Playbook para alertas de Scan de Portas

Nome	Playbook de Resposta para alertas de Scan de Portas
Descrição	O scan de portas é um processo de descoberta de serviços em que uma origem IP realiza múltiplas conexões em diferentes portas de um destino. O objetivo é identificar quais serviços estão ativos e acessíveis. Esse comportamento pode indicar uma tentativa de mapeamento de rede ou um a ataques mais direcionados.
Autores	SecDay
Versão	1.0.0
Data da Versão	Data de criação: 26/06/2024 Data de atualização: 26/06/2024
Neste Playbook	

Quando Utilizar

Este playbook deve ser utilizado sempre que as ferramentas de segurança detectarem um alerta de Scan de portas.

Detecção

Os alertas de scans de portas são detectados por diversas ferramentas de segurança, incluindo, mas não limitando-se a:

- Sistemas de Prevenção e Detecção de Intrusões (IPS/IDS);
- Plataformas de Gestão de Informações e Eventos de Segurança (SIEMs);
- Ferramentas de Detecção e Resposta a Endpoint (EDR);
- Firewalls;
- Arquivos de Captura de Pacotes (PCAPs).

Alguns dos principais indicadores de comprometimento que podem sinalizar um scan de portas incluem:

- **Conexões de Origem IP Desconhecida**: Observa-se quando um endereço IP não familiar ou suspeito tenta estabelecer conexões em múltiplas portas diferentes de um único Destino IP, indicando uma possível tentativa de mapear os serviços disponíveis.
- **Padrões Anormais de Tráfego**: Aumentos incomuns no volume de tráfego, especialmente aqueles que envolvem solicitações a portas não padrão ou pouco utilizadas, podem indicar scans de portas.
- **Alertas de Ferramentas de Segurança**: Ferramentas de segurança como IPS/IDS, firewalls e SIEMs podem gerar alertas específicos quando detectam atividades que correspondem aos padrões de scans de portas.
- **Logs de Tentativas de Conexão Malsucedidas**: Múltiplas tentativas de conexão falhadas registradas nos logs de um servidor ou dispositivo de rede podem ser um sinal de um ataque de scan de portas em andamento.

Investigação e Análise

- **Determinação do Contexto**: Avaliar se os scans de portas se originam de IPs externos ou internos e identificar se há alvos específicos dentro da rede, como sistemas críticos ou servidores de dados sensíveis.
- **Identificação de Vulnerabilidades Conhecidas**: Avaliar o host alvo do scan para identificar se existe alguma vulnerabilidade conhecida que possa ter sido explorada.
- **Verificação de Alertas**: Confirmar a validade dos alertas de scans de portas para distinguir entre atividades legítimas e potenciais ameaças.
    - **Exemplos de Atividade Legítima Incluem**:
        - Ferramenta de Scans de vulnerabilidades autorizadas;
        - Pentest (Testes de Penetração) autorizados;
        - Ferramentas de descobertas de redes autorizadas.
- **Coleta de Evidências**: Compilar dados de tráfego, logs de conexão, e informações de portas visadas para uma análise mais aprofundada. Utilizar dados históricos do SIEM para comparar padrões de tráfego anteriores e atuais, ajudando a determinar se a atividade é consistente com operações normais ou se representa uma ameaça.

Contenção e Erradicação

- **Isolamento Imediato**: Utilizar soluções de Detecção e Resposta a Endpoints (EDR) ou tecnologias similares para isolar rapidamente o dispositivo de onde o scan pode estar sendo originado.
- **Bloqueio de Tráfego**: Bloquear o IP ofensor no firewall ou utilizar ferramentas similares para impedir qualquer comunicação adicional com a rede.
- **Ações Corretivas**: Fechar portas desnecessárias, aplicar patches a serviços vulneráveis, e ajustar as regras de firewall para prevenir incidentes futuros.

Recuperação

- **Recuperação dos Sistemas**: Garantir que todos os sistemas afetados estejam seguros e livres de qualquer comprometimento antes de reintegrá-los à rede operacional.
- **Restauração de Operações**: Reabilitar contas ou serviços que foram suspensos durante a investigação após a verificação de sua segurança.

Pós Incidente

- **Documentação do Incidente**: Documentar o incidente, incluindo técnicas utilizadas, sistemas afetados, e medidas de resposta adotadas.
- **Revisão e Melhoria**: Avaliar a eficácia das medidas de resposta e adaptar os procedimentos de segurança para melhorar a detecção e a resposta a scans de portas no futuro.
- **Desenvolvimento de Novos Alertas**: Criar e implementar novos alertas no SIEM ou ferramentas similares com base nos comportamentos identificados durante o incidente que anteriormente não geravam alertas;
- **Atualização da Base de IoCs**: Enriquecer a base de Indicadores de Comprometimento (IoCs) com os dados coletados durante a investigação do incidente. Incluir detalhes como IPs ofensores, padrões de tráfego anormal, hashes de arquivos maliciosos e outras assinaturas digitais que possam ajudar a identificar e prevenir futuras tentativas de intrusão;
- **Comunicação**: Comunicar as descobertas e as ações tomadas a todas as partes interessadas.