SecHack365

(σ▬>▽<)σ[ENJOY HACKING]

sisakuterm しさくたーむ

PASS OFF | TARGET IP | SOURCE IP

LOG OFF

High

Kali@Kali : ~ $

～最高の相棒となるターミナルを！～

思索駆動コース 36C 山口翔大

憧れのペンテスターになったけど...

常に事務作業&訴訟リスクと隣り合わせ！

ドラマや映画からもかっこいいイメージしかないハッカーですが、仕事で行う場合は常に事務作業と訴訟リスクが隣り合わせです！ただでさえ難しい領域なのに事務作業が多く、訴訟リスクも大きいと誰も手を出そうと思いません。。

課題点の洗い出し

1. 報告書作成が大変
   対象の多さ/期間の長さに応じて作業量増
2. コマンドの実行ミス
   重大インシデント発生による訴訟リスク
3. 大量の出力精査
   出力の見落としによる訴訟リスク&出力を抽出し報告書へ記入する事務作業

1 報告書作成が大変

報告書の作成はかなり大変です。ペネトレでは、作業員が行った全てをログに残す必要があり、対象が多く期間が長いようなときは、膨大な量のログが作られます。報告書作成時はそのログから重要な部分のみを抽出する必要があり、ペネトレと同じぐらい工数がかかる場合もあります。

2 コマンド実行ミス

複雑なオプションを複数持っているコマンドでは、一つのオプションを変更するだけで動作が大きく変わることがあります。そのようなコマンドの動作を作業員が間違って理解しているとき、コマンドの実行ミスが発生し重大インシデントを引き起こす可能性があります。

3 大量の出力精査

コマンドによっては大量の出力が見られることもあり、そのような出力を精査するには時間がかかりすぎてしまいます。時間がかかりすぎると、決められた期間内にテストが行える範囲が狭まり、網羅的なテストを行うことができません。また、量が多いことで、重要な部分を見落とす可能性も。

sisakuterm

1. ログモードの実装

ログモードを実装！報告書で使用するような重要なログはログモードをONにすることで、自動的にもう一つのログファイル(.md)にタイトル付きで保存されます。ログモードがOFFであっても、すべての作業を記録するログファイルには出力が記録されていくので、ログモードをONにし忘れた時も安心です。モードの切り替えは「LOG OFF」/「LOG ON」のボタンを押すだけです。簡単に切り替えが行えるので、テストにかける時間を消費することはありません。

実際にできるログファイルは下の通りです。ログモードでは追加機能としてコマンドの重要な出力部分のみを抽出し記録します。（例 nmapではポート部分のみ）これにより報告書作成者が本当に必要としているログファイルを作成できます。また、ログファイルはマークダウン形式なのでプレビュー可能です。

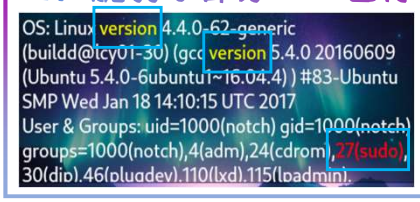
```
### Executed command: sudo nmap -v -sV 10.10.11.224
```
```
22/tcp    open      ssh      OpenSSH 8.2p1 Ubuntu 4ubu
80/tcp    filtered  http
55555/tcp open      unknown
```

2. 危険度表示機能

コマンドの実行ミスへのアプローチとして、危険度表示機能を実装しました。危険度を表示させることで、作業員がコマンドの動作を勘違いしていることに気付く可能性を高めることができます！危険度には、None,Low, Medium, High の4種類を用意しており、Highになるにつれ危険度が高いことを示します。

上の画像では、crackmapexec というコマンドを使用し総当たり攻撃を行おうとしているため、危険度は一番高いHighになっています。画像ではわかりませんが、Highになると、枠が点滅し、ユーザに気付きてもらいやすい工夫をしています。また、危険度表示機能はテスト時だけでなく、学習時にも使うことができます。ペネトレの学習では攻撃手法を学ぶことに注力し、システムへの影響を後回しにすることが多いです。しかし、sisakutermを使用して勉強するだけで、コマンドの危険度も同時に学ぶことが可能です。

3. 脆弱な部分への色付け



大量の出力の精査へのアプローチとしては、色付けを実装しました。脆弱な部分には赤色を、情報を示すような部分には黄色を付けることで精査にかける時間を短縮できます。ターミナルで実装しているのでいつでも色付けされた出力を確認可能です

4. パスワードモードの実装

パスワードモード自体は課題点へのアプローチではないですが普段ターミナルを使用していてパスワード入力時に入力が見えないことに少し使いずらさを感じていたので、今回パスワードモードを実装しマスク化された状態で入力が見えるようにしました。またパスワードモードで実施するとログへの保存もマスク化された状態で行われるので、よりセキュアなログファイルを作成することができるため、安全性の向上にも繋がります。

使う人それぞれの相棒へ！

上記の機能は全て定義ファイルを書き換えるだけで変更することができます！なので、ペネトレを行わない人でも使うことができます！例えば、運用の方であれば運用上実行してはいけないコマンドの危険度をHighにしたり、危険なエラーメッセージの色を赤色にすることも可能です。私だけでなく、sisakutermを使う全ての人の相棒となることができるようにカスタマイズ性を高めました。

今後の展望

今後の展望としては、GUIによるカスタマイズ機能の追加、対応正規表現コマンドの増加、ログファイルのWordへの対応を目指しています。さらに使いやすいターミナルへとアップグレードさせ、より多くの人の相棒として活躍してほしいです。

NICT

思索のトレーナー、アシスタント、トレーニーをはじめ、SecHack365で関わってくださった全ての方に感謝します。ありがとうございました！SecHack365を通して技術力だけでなく、様々なつながりもでき、間違い無く今後の活動に活かすことが出来ると思います。とても楽しい1年間でした。

HackTheBox X:shoo Qiita