INTERNET/REDES DE COMPUTADORES III

DIRETO DO CONCURSO

66. (Q3243405/2024/FUNDAÇÃO GETÚLIO VARGAS/FGV/ALE TO/TÉCNICO/ASSISTÊNCIA ADMINISTRATIVA) Os ataques de negação de serviço distribuídos, conhecidos como DDoS, representam uma ameaça significativa para a segurança da internet. Com base nesse contexto, assinale a afirmativa incorreta.

a) Em um ataque DDoS, os atacantes usam uma rede de computadores comprometidos, conhecidos como botnets.

b) Os ataques DDoS geralmente visam comprometer os dados, tornando-os inacessíveis, mesmo para usuários autorizados.

c) Os ataques DDoS podem causar interrupções significativas nos serviços online.

d) Embora não seja usual, ataques DDoS já foram feitos a partir de dispositivos IoT comprometidos, como câmeras de segurança.

e) Os ataques de DDoS podem ter como alvo vários recursos de rede, incluindo servidores web, jogos online e infraestrutura de nuvem.

a) Isso não é uma regra, mas pode ocorrer.

b) Nesse caso, ninguém terá acesso aos dados.

c) Essa é a destinação desse tipo de ataque.

d) IoT é a internet das coisas. São dispositivos conectados à internet, como câmeras e televisores, assistentes como Alexa etc. Como não são projetados com ênfase na segurança, esses dispositivos são facilmente invadidos e comprometidos.

e) Não há um alvo específico para os ataques DDoS.

---

67. (Q3508214/FADESP/PREFEITURA DE CAPANEMA/AGENTE DE FISCALIZAÇÃO DE OBRAS/2024) No contexto cibernético, o ataque que se caracteriza como tentativas automatizadas de adivinhar senhas ou chaves criptográficas, explorando todas as combinações possíveis até encontrar a correta, é denominado ataque de

a) DDoS.

b) força bruta.

c) *ransomware*.

d) *spoofing*.

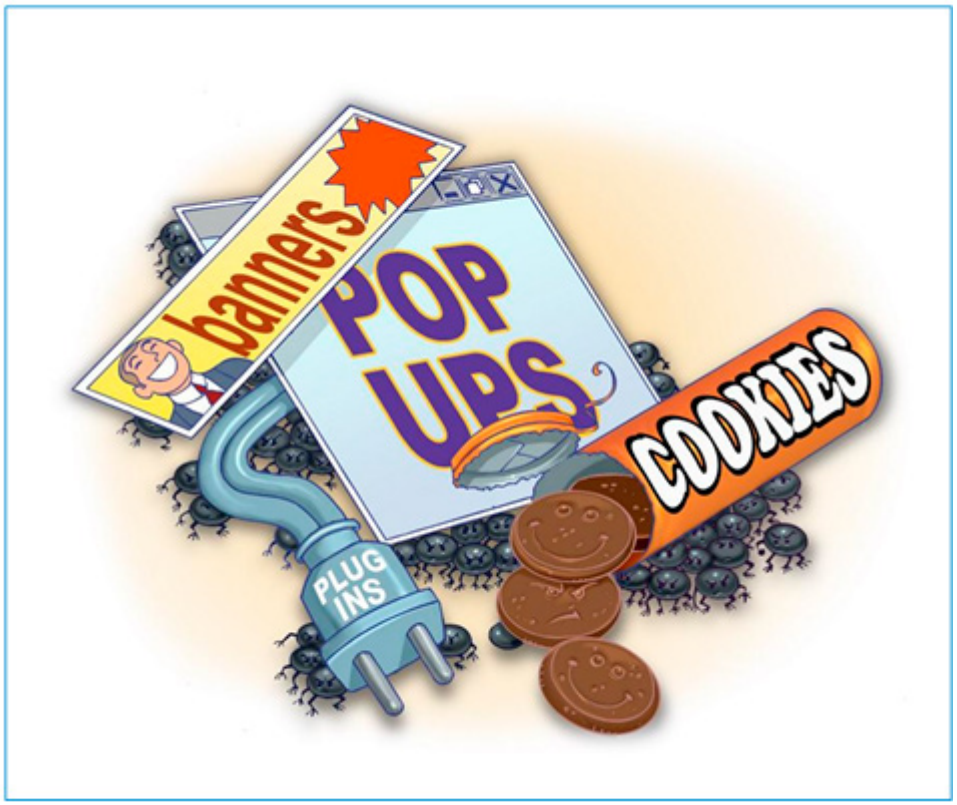
b) A questão descreve o ataque de força bruta.

c) *Ransomware* é o ataque que sequestra os dados.

d) *Spoofing* é o caso de alterar o cabeçalho do e-mail ou outra falsificação

---

OUTROS RISCOS



1) PHISHING (PHISHING SCAM)

Phishing é um golpe em que a pessoa tenta induzir o usuário a fornecer seus dados. Uma mensagem pode chegar por e-mail dizendo que o cartão foi clonado. Muita gente fica tão transtornada com o possível golpe que acaba fornecendo até a senha do cartão.

EXEMPLO:

Comprovante N. 002526

Anexo: Depósito 002526 doc (103kb)

O dinheiro já foi transferido via transferência interbancária para sua conta e já deve ter sido compensado, segue na mensagem o comprovante com os dados e o valor, desculpe o transtorno.

Muito obrigada!

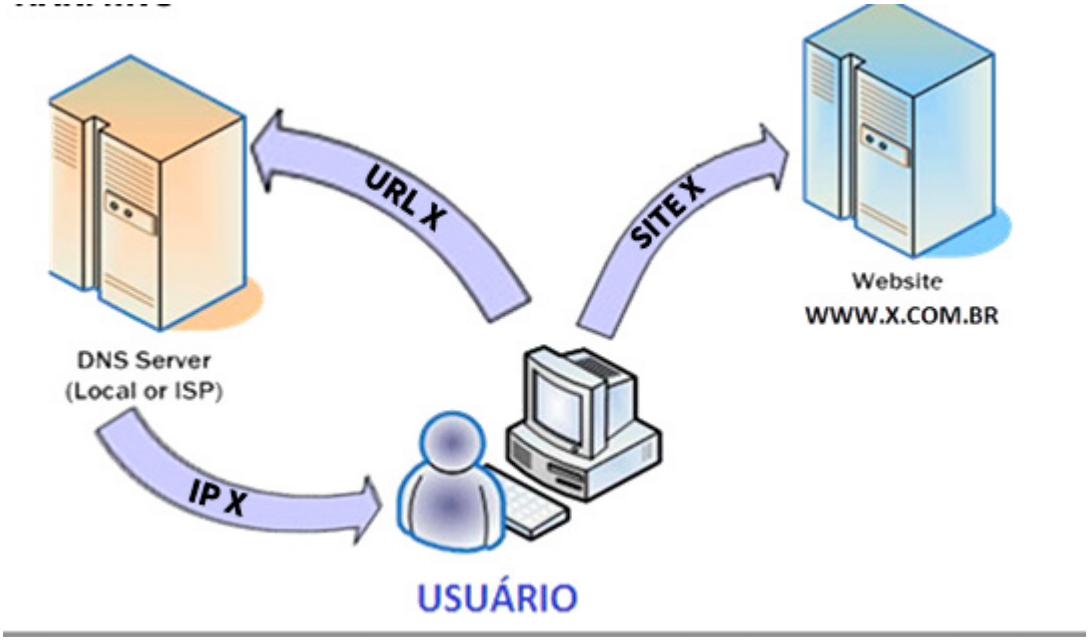
Alice Pacheco Silva

Ao clicar no anexo, provavelmente o usuário instalará um programa malicioso ou será direcionado a um site falso.

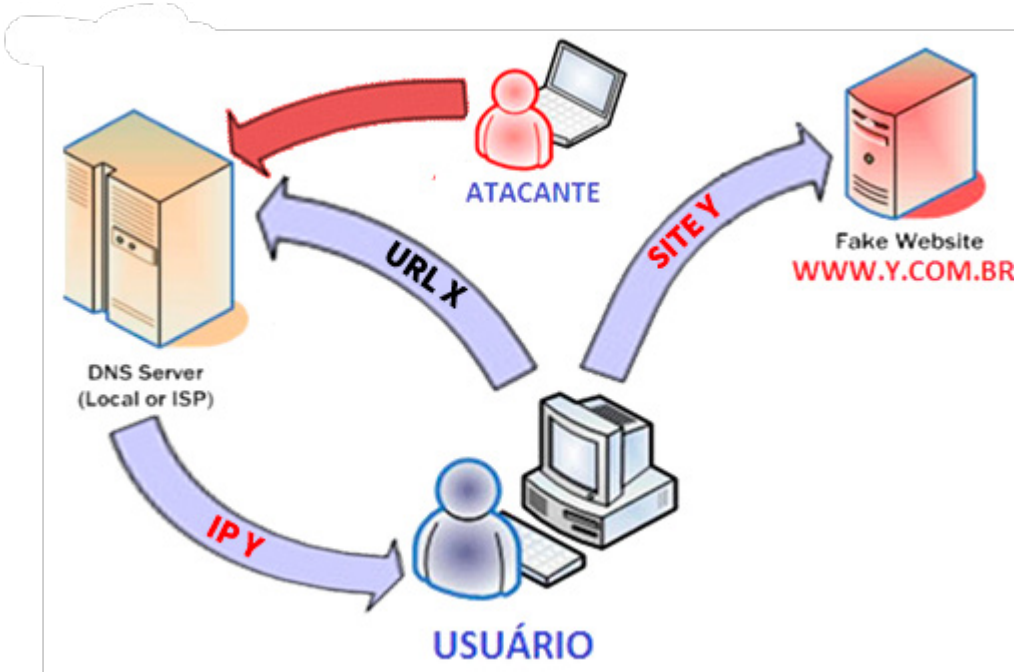
5m

1.1) PHARMING

O *pharming* é um tipo de *phishing*. O DNS é o servidor que traduz uma URL no respectivo IP. Há o fornecimento de uma URL X para o DNS, o qual resolverá e devolverá o IP X. Dessa maneira, o usuário será direcionado para o Site X.

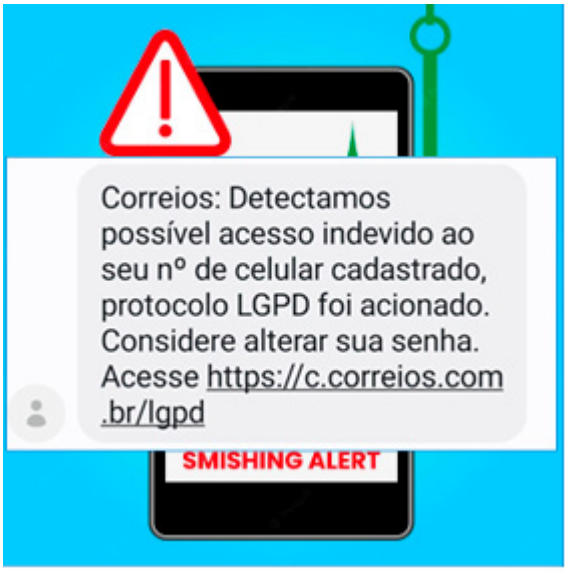


Quando há o ataque de *pharming*, o servidor DNS será envenenado. Ao enviar o URL X, o DNS devolverá o IP Y, o qual direcionará para o Site Y. Provavelmente, para que o ataque seja bem sucedido, a pessoa vai clonar o site para que fique muito parecido com o legítimo.



1.2) SMISHING

É um tipo de *Phishing* praticado por SMS. Após as redes sociais, essa ferramenta entrou em desuso. A seguir, é possível observar uma mensagem recebida supostamente dos correios:



Ao alterar a senha, o usuário passará a senha verdadeira aos atacantes.

2) SPAM

Spam é o e-mail não solicitado, geralmente enviado para muitas pessoas.

2.1) SPAMMER

Spammer é a pessoa que faz o envio de *spam*. Eles usam programas que geram e-mails aleatórios e que capturam e-mails de diversas fontes.

2.1) MALVERTISING

Quanto ao *malvertising*, o atacante serve um site com uma propaganda maliciosa, contendo link para um local ou algo do tipo.

DIRETO DO CONCURSO

68. (Q3179165/2024/INSTITUTO UNIFIL/PREFEITURA DE BANDEIRANTES/ANALISTA DE SISTEMAS) Entre as diversas ameaças virtuais destaca-se o "phishing", uma técnica de engenharia social que visa enganar os usuários para obtenção de informações confidenciais.

Considerando essas informações, assinale a alternativa que descreve corretamente o "phishing".

a) Um tipo de ataque que utiliza códigos maliciosos para se infiltrar em sistemas de segurança.

b) Um método de ataque que envolve a criação de redes fictícias para interceptar comunicações.

c) Um processo de monitoramento constante de atividades online para identificar comportamentos suspeitos.

d) Uma técnica que utiliza e-mails falsos ou sites fraudulentos para obter informações pessoais.

d) O *phishing* é um golpe que tenta obter dados pessoais do usuário.

c) Nesse caso, observa-se que há um tipo de proteção.

FORMAS DE PREVENÇÃO

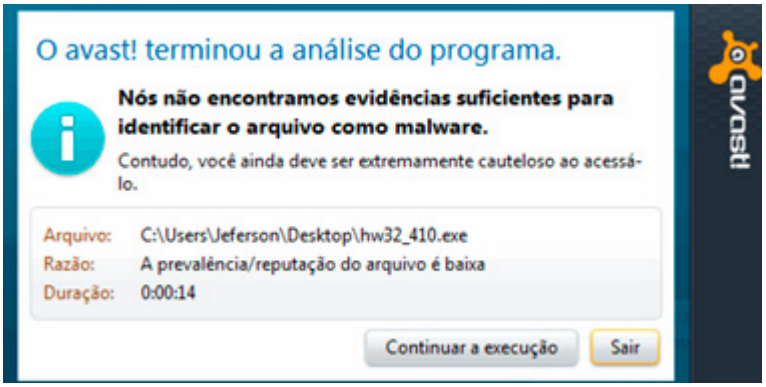
1) ANTIVÍRUS

10m

O antivírus pode usar dois processos para detectar ameaça: a heurística e assinatura.

1.1) HEURÍSTICA

A heurística é a detecção que ocorre quando o antivírus não conhece a ameaça. Ou seja, o antivírus baseia-se no comportamento anômalo e adverso. Isso é feito por meio de algorítimo e programação. No entanto, por não conhecer a ameaça, a heurística funciona parecido com o serviço de polícia, que às vezes atua com base na observação de um comportamento suspeito, como uma pessoa pulando um muro de uma casa 3 horas da manhã. Pode se tratar do caso de alguém que esqueceu a chave e está pulando o muro para não acordar sua esposa. Ou seja, parecia uma ameaça, mas não era (falso positivo). É possível que um cidadão abra o portão de uma casa 3 horas da tarde, sem levantar suspeitas para a polícia. Nesse caso, pode ser um ladrão usando uma chave falsa, caracterizando um caso de falso negativo.



Heurística: Criação de um novo Malware → Detecção baseado no comportamento (não se sabe se é, de fato, uma ameaça) → Sistema Protegido

Assinatura: Criação de um novo Malware → Definição da sequência de dados (desenvolvedor) e lançamento da atualização (identificação do vírus ou programa malicioso e como ele trabalha) → Antivírus recebe a atualização com a defesa (como se fosse uma vacina) → Sistema Protegido

O processo de assinatura demora mais tempo.

2) FIREWALL: SOFTWARE E/OU HARDWARE;

O *firewall* não faz o papel do antivírus, tendo como objetivo filtrar os dados das conexões que chegam e das que saem. Nesse sentido, há o bloqueio de conexões indevidas e permitindo as conexões configuradas adequadamente. O *firewall* pode impedir a entrada de um vírus, porém ao executar um arquivo de um pendrive, o *firewall* não poderá fazer nada.

Quando o *firewall* é apenas um *software*, é chamado de *fire* pessoal da máquina. QUando é *software* e *hardware*, será um *fire* de rede, pois estará na ponta impedindo a invasão da rede toda.

A filtragem é feita a partir de regras que são previamente cadastradas, também chamadas de políticas de segurança.

15m

3) IDS E IPS

IPS – (INTRUSION PREVENTION SYSTEM)

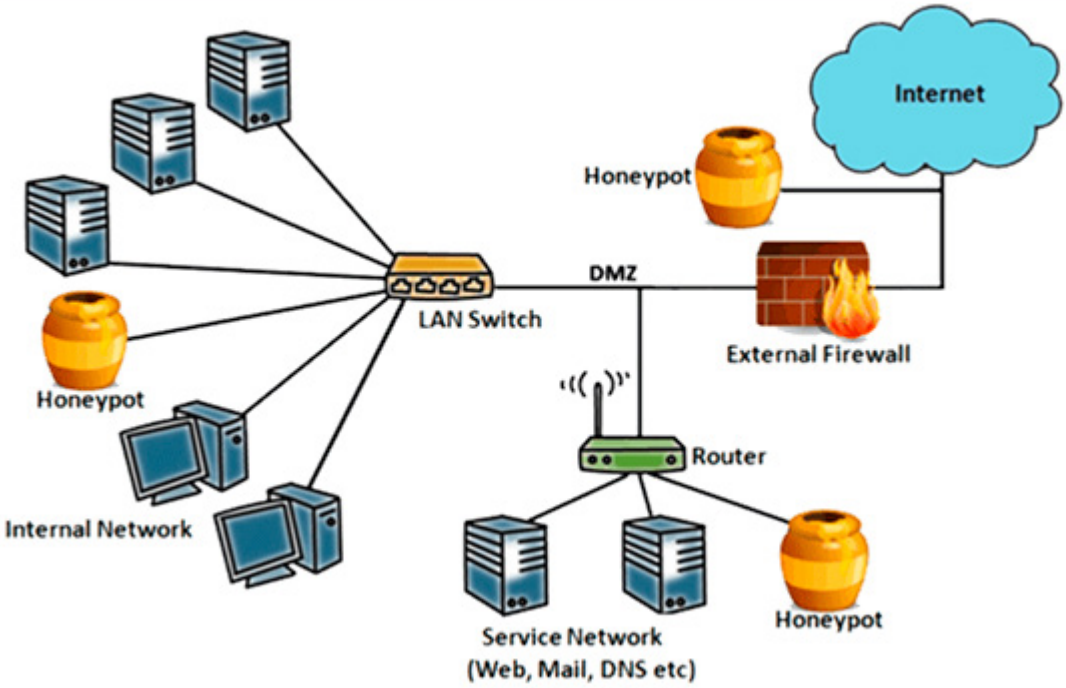
O IPS (sistema de prevenção de intrusão) é ativo, avisando e bloqueando a conexão. No entanto, é possível ocorrer um falso negativo diante de uma aparente invasão indevida. Nesse caso, o sistema bloqueia e emite um alerta para que alguém observe e resolva a situação. Sendo de madrugada, pode ser que não tenha uma pessoa de plantão. Isso faz com que o sistema fique parado. Sendo um sistema de vendas, isso impossibilitaria que as pessoas continuassem comprando.

É possível fazer uma analogia do IPS com a porta do banco. Uma pessoa com um molho de chaves ou um celular no bolso será parada pela porta, emitindo um alerta luminoso e sonoro. A pessoa só será liberada quando um vigilante aparecer e pedir para que a pessoa retire o que há no bolso.

IDS (INTRUSION DETECTION SYSTEM)

Seguindo a analogia das portas, o IDS emite um alerta sonoro e luminoso, porém é possível passar. Nesse caso, a conexão indevida na madrugada passará.

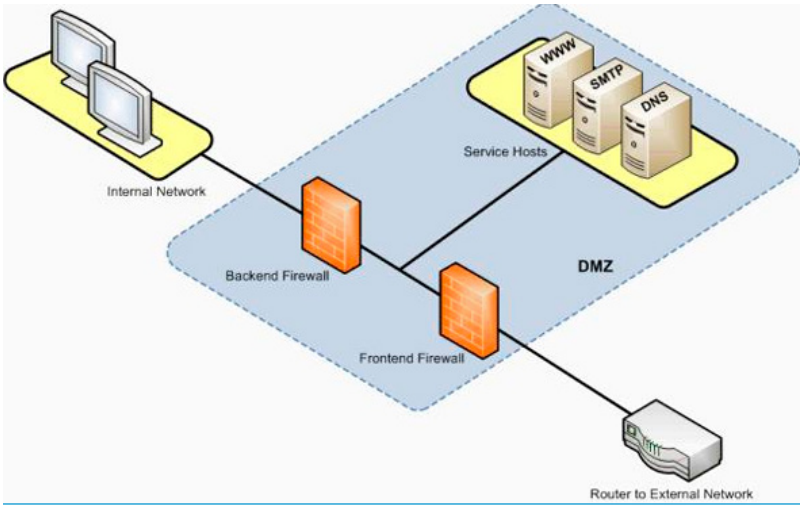
4) HONEYPOT



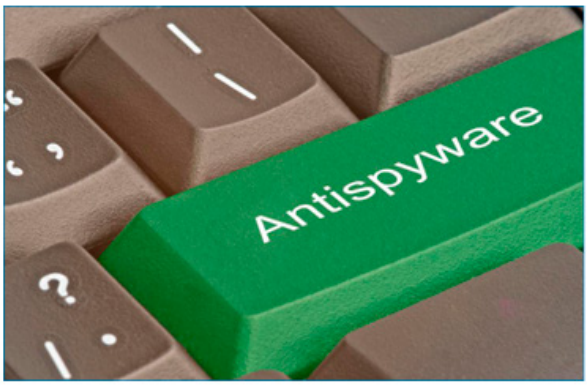
Honeypot são iscas deixadas na rede para que o invasor invada os computadores. Nos Estados Unidos é permitido deixar iscas. É como deixar um carro com a chave no contato. A pessoa entra e, ao perceberem que a pessoa quer se apoderar do carro, elas efetuam o bloqueio, impedindo que a pessoa trafegue para prendê-la. A legislação brasileira não permite esse tipo de conduta.

No *honeypot*, o computador apresentará uma certa fragilidade em relação aos demais. O invasor passará por uma rede de segurança achando que está invadindo uma máquina legítima. Ao fazê-lo, passará a ser monitorado. Dessa forma, é possível verificar que o objetivo do invasor é apagar arquivos, copiá-los, bem como descobrir de onde ele está invadindo.

5) DMZ (DEMILITARIZED ZONE – ZONA DESMILITARIZADA)



A zona desmilitarizada possui dois *firewalls*. Ao redor da DMZ há uma rede interna e roteador. Uma pessoa de fora que tente acessar a *service hosts* não conseguirá acessar a rede interna. As tentativas de invasão negativas serão bloqueadas no *frontend firewall*. As autorizadas passarão e acessarão o servidor web, servidor de e-mail e servidor DNS.



O nome *anti malware* não é comercialmente muito usado.

O *antispyware* no *Windows* é o *Windows Defender*.

20m

- No *Windows 7*, o *Windows Defender* é só um *antispyware*. A partir do *Windows 8.1* ele se tornou um antivírus e um *antispyware*.

DIRETO DO CONCURSO

69. (Q3116813/2024/FUNDAÇÃO GETÚLIO VARGAS/FGV/PREFEITURA DE SÃO JOSÉ DOS CAMPOS/TÉCNICO TRIBUTÁRIO) Considere as seguintes afirmativas acerca de técnicas e aplicativos de segurança:

I – Um programa antivírus bloqueia o acesso de usuários não autorizados ao computador local e adicionalmente pode determinar quais formatos de senha são seguros para serem utilizados.

II – Um firewall analisa o tráfego de rede para determinar quais operações de entrada e saída podem ser executadas, a partir de um conjunto de regras.

III – Um firewall pode ser um aplicativo de software executando em um computador local.

Está correto o que se afirma em

a) I e II, apenas.

b) II e III, apenas.

c) III, apenas.

d) I, apenas.

e) I, II e III.

I – Essa não é uma característica do antivírus.

70. (Q3160357/2024/FUNDAÇÃO GETÚLIO VARGAS/FGV/DNIT/ANALISTA ADMINISTRATIVO) Associe os controles de segurança relacionados à solução para a segurança da informação com suas respectivas definições.

1. *Firewall*
2. *Intrusion Detection Systems* (IDS)
3. *Intrusion Prevention Systems* (IPS)
4. Antivírus *software*

( ) Previne, detecta e remove malware, incluindo vírus de computador, worms de computador, cavalos de Troia, spyware e adware.

( ) É uma ferramenta de monitoramento em tempo integral colocada nos pontos mais vulneráveis ou pontos críticos das redes corporativas para detectar e deter intrusos continuamente.

( ) É uma ferramenta para monitorar o tráfego de rede e as atividades do sistema para prevenir e bloquear possíveis invasões ou ataques. Esta ferramenta é essencial para identificar e mitigar ameaças em tempo real, melhorando a postura geral de segurança de uma organização.

( ) Impede que usuários não autorizados acessem redes privadas. É uma combinação de hardware e software que controla o fluxo de tráfego de entrada e saída da rede.

Assinale a opção que indica a relação correta, na ordem apresentada.

a) 1 – 2 – 3 – 4.

b) 2 – 1 – 3 – 4.

c) 4 – 2 – 3 – 1.

d) 3 – 2 – 1 – 4.

e) 4 – 3 – 2 – 1.

Antivírus *software:* Previne, detecta e remove malware, incluindo vírus de computador, worms de computador, cavalos de Troia, spyware e adware.

Intrusion Detection Systems (IDS): É uma ferramenta de monitoramento em tempo integral colocada nos pontos mais vulneráveis ou pontos críticos das redes corporativas para detectar e deter intrusos continuamente.

Intrusion Prevention Systems (IPS): É uma ferramenta para monitorar o tráfego de rede e as atividades do sistema para prevenir e bloquear possíveis invasões ou ataques. Esta

ferramenta é essencial para identificar e mitigar ameaças em tempo real, melhorando a postura geral de segurança de uma organização.

Firewall: Impede que usuários não autorizados acessem redes privadas. É uma combinação de hardware e software que controla o fluxo de tráfego de entrada e saída da rede.

---

71. (Q3133975/2024/CEBRASPE/CAU/ADVOGADO) O *Windows Defender* Antivírus, uma solução de segurança do sistema operacional Windows, é instalado na máquina do usuário junto a outros antivírus do mercado para uma melhor cobertura contra malwares e vírus.

Tecnicamente, é errado instalar o *Windows Defender* Antivírus com outros antivírus. O *Windows Defender* tem um mecanismo que ao instalar outro antivírus ele desativa os módulos principais e continua com alguns módulos alternativos. É como se ele ficasse funcionando em paralelo. Não é recomendável usar dois antivírus em uma máquina, pois um pode interferir no funcionamento do outro.

25m

GABARITO

66. b

67. b

68. d

69. b

70. c

71. E