

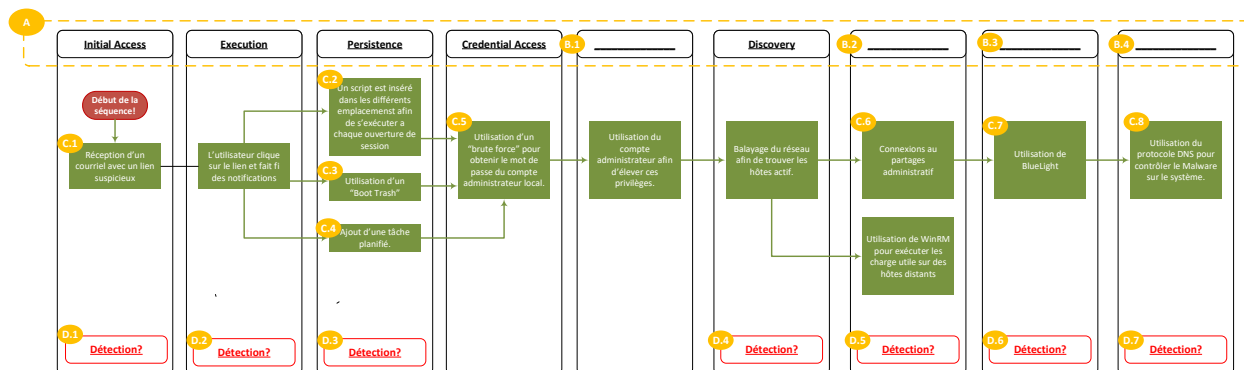
Consigne

- L'ensemble des réponses doivent être documentées et appuyées de captures d'écran. Même si la réponse est correcte si elle n'est pas documentée votre note sera de 0 point.
- Vous devez faire preuve d'analyse et de recherche dans les réponses que vous fournissez.
- Veuillez soumettre vos devoirs sous forme de fichiers PDF ou DOC et présenter vos réponses sous les questions ci-dessous en les copiant telles quelles avec leur numéro de question.
- Attention, utilisez votre propre compte utilisateur afin d'effectuer les opérations dans la plateforme Security Onion.
- L'ensemble des règles que vous allez créer pour les exercices 7 et 8 doivent contenir votre nom et prénom.

Exercice #1 : MITRE ATT&CK (15p)

La figure qui suit, représente la modélisation d'un « malware » fictif via le modèle MITRE ATT&CK. Analysez ce dernier, et répondez aux différentes questions.

Afin de répondre à chacune des questions, référez-vous à la lettre correspondante de la figure.



A) Sur la figure, à quoi correspond les titres de l'encadré? (1p)

Aux tactiques

B) Complétez ce qui manque : (2p)

B.1 : Privilege Escalation

B.2 : Lateral Movement

B.3 : Collection

B.4 : Command and Control

C) Identifiez les techniques du MITRE ATT&CK correspondantes : (4p)

C.1 : Phishing

C.2 : Boot or Logon Autostart Execution

C.3 : Pre-OS Boot

C.4 : Scheduled Task/Job

C.5 : Brute Force

C.6 : Remote Services

C.7 : Archive Collected Data

C.8 : Application Layer Protocol

D) Identifiez comment chacune des techniques mentionnées auraient pu être détecté dans le cadre de l'attaque en cause (outil / exemple etc.). (8p)

D1

Surveiller les nouveaux fichiers créés à partir de messages de phishing pour accéder aux systèmes des victimes. Nous aurions également pu surveiller les journaux d'applications tierces, les messages et/ou autres artefacts qui peuvent envoyer des messages de phishing pour accéder aux systèmes des victimes. Le filtrage basé sur DKIM+SPF ou l'analyse des en-têtes peut aider à détecter lorsque l'expéditeur de l'e-mail est usurpé. L'inspection des URL dans les e-mails (y compris l'expansion des liens raccourcis) peut aider à détecter les liens menant à des sites malveillants connus. Les chambres de détonation peuvent être utilisées pour détecter ces liens et soit aller automatiquement sur ces sites pour déterminer s'ils sont potentiellement malveillants, soit attendre et capturer le contenu si un utilisateur visite le lien.

D2

Mettre un contrôle d'application puisque ce dernier peut être en mesure d'empêcher l'exécution d'exécutables se faisant passer pour d'autres fichiers. Aussi, si un lien est visité par un utilisateur, les systèmes de prévention d'intrusion réseau comme suricata, snort, etc. et les systèmes conçus pour

analyser et supprimer les téléchargements malveillants peuvent être utilisés pour bloquer l'activité. Finalement, si un lien est visité par un utilisateur, bloquez par défaut les fichiers inconnus ou inutilisés en transit qui ne devraient pas être téléchargés ou selon une politique à partir de sites suspects comme bonne pratique pour prévenir certains vecteurs, tels que .scr, .exe, .pif, .cpl, etc. Certains dispositifs d'analyse de téléchargement peuvent ouvrir et analyser des formats compressés et cryptés, tels que zip et rar qui peuvent être utilisés pour dissimuler des fichiers malveillants.

D3

Surveiller les commandes exécutées et les arguments qui peuvent configurer les paramètres système pour exécuter automatiquement un programme lors du démarrage ou de la connexion au système afin de maintenir la persistance ou de gagner des privilèges de niveau supérieur sur les systèmes compromis. Nous pourrions aussi surveiller toute activité inhabituelle d'installation de pilote de noyau (kernel) qui pourrait configurer les paramètres système pour exécuter automatiquement un programme lors du démarrage ou de la connexion au système afin de maintenir la persistance ou de gagner des privilèges de niveau supérieur sur les systèmes compromis. Aussi, configurer les paramètres des tâches planifiées pour forcer les tâches à s'exécuter sous le contexte du compte authentifié plutôt que de les laisser s'exécuter en tant que SYSTEM. La clé de registre associée se trouve HKLM\SYSTEM\CurrentControlSet\Control\Lsa\SubmitControl. Le paramètre peut être configuré via GPO : Configuration de l'ordinateur > [Stratégies] > Paramètres Windows > Paramètres de sécurité > Options de sécurité > Contrôleur de domaine : Autoriser les opérateurs de serveurs à planifier des tâches, définir sur désactivé.

D4

Pour prévenir la technique de l'image pour la tactique Discovery, nous devons nous assurer que les ports et services inutiles sont fermés pour prévenir tout risque de découverte et d'exploitation potentielle. Deuxièmement, utiliser des systèmes de détection/prévention d'intrusions réseau pour détecter et prévenir les scans de service à distance. Finalement, nous devons nous assurer que la segmentation de réseau appropriée est suivie pour protéger les serveurs et les appareils critiques. Pour la détecter, nous pouvons surveiller les commandes exécutées et les arguments qui peuvent tenter d'obtenir une liste des services en cours

d'exécution sur des hôtes distants, y compris ceux qui peuvent être vulnérables à une exploitation logicielle à distance.

D5

Utiliser l'authentification à facteurs multiples pour les connexions distantes aux services lorsque c'est possible. Aussi, limiter les comptes qui peuvent utiliser les services à distance. Limiter les autorisations pour les comptes qui sont plus susceptibles d'être compromis ; par exemple, configurer SSH pour que les utilisateurs ne puissent exécuter que des programmes spécifiques. Pour la détection, surveiller les comptes d'utilisateurs connectés à des systèmes auxquels ils n'auraient normalement pas accès ou à des schémas d'accès anormaux, tels que plusieurs systèmes sur une période relativement courte. Corréler l'utilisation de l'activité de connexion liée aux services à distance avec un comportement inhabituel ou une autre activité malveillante ou suspecte. Les adversaires devront probablement apprendre à connaître l'environnement et les relations entre les systèmes grâce aux techniques de découverte avant de tenter un mouvement latéral. Par exemple, sur macOS, vous pouvez consulter les journaux pour les messages d'événements "screensharing" et "Authentication".

D6

Pour la détecter, surveiller les commandes exécutées et les arguments pour des actions qui faciliteront la compression ou le chiffrement des données collectées avant l'exfiltration, telles que tar. Aussi, surveiller les nouveaux fichiers construits qui sont écrits avec des extensions et/ou des en-têtes associés à des types de fichiers compressés ou chiffrés. Les efforts de détection peuvent se concentrer sur l'activité d'exfiltration suivante, où les fichiers compressés ou chiffrés peuvent être détectés en transit avec un système de détection d'intrusion réseau ou de prévention de perte de données analysant les en-têtes de fichier. Finalement, nous pouvons aussi surveiller les processus nouvellement créés et/ou les lignes de commande qui facilitent la compression ou le chiffrement des données collectées avant l'exfiltration, telles que 7-Zip, WinRAR et WinZip.

D7

Surveiller et analyser les modèles de trafic et l'inspection de paquets associés aux protocoles, en utilisant l'inspection SSL/TLS pour le trafic chiffré, qui ne suivent pas les normes de protocole et les flux

de trafic attendus (par exemple, les paquets superflus qui n'appartiennent pas aux flux établis, les modèles de trafic gratuits ou anormaux, la syntaxe ou la structure anormale). Considérer la corrélation avec la surveillance des processus et la ligne de commande pour détecter l'exécution de processus anormaux et les arguments de ligne de commande associés aux modèles de trafic (par exemple, surveiller les anomalies dans l'utilisation de fichiers qui n'initient normalement pas de connexions pour les protocoles respectifs). Aussi, nous pouvons également surveiller et analyser les flux de trafic qui ne suivent pas les normes de protocole et les flux de trafic attendus (par exemple, les paquets superflus qui n'appartiennent pas aux flux établis, ou les modèles de trafic gratuits ou anormaux). Considérer la corrélation avec la surveillance des processus et la ligne de commande pour détecter l'exécution de processus anormaux et les arguments de ligne de commande associés aux modèles de trafic (par exemple, surveiller les anomalies dans l'utilisation de fichiers qui n'initient normalement pas de connexions pour les protocoles respectifs).

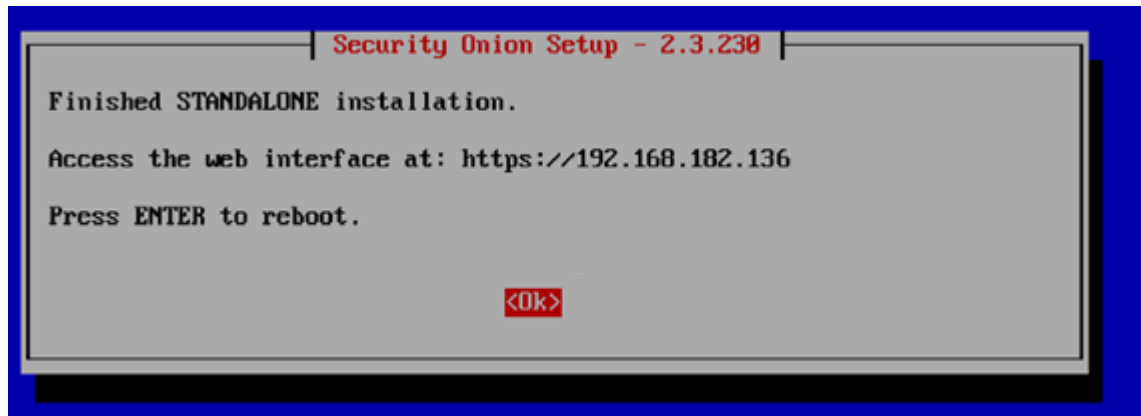
Exercise 2– Purple Teaming (55p)

Pour cet exercice, vous utiliserez WinADHD et SecurityOnion configuré avec une configuration Standalone.

- a) Configurez Security Onion en mode Standalone et installez Sysmon sur WinADHD et envoyez les journaux Sysmon à Security Onion. **Vous n'avez pas besoin de documenter toutes les étapes, juste une capture d'écran de votre page Hunt de Security Onion où nous pouvons voir les topics Sysmon est suffisant (7p)**
 - a. Si vous voulez, vous pouvez utiliser la version CentOS de Security Onion
<https://docs.securityonion.net/en/2.3/installation.html>

Réponse

Nous commençons par installer security onion en mode *standalone*



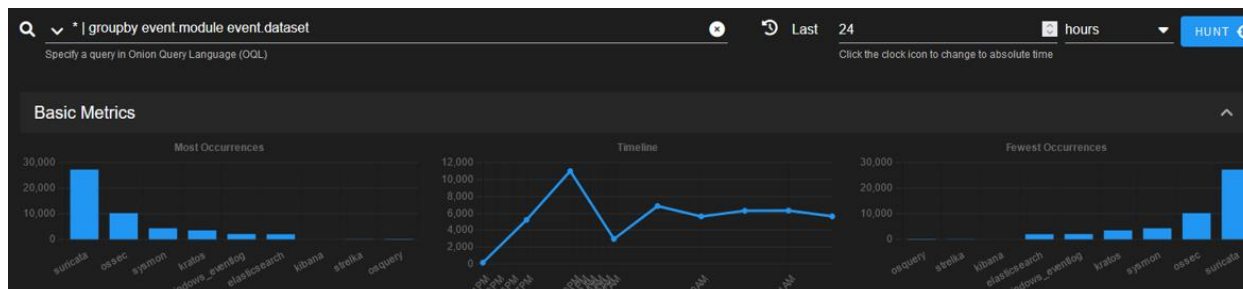
Installation et configuration de sysmon

```
PS C:\Users\adhd\Desktop\sysmon> .\Sysmon64.exe -accepteula -i sysmonconfig-export.xml

System Monitor v14.16 - System activity monitor
By Mark Russinovich and Thomas Garnier
Copyright (C) 2014-2023 Microsoft Corporation
Using libxml2. libxml2 is Copyright (C) 1998-2012 Daniel Veillard. All Rights Reserved.
Sysinternals - www.sysinternals.com

Loading configuration file with schema version 4.50
Sysmon schema version: 4.83
Configuration file validated.
Sysmon64 installed.
SysmonDrv installed.
Starting SysmonDrv.
SysmonDrv started.
Starting Sysmon64..
Sysmon64 started.
```

Info sysmon dans le Security Onion Hunt



- b) Mettez à jour votre Atomic Read Team dans la machine ADHD. Exécutez les tests suivants et identifiez-le dans Security Onion (Hunt ou Kibana)
 - a. T1059.005 - Command and Scripting Interpreter: Visual Basic – 1 test (3p)

Nous pouvons voir ici où nous mettons à jour le *AtomicRedTeam*

```
PS C:\AtomicRedTeam> IEX ([MR 'https://raw.githubusercontent.com/redcanaryco/Invoke-AtomicRedTeam/master/install-atomicredteam.ps1' -UseBasicParsing);
PS C:\AtomicRedTeam> Install-AtomicRedTeam -getAtomics -Force
Installation of Invoke-AtomicRedTeam is complete. You can now use the Invoke-AtomicTest Function
See Wiki at https://github.com/redcanaryco/Invoke-AtomicRedTeam/wiki for complete details
```

Nous effectuons la commande pour pouvoir voir les brefs détails du test en question

```
Administrator: Windows PowerShell
PS C:\AtomicRedTeam> Invoke-AtomicTest T1059.005 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1059.005-1 Visual Basic script execution to gather local computer information
T1059.005-2 Encoded VBS code execution
T1059.005-3 Extract Memory via VBA
PS C:\AtomicRedTeam>
```

Nous regardons ensuite les prérequis et lorsqu'il n'y en a pas, nous commençons simplement le test

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1059.005 -TestNumbers 1 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1059.005-1 Visual Basic script execution to gather local computer information
Prerequisites met: T1059.005-1 Visual Basic script execution to gather local computer information
PS C:\AtomicRedTeam>
```

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1059.005 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1059.005-1 Visual Basic script execution to gather local computer information
Done executing test: T1059.005-1 Visual Basic script execution to gather local computer information
PS C:\AtomicRedTeam>
```

Résultats dans *Hunt*

```
Process Details:
RuleName: -
UtcTime: 2023-04-24 18:21:56.623
ProcessGuid: {b1a62ae4-c8c4-6446-d205-000000003500}
ProcessId: 8068
Image: C:\Windows\System32\cmd.exe
FileVersion: 5.812.10240.16384
Description: Microsoft® Console Based Script Host
Product: Microsoft® Windows Script Host
Company: Microsoft Corporation
OriginalFileName: cmd.exe
CommandLine: "C:\WINDOWS\system32\cmd.exe" C:\AtomicRedTeam\atomics\T1059.005\src\ays_info.vbs
CurrentDirectory: C:\Users\adhd\AppData\Local\Temp\
User: DESKTOP-H12G01\adhd
LogonGuid: {b1a62ae4-d332-6445-204c-060000000000}
LogonId: 0x64C20
TerminalSessionId: 1
IntegrityLevel: High
Hashes: MD5-24590BF74B888FD7D7AC076F4E3C44FD.SHA256-AE37FD18642E797836B9FFCEC8A6E986732D011581061809C6B74426C26A9D03.MPH
ParentProcessGuid: {b1a62ae4-c8c4-6446-d205-000000003500}
ParentProcessId: 3068
ParentImage: C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe
ParentCommandLine: "powershell.exe" & {&script C:\AtomicRedTeam\atomics\T1059.005\src\ays_info.vbs > $env:TEMP\T1059.005.out.txt}
DwellTime: 000000000000000000
```

- b. T1053.005 - Scheduled Task/Job: Scheduled Task, 4 tests de votre choix (12p)

Nous pouvons voir ici les différents tests dispo pour effectuer certains tests

```
T1053.005-5 Extract Memory via VBA
PS C:\AtomicRedTeam> Invoke-AtomicTest T1053.005 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1053.005-1 Scheduled Task Startup Script
T1053.005-2 Scheduled task Local
T1053.005-3 Scheduled task Remote
T1053.005-4 Powershell Cmdlet Scheduled Task
T1053.005-5 Task Scheduler via VBA
T1053.005-6 WMI Invoke-CimMethod Scheduled Task
T1053.005-7 Scheduled Task Executing Base64 Encoded Commands From Registry
T1053.005-8 Import XML Schedule Task with Hidden Attribute
T1053.005-9 PowerShell Modify A Scheduled Task
PS C:\AtomicRedTeam>
```

Ensuite, comme le test précédent, nous regardons les prérequis pour s'assurer qu'on est en mesure de les effectuer

```
T1053.005-9 PowerShell Modify A Scheduled Task
PS C:\AtomicRedTeam> invoke-atomictest t1053.005 -TestNumbers 1 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1053.005-1 Scheduled Task Startup Script
Prerequisites met: T1053.005-1 Scheduled Task Startup Script
PS C:\AtomicRedTeam> invoke-atomictest t1053.005 -TestNumbers 2 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1053.005-2 Scheduled task Local
Prerequisites met: T1053.005-2 Scheduled task Local
PS C:\AtomicRedTeam> invoke-atomictest t1053.005 -TestNumbers 3 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1053.005-3 Scheduled task Remote
Prerequisites met: T1053.005-3 Scheduled task Remote
PS C:\AtomicRedTeam> invoke-atomictest t1053.005 -TestNumbers 4 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1053.005-4 Powershell Cmdlet Scheduled Task
Prerequisites met: T1053.005-4 Powershell Cmdlet Scheduled Task
```

Résultats après les avoir tous exécutés + la photo suivante sera les résultats dans *Onion*

```
CheckPrereq's for: T1053.005-4 Powershell Cmdlet Scheduled Task
Prerequisites met: T1053.005-4 Powershell Cmdlet Scheduled Task
PS C:\AtomicRedTeam> invoke-atomictest t1053.005 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-1 Scheduled Task Startup Script
SUCCESS: The scheduled task "T1053.005_OnLogon" has successfully been created.
SUCCESS: The scheduled task "T1053.005_OnStartup" has successfully been created.
Done executing test: T1053.005-1 Scheduled Task Startup Script
PS C:\AtomicRedTeam> invoke-atomictest t1053.005 -TestNumbers 2
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-2 Scheduled task Local
SUCCESS: The scheduled task "spawn" has successfully been created.
Done executing test: T1053.005-2 Scheduled task Local
PS C:\AtomicRedTeam> invoke-atomictest t1053.005 -TestNumbers 3
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-3 Scheduled task Remote
ERROR: No mapping between account names and security IDs was done.
Done executing test: T1053.005-3 Scheduled task Remote
PS C:\AtomicRedTeam> invoke-atomictest t1053.005 -TestNumbers 4
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1053.005-4 Powershell Cmdlet Scheduled Task
TaskPath TaskName State
-----
\ AtomicTask Ready
Done executing test: T1053.005-4 Powershell Cmdlet Scheduled Task
PS C:\AtomicRedTeam>
```



```

672 -06:00 schtasks /Create /SC ONCE /TN spawn /TR C:\windows\system32\cmd.exe /ST 20:10
650 -06:00 "cmd.exe" /c "schtasks /Create /SC ONCE /TN spawn /TR C:\windows\system32\cmd.exe /ST 20:10"
501 -06:00 "C:\WINDOWS\system32\whoami.exe"
487 -06:00 "C:\WINDOWS\system32\HOSTNAME.EXE"
545 -06:00 schtasks /create /tn "T1053_005_OnStartup" /sc onstart /ru system /tr "cmd.exe /c calc.exe"
527 -06:00 schtasks /create /tn "T1053_005_OnLogon" /sc onlogon /tr "cmd.exe /c calc.exe"
503 -06:00 "cmd.exe" /c "schtasks /create /tn "T1053_005_OnLogon" /sc onlogon /tr "cmd.exe /c calc.exe" & schtasks /create /tn "T1053_005_O

```

c. T1569.002 - System Services: Service Execution, 4 tests de votre choix (12p)

Une fois de plus, nous commençons par demander les détails reliés aux tests que nous désirons exécuter

```

PS C:\AtomicRedTeam> Invoke-AtomicTest T1569.002 -ShowDetailsBrief
PathToAtomicFolder = C:\AtomicRedTeam\atomics

T1569.002-1 Execute a Command as a Service
T1569.002-2 Use PsExec to execute a command on a remote host
T1569.002-4 BlackCat pre-encryption cmds with Lateral Movement
T1569.002-5 Use RemCom to execute a command on a remote host
PS C:\AtomicRedTeam>

```

Nous avons, pour la première fois, des prérequis à installer pour ces tests

```

PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 1 -CheckPrereqs
PathToAtomicFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1569.002-1 Execute a Command as a Service
Prerequisites met: T1569.002-1 Execute a Command as a Service
PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 2 -CheckPrereqs
PathToAtomicFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1569.002-2 Use PsExec to execute a command on a remote host
Prerequisites not met: T1569.002-2 Use PsExec to execute a command on a remote host
[*] PsExec tool from Sysinternals must exist on disk at specified location (C:\PSTools\PsExec.exe)

Try installing prereq's with the -GetPrereqs switch
PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 4 -CheckPrereqs
PathToAtomicFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1569.002-4 BlackCat pre-encryption cmds with Lateral Movement
Prerequisites met: T1569.002-4 BlackCat pre-encryption cmds with Lateral Movement
PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 5 -CheckPrereqs
PathToAtomicFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1569.002-5 Use RemCom to execute a command on a remote host
Prerequisites not met: T1569.002-5 Use RemCom to execute a command on a remote host
[*] RemCom tool must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1569.002\bin\remcom.exe)

Try installing prereq's with the -GetPrereqs switch
PS C:\AtomicRedTeam>

```

Nous pouvons voir où nous acquérons les prérequis ici pour les tests numéro 5 & 2

```

PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 5 -GetPrereqs
PathToAtomicFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1569.002-5 Use RemCom to execute a command on a remote host
Attempting to satisfy prereq: RemCom tool must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1569.002\bin\remcom.exe)
Prereq successfully met: RemCom tool must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1569.002\bin\remcom.exe)
PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 2 -GetPrereqs
PathToAtomicFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1569.002-2 Use PsExec to execute a command on a remote host
Attempting to satisfy prereq: PsExec tool from Sysinternals must exist on disk at specified location (C:\PSTools\PsExec.exe)
Prereq successfully met: PsExec tool from Sysinternals must exist on disk at specified location (C:\PSTools\PsExec.exe)
PS C:\AtomicRedTeam>

```

Ici nous pouvons voir où les prérequis sont maintenant obtenus

```
PS C:\AtomicRedTeam> invoke-atomicTest t1569.002 -TestNumbers 2 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1569.002-2 Use PsExec to execute a command on a remote host
Prerequisites met: T1569.002-2 Use PsExec to execute a command on a remote host
PS C:\AtomicRedTeam> invoke-atomicTest t1569.002 -TestNumbers 5 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1569.002-5 Use RemCom to execute a command on a remote host
Prerequisites met: T1569.002-5 Use RemCom to execute a command on a remote host
PS C:\AtomicRedTeam>
```

Et les résultats lorsque nous effectuons les tests

```
PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 1
PathToAtomicFolder = C:\AtomicRedTeam\atomicms

The service did not respond

StartService FAILED 1053:

PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 2
PathToAtomicFolder = C:\AtomicRedTeam\atomicms

Executing test: T1569.002-2 Use PsExec to execute a command on a remote host
PsExec v2.43 - Execute processes remotely
Copyright (C) 2001-2023 Mark Russinovich
Sysinternals - www.sysinternals.com
Connecting to localhost...
Starting PSEXESVC service on localhost...
Copying authentication key to localhost...
Connecting with PsExec service on localhost...
Starting C:\Windows\System32\calc.exe on localhost...
PsExec could not start C:\Windows\System32\calc.exe on localhost:
The user name or password is incorrect.
Done executing test: T1569.002-2 Use PsExec to execute a command on a remote host
PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 4
PathToAtomicFolder = C:\AtomicRedTeam\atomicms

Executing test: T1569.002-4 BlackCat pre-encryption cmds with Lateral Movement
UUID
14034D56-80E3-92D6-8F99-DCDAC42F472F
The operation completed successfully.
PsExec v2.4 - Execute processes remotely
Copyright (C) 2001-2022 Mark Russinovich
Sysinternals - www.sysinternals.com
cmd.exe exited with error code 0.
Done executing test: T1569.002-4 BlackCat pre-encryption cmds with Lateral Movement
PS C:\AtomicRedTeam> invoke-atomictest t1569.002 -TestNumbers 5
PathToAtomicFolder = C:\AtomicRedTeam\atomicms

Executing test: T1569.002-5 Use RemCom to execute a command on a remote host
Localhost entered for Target Machine .. Going to RunAs Command
Remote Command Executor
Copyright 2006 The WiseGuyz [ http://talhatarq.wordpress.com ]
Copyright 2012 Telefonica Global Technology
Author: Talha Tariq [talha.tariq@gmail.com]
Contributor: Luke Suchocki
Contributor: Merlyn Morgan-Graha
Contributor: Andres Ederra
Local Admin
Launching Local Process ...
Done executing test: T1569.002-5 Use RemCom to execute a command on a remote host
PS C:\AtomicRedTeam>
```

Maintenant, les résultats de ces derniers dans *Onion Hunt*

06:00	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2
06:00	C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2
06:00	C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2
06:00	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2
06:00	C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2
06:00	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2
06:00	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2
06:00	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2
06:00	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	DESKTOP-4IT2

14:47:21.262 -06:00	C:\AtomicRedTeam\atomics\T1569.002\bin\remcom.exe	DESKTOP-
14:42:52.999 -06:00	C:\AtomicRedTeam\atomics\T1569.002\bin\remcom.exe	DESKTOP-

d. T1003.001 - OS Credential Dumping: LSASS Memory – 5 tests de votre choix (15p)

Encore une fois, nous commençons par acquérir les détails pour les tests demandés

```
T1003.001-3 Use REMCOM to execute a command on a remote host
PS C:\AtomicRedTeam> Invoke-AtomicTest T1003.001 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1003.001-1 Dump LSASS.exe Memory using ProcDump
T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
T1003.001-4 Dump LSASS.exe Memory using NanoDump
T1003.001-6 Offline Credential Theft With Mimikatz
T1003.001-7 LSASS read with pypykatz
T1003.001-8 Dump LSASS.exe Memory using Out-Minidump.ps1
T1003.001-9 Create Mini Dump of LSASS.exe using ProcDump
T1003.001-10 Powershell Mimikatz
T1003.001-11 Dump LSASS with createdump.exe from .Net v5
T1003.001-12 Dump LSASS.exe using imported Microsoft DLLs
PS C:\AtomicRedTeam>
```

Nous avons cette fois, plus que 2 tests sans les prérequis. Nous devons les obtenir

```
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 1 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-1 Dump LSASS.exe Memory using ProcDump
Prerequisites not met: T1003.001-1 Dump LSASS.exe Memory using ProcDump
[*] ProcDump tool from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\

Try installing prereq's with the -GetPrereqs switch
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 2 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
Prerequisites met: T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 3 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
Prerequisites not met: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
[*] Dumpert executable must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\Outflank-Dump

Try installing prereq's with the -GetPrereqs switch
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 4 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-4 Dump LSASS.exe Memory using NanoDump
Prerequisites not met: T1003.001-4 Dump LSASS.exe Memory using NanoDump
[*] NanoDump executable must exist on disk at specified location ($env:TEMP\nanodump.x64.exe)

Try installing prereq's with the -GetPrereqs switch
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 6 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-6 Offline Credential Theft With Mimikatz
Prerequisites not met: T1003.001-6 Offline Credential Theft With Mimikatz
[*] Mimikatz must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\x64\mimikatz.exe)

Try installing prereq's with the -GetPrereqs switch
PS C:\AtomicRedTeam>
```

Nous acquérons ensuite les prérequis nécessaires

```
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 1 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1003.001-1 Dump LSASS.exe Memory using ProcDump
Attempting to satisfy prereq: Procdump tool from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\procdump.exe)
Prereq successfully met: Procdump tool from Sysinternals must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\procdump.exe)
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 3 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
Attempting to satisfy prereq: Dumpert executable must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\Outflank-Dumpert.exe)
Prereq successfully met: Dumpert executable must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\Outflank-Dumpert.exe)
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 4 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1003.001-4 Dump LSASS.exe Memory using NanoDump
Attempting to satisfy prereq: NanoDump executable must exist on disk at specified location ($env:TEMP\nanodump.x64.exe)
Prereq successfully met: NanoDump executable must exist on disk at specified location ($env:TEMP\nanodump.x64.exe)
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 6 -GetPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

GetPrereq's for: T1003.001-6 Offline Credential Theft With Mimikatz
Attempting to satisfy prereq: Mimikatz must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\x64\mimikatz.exe)
Prereq successfully met: Mimikatz must exist on disk at specified location (C:\AtomicRedTeam\atomics\T1003.001\bin\x64\mimikatz.exe)
Attempting to satisfy prereq: Lsass dump must exist at specified location (%tmp%\lsass.DMP)
Prereq already met: Lsass dump must exist at specified location (%tmp%\lsass.DMP)
```

Ensuite nous faisons comme d'habitude, nous regardons les prérequis une fois de plus pour s'assurer qu'ils ont bien été intégrés

```
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 1 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-1 Dump LSASS.exe Memory using ProcDump
Prerequisites met: T1003.001-1 Dump LSASS.exe Memory using ProcDump
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 2 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
Prerequisites met: T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 3 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
Prerequisites met: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 4 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-4 Dump LSASS.exe Memory using NanoDump
Prerequisites met: T1003.001-4 Dump LSASS.exe Memory using NanoDump
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 6 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1003.001-6 Offline Credential Theft With Mimikatz
Prerequisites met: T1003.001-6 Offline Credential Theft With Mimikatz
PS C:\AtomicRedTeam>
```

Ensuite, nous pouvons effectuer les tests, sur des commandes différentes, pour le tests 1,2,3 (les tests choisis sont les numéros 1,2,3,4 & 6)

```
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 1
PathToAtomicsFolder = C:\AtomicRedTeam\atomics


Executing test: T1003.001-1 Dump LSASS.exe Memory using ProcDump
Copyright (C) 2009-2022 Mark Russinovich and Andrew Richards
Sysinternals - www.sysinternals.com
Procdump v11.0 - Sysinternals process dump utility
[15:19:02] Dump 1 initiated: C:\Windows\Temp\lsass_dump.dmp
[15:19:02] Dump 1 writing: Estimated dump file size is 58 MB.
[15:19:03] Dump 1 complete: 59 MB written in 0.8 seconds
[15:19:03] Dump count reached.
Done executing test: T1003.001-1 Dump LSASS.exe Memory using ProcDump
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 2
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
Done executing test: T1003.001-2 Dump LSASS.exe Memory using comsvcs.dll
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 3
PathToAtomicsFolder = C:\AtomicRedTeam\atomics
```

Ensuite, sur des commandes différentes, nous testons le test numéro 4

```
PathToAtomicFolder = C:\AtomicRedTeam\atomic
```

Executing test: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking



Dumpert
By Cneeliz @Outflank 2019

```
[1] Checking OS version details:  
[+] Operating System is Windows 10 or Server 2016, build number 19045  
[+] Mapping version specific System calls.  
  
[2] Checking Process details:  
[+] Process ID of lsass.exe is: 704  
[+] NtReadVirtualMemory function pointer at: 0x0000FFD8FE4D890  
[+] NtReadVirtualMemory System call nr is: 0x3f  
[+] Unhooking NtReadVirtualMemory.  
  
[3] Create memorydump file:  
[+] Open a process handle.  
[+] Dump lsass.exe memory to: \\?\C:\WINDOWS\Temp\dumpert.dmp  
[+] Dump succesful.
```

Done executing test: T1003.001-3 Dump LSASS.exe Memory using direct system calls and API unhooking

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1003.001 -TestNumbers 4  
PathToAtomicFolder = C:\AtomicRedTeam\atomic
```

Executing test: T1003.001-4 Dump LSASS.exe Memory using NanoDump

Failed to call NtReadVirtualMemory, status: 0xc0000005

The minidump has an invalid signature, restore it running:

```
bash restore_signature.sh nanodump.dmp  
Done, to get the secretz run:  
python3 -m pyppkatz lsa minidump nanodump.dmp  
Done executing test: T1003.001-4 Dump LSASS.exe Memory using NanoDump
```

Et finalement le test du test numéro 6

```
PS C:\AtomicRedTeam> Invoke-AtomicTest t1003.001 -TestNumbers 6
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1003.001-6 Offline Credential Theft With Mimikatz
#####. mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
.##. #.##. "A La Vie, A L'Amour" - (oe.eo)
## / \ ## /** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
## \ / ## > https://blog.gentilkiwi.com/mimikatz
'## v ##' Vincent LE TOUX ( vincent.letoux@gmail.com )
'#####' > https://pingcastle.com / https://mysmartlogon.com ***/
mimikatz(commandline) # sekurlsa:minidump C:\Users\adhd\AppData\Local\Temp\lsass.f
Switch to MINIDUMP : 'C:\Users\adhd\AppData\Local\Temp\lsass.DMP'
mimikatz(commandline) # sekurlsa:logonpasswords full
Opening : 'C:\Users\adhd\AppData\Local\Temp\lsass.DMP' file for minidump...
ERROR kuhl_m_sekurlsa_acquireLSA ; Handle on memory (0x00000002)
mimikatz(commandline) # exit
Bye!
Done executing test: T1003.001-6 Offline Credential Theft With Mimikatz
PS C:\AtomicRedTeam>
```

Résultats dans *Security Onion Hunt*

File query name	File contents name	Accession number	Accession number
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005671	005671
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005672	005672
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005673	005673
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005674	005674
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005675	005675
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005676	005676
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005677	005677
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005678	005678
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005679	005679
C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	C:\Users\RedTeam\Documents\T-1000-361\bin\cmdump.exe	005680	005680

e. T1136.001 - Create Account: Local Account, 2 tests de votre choix (6p)

Pour le dernier test, voici la commande pour voir les détails de ce dernier

```
T1136.001-12 Dump LSASS.exe using imported WinPcap DLLs
PS C:\AtomicRedTeam> Invoke-AtomicTest T1136.001 -ShowDetailsBrief
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

T1136.001-3 Create a new user in a command prompt
T1136.001-4 Create a new user in PowerShell
T1136.001-6 Create a new Windows admin user
PS C:\AtomicRedTeam>
```

Nous regardons si nous avons bel et bien les prérequis pour le test

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1136.001 -TestNumbers 3 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1136.001-3 Create a new user in a command prompt
Prerequisites met: T1136.001-3 Create a new user in a command prompt
PS C:\AtomicRedTeam> Invoke-AtomicTest T1136.001 -TestNumbers 4 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1136.001-4 Create a new user in PowerShell
Prerequisites met: T1136.001-4 Create a new user in PowerShell
PS C:\AtomicRedTeam> Invoke-AtomicTest T1136.001 -TestNumbers 6 -CheckPrereqs
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

CheckPrereq's for: T1136.001-6 Create a new Windows admin user
Prerequisites met: T1136.001-6 Create a new Windows admin user
PS C:\AtomicRedTeam>
```

Vu que nous avons déjà les prérequis, nous pouvons simplement exécuter les tests

```
PS C:\AtomicRedTeam> Invoke-AtomicTest T1136.001 -TestNumbers 3
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1136.001-3 Create a new user in a command prompt
The command completed successfully.
Done executing test: T1136.001-3 Create a new user in a command prompt
PS C:\AtomicRedTeam> Invoke-AtomicTest T1136.001 -TestNumbers 4
PathToAtomicsFolder = C:\AtomicRedTeam\atomics

Executing test: T1136.001-4 Create a new user in PowerShell
Name           Enabled Description
----
T1136.001_PowerShell True
Done executing test: T1136.001-4 Create a new user in PowerShell
PS C:\AtomicRedTeam>
```

Résultats dans *Onion*

>	▲	2023-04-24 17:03:20.046 -06:00	C:\WINDOWS\system32\net1 localgroup administrators "T1136.001_Admin" /add	7120	C:\Windows\System32\net.exe	C:\Users\adhd\AppData\Local\Temp\
>	▲	2023-04-24 17:03:20.038 -06:00	net localgroup administrators "T1136.001_Admin" /add	10492	C:\Windows\System32\cmd.exe	C:\Users\adhd\AppData\Local\Temp\

11:20:04 -05:00	C:\Windows\System32\cmd.exe	4136	C:\Windows\System32\cmd.exe	C:\Users\adht\AppData\Local\Temp\
11:19:59 -05:00	net user /add "T1136_001_Admin" "T1136_pass"	9644	C:\Windows\System32\cmd.exe	C:\Users\adht\AppData\Local\Temp\
11:19:57 -05:00	"cmd.exe" /s "net user /add "T1136_001_Admin" "T1136_pass" & net localgroup administrators "T1136_001_Admin" /add"	2000	C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe	C:\Users\adht\AppData\Local\Temp\

Exercise 3 – Alerting (30p)

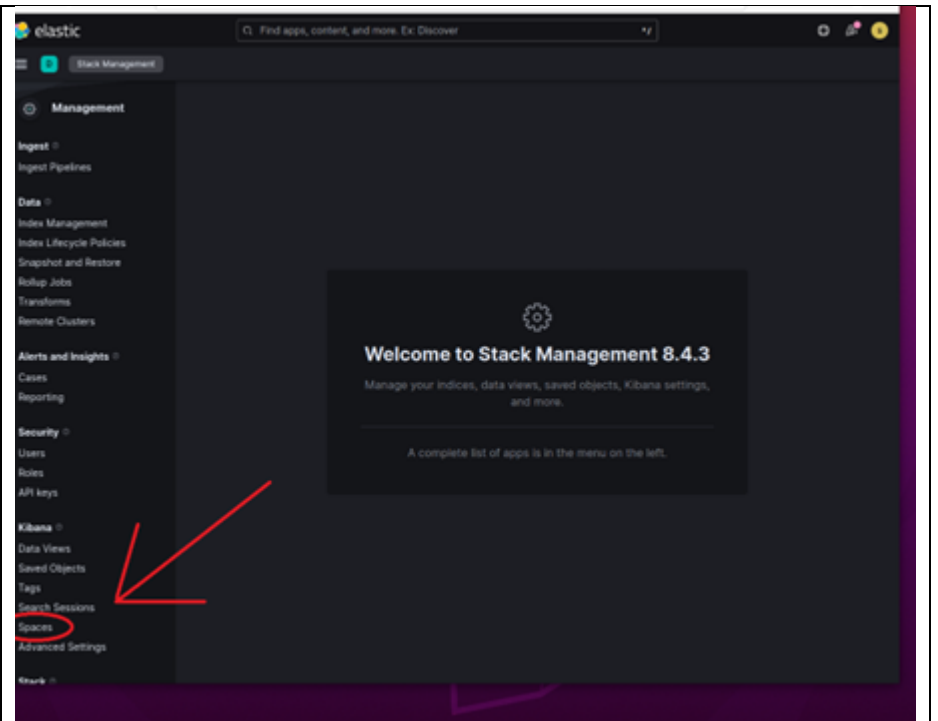
- a) Effectuez les laboratoires de cours 12, utilisez des noms d'utilisateur liés à votre prénom ou à votre nom de famille. (10p)

Pour chacune des règles, ajoutez une capture d'écran :

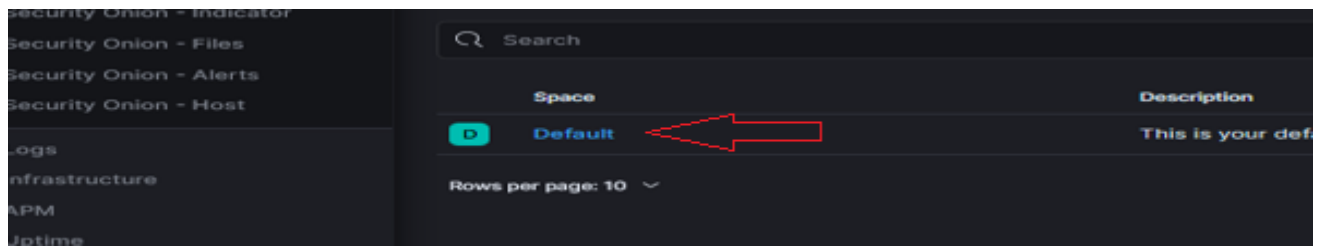
- De la règle
- De l'évènement de base (utilisé pour frapper la règle)
- De l'évènement corrélé

Réponse

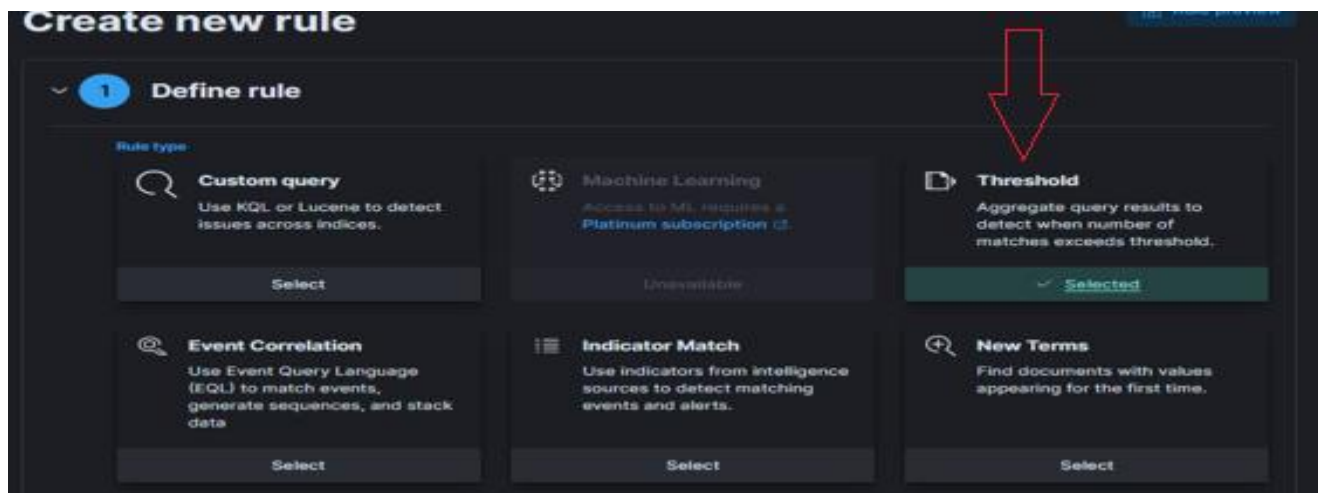
Nous commençons par repérer <<Spaces>> en dessous de Kibana.



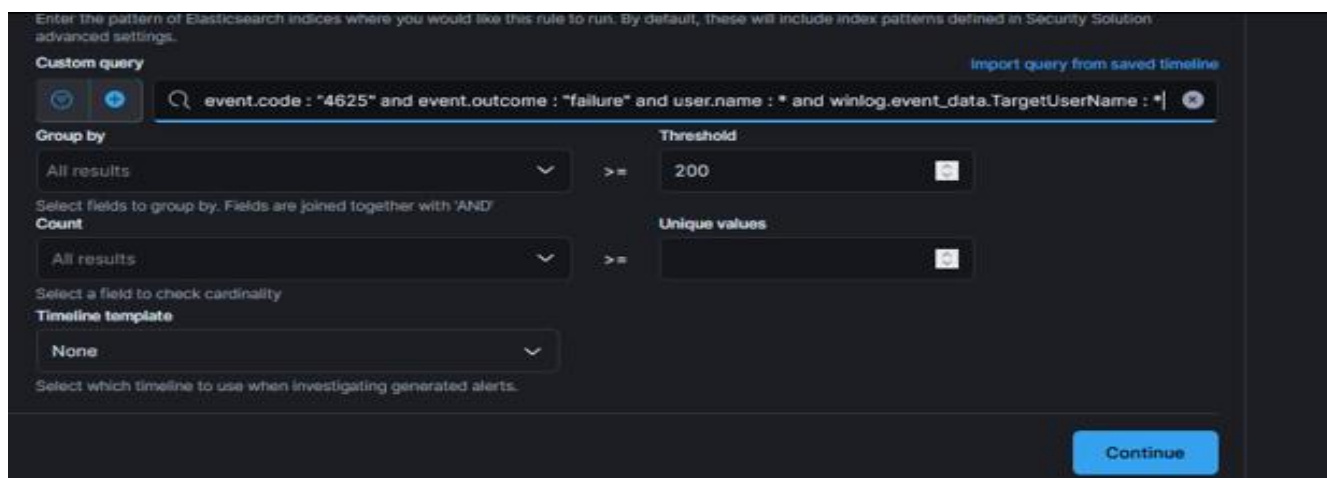
Ensuite, on va dans *Defaults*



On se créer notre propre règle avec la section *Threshold*



Notre règle



Nous devons par la suite changer le *group* et *count*

The screenshot shows a configuration interface for a rule. It features two rows of field selection. The first row has a field labeled 'host.ip' with a dropdown arrow, followed by a comparison operator '>=' and a value '1'. Below this, a text prompt says 'Select fields to group by. Fields are joined together with 'AND''. The second row has a field labeled '@timestamp' with a dropdown arrow, followed by a comparison operator '>=' and a value '3'. To the right of this row is a label 'Unique values'. Below these rows, there is a section labeled 'Timeline template' with a dropdown menu currently set to 'None'.

Nous pouvons ensuite créer la règle

The screenshot shows the 'About rule' configuration page, which is the second step in creating a rule. It includes several sections: 'Name' with the text 'CR450-Frederic-Perron'; 'Description' with the text '450'; 'Default severity' with a dropdown menu set to 'Low'; a checkbox for 'Severity override' with the description 'Use source event values to override the default severity.'; 'Default risk score' with a slider ranging from 0 to 100, currently set at 21; a checkbox for 'Risk score override' with the description 'Use a source event value to override the default risk score.'; and a 'Tags' section with a text input field and the label 'Optional'. At the bottom, there is a note: 'Type one or more custom identifying tags for this rule. Press enter after each tag to begin a new one.'

On set ensuite l'horaire de la règle

The screenshot shows the 'Schedule rule' configuration page, which is the third step in creating a rule. It includes two main sections: 'Runs every' with a numeric input set to '5' and a dropdown menu set to 'Minutes'; and 'Additional look-back time' with a numeric input set to '15' and a dropdown menu set to 'Minutes'. Below the first section, there is a text prompt: 'Rules run periodically and detect alerts within the specified time frame.' Below the second section, there is a text prompt: 'Adds time to the look-back period to prevent missed alerts.'

On met ensuite la règle avec notre nom et prénom

2 About rule

Name
CR450-Frederic-Perron

Description
450

Default severity
Select a severity level for all alerts generated by this rule.
☒ Low

☐ Severity override
Use source event values to override the default severity.

Default risk score
Select a risk score for all alerts generated by this rule.
0 25 50 75 100 21

☐ Risk score override
Use a source event value to override the default risk score.

Tags Optional

Type one or more custom identifying tags for this rule. Press enter after each tag to begin a new one.

On duplicate la règle

Duplicate the rule with exceptions?

You are duplicating 1 selected rule, please select how you would like to duplicate the existing exceptions

☒ Duplicate rule and their exceptions
☐ Only duplicate the rule

Cancel Duplicate

On ajoute ensuite le winlog string après avoir fait le test cmd prompt

event.code : "4625" and event.outcome : "failure" and user.name : * and winlog.event_data.TargetU

Group by
host.ip x

Threshold
1

Select fields to group by. Fields are joined together with 'AND'
Count
winlog.event_data.TargetUserName x

Unique values
3

Select a field to check cardinality
Timeline template
None

Select which timeline to use when investigating generated alerts.

On peut ensuite faire faire des tests randoms. Nous avons simplement choisi les noms hello1, hello2 et hello3 pour les utilisateurs

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.19041.1415]
(c) Microsoft Corporation. All rights reserved.

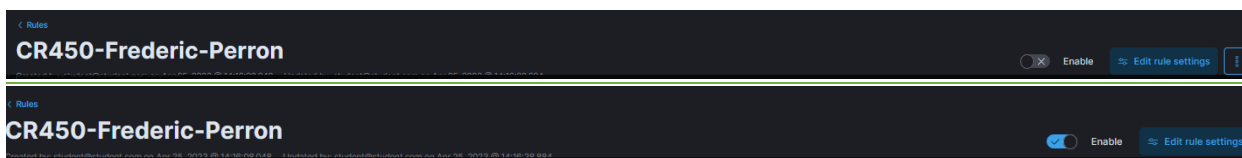
C:\WINDOWS\system32>runas /user:hello1 cmd
Enter the password for hello1:
Attempting to start cmd as user "ADHD\hello1" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\WINDOWS\system32>runas /user:hello2 cmd
Enter the password for hello2:
Attempting to start cmd as user "ADHD\hello2" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\WINDOWS\system32>runas /user:hello3 cmd
Enter the password for hello3:
Attempting to start cmd as user "ADHD\hello3" ...
RUNAS ERROR: Unable to run - cmd
1326: The user name or password is incorrect.

C:\WINDOWS\system32>
```

On peut voir ici la règle d'activée après 5 minutes



- b) Activez deux règles de votre choix dans la Built-in rules d'Elastic. Utilisez n'importe quel outil de votre choix (Atomics, Powershell...) pour faire trigger les règles. Documentez vos résultats. (20p)

Pour chacune, ajoutez une capture d'écran :

- De la règle
- De l'évènement de base (utilisé pour frapper la règle)
- De l'évènement corrélé

Nous commençons par ajouter la règle proxy

```
C:\WINDOWS\system32>netsh interface portproxy show all

Listen on ipv4:          Connect to ipv4:
Address                 Port                 Address                 Port
-----
127.0.0.1               8080                192.168.182.158        80
```

Je ne vois toujours pas l'alerte par exemple, seulement un avertissement

Port Forwarding Rule Addition

Created by: student@student.com on Apr 25, 2023 @ 14:00:08.772 Updated by: student@student.com on Apr 25, 2023 @ 19:13:38.727

Last response: ● warning at Apr 25, 2023 @ 19:18:43.002

⚠ Warning at Apr 25, 2023 @ 19:18:43.002

This rule is attempting to query data from Elasticsearch indices listed in the "Index pattern" section of the rule definition, however no index matching: ["winlogbeat-*"] until a matching index is created or this rule is disabled.

Cela est la règle que nous allons utiliser avec les informations et commandes

RDP Enabled via Registry

Created by: student@student.com on Apr 25, 2023 @ 14:00:08.780 Updated by: student@student.com on Apr 25, 2023 @ 14:00:08.780

Last response: ●

About

Identifies registry write modifications to enable Remote Desktop Protocol (RDP) access. This could be indicative of adversary lateral movement preparation.

Author Elastic

Severity Medium

Risk score 47

License Elastic License v2

MITRE ATTACK™ Lateral Movement (TA0008) Remote Services (T1021) Remote Desktop Protocol (T1021.001)

Timestamp override event.ingested

Definition

Index patterns logs-endpoint.events.* winlogbeat-* logs-windows.* endgame.*

Custom query registry where host.os.type == "windows" and event.type in ("creation", "change") and registry.path: ("HKLM\SYSTEM\CurrentControlSet\Control\Terminal Server\DenyTSConnections", "(REGISTRY\MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\DenyTSConnections") and registry.data.strings: ("0", "0x00000000") and not (process.name: "svchost.exe" and user.domain == "NT AUTHORITY") and not process.executable: "C:\Windows\System32\SystemPropertiesRemote.exe"

Rule type Event Correlation

Nous exécutons ensuite la commande dans le PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/powershell

PS C:\WINDOWS\system32> Set-ItemProperty -Path 'HKLM:\System\CurrentControlSet\Control\Terminal Server'-name "fDenyTSConnections" -Value 0
```

On recommence suite les services pour que la machine accepte maintenant RDP

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

Try the new cross-platform PowerShell https://aka.ms/pscore6

PS C:\WINDOWS\system32> Restart-Service TermService -Force
```

Avant d'essayer de déclencher l'alerte, on va activer la règle et attendre quelques minutes comme recommandé

RDP Enabled via Registry Enable [Edit rule settings](#)

Created by: student@student.com on Apr 25, 2023 @ 14:00:08.780 Updated by: student@student.com on Apr 25, 2023 @ 19:28:00.810

Last response:

About Details Investigation guide Setup guide

Identifies registry write modifications to enable Remote Desktop Protocol (RDP) access. This could be indicative of adversary lateral movement preparation.

Author Elastic

Severity Medium

Risk score 47

License Elastic License v2

Definition

Index patterns logs-endpoint.events.* winlogbeat-* logs-windows.* endgame-*

Custom query

registry where host.os.type == "windows" and event.type in ("creation", "change") and registry.path : ("HKLM\\SYSTEM\\ControlSet001\\Control\\Terminal Server\\fDenyTSConnections", "\\REGISTRY\\MACHINE\\SYSTEM\\ControlSet001\\Control\\Terminal Server\\fDenyTSConnections") and

Et même chose qu'auparavant, nous n'avons pas d'alerte, seulement l'avertissement, même après avoir suivi le labo de A à Z

RDP Enabled via Registry Enable [Edit rule settings](#)

Created by: student@student.com on Apr 25, 2023 @ 14:00:08.780 Updated by: student@student.com on Apr 25, 2023 @ 19:28:00.810

Last response: warning at Apr 25, 2023 @ 19:33:03.696

Warning at Apr 25, 2023 @ 19:33:03.696

This rule is attempting to query data from Elasticsearch indices listed in the "Index pattern" section of the rule definition, however no index matching: ["logs-endpoint.events.*", "winlogbeat-*", "logs-windows.*", "endgame-*"] was found. This warning will continue to appear until a matching index is created or this rule is disabled.