Rapport forensic — scénario pédagogique Red Petya

1. Sommaire

2. Rapport exécutif

Ce rapport a été réalisé dans le cadre du cas pédagogique “Intrusion sur un serveur Windows” fourni par la plateforme.
L’objectif est d’analyser une image forensique d’un serveur Windows Server 2022, simulant une compromission par accès RDP et le déploiement du ransomware Red Petya.

L’investigation a porté sur les journaux d’événements (EVTX) extraits de la machine cible.
L’analyse a révélé plusieurs éléments clés :

- Une campagne de brute-force massive : plus de 100 000 échecs d'authentification (EventId 4625) enregistrés depuis l'adresse IP `36.133.110.87` (hôte identifié comme kali). La cadence et le volume observés sont compatibles avec l'usage d'un outil automatisé (type Hydra/Ncrack).
- Une connexion RDP réussie : un `EventId 4624` (LogonType=10) a confirmé une session RDP acceptée depuis l'adresse IP `31.220.85.162` sur la machine WIN-NI9FBK23SLO.branchoffice.example.com.
- Des actions post-compromission : à peine quelques secondes après la connexion, un `EventId 4648` (logon avec identifiants explicites) et un `EventId 4672` (privilèges spéciaux attribués) ont été enregistrés pour le même utilisateur. Cette séquence traduit une élévation de privilèges immédiate.

Ces observations permettent de reconstituer une chronologie claire de l'attaque :

1. Brute-force massif depuis l'extérieur (36.133.110.87).
2. Connexion RDP réussie depuis une autre IP (31.220.85.162).
3. Usage d'identifiants explicites (4648).
4. Attribution de privilèges élevés (4672).

Conclusion : l'image forensique met en évidence un scénario de compromission complet, allant de la tentative d'intrusion par brute-force à l'obtention d'un accès privilégié sur la cible. L'ensemble des éléments analysés s'inscrit dans un cadre strictement académique et simulé, et ne concerne pas un système de production réel.

3. Contexte et périmètre

3.1 Contexte

Ce scénario simule une attaque RDP réussie dans le but de déployer le ransomware Red Petya sur l'infrastructure cible. Notre analyse se concentre sur la phase d'intrusion et de compromission initiale (accès et élévation de privilèges), qui constitue le prérequis à l'exécution du ransomware.

3.2 Périmètre

L'analyse porte exclusivement sur :

- Les journaux d'événements Windows (EVTX) extraits de l'image disque de la machine cible.
- Les événements d'authentification (`4625` , `4624` , `4648`) et de privilèges (`4672`), considérés comme les indicateurs principaux d'une compromission via RDP.

- La corrélation temporelle entre les échecs d'authentification massifs, la connexion réussie et l'attribution de privilèges.

Ne sont pas inclus dans ce rapport :

- L'analyse mémoire (RAM dump) ;
- L'examen complet des fichiers système ou artefacts (prefetch, registry hives, etc.) ;
- L'analyse réseau en temps réel.

3.3 Objectifs

Les objectifs de cette investigation sont :

1. Identifier les tentatives d'authentification suspectes et leur origine.
2. Mettre en évidence une ou plusieurs connexions RDP réussies suite à ces tentatives.
3. Corréler ces événements avec l'attribution de privilèges administratifs.
4. Reconstituer une chronologie d'intrusion claire et étayée par des preuves.

4. Méthodologie et outils

4.1 Méthodologie

L'image disque fournie a été traitée en mode forensic afin de préserver l'intégrité des preuves. L'accès aux journaux d'événements Windows (`*.evtx`) a été réalisé à l'aide de FTK Imager en mode lecture seule. Les étapes opérées sont les suivantes :

1. **Monture/accès :** l'image forensique (`20240212-decrypted-Windows_Server_2022.E01`) a été montée en lecture seule via FTK Imager sur la station d'analyse. Aucun écrit n'a été effectué sur l'image d'origine.
2. **Extraction :** les fichiers d'événements Windows ont été extraits depuis le chemin logique de l'OS : `\Windows\System32\winevt\Logs\*.evtx` et copiés vers un répertoire d'analyse local sécurisé.
3. **Vérification d'intégrité :** Des sommes de contrôle (SHA-256) ont été calculées pour l'image d'origine et pour chaque artefact extrait afin d'assurer l'intégrité des éléments collectés (cf. annexe — hash).
4. **Parsing et analyse :** les EVTX ont été parsés en CSV à l'aide de EvtxECmd (Eric Zimmerman) pour produire `AllLogs.csv` . L'analyse exploratoire, le filtrage et la corrélation temporelle ont été effectués avec Timeline Explorer et des scripts PowerShell (filtres ciblés sur `EventId` 4625/4624/4648/4672). Pour des extractions résumées, l'outil Events-Ripper a été utilisé en complément lorsque nécessaire.
5. **Préservation et traçabilité :** toutes les copies étudiées (CSV, exports, screenshots Timeline Explorer) ont été conservées en lecture seule dans un répertoire d'evidence chiffré

et horodaté. Un registre de chaînage (chain-of-custody) documente les opérations effectuées (qui, quand, quelle commande/outils).

4.2 Outils

Outils utilisés (liste) :

- FTK Imager — montage et extraction des fichiers EVTX en lecture seule.
- EvtxECmd (Eric Zimmerman) — parsing EVTX → CSV/JSON.
- Timeline Explorer — analyse chronologique, filtres et exports.
- PowerShell — filtrage, agrégation, corrélation, génération d'exports.
- Events-Ripper (ERip) — résumé plugin-based (optionnel).
- Support : stockage chiffré pour preuves, horodatage et calcul SHA-256.

5. Résultats

5.1 Synthèse rapide

L'analyse des journaux EVTX de l'image montre un scénario cohérent et corrélé :

1. une campagne de brute-force externe (énormes rafales d'échecs d'authentification),
2. au moins une connexion RDP réussie quelques instants après, depuis une autre IP,
3. puis des actions locales signalées (usage d'identifiants explicites et attribution de privilèges).

> **Remarque**
>
> Ces éléments, pris ensemble, constituent une preuve forte d'une compromission de session suivie d'une élévation de privilèges sur l'hôte ciblé.

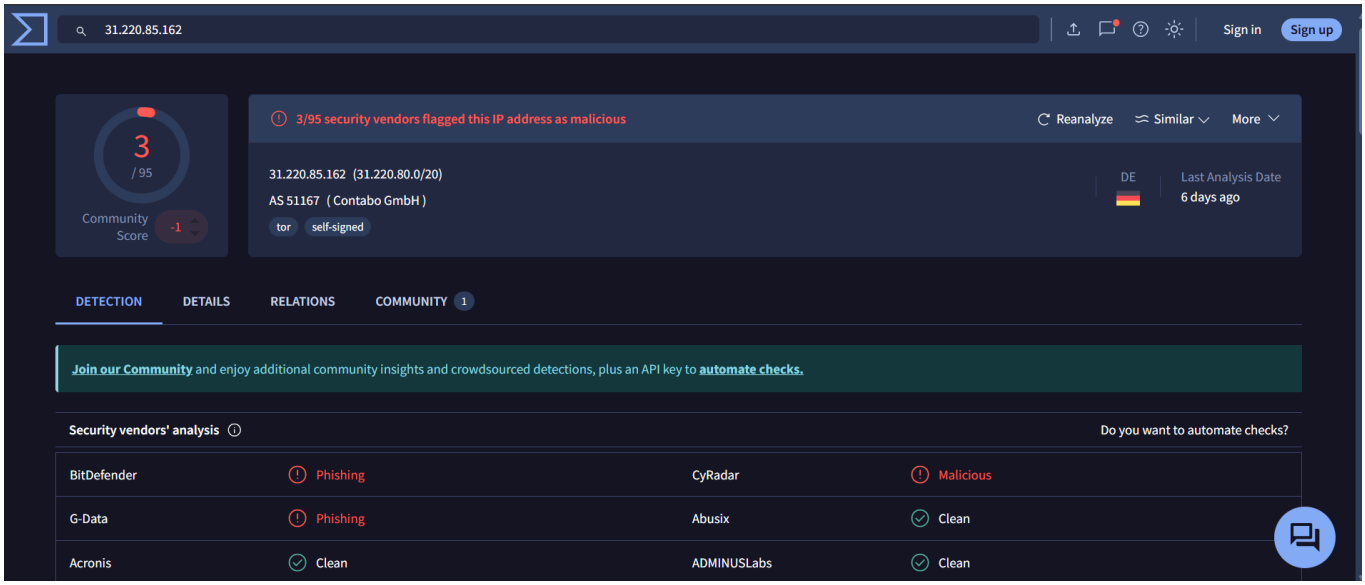
5.2. Authentifications échouées — EventId 4625 (Brute-force)

Les journaux montrent plus de 100 000 événements `EventId 4625` (échecs d'authentification), majoritairement provenant de `36.133.110.87` (hôte « kali »).

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing"/>
    <EventID>4625</EventID>
    <Level>LogAlways</Level>
    <TimeCreated SystemTime="2024-02-04T23:37:28Z"/>
    <Computer>WIN-NI9FBK23SLO.branchoffice.example.com</Computer>
```

```
    <Channel>Security</Channel>
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-0-0</Data>
    <Data Name="SubjectUserName">-</Data>
    <Data Name="SubjectDomainName">-</Data>
    <Data Name="SubjectLogonId">0x0</Data>
    <Data Name="TargetUserSid">S-1-0-0</Data>
    <Data Name="TargetUserName">Administrator</Data>
    <Data Name="Status">0xC000006D</Data>
    <Data Name="SubStatus">0xC000006A</Data>
    <Data Name="FailureReason">%%2313 (Nom correct mais mot de passe erroné)
</Data>
    <Data Name="LogonType">3</Data>
    <Data Name="LogonProcessName">NtLmSsp</Data>
    <Data Name="AuthenticationPackageName">NTLM</Data>
    <Data Name="WorkstationName">kali</Data>
    <Data Name="IpAddress">36.133.110.87</Data>
    <Data Name="IpPort">0</Data>
    <Data Name="KeyLength">0</Data>
  </EventData>
</Event>
```

La vitesse et le volume sont compatibles avec une attaque automatisée de type brute-force visant des comptes génériques et le compte `BRANCHOFFICE\admin`.



Nous constatons que c'est une IP déjà recensé malveillante.

Name,"Count"
2024-02-05 20:53,"88"
2024-02-05 19:04,"88"
2024-02-05 19:38,"87"
2024-02-05 09:45,"87"
2024-02-05 20:55,"87"
2024-02-05 18:11,"87"
2024-02-05 19:03,"87"
2024-02-05 17:59,"87"
2024-02-05 17:57,"87"
2024-02-05 17:58,"87"
2024-02-05 19:37,"87"
2024-02-05 19:10,"86"
2024-02-05 19:36,"86"
2024-02-05 18:10,"86"

Provenant du fichier `4625_by_minute` que j'ai généré à partir des logs.

5.3 Connexion RDP réussie — EventId 4624 (LogonType = 10)

À 2024-02-06 19:52:39 UTC, un événement `4624` (Successful logon, LogonType=10) a été enregistré pour `admin` sur `WIN-NI9FBK23SLO.branchoffice.example.com`. La source de la connexion est `31.220.85.162` (hôte « kali »).

```
<TimelineEntry>
  <EventRecordId>2457634</EventRecordId>
  <TimeCreated>2024-02-06 19:52:39</TimeCreated>
  <EventID>4624</EventID>
  <Computer>WIN-NI9FBK23SLO.branchoffice.example.com</Computer>
  <Provider>Microsoft-Windows-Security-Auditing</Provider>
  <Channel>Security</Channel>
  <Keywords>Audit success</Keywords>
  <SourceFile>C:\Users\Bang\Desktop\EVTX\evtx\Security.evtx</SourceFile>

  <TargetAccount>
    <Domain>BRANCHOFFICE</Domain>
    <Username>Administrator</Username>
    <Sid>S-1-5-21-1057484085-1795310446-2370380301-500</Sid>
    <TargetLogonId>0x2E2FDE25</TargetLogonId>
  </TargetAccount>

  <NetworkAuth>
    <LogonType>3</LogonType>
    <AuthenticationPackage>NTLM</AuthenticationPackage>
    <LogonProcess>NtLmSsp</LogonProcess>
    <Workstation>kali</Workstation>
    <IpAddress>31.220.85.162</IpAddress>
```

```
    <IpPort>0</IpPort>
    <LmPackageName>NTLM V2</LmPackageName>
    <KeyLength>128</KeyLength>
  </NetworkAuth>
</TimelineEntry>
```

Interprétation :

- La séquence brute-force (36.133.110.87) → connexion réussie (31.220.85.162) est cohérente avec : l'attaquant teste depuis une IP/VM, puis utilise une autre machine/IP pour établir la session réelle après obtention des credentials.

5.4 Actions post-compromission : EventId 4648 & 4672

4 secondes après la connexion RDP du 2024-02-06 19:52:39 UTC, un `4648` est enregistré à 19:52:43 UTC (usage d'identifiants explicites), suivi d'un `4672` (privilèges spéciaux). Ces événements montrent que la session compromise a conduit rapidement à une élévation de privilèges.

```
<Event xmlns="http://schemas.microsoft.com/win/2004/08/events/event">
  <System>
    <Provider Name="Microsoft-Windows-Security-Auditing"/>
    <EventID>4648</EventID>
    <Channel>Security</Channel>
    <Level>LogAlways</Level>
    <Computer>WIN-NI9FBK23SLO.branchoffice.example.com</Computer>
    <TimeCreated>2024-02-06 19:52:43</TimeCreated>
    <EventRecordID>2457645</EventRecordID>
  </System>
  <EventData>
    <Data Name="SubjectUserSid">S-1-5-18</Data>
    <Data Name="SubjectUserName">WIN-NI9FBK23SLO$</Data>
    <Data Name="SubjectDomainName">BRANCHOFFICE</Data>
    <Data Name="SubjectLogonId">0x3E7</Data>
    <Data Name="LogonGuid">00000000-0000-0000-0000-000000000000</Data>
    <Data Name="TargetUserName">Administrator</Data>
    <Data Name="TargetDomainName">BRANCHOFFICE</Data>
    <Data Name="TargetLogonGuid">dfb7284d-0517-fca0-8fc8-b3726177616b</Data>
    <Data Name="TargetServerName">localhost</Data>
    <Data Name="TargetInfo">localhost</Data>
    <Data Name="ProcessId">0x8</Data>
    <Data Name="ProcessName">C:\Windows\System32\svchost.exe</Data>
    <Data Name="IpAddress">31.220.85.162</Data>
    <Data Name="IpPort">0</Data>
  </EventData>
```

```
</Event>
```

```
<Event>
  <EventID>4672</EventID>
  <TimeCreated>2024-02-06T19:52:42</TimeCreated>
  <Computer>WIN-NI9FBK23SLO.branchoffice.example.com</Computer>
  <LogonType>Administrative logon</LogonType>
  <User>
    <SID>S-1-5-90-0-4</SID>
    <UserName>DWM-4</UserName>
    <Domain>Window Manager</Domain>
    <LogonId>0x2E2FEDA1</LogonId>
  </User>
  <Privileges>
    SeAssignPrimaryTokenPrivilege
    SeAuditPrivilege
    SeImpersonatePrivilege
  </Privileges>
  <Status>Audit success</Status>
  <SourceFile>C:\Users\Bang\Desktop\EVTX\evtx\Security.evtx</SourceFile>
</Event>
```

Bien que notre analyse se concentre sur les événements d'authentification et d'élévation de privilèges, le scénario de référence indique que l'objectif final de l'attaquant est l'exécution du ransomware Red Petya. Les privilèges obtenus via le `4672` fournissent le niveau de contrôle requis pour installer ou déclencher un tel malware à l'échelle du système.

5.5 Corrélation et timeline consolidée

Time (UTC)	EventId	Description	Src IP	Host (Computer)
2024-02-04T23:37:28	4625	Rafale d'échecs (brute-force)	36.133.110.87	Target server
2024-02-06T19:52:39	4624	Connexion RDP réussie (LogonType=10)	31.220.85.162	WIN-NI9FBK23SLO
2024-02-06T19:52:42	4672	Privilèges spéciaux attribués (élévation)	(IP via 4624)	WIN-NI9FBK23SLO
2024-02-06T19:52:43	4648	Logon with explicit credentials (post-logon action)	31.220.85.162	WIN-NI9FBK23SLO

6. Analyse et interprétation

6.1 Conclusions techniques

- Le pattern temporel et la volumétrie montrent clairement une attaque par brute-force (EventId 4625) depuis `36.133.110.87`.
- Une connexion RDP réussie (EventId 4624, LogonType=10) a été établie peu après depuis `31.220.85.162` sur `WIN-NI9FBK23SLO.branchoffice.example.com`.
- La séquence `4624 → 4648 → 4672` indique que, une fois la session ouverte, l'opérateur a tenté d'utiliser des identifiants explicites et la session a rapidement obtenu privilèges élevés.
- Niveau de confiance : élevé — corrélation temporelle nette + preuves multiples (4625 massifs → 4624 succès → actions post-logon).

6.2 Scénario le plus plausible (reconstruit)

1. Attaquant(s) lance(nt) un bruteforce automatisé depuis une machine (36.133.110.87) pour tester des identifiants RDP.
2. Dès obtention d'un couple username/password valide, l'attaquant se connecte depuis une autre instance (`31.220.85.162`) pour exécuter des actions (probablement pour éviter la détection).
3. Une fois connecté, l'attaquant exécute un process utilisant des credentials explicites (4648) puis obtient des privilèges (4672). Avec ces droits il peut installer/pivoter/déployer du code malveillant (ici, dans le scénario pédagogique, Red Petya).

6.3 Points de vérification / incertitudes

- Aucun artefact binaire (hash de malware) n'a été confirmé dans l'axe d'analyse EVTX seul — pour confirmer l'exécution de Petya il faut analyser disque/mémoire (fichiers, services, scheduled tasks, processus suspects).
- L'identification précise de l'outil de brute-force (Hydra / Ncrack / patator) n'est pas possible uniquement via EVTX — il faudrait des captures réseau ou fichiers d'outil sur la machine d'attaque.
- Il est possible que l'attaquant ait utilisé un botnet avec répartition d'IP ; néanmoins, la corrélation IP/time est suffisante pour alerter/mitiger.

7. Conclusions

L'analyse des journaux d'événements montre une compromission réussie d'un serveur Windows via RDP. Le scénario est clair : brute-force externe, session RDP réussie depuis une IP distincte, usage d'identifiants explicites et élévation de privilèges.

Dans le cadre pédagogique, ces éléments constituent la phase initiale nécessaire au déploiement du ransomware Red Petya. Le risque opérationnel est élevé : accès administratif, possibilité de persistence, exfiltration et déploiement de code destructeur.

Type	Valeur	Contexte / preuve
IP	36.133.110.87	100k+ EventId 4625 (brute-force).
IP	31.220.85.162	EventId 4624 (RDP success).
Host	WIN-NI9FBK23SLO.branchoffice.example.com	Hôte compromis / cible principale
Compte	BRANCHOFFICE\admin	Compte ciblé/présent dans logs
Events	4625, 4624, 4648, 4672	Séquence d'attaque (Initial access → PrivEsc)

8. Recommandations

8.1 Actions immédiates

1. Isoler la machine compromise ou patient zéro (`WIN-NI9FBK23SLO...`) du réseau (coupure physique ou mise en VLAN isolé) — conserver l'accès local si nécessaire pour la collecte de preuves.
2. Bloquer immédiatement les IPs identifiées :
   - 36.133.110.87 (source brute-force)
   - 31.220.85.162 (source RDP réussie)
   - Commande firewall (ex. Windows Defender Firewall ou appliance) : bloque IPs en entrée RDP.
3. Sauvegarder une image forensique immuable de la machine (si pas déjà fait) et copier les fichiers logs/CSV/export sur support chiffré. Calculer SHA-256.
4. Réinitialiser tous les mots de passe administrateurs à partir d'un système sécurisé. Forcer expiration et rotation.
5. Désactiver l'accès RDP externe immédiatement (ou n'autoriser que via VPN/Jumphost).

8.2 Actions COURT TERME (24–72 heures)

1. Activer **MFA** pour tous les comptes ayant accès à distance.
2. Rechercher et neutraliser persistance :
   - Services récemment créés (EventId 7045).
   - Tâches planifiées (4698 & 106).
   - Nouveaux comptes locaux ou modifications de comptes existants.

- Fichiers ou exécutables nouvellement créés sous `C:\Windows\System32`,

3. Examiner la mémoire (si image RAM dispo) pour rechercher processus malveillants, connexions réseau actives et credentials en cleartext.

8.3 Actions MOYEN TERME (Semaine)

1. Revoir la politique RDP : désactiver RDP public, déplacer sur jumpbox / bastion, restreindre par ACL, limiter par IP.
2. Mettre en place détection et response : règles SIEM pour :
   - bursts de `4625` par minute (> X échecs)
   - `4624` externes suivis de `4672` dans 0–2 minutes
   - `4648` hors maintenance windows
3. Sensibiliser sur la politique de verrouillage de compte (account lockout après 5–10 échecs) et surveiller tentative d'escalade.

8.4 Message pour l'équipe SOC

Bonjour,
Lors de l'analyse pédagogique (cas « Intrusion sur un serveur Windows »), nous avons identifié une compromission RDP sur `WIN-NI9FBK23SLO.branchoffice.example.com`.
Résumé : brute-force massif depuis `36.133.110.87` → connexion RDP réussie depuis `31.220.85.162` à `2024-02-06T19:52:39Z` → usage d'identifiants explicites et attribution de privilèges (4648/4672).
Action immédiate recommandée : isoler la machine, bloquer les IPs identifiées, prendre une image forensique, désactiver RDP externe, rotation des mots de passe admins.
Je joins les exports (4625_sample, 4624_RDP_exact, 4648_4672_window) et reste disponible pour assistance sur la mise en quarantaine / récupération des preuves.