情報セキュリティマネジメント試験対策動画。今回のテーマはポートスキャナです。

このテーマを取り上げた理由としては、当チャンネルのコミュニティで実施しております、情報セキュリティマネジメント試験一問一答にて正答率が70パーセントを割っていたため作成いたしました。

ポートスキャナ。。

ネットワークに接続されているコンピューターやルータのポートを特定するためのソフトウェアのことです。ポートスキャナを利用し、特定のデータを送信してその応答状況を調べることで、ポートの稼働状況や開いているポート、サービスの種類などを把握することをポートスキャンといいます。一方、攻撃者がサイバー攻撃の前段階としてポートスキャンを行うこともあります。攻撃者は、ポートスキャンで得られた情報をもとに、侵入経路を調査したり、脆弱なアクセスポイントを探したりする。ポートスキャンによって得られた情報が悪用されると、情報漏洩やマルウェア感染、データ破壊などの被害が発生する可能性があります。

ポートスキャンへの対策は以下の通りです。。

１．ファイアウォールやIDS、IPS、わふなどのツールを導入する。。

２．不要なポートを閉じる。。

３．OSやソフトウェアを常に最新の状態に保つなどです

それでは早速かこもん研究に移ります。

科目A、B、サンプル問題。。

とい30。Webサーバの検査におけるポートスキャナの利用目的はどれか？。。

ア．Webサーバで稼働しているサービスを列挙して、不要なサービスが稼働していないことを確認する。。

イ．Webサーバの利用者IDの管理状況を運用者に確認して、情報セキュリティポリシから逸脱がないことを調べる。。

ウ．Webサーバへのアクセスの履歴を解析して、不正利用を検出する。。

エ．正規の利用者IDでログインし、Webサーバのコンテンツを直接確認して、コンテンツの脆弱性を検出する。

せいかいわ。ア．Webサーバで稼働しているサービスを列挙して、不要なサービスが稼働していないことを確認するです。。簡単でしたよね？。。

分からなかった人は、この動画を始めから見返してみてください。

平成29年度。春季。午前。

とい30。この問題をよく見てみましょう。

先ほどの科目A、B、サンプル問題、とい30と全く同じです。。

ということで解説は省かせていただきます。

平成28年度。秋季。午前。

とい29。攻撃者がシステムに進入するときにポートスキャンを行う目的はどれか？。。

あ。事前調査の段階で、攻撃できそうなサービスがあるかどうかを調査する。。

イ．権限取得の段階で、権限を奪取できそうなアカウントがあるかどうかを調査する。。

ウ．不正実行の段階で、攻撃者によって有益な利用者情報があるかどうかを調査する。。

エ．後処理の段階で、システムログに攻撃の痕跡が残っていないかどうかを調査する。

せいかいわ。あ。事前調査の段階で、攻撃できそうなサービスがあるかどうかを調査するです。。。事前調査段階というところと攻撃できそうなサービスというところがポイントですね。

れいわがんねんど。秋季。午前。

とい21。情報セキュリティにおいてバックドアに該当するものはどれか？。。

ア．アクセスするさいにパスワード認証などの正規の手続きが必要なWebサイトに、当該手続きをへないでアクセス可能なURL。。

イ．インターネットに公開されているサーバのTCPポートの中からアクティブになっているポートを探して、稼働中のサービスを特定するためのツール。。

ウ．ネットワーク上の通信パケットを取得して通信内容を見るために設けられたスイッチのランポート。。

エ．プログラムが確保するメモリ領域に、領域の大きさを超える長さの文字列を入力してあふれさせ、ダウンさせる攻撃

せいかいわ。ア．アクセスするさいにパスワード認証などの正規の手続きが必要なWebサイトに、当該手続きをへないでアクセス可能なURLです。。。

この問題は、選択肢の中にポートスキャナがあるものとなります。。。

いわ、ポートスキャナのことなので非該当です。。

うわ、ミラーポートのことなので非該当です。。

えわ、バッファオーバーフロー攻撃のことなので非該当です。