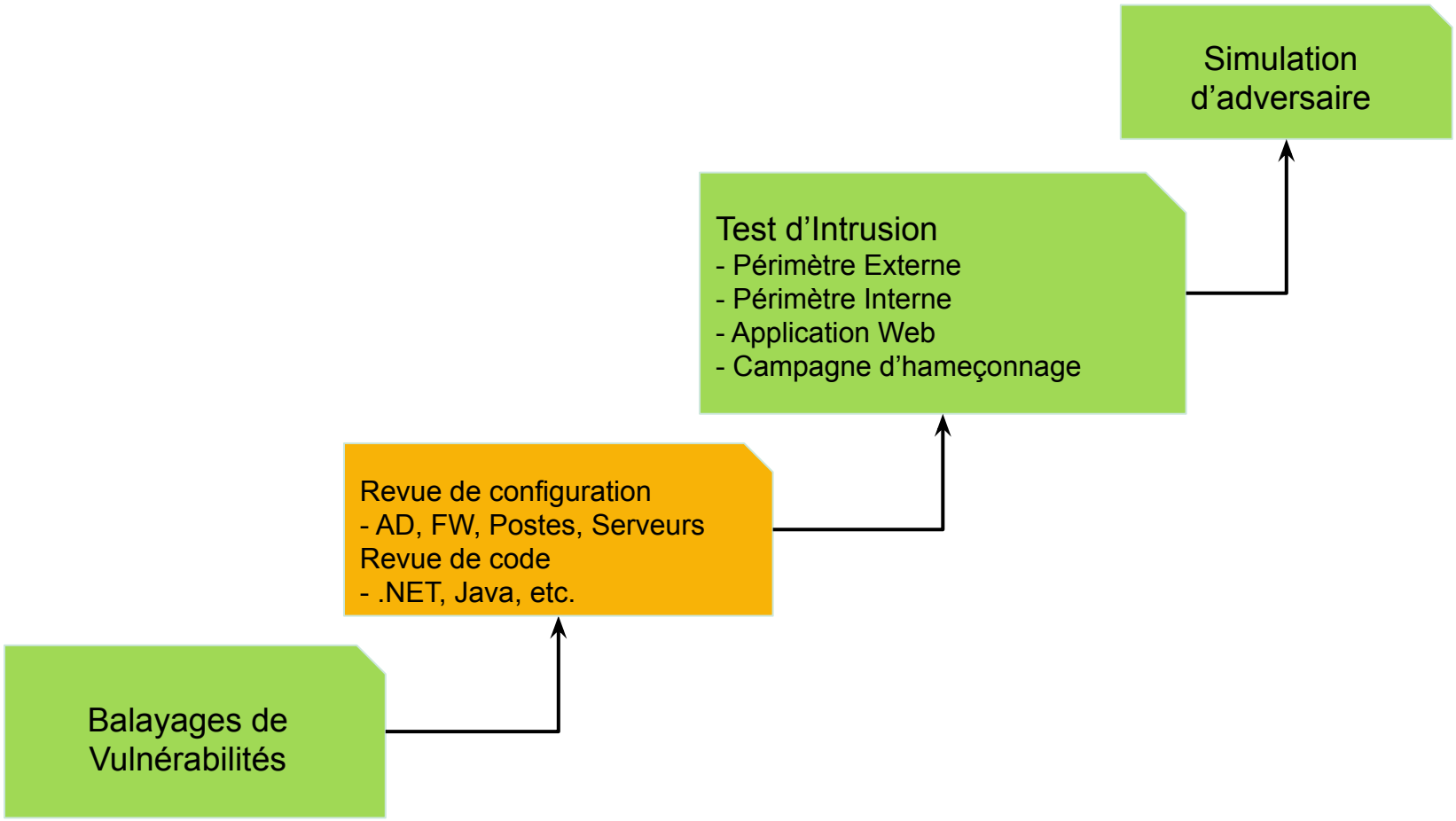
Quoi (*Blue Team*)	Comment (*Red Team*)
❑ Balayage de Vulnérabilités	▪ Authentifié? Tous les ports? Tous les modules?
❑ Test d'intrusion	▪ Scope limité? Combien de temps?
❑ Anti-Virus	▪ Déployé partout? Activé partout? Alertes centralisés?
❑ Pare-feu sur les postes	▪ Activé inbound? Activé outbound?

Solution #1 - Impliquer la sécurité offensive

- Modèle **simplifié** de croissance en sécurité



Solution #1 - Impliquer la sécurité offensive



Il n’est plus question de **si** on sera compromis mais plutôt de **quand**.

Solution #2 - *Purple Teaming*

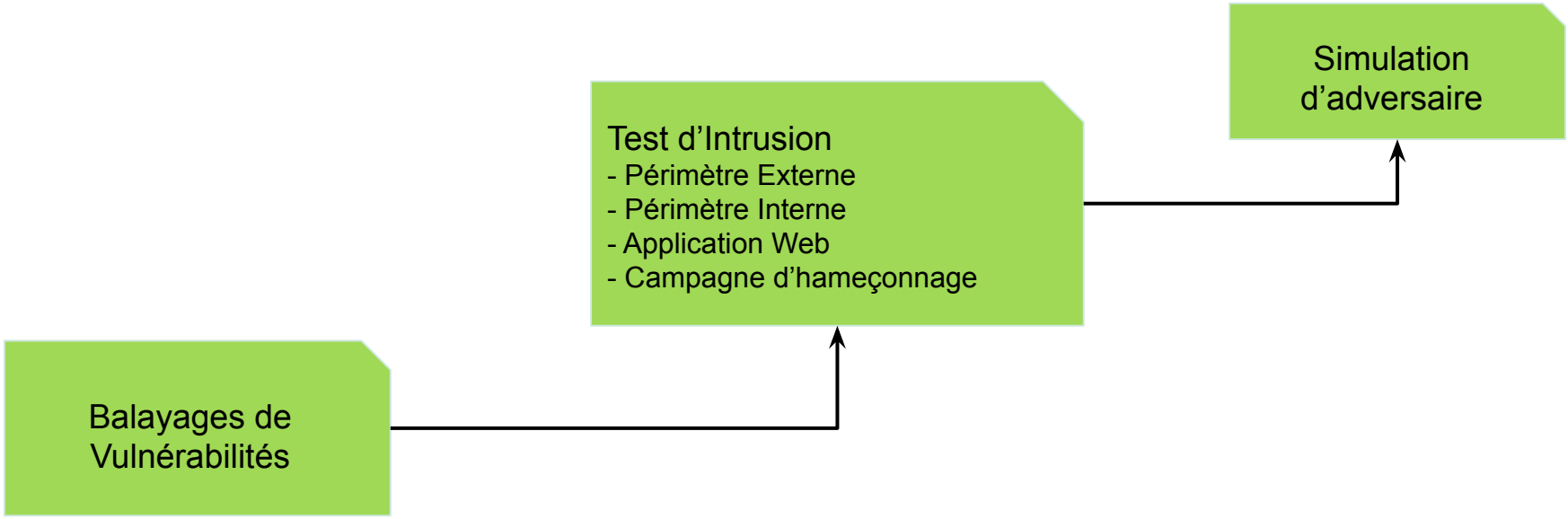
- À quoi bon se battre à arme inégale…
- Solution: Purple Team
  - Red font leurs attaques
  - Blue font leur surveillance
  - Communications rapprochés
  - Résultat: Développement de cas de détection en accéléré (*use case*)

- Orienté sur le partage de connaissance
  - On se dit ***TOUT***
  - Aucune cachette sur les TTPs
  - Aucune cachette sur les cas de détection

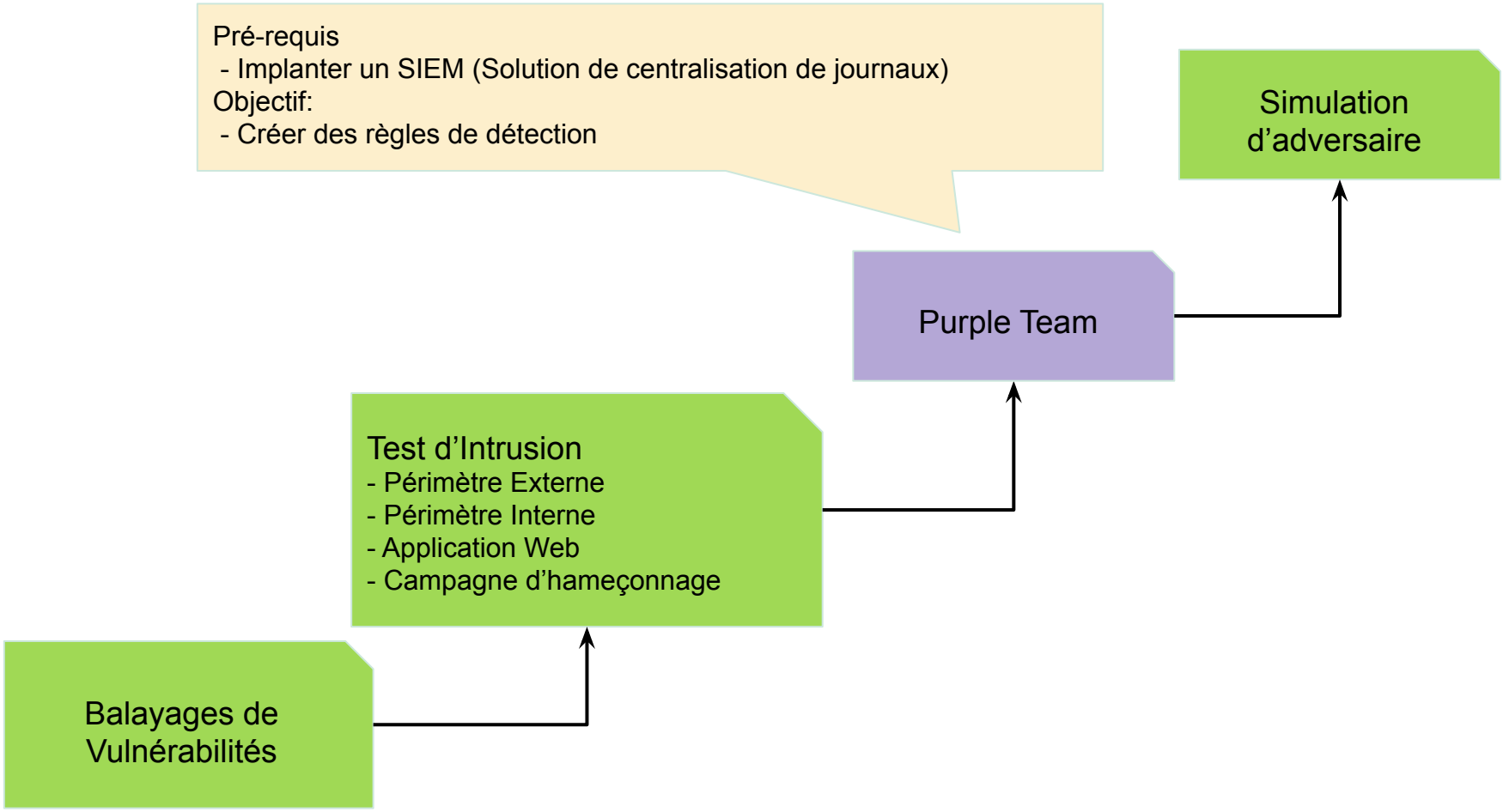
- Permet aux 2 équipes de se développer

Solution #2 - *Purple Teaming*

- Modèle **simplifié** de croissance en sécurité



Solution #2 - *Purple Teaming*



Solution #2 - *Purple Teaming* (Choses à éviter)

- Discours toxique de Red Team
  - Ça c'est de la marde
  - Il faut être incompétent pour faire ça
- Discours toxique de Blue Team
  - Les Red brisent, les Blue réparent
  - Est-ce que c'est vous?
  - C'était en dehors de la portée!
- L'ignorance n'est pas de l'incompétence
  - On est tous ignorant de quelque chose
- La passion n'excuse pas les discours rude
  - À chacun son niveau de passion

Solution #2 - *Purple Teaming* (Choses à éviter)

- Les *Fails* sont partout et il y en aura toujours
  - Red fait crasher un contrôleur de domaine. Oops
  - Blue désactive une règle de détection “temporairement”. Oops
  - Un sysadmin met le mot de passe “Password1” à un compte. Oops

- Essayez-vous de gagner ou de protéger?
  - L'ego est une énergie qui se canalise
  - Autant Blue et Red sont fier de ce qu’ils font, il faut respecter ça!
  - Quand Red réussit, ils célèbrent l’exploit et non la vulnérabilité
  - Quand Blue réussit, ils célèbrent que le mécanisme fonctionne, non pas l’échec de Red

Conclusion

- Restez positif! Il y a des solutions!
- Un éléphant se mange 1 bouché à la fois.
- Soyez créatif (les 2 équipes)!
- Entraînez-vous!
  - https://ringzer0ctf.com/
  - https://hackfest.ca/fr/ctf/
  - https://www.nsec.io/competition/

- Inspiration pour cette présentation:
  - Victor or Victim Strategies for Avoiding an InfoSec Cold War https://www.youtube.com/watch?v=9_cZ5xn-huc
  - Red Vs. Blue: Modern Active Directory Attacks, Detection, And Protection https://www.youtube.com/watch?v=b6GUXerE9Ac

Merci!

Questions?

p.s. on recrute: https://desjardins.wd3.myworkdayjobs.com/Desjardins

Desjardins