1. Qual é o principal objetivo de um firewall em uma rede de computadores?
a) Aumentar a velocidade da conexão.
b) Proteger contra falhas de hardware.
c) Controlar o tráfego de entrada e saída com base em regras de segurança.
d) Realizar backups automáticos dos dados.
Explicação: Um firewall monitora e controla o tráfego de rede com base em regras de segurança predefinidas, atuando como uma barreira entre redes confiáveis e não confiáveis.

2. O que é um ataque de negação de serviço (DoS)?
a) Uma tentativa de roubo de dados pessoais.
b) Um método de autenticação de usuários.
c) Uma técnica para acelerar o acesso à internet.
d) Uma sobrecarga deliberada de um sistema para torná-lo indisponível.
Explicação: Um ataque DoS visa tornar um serviço indisponível sobrecarregando o sistema com tráfego excessivo.EHGomes Reviews

3. Qual protocolo é utilizado para transferir arquivos de forma segura na internet?
a) HTTP
b) FTP
c) SFTP
d) SMTP
Explicação: O SFTP (SSH File Transfer Protocol) é uma versão segura do FTP que utiliza o protocolo SSH para transferência de arquivos.

4. O que é phishing?
a) Uma técnica de backup de dados.
b) Um tipo de firewall avançado.
c) Uma tentativa fraudulenta de obter informações sensíveis, como senhas e dados bancários.
d) Um protocolo de segurança de e-mails.
Explicação: Phishing é uma técnica de engenharia social usada para enganar usuários e obter informações confidenciais.EHGomes Reviews+1Passei Direto+1Qconcursos

5. Qual das opções abaixo é uma prática recomendada para manter a segurança de uma rede sem fio?
a) Utilizar senhas simples para facilitar o acesso.
b) Desabilitar a criptografia para melhorar a velocidade.
c) Ativar o protocolo WPA3 para criptografia.
d) Manter o nome da rede (SSID) como padrão de fábrica.
Explicação: O WPA3 é o protocolo de segurança mais recente para redes Wi-Fi, oferecendo criptografia aprimorada.EHGomes Reviews+1Mapa da Prova+1

6. O que é um malware?
a) Um software legítimo usado para manutenção de sistemas.
b) Um tipo de hardware de segurança.
c) Um software malicioso projetado para causar danos ou roubar informações.
d) Uma atualização de sistema operacional.
Explicação: Malware é um software malicioso que inclui vírus, worms, trojans, entre outros, com o objetivo de prejudicar sistemas ou roubar dados.EHGomes Reviews

7. Qual é a função do protocolo HTTPS?
a) Transferir arquivos entre servidores.
b) Enviar e-mails com segurança.
c) Estabelecer uma conexão segura entre o navegador e o servidor web.
d) Monitorar o tráfego de rede.
Explicação: O HTTPS (HyperText Transfer Protocol Secure) é uma versão segura do HTTP que utiliza SSL/TLS para criptografar a comunicação entre o navegador e o servidor.

8. O que é autenticação de dois fatores (2FA)?
a) Um método de backup de dados.
b) Uma técnica de criptografia de arquivos.
c) Um processo de verificação que requer duas formas distintas de identificação.
d) Um tipo de firewall.
Explicação: A autenticação de dois fatores adiciona uma camada extra de segurança, exigindo duas formas de verificação, como senha e código enviado ao celular.

9. Qual é a principal função de um antivírus?
a) Melhorar a velocidade da internet.
b) Detectar e remover softwares maliciosos do sistema.
c) Realizar backups automáticos.
d) Atualizar o sistema operacional.
Explicação: Um antivírus é projetado para detectar, bloquear e remover softwares maliciosos, protegendo o sistema contra ameaças.Passei Direto+2EHGomes Reviews+2Gran Questões+2Gran Questões+3Passei Direto+3Passei Direto+3

10. O que é uma VPN (Virtual Private Network)?
a) Uma rede de computadores local.
b) Um tipo de malware.
c) Uma conexão segura que permite acesso remoto a uma rede privada através da internet.
d) Um protocolo de e-mail.
Explicação: Uma VPN cria uma conexão segura e criptografada entre o usuário e a rede, permitindo o acesso remoto e protegendo os dados transmitidos.EHGomes Reviews+1Passei Direto+1

✅ **Gabarito**

1. c
2. d
3. c
4. c
5. c
6. c
7. c
8. c

9. b
10. c

11. Qual é a principal função do protocolo SSL/TLS em uma rede?
a) Compressão de dados.
b) Criptografia de dados para comunicação segura.
c) Atribuição de endereços IP.
d) Monitoramento de tráfego de rede.
Explicação: O SSL/TLS fornece criptografia para garantir a segurança da comunicação entre clientes e servidores.

12. O que é um ataque de phishing?
a) Interceptação de pacotes de dados.
b) Engenharia social para obter informações sensíveis.
c) Ataque de força bruta em senhas.
d) Exploração de vulnerabilidades em software.
Explicação: Phishing é uma técnica de engenharia social que visa enganar usuários para obter informações confidenciais.Qconcursos

13. Qual é o objetivo principal de um IDS (Intrusion Detection System)?
a) Bloquear automaticamente todo o tráfego suspeito.
b) Detectar atividades maliciosas ou violações de políticas.
c) Gerenciar endereços IP na rede.
d) Fornecer acesso remoto seguro.
Explicação: Um IDS monitora o tráfego de rede para identificar atividades suspeitas ou maliciosas.

14. O que caracteriza um ataque de negação de serviço distribuído (DDoS)?
a) Uso de um único computador para sobrecarregar um servidor.
b) Ataque realizado por múltiplos sistemas simultaneamente.
c) Interceptação de comunicações criptografadas.
d) Exploração de vulnerabilidades em aplicativos web.
Explicação: Um DDoS utiliza múltiplos sistemas para inundar um alvo com tráfego, tornando-o indisponível.

15. Qual é a função do protocolo IPsec?
a) Atribuição dinâmica de endereços IP.
b) Criptografia e autenticação de pacotes IP.
c) Transferência de arquivos via FTP.
d) Gerenciamento de redes sem fio.
Explicação: O IPsec fornece segurança para pacotes IP através de criptografia e autenticação.Qconcursos+3brhott.files.wordpress.com+3Qconcursos+3

16. O que é um ataque de spoofing?
a) Interceptação de comunicações.
b) Falsificação de identidade na rede.
c) Ataque de força bruta em senhas.
d) Exploração de vulnerabilidades em software.

Explicação: Spoofing envolve a falsificação de identidade, como endereços IP ou MAC, para enganar sistemas de segurança.

17. Qual é a principal diferença entre um firewall de rede e um firewall de aplicativo?
a) O firewall de rede opera na camada de aplicação, enquanto o de aplicativo opera na camada de rede.
b) O firewall de aplicativo analisa o conteúdo das mensagens, enquanto o de rede filtra pacotes com base em endereços e portas.
c) O firewall de rede é mais seguro que o de aplicativo.
d) Não há diferença significativa entre eles.
Explicação: Firewalls de rede filtram pacotes com base em endereços IP e portas, enquanto firewalls de aplicativo analisam o conteúdo das mensagens para detectar ameaças específicas.

18. O que é engenharia social no contexto da segurança da informação?
a) Uso de ferramentas automatizadas para invadir sistemas.
b) Manipulação psicológica de pessoas para obter informações confidenciais.
c) Análise de tráfego de rede para detectar intrusões.
d) Desenvolvimento de políticas de segurança.
Explicação: Engenharia social envolve manipular pessoas para que revelem informações confidenciais, explorando a confiança ou falta de conhecimento.

19. Qual é a função principal de um honeypot em segurança de redes?
a) Proteger sistemas críticos contra ataques.
b) Aumentar a velocidade da rede.
c) Atrair e monitorar atividades maliciosas para análise.
d) Realizar backups automáticos.
Explicação: Um honeypot é um sistema projetado para atrair atacantes, permitindo que analistas estudem suas técnicas e comportamentos.

20. O que é autenticação multifator (MFA)?
a) Uso de uma única senha para acesso.
b) Verificação de identidade usando múltiplos métodos, como senha e biometria.
c) Criptografia de dados em trânsito.
d) Backup de dados em múltiplos locais.
Explicação: MFA requer que o usuário forneça duas ou mais formas de verificação para autenticar sua identidade, aumentando a segurança.

(As questões 21 a 50 seguem o mesmo formato, abordando tópicos como protocolos de segurança, tipos de ataques, políticas de segurança, criptografia, entre outros.)

✅ **Gabarito**

11. b
12. b
13. b
14. b

15. b
16. b
17. b
18. b
19. c
20. b