# **CompTIA PenTest+**

**Orientações gerais:**

A Pentest+ não é uma prova prática; no entanto, exige um conhecimento prático considerável por parte do profissional, incluindo habilidades em ferramentas e compreensão do cotidiano de trabalho de um pentester, desde a formalização de contratos para o início do pentest até a entrega do relatório e os acompanhamentos subsequentes. Trata-se de uma prova baseada em desempenho e questões com múltipla escolha. Assim durante a prova, nos depararemos com questões que simulam atividades reais do dia a dia de um pentester.

Cursos e livros desempenham um papel crucial ao relembrar e internalizar detalhes específicos, especialmente em áreas teóricas como contratos de trabalho e leis. No entanto, a prática é fundamental para o sucesso na prova. Se você não tem uma experiência prática no seu trabalho diário, eu altamente recomendaria a participação em laboratórios de exercícios práticos e de Capture The Flag (CTF) para se familiarizar especialmente com as ferramentas envolvidas nos testes. Ao considerar as referências, incluirei alguns links que considero excelentes para estudar para a prova.

**O exame**

O exame Pentest+ vai cobrar 5 dominios, sendo eles:

***Planning and Scoping 14%***

***Information Gathering and Vulnerability Scanning 22%***

***Attacks and Exploits 30%***

***Reporting and Communication 18%***

***Tools and Code Analysis 16%***

***Total 100%***

A prova pode ter um número máximo de 85 questões, mas isso não significa que a sua prova terá 85 questões. No meu caso, fiz um total de 68 questões, incluindo 3 questões de desempenho. O exame tem uma duração de 165 minutos e pode ser realizado em inglês, japonês, português e tailandês.

**Exemplos de perguntas (Respostas no final)**

1. **Que tipo de documento legal é frequentemente usado para proteger a confidencialidade dos dados e outras informações que pentesters podem encontrar?**
   1. SOW
   2. NDA
   3. MSA
   4. Clausura de não-competição
2. **As redes da sua organização contêm quatro sub-redes: 10.0.0.0, 10.0.1.0, 10.0.2.0 e 10.0.3.0. Usando o nmap, como você pode verificar todas as 4 sub-redes usando um único comando?**
   1. nmap -Pn 10.0.0.0/25
   2. nmap -Pn 10.0.0-3.0
   3. nmap -Pn 10.0.0.0,1.0,2.0,3.0
   4. nmap -Pn 10.0.0.0/23

**Questões de desempenho**

No meu caso, enfrentei três questões de desempenho, cada uma dividido em duas partes:

* A primeira parte do cenário 1 consistiu em analisar a saída da ferramenta Nmap e, com base nisso, identificar as flags utilizadas para obter aquele resultado. Na segunda parte da questão, foi necessário analisar os resultados da saída e identificar o ponto mais interessante para exploração, que serviria como ponto de partida para um pentester. **Conhecimentos necessários para essa questão:** Nmap: flags e análise de saídas, básico de exploração.
* No segundo cenário, referente a vulnerabilidades web, foram apresentados 10 trechos de códigos e payloads de exploração. A tarefa consistia em associar cada um deles à sua vulnerabilidade correspondente, seja explorada ou potencial. As opções incluíam: Open redirect, XSS refletido, XSS Dom, XSS armazenado, SQLi boolean e SQLi blind. Na segunda parte da questão, solicitava-se a associação de cada uma dessas vulnerabilidades catalogadas às suas respectivas medidas de prevenção, que incluíam limitação de URL, parametrização de entradas e algumas possibilidades de Regex. **Conhecimentos necessários para essa questão:** OWASP top 10: exploração e correções, Regex.
* No terceiro cenário, ainda focado no ambiente web, era necessário analisar alguns cenários e identificar a quais vulnerabilidades cada um deles estava sujeito. O primeiro cenário redirecionava para uma segunda página, a qual abria um certificado digital com algumas informações importantes expostas. O segundo mostrava o código fonte de uma página de login, e o terceiro exibia uma série de cookies que um site armazenava. Após a análise dos três cenários e a identificação das vulnerabilidades tratadas por cada um deles, na segunda parte da questão, foi necessário identificar as correções necessárias para cada cenário. **Conhecimentos necessários para essa questão:** Ciclo de vida de um certificado digital, análise de cookies, análise de código.

**Conteúdos de estudos**

* **Contratos legais:**

**Declaração de trabalho (statement of work (SOW))** é um documento formal que detalha as tarefas, restrições, remuneração e outros termos acordados para a realização de um compromisso profissional. Inclui informações sobre o que deve ser feito, o que não é permitido, o valor a ser pago e as responsabilidades do testador e do cliente. Além disso, costuma abranger o cronograma, as entregas esperadas e os detalhes para pagamentos.

**Contrato de serviço principal (master service agreement (MSA))** é um contrato especializado utilizado por aqueles que realizam trabalhos recorrentes para a mesma organização. Ele funciona como um acordo-quadro, estabelecendo antecipadamente a maioria dos termos, o que agiliza a emissão rápida de novos contratos por meio de breves declarações de trabalho. Isso simplifica o processo de contratação, pois a maior parte dos detalhes já está previamente acordada no contrato principal de serviços.

**Contrato de nível de serviço (service-level agreement (SLA))** descreve não apenas os serviços e seus níveis esperados, mas também incorpora métricas para avaliação. Ele delineia responsabilidades, penalidades por violações, e um protocolo para ajustar métricas. O SLA estabelece padrões e expectativas claros para as partes envolvidas no contrato de prestação de serviços.

**Acordo de Confidencialidade (Non-Disclosure Agreement - NDA)** é um documento legal que estipula que as partes concordam em não compartilhar informações confidenciais, conhecimento ou materiais com terceiros não autorizados.

* **Leis e regulamentos:**

**Lei Geral de Proteção de Dados (GDPR)** da União Europeia estabelece requisitos específicos para a proteção de dados do consumidor. Ele afirma que a coleta, processamento e retenção de dados pessoais só podem ocorrer com o consentimento informado do indivíduo. Os dados devem ser coletados e processados apenas para o propósito declarado, o qual deve ser claramente descrito ao usuário. Além disso, o GDPR inclui disposições legais para garantir que o usuário tenha o direito de retirar seu consentimento a qualquer momento.

**Padrão de Segurança de Dados do Setor de Cartões de Pagamento (PCI DSS)** não é um regulamento, mas sim um padrão estabelecido pela indústria. Enquanto os padrões não têm a aplicação legal de regulamentos, o PCI DSS impõe penalidades por não conformidade. Este padrão é um acordo contratual que organizações que lidam com informações de cartões de crédito devem seguir.O PCI DSS define controles que as organizações devem implementar para reduzir vulnerabilidades, aplicar controle de acesso robusto e realizar testes e monitoramento consistentes da infraestrutura. As organizações são categorizadas em quatro níveis de segurança com base no volume de transações que realizam anualmente. **Nível 1:** Grandes comerciantes que processam mais de seis milhões de transações por ano, requerem um auditor externo, conhecido como Avaliador de Segurança Qualificado (QSA), para conduzir a avaliação do PCI DSS, e devem apresentar um Relatório de Conformidade (ROC). **Níveis 2, 3 e 4:** Comerciantes de menor porte, também necessitam apresentar um Relatório de Conformidade, mas têm a opção de realizar autoavaliações, sem a necessidade de um auditor externo. Os níveis 2, 3 e 4 diferem com base no volume de transações, com o nível 2 processando entre um e seis milhões, o nível 3 entre 20.000 e um milhão, e o nível 4 menos de 20.000 transações por ano.

Além disso, o PCI DSS exige varreduras de vulnerabilidade a serem realizadas a cada 90 dias e após mudanças significativas na infraestrutura. Estas medidas visam garantir a segurança das transações com cartões de crédito e proteger as informações dos titulares dos cartões.

**HIPAA (Health Insurance Portability and Accountability Act)** Essa lei estabelece padrões para preservar a privacidade e segurança das informações de saúde, assegurando a confidencialidade e integridade desses dados.

**Sarbanes-Oxley (SOX)** é uma legislação que afeta corporações americanas de capital aberto. As organizações sob essa regulamentação devem aderir a métodos contábeis e práticas de relatórios financeiros específicos.

**Gramm-Leach-Bliley (GLBA):** A GLBA impacta instituições financeiras, regulamentando a segurança de informações pessoais e financeiras (PII) e proibindo o compartilhamento desses dados com terceiros, enquanto fornece orientações para sua proteção.

**Federal Information Security Management Act (FISMA):** O FISMA afeta órgãos federais dos EUA, estabelecendo a obrigação de desenvolver, documentar e implementar programas de segurança da informação para fortalecer as redes em todo o governo federal.**Lei Federal de Privacidade de 1974:** Esta lei se aplica aos sistemas de computadores do governo dos EUA, regulamentando a coleta, armazenamento, uso e disseminação de informações pessoalmente identificáveis (PII).

**Lei de Privacidade e Direitos Educacionais da Família (FERPA):** A FERPA protege a privacidade dos registros educacionais dos alunos em instituições financiadas pelo Departamento de Educação dos EUA, cobrindo faculdades e universidades no país.

**Lei de Proteção à Privacidade Online das Crianças (COPPA):** A COPPA impõe requisitos a sites e serviços online direcionados a crianças menores de 13 anos, bem como a outros que coletam informações pessoais online de crianças dessa faixa etária.

* **Cyber kill chain:**

**Reconhecimento (Recon):** Fase inicial de coleta de informações e análise de vulnerabilidades no sistema, visando identificar possíveis brechas para exploração.

**Armamento (Weaponization):** Nesta fase, o profissional busca e desenvolve ferramentas e técnicas específicas para a exploração do alvo.

**Entrega (Delivery):** Após a escolha da ferramenta, esta etapa envolve a entrega dos payloads no alvo, através de métodos como e-mails maliciosos, engenharia social ou dispositivos USB infectados.

**Exploração (Exploitation):** Após a entrega do malware no escopo da organização, esta fase inicia o processo de exploração do alvo, aguardando um gatilho que ative o malware, como a execução de um arquivo malicioso ou a exploração de uma vulnerabilidade na rede.

**Instalação (Installation):** Após o acesso inicial, esta fase é usada para estabelecer permanência no alvo, geralmente por meio de backdoors ou web shells.

**Comando e Controle (Command and Control, C2C):** Após estabelecer o acesso ao sistema, esta fase permite o controle do sistema através da execução de comandos, possibilitando a exploração completa e o tratamento desses sistemas como bots para ataques de DDoS.

**Ações no Objetivo (Actions on Objectives):** Nesta fase, que ocorre após o C2C, são realizadas as ações que motivaram o ataque, como escalonamento de privilégios, movimentação lateral, exclusão, alteração ou coleta de dados, ou o uso do sistema como um bot.

* **Padrões e metodologias de testes**

**MITRE ATT&CK Framework:** O MITRE ATT&CK Framework é uma base de conhecimento abrangente que aborda táticas e técnicas adversárias, oferecendo descrições detalhadas e exemplos para o ciclo de vida da ameaça. Embora não seja um padrão completo de teste de penetração, é valioso para testadores focados em conceitos e práticas.

**Open Web Application Security Project (OWASP):** O OWASP fornece guias de teste para segurança na web, móvel e firmware, além de orientações sobre o uso de outras metodologias e padrões de teste. Sua ênfase está na segurança de aplicações web.

**Padrão de Execução de Teste de Penetração (PTES):** O PTES abrange desde interações pré-engajamento até detalhes sobre lidar com terceiros, oferecendo uma gama completa de técnicas e conceitos de teste de penetração. É considerado um dos padrões mais completos e modernos disponíveis abertamente.

**Manual de Metodologia de Teste de Segurança de Código Aberto (OSSTMM):** O OSSTMM é um guia amplo de metodologia de teste de penetração, abordando análise, métricas, fluxos de trabalho, segurança humana, física e sem fio. No entanto, sua última atualização foi em 2010.

**Instituto Nacional de Padrões e Tecnologia (NIST):** O NIST fornece padrões, incluindo testes de penetração, como parte da publicação NIST 800-115. No entanto, sua última atualização foi em 2008, e embora continue a influenciar metodologias de teste de segurança, não é considerado um documento moderno.

**Estrutura de Avaliação de Segurança de Sistemas de Informação (ISSAF):** O ISSAF do OSSIG é uma estrutura detalhada de teste de penetração, mas está desatualizado, com a última atualização em 2005. Embora ofereça informações valiosas, os testadores modernos podem preferir outras estruturas mais atualizadas.

* **Reconhecimento ativo e passivo**

O reconhecimento passivo no pentest é uma fase em que informações sobre um alvo são coletadas sem interações diretas com os sistemas. Isso inclui a pesquisa online, consulta de fontes abertas, análise de registros DNS e identificação de redes. O objetivo é obter dados sem alertar o alvo sobre a atividade de coleta.

Já o reconhecimento ativo no pentest envolve interações diretas com os sistemas-alvo para identificar vulnerabilidades e pontos de entrada. Isso inclui varreduras de portas, busca por vulnerabilidades e tentativas de autenticação. Diferentemente do reconhecimento passivo, as atividades podem ser detectadas pelos sistemas de segurança do alvo.

* **Sistemas Embarcados:**

**PLC (Program Logic Controller):** Computador industrial projetado para automação e monitoramento de sistemas mecânicos em ambientes industriais.

**System on chip**: Integração de vários componentes de controle em um único chip, reduzindo a complexidade.

**FPGA (Field Programmable Gate Array**): Processador programável para executar funções específicas após a fabricação, oferecendo flexibilidade.

**Rede de Área do Controlador (CAN):** Rede serial para comunicação entre controladores lógicos programáveis, comumente utilizada em veículos para interligar sistemas.

**Serviço de Distribuição de Dados (DDS**): Facilita interoperabilidade em redes de máquinas conectadas, garantindo escalabilidade e desempenho em aplicações industriais.

**Sistema Instrumentado de Segurança (SIS):** Composto por sensores, solucionadores lógicos e elementos de controle para retornar um processo industrial a um estado seguro após a detecção de condições predeterminadas.

* **Mobile**

**Enterprise Mobility Management (EMM) e Gerenciamento de Dispositivos Móveis (MDM):** Descreve um conjunto de políticas e ferramentas tecnológicas para a gestão centralizada e controle de dispositivos móveis em um ambiente corporativo.

**EMM:** Refere-se às políticas e ferramentas implementadas.

**MDM:** Envolve os controles técnicos utilizados para assegurar a conformidade.

**Técnicas de aquisição de dispositivos:**

**COBO (Corporate-Owned, Business-Only):** Propriedade e gestão integral pela organização.

**COPE (Corporate-Owned, Personally Enabled):** Dispositivos gerenciados pela empresa, permitindo uso pessoal.

**CYOD (Choose Your Own Device):** Funcionários escolhem dispositivos de uma lista aprovada.

**BYOD (Bring Your Own Device):** Funcionários usam dispositivos pessoais conectados à rede corporativa.

**VMI (Virtual Mobile Infrastructure):** Utiliza um sistema operacional móvel virtualizado, semelhante ao VDI.

* **Engenharia Social e Ataques Físicos**

**Engenharia social:** é a manipulação de usuários para obter informações confidenciais, contornando controles técnicos ao focar no elemento humano, buscando hackear comportamentos em vez de sistemas tecnológicos.

**Phishing:** Phishing é um tipo de ataque em que um ator malicioso se comunica com a vítima, aparentando ser de uma fonte confiável, para obter informações confidenciais. Existem variantes específicas desse método.

**Tipos de ataques: Phishing:** Ataque genérico por e-mail, busca atingir um amplo público, esperando que alguém clique no link fornecido.

**Spearphishing:** Variação mais direcionada do phishing, focalizada em uma pessoa ou grupo específico, utilizando tecnologia e técnicas similares.

**Whaling:** Foco altamente específico, direcionado aos principais executivos da organização, como CEO, CFO, entre outros.

**Smishing:** Envio de mensagens de texto com links maliciosos ou números de telefone falsos para enganar as vítimas.

**Vishing:** Comunicação por voz, geralmente por telefone, onde o invasor finge ser outra pessoa.

**Comprometimento de E-mail Comercial (BEC):** Ocorre quando um invasor se passa por um executivo de alto nível ou compromete a conta de e-mail desse executivo.

**Pharming:** Diferente do phishing, envolve redirecionar vítimas para um site malicioso manipulando configurações do navegador ou executando processos em segundo plano.

**Baiting:** Explora a curiosidade ou ganância da vítima. Oferece conteúdo tentador, como a promessa de um prêmio. Exemplo: "Parabéns! Você ganhou um prêmio!"

* **Physical Attacks**

**Tailgating:** Invasor segue uma pessoa autorizada para acessar uma área segura sem permissão.

**Piggybacking:** Invasor entra em uma área restrita seguindo um funcionário autorizado com conhecimento ou consentimento.

**Shoulder surfing:** Invasor observa o comportamento do alvo de perto para obter informações confidenciais.

**Eavesdropping (Escuta clandestina):** Escuta conversas importantes para o ataque.

**Dumpster diving:** Coleta de informações de arquivos descartados no lixo.

**Badge cloning:** Copia dados de autenticação do crachá de um usuário autorizado.

**Gatilhos ExploradosAutoridade:** Pessoas mais propensas a cumprir instruções de quem está em posição de autoridade.

**Urgência:** A pressa constante leva as pessoas a agirem mais rapidamente.

**Prova Social (Social Proof):** Maior propensão a seguir ações com base em curtidas, compartilhamentos e comportamentos de amigos.

**Escassez:** Induzir ação rápida através da sensação de falta.

**Semelhança/Simpatia:** Preferência por interagir com pessoas amigáveis, atraentes e confiáveis.

**Medo:** Utilização de ameaças ou exigências para forçar ações, como em casos de ransomware.

* **Cloud based attacks**

**Ataque de canal lateral (side-Channel attack):** é um tipo de ataque que tem como objetivo medir ou explorar os efeitos indiretos de um sistema em vez de direcionar o código ou programa diretamente.

**Ataque direto à origem ou D2O (Direct-to-origin):** Um ataque direto à origem tentará para ignorar os proxies reversos para atacar diretamente a rede original ou endereço IP desse servidor baseado em nuvem.

**DoS - Amplification/Volumetric attacks:** Uma amplificação ou ataque volumétrico é usado para saturar a largura de banda de um determinado recurso de rede.

**DoS - Fragmentation of requests:** Enviar múltiplos fragmentos de solicitações HTTP para o servidor

* **Ataques a redes sem fio**

**Eavesdropping (Sniffing de Rede):** Monitorar o tráfego de rede em modo promíscuo para realizar escutas sem fio.

**Deauthentication:** Forçar um cliente sem fio a se desconectar, visando capturar o handshake de reautenticação para ataques subsequentes.

**Jamming:** Interromper o sinal Wi-Fi transmitindo na mesma frequência de um ponto de acesso, causando interferência.

**WEP Hacking:**

Detectar redes habilitadas para WEP.

Capturar handshakes.

Quebrar a criptografia explorando vulnerabilidades para obter a chave pré-compartilhada.

**WPA/WPA2 Hacking:**

Colocar a placa de rede em modo monitor.

Encontrar redes WPA/WPA2.

Capturar handshakes.

Realizar ataque de dicionário com aircrack-ng para obter a senha.

**WPS Pin Ataque:**

Recuperar PIN WPS por meio de ataque de força bruta para obter a chave pré-compartilhada.

**Ataques Bluetooth:**

**Bluejacking**: Envio de mensagens não solicitadas para dispositivos Bluetooth.

**Bluesnarfing**: Acesso não autorizado a dispositivos Bluetooth para roubo de informações.

**BlueBorne**: Conjunto de vulnerabilidades explorando o protocolo Bluetooth para obter controle total sobre dispositivos Windows, Linux, Android e Apple.

* **Ferramentas**

**Reconhecimento:**

**WHOIS**: Coleta informações de registros públicos sobre a propriedade do domínio.

**Nslookup**: Identifica endereços IP associados a uma organização.

**theHarvester**: Vasculha mecanismos de pesquisa para encontrar informações sobre uma organização.

**Recon-ng:** Estrutura modular de reconhecimento web para gerenciar OSINT.

**Censys**: Ferramenta web para investigar endereços IP na Internet.

**FOCA**: Encontra metadados em documentos comuns.

**Shodan**: Mecanismo de busca especializado para descoberta de dispositivos IoT.

**Maltego**: Auxilia na visualização de dados coletados do OSINT.

**Scanner de Vulnerabilidades:**

**Nessus**: Ferramenta comercial de verificação de vulnerabilidades.

**OpenVAS**: Alternativa de código aberto para varreduras de vulnerabilidade.

**Sqlmap**: Automatiza ataques de injeção SQL em aplicativos web.

**Nikto**, **Wapiti**, **W3AF**: Scanners de vulnerabilidade para aplicativos web.

**WPScan**: Teste de aplicativos web WordPress.

**SCAP**: Conjunto de ferramentas para gerenciar conformidade com padrões de segurança.

**Engenharia Social:**

**Social Engineering Toolkit (SET):** Automatização de processos de engenharia social, incluindo phishing e criação de sites falsos.

**Browser Exploitation Framework (BeEF):** Exploração do lado do cliente para avaliação de segurança.

**Teste de Credenciais:**

**Hashcat, John the Ripper, Hydra, Medusa, Patator, Cain**: Ferramentas de quebra de senha.

**CeWL**: Gerador de lista de palavras personalizado para ataques de adivinhação.

**Mimikatz**: Recupera informações de credenciais da memória.

**DirBuster**: Ferramenta de força bruta para enumerar arquivos e diretórios.

**Debuggers e Ferramentas para Teste de Software:**

**Immunity Debugger, GDB, OllyDbg, WinDbg, IDA:** Ferramentas de depuração.

**Brakeman, Covenant, TruffleHog**: Ferramentas para análise de segurança de software.

**Teste de Rede:**

**Wireshark, Hping:** Analisador de protocolo e ferramenta de geração de tráfego.

**Aircrack-ng, WiFite, mdk4, Fern, Kismet:** Ferramentas de teste de segurança para redes sem fio.

**EAPHammer, Reaver, Spooftooph**: Ferramentas para ataques a redes sem fio e Bluetooth.

**WIGLE**: Banco de dados aberto de informações sobre redes sem fio.

**Acesso Remoto:**

**SSH, Ncat, Netcat, Proxychains:** Ferramentas para conexões seguras e redirecionamento de tráfego.

**Exploração:**

**Metasploit**: Estrutura de exploração popular com milhares de plug-ins.

**SearchSploit**: Ferramenta de pesquisa em banco de dados de explorações conhecidas.

**PowerSploit**, **Empire**, **Responder**, **Impacket**, **Mitm6**, **CrackMapExec**: Conjuntos de ferramentas para automação e avaliação pós-acesso em redes.

**Steganografia:**

**Open Steg, Steghide, Coagula, Sonic Visualiser, Snow, TinEye, Metagoofil**: Ferramentas de esteganografia para ocultar informações em arquivos.

**Cloud**:

**ScoutSuite, CloudBrute, Pacu, Cloud Custodian**: Ferramentas para auditoria e segurança em ambientes de nuvem.

**Mobile**:

**Drozer, APKX, APK Studio, SDKs do Android, Frida, Objection, Needle, Ettercap:** Ferramentas para avaliação de segurança em dispositivos móveis.

**Engenharia Social:**

**Social Engineering Toolkit (SET), BeEF:** Ferramentas focadas em engenharia social para testes de penetração.

* **Certificado digital**

**OCSP (Online Certificate Status Protocol):** O OCSP é um protocolo que determina o status de revogação de um certificado digital usando seu número de série.

**CRL (Certificate Revocation List):** A CRL é uma lista de certificados digitais revogados antes da expiração, tornando-os inválidos.

**SAN (Subject Alternative Name):** O SAN é um campo em certificados digitais que permite a identificação de um host por vários nomes de host ou domínios, sendo utilizado em certificados de vários domínios.

**CSR (Certificate Signing Request):** O CSR é um arquivo gerado em um dispositivo que precisa de um certificado, contendo informações necessárias para a autoridade de certificação criar o certificado.

**Ciclo de vidaGerar**: Processos que permitem solicitar a emissão de um certificado para um cliente ou dispositivo.

**Provisionar**: Emissão formal de certificados pela nossa organização.

**Descoberta**: Foco na incorporação de capacidades modernas para digitalizar e identificar os certificados em uso no ambiente.

**Inventário**: Documentação formal de cada certificado em uso, incluindo informações detalhadas.

**Monitoramento**: Utilização de mecanismos para identificar alterações nos certificados ou atividades suspeitas relacionadas ao seu uso.

**Proteção**: Ênfase na segurança das chaves privadas por meio de controles técnicos, como o uso de criptografia e técnicas de divisão de bits.

**Renovação**: Identificação proativa de certificados com data de validade pendente para substituição por novas chaves.

**Revogação**: Implementação de processos para identificar a necessidade de revogação de certificados digitais e seguimento de procedimentos quando necessário.

* **Relatório e comunicação**

**Partes de Comunicação:**

**Contato Primário:** Responsável pelo gerenciamento diário do teste, aspectos administrativos.

**Contato Técnico:** Responsável por questões relacionadas a tecnologias e processos técnicos.

**Contato de Emergência:** Disponível 24/7, geralmente um SOC, para respostas rápidas em situações de emergência durante o teste.

**Relatório:**

**Estrutura do Relatório:** Sumário Executivo, Escopo Detalhado, Metodologia utilizada, achados e Remediações, Conclusão e Apêndice

* **Estratégias de Recomendação:**

**Controles Técnicos:** Defesas lógicas, como filtros de e-mail.

**Controles Administrativos:** Processos baseados em controle para aprimorar a segurança.

**Controles Operacionais:** Implementação de procedimentos padrão para melhorar a segurança.

**Controles Físicos:** Previnem o acesso físico não autorizado ao ambiente.

**Respostas:**

1. B. Um acordo de confidencialidade, ou NDA, é um acordo legal concebido para proteger a confidencialidade dos dados do cliente e outras informações que o testador de penetração possa encontrar durante o teste. Um SOW é uma declaração de trabalho, que define o que será feito durante um trabalho, um MSA é um acordo mestre de serviços que define os termos gerais entre duas organizações, uma clausura de não-competição impede duas partes de competirem com um mesmo cliente, por exemplo.
2. B. A maneira mais simples de varrer múltiplas sub-redes adjacentes umas às outras é usar o comando -Pn para conduzir uma varredura somente de host de cada IP neste espaço de destino sem usar ping. Usar o traço (-) no endereço IP significa verificar “esta rede através desta rede”. Portanto, 10.0.0-3.0 verificará todos os IPs de 10.0.0.0 a 10.0.3.255.

**Referências:**

<https://www.comptia.org/pt/certificacoes/pentest>

<https://tryhackme.com/paths> (Comptia Pentest+) (Prática)

<https://owasp.org/www-project-top-ten/> (Teórica)

<https://pentesterlab.com/exercises/> (Prática)

<https://www.amazon.com/CompTIA-PenTest-Study-Guide-PT0-002/dp/1119823811> (Livro)