|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | | |  | | --- | | **Atividade 1** | | |  | | https://ssl-w03dnn0470.websiteseguro.com/bou/campusonline/modulos/saladeaula/clean/baixo.gif | | |

|  |  |
| --- | --- |
| **1** - Assinale a afirmativa correta. Do ponto de vista da segurança, temos algumas preocupações que se destacam, são elas: | |
| **Resposta Correta. Letra A.** | |
| **A.** | Diversidade de tecnologia, Preservação das informações e Acesso de informação. |
| **B.** | Catástrofes, Supressão de serviços, Falha de energia, Falha de equipamentos, Temperatura do equipamento e Queda de comunicação. |
| **C.** | Ameaças acidentais, Ameaças intencionais e Ameaças Ativas. |
| **D.** | Ameaças Passivas, Ameaças acidentais e Ameaças intencionais. |
| **2** - Assinale a afirmativa correta. São exemplos de ameaças físicas, as seguintes: | |
| **Resposta Correta. Letra B.** | |
| **A.** | Hacker, Alteração e distribuição de dados de forma ilegal e destrutiva, Roubo de equipamentos e Pirataria de software. |
| **B.** | Catástrofes, Supressão de serviços, Falha de energia, Falha de equipamentos, Temperatura do equipamento e Queda de comunicação. |
| **C.** | Espaço físico, Layout, Temperatura e Iluminação. |
| **D.** | Destruição de informação ou de outros recursos, Modificação ou deturpação da informação, Roubo, remoção ou perda da informação ou de outros recursos, Revelação de informações e Interrupção de Serviços |
| **3** - Assinale a afirmativa correta. São exemplos de ameaças ambientais, as seguintes: | |
| **Resposta Correta. Letra D.** | |
| **A.** | Hacker, Alteração e distribuição de dados de forma ilegal e destrutiva, Roubo de equipamentos e Pirataria de software. |
| **B.** | Catástrofes, Supressão de serviços, Falha de energia, Falha de equipamentos, Temperatura do equipamento e Queda de comunicação. |
| **C.** | Espaço físico, Layout, Temperatura e Iluminação. |
| **D.** | Destruição de informação ou de outros recursos, Modificação ou deturpação da informação, Roubo, remoção ou perda da informação ou de outros recursos, Revelação de informações e Interrupção de Serviços |
| **4** - Assinale a afirmativa correta. São exemplos de ameaças lógicas, as seguintes: | |
| **Resposta Correta. Letra A.** | |
| **A.** | Hacker, Alteração e distribuição de dados de forma ilegal e destrutiva, Roubo de equipamentos e Pirataria de software. |
| **B.** | Catástrofes, Supressão de serviços, Falha de energia, Falha de equipamentos, Temperatura do equipamento e Queda de comunicação. |
| **C.** | Espaço físico, Layout, Temperatura e Iluminação. |
| **D.** | Destruição de informação ou de outros recursos, Modificação ou deturpação da informação, Roubo, remoção ou perda da informação ou de outros recursos, Revelação de informações e Interrupção de Serviços |
| **5** - Assinale a afirmativa correta. Entende-se por Full Fledged ou Crackers, os atacantes que: | |
| **Resposta Correta. Letra C.** | |
| **A.** | são hackers que se dedicam à invasão por divertimento e desafio. Possuem profundos conhecimentos e preservam sua privacidade, utilizando criptografia em suas comunicações. Eles acreditam que o governo tenta captar as informações das pessoas na Internet, tornando-se um grande inimigo. São os mais extremistas que acreditam e divulgam as teorias de conspiração que, muitas vezes, encontramos na Web. |
| **B.** | são 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. Gostam de falar em salas de chat que conseguem invadir sistemas, querendo se apresentar a Internet. Às vezes, em chat fazem "flood" (ou inundação de informações). Felizmente, para cada grupo de Lammers que aparecem hoje na Internet, somente uns poucos conseguem chegar a se tornarem hackers propriamente ditos. |
| **C.** | 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. Não medem conseqüências, contanto que consigam o que querem. Não são de confiança e costumam ser desprezados pelos próprios hackers. É comum vender as informações para a própria vitima, ameaçando a divulgação do roubo, no caso da empresa não negociar. Este ato é chamado de blackmail. |
| **D.** | 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 freqüentadores de salas de chat, onde procuram trocar informações com pessoas mais experientes. |
| **6** - Assinale a afirmativa correta. Entende-se por Lammers, os atacantes que: | |
| **Resposta Correta. Letra B.** | |
| **A.** | são hackers que se dedicam à invasão por divertimento e desafio. Possuem profundos conhecimentos e preservam sua privacidade, utilizando criptografia em suas comunicações. Eles acreditam que o governo tenta captar as informações das pessoas na Internet, tornando-se um grande inimigo. São os mais extremistas que acreditam e divulgam as teorias de conspiração que, muitas vezes, encontramos na Web. |
| **B.** | são 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. Gostam de falar em salas de chat que conseguem invadir sistemas, querendo se apresentar a Internet. Às vezes, em chat fazem "flood" (ou inundação de informações). Felizmente, para cada grupo de Lammers que aparecem hoje na Internet, somente uns poucos conseguem chegar a se tornarem hackers propriamente ditos. |
| **C.** | 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. Não medem conseqüências, contanto que consigam o que querem. Não são de confiança e costumam ser desprezados pelos próprios hackers. É comum vender as informações para a própria vitima, ameaçando a divulgação do roubo, no caso da empresa não negociar. Este ato é chamado de blackmail. |
| **D.** | Em geral, 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 freqüentadores de salas de chat, onde procuram trocar informações com pessoas mais experientes. |
| **7** - Assinale a afirmativa correta. Entende-se por Script kiddies ou Newbies, os atacantes que: | |
| **Resposta Correta. Letra D.** | |
| **A.** | são hackers que se dedicam à invasão por divertimento e desafio. Possuem profundos conhecimentos e preservam sua privacidade, utilizando criptografia em suas comunicações. Eles acreditam que o governo tenta captar as informações das pessoas na Internet, tornando-se um grande inimigo. São os mais extremistas que acreditam e divulgam as teorias de conspiração que, muitas vezes, encontramos na Web. |
| **B.** | são 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. Gostam de falar em salas de chat que conseguem invadir sistemas, querendo se apresentar a Internet. Às vezes, em chat fazem "flood" (ou inundação de informações). Felizmente, para cada grupo de Lammers que aparecem hoje na Internet, somente uns poucos conseguem chegar a se tornarem hackers propriamente ditos. |
| **C.** | 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. Não medem conseqüências, contanto que consigam o que querem. Não são de confiança e costumam ser desprezados pelos próprios hackers. É comum vender as informações para a própria vitima, ameaçando a divulgação do roubo, no caso da empresa não negociar. Este ato é chamado de blackmail. |
| **D.** | Em geral, 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 freqüentadores de salas de chat, onde procuram trocar informações com pessoas mais experientes. |
| **8** - Assinale a afirmativa correta. O sucesso do ataque de um hacker está em obter informações de um sistema sem ser percebido, podemos considerar como ataques para obtenção de informações, os seguintes: | |
| **Resposta Correta. Letra D.** | |
| **A.** | Cyberterrorista e Gray hat |
| **B.** | War Dialing e eavesdropping |
| **C.** | White hat e Gray hat |
| **D.** | Dumpster diving ou trashing e Engenharia social |
| **9** - Assinale a afirmativa correta. Entende-se por PortScanning como sendo: | |
| **Resposta Correta. Letra B.** | |
| **A.** | o responsável pela realização de diversos testes na rede, tanto em protocolos, serviços, aplicativos ou sistemas operacionais. |
| **B.** | um conjunto de ferramentas utilizadas para obter informações dos serviços executados por um equipamento, através do mapeamento de portas, pelo qual portas ativas para um endereço IP são identificadas. Cada porta é designada para uma aplicação específica (SMTP 25, SSH 22, etc). |
| **C.** | um analisador de pacotes similar ao traceroute, que obtém informações de redes remotas protegidas por Firewall, através do protocolo ICMP. |
| **D.** | uma técnica onde o endereço real do atacante é mascarado, evitando do mesmo ser encontrado. É bem utilizado em sistemas autenticadores e em ataque de negação de serviço ou Denial of Service (DoS), nos quais os pacotes de respostas não são esperados. |
| **10** - Assinale a afirmativa correta. Entende-se por Firewalking como sendo: | |
| **Resposta Correta. Letra C.** | |
| **A.** | o responsável pela realização de diversos testes na rede, tanto em protocolos, serviços, aplicativos ou sistemas operacionais. |
| **B.** | um conjunto de ferramentas utilizadas para obter informações dos serviços executados por um equipamento, através do mapeamento de portas, pelo qual portas ativas para um endereço IP são identificadas. Cada porta é designada para uma aplicação específica (SMTP 25, SSH 22, etc). |
| **C.** | um analisador de pacotes similar ao traceroute, que obtém informações de redes remotas protegidas por Firewall, através do protocolo ICMP. |
| **D.** | uma técnica onde o endereço real do atacante é mascarado, evitando do mesmo ser encontrado. É bem utilizado em sistemas autenticadores e em ataque de negação de serviço ou Denial of Service (DoS), nos quais os pacotes de respostas não são esperados. |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  | | --- | --- | --- | --- | | |  |  | | --- | --- | | |  | | --- | | **Atividade 2** | | |  | | https://ssl-w03dnn0470.websiteseguro.com/bou/campusonline/modulos/saladeaula/clean/baixo.gif | | |

|  |  |
| --- | --- |
| **1** - Assinale a afirmativa correta. Entende-se por IP Spoofing como sendo: | |
| **Resposta Correta. Letra D.** | |
| **A.** | o responsável pela realização de diversos testes na rede, tanto em protocolos, serviços, aplicativos ou sistemas operacionais. |
| **B.** | um conjunto de ferramentas utilizadas para obter informações dos serviços executados por um equipamento, através do mapeamento de portas, pelo qual portas ativas para um endereço IP são identificadas. Cada porta é designada para uma aplicação específica (SMTP 25, SSH 22, etc). |
| **C.** | um analisador de pacotes similar ao traceroute, que obtém informações de redes remotas protegidas por Firewall, através do protocolo ICMP. |
| **D.** | uma técnica onde o endereço real do atacante é mascarado, evitando do mesmo ser encontrado. É bem utilizado em sistemas autenticadores e em ataque de negação de serviço ou Denial of Service (DoS), nos quais os pacotes de respostas não são esperados. |
| **2** - Assinale a afirmativa correta. Entende-se por Smurf como sendo: | |
| **Resposta Correta. Letra D.** | |
| **A.** | uma técnica onde o endereço real do atacante é mascarado, evitando do mesmo ser encontrado. É bem utilizado em sistemas autenticadores e em ataque de negação de serviço ou Denial of Service (DoS), nos quais os pacotes de respostas não são esperados. |
| **B.** | um conjunto de ferramentas utilizadas para obter informações dos serviços executados por um equipamento, através do mapeamento de portas, pelo qual portas ativas para um endereço IP são identificadas. Cada porta é designada para uma aplicação específica (SMTP 25, SSH 22, etc). |
| **C.** | hackers que se dedicam à invasão por divertimento e desafio. Possuem profundos conhecimentos e preservam sua privacidade, utilizando criptografia em suas comunicações. Eles acreditam que o governo tenta captar as informações das pessoas na Internet, tornando-se um grande inimigo. São os mais extremistas que acreditam e divulgam as teorias de conspiração que, muitas vezes, encontramos na Web. |
| **D.** | uma técnica que gera tráfego na rede através de broadcast de ping (ICMPecho) na rede, a partir de um IP falsificado (IP Spoofing). Desta forma, a rede tenta responder à requisição e não consegue, afetando o seu desempenho. O fraggle seria a mesma técnica, porém utilizando o UDP echo. |
| **3** - Assinale a afirmativa correta. As medidas de segurança podem ser divididas em: | |
| **Resposta Correta. Letra A.** | |
| **A.** | Preventiva, Detectiva e Corretiva. |
| **B.** | Curtas, Médias e Longas |
| **C.** | Monitoramento, Avaliação de Riscos e Vulnerabilidade |
| **D.** | Definição de diretiva, Monitoramento e Vulnerabilidade |
| **4** - Assinale a afirmativa correta. Nas áreas de controle do ISO 17799, o Gerenciamento de Operações e Comunicações, tem como objetivos: | |
| **Resposta Correta. Letra B.** | |
| **A.** | Registro de operação; Registro de falhas; Gerenciamento de Rede; Controle da Rede; Gerenciamento de mídias removíveis. |
| **B.** | Garantir instalações para a operação correta e segura do processamento de informações; Minimizar o risco de falhas dos sistemas; Proteger a integridade do software e/ou das informações; Manter a integridade e disponibilidade do processamento de informações e comunicações; dentre outras. |
| **C.** | Segurança corporativa aprimorada; Planejamento e Gerenciamento de segurança mais efetivo; Parcerias e e-commerce mais seguros; Confiança aprimorada do cliente; Auditorias de segurança mais seguras e precisas; Redução de responsabilidades legais; dentre outras. |
| **D.** | Processo de gestão da continuidade do negócio; Análise do Impacto; Documentando e Implementando planos de continuidade; Estrutura do plano; Testes, manutenção dos planos de continuidade. |
| **5** - Assinale a afirmativa correta. Os candidatos potenciais devem ser devidamente analisados, especialmente para trabalhos sensíveis, que todos os funcionários e prestadores de serviço, usuários das instalações de processamento da informação, assinem um acordo de sigilo. Este acordo deve constar: | |
| **Resposta Correta. Letra C.** | |
| **A.** | Registro de operação; Registro de falhas; Gerenciamento de Rede; Controle da Rede; Gerenciamento de mídias removíveis. |
| **B.** | Garantir instalações para a operação correta e segura do processamento de informações; Minimizar o risco de falhas dos sistemas; Proteger a integridade do software e/ou das informações; Manter a integridade e disponibilidade do processamento de informações e comunicações; dentre outras. |
| **C.** | Segurança nas responsabilidades do trabalho; Seleção e política de pessoal; Acordos de confidencialidade; Termos e condições de trabalho; Treinamento do usuário; Educação e treinamento em segurança da informação; Respondendo aos incidentes de segurança e ao mau funcionamento; Notificação dos incidentes de segurança; Processo disciplinar; dentre outras. |
| **D.** | Segurança corporativa aprimorada; Planejamento e Gerenciamento de segurança mais efetivo; Parcerias e e-commerce mais seguros; Confiança aprimorada do cliente; Auditorias de segurança mais seguras e precisas; Redução de responsabilidades legais; dentre outras. |
| **6** - Assinale a afirmativa correta. As principais vantagens na utilização de Filtros de Pacotes por estado são: | |
| **Resposta Correta. Letra C.** | |
| **A.** | Segurança corporativa aprimorada; Planejamento e Gerenciamento de segurança mais efetivo; Parcerias e e-commerce mais seguros; Confiança aprimorada do cliente; Auditorias de segurança mais seguras e precisas; Redução de responsabilidades legais; dentre outras. |
| **B.** | Garantir instalações para a operação correta e segura do processamento de informações; Minimizar o risco de falhas dos sistemas; Proteger a integridade do software e/ou das informações; Manter a integridade e disponibilidade do processamento de informações e comunicações; dentre outras. |
| **C.** | Bom desempenho, por trabalhar no nível de transporte e rede; Log de conexões abertas ou não; Abertura temporária da rede; Baixo overhead e alto throughtput e Compatibilidade com quase todos os tipos de protocolos. |
| **D.** | Permite conexão direta para máquinas internas da rede externa; A autenticação é somente realizada via gateway de aplicação (application gateway); Apesar de divulgarem que o filtro de pacotes por estado atua na camada de aplicação é necessário, na maioria dos Firewalls, outros softwares para realizar esta atividade. |
| **7** - Assinale a afirmativa correta. As principais desvantagens na utilização de Filtros de Pacotes por estado são: | |
| **Resposta Correta. Letra D.** | |
| **A.** | Segurança corporativa aprimorada; Planejamento e Gerenciamento de segurança mais efetivo; Parcerias e e-commerce mais seguros; Confiança aprimorada do cliente; Auditorias de segurança mais seguras e precisas; Redução de responsabilidades legais; dentre outras. |
| **B.** | Garantir instalações para a operação correta e segura do processamento de informações; Minimizar o risco de falhas dos sistemas; Proteger a integridade do software e/ou das informações; Manter a integridade e disponibilidade do processamento de informações e comunicações; dentre outras. |
| **C.** | Bom desempenho, por trabalhar no nível de transporte e rede; Log de conexões abertas ou não; Abertura temporária da rede; Baixo overhead e alto throughtput e Compatibilidade com quase todos os tipos de protocolos. |
| **D.** | Permite conexão direta para máquinas internas da rede externa; A autenticação é somente realizada via gateway de aplicação (application gateway); Apesar de divulgarem que o filtro de pacotes por estado atua na camada de aplicação é necessário, na maioria dos Firewalls, outros softwares para realizar esta atividade. |
| **8** - Assinale a afirmativa correta. Entende-se por Stateful Multi-Layer Inspection Firewalls, como sendo: | |
| **Resposta Correta. Letra A.** | |
| **A.** | a tecnologia de Inspeção de estado multi-camada, considerada a terceira geração dos Firewalls, 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. |
| **B.** | expostos a possíveis elementos hostis, que tendo ou não permissão, precisam inicialmente passar pelo Bastion Hosts antes de alcançarem a rede interna. Quando mais simples forem, mais simples será mantê-lo seguro. |
| **C.** | uma das soluções que existem para a economia de endereços IP. É 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. |
| **D.** | uma rede que fica entre a rede interna e externa, caso algum equipamento bastion host seja atacado na rede DMZ, a rede interna continuará sua operacionalidade de forma intacta e segura. |
| **9** - Assinale a afirmativa correta. Entende-se por Network Address Translation, como sendo: | |
| **Resposta Correta. Letra C.** | |
| **A.** | a tecnologia de Inspeção de estado multi-camada, considerada a terceira geração dos Firewalls, 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. |
| **B.** | expostos a possíveis elementos hostis, que tendo ou não permissão, precisam inicialmente passar pelo Bastion Hosts antes de alcançarem a rede interna. Quando mais simples forem, mais simples será mantê-lo seguro. |
| **C.** | uma das soluções que existem para a economia de endereços IP. É 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. |
| **D.** | uma rede que fica entre a rede interna e externa, caso algum equipamento bastion host seja atacado na rede DMZ, a rede interna continuará sua operacionalidade de forma intacta e segura. |
| **10** - Assinale a afirmativa correta. Entende-se por Proxy, como sendo: | |
| **Resposta Correta. Letra B.** | |
| **A.** | uma rede que fica entre a rede interna e externa, caso algum equipamento bastion host seja atacado na rede DMZ, a rede interna continuará sua operacionalidade de forma intacta e segura. |
| **B.** | um tradutor de endereços de aplicações. Trabalha tanto na camada de sessão, transporte e aplicação. Seu objetivo é não permitir que estações internas se comuniquem a servidores externos sem reendereçamento, promovendo assim, uma maior segurança dentro da rede, já que externamente o endereço interno está mascarado. Funciona como um daemon e não utiliza um mecanismo único para controle do tráfego, sendo necessário um código especial para cada tipo de aplicação. Sua implementação é simples, minimizando ataque no mesmo. Por possuir um sistema de alarme, é possível registrar todo o tráfego da rede, tanto interno quanto externo |
| **C.** | a tecnologia de Inspeção de estado multi-camada, considerada a terceira geração dos Firewalls, 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. |
| **D.** | equipamentos que prestam serviços à Internet. É a sua presença pública na Internet. Imagine a recepção de um prédio, onde estranhos podem não ter permissão de subir as escadas nem utilizar os elevadores, mas podem vagar livremente pela recepção e se informarem do que necessitam. Como numa recepção de edifício, os Bastion Hosts são expostos a possíveis elementos hostis, que tendo ou não permissão, precisam inicialmente passar pelo Bastion Hosts antes de alcançarem a rede interna. Quando mais simples forem, mais simples será mantê-lo seguro. |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | | |  |  |  |  | | --- | --- | --- | --- | |  | | | | | |  | | --- | | **Atividade 3** | |  |  |  | |  | | https://ssl-w03dnn0470.websiteseguro.com/bou/campusonline/modulos/saladeaula/clean/baixo.gif | | |

|  |  |
| --- | --- |
| **1** - Assinale a afirmativa correta. Entende-se por Bastion Hosts, como sendo: | |
| **Resposta Correta. Letra D.** | |
| **A.** | uma rede que fica entre a rede interna e externa, caso algum equipamento bastion host seja atacado na rede DMZ, a rede interna continuará sua operacionalidade de forma intacta e segura. |
| **B.** | um tradutor de endereços de aplicações. Trabalha tanto na camada de sessão, transporte e aplicação. Seu objetivo é não permitir que estações internas se comuniquem a servidores externos sem reendereçamento, promovendo assim, uma maior segurança dentro da rede, já que externamente o endereço interno está mascarado. Funciona como um daemon e não utiliza um mecanismo único para controle do tráfego, sendo necessário um código especial para cada tipo de aplicação. Sua implementação é simples, minimizando ataque no mesmo. Por possuir um sistema de alarme, é possível registrar todo o tráfego da rede, tanto interno quanto externo |
| **C.** | a tecnologia de Inspeção de estado multi-camada, considerada a terceira geração dos Firewalls, 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. |
| **D.** | equipamentos que prestam serviços à Internet. É a sua presença pública na Internet. Imagine a recepção de um prédio, onde estranhos podem não ter permissão de subir as escadas nem utilizar os elevadores, mas podem vagar livremente pela recepção e se informarem do que necessitam. Como numa recepção de edifício, são expostos a possíveis elementos hostis, que tendo ou não permissão, precisam inicialmente passar por eles antes de alcançarem a rede interna. Quando mais simples forem, mais simples será mantê-lo seguro. |
| **2** - Assinale a afirmativa correta. Existem assinaturas que detectam falhas de conexões TCP em diversas portas, identificando assim scanning na rede. Este tipo de assinatura é dividido em três partes, que são: | |
| **Resposta Correta. Letra B.** | |
| **A.** | legível, ilegível e rubrica |
| **B.** | String, Portas e Cabeçalho |
| **C.** | VPN, L2TP e PPTP |
| **D.** | Estabilidade, Segurança e confiabilidade |
| **3** - Assinale a afirmativa correta. São características de chaves de criptografia simétricas: | |
| **Resposta Correta. Letra C.** | |
| **A.** | Processamento lento; Gerenciamento e distribuição de chaves de forma simples; Facilidade em estabelecer relacionamento com entidades desconhecidas e Suporta assinatura digital |
| **B.** | Processamento rápido; Gerenciamento e distribuição de chaves de forma simples; Relacionamento com entidades desconhecidas de forma não digital ou em servidores centralizadores e Suporta assinatura digital. |
| **C.** | Processamento rápido; Gerenciamento e distribuição de chaves complicadas; Relacionamento com entidades desconhecidas de forma não digital ou em servidores centralizadores e Não suporta assinatura digital. |
| **D.** | Processamento lento; Gerenciamento e distribuição de chaves complicadas; Facilidade em estabelecer relacionamento com entidades desconhecidas e Não suporta assinatura digital |
| **4** - Assinale a afirmativa correta. São características de chaves de criptografia Assimétrica: | |
| **Resposta Correta. Letra A.** | |
| **A.** | Processamento lento; Gerenciamento e distribuição de chaves de forma simples; Facilidade em estabelecer relacionamento com entidades desconhecidas e Suporta assinatura digital |
| **B.** | Processamento rápido; Gerenciamento e distribuição de chaves de forma simples; Relacionamento com entidades desconhecidas de forma não digital ou em servidores centralizadores e Suporta assinatura digital. |
| **C.** | Processamento rápido; Gerenciamento e distribuição de chaves complicadas; Relacionamento com entidades desconhecidas de forma não digital ou em servidores centralizadores e Não suporta assinatura digital. |
| **D.** | Processamento lento; Gerenciamento e distribuição de chaves complicadas; Facilidade em estabelecer relacionamento com entidades desconhecidas e Não suporta assinatura digital |
| **5** - Assinale a afirmativa correta. As Principais vantagens do uso do algoritmo DH ou DSS, são: | |
| **Resposta Correta. Letra A.** | |
| **A.** | Não possuem patentes e podem ser utilizados universalmente; ElGamal é considerado com melhor desempenho em criptografia do que o RSA e Serviços separados, garantindo a revogação de chaves sem comprometer assinaturas relacionadas. |
| **B.** | Os dados criptografados com RSA apresentam a metade do tamanho; O limite da padronização da assinatura DSS é de 1024, enquanto a RSA utiliza chaves de 2.048 ou 4.096, dependendo da implementação e Maior tempo de processamento do algoritmo DH ou DSS comparado ao RSA. |
| **C.** | Nome da organização associada; Data de emissão do certificado e Período de validade da chave. |
| **D.** | O número de série do certificado; O período de validade do certificado. e A assinatura digital da AC. |
| **6** - Assinale a afirmativa correta. As Principais desvantagens do uso do algoritmo DH ou DSS em relação ao RSA são: | |
| **Resposta Correta. Letra B.** | |
| **A.** | Não possuem patentes e podem ser utilizados universalmente; ElGamal é considerado com melhor desempenho em criptografia do que o RSA e Serviços separados, garantindo a revogação de chaves sem comprometer assinaturas relacionadas. |
| **B.** | Os dados criptografados com RSA apresentam a metade do tamanho; O limite da padronização da assinatura DSS é de 1024, enquanto a RSA utiliza chaves de 2.048 ou 4.096, dependendo da implementação e Maior tempo de processamento do algoritmo DH ou DSS comparado ao RSA. |
| **C.** | Nome da organização associada; Data de emissão do certificado e Período de validade da chave. |
| **D.** | O número de série do certificado; O período de validade do certificado. e A assinatura digital da AC. |
| **7** - Assinale a afirmativa correta. Uma forma de minimizar os efeitos negativos do uso de senha é a utilização das mesmas uma única vez, sendo trocada a cada novo acesso. Porém, o usuário não se sentirá confortável nesta situação. Mesmo desta forma, existem ataques que podem ser realizados pelos hackers, que são: | |
| **Resposta Correta. Letra D.** | |
| **A.** | Safe Message e Private Message |
| **B.** | TGS e TGT |
| **C.** | Radius e Kerberos |
| **D.** | Man-in-the-middle e Race |
| **8** - Assinale a afirmativa correta. No Protocolo Kerberos, a comunicação entre o cliente e o serviço poderá ser feita de três formas diferentes: | |
| **Resposta Correta. Letra A.** | |
| **A.** | Normal, Safe Message e Private Message |
| **B.** | RSA, TGS e TGT |
| **C.** | Ticket, Radius e Kerberos |
| **D.** | Normal, Man-in-the-middle e Race |
| **9** - Assinale a afirmativa correta. Entende-se por Single Sign-On (SSO) como sendo | |
| **Resposta Correta. Letra B.** | |
| **A.** | as habilidades para invadir sistemas e roubar informações secretas das empresas, sendo os verdadeiros terroristas da Internet, com intuito de roubar e destruir dados. Não medem conseqüências, contanto que consigam o que querem. Não são de confiança e costumam ser desprezados pelos próprios hackers. É comum vender as informações para a própria vitima, ameaçando a divulgação do roubo, no caso da empresa não negociar. Este ato é chamado de blackmail. |
| **B.** | É um método de identificação e autorização de usuário que utiliza autenticação única e transparente, para diversos sistemas corporativos, facilitando a administração de senhas ? tanto por parte dos usuários quanto por parte dos administradores de sistema. Esta solução pode utilizar qualquer metodologia de autenticação, desde certificados digitais, até tokens, smartcards ou senha. |
| **C.** | Os protocolos Radius e Kerberos |
| **D.** | Catástrofes, Supressão de serviços, Falha de energia, Falha de equipamentos, Temperatura do equipamento e Queda de comunicação. |
| **10** - Assinale a afirmativa correta. Os protocolos de autenticação que são geralmente utilizados na autenticação de acesso remoto as organizações são: | |
| **Resposta Correta. Letra C.** | |
| **A.** | Safe Message e Private Message |
| **B.** | TGS e TGT |
| **C.** | Radius e Kerberos |
| **D.** | Man-in-the-middle e Race |

|  |  |
| --- | --- |
| Veja abaixo a correção da prova: | |
| **1 -** Assinale a afirmativa correta - São Tipos de IDS: | |
| **A)** | PPoE, POP e Dumpster diving. |
| **B)** | Dumpster diving - Poison defacement - Spoofing null. |
| **C)** | Web defacement - Poison null - Upload Bombing. |
| **D)** | Resposta Correta 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. |
| **2 -** Assinale a afirmativa correta - Conhecendo um pouco os atacantes, Gray hat são aquelas que: | |
| **A)** | Resposta Correta são os black hats que fazem papel de white hats, exercendo função na área de segurança, tendo conhecimento em hacking. |
| **B)** | são aqueles 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). |
| **C)** | são "hackers do bem", "hackers éticos", samurais ou sneakers, são os que utilizam seus conhecimentos para descobrir vulnerabilidades nos sites, aplicando as correções necessárias. Em geral, trabalham de maneira legal dentro da organização, exercendo a função de assegurar a segurança organizacional. |
| **D)** | são os hackers que compartilham seus conhecimentos escrevendo livros, ministrando palestras e seminários sobre sua experiência tornando uma atividade lucrativa. |
| **3 -** Assinale a afirmativa correta - Entende-se por Gateway de circuito, como sendo: | |
| **A)** | Resposta Correta 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). |
| **B)** | Uma aplicação permite ao administrador de redes implementar uma política de segurança muito mais restritiva do que um roteador. |
| **C)** | 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. |
| **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. |
| **4 -** Assinale a afirmativa correta - As características de confidencialidade, integridade, autenticação, certificação e não-repudio; estão presentes em protocolos com: | |
| **A)** | Resposta Correta Secure Shell (SSH) e IP Security (IPSec). |
| **B)** | FTP e http. |
| **C)** | Vírus e Worm. |
| **D)** | Smurf e fraggle. |
| **5 -** Assinale a afirmativa correta - Entende-se por Load Detecction como sendo: | |
| **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 do hacker aproveitar a vulnerabilidade do endereço IP em equipamentos que não estão implementados o TCP/IP corretamente. |
| **C)** | Resposta Correta 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 analise 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. |
| **6 -** Assinale a afirmativa correta - São exemplos de ameaças lógicas: | |
| **A)** | Resposta Correta Hackers, alteração e distribuição de dados de forma ilegal, vírus e pirataria de software. |
| **B)** | Ameaças jurídicas, Ameaças funcionais e Ameaça moral. |
| **C)** | Catástrofes, Supressão de serviços e Falha de energia. |
| **D)** | Falha de equipamentos e Queda de comunicação por acidente natural ou erro operacional. |
| **7 -** Assinale a afirmativa correta - O que se entende por Syn Flood? | |
| **A)** | Rede que possui memória associativa com uma pequena quantidade de aplicações práticas e habilidade de fazer mapeamentos entre dados. |
| **B)** | Análise de características demográficas para marketing para lançamento de novos produtos e utilizada no processamento de reconhecimento, análise e classificação de dados. |
| **C)** | Rede competitiva desenhada para funcionar como tabela de consulta e pode determinar a rotação angular de um objeto. |
| **D)** | Resposta Correta É tipo de ataque que se dá com o envio de conexões em quantidade capaz de fazer com que o servidor não consiga responder. A pilha da memória sofre overflow, desprezando as requisições legítimas dos usuários. |
| **8 -** Assinale a afirmativa correta - Entende-se por Engenharia social como sendo: | |
| **A)** | uma ferramenta que explora a fragmentação de pacotes IP, auxiliando os administradores para a defesa de ataque por fragmentação de pacotes. |
| **B)** | brechas em softwares de uso constante - como navegadores, clientes de email e programas de mensagens instantâneas - que funcionam como portas para invasões. |
| **C)** | Resposta Correta a técnica que explora as fraquezas humanas e sociais, ao invés da tecnologia. Ela possui como objetivo a persuasão de pessoas, através da enganação, empregando falsas identidades, a fim de obter informações como senhas, ou dados que sejam importantes para invadir o sistema. |
| **D)** | uma técnica que gera tráfego na rede através de broadcast de ping (ICMPecho) na rede, a partir de um IP falsificado (IP Spoofing). Desta maneira, a rede tenta responder à requisição e não consegue, afetando a sua performance. |
| **9 -** Assinale a afirmativa correta - Entende-se por Medida Detectiva como sendo: | |
| **A)** | Esforços como procedimentos, software, configurações, hardware e técnicas empregadas para atenuar as vulnerabilidades com intuito de reduzir a probabilidade de ocorrência da ação de ameaças e, por conseguinte, os incidentes de segurança. |
| **B)** | Tipo de estratégia possui como foco a prevenção da ocorrência de incidentes de segurança. Todos os esforços estão baseados na precaução e, por esta razão, o conjunto de ferramentas e/ ou treinamentos estão voltados para esta necessidade. |
| **C)** | Resposta Correta A estratégia utilizada quando se tem a necessidade de obter auditabilidade, monitoramento e detecção em tempo real de tentativas de invasão. |
| **D)** | Ações corretivas, na maioria das vezes ocorrem de forma emergencial, sem planejamento e dependendo do procedimento e das ferramentas adotados podem ser mais nocivas para o ambiente de TI do que benéficas. |
| **10 -** Assinale a afirmativa correta - Conhecendo um pouco os atacantes, Cyberterrorista são aquelas que: | |
| **A)** | são os black hats que fazem papel de white hats, exercendo função na área de segurança, tendo conhecimento em hacking. |
| **B)** | Resposta Correta são aqueles 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). |
| **C)** | são "hackers do bem", "hackers éticos", samurais ou sneakers, são os que utilizam seus conhecimentos para descobrir vulnerabilidades nos sites, aplicando as correções necessárias. Em geral, trabalham de maneira legal dentro da organização, exercendo a função de assegurar a segurança organizacional. |
| **D)** | são os hackers que compartilham seus conhecimentos escrevendo livros, ministrando palestras e seminários sobre sua experiência tornando uma atividade lucrativa. |
|  | |