RELATÓRIO TÉCNICO DE TESTE DE INTRUSÃO

Cliente: TechCorp Solutions

Alvo: 98.95.207.28

Data: 01/12/2025

Nome: Lucca Corrêa da Silva

1. Sumário Executivo

Este documento detalha as descobertas de segurança resultantes do teste de intrusão realizado na infraestrutura da TechCorp Solutions. O objetivo foi simular um ataque real (Black Box) para identificar vulnerabilidades que poderiam comprometer o negócio.

Conclusão Geral: O nível de segurança do servidor analisado é considerado CRÍTICO.
Um atacante externo, sem credenciais iniciais, foi capaz de comprometer totalmente o servidor, escalando privilégios até obter acesso ROOT (Administrador Máximo). Isso permitiu acesso irrestrito a bancos de dados de clientes, arquivos de configuração, código-fonte e backups.
Resumo do Impacto:

- **Confidencialidade:** Totalmente comprometida (vazamento de senhas e dados de clientes).
- **Integridade:** Totalmente comprometida (capacidade de alterar ou deletar dados).
- **Disponibilidade:** Em risco (capacidade de desligar serviços ou apagar o servidor).

2. Resumo das Vulnerabilidades

ID	Vulnerabilidade	Severidade	Status
VULN-01	Local File Inclusion (LFI) - Painel Admin	Crítica	Explorada
VULN-02	Credenciais em Texto Claro (Hardcoded)	Crítica	Explorada

VULN-03	Escalação de Privilégio para Root	🟤 Crítica	Explorada
VULN-04	Exposição de Informação (Docker/Backups)	🟠 Alta	Explorada
VULN-05	Directory Listing (Listagem de Diretório)	🟠 Alta	Explorada

3. Detalhamento Técnico (Findings)

Esta seção descreve tecnicamente como as falhas foram encontradas e exploradas.

🟤 VULN-01: Local File Inclusion (LFI)

Descrição:
O painel administrativo (panel.php) não valida corretamente a entrada do usuário no parâmetro file. Isso permite que um atacante manipule a URL para ler arquivos fora do diretório web.
Exploração:
Ao acessar a URL manipulada, o servidor retornou o conteúdo de arquivos sensíveis do sistema operacional.

- **Vetor de Ataque:** http://98.95.207.28/panel.php?file=/etc/passwd
- **Arquivo Lido:** /etc/passwd (Lista de usuários) e /home/techcorp/.bash_history.

Evidência:

Recomendação:
Implementar uma "allowlist" (lista branca) de arquivos permitidos no código PHP e bloquear caracteres de navegação de diretório como ../.

🟤 VULN-02: Exposição de Credenciais (Hardcoded Credentials)

Descrição:
Foram encontradas senhas administrativas salvas em texto puro em arquivos de configuração acessíveis publicamente e scripts de sistema.
Credenciais Comprometidas:

1. **MySQL:** Encontrada em /config/database.php.txt (via Directory Listing).
- Senha: T3chC0rp_S3cr3t_2024!
2. **FTP Admin:** Encontrada no arquivo users.conf.
- Senha: ftp@dm1n123

3. **Root:** Encontrada no script /opt/backup_script.sh.
- Senha: r00t_P4ssw0rd_2024

Recomendação:
Remover todas as credenciais do código-fonte. Utilizar variáveis de ambiente ou cofres de senhas (Vaults).

🟠 VULN-03: Escalação de Privilégios (Privilege Escalation)

Descrição:
O usuário techcorp (comprometido via vazamento de senha) possuía permissão de leitura em arquivos críticos de automação.
Exploração:

1. Foi identificado o script /opt/backup_script.sh.
2. O script continha a credencial de root em texto claro.
3. Além disso, o histórico de comandos (.bash_history) do usuário root continha flags e evidências de atividades administrativas anteriores.

Recomendação:
Restringir as permissões de arquivos sensíveis (chmod 700) e auditar scripts de automação.

🟠 VULN-04: Information Disclosure (Backup & Docker)

Descrição:
O servidor expunha arquivos de infraestrutura, como o Dockerfile e backups antigos (backup_20240115.tar.gz), revelando a arquitetura interna de diretórios e locais de arquivos confidenciais (/srv/confidential).

Recomendação:
Configurar o servidor web para bloquear o acesso a extensões de arquivos sensíveis (.sh, .bak, .old, Dockerfile).

4. Plano de Ação Imediato

Para mitigar os riscos apresentados, recomenda-se seguir a seguinte ordem de prioridade:

1. **Imediato:** Alterar todas as senhas comprometidas (Root, MySQL, FTP, Usuário TechCorp).
2. **Imediato:** Remover o arquivo /config/database.php.txt e desabilitar a listagem de diretórios no Apache.
3. **Curto Prazo:** Corrigir a vulnerabilidade de LFI no panel.php.
4. **Médio Prazo:** Realizar uma varredura completa para remover outros arquivos de backup antigos do diretório público.