Relatório de Pentest - Análise de Vulnerabilidades no Servidor (10.0.0.6) - Nmap

---

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

Ferramenta Utilizada: Nmap versão 7.94SVN, com o script `vuln` para detectar vulnerabilidades.

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

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.

Resultados do Scan

1. **Estado da Porta**:
   - **Porta 8080/tcp**: Aberta, servindo como um proxy HTTP.
2. **Vulnerabilidades Identificadas**:
   - **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).
   - **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.
3. **Informações do Servidor**:
   - **Servidor Web**: Apache/2.4.10 (Debian).
   - **Endereço MAC**: 08:00:27:D7:5B:12 (Oracle VirtualBox Virtual NIC).

Recomendações

1. **Segurança de Cookies**:
   - **Configurar a flag `HttpOnly` nos cookies de sessão**, especialmente o `PHPSESSID`, para proteger contra ataques XSS.
   - Adicionalmente, considerar o uso da flag `Secure` para garantir que os cookies sejam enviados apenas por conexões seguras (HTTPS).
2. **Proteção de Diretórios Sensíveis**:
   - **Restringir o acesso aos diretórios `/config/`, `/docs/` e `/external/`** através de regras adequadas no servidor web (exemplo: `.htaccess` no Apache) para evitar a exposição acidental de informações sensíveis.

- **Configurar o arquivo** `robots.txt` para bloquear motores de busca de indexarem arquivos ou diretórios sensíveis.

3. **Acesso à Página de Login**:
   - Implementar **medidas adicionais de segurança na página de login**, como limitar tentativas de login, usar CAPTCHA, e autenticação multifatorial (MFA), para proteger contra ataques de força bruta.
4. **Revisão e Hardening do Servidor**:
   - **Revisar configurações do Apache** para garantir que diretórios com listagem de arquivos habilitada sejam restritos, evitando a exposição de informações que possam ser exploradas.
   - Atualizar o **servidor Apache e outros softwares** para versões mais recentes, que corrigem vulnerabilidades de segurança conhecidas.