Segurança em Rede Wi-Fi

Relatório de Auditoria de Segurança em Rede Wi-Fi

Equipe de Análise:	**Manuella Carvalho e Luis Eduardo Cordeiro**
Disciplina:	Segurança Cibernética
Classificação:	**CONFIDENCIAL / ACADÊMICO**

1. Sumário Executivo

Este relatório apresenta os resultados de uma auditoria de segurança conduzida em um ambiente de rede sem fio (Wi-Fi) autorizado e controlado. O objetivo do projeto foi aplicar uma metodologia estruturada de teste de intrusão para identificar, explorar e documentar vulnerabilidades críticas. Utilizando o conjunto de ferramentas Aircrack-ng e outras utilidades de análise de rede, a equipe realizou ataques simulados, incluindo a captura de handshakes de autenticação WPA2, ataques de negação de serviço (DoS) por desautenticação e a exploração de falhas no protocolo WPS (Wi-Fi Protected Setup).

A análise revelou vulnerabilidades de severidade **Alta** e **Crítica** na rede alvo, "Corp-WiFi-Guest". A principal falha identificada foi a ativação do WPS, que permitiu a recuperação da chave pré-compartilhada (PSK) da rede em um curto espaço de tempo. Adicionalmente, a rede mostrou-se suscetível a ataques de desautenticação, impactando a disponibilidade do serviço para usuários legítimos.

As recomendações prioritárias incluem a desativação imediata do WPS, a migração para o padrão de segurança WPA3 e a ativação da proteção de quadros de gerenciamento (IEEE 802.11w) para mitigar os riscos identificados.

2. Introdução e Metodologia

2.1. Escopo e Objetivos da Auditoria

O principal objetivo deste trabalho foi realizar uma avaliação de segurança prática em uma rede Wi-Fi, aplicando os conhecimentos teóricos adquiridos na disciplina de Segurança Cibernética. Os objetivos específicos foram:

- **Mapear** a topologia da rede sem fio e identificar seus ativos principais (pontos de acesso e clientes).
- **Identificar** vulnerabilidades relacionadas à configuração, criptografia e protocolos de autenticação.
- **Executar** ataques controlados para validar o impacto das vulnerabilidades.
- **Documentar** os achados e propor um plano de mitigação eficaz.

2.2. Fases da Auditoria

A análise seguiu uma metodologia estruturada em quatro fases distintas:

1. **Planejamento e Reconhecimento:** Definição do escopo no ambiente autorizado e levantamento inicial de informações sobre a rede alvo (SSID, BSSID, canal, tipo de criptografia) utilizando a suíte Aircrack-ng em modo de monitoramento.

2. **Mapeamento e Enumeração:** Coleta passiva e ativa de dados para aprofundar o conhecimento sobre o alvo, incluindo a identificação de clientes conectados e a verificação de protocolos vulneráveis como o WPS.
3. **Análise e Exploração:** Execução de testes práticos para explorar as vulnerabilidades identificadas, como a captura de handshakes WPA2 e ataques de força bruta contra o PIN do WPS.
4. **Relatório e Recomendações:** Consolidação de todos os dados coletados, formalização dos achados e elaboração de um plano de ação para a correção das falhas.

3. Ambiente e Ferramentas

- **Ambiente de Teste:** A análise foi conduzida em uma rede Wi-Fi de laboratório, configurada com as seguintes características:
  - **SSID:** `Corp-WiFi-Guest`
  - **BSSID (MAC do Roteador):** `C0:3E:BA:C1:A0:DE`
  - **Criptografia:** `WPA2-PSK (CCMP)`
  - **Canal:** `11`
- **Arsenal Técnico:**
  - **Suíte Aircrack-ng:** `airodump-ng`, `aireplay-ng`, `aircrack-ng` para mapeamento, injeção de pacotes e quebra de senhas.
  - **Wash e Reaver:** Para detecção e exploração de vulnerabilidades WPS.
  - **Nmap:** Para varredura de hosts na rede após obter acesso.
  - **Wireshark:** Para análise detalhada de pacotes e do handshake capturado.

4. Execução e Detalhamento dos Achados

Esta seção descreve os procedimentos técnicos realizados e as vulnerabilidades descobertas.

4.1. Fase de Mapeamento e Coleta de Dados

A interface de rede sem fio foi colocada em modo monitor e o `airodump-ng` foi utilizado para identificar as redes no alcance.

```
# Colocar a placa de rede em modo monitor
sudo airmon-ng start wlan0

# Iniciar o airodump-ng para escanear as redes
sudo airodump-ng wlan0mon
```

- **Resultado:** A rede `Corp-WiFi-Guest` foi identificada no canal 11, utilizando criptografia WPA2. Múltiplos clientes foram vistos conectados a ela.

Em seguida, a ferramenta `wash` foi usada para verificar a presença do WPS.

```
# Verificar por redes com WPS habilitado
sudo wash -i wlan0mon
```

- **Achado (V-01):** O `wash` confirmou que o BSSID `C0:3E:BA:C1:A0:DE` possuía WPS habilitado e desbloqueado, representando uma vulnerabilidade crítica.

4.2. Exploração de Vulnerabilidades

Ataque 1: Exploração da Vulnerabilidade WPS (V-01)

Com o WPS confirmado, a ferramenta `reaver` foi utilizada para realizar um ataque de força bruta contra o PIN.

```
# Iniciar o Reaver contra o alvo, com modo verboso e ignorando avisos
sudo reaver -i wlan0mon -b C0:3E:BA:C1:A0:DE -vv --ignore-locks
```

- **Resultado:** O ataque foi bem-sucedido em menos de 4 horas. O Reaver conseguiu adivinhar o PIN do WPS e, como consequência, revelou a senha (PSK) da rede em texto claro: `Senha@Corp123`. Este achado compromete totalmente a **confidencialidade** da rede.

Ataque 2: Ataque de Negação de Serviço por Desautenticação (V-02)

Para testar a resiliência da rede contra ataques de disponibilidade, um ataque de desautenticação foi direcionado a um cliente específico conectado à rede.

```
# Capturar informações do alvo para o ataque de desautenticação
sudo airodump-ng --bssid C0:3E:BA:C1:A0:DE -c 11 wlan0mon

# Enviar 10 pacotes de desautenticação para o cliente (e.g., MAC F8:E4:3B:9A:B1:C2)
# O "-0" indica o ataque de desautenticação
sudo aireplay-ng -0 10 -a C0:3E:BA:C1:A0:DE -c F8:E4:3B:9A:B1:C2 wlan0mon
```

- **Resultado:** O cliente `F8:E4:3B:9A:B1:C2` foi imediatamente desconectado da rede, confirmando que a rede não possui proteção de quadros de gerenciamento (IEEE 802.11w). Este achado compromete a **disponibilidade** do serviço.

Ataque 3: Captura de Handshake WPA2 para Análise Offline (V-03)

Mesmo com a senha já descoberta via WPS, o procedimento de captura do handshake foi realizado para demonstrar outro vetor de ataque comum.

```
# 1. Isolar o tráfego do alvo e salvar a captura em um arquivo
sudo airodump-ng --bssid C0:3E:BA:C1:A0:DE -c 11 -w captura_handshake wlan0mon

# 2. Em outro terminal, forçar a reconexão de um cliente para capturar o handshake
sudo aireplay-ng -0 5 -a C0:3E:BA:C1:A0:DE -c F8:E4:3B:9A:B1:C2 wlan0mon
```

- **Resultado:** O `airodump-ng` indicou `[ WPA handshake: C0:3E:BA:C1:A0:DE ]` no canto superior direito, confirmando a captura bem-sucedida. O arquivo `captura_handshake-01.cap` poderia então ser submetido a um ataque de força bruta offline com o `aircrack-ng` e uma wordlist. Isso demonstra um risco à **confidencialidade** se a senha for fraca.

5. Sumário de Riscos e Recomendações

ID	Vulnerabilidade	Severidade	Princípio CID Afetado	Recomendação de Mitigação
V-01	WPS Habilitado e Vulnerável	**Crítica**	Confidencialidade	**Desativar o WPS imediatamente** nas configurações do roteador. Esta é a contramedida mais urgente.
V-02	Ausência de Proteção 802.11w	**Alta**	Disponibilidade	**Habilitar a Proteção de Quadros de Gerenciamento (PMF/MFP)** no roteador para proteger contra ataques de desautenticação.
V-03	Risco de Quebra de Senha Offline	**Média**	Confidencialidade	**Implementar uma política de senhas fortes e complexas** (mais de 16 caracteres, com variedade) e **migrar para WPA3**, que oferece proteção superior contra este tipo de ataque.
Geral	Firmware Desatualizado (Risco Inferido)	**Média**	Integridade, Confidencialidade	**Manter o firmware do roteador sempre atualizado** para corrigir vulnerabilidades conhecidas que podem ser exploradas por atacantes.

6. Conclusão

A auditoria de segurança realizada na rede `Corp-WiFi-Guest` demonstrou que configurações padrão e protocolos legados representam um risco significativo para a segurança de ambientes sem fio. A vulnerabilidade mais crítica, a ativação do WPS, permitiu o comprometimento total da confidencialidade da rede, provando que uma única falha de configuração pode invalidar outras medidas de segurança, como o uso de WPA2 com uma senha forte.

Esta atividade prática foi de valor inestimável para consolidar a compreensão sobre os vetores de ataque em redes Wi-Fi e a importância de uma abordagem de defesa em camadas. A segurança de uma rede sem fio não depende apenas da criptografia utilizada, mas de um conjunto de boas práticas que inclui o hardening das configurações do roteador, a atualização constante de firmware e a adoção de padrões de segurança modernos como o WPA3.