Relatório de Teste de Intrusão

CONFIDENCIAL

Controle de Versões

DATA	VERSÃO	AUTOR	ALTERAÇÃO
03/01/1900	1.0	NOME_COMPLETO	Versão Final

CONFIDENCIAL

Este documento contém informações proprietárias e confidenciais. Todos os dados encontrados durante os testes e apresentados neste documento foram tratados de forma a garantir sua privacidade e seu sigilo. A duplicação, redistribuição ou uso, no todo ou em parte, de qualquer forma, requer o consentimento da Business Corp.

Sumário

Aviso Legal

O *Pentest* foi realizado no período de **01/01/1900** até **02/01/1900**. As constatações e recomendações refletem as informações coletadas durante a avaliação e o estado do ambiente naquele momento, e não consideram quaisquer alterações realizadas posteriormente, fora desse período.

O trabalho desenvolvido pela DESEC SECURITY **NÃO** tem como objetivo corrigir possíveis vulnerabilidades nem proteger a CONTRATANTE contra ataques internos e externos. Nosso objetivo é levantar os riscos e recomendar formas de minimizá-los.

As recomendações sugeridas neste relatório devem ser testadas e validadas pela equipe técnica da empresa CONTRATANTE antes de serem implementadas no ambiente de produção. A DESEC SECURITY **não se responsabiliza** por essa implementação, nem por possíveis impactos que possam ocorrer em outras aplicações ou serviços.

Informações de Contato

NOME	CARGO	INFORMAÇÕES
BUSINESS CORP		
José dos Santos	Diretor de TI	Telefone: (00)01234-4321 Email: jsantos@grupobusinesscorp.com
CORPO TÉCNICO | DESEC SECURITY		
NOME_COMPLETO	Penetration Tester	Telefone: (xx)xxxxx-xxxx Email: candidato@desec.com.br

Sumário Executivo

A Desec Security avaliou a postura de segurança da Business Corp por meio de um Pentest Externo, realizado no período de 01/01/1900 até 02/01/1900. Os resultados das avaliações conduzidas a partir da internet demonstram que a empresa enfrenta sérios riscos cibernéticos, com vulnerabilidades de nível **CRÍTICO** que **comprometem a integridade, a disponibilidade e o sigilo de informações sensíveis**.

Principais Riscos

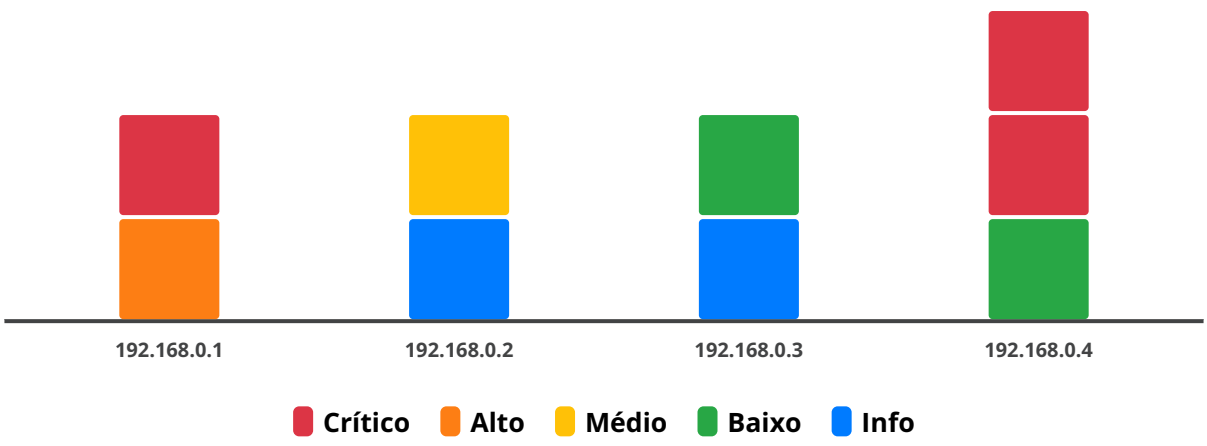

Figura 1 - Distribuição de riscos detalhados por sistema

RISCO	VULNERABILIDADES
CRÍTICO	Breve descrição da vulnerabilidade 1.2
CRÍTICO	Breve descrição da vulnerabilidade 4.1
CRÍTICO	Breve descrição da vulnerabilidade 4.2
ALTO	Breve descrição da vulnerabilidade 1.1

É altamente recomendável que a Business Corp resolva, com **alta prioridade**, as vulnerabilidades classificadas como risco crítico, a fim de evitar impactos negativos para o

negócio, considerando a criticidade das falhas encontradas e passíveis de exploração pela internet.

As tabelas abaixo resumem as principais vulnerabilidades e riscos encontrados durante os testes realizados. Ao final deste relatório, são propostas recomendações para mitigar os problemas identificados.

Descrição	Breve descrição da vulnerabilidade 1.2
Risco	**CRÍTICO**
Impacto	Breve descrição do impacto 3
Sistema	192.168.0.1
Recomendação	Consertar a vulnerabilidade 1.2

Descrição	Breve descrição da vulnerabilidade 4.1
Risco	**CRÍTICO**
Impacto	Breve descrição do impacto 4.1
Sistema	192.168.0.4
Recomendação	Consertar a vulnerabilidade 4.1

Descrição	Breve descrição da vulnerabilidade 4.2
Risco	**CRÍTICO**
Impacto	Breve descrição do impacto 4.2
Sistema	192.168.0.4
Recomendação	Consertar a vulnerabilidade 4.2

Introdução

A Desec Security foi contratada para conduzir uma avaliação de segurança (*Penetration Testing*) no ambiente digital da Business Corp.

A avaliação foi conduzida de maneira a simular um ciberataque à partir da internet com o objetivo de determinar o impacto que possíveis vulnerabilidades de segurança possam ter no que diz respeito à **integridade, disponibilidade e confidencialidade** das informações da empresa contratante.

Os testes foram realizados entre os dias **01/01/1900** e **02/01/1900** e este documento contém todos os resultados.

O método utilizado para a execução do serviço proposto segue rigorosamente as melhores práticas de mercado, garantindo a adequação às normas internacionais de segurança da informação, e os relatórios gerados apontam evidências quanto à segurança do ambiente definido no escopo.

Escopo

TIPO DE AVALIAÇÃO	DETALHES
Pentest Black Box Externo	192.168.0.1
Pentest Black Box Externo	192.168.0.2
Pentest Black Box Externo	192.168.0.3
Pentest Black Box Externo	192.168.0.4

De acordo com o combinado e acordado entre as partes, a avaliação escolhida foi do tipo **Black Box (sem conhecimento de informações)**, ou seja, a única informação oferecida pela CONTRATANTE foram os endereços IP informados na tabela acima.

Limitações do Escopo

As **limitações** impostas pela CONTRATANTE foram:

- Os testes devem encerrar caso seja possível comprometer algum host na rede interna
- Ataques DoS e DDoS (Negação de Serviço)
- Ataques de Engenharia Social

Metodologia

Para execução destes trabalhos, a Desec Security adotou a metodologia própria mesclada com padrões existentes e solidamente reconhecidos, tais como *PTES (Penetration Testing Execution Standard) e OWASP Top Ten* nas quais foram executados nas seguintes fases:

- Coleta de Informações
- Varredura
- Enumeração
- Exploração
- Pós Exploração
- Documentação

A fase de coleta de informações tem como objetivo mapear a superfície de ataque, identificando informações sobre blocos de ip, subdomínios e ambientes digitais de propriedade da Business Corp.

A fase de varredura consiste em identificar portas abertas, serviços ativos e possíveis mecanismos de defesa.

A fase de enumeração permite identificar detalhes sobre os serviços ativos, identificando possíveis versões, fornecedores, usuários e informações que possam ser úteis para o sucesso de um ataque.

A fase de exploração tem como objetivo explorar as possíveis vulnerabilidades identificadas nos serviços e sistemas identificados nas fases anteriores e obter acesso ao sistema.

A fase de pós exploração tem como objetivo aprofundar o ataque obtendo mais privilégios e aumentando o nível de acesso, se deslocando para outros sistemas a fim de controlar ou extrair dados mais sensíveis.

A fase de documentação consiste em relatar todos os resultados obtidos nas fases anteriores.

Narrativa da Análise Técnica

Os testes iniciaram no dia 01/01/1900 de posse apenas dos endereços informados pelo cliente.

HOST 192.168.0.1 - NOME DA MÁQUINA (SE HOUVER) (1)

Coleta de Informações

Texto Coleta de Informações 1

Vetores de Ataque

Texto Vetores de Ataque 1

Exploração de Vulnerabilidade

Texto Exploração de Vulnerabilidades 1

Flag de Usuário

Texto Flag de Usuário 1

Escalação de Privilégios

Texto Escalação de Privilégios 1

Flag de Root

Texto Flag de Root 1

HOST 192.168.0.2 - NOME DA MÁQUINA (SE HOUVER) (2)

Coleta de Informações

Texto Coleta de Informações. 2

Vetores de Ataque

Texto Vetores de Ataque. 2

Exploração de Vulnerabilidade

Texto exploração de Vulnerabilidades. 2

Flag de Usuário

Texto Flag de Usuário. 2

Escalação de Privilégios

Texto Escalação de Privilégios. 2

Flag de Root

Texto Flag de Root. 2

HOST 192.168.0.3 - NOME DA MÁQUINA (SE HOUVER) (3)

Coleta de Informações

Texto Coleta de Informações 3

Vetores de Ataque

Texto Vetores de Ataque 3

Exploração de Vulnerabilidade

Texto Exploração de Vulnerabilidades 3

Flag de Usuário

Texto Flag de Usuário 3

Escalação de Privilégios

Texto Escalação de Privilégios 3

Flag de Root

Texto Flag de Root 3

HOST 192.168.0.4 - NOME DA MÁQUINA (SE HOUVER) (4)

Coleta de Informações

Texto Coleta de Informações 4

Vetores de Ataque

Texto Vetores de Ataque 4

Exploração de Vulnerabilidade

Texto Exploração de Vulnerabilidades 4

Flag de Usuário

Texto Flag de Usuário 4

Escalação de Privilégios

Texto Escalação de Privilégios 4

Flag de Root

Texto Flag de Root 4

Conclusão da Análise Técnica

Conforme definido no escopo, os testes deveriam encerrar se fosse possível chegar até a rede interna da empresa através da internet.

LIMPEZA DE RASTROS

Após a coleta das informações e evidências acima demonstradas, restauramos os sistemas exatamente conforme encontramos, os usuários criados para a prova de conceito foram removidos, assim como, os exploits utilizados durante o ataque foram devidamente excluídos.

Vulnerabilidades e Recomendações

HOST	192.168.0.1
Descrição	Breve descrição da vulnerabilidade 1.1
Risco	**ALTO**
Impacto	Breve descrição do impacto 1.1
Referências	Links do CWE MITRE, OWASP ou CVE NIST 1.1

Problemas

Está vulnerável. 1.1

Recomendações

Consertar a vulnerabilidade. 1.1

HOST	192.168.0.1
Descrição	Breve descrição da vulnerabilidade 1.2
Risco	**CRÍTICO**
Impacto	Breve descrição do impacto 3
Referências	Links do CWE MITRE, OWASP ou CVE NIST 1.2

Problemas

Está vulnerável 1.2

Recomendações

Consertar a vulnerabilidade 1.2

HOST	192.168.0.2
Descrição	Breve descrição da vulnerabilidade 2.1
Risco	**MÉDIO**
Impacto	Breve descrição do impacto 2.1
Referências	Links do CWE MITRE, OWASP ou CVE NIST 2.1

Problemas

Está vulnerável 2.1

Recomendações

Consertar a vulnerabilidade 2.1

HOST	192.168.0.2
Descrição	Breve descrição da vulnerabilidade 2.2
Risco	**INFO**
Impacto	Breve descrição do impacto 2.2
Referências	Links do CWE MITRE, OWASP ou CVE NIST. 2.2

Problemas

Está vulnerável. 2.2

Recomendações

Consertar a vulnerabilidade. 2.2

HOST	192.168.0.3
Descrição	Breve descrição da vulnerabilidade 3.1
Risco	**BAIXO**
Impacto	Breve descrição do impacto 3.1
Referências	Links do CWE MITRE, OWASP ou CVE NIST 3.1

Problemas

Está vulnerável 3.1

Recomendações

Consertar a vulnerabilidade 3.1

HOST	192.168.0.3
Descrição	Breve descrição da vulnerabilidade 3.2
Risco	**INFO**
Impacto	Breve descrição do impacto 3.2
Referências	Links do CWE MITRE, OWASP ou CVE NIST 3.2

Problemas

Está vulnerável 3.2

Recomendações

Consertar a vulnerabilidade 3.2

HOST	192.168.0.4
Descrição	Breve descrição da vulnerabilidade 4.1
Risco	**CRÍTICO**
Impacto	Breve descrição do impacto 4.1
Referências	Links do CWE MITRE, OWASP ou CVE NIST 4.1

Problemas

Está vulnerável 4.1

Recomendações

Consertar a vulnerabilidade 4.1

HOST	192.168.0.4
Descrição	Breve descrição da vulnerabilidade 4.2
Risco	**CRÍTICO**
Impacto	Breve descrição do impacto 4.2
Referências	Links do CWE MITRE, OWASP ou CVE NIST 4.2

Problemas

Está vulnerável 4.2

Recomendações

Consertar a vulnerabilidade 4.2

HOST	192.168.0.4
Descrição	Breve descrição da vulnerabilidade 4.3
Risco	**BAIXO**
Impacto	Breve descrição do impacto 4.3
Referências	Links do CWE MITRE, OWASP ou CVE NIST 4.3

Problemas

Está vulnerável 4.3

Recomendações

Consertar a vulnerabilidade 4.3

Considerações Finais

A realização deste teste de segurança permitiu identificar vulnerabilidades e problemas de segurança que **poderiam causar um impacto negativo** aos negócios do cliente. Com isso podemos concluir que o teste atingiu o objetivo proposto.

Podemos concluir que a avaliação de segurança como o **teste de invasão** apresentado neste relatório é **fundamental** para identificar vulnerabilidades, testar e melhorar controles e mecanismos de defesa afim de garantir um bom grau de segurança da informação em seu ambiente digital.

Após a **CONTRATANTE** aplicar todas as correções sugeridas faremos um reteste nas vulnerabilidades apresentadas para comprovar que os problemas foram devidamente resolvidos.

Desde já agradecemos a Business Corp pela oportunidade em oferecer nossos serviços de segurança ofensiva.