Relatório de Pentest - Vulnerabilidades no Servidor (10.0.0.6)

Objetivo: Identificação de vulnerabilidades em um servidor com o IP 10.0.0.6, especificamente na porta 8080.

Ferramentas Utilizada:

1. Nmap versão 7.94SVN, com o script `vuln` para detectar vulnerabilidades
2. Nikito
3. MetaExploit Framework

Data da Análise: 29 de março de 2025, 22:02 -03.

---

1 Resumo da Análise

A análise foi realizada na máquina alvo com o IP `10.0.0.6`, na porta `8080`. O Nmap detectou o serviço `http-proxy` ativo na porta mencionada, bem como várias vulnerabilidades e informações sensíveis sobre a configuração do servidor web.

Através da execução do Nikto, um scanner de vulnerabilidades, foi identificado um conjunto de possíveis falhas de segurança no servidor web hospedado no endereço IP 10.0.0.6, porta 8080. Algumas dessas vulnerabilidades podem expor o sistema a riscos de exploração, sendo essencial implementar correções e mitigação.

2 Resultados do Scans

2.1 Vulnerabilidades Identificadas:

1. **Cookies Inseguros**:
   - O cookie `PHPSESSID`, utilizado para identificar sessões de usuários, **não possui a flag HttpOnly** configurada.
   - **Risco**: A falta da flag `HttpOnly` permite que scripts no navegador possam acessar o valor do cookie, o que pode ser explorado por atacantes que realizam ataques XSS (Cross-Site Scripting).
2. **Enumeração HTTP**:
   - **/login.php**: Detectada a possibilidade de acesso a uma página de login, que pode ser uma página de administração do sistema.
   - **/robots.txt**: Arquivo encontrado, pode revelar informações sobre áreas restritas do servidor ou diretórios que não devem ser indexados por motores de busca.
   - **/config/**: Diretório identificado como **interessante**, potencialmente com informações sensíveis sobre a configuração do servidor.
   - **/docs/**: Diretório de documentos encontrado, com listagem de arquivos visível, sugerindo que há informações potencialmente sensíveis.
   - **/external/**: Diretório encontrado, possivelmente com arquivos externos ou links para recursos importantes.
   - **Cookie PHPSESSID Criado sem o Flag HttpOnly**
     - **Descrição**: O cookie PHPSESSID foi encontrado sem a flag `HttpOnly`. Isso significa que o cookie pode ser acessado via JavaScript, o que facilita ataques de XSS (Cross-Site Scripting) que visem roubar sessões do usuário.
     - **Recomendação**: Configurar o servidor para adicionar a flag `HttpOnly` aos cookies de sessão para evitar o acesso via scripts.
   - **Ausência do Cabeçalho X-Frame-Options (Anti-Clickjacking)**
     - **Descrição**: O cabeçalho `X-Frame-Options` não foi encontrado na resposta HTTP, o que permite que a página seja carregada dentro de um iframe. Isso torna o site vulnerável a ataques de Clickjacking.
     - **Recomendação**: Adicionar o cabeçalho `X-Frame-Options` com valor `DENY` ou `SAMEORIGIN` para prevenir ataques de Clickjacking.
   - **Redirecionamento para login.php**

        - **Descrição**: A página raiz (`/`) realiza um redirecionamento para `login.php`, sugerindo que há uma área de login exposta que pode ser alvo de ataques de brute-force ou outras tentativas de exploração.
        - **Recomendação**: Garantir que o mecanismo de login esteja protegido com autenticação forte e implementações adequadas de controle de acesso.
    - **Divulgação de ETags com Inodes**
        - **Descrição**: O servidor web está vazando inodes através do cabeçalho `ETag`, o que pode fornecer informações sobre a estrutura de arquivos internos do servidor.
        - **Recomendação**: Configurar o servidor Apache para desabilitar ou modificar a geração de ETags que incluam inodes, de modo a proteger informações sensíveis do sistema de arquivos.
    - **Indexação de Diretórios de Configuração e Documentação**
        - **Descrição**: O servidor apresenta diretórios com indexação habilitada, como `/config/` e `/docs/`, que podem expor arquivos de configuração ou documentação sensível.
        - **Recomendação**: Desabilitar a indexação de diretórios no servidor Apache e revisar a configuração para garantir que diretórios sensíveis não sejam acessíveis.
    - **Arquivo `README` Padrão do Apache Encontrado**
        - **Descrição**: O arquivo `README` padrão do Apache foi encontrado no diretório `/icons/`, o que pode fornecer informações sobre a instalação do servidor e possíveis vulnerabilidades.
        - **Recomendação**: Remover arquivos de exemplo e documentação padrão do Apache, que podem fornecer informações úteis para um atacante.
    - **Página de Login Admin Acessível**
        - **Descrição**: A página `/login.php` foi identificada como uma página de login admin, o que pode ser um ponto de entrada crítico para ataques direcionados a privilégios administrativos.
        - **Recomendação**: Proteger a página de login com autenticação multifatorial (MFA) e limitar tentativas de login para evitar ataques de força bruta.
- SSH (Porta 22)
  Serviço: OpenSSH 9.6p1 (Ubuntu Linux; protocolo 2.0)
  Chaves de host:
  ECDSA: e5:3b:47:59:b2:fa:9e:f7:43:2e:71:90:f8:d3:3b:8ao
  ED25519: 5b:c2:c2:da:a9:6b:b3:74:39:a2:59:17:b0:2a:88:bd

3.2. MySQL (Porta 3306)
•Versão: MySQL 5.5.54-0+deb8u1-log
•Protocolo: 10
•Plugins de Autenticação: mysql_native_password
•Possíveis Riscos:
MySQL 5.5.54 é uma versão desatualizada e pode conter vulnerabilidades conhecidas.
Se acesso remoto estiver permitido, pode ser explorado por atacantes

4 Conclusões e Recomendações Gerais

O servidor web identificado apresenta diversas vulnerabilidades que podem ser exploradas para comprometer a segurança do sistema. A principal recomendação é realizar as configurações apropriadas no servidor Apache, como a habilitação de segurança em cookies, proteção contra clickjacking e a remoção de diretórios sensíveis. Além disso, é crucial realizar uma revisão mais aprofundada do código do servidor e aplicar práticas recomendadas de segurança.

Ações Prioritárias:

- Habilitar a flag `HttpOnly` para os cookies.
- Adicionar o cabeçalho `X-Frame-Options`.
- Remover a indexação de diretórios sensíveis.

- Desabilitar a geração de ETags com inodes.

3. **Informações do Servidor**:
    - **Servidor Web**: Apache/2.4.10 (Debian).
    - **Endereço MAC**: 08:00:27:D7:5B:12 (Oracle VirtualBox Virtual NIC).