ITパスポート試験対策動画。今回のテーマはわふです。

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、ITパスポー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。

わふ。ウェブアプリケーションファイアーウォール。。

わふと読みます。Webアプリケーションの脆弱性を狙うサイバー攻撃からWebサイトを保護するセキュリティ対策のことです。Webサーバの前に設置して通信を解析、検査し、攻撃と判断した通信を遮断します。従来のファイアウォールやIPS、不正侵入防御とは異なり、アプリケーションレベルで通信を制御するセキュリティ対策です。このイラストのイメージで覚えてください。

ホワイトリスト方式とブラックリスト方式の違いについて解説いたします。。

ホワイトリスト方式は、あらかじめ定義された正当パターンに該当する通信を許可する方式のことです。害のない安全な通信パターンを定義し、他の通信はすべてブロックします。

ブラックリスト方式は、あらかじめ定義された不正パターンに該当する通信を検知、防御する方式のことです。シグネチャと呼ばれる定義された不正パターンのリストと通信を照合し、一致した通信をブロックします。

フォールスポジティブとフォールスネガティブについて解説いたします。。

フォールスポジティブは、正常なものを不正なものと間違って判断することです。いわゆる誤検知のことです。

フォールスネガティブは、不正なものを正常なものとみなして通過させてしまうことです。いわゆる見逃しのことです。

下のイラストのイメージで覚えましょう。

ファイアウォールとIPS、IDS、わふの違いをもう少し詳しく解説いたします。

先ほどご説明した通り、Webアプリケーションの脆弱性を利用した攻撃を防ぐのがワフです。ワフで防御できる攻撃は、SQLインジェクション、クロスサイトスクリプティング、OSコマンドインジェクションなどがあげられます。。

サーバやOSなどへの不正アクセスによる攻撃を防ぐのが、IPSやIDSになります。IPSやIDSで防御できる攻撃は、ディードス攻撃やどす攻撃などがあげられます。。

ネットワークを利用した攻撃を防ぐのがファイアウォールです。ファイアウォールで防御できる攻撃は、ポートスキャンなどが上げられます。

このようなイラストのイメージで脳に叩き込んでください。

また、わふには導入形態がみっつ存在しています。。

ひとつめわアプライアンス型です。これはネットワーク上にわふの専用機器を設置する方法です。。

メリットは、カスタマイズが柔軟にできるという点です。。

デメリットは、導入コストが高く、運用に高い技術が求められるという点です。。

ふたつめわホスト型です。これはウェブサーバにわふをインストールする方法です。。

メリットは、導入コストが低い点です。。

デメリットは、攻撃遮断時のサーバの負荷が高いてんと、わふをサーバごとに構築する必要があるというてんです。。

みっつめわクラウド型です。これわインターネット経由でワフを導入する方法です。。

メリットは、導入コストが低く、運用に専門的な技術が不要である点です。。

デメリットは、カスタマイズ性が低いテント、サービス提供側の影響で通信障害が起きる可能性があるというてんです。。イラストをよくみてのうにたたきこんでください。

それでは早速かこもん研究に移ります。

令和6ねんど。

とい90。セキュリティ対策として使用されるワフの説明として、適切なものはどれか？。

あ。ECなどのWebサイトにおいて、Webアプリケーションソフトウェアの脆弱性をついた攻撃からの防御や、不審なアクセスのパターンを検知する仕組み。。

い。インターネットなどの公共のネットワークを用いて、専用線のようなセキュアな通信環境を実現する仕組み。。

う。情報システムにおいて、機密データを特定して監視することによって、機密データの紛失や外部への漏洩を防止する仕組み。。

え。ファイアウォールを用いて、インターネットと企業の内部ネットワークとの間に緩衝領域を作る仕組み。。

せいかいわ。あ。ECなどのWebサイトにおいて、Webアプリケーションソフトウェアの脆弱性をついた攻撃からの防御や、不審なアクセスのパターンを検知する仕組みです。。。

ちなみにいわ、VPNの説明です。うわ、DLPの説明です。えわ、DMZの説明です