

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

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、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、本コンテンツは初動調査に特化しています。

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

ハンズオンに取り組むにあたって、前提知識は「基本編」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

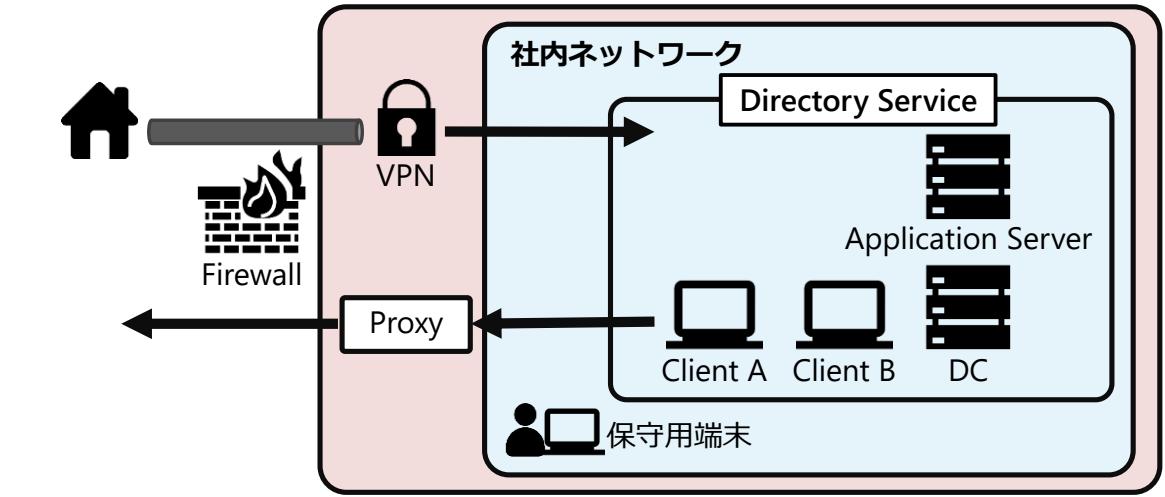
あなたは会社のセキュリティ担当者です。

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。

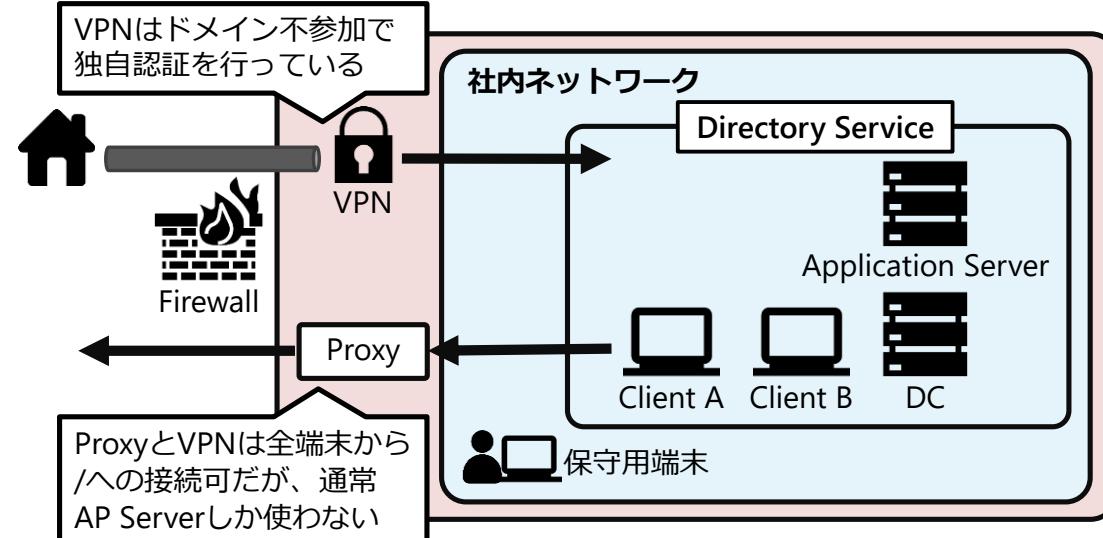
さて、このファイルはどこから来て、誰が設置したものなのでしょうか。

ハンズオン システム構成図

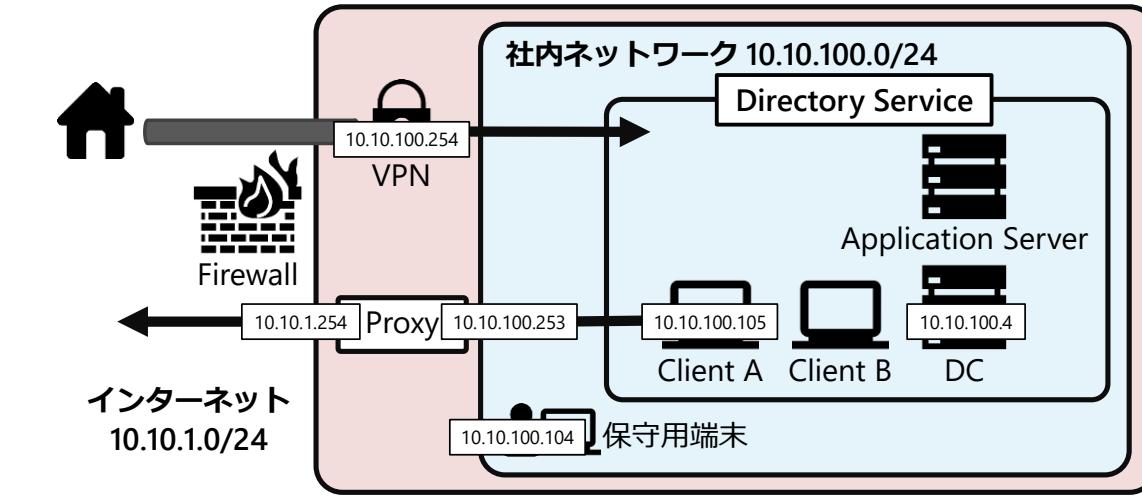


今回ハンズオンで分析するログを取得した環境を図に示します。

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

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アドレスを特定できれば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**

ハンズオン1

演習

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

The screenshot shows the Windows Event Viewer interface. A specific log entry for event ID 4624 (Logon) is highlighted. The event details are as follows:

アカウント名	domadm
ログオン ID	0x1AAD728
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]

Below this, network information is shown:

ソース ネットワーク アドレス	10.10.100.254
ポート	0

ハンズオン1

演習

- 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">
      *[EventID=4624]
      System[EventID=4624] and
      EventData[@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月11日10:17にdomuserからdomadmへKerberoast

The screenshot shows the Windows Event Viewer interface. The left pane lists several log types: イベントビューアー (ローカル), カスタムビューアー, 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 (which is selected), and サブスクリプション. The right pane displays a single event from the Security log:

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 10:17:17	Micros...	4769	Kerberos Service Ticket Operations

Event details:

Kerberos サービス チケットが要求されました。

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
ログイン GUID	{19a74800-2ce8-0572-0cb7-b5c4ff929b96}

サービス情報

サービス名	domadm
サービス ID	S-1-5-21-2544083802-1242352081-370156364-1105

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 脱晩化の種類	0x17
エラー コード	0x0
移行されたサービス	-

ハンズオン1

演習

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>
```

ハンズオン1

演習

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

The screenshot shows the Windows Event Viewer interface. A specific logon event (ID 4624) is selected from a list of 145 events. The event details show a new logon for user 'domuser' on the 'HANDSONLAB.LOCAL' domain. The source IP address is listed as '10.10.100.105'. The 'Source Network Address' field is also highlighted.

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 10:59:01	Micros...	4624	Logon

イベント 4624, Microsoft Windows security auditing.

新しいログオン:
セキュリティ ID: S-1-5-21-2544083802-1242852091-370156364-1106
アカウント名: domuser
アカウントドメイン: HANDSONLAB.LOCAL
ログオン ID: 0x15D19B5
リクエストログオン 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:
ローカルマシン名: -
ソースネットワーク アドレス: 10.10.100.105
ソースポート: 61032

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が怪しいと判断します。

ハンズオン1

演習

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

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、問題にはありません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

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
 - ✓ 誰が
 - ✓ 何を
 - ✓ どのように

「ハンズオン1から得られた情報」とは、10月11日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
- 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

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

ハンズオン2

演習

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

The screenshot shows the Windows Event Viewer interface. The left pane displays a navigation tree with 'イベントビューアー (ローカル)' selected. Under 'Security', there are three log entries:

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

The third entry is expanded to show detailed information:

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: ウィンドウズ ID: S-1-5-21-874346484-44980746-988080542-1001
アカウント名: eviluser
ログオン ドメイン: client-winx-0
ログオン ID: 0x2388D79

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:
ウィンドウズ ID: S-1-5-21-2544088302-1242352091-870156864-1106
アカウント名: domuser
ログオン ドメイン: randomlab

10月11日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月11日9:47にeviluserでRDP接続



ハンズオン2

演習

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

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: 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, and サブスクリプション. The right pane is titled "Security" and shows "イベント数: 11,640". A specific event is selected: 情報, 2023/10/11 9:46:32, Microsoft Windows security auditing, ID 4720, User Account Management. The event details show:

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

ハンズオン2

演習

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

The screenshot shows the Windows Event Viewer interface. The left pane lists several log types: イベントビューアー (ローカル), カスタムビューアー, Windowsログ, アプリケーションとサービスログ, and 保存されたログ. The right pane displays the Security log with 11,640 events. A specific event (Event ID 4624) is selected, which occurred at 2023/10/11 9:44:54. The event details are as follows:

セッション ID	イベント ID	ソース	イベント...
S-1-5-21-1074346454-44980746-988080542-1000	4624	Micros...	タスクの...
(1) 情報	2023/10/11 9:44:54	Micros...	4672 Special...

Event details (Event 4624):

- 新しいログオン: ソースセッション ID: S-1-5-21-1074346454-44980746-988080542-1000
アカウント名: itmanager
プロセス ID: 0x231B60B
プロセス名: -
ログオン ID: 0x0
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:
 - ローカルコンピュータ名: clientwin1-C
ソース ネットワーク アドレス: 10.10.100.104
ポート ID: 3389
- 詳細な認証情報:
 - アカウント: プロセス: NTLM
認証リクエスト: NTLM
接続元アカウント: -
パッケージ名 (NTLM のみ): NTLM V2
バージョン: 1

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2

演習

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

ハンズオン1とハンズオン2の結果をあ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

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はどこからか？

接続元IPアドレスを特定できればOK

ハンズオン2で判明した調査結果は、「10月11日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

ハンズオン3

演習

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

The screenshot shows the Windows Event Viewer interface. The left pane lists various log types: イベントビューアー (ローカル), カスタムビューア, Windows ログ, アプリケーションとサービス ログ, and 保存されたログ. Under 保存されたログ, the Security log is selected. The right pane displays a table of events with columns: レベル (Level), 日付と時刻 (Date and Time), ソース (Source), イベント (Event ID), and タスクの種類 (Task Type). Three events are listed:

レベル	日付と時刻	ソース	イベント	タスクの種類
情報	2023/10/11 9:44:17	Micros...	4624 Logon	
情報	2023/10/11 9:42:32	Micros...	4624 Logon	
情報	2023/10/11 9:41:55	Micros...	4624 Logon	

A detailed view of the first event (Event ID 4624) is shown in a modal window. The "Security auditing" tab is selected. The "General" tab is active, showing the following details:

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
ノード名: client-wifi-0
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
ホスト ノード名: client-wifi-0
ログオン GUID: {00000000-0000-0000-0000-000000000000}

プロセス情報:

29 | © 2026 JPCERT/CC Japan Computer Emergency Response Team Coordination Center JPCERT/CC®

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

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of event logs, and the right pane shows a detailed list of security events. Two specific logon events are highlighted:

アカウント名	ログインID
testuser	0x100C71B
testadmin001	0x1E16DCB

Both events occurred at 2023/10/11 9:30:07.

ハンズオン3

演習

回答 3. 10月11日9:26にVPNからtestuserへログイン

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: 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. The right pane is titled "Security イベント数: 11,294". It lists two events under the "Security" category:

レベル	日付と時刻	ソース	イベント ...	タスクの...
情報	2023/10/11 9:26:13	Micros...	4624 Logon	
情報	2023/10/11 9:26:11	Micros...	4624 Logon	

A detailed view of the first event (Event ID 4624) is shown in a modal window. The "新しいログオン" section contains the following information:

セッション ID	C-1-E-01-0031698157-2874844595-1753093504-1002
アカウント名	testuser
アカウント ドメイン	client-wini-C
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}

The "プロセス情報" section shows:

プロセス ID	0x0
プロセス名	-

The "ネットワーク情報" section shows:

ソース ネットワーク アドレス	10.10.100.254
ソース ポート	0

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sedlogo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

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

ハンズオン4では、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

ハンズオン4

演習

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/UE088QA AAAAAGa_51cAAAAAAA AAAAAAAAbnRkcyxaXQvN8axZ1IerpVmVjd09ye59Q - 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/MEFAAAAG_aAa_9LVi2HKH1rnhAAACAAStAAAbudGRlrmRpC98Y3PdmUgK6j2nWbN635L29 - 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://10.10.1.4/24MnZG107j0JBvhce_5fctf75KnxcdyJkm4Maah3F-2E2Qkxkz6l09JH3mcOsUhsWdTR8vd1Qd - 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://10.10.1.4/3QV16f59lbbtbtmN1Qqd3gtz2b+3D1RzQghthjQNECr23TTeilR1RqRv8ES62uzuc6awly7t - 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/mq2-2Bzsdn-77yH7M702Lcr1s0VG195_gdv_eFmQe8xcb5uv97_E996kRL7wIgde5X2r - 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/eOx2hmeIDmPc2z_vh3jEx97-cLw67-Wanp_mPNuN4JeszTQBytNmwe692LzLyOvHQb5xs-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/FeCf7xwPGzFLWf_PAAAAAAG_aAaAgOr_Pz_Zw4_9FB8_AAAAAAAAAAAA - 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/AAAAAAAAP_27hOpTgSqcj1uo9wTx9181M/reSSb9yv0v5_T5Q29AAAAAAA - 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/ABgdp2-swxNs18pd1t1vP45_xT2kWbXfRkuIXX28c127FY77-31vgpgetLAAA - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.108 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/AAAAAF_xInqT5_3m8:BAAMAAA - eTBu35_88x67jLF_9k679nG6-2G6MMasv7b/U6NF6 - 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/_Ng8a_24BAAAAAAAAMAUrye_-3taenCMAAAAMAAAAsAt6evP_P8_TffffXwp7vBv2 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.237 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/5f2f719Rsds19L_2699se_aTHfr3rQ1qRg8t87Nw16N253PPRUo_Og6-2r4dJ3iSD3vCmKhN - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.397 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/Nc1p_txdge6bHPm_o_FtEd_1_KN8-61mlm1Xo_fMyAVp230oy7n8dct3x-59kxz2_9_VCTVbM - 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/c3m_r_yhne_1991b3t8pxw6_RkVcp6sYXcodXg1m30M04_tu196-Jus3FB-3Thm4uH1p68d - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.587 3 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/B_sq_MeLhs1oV9QzE720jW44n1kv9a120fj401Mba2z2b2mWLL10m_v1nLWUmpl1ho1 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.599 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/2emyc1wF0SpVxhdeewgW178Qn20f8d1c7yxXpozo1wbyxp_jeFvOe2tpdnk812 - 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://10.10.1.4/9Ku1XX8jCVBj1500U88H1tx24r1y46_Urtdtmfayjo_3x93f2judic17zx24in-dH1 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.781 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/ok1s1zeHnTch7-usC3f1FnQ_MHueuxowuod1DyXhD1-4nP1m9povkC66akovfztcoMcLy7 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.859 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/23qisuxoHo_eufgh1m_Hc1k2f3te2BMO5-15M2m2iply_cdkfrkvgQygtQu-JU5c110F5 - 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/x0tul1cznogdy_WoXhHgsv0u5wam44u0trkrnpgrLco1_STN7zshNfHss5yovf77yAn50E - 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://10.10.1.4/0u1312q1tbnsn9NLDhbgq_e7N1R53p_w001xmmsm_w55d0Tatax00TnsTpzbv7QLE - 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://10.10.1.4/0u10Dq1s5kf_j110Bpzmh7v7D055_w52cXw5w9y897t87z2aX47c5Vh9x_Nk53p9m - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.125 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/xCh-a12j0Bxhs8_lfpmh0Jifcwca5kgx1u0L7oHmmitusvA-153RVj0eywJ07915qao-kuer - 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/n05IK1llowQm3uy48exVh0HogJruLzuiYIMr12Xcw0mzXOvM1Ekyv13muF9qjcoox1D - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.271 1 10.10.100.105 TCP_MISS/200 276 GET http://10.10.1.4/0u10Dq1s5kf_j110Bpzmh7v7D055_w52cXw5w9y897t87z2aX47c5Vh9x_Nk53p9m - 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？）ハンズオン3
- 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

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