

Coloque V (verdadeiro) ou F (falso), nas afirmativas abaixo, assinalando, a seguir, a opção correta.

( ) Um ataque de negação de serviço (*Denial of Service* - DoS) é uma tentativa de impedir que usuários legítimos de um serviço usem esse serviço.

( ) Em um ataque de DDoS *Refletor*, as máquinas escravas criam pacotes que solicitam uma resposta que contenha o IP de máquinas não infectadas como IP de origem no cabeçalho do pacote. As máquinas escravas enviam tais pacotes à máquina alvo, que responde com pacotes dirigidos para máquinas não infectadas, conhecidas como refletoras.

( ) Em um ataque de negação de serviço distribuído (*Distributes Denial of Service* - DDoS), realizado por meio da inundação de pacotes SYN (*SYN flooding attack*), as máquinas escravas ou zumbis enviam para o alvo selecionado pacotes SYN do TCP/IP, com informações de endereço IP de retorno falso; isso causa lentidão e até o travamento da máquina alvo pois a mesma fica esperando para completar as falsas conexões.

( ) O rastreamento e identificação da origem do ataque é uma linha de defesa contra ataques DDoS, que é facilmente alcançável e sempre eficaz para anular os efeitos do DDoS.

Escolha uma opção:

- ☒ a. (V) (F) (V) (F)
- ☐ b. (V) (F) (F) (V)
- ☐ c. (F) (V) (F) (V)
- ☐ d. (F) (F) (V) (V)
- ☐ e. (V) (V) (F) (F)



Parabéns

Um provedor de serviços de segurança de redes enumerou três componentes de rede essenciais para a garantia da segurança dos dados corporativos: *firewall* de rede; sistemas de prevenção e detecção de intrusão; *gateways* antivírus.

Acerca desses componentes de rede, assinale a opção **CORRETA**.

(Questão baseada no ENADE)

- ☐ a. Um *firewall* de camada de rede ou por filtragem de pacotes permite uma filtragem mais detalhada dos dados do que um *firewall* de camada de aplicação ao custo de um desempenho pior.
- ☐ b. Os *gateways* antivírus trabalham no nível da camada de rede e verificam o fluxo de dados em busca de assinaturas de vírus conhecidas.
- ☐ c. O sistema de detecção de intrusão, IDS, é capaz de identificar ataques iniciados dentro da rede protegida e agir proativamente para neutralizar a ameaça.
- ☒ d. Os sistemas de prevenção de intrusão, IPS, são vistos como uma extensão do *firewall* e são capazes de detectar anomalias de tráfego ou conteúdo malicioso.
- ☐ e. O firewall de rede deve ser configurado para detectar transferência de informação por meio de um canal camuflado (*covert channel*) baseado em túneis.



Indique qual é o tipo de problema de segurança em cada descrição a seguir.

Quando um aplicativo mal-intencionado acessa a memória alocada para outros processos.

Buffer overflow



Quando uma transição legítima e autenticada é reenviada por um atacante.

Ataque de repetição (replay)



Quando os controles e/ou requisitos de segurança não são ou são pouco verificados.

Carência de testes de segurança




Sua resposta está correta.

A resposta correta é: Quando um aplicativo mal-intencionado acessa a memória alocada para outros processos. → Buffer overflow, Quando uma transição legítima e autenticada é reenviada por um atacante. → Ataque de repetição (replay), Quando os controles e/ou requisitos de segurança não são ou são pouco verificados. → Carência de testes de segurança.

Considere que tenha ocorrido o vazamento de imagens íntimas, por meio de aplicativo de comunicação instantânea de celular, disponibilizado por provedor de aplicações, sem autorização das pessoas que aparecem nas imagens.

Nesse contexto, de acordo com a Lei n. 12.965/2014, conhecida popularmente como Marco Civil da Internet, o provedor de aplicações poderá:

(Questão baseada no ENADE)

- ☐ a. ser declarado inocente, caso fique provado que as imagens foram disponibilizadas à pedido da vítima.
- ☐ b. encerrar seu contrato com a vítima devido à falha de segurança ocorrida.
- ☒ c. ser responsabilizado se deixar de remover as imagens disponibilizadas, dentro de seus limites técnicos. 
- ☐ d. mover uma ação contra a vítima, pelo uso indevido de seus serviços, por ela ter disponibilizado imagens íntimas na rede.
- ☐ e. tornar indisponíveis todas as imagens da vítima compartilhadas e disponíveis na Internet.

A principal alternativa segura para acesso remoto consiste nas redes privadas virtuais, ou VPN (*Virtual Private Networks*). Uma VPN permite que usuários geograficamente remotos troquem dados por meio de uma rede existente, tipicamente a Internet, de forma segura. A técnica básica fornece um caminho seguro de transmissão, conhecido como um túnel que pode conectar dois sistemas ou duas redes. Duas técnicas populares de implementação de VPNs são a que utiliza o IPsec (*Internet Protocol Security*) e a que utiliza o SSL (*Secure Socket Layer*) ou TLS (*Transport Layer Security*).

Em relação às técnicas de VPNs IPsec e VPNs SSL, avalie as asserções a seguir e a relação proposta entre elas.

1. Na definição de uma VPN, na qual são exigidos alto volume de transações e baixa latência, é mais indicado o uso do IPsec do que do SSL.
2. Tanto o IPsec quanto o SSL normalmente usam a técnica de sequenciamento de pacotes para detectar ataques de *replay* (repetição de mensagens válidas), sendo o IPsec mais eficiente que o SSL nesse caso.

Assinale a opção **CORRETA**:

(Questão baseada no ENADE)

- ☐ a. As asserções 1 e 2 são falsas.
- ☒ b. As asserções 1 e 2 são verdadeiras e 2 é uma justificativa correta de 1.
- ☐ c. As asserções 1 e 2 são verdadeiras, mas 2 não é uma justificativa correta de 1.
- ☐ d. A asserção 1 é falsa e 2 é verdadeira.
- ☐ e. A asserção 1 é verdadeira e 2 é falsa.

Sua resposta está incorreta.

O IPsec trabalha na camada de rede e o SSL na camada de aplicação, por isso, processar o IPsec é mais rápido do que o SSL, que precisa executar funções de mais camadas.

A resposta correta é: As asserções 1 e 2 são verdadeiras e 2 é uma justificativa correta de 1.

Qual desses exemplos **não** se classifica como um ataque MITM na vida *offline*:

- ☐ a. Um porteiro analisando as encomendas que chegam para os moradores de um prédio.
- ☐ b. Um estranho modificando cartas antes delas chegarem ao destinatário.
- ☐ c. Conversar com alguém que acredita que você é outra pessoa.
- ☐ d. Um carteiro lendo correspondências pessoais.
- ☒ e. Ler o diário de outra pessoa, sem seu consentimento.

Sua resposta está correta.

Ler o diário de outra pessoa, sem seu consentimento não é um exemplo de interceptação de informação entre duas entidades comunicantes, que é a característica principal do ataque.

A resposta correta é: Ler o diário de outra pessoa, sem seu consentimento.

Qual das opções a seguir contempla **prioridades** das defesas em segurança da informação?

Escolha uma opção:

- ☒ a. Proteger a vida humana e a integridade física das pessoas; proteger dados sigilosos; proteger dados tais como dados proprietários, científicos, gerenciais; impedir danos aos sistemas; minimizar a indisponibilidade de recursos computacionais.
- ☐ b. Evitar senhas fáceis de serem descobertas; usar um bom antivírus sempre atualizado; usar um bom firewall; usar um bom *antispyware*; colocar sempre o navegador com as opções de segurança colocadas em "nível alto", tomar cuidado com a engenharia social, evitando sempre fornecer dados pela internet como telefone, endereço, senhas (como a de acesso ao seu provedor), número do seu cartão de crédito, CPF, email, etc.
- ☐ c. Realizar treinamentos e atividades educativas sobre segurança da informação com todos os funcionários, terceiros e prestadores de serviços; realizar testes periódicos de software, de invasão e das contramedidas existentes; manter-se atualizado com as notícias sobre novos ataques e das listas de ataques mais comuns.
- ☐ d. Assinar boletins periódicos editados pelas equipes de resposta a incidentes de segurança; acompanhar o lançamento de *patches* (remendos) de segurança produzidos pelos fabricantes de seus equipamentos; observar ativamente as configurações dos sistemas e identificar quaisquer mudanças ocorridas e investigue todas as anomalias; rever todas as políticas e procedimentos de segurança pelo menos uma vez por ano; verificar regularmente a obediência às políticas e procedimentos de segurança; assinar listas de discussão relevantes para se manter atualizado com as informações mais recentes compartilhadas por colegas administradores.
- ☐ e. Fazer levantamento cuidadoso dos ativos do sistema deve ser realizado (ou seja, um exame cuidadoso para saber como o sistema foi afetado pelo incidente); incluir as lições aprendidas como resultados dos incidentes na revisão do plano de segurança para evitar que o incidente ocorra novamente; desenvolver uma nova análise de risco.

✔ Parabéns

Qualquer pessoa ou instituição corre o risco de sofrer um ataque cibernético, a diferença está entre sofrer um ataque e este ser bem sucedido ou não. Para se proteger de um ataque cibernético, é necessário seguir alguns requisitos como: deixar sempre o sistema operacional atualizado, utilizar um programa de antivírus/*firewall* sempre atualizado, não abrir anexos de e-mails suspeitos e possuir uma política de backup de arquivos diária/semanal/mensal/trimestral. São atitudes como essa que irão ajudar a não sofrer com esse tipo de ataque.

Escolha uma opção:

- ☒ Verdadeiro ✔
- ☐ Falso

Sim, atitudes podem ajudar a evitar ataques, apesar de nada garantir 100% de proteção.

A resposta correta é 'Verdadeiro'.

Honda é alvo de ataque hacker e suspende parte da produção, incluindo no Brasil

Empresa teria sido afetada por um vírus de resgate, que impediu a utilização de alguns sistemas computacionais.

A Honda suspendeu parte da produção global de automóveis e motocicletas, após ter sido alvo de um ataque hacker. Além de fábricas, a operação de serviços ao consumidor e serviços financeiros também foi afetada.

...

Segundo o portal The Verge, a praga foi do tipo *ransomware*, um vírus de resgate, que geralmente embaralha informações e arquivos dos computadores, impossibilitando o uso. Vírus de resgate são assim chamados porque exigem que a vítima desembolse uma quantia financeira para restaurar arquivos e o funcionamento de sistemas "sequestrados".

Fonte: <https://g1.globo.com/carros/noticia/2020/06/09/honda-e-alvo-de-ataque-hacker-e-suspende-parte-da-producao-incluindo-no-brasil.ghtml>

O ataque noticiado pode ser categorizado como (marque quantas opções forem necessárias, mas itens errados tem valor negativo):

- ☒ a. Sequestro de dados e sistemas
- ☐ b. Vazamento de dados
- ☐ c. Negação de serviço
- ☐ d. Injeção de código
- ☒ e. *Malware*



Sua resposta está parcialmente correta.

Você selecionou corretamente 2.

As respostas corretas são: *Malware*, Negação de serviço, Sequestro de dados e sistemas

Ativar o Windows

Uma das técnicas de ataques em ambientes de TI é denominada "homem do meio" (*man in the middle*). Ela pode ser aplicada em uma rede Wi-Fi com o objetivo de associar o endereço MAC do intruso ao endereço IP do ponto de acesso (*Access Point* - AP) Wi-Fi da rede. Como o AP é o *gateway* dessa sub-rede sem fio, todo o tráfego direcionado ao ponto de acesso pode ser interceptado pelo intruso. Esse ataque explora deficiências conhecidas no projeto de segurança do IEEE 802.11 ou Wi-Fi.

Considerando um ataque "homem no meio", por meio de *Address Resolution Protocol* (ARP) *spoofing*, no contexto descrito acima, avalie as afirmações a seguir:

1. O problema do compartilhamento de chave presente no projeto de segurança do AP pode ser resolvido com a utilização de um protocolo baseado em chave pública para negociar chaves individuais, como é feito no *Transport Layer Security* (TLS) / *Secure Socket Layer* (SSL).
2. O problema de desvio de tráfego causado pelo ataque pode ser evitado com a configuração de um *firewall* nos pontos de acesso que filtram tráfego entre clientes de uma mesma sub-rede.
3. O problema da falta de autenticação dos pontos de acesso sem fio pode ser contornado obrigando-se o ponto de acesso a fornecer um certificado que possa ser autenticado pelo uso de uma chave pública obtida de terceiros.
4. A vulnerabilidade das chaves de 40 ou 64 bits a ataques de força bruta pode ser evitada utilizando-se um AP que permita chaves de 128 bits e limitando-se o tráfego a dispositivos compatíveis com estas chaves.

É correto o que se afirma em:

(Questão baseada no ENADE)

- ☐ a. 1 e 2
- ☐ b. 1 e 3
- ☒ c. 1, 3, e 4
- ☐ d. 2, 3 e 4
- ☐ e. 2 e 4



Ativar o Windows



A criptografia utilizada para garantir que somente o remetente e o destinatário possam entender o conteúdo de uma mensagem transmitida caracteriza uma propriedade de comunicação segura denominada:

Escolha uma opção:

- ☐ a. Disponibilidade
- ☒ b. Confidencialidade
- ☐ c. Integridade
- ☐ d. Autenticidade
- ☐ e. Irretratabilidade

✓ Parabéns

Os mecanismos de busca, como o Google, classificam as páginas e apresentam resultados relevantes com base nas consultas da pesquisa dos usuários. Dependendo da relevância do conteúdo do site, ele pode aparecer mais alto ou mais baixo na lista de resultado da pesquisa. SEO, abreviação de *Search Engine Optimization* (otimização de mecanismos de busca), é um conjunto de técnicas usadas para melhorar a classificação do site por um mecanismo de pesquisa. Embora muitas empresas legítimas se especializem na otimização de sites para melhor posicioná-las, um usuário mal-intencionado pode usar o SEO para que um site mal-intencionado fique mais alto nos resultados da pesquisa. Esta técnica é chamada de envenenamento de SEO.

Ataques de negação de serviço são muito comuns na Internet para indisponibilizar servidores, serviços, aplicativos etc. Podem ser feitos isoladamente ou combinados com outras técnicas de ataque.

Com relação aos ataques de negação de serviço e/ou de *Search Engine Optimization* (SEO), classifique corretamente as situações apresentadas a seguir.

DoS

Quando uma rede, *host* ou aplicativo recebe uma enorme quantidade de dados a uma taxa que não consegue processar.

DDoS

✖

Um invasor cria uma *botnet*, rede de *hosts* infectados.

DDoS

✓

Quando um pacote formatado de maneira mal-intencionada é enviado a um host ou aplicativo que não consegue contê-lo.

DoS

✓

Sua resposta está parcialmente correta.

A resposta correta é: Quando uma rede, *host* ou aplicativo recebe uma enorme quantidade de dados a uma taxa que não consegue processar. → DoS, Um invasor cria uma *botnet*, rede de *hosts* infectados. → DDoS, Quando um pacote formatado de maneira mal-intencionada é enviado a um host ou aplicativo que não consegue contê-lo. → DoS.

Relacione cada conceito de segurança da informação à sua correta descrição.

Verificada com decifragem por chave pública.	Autenticidade	✓
Ataques DoS ou DDoS a prejudicam.	Disponibilidade	✓
Conformidade com regras ou leis ou normas.	Legalidade	✓
Garantida pela cifragem com chave pública.	Confidencialidade	✓

Sua resposta está correta.

A resposta correta é: Verificada com decifragem por chave pública. → Autenticidade, Ataques DoS ou DDoS a prejudicam. → Disponibilidade, Conformidade com regras ou leis ou normas. → Legalidade, Garantida pela cifragem com chave pública. → Confidencialidade.

Dados de 16 milhões de brasileiros que foram diagnosticados com Covid-19 ou que tiveram suspeitas da doença ficaram indevidamente expostos na internet. O banco do Ministério da Saúde estava facilmente acessível, graças a um descuido de segurança que deixou públicas as senhas de acesso.

Como relata o Estado de S. Paulo, a vulnerabilidade continha dados não apenas de cidadãos comuns, mas também de autoridades da esfera política, incluindo o presidente Jair Bolsonaro e outras figuras públicas que foram diagnosticadas com Covid-19 ao longo dos últimos meses, como o governador de São Paulo João Doria e o ministro da Saúde Eduardo Pazuello.

Os bancos incluíam não apenas informações pessoais, como CPF e endereço, mas também o histórico médico dos pacientes cujos dados foram expostos.

Segundo a reportagem, a brecha em questão foi causada por um funcionário do Hospital Albert Einstein, que acabou tornando públicas as senhas para acessar o banco de dados na plataforma de desenvolvimento GitHub em texto simples, sem nenhum tipo de criptografia. Com elas, era possível acessar as informações do E-SUS-VE, onde são notificados casos leves e moderados, e o Sivep-Gripe, por onde são notificados todos os casos de Síndrome Respiratória Aguda Grave (SRAG).

...

Fonte: <https://olhardigital.com.br/2020/11/26/noticias/dados-de-16-milhoes-de-brasileiro-sao-expostos-em-vazamento-do-ministerio-da-saude/>

São **consequências diretas** de ataques como esse (marque quantas opções forem necessárias, mas itens errados tem valor negativo):

- ☒ a. Perda de credibilidade da instituição
- ☒ b. Exposição dos pacientes
- ☐ c. Falhas na conscientização dos usuários
- ☐ d. Perda financeira
- ☒ e. Falta de criptografia dos dados

Ativar o Windows  
Acesse Configurações para ativar o Windows.

Identifique abaixo quais os tipos de meio físico e sinais quanto à sua sensibilidade às interferências eletromagnéticas da seguinte forma: DS (Delimitado pelo meio físico e Sensível à interferência), DI (Delimitado pelo meio físico e Insensível à interferência), NS (Não delimitado pelo meio físico e Sensível à interferência) e NI (Não delimitado pelo meio físico e Insensível à interferência).

Obs. Considere como "interferência" sinais eletromagnéticos indesejáveis.

- ☐ ( ) Cabo de Fibra Ótica
- ☐ ( ) Feixe de Ondas de Rádio
- ☐ ( ) Cabo coaxial blindagem simples
- ☐ ( ) Cabo de Par Trançado STP
- ☐ ( ) Comunicação por infravermelho no ar
- ☐ ( ) PLC (POWER LINE COMMUNICATIONS)
- ☐ ( ) Wireless

A sequencia que contem a resposta correta é:

Escolha uma opção:

- ☒ a. DI, NS, DS, DS, NI, DS, NS
- ☐ b. NS, NI, DS, DI, NI, DI, DI
- ☒ c. NI, NS, NS, NI, NS, DS, DS
- ☐ d. NS, NI, NS, NI, NS, DS, DI

✖ Reflita melhor

Sua resposta está incorreta.

As redes computacionais sofrem variedades tipos de interferência e isto é um serio problema que causa degradação no sinal. conhecê-los é uma tarefa de importante no nosso estudo.

A resposta correta é: DI, NS, DS, DS, NI, DS, NS

Ativar o Windows  
Acesse Configurações para ativar o Windows.

Sobre um roteador, qual das alternativas a seguir é **FALSA**?

- ☒ a. Interliga somente sub-redes da mesma rede.
- ☐ b. Executa protocolos de encaminhamento, como o IP, e de roteamento, como o BGP.
- ☐ c. Pode possuir funcionalidades de *firewall*, de *proxy* e de DNS.
- ☐ d. Possui um endereço IP para cada rede por ele interligada.
- ☐ e. Possui uma interface de rede para cada rede por ele interligada.



Sua resposta está correta.

Roteadores não só interligam sub-redes da mesma rede como também redes distintas. As demais alternativas caracterizam os roteadores.

A resposta correta é: Interliga somente sub-redes da mesma rede.

Um arquivo confidencial precisa ser enviado de uma empresa A para uma empresa B por meio da Internet. Existe uma preocupação com a possibilidade de interceptação e alteração do documento durante sua transmissão. Para reduzir a possibilidade de que um *hacker* tenha acesso ao conteúdo da mensagem, foi adotado um procedimento de criptografia de chave pública e de assinatura digital.

Considerando a utilização dessas tecnologias para a codificação dos dados, avalie as afirmações que se seguem:

1. Para o procedimento de cifragem do documento é utilizada a chave pública do destinatário.
2. Para o procedimento de assinatura digital do documento é utilizada a chave privada do destinatário.
3. Para o procedimento de decifragem do documento é utilizada a chave privada do remetente.
4. Para o procedimento de verificação da assinatura digital do documento é utilizada a chave pública do remetente.

É correto apenas o que se afirma em:

(Questão baseada no ENADE)

- ☐ a. 2 e 3
- ☐ b. 2
- ☒ c. 1 e 4
- ☐ d. 1
- ☐ e. 3 e 4



Sua resposta está correta.

Atenção ao uso de criptografia assimétrica para garantir confidencialidade e para assinatura digital.

A resposta correta é: 1 e 4



Os dispositivos de interconexão de rede são usados nas mais diversas aplicações, seja em uma LAN (*Local Area Network*) ou em grandes redes como a Internet. Entre os mais comuns estão concentradores, repetidores, pontes, *switches*, roteadores e *gateways*. Estes últimos podem ser um *hardware*, um *software*, ou a combinação de ambos. O *gateway* pode traduzir endereços e formatos de mensagens, tornando possível a comunicação entre redes heterogêneas, isto é redes que utilizam tecnologias diferentes. O *gateway* pode estar associado a um simples roteador doméstico e atuar como um servidor *proxy*, entre outras aplicações.

Considerando as informações apresentadas, avalie as ações a seguir, em relação ao que o *gateway* permite.

1. Interligar redes que utilizam diferentes protocolos de rede.
2. Implementar VLANs (*Virtual LANs*) para melhorar o desempenho e a segurança da rede.
3. Traduzir pacotes originários da rede local para que eles possam atingir o destinatário em outras redes.
4. Atuar como *firewall*, pois serve de intermediário entre o *host* e a Internet, por exemplo.
5. Compartilhar a conexão com a Internet entre vários *hosts*, desde que o endereço do *gateway* seja definido nas propriedades de rede, não sendo possível a alocação automática de endereços.

É correto apenas o que se menciona em:

(Questão baseada no ENADE)

- ☒ a. 1, 3 e 4
- ☐ b. 1 e 2
- ☐ c. 1, 2 e 5
- ☐ d. 3, 4 e 5
- ☒ e. 2, 3, 4 e 5

Sua resposta está incorreta.

Implementar VLANs (*Virtual LANs*) para melhorar o desempenho e a segurança da rede é papel de *switch*, não de *gateway*.

O *gateway* compartilhar a conexão com a Internet entre vários *hosts*, desde que o endereço do *gateway* seja definido nas propriedades de rede e é possível sim a alocação automática de endereços (DHCP).

A resposta correta é: 1, 3 e 4

Quando mais crítica a confidencialidade de uma informação, mais os métodos biométricos de controle de acesso devem ser usados combinados com outros tipos de métodos de acesso como senhas ou *tokens*.

Escolha uma opção:

- ☒ Verdadeiro ✓
- ☐ Falso

A combinação de métodos de controle de acesso é fundamental para dados críticos.

A resposta correta é 'Verdadeiro'.

Ataques ao SMTP, e-mail, normalmente são combinados com outros ataques como *phishing* (captura de dados por meio de uma página falsa) ou *Man in The Middle* (interceptação de pacotes) para se roubar informações do usuário.

Escolha uma opção:

- ☒ Verdadeiro ✓
- ☐ Falso

Sim, ataques de e-mail raramente são feitos apenas para "encher" as caixas postais, a grande maioria é utilizada por golpistas.



A resposta correta é 'Verdadeiro'.

Para cada descrição a seguir, indique o tipo correto de teste de invasão.

Realizado com total conhecimento sobre o alvo

Whitebox  

Verifica as vulnerabilidades da infraestrutura de comunicação

Rede  

Realizado com poucos conhecimentos sobre o alvo

Graybox  

Sua resposta está correta.

A resposta correta é: Realizado com total conhecimento sobre o alvo → Whitebox, Verifica as vulnerabilidades da infraestrutura de comunicação → Rede, Realizado com poucos conhecimentos sobre o alvo → Graybox.