

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

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 イン트로ダクション

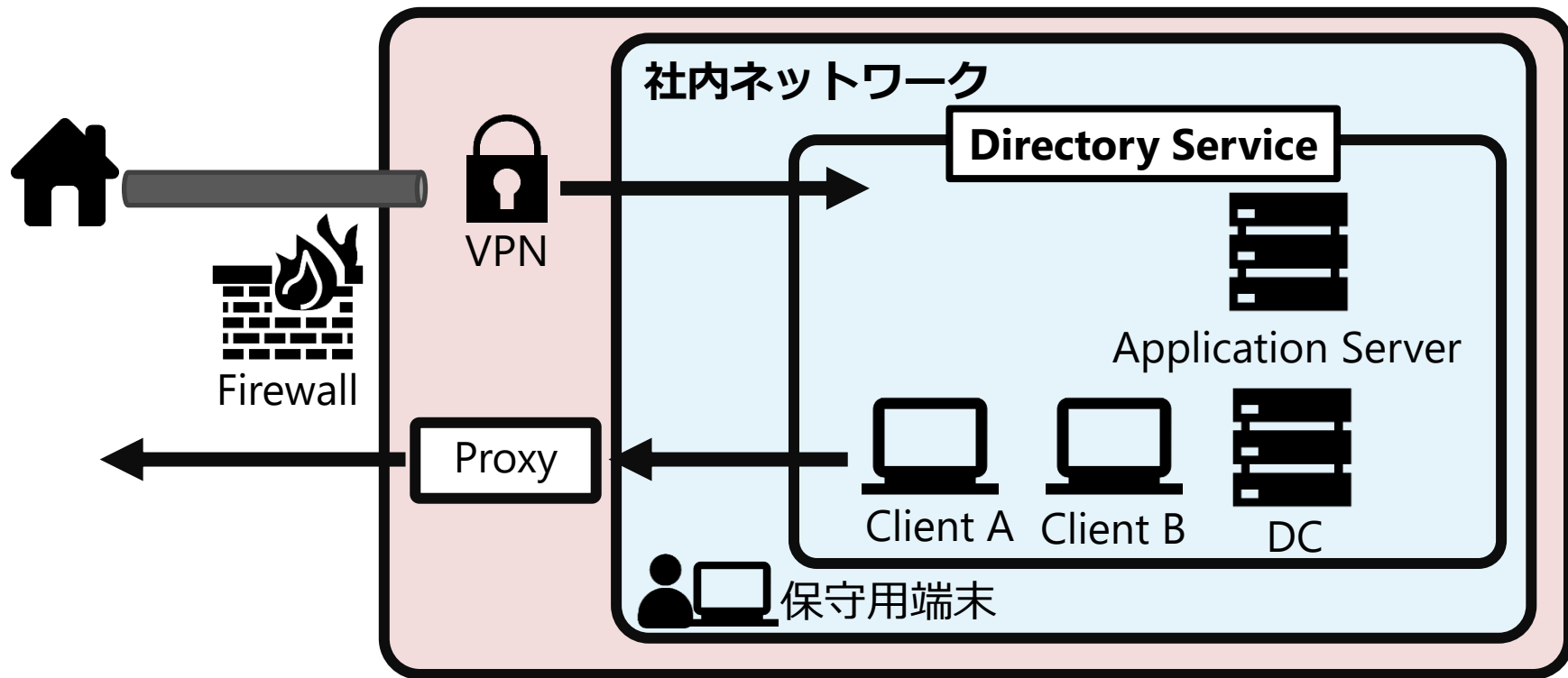
あなたは会社のセキュリティ担当者です。

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。

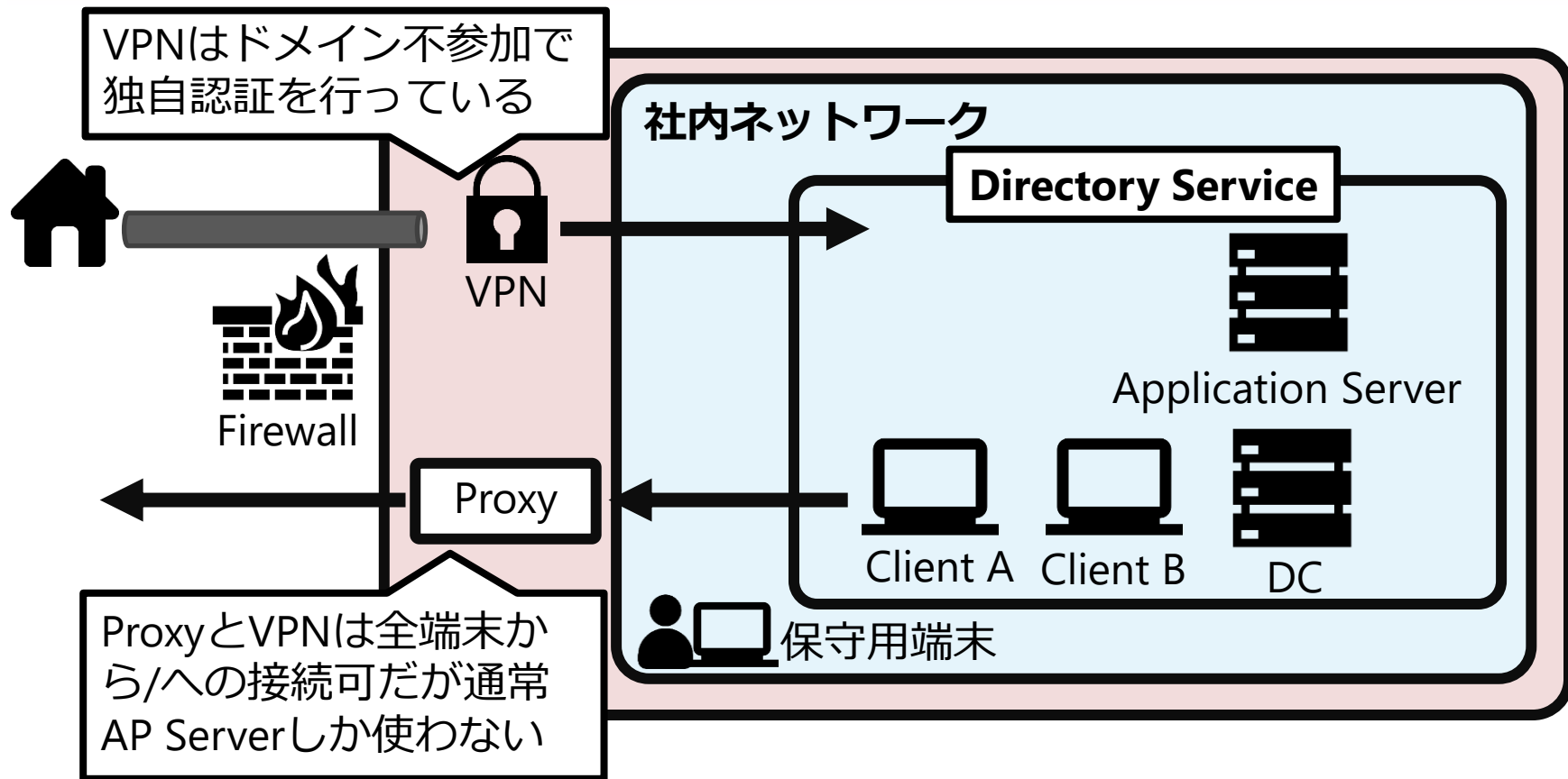
Windows Update等による影響かと考えましたが、ほぼ同じ構成の私用PCではそういったファイルが生成されておらず、自社の業務PCでのみ確認される事象であることが分かりました。

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。

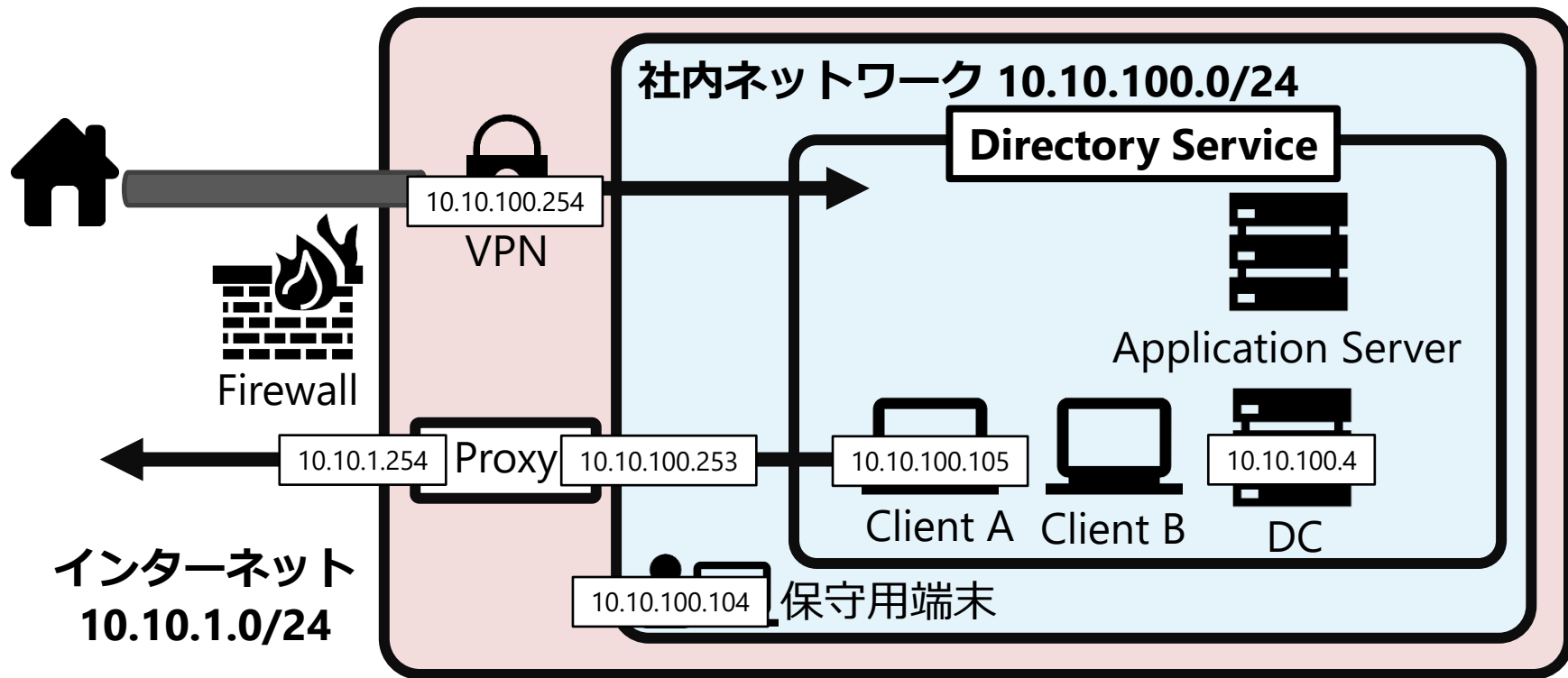
ハンズオン システム構成図



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、10/12 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

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

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**

回答

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

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

項目	値
新しいログオン:	
セキュリティ ID:	S-1-5-21-3544083802-1242352091-370156364-1105
アカウント名:	domadm
アカウント ドメイン:	handsonlab
ログオン ID:	0x1AAD725
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:	
ソース ネットワーク アドレス:	10.10.100.254
ソース ホスト:	0

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>
```

回答

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

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: 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-1-0-21-2544083802-1242352091-370156364-1105

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. 10/11 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>
```

回答

3. 10/11 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 pane shows the 'Security' log selected. The main pane shows a list of events, with event ID 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-1-5-81-9544083802-1242352091-370156364-1106
アカウント名:	domuser
アカウント ドメイン:	HANDSONLAB.LOCAL
ログオン ID:	0x15D13B5
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:	
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

10/11 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

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

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
 - ✓ だれが
 - ✓ 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

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

回答

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

The screenshot displays the Windows Security Event Viewer interface. On the left, the 'Security' log is selected. The main pane shows a list of events, with event 4624 (Logon) selected. The details pane below shows the logon information for the user 'eviluser'.

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
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: 0x1501-0710-846464-44980746-988080542-1001

アカウント名: eviluser

アカウントドメイン: client-win20

ログオン ID: 0x2838D79

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: 0x1501-0710-883802-1242352091-370156364-1106

アカウント名: domuser

アカウントドメイン: randomad

回答

2. 10/11 9:47 に eviluser でRDP接続

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: 6

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

The screenshot shows the Windows Event Viewer interface. The left pane displays the 'Security' log. The right pane shows the details of event ID 4720, 'User Account Management'. The event description states: 'ユーザー アカウントが作成されました。' (User account created). The 'Subject' section lists details for the created account: 'itmanager'. The 'New Account' section lists details for the account being created: 'eviluser'. Red boxes highlight the event ID '4720', the account name 'itmanager', and the account name '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 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:	0x281C149

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

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itmager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

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

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

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

回答

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

The screenshot shows the Windows Event Viewer interface. The left pane displays the tree view with 'Security' selected. The right pane shows a list of events, with event 4624 (Logon) selected. Below the list, the details for event 4624 are displayed, showing the logon information for user testadmin001.

レベル	日付と時刻	ソース	イベント...	タスクの...
情報	2023/10/11 9:44:17	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

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-1-5-21-2931698157-2874844595-1753093504-1003
アカウント名:	testadmin001
アカウントタイプ:	Client-win...
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:	
ログオン GUID:	{00000000-0000-0000-0000-000000000000}

プロセス情報:

プロセス ID:	0x00000000
----------	------------

回答

2. 10/11 9:30 に testuser から testadmin001 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 shows a list of events, with event 4624 (Logon) selected. The details pane below shows the event information for event 4624, Microsoft Windows security auditing.

Event 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-1-5-21-238163067-2874844595-1753093504-1002

アカウント名: testuser

アカウントのドメイン: client-win10

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:

セキュリティ ID: S-1-5-21-238163067-2874844595-1753093504-1003

アカウント名: testadmin001

アカウントのドメイン: client-win10

ログオン ID: 0x1E16DCB

回答

3. 10/11 9:26 に VPN から testuser へログイン

The screenshot displays the Windows Security Event Viewer interface. The left-hand pane shows the 'Security' log selected. The main pane shows a list of events, with event 4624 (Logon) selected. The details pane on the right shows the 'General' tab for event 4624, 'Microsoft Windows security auditing'. The 'New Logon' section contains the following information:

- セキュリティ ID: S-1-5-21-2931698157-2874844595-1753093504-1002
- アカウント名: testuser
- クライアント IP: client=win1-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 'Process Information' section shows:

- プロセス ID: 0x0
- プロセス名: -

The 'Network Information' section shows:

- ソース ネットワーク アドレス: 10.10.100.254
- ソース ホード: 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

10/11 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

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

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. 10/12 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

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/UESDBBQAAAAAGa_S1cAAAAAAAAAAAAAAAAAAAAbnRkcy5kaXQvQW0hZlZlIERpcmVjdG9yeS9Q - 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/SwMEFAAAAAAGaAal9LVzHK8HIZnhsAAACAASIAAAABudGRzLmRpdC9BY3RpdMUGRlyZWNo63Jl250 - 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_5ft175Nk2dyjknM4h3f-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://10.10.1.4/3QVE6fS0L8b8t6mBniiQgG3gtkZbo3DiR2GgthEjJQNECrR23TeqilRIQ0Rv0ESS6zuzucGawY7tT - 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-f7fzM70ZLcncisOvG195_gdv_e6FnQeY8Xcb5uvK97_6T9E9W6KRL7waIgd5X2r - 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_nPHN6W3esZfQ8YtWmWz69ZLy0v9HQ85xs-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/Fec17FwxuPq3zfLWwFJPAAAAAAAAAAAAAAAAAAAAAAG0Tr-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/AAAAAAAAAP0B_z7MvGPTg5Qcvjzu08w9fX9tB1M7eeS8RbVe0v5-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/ABgbdpZ-swXrn5818pdK1tv1vP45_xf2kH0KFLRrkuNX8X28c327fY77-W_81rvpgpetLAAAAAA - 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-3m8z8AAAAAAAAAAAAA-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_240mAAAAAAAAAAAAAAuIrYz_-3ta9nCAAAAAAAAAAAG8t6vP_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_aTHF3rb0iRpR6ETNw16NzS3kPPRUq_Q0p62n4dAj3c5D3vCmhKn - 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_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_I99ib3T6qXW6jRKVCpb6YxcodXqIM3J0W04_tw19d-Ju51FB-sThbm14uHi7p6oBU - 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_TReLh5e1oVBKQw2E7ZQjhw4nF3KVGaLZUJfJ401HbaDk2wbZmmVLLiDmp_y1WLUVUwIlhoi - 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://10.10.1.4/2etMyCwLRF0VSPVXWdkeekgWeIr7RHQW2UKF0dLFCrJYKxYP02oZ1wbywXpK_dFEvOEZTPdnK0l22 - 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://10.10.1.4/0KH1U1XXr8jCV8jlbG0ULB0qHitXZ4rlY46yT0vtaTdtmPaVjo-X59J3R2udkcIz7sKZ41K-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-uSC3Pz1fnKQrHMeuxowuOoiOyvXhDi-4hPNi9mPOYKc66dK6oVEfz0nCWjvI - 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://10.10.1.4/23qisuxo6HOY6ufcqh61wrHFCikzf3Te2bnOS-15N2mQZkPLy-yccddFKbvgJgtQvrJUTSc11UFS - 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-WDXdkHksVqUdcaUmu4abultrRYWpgrLcz0L_STNTzSh8fNB5sySovFJTYaMj06 - 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://10.10.1.4/0iuv3iZKPtKnsV9NWLdHk0qfe71NJRsJpaWl01xmXsWHX_rwu5duTtaTxaOOYRSnSpGzbvkTOLI - 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/sYUHQoqfs9RsFjfM118tpznSDXN7DUS5S_wKn3ZXW5edyB9fzh68vzRbXc4fKc5VHqX7MMs3ePnW - 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-aiZdJbkh5Mb-TpmAHNoj1fwcXASKq1UOL7o0HmJztusVA-153RVjbeypWJ79b1SsqGo-ku8r - 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/ND5Zkii1loaQmsUy48EsXvDLHog1RuLZUIYIMiRi2XcWUnZOXvHMiEkYVI3HMUe9pQsc00XtIjD - 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/cuAimVcUvT133A5E9tZ1UvvaTdsQv4Tui8BuL3Y3dVkvW3Y3j5Z7Ht4Q5Wt6uhU21islyTz8m - 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 ハンズオン 2
- 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 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

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