

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



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

自身に合ったツールを使ったり、自分のお好みのツールを見つけるために様々なツールを使ってみるのも
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」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。

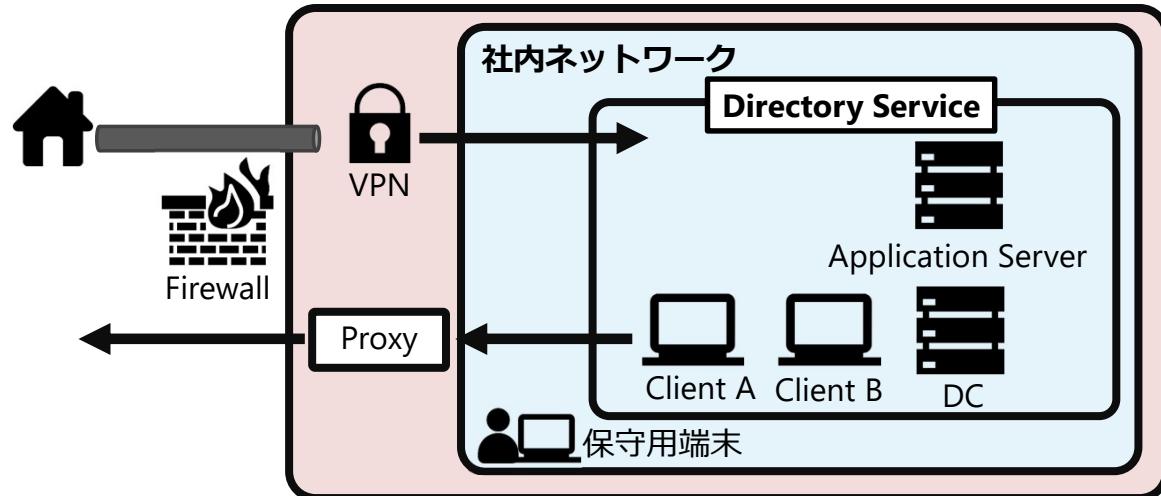
ある日、いくつかの部の職員から「見覚えのないファイルがデスクトップに生成されている」という報告を受けました。

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ではそういう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。

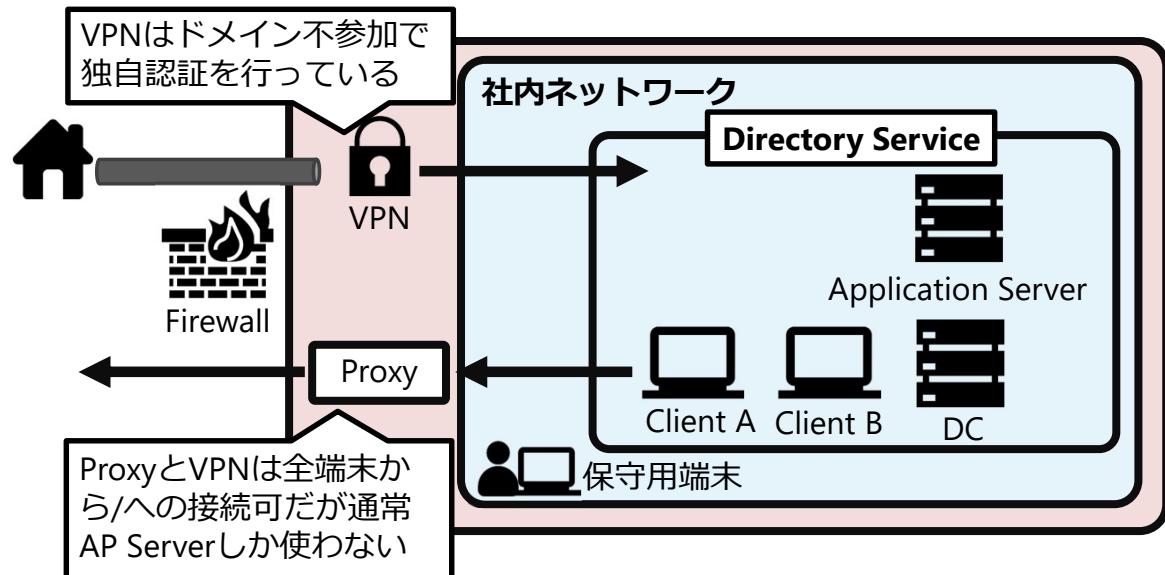
本ハンズオンでは、インシデント発生組織のログを分析することを想定して進めます。

ハンズオンシステム構成図

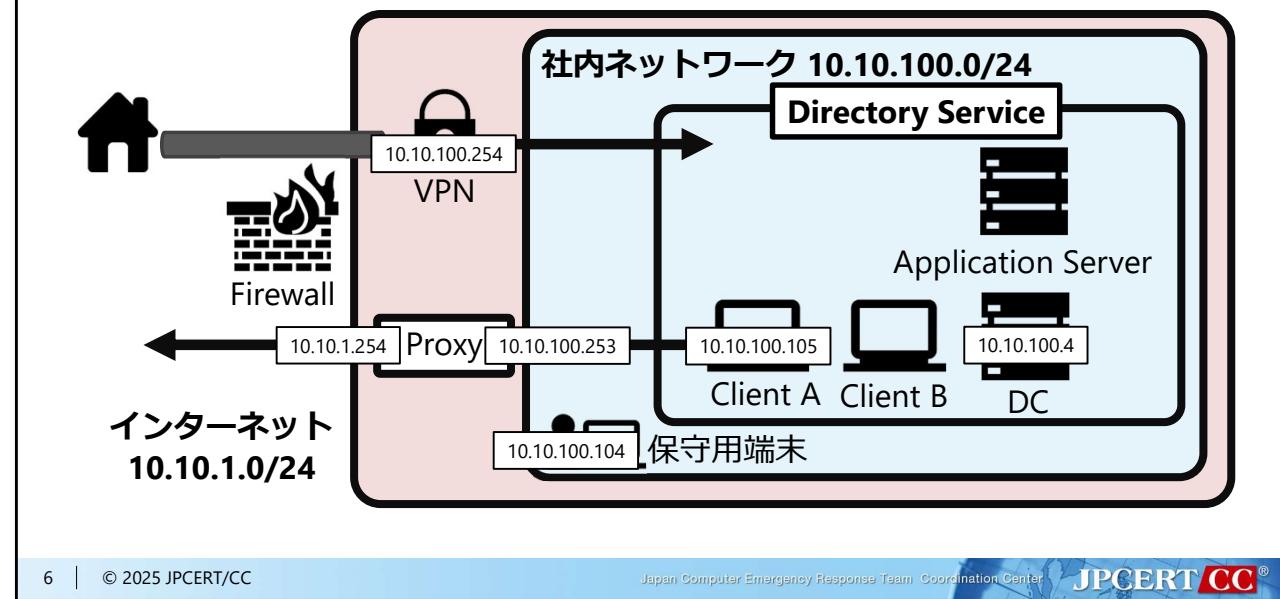


今回ハンズオンで分析するログを取得した環境を図に示します。

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、10/12 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

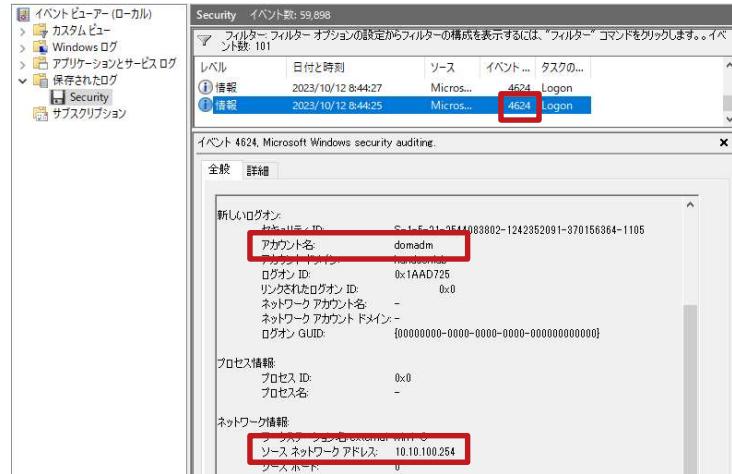
回答

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[@Name="TargetUserName"] = "domadm" and
        Data[@Name="IpAddress"] = "10.10.100.254"
      ]
    </Select>
  </Query>
</QueryList>
```

ハンズオン1

回答

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

Security イベント数: 59,898

フィルター: フィルター オプションの設定からフィルターの構成を表示するには、"フィルター" コマンドをクリックします。。イベント数: 1

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

イベント 4769, Microsoft Windows security auditing

全般 詳細

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 メンバー:	HANDSONLAB.LOCAL
ログオン GUID:	{19a74800-2ce3-0572-0cb7-b5c4ff929b96}

サービス情報

サービス名:	domadm
リード SID:	S-1-5-21-2544083802-1242852091-370156364-1105

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:	-

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">
      *[EventID=4769] and
      EventData[Data[@Name="ServiceName"] = "domadm"]
    </Select>
  </Query>
</QueryList>
```

ハンズオン1

回答

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

The screenshot shows the Windows Event Viewer interface. The left pane displays a tree view of logs: Event Viewer (Local), Custom View, Windows Log, Application and Service Log, and Security. The Security log is selected. The right pane shows a list of events with a total of 59,898 events. One event is highlighted, showing details for a logon event:

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

A detailed view of the selected event (Event ID 4624) is shown below:

新しいログオン:	
セッション ID:	0x15
アカウント名:	domuser
アカウント ドメイン:	HANDSONLAB.LOCAL
ログオン ID:	0x15D1B85
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}

Below this, there is a "プロセス情報" (Process Information) section:

プロセス ID:	0x0
プロセス名:	-

Finally, there is a "ネットワーク情報" (Network Information) section:

ソース ネットワーク ジョブ ID:	-
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が怪しいという判断をします。

ハンズオン1

演習

タイムライン

10/11 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

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

✓イベントID:4769で10/12 8:43以前をdomadmで検索

10/12 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

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: 11,640

▽ フィルター フィルター オプションの設定からフィルターの構成を表示するには、"フィルター" コマンドをクリックします。イベント数: 7

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

サブエント:

アカウント名:	eviluser
アカウント ID:	client-WIN-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:	-
仮想化アカウント:	いいえ
昇格されたトーケン:	いいえ

(偽装)情報 (偽装)

新しいログオン:

アカウント名:	domuser
アカウント ID:	domuser

21 | © 2025 JPCERT/CC

Japan Computer Emergency Response Team Coordination Center

JPCERT CC

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

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 ログ, 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 shows a list of events with the title "Security イベント数: 11,640". One event is expanded, titled "イベント 4624, Microsoft Windows security auditing". The details pane shows the following information:

アカウント名	セッション ID	ログオン ID	ログオン タイプ	サブジェクト
client-win2-C\$	0x3E7	0x3E7	10	SYSTEM
client-win2-C\$	0x3E7	0x3E7	10	client-win2-C\$
client-win2-C\$	0x3E7	0x3E7	10	handsoniab

Additional details include:

- 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: handsoniab
ログオン ID: 0x3E7
- ログオン タイプ: 10
新規セッション ID: 1
仮想アカウント: (なし)
昇格されたトークン: (なし)
- 偽装レベル: 偽装
- 新しいログオン:
セッション ID: S-1-5-21-97348464-44900746-90000542-1001
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 3. 10/11 9:46 に itmanager が eviluser を作成

The screenshot shows the Windows Event Viewer interface. On the left, there's a navigation pane with options like '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' (which is selected), and 'サブスクリプション'. The main pane displays a table of events. One event is 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 9:46:32	Micros...	4720	User Account Management

Below the table, a message says 'イベント 4720, Microsoft Windows security auditing.' and it details the event: 'ユーザー アカウントが作成されました。' (A user account was created). It shows two entries under 'サブジェクト':

セキュリティ ID:	
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

And under '新しいアカウント':

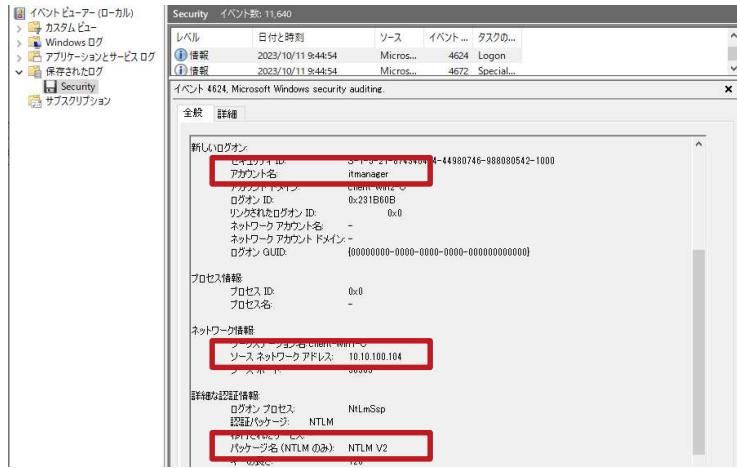
セキュリティ ID:	
アカウント名:	eviluser
アカウント ドメイン:	client-win2-C

At the bottom of the window, there are copyright notices: '© 2025 JPCERT/CC' and 'Japan Computer Emergency Response Team Coordination Center JPCERT CC®'.

ハンズオン2

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2

演習

タイムライン

10/11 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

10/11 9:46 itmanagerがeviluserを作成

✓イベントID: 4720で検索

10/11 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

10/11 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

10/11 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 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 ヘログイン
2. 10/11 9:30 に testuser から testadmin001 ヘログイン
➡ 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 ヘログイン

ハンズオン3

演習

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

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 selected), and サブスクリプション. The right pane shows a list of events under the Security log. A specific event is selected, which is a Logon event (Event ID 4624) from Microsoft Windows security auditing. The event details are as follows:

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
アカウントタイプ: client-win32
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タイプ: 0
ログオン GUID: {00000000-0000-0000-0000-000000000000}

At the bottom of the event details, there is a "プロセス情報" section.

29 | © 2025 JPCERT/CC Japan Computer Emergency Response Team Coordination Center JPCERT CC®

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

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 shows a list of events under the Security category. A specific event (Event ID 4624) is selected, which details a successful Logon event. The event information includes:

レベル	日付と時刻	ソース	イベントID	タスクの名前
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

The event details show the account was successfully logged on. The subject account is testuser, and the target account is testadmin001. The logon type is 2 (Interactive). The new logon information also shows the transition from testuser to testadmin001.

ハンズオン3

回答 3. 10/11 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, and 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:

レベル	日付と時刻	ソース	イベント ID	タスクの名前
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 (ID 4624) is shown in the bottom pane. The event details are as follows:

新しいログオン:
アカウント名: testuser
ノード名: client-win10
ログオン ID: 0x1BF1A127
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: [00000000-0000-0000-000000000000]

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:
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

10/11 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seologo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

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 10.10.190.105 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 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/5e6db0aaaaaaagb_S1cAAAAAAAAAAAAAAaAbnRkcy5kaXqvQwN0aXZ1ERpcmVjdg9yeS9Q - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.497 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/5wEfAAAAGaaL9lV2HK8H1zhnsAACASA1SA1AbdGrLmRpdc9By3RpdmUgJG1yWb3J5L25b - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.573 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/27HmuzG107J0ljbvHece_5ft175Nk2d7jkNM4n4h3F-2Ezqkkz6LF09JH3tmCD5vUHSw0d1Qd - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.651 2 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/7QVEef50Lb8bt6mN1iq0g3gtkZbo3D1r2gthetj0NEcR23TseqlRL1Q0Rv0E5S6zuzucGalwy7t - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.716 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/m1o2_-8dzsnd-f7fz70z1cris0vG195_gdv_e6Fn0F8xcb5uV97_679E996KRL7waTgde5x2r - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.781 2 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/p0XNmee1DmPccz0_wH3LEx97_ctv67-Wang_nPHN6j3esZfQBYtMwZ69ZLyQv9HQB5xs-40x - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.884 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/Fec17xwuPg3zFLwfrjPAAAAKAAAAAAaAAAaAAAaAAAaAg0Tr-Pz_Zw4_-9FB5_8AAAaaaaAAA - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:34.955 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/AAAAAAAAPB_z7MwGFTg5Qcvjzuo8w9Fx9tB1M7ee58RbvOv5_f5QMAAAAASQCV - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.027 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/AABgbdpz-swXRM518pdK1tv1v45_xFkH0KFLRkuhXwX28c32f777-W_31vgepeLAAAAAA - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.100 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/AAAAAFxd1nQTs-3m8z8AaaaaAAAaAAAaAAA-aK7obU35_80x6fJLF_9k079m36-02kHmWs7brU6Hf6 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.169 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/_NgbAn_240nAAAaaaaAAU1rYz_-3ta9nCAAAAAAaAg8t6v_P8_2rfFFfxwp78v0z - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.257 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/5zv8F7c79Rsds19L_Z69YSa_atHF3rbQjR6ETNw1Ghz53kPPRUu_QQ6z2r4dA3s5D3CmhkNn - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.359 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/NzSp-Txbg6gdHPWy_efc5D_l_KNBs61wn1k3e_fnKy4Ap23Doy7n60Tcsx-59kx2y3_VtV1m - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.432 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/3cM_yohEm_I99ib3tEqXw0jRKVcPb6YxcodXqiMj30W04_tw19d_ju5ifB-sThbm14uH1p6oBU - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.502 3 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/85qp_TReLh5e1oV8KQw2E7ZQjM4n4F5KvGalZufJJ401HbaK2wzbzmnVL1iDmry1WLvUnp1h01 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.595 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/2emEyCw1RFOVSpVxIddeekWeIt7RQj2uKf8dLfcRjYkxPO2z1lwbymkpx_dFv0EZTpdkn01Z - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.671 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/4KH11uL1Xx-8jCVBj1bQULBL0oHi7x24r1Y46y70vaTdtMpavjo-X59jR2udkci7zX241k-dhi - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.789 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/OKsLz0erHwTdhj-_uSC3Pz1fnkOrHmeueoxwuoOioiyXhD1-4hPN19Mp0YKc6dK6oEfZtOnCw1Vt - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.858 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/23oisuxo6HoY6ufcqh61wnHFcikf3Te2bnOS-15Nz02kpl-ycdkfKbvg7gtQvJ7U7Sc11lF5 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.925 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/btw1CR2h0gUy-WDdkHksVqUdcalUmu4abultrnRYWpgrLcz0l_STNTzSh0fFN5sySovF3TYmJ06 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:35.990 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/g1uV3z1Kptmsn9wNLDhkoqfe71NjR3paw10lxmwsx_rwsduTtaix00RStnSpzGbvwT0L1 - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.057 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/yUH0loqfsRFsfy11Btp2nsDXn7DU55_WkN3ZkSwed9yf2h68vRbx4x4F5c5hVq77MssePnW - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.123 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/XCh-a1zDjBkh5mB-TpmAhnoj1fwcxASkgX1U0L7oHm1ztusVA-153RVjbeypW79b1Sqgo-ku0r - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.197 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/ND5ZkiloaQmsuy48esxVxDLhdog1RulZUY1Miri2XcwlnzXOvH1EKyV13HMuE9pqscOxit1Jd - HIER_DIRECT/10.10.1.4 text/html
2023/10/12 02:51:36.274 1 10.10.190.105 TCP_MISS/200 276 GET http://10.10.1.4/luuimwCw1T133A_E59t1mP1TdQ47w4Bm3V3AVukue1V11eF7Hd4oT-Tegh1Rj21i1uXt8mo - 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** eviluser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

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？）VPNの調査は省略
- 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？）ハンズオン 3
- 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 eviluserでRDP接続 ハンズオン 2
- 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 ハンズオン 1
- 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 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ます
- ▣ 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、どこで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