Aトラック 選考問題（１）

【 質問１】共通

あなたがミニキャンプに応募された動機について教えてください。また、この講義で学んだことを何に役立てたいかを教えてください。

【 質問２】

OWASP Top Tenの「A04:2021 - 安全が確認されない不安な設計」を読み、自分の興味のある一つ以上のCWEについて現実的に発生しうる実装と、その対策をできる限り自分なりの言葉で説明してください。難しい場合は、リンク等を例示しどのような観点で答えようとしていたかを教えてください。

Aトラック 選考問題（２）

【 質問３】

Unix / Linux系列のサーバー上で動作するアプリケーションにおいて、攻撃者が環境変数へアクセスしたい場合、どのような脆弱性を用いることでアクセスすることができるか、前提と攻撃手法を踏まえながが具体的に説明してください。また、可能な場合どのような対策をすべきかも添えてください。

【 質問４】

既存のサイドチャネル攻撃を調べ（spectre や Meltdown など）、わかったことをできる範囲で教えてください。解答には以下を含めてください。　1．攻撃者の目的　2．攻撃の手順とその原理　　3．考えられる対策方法　　4．そのほか分かったこと

Bトラック 選考問題

【 質問１】共通

あなたがミニキャンプに応募された動機について教えてください。また、この講義で学んだことを何に役立てたいかを教えてください。

【 質問２】

自分のPC上に残るプログラムの実行痕跡(過去にどのようなプログラムがどのように実行されたかを示すもの)に関わる情報を探し、何処にどのような情報が存在していたかレポートしなさい。

【 質問２の補足】

・実際に実行されていた具体的なプログラム名は個人的なものなので無理に書かなくても良いです。

・どのような情報(ファイル名があった、実行時間があった等)がどこにあったかさえ記載すれば、そこに格納されていた全てのレコードについて記載しなくても良いです。例えば、ある場所に1024個(レコード)の実行痕跡があった場合、その全レコードについて詳細にレポートせずに、そこにあるレコード達がどのような情報を持っているか記載すれば良いです。

・それが実行痕跡だと思った根拠(質問３と絡めても良いです)、どのように調査したかなども記載しなさい。

・OSはできればWindowsが良いですが、持っていなければMacやLinuxでも良いです。

・探す手段は問いません

Bトラック 選考問題（２）

【 質問３】

質問２で自分が見つけた実行痕跡について、それが本当に自分またはシステムが実行したプログラム実行に関する情報かどうか、自分で検証する方法を考え検証し、その方法と結果をレポートしなさい。

Cトラック 選考問題

【 質問１】共通

あなたがミニキャンプに応募された動機について教えてください。また、この講義で学んだことを何に役立てたいかを教えてください。

【 質問２】

マルウェア解析の手法の1つに、実際にマルウェアを動かす手法があります。この手法を行う場合に、どのようなことに注意が必要だと思いますか？ 理由とともに挙げてください。また、対策方法があれば、そちらも挙げてください。

【 質問３】

あなたはある企業の情報システム部に所属しています。社員Aから、「メールの添付ファイルを実行したところデスクトップの壁紙が変更された。壁紙には金銭を要求する文章が書かれている。」と連絡を受けました。 １．どのような種類のマルウェアに感染したことが疑われますか？ ２．社員Aにどのような処置を指示しますか？ ３．このような攻撃の被害を軽減するにはどのような対策が有効ですか？

Dトラック 選考問題

【 質問１】共通

あなたがミニキャンプに応募された動機について教えてください。また、この講義で学んだことを何に役立てたいかを教えてください。