



Security
Standards Council®

Padrão: Padrão de Segurança de Dados do PCI (PCI DSS)
Versão: 1.1
Data: Setembro de 2017
Autor: Grupo de Interesse Especial para Guia do Teste de Penetração do Conselho de Padrões de Segurança da PCI

Suplemento de Informações: Guia do Teste de Penetração

Alterações no documento

Data	Versão do documento	Descrição	Páginas
Março de 2015	1.0	Primeira versão	Todas
Setembro de 2017	1.1	Vários esclarecimentos, incluindo: <ul style="list-style-type: none">• Esclarecida a intenção de “engenharia social” na terminologia.• Esclarecida a orientação sobre testes de caixa preta.• Seção 2.2 reestruturada para melhor fluxo e texto mais claro descrevendo a intenção do Requisito 11.3 do PCI DSS.• Orientação expandida relacionada a APIs back-end.• Referências atualizadas para recursos do PCI SSC.• Pequenas atualizações gramaticais.	Vários

Índice

1	Introdução	4
1.1	Objetivo	4
1.2	Público-alvo	4
1.3	Terminologia	4
1.4	Navegando neste documento	5
2	Componentes do teste de penetração	6
2.1	Qual é a diferença entre um teste de penetração e uma varredura de vulnerabilidade?	6
2.2	Escopo	7
2.2.1	Teste de penetração externa	8
2.2.2	Teste de penetração interna	8
2.2.3	Testando Controles de Segmentação	8
2.2.4	Sistemas críticos	9
2.3	Teste de camada de aplicativo e camada de rede	9
2.3.1	Autenticação	9
2.3.2	Aplicativos compatíveis com PA-DSS	9
2.3.3	Aplicativos Web	10
2.3.4	Ambiente de teste separado	10
2.4	Verificações de segmentação	10
2.5	Engenharia social	11
2.6	O que é considerado uma “mudança significativa”?	11
3	Qualificações de um testador de penetração	12
3.1	Certificações	12
3.2	Experiência anterior	12
4	Metodologia	14
4.1	Pré-engajamento	14
4.1.1	Escopo	14
4.1.2	Documentação	14
4.1.3	Regras de engajamento	15
4.1.4	Ambientes na nuvem/hospedados por terceiros	16
4.1.5	Critérios de sucesso	16
4.1.6	Análise de ameaças e vulnerabilidades anteriores	16
4.1.7	Evite a interferência de varredura em dispositivos de segurança.	17
4.2	Engajamento: Teste de Penetração	17
4.2.1	Camada de aplicativo	18
4.2.2	Camada de rede	18
4.2.3	Segmentação	19

4.2.4	O que fazer quando os dados do titular do cartão são encontrados	19
4.2.5	Pós-exploração	19
4.3	Pós-engajamento	19
4.3.1	Melhores práticas de remediação	19
4.3.2	Novo teste de vulnerabilidades identificadas	20
4.3.3	Limpeza do ambiente	20
4.4	Recursos adicionais	20
5	Relatórios e documentação	21
5.1	Relatório de vulnerabilidade identificada	21
5.1.1	Atribuição de uma pontuação de gravidade	21
5.1.2	Referências padrão do setor	22
5.2	Diretrizes para relatórios	22
5.2.1	Descrição do relatório do teste de penetração	22
5.2.2	Considerações sobre o novo teste e esboço de relatório	23
5.3	Retenção de evidências	24
5.3.1	O que é considerado evidência?	24
5.3.2	Retenção	24
5.4	Ferramenta de avaliação do relatório de teste de penetração	25
6	Estudos de caso/Exemplos de escopo	27
6.1	Estudo de caso de teste de penetração de comércio eletrônico	27
6.2	Estudo de caso do teste de penetração do provedor de hospedagem	30
6.3	Estudo de caso de teste de penetração no comerciante de varejo	35
Anexo A: Tabela de referência rápida para orientação sobre requisitos de teste de penetração do PCI DSS		40
Agradecimentos		41
Sobre o PCI Security Standards Council		43

1 Introdução

1.1 Objetivo

Este suplemento de informações fornece orientações gerais e diretrizes para testes de penetração. A orientação se concentra no seguinte:

- **Componentes de teste de penetração:** Compreensão dos diferentes componentes que compõem um teste de penetração e a diferença para uma varredura de vulnerabilidade, incluindo escopo, aplicação e teste de camada de rede, verificações de segmentação e engenharia social.
- **Qualificações de um testador de penetração:** Determinar as qualificações de um testador de penetração, interno ou externo, através de sua experiência e certificações.
- **Metodologias de teste de penetração:** Informações detalhadas relacionadas às três partes principais de um teste de penetração: pré-engajamento, engajamento e pós-engajamento.
- **Diretrizes para relatórios de testes de penetração:** Orientação para desenvolver um abrangente relatório de teste de penetração, que inclua as informações necessárias para documentar o teste e uma lista de verificação, que possa ser usada pela organização ou pelo avaliador para verificar se o conteúdo necessário está incluído.

As informações contidas neste documento destinam-se à orientação suplementar e não substituem, anulam ou estendem os requisitos do PCI DSS. A versão atual do PCI DSS, no momento da publicação, é v3.2; no entanto, os princípios e práticas gerais oferecidos aqui também podem ser aplicáveis a outras versões do PCI DSS.

1.2 Público-alvo

Esta orientação é destinada a entidades que precisam conduzir um teste de penetração, usando um recurso interno ou externo. Além disso, este documento destina-se a empresas especializadas na oferta de serviços de teste de penetração e aos assessores que ajudam a definir o escopo dos testes de penetração e a revisar os relatórios finais de testes. A orientação é aplicável a organizações de todos os tamanhos, orçamentos e setores.

1.3 Terminologia

Os seguintes termos são usados ao longo deste documento:

- **Teste de camada de aplicativo:** Testes que normalmente incluem sites, aplicativos da web, thick clients ou outros aplicativos.
- **Teste de caixa preta:** Testes realizados sem conhecimento prévio da estrutura interna/projeto/implementação do objeto sendo testado.
- **Sistema comum de pontuação de vulnerabilidade (Common Vulnerability Scoring System, CVSS):** Fornece uma estrutura aberta para comunicar as características e os impactos das vulnerabilidades de TI.
- **Teste de caixa cinza:** Testes realizados com conhecimento parcial da estrutura interna/projeto/implementação do objeto sendo testado.

- **Banco de dados nacional de vulnerabilidade (National Vulnerability Database, NVD):** O repositório do governo dos EUA de dados de gerenciamento de vulnerabilidade baseados em padrões. Esses dados permitem a automação da gestão de vulnerabilidades, medição de segurança e conformidade (por exemplo, FISMA).
- **Teste de camada de rede:** Testes que normalmente incluem testes externos/internos de redes (LANS/VLANS), entre sistemas interconectados e redes sem fio.
- **Equipe, testador de penetração ou testador:** O(s) indivíduo(s) que conduzem o teste de penetração para a entidade. Podem ser um recurso interno ou externo à entidade.
- **Engenharia social:** Manipulação ou engano de indivíduos para divulgar informações confidenciais ou pessoais.
- **Teste de caixa branca:** Testes realizados com conhecimento da estrutura interna/projeto/implementação do objeto sendo testado.

1.4 Navegando neste documento

Este documento é organizado de forma a ajudar o leitor a entender melhor o teste de penetração, em um sentido holístico. Começa fornecendo histórico e definições para tópicos comuns a todos os esforços de teste de penetração (incluindo o escopo do teste, sistemas críticos para testar, aplicações e inclusões de teste de camada de rede etc.). O documento depois apresenta orientação prática sobre a seleção de um testador de penetração, metodologias que são usadas antes, durante e depois de um teste, diretrizes para relatar e avaliar os resultados do teste. O documento conclui com estudos de caso que tentam ilustrar os conceitos apresentados neste suplemento.

O Anexo A fornece uma tabela de referência rápida para seções específicas deste documento, quando a orientação sobre um requisito específico do PCI DSS pode ser encontrada. Isso pode ser útil para quem deseja correlacionar rapidamente os requisitos e diretrizes de teste de penetração apresentados no Requisito 11.3 do PCI DSS.

2 Componentes do teste de penetração

As metas dos testes de penetração são:

1. Determinar se e como um usuário mal-intencionado pode obter acesso não autorizado a ativos que afetam a segurança fundamental do sistema, arquivos, logs e/ou dados do titular do cartão.
2. Confirmar que os controles aplicáveis exigidos pelo PCI DSS — como escopo, gerenciamento de vulnerabilidades, metodologia e segmentação — estão em vigor.

Há três tipos de testes de penetração: caixa preta, caixa branca e caixa cinza. Em uma avaliação de caixa preta, o cliente não fornece nenhuma informação antes do início do teste. Em uma avaliação de caixa branca, a entidade pode fornecer ao testador de penetração os detalhes completos da rede e dos aplicativos. Para avaliações de caixa cinza, a entidade pode fornecer detalhes parciais dos sistemas de destino. Os testes de penetração do PCI DSS são normalmente realizados como avaliações de caixa branca ou caixa cinza. Esses tipos de avaliações produzem resultados mais precisos e fornecem um teste mais abrangente da postura de segurança do ambiente do que uma avaliação pura da caixa preta. Realizar uma avaliação de caixa preta, quando a entidade não fornece detalhes dos sistemas de destino antes do início do teste, pode exigir mais tempo, dinheiro e recursos para que os resultados atendam aos requisitos do PCI DSS.

2.1 Qual é a diferença entre um teste de penetração e uma varredura de vulnerabilidade?

As diferenças entre testes de penetração e varredura de vulnerabilidade, conforme exigido pelo PCI DSS, podem ser resumidas da seguinte forma:

	Varredura de vulnerabilidades	Teste de penetração
Finalidade	Identificar, classificar e relatar vulnerabilidades que, se exploradas, podem resultar em um comprometimento intencional ou não intencional de um sistema.	Identificar modos de explorar as vulnerabilidades a fim de enganar ou anular os recursos de segurança dos componentes do sistema.
Quando	Pelo menos trimestralmente, e após mudanças significativas ¹ .	Pelo menos uma vez por ano, e mediante mudanças significativas ² .
Como	Normalmente, uma variedade de ferramentas automatizadas combinadas com verificação manual de problemas identificados.	Um processo manual que pode incluir o uso de varredura de vulnerabilidades ou outras ferramentas automatizadas, resultando em um relatório abrangente.

¹ Consulte a Seção 2.6 deste documento para obter orientação sobre mudanças significativas.

² Algumas entidades podem ter de realizar testes de penetração com mais frequência. Consulte a versão atual do PCI DSS para entender os requisitos específicos.

	Varredura de vulnerabilidades	Teste de penetração
Relatórios	<p>Riscos potenciais apresentados por vulnerabilidades conhecidas, classificados de acordo com as pontuações base NVD/CVSS associadas a cada vulnerabilidade.</p> <p>Para o PCI DSS, as varreduras de vulnerabilidade externa devem ser realizadas por um ASV e os riscos classificados de acordo com o CVSS. As varreduras internas de vulnerabilidade podem ser realizadas por pessoal qualificado (não requer um ASV) e riscos classificados de acordo com o processo de classificação de risco da organização, conforme definido no Requisito 6.1 do PCI DSS.</p> <p>Uma varredura de vulnerabilidade externa é conduzida de fora da organização alvo. Uma varredura de vulnerabilidade interna é conduzida de dentro da organização alvo.</p>	<p>Descrição de cada problema verificado e/ou possível problema descoberto. Riscos mais específicos que a vulnerabilidade pode representar, incluindo métodos específicos como e até que ponto ele pode ser explorado. Exemplos de vulnerabilidades incluem, entre outros, injeção de SQL, escalonamento de privilégio, script entre sites ou protocolos obsoletos.</p>
Duração	<p>Quantidade relativamente curta de tempo, tipicamente vários segundos a vários minutos por host digitalizado.</p>	<p>Os engajamentos podem durar dias ou semanas, dependendo do escopo do teste e do tamanho do ambiente a ser testado. Os testes podem aumentar em tempo e complexidade, se os esforços revelarem um escopo adicional.</p>

2.2 Escopo

PCI DSS define o ambiente de dados do titular do cartão (CDE), como “pessoas, processos e tecnologias que armazenam, processam ou transmitem os dados do titular do cartão ou dados de autenticação confidenciais”.

O escopo de um teste de penetração, conforme definido no Requisito 11.3 do PCI DSS, inclui todo o perímetro do CDE e quaisquer sistemas críticos. Isso se aplica tanto ao perímetro externo (superfícies de ataque voltadas para o público) quanto ao perímetro interno do CDE (superfícies de ataque LAN-LAN).

O escopo dos testes pode incluir locais de dados do titular do cartão, aplicativos que armazenam, processam ou transmitem dados do portador do cartão, conexões de rede críticas, pontos de acesso e outros alvos apropriados para a complexidade e o tamanho da organização. Isso deve incluir recursos e ativos utilizados pelo pessoal para manter sistemas no CDE ou para acessar dados do titular do cartão, pois o comprometimento desses ativos poderia permitir que um invasor obtenha credenciais com acesso ou uma rota para o CDE.

Todos os testes de penetração devem ser conduzidos apenas conforme definido pelas regras de engajamento acordadas por ambas as partes. Consulte a Seção 4.1.3, “Regras de engajamento”.

2.2.1 *Teste de penetração externa*

O escopo de um teste de penetração externa é o perímetro externo exposto do CDE e sistemas críticos conectados ou acessíveis a infraestruturas de rede pública. Deve avaliar qualquer acesso exclusivo ao escopo das redes públicas, incluindo serviços que tenham acesso restrito a endereços de IP externos individuais. Os testes devem incluir avaliações de camada de aplicativo e camada de rede. Os testes de penetração externa também incluem vetores de acesso remoto, como conexões dial-up e VPN.

2.2.2 *Teste de penetração interna*

O escopo do teste de penetração interna é o perímetro interno do CDE e sistemas críticos, pela perspectiva da rede interna. Os testes devem incluir avaliações de camada de aplicativo e camada de rede.

Quando o CDE for também a única rede interna e não houver perímetro interno de CDE, o escopo dos testes normalmente se concentrará nos sistemas críticos. Por exemplo, as atividades de teste podem incluir a tentativa de ignorar controles de acesso interno destinados a impedir o acesso não autorizado ou o uso de sistemas que armazenam, processam ou transmitem CHD (dados do portador do cartão) daqueles que não fazem.

Nos casos em que houver um perímetro interno de CDE, o escopo dos testes precisará considerar o perímetro CDE, bem como os sistemas críticos dentro e fora do CDE. Por exemplo, o teste pode tentar explorar caminhos de acesso permitidos de sistemas em um segmento de rede interna no CDE.

Quando o acesso ao CDE for obtido como resultado do teste, o escopo do teste de penetração pode permitir que o testador continue explorando dentro e além da rede e adiante o ataque contra outros sistemas no CDE, e também pode incluir testar qualquer controle de prevenção de ex-filtração de dados (prevenção de perda de dados) que esteja em vigor.

Em todos os casos, o escopo dos testes internos deve considerar o ambiente específico e a avaliação de risco da entidade. As entidades são incentivadas a consultar seu avaliador e o testador de penetração, para garantir que o escopo do teste de penetração seja suficiente e apropriado para o seu ambiente específico.

2.2.3 *Testando Controles de Segmentação*

A intenção da segmentação é evitar que sistemas fora do escopo possam se comunicar com sistemas no CDE ou afetar a segurança do CDE. Quando implementado adequadamente, um componente de sistema segmentado (fora do escopo) não pode afetar a segurança do CDE, mesmo que um invasor obtenha controle do sistema fora do escopo.

Se controles de segmentação forem implementados, é necessário testar os controles para confirmar que os métodos de segmentação estejam funcionando conforme pretendido e que todos os sistemas e redes fora do escopo estejam isolados dos sistemas no CDE. O escopo dos testes de segmentação deve considerar quaisquer redes e sistemas considerados fora do escopo, para o PCI DSS verificar se eles não têm conectividade com o CDE e não podem ser usados para afetar a segurança do CDE.

A intenção desta avaliação é validar a eficácia dos controles de segmentação separando os ambientes fora do escopo do CDE e garantir que os controles estejam operando conforme pretendido.

2.2.4 *Sistemas críticos*

O termo “sistemas críticos” é usado no PCI DSS para referenciar sistemas envolvidos no processamento ou proteção dos dados do portador do cartão. O PCI DSS fornece exemplos de sistemas críticos que podem ser afetados por vulnerabilidades identificadas, incluindo “sistemas de segurança, dispositivos voltados ao público e sistemas, bancos de dados e outros sistemas que armazenam, processam ou transmitem dados do titular do cartão” (Requisito 6.1). No entanto, para fins do teste de penetração, pode haver sistemas adicionais fora dos limites CDE que poderiam afetar a segurança do CDE. Esses sistemas também devem ser considerados sistemas críticos. Exemplos comuns de sistemas críticos relevantes para um teste de penetração podem incluir: sistemas de segurança (por exemplo, firewalls, sistemas de detecção de invasões/sistemas de prevenção de intrusão [IDS/IPS], servidores de autenticação, servidores de redirecionamento de comércio eletrônico etc.), ou quaisquer ativos utilizados por usuários privilegiados para dar suporte e gerenciar o CDE. Observe que sistemas críticos são definidos pela entidade, pois cada ambiente é diferente.

2.3 *Teste de camada de aplicativo e camada de rede*

Qualquer software escrito ou especificamente criado para a organização que faça parte do escopo do teste de penetração deve estar sujeito ao teste de penetração da camada de rede e da aplicação. Esta avaliação ajuda a identificar defeitos de segurança que resultam do projeto ou configuração insegura do aplicativo, ou de empregar práticas de codificação inseguras ou defeitos de segurança que possam resultar da implementação, configuração, uso ou manutenção insegura do software.

A correção das vulnerabilidades identificadas durante uma avaliação de camada de aplicativo pode envolver redesenhar ou reescrever código inseguro. A remediação das vulnerabilidades identificadas durante uma avaliação de camada de rede normalmente envolve reconfigurar ou atualizar o software. Em alguns casos, a remediação pode incluir a implantação de uma alternativa segura para o software inseguro.

2.3.1 *Autenticação*

Se o aplicativo exigir autenticação de usuário para o software personalizado, o teste deve ser realizado em relação a todas as funções ou tipos de acesso assumidos por essas partes. Além disso, os testes devem ser realizados para qualquer função ou tipo de acesso que *não* tenha autorização explícita para os dados do titular do cartão para verificar se as contas sem acesso não podem comprometer tais dados.

Para clientes que executam aplicativos em servidores multitenant que fornecem acesso aos dados do portador do cartão a clientes, testes autenticados devem ser realizados para garantir que o acesso do cliente seja restrito adequadamente apenas aos seus próprios dados do portador do cartão. O cliente deve fornecer ao testador de penetração credenciais que tenham permissão(s) equivalente(s) como usuário do cliente, para permitir que o testador de penetração determine se essas credenciais permitem acesso aos dados além dos dados da entidade.

2.3.2 *Aplicativos compatíveis com PA-DSS*

Se um aplicativo de pagamento for validado pelo PA-DSS, a funcionalidade do aplicativo não precisa ser testada como parte da validação de conformidade do PCI DSS da entidade. No entanto, a implementação do aplicativo precisa ser testada. Isso inclui o sistema operacional e quaisquer serviços expostos, mas não a funcionalidade do aplicativo de pagamento (por exemplo, autenticação, gerenciamento de chaves, processamento de transações etc.), uma vez que isso foi validado como parte da validação do aplicativo PA-DSS.

2.3.3 *Aplicativos Web*

É comum para um ambiente hospedar um aplicativo web que não tenha sido especificamente codificado para a organização, como interfaces comerciais, de web-mail prontas para uso, ferramentas de compartilhamento de documentos, serviços de transferência de arquivos, interfaces administrativas de dispositivos de rede etc. Nesses casos, o aplicativo da Web normalmente não precisa de um teste de penetração de camada de aplicativo, pois a entidade não é responsável pelo código-fonte deste tipo de software. Em vez disso, o testador deve realizar um teste de camada de rede e garantir que o software foi implementado, configurado e está sendo mantido de forma segura (desabilitando ou desinstalando serviços não utilizados, bloqueando portas não utilizadas, aplicando atualizações atuais etc.).

2.3.4 *Ambiente de teste separado*

Por causa da natureza e da intenção dos testes de penetração, tais testes em um ambiente de produção durante o horário comercial normal podem afetar as operações comerciais, e tentativas de evitar interrupções podem aumentar o tempo, os recursos e a complexidade dos testes. Isso é especialmente importante para sistemas de alta disponibilidade, que podem ser afetados por testes de penetração em um ambiente de produção. Para evitar interrupções e acelerar o teste, um ambiente separado idêntico ao ambiente de produção pode ser usado para testes, em vez do ambiente de produção. O testador de penetração precisaria garantir os mesmos controles de aplicação e camada de rede, uma vez que a produção existe no ambiente de teste. Isso pode ser realizado através de métodos para mapear o ambiente de produção para verificar se ele corresponde ao ambiente de teste. Isso deve ser incluído nas regras de engajamento. Todas as vulnerabilidades exploráveis identificadas durante o teste devem ser corrigidas nos sistemas de produção e os testes devem ser repetidos, para verificar se os pontos fracos de segurança foram abordados.

2.4 Verificações de segmentação

O Requisito 11.3.4 do PCI DSS requer que os testes de penetração validem se os controles/métodos de segmentação estejam operacionais, efetivos e isolam todos os sistemas fora de escopo dos sistemas no CDE.

Portanto, recomenda-se uma abordagem robusta para o teste de penetração, que satisfaça essa exigência ao tentar identificar ativamente rotas e caminhos de redes de fora para dentro do CDE. Todos os métodos de segmentação precisam ser testados especificamente. Em redes muito grandes, com diversos segmentos internos de LAN, pode ser inviável para o testador de penetração conduzir testes específicos de cada segmento individual de LAN. Neste caso, o teste precisa ser planejado para examinar cada tipo de metodologia de segmentação em uso (ou seja, firewall, VLAN ACL etc.) para validar a eficácia dos controles de segmentação. O nível de teste para cada metodologia de segmentação deve fornecer garantia de que a metodologia é eficaz em todas as instâncias de uso. Para validar efetivamente as metodologias de segmentação, espera-se que o testador de penetração tenha trabalhado com a organização (ou com o QSA da organização) para entender claramente todas as metodologias em uso para fornecer cobertura completa ao testar.

O testador de penetração pode optar por incluir sistemas localizados nesses segmentos de LAN isolados não diretamente relacionados ao processamento, transmissão ou armazenamento dos dados do titular do cartão, para garantir que esses sistemas não afetem a segurança do CDE se estiverem comprometidos. Consulte a Seção 4.2.3 para obter orientação específica sobre as metodologias de teste para validar controles de segmentação.

2.5 Engenharia social

A engenharia social é a tentativa de obter informações, acesso ou de introduzir software não autorizado no ambiente através da manipulação de usuários finais. O PCI DSS reconfirma os testes, exigindo abordagens aceitas pelo setor de testes de penetração (muitos dos quais incluem engenharia social como parte de sua abordagem) e para ter uma abordagem para testes de penetração que "considera as ameaças e vulnerabilidades experimentadas pelos comerciantes nos últimos 12 meses". Isso pode incluir ataques de engenharia social como um método usado para introduzir malware no ambiente.

Os testes de engenharia social são um método eficaz de identificar riscos associados à falha dos usuários finais em seguir as políticas e procedimentos documentados. Não há uma abordagem genérica para engajamentos de engenharia social. Se uma organização optar por incluir testes de engenharia social como parte de sua revisão anual de segurança, os testes realizados devem ser apropriados para o tamanho e a complexidade da organização, e devem considerar a maturidade do programa de conscientização de segurança da organização. Esses testes podem incluir interações pessoais e não tecnológicas, como persuadir alguém a manter aberta uma porta, interações remotas, como fazer alguém fornecer ou redefinir uma senha, ou convencer o usuário final a abrir um anexo de e-mail ou hiperlink vulnerável.

Embora o PCI DSS não exija que testes incluam técnicas de engenharia social, uma entidade pode incorporá-las à sua metodologia de teste de penetração como um método contínuo para determinar a eficácia do programa de conscientização de segurança. A frequência de testes de engenharia social seria determinada pela entidade, ao estabelecer seu programa de conscientização de segurança. A reeducação e conscientização de segurança do usuário final pode ser uma remediação suficiente para usuários que falham em um teste de engenharia social. O objetivo é que, ao longo do tempo, menos funcionários tomem decisões ruins que poderiam permitir que um ataque comprometesse a segurança. Orientações adicionais sobre o estabelecimento de um programa de conscientização de segurança eficaz e robusto podem ser encontradas na Biblioteca de Documentos, no site do PCI SSC.

O teste de engenharia social pode não ser apropriado ou não fornecer um resultado significativo para todas as organizações. Embora o teste de engenharia social não seja um requisito do PCI DSS, uma organização pode considerar documentar o(s) motivo(s) para testes de engenharia social acima e incluir a documentação aplicável aos relatórios de teste de penetração interna e externa, particularmente se ataques de engenharia social foram encontrados nos últimos 12 meses.

2.6 O que é considerado uma “mudança significativa”?

De acordo com os Requisitos 11.3.1 e 11.3.2 do PCI DSS, os testes de penetração devem ser realizados pelo menos anualmente e após qualquer alteração significativa — por exemplo, atualização ou modificação de infraestrutura ou aplicativo — ou novas instalações de componentes do sistema. O que é considerado “significativo” depende altamente do processo de avaliação de risco de uma entidade e da configuração de um determinado ambiente. Devido a essa variabilidade, uma alteração significativa não é prescrita pelo PCI DSS. Se a mudança puder afetar a segurança da rede ou permitir acesso aos dados do portador do cartão, ela pode ser considerada significativa pela entidade. O teste de penetração de mudanças significativas é realizado para garantir que os controles que se espera estarem funcionando funcionem efetivamente após a atualização ou modificação.

3 Qualificações de um testador de penetração

Recursos internos qualificados ou terceiros qualificados podem realizar o teste de penetração, desde que sejam independentes organizacionalmente. Isso significa que o testador de penetração deve ser organizacionalmente separado da gestão dos sistemas de destino. Por exemplo, em situações em que uma empresa terceirizada está realizando a avaliação do PCI DSS para a entidade, ela não pode realizar o teste de penetração se estiver envolvida na instalação, manutenção ou suporte dos sistemas de destino.

As diretrizes a seguir podem ser úteis ao selecionar um testador (ou equipe), para compreender suas qualificações para realizar testes de penetração.

3.1 Certificações

As certificações de um testador de penetração podem ser uma indicação do nível de habilidade e competência de um possível testador ou empresa de penetração. Embora estas não sejam certificações necessárias, elas podem indicar um corpo de conhecimento comum do candidato. A seguir estão alguns exemplos de certificações comuns de testes de penetração:

- Profissional Certificado de Segurança Ofensiva (Offensive Security Certified Professional, OSCP)
- Hacker Ético Certificado (Certified Ethical Hacker, CEH)
- Certificação de Garantia de Informações Globais (Global Information Assurance Certification, GIAC; por exemplo, Testador de Penetração Certificado GIAC [GIAC Certified Penetration Tester, GPEN], Testador de Penetração de Aplicativo Web GIAC [GIAC Web Application Penetration Tester, GWAPT] ou Pesquisador Explorador GIAC e Testador de Penetração Avançada [GIAC Exploit Researcher and Advanced Penetration Tester, GXPN])
- Certificações de teste de penetração CREST
- Certificação de Serviço de Verificação de Integridade de TI (IT Health Check Service, CHECK) do Grupo de Segurança da Comunicação Eletrônica (Communication Electronic Security Group, CESG)

Observação: O PCI SSC não valida nem endossa essas certificações.

3.2 Experiência anterior

A experiência e as qualificações apropriadas para testes de penetração não podem ser atendidas apenas pelas certificações. Portanto, a confirmação de critérios adicionais é necessária. Por exemplo, a análise da extensão dos engajamentos reais que foram realizados e da experiência profissional relevante são considerações importantes ao selecionar um testador ou uma equipe de penetração. As perguntas a seguir são exemplos para avaliar as qualificações e a competência de um testador ou equipe de penetração. Esta não é uma lista definitiva:

P Quantos anos de experiência o testador de penetração possui?

- Se o testador de penetração estiver em seu primeiro ano de teste de penetração, deve-se considerar cuidadosamente as seguintes perguntas para garantir que o testador de penetração tenha conhecimento suficiente e seja adequadamente treinado para realizar o teste de penetração. Também deve ser dada consideração à própria organização verificando o treinamento e os processos de controle de qualidade, para garantir que o testador de penetração seja qualificado.

P Há quantos anos a organização que emprega o testador de penetração realiza testes de penetração?

- Referências de outros clientes podem ser úteis em consideração.

P O testador de penetração realizou avaliações para organizações de tamanho e escopo semelhantes?

- Para ambientes com restrições de alta disponibilidade, componentes instáveis do sistema ou grandes infraestruturas, é importante avaliar a capacidade de um testador de lidar com essas restrições (restrições de largura de banda, restrições de tempo etc.).

P Qual experiência de teste de penetração tem o testador ou a equipe com as tecnologias no ambiente de destino (ou seja, sistemas operacionais, hardware, aplicativos da web, aplicativos altamente personalizados, serviços de rede, protocolos etc.)?

- Ao selecionar um testador de penetração, é importante avaliar a experiência de teste anterior da organização para a qual o testador trabalha, pois se refere às tecnologias especificamente implantadas dentro do ambiente de destino.
- Mesmo que o testador de penetração não tenha realizado uma avaliação de determinadas tecnologias específicas, se o testador tiver gerenciado, mantido, treinado ou desenvolvido tais tecnologias, o testador ainda poderá ser qualificado para realizar o teste de penetração.

P Considere quais outras habilidades/qualificações o testador de penetração tem e que contribuirão para sua capacidade de avaliar o ambiente.

- O testador de penetração possui certificações de teste de penetração padrão do setor? (Consulte a Seção 3.1.)
- Que tipo de experiência o testador de penetração tem realizando testes de penetração na camada de rede? A discussão de exemplos de testes de penetração de rede conduzidos pela organização pode ser garantida.
- O testador de penetração tem experiência com testes de penetração na camada de aplicativo? A discussão da familiaridade do testador de penetração com o teste para validar o OWASP Top 10 e outros padrões de codificação segura de aplicativos similares e exemplos de teste de penetração de aplicativos conduzidos pela organização pode ser garantida.

Observação: Uma organização pode ter um laboratório de ambiente de desenvolvimento, onde testes de penetração podem ser realizados fora do ambiente de produção e os recursos internos possam ser treinados e aumentar sua experiência para melhorar suas habilidades e certificações potenciais.

4 Metodologia

Para garantir um teste de penetração bem-sucedido, existem várias atividades e processos a serem considerados além do próprio teste. Esta seção fornece orientação para essas atividades e é organizada pelas fases típicas que ocorrem durante um teste de penetração: pré-engajamento, engajamento e pós-engajamento.

4.1 Pré-engajamento

Antes de o engajamento ou teste começar, recomenda-se que todas as partes envolvidas (a organização, o testador e onde aplicável, o avaliador) sejam informadas sobre os tipos de testes (ou seja, internos, externos, camada de aplicação ou camada de rede) a serem realizados, como os testes serão realizados e quais serão os testes. Ao coordenar esses detalhes primeiro, os problemas em que o escopo do CDE seja definido incorretamente ou outros problemas surgidos que exigiriam um novo teste podem ser evitados. Essas informações podem ser coletadas através da realização de uma chamada ou reunião, no local, de pré-engajamento.

4.1.1 Escopo

A organização avaliada é responsável pela definição do CDE e de quaisquer sistemas críticos. Recomenda-se que a organização trabalhe com o testador e, quando aplicável, o avaliador, para verificar se nenhum componente foi ignorado e para determinar se algum sistema adicional deve ser incluído no escopo. O escopo do teste de penetração deve ser representativo de todos os pontos de acesso, sistemas críticos e metodologias de segmentação para o CDE.

4.1.2 Documentação

Sempre que possível, a documentação detalhada de quaisquer componentes dentro do escopo deve ser disponibilizada ao testador. Exemplos comuns de tais documentos são documentação de interface de aplicativo e guias de implementação. Essas informações assegurarão que o testador entenda como a funcionalidade deve operar e se os resultados recebidos são esperados para o cenário determinado.

Como parte do processo de escopo, a organização deve fornecer ao testador a seguinte documentação:

- Um diagrama de rede representando todos os segmentos de rede no escopo para o teste (consulte os Requisitos 1.1.2 e 1.1.3 do PCI DSS).
- Diagrama de fluxo de dados do titular do cartão
- Uma lista de todos os serviços e portas que se espera sejam expostas no perímetro CDE
- Detalhes de como os usuários autorizados acessam o CDE
- Uma lista de todos os segmentos de rede que foram isolados do CDE para reduzir o escopo

O testador de penetração usará essas informações durante a avaliação para identificar vetores de ataque inesperados do CDE, além de vetores de ataque conhecidos, controles de autenticação insuficientes e para confirmar a segmentação adequada de ambientes fora do escopo.

4.1.3 Regras de engajamento

Antes do início de qualquer teste, é importante documentar e concordar sobre as condições em que o teste deve ser realizado e o grau de exploração, se houver, que é permitido. Isso autoriza o testador a testar o ambiente e garantir que a organização entenda o que esperar do teste de penetração.

Abaixo estão alguns exemplos de considerações que podem ser incluídas nas regras de engajamento:

- O teste precisará ser conduzido em qual período?
- Há algum sistema antigo que tenha problemas conhecidos com varredura automatizada? Em caso afirmativo, como os testes devem ser realizados para esses sistemas?
- Existe um método preferido de comunicação sobre o escopo e os problemas encontrados durante o engajamento?
- A entidade quer atualizações sobre a exploração contínua dos sistemas durante o teste? Se for o caso, a entidade precisará determinar se irá ou não agir com base nessas informações ou fazer alterações no ambiente. A entidade também pode implementar seu plano de resposta a incidentes, como resposta a uma exploração.
- Existem controles de segurança que detectariam ou impediriam o teste? Considere se estes devem ser desativados ou configurados para não interferir durante o teste. (Consulte a Seção 4.1.7 para obter mais orientações.)
- Se senhas ou outros dados confidenciais forem comprometidos durante o teste, o testador precisa divulgar uma lista de todas as senhas e/ou dados confidenciais acessados?
- Se o equipamento de propriedade do testador for conectado à rede da organização, quais etapas devem ser tomadas para garantir que o equipamento não apresente uma ameaça ao ambiente (atualizado para o sistema operacional mais recente, pacotes de serviços e/ou patches aplicados etc.)?
- O testador precisa fornecer todos os endereços de IP a partir dos quais os testes serão originados?
- Os dados sensíveis, mostrados como acessíveis durante o teste, serão mantidos pelo testador durante e após o teste de penetração? Apenas um teste de prova de conceito deve ser realizado, e todos os dados do titular do cartão obtidos devem ser protegidos de acordo com o PCI DSS. (Consulte a Seção 4.2.4 para obter mais orientações.)
- Quais etapas serão executadas se o testador detectar um comprometimento anterior ou ativo para os sistemas sendo testados? (Por exemplo, ative os procedimentos de resposta a incidentes e pare o teste de penetração até a resolução da situação de comprometimento.)

4.1.4 Ambientes na nuvem/hospedados por terceiros

Abaixo estão exemplos de considerações que podem ser incluídas nas regras de engajamento para ambientes hospedados/em nuvem da entidade:

- Se um acordo de nível de serviço exigir aprovação de terceiros antes que os testes de penetração possam ser realizados, a organização deve receber aprovação do terceiro (ou seja, provedor de hospedagem etc.) antes da avaliação ser realizada.
- O escopo pode não incluir a infraestrutura fornecida pelo terceiro para a entidade. O escopo pode incluir qualquer sistema gerenciado, construído ou utilizado pela organização.
- A menos que indicado de outra forma no escopo, os portais de gerenciamento da Web fornecidos pelo terceiro para que a entidade gerencie sua infraestrutura não devem ser incluídos no teste de penetração. Essas interfaces devem ser testadas e validadas como parte dos esforços de conformidade do PCI DSS de terceiros, e evidências ou atestado de validação devem ser fornecidos ao cliente.

4.1.5 Critérios de sucesso

O objetivo de um teste de penetração é estimular uma situação de invasão real, com o objetivo de identificar até onde um invasor pode penetrar no ambiente. Definir os critérios de sucesso para o teste de penetração permite que a entidade defina limites na profundidade do teste de penetração. Sem concordar com o ponto em que o teste de penetração está concluído, existe a possibilidade do testador exceder os limites e as expectativas da entidade-alvo. Isso deve ser incluído nas regras de engajamento.

Possíveis critérios de sucesso podem incluir:

- Observação direta de serviços ou dados restritos na ausência de controles de acesso esperados
- Comprometimento de um dispositivo intermediário usado por usuários privilegiados para acessar o CDE
- Comprometimento do domínio usado por usuários privilegiados
- Sem comprometimento dos sistemas de destino

Os critérios de sucesso serão diferentes para cada ambiente e devem ser estabelecidos durante a reunião inicial de pré-engajamento antes do teste.

4.1.6 Análise de ameaças e vulnerabilidades anteriores

O Requisito 11.3 do PCI DSS exige análise e consideração de ameaças e vulnerabilidades encontradas pela entidade avaliada nos últimos 12 meses. Este é um olhar histórico às vulnerabilidades reais vividas ou descobertas no ambiente da entidade, desde a última avaliação. Essas informações podem fornecer ideias sobre o processo em vigor, para lidar com essas vulnerabilidades.

O testador de penetração deve estar familiarizado com as vulnerabilidades atuais vistas pelo setor nos últimos 12 meses, bem como analisar detalhadamente as vulnerabilidades recentes da entidade.

Dependendo do tipo de teste a ser realizado (ou seja, caixa branca, caixa cinza, caixa preta), o seguinte pode ou não ser considerado em tal revisão:

- Vulnerabilidades descobertas pela entidade que não foram remediadas dentro do período exigido pelo PCI DSS (exemplo: trimestralmente) e/ou pelos requisitos de remediação de vulnerabilidade documentados na política de segurança corporativa
- Controles de compensação existentes mitigando as vulnerabilidades observadas
- Implantações ou atualizações em andamento (considere hardware e software)
- Se aplicável, ameaças ou vulnerabilidades que possam ter levado a uma violação de dados
- Validação da remediação dos achados do teste de penetração dos anos anteriores
- Identificação do “estado de vulnerabilidades existentes” do setor, para fins de rastreamento de vulnerabilidades que podem não ter sido detectadas no momento do teste de penetração mais recente

O testador pode obter uma percepção adicional do ambiente-alvo para esta revisão por:

- Revisão dos relatórios de teste de penetração anteriores
- Revisão de relatórios emitidos anteriormente sobre conformidade ou atestado de conformidade
- Revisão dos resultados atuais do teste de varredura de vulnerabilidade

4.1.7 Evite a interferência de varredura em dispositivos de segurança.

Em muitos ambientes, controles de proteção ativos, como sistemas de prevenção de intrusão ou sistemas de proteção ativa da Web, como sistemas de proteção contra intrusão (IPS) e firewalls de aplicativos da Web (WAF) podem ser implantados para proteger os serviços expostos. Como a intenção do teste de penetração é avaliar a suscetibilidade dos serviços à exploração (vs. a capacidade dos sistemas de proteção ativa para evitar ataques), a interferência no teste de penetração deve ser evitada. As entidades são incentivadas a revisar e estar familiarizadas com a seção intitulada “Scan Interference” no Guia do Programa ASV e configurar os sistemas de proteção ativos de acordo durante o teste.

Esta prática ajuda a garantir que os próprios serviços sejam configurados adequadamente e tenham o risco mínimo de serem explorados, caso o sistema de proteção ativa falhe, seja vencido ou desviado por um invasor.

4.2 Engajamento: Teste de Penetração

Cada ambiente tem aspectos/tecnologia únicos que exigem que o testador selecione a abordagem mais adequada e as ferramentas necessárias para realizar o teste de penetração. Está além do escopo deste documento definir ou descrever qual abordagem, ferramentas ou técnicas são adequadas para cada teste de penetração. Em vez disso, as seções a seguir fornecem orientação de alto nível sobre considerações para a abordagem, ferramentas ou técnicas.

O teste de penetração é essencialmente um esforço manual. Em muitos casos, existem ferramentas que podem ajudar o testador a realizar o teste e aliviar algumas das tarefas repetitivas. O julgamento é necessário na seleção das ferramentas apropriadas e na identificação de vetores de ataque que normalmente não podem ser identificados através de meios automatizados.

O teste de penetração também deve ser realizado a partir de um local adequado, sem restrições de portas ou serviços pelo provedor de Internet. Por exemplo, um testador de penetração que utiliza conectividade de Internet fornecida a consumidores e residências pode ter SMTP, SNMP, SMB e outras portas restritas pelo provedor de Internet, para minimizar o impacto por vírus e malware. Se o teste for realizado por um recurso interno qualificado, deve ser realizado a partir de uma conexão de internet neutra não afetada pelos controles de acesso que possam estar presentes nos ambientes corporativos ou de suporte.

4.2.1 Camada de aplicativo

Conforme mencionado na Seção 2.3, o testador de penetração deve realizar testes pela perspectiva das funções definidas do aplicativo. A organização é amplamente incentivada a fornecer credenciais para permitir que o testador assuma as funções necessárias. Isso permitirá que o testador determine se, em qualquer função, o usuário pode obter mais privilégios ou, de outra forma, obter acesso aos dados que não estão explicitamente autorizados a acessar.

Nos casos em que a organização criou novas contas para o testador usar, é importante que a organização garanta que todas as funções e a segurança aplicável no aplicativo tenham sido configuradas para permitir que o testador teste com eficácia todas as funcionalidades.

Nos casos em que um aplicativo da Web utiliza API de back-end, o API pode estar no escopo para o teste. O testador deve compreender a interação entre o aplicativo da web e o backend, a funcionalidade exposta pelo API, bem como quaisquer controles de segurança implementados para proteger o acesso ao API. Esses e outros fatores ajudarão a determinar se API de back-end deve ser testado independentemente do aplicativo da web.

4.2.2 Camada de rede

Como a maioria dos protocolos é bem definida e tem modos padrão de interação, testes de camada de rede são mais adequados para testes automatizados. Isso torna a automação a primeira etapa lógica em um teste de camada de rede. Devido a tal padronização, ferramentas podem ser usadas para identificar rapidamente um serviço, a versão do software, testar as configurações incorretas comuns e até mesmo identificar vulnerabilidades. Testes automatizados podem ser realizados muito mais rápido do que se espera de um humano. No entanto, simplesmente executar uma ferramenta automatizada não satisfaz o requisito de teste de penetração. Ferramentas automatizadas não podem interpretar vulnerabilidades, configurações incorretas ou até mesmo os serviços expostos para avaliar o verdadeiro risco ao ambiente. A ferramenta automatizada serve apenas como indicação basal da superfície de ataque potencial do ambiente. O testador de penetração deve interpretar os resultados de quaisquer ferramentas automatizadas e determinar se são necessários testes adicionais.

Usando a documentação fornecida pela organização durante o pré-engajamento, o testador deve:

- Verificar se apenas os serviços autorizados estão expostos no perímetro CDE.
- Tentar ignorar controles de autenticação de todos os segmentos de rede onde usuários autorizados acessam o CDE, bem como segmentos não autorizados a acessar o CDE.

4.2.3 Segmentação

A verificação da segmentação é realizada através da realização de testes usados nos estágios iniciais de um teste de penetração de rede (ou seja, descoberta de host, varredura de porta etc.). Deve verificar se todas as LANs fora do escopo realmente não têm acesso ao CDE. Para ambientes com um grande número de segmentos de rede considerados fora do escopo ou isolados do CDE, um subconjunto representativo pode ser usado para testes, reduzindo o número de verificações de segmentação que precisam ser executadas. Cada método de segmentação exclusivo deve ser testado para garantir que todos os controles de segurança estejam funcionando conforme pretendido.

Se for determinado durante a verificação de segmentação que um segmento de LAN considerado fora do escopo tem acesso ao CDE, a organização precisará ajustar os controles de segmentação para bloquear esse acesso ou realizar um teste de penetração completo da camada de rede, para caracterizar o acesso e o impacto no escopo do PCI DSS.

4.2.4 O que fazer quando os dados do titular do cartão são encontrados

Se os dados do titular do cartão forem acessados durante o teste de penetração, é importante que o testador notifique a organização imediatamente. O testador deve manter a documentação detalhada para saber exatamente que dados foram acessados e como foram acessados.

Após ser notificada, a organização deve analisar imediatamente como os dados do titular do cartão foram recuperados e, conforme apropriado, tomar medidas para executar seu plano de resposta a incidentes.

Se a saída de ferramentas ou atividades de teste incluir dados do titular do cartão que foram acessados pelo testador durante o engajamento, é importante que essa saída seja protegida de acordo com o PCI DSS.

4.2.5 Pós-exploração

O termo "pós-exploração" refere-se às ações tomadas após o comprometimento inicial de um sistema ou dispositivo. Ele geralmente descreve a abordagem metódica de usar técnicas de aumento de privilégios ou de pivotagem, o que permite que o testador, neste caso, estabeleça uma nova fonte de ataque do novo ponto de vista no sistema — para obter acesso adicional a sistemas ou recursos de rede. Os testadores de penetração devem poder demonstrar o risco apresentado por sistemas exploráveis para o CDE e o que pode ocorrer após a exploração com esses sistemas.

4.3 Pós-engajamento

Após o engajamento ou teste ter sido realizado, há atividades que ambas as partes devem realizar.

4.3.1 Melhores práticas de remediação

Os esforços de teste de penetração, embora completos, nem sempre garantem a identificação completa de cada instância em que a eficácia de um controle de segurança seja insuficiente — por exemplo, encontrar uma vulnerabilidade de scripting entre sites em uma área de um aplicativo pode não revelar todas as instâncias desta vulnerabilidade no aplicativo. Muitas vezes, a presença de vulnerabilidade em uma área pode indicar fraqueza em práticas de processo ou desenvolvimento que poderiam ter replicado ou habilitado vulnerabilidade semelhante em outros locais.

Portanto, é importante para a entidade testada investigar cuidadosamente sistemas ou aplicativos, com controles de segurança ineficazes em mente, ao remediar.

4.3.2 ***Novo teste de vulnerabilidades identificadas***

A organização deve tomar medidas para remediar toda vulnerabilidade explorável, dentro de um período razoável após o teste original. Quando a organização tiver concluído essas etapas, o testador deve realizar um novo teste para comprovar que os controles recém-implementados mitigam o risco original.

Esforços de remediação que se estendem por um longo período após o teste inicial podem exigir um novo teste de engajamento, para garantir que resultados precisos do ambiente mais atual sejam relatados. Essa determinação pode ser feita após uma análise de risco de quanta mudança ocorreu desde que o teste original foi concluído.

Em condições específicas, o problema de segurança sinalizado pode representar uma falha fundamental em um ambiente ou aplicativo. O escopo de um novo teste deve considerar se qualquer alteração que ocorra como resultado da remediação identificada do teste é classificada como significativa. Todas as alterações devem ser testadas novamente; no entanto, se um novo teste completo do sistema for necessário, será determinado pela avaliação de risco dessas alterações.

4.3.3 ***Limpeza do ambiente***

É importante que o testador documente e divulgue à organização todas as alterações feitas ao ambiente (conforme permitido nas Regras de Engajamento) durante o teste, incluindo, entre outras:

- Contas que foram criadas como parte da avaliação pela entidade ou pelo testador: a organização deve remover essas contas.
- Ferramentas instaladas pelo testador nos sistemas da organização: essas ferramentas devem ser removidas no final do teste.

A remoção de contas e ferramentas de teste garantirá que as contas ou ferramentas remanescentes não possam ser exploradas ou usadas contra a organização.

4.4 **Recursos adicionais**

Existem várias metodologias aceitas pelo setor que podem fornecer orientação adicional sobre as atividades de teste de penetração, incluindo, entre outras:

- Manual de Metodologia de Teste de Segurança de Código Aberto (Open Source Security Testing Methodology Manual, “OSSTMM”)
- Publicação especial do The National Institute of Standards and Technology (“NIST”) 800-115
- Guia de testes do OWASP
- Padrão de Execução do Teste de Penetração
- Estrutura de testes de penetração

5 Relatórios e documentação

O objetivo do relatório é auxiliar a organização em seus esforços para melhorar sua postura de segurança, identificando áreas de risco potencial que podem precisar ser remediadas. Apenas relatar listas de vulnerabilidades não ajuda neste esforço e não atende à intenção do teste de penetração. O relatório deve ser estruturado de forma a comunicar claramente o que foi testado, como foi testado e os resultados dos testes.

Esta seção fornece orientação sobre a documentação de vulnerabilidades identificadas e/ou exploradas, criação de modelos de relatórios e avaliação de um relatório de teste de penetração.

5.1 Relatório de vulnerabilidade identificada

Os relatórios de teste de penetração devem incluir uma discussão das etapas, vetores e vulnerabilidades exploradas que levam à penetração durante o teste para o qual são necessárias remediações e retestes. No entanto, é possível que o testador identifique vulnerabilidades que não foram necessariamente exploráveis, mas que são consideradas como tendo um risco potencial para o ambiente. Recomenda-se que o relatório contenha todas as conclusões que afetem a postura de segurança da entidade avaliada, mesmo nos casos em que a exploração não ocorreu. Alguns exemplos de vulnerabilidades identificadas que não foram exploradas por razões válidas e devem ser incluídas no relatório podem ser:

- Configurações incorretas de firewall, que permitem tráfego não autorizado entre zonas seguras e inseguras
- Detecção de credenciais obtidas através da manipulação de uma mensagem de erro de aplicativo web, que não foi sinalizada durante uma varredura de ASV devido a uma pontuação de base de CVSS baixa

5.1.1 Atribuição de uma pontuação de gravidade

Para priorizar a remediação dos resultados do teste de penetração, é prática comum durante a fase de relatório classificar a gravidade ou risco atribuído a cada problema de segurança detectado. O relatório deve documentar claramente como a classificação de gravidade/risco é derivada.

Na maioria dos casos, a classificação de gravidade/risco pode ser aplicada como resultado da avaliação de uma pontuação padrão do setor (por exemplo, NVD, CVSS) em relação a um limite ou valor que indica risco (ou seja, alto, médio e baixo). No entanto, deve-se observar que é possível que uma vulnerabilidade existente seja inerente a um ambiente específico; portanto, uma pontuação padronizada não está disponível.

Quando a pontuação personalizada faz parte do processo de classificação de risco, o relatório deve refletir um conjunto rastreável de raciocínio para a modificação das pontuações padrão do setor ou, quando aplicável, para a criação de uma pontuação a uma vulnerabilidade sem pontuação padrão do setor definida.

5.1.2 Referências padrão do setor

Algumas referências bem conhecidas do setor incluem:

- Banco de dados nacional de vulnerabilidade (National Vulnerability Database, NVD)
- Sistema comum de pontuação de vulnerabilidade (Common Vulnerability Scoring System, CVSS)
- Vulnerabilidades e exposição comuns (Common Vulnerabilities and Exposure, CVE)
- Enumeração de fraqueza comum (Common Weakness Enumeration, CWE)
- Bugtraq ID (BID)
- Banco de dados de vulnerabilidade de código aberto (Open Source Vulnerability Database, OSVDB)

O Sistema comum de pontuação de vulnerabilidade (Common Vulnerability Scoring System, CVSS) é um exemplo de estrutura aberta que pode ser referenciada para atribuir uma classificação de risco basal. O CVSS é o sistema de pontuação necessário para fornecedores de varredura aprovados (ASVs) para identificar vulnerabilidades detectadas durante as varreduras de vulnerabilidade do PCI. Usando este sistema, uma pontuação de vulnerabilidade padronizada pode ser ajustada através da avaliação dos traços de vulnerabilidade dentro do contexto de um ambiente específico.

5.2 Diretrizes para relatórios

Relatórios abrangentes e consistentes são uma fase crítica de um teste de penetração. Esta seção fornece diretrizes sobre o conteúdo comum de um teste de penetração padrão do setor. Deve-se observar que estes são apenas os esboços sugeridos e não definem requisitos de relatório específicos para testes de penetração do PCI DSS. Os testadores podem ter seções diferentes, títulos alternativos e/ou formato de relatório etc.; este esboço representa dados coletados de vários provedores de testes de penetração e os desejos dos clientes.

5.2.1 Descrição do relatório do teste de penetração

- Resumo executivo
 - Breve resumo de alto nível do escopo do teste de penetração e dos principais achados
- Declaração de escopo
 - Uma definição detalhada do escopo da rede e dos sistemas testados como parte do engajamento
 - Diferenciação entre sistemas ou segmentos CDE e não CDE, que foram considerados durante o teste
 - Identificação de sistemas críticos dentro ou fora do CDE e explicação do motivo de eles estarem incluídos no teste como alvos
- Declaração de metodologia
 - Detalhes sobre as metodologias usadas para concluir o teste (varredura de porta, nmap etc.). Consulte a Seção 4 para obter detalhes sobre as metodologias que devem ser documentadas.
- Declaração de limitações
 - Documentar quaisquer restrições impostas ao teste, como horas de teste designadas, restrições de largura de banda, requisitos de teste especiais para sistemas legados etc.

- **Narrativa do teste**
 - Fornecer detalhes sobre a metodologia de testes e como os testes progrediram. Por exemplo, se o ambiente não tiver nenhum serviço ativo, explique qual teste foi realizado para verificar o acesso restrito.
 - Documentar quaisquer problemas encontrados durante o teste (por exemplo, interferência encontrada como resultado de sistemas de proteção ativos bloqueando o tráfego).
- **Resultados do teste de segmentação**
 - Resumir os testes realizados, para validar os controles de segmentação, se usados para reduzir o escopo do PCI DSS.
- **Resultados**
 - Se/como o CDE pode ser explorado usando cada vulnerabilidade.
 - Classificação/gravidade de risco de cada vulnerabilidade
 - Alvos afetados
 - Referências (se disponíveis)
 - CVE, CWE, BID, OSBDB etc.
 - Fornecedor e/ou pesquisador
 - Descrição da descoberta
- **Ferramentas usadas**
- **Limpeza do teste de pós-penetração do ambiente**

Após o teste, pode haver tarefas que o testador ou o cliente precise executar para restaurar o ambiente de destino (ou seja, atualização/remoção de contas de teste ou entradas de banco de dados adicionadas ou modificadas durante o teste, desinstalação de ferramentas de teste ou outros artefatos, restauração de configurações de sistema de proteção ativa e/ou outras atividades que o testador possa não ter permissões para executar etc.).

 - Forneça instruções sobre como a limpeza deve ser realizada e como verificar se os controles de segurança foram restaurados.

5.2.2 Considerações sobre o novo teste e esboço de relatório

Se os achados observados exigirem remediação e repetição de testes antes que um avaliador possa determinar que a entidade atende ao Requisito 11.3 do PCI DSS, um relatório de teste de acompanhamento pode ser fornecido. Todos os esforços de remediação devem ser concluídos e testados novamente dentro de um período razoável, após o relatório de teste de penetração original ter sido fornecido.

Espera-se que o relatório de teste de remediação cubra todas as vulnerabilidades identificadas/exploráveis que exijam remediação. Essas vulnerabilidades identificadas podem ser médias ou altas, para testes de penetração externa, e aquelas definidas pela organização como médias ou altas, para testes internos.

Segue um exemplo das seções para incluir em um relatório de novo teste, conforme definido na Seção 5.2.1:

- Resumo executivo
- Data do teste original
- Data do novo teste
- Achados originais
- Resultados do novo teste

5.3 Retenção de evidências

5.3.1 O que é considerado evidência?

Um teste de penetração típico envolve a obtenção e avaliação de evidências usando uma metodologia formal; a evidência coletada do teste de penetração é usada para determinar a conclusão. A evidência é composta por todas as informações que apoiam as conclusões do testador de penetração sobre a eficácia dos controles de segurança e a postura de segurança geral do ambiente. O testador de penetração deve seguir um processo sistemático para coletar, manusear e armazenar as evidências com segurança.

Exemplos de evidências incluem, entre outras, capturas de tela, saída de ferramentas brutas (ou seja, NMAP, pacote de burp, Nessus, TCPDump Wireshark etc.), dumps adquiridas em caso de exploração (ou seja, arquivos de banco de dados, registros, arquivos de configuração etc.), fotos, gravações e qualquer coisa que possa apoiar a conclusão final do relatório de teste de penetração.

Deve-se observar que, se os dados do portador do cartão forem adquiridos durante o teste de penetração, recomenda-se que seja mantido ao mínimo. Por exemplo, um banco de dados cheio de dados do titular do cartão não deve ser descarregado na máquina ou sistema do testador.

5.3.2 Retenção

Recomenda-se que os procedimentos para retenção e destruição de evidências sejam documentados para todas as partes envolvidas, antes de iniciar o teste de penetração. Se um terceiro for usado para realizar o teste de penetração, o texto do contrato deve ser revisado para confirmar se esses procedimentos estão claros.

Embora não existam atualmente requisitos do PCI DSS com relação à retenção de evidências coletadas pelo testador de penetração, é recomendável que essas evidências sejam retidas pelo testador (internas à organização ou um provedor terceirizado) por um período, considerando as leis locais, regionais ou da empresa que devem ser seguidas para a retenção de evidências. Esta evidência deve estar disponível mediante solicitação da entidade-alvo ou de outras entidades autorizadas, conforme definido nas regras de engajamento.

Se, no entanto, um testador armazenar os dados do titular do cartão obtidos durante o engajamento, os dados devem ser armazenados pelo testador seguindo as diretrizes do PCI DSS para o armazenamento de dados da conta, ou seja, criptografados usando criptografia forte, truncado/embaralhado ou não armazenado. Não é recomendado armazenamento de dados de conta pelo testador. Esses dados devem ser limpos com segurança dos sistemas de testador na conclusão do engajamento.

5.4 Ferramenta de avaliação do relatório de teste de penetração

Esta seção destina-se a entidades que recebem um relatório de teste de penetração e precisam interpretar e avaliar a completude do relatório.

A intenção é fornecer uma ferramenta que poderia ser usada por comerciantes, prestadores de serviços e avaliadores para determinar rapidamente a profundidade dos testes e a qualidade do relatório, com base no acordo contratual entre a organização e o testador. Deve-se observar que esta lista de verificação não tem a intenção de realizar a inspeção completa do relatório, a interpretação dos resultados e a ação apropriada.

A **Tabela 1** detalha as perguntas, um lugar para registrar se o item está incluído no relatório e o número da página onde ele é encontrado. Não é intenção gerar qualquer tipo de "pontuação" com os resultados, pois sua intenção é fornecer uma ferramenta de comunicação que possa ser usada entre a entidade e o testador após um relatório ter sido escrito e os resultados avaliados. Deve-se observar que esses itens representam um conjunto mínimo sugerido de itens para inclusão ao relatório; pode haver conteúdo adicional.

Tabela 1: Lista de verificação de avaliação de relatório

Pergunta do relatório	Incluído no relatório		Página
	Sim	Não	
Nome/organização do testador de penetração			
Informações de contato	<input type="checkbox"/>	<input type="checkbox"/>	
Credenciais/qualificações de analistas	<input type="checkbox"/>	<input type="checkbox"/>	
Há evidência suficiente de que as pessoas sejam organizacionalmente independentes da gestão do ambiente sendo testado?	<input type="checkbox"/>	<input type="checkbox"/>	
Datas em que o engajamento foi realizado	<input type="checkbox"/>	<input type="checkbox"/>	
Data em que o relatório foi emitido	<input type="checkbox"/>	<input type="checkbox"/>	
Resumo executivo			
Resume os testes realizados	<input type="checkbox"/>	<input type="checkbox"/>	
Resume os resultados dos testes	<input type="checkbox"/>	<input type="checkbox"/>	
Resume as etapas para remediação	<input type="checkbox"/>	<input type="checkbox"/>	
Escopo			
O escopo está claramente documentado?	<input type="checkbox"/>	<input type="checkbox"/>	
Como o escopo foi determinado	<input type="checkbox"/>	<input type="checkbox"/>	
A perspectiva de ataque do engajamento está claramente definida (interna, externa ou ambas)?	<input type="checkbox"/>	<input type="checkbox"/>	

Pergunta do relatório	Incluído no relatório		Página
	Sim	Não	
O tipo de teste está claramente definido (camada de aplicativo, camada de rede ou ambos)?	<input type="checkbox"/>	<input type="checkbox"/>	
Houve restrições sobre o teste (tempo, limitações de largura de banda etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	
Metodologia			
A metodologia está claramente declarada?	<input type="checkbox"/>	<input type="checkbox"/>	
A metodologia reflete as melhores práticas do setor (OWASP, NIST etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	
Narrativa			
Existe uma discussão clara sobre os testes automatizados e manuais que foram realizados?	<input type="checkbox"/>	<input type="checkbox"/>	
Existe documentação clara de quaisquer problemas encontrados durante o teste (interferência de sistemas de proteção ativos, ambiente de destino controla bloqueio ou queda de pacotes etc.)?	<input type="checkbox"/>	<input type="checkbox"/>	
Descoberta			
Há uma seção que documenta todas as portas/serviços de rede abertos identificados para o escopo alvo e a perspectiva de origem (exposição interna ou externa)?	<input type="checkbox"/>	<input type="checkbox"/>	
Resultados			
Há uma indicação clara de que a repetição do teste é necessária e, se for o caso, quais áreas específicas exigem novo teste?	<input type="checkbox"/>	<input type="checkbox"/>	
Há uma lista resumida de itens que precisam de remediação e novo teste?	<input type="checkbox"/>	<input type="checkbox"/>	
Há uma lista detalhada de itens que precisam de remediação e novo teste?	<input type="checkbox"/>	<input type="checkbox"/>	
O testador demonstrou tentativas de explorar a vulnerabilidade identificada e declarar claramente o possível resultado/risco que cada possível exploração pode representar ao ambiente? (Consulte a Seção 5.1.1 para discussão sobre classificação de risco.)	<input type="checkbox"/>	<input type="checkbox"/>	

6 Estudos de caso/Exemplos de escopo

Esta seção fornece vários estudos de caso que ilustram vários conceitos e metodologias abrangidos neste documento.

6.1 Estudo de caso de teste de penetração de comércio eletrônico

Introdução ao caso

O Cliente é um comerciante de nível um e varejista de roupas femininas. O Cliente tem três marcas exclusivas que operam em vários sites de comércio eletrônico. A marca A é executada em uma plataforma de comércio eletrônico de terceiros, escrita usando uma plataforma Java com o Apache Tomcat e o banco de dados DB2 da IBM, e utiliza uma rede de entrega de conteúdo para distribuição de imagens. A marca B e a marca C utilizam um carrinho de compras de comércio eletrônico codificado interno, escrito no ColdFusion com Microsoft SQL, e compartilham o mesmo código subjacente. Todas as marcas enviam dados do titular do cartão para processamento em HTTPS. Todos os sites são hospedados em um provedor de hospedagem terceirizado em sistemas dedicados. Os firewalls do Cliente têm recursos integrados de prevenção de intrusão. O cliente tem controle exclusivo do código e do conteúdo. Os gerentes de produtos atualizam as informações do produto usando servidores de disponibilização no ambiente corporativo, e as atualizações são promovidas para produção pela equipe de suporte de TI. O cliente tem controle total do DNS.

Descrição do ambiente

O ambiente para as marcas A, B e C é composto por cinco redes. A Web DMZ contém os firewalls, servidores DNS, balanceadores de carga e servidores web para todas as marcas. Apenas os balanceadores de carga são NAT e têm endereços de IP que podem ser roteados publicamente.

A camada do aplicativo contém os servidores de middleware Apache Tomcat e ColdFusion. Ele é segmentado a partir das camadas DMZ e de banco de dados usando controles de acesso de firewall. A camada do banco de dados contém os servidores Microsoft SQL e IBM DB2. Ele é segmentado a partir da camada do aplicativo, usando controles de acesso de firewall. A rede de gerenciamento é usada para backups, servidores de gerenciamento de patches, servidores NTP, dispositivos de análise de tráfego de rede e coletores syslog. A rede de gerenciamento é acessada usando jumpboxes, com autenticação de dois fatores da rede corporativa, em uma VPN ponto a ponto.

Atividades de pré-engajamento (planejamento)

Uma vez confirmada a contratação, a Empresa de Teste de Penetração agendou uma chamada de lançamento e forneceu ao Cliente um questionário de teste e formulário de autorização de teste, a ser preenchido antes da próxima reunião.

A chamada inicial é geralmente usada para revisar as regras de engajamento, definir os critérios de sucesso e analisar a metodologia a ser usada. Um exame desse tipo pode ser conduzido de acordo com as melhores práticas de avaliação de segurança do sistema de informação, como descrito pelo *Manual da metodologia de teste de segurança de código aberto* ("OSSTMM"), *Publicação especial do National Institute of Standards and Technology* ("NIST") 800-115, *Guia técnico para testes e avaliação de segurança da informação* ou a metodologia de teste Open Web Application Security Project (OWASP), conforme definido no *Guia de testes do OWASP v.3.0*.

O escopo é fundamental e quanto mais complexo o ambiente, mais difícil ele se torna. Neste caso, todos os IPs externos usados para DMZ e camada web foram incluídos no escopo. Isso incluiria todos os sistemas que armazenam, processam ou transmitem os dados do titular do cartão diretamente. Como o cliente tem total controle e responsabilidade por sua segurança, o servidor DNS foi incluído no escopo do teste para determinar se um invasor poderia comprometer o servidor e redirecionar o tráfego destinado aos locais do cliente para um site malicioso ou fraudulento. Os servidores CDN de imagem foram determinados fora do escopo, porque nenhum dado PAN é transmitido ou processado e os sistemas são totalmente segmentados. Os sistemas de preparação não estão disponíveis na Internet e, portanto, não podem ser testados.

Os aplicativos da Web para a Marca A e a Marca B estarão completamente no escopo. Presume-se que o aplicativo da Web para a Marca C seja uma cópia exata e exclusiva das informações do produto, aparência e sensação. O testador fará a amostra do aplicativo da Web para a Marca C para verificar se as aplicações são as mesmas que a Marca B. Se for determinado que há diferenças substanciais entre as aplicações da Marca B e da Marca C, a Marca C será trazida totalmente no escopo.

O Cliente e a Empresa de Teste de Penetração concordaram que os testes serão realizados em relação aos sistemas de produção, já que nenhum sistema de preparação ou de análise adequado está disponível publicamente. Devido a essa limitação, o teste deve ser realizado com o sistema de prevenção de intrusão ativado. No entanto, como o cronograma para testes não pode acomodar o tempo necessário para usar técnicas que possam ignorar o IPS, o cliente concordou em remover qualquer bloco habilitado pelo sistema durante o teste.

Para este engajamento, o Cliente solicitou que regras adicionais de engajamento incluam que o teste seja limitado a horas que não sejam de pico, e que qualquer tentativa de executar o código de exploração nos sistemas remotos seja realizada somente após notificar o Cliente. Além disso, todas as contas criadas pelo testador ou pedidos bem-sucedidos colocados no sistema devem ser identificados no final do teste de cada dia.

Todas as partes concordaram que nenhum teste adicional será necessário se o testador de penetração puder extrair dados de um dos bancos de dados ou obter acesso de shell em qualquer servidor na farm da Web.

Fase de engajamento (descoberta e ataque/execução)

O testador de penetração começou comparando o escopo fornecido pelo cliente com o último relatório ASV, para garantir que eles concordem sobre os ativos e alvos em exame. Todas as diferenças no escopo foram observadas e investigadas.

O testador de penetração então reuniu informações sobre a organização alvo através de sites e servidores de e-mail, registros públicos e bancos de dados. Esta coleta de inteligência de código aberto (OSINT) é uma próxima etapa importante para confirmar o escopo e determinar que todos os ativos apropriados foram incluídos no teste. Os ativos recém-descobertos foram verificados pelo Cliente para determinar se deveriam ser incluídos no teste de penetração. Durante esta fase da avaliação, um local adicional de recuperação de desastres foi identificado no DNS, e o cliente confirmou que é um backup ativo (warm backup) em caso de falha dos locais primários. Todos os ativos relevantes foram adicionados ao escopo.

Assim que os ativos foram confirmados, o testador de penetração enumera os serviços disponíveis publicamente fornecidos pelos alvos. O testador tentou ativamente obter nomes de usuário, informações de compartilhamento de rede e informações de versão de aplicativo de todos os serviços e aplicativos de execução. Nesta fase, o testador de penetração começou a indexação (spider) e o mapeamento dos aplicativos, com e sem credenciais, em preparação para a fase de exploração. O testador recebeu permissão para concluir uma transação completa até o check-out e a confirmação de pedido.

Com a enumeração de destino concluída, o testador realizou o mapeamento de vulnerabilidade de serviços identificados usando ferramentas automatizadas e comparando a impressão digital de porta e serviço em relação a bancos de dados de vulnerabilidades conhecidas. Isso produziu uma lista de vulnerabilidades não confirmadas, que foram examinadas adicionalmente na fase de exploração dos testes.

A fase de exploração incluiu testes e técnicas concebidas para atender aos objetivos do teste. (Estes devem ser explorados e também podem ser usados para confirmar a eficácia dos controles de segurança auxiliares, como sistemas de detecção de invasão ou firewalls de aplicativos da Web). Durante esse passo, ocorreu o teste dos aplicativos para problemas relacionados ao OWASP Top 10 e outras estruturas de aplicativos da Web.

A fase final dos testes incluiu técnicas pós-exploração. O termo "pós-exploração" refere-se às ações tomadas após o comprometimento inicial de um sistema ou dispositivo. Geralmente descreve a abordagem metódica de usar técnicas de aumento de privilégios para obter acesso adicional a sistemas ou recursos de rede. A extensão em que foram realizadas técnicas pós-exploração foi definida antes do início do teste, para evitar que o testador colocasse sistemas de produção em risco de desestabilização.

As principais vulnerabilidades identificadas foram:

Alta:	<ul style="list-style-type: none"> ▪ Execução de código autenticado do aplicativo Apache Tomcat Manager ▪ Scripting entre sites (reflexivo) ▪ Diretório transversal
Média:	<ul style="list-style-type: none"> ▪ Protocolos obsoletos - SSLv2, SSLv3 ▪ Encriptadores SSL fracos ▪ Divulgação de endereço de IP interno
Baixo:	<ul style="list-style-type: none"> ▪ IPS não habilitado para local de recuperação de desastres ▪ Ataque lento de negação de serviço HTTP

Pós-engajamento (fase pós-execução)

Na conclusão deste exame, o testador de penetração se reuniu com o Cliente para descrever os resultados preliminares do teste e abordar quaisquer preocupações imediatas antes do relatório. A fase de pós-execução concentrou-se na análise das vulnerabilidades identificadas para determinar as causas raiz, estabelecer recomendações e/ou atividades de remediação e desenvolver um relatório final, onde todas as vulnerabilidades observadas durante o teste foram documentadas, mesmo que não tenham impacto sobre o ambiente de dados do portador do cartão.

O relatório de teste de penetração foi apresentado ao Cliente e foi discutido como o Cliente poderia remediar as vulnerabilidades observadas durante o teste de penetração. Observou-se que o ataque de negação de serviço e a falta de IPS, mesmo que problemas sérios para um varejista, não foram considerados relevantes para o PCI e não seriam necessários para obter um relatório limpo.

O Cliente corrigiu todas as vulnerabilidades de alta e média gravidade em 90 dias e a Empresa de Teste de Penetração forneceu a documentação de remediação bem-sucedida ao Cliente.

6.2 Estudo de caso do teste de penetração do provedor de hospedagem

Introdução ao caso

A PCIData Hosting é um provedor de serviços de hospedagem. O único ambiente de dados do titular do cartão que existe dentro da PCIData Hosting pertence ao seu cliente, compatível com PCI DSS, TechMerchant. A TechMerchant está operando um ambiente web de comércio eletrônico no hardware de hospedagem PCIData. A TechMerchant é a única responsável pela administração e manutenção de todos os softwares e aplicativos usados em seu ambiente de e-commerce. A PCIData Hosting está vinculada por contrato com a TechMerchant para manter a conformidade com o PCI. A PCIData Hosting precisa manter a conformidade com o PCI pela TechMerchant, uma vez que a PCIData Hosting oferece serviços críticos de segurança para a TechMerchant para sua conformidade com o PCI DSS. Além disso, a PCIData Hosting deseja estender esse tipo de serviço de hospedagem PCI DSS para mais clientes no setor de cartões de pagamento.

A PCIData Hosting está gerenciando os sistemas no ambiente de dados do portador do cartão e é responsável pela segurança física, hardware, rede, firewalls e SO, incluindo atualizações, configuração etc.

Aplicativos e bancos de dados não são de responsabilidade da PCIData Hosting.

Armazenar, processar e transmitir dados do titular do cartão está no escopo da TechMerchant, sendo descrito e avaliado em sua própria Avaliação do PCI DSS. A PCIData Hosting não tem nenhum tipo de transações de dados do titular do cartão no escopo, e a única entidade hospedada pela PCI é a TechMerchant, para quem só fornecem serviços de hospedagem de hardware e gerenciamento lógico do sistema.

Descrição do ambiente

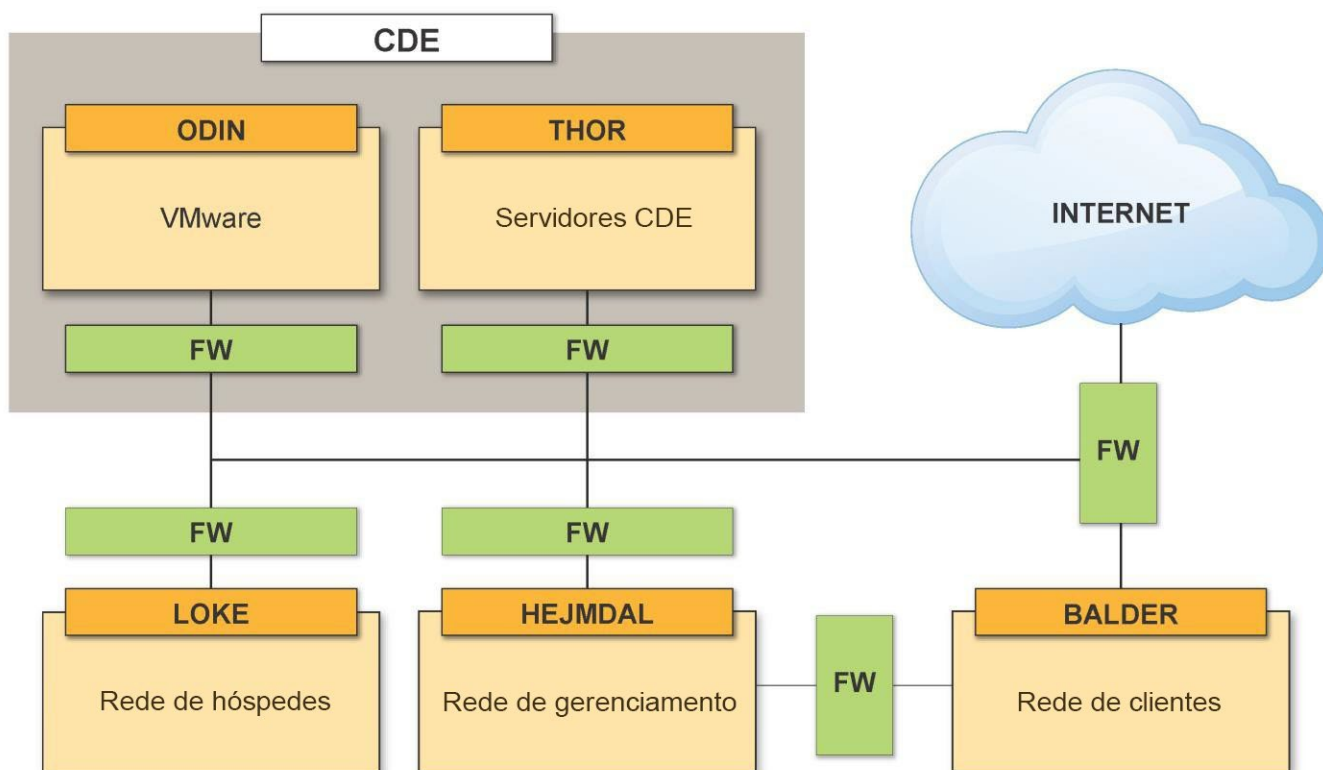
O ambiente na PCIData Hosting consiste em cinco redes diferentes:

- **Zona de rede ODIN:** Apenas os VMware Hypervisors usados para os servidores e ambiente do CDE da TechMerchant estão hospedados neste segmento de rede. Esta rede não está acessível a partir da rede THOR.
- **Zona de rede THOR:** Esta rede é o ambiente CDE onde a TechMerchant colocou seus servidores virtuais; todos os servidores localizados nesta rede estão no escopo PCI. A rede é separada em redes menores: DMZ, zona de banco de dados segura e uma zona de aplicação. Essas redes estão incluídas no teste de penetração realizado na TechMerchant.
- **Zona de rede LOKE:** Rede para convidados, usada para consultores externos, outros convidados, dispositivos BYOD etc. Esta é a única rede que tem pontos de acesso sem fio conectados.

- **Zona de rede HEJMDAL:** Rede de gerenciamento, a partir da qual a hospedagem PCIData gerencia as diferentes redes de clientes que não se enquadram no escopo PCI. Esta rede é usada apenas para gerenciar servidores não CDE.
- **BALDER:** Todos os outros clientes são hospedados nesta rede, incluindo a própria rede de escritório da PCIData Hosting.

Todas as redes são separadas por firewalls e o acesso aos segmentos de rede ODIN e THOR é restrito à autenticação de dois fatores. A única rede sem fio está conectada ao LOKE (a rede para convidados). O centro de dados está localizado na hospedagem PCIData e também está no escopo para conformidade com PCI.

Diagrama de rede de alto nível



Critérios de sucesso – Os critérios de sucesso para o teste de penetração são a obtenção de acesso ao CDE.

Lista de recursos (ambiente CDE)

- **ODIN** – Servidores VMware
- **THOR** – Servidores baseados em UNIX, incluindo servidores web; bancos de dados Oracle em uma zona segura
- Todos os funcionários da PCIData Hosting usam estações de trabalho baseadas na Microsoft para acessar o ambiente CDE.

Ativos de pré-engajamento (planejamento)

A metodologia usada para o teste de penetração foi baseada no NIST SP800-115; o teste de penetração incluiu as seguintes fases: Planejamento, descoberta, ataque/execução, pós-execução e relatório.

A fase de planejamento foi usada para reunir informações necessárias para a execução da avaliação, como os ativos a serem avaliados, as ameaças de interesse contra os ativos e os controles de segurança a serem usados para mitigar essas ameaças e desenvolver a abordagem de avaliação.

As redes ODIN (VMware) e THOR (servidores CDE) são os alvos do teste de penetração, já que esses servidores armazenam, processam e transmitem dados do titular do cartão.

Discussão de escopo

Foi discutido com a PCIData Hosting como gerenciaram seu ambiente CDE, incluindo servidores e bancos de dados. Os sistemas operacionais são administrados pela PCIData Hosting; todos os aplicativos e desenvolvimento são tratados pela TechMerchant. A PCIData Hosting e a TechMerchant administram bancos de dados. As informações criptografadas no banco de dados só são acessíveis com as chaves de criptografia mantidas pela TechMerchant. Todos os acessos ao ODIN e THOR são autenticados por uma solução de dois fatores. Isso também se aplica quando acessado de redes internas na PCIData Hosting.

O último teste de penetração da TechMerchant foi revisado para garantir que todos os perímetros, servidores etc., foram cobertos pelos testes. O aplicativo foi testado como parte do teste de penetração anual de PCI da TechMerchant e não foi considerado no escopo do teste de penetração PCI da PCIData Hosting, portanto o foco é o teste de camada de rede.

A seguinte documentação foi revisada antes da avaliação:

- Um diagrama de rede
- Os resultados de varreduras trimestrais de vulnerabilidade externa e interna
- Os resultados do último teste de penetração
- O escopo do último teste de penetração da TechMerchant
- Políticas de segurança
- Análise da análise de risco da PCIData Hosting.

Os seguintes testes foram realizados durante a avaliação:

- Testes de penetração interna em LOKE (rede para convidados), HEJMDAL (rede de gerenciamento) e da rede de escritório localizada em BALDER (Cliente).
- Engenharia social contra administradores de ODIN (VMware) e THOR (servidores CDE), da PCIData Holding, em forma de e-mails de phishing
- Avaliação de segurança física como parte do teste de penetração.
- Testes externos da PCIData Hosting de seus endereços de IP externos.

Todos os servidores, bancos de dados, funcionários com acesso ao CDE etc., foram considerados no escopo para o teste de penetração.

Preparações pré-teste

Uma conta de usuário foi criada para o testador de penetração, segundo os procedimentos regulares para conceder acesso a novos funcionários. Credenciais de acesso para a rede de convidados também foram concedidas ao testador.

Fase de engajamento (descoberta e ataque/execução)

A descoberta foi realizada nas redes LOKE (convidado), HEJMDAL (gerenciamento) e BALDER (escritório) para identificar alvos (servidores, componentes de rede, estações de trabalho etc.) nas redes, e as técnicas de análise foram usadas para compreender o ambiente. Os objetivos desta fase foram identificar sistemas, portas, serviços e possíveis vulnerabilidades. Esta fase foi realizada manualmente e por meio de ferramentas automatizadas, incluindo descoberta de rede e detecção de porta e serviço.

Quando dados suficientes foram coletados na fase de descoberta, o testador de penetração tentou obter acesso aos alvos descobertos. Quando o acesso foi obtido aos alvos, o testador tentou aumentar os privilégios para obter o controle total do alvo. O acesso obtido foi então usado para obter mais informações sobre o ambiente e uma nova fase de descoberta foi iniciada.

O objetivo principal para a descoberta e o ataque/execução era obter acesso ao CDE, incluindo os hosts VMware. As técnicas usadas incluíram craqueamento de senha, varredura de vulnerabilidades, engenharia social e testes de camada de rede.

Os procedimentos acima foram executados para as seguintes perspectivas, durante a avaliação:

- Atacante externo sem conhecimento do ambiente
- Atacante interno (convidado, terceirizado etc.)
- Atacante interno (funcionário sem acesso ao CDE) Os

seguintes testes foram realizados durante a avaliação:

- **Atacante externo sem conhecimento do ambiente**
 - A conexão VPN externa foi testada.
 - Foram enviados e-mails de phishing para vítimas cuidadosamente selecionadas, que estão trabalhando com a administração do ambiente CDE.
 - Tentativas de obter acesso ao data center sem ter notificado o data center antes.

Não foram encontradas vulnerabilidades relacionadas à conexão VPN durante o teste externo. Os e-mails de phishing foram enviados, mas as explorações foram capturadas pela instalação do antivírus da PCIData Hosting. Não foi possível obter acesso ao data center sem primeiro ser autorizado pela PCIData Hosting.

- **Atacante interno**
 - Foram realizados ataques da rede para convidados
 - Foram realizados ataques da rede de gerenciamento
 - Foram realizados ataques da rede do escritório

Vulnerabilidades foram encontradas nas diferentes redes e o testador conseguiu explorar essas vulnerabilidades, mas não conseguiu usá-las para obter acesso ao ODIN ou THOR.

As principais vulnerabilidades identificadas foram:

- ***Man in the middle*** – Foi possível realizar um ataque "man-in-the-middle" usando envenenamento por ARP, mas o testador não pode extrair nenhuma informação sensível que pudesse fornecer informações sobre como obter acesso ao ODIN ou THOR.
- ***Política de senha fraca implementada*** – Configurações de senha fraca em servidores locais na rede BALDER foram usadas para comprometer contas nesta rede. O testador não pode usar essas contas para obter acesso ao ODIN ou THOR. Como esses servidores não estão no escopo da PCI, a política de senha fraca não foi considerada como tendo impacto sobre a conformidade.
- ***Contas de usuários antigos foram comprometidas*** – O testador pode comprometer as contas de usuário que foram criadas, mas nunca foram usadas na rede BALDER. As contas comprometidas não concederam acesso ao ODIN ou THOR.
- ***Outras*** – Outras vulnerabilidades foram identificadas, como transferência de zona, software desatualizado e uso de protocolos não criptografados; essas vulnerabilidades foram relacionadas à rede LOKE ou BALDER e não concederam acesso ao ODIN ou THOR mesmo quando exploradas.

Pós-engajamento (fase pós-execução)

A fase de pós-execução concentrou-se na análise das vulnerabilidades identificadas para determinar as causas raiz, estabelecer recomendações e/ou atividades de remediação e desenvolver um relatório final, onde todas as vulnerabilidades observadas durante o teste foram documentadas, mesmo que elas não tenham impacto sobre o ambiente de dados do portador do cartão.

O relatório de teste de penetração foi apresentado ao Cliente e foi discutido como o Cliente poderia remediar as vulnerabilidades observadas durante o teste de penetração. Foi confirmado que nenhuma das vulnerabilidades teve efeito sobre o ambiente de dados do portador do cartão.

Uma vez que não foram detectadas vulnerabilidades significativas relacionadas ao ambiente CDE e o acesso ao ambiente CDE não foi obtido, não foi realizado o teste de correção.

6.3 Estudo de caso de teste de penetração no comerciante de varejo

Introdução ao caso

Neste exemplo, o negócio é uma empresa de vestuário de varejo chamada Green Clothing. Os dados do titular do cartão são coletados como uma transação de cartão, passando ou digitando o cartão em um terminal POS. As informações são então enviadas para um servidor local em cada loja, antes de serem enviadas para o processador. Nenhum dado do titular do cartão é transmitido entre lojas ou de volta para a empresa. Após receber uma confirmação do processador, os dados do titular do cartão são removidos do servidor POS. O servidor POS executa um aplicativo de ponto de venda do PA-DSS.

A empresa tem uma conexão VPN persistente em cada loja, para permitir a administração de recursos em rede, acesso a gravações de CCTV e verificação de estoque.

Descrição do ambiente

O ambiente na Green Clothing consiste de seis lojas e um escritório corporativo.

Todas as lojas foram determinadas como sendo configuradas de forma idêntica e foram segmentadas em duas redes:

- Rede POS – Ambiente de dados do titular do cartão (CDE)
 - 2 dispositivos POS
 - 1 Servidor POS
- Rede geral da loja (não CDE)
 - 1 estação de trabalho do gerente
 - 1 servidor de CCTV

A empresa é composta por dois segmentos de rede:

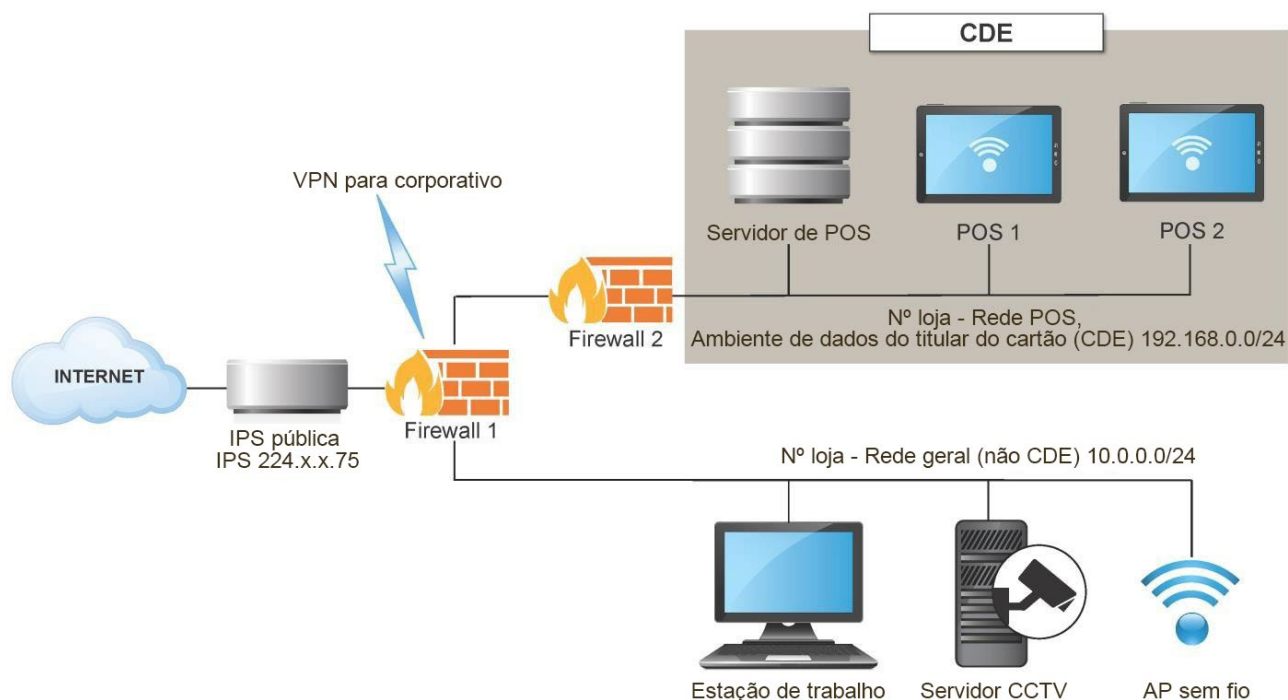
- Rede de usuários gerais corporativos (não CDE)
 - 4 estações de trabalho
 - 1 ponto de acesso wireless
- Rede de gerenciamento de TI corporativa (não CDE)
 - 3 estações de trabalho usadas para gerenciar servidores CDE

Descrição do acesso

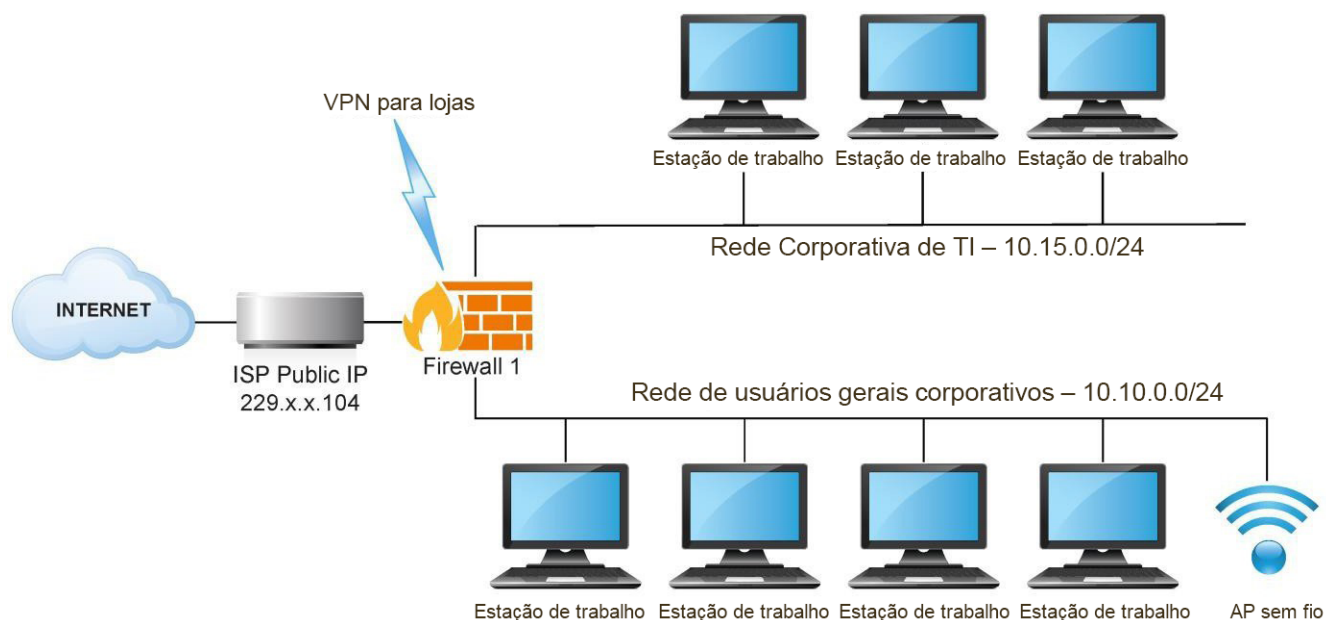
A tabela abaixo descreve o acesso de todas as redes não CDE ao CDE. Esta definição de acesso ajudará a determinar que tipos de testes devem ser realizados e de onde.

Rede de origem (não CDE)	Rede de destino (CDE)	Acesso
Rede de usuários gerais corporativos	Rede de POS da loja	Nenhum – Segmentado
Rede de gerenciamento de TI corporativa	Rede de POS da loja	SSH para servidor POS
Rede geral da loja	Rede de POS da loja	Nenhum – Segmentado

Exemplo de diagrama de rede de lojas



Exemplo de diagrama de rede corporativa



Atividades de pré-engajamento

As redes de POS em cada loja são consideradas como o ambiente de dados do portador do cartão e são o alvo do teste de penetração. Os servidores desta rede em cada loja são os servidores que armazenam, processam e transmitem dados do titular do cartão.

Discussão de escopo

Foi discutido com a empresa Green Clothing como ela gerenciou seu ambiente CDE, especificamente como os servidores e bancos de dados são administrados. Toda a administração é realizada da rede de TI na empresa através da conexão VPN.

A seguinte documentação foi revisada antes da avaliação:

- Um diagrama de rede
- Os resultados de varreduras trimestrais de vulnerabilidade externa e interna
- Os resultados do último teste de penetração
- O escopo do último teste de penetração da Green Clothing
- Políticas de segurança
- Revisão da análise de risco da Green Clothing

Definição do escopo final

Após a revisão de todos os materiais fornecidos, a Green Clothing e o testador de penetração chegaram a um acordo sobre a definição do escopo.

Teste de penetração externa

Os testes incluíram avaliação dos seguintes recursos voltados para a Internet:

- Seis IPs públicos de loja

Teste de penetração interna

Com base nas informações que todas as lojas são configuradas de forma idêntica, testes internos foram realizados em duas lojas. Qualquer vulnerabilidade identificada deve existir em todas as lojas. Os testes incluíram avaliação das seguintes perspectivas de teste exclusivas, visando duas redes POS de lojas:

Tabela x: Escopo de testes de penetração na camada de rede

Rede de perspectiva	Rede direcionada
Rede corporativa de TI	Loja nº 1 – Rede POS
Rede corporativa de TI	Loja nº 2 – Rede POS

Tabela y: Escopo do teste de segmentação

Rede de perspectiva	Rede direcionada
Rede de usuários gerais corporativos	Loja nº 1 – Rede POS
Loja 1 – Rede geral	Loja nº 1 – Rede POS
Rede de usuários gerais corporativos	Loja nº 2 – Rede POS
Loja 2 – Rede geral	Loja nº 2 – Rede POS

Preparações pré-teste

O testador de penetração recebeu um acesso de nível de rede em cada uma das perspectivas de teste definidas.

- Rede corporativa de TI
- Rede de usuários gerais corporativos
- Rede geral da Loja 1
- Rede geral da Loja 2

O testador de penetração também recebeu as informações internas de IP para a rede POS na loja de destino de amostra. Nenhum outro acesso de rede ou credenciais de usuário foram fornecidos.

Fase de engajamento

Os critérios de sucesso para o teste de penetração foram definidos como acesso ao ambiente CDE e acesso aos dados do portador do cartão.

Com base no escopo definido, os seguintes cenários de ataque diferentes foram avaliados:

- Atacante externo sem conhecimento do ambiente
- Atacante interno sem acesso CDE (convidado, terceirizado etc.) na rede geral da loja ou na rede geral corporativa
- Atacante interno obtendo acesso não autorizado ao segmento de rede de gerenciamento de TI corporativa e passando a atacar as lojas como administrador

Fase de relatório

O testador de penetração relatou os seguintes itens após concluir o teste.

Teste de penetração externa

Nenhum item notável relatado. Determinou-se que os únicos serviços acessíveis publicamente eram os pontos de conexão VPN, que foram verificados e considerados seguros.

Teste de penetração interna

Abaixo estão descritas as vulnerabilidades identificadas durante o teste de penetração interna.

- ***Vulnerabilidade n.º 1 – Falha na segmentação***

Resumo: Descobriu-se que o firewall n.º 2 (firewall CDE) foi configurado para permitir acesso irrestrito (todas as portas e serviços) da rede geral da loja (10.0.0.0/24) à rede POS da loja (192.168.0.0/24).

- ***Vulnerabilidade n.º 2 – Credenciais de usuário padrão no servidor POS***

Resumo: Credenciais padrão foram habilitadas no aplicativo de terceiros, executado no servidor POS. Usando essas credenciais, o testador de penetração conseguiu obter acesso de nível administrativo ao servidor POS.

Pós-engajamento

A Green Clothing analisou o relatório de teste de penetração e implementou correções para cada item identificado.

O testador de penetração realizou testes adicionais para confirmar que as atividades de remediação resolveram suficientemente os itens relatados. Foi fornecido um relatório atualizado, que mostrou os itens como remediados.

Anexo A: Tabela de referência rápida para orientação sobre requisitos de teste de penetração do PCI DSS

Requisito 11.3x do PCI DSS	Seção(s) de Suplemento Informativo(s) Contendo Orientação
Sub-itens da metodologia de teste de penetração 11.3:	
– Com base em abordagens aceitas pelo setor	3.1, 4.4, 5.1.1, 5.1.2, 5.2
– Cobertura para CDE e sistemas críticos	2.2, 2.2.4, 4.1.1
– Inclui testes externos e internos	2.2.1, 2.2.2
– Teste para validar controles de segmentação	2.2.3, 4.2.3
– Teste de camada de aplicativo	2.3, 4.2.1
– Testes de camada de rede para rede e SO	2.3, 4.2.2

Agradecimentos

O PCI SSC gostaria de reconhecer a contribuição do Grupo de Interesse Especial de Orientação de Teste de Penetração (Penetration Testing Guidance Special Interest Group, SIG) na preparação do documento original, publicado em 2015. A Diretriz de Teste de Penetração SIG consistiu de representantes das seguintes organizações:

Accuvant, Inc	Convergys Corp
Agio, LLC	CradlePoint
Alaska Airlines	Crosskey Banking Solutions
A-align Security and Compliance Services	Crowe Horwath LLP
Allstate Insurance	DataFlight Europe AS
Aperia Solutions	Delhaize America Shared Services Group, LLC
AT&T Consulting Solutions	Dell, Inc.
atsec (Beijing) Information Technology Co., Ltd	Deluxe Corp.
Bally Total Fitness	Diamond Resorts Corp.
Bank Of New Zealand	Digital Defense, Inc.
Bashas' Inc.	Domino's Pizza, Inc.
BB&T Corporation	DST Output
Conselho de Curadores da University of Arkansas	Enterprise Holdings, Inc.
Bridge Point Communications	EVO Payments International
The Brick Group	EVERY A/S
BrightLine CPAs & Associates, Inc.	Experian Information Services
British Airways PLC	Exxon Mobil Corporation
BT PLC	Tax Systems, Inc.
Canadian Tire Financial Services	Fiserv Solutions, Inc.
CBIZ Security & Advisory Services, LLC	FishNet Security
CDG Commerce	Foregenix
CenturyLink	Foresight IT Consulting Pty Ltd.
Cisco Systems, Inc.	FortConsult A-S
Citigroup Inc.	Games Workshop Ltd
Clydesdale Bank PLC	Gap Inc.
Coalfire Systems, Inc.	Global Payments Direct, Inc.
Compass IT Compliance, LLC	Grant Thornton
Computer Services, Inc.	Groupement Interbancaire Monétique de L'uemoa (GIM-UEMOA)
Comsec	GuidePoint Security, LLC
ControlScan Inc.	

Hewlett-Packard	SecurityMetrics, Inc.
Hitachi-Omron Terminal Solutions, Corp.	Sense of Security Pty Ltd.
IBM Corporation	Sikich LLP
Internet Security Auditors	SISA
IQ Information Quality	SIX Payment Services Ltd
Isis Mobile Commerce	Solutionary, Inc.
Jet Infosystems	Starwood Hotels & Resorts Worldwide, Inc.
Liverpool Victoria Friendly Society	State Farm Mutual Automobile Insurance Company
Lloyds Banking Group	StoreFinancial Services
MegApath Inc.	Structured Communication Systems, Inc.
MobileIron, Inc.	Sword & Shield Enterprise Security, Inc.
Módulo Security Solutions S.A.	Symantec Corporation
MTI Technology, Ltd.	Sysnet Limited
National Australia Bank	Telstra
Nettitude, Ltd.	Tesco Stores Ltd.
NIC Inc.	Tieto Latvia SIA
Novacoast	TIVIT (Terceirização de Tecnologia e Serviços S/A)
NRI Secure Technologies	Trustwave Holdings, Inc.
NTA Monitor Ltd.	TSYS
NTT Security Ltd.	TUI Travel PLC
Online Enterprises	U.S. Bancorp
Outerwall	U.S. Cellular
Payment Software Company (PSC)	UL Transaction Security PTY Ltd.
PayPal, Inc.	University of Oklahoma
Pier1 Imports	UPS (United Parcel Service)
Princeton Payment Solutions LLC	usd AG
Progressive Casualty Insurance Company	Verizon Wireless
Promocion y Operacion SA de CV	VigiTrust Ltd.
Rapid7 LLC	Vodat International Ltd.
RBC Royal Bank	The Walt Disney Company
RBS	Westpac Banking Corporation
Right Time Limited	Xpient Solutions LLC
Secured Net Solutions Inc.	
SecureNet	

Sobre o PCI Security Standards Council

O PCI Security Standards Council é um fórum global aberto, responsável pelo desenvolvimento, gerenciamento, educação e conscientização dos Padrões de Segurança do PCI (PCI DSS) e outros padrões que aumentam a segurança de dados de pagamento. Fundado em 2006 pelas marcas de cartões de pagamento American Express, Discover Financial Services, JCB International, Mastercard e Visa Inc., o conselho tem mais de 700 empresas participantes, representando comerciantes, bancos, processadores e fornecedores, em todo o mundo. Para saber mais sobre como participar de dados de cartão de pagamento globalmente, acesse: pcisecuritystandards.org.