Penetration Testing

QUESTIONÁRIO DE ESCOPO

Comercial e Restrito

Joas Antonio

1 INTRODUÇÃO

Este é um documento editável. Preencha os campos eletronicamente, salve o documento e envie-o de volta para

seu email

Este documento reunimos os requisitos para definir o escopo de seu Penetration Testing de maneira precisa e concisa. Seja o mais preciso e detalhado possível, pois isso nos ajudará a garantir que você obtenha o teste certo que melhor se adapta às suas necessidades.

Todos os detalhes fornecidos por você serão mantidos em sigilo. Se você acha que alguma informação é de natureza sensível, recomendamos colocar um NDA em vigor antes de nos fornecer as informações.

Algumas respostas afetarão os detalhes que você precisa fornecer mais tarde, portanto, leia cada pergunta na íntegra e certifique-se de preencher todas as seções aplicáveis. Se precisar de ajuda no preenchimento do questionário, não hesite em entrar em contato.

Se você tiver vários aplicativos ou várias infraestruturas para testar, preencha várias cópias deste documento com todas as informações apropriadas.

Joas Antonio

2 EMPRESA E INFORMAÇÕES DE CONTATO

2,1 Por favor, insira os seus dados e os da sua empresa

Nome da Empresa	
Endereço	
Seu Nome	
Seu E-mail	
Seu Telefone	

2,2 Você será o principal ponto de contato para este teste?

SIM		NÃO	

Se NÃO, forneça os dados de contato abaixo:

Nome do Contato	
E-mail de Contato	
Telefone de Contato	

3 PERGUNTAS DE ALTO NÍVEL

3,1 A conformidade está conduzindo os requisitos de teste?

SIM		NÃO	

Se você selecionou SIM, indique o (s) padrão (ões) que orientam o requisito para o teste.

Por favor selecione tudo que se aplica.

PCI-DSS	
FCA	
ISO	
GOVERNO (PSN, ITHC, ETC)	
LGPD/GDPR	
Outros	

3,2 Que tipo de teste (s) você exige?

Por favor selecione tudo que se aplica.

TESTE DE INFRAESTRUTURA	
TESTE DE APLICAÇÕES	
ENGENHARIA SOCIAL	
OUTROS (Declarar)	
INCERTO (Avisaremos)	

3,3 Quais são os seus motivos para este teste?

Por favor selecione tudo que se aplica.

ATENDER OS REQUISITOS DE CONFORMIDADE	
SOLICITAÇÃO DE CLIENTE	
QUEREMOS VALIDAR A NOSSA SEGURANÇA	
SOLICITAÇÃO INTERNA	

3,4 Que tipo de teste você exige?

Caixa preta os testes são onde o testador de penetração não sabe nada sobre a infraestrutura a ser testada. É mais indicativo de um ataque do mundo real, mas esse método nem sempre expõe todas as vulnerabilidades.

Caixa branca os testes são onde o testador de penetração tem acesso a informações completas e detalhadas sobre a infraestrutura a ser testada. Embora não seja tão realista quanto um teste de caixa preta, ele permite um teste muito completo.

Caixa cinza os testes são a forma mais popular de teste que faz uma abordagem equilibrada entre as caixas brancas e pretas. Um teste de caixa cinza revela apenas informações suficientes para realizar um teste metódico e completo, enquanto mantém o cenário relevante e realista.

CAIXA PRETA (BLACK BOX)	
CAIXA CINZA (GRAY BOX)	
CAIXA BRANCA (WHITE BOX)	
INCERTO (AVISAREMOS)	

3,5 Existe um período de tempo específico para a realização dos testes (datas ou horas do dia específicas)?

SIM		**NÃO**	

Se você selecionou SIM, por favor, detalhe as horas / datas necessárias:

Por favor selecione tudo que se aplica.

DIAS ÚTEIS	
FINAIS DE SEMANAS	
HORÁRIOS DE TRABALHO	
FORA DO HORÁRIO DE TRABALHO	
DATA ESPECIFICA	

3,6 O teste deve ser realizado em um ambiente ativo (de produção)?

SIM		**NÃO**	

4 PERGUNTAS DETALHADAS: INFRAESTRUTURA

Complete esta seção apenas se você selecionou 'Infraestrutura' na Questão 3.2 acima.

As próximas perguntas dependem das respostas que você forneceu anteriormente. Leia todas as perguntas cuidadosamente para se certificar de que não perdeu nenhuma seção aplicável.

4,1 Se você selecionou BLACK BOX na Questão 3.4

Como um teste de caixa preta não assume nada do ambiente, precisamos apenas dos detalhes mínimos para realizar o teste. Os testes de caixa preta duram apenas uma quantidade predeterminada de dias.

4.1.1 Forneça uma lista de nomes de host / endereços IP a serem testados.

Se precisar de mais espaço, inclua a lista completa em um documento separado, como uma planilha.

HOSTNAME / IP ADDRESSES

HOSTNAME / IP ADDRESSES

4.1.2 Liste quaisquer outros detalhes que possamos considerar relevantes

DETALHES ADICIONAIS

4,2 Se você selecionou WHITE BOX ou GREY BOX na Questão 3.4

4.2.1 Forneça informações sobre o ambiente a ser testado. Se for IaaS, inclua firewalls, balanceadores de carga, roteadores, switches, servidores, armazenamento e outros dispositivos físicos. Se for PaaS, forneça detalhes sobre o PaaS e como está sendo usado e consumido:

Se precisar de mais espaço, inclua a lista completa em um documento separado, como uma planilha.

TIPO DE EQUIPAMENTO	DETALHES

DETALHES PaaS

4.2.2 Forneça uma lista de nomes de host / endereços IP a serem testados:

Se precisar de mais espaço, inclua a lista completa em um documento separado, como uma planilha.

HOSTNAME / IP ADDRESSES

HOSTNAME / IP ADDRESSES

4,3 Se você selecionou GREY BOX na Questão 3.4, você precisa de um teste INTERNO ou EXTERNO?

interno os testes simulam um ataque que já ultrapassou seu perímetro de segurança. Isso descobre o que um invasor pode fazer internamente, como mover-se entre sistemas e redes. Ele também simula o que um ataque interno pode fazer.

Externo os testes simulam a capacidade de um invasor de obter acesso à sua rede interna e infraestrutura de fora do perímetro de segurança.

INTERNO (vá para 4.3.A)		**EXTERNO (vá para 4.3.B)**	

4.3.A Se você respondeu INTERNO à pergunta 4.3

Você prefere que o teste seja realizado em suas instalações ou fornecendo uma VPN segura no ambiente interno?

NAS INSTALAÇÕES		**VIA VPN**	

4.3.B Se você respondeu EXTERNAL à pergunta 4.3

4.3.B.1 Que tipo de ambiente hospedado você precisa testar?

TIPO DE HOSPEDAGEM	NOME DO PROVEDOR DE HOSPEDAGEM
PUBLIC IaaS (EG AWS, AZURE)	
PaaS PÚBLICO	
NAS INSTALAÇÕES	
NUVEM PRIVADA	
OUTROS (DECLARAR)	

4.3.B.2 Você tem controles de segurança que precisam permitir que nossos endereços IP sejam colocados na lista de permissões antes que o teste possa começar?

SIM		**NÃO**	

Se você selecionou SIM a 4.3.B.2 (acima), detalhe o que são.

DETALHES DE SEGURANÇA

5 PERGUNTAS DETALHADAS: APLICAÇÕES

Apenas complete esta seção se você selecionou 'Aplicação' na Questão 3.2 acima.

As próximas perguntas dependem das respostas que você forneceu anteriormente. Leia todas as perguntas cuidadosamente para se certificar de que não perdeu nenhuma seção aplicável.

5,1 É um único aplicativo ou vários aplicativos a serem testados?

ÚNICO		MÚLTIPLO (QUANTIDADE)	

5,2 Tipo de aplicação

Por favor selecione tudo que se aplica.

REDE	
MOBILE	
DESKTOP	
OUTROS	

5,3 Para que serve o aplicativo? Forneça uma descrição detalhada, incluindo a funcionalidade do aplicativo, componentes principais e outras informações relevantes.

DESCRIÇÃO DA APLICAÇÃO

5,4 Quais frameworks / linguagens foram usados para construir o aplicativo?

FRAMEWORKS/LINGUAGENS USADAS

5,5 O aplicativo está acessível na web?

SIM		NÃO	

5,6 Se você selecionou o aplicativo WEB na pergunta 5.2.1 (acima), informe-nos o nome do host / endereço IP do aplicativo hospedado:

HOSTNAME/IP ADDRESS

5,7 Se você selecionou o aplicativo MOBILE na pergunta 5.2.1 (acima), ele está disponível gratuitamente para download?

Por favor selecione tudo que se aplica.

NÃO DISPONÍVEL	
DISPONÍVEL VIA:	
GOOGLE PLAY	
IOS APP STORE	
AMAZON APP STORE	
OUTRO (POR FAVOR, ESPECIFIQUE)	

Se você respondeu NÃO DISPONÍVEL acima, detalhe como você nos fornecerá o aplicativo

DETALHES DO PROVISIONAMENTO DA APLICAÇÃO

5,8 Que tipo de teste você exige?

AUTENTICADO	
NÃO AUTENTICADO	
INCERTO (NÓS ACONSELHAREMOS)	

6 PERGUNTAS DETALHADAS: ENGENHARIA SOCIAL

Apenas complete esta seção se você selecionou 'Engenharia Social' na Questão 3.2 acima.

As próximas perguntas dependem das respostas que você forneceu anteriormente. Leia todas as perguntas cuidadosamente para se certificar de que não perdeu nenhuma seção aplicável.

6,1 Que tipo de engenharia social você exige?

Por favor selecione tudo que se aplica.

PHISHING	
VISHING	
BYPASS DE SEGURANÇA FÍSICA	

6,2 Se você selecionou PHISHING ou VISHING na Questão 6.1 (acima), as informações sobre os usuários a serem alvos serão fornecidas antes do teste?

SIM		**NÃO**	

6.2.1 Se você selecionou SIM, informe-nos o número de usuários.

INFORME O NÚMERO DE USUÁRIOS	

6,3 Se você selecionou ANULAÇÃO DE SEGURANÇA FÍSICA na Questão 6.1 (acima), descreva o tipo de teste que deseja realizar.

Por exemplo, passar pela segurança da portaria e obter acesso a um edifício ou área específica

BYPASS DE SEGURANÇA FÍSICA

7 INFORMAÇÕES ADICIONAIS

Existe alguma outra informação que você acha que devemos saber? Talvez você queira expandir alguma de suas respostas ou fornecer detalhes adicionais que não solicitamos explicitamente. Use esta caixa:

INFORMAÇÕES ADICIONAIS