Teste de Intrusão

Análise de Metodologias de Teste de Intrusão em Ambientes Simulados

Equipe de Análise:	**Manuella Carvalho, João Lucas Carvalho e Luis Eduardo Cordeiro**
Disciplina:	Segurança Cibernética
Classificação:	**ACADÊMICO**

1. Sumário Executivo

Este documento detalha os procedimentos e resultados de uma série de testes de intrusão práticos, realizados com o objetivo de explorar e contrastar as metodologias de **Caixa Branca (White-Box)**, **Caixa Cinza (Grey-Box)** e **Caixa Preta (Black-Box)**. Utilizando um arsenal técnico composto pelas ferramentas **Nmap**, **Nikto** e **Wireshark**, nossa equipe conduziu análises em ambientes controlados para mapear superfícies de ataque, identificar vulnerabilidades em servidores web e inspecionar o tráfego de rede. A atividade permitiu a aplicação prática de conceitos teóricos de segurança, resultando em uma compreensão aprofundada sobre como o nível de conhecimento prévio do alvo impacta diretamente o escopo, a profundidade e a eficácia de um teste de segurança.

2. Introdução

2.1. Contexto e Objetivos

A segurança cibernética moderna exige uma abordagem multifacetada para a identificação de vulnerabilidades. Compreender as diferentes metodologias de teste é fundamental para a formação de um profissional da área. Este relatório documenta um exercício prático focado em:

- **Aplicar** técnicas de varredura, enumeração e análise de tráfego em cenários distintos.
- **Contrastar** os resultados obtidos em testes White-Box, Grey-Box e Black-Box.
- **Aprimorar** o domínio técnico das ferramentas Nmap, Nikto e Wireshark.
- **Desenvolver** a capacidade de relatar achados técnicos e propor mitigação de forma clara e objetiva.

2.2. Metodologias de Teste Exploradas

Os testes foram segmentados em três abordagens distintas, cada uma simulando um nível diferente de informação disponível para o analista de segurança:

- **Teste de Caixa Branca (White-Box):** Simula um auditor interno ou um desenvolvedor com acesso total à infraestrutura, código-fonte e documentação. O foco é a análise aprofundada e a validação de configurações de segurança.
- **Teste de Caixa Preta (Black-Box):** Simula um atacante externo sem nenhum conhecimento prévio do ambiente-alvo. A análise parte do zero, focando na descoberta e exploração de vulnerabilidades expostas publicamente.
- **Teste de Caixa Cinza (Grey-Box):** Simula um usuário comum, um parceiro ou um atacante que obteve acesso limitado (e.g., credenciais de baixo privilégio). O teste avalia o que um ator com algum conhecimento interno pode alcançar.

3. Arsenal Técnico Empregado

Para a execução dos testes, foram selecionadas três ferramentas padrão da indústria, cada uma com uma função específica no processo de análise:

- **Nmap (Network Mapper):** Ferramenta essencial para a fase de reconhecimento. Foi utilizada para mapear redes, identificar hosts ativos, enumerar portas e serviços, e obter impressões digitais de sistemas operacionais e aplicações.
- **Nikto:** Scanner de vulnerabilidades focado em servidores web. Foi empregado para identificar rapidamente falhas de configuração, softwares desatualizados, arquivos perigosos e outras vulnerabilidades comuns em aplicações web.
- **Wireshark:** Analisador de protocolos de rede. Foi indispensável para a captura e inspeção de tráfego, permitindo a análise de comunicações não criptografadas, a identificação de vazamento de informações e a validação de controles de segurança na camada de rede.

4. Execução dos Testes e Análise de Resultados

Esta seção detalha os procedimentos adotados e os achados fictícios para cada metodologia de teste.

4.1. Cenário 1: Teste de Caixa Branca

- **Contexto:** Análise de um servidor web interno (`10.0.2.15`) com acesso total às suas configurações e código.
- **Procedimento e Achados:**
  1. **Análise de Configuração:** A revisão do arquivo `httpd.conf` do servidor Apache revelou que o módulo `mod_status` estava habilitado e exposto para toda a rede interna, vazando informações detalhadas sobre as requisições ativas.
  2. **Varredura com Nmap:** Uma varredura completa foi executada para validar os serviços expostos.

     ```
     # Varredura agressiva para detectar versões e executar scripts em todas as portas
     nmap -A -p- 10.0.2.15
     ```

  3. **Análise com Nikto:** O Nikto foi direcionado ao servidor para uma verificação aprofundada.

     ```
     # Análise completa do servidor web
     nikto -h http://10.0.2.15 -Tuning 1,2,3,4,5
     ```

     - **Achado:** O Nikto confirmou a exposição da página de status do Apache (`/server-status`) e identificou que a versão do PHP (`7.2.1`) estava desatualizada e vulnerável a múltiplas CVEs.
  4. **Análise de Tráfego com Wireshark:** O monitoramento da comunicação entre a aplicação e o banco de dados revelou que as credenciais de conexão estavam sendo transmitidas em texto claro pela rede.

4.2. Cenário 2: Teste de Caixa Preta

- **Contexto:** Análise externa do domínio `www.joaolisboa.ma.gov.br` sem nenhum conhecimento prévio. **(Nota: Os resultados a seguir são puramente fictícios e para fins educacionais)**.
- **Procedimento e Achados:**
  1. **Reconhecimento com Nmap:** Uma varredura inicial foi focada nas portas web mais comuns.

```
# Varredura SYN (stealth) nas portas 80 e 443 para identificar o serviço web
nmap -sS -p 80,443 --script=http-headers www.joaolisboa.ma.gov.br
```

- **Achado Fictício:** A análise dos cabeçalhos HTTP retornados pelo script do Nmap revelou a ausência do cabeçalho `Strict-Transport-Security`, indicando uma potencial falha na implementação do HSTS.

2. **Verificação com Nikto:** O Nikto foi lançado contra o domínio para buscar vulnerabilidades comuns.

```
# Análise padrão do Nikto no alvo
nikto -h https://www.joaolisboa.ma.gov.br
```

- **Achado Fictício:** O Nikto reportou que o software do servidor web (Apache 2.4.29) estava publicamente identificado e que um arquivo `robots.txt` listava diretórios que poderiam ser sensíveis, como `/painel-administrativo/`.

3. **Análise Passiva com Wireshark:** Ao simplesmente navegar no site e preencher formulários de contato, o Wireshark foi usado para inspecionar o tráfego gerado. Não foram encontradas transmissões de dados sensíveis em texto claro, indicando o uso correto de HTTPS.

4.3. Cenário 3: Teste de Caixa Cinza

- **Contexto:** Análise de uma aplicação web (`app.empresa.fict`) com acesso a credenciais de um usuário de baixo privilégio.
- **Procedimento e Achados:**
  1. **Análise Autenticada:** Após o login na aplicação, foi possível navegar por funcionalidades restritas a usuários autenticados.
  2. **Inspeção com Ferramentas de Proxy (e.g., Burp Suite):** Ao interceptar as requisições com um proxy, notou-se que o ID de usuário era passado como um parâmetro numérico em uma chamada de API (`/api/v1/userdata?user_id=105`).
  3. **Teste de Controle de Acesso Quebrado:** Alterando o parâmetro `user_id` para `104` (outro usuário), a API retornou os dados deste outro usuário. Isso caracteriza uma vulnerabilidade crítica de **Insecure Direct Object Reference (IDOR)**.
  4. **Validação com Wireshark:** O Wireshark confirmou que, embora a comunicação fosse via HTTPS, a lógica de autorização falha da API poderia ser explorada para acessar dados de qualquer usuário da plataforma, bastando para isso enumerar os IDs.

5. Sumário de Vulnerabilidades Identificadas

ID	Vulnerabilidade	Severidade	Metodologia	Ferramenta Chave	Impacto Potencial
V-01	Exposição do `server-status` do Apache	**Média**	Caixa Branca	Nikto	Vazamento de informações sobre a infraestrutura e atividade do servidor.
V-02	Credenciais de DB em Texto Claro	**Alta**	Caixa Branca	Wireshark	Interceptação de credenciais e acesso não autorizado ao banco de dados.
V-03	Ausência do Cabeçalho HSTS	**Baixa**	Caixa Preta	Nmap	Risco de ataques de downgrade de protocolo (SSL stripping) em

					conexões iniciais.
V-04	Referência Insegura a Objeto Direto (IDOR)	**Crítica**	Caixa Cinza	Proxy Web	Acesso e modificação não autorizados de dados de outros usuários.

6. Plano de Mitigação

Com base nos achados, recomendamos as seguintes ações corretivas:

- **Para V-01:** Restringir o acesso ao `mod_status` apenas para IPs de gerenciamento na configuração do Apache.
- **Para V-02:** Implementar criptografia na comunicação entre o servidor de aplicação e o banco de dados (e.g., usando SSL/TLS) e armazenar as credenciais de forma segura, utilizando um cofre de segredos.
- **Para V-03:** Implementar o cabeçalho HTTP `Strict-Transport-Security` em todas as respostas do servidor web para forçar o uso de HTTPS.
- **Para V-04:** Refatorar a API para validar se o usuário autenticado tem permissão para acessar os dados solicitados antes de retornar a resposta. A validação deve ser feita no backend.

7. Conclusão

A execução prática destes três tipos de teste de intrusão demonstrou de forma inequívoca como o contexto e o nível de informação influenciam a estratégia de segurança. O teste de Caixa Preta foi eficaz para identificar falhas de configuração externas, enquanto o de Caixa Branca permitiu encontrar vulnerabilidades profundas na arquitetura e no código. Por fim, o teste de Caixa Cinza provou ser extremamente valioso para descobrir falhas de lógica de negócio e de controle de acesso, que muitas vezes não são visíveis de uma perspectiva externa ou interna estática.

Esta atividade solidificou nossa compreensão de que uma estratégia de defesa em profundidade deve necessariamente abranger auditorias com todas as três abordagens, pois cada uma revela um tipo diferente de risco. O domínio prático de ferramentas como Nmap, Nikto e Wireshark mostrou-se essencial para traduzir a teoria em resultados tangíveis.