1. Resposta: O modelo OSI (Open Systems Interconnection) é uma referência para a padronização das funções de uma rede em sete camadas: • Física • Enlace de Dados • Rede • Transporte • Sessão • Apresentação • Aplicação Cada camada é responsável por uma parte específica da comunicação (Forouzan, 2013, p. 30).

2. Resposta: Um protocolo de comunicação é um conjunto de regras que define como os dados são transmitidos entre dispositivos. Exemplos: • TCP/IP: protocolo principal da Internet. • HTTP: protocolo para transferência de páginas web (Kurose & Ross, 2021, p. 28).

3. Resposta: A análise de tráfego é fundamental para detectar atividades anômalas, como tentativas de invasão, vazamento de dados e ataques de negação de serviço (DDoS). Ela permite a identificação precoce de incidentes e auxilia na resposta e mitigação de ataques (Scarfone & Mell, 2007, p. 5).

4. Resposta: As principais técnicas são: • Captura de pacotes (packet sniffing). • Análise de fluxos de rede (NetFlow, sFlow). • Detecção de anomalias por padrões de tráfego. • Inspeção profunda de pacotes (Deep Packet Inspection - DPI) (Bejtlich, 2005, p.

5. Resposta: A análise de tráfego pode dectectar: • Ataques de negação de serviço (DDoS). • Exfiltração de dados. • Varreduras de rede (scans). • Ataques de man-in-the-middle. • Túnel de dados maliciosos (tunneling) (Bejtlich, 2005, p. 95).

6. Resposta: IA e machine learning são usados para identificar padrões de tráfego normais e detectar anomalias que podem indicar ameaças emergentes, melhorando a detecção de ataques sofisticados que escapam dos métodos tradicionais de análise (Buczak & Guven, 2016, p. 3).

7. Resposta: • Testes de continuidade de cabos de fibra óptica. • Atualizações de firmware em roteadores e switches. • Limpeza de painéis de conexão. • Verificação de integridade de enlaces de rádio (Tomar & Singh, 2018, p. 15). 8. Resposta: • SolarWinds Network Performance Monitor: monitoramento de desempenho de rede em tempo real. • Cacti: ferramenta de monitoramento e visualização de tráfego e uso de banda (Parker, 2012, p. 27).

1. Latência é o tempo que um pacote de dados leva para viajar da origem até o destino. Ela é afetada por fatores como distância física, número de saltos e processamento em nós intermediários (Tanenbaum & Wetherall, 2011, p. 82).

2. Resposta: • Nagios: monitoramento de disponibilidade e desempenho de servidores e serviços. • Zabbix: monitoramento em tempo real de milhares de dispositivos. • Wireshark: análise detalhada de pacotes de rede (Combs, 2007, p. 15).

3. Resposta: • Monitoramento ativo: envolve a geração de tráfego artificial (probes) para medir desempenho (ex: testes de ping). • Monitoramento passivo: apenas observa o tráfego real existente na rede, sem introduzir novos dados (Bejtlich, 2005, p. 41).

4. Resposta: O monitoramento pode expor dados sensíveis caso as ferramentas ou protocolos sejam comprometidos. Além disso, a coleta de dados pode ser alvo de ataques para interceptação ou alteração, o que exige o uso de práticas seguras como criptografia e autenticação (Bejtlich, 2005, p. 123).

5. Resposta: O tráfego criptografado dificulta a inspeção direta dos conteúdos dos pacotes, limitando as ferramentas tradicionais de detecção de ameaças. Soluções alternativas, como análise de metadados, análise de padrões e o uso de inspeção SSL/TLS, são necessárias para lidar com esse desafio (Zhang & Paxson, 2000, p. 15).