|  |
| --- |
| **Prova de Segurança de Redes** |
| |  |  | | --- | --- | |  | **Questão** | | Resposta Correta: b | | | **1)** | **Assinale a afirmativa correta - Entende-se trinoo como sendo:** |  | |  | |  | |  | **JUSTIFICATIVA:  Conforme o material do módulo: Ataques - trinoo é um ataque DDoS para o protocolo UDP. Ele utiliza um reduzido número de servidores masters e grande número de daemons, instruídos para atacar certos IP´s e não utiliza IP Spoofing e o tráfego com os servidores masters requerem senhas.** |  | |  | |  | | **a)** | O estudo dos princípios e das técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, a menos que seja conhecida uma "chave secreta", o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade. |  | |  | |  | | **b)** | Um ataque DDoS para o protocolo UDP. Ele utiliza um reduzido número de servidores masters e grande número de daemons, instruídos para atacar certos IP´s e não utiliza IP Spoofing e o tráfego com os servidores masters requerem senhas. |  | |  | |  | | **c)** | Um ataque onde o hacker envia mais dados do que o tamanho do buffer, preenchendo o espaço da pilha, com intuito de que os dados sejam perdidos devido a falha na camada de aplicação, sendo possível a execução de comandos que podem dar permissão, até mesmo de administradores do sistema, reescrevendo o código na pilha do sistema. |  | |  | |  | | **d)** | Um ataque DDoS para o protocolo TCP e implementa o IP Spoofing, TCP SYN Flooding e ICMP. O processo de ataque é acionado quando o hacker dá especificação aos masters para iniciar o ataque através dos daemons. |  | |  | |  | |  | |  | | Resposta Correta: c | |  | | **2)** | **Assinale a afirmativa correta - Entende-se Load Detecction como sendo:** |  | |  | |  | |  | **JUSTIFICATIVA:  Conforme o material do módulo: Load Detecction é a detecção a partir do comportamento de um equipamento quanto a tempo de resposta, levando em consideração que o equipamento onde está sendo executado sniffer possui um tempo de resposta maior do que o normal. Em geral, é enviado um pacote teste para realizar a análise estatística.** |  | |  | |  | | **a)** | A característica de alguns sniffers de realizar o DNS Reverso onde um tráfego com endereço falso é colocado na rede e, o sniffer captura o trafego e tenta resolver o nome através do DNS. |  | |  | |  | | **b)** | Uma maneira de o hacker aproveitar a vulnerabilidade do endereço IP em equipamentos que não estão implementados o TCP/IP corretamente. |  | |  | |  | | **c)** | A detecção a partir do comportamento de um equipamento quanto a tempo de resposta, levando em consideração que o equipamento onde está sendo executado sniffer possui um tempo de resposta maior do que o normal. Em geral, é enviado um pacote teste para realizar a análise estatística. |  | |  | |  | | **d)** | A detecção a partir do comportamento de um equipamento quanto vulnerabilidade, levando em consideração que o equipamento onde está sendo executado sniffer possui um tempo de resposta maior do que o usual. |  | |  | |  | |  | |  | | Resposta Correta: c | |  | | **3)** | **Assinale a afirmativa correta - São Tipos de IDS:** |  | |  | |  | |  | **JUSTIFICATIVA:  Sistemas baseados em estação ou Host-Based Intrusion Detection (HIDS); Sistemas baseados em redes ou Network-Based Intrusion Detection (NIDS) e; Hybrid IDS ou IDS híbrido.** |  | |  | |  | | **a)** | Dumpster diving - Poison defacement - Spoofing null. |  | |  | |  | | **b)** | PPoE, POP e Dumpster diving. |  | |  | |  | | **c)** | Sistemas baseados em estação ou Host-Based Intrusion Detection (HIDS); Sistemas baseados em redes ou Network-Based Intrusion Detection (NIDS) e; Hybrid IDS ou IDS híbrido. |  | |  | |  | | **d)** | Web defacement - Poison null - Upload Bombing. |  | |  | |  | |  | |  | | Resposta Correta: d | |  | | **4)** | **Assinale a afirmativa correta - No universo de sistemas criptográficos, um método é seguro se atender a dois quesitos, que são:** |  | |  | |  | |  | **JUSTIFICATIVA:  A chave deve ser um segredo difícil de descobrir, mesmo com tentativas exaustivas de processamento e quanto mais testado pelos cientistas e conhecido for o algoritmo, maior a probabilidade da sua estabilidade quanto à falhas de segurança.** |  | |  | |  | | **a)** | Endereço de IP do cliente e Porta de TCP do servidor. |  | |  | |  | | **b)** | Ter chave pública e privada. |  | |  | |  | | **c)** | Permitir a assinatura e certificação digital. |  | |  | |  | | **d)** | A chave deve ser um segredo difícil de descobrir, mesmo com tentativas exaustivas de processamento e quanto mais testado pelos cientistas e conhecido for o algoritmo, maior a probabilidade da sua estabilidade quanto à falhas de segurança. |  | |  | |  | |  | |  | | Resposta Correta: b | |  | | **5)** | **Assinale a afirmativa correta - Ameaças lógicas são aquelas que:** |  | |  | |  | |  | **JUSTIFICATIVA:  As ameaças lógicas são aquelas que ocorrem quando acontece uma modificação da capacidade funcional devido a dolo, acidente ou erro de recursos.** |  | |  | |  | | **a)** | As ameaças lógicas são aquelas que os recursos materiais utilizados no ambiente de informação estão expostos, colocando em risco a integridade operacional da organização. |  | |  | |  | | **b)** | As ameaças lógicas são aquelas que ocorrem quando acontece uma modificação da capacidade funcional devido a dolo, acidente ou erro de recursos. |  | |  | |  | | **c)** | As ameaças lógicas ocorrem quando acontece uma desestabilização de recursos humanos, modificando a capacidade funcional da organização. |  | |  | |  | | **d)** | As ameaças lógicas ocorrem quando intencionalmente ou acidentalmente alguém consegue acesso a um recurso que não tem autorização de possuir. |  | |  | |  | |  | |  | | Resposta Correta: c | |  | | **6)** | **Como são chamados os programas que permitem a um atacante roubar sua senha e assim utilizar a sua conta como se fosse você?** |  | |  | |  | |  | **JUSTIFICATIVA:  Sniffers.** |  | |  | |  | | **a)** | Log file. |  | |  | |  | | **b)** | Load Detection. |  | |  | |  | | **c)** | Sniffers. |  | |  | |  | | **d)** | Telnet. |  | |  | |  | |  | |  | | Resposta Correta: b | |  | | **7)** | **Assinale a afirmativa correta - Pode-se dizer da Internet que:** |  | |  | |  | |  | **JUSTIFICATIVA:  É uma rede que não nasceu pretendendo ser a grande rede mundial.** |  | |  | |  | | **a)** | É uma rede que nasceu pretendendo ser a grande rede mundial. |  | |  | |  | | **b)** | É uma rede que não nasceu pretendendo ser a grande rede mundial. |  | |  | |  | | **c)** | Existem poucas vulnerabilidades de segurança, porém já resolvidas. |  | |  | |  | | **d)** | Existem muitas vulnerabilidades de segurança, porém já resolvidas. |  | |  | |  | |  | |  | | Resposta Correta: d | |  | | **8)** | **Quais dos itens abaixo podem ser considerados como ameaças físicas?  1.Falha de energia. 2.Temperatura do equipamento. 3.Catástrofes. 4.Falha de equipamentos.** |  | |  | |  | |  | **JUSTIFICATIVA:  1.Falha de energia 2.Temperatura do equipamento 3.Catástrofes 4.Falha de equipamentos.** |  | |  | |  | | **a)** | Somente 1 e 2 são ameaças físicas. |  | |  | |  | | **b)** | Somente 2 e 3 são ameaças físicas. |  | |  | |  | | **c)** | Somente 3 e 4 são ameaças físicas. |  | |  | |  | | **d)** | Todos os itens são ameaças físicas. |  | |  | |  | |  | |  | | Resposta Correta: c | |  | | **9)** | **Os atacantes que realizam ataques a um alvo direcionado, escolhido cuidadosamente por questões religiosas, políticas ou comerciais, derrubando a comunicação entre a Internet e a empresa, principalmente com ataques DoS (Denial of Service) são chamados de:** |  | |  | |  | |  | **JUSTIFICATIVA:  Opção correta: Cyberterrorista.** |  | |  | |  | | **a)** | Coders. |  | |  | |  | | **b)** | Cyberpunks. |  | |  | |  | | **c)** | Cyberterroristas. |  | |  | |  | | **d)** | Phreakers. |  | |  | |  | |  | |  | | Resposta Correta: c | |  | | **10)** | **Assinale a afirmativa correta - Entende-se conhecimento como sendo:** |  | |  | |  | |  | **JUSTIFICATIVA:  Um conjunto de informações, dados pessoais, comerciais e religiosos de alguém, por exemplo, podemos traçar um melhor perfil da pessoa e dependendo deste conjunto de informações posso atuar de diferentes formas. Este agir diferente agrega valor ao ser humano e a organização, podendo trazer vantagem competitiva.** |  | |  | |  | | **a)** | A associação do nome a uma pessoa específica, com sua cor de olhos e pele, data de nascimento, temos uma informação, pois os dados começam a ter sentido. |  | |  | |  | | **b)** | A característica qualquer de um objeto, como um nome, data de nascimento de alguém ou a cor dos olhos de uma pessoa. Em informática, é uma sequência qualquer de bits armazenados. |  | |  | |  | | **c)** | Um conjunto de informações, dados pessoais, comerciais e religiosos de alguém, por exemplo, podemos traçar um melhor perfil da pessoa e dependendo deste conjunto de informações posso atuar de diferentes formas. Este agir diferente agrega valor ao ser humano e a organização, podendo trazer vantagem competitiva. |  | |  | |  | | **d)** | Um Monitoramento Off-Line, Operação Preemptiva, Permitir o gerenciamento inativo da rede, Detectar, registrar e informar à estação gerente condições de gerenciamento contínuo de segmentos de redes. |  | |  | |  | |  | |  | | Resposta Correta: a | |  | | **11)** | **Quando adota-se um Plano como forma de amenizar os riscos de TI, ou até mesmo de reduzí-los a um nível mínimo, estamos falando especificamente de:** |  | |  | |  | |  | **JUSTIFICATIVA:  Plano de Contingência.** |  | |  | |  | | **a)** | Plano de Contingência. |  | |  | |  | | **b)** | Plano de Segurança. |  | |  | |  | | **c)** | Plano de Seguros. |  | |  | |  | | **d)** | Plano Diretor de Informática. |  | |  | |  | |  | |  | | Resposta Correta: b | |  | | **12)** | **Assinale a afirmativa correta - Entende-se Sniffers como sendo:** |  | |  | |  | |  | **JUSTIFICATIVA:  Conforme o material do módulo: Sniffers são aplicações passivas, não geram nada que possa ser sentido facilmente pelos usuários e/ou administradores e, geralmente, não deixam rastros.** |  | |  | |  | | **a)** | A característica de alguns hackers de realizar o DNS Reverso onde um tráfego com endereço falso é colocado na rede e, o sniffer captura o trafego e tenta resolver o nome através do DNS. |  | |  | |  | | **b)** | São aplicações passivas, não geram nada que possa ser sentido facilmente pelos usuários e/ou administradores e, geralmente, não deixam rastros. |  | |  | |  | | **c)** | Um método ou técnica de busca de números de telefone para conexões de modem analógicos em uma combinação de determinado prefixo de área e prefixo de telefone. |  | |  | |  | | **d)** | A detecção a partir do comportamento de um equipamento quanto ao tempo de resposta, levando em consideração que o equipamento onde está sendo executado sniffer possui um tempo de resposta maior do que o normal. |  | |  | |  | |  | |  | | Resposta Correta: c | |  | | **13)** | **Assinale a afirmativa correta - Entende-se Gateway de Circuito como sendo:** |  | |  | |  | |  | **JUSTIFICATIVA:  Uma função especializada que pode ser realizada por um gateway de aplicação (uma estação segura - um computador - que permite aos usuários comunicarem-se com a Internet através de um servidor proxy, código especial que aceita ou recusa características ou comandos específicos de certas aplicações, ou mesmo aceita ou recusa a própria aplicação).** |  | |  | |  | | **a)** | Uma aplicação que permite ao administrador de redes implementar uma política de segurança muito mais restritiva do que um roteador. |  | |  | |  | | **b)** | Um tradutor de endereços de rede que visa minimizar a escassez dos endereços IP, pois o crescimento da Internet tem sido grande e, para que uma máquina tenha acesso à rede, é preciso ter um endereço IP válido. |  | |  | |  | | **c)** | Uma função especializada que pode ser realizada por um gateway de aplicação (uma estação segura - um computador - que permite aos usuários comunicarem-se com a Internet através de um servidor proxy, código especial que aceita ou recusa características ou comandos específicos de certas aplicações, ou mesmo aceita ou recusa a própria aplicação). |  | |  | |  | | **d)** | A tecnologia de Inspeção de estado multi-camada permite examinar cada pacote em todas as suas camadas do modelo OSI, desde a rede (camada 3) até a aplicação (camada 7), sem a necessidade de processar a mensagem. |  | |  | |  | |  | |  | | Resposta Correta: a | |  | | **14)** | **Assinale a afirmativa correta - Como é chamada a técnica que explora as fraquezas humanas e sociais, ao invés da tecnologia?** |  | |  | |  | |  | **JUSTIFICATIVA:  Opção correta: Engenharia Social.** |  | |  | |  | | **a)** | Engenharia Social. |  | |  | |  | | **b)** | Engenharia Sociocomputacional. |  | |  | |  | | **c)** | Engenharia Humanitária. |  | |  | |  | | **d)** | Engenharia Tecnosocial. |  | |  | |  | |  | |  | | Resposta Correta: a | |  | | **15)** | **Assinale a afirmativa correta - Entende-se Script kiddies ou Newbies como sendo:** |  | |  | |  | |  | **JUSTIFICATIVA:  Conforme Conteúdo - 4.1.3. Script kiddies ou Newbies: Os scripts kiddies ou newbies (novatos) são os principiantes, e apesar de muitos descartarem este tipo, trazem diversos problemas para as empresas. Em geral, são pessoas inexperientes, que possuem conhecimento médio sobre como navegar na Internet, e utilizam pequenos programas para tentar invadir computadores (normalmente de usuários domésticos) disponíveis na Internet. Eles não entendem o que estão fazendo, nem o que significa o programa. São frequentadores de salas de chat, onde procuram trocar informações com pessoas mais experientes. Este tipo de hacker é perigoso para as organizações que não possuem uma política de segurança adequada, por isso apresentam algumas vulnerabilidades, como atualização de patch em servidor, sistemas operacionais e banco de dados. Porém, foi devido a este tipo de hacker que as organizações começaram a perceber o valor da segurança e realizarem procedimentos que minimizem os efeitos deste tipo de ataque. Este tipo de hacker é a imensa maioria na Internet e também é o que mais causa incidente. Um fator interessante é que por os conhecimentos serem limitados dos scripts kiddies, muitas vezes servidores Windows sofrem ataques com comandos Unix.** |  | |  | |  | | **a)** | Os "atacantes" principiantes, e apesar de muitos descartarem este tipo, trazem diversos problemas para as empresas; normalmente são usuários domésticos que não entendem o que estão fazendo, nem o que significa o programa. São frequentadores de salas de chat, onde procuram trocar informações com pessoas mais experientes. |  | |  | |  | | **b)** | Script kiddies que estão começando a entender como o programa de invasão funciona, e descobrem locais onde podem trocar informações e aprender alguma técnica de hackerismo. |  | |  | |  | | **c)** | Agentes que utilizam suas habilidades para invadir sistemas e roubar informações secretas das empresas, sendo os verdadeiros terroristas da Internet, com intuito de roubar e destruir dados. |  | |  | |  | | **d)** | Hackers que se dedicam à invasão por divertimento e desafio. Possuem profundos conhecimentos e preservam sua privacidade, utilizando criptografia em suas comunicações. |  | |  | |  | |  | |  | |