\*\*Relatório de Análise de Tráfego Suspeito\*\*

## 1. Introdução

Este relatório tem como objetivo apresentar a análise de um conjunto de dados de tráfego, identificando potenciais riscos de segurança e propondo medidas de mitigação e prevenção, alinhadas com boas práticas de frameworks de segurança como \*\*NIST\*\* e \*\*OWASP\*\*.

## 2. Principais Ameaças Identificadas

### 2.1 Tráfego Suspeito por Método HTTP

- Foram detectadas requisições utilizando os métodos `POST`, `PUT`, `DELETE` e `OPTIONS`.

- Esses métodos podem ser explorados para ataques de injeção de comandos, upload de arquivos maliciosos e manipulação de recursos.

- \*\*Possíveis ataques\*\*: Injeção SQL, Cross-Site Request Forgery (CSRF), Remote Code Execution (RCE).

### 2.2 User-Agents Suspeitos ou Ausentes

- Algumas requisições apresentam User-Agent ausente ou incomum.

- Esse comportamento pode indicar a presença de bots maliciosos, scanners de vulnerabilidades ou ataques automatizados.

- \*\*Possíveis ataques\*\*: Web scraping, brute force, ataques de enumeração.

### 2.3 Requisições para URLs Sensíveis

- Foram detectadas requisições para \*\*caminhos críticos\*\*, como:

- `/admin`, `/login`, `/wp-login.php`, `/phpmyadmin`, `/shell`, `/cmd`

- Esses caminhos geralmente são alvos de tentativas de brute force e exploração de vulnerabilidades.

- \*\*Possíveis ataques\*\*: Credential Stuffing, exploração de credenciais padrão, descoberta de painéis de administração.

### 2.4 IPs com Alto Volume de Requisições

- Alguns endereços IP realizaram um número anormalmente alto de requisições em curtos períodos de tempo.

- Esse comportamento pode indicar tentativas de \*\*força bruta, DDoS ou scans automatizados\*\*.

- \*\*Possíveis ataques\*\*: Distributed Denial of Service (DDoS), brute force, reconhecimento de rede.

## 3. Recomendações de Mitigação e Prevenção

### 3.1 Implementação de Políticas de Firewall

- Configurar \*\*Web Application Firewall (WAF)\*\* para bloquear acessos suspeitos e filtrar tráfego malicioso.

- Regras específicas para bloquear \*\*IPs com alto volume de requisições suspeitas\*\*.

### 3.2 Autenticação e Controle de Acesso

- Implementar \*\*Multi-Factor Authentication (MFA)\*\* para acessos administrativos e áreas sensíveis.

- Restringir o acesso a \*\*endpoints sensíveis\*\* utilizando listas de controle de acesso (ACLs).

### 3.3 Monitoramento Contínuo e Resposta a Incidentes

- Implementar um \*\*SIEM (Security Information and Event Management)\*\* para monitoramento e detecção de anomalias.

- Criar \*\*playbooks de resposta a incidentes\*\* baseados no \*\*NIST Cybersecurity Framework\*\*.

### 3.4 Proteção Contra Ataques Automatizados

- Implementar \*\*CAPTCHAs\*\* em formulários de login para mitigar ataques de brute force.

- Utilizar soluções de \*\*rate limiting\*\* para limitar requisições suspeitas de um mesmo IP.

### 3.5 Endurecimento de Servidor e Aplicativo

- Desativar \*\*métodos HTTP não utilizados\*\*, como `PUT`, `DELETE`, `OPTIONS`, caso não sejam necessários.

- Utilizar \*\*headers de segurança\*\* como Content Security Policy (CSP) e HTTP Strict Transport Security (HSTS).

## 4. Alinhamento com Frameworks de Segurança

### \*\*NIST Cybersecurity Framework\*\*

As recomendações deste relatório estão alinhadas com os pilares do \*\*NIST CSF\*\*:

- \*\*Identify\*\*: Monitoramento e análise de ameaças.

- \*\*Protect\*\*: Implementação de WAF, autenticação robusta e controle de acesso.

- \*\*Detect\*\*: Uso de SIEM para monitoramento de eventos suspeitos.

- \*\*Respond\*\*: Playbooks de resposta a incidentes.

- \*\*Recover\*\*: Plano de recuperação para mitigar impacto de ataques.

### \*\*OWASP Top 10\*\*

As ameaças identificadas estão diretamente relacionadas a vulnerabilidades do \*\*OWASP Top 10\*\*, incluindo:

- \*\*A01:2021 - Broken Access Control\*\*: Requisições para URLs sensíveis.

- \*\*A07:2021 - Identification and Authentication Failures\*\*: Tentativas de brute force.

- \*\*A08:2021 - Software and Data Integrity Failures\*\*: Exploração de endpoints vulneráveis.

## 5. Conclusão

A análise revelou sinais claros de tráfego potencialmente malicioso, incluindo tentativas de acesso a URLs sensíveis, uso de métodos HTTP suspeitos e altos volumes de requisições de determinados IPs. Para mitigar esses riscos, é essencial implementar controles de segurança robustos alinhados com as diretrizes do \*\*NIST Cybersecurity Framework\*\* e do \*\*OWASP Top 10\*\*.

A aplicação das recomendações descritas neste relatório ajudará a reduzir significativamente as chances de exploração de vulnerabilidades e garantir a segurança do ambiente analisado.