SecurityScorecard

SecurityScorecard で検出される問題

ネットワークセキュリティ

問題の種別	説明
DDoS 保護サービスの検出	分散型サービス拒否（DDoS）攻撃は、悪意のある攻撃者が膨大な量のデータを Web サイトに送りつけることで、Web サイトが使用または応答できなくなり、最悪クラッシュしてしまうという状態を引き起こします。このような攻撃から防御するアプローチのひとつとして、企業は Web トラフィックの中から悪意のあるトラフィックを取り除くサードパーティー情報セキュリティサービス（Cloudflare など）を使用してルーティングさせます。これらのセキュリティサービスプロバイダーの IP アドレスは公開されており、Security Scorecard は、組織がこれらのサービスプロバイダーを介してトラフィックをルーティングするタイミングを監視することができます。
MongoDB サービスの検出	MongoDB は、オープンソースのデータベース管理システム（DBMS）であり、DBMS は、大量の情報を保存するためのシステムです。インターネット上で不特定多数が MongoDB サービスにアクセスできることを確認しました。 DBMS 内のデータは攻撃者にとって魅力的なターゲットです。DBMS に侵入した攻撃者は、内部にあるデータベースを販売したり、脅迫に使用したり、次の攻撃のために情報を悪用する可能性があります。侵害されたデータベースが原因で、法的手続きや公開通知が必要となったり、企業イメージ悪化につながったり、保険に影響が生じる場合があります。 攻撃者はホストを制御したり、データベースを密かに抽出するために、認証バイパス攻撃（ブルートフォーシング、バッファオーバーフロー、空のパスワードなど）を介してサービスを標的にする可能性があります。攻撃者は、標的として定めたサービスに対してサービス拒否（DoS）攻撃を仕掛け、承認済みエンティティを使用不可にすることができます。攻撃者は、侵害したホストを介して、そのホストが関係するインフラストラクチャに深く侵入することができます。
失効制御のない TLS 証明書	証明書失効リスト（CRL）は、認証局（CA）からオンライン公開されるファイルです。これらのリストは、どの証明書が CA により無効化されたか示し、該当する証明書を失効させます。TLS クライアント（Web ブラウザなど）は、TLS サーバーの証明書が照合する CRL をダウンロードし、証明書が有効であることを確認します。CA は、オンライン証明書ステータスプロトコル（OCSP）サーバーを運用することで、TLS クライアントが証明書の有効性を照合できるようにします。OCSP クエリへの応答は、TLS サーバーにより、証明書に「添付」されます（バンドルされる）。OCSP ステープリングにより、TLS クライアントは OCSP サーバーを照合しなくて済むため、 TLS 接続が高速になります。 攻撃者が証明書の秘密鍵を入手したり、秘密鍵においてその他の侵害が発生した場合、CA は上記の失効制御を使用して TLS クライアントに証明書が失効していることを通知します。失効制御を含まない証明書は失効できません。攻撃者が証明書の秘密鍵を入手した場合、その証明書は有効期限までは有効です。
開いている TCP ポートの検出	TCP プロトコルを介して通信するすべてのサービスは、1 つ以上のポートにバインドされます。サービスがリッスン中（待ち受け状態）のポート番号は、HTTPS がデフォルトで使用するポート 443 番のようにサービス ID を示していますが、サービスはどのポート上でも実行できます。クライアントが TCP ポートへの接続を確立した後、リスニングサービスは通信を開始するか、クライアントによる通信を待機します。 スキャン実行中、インターネットホスト上の TCP ポートに接続し、そのポート上でリッスンしているサービスを検出します。ポートが開いているのを確認後、ポートに接続・通信し、リッスンしているサービスを特定します。

問題の種別	説明
Apache Cassandra サービスの検出	Apache Cassandra は、オープンソースのデータベース管理システム（DBMS）です。 DBMS は大容量の情報を保存することを目的としています。 インターネット上で不特定多数が Apache Cassandra サービスにアクセスできることを確認しました。 DBMS 内のデータは攻撃者にとって魅力的なターゲットです。DBMS に侵入した攻撃者は、内部にあるデータベースを販売したり、脅迫に使用したり、次の攻撃のために情報を悪用する可能性があります。侵害されたデータベースが原因で、法的手続きや公開通知が必要となったり、（企業）イメージ悪化につながったり、保険に影響が生じる場合があります。 攻撃者はホストを制御したり、データベースを密かに抽出するために、認証バイパス攻撃（ブルートフォーシング、バッファオーバーフロー、空のパスワードなど）を介してサービスを標的にする可能性があります。攻撃者は、標的として定めたサービスに対してサービス拒否（DoS）攻撃を仕掛け、許可されたエンティティを使用不可にすることができます。攻撃者は、侵害したホストを介して、そのホストが関係するインフラストラクチャに深く侵入することができます。
Apache CouchDB サービスの検出	Apache CouchDB は、オープンソースのデータベース管理システム（DBMS）です。DBMS は大容量の情報を保存することを目的としています。 インターネット上で不特定多数が Apache CouchDB サービスにアクセスできることを確認しました。 DBMS 内のデータは攻撃者にとって魅力的なターゲットです。DBMS に侵入した攻撃者は、内部にあるデータベースを販売したり、脅迫に使用したり、次の攻撃のために情報を悪用する可能性があります。侵害されたデータベースが原因で、法的手続きや公開通知が必要となったり、（企業）イメージ悪化につながったり、保険に影響が生じる場合があります。 攻撃者はホストを制御したり、データベースを密かに抽出するために、認証バイパス攻撃（ブルートフォーシング、バッファオーバーフロー、空のパスワードなど）を介してサービスを標的にする可能性があります。攻撃者は、標的として定めたサービスに対してサービス拒否（DoS）攻撃を仕掛け、承認済みエンティティを使用不可にすることができます。攻撃者は、侵害したホストを介して、そのホストが関係するインフラストラクチャに深く侵入することができます。
未認証の Elasticsearch サービスの検出	Elasticsearch は、オープンソースのデータベース管理システム（DBMS）です。DBMS は大容量の情報を保存することを目的としています。 Elasticsearch は現行の設定では認証のサポートを行いません。Elasticsearch 内に保存されているすべてのデータは公開されています。 DBMS 内のデータは攻撃者にとって魅力的なターゲットです。DBMS に侵入した攻撃者は、内部にあるデータベースを販売したり、脅迫に使用したり、次の攻撃のために情報を悪用する可能性があります。侵害されたデータベースが原因で、法的手続きや公開通知が必要となったり、（企業）イメージ悪化につながったり、保険に影響が生じる場合があります。