MWS Cup 2024 x DFIR ポストミーティング

MWS Cup 2024
DFIR作問チーム
阿部　航太

アジェンダ

- 今年の出題について
- 競技結果
- アンケート結果
- 反省・考察

DFIR課題メンバー

- ソリトンシステムズ
  - 荒木 粧子
  - 尾曲 晃忠
  - 木野田 渉
  - 伊神 和馬
  - 後藤 公太
  - 西井 雅人
  - 白鳥 隆史
  - 近藤 龍一
  - 朴 淑喜
- 日立製作所
  - 鬼頭 哲郎
- 日立システムズ
  - 関谷 信吾
- NTT西日本
  - 鴨下 将成
  - 市川 久哲
- NTTセキュリティ・ジャパン
  - 大倉 有喜
  - 戸祭 隆行
- NTTコミュニケーションズ
  - 二瓶 雄貴
  - 遠藤 行人
  - 阿部 航太
- 無所属
  - 天笠 智哉

あらすじ

イーデン・カレッジは、学問、スポーツ、芸術など様々な分野において優れた学生が集まる小中高一貫の国を代表する学校である。そのため、国を代表する著名人の子息も多く在学している。

Henderson先生からIT管理者に、Fileサーバにアクセスすることができないと連絡があった。IT管理者が確認したところ、確かにアクセスできないことが確認された。Webコンソールでファイルサーバを確認したところ、以下の画面が表示されていた。

事件を解決せよ！

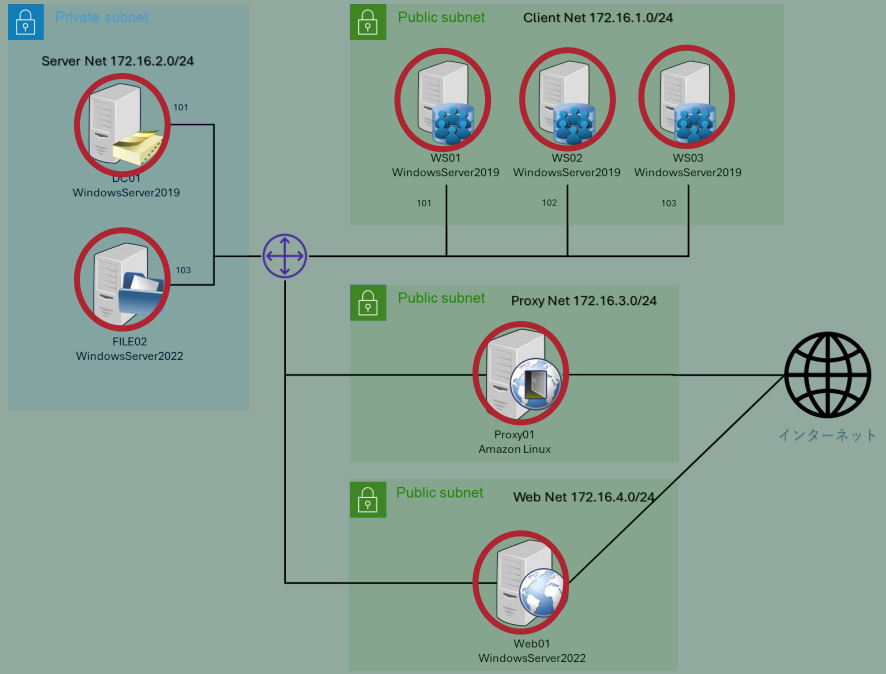
Bitlockerの有効化について、誰にも心当たりがない。

昨年に引き続き、敵国の諜報活動が活発化しているとの情報がある。そのため、敵国スパイの諜報活動かもしれない。。

EDRログ、プロキシログ、Webサーバーのアクセスログを解析し、イーデン・カレッジでどのような出来事が起きたか明らかにして欲しい。

競技で解析するログ

- 各エンドポイントのEDRログ
- インターネットの接続点に設置したProxyのログ
- Webサーバーのアクセスログ



解析するログ

EDRログ

- Soliton InfoTrace Mark II のログ
  - Soliton Dataset で提供されているデータと同様のフォーマット
- 記録されている情報
  - プロセスの起動・終了
  - ファイルの作成・削除
  - レジストリ操作
  - ネットワーク接続・切断
  - Windowsイベントログ情報
  - など

解析するログ

Proxyログ

- OSSのプロキシソフトウェア Squid のアクセスログ
- 記録されている情報
  - クライアントIPアドレス
  - HTTP リクエストメソッド
  - HTTP アクセス先URL
  - HTTP レスポンスステータスコード
  - クライアントから送信（アップロード）されたデータ量の合計
  - クライアントへ送信（ダウンロード）したデータ量の合計
  - リファラ
  - User-Agent
  - など

解析するログ

Webサーバーのアクセスログ

- OSSのプロキシソフトウェア Apache Web Server のアクセスログ
- 記録されている情報
  - クライアントIPアドレス
  - HTTP リクエストメソッド
  - HTTP アクセス先URL
  - HTTP レスポンスステータスコード
  - 転送容量
  - User-Agent
  - など

課題概要

0. Prologue 1			
1.1. Impact 1	1.2. Impact 1	.-3. Impact 1	1.4. Impact 1
2.1. Initial Access 1	2.2. Initial Access 1	3.1. Discovery 1	3.2. Discovery 1
4. Lateral Movement 1	5. Credential Access 2	6.1. Lateral Movement 1	6.2. Lateral Movement 1
6.3 . Lateral Movement 1	7. Exfiltration 1	8.1. Incident Response 1	8.2. Incident Response 1
8.3. Incident Response 1	8.4. Incident Response 2	8-5. Incident Response 2	8-6. Incident Response 2

FLAG/選択形式 : 20pts

記述形式 : 5pts

今年のテーマ

BitLockerを利用するランサムアクター

今年のテーマ

https://www.kaspersky.co.jp/about/press-releases/vir28052024

競技結果

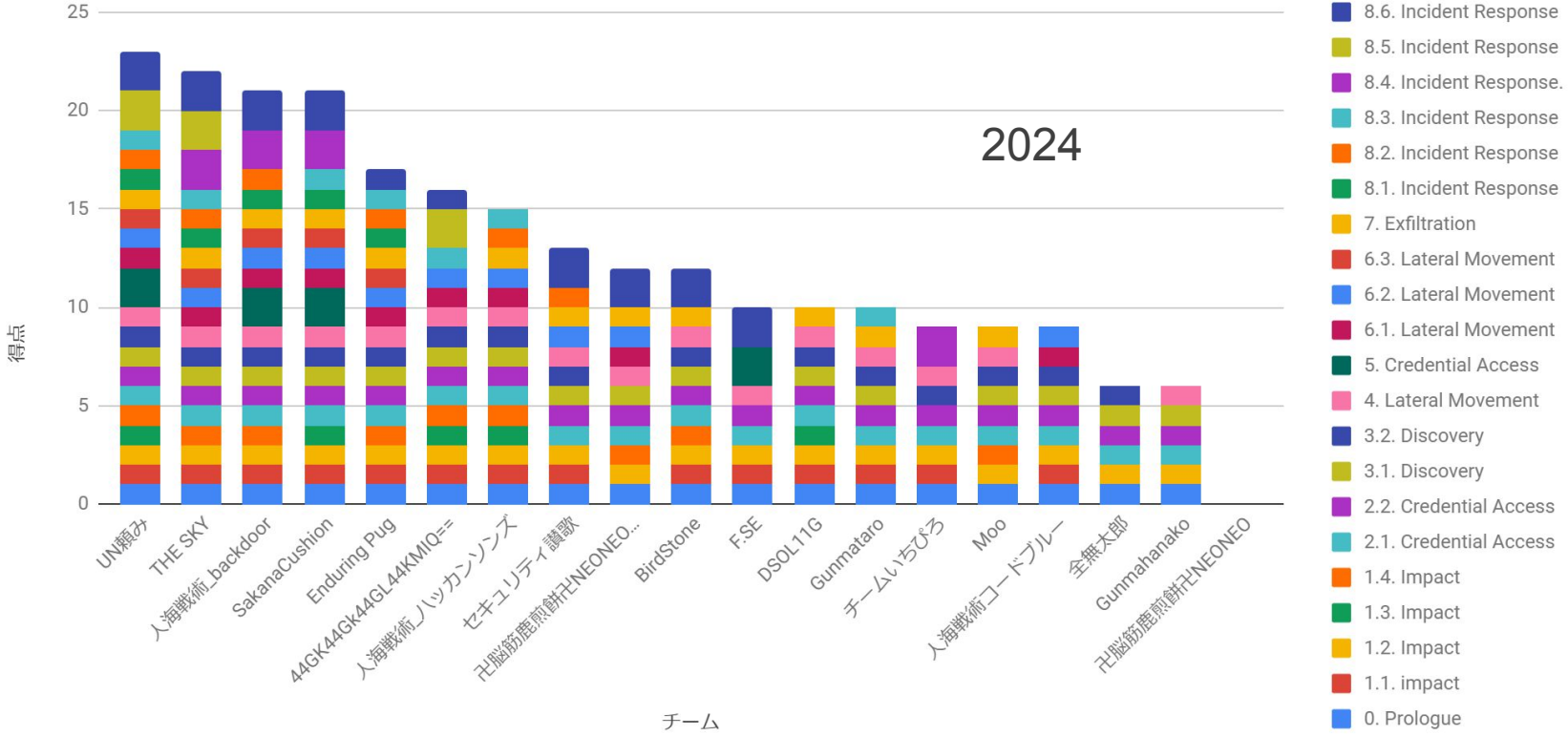
攻撃シナリオまとめ

Timestamp	Tactics	Event	Host	User
17:04:20	Initial Access	web01のXAMPPにExploit	Web01	Green
17:04:40	Discovery	簡単な環境の調査		
17:05:32	Discovery	SharpHoundを持ち込んで実行		
17:08:05	Discovery	SharpHoundの結果を持ち出し		
17:10:26	C2	meterpreterを持ち込んで実行		
17:11:43	Lateral Movement	WinRMでWeb01からWS01に横展開		
17:12:25	C2	meterpreterを持ち込んで実行	WS01	
17:13:21	Discovery	簡単な環境の調査		
17:15:00	Credential Access	Royal TSのクレデンシャルファイル(.rtsz) を出力し持ち出す		

攻撃シナリオまとめ

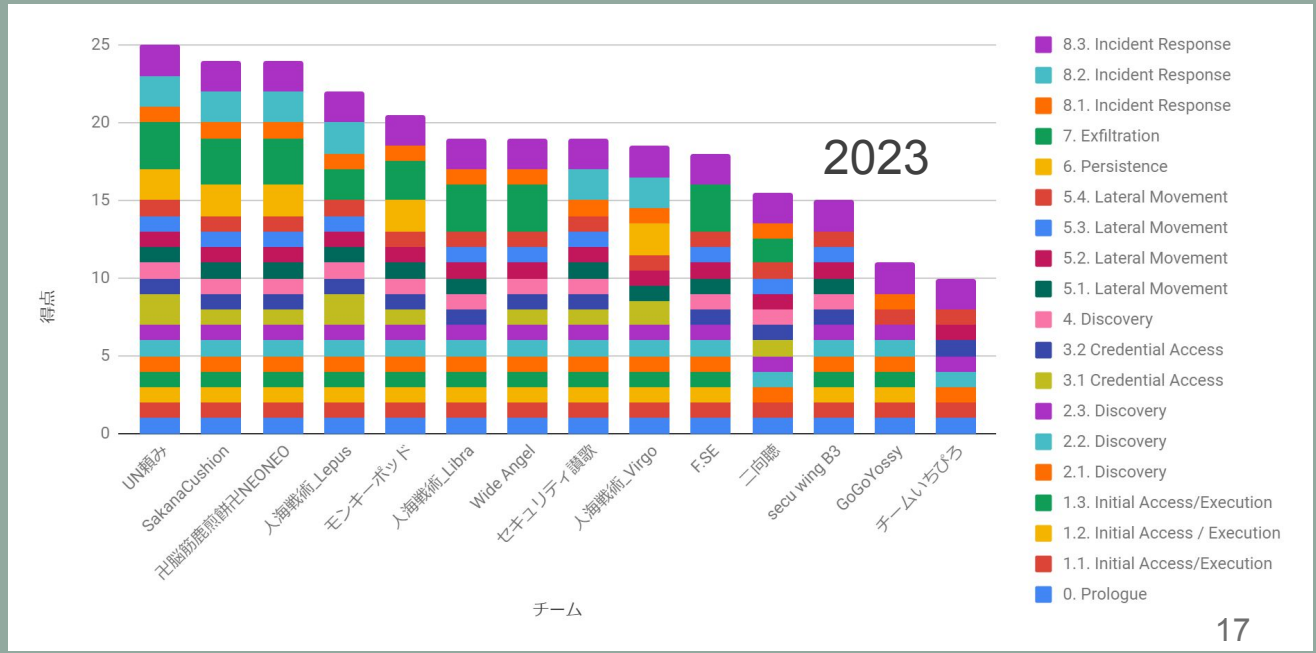
Timestamp	Tactics	Event	Host	User
17:19:05	C2	Ngrokを持ち込んでインターネットからWeb01を経由してDC01にRDPできるようにする	Web01	Green
17:20:33	Lateral Movement	DC01にRDPで接続	DC01	Viehmann
17:21:37	Credential Access	ntdsutil.exeを用いたNTDSの取得		
17:24:14	Exfiltration	FILE02の機密ファイルのRDP経由での持ち出し		
17:26:08	Impact	FILE02をBitlockerで暗号化		

チーム別

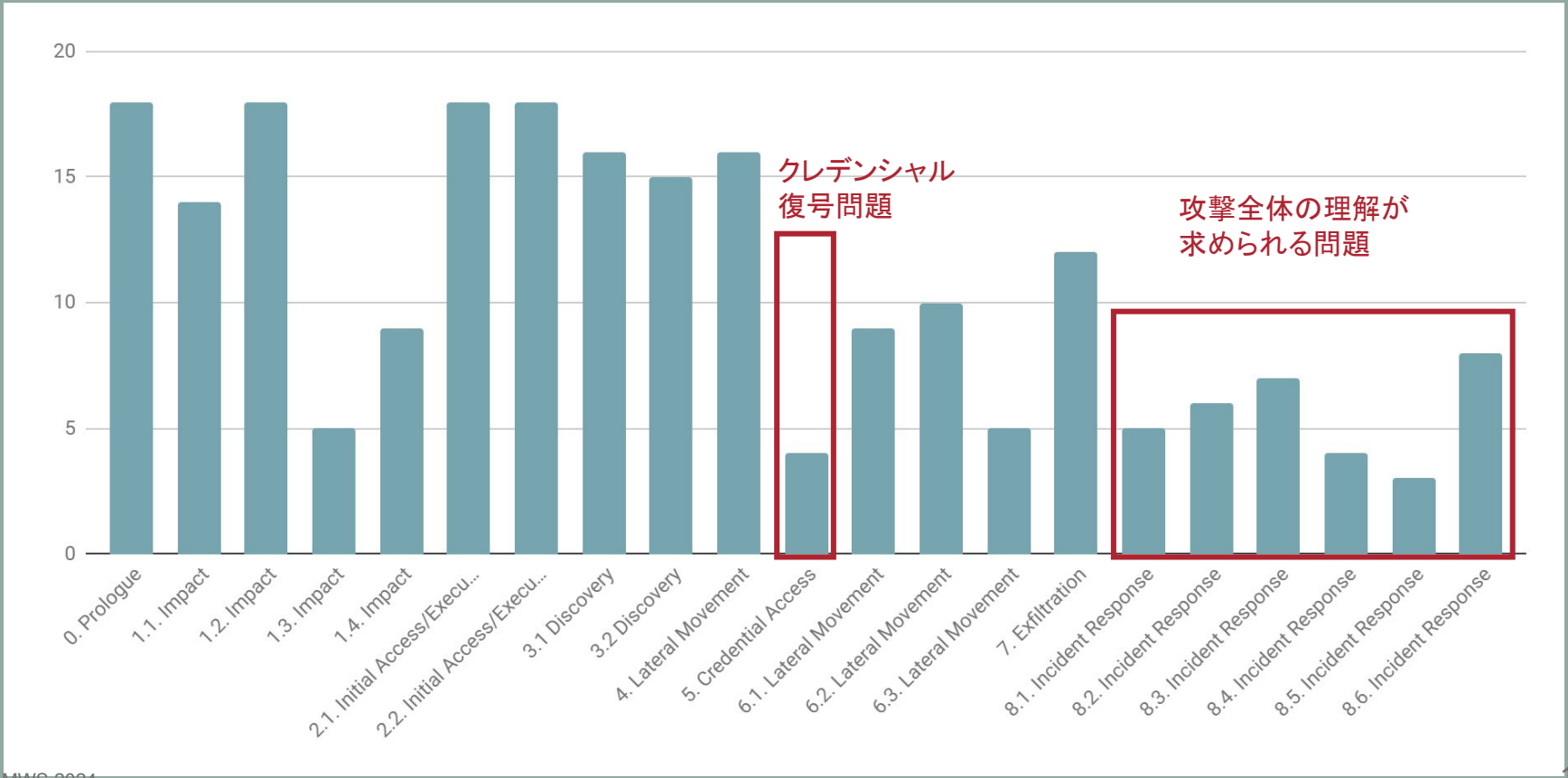

2024
得点
チーム
25
20
15
10
5
0
UN頼み
THE SKY
人海戦術_backdoor
SakanaCushion
Enduring Pug
44GK44Gk44GL44KMIQ==
人海戦術ハッカンソンズ
セキュリティ讃歌
卍脳筋鹿煎餅卍NEONEO...
BirdStone
F.SE
DSOL11G
Gunmataro
チームいちぴろ
Moo
人海戦術コードブルー
全無太郎
Gunmahanako
卍脳筋鹿煎餅卍NEONEO
8.6. Incident Response
8.5. Incident Response
8.4. Incident Response.
8.3. Incident Response
8.2. Incident Response
8.1. Incident Response
7. Exfiltration
6.3. Lateral Movement
6.2. Lateral Movement
6.1. Lateral Movement
5. Credential Access
4. Lateral Movement
3.2. Discovery
3.1. Discovery
2.2. Credential Access
2.1. Credential Access
1.4. Impact
1.3. Impact
1.2. Impact
1.1. impact
0. Prologue

チーム別

- 今年は問題8の出来で差がついた
- 平均点 （25点満点）
  - 2023: 17.2点
  - 2024: 12.7点

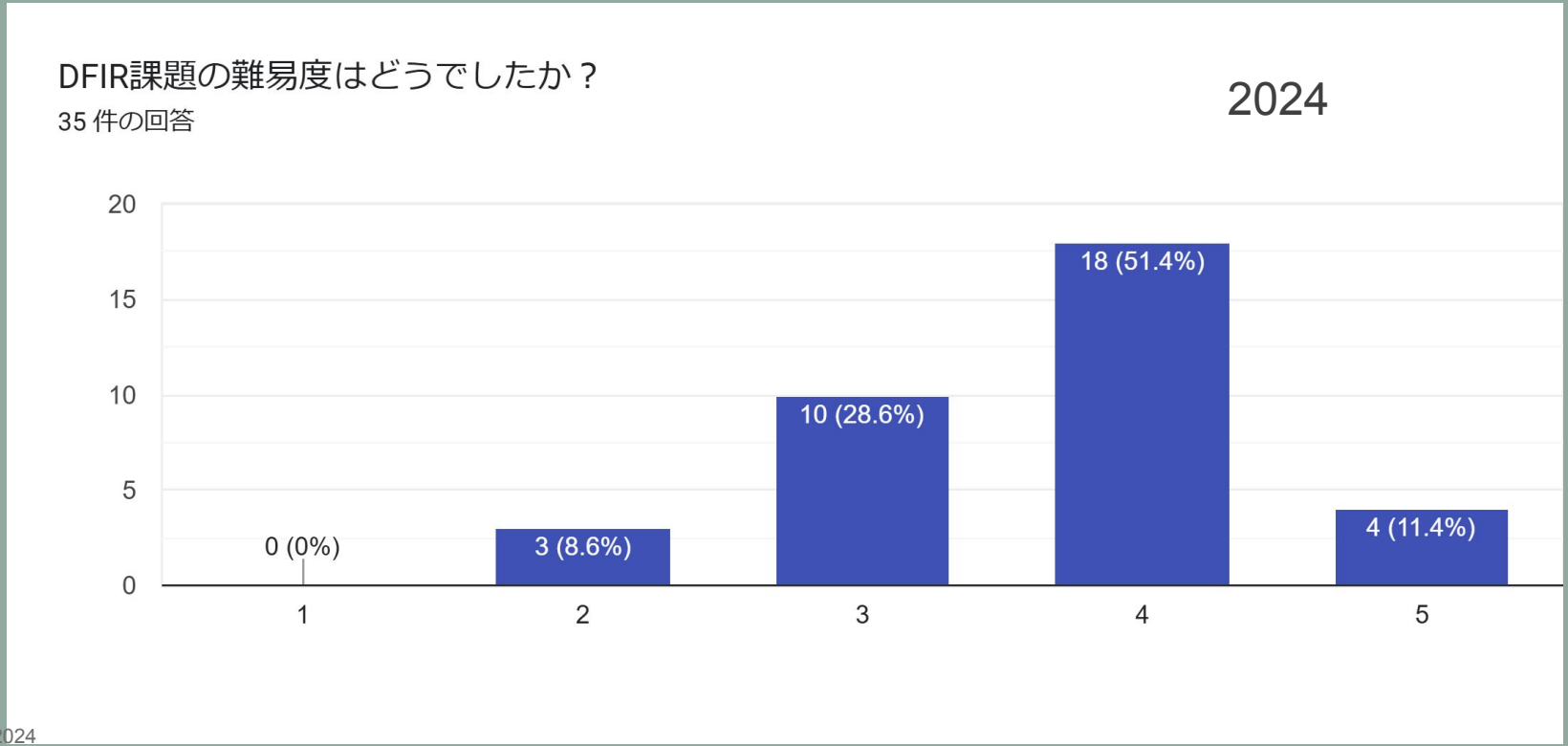


問題別

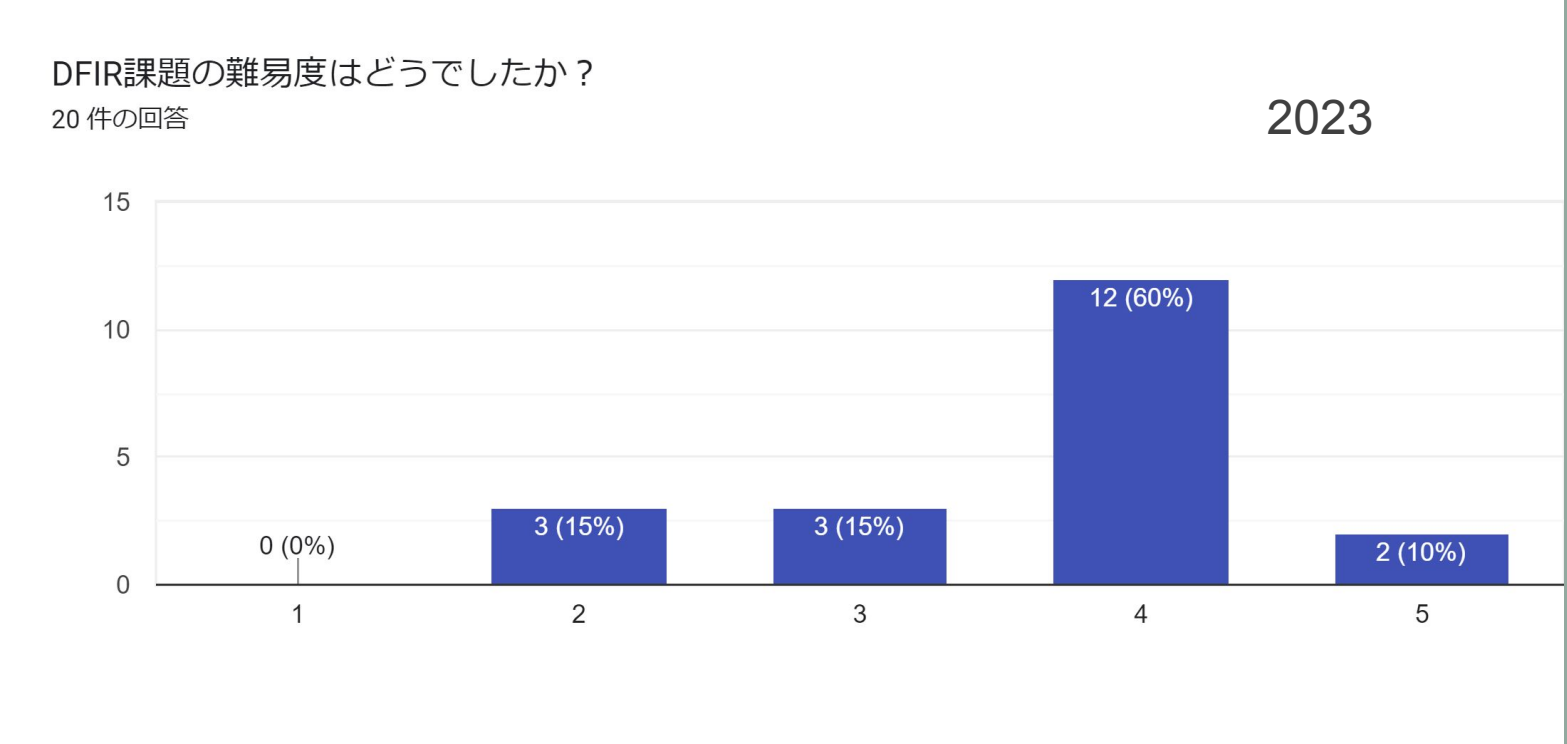

20
15
10
5
0
クレデンシャル
復号問題
攻撃全体の理解が
求められる問題
0. Prologue
1.1. Impact
1.2. Impact
1.3. Impact
1.4. Impact
2.1. Initial Access/Execu...
2.2. Initial Access/Execu...
3.1 Discovery
3.2 Discovery
4. Lateral Movement
5. Credential Access
6.1. Lateral Movement
6.2. Lateral Movement
6.3. Lateral Movement
7. Exfiltration
8.1. Incident Response
8.2. Incident Response
8.3. Incident Response
8.4. Incident Response
8.5. Incident Response
8.6. Incident Response

アンケート結果

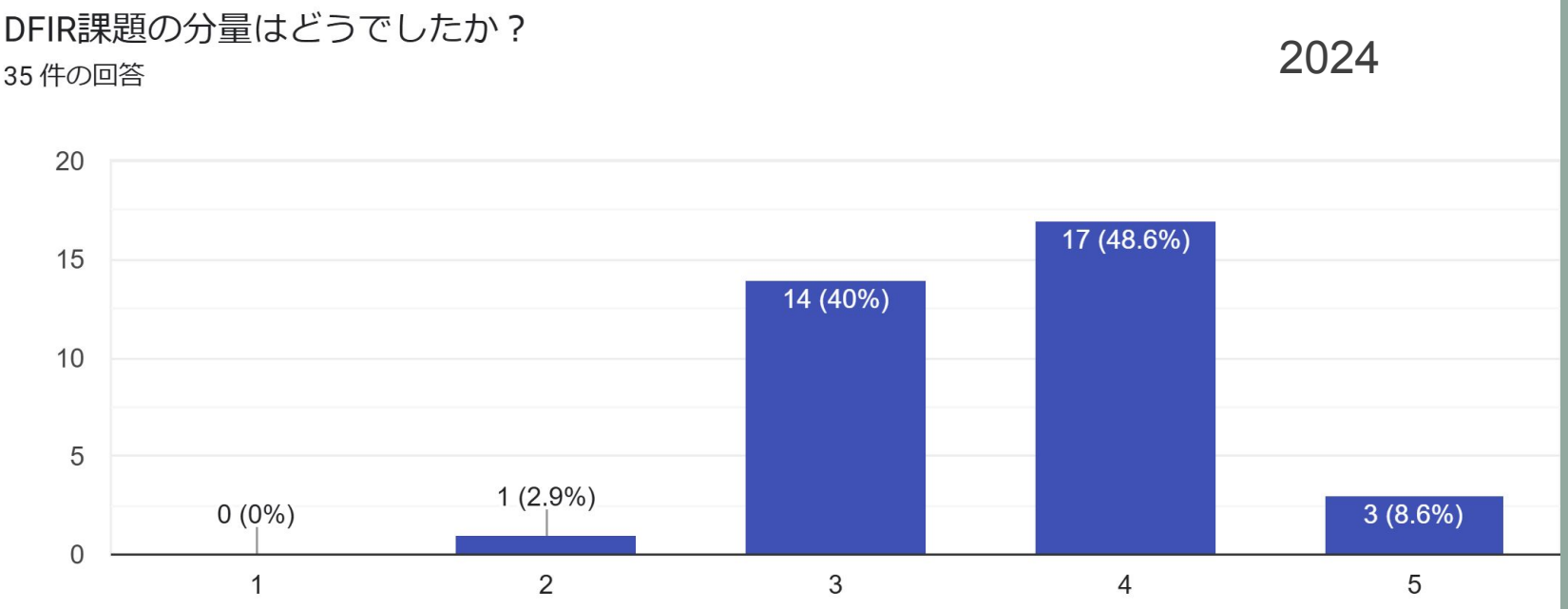
難易度


DFIR課題の難易度はどうでしたか？
35 件の回答
2024
20
15
10
5
0
0 (0%)
3 (8.6%)
10 (28.6%)
18 (51.4%)
4 (11.4%)
1
2
3
4
5

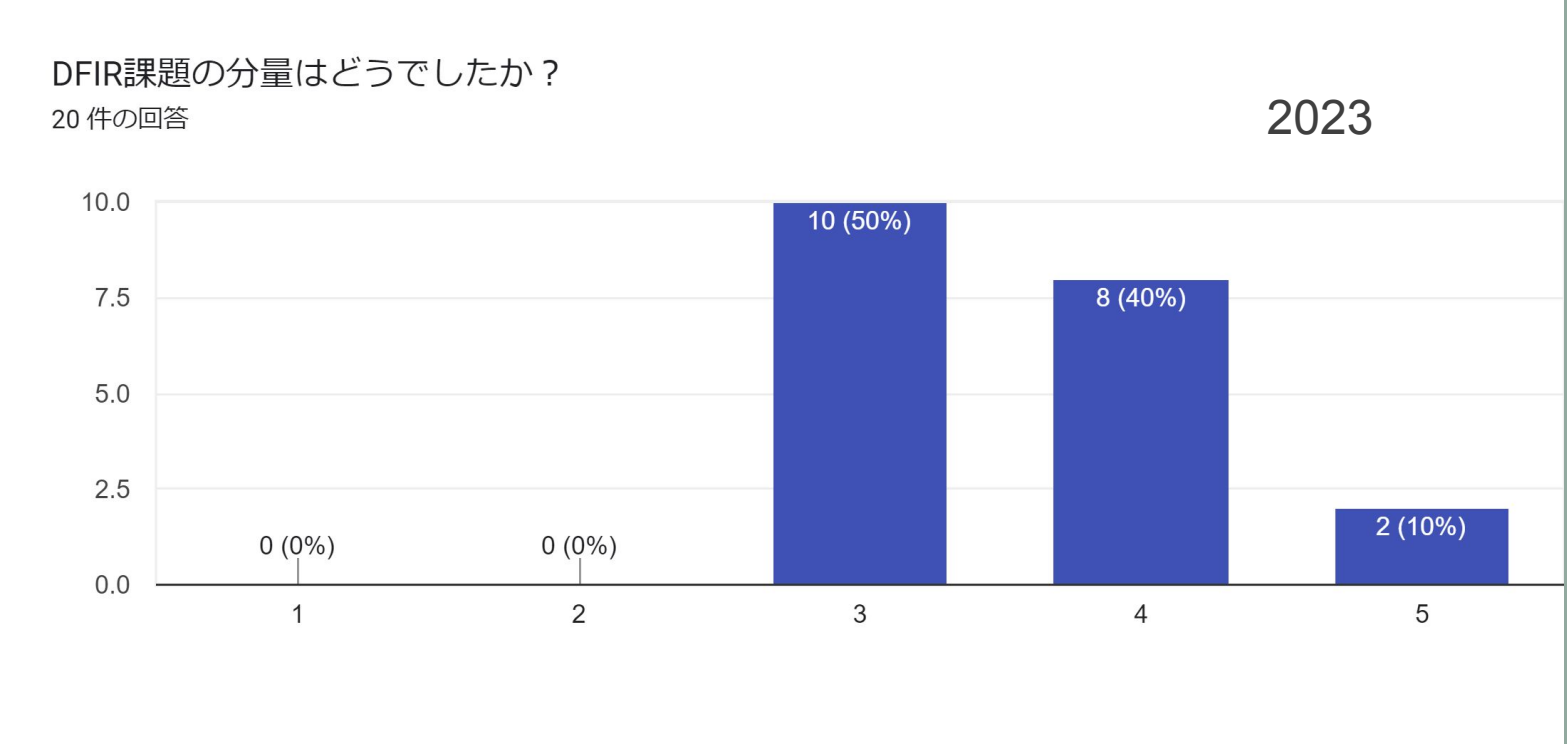
難易度 (去年)


DFIR課題の難易度はどうでしたか？
20 件の回答
2023
15
10
5
0
0 (0%)
3 (15%)
3 (15%)
12 (60%)
2 (10%)
1
2
3
4
5

分量

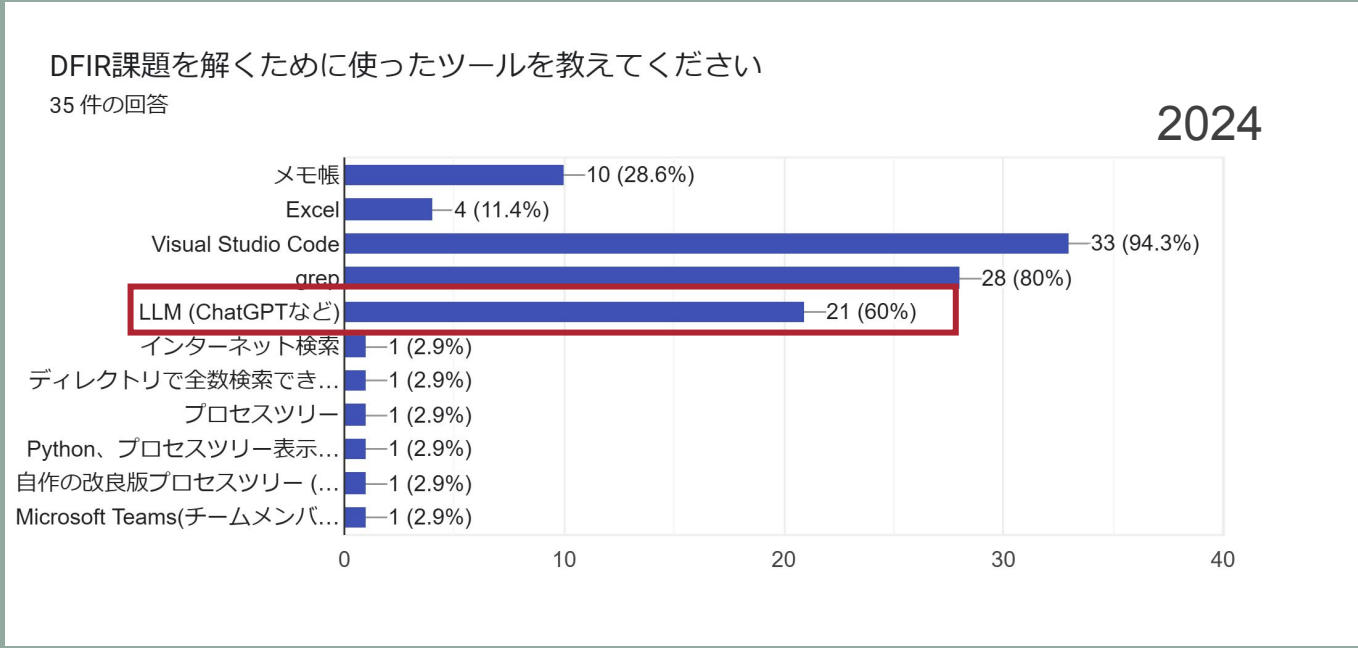

DFIR課題の分量はどうでしたか？
35 件の回答
2024
20
15
10
5
0
0 (0%)
1 (2.9%)
14 (40%)
17 (48.6%)
3 (8.6%)
1
2
3
4
5

分量 (去年)

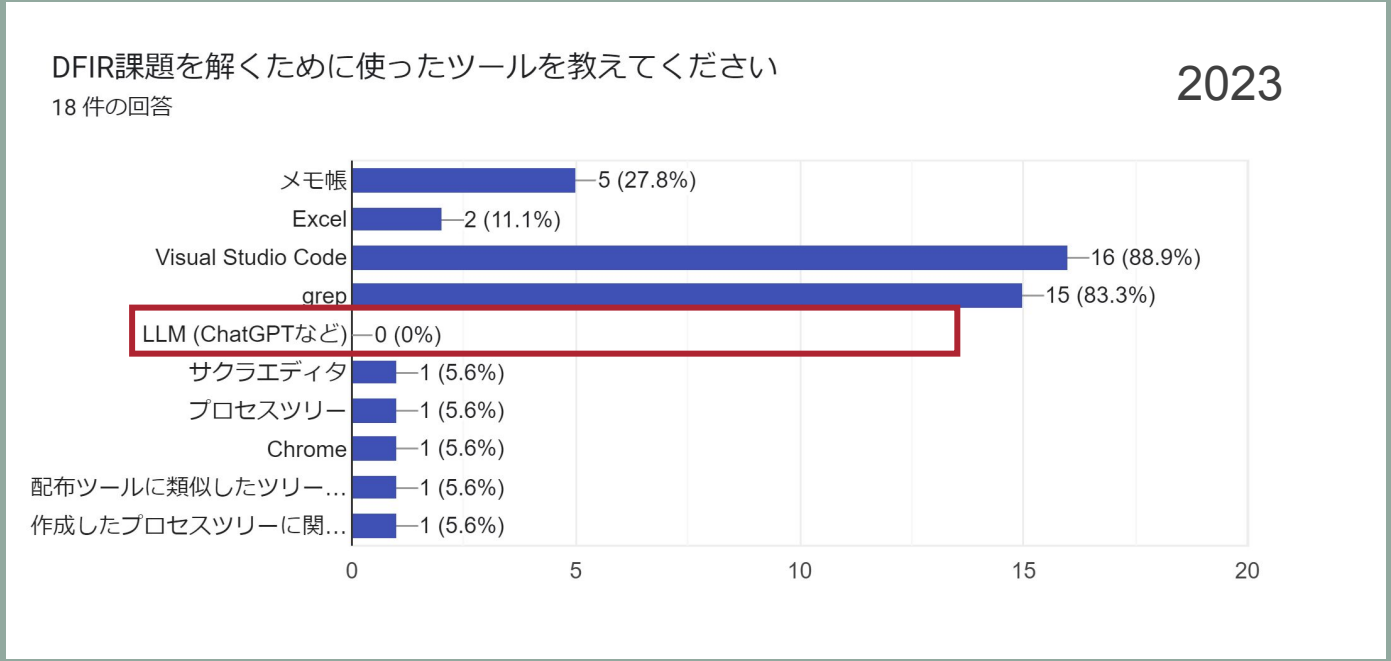

DFIR課題の分量はどうでしたか？
20 件の回答
2023
10.0
7.5
5.0
2.5
0.0
0 (0%)
0 (0%)
10 (50%)
8 (40%)
2 (10%)
1
2
3
4
5

使用したツール

LLMを利用している参加者が半分以上



使用したツール


DFIR課題を解くために使ったツールを教えてください
18 件の回答
2023
メモ帳
5 (27.8%)
Excel
2 (11.1%)
Visual Studio Code
16 (88.9%)
grep
15 (83.3%)
LLM (ChatGPTなど)
0 (0%)
サクラエディタ
1 (5.6%)
プロセスツリー
1 (5.6%)
Chrome
1 (5.6%)
配布ツールに類似したツリー…
1 (5.6%)
作成したプロセスツリーに関…
1 (5.6%)
0
5
10
15
20

事前学習

DFIR課題の環境情報を事前に提供しましたが、事前学習は行えましたか？

36 件の回答

扱ってほしい攻撃シナリオはありますか？（記述）

- 差分プライバシー、秘密計算などのプライバシー保護技術に関わる攻撃シナリオの問題
- Linuxサーバへの侵入
- 一部のログが削除されるような問題
- USB・BYOD経由でのマルウェア感染、今年度のような脆弱性を突いた攻撃

課題を解く上で、行き詰まった箇所 （記述）

- XML形式のCredentialファイルの暗号化されたパスワードの復号方法
- 暗号化されたパスワードについてログ上で探索を行ってしまった
  もう少し誘導がほしいと感じた
- パスワード解析
- 5. Credential Access
- 課題5
- クレデンシャルファイルの解析問題で、パスワードの解析方法の調査に時間が掛かった

5. Credential Access

ログを分析した結果、攻撃者はWS01に存在する次のパスのファイルを参照していることが分かった。

C:\Users\green\Documents\ViehmannCredential.rtsz

このファイルについてIT管理者から入手した。（zipファイル中の`ViehmannCredential.rtsz`）

このファイルを解析することで得られる認証情報のうち、ユーザ名とパスワードを答えよ。

- フォーマット：ユーザ名_パスワード (case sensitive)
- 回答例：Henderson_Elllllllleganunnnnnnnnnnyas!!!

5. Credential Access

ヒント：WS01にインストールされているソフトウェアの一覧は以下である

Python Launcher
aws-cfn-bootstrap
Microsoft Visual C++ 2019 X64 Minimum Runtime - 14.29.30139
Microsoft Visual C++ 2019 X64 Additional Runtime - 14.29.30139
Royal TS V7
AWS Tools for Windows
Mark II Updater
Mark II Recorder
AWS PV Drivers
Amazon SSM Agent

5. Credential Access

拡張子でググるとRoyal TSのファイルと分かる

5. Credential Access

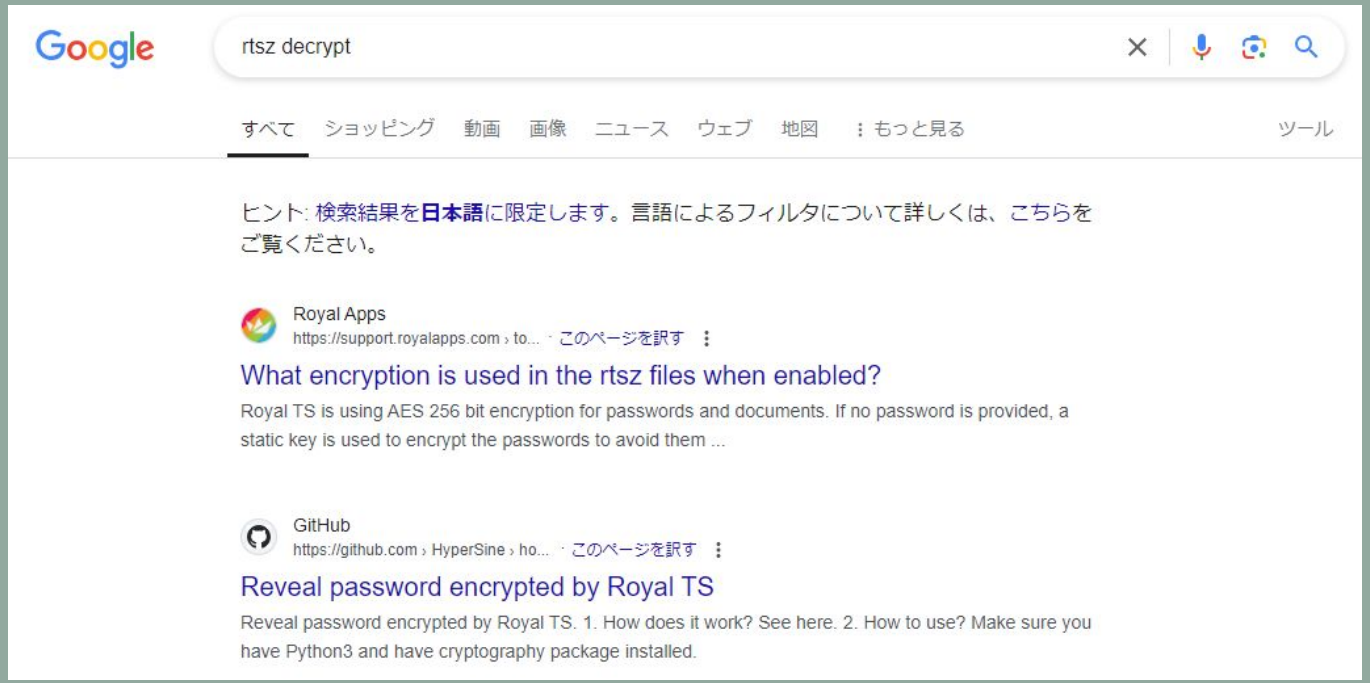
ファイルの中身を見ると、ユーザー名および暗号化されたパスワードや
接続先のサーバーの記載を見ることができる。

```
<CredentialPassword>H0Ru4w7zSQ5sXSnpcmDF8y77PMoHBBk2I/scYLkNA0MFtatAZAEMswdObRdR9j+4dd0KqwW/iwd
+XBDGt/8VDWxK4/k1tKQgtnsJp/LD4UM=</CredentialPassword>
<CredentialUsername>Viehmann</CredentialUsername>
```

```
<URI>DC01.eden-college.local</URI>
```

5. Credential Access

パスワードを復号する方法がないか調べる



5. Credential Access

Decryptツールが存在

AES鍵が固定なため、
復号できてしまう

Reveal password encrypted by Royal TS

1. How does it work?

See here.

2. How to use?

- Make sure you have Python3 and have `cryptography` package installed.

  You can install it via

```
$ pip3 install cryptography
```

```
Usage:
    RoyalTSCipher.py <enc|dec> [-p Password] <plaintext|ciphertext>
        <enc|dec>               `enc` for encryption, `dec` for decryption.
                                This parameter must be specified.

        [-p Password]           The password that Royal TS Document uses.
                                This parameter must be specified.

        <plaintext|ciphertext>  Plaintext string or ciphertext string.
                                This parameter must be specified.
```

https://github.com/HyperSine/how-does-RoyalTS-encrypt-password

5. Credential Access

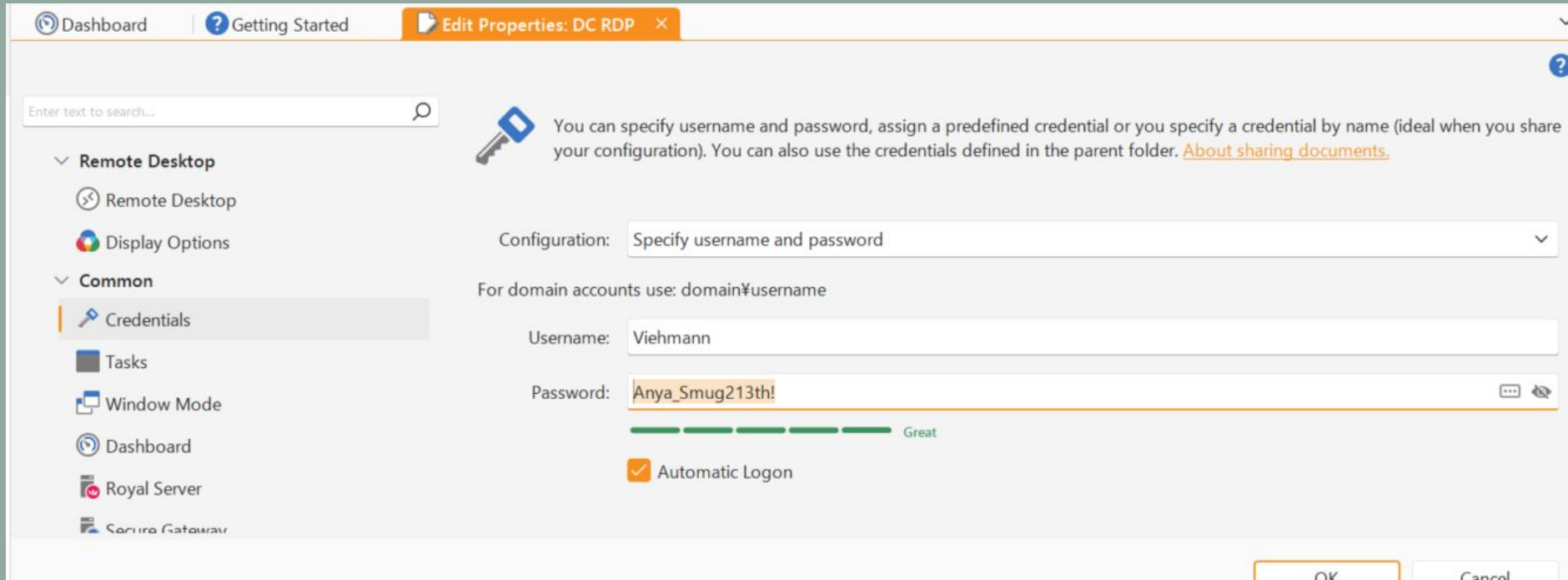
実行結果

```
┌──(user㉿kali)-[~/how-does-RoyalTS-encrypt-password/python3]
└─$ python RoyalTSCipher.py dec H0Ru4w7zSQ5sXSnpcmDF8y77PMoHBBk2I/scYLkNA0MFtatAZAEMswdObRdR9j+4dd0KqwW/iwd+XBDGt/8VDWxK4/k1tKQgtnsJp/LD4UM=
Anya_Smug213th!
```

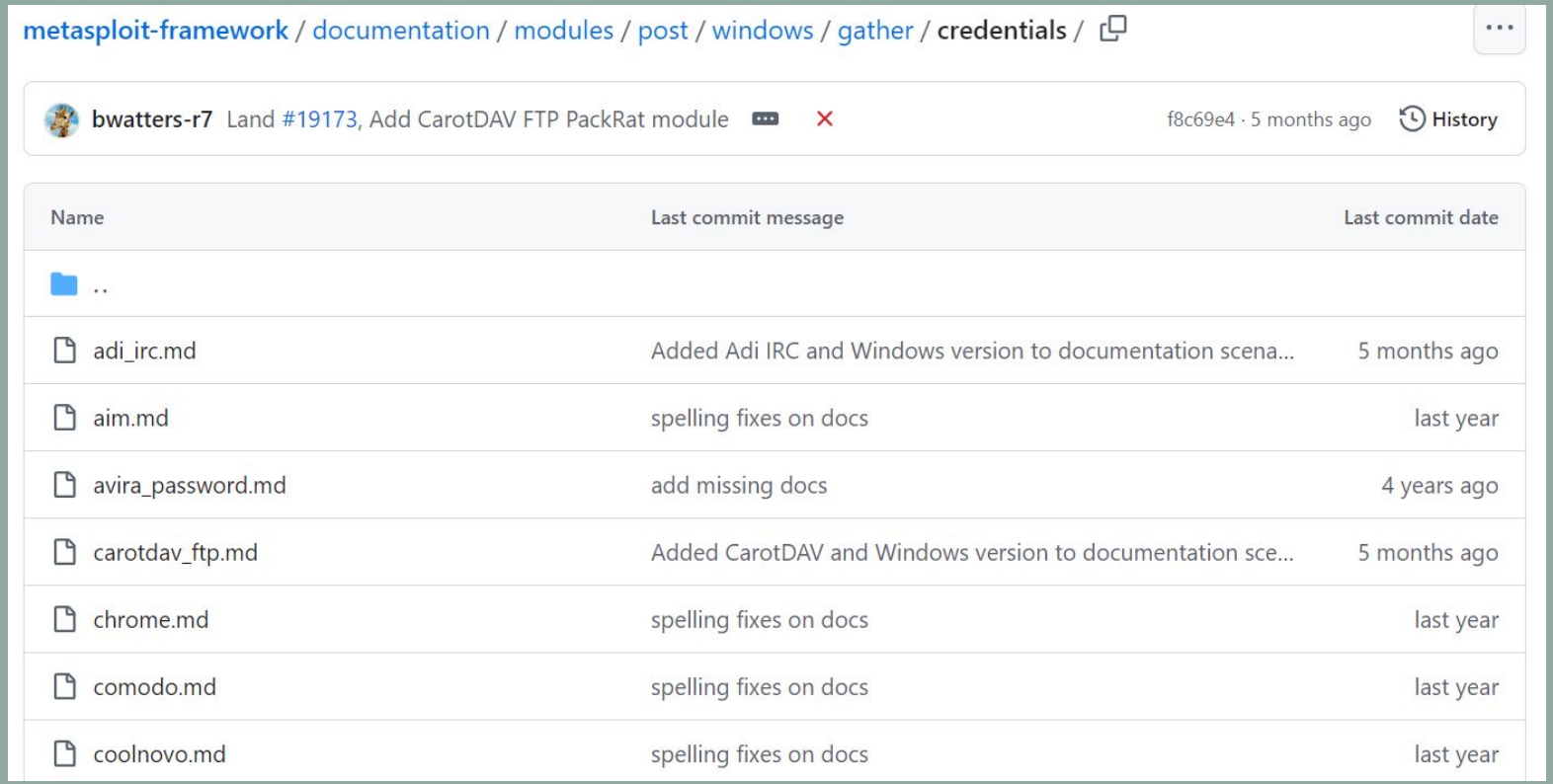
A. Viehmann_Anya_Smug213th!

5. Credential Access

別解：適当なマシンにRoyal TSをインストールする



端末内に保存されているクレデンシャル



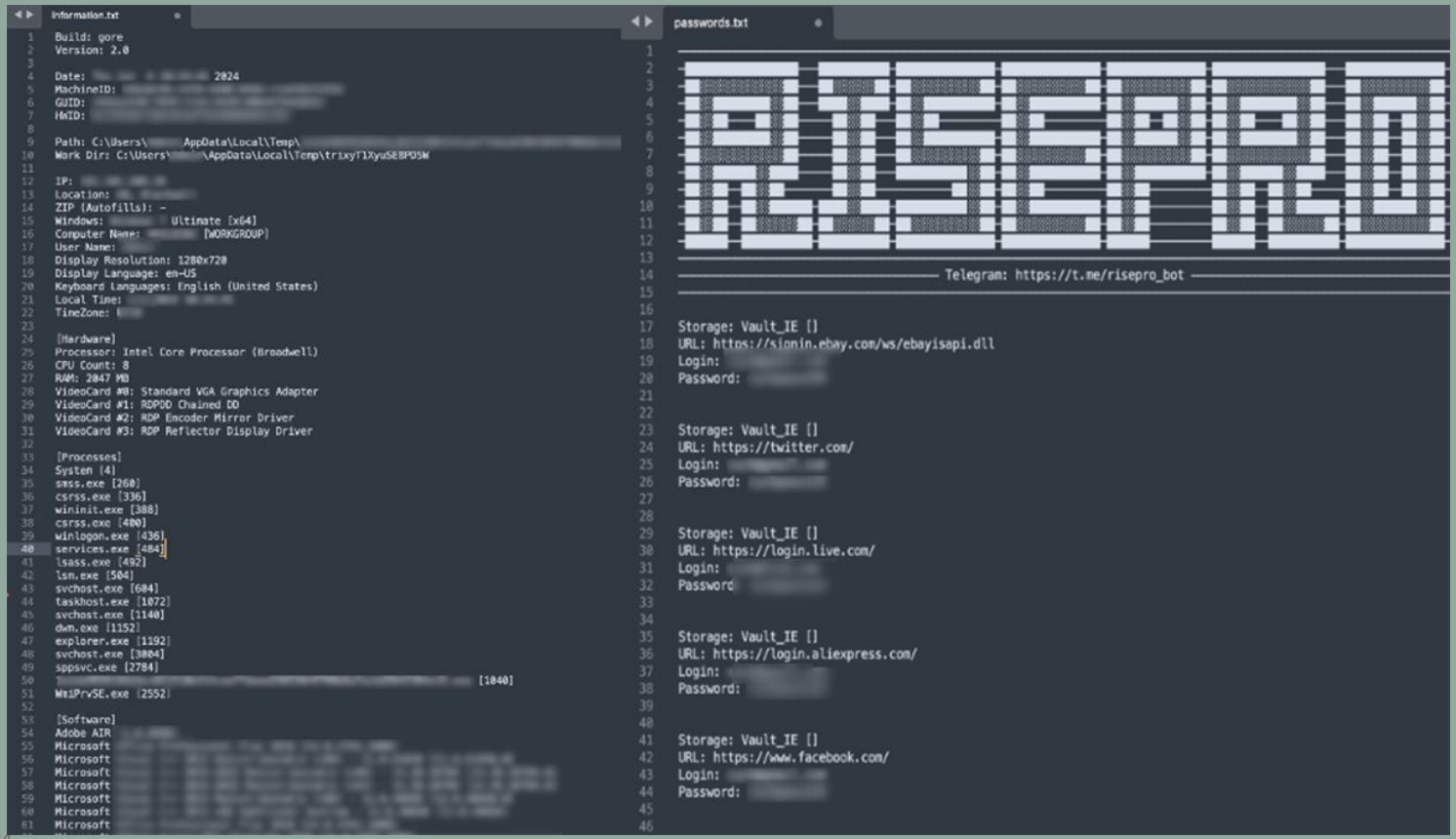
metasploit-framework / documentation / modules / post / windows / gather / credentials /

bwatters-r7 Land #19173, Add CarotDAV FTP PackRat module — f8c69e4 · 5 months ago — History

Name	Last commit message	Last commit date
..		
adi_irc.md	Added Adi IRC and Windows version to documentation scena...	5 months ago
aim.md	spelling fixes on docs	last year
avira_password.md	add missing docs	4 years ago
carotdav_ftp.md	Added CarotDAV and Windows version to documentation sce...	5 months ago
chrome.md	spelling fixes on docs	last year
comodo.md	spelling fixes on docs	last year
coolnovo.md	spelling fixes on docs	last year

https://github.com/rapid7/metasploit-framework/tree/master/documentation/modules/post/windows/gather/credentials

マルウェアによるクレデンシャル取得の例



information.txt

```
Build: gore
Version: 2.0

Date:  2024
MachineID:
GUID:
HWID:

Path: C:\Users\      AppData\Local\Temp\
Work Dir: C:\Users\      \AppData\Local\Temp\trixyT1XyuSEBPOSW

IP:
Location:
ZIP (Autofills): -
Windows:        Ultimate [x64]
Computer Name:        [WORKGROUP]
User Name:
Display Resolution: 1280x720
Display Language: en-US
Keyboard Languages: English (United States)
Local Time:
TimeZone:

[Hardware]
Processor: Intel Core Processor (Broadwell)
CPU Count: 8
RAM: 2047 MB
VideoCard #0: Standard VGA Graphics Adapter
VideoCard #1: RDPDD Chained DD
VideoCard #2: RDP Encoder Mirror Driver
VideoCard #3: RDP Reflector Display Driver

[Processes]
System [4]
smss.exe [260]
csrss.exe [336]
wininit.exe [388]
csrss.exe [400]
winlogon.exe [436]
services.exe [484]
lsass.exe [492]
lsm.exe [504]
svchost.exe [604]
taskhost.exe [1072]
svchost.exe [1140]
dwm.exe [1152]
explorer.exe [1192]
svchost.exe [3004]
sppsvc.exe [2784]
                                                    [1840]
WmiPrvSE.exe [2552]

[Software]
Adobe AIR
Microsoft
Microsoft
Microsoft
Microsoft
Microsoft
Microsoft
Microsoft
```

passwords.txt

```
Telegram: https://t.me/risepro_bot

Storage: Vault_IE []
URL: https://signin.ebay.com/ws/ebayisapi.dll
Login:
Password:


Storage: Vault_IE []
URL: https://twitter.com/
Login:
Password:


Storage: Vault_IE []
URL: https://login.live.com/
Login:
Password


Storage: Vault_IE []
URL: https://login.aliexpress.com/
Login:
Password:


Storage: Vault_IE []
URL: https://www.facebook.com/
Login:
Password:
```

https://blogs.blackberry.com/en/2024/06/threat-analysis-insight-risepro-information-stealer

課題を解く上で、行き詰まった箇所 （記述）

- 普段の開発環境は Linux 中心だったので Powershell のコマンドに慣れていなかった
- Windowsの仕様を知らないとなかなか分かりにくかった
- 攻撃者が残したわけではないログと攻撃者が残したログの切り分けが難しかった

DFIR課題に関して良かった点（記述）

- 問題を解いていくことで1つのシナリオに沿ったログの調査から対策までの一連のプロセスを経験できる点が面白く有用でした
- 私にはまだ難易度が高く中々解くことはできなかったが，順に解くことでどんどん情報が分かっていく上に，様々なログを見ないと解けないようになっているとても質のいい問題であった点がよかった．また，解説がとても分かりやすかった．
- 昨年度と比べてクレデンシャルファイルの解析など、ログ分析以外のフォレンジック技術についても問われる問題が出題され非常に面白かった

DFIR課題に関して悪かった点（記述）

- 回数制限のある問題が多い／回数制限が少ないことより、回答が真に正しいか確認するために時間を要し、幅広い問題を解くための十分な時間がなかった
- 複数の解釈ができる問題や選択肢があり戸惑った.
- 日本語を入力する際、変換後エンターを押すと変換確定後submitされてしまうことがあったので、英数字以外の入力は避けて欲しかった
- FLAG/選択形式の問題なのか、記述形式なのか問題を開かないと分からないようになっていたため、記述式の問題のタイトルに【記述式】と書いたりしてほしい

競技、アンケート結果に対する考察・今後に向けて

競技、アンケート結果に対する考察・今後に向けて

- 解釈の揺らぎで回答不能になる問題の撲滅
- LLM課金ゲー化の回避
- 攻撃の裏での正規ユーザーの操作について、来年以降も継続
  - 実際のIRでも、攻撃者のログと正規ユーザーのログが混じっている
- 攻撃者視点の問題
- Linuxマシンのログも出題？

まとめ

- 今日話したこと
  - 今年のDFIR課題 振り返り
  - 競技結果
  - アンケート結果の共有

- 作問にご協力いただける方がいれば、ご連絡お待ちしております
  - 自分の経験を下の世代に還元したい方
  - リアルなフォレンジック業務や攻撃手法に精通している方
  - 様々な攻撃ツールを検証してみたい方

- ご意見・ご質問は Slack-MWSの #mwscup までお気軽にどうぞ！

Thank you!!