AMOSTRA

Ataques a Redes de Computadores e Malwares

Ataques a Redes de Computadores e Malwares

Pergunta: O que é o conceito do elo mais fraco em relação à segurança da informação?

Resposta: O conceito do elo mais fraco está relacionado à ideia de um atacante sempre buscar descobrir uma vulnerabilidade ou um meio que, através do menor esforço possível, ele conseguirá alcançar o objetivo do ataque.

Pergunta: Por que é importante ter um ambiente equilibrado em todos os setores e áreas nos diversos quesitos de segurança?

Resposta: É importante ter um ambiente equilibrado em segurança porque de nada adianta um ambiente ter regras de firewall altamente precisas e outros equipamentos robustos se não houver conscientização dos usuários, através de normas e políticas, para evitar o vazamento de dados através da engenharia social. Em regra, esse tipo de ataque é aquele que gera o resultado com o menor esforço.

Pergunta: Quais são algumas das possíveis motivações para ataques a redes de computadores?

Resposta: As possíveis motivações para ataques a redes de computadores incluem: demonstração de poder, motivações financeiras, motivações ideológicas e motivações comerciais.

Pergunta: O que significa a motivação de 'demonstração de poder' para ataques a redes de computadores?

Resposta: A motivação de 'demonstração de poder' para ataques a redes de computadores significa expor vulnerabilidades de empresas ou ambientes específicos com o objetivo de obter algum tipo de vantagem pessoal no futuro.

Pergunta: O que significa a motivação 'financeira' para ataques a redes de computadores?

Resposta: A motivação 'financeira' para ataques a redes de computadores significa obter informações confidenciais e privilegiadas para desenvolver golpes que geram algum tipo de 'lucro'.

Pergunta: O que significa a motivação 'ideológica' para ataques a redes de computadores?

Resposta: A motivação 'ideológica' para ataques a redes de computadores significa invadir sistemas para passar um recado ou divulgar uma imagem que representa uma ideologia ou determinada linha de pensamento.

Pergunta: O que significa a motivação 'comercial' para ataques a redes de computadores?

Resposta: A motivação 'comercial' para ataques a redes de computadores significa agir de forma mal intencionada para causar indisponibilidade de serviços e sistemas, gerando grandes prejuízos financeiros e de imagem em um mercado cada vez mais competitivo.

Pergunta: O que é uma vulnerabilidade de acordo com Cert.br?

Resposta: Uma vulnerabilidade é definida como uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.

Pergunta: Onde as vulnerabilidades podem estar presentes?

Resposta: As vulnerabilidades podem estar presentes em vários lugares, equipamentos, softwares ou pessoas. Isso pode incluir um desenvolvimento falho de um sistema operacional ou programa, ou ainda bugs intrínsecos em equipamentos, como switches, roteadores ou firewalls.

Pergunta: Quais as consequências de um atacante explorar uma vulnerabilidade?

Resposta: A partir da exploração de uma vulnerabilidade, o atacante pode obter informações privadas, invadir sistemas e até controlar a máquina da vítima para ser usada em outros ataques.

Pergunta: Quais são as etapas de um ataque?

Resposta: Um ataque pode ser dividido em 1. Identificação e reconhecimento do ambiente; 2. Identificação de vulnerabilidade; 3. Análise da melhor estratégia; 4. Aplicação do ataque.

Pergunta: O que é feito na primeira etapa de um ataque?

Resposta: Na primeira etapa, o atacante busca conhecer o ambiente e a área da vítima, como os equipamentos estão distribuídos, quem são esses equipamentos em termos de fabricantes, versões do software, sistema operacional, endereços de rede, entre outros.

Pergunta: O que são 'exploits' no contexto de um ataque?

Resposta: Exploits são ferramentas que já possuem em suas bases diversas vulnerabilidades a partir das informações dos sistemas e equipamentos. Este é um grande atalho para quem quer efetuar um ataque a partir de vulnerabilidades já conhecidas.

Pergunta: O que é o Sistema Operacional KALI do Linux?

Resposta: O Sistema Operacional KALI do Linux é customizado para realização de ataques e exploração de vulnerabilidades, contendo diversas ferramentas específicas para essas finalidades.

Pergunta: O que significa a estratégia do 'menor esforço' no contexto de ataques de segurança?

Resposta: A estratégia do 'menor esforço' refere-se à busca pelo tipo de ataque que gerará o resultado esperado a partir da menor complexidade e esforço.

Pergunta: Por que profissionais de segurança e auditoria são contratados para fazer análises nos ambientes e tentar explorá-los?

Resposta: Profissionais de segurança e auditoria são contratados para fazer análises nos ambientes e tentar explorá-los para entender como os ataques ocorrem e assim poder se defender melhor deles.

Pergunta: O que são 'pentesters' ou testes de penetração?

Resposta: Pentesters ou testes de penetração são práticas onde profissionais de segurança tentam invadir um sistema para identificar vulnerabilidades que possam ser exploradas por atacantes.

Pergunta: Quais são os três tipos de perfis de um atacante?

Resposta: Os três tipos de perfis de um atacante podem ser alguém totalmente externo à corporação, alguém de dentro da corporação, ou algum parceiro que possui informações parciais.

Pergunta: O que é o teste Blackbox?

Resposta: É um tipo de teste de segurança onde não se tem nenhum tipo de informação da rede ou do ambiente da organização. O teste de exploração deve cumprir todas as etapas que envolvem a identificação e exploração do ambiente para adquirir conhecimento. As principais entradas para este tipo de teste são os ataques de engenharia social e phishing. Este teste busca avaliar o princípio da segurança da obscuridade, que consiste em não fornecer ou divulgar informações sobre a rede para fora.

Pergunta: O que é o teste Whitebox?

Resposta: É um tipo de teste de segurança onde todas as informações básicas necessárias de conhecimento da rede são fornecidas ao pentester, pulando a etapa de identificação. Este tipo de teste busca verificar a robustez das configurações dos equipamentos e a inexistência de exploits conhecidos para as soluções.

Pergunta: O que é o teste Greybox?

Resposta: É um tipo de teste de segurança intermediário, onde algumas informações básicas que são facilmente descobertas são fornecidas e não fazem parte do escopo do princípio da obscuridade.

Pergunta: O que é REDTEAM?

Resposta: É uma perspectiva dos profissionais de segurança especializados em pentester e invasão, em busca de brechas e vulnerabilidades no ambiente de rede e sistemas em geral.

Pergunta: O que é a equipe BLUETEAM?

Resposta: A equipe BLUETEAM é responsável por manter o ambiente seguro na perspectiva de defesa, buscando eliminar constantemente as brechas existentes e descobertas pelo próprio time, ou derivado das descobertas do REDTEAM.

Pergunta: O que é avaliado na dinâmica entre as equipes REDTEAM e BLUETEAM?

Resposta: Avalia-se como o BLUETEAM reagirá em eventual descoberta de ataque frente a sucessos totais ou parciais do REDTEAM. Avaliar se as políticas e processos estabelecidos serão respeitados e surtirão os efeitos desejados.

Pergunta: O que significa um teste Black-Box em auditoria de segurança da informação?

Resposta: Black-Box é um tipo de teste de intrusão onde o pentester não tem qualquer tipo de informação sobre a infraestrutura de sistemas e de rede da empresa que será auditada. Ele deve construir uma estratégia para identificar e mapear esses recursos, para posteriormente avaliar suas vulnerabilidades.

Pergunta: O que é Spoofing no contexto de segurança da informação?

Resposta: Spoofing é o ato de personificar algo ou outra pessoa.

Pergunta: O que é Tampering no contexto de segurança da informação?

Resposta: Tampering é o ato de modificar dados ou código.

Pergunta: O que é Repudiation no contexto de segurança da informação?

Resposta: Repudiation é o ato de alegar não ter realizado uma ação.

Pergunta: O que é Information Disclosure no contexto de segurança da informação?

Resposta: Information Disclosure é o ato de expor informações a alguém não autorizado a vê-las.

Pergunta: O que é Denial of Service no contexto de segurança da informação?

Resposta: Denial of Service é o ato de negar ou degradar o serviço aos usuários.

Pergunta: O que é Elevation of Privilege no contexto de segurança da informação?

Resposta: Elevation of Privilege é o ato de obter recursos sem a autorização adequada.

Pergunta: Qual ameaça no modelo STRIDE tenta violar o princípio da confidencialidade?

Resposta: No modelo STRIDE, a ameaça que tenta violar o princípio da confidencialidade é a Information Disclosure.

Pergunta: O que é varredura em redes?

Resposta: A varredura em redes é uma técnica que geralmente antecede ataques. Essa técnica visa a obtenção de informações que subsidiarão as ações dos atacantes, como a busca de vulnerabilidades. Um ataque bem planejado busca conhecer o ambiente da vítima para traçar um plano de ação com vistas a reduzir os esforços e não deixar rastros.

Pergunta: Quais informações podem ser obtidas através da varredura em redes?

Resposta: Podem ser obtidas informações dos sistemas operacionais dos servidores e de suas atualizações, além de informações dos serviços e portas utilizadas por um servidor.

Pergunta: Qual é uma das principais ferramentas utilizadas para a varredura em redes?

Resposta: Uma das principais ferramentas utilizadas para a varredura em redes é o NMAP.

Pergunta: Em que situação a varredura em redes pode ser considerada legítima?

Resposta: A varredura em redes pode ser considerada legítima quando pessoas devidamente autorizadas e mediante um plano de comunicação do procedimento a ser realizado, fazem a varredura para efeito de auditoria ou verificação de aspectos de segurança, sejam eles preventivas ou corretivas.

Pergunta: O que é Web Spidering ou Crawler?

Resposta: Web Spidering ou Crawler é um tipo de indexador, como o indexador de busca do Google (Google Search), que pode ser utilizado para realizar uma série de levantamentos de informações nos domínios diversos na Internet.

Pergunta: Quais métodos são utilizados pelo indexador baseado no GET do HTTP?

Resposta: Os métodos utilizados pelo indexador são baseados no GET do HTTP. Todo campo de entrada pode ser tratado diretamente no Browser, como os parâmetros a seguir: https://www.google.com/search?q=cyber+security, site:nist.gov 'cyber security', site:www.nameoftargetsite.com filetype:pdf intext:password.

Pergunta: O que a primeira sequência 'https://www.google.com/search?q=cyber+security' representa?

Resposta: A primeira sequência representa uma busca pelo conjunto 'cyber security', com cada palavra isolada. O motor de busca do Google priorizará o conjunto, mas não excluirá as ocorrências individuais.

Pergunta: O que a segunda sequência 'site:nist.gov "cyber security"' representa?

Resposta: A segunda sequência representa uma busca pelo conjunto fechado 'cyber security' dentro de um domínio específico, no caso, nist.gov. Ou seja, todas as ocorrências dessa sequência de palavras dentro do site.

Pergunta: O que a terceira sequência 'site:www.nameoftargetsite.com filetype:pdf intext:password' representa?

Resposta: A terceira sequência é uma exploração de possibilidades, onde se busca, no referido domínio apresentado, documentos com a extensão PDF, contendo dentro dele o texto com a palavra 'password'. Ou seja, uma tentativa de busca por senhas expostas indevidamente em algum arquivo do site em questão.

Pergunta: Quais são os parâmetros para composição de expressões regulares na pesquisa?

Resposta: Os parâmetros para composição de expressões regulares na pesquisa são: (+) para forçar inclusão de algo comum; (-) para excluir um termo de pesquisa; (") para usar aspas em torno de frases de pesquisa; (.) um único caractere curinga; (*) qualquer palavra; (&) boolean 'AND'; (|) boolean 'OR'.

Pergunta: Error: Content Not Found

Resposta: Error: Relevant Content Not Provided

Pergunta: O que é GOOGLE HACKING?

Resposta: GOOGLE HACKING é uma técnica que consiste em usar a ferramenta de busca Google para identificar falhas de segurança em sistemas e reunir informações sobre eles. Essa técnica pode ser usada para encontrar vulnerabilidades específicas em sites.

Pergunta: O que é um teste de penetração?

Resposta: Um teste de penetração é um tipo de avaliação de segurança onde uma equipe de segurança tenta explorar as vulnerabilidades de um sistema para entender o quão seguro ele é.

Pergunta: O que a busca 'site:tjdft.jus.br' no Google retorna?

Resposta: A busca 'site:tjdft.jus.br' no Google retorna todas as páginas dentro do domínio tjdft.jus.br. Isso inclui qualquer subdomínio associado a tjdft.jus.br.

Pergunta: O que são ferramentas de spidering e para que são usadas?

Resposta: As ferramentas de spidering ou web spidering têm a finalidade de indexação de páginas e recursos na WEB.

Pergunta: O que significa o termo 'Spoofing' em termos de segurança da informação?

Resposta: O termo 'Spoofing' está diretamente relacionado ao assunto de falsificação ou adulteração de informação com o objetivo de alterar algum tipo de identidade ou identificador. Isso pode ser feito para se passar por uma pessoa, instituição ou dispositivo que possua certo grau de confiabilidade e legitimidade para dar confiança à informação enviada ou para esconder informações da origem de forma que não seja possível a identificação ou o rastreamento do atacante.

Pergunta: O que é 'E-mail spoofing'?

Resposta: 'E-mail spoofing' é uma aplicação do termo 'Spoofing' aos e-mails, onde o remetente do e-mail é falsificado para parecer que veio de outra fonte confiável ou para esconder a verdadeira origem do e-mail.

Pergunta: O que é e-mail spoofing?

Resposta: E-mail spoofing é uma técnica geralmente utilizada previamente a outro tipo de ataque mais prejudicial, como a propagação de códigos maliciosos, envios e replicação de spans e golpes de phishing. É um recurso básico para realização de SCAM.

Pergunta: O que é SCAM?

Resposta: SCAM é um foco na enganação do usuário, é utilizado em e-mail spoofing para atrair o usuário a cair em algum tipo de golpe.

Pergunta: Como se manipulam as informações dos e-mails para o e-mail spoofing?

Resposta: Para manipular as informações dos e-mails, basta adulterar os dados do cabeçalho do SMTP, mais especificamente, do campo FROM, além dos campos REPLY-TO e RETURN-PATH.

Pergunta: Quais são alguns exemplos clássicos de e-mail spoofing que recebemos todos os dias?

Resposta: Alguns exemplos clássicos são atacantes se passando por alguém conhecido, solicitando que você clique em um link ou execute um arquivo anexo; atacantes se passando por seu banco, solicitando que você siga um link fornecido na própria mensagem e informe dados da sua conta bancária; atacantes se passando por administrador do serviço de e-mail que você utiliza, solicitando informações pessoais e ameaçando bloquear a sua conta caso você não as envie.

Pergunta: O que é um ataque 'Man in the Middle'?

Resposta: Man in the Middle é um tipo de ataque básico que possui mais um caráter conceitual, de modo que pode ser implementado por diversas técnicas.

Pergunta: Qual é a principal característica do ARP Spoofing ou ARP Poisoning?

Resposta: A principal característica do ARP Spoofing ou ARP Poisoning é a capacidade de se inserir no meio de uma comunicação entre dois nós, permitindo ao atacante acesso a todos os dados trafegados na comunicação.

Pergunta: Quais são as possíveis ações de um atacante durante um ARP Spoofing?

Resposta: O atacante pode acessar e extrair dados, violando a confidencialidade; pode modificar os dados, violando a integridade; pode escolher quais mensagens devem ou não chegar até o destino, violando a disponibilidade; e pode usar a identidade do usuário para realizar a autenticação em serviços diversos, violando a autenticidade.

Pergunta: Como pode ser mitigado o ataque que viola a confidencialidade?

Resposta: Para mitigar esse tipo de ataque, pode-se utilizar a criptografia para tornar os dados ilegíveis.

Pergunta: Como pode ser mitigado o ataque que viola a integridade?

Resposta: Para mitigar esse tipo de ataque, pode-se utilizar recursos que visam controlar a integridade dos dados como cálculos de verificação ou funções HASH.

Pergunta: Como pode ser mitigado o ataque que viola a disponibilidade?

Resposta: Para mitigar esse tipo de ataque, pode-se utilizar técnicas de controle semelhantes às que são implementadas pelo protocolo TCP para confirmação de recebimento.

Pergunta: Como pode ser mitigado o ataque que viola a autenticidade?

Resposta: Para mitigar esse tipo de ataque, pode-se utilizar de chaves dinâmicas de sessão com prazo curto e temporário de validade.

Pergunta: Qual é o objetivo do ARP Poisoning?

Resposta: O objetivo do ARP Poisoning é assumir a identidade de outro host da rede com vistas a interceptar o tráfego que deveria ser direcionado à vítima, passando a obter informações privadas.

Pergunta: O que acontece quando um atacante envia informações falsas para Bob e Alice?

Resposta: O atacante se passa por Alice e diz a Bob que o IP 10.0.0.7 corresponde ao MAC cc:cc:cc:cc:cc:cc, quando na verdade o correto seria aa:aa:aa:aa:aa:aa, que é o endereço de Alice. O mesmo procedimento é feito com Alice, onde o atacante se passa por Bob e informa que o endereço 10.0.0.1 corresponde ao MAC cc:cc:cc:cc:cc:cc, quando o correto seria bb:bb:bb:bb:bb:bb. Este processo é conhecido como envenenamento da tabela ARP.

Pergunta: O que acontece após o ataque de envenenamento da tabela ARP?

Resposta: Após o ataque de envenenamento da tabela ARP, sempre que Alice enviar uma mensagem para Bob, ela será redirecionada para o atacante e vice-versa. Este ataque é fácil de ser realizado, tanto a nível do próprio Sistema Operacional como através de ferramentas, como CAIN&ABEL.

Pergunta: O que é IP Spoofing?

Resposta: IP Spoofing é um ataque simples com o objetivo de mascarar ataques de rede para não deixar rastros que possam incriminar o atacante. O atacante adultera os pacotes IP para mascarar seu IP real. Esse princípio também se aplica quando se objetiva a derrubada de um servidor, através de DoS, por exemplo.

Pergunta: O que acontece quando um volume muito grande de requisições parte de um mesmo host?

Resposta: Quando um volume muito grande de requisições parte de um mesmo host, gera-se uma suspeita de que está sendo realizado um ataque. Para evitar isso, o atacante pode adulterar os pacotes, dando a impressão de que são vários hosts realizando requisições distintas. Este é outro tipo de ataque que pode ser gerado a partir do IP Spoofing.

Pergunta: O que acontece quando um atacante envia uma informação para um destinatário e adultera a origem?

Resposta: O atacante envia a informação com seu IP original, neste caso, 10.10.50.50. Ele então adultera a origem de modo que a resposta enviada pelo destinatário, JOHN, vá para o endereço adulterado, neste caso, 10.10.20.30. Este princípio é utilizado para gerar ataques de negação de serviço.

Pergunta: O que é um ataque SMURF?

Resposta: O ataque SMURF é um tipo de ataque que consiste em enviar ataques de resposta à vítima a partir de mensagens do tipo echo request para um endereço de broadcast com o IP 'SPOOFADO' da vítima. É um exemplo de ataque mais elaborado e potente que pode ser gerado a partir do SPOOFING de IP.

Pergunta: Como o atacante realiza o ataque SMURF?

Resposta: O atacante, sabendo que o IP da vítima é, digamos, 9.9.9.9, adultera o campo FROM do pacote IP de uma mensagem do tipo echo request. Essa mensagem possui como destino um IP de Broadcast de alguma rede que responde a PINGS. Em seguida, o roteador distribuirá essas mensagens para todos os nós que fazem parte daquela rede. Cada nó responderá às requisições com uma mensagem do tipo ECHO REPLY.

Pergunta: O que acontece quando o IP de origem corresponde ao endereço IP da vítima?

Resposta: Todo o tráfego será redirecionado à vítima, gerando indisponibilidade do serviço.

Pergunta: O que é a técnica de Interceptação de tráfego ou Sniffing?

Resposta: É uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de sniffers, como Wireshark e TCPDump.

Pergunta: Quando a técnica de Sniffing pode ser utilizada de forma legítima?

Resposta: Por administradores de redes, para detectar problemas, analisar desempenho e monitorar atividades maliciosas relativas aos computadores ou redes por eles administrados.

Pergunta: Quando a técnica de Sniffing pode ser utilizada de forma maliciosa?

Resposta: Por atacantes, para capturar informações sensíveis, como senhas, números de cartão de crédito e o conteúdo de arquivos confidenciais que estejam trafegando por meio de conexões inseguras, ou seja, sem criptografia.

Pergunta: As informações capturadas por sniffing são úteis ao atacante se estiverem criptografadas?

Resposta: Informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las.

Pergunta: Qual é o mecanismo mais eficiente para mitigar a ameaça de sniffing?

Resposta: A criptografia é o mecanismo mais eficiente para mitigar a ameaça de sniffing, pois a técnica não surte efeito sobre tráfego criptografado.

Pergunta: O que é um ataque de Força Bruta?

Resposta: É um tipo de ataque que busca descobrir uma senha ou alguma outra informação através do método de tentativa e erro de forma exaustiva.

Pergunta: Qual a importância de ter senhas grandes e complexas?

Resposta: Ter senhas grandes e complexas torna ataques de força bruta inviáveis.

Pergunta: O que influencia o desempenho de um ataque de Força Bruta?

Resposta: O desempenho de um ataque de Força Bruta está diretamente relacionado à capacidade de processamento computacional de um atacante.

Pergunta: A força bruta se aplica apenas a senhas?

Resposta: Não, os conceitos de força bruta também se aplicam à quebra de chaves criptográficas para interpretação de dados criptografados.

Pergunta: Quais são algumas das bases para tentativas de adivinhação em um ataque de Força Bruta?

Resposta: As tentativas de adivinhação podem basear-se em dicionários de diferentes idiomas, listas de palavras comumente usadas, substituições óbvias de caracteres, sequências numéricas e de teclado, e informações pessoais do alvo.

Pergunta: O que pode resultar em negação de serviço em um ataque de Força Bruta?

Resposta: A negação de serviço pode ocorrer quando a quantidade de tentativas realizadas em um curto período de tempo é grande.

Pergunta: Qual é a técnica utilizada pelos hackers que utilizam software automático para descobrir senhas fracas?

Resposta: A técnica é chamada de 'brute force'.

Pergunta: Como a criação de senhas fortes pode ajudar na segurança dos sistemas?

Resposta: Políticas bem estabelecidas para criação de senhas fortes, que utilizem uma grande quantidade de caracteres (8 ou mais), sendo obrigatório letras minúsculas e maiúsculas, além da utilização de números e caracteres especiais ajudam no combate a técnicas automatizadas (robôs) para quebra de senhas por meio da força bruta.

Pergunta: O que são CAPTCHAS e para que são utilizados?

Resposta: CAPTCHAS são imagens ou sequências de letras que precisamos inserir, por vezes, antes de logar em alguma aplicação. Essa técnica é criada e utilizada para combater o uso de robôs que eventualmente tentem realizar ataques de força bruta na aplicação.

Pergunta: O que é um ataque de personificação em uma rede?

Resposta: Um ataque de personificação ocorre quando um atacante introduz ou substitui um dispositivo de rede para induzir outros a se conectarem a este, ao invés do dispositivo legítimo, permitindo a captura de senhas de acesso e informações que por ele passem a trafegar.

Pergunta: O que é desfiguração de página (Defacement)?

Resposta: Desfiguração de página, defacement ou pichação, é uma técnica que consiste em alterar o conteúdo da página Web de um site. Possui um caráter unicamente de vandalismo.

Pergunta: Quais são as principais formas que um atacante pode utilizar para desfigurar uma página Web?

Resposta: Um atacante, neste caso, também chamado de defacer, pode utilizar as seguintes formas para desfigurar uma página Web: explorar erros da aplicação Web; explorar vulnerabilidades do servidor de aplicação Web; explorar vulnerabilidades da linguagem de programação ou dos pacotes utilizados no desenvolvimento da aplicação Web; invadir o servidor onde a aplicação Web está hospedada e alterar diretamente os arquivos que compõem o site.

Pergunta: O que significa furtar senhas de acesso à interface Web usada para administração remota?

Resposta: Significa obter de maneira ilícita as senhas que permitem o acesso à interface de administração de um site, geralmente com o objetivo de realizar alterações não autorizadas.

Pergunta: O que os atacantes geralmente alteram para ganhar mais visibilidade e atingir um maior número de visitantes?

Resposta: Os atacantes geralmente alteram a página principal do site, mas páginas internas também podem ser alteradas.

Pergunta: Como o conceito de furtar senhas de acesso à interface Web para administração remota difere do PHISHING?

Resposta: O Phishing é uma técnica de fraude online usada para roubar senhas e informações financeiras através da imitação de empresas confiáveis. Já o furto de senhas de acesso à interface Web para administração remota geralmente implica em acessar diretamente o sistema ou a página web e realizar alterações não autorizadas.

Pergunta: O que são ataques de substituição de uma página web facilitados por vazamento de senhas na Internet?

Resposta: São ataques que ocorrem quando as senhas de acesso à interface web de administração são obtidas de maneira ilícita, permitindo que os atacantes alterem ou substituam a página web original.

Pergunta: Quais aspectos da segurança da informação são violados em ataques bem-sucedidos de substituição de uma página web facilitados por vazamento de senhas na Internet?

Resposta: Os aspectos de integridade e disponibilidade da segurança da informação são violados. A integridade é comprometida pela alteração do conteúdo original e a disponibilidade é afetada pois o conteúdo original, que deveria ser acessado pelo público, fica inacessível.

Pergunta: O que é Phishing?

Resposta: Phishing é uma técnica de fraude online usada para enganar pessoas com o intuito de obter suas informações pessoais, como senhas e números de cartão de crédito. Isso geralmente é feito através de emails ou sites falsos que se parecem com os sites legítimos.

Pergunta: Como funciona um ataque de Phishing?

Resposta: Um ataque de Phishing geralmente envolve o envio de um email ou a criação de um site que parece ser de uma organização legítima. Quando a vítima clica no link ou fornece suas informações pessoais, o atacante ganha acesso a essas informações.

Pergunta: O que é Spear Phishing?

Resposta: Spear Phishing é uma forma de Phishing que é direcionada a uma vítima específica, geralmente uma organização ou indivíduo específico. É um ataque mais sofisticado que geralmente envolve a falsificação de emails para parecerem mais legítimos.

Pergunta: Qual é a melhor maneira de se proteger contra Phishing?

Resposta: A melhor maneira de se proteger contra o Phishing é estar sempre atento às URLs dos sites que você visita e aos emails que você recebe. Sempre verifique se os endereços correspondem aos sites legítimos.

Pergunta: Qual é a resposta correta para a pergunta: 'O ataque digital que tem como objetivo capturar informações sensíveis por meio de fraudes eletrônicas e que se utiliza de pretextos falsos, com o intuito de receber informações sensíveis dos usuários, e que ocorre com mais frequência por meio do envio de e-mails e páginas web falsas, denomina-se'?

Resposta: A resposta correta é D. Phishing.

Pergunta: O que caracteriza os ataques de phishing?

Resposta: Os ataques de phishing caracterizam-se pelo envio de mensagens eletrônicas que despertam a atenção de usuários por meio da sugestão de vantagens ou ameaças de prejuízos e também por induzirem os usuários a fornecer dados pessoais e(ou) financeiros.

Pergunta: O que é um ataque de pharming?

Resposta: Este tipo de ataque ocorre quando um tráfego que originalmente deveria ir para um site legítimo é redirecionado para outro. Pode ocorrer de diversas formas, como por meio da alteração do servidor DNS (DNS Poisoning), em que se faz um apontamento para um IP de destino que armazena conteúdo similar, porém, é um site malicioso para se obter dados.

Pergunta: Qual é a diferença entre phishing e pharming?

Resposta: No phishing, o usuário já dispara o acesso à uma página falsa na origem, enquanto no pharming, há um desvio ao longo da rede, sendo quase que transparente para o usuário.

Pergunta: Como pode ocorrer um ataque de pharming?

Resposta: Essa forma de ataque pode ocorrer de diversas formas, como por meio da alteração do servidor DNS (DNS Poisoning), em que se faz um apontamento para um IP de destino que armazena conteúdo similar, porém, é um site malicioso para se obter dados. Esse tipo de ataque pode acontecer tanto nos arquivos de configuração de DNS local (Cache Poisoning) quando em um servidor de consulta.

Pergunta: Qual é o nome do ataque onde houve um redirecionamento das conexões a outro servidor Web controlado por um atacante, através da invasão de um servidor de resolução de nomes e da alteração de um dos seus registros?

Resposta: Esse tipo de ataque é conhecido como Envenenamento de DNS.

Pergunta: O que é DNSSEC?

Resposta: DNSSEC é um serviço que implementa o DNS por meio de uma estrutura de chaves públicas associadas que permite a autenticação mútua entre os servidores autoritativos, além da garantia da troca segura de informações de zonas e seus conjuntos de DNS's associados. Esta implementação permite combater ataques como o DNS POISONING.

Pergunta: O que é um ataque de Negação de Serviço (Denial of Service – DoS)?

Resposta: Um ataque de Negação de Serviço busca comprometer o princípio de Segurança conhecido como disponibilidade. O atacante tenta 'tirar' um serviço do ar, esgotando algum tipo de recurso do sistema, que inviabilize o atendimento de novas requisições.

Pergunta: Quais são algumas formas que um ataque de Negação de Serviço pode ocorrer?

Resposta: Um ataque de Negação de Serviço pode ocorrer através do envio de um grande volume de requisições para um serviço específico, consumindo seus recursos de processamento, quantidade de sessões suportadas, banda de internet, memória, disco, entre outros. Também pode ocorrer através da exploração de vulnerabilidades em programas causando sua indisponibilidade.

Pergunta: Qual o nome do ataque cibernético que inunda servidores da Web com solicitações que impedem a conexão de seus usuários regulares?

Resposta: O nome desse tipo de ataque é DoS (Denial of Service).

Pergunta: Quais são alguns dos modos de ataques DoS?

Resposta: Um dos modos de ataques DoS é tentar abrir sessões legítimas via HTTP, por exemplo, no servidor vítima.

Pergunta: Qual foi a técnica de ataque utilizada para indisponibilizar o site da empresa ABCTech?

Resposta: A técnica de ataque utilizada foi denial of service (DoS).

Pergunta: O que é Negação de Serviço Distribuído (Distributed Denial of Service - DDoS)?

Resposta: DDoS tem os mesmos princípios do ataque DoS, porém, é tratado de forma coordenada e distribuída, seja por computadores envolvidos de forma voluntária ou de forma involuntária (zumbis). O mais usual é o segundo método. Assim, antes de efetuar esse tipo de ataque, um atacante precisa controlar uma rede de computadores zumbis, muitas vezes chamadas de botnets. O atacante envia o comando para que todos os dispositivos controlados enviem requisições de forma simultânea a um host específico (vítima), gerando indisponibilidade do serviço. Tem um alto grau de sucesso devido à grande dificuldade de se detectar e reagir a tempo a esse tipo de ataque.

Pergunta: Como é a reação mais comum a um ataque DDoS?

Resposta: A principal reação se dá através do contato com a operadora responsável pelo provimento do acesso à Internet com vistas a bloquear determinada região ou rota BGP que está originando esse grande volume de requisições.

Pergunta: Como são os ataques DDoS mais elaborados e robustos?

Resposta: Ataques mais elaborados e robustos de DDoS acabam por construir redes hierárquicas com controles descentralizados, gerando um volume ainda maior.

Pergunta: O que acontece quando um site importante usa um único servidor web para hospedá-lo e esse servidor se torna vulnerável a ataques?

Resposta: Este servidor pode se tornar alvo de um ataque que tenta sobrecarregá-lo com um número muito grande de requisições HTTP coordenadas e distribuídas, utilizando um conjunto de computadores e/ou dispositivos móveis. Este tipo de ataque pode fazer com que o servidor não consiga responder às requisições legítimas e se torne inoperante.

Pergunta: Como é chamado o tipo de ataque que tenta sobrecarregar um servidor com um número muito grande de requisições HTTP coordenadas e distribuídas?

Resposta: Este tipo de ataque é conhecido como DDoS.

Pergunta: O que é um ataque DRDoS?

Resposta: DRDoS, ou DDoS Refletor, é um tipo específico de ataque DDoS que usa zumbis para enviar requisições com endereços IP forjados para usuários legítimos e não infectados. Devido

ao IP forjado gerado pelos zumbis, os hosts legítimos encaminham o tráfego (resposta às requisições) à vítima.

Pergunta: Como o ataque DRDoS difere de um ataque DDoS padrão?

Resposta: Diferentemente do DDoS padrão, o ataque DRDoS não ocorre de forma direta dos zumbis para a vítima. Em vez disso, ele usa intermediários que funcionam como refletores, aumentando o 'poder de fogo' do ataque.

Pergunta: O que é um ataque DDoS?

Resposta: Um ataque DDoS busca esgotar recursos de sistemas específicos, seja no processamento, consumo de memória, banda, entre outros.

Pergunta: Como evitar pontos únicos de falha pode ajudar contra ataques DDoS?

Resposta: Ao se evitar pontos únicos de falha, ou seja, possíveis gargalos, inevitavelmente obtém-se um ambiente mais robusto e resistente a ataques DDoS.

Pergunta: Qual é a ideia por trás da superestimação de recursos de rede e recursos computacionais como medida contra ataques DDoS?

Resposta: A ideia é ter cada vez mais largura de banda e recursos computacionais de tal modo que exigirá ainda mais potência nos ataques de DDoS para esgotar os recursos. Entretanto, é uma solução um tanto cara manter recursos dessa forma, principalmente, considerando que estes ficarão ociosos em condições normais.

Pergunta: O que significa estabelecer padrões de tráfego como medida contra ataques DDoS?

Resposta: Estabelecer padrões de tráfego significa monitorar o fluxo e traçar perfil de acesso e utilização. Isso permite aos gerentes de rede bloquearem acessos que fogem ao padrão. Pode-se determinar marcos específicos como uma Baseline de comportamento que permite uma reação de forma mais rápida em caso de comportamento estranho.

Pergunta: Quais são os possíveis problemas ao estabelecer padrões de tráfego como medida de proteção contra ataques DDoS?

Resposta: Esse tipo de operação pode gerar falsos positivos, ou seja, tráfego legítimo que possui um caráter de exceção e será tratado como possíveis ataques.

Pergunta: O que significa encaminhar o tráfego inválido para 'buracos negros' em termos de segurança da informação?

Resposta: Encaminhar o tráfego inválido para 'buracos negros' se refere ao redirecionamento de requisições falsas ou incompletas, geralmente utilizadas em ataques, por rotas nulas, chamadas de 'buracos negros'. Como não há a resposta de informação de que os pacotes estão sendo descartados, dificulta-se a ação alternativa por parte dos atacantes.

Pergunta: O que são serviços de distribuição de conteúdo (CDN's) e como eles podem ajudar a mitigar um ataque?

Resposta: Serviços de distribuição de conteúdo (CDN's) são serviços específicos de fornecimento de conteúdo que podem ser utilizados para reduzir a carga de um eventual ataque, mantendo informações específicas nas CDN's de modo a desonerar o consumo de recursos nos servidores principais da aplicação.

Pergunta: O que é Hardening de Sistemas?

Resposta: Hardening de Sistemas é a configuração segura com vistas a eliminar possíveis vulnerabilidades de sistemas operacionais e serviços. Assim, o ambiente pode se tornar mais robusto e menos suscetível a ataques.

Pergunta: Quais são algumas medidas para evitar um ataque de DDoS?

Resposta: Para evitar um ataque de DDoS, um procedimento apropriado é identificar padrões de comportamento suspeitos e, então, aplicar filtros aos pacotes cujas características indicam risco de ataque.

Pergunta: O que é SPIM?

Resposta: SPIM (Spam over Instant Message) é uma variação do SPAM para serviços de mensagem instantânea. Os indivíduos mal-intencionados utilizam dois métodos de transferência de código malicioso. Eles podem enviar um arquivo com vírus, trojan ou spyware, ou podem fazer uso de engenharia social. Uma vez que o código é executado, o usuário poderá ter sua lista de contados violada e roubada, propagando o ataque para outros usuários.

Pergunta: O que são ataques de engenharia social?

Resposta: Ataques de engenharia social são aqueles em que se engana a vítima por meio social para obter informações privilegiadas para se gerar ataques. Eles podem ser realizados através de diversas técnicas, como Vishing, Phishing ou Spear Phishing, Hoax, e Whaling.

Pergunta: O que é Vishing?

Resposta: Vishing é uma prática em que o sujeito que inicia um ataque faz uso de um sistema telefônico (VoiP, por exemplo) para ter acesso a informações pessoais da vítima.

Pergunta: O que é Hoax?

Resposta: Hoax é uma mentira que, quando divulgada por veículos de disseminação em massa, pode parecer verdade. Essa disseminação pode utilizar os diversos meios de comunicação.

Pergunta: O que é Whaling?

Resposta: Whaling são ataques altamente direcionados com vistas a ludibriar executivos do alto escalão de uma organização.

Pergunta: Qual técnica foi empregada pelo falso funcionário para conseguir as informações de Marina?

Resposta: A técnica empregada pelo falso funcionário para conseguir as informações de Marina é a engenharia social.

Pergunta: O que é um ataque de sequestro de dados?

Resposta: Um ataque de sequestro de dados é um tipo de ataque onde o atacante obtém acesso privilegiado ao sistema da vítima e realiza a criptografia dos dados da vítima, tornando-os inacessíveis sem a chave criptográfica necessária para descriptografá-los.

Pergunta: O que é Ransomware?

Resposta: Ransomware é um tipo de ataque de sequestro de dados. O atacante exige um valor a ser pago para a disponibilização da chave à vítima, para que ela possa acessar seus dados novamente. O atacante geralmente agrega ameaças de destruição dos dados e que o “resgate” deve ser pago em um período específico, geralmente, 3 dias.

Pergunta: Qual é a função do software em negociação para proteger contra o sequestro de dados?

Resposta: A função do software em negociação é a defesa de ransomware.

Pergunta: Qual é o tipo de ataque mais comumente utilizado como precursor para viabilizar ataques de ransomware contra estações de trabalho de usuários?

Resposta: O tipo de ataque mais comumente utilizado como precursor para viabilizar ataques de ransomware contra estações de trabalho de usuários é o ataque de phishing.

Pergunta: Paola recebeu um e-mail que continha um anexo desconhecido. Ao tentar fazer o download desse anexo, um código malicioso que criptografou os arquivos do sistema foi

executado. Em seguida, Paola recebeu uma notificação de que seus dados estavam inacessíveis e que seria necessário um pagamento de resgate para restabelecer o acesso. Paola foi vítima de que tipo de ataque?

Resposta: Paola foi vítima de um ataque de Ransomware.

Pergunta: Qual é o software malicioso que toma como refém informações pessoais ou corporativas e que depende do pagamento de uma quantia em dinheiro ou bitcoins para a liberação desses dados?

Resposta: O software malicioso que toma como refém informações pessoais ou corporativas e que depende do pagamento de uma quantia em dinheiro ou bitcoins para a liberação desses dados é conhecido como Ransomware.

Pergunta: O que é Malware?

Resposta: Malware é um software malicioso, dando origem ao termo em questão (Malicious Software). É o conceito mais genérico no que tange a ataques a rede. Podemos ter malwares com o objetivo de roubar dados, roubar identidades, traçar perfis, gerar danos aos hardwares e sistemas, entre muitas outras hipóteses.

Pergunta: Como os Malwares podem infectar os dispositivos?

Resposta: Os malwares podem infectar os dispositivos de várias formas como: exploração de vulnerabilidades intrínsecas em programas, execução automática de mídias removíveis infectadas, acesso a páginas Web maliciosas e ação direta de atacantes que ao invadir os computadores, inserem códigos e programas indesejados.

Pergunta: Por que é importante manter programas atualizados e sempre utilizar programas legítimos?

Resposta: É importante para evitar a exploração de vulnerabilidades intrínsecas nos programas pelos malwares.

Pergunta: Como pode ser evitada a infecção por malware através de mídias removíveis?

Resposta: Recomenda-se desabilitar a auto execução de mídias para evitar este tipo de ataque. Caso tenha um arquivo infectado, ele dependerá de execução para se propagar, ou seja, sem a auto execução, já teremos um fator de dificuldade para o sucesso do malware.

Pergunta: O que pode acontecer ao acessar páginas Web maliciosas?

Resposta: Ao acessar páginas maliciosas, vários pontos podem ser explorados pelos malwares, seja através da exploração de vulnerabilidade do próprio Browser, ou downloads de arquivos infectados, entre outros.

Pergunta: O que é Hardening?

Resposta: Hardening é um conjunto de procedimentos que busca-se “endurecer” o servidor de tal forma que ele não fique tão vulnerável. Isso inclui ter senhas de acesso mais complexas, controlar as portas de acesso aos dispositivos, entre outras técnicas que dificultam o acesso indevido às máquinas.

Pergunta: O que é um vírus de computador?

Resposta: Um vírus de computador é um tipo de malware que é um código que pode ser representado por um programa ou parte de um programa com a capacidade de gerar cópias de si mesmo e se inserir em outros programas ou arquivos. Ele pode executar tarefas específicas no computador da vítima, como deleção de arquivos, instalação de outros programas, redução de configurações de segurança, desestabilização dos sistemas e ocupação de espaço de armazenamento.

Pergunta: Como um vírus de computador se propaga?

Resposta: Um vírus de computador se propaga principalmente através da Internet ou de mídias removíveis, como pen drives. Ele depende de uma ação direta do usuário ou do sistema operacional para ser executado ou abrir um arquivo infectado.

Pergunta: O que é um vírus de Boot?

Resposta: Um vírus de Boot é um tipo de vírus que infecta a área de inicialização dos sistemas operacionais, também conhecido como MBR (Master Boot Record) do disco rígido. Esse tipo de vírus não corrompe arquivos específicos, mas sim, todo o disco. Os antivírus comuns de sistemas operacionais não são capazes de detectar esse tipo de vírus, sendo necessário uma varredura antes da inicialização do sistema para sua detecção.

Pergunta: O que é um vírus de Arquivo?

Resposta: Um vírus de Arquivo é um tipo de vírus que infecta arquivos de programas executáveis, geralmente, nas extensões .EXE e .COM. Ao se executar o referido programa, ativa-se o vírus.

Pergunta: O que é um vírus Residente?

Resposta: Um vírus Residente é um tipo de vírus que é carregado diretamente na memória RAM do sistema operacional toda vez que o sistema operacional é iniciado. Este tipo de vírus

pode ser extremamente danoso, bloqueando acessos à memória RAM, interrompendo determinados processos e funções a serem executadas e inclusive, alterando tais funções para fins maliciosos.

Pergunta: O que é um vírus propagado por e-mail?

Resposta: Um vírus propagado por e-mail é um tipo de vírus que é recebido como um arquivo anexo a um e-mail cujo conteúdo tenta induzir o usuário a clicar sobre este arquivo, fazendo com que seja executado. Quando entra em ação, infecta arquivos e programas e envia cópias de si mesmo para os e-mails encontrados nas listas de contatos gravadas no computador.

Pergunta: O que é um vírus de script?

Resposta: Um vírus de script é um tipo de vírus escrito em linguagem de script, como VBScript e JavaScript, e é recebido ao acessar uma página Web ou também por e-mail, como um arquivo anexo ou como parte do próprio e-mail escrito em formato HTML. Pode ser automaticamente executado, dependendo da configuração do navegador Web e do programa leitor de e-mails do usuário.

Pergunta: O que é um vírus de macro?

Resposta: Um vírus de macro é um tipo específico de vírus de script, escrito em linguagem de macro (série de comandos e instruções que podem ser agrupadas em um simples comando), que tenta infectar arquivos manipulados por aplicativos que utilizam linguagem de macro.

Pergunta: O que compõe a suíte Microsoft Office e que linguagem geralmente é usada para escrever macros para esses programas?

Resposta: Os programas que compõem a suíte Microsoft Office incluem Excel, Word e PowerPoint, entre outros. As macros para esses programas são geralmente escritas em Visual Basic para Aplicações (VBA).

Pergunta: Por que as macros são geralmente bloqueadas nos programas do Microsoft Office?

Resposta: As macros são bloqueadas nesses programas porque são armazenadas nos próprios documentos, o que pode representar um risco de segurança. O usuário deve habilitar manualmente as macros legítimas.

Pergunta: Como os vírus de telefone celular se propagam?

Resposta: Os vírus de telefone celular se propagam de celular para celular através da tecnologia bluetooth ou de mensagens MMS (Multimedia Message Service). A infecção ocorre quando um usuário permite o recebimento de um arquivo infectado e o executa.

Pergunta: Quais são os efeitos possíveis de um vírus de telefone celular?

Resposta: Após infectar o celular, o vírus pode destruir ou sobrescrever arquivos, remover ou transmitir contatos da agenda, efetuar ligações telefônicas, drenar a carga da bateria e tentar se propagar para outros celulares.

Pergunta: O que é um Vírus Stealth?

Resposta: O Vírus Stealth é um malware que evita a sua detecção através de técnicas de programação.

Pergunta: O que são vírus metamórficos e polimórficos?

Resposta: Os vírus metamórficos e polimórficos são executados e conseguem transformar-se automaticamente, ou seja, modificam seu próprio código ou assinatura, dificultando e adiando a detecção da ameaça pelo antivírus.

Pergunta: Como um vírus polimórfico se altera?

Resposta: Um vírus polimórfico adota diferentes formas a cada infecção com foco em não ser identificado pelo antivírus. Ele altera sua assinatura, mantendo suas funcionalidades e alterando apenas o seu padrão de bits.

Pergunta: Como um vírus metamórfico se altera?

Resposta: Um vírus metamórfico pode se alterar a cada infecção. Ele pode mudar seu tamanho, característica e inclusive comportamento, aumentando a dificuldade de detecção. Ele não muda somente sua assinatura, mas também sua funcionalidade.

Pergunta: O que é um vírus do tipo polimórfico?

Resposta: Um vírus do tipo polimórfico é um vírus que se transforma a cada infecção, o que impossibilita a detecção pela assinatura do vírus.

Pergunta: Como um vírus polimórfico se esconde de um antivírus?

Resposta: Um vírus polimórfico muda de sua assinatura a cada infecção. Isso impede sua detecção com base em assinatura, mas ainda é possível detectá-lo por meio de seu comportamento.

Pergunta: Qual é a diferença entre um vírus polimórfico e um vírus metamórfico?

Resposta: Um vírus polimórfico muda sua assinatura para evitar detecção, enquanto um vírus metamórfico pode mudar seu comportamento e aparência, o que aumenta a dificuldade de detecção.

Pergunta: O que é um WORM?

Resposta: WORM é um tipo de malware que tem a capacidade de se propagar pela rede de computadores através do envio de cópias de seu código a outros dispositivos. Ele busca explorar vulnerabilidades específicas dos sistemas, diferentemente do Vírus.

Pergunta: Qual é o impacto de um WORM na rede de computadores?

Resposta: Devido ao seu grande poder de propagação na rede, um WORM pode gerar um grande consumo de processamento e banda, prejudicando a qualidade dos sistemas e da rede. Pode ter uma propagação a nível global ao longo da Internet nos casos da existência de vulnerabilidades presentes nos mais diversos sistemas.

Pergunta: Um programa malicioso do tipo worm pode ser considerado um vírus?

Resposta: Não, um worm não pode ser considerado um vírus.

Pergunta: Os worms se replicam automaticamente?

Resposta: Sim, os worms são capazes de se multiplicar de forma automática.

Pergunta: Como o worm se difere do vírus?

Resposta: O worm se diferencia do vírus pela sua capacidade de se propagar sem precisar incluir cópias de si mesmo em outros programas ou arquivos. Em contrapartida, o vírus se propaga pela execução direta de uma de suas cópias.

Pergunta: O vírus se propaga por meio da inclusão de cópias de si mesmo em outros programas?

Resposta: Não, ao contrário do worm, o vírus não se propaga por meio da inclusão de cópias de si mesmo em outros programas. Ele se propaga pela execução direta de uma de suas cópias.

Pergunta: O que é um spyware?

Resposta: Spyware é um tipo de malware que se concentra na obtenção de informações de um host ou sistemas através do monitoramento de suas atividades. As informações coletadas podem ser enviadas a terceiros para consolidação e uso para outros fins.

Pergunta: Quais são os dois usos de um spyware?

Resposta: Spyware pode ter um uso legítimo ou malicioso. O uso legítimo pode ser instalado pelo próprio usuário para monitorar ações em seu dispositivo por outros usuários ou com o consentimento do usuário para monitoramento de uma instituição de trabalho. O uso malicioso infringe a privacidade do usuário, podendo obter senhas de acesso e outras informações privilegiadas.

Pergunta: O que é um keylogger?

Resposta: Um keylogger é um tipo de spyware que é capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Em muitos casos, é ativado por uma ação prévia do usuário, como o acesso a um site específico de comércio eletrônico ou de Internet Banking.

Pergunta: Como o teclado virtual ajuda a prevenir ataques de keylogger?

Resposta: O teclado virtual foi desenvolvido para que o usuário não precise digitar senhas diretamente em seu teclado, mas através de cliques do mouse. Dessa forma, se houver um keylogger na máquina do usuário, ele não será capaz de coletar as informações digitadas.

Pergunta: O que é um screenlogger?

Resposta: Um screenlogger é um tipo de spyware semelhante ao keylogger, mas que é capaz de armazenar a posição do cursor e a tela apresentada no monitor nos momentos em que o mouse é clicado. É muito utilizado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em sites de Internet Banking.

Pergunta: Como teclados virtuais que 'embaralham' os caracteres ajudam a prevenir ataques de screenlogger?

Resposta: Teclados virtuais que 'embaralham' os caracteres em cada acesso garantem que a sequência de digitação da senha nunca será a mesma, tornando impossível deduzir os números e letras pela posição do teclado virtual.

Pergunta: O que é um adware?

Resposta: Adware é um tipo de spyware projetado especificamente para apresentar propagandas direcionadas ao perfil do usuário. Pode ser usado para fins legítimos, quando incorporado a programas e serviços, como forma de patrocínio ou retorno financeiro para quem desenvolve programas livres ou presta serviços gratuitos.

Pergunta: O que é um adware?

Resposta: Adware é um software indesejado que exibe anúncios publicitários, geralmente na forma de pop-ups. Pode ser usado para fins maliciosos, quando as propagandas apresentadas são direcionadas de acordo com a navegação do usuário e sem que este saiba que tal monitoramento está sendo feito. Alguns adwares mais complexos e danosos possuem a capacidade de sequestrar e invadir os navegadores dos usuários, alterando páginas iniciais de acesso, mecanismos de pesquisas, redirecionamentos automáticos, entre outros, com a finalidade de controlar, até certo ponto, a navegação do usuário.

Pergunta: Qual é a ação principal de um adware?

Resposta: A ação principal de um adware é exibir anúncios publicitários ao usuário, podendo sequestrar e invadir os navegadores para controlar a navegação do usuário. No entanto, a finalidade não é criar zumbis ou inserir vírus.

Pergunta: Em um cenário de ataques de keylogger e screenlog, qual é o tipo de ataque que deve ser protegido?

Resposta: Em um cenário de ataques de keylogger e screenlog, deve-se proteger a rede de ataques do tipo spyware.

Pergunta: O que são keylogger e screenlog?

Resposta: Keylogger e Screenlog são variantes de spyware. Keylogger é um tipo de software que registra as teclas digitadas no teclado do usuário, enquanto Screenlog registra as atividades na tela do usuário.

Pergunta: Qual foi o tipo de ataque spyware que João sofreu quando sua conta foi acessada por terceiros e houve uma interação de inserção de informação por meio da tela com o ponteiro do mouse?

Resposta: João sofreu um ataque de ScreenLogger.

Pergunta: Como são denominados os softwares que realizam ações maliciosas, publicidade indevida, coleta de informações pessoais ou alteração da configuração do computador, sem o consentimento do usuário?

Resposta: Estes softwares são denominados Spywares.

Pergunta: Um spyware instalado e ativo em um computador pode ser detectado pelo uso de qual ferramenta?

Resposta: Firewall.

Pergunta: Como um firewall pode ajudar a detectar a presença de um spyware ativo?

Resposta: O firewall gerencia o tráfego interno gerado pelo spyware para envio a algum serviço externo do atacante, reconhecendo esse tráfego de saída sem lastro em outras requisições, alertando o administrador sobre um tráfego estranho na rede que está enviando dados dos elementos de origem.

Pergunta: O que são Cavalos de Tróia?

Resposta: Cavalos de Tróia são programas que entram no sistema operacional com outros programas escondidos dentro de si. Eles podem executar operações esperadas para ganhar a confiança do usuário enquanto escondem códigos maliciosos.

Pergunta: Os Cavalos de Tróia se restringem a esconder um único tipo de malware?

Resposta: Não, Cavalos de Tróia não se restringem a esconder um único tipo de malware. Eles podem carregar diversos tipos, sejam simultâneos ou não.

Pergunta: O que é um Backdoor em termos de Segurança da Informação?

Resposta: Um Backdoor é um código malicioso que busca criar uma forma de acesso futuro para um atacante. A ideia é não apenas invadir um sistema, mas manter o acesso. Após uma invasão, como por exemplo, através de um Cavalo de Tróia, o atacante instala um backdoor que abrirá uma porta no dispositivo para acesso futuro, podendo adicionar outros códigos e tomar controle total da vítima.

Pergunta: O que é um RAT (Remote Access Trojan) e quais características ele combina?

Resposta: RAT é um programa malicioso que permite ao atacante acessar o equipamento remotamente e executar ações como se fosse o usuário. Combina as características de um trojan e de uma backdoor.

Pergunta: O que é um Rootkit e quais são suas principais operações?

Resposta: Rootkit é um tipo de malware que tem se popularizado pela sua efetividade de invasão e controle, além da dificuldade de detecção. É um conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Suas principais operações incluem: remover evidências de registros em arquivos de logs, instalar outros códigos maliciosos, como backdoors, esconder atividades e informações como arquivos, diretórios, processos, entre outros, e mapear potenciais vulnerabilidades a serem exploradas em outros computadores na rede a qual a vítima está inserida e capturar informações através da interceptação de tráfego.

Pergunta: O que acontece após a invasão e escalada de privilégios em um Sistema Operacional?

Resposta: O invasor obtém o maior nível de acesso possível em um computador. Nos casos de ambientes UNIX, temos o modo ROOT. Para ambientes Windows, temos o modo SYSTEM.

Pergunta: Quais são os tipos de Rootkits que podem ser carregados em um sistema?

Resposta: Os tipos de Rootkits que podem ser carregados em um sistema incluem: Kernel Rootkits (carregado no Kernel do SO); Virtual Rootkits (Agem na camada de virtualização de um sistema); Firmware Rootkit (Agem nos componentes de hardware, como placas de vídeo, controladoras, etc); Library Rootkit (Carregado no módulo de bibliotecas de um SO).

Pergunta: Se Carlos recebeu um e-mail que parecia pertencer ao seu banco e, sem perceber, baixou e instalou um software malicioso no seu computador. A partir desse software, um criminoso cibernético passou a ter o controle do computador de Carlos. Qual é o nome desse software malicioso?

Resposta: O software malicioso instalado no computador de Carlos é um rootkit.

Pergunta: O que é um rootkit e qual é a sua função?

Resposta: Rootkit é um conjunto de programas e técnicas que permitem esconder e assegurar a presença de um invasor ou de outro código malicioso em um computador comprometido. Sua função básica é esconder e assegurar a presença do invasor na máquina.

Pergunta: Qual é a solução técnica de alta prioridade quando um rootkit é identificado como ativo no sistema operacional de um computador?

Resposta: A solução técnica de alta prioridade quando um rootkit é identificado como ativo no sistema operacional de um computador é formatar e reinstalar todo o sistema operacional a partir do zero. Isso garante uma maior segurança, apesar de ser uma prática mais radical.

Pergunta: O que são BOTS e como eles se propagam?

Resposta: BOTS são programas que permitem a comunicação e controle do invasor sobre o sistema da vítima por intermédio de acessos remotos. Eles se propagam de modo semelhante ao Worm, através da replicação de seus códigos e envio pela rede, e-mail ou outros meios.

Pergunta: Quais ações um invasor pode realizar ao ter controle sobre o sistema da vítima através de BOTS?

Resposta: Ao ter controle sobre o sistema da vítima através de BOTS, o invasor pode disparar diversos tipos de ataques utilizando o sistema da vítima, como ataques de negação de serviço,

furto de dados de outras vítimas e envios de SPAM. Isso torna difícil rastrear a origem real do ataque.

Pergunta: O que são BOTS conhecidos como zumbis (Zombies)?

Resposta: BOTS são programas que ficam inertes até que haja o interesse do invasor para utilizá-los para algum fim específico. São conhecidos como zumbis porque ficam dormentes até serem ativados para uso malicioso.

Pergunta: O que é uma BOTNET?

Resposta: Uma BOTNET é uma rede de BOTS ou zumbis. É criada quando se constrói diversos controles de vários BOTS. Essas redes são inclusive comercializadas no mercado negro, podendo ser usadas para potencializar ataques.

Pergunta: O que é um bot no contexto de software malicioso?

Resposta: Bot é um software malicioso que, quando instalado em um computador, possui a capacidade de controlá-lo remotamente.

Pergunta: Qual é a diferença entre um Rootkit e um Bot?

Resposta: O Rootkit e o Bot têm funcionalidades semelhantes, pois ambos podem controlar uma máquina remotamente. No entanto, o Rootkit possui outras perspectivas além das funcionalidades básicas de Bot.

Pergunta: O que é um botnet de acordo com o questionário CESPE / CEBRASPE - 2021 - PG-DF - Analista Jurídico - Analista de Sistema - Suporte e Infraestrutura?

Resposta: Segundo este questionário, um botnet é um tipo de malware que cria uma rede de computadores contaminados.

Pergunta: O que é uma bomba lógica?

Resposta: Uma bomba lógica é um tipo de malware que consiste em programas que são disparados a partir de eventos específicos e predefinidos, como uma data ou um conjunto de caracteres digitados. Geralmente são instaladas a partir de usuários que já possuem acesso ao sistema da vítima.

Pergunta: Onde se pode encontrar um resumo das principais características de alguns tipos de malware?

Resposta: Um resumo das principais características de alguns tipos de malware pode ser encontrado na cartilha do cert.br através do link cartilha.cert.br/malware.

Pergunta: Quais são os tipos de malwares numerados de I a V?

Resposta: I - Rootkit; II - Backdoor; III - Pharming; IV - Vírus; V - Worm

Pergunta: O que significa ataque na camada de aplicação?

Resposta: É um tipo de ataque que tem crescido bastante e que não depende de conhecimento de aspectos da rede, mas tão somente uma codificação e programação maliciosa a nível da camada 7 do modelo OSI.

Pergunta: O que é LFI – Local Files Insert ou Inclusão de Arquivo local?

Resposta: É uma aplicação básica que acontece na tentativa de burlar as técnicas de controle de acesso por intermédio de consultas a arquivos locais no servidor que armazenam informações.

Pergunta: O que é a técnica que utiliza a passagem de parâmetros em suas requisições para manipulação no lado do servidor?

Resposta: Essa técnica é chamada de RFI - Remote File Insert, ou Inclusão de Arquivo Remoto.

Pergunta: Como o RFI funciona?

Resposta: O RFI utiliza um servidor comprometido para inserir arquivos em outro servidor alvo. Isso é feito através da passagem de URL do servidor comprometido para o envio do arquivo em áreas do servidor alvo que suportam a inserção de arquivos.

Pergunta: Quais áreas são mais suscetíveis a ataques de RFI?

Resposta: É mais fácil realizar esse ataque em áreas do site que aceitam a entrada de arquivos e têm códigos que permitem a inserção de URLs como passagem de parâmetro.

Pergunta: O que um atacante fez para detectar um website com componentes vulneráveis?

Resposta: O atacante utilizou um motor de buscas para detectar o website. Ele verificou que a aplicação incluía dinamicamente scripts externos, e assim conseguiu fazer o upload de um script malicioso hospedado em um site controlado por ele.

Pergunta: Quais foram as consequências do comprometimento do website?

Resposta: O comprometimento permitiu a alteração e remoção de páginas, o sequestro do servidor para ser utilizado como um bot de DDoS, e afetou dados com roubo de senhas e informações.

Pergunta: Qual foi a primeira vulnerabilidade explorada que permitiu todos esses ataques?

Resposta: A primeira vulnerabilidade explorada foi a 'remote file inclusion'.

Pergunta: O que é Cross-Site-Scripting (XSS)?

Resposta: O XSS é uma técnica de obter informações do usuário após este ser persuadido a entrar em um site com scripts que são executados no computador da vítima. Uma vez que se executa tal script, com os devidos privilégios de usuário, podem ser executadas rotinas diversas no dispositivo.

Pergunta: O que é um ataque XSS?

Resposta: Um ataque XSS, ou Cross-Site Scripting, é um tipo de ataque que explora uma vulnerabilidade no servidor de aplicação de um sistema e insere código malicioso. Este código afetará todos os usuários que acessarem o link legítimo.

Pergunta: Quais são os dois principais tipos de ataques XSS?

Resposta: Os dois principais tipos de ataques XSS são não persistente e persistente.

Pergunta: Quem é o alvo de um ataque XSS?

Resposta: Contrariamente ao que se pode pensar, o alvo de um ataque XSS não é o servidor de aplicação, mas sim os usuários desse serviço, onde o script malicioso será executado.

Pergunta: Quais são algumas maneiras que um ataque XSS pode ser usado para causar danos?

Resposta: Ataques XSS podem ser usados para sequestrar sessões de usuários através de cookies, alterar códigos HTML no lado do cliente, redirecionar usuários para sites maliciosos (phishing) e alterar os objetos para captura de entradas de usuários.

Pergunta: Como pode-se evitar um ataque XSS?

Resposta: Para evitar um ataque XSS, deve-se separar os dados não confiáveis do ativo no navegador. É possível fazer isso por meio de filtragem adequada de todos os dados não confiáveis, criação de listas brancas ou de entradas positivas, uso de bibliotecas de auto sanitização para conteúdo RICH e implementação de CSP - Content Security Policy em todo o site.

Pergunta: Quais são as medidas que os desenvolvedores/proprietários de sites podem tomar para minimizar a vulnerabilidade de cross-site scripting?

Resposta: Eles podem garantir que qualquer página em seu site que aceite entrada do usuário filtre as entradas de código, como HTML e JavaScript, fazer varredura em busca de vulnerabilidades de aplicativos da Web e corrigi-las, e atualizar seu site e software de servidor para evitar a exploração futura de vulnerabilidades que podem ser visadas por um ataque XSS.

Pergunta: Quais são as ações que os usuários individuais podem fazer para evitar serem vítimas de um ataque XSS?

Resposta: Eles podem desativar os scripts em páginas em que eles não são necessários ou desativá-los completamente, evitar clicar em links de e-mails ou postagens suspeitas em painéis de mensagens, acessar sites diretamente digitando o URL em seu navegador, manter o software atualizado, e fazer a auditoria de aplicativos para determinar quais são necessários e quais raramente são usados.

Pergunta: Quais são as três categorias de cross-site scripting (XSS)?

Resposta: As três categorias de XSS são: o Cross-site scripting armazenado (ou XSS Persistente ou armazenado), o Cross-site scripting Refletido (ou XSS Não persistente ou refletido), e o XSS baseado em DOM.

Pergunta: O que é Cross-site scripting armazenado?

Resposta: O Cross-site scripting armazenado, ou XSS Persistente ou armazenado, é o mais danoso. Ele envolve uma entrada do usuário direto para o processamento em uma página web. Geralmente associada a fóruns de mensagens ou redes sociais, por meio dos comentários e interações. O atacante injeta o código malicioso no servidor, provedor do serviço. Essa carga está armazenada no servidor e será processada, tão logo seja acessado, pelo cliente no navegador da própria vítima.

Pergunta: O que é Cross-site scripting Refletido?

Resposta: O Cross-site scripting Refletido, ou XSS Não persistente ou refletido, não é o mais danoso, mas é o mais comum. Nesse caso, a carga não é armazenada no servidor, e, portanto, deverá fazer parte da carga envolvida na requisição do usuário. Por isso é conhecido como refletido, pois parte do próprio usuário, para ele mesmo. Na prática, a resposta HTTP inclui a carga útil da solicitação HTTP.

Pergunta: O que é Cross-site Scripting (XSS) refletido?

Resposta: É um tipo de ataque que é deflagrado por uma interação anterior da vítima com algum site ou serviço malicioso. Por não ser persistente, o invasor precisa que a carga útil maliciosa seja repassada a cada vítima.

Pergunta: Qual é a diferença entre Cross-site Scripting (XSS) refletido e persistente?

Resposta: No XSS persistente, basta que a carga útil maliciosa seja inserida no servidor, não tendo que ser propagada para cada potencial vítima. No XSS refletido, a carga útil maliciosa precisa ser repassada a cada vítima.

Pergunta: O que é Cross-site Scripting baseado em DOM?

Resposta: É um tipo de ataque associado diretamente ao DOM e não ao HTML. A carga útil da vulnerabilidade não pode ser encontrada na resposta, mas apenas em tempo de execução ou investigando o DOM da página. Geralmente o ataque é aplicado diretamente e exclusivamente no lado do cliente, não sendo enviada ao servidor.

Pergunta: Qual é a característica principal do ataque Cross-site scripting (XSS)?

Resposta: Cross-site scripting (XSS) pode ser realizado de três maneiras: armazenado, refletido e baseado em DOM. O método envolve o envio de códigos JavaScript pelos formulários de cadastro de uma aplicação web com a finalidade de manipular as informações no navegador do usuário.

Pergunta: O que caracteriza um ataque Cross-Site Scripting (XSS) persistente?

Resposta: Um ataque XSS persistente é caracterizado pela inserção do código malicioso no servidor, o que permite que tags HTML sejam incorporadas na seção de comentários da página, de maneira permanente.

Pergunta: Como um ataque de execução de script entre sites (XSS) interfere no fluxo de execução de um programa?

Resposta: Um ataque XSS interfere no fluxo de execução de outros programas ao injetar scripts que serão processados nos dispositivos/browsers das vítimas. O XSS apenas injeta o código/script no servidor WEB que funcionará como vetor de ataque.

Pergunta: Um ataque de XSS (cross site script) permite a injeção de código em formulários HTTP?

Resposta: Sim, a ideia de um ataque XSS é justamente injetar códigos, como Javascript, em páginas e formulários para a posterior captura de dados dos usuários.

Pergunta: O que é um ataque em que um invasor detecta e explora uma vulnerabilidade em um campo de formulário em uma aplicação Web e consegue injetar um script malicioso dentro de uma postagem em uma rede social?

Resposta: Este é um ataque conhecido como XSS armazenado.

Pergunta: Qual é a principal característica de um ataque CSRF (Cross-Site Request Forgery) ou XSRF?

Resposta: O CSRF não busca obter informações ou roubar dados, mas redirecionar ações legítimas do usuário, transformando-as e aplicando no serviço em questão. Pode forçar a vítima a realizar ações indesejadas em aplicações WEB nas quais está autenticada.

Pergunta: Como o ataque CSRF (Cross-Site Request Forgery) ou XSRF é geralmente realizado?

Resposta: Geralmente, a partir de engenharia social, como envio de links. A vítima, ao clicar no link, se torna vítima em todos os ambientes no qual está autenticado, passando a estar suscetível a qualquer manipulação das requisições.

Pergunta: O atacante precisa conhecer a senha da vítima para realizar um ataque CSRF (Cross-Site Request Forgery) ou XSRF?

Resposta: Não, o atacante, apesar de não conhecer a senha da vítima, consegue se utilizar das identidades dela para gerar o ataque.

Pergunta: O que acontece na etapa 1 do ataque cibernético descrito?

Resposta: Na etapa 1, há uma conexão legítima com um servidor correto.

Pergunta: O que ocorre na etapa 2 e 3 do ataque cibernético descrito?

Resposta: Na etapa 2, o próprio usuário acessa um outro site/serviço malicioso. Na etapa 3, ele recebe o conteúdo malicioso, geralmente uma página, em que, ao acessar, passa a estar vulnerável.

Pergunta: O que o atacante é capaz de fazer na etapa 4 do ataque cibernético descrito?

Resposta: Na etapa 4, o atacante é capaz de forjar as requisições a partir da sessão aberta e autenticada de um usuário.

Pergunta: Qual é uma técnica implementada para tentar mitigar os impactos e oportunidades desse tipo de ataque?

Resposta: Uma das técnicas é o recurso HSTS - HTTP Strict Transport Security. Sua implementação reside no estabelecimento da obrigatoriedade por parte de um site ou serviço WEB de que suas requisições sejam realizadas por meio DO HTTPS apenas.

Pergunta: Quais são os problemas observados quando muitos sites e serviços recepcionam as requisições tanto em HTTP quanto em HTTPS?

Resposta: Muitos sites simplesmente implementam um redirecionamento das chamadas HTTP para a página HTTPS. Nessa transição, o usuário está vulnerável e pode ser atacado.

Pergunta: O que é SSL STRIP ATTACK ou SSL DOWNGRADE?

Resposta: É uma forma de ataque onde basicamente o usuário malicioso aplica uma ataque man-in-the-middle, e, antes do estabelecimento da conexão HTTPS entre o usuário e o servidor, ele consegue antecipar.

Pergunta: O que é um token anti-csrf e como ele contribui para a segurança?

Resposta: Um token anti-csrf é uma técnica de segurança que garante que o usuário autenticado é quem deve realizar as requisições. A segurança reside na geração desse token para cada sessão aberta a partir do nó do usuário e só é alterado no ato da renovação da sessão do próprio usuário.

Pergunta: Que medidas de prevenção são difundidas na WEB para prevenir o CSRF?

Resposta: Algumas medidas de prevenção incluem: exigir um segredo específico do token do usuário em todos os formulários de submissões; exigir que o cliente forneça dados de autenticação na solicitação HTTP mesmo se utilizado para realizar qualquer operação com implicações de segurança; limitar o tempo de vida de cookies da sessão; verificar o cabeçalho HTTP Referer; assegurar que não há nenhum arquivo clientaccesspolicy.xml para a concessão de acesso não intencional aos controles Silverlight; e assegurar que não há nenhum arquivo crossdomain.xml concedendo acesso não intencional de vídeos em Flash.

Pergunta: O que é a vulnerabilidade CSRF (crosssite request forgery) em aplicações Web?

Resposta: A vulnerabilidade CSRF ocorre quando solicitações não autorizadas a um website são enviadas a partir de um equipamento onde existe uma sessão ativa em que o website confia.

Pergunta: Qual é uma forma de se proteger do ataque CSRF?

Resposta: Uma forma de se proteger desse ataque é o uso de tokens anti-csrf pela aplicação.

Pergunta: Como o ataque CSRF explora a relação de confiança entre o sítio e o navegador?

Resposta: O ataque CSRF explora a relação de confiança que um sítio possui com o navegador que o acessa, que é uma sessão estabelecida e já reconhecida pelas partes envolvidas.

Pergunta: O que é Injeção SQL (SQL Injection)?

Resposta: Injeção SQL é um ataque que explora uma vulnerabilidade da aplicação, que permite que um usuário malicioso manipule as entradas de banco de dados nos envios de requisições ou consultas à base de dados de alguma aplicação.

Pergunta: Quais danos um ataque de injeção SQL pode causar?

Resposta: Se não houver o devido bloqueio de operações, um ataque de injeção SQL pode, por exemplo, complementar um comando de consulta a uma tabela com um “DROP TABLE”, podendo gerar a perda de todos os dados armazenados ali.

Pergunta: O que acontece se uma aplicação permitir que comandos SQL sejam digitados nos inputs de seus formulários e concatenados diretamente nos comandos SQL da própria aplicação, sem que seja realizada uma validação ou tratamento antecedente?

Resposta: Essa aplicação estará vulnerável ao ataque conhecido como SQL Injection.

Pergunta: O que é SQL Injection?

Resposta: SQL Injection é uma técnica de ataque na qual o invasor se aproveita de falhas em aplicativos web que interagem com bases de dados para inserir uma instrução SQL personalizada e indevida.

Pergunta: O que pode ser feito para evitar a ameaça de SQL Injection?

Resposta: Para evitar essa ameaça de segurança, é necessário validar todas as entradas de dados, como formulários ou URL da aplicação.

Pergunta: É correto usar expressões regulares para cifrar as variáveis enviadas para o sistema para prevenir SQL Injection?

Resposta: Não, a utilização de expressões regulares para controlar a entrada é sempre bem-vinda, mas não com o propósito de cifrar as variáveis enviadas para o sistema.

Pergunta: O que é SQL injection e qual é o seu objetivo?

Resposta: SQL injection consiste em inserir ou manipular consultas efetuadas pela aplicação, não com o objetivo de alterar a performance, mas sim influenciar as estruturas de dados, seja para apagar, alterar, incluir informações diretamente nas tabelas.

Pergunta: O que é a Injeção LDAP (LDAP Injection) e como funciona?

Resposta: A Injeção LDAP tem uma estrutura de funcionamento semelhante ao SQL injection no sentido de manipulação de entradas. É uma técnica para explorar aplicações web que fazem interface com servidores LDAP sem que as informações inseridas sejam verificadas, podendo assim, enviar comandos indesejados, ganhar acessos indevidos, modificar informações e executar comandos com acessos privilegiados.

Pergunta: O que é a Injeção XML (XML Injection) e como ocorre?

Resposta: A Injeção XML segue o mesmo modelo de SQL injection e LDAP injection, ocorre quando o atacante cria um XML com entradas maliciosas explorando vulnerabilidades em sistemas que não aplicam as validações devidas.

Pergunta: O que é uma vulnerabilidade Dia Zero?

Resposta: É a vulnerabilidade existente entre o período de descoberta e de correção de uma falha ou vulnerabilidade em sistemas ou aplicações. Estas vulnerabilidades são descobertas posteriormente pelo fabricante ou desenvolvedor.

Pergunta: O que é Buffer Overflow?

Resposta: É uma clássica falha de programação que possibilita ao usuário malicioso gerar indisponibilidade de serviços ou sistemas. Acontece quando se aloca uma informação que exige espaço em memória ou registradores maiores do que se suporta, gerando um travamento da aplicação.

Pergunta: Como o Buffer Overflow pode ser explorado em um ataque?

Resposta: Um invasor pode injetar strings que extrapolam o tamanho máximo permitido na entrada de um campo, explorando áreas indevidas na memória do servidor ou da vítima. Ao fazer isso, o invasor consegue injetar códigos nas áreas de memória que não deveriam ser acessadas.

Pergunta: O que é o ataque TCP SYN flood?

Resposta: É um ataque que explora a utilização do buffer de espaço durante a inicialização de uma sessão do protocolo de controle de transmissão. Ele pode ser utilizado tanto para indisponibilidade, gerando negação de serviços - DoS, ou também para vazamento de informações.

Pergunta: O que são Complementos Maliciosos (Malicious Add-Ons)?

Resposta: Os Add-ons são complementos a diversos sistemas que permitem a inclusão de recursos adicionais, sejam em navegadores, aplicativos de PC, entre outros. Nem sempre se verifica a legitimidade dos complementos disponibilizados, situação essa que pode gerar a instalação de códigos maliciosos.

Pergunta: O que é Sequestro de Sessão (Session Hijacking)?

Resposta: Sequestro de Sessão é quando a vítima realiza o estabelecimento de uma sessão com determinado servidor web. Um terceiro malicioso, monitorando a comunicação, realiza o spoofing de IP da máquina da vítima e força com que o servidor responda à requisição original para ele. Ele então se passa pela vítima com a sessão já estabelecida, encerrando a sessão com a vítima e tomando controle da comunicação.

Pergunta: Quais são os dois modos de Sequestro de Sessão?

Resposta: Os dois modos de Sequestro de Sessão são o ativo, onde o atacante se passa pela vítima e encerra a sessão com ela, e o passivo, que apenas monitora e coleta dados da sessão, sem encerrar a sessão com a vítima.

Pergunta: O que é uma Ameaça Persistente Avançada (APT - Advanced Persistent Threat)?

Resposta: Uma Ameaça Persistente Avançada é um ataque direcionado a uma vítima de forma concentrada, utilizando diversas técnicas e recursos da rede para processamento dessas investidas. Geralmente se organizam em times ou grupos altamente coordenados para efetuarem os ataques. No entanto, nem todos os ataques direcionados são do tipo APT.

Pergunta: Quais são as cinco fases básicas de um ataque APT?

Resposta: As cinco fases básicas de um ataque APT são: Reconhecimento, onde se faz o levantamento de informações do ambiente da vítima; Incursão ou Investida, onde se utiliza de engenharia social para invadir a rede da organização; Descoberta, onde o atacante mapeia as defesas a partir de uma visão interna da organização; e Captura, onde o atacante consegue invadir os sistemas e capturar informações.

Pergunta: Qual é o objetivo de um ataque APT?

Resposta: O objetivo de um ataque APT é o roubo de dados confidenciais, como descrições de projetos, contratos e informações patenteadas. A finalidade não é 'roubo' ou 'desvio' de dinheiro, mas sim obter informações para que o atacante se torne tão capaz em conhecimento quanto a vítima.

Pergunta: O que são ataques a redes sem fio?

Resposta: Os ataques a redes sem fio buscam explorar as diversas brechas existentes na própria estrutura ou arquitetura de implementação da tecnologia. Nos ambientes de redes sem fio, os dados enviados pelos dispositivos possuem um caráter de Broadcast, ou seja, todos os dispositivos dentro daquele range específico de alcance do sinal podem interceptar o tráfego.

Pergunta: Quais ataques podem ser realizados em redes sem fio?

Resposta: A maioria dos ataques possíveis de serem realizados nos ambientes com fio também poderão ser utilizados nas redes sem fio.

Pergunta: O que é a técnica de EavesDropping?

Resposta: EavesDropping é uma técnica associada à violação do princípio da confidencialidade. Alguém não autorizado se utiliza de algum método ou técnica específica que possibilite a escuta ou o monitoramento do tráfego da vítima, com vistas a obter informações que estão trafegando de forma aberta e sem criptografia.

Pergunta: Em que situações o EavesDropping é comumente utilizado?

Resposta: Um dos principais vetores do EavesDropping está associado a redes sem fio abertas ou com vulnerabilidades associadas às suas fragilidades de segurança, como é o caso dos algoritmos de segurança com vulnerabilidades conhecidas: WEP e WPA. Embora não se restrinja a redes sem fio, é mais utilizado nesse contexto.

Pergunta: Cléber foi vítima de qual tipo de ataque passivo?

Resposta: Cléber foi vítima de um ataque passivo do tipo eavesdropping.

Pergunta: O que é Wardriving?

Resposta: Wardriving é um método que busca procurar redes sem fio através de uma antena de alto alcance conectada a um dispositivo móvel qualquer, geralmente feita a partir de um automóvel, com o objetivo de enumerar redes em busca de redes abertas, desprotegidas ou com sistemas de proteção suscetíveis a quebra.

Pergunta: Como o Wardriving utiliza recursos de GPS?

Resposta: O Wardriving utiliza recursos de GPS para mapear em softwares que disponibilizam mapas, como o Google Maps, apresentando no mapa as diversas redes com os seus respectivos nomes (SSID), bem como suas tecnologias de acesso e autenticação (WEP, WPA, WPA2).

Pergunta: Existe algum software específico para realizar tarefas de Wardriving?

Resposta: Sim, existe o software Kismet, para ambientes UNIX, que realiza tarefas de Wardriving.

Pergunta: O que é um Rogue Access Point e como ele é usado em ataques cibernéticos?

Resposta: Um Rogue Access Point é um ponto de acesso não autorizado que é configurado para receber conexões de outros dispositivos na rede como se fosse um ponto de acesso legítimo. Este tipo de ataque explora brechas na infraestrutura de uma rede sem fio. Uma vez configurado, todos os dados enviados e recebidos pelos dispositivos conectados a ele podem ser capturados e tratados pelo atacante. Este tipo de ataque pode ser amplificado ao configurar pontos de acesso com técnicas de autenticação fracas ou abertas, tornando-se um atrativo para as vítimas.

Pergunta: O que é um ataque de Engenharia Elétrica?

Resposta: Um ataque de Engenharia Elétrica tem como objetivo gerar indisponibilidade da rede sem fio ou prejudicar a qualidade da transmissão de dados. A rede sem fio, que opera em frequências específicas que podem ser facilmente obtidas pelos atacantes, fica vulnerável a um alto grau de interferência. O ataque é realizado através de um equipamento ou antena que gera sinal de alta intensidade na mesma frequência de operação da rede, criando uma relação Sinal-Ruído baixa que impede o funcionamento adequado da rede.

Pergunta: O que é Bluejacking?

Resposta: Bluejacking é um tipo de ataque que explora o modelo de comunicação por bluetooth. Seu funcionamento é similar ao SPAM no contexto de correio eletrônico, mas para o bluetooth, utiliza-se o protocolo OBEX. Este tipo de ataque geralmente não causa danos às vítimas, que acabam recebendo mensagens de texto com propagandas ou informações indesejadas de outros dispositivos que estejam próximos. Caso o dispositivo suporte mensagens multimídia (MMS), estas também podem ser utilizadas.

Pergunta: Qual a principal proteção contra ataques ao usar o bluetooth?

Resposta: A principal proteção contra ataques ao usar o bluetooth é não habilitar o modo 'visível' do aparelho quando o bluetooth está ativado, invocando assim o método de segurança por obscuridade ou desconhecimento.

Pergunta: O que é bluesnarfing?

Resposta: Bluesnarfing é um tipo de ataque que ocorre em redes bluetooth e possui um caráter invasivo que fere a privacidade e pode atingir a confidencialidade de dados nos aparelhos das vítimas. Esta técnica permite que o atacante tenha acesso à agenda, lista de

contatos, correios eletrônicos, mensagens de textos, entre outros recursos do aparelho da vítima.

Pergunta: Qual foi o impacto das técnicas de autenticação para a sincronização ou emparelhamento de dispositivos via bluetooth no bluesnarfing?

Resposta: Com o surgimento de técnicas de autenticação para a sincronização ou o emparelhamento de dispositivos via bluetooth, a técnica de bluesnarfing perdeu força.

Pergunta: O que é o NMAP?

Resposta: O NMAP é uma ferramenta gratuita e de código aberto utilizada tanto de forma legítima (auditoria de segurança) como ilegítima (descoberta de informações da rede).

Pergunta: Como é a estrutura padrão do comando executado pelo NMAP?

Resposta: A estrutura padrão do comando executado pelo NMAP se dá da seguinte forma: # nmap [Scan Type(s)] [Options] {target specification}. Onde Scan Type(s) determina a técnica utilizada e o tipo de resultado esperado, Options é um campo opcional para complemento da varredura e Target specification é o IP do alvo.

Pergunta: O que o parâmetro '-p' faz na varredura de um alvo?

Resposta: O parâmetro '-p' é utilizado para determinar portas específicas a serem varridas no alvo.

Pergunta: O que o parâmetro '-sT' faz na varredura de um alvo?

Resposta: O parâmetro '-sT' realiza um escaneamento através de tentativas de conexão TCP – TCP (CONNECT). Caso se consiga uma conexão em determinada porta, indica que esta porta está aberta.

Pergunta: O que o parâmetro '-sS' faz na varredura de um alvo?

Resposta: O parâmetro '-sS' realiza uma tentativa com pacotes TCP com a flag SYN ligada, como uma requisição de conexão – TCP SYN (HALF OPEN). Se um pacote SYN-ACK é recebido, indica que a porta está aberta.

Pergunta: O que o parâmetro '-sF' faz na varredura de um alvo?

Resposta: O parâmetro '-sF', também conhecido como método STEALTH, envia pacotes FIN para o alvo. Se não houver resposta, a porta está aberta, se um pacote RST for recebido, a porta está fechada.

Pergunta: O que o parâmetro '-sA' faz na varredura de um alvo?

Resposta: O parâmetro '-sA', também conhecido como ACK SCAN, é utilizado para mapear o firewall alvo. Ele pode determinar o tipo de firewall e se ele apenas bloqueia os pacotes SYN.

Pergunta: O que o parâmetro '-sP' faz na varredura de um alvo?

Resposta: O parâmetro '-sP', também conhecido como PING SCAN, envia pacotes 'ICMP echo request' para o alvo. É utilizado para verificar se a máquina alvo está ativa ou não.

Pergunta: O que o parâmetro '-sV' faz na varredura de um alvo?

Resposta: O parâmetro '-sV' habilita a detecção de versão. Alternativamente, pode-se utilizar o parâmetro '-A' para habilitar tanto a detecção de SO como a detecção de versão.

Pergunta: O que o parâmetro '-sU' faz na varredura de um alvo?

Resposta: O parâmetro '-sU' envia um pacote UDP de 0 byte. Caso seja recebido um 'ICMP port Unreachable', a porta está fechada, caso contrário, está aberta.

Pergunta: O que o parâmetro '-sO' faz na varredura de um alvo?

Resposta: O parâmetro '-sO' é usado para tentar determinar os protocolos suportados pelo host.

Pergunta: O que o parâmetro '-O' faz na varredura de um alvo?

Resposta: O parâmetro '-O', também conhecido como TCP/IP FINGERPRINT, ativa a identificação remota do sistema operacional.

Pergunta: O que o nmap verifica em um sistema operacional?

Resposta: O nmap verifica a base de dados dos sistemas operacionais conhecidos, detectando qual o sistema é usado na máquina. Também verifica a porta e o serviço que estão rodando.

Pergunta: Quais são algumas das opções adicionais que o nmap oferece?

Resposta: O nmap oferece opções como o scan rápido (nmap -F) e a opção de não pingar a máquina antes de realizar o scan (nmap -P0). Ele também oferece a opção de escolher 'políticas' para dificultar a detecção pelo IDS da máquina alvo. As opções são 'Paranoid', 'Sneaky', 'Polite', 'Normal', 'Aggressive' ou 'Insane'.

Pergunta: Como as políticas do nmap funcionam?

Resposta: A política 'Paranoid' escaneia de 5 em 5 minutos cada porta, a 'Sneaky', de 15 em 15 segundos e assim por diante. A vantagem do scan ser mais lento é que dificulta a descoberta pelo IDS da máquina alvo. A opção padrão é a normal.

Pergunta: O que será apresentado após um SCAN de uma rede através do comando # nmap -sS 192.168.0.0/24 -p 1-150?

Resposta: Serão apresentadas quais portas TCP estão abertas em cada host ativo na rede.

Pergunta: Como podemos proteger nossos sistemas contra varreduras do nmap?

Resposta: Na prática, devemos sempre buscar por firewalls e IPS para identificar e filtrar esse tipo de varredura.

Pergunta: O que é HARDENING de servidores?

Resposta: HARDENING de servidores é a aplicação de regras rígidas para garantir a segurança. Uma das técnicas altamente recomendadas é a configuração apenas dos serviços essenciais em cada servidor.

Pergunta: O que acontece quando o valor off é atribuído à variável server_tokens no servidor nginx?

Resposta: Quando o valor off é atribuído à variável server_tokens, a versão do servidor nginx não será exibida em páginas de erro e no cabeçalho http/s. Isso significa que o comando nmap não receberá essa informação e não mostrará a versão do nginx.

Pergunta: O que é OWASP Top 10?

Resposta: O OWASP Top 10 é um documento de conscientização padrão para desenvolvedores e segurança de aplicativos da web. Ele representa um amplo consenso sobre os riscos de segurança mais críticos para aplicativos da web. É reconhecido globalmente pelos desenvolvedores como o primeiro passo para uma codificação mais segura.

Pergunta: Qual é a importância do OWASP Top 10 para as empresas?

Resposta: As empresas devem adotar o OWASP Top 10 e iniciar o processo de garantir que suas aplicações web minimizem esses riscos. Usar o OWASP Top 10 pode ser o primeiro passo mais eficaz para mudar a cultura de desenvolvimento de software em uma organização para uma que produza um código mais seguro.

Pergunta: O que é o OWASP Top 10?

Resposta: O OWASP Top 10 é uma lista que reflete as vulnerabilidades mais comuns identificadas em centenas de organizações, aplicações e APIs. Os tópicos do Top 10 são selecionados e ordenados de acordo com a sua prevalência, combinada com uma estimativa ponderada do potencial de abuso, detecção e impacto.

Pergunta: Qual o principal objetivo do OWASP Top 10?

Resposta: O principal objetivo do OWASP Top 10 é o de educar programadores, desenhadores e arquitetos de aplicações, bem como gestores e as próprias organizações sobre as consequências dos problemas de segurança mais comuns e mais importantes no contexto das aplicações web.

Pergunta: O que o Top 10 da OWASP oferece?

Resposta: O Top 10 da OWASP oferece técnicas básicas para proteção nestas áreas problemáticas e de elevado risco, além de direções sobre onde encontrar informação adicional sobre estes assuntos.

Pergunta: O que é a Classificação de Risco para o Top 10 da OWASP?

Resposta: A Classificação de Risco para o Top 10 da OWASP é uma metodologia baseada na OWASP Risk Rating Methodology e consiste em estimar, para cada categoria do Top 10, o risco peculiar que cada falha introduz em uma aplicação web típica e, posteriormente, ordenar o Top 10 de acordo com as falhas que tipicamente introduzem o risco mais significativo para uma aplicação.

Pergunta: Como funciona a metodologia de classificação de riscos da OWASP?

Resposta: A metodologia de classificação de riscos da OWASP envolve mapear CWEs, calcular a taxa de incidência máxima e média, a exploração média ponderada, o impacto médio ponderado, e a cobertura máxima e média para chegar à classificação.

Pergunta: Quantas ocorrências e CVEs foram registradas?

Resposta: Foram registradas um total de 318,487 ocorrências e 19,13 CVEs.

Pergunta: Quais foram as três categorias que deixaram de existir em 2017?

Resposta: As três categorias que deixaram de existir em 2017 foram: A04:2017 - XML External Entities (XXE), A07:2017 - Cross-Site Scripting (XSS) e A08:2017 -Insecure Deserialization.

Pergunta: Quais são as três novas categorias que surgiram nesse processo?

Resposta: As três novas categorias que surgiram nesse processo são: A04:2021 - Security Misconfiguration, A08:2021 - Software and Data Integrity Failures e A10:2021 - Server-Side Request Forgery (SSRF).

Pergunta: Quantas categorias estão previstas no OWASP?

Resposta: Estão previstas 10 categorias no OWASP.

Pergunta: O que cada categoria no OWASP apresenta?

Resposta: Cada categoria no OWASP apresenta uma visão geral da vulnerabilidade, com uma descrição associada, e contramedidas/prevenções que devem ser aplicadas ou realizadas.

Pergunta: O que é a Quebra de Controle de Acesso?

Resposta: É uma falha no processo de restrição de ações com base em permissões que pode levar a divulgação, modificação ou destruição não autorizadas da informação.

Pergunta: Quais são algumas vulnerabilidades relacionadas à Quebra de Controle de Acesso?

Resposta: Algumas vulnerabilidades incluem violação do princípio de privilégio mínimo, ignorar verificações de controle de acesso modificando a URL ou estado interno do aplicativo, permitir visualização ou edição da conta de outra pessoa, acessar API com controles de acesso ausentes, elevação de privilégio, manipulação de metadados, configuração incorreta do CORS e forçar a navegação em páginas autenticadas como usuário não autenticado.

Pergunta: O que é o princípio de privilégio mínimo?

Resposta: É um princípio onde o acesso deve ser concedido apenas para recursos, funções ou usuários específicos.

Pergunta: O que é a manipulação de metadados?

Resposta: É uma prática onde um invasor pode reproduzir ou adulterar um token de controle de acesso, como um JSON Web Token (JWT), ou um cookie ou campo oculto para elevar privilégios ou abusar da invalidação de JWT.

Pergunta: Como podem ser prevenidas as quebras de controle de acesso?

Resposta: Algumas medidas de prevenção incluem negar por padrão, exceto para recursos públicos, implementar mecanismos de controle de acesso uma vez e reutilizá-los em todo o aplicativo, impor a propriedade do registro através dos modelos de controle de acesso, impor

requisitos exclusivos de limite de negócios por modelos de domínio e desativar a listagem de diretórios do servidor web.

Pergunta: O que deve ser registrado e alertado aos administradores no controle de acesso?

Resposta: Falhas de controle de acesso, especialmente falhas repetidas.

Pergunta: Por que se deve limitar a taxa de acesso à API e ao controlador?

Resposta: Para minimizar os danos das ferramentas de ataque automatizadas.

Pergunta: O que deve acontecer com os identificadores de sessão com estado após o logout?

Resposta: Os identificadores de sessão com estado devem ser invalidados no servidor após o logout.

Pergunta: Quais são as recomendações para tokens JWT sem estado?

Resposta: Os tokens JWT sem estado devem ser de curta duração para minimizar a janela de oportunidade para um invasor. Para JWTs de vida mais longa, é altamente recomendável seguir os padrões OAuth para revogar o acesso.

Pergunta: O que é a falha ou quebra de controle de acesso?

Resposta: "Broken Access Control" é um risco de segurança crítico para aplicações Web.

Pergunta: Quais são as recomendações do OWASP para prevenir a quebra de controle de acesso?

Resposta: Desativar a listagem de diretórios do servidor web, garantir que os tokens JWT stateless sejam de curta duração, invalidar as sessões stateful no servidor após o logout, evitar reutilizar os mecanismos de controle de acesso, e limitar a taxa de requisições de APIs.

Pergunta: O que é A02:2021 - Falhas criptográficas?

Resposta: São falhas relacionadas à criptografia ou falta dela.

Pergunta: Quais são os riscos de exposição de dados sensíveis ou confidenciais?

Resposta: Os riscos incluem violação da privacidade, perda de propriedade intelectual, danos à reputação e possíveis penalidades legais.

Pergunta: Por que é importante a determinação de segurança de dados em trânsito ou repouso?

Resposta: A determinação de segurança de dados em trânsito ou repouso é importante para proteger os dados contra acesso não autorizado, alteração ou destruição.

Pergunta: Qual é a importância do uso da criptografia para dados em repouso e em trânsito?

Resposta: A criptografia é importante para proteger os dados contra acesso não autorizado, garantindo que apenas as pessoas com a chave adequada possam descriptografar e acessar os dados.

Pergunta: O que são vulnerabilidades em relação à segurança de dados?

Resposta: Vulnerabilidades são falhas ou lacunas na segurança que podem ser exploradas para ganhar acesso não autorizado, alterar ou destruir dados.

Pergunta: Quais são as consequências de transmitir dados em texto simples?

Resposta: Transmitir dados em texto simples pode permitir que atacantes interceptem e leiam os dados, potencialmente levando a uma violação de dados.

Pergunta: Quais são os riscos de usar um algoritmo ou protocolo criptográfico antigo ou fraco?

Resposta: Usar um algoritmo ou protocolo criptográfico antigo ou fraco pode permitir que atacantes decifrem os dados criptografados, comprometendo a segurança dos dados.

Pergunta: Quais são os problemas com o uso de chaves criptográficas padrão ou fracas?

Resposta: O uso de chaves criptográficas padrão ou fracas pode facilitar a decifração dos dados por atacantes, comprometendo a segurança dos dados.

Pergunta: Por que é importante validar o certificado do servidor recebido e a cadeia de confiança?

Resposta: A validação do certificado do servidor recebido e da cadeia de confiança é importante para garantir a autenticidade do servidor e a segurança dos dados.

Pergunta: Quais são os problemas com o uso de funções de hash obsoletas ou não criptográficas?

Resposta: O uso de funções de hash obsoletas ou não criptográficas pode facilitar a decifração dos dados por atacantes, comprometendo a segurança dos dados.

Pergunta: Quais são os riscos de usar métodos de preenchimento criptográfico obsoletos?

Resposta: O uso de métodos de preenchimento criptográfico obsoletos pode facilitar a decifração dos dados por atacantes, comprometendo a segurança dos dados.

Pergunta: Quais são os riscos de exploração de mensagens de erro criptográficas ou informações de canal lateral?

Resposta: A exploração de mensagens de erro criptográficas ou informações de canal lateral pode permitir que atacantes obtenham informações sensíveis, comprometendo a segurança dos dados.

Pergunta: O que é quebra de autenticação e utilização indevida de acessos?

Resposta: É a interação com domínios não autorizados ou restritos, gerando vulnerabilidades.

Pergunta: Como você deve classificar os dados processados, armazenados ou transmitidos por um aplicativo?

Resposta: Os dados devem ser identificados e classificados como confidenciais de acordo com as leis de privacidade, requisitos regulatórios ou necessidades de negócios.

Pergunta: Por que é importante não armazenar dados confidenciais desnecessariamente?

Resposta: Os dados que não são retidos não podem ser roubados, portanto, é recomendável descartá-los o mais rápido possível ou usar tokenização compatível com PCI DSS ou até mesmo truncamento.

Pergunta: O que significa criptografar todos os dados confidenciais em repouso?

Resposta: Significa que todos os dados confidenciais que estão armazenados devem ser criptografados para melhorar a segurança.

Pergunta: Por que é importante garantir que algoritmos, protocolos e chaves padrão atualizados e fortes estejam em vigor?

Resposta: É importante para garantir a segurança dos dados. Além disso, é necessário usar o gerenciamento de chaves adequado.

Pergunta: O que é TLS com cifras de sigilo de encaminhamento (FS)?

Resposta: É um protocolo seguro usado para criptografar todos os dados em trânsito, priorizando as cifras pelo servidor e parâmetros seguros. Deve-se impor a criptografia usando diretivas como HTTP Strict Transport Security (HSTS).

Pergunta: Por que é recomendável desabilitar o armazenamento em cache para respostas que contenham dados confidenciais?

Resposta: É recomendável porque ajuda a proteger esses dados confidenciais de serem acessados indevidamente.

Pergunta: Por que não se deve usar protocolos legados, como FTP e SMTP, para transportar dados confidenciais?

Resposta: Esses protocolos são considerados inseguros e podem levar a vazamentos de dados confidenciais.

Pergunta: Como devem ser armazenadas as senhas?

Resposta: As senhas devem ser armazenadas usando funções de hashing adaptáveis e Salt com um fator de trabalho (fator de atraso), como Argon2, scrypt, bcrypt ou PBKDF2.

Pergunta: O que são vetores de inicialização e como devem ser escolhidos?

Resposta: Vetores de inicialização são usados em criptografia. Para muitos modos, isso significa usar um CSPRNG (gerador de números pseudo-aleatórios criptograficamente seguro). Para modos que exigem um nonce, o vetor de inicialização (IV) não precisa de um CSPRNG. Em todos os casos, o IV nunca deve ser usado duas vezes para uma chave fixa.

Pergunta: Por que é importante usar criptografia autenticada em vez de apenas criptografia?

Resposta: Criptografia autenticada oferece um nível adicional de segurança, garantindo que os dados não foram alterados durante o trânsito.

Pergunta: Como devem ser geradas e armazenadas as chaves na criptografia?

Resposta: As chaves devem ser geradas criptograficamente aleatoriamente e armazenadas na memória como arrays de bytes. Se uma senha for usada, ela deverá ser convertida em uma chave por meio de uma função de derivação de chave de base de senha apropriada.

Pergunta: O que é aleatoriedade criptográfica e por que é importante?

Resposta: Aleatoriedade criptográfica é uma propriedade importante na criptografia que ajuda a garantir a segurança dos dados. Deve ser usada quando apropriado e que não tenha sido propagada de maneira previsível ou com baixa entropia.

Pergunta: Por que é importante evitar funções criptográficas obsoletas e esquemas de preenchimento, como MD5, SHA1, PKCS número 1 v1.5?

Resposta: Essas funções e esquemas são considerados inseguros e podem levar a vazamentos de dados.

Pergunta: O que significa verificar de forma independente a eficácia da configuração e configurações?

Resposta: Significa que você deve verificar regularmente as configurações de segurança para garantir que elas estejam funcionando efetivamente.

Pergunta: O que é o Controle A02:2021 - Falhas Criptográficas do OWASP?

Resposta: É uma medida de prevenção contra falhas de segurança relacionadas a criptografia, incluindo a proteção de dados sensíveis contra exposição.

Pergunta: O que é o A03:2021 - Injeção?

Resposta: A03:2021 - Injeção é uma vulnerabilidade de segurança que congrega diversas técnicas de ataque, incluindo XSS, CSRF e SQL Injection. É caracterizada pela injeção de código malicioso ou scripts em um programa ou sistema.

Pergunta: Quais são as ferramentas utilizadas para identificar vulnerabilidades?

Resposta: As ferramentas utilizadas para identificar vulnerabilidades incluem SAST (que verifica o código estático ou código fonte), DAST (foca nas funcionalidades do sistema, simulando a ótica do usuário), e IAST (traz uma perspectiva das interações do código e produto).

Pergunta: Quais são as vulnerabilidades comuns relacionadas à injeção de código?

Resposta: As vulnerabilidades comuns relacionadas à injeção de código incluem: dados fornecidos pelo usuário não são validados, filtrados ou higienizados pelo aplicativo; consultas dinâmicas ou chamadas não parametrizadas sem escape sensível ao contexto são usadas diretamente no interpretador; e dados hostis são usados em parâmetros de pesquisa de mapeamento relacional de objeto (ORM) para extrair registros confidenciais adicionais.

Pergunta: O que são dados hostis em consultas dinâmicas?

Resposta: Dados hostis são usados diretamente ou concatenados. O SQL ou comando contém a estrutura e os dados maliciosos em consultas dinâmicas, comandos ou procedimentos armazenados.

Pergunta: Quais são as principais vulnerabilidades associadas à entrada de dados diretamente nas páginas?

Resposta: As vulnerabilidades são principalmente associadas à entrada de dados diretamente nas páginas por parte de áreas dinâmicas e chamadas diversas ao código por parte do usuário.

Pergunta: Como prevenir a injeção de dados maliciosos?

Resposta: Para prevenir a injeção de dados maliciosos, é importante manter os dados separados de comandos e consultas, usar uma API segura, validar a entrada de dados do lado do servidor, escapar caracteres especiais em consultas dinâmicas e usar LIMIT e outros controles SQL nas consultas.

Pergunta: O que deve ser feito mesmo quando os procedimentos armazenados estão parametrizados?

Resposta: Mesmo quando parametrizados, os procedimentos armazenados ainda podem introduzir injeção de SQL se PL/SQL ou T-SQL concatenar consultas e dados ou executar dados hostis com EXECUTE IMMEDIATE ou exec().

Pergunta: Por que é importante usar validação de entrada positiva do lado do servidor?

Resposta: A validação de entrada positiva do lado do servidor é importante porque muitos aplicativos exigem caracteres especiais, como áreas de texto ou APIs para aplicativos móveis.

Pergunta: O que deve ser feito para evitar a divulgação em massa de registros em caso de injeção de SQL?

Resposta: É preciso usar LIMIT e outros controles SQL nas consultas para evitar a divulgação em massa de registros em caso de injeção de SQL.

Pergunta: Por que não é recomendado usar protocolos legados, como FTP e SMTP, para o transporte de dados confidenciais?

Resposta: O uso de protocolos legados, como FTP e SMTP, para o transporte de dados confidenciais pode levar a falhas criptográficas, e não de injeção de dados.

Pergunta: O que é design inseguro?

Resposta: Design inseguro é uma categoria que se concentra nos aspectos relacionados a problemas de arquitetura e design do produto. Esta categoria é focada na pré-codificação, ou seja, antes do código ser desenvolvido. O problema pode ser devido à ausência de controles ou à ineficácia desses controles durante o período de design. É necessário fortalecer as ações associadas ao processo de coleta de requisitos e ao Ciclo de Desenvolvimento Seguro.

Pergunta: Um design seguro pode ainda ter defeitos de implementação?

Resposta: Sim, um design seguro ainda pode ter defeitos de implementação levando a vulnerabilidades que podem ser exploradas.

Pergunta: Por que um design inseguro não pode ser corrigido por uma implementação perfeita?

Resposta: Um design inseguro não pode ser corrigido por uma implementação perfeita, pois, por definição, os controles de segurança necessários nunca foram criados para se defender contra ataques específicos.

Pergunta: Qual é a importância de ter um processo bem definido e desenhado na construção de uma solução?

Resposta: É crucial ter um processo bem definido e desenhado na construção de uma solução, incorporando questões de segurança antes do desenvolvimento. Isso é semelhante à fundação de uma casa. Se a fundação tiver problemas, a casa sempre terá problemas estruturais, independentemente da qualidade do código que será desenvolvido.

Pergunta: Quais são algumas das medidas de prevenção contra o design inseguro?

Resposta: Algumas das medidas de prevenção incluem: estabelecer e usar um ciclo de vida de desenvolvimento seguro com profissionais da AppSec, estabelecer e usar uma biblioteca de padrões de projeto seguros, usar a modelagem de ameaças para autenticação crítica, integrar linguagem e controles de segurança em histórias de usuários, integrar verificações de plausibilidade em cada camada do seu aplicativo, escrever testes de unidade e integração, segregar camadas de camadas no sistema e nas camadas de rede, e separar os locatários de forma robusta por design em todas as camadas.

Pergunta: Quais são as medidas de prevenção para o desenvolvimento seguro de acordo com a OWASP TOP 10 2021 para o risco de design inseguro?

Resposta: As medidas de prevenção para o desenvolvimento seguro são o uso da modelagem de ameaças para autenticações críticas, controle de acesso e lógica de negócios.

Pergunta: O que é a configuração incorreta de segurança de acordo com a OWASP TOP 10 2021?

Resposta: A configuração incorreta de segurança envolve a configuração de ambientes e servidores, ausências de baselines seguras e ferramentas de compliance.

Pergunta: O que é uma baseline de segurança?

Resposta: Uma baseline de segurança é uma configuração de referência que pode ser incorporada e espelhada, com todas as diretrizes e padrões de segurança já conhecidos e mapeados.

Pergunta: Quais são as vulnerabilidades listadas na configuração incorreta de segurança de acordo com a OWASP TOP 10 2021?

Resposta: As vulnerabilidades incluem falta de proteção de segurança apropriada, recursos desnecessários ativados ou instalados, contas padrão e suas senhas ainda habilitadas e inalteradas, tratamento de erros que revelam excesso de informações, recursos de segurança mais recentes desabilitados ou mal configurados, configurações de segurança inseguras em servidores de aplicativos e outros componentes, servidor não enviando cabeçalhos ou diretivas de segurança, e software desatualizado ou vulnerável.

Pergunta: Quais são as medidas de prevenção listadas para a configuração incorreta de segurança de acordo com a OWASP TOP 10 2021?

Resposta: Uma das medidas de prevenção é um processo de proteção repetível que torna rápido e fácil a implantação de outro ambiente devidamente bloqueado. Os ambientes de desenvolvimento e controle também devem ser considerados.

Pergunta: Como devem ser configurados os ambientes de qualidade e produção?

Resposta: Qualidade e produção devem ser configurados de forma idêntica, com credenciais diferentes usadas em cada ambiente. Esse processo deve ser automatizado para minimizar o esforço necessário para configurar um novo ambiente seguro.

Pergunta: O que é uma plataforma mínima?

Resposta: Uma plataforma mínima é aquela sem recursos, componentes, documentação e amostras desnecessários. Recursos e estruturas não utilizados são removidos ou não instalados.

Pergunta: Qual é a tarefa necessária para manter as configurações de segurança atualizadas?

Resposta: Uma tarefa para revisar e atualizar as configurações apropriadas para todas as notas de segurança, atualizações e patches como parte do processo de gerenciamento de patches. Isso inclui a revisão das permissões de armazenamento em nuvem, por exemplo, permissões de bucket do S3.

Pergunta: O que é uma arquitetura de aplicativo segmentada?

Resposta: Uma arquitetura de aplicativo segmentada fornece separação eficaz e segura entre componentes ou locatários, com segmentação, conteinerização ou grupos de segurança de nuvem (ACLs).

Pergunta: O que são diretivas de segurança?

Resposta: Diretivas de segurança são instruções enviadas para clientes para melhorar a segurança, por exemplo, Cabeçalhos de Segurança.

Pergunta: Como verificar a eficácia das configurações de segurança?

Resposta: Um processo automatizado deve ser usado para verificar a eficácia das configurações e ajustes em todos os ambientes.

Pergunta: A inadequada configuração de segurança pode ocorrer em qualquer nível de serviço de uma aplicação?

Resposta: Sim, a inadequada configuração de segurança, um dos riscos da OWASP Top 10, pode ocorrer em qualquer nível de serviço de uma aplicação.

Pergunta: São ineficazes os scanners e testes automatizados na tarefa de detectar falhas de configuração?

Resposta: Não, na verdade, scanners e testes automatizados são muito eficazes na detecção de falhas de configuração.

Pergunta: O que são Componentes Vulneráveis e Desatualizados no contexto de segurança da informação?

Resposta: Componentes Vulneráveis e Desatualizados estão associados ao processo de inventário de software. Ao conhecer o parque de software, é possível entender possíveis vulnerabilidades e planejar ações de mitigação.

Pergunta: Como as atualizações automáticas se relacionam com a segurança da informação?

Resposta: Atualizações automáticas são uma forma de mitigar vulnerabilidades, mas nem sempre são simples e podem gerar quebras na aplicação utilizada, exigindo retrabalho.

Pergunta: O que pode ser uma vulnerabilidade se não conhecermos todas as versões dos componentes que usamos?

Resposta: Se não conhecermos as versões de todos os componentes que usamos, tanto do lado do cliente quanto do lado do servidor, isso pode ser uma vulnerabilidade. Isso inclui componentes que usamos diretamente, bem como dependências aninhadas.

Pergunta: Como um software pode se tornar vulnerável?

Resposta: O software pode se tornar vulnerável se for sem suporte ou desatualizado. Isso inclui o sistema operacional, servidor de aplicativos/web, sistema de gerenciamento de banco de dados (DBMS), aplicativos, APIs e todos os componentes, ambientes de tempo de execução e bibliotecas.

Pergunta: Por que é importante verificar regularmente as vulnerabilidades e assinar boletins de segurança?

Resposta: É importante verificar regularmente as vulnerabilidades e assinar boletins de segurança porque se você não fizer isso, você pode estar exposto a riscos relacionados aos componentes que você usa.

Pergunta: O que pode acontecer se você não corrigir ou atualizar a plataforma, as estruturas e as dependências subjacentes de maneira oportuna e baseada em risco?

Resposta: Se você não corrigir ou atualizar a plataforma, as estruturas e as dependências subjacentes de maneira oportuna e baseada em risco, isso pode deixar as organizações abertas a dias ou meses de exposição desnecessária a vulnerabilidades corrigidas. Isso geralmente acontece em ambientes em que a correção é uma tarefa mensal ou trimestral sob controle de alterações.

Pergunta: Por que os desenvolvedores de software devem testar a compatibilidade de bibliotecas atualizadas, atualizadas ou corrigidas?

Resposta: Os desenvolvedores de software devem testar a compatibilidade de bibliotecas atualizadas, atualizadas ou corrigidas para garantir que não haja vulnerabilidades ou problemas que possam ser explorados.

Pergunta: Por que é importante proteger as configurações dos componentes?

Resposta: É importante proteger as configurações dos componentes para evitar a configuração incorreta de segurança, que pode levar a vulnerabilidades e exposições desnecessárias.

Pergunta: Como você pode prevenir vulnerabilidades?

Resposta: Algumas maneiras de prevenir vulnerabilidades incluem: remover dependências não utilizadas, recursos, componentes, arquivos e documentação desnecessários; fazer um inventário contínuo das versões de componentes do lado do cliente e do lado do servidor e

suas dependências; obter apenas componentes de fontes oficiais em links seguros; e monitorar bibliotecas e componentes que não são mantidos ou não criam patches de segurança para versões mais antigas.

Pergunta: Por que é importante monitorar fontes como a Vulnerabilidade e exposições comuns (CVE) e a National Vulnerability Database (NVD)?

Resposta: É importante monitorar fontes como a Vulnerabilidade e exposições comuns (CVE) e a National Vulnerability Database (NVD) para ficar atualizado sobre as vulnerabilidades mais recentes que podem afetar os componentes que você usa. Ferramentas de análise de composição de software podem ser usadas para automatizar este processo.

Pergunta: Por que devemos preferir pacotes assinados ao adquirir componentes?

Resposta: Devemos preferir pacotes assinados ao adquirir componentes para reduzir a chance de incluir um componente mal-intencionado modificado.

Pergunta: O que fazer se a aplicação de patches não for possível?

Resposta: Se a aplicação de patches não for possível, devemos considerar a implantação de um patch virtual para monitorar, detectar ou proteger contra o problema descoberto.

Pergunta: O que é Falhas de Identificação e Autenticação?

Resposta: Falhas de Identificação e Autenticação se refere a vulnerabilidades no processo de identificação e autenticação de usuários. Isso é diferente do A01, que trata de autorização. As falhas de identificação e autenticação podem levar a ataques de personificação ou falsificação de identidade.

Pergunta: Quais são as vulnerabilidades associadas às Falhas de Identificação e Autenticação?

Resposta: As vulnerabilidades associadas incluem: permissão para ataques automatizados (como preenchimento de credenciais), permissão para ataques de força bruta, uso de senhas padrão, fracas ou conhecidas, processos fracos de recuperação de credenciais, armazenamento de senhas de texto simples, ausência de autenticação multifator eficaz, exposição do identificador de sessão na URL e reutilização do identificador de sessão após o login.

Pergunta: O que são medidas de prevenção contra as Falhas de Identificação e Autenticação?

Resposta: As medidas de prevenção incluem: implementação de autenticação multifator para evitar ataques automatizados, não enviar ou implantar com credenciais padrão (especialmente para usuários administradores) e implementar verificações de senhas fracas, como testar novas ou alteradas senhas na lista das 10.000 piores senhas.

Pergunta: Quais diretrizes devem ser seguidas para políticas de comprimento, complexidade e rotação de senha?

Resposta: As políticas de comprimento, complexidade e rotação de senha devem ser alinhadas com as diretrizes do Instituto Nacional de Padrões e Tecnologia (NIST) 800-63b na seção 5.1.1 para Segredos Memorizados ou outras políticas de senha modernas baseadas em evidências.

Pergunta: Como podem ser protegidos os caminhos de registro, recuperação de credenciais e API contra ataques de enumeração de conta?

Resposta: Os caminhos de registro, recuperação de credenciais e API podem ser protegidos contra ataques de enumeração de conta usando as mesmas mensagens para todos os resultados.

Pergunta: Qual ação deve ser tomada em relação às tentativas de login com falha?

Resposta: Cada vez mais, deve-se limitar ou retardar as tentativas de login com falha, mas com cuidado para não criar um cenário de negação de serviço. É preciso registrar todas as falhas e alertar os administradores quando forem detectados preenchimento de credenciais, força bruta ou outros ataques.

Pergunta: Como deve funcionar um gerenciador de sessão seguro?

Resposta: Um gerenciador de sessão seguro deve ser integrado, seguro e do lado do servidor, gerando um novo ID de sessão aleatório com alta entropia após o login. O identificador de sessão não deve estar no URL, deve ser armazenado com segurança e invalidado após o logout, inatividade e tempos limites absolutos.

Pergunta: Como podem ser enviados códigos de verificação de um sistema de autenticação de dois fatores?

Resposta: Os códigos de verificação de um sistema de autenticação de dois fatores podem ser enviados por email ou gerados por um aplicativo autenticador instalado no dispositivo móvel do usuário.

Pergunta: O que significa falhas de integridade de software e dados?

Resposta: Falhas de integridade de software e dados estão associadas ao processo de deploy ou disponibilização em produção, alcançando as esteiras de Integração Contínua e Entrega contínua, quando não há verificações de integridades no processo. Isso acontece quando um aplicativo depende de plugins, bibliotecas ou módulos de fontes não confiáveis, repositórios e redes de entrega de conteúdo (CDNs). Um pipeline de CI/CD inseguro pode introduzir o potencial de acesso não autorizado, código malicioso ou comprometimento do sistema.

Pergunta: Como prevenir falhas de integridade de software e dados?

Resposta: Para prevenir falhas de integridade de software e dados, deve-se usar assinaturas digitais ou mecanismos semelhantes para verificar se o software ou os dados são da fonte esperada e não foram alterados.

Pergunta: Como garantir que bibliotecas e dependências estejam consumindo repositórios confiáveis?

Resposta: Se você tiver um perfil de risco mais alto, considere hospedar um repositório interno em boas condições que seja verificado.

Pergunta: Qual ferramenta deveria ser usada para verificar se os componentes não contêm vulnerabilidades conhecidas?

Resposta: Uma ferramenta de segurança da cadeia de suprimentos de software, como OWASP Dependency Check ou OWASP CycloneDX.

Pergunta: Qual é a importância de um processo de revisão para alterações de código e configuração?

Resposta: Um processo de revisão minimiza a chance de que código ou configuração mal-intencionados possam ser introduzidos no pipeline de software.

Pergunta: Quais são os requisitos para um pipeline de CI/CD seguro?

Resposta: O pipeline de CI/CD deve ter segregação, configuração e controle de acesso adequados para garantir a integridade do código que flui pelos processos de compilação e implantação.

Pergunta: Por que não devemos enviar dados serializados não assinados ou não criptografados para clientes não confiáveis sem alguma forma de verificação de integridade?

Resposta: A verificação de integridade ou assinatura digital é necessária para detectar adulteração ou repetição dos dados serializados.

Pergunta: O que é falha de registro e monitoramento de segurança?

Resposta: Falha de registro e monitoramento de segurança é a falta de detecção, escalação e resposta às violações ativas. Sem registro e monitoramento, as violações não podem ser detectadas, tratadas e conhecidas de forma eficiente.

Pergunta: Quais são as vulnerabilidades comuns no registro e monitoramento de segurança?

Resposta: Eventos auditáveis não são registrados, avisos e erros geram mensagens de log inexistentes, inadequadas ou pouco claras, os logs de aplicativos e APIs não são monitorados quanto a atividades suspeitas, os logs são armazenados apenas localmente, limites de alerta apropriados e processos de escalação de resposta não estão em vigor ou não são eficazes, e testes de penetração e varreduras por ferramentas de teste de segurança de aplicativos dinâmicos (DAST) não acionam alertas.

Pergunta: Como garantir que todas as falhas de login, controle de acesso e validação de entrada do lado do servidor possam ser registradas?

Resposta: Devem ser registradas com contexto de usuário suficiente para identificar contas suspeitas ou maliciosas e mantidas por tempo suficiente para permitir análises forenses atrasadas.

Pergunta: Como os logs devem ser gerados?

Resposta: Os logs devem ser gerados em um formato que as soluções de gerenciamento de log possam consumir facilmente.

Pergunta: Como se deve codificar os dados de log para evitar injeções ou ataques nos sistemas de log ou monitoramento?

Resposta: Os dados de log devem ser codificados corretamente para evitar injeções ou ataques nos sistemas de log ou monitoramento.

Pergunta: Que precaução deve ser tomada para transações de alto valor?

Resposta: As transações de alto valor devem ter uma trilha de auditoria com controles de integridade para evitar adulteração ou exclusão, como tabelas de banco de dados somente anexadas ou similares.

Pergunta: Qual a responsabilidade das equipes de DevSecOps?

Resposta: As equipes de DevSecOps devem estabelecer monitoramento e alertas eficazes para que atividades suspeitas sejam detectadas e respondidas rapidamente.

Pergunta: Qual plano de resposta e recuperação de incidentes deve ser estabelecido ou adotado?

Resposta: Deve-se estabelecer ou adotar um plano de resposta e recuperação de incidentes, como o Instituto Nacional de Padrões e Tecnologia (NIST) 800-61r2 ou posterior.

Pergunta: O que é a Falsificação de solicitação do lado do servidor (SSRF)?

Resposta: SSRF é um ataque onde o servidor WEB envolvido na condição de vítima, nada mais é do que um vetor para um outro ataque. São criadas requisições no lado do servidor para URL's ou serviços de terceiros indevidamente. Um dos destaques dessa categoria é a possibilidade de conseguir burlar firewalls internos na rede.

Pergunta: Como prevenir o SSRF na camada de rede?

Resposta: Para prevenir o SSRF na camada de rede, segmente a funcionalidade de acesso remoto a recursos em redes separadas, aplique políticas de firewall 'negar por padrão' ou regras de controle de acesso à rede para bloquear todo o tráfego de intranet, exceto o essencial. Estabeleça uma propriedade e um ciclo de vida para regras de firewall baseadas em aplicativos. Registre todos os fluxos de rede aceitos e bloqueados em firewalls.

Pergunta: Como prevenir o SSRF na camada de aplicação?

Resposta: Para prevenir o SSRF na camada de aplicação, higienize e valide todos os dados de entrada fornecidos pelo cliente, aplique o esquema de URL, a porta e o destino com uma lista de permissões positiva, não envie respostas brutas aos clientes e desabilite redirecionamentos HTTP.

Pergunta: O que é importante para evitar ataques como religação de DNS e condições de corrida 'tempo de verificação, tempo de uso' (TOCTOU)?

Resposta: É importante estar ciente da consistência do URL.

Pergunta: Por que não se deve reduzir o SSRF por meio do uso de uma lista de negação ou expressão regular?

Resposta: Os invasores têm listas de carga útil, ferramentas e habilidades para contornar as listas de negação.

Pergunta: O que não deve ser implantado em sistemas frontais em termos de segurança?

Resposta: Não se deve implantar outros serviços relevantes de segurança em sistemas frontais, como o OpenID. É importante controlar o tráfego local nesses sistemas.

Pergunta: Como proteger frontends com grupos de usuários dedicados e gerenciáveis?

Resposta: Use criptografia de rede, como VPNs, em sistemas independentes para considerar necessidades de proteção muito altas.

Pergunta: O que um invasor pode fazer se explorar a vulnerabilidade SSRF?

Resposta: Se um invasor explorar a vulnerabilidade SSRF, ele poderá realizar requisições não autorizadas a outras localidades por meio do lado servidor dessa aplicação web vulnerável.

Pergunta: O que ocorre com as vulnerabilidades da família Server-Side Request Forgery (SSRF)?

Resposta: As vulnerabilidades da família Server-Side Request Forgery (SSRF) ocorrem sempre que uma aplicação busca um recurso remoto, sem validar a URL fornecida pelo usuário.