Red TEAM vs Blue TEAM
du concept au retour d'expérience

COMCYBER - Sébastien BOMBAL
DGA Maitrise de l'Information – Gilles YONNET
Conférences C&ESAR 2017




Pourquoi monter un exercice Red Team Vs Blue Team ?

Risque subi
- Incidents
- Crises

Risque évité
- Audits / tests d'intrusion
- Anticipation

Risque imaginé
- Analyses de risque

Réduire le risque

Et si le risque résiduel se matérialisait…

- Avons-nous bien évalué l'impact ?
- Peut-on encore le réduire ?
- Quel est le niveau de maturité et de préparation opérationnelle pour y faire face ?

Comment concrétiser pour convaincre d'un risque systémique ?
Comment identifier de nouveaux risques ?
Quel est le niveau de préparation face à une menace spécifique ?
Serons nous en mesure de détecter ? Chasser ? Entraver ? Reconquérir ? Reconstruire ? Répondre ?
….

De la SSI Cyberprotection → Anticipation, Planification, Préparation opérationnelle, Exercices → A la lutte informatique défensive

Comment monter un exercice Red Team Vs Blue Team ?

- Anticipation
- Définir les objectifs d'entrainement
- Planification (opération offensive)
- Définir/préparer le terrain d'entrainement
- Définir l'organisation de l'exercice

Cibler, se renseigner , identifier les effets redoutés sur la situation ami
Se renseigner et anticiper les modes d'action ennemie

Scénario, effets à obtenir, processus de ciblage, idée de manœuvre, conditions initiales, menace simulée, renseignement disponible, périmètre...

« Cyber range » versus « LIVEX/Live exercice »

Précision des rôles, des responsabilités et de processus en particulier
1° le processus de déconfliction,
2° les règles de SEC OPS,
3° les règles d'engagement (ROE).

Manning des équipes BLUE, RED, WHITE, YELLOW, GREEN… Média.

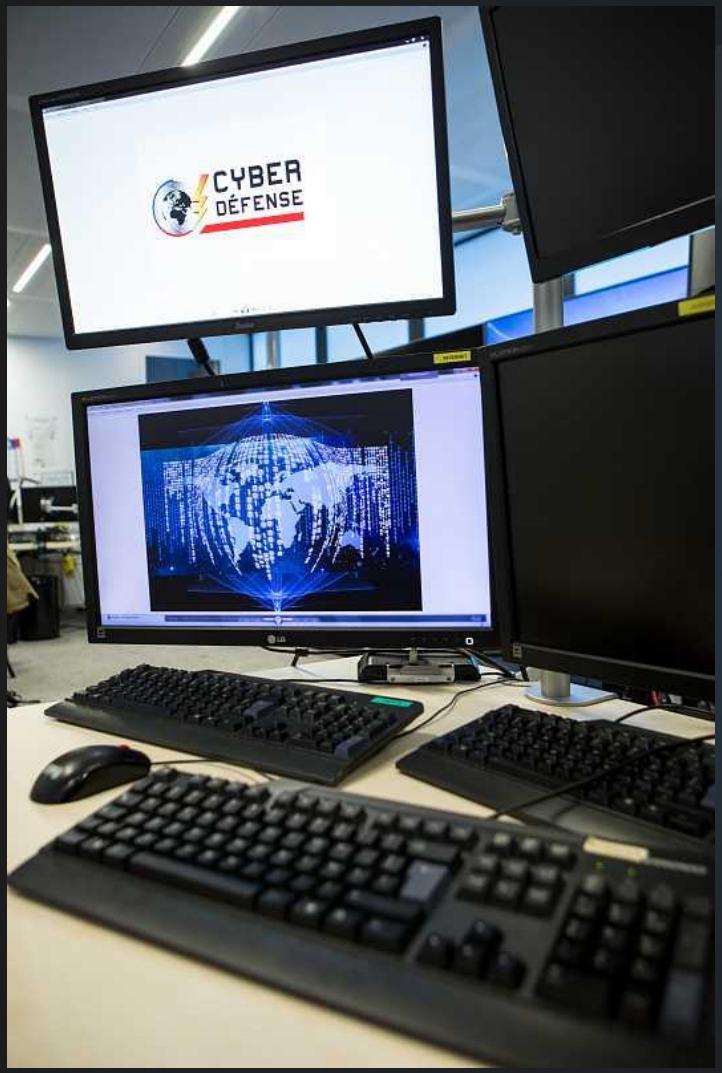
Processus de planification d'un exercice (CYBER)

- IPC : Initial Planning Conference
- MPC : Mid-Term Planning Conference
- FPC : Final Planning Conference

→ MSEL Master Scenario Event List

→
- Note d'organisation de l'exercice ou
- ordre d'opération

RETEX in a nutshell



Durée ?

- Entrainement face à un APT ➔ plusieurs mois
- Entrainement face à un DDOS ➔ quelques jours

ROE ?

- Intérêts d'entrainer face à des modes d'action ennemie
- Ex : type social engineering, détournement des moyens de lutte informatique défensive, usage de la tromperie, technique de sabotage, dénis de service, persistance/backdoor…

Terrain ?

- LIVEX définitivement
- Bien choisir les trophées/cibles à atteindre
- Bien préparer en amont la MSEL et la planification pour les RED

Manning

- Ne pas sous-estimer le rôle des WHITE et GREEN TEAM
- Bien dimensionner une phase d'assainissement, renforcement immédiat post exercice

Red Team vue des tranchées

Illustration et RETEX

Objectif, Cible & Positionnement

Objectif : vol de données à caractères sensibles

Risque associé : opération de déstabilisation/influence

Cible : application web sur intranet d'une enclave

Positionnement Red Team : Sur Internet

Infiltration

Aucun service accessible depuis Internet

→ Accès Physique (direct ou indirect) (Clé USB…)

… Ou Phishing…:

1. Trouver des adresses cibles :
   - Il y a forcément des adresses exposées :
     - Pour des obligations métiers : service achat, communication, RH…
     - Parfois par négligence…

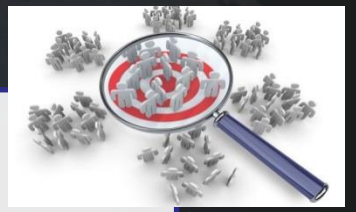
   Google is your friend !
2. Crédibiliser le mail envoyé
   - Chartes graphiques facilement récupérables
   - Nom de domaine et adresse émettrice crédible
   - Exploiter des préoccupations universelles : candidature, info formation etc…
3. Elaborer et distribuer la charge utile
   - Degré d'intelligence embarquée
   - Canal, protocole

→Efficacité faible… mais pas nulle (30% dans certains cas)

Recherche cible

Infiltration

Recherche cible



- Utilisation des ressources internes :
  - DNS
  - Documents
  - Intranet / Moteur de recherche
  - Annuaire

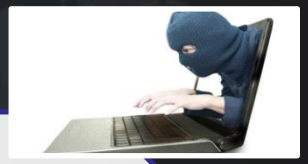
… Le contact est indiqué sur la page web

Prise de contrôle cible

Infiltration

Recherche cible

Prise de contrôle cible



1. Récupération des identifiants d'administration locaux

2. Tentative de connexion distante sur poste cible : Echec
3. Tentative de connexion sur contrôleur de domaine : Succès !
4. Extraction des identifiants d'administration du domaine
5. Connexion au poste du contact ciblé

Compte oublié sur le contrôleur de domaine = maillon faible

Atteinte objectifs

Infiltration

Recherche cible

Prise de contrôle cible

Atteinte objectif

- Extraction des mots de passe de connexion à l'application web dans son trousseau de navigateur
- Extraction et exfiltration des données à caractères sensibles du serveur

Mais alors ?

- La Red Team gagne toujours à la fin ?
  - NON !
  - Ce n’est toujours qu’une question de temps pour que la Blue team trouve et entrave
  - La répétition d’exercices bleu-rouge permet de diminuer ce délai
- Conditions de la réussite : une relation de confiance à construire dans la durée
  - Un exercice ou un test d’intrusion n’est pas une sanction
    - Eviter les surréactions de la défense
    - Valoriser les avancées obtenues par les exercices


KEEP
CALM
AND
ASK
QUESTIONS