1. 攻撃者が Quickfile.inc 環境に最初の足掛かりを得た後、権限昇格に使用したオブジェクト、ツール、またはファイルの名前は何ですか?
linpeas
解答　0d9b448b1e29d0acb01b8947730582b9

2. 攻撃者がデータの流出を準備するために使用するスクリプト、アプリケーション、またはコマンドレットの名前は何ですか?
compress-archive
解答　11eb6c71388f19ec3f49c87f378903b1

3. 攻撃者は、権限昇格や横展開といった特定のアクションの後に、様々な永続化メカニズムを利用することで知られています。Quickfile Inc 環境で利用されている永続化メカニズムとして使用されるオブジェクトの名前は何ですか？オブジェクトとは、ファイル名、レジストリキー、ユーザー名、スケジュールされたタスク名などです。（形式：パス、ドメイン名、コンピュータ名、デバイス文字などのプレフィックスやサフィックスを含まない ObjectName）
bits.exe
解答　c5cd05984c5f81d73cd511946734abe3

4. 攻撃者が Quickfile.inc 環境外に持ち出したファイルの名前は何ですか?
horilla.zip
解答　24114fb0ff823b1509aa1a48b76c5aa5

5. 攻撃者がQuickfile.inc環境に最初にアクセスしたファイルまたは実行可能ペイロードは、いつ最初に実行されましたか？タイムスタンプを入力してください。
6/23/25 10:07:11.000 AM
解答　abce74bc703db883a1ca103c0cc60ef2

6. 攻撃者が Active Directory 環境での永続性を実現するために使用するスクリプト、アプリケーション、またはコマンドレットの SHA-256 ハッシュは何ですか?
SharPersist.exe
E9711F47CF9171F79BF34B342279F6FD9275C8AE65F3EB2C6EBB0B8432EA14F8
解答　9781a33bf73d9d78c8370d59de5436ad

7. 攻撃者は1台以上の外部マシンを悪意のある目的で使用しました。攻撃者が使用したホスト名、DNS名、またはIPアドレスは何ですか？
192.168.12.60
解答　c279533ccca5e32fe88d287e1f6c1fee