Faculdade Adventista
BAHIA

# Relatório de Análise de Vulnerabilidades

Orientador: Jean do Ouro

**2022**

Eduardo Campos da Silva

Suellen Silva de Araújo

# PENTESTER

Realizar um teste de vulnerabilidade no site da Octopus Deploy.

Orientador(a): Prof Jean Ouro

**2022**

Sumário

## 1 Introdução

Foi realizado análises de vulnerabilidades na plataforma Octopus Deploy, conforme definido no "Escopo" deste relatório, cujos resultados serão abordados adiante.
Os testes de segurança foram realizados no período de 20/11/2022 a 30/11/2022 e seu objetivo foi identificar vulnerabilidades e propor recomendações para sua correção.
As fragilidades identificadas foram avaliadas e priorizadas de acordo com seu risco relativo e medidas para sua remediação também foram propostas.

## 2 Descrição da empresa

A Octopus é um servidor de automação de implantação para toda a equipe, projetado para facilitar a organização de versões e implantação de aplicativos, no local ou na nuvem.
Ela foi criada para profissionais em programação de banco de dados, setores de TI de empresas de diversos portes.

## 3 Objetivo

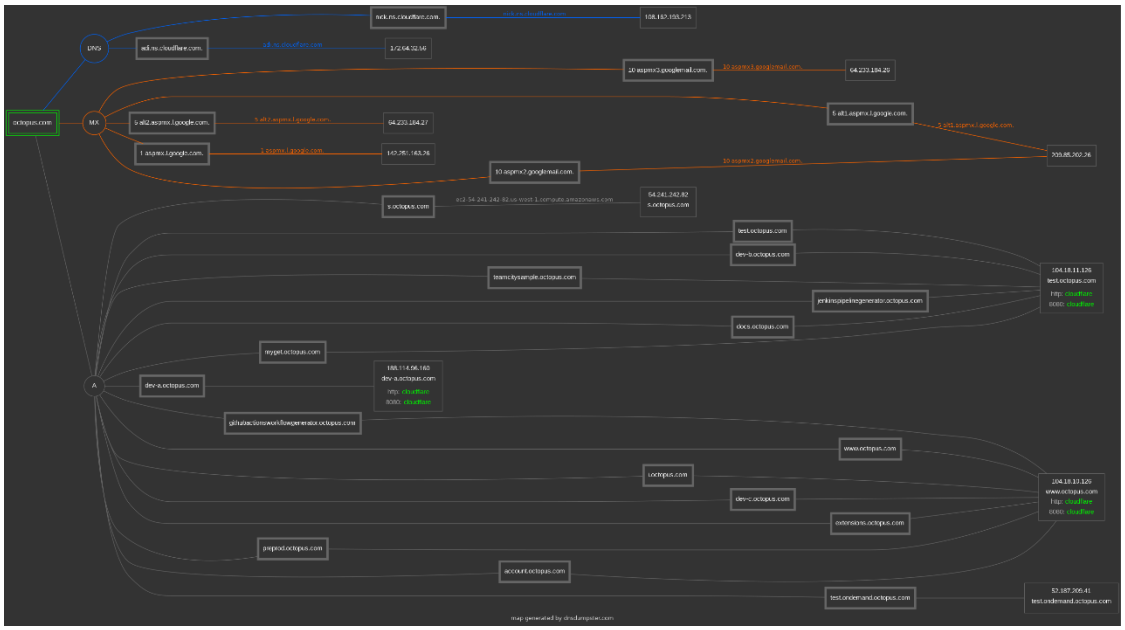
O objetivo geral: Realizar diversos testes para tentar descobrir vulnerabilidades no site “www.octopus.com” e em seus subdomínios

## 4 Escopo

Os testes realizados foram do tipo “White Box” e seguiram uma abordagem com base nos limites impostos pela empresa. Portanto, o principal objetivo alcançado através da adoção de metodologia, detalha adiante, que consistiu em priorizar e otimizar as validações realizadas, fornecendo garantias em termos de cobertura ao minimizar as chances de uma falha evidente escapar ao processo de análise. Ademais, foram reunidas informações sobre a

organização para que seja possível determinar o ambiente em que ela opera e a relevância desse ambiente para o processo de gestão de riscos de segurança da informação. Nesse sentido, foram realizados testes básicos de verificação de segurança em IPs obtidos indiretamente, isto é, IPs que são públicos e que foram conseguidos através de consulta ao “DNSdumpster” - ferramenta de pesquisa de domínio gratuitos que visam descobrir hosts relacionados a um domínio, conforme mostrados na Figura 1.

**Figura 1 - Mapeamento dos endereços IP para o domínio “www.octopus.com”.**




## 5 Limites

Todos os devidos cuidados foram tomados com base na especificação e critérios da empresa (Octopus Deploy) e as orientações do professor (FADBA) para não prejudicar o funcionamento da empresa, a fim de não causar impacto em seus sistemas ou interferir nos negócios diários da plataforma.

## 6 Não fazem parte do escopo:

Falsificação de conteúdo, Força bruta da página Login ou Esqueceu a senha e bloqueio de conta não aplicado, Cabeçalhos de segurança HTTP ausentes,

Especificamente(https://www.owasp.org/index.php/List_of_useful_HTTP_headers), Ataques CSRF que requerem conhecimento do token CSRF (por exemplo, ataques envolvendo uma máquina local), Nenhum teste de carga (DoS/DDoS, etc.) é permitido nos sites de teste, bombardeio por e-mail, Qualquer tipo de divulgação do código-fonte, Registros DMARC ausentes ou incorretos de qualquer tipo, Content-Security-Policy-Report-Only, O uso de scanners automatizados é proibido, Falsificação de solicitação entre sites de logout (saída CSRF).

**7 Além disso, não foi permito realização de testes nos seguintes alvos:**

- myget.octopus.com
- artifactorysample.octopus.com
- bamboosample.octopus.com
- jenkinssample.octopus.com
- teamcitysample.octopus.com
- nexussample.octopus.com

**8 Detalhamento dos Softwares Instalados**

Todos os testes foram realizados utilizando uma máquina virtual, VMware, usando o Kali Linux na versão 2022.3.

1. **Wafw00f**

   Este pacote identifica e imprime os produtos do Web Application Firewall (WAF) usando a seguinte logica:

   - Envia uma solicitação HTTP normal e analisa a resposta; isso identifica várias soluções WAF.
   - Se isso não for bem-sucedido, ele envia uma série de solicitações HTTP (potencialmente mal-intencionadas) e usa uma lógica simples para deduzir qual WAF é.

- Se isso também não for bem-sucedido, ele analisa as respostas retornadas anteriormente e usa outro algoritmo simples para adivinhar se um WAF ou solução de segurança está respondendo ativamente aos ataques.

## 2. Nmap

Nmap ('Network Mapper') é um utilitário gratuito e de código aberto (licença) para descoberta de rede e auditoria de segurança. Muitos sistemas e administradores de rede também o consideram útil para tarefas como inventário de rede, gerenciamento de agendas de atualização de serviço e monitoramento de host ou tempo de atividade de serviço.

## 3. Whois

Este pacote fornece um cliente de linha de comando para o protocolo WHOIS (RFC 3912), que consulta os servidores online em busca de informações, como detalhes de contato para domínios e atribuições de endereços IP. Ele pode selecionar de forma inteligente o serviço WHOIS apropriado para a maioria das consultas.

## 4. Dnsenum

Dnsenum é um script multithread para enumerar as informações DNS de um domínio e descobrir blocos de ip não contíguos. O objetivo principal do Dnsenum é reunir o máximo de informações possível sobre um domínio. O programa atualmente executa as seguintes operações:

1. Obtenha os endereços do host (registro A).
2. Obtenha os serviços nams (encadeados).
3. Obtenha o registro MX (encadeado).
4. Execute consultas axfr em servidores de nomes e obtenha versões BIND (encadeadas).

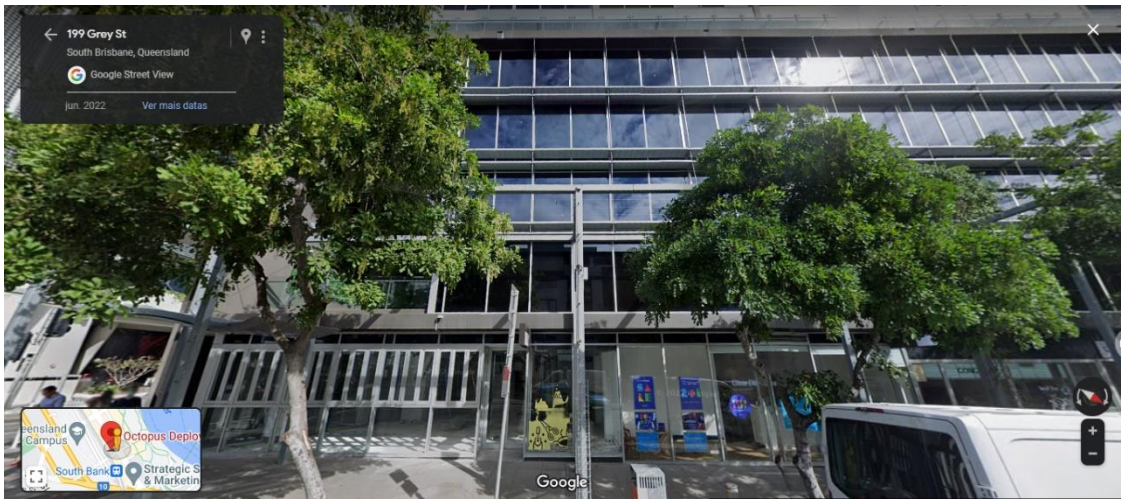
5. Obtenha nomes e subdomínios extras por meio do google scraping.
6. Subdomínios de força bruta do arquivo; também podem realizar recursão em subdomínios que possuem registro NS (todos encadeados).
7. Calcule intervalos de rede de domínio de classe C e execute consultas whois neles (encadeados).
8. Execute pesquisas reversas em netranges (classe C ou/e netranges whois) (encadeados).
9. Grave blocos de ip do arquivo domain_ips.txt.

**5. DNSdumpster.com**

É uma ferramenta GRATUITA de pesquisa de domínio que pode descobrir hosts relacionados a um domínio. E encontrar hosts visíveis da perspectiva dos invasores é uma parte importante do processo de avaliação de segurança.

## 9 Vulnerabilidades de engenharia social

Aconselhamos que a empresa crie uma cultura de preservação da identidade e ambiente empresarial. Ter política de segurança de segurança da informação bem cultivado dentro e fora da empresa. Promover treinamentos para evitar os riscos de um ataque causada por brechas humanas; trabalhar temas como de o que é Engenharia social? Como evitar cryptojacking E outros temas de segurança.




## 10 Vulnerabilidades relatadas pelos softwares

### 1. NMAP

Foram realizados testes com o intuito de:

- Vê serviços
- Versão do serviço
- Retorna informações
- Não pingar
- Não fazer resoluções reversa, agressivo
- Modo norma T3

Nada que comprometa a segurança da empresa foi encontrado nesse link “www.octopus.com”.

```
┌──(kali㉿DUDUH)-[~]
└─$ nmap  www.octopus.com
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-23 16:10 -03
Nmap scan report for www.octopus.com (104.18.26.53)
Host is up (0.031s latency).
Other addresses for www.octopus.com (not scanned): 104.18.27.53 2606:4700::6812:1a35 2606:4700::6812:1b35
Not shown: 995 filtered tcp ports (no-response)
PORT     STATE SERVICE
53/tcp   open  domain
80/tcp   open  http
443/tcp  open  https
8080/tcp open  http-proxy
8443/tcp open  https-alt

Nmap done: 1 IP address (1 host up) scanned in 8.65 seconds


┌──(kali㉿DUDUH)-[~]
└─$
```

Encontramos algumas portas abertas nessa URL.

2. **WAF00F**

   Foram realizados testes com o intuito de encontrar o firewall que o site utiliza, não foi possível ver o firewall da empresa.

3. **DNSENUM**

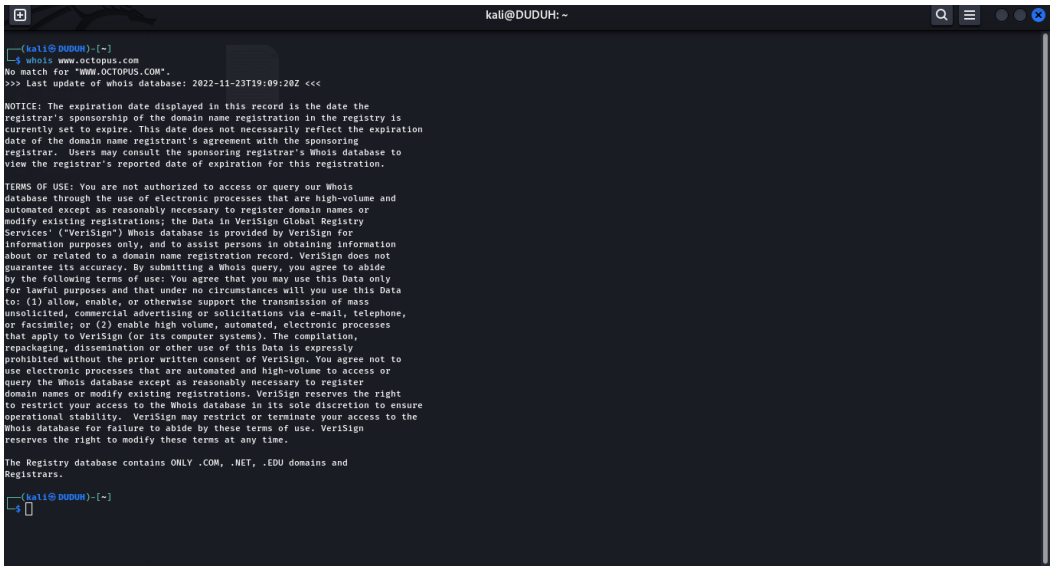
   Foram realizados testes com intuito de enumerar as informações DNS de um domínio e descobrir blocos de IPS não contíguos e reunir o máximo de informações possível sobre o domínio, mas o site bloqueou o software.

   Portanto, so foi obtido o host adress do link “www.octopus.com” .


4. **WHOIS**

   Foram realizados testes com intuito de consultar os servidores online em busca de informações, como detalhes de contato para domínios e atribuições de endereços IPs, mas o site bloqueou o software.

   Portanto não foi possível extrair informações através do mesmo.




## 11 Quadro Swot

## 12 Cronograma de atividades

| ATIVIDADE | DATA DA REALIZAÇÃO |
|---|---|
| Pesquisas e reconhecimento de sistemas computacionais envolvidos no escopo. | 21 de novembro de 2022 |
| Provas de conceito e conclusão dos testes. | 23 de novembro de 2022 |
| Avaliação de riscos e esboço do relatório. | 25 de novembro de 2022 |
| Conclusão e revisão final do relatório | 30 de novembro de 2022 |

## 13 E-mail comprometidos

- matthew.casperson@octopus.com
- bob.walker@octopus.com
- devops@octopus.com
- support@octopus.com

## 14 Sugestões para o contratante

1. **Política de senha**
   - Conter pelo menos 3 das 4 diretrizes abaixo:
     - Conter pelo menos uma letra maiúscula;
     - Conter pelo menos uma letra minúscula;
     - Conter números (0 a 9);
     - Conter símbolos, incluindo: ! @ # $ % ¨& * = + _ 0 ;

   Tamanho de no mínimo 8 caracteres;

   Não usar as 5 últimas senhas cadastradas;

   Mandatório alterar a senha a cada 180 dias;

2. **Números de tentativas sem restrições (LOCK OUT)**

A conta do usuário e bloqueada após 10 tentativas de acesso com senha errada;

A conta permanecerá bloqueada por 30 minutos. Após os 30 minutos, a conta e automaticamente desbloqueada para até 10 tentativas de acesso;

## 15 Termos de Pagamento

| Condições | | |
|---|---|---|
| Descrição | Valor/hora – R$ 128,03 | Período 18 Dias |
| | Hora | Valor |
| Pesquisas e reconhecimento de sistemas computacionais envolvidos no escopo | 30 Horas | R$ 3.840,9 |
| Provas de conceito e conclusão dos testes. | 12 horas | R$ 1.536,36 |
| Avaliação de riscos e esboço do relatório. | 8 horas | R$ 1.024,24 |
| Conclusão e revisão final do relatório | 8 horas | R$ 1.024,24 |
| **Valor total** | | R$ 7.425,74 |

# Anexo I

## DECLARAÇÃO DE AUTORIZAÇÃO DO CONTRATANTE

**INSTRUMENTO PARTICULAR DE PRESTAÇÃO DE SERVIÇOS DE TESTE DE INTRUSÃO (PENTEST)**

CONTRATATADA: **EDUARDO CAMPOS DA SILVA E SUELLEN SILVA DE ARAÚJO**, estabelecida **NA RODOVIA BR 101, KM 197, CAPOEIRUÇU, CACHOEIRA - BA**, inscrita no CNPJ sob **nº 05.115.657/0001-00**, neste ato representada pelo Sr., brasileiro**, EDUARDO CAMPOS DA SILVA**, Portador do RG **nº 00.000.000-3** e inscrito no CPF sob **nº 000.111.111-12**.

CONTRATANTE:**OCTOPUS DEPLOY**, estabelecida **G29F+M3 SOUTH BRISBANE, QUEENSLAND, 4101, AUTRÁLIA**, As partes acima identificadas têm, entre si, justo e certado o presente Contrato de Prestação de Serviços de Teste de Intrusão (Pentest), que se regerá pelas cláusulas seguintes e pelas condições descritas no presente.

**1) DO OBJETO**

O presente contrato tem por objeto, a realização de Teste de Intrusão (Pentest), a ser realizado pela CONTRATADA junto à CONTRATANTE, sendo que referidos testes somente poderão ser realizados nos dias e horários acordados, discriminados na Cláusula 2ª. A CONTRATADA conduzirá um PENETRATION TESTING contra Octopus.com.

Tais testes, consistem em simulações de ataques reais, resultando na descoberta de falhas da configuração e/ou vulnerabilidades. Vulnerabilidades estas que possam vir a permitir que a CONTRATANTE sofra impactos com ataques direcionados, perdendo a disponibilidade, integridade e confidencialidade de informações e sistemas.

## 2) DA EXECUÇÃO DOS SERVIÇOS

### 2.1 Escopo

O PENETRATION TESTING escolhido foi do tipo BLACKBOX (Sem conhecimento de informações), ou seja, a única informação oferecida pela CONTRATANTE foi uma URL.

O trabalho deve ser executado no seguinte escopo:

**https://www.octopus.com**

A CONTRATADA tem permissão de explorar o Escopo em sua Integralidade

### 2.2 Limitações do Escopo

A CONTRATANTE determina as seguintes limitações à realização dos referidos testes:

**ATIVIDADES/ATAQUES DE TESTES DE SEGURANÇA FÍSICA, WEBSITES DE FRONT-END DE MÍDIA PAGA, DDOS, PHISHING, SOFTWARE / EXTENSÕES MALICIOSOS, TESTES DE INSCRIÇÕES E AUTENTICAÇÕES, OUTROS DOMÍNIOS, SUBDOMÍNIOS OU CAMINHOS NÃO LISTADOS NA SEÇÃO DE DESTINOS, APLICATIVOS IOS E ANDROID, VARREDURAS AUTOMATIZADAS AGRESSIVAS, POIS PROVAVELMENTE IRÃO BLOQUEÁ-LO (POR AWS), ATAQUES QUE REQUEREM ACESSO FÍSICO AO DISPOSITIVO DE UM USUÁRIO, TODOS OS APLICATIVOS DE TERCEIROS OU BIBLIOTECAS / DEPENDÊNCIAS QUE NÃO ESTÃO SOB CONTROLE DA OCTOPUS DEPLOY, ATAQUES QUE REQUEREM ACESSO FÍSICO OU ADMINISTRATIVO À**

**HOSPEDAGEM DO SISTEMA, VULNERABILIDADES QUE AFETAM USUÁRIOS DE NAVEGADORES OU PLATAFORMAS DESATUALIZADOS, COOKIES AUSENTES SÃO SEGUROS OU HTTPONLY, CLICKJACKING E PROBLEMAS QUE SÓ PODEM SER EXPLORADOS POR MEIO DE CLICKJACKING, CABEÇALHOS DE SEGURANÇA HTTP AUSENTES, ESPECIFICAMENTE (HTTPS://OWASP.ORG/WWW-PROJECT-SECURE-HEADERS/), POR EXEMPLO.**

## 2.3 JANELA DE TESTES

Referidos testes, deverão ser realizados dentro do horário comercial, ou seja, de segunda à sexta-feira das 09:00 às 18 :00 horas.

Todas as fases do teste poderão ser acompanhadas e supervisionadas à critério da CONTRATANTE. Caso opte pelo acompanhamento, tal supervisão somente poderá ser realizada pelo responsável indicado e qualificado pela CONTRATANTE na Cláusula 3ª.

O teste de invasão deverá obedecer às seguintes fases:

1 Planejamento;

2 Descoberta;

3 Ataque (exploração);

4. Relatório de recomendações

5. Reunião para apresentação do relatório de recomendações e descrição das atividades executada durante o teste.

6. Reavaliação, novo teste pós remediação

7. Relatório final pós remediação

## 3) DAS RESPONSABILIDADES

A responsabilidade da CONTRATADA restringe-se apenas detectar e apontar os riscos existentes com relação à integridade e vulnerabilidade dos sistemas da CONTRATANTE e tão somente, apresentar formas para minimizá-los.

O trabalho desenvolvido pela CONTRATADA não tem como objetivo corrigir as possíveis vulnerabilidades, tampouco, proteger a CONTRATANTE contra-ataques internos e externos.

As recomendações feitas pela CONTRATADA de vem ser validadas antes de serem colocadas em produção, a CONTRATADA não se responsabilizará por erros de implementações.

Será de responsabilidade da CONTRATANTE, garantir a segurança ao acesso dos relatórios entregues pela CONTRATADA, bem como a indicação dos responsáveis pelo acompanhamento da realização dos referidos testes, conforme disposto no competente TERMO DE ACORDO DE CONFIDENCIALIDADE DE INFORMAÇÕES em sua cláusula 4ª, item 4.2, anexo á este instrumento, sendo a pessoa indicada pela CONTRATANTE, devidamente qualificada abaixo:

**Responsável nomeado pela CONTRATANTE:**

**Nome: OCTOPUS DEPLOY**

**TELEFONE: +1 512-823-0256**

**E-MAIL: sales@octopus.com**

**CIENTE: EDUARDO CAMPOS DA SILVA E SUELLEN SILVA DE ARAÚJO**

## 4) DO PRAZO CONTRATUAL

O presente contrato terá validade única e exclusivamente durante o período de realização da atividade contratada, ou seja, 40 (quarenta) horas testes, a partir da data da assinatura do presente contrato, podendo ser prorrogado por comum acordo entre as partes até a conclusão dos serviços contratados.

O presente contrato poderá ser rescindido ocorrendo pelo menos uma das seguintes situações:

a) por mútuo consentimento;

b) por qualquer das partes, mediante manifestação por escrito com antecedência mínima de 30 (trinta) dias, se a outra parte descumprir quaisquer obrigações assumidas no presente Contrato.

Fica estipulada a multa de 20% (vinte por cento), sobre o valor contratual, na qual incorrerá a parte que infringir qualquer uma das cláusulas deste contrato, ressalvada à parte inocente o direito de poder considerar simultaneamente rescindido o presente contrato, independentemente de qualquer outra formalidade judicial ou extrajudicial. A multa será sempre paga integralmente seja qual for o prazo decorrido do presente contrato ficando claro que o pagamento dessa multa não exime o pagamento de outras despesas inerentes ao contrato.

## 5) DO PAGAMENTO

Em contrapartida aos serviços contratados, a CONTRATANTE pagará à CONTRATADA, o valor **de R$ 7.425,74 (SETE MIL, QUATROCENTOS E VINTE E CINCO REAIS E SETENTA E QUATRO CENTAVOS)** por **58 HORAS** de serviços prestados, que serão pagos da seguinte forma:
A não efetivação do pagamento na forma e prazo pactuados acima, por culpa da CONTRATANTE fica estipulada a multa de 10% (dez por cento), juros moratórios à razão de 1% (um por cento) ao mês e correção monetária, além de outras despesas decorrentes de cobrança judicial ou extrajudicial.

## 6) DA AUTORIZAÇÃO

Para que seja alcançado o objetivo da atividade contratada e, para que esta possa ser realizada em sua integralidade, a CONTRATANTE, neste ato, AUTORIZA a CONTRATADA, a realizar o Teste de Intrusão (pentest), objeto do presente contrato, devendo-se sempre, ambas as partes, assegurar a

segurança das informações obtidas e fornecidas, bem como, cumprirem com seus deveres de confidencialidade de informações, devidamente pactuado entre as partes, conforme TERMO DE CONFIDENCIALIDADE DE INFORMAÇÕES, parte integrante do presente contrato.

## 7) DAS CONDIÇÕES GERAIS

Este Contrato constitui o único documento que regula os direitos e obrigações das partes, com relação aos serviços contratados, ficando expressamente cancelado e revogado, todo e qualquer entendimento ou ajuste porventura existente que não esteja explicitamente consignado neste Contrato.
Caso as partes envolvidas deixem de exigir em qualquer tempo o cumprimento de quaisquer cláusulas ou condições deste contrato, a parte prejudicada não ficará impedida de, quando o entender, fazer com que a parte inadimplente cumpra rigorosamente todas as condições contratuais.
Caso a CONTRATADA admitir em benefício do CONTRATANTE qualquer atraso no pagamento das mensalidades ou no cumprimento de qualquer outra obrigação contratual, essa tolerância não poderá ser considerada como alteração das condições deste contrato, pois se constituirá em ato de mera liberdade da CONTRATADA.
As partes contratantes elegem o foro da comarca de São Paulo, cujo foro é o único competente, com renúncia expressa de qualquer outro por mais privilegiado que seja, para dirimir as questões que porventura surgirem na execução do presente Contrato.
E, por estarem justos e contratados, cientes e de acordo com todas as cláusulas e condições do presente Contrato de Prestação de Serviços de Teste de Intrusão (Penterster), assinam este instrumento em duas vias para um só efeito na presença das testemunhas abaixo.

Cachoeira-BA, 1 de dezembro de 2022

**EDUARDO CAMPOS DA SILVA**

**SUELLEN SILVA DE ARAÚJO** **OCTOPUS DEPLOY**

CONTRATADA CONTRATANTE

**TESTEMUNHAS:**

Nome: _____

CPF: _____

Nome: _____

CPF: _____