1. Ataques de negação de serviço (DoS) visam exclusivamente comprometer a integridade dos dados no sistema, sem afetar a disponibilidade dos recursos locais como processador, memória, arquivos abertos, sockets de rede ou semáforos.
Verdadeiro Falso

2. Qual das seguintes opções representa corretamente a função do "sal" em sistemas de autenticação por senhas?
O "sal" é um método de criptografia simétrica usado para cifrar senhas.
O "sal" é um número aleatório adicionado à senha antes de calcular o hash, dificultando ataques de dicionário.
O "sal" é uma técnica de compressão usada para reduzir o tamanho das senhas armazenadas.
O "sal" é um algoritmo de resumo usado para verificar a autenticidade das senhas.
O "sal" é um método de encriptação usado para proteger os dados transmitidos pela rede.

3. O princípio de "Privilégio Mínimo" sugere que todos os usuários e programas devem ter acesso completo a todos os recursos do sistema para garantir o bom funcionamento do sistema.
Verdadeiro Falso

4. Qual das seguintes técnicas de autenticação é baseada em características intrinsecamente associadas ao usuário, como dados biométricos?
SYK (Something You Know)
SYH (Something You Have)
SYA (Something You Are)
OTP (One-Time Password)
Challenge-Response

5. Qual das seguintes afirmações descreve corretamente o conceito de autenticação em sistemas computacionais?
Autenticação é o processo de verificar a integridade dos dados armazenados em um sistema.
Autenticação é o procedimento de verificar a autenticidade de uma entidade no sistema computacional, garantindo que as informações associadas a essa entidade sejam verdadeiras e correspondam às informações do mundo real que elas representam.
Autenticação é o método de garantir a disponibilidade dos recursos do sistema para todos os usuários registrados.
Autenticação é o processo de criptografar dados para proteger a confidencialidade das informações transmitidas pela rede.
Autenticação é a técnica de realizar backups regulares para evitar a perda de dados importantes.

6. Quais das seguintes afirmações sobre a coleta de dados para auditoria em sistemas operacionais são corretas?
A coleta de dados para auditoria em sistemas operacionais geralmente é feita em tempo real, sem registro de eventos passados.
Arquivos de registro (logfiles) são uma abordagem moderna e rara para representar dados de auditoria.

Arquivos de registro (logfiles) contêm uma sequência cronológica de descrições textuais de eventos associados a uma fonte de dados, geralmente uma linha por evento.
A representação de dados de auditoria em sistemas UNIX utiliza arquivos de registro para reportar eventos associados à autenticação de usuários.
A coleta de dados para auditoria não considera a autenticação de usuários como um evento importante.

7. Qual dos seguintes ataques é considerado um ataque passivo, visando capturar informações confidenciais?
Ataque de negação de serviço (DoS)
Ataque de interrupção
Ataque de fabricação
Ataque de interceptação
Ataque de modificação

8. A técnica de autenticação por senhas descartáveis (OTP - One-Time Password) implica que cada senha só pode ser usada uma única vez, aumentando a segurança do sistema.
Verdadeiro Falso

9. Qual das seguintes afirmações sobre controle de acesso em sistemas operacionais é correta?
Em um sistema de controle de acesso, um sujeito é uma entidade que realiza ações no sistema, como processos ou threads.
O controle de acesso é responsável apenas por garantir que os usuários autenticados possam acessar qualquer recurso do sistema.
O controle de acesso discricionário (DAC) baseia-se em regras globais que não dependem das identidades dos sujeitos e objetos.
As listas de controle de acesso (ACLs) permitem apenas definir permissões de acesso para usuários individuais, não para grupos.
O controle de acesso obrigatório (MAC) permite que os proprietários dos objetos definam as permissões de acesso aos seus próprios recursos.

10. A autenticação multifator envolve a combinação de duas ou mais técnicas de autenticação, como senha e reconhecimento de íris, para aumentar a segurança.
Verdadeiro Falso

11. As políticas de controle de acesso definem de forma concreta e detalhada cada operação que um sujeito pode realizar em um objeto do sistema.
Verdadeiro Falso

12. Qual das seguintes opções **NÃO** é considerada uma propriedade fundamental de segurança em sistemas computacionais?
Confidencialidade
Integridade
Disponibilidade
Autenticação
Irretratabilidade

13. Quais das seguintes afirmações sobre o controle de acesso em sistemas UNIX são corretas?
Em sistemas UNIX, cada arquivo ou diretório pode ter permissões definidas para apenas um usuário.
As permissões em sistemas UNIX são definidas usando três classes: proprietário, grupo e outros.
Em sistemas UNIX, as permissões de acesso a arquivos são verificadas continuamente durante cada operação de leitura ou escrita.
O sistema UNIX suporta listas de controle de acesso (ACLs) avançadas.
As permissões de um arquivo em sistemas UNIX são armazenadas em um arquivo separado chamado de "permissão.conf".

14. Relacione as situações abaixo a ataques diretos à (C)onfidencialidade, (I)ntegridade, (D)isponibilidade ou (A)utenticidade. A opção que representa corretamente a sequência de ataques é:
(A)Um programa que permite injetar pacotes falsos na rede.
(D)Um ataque de negação de serviços através da rede.
(D)int main { while (1) fork(); }
(C)Um programa quebrador de senhas.
(I)Um processo que modifica o arquivo de sistema /etc/hosts para redirecionar acessos de rede.
(C)Um programa de captura de pacotes de rede.

15. Sobre as afirmações a seguir, relativas às propriedades de segurança, indique quais são **incorretas**:
A Confidencialidade consiste em garantir que as informações do sistema estarão criptografadas. Confidencialidade não se limita apenas à criptografia das informações. Ela envolve garantir que os recursos do sistema só podem ser consultados por usuários devidamente autorizados.
A Integridade consiste em garantir que as informações do sistema só poderão ser modificadas por usuários autorizados.
A Disponibilidade implica em assegurar que os recursos do sistema estarão disponíveis para consulta por qualquer usuário. Disponibilidade não implica que os recursos do sistema estarão disponíveis para consulta por qualquer usuário, mas sim para aqueles que tiverem direito de usá-los, a qualquer momento.
A Autenticidade implica em assegurar que os dados das entidades atuantes no sistema sejam verdadeiros e correspondam às informações do mundo real que elas representam.
A Irretratabilidade implica em garantir que nenhuma ação possa ser desfeita no sistema Irretratabilidade (ou não-repúdio) implica que todas as ações realizadas no sistema são conhecidas e não podem ser escondidas ou negadas por seus autores, mas isso não significa que nenhuma ação possa ser desfeita no sistema.

16. Qual das seguintes afirmações sobre a infraestrutura tradicional de registro de eventos dos sistemas UNIX é correta?
Os eventos recebidos pelo daemon syslogd são descritos por mensagens de texto e rotulados por suas fontes em serviços e níveis.
O daemon syslogd usa apenas um socket UDP para receber mensagens de eventos.

O daemon syslogd pode registrar eventos, mas não pode enviá-los a outros daemons em outros computadores.
O daemon syslogd não utiliza um arquivo de configuração para determinar o destino dos eventos recebidos.
A infraestrutura de registro de eventos em UNIX não permite que eventos sejam enviados a terminais ou ativem programas externos.