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、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。

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。

令和がんねんど。しゅうき。午前。

とい14。わふにおけるフォールスポジティブに該当するものはどれか？。。

あ。HTMLの特殊文字、しょうなりを検出したときに通信を遮断するようにわふを設定した場合、しょうなりなどの数式を含んだ正当なHTTPリクエストが送信されたとき、ワフが攻撃として検知し、遮断する。。

い。HTTPリクエストのうち、RFCなどに使用が明確に定義されておらず、Webアプリケーションソフトウェアの開発者が独自の仕様で追加したフィールドについてはわふが検査しないという仕様を悪用して、攻撃の命令を埋め込んだHTTPリクエストが送信されたとき、ワフが遮断しない。。

う。HTTPリクエストのパラメタとして許可する文字列以外を検出したときに通信を遮断するようにワフを設定した場合、許可しない文字列を含んだ不正なHTTPリクエストが送信されたとき、ワフが攻撃として検知し、遮断する。。

え。悪意のある通信を正常な通信と見せかけ、HTTPリクエストを分割して送信されたとき、ワフが遮断しない。

せいかいわ。あ。HTMLの特殊文字、しょうなりを検出したときに通信を遮断するようにわふを設定した場合、しょうなりなどの数式を含んだ正当なHTTPリクエストが送信されたとき、ワフが攻撃として検知し、遮断するです。。。

ちなみにいわ、フォールスネガティブなので誤りです。うわ、処理自体は適切なので誤りです。えわ、フォールスネガティブなので誤りです。

平成30年度。秋季。午前。

とい30。わふ、ウェブアプリケーションファイアーウォールにおけるブラックリストまたはホワイトリストに関する記述のうち、適切なものはどれか？。。

あ。ブラックリストは、脆弱性があるwebサイトのIPアドレスを登録したものであり、該当するIPアドレスからの通信を遮断する。。

い。ブラックリストは、問題がある通信データパターンを定義したものであり、該当する通信を遮断する。。

う。ホワイトリストは、暗号化された受信データをどのように復号するかを定義したものであり、復号鍵が登録されていないデータを遮断する。。

え。ホワイトリストは、脆弱性がないwebサイトのfqdnを登録したものであり、登録が無いwebサイトへの通信を遮断する。

せいかいわ。い。ブラックリストは、問題がある通信データパターンを定義したものであり、該当する通信を遮断するです。。

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ください。。

平成30年度。春季。午前。

とい12。わふの説明はどれか？。。

あ。Webサイトに対するアクセス内容を監視し、攻撃とみなされるパターンを検知したときに当該アクセスを遮断する。。

い。わいふぁいアライアンスが認定した無線ランの暗号化方式の規格であり、えーいーえす暗号に対応している。。

う。様々なシステムの動作ログを一元的に蓄積、管理し、セキュリティじょうの脅威となる事象をいちはやく検知、分析する。。

え。ファイアウォール機能をゆうし、マルウェア対策機能、侵入検知機能などの複数のセキュリティ機能を連携させ、統合的に管理する。

せいかいわ。あ。Webサイトに対するアクセス内容を監視し、攻撃とみなされるパターンを検知したときに当該アクセスを遮断するです。。。

なお、いわ、だぶるぴーえーつー。わいふぁいプロてくてっどアクセスつーの説明なので誤りです。。

うわ、しーむ。セキュリティインフォメーションアンドイベントマネージメントの説明なので誤りです。。

えわ、ゆーてぃーえむ。ユニファイドスレットマネージメントの説明なので誤りです。

平成29年度。秋季。午前。

とい20。わふの説明として、適切なものはどれか？。。

あ。DMZに設置されているwebサーバへの侵入を外部から実際に試みる。。

い。TLSによる暗号化と復号の処理を、webサーバではなく専用のハードウェアで行うことによって、webサーバのcpu負荷を軽減するために導入する。。

う。システム管理者が質問に答える形式で、自組織の情報セキュリティ対策のレベルを診断する。。

え。特徴的なパターンが含まれるかなどをwebアプリケーションへの通信内容を検査して、不正な通信を遮断する。

せいかいわ。え。特徴的なパターンが含まれるかなどをwebアプリケーションへの通信内容を検査して、不正な通信を遮断するです。。。

なお、あわ、ペネトレーションテストの説明なので誤りです。。

いわ、SSLアクセラレータの説明なので誤りです。。

うわ、IPA発行の組織の情報セキュリティ対策自己診断テストの説明なので誤りです。

ちなみにIPAで公開されている組織の情報セキュリティ対策自己診断テストのページはこのようになっております。興味のある方は概要欄にURLを貼っていますのでご覧ください。自己診断のやり方が載っていますので面白いと思います。

平成28年度。春季。午前。

とい13。クライアントとwebサーバのあいだにおいて、クライアントからwebサーバに送信されたデータを検査して、SQLインジェクション等の攻撃を遮断するためのものはどれか？。。

あ。SSL、VPN機能。。

い。わふ。。

う。クラスタ構成。。

え。ロードバランシング機能

せいかいわ。い。わふです。。。

クライアントとwebさーばのあいだ。。SQLインジェクションなどがポイントですね