脆弱性スキャンツールの悪用について

はじめに

今回は現代のサイバー攻撃者による脆弱性スキャンツールの悪用について
ご説明します。

脆弱性スキャンツールについて

脆弱性スキャンツールは、企業のセキュリティ強度などを調査する目的で提供されているソフトウェアです。ネットワーク・OS・ミドルウェアなどの脆弱性を調査することが可能になります。

主な脆弱性スキャンツールの種類

- Web アプリケーション脆弱性スキャンツール
  Web アプリケーションの脆弱性を検出することを目的としたツール。
  不正な HTTP リクエストを送信し、擬似攻撃を行うことで、クロスサイトスクリプティングや SQL インジェクションなどの攻撃に対応しているかを見つけることが可能です。
  ■代表的なツール：OWASP ZAP、VAddy ...など

- ネットワーク脆弱性スキャンツール
  ネットワークレイヤの脆弱性を見つけることを目的としたツール。
  サーバやネットワーク機器の設定不備やパッチ適用の不備による、バッファオーバーフローなどの脆弱性を見つけることが可能です。
  ■代表的なツール：InsightVM、Nessus ...など

攻撃者は、事前準備として上記に記述した脆弱性スキャンツールを利用してスキャンを行います。

スキャンした結果、もし脆弱性が見つかれば、その種類に応じた攻撃を行う手口が増加しております。
日本におけるスキャン活動は、報告されているだけで年間約 1 万件も発生しており、今後も増加していくことが予想されます。

NetStable での検知

NetStable のシグネチャで、外部の攻撃者が悪用したと報告されている脆弱性スキャンツールの通信を検出することが出来ます。

- 2001384　Vulnerability Scan Tool (Nmap Scripting Engine)
- 2001385　Vulnerability Scan Tool (AWS Security Scanner)
- 2001386　Vulnerability Scan Tool (ApiTool)
- 2001387　Vulnerability Scan Tool (ZmEu)
- 2001388　Vulnerability Scan Tool (Zgrab)
- 2001389　Vulnerability Scan Tool (Auto Spider)
- 2000255　Vulnerability Scan Tool (masscan)
- 2001509　Vulnerability Scan Tool (Acunetix)
- 2001510　Vulnerability Scan Tool (Nessus)
- 2001511　Vulnerability Scan Tool (Nikto)
- 2001512　Vulnerability Scan Tool (OpenVAS)

各脆弱性スキャンツールを利用している際の通信を遮断するシグネチャです。
各脆弱性スキャンツールを利用して、脆弱性を悪用される可能性があります。
送信元 IP アドレスに心あたりがない場合は、ファイアウォール等のセキュリティ設定にてアクセス制限を行ってください。

まとめ

- 脆弱性スキャンツールは、社内のセキュリティ強度、脆弱性を調査するツール
- 脆弱性スキャンツールを悪用した外部からのスキャン活動が増加している
- 社内で運用しているソフトウェアのバージョンを確認し、アップデートを行う