1 - Um pentest (ou teste de penetração) é um tipo de avaliação de segurança em que profissionais simulam ataques cibernéticos controlados a sistemas, redes ou aplicações, com o objetivo de identificar vulnerabilidades que poderiam ser exploradas por atacantes maliciosos. A ideia é encontrar e corrigir falhas antes que sejam usadas de forma maliciosa.

Etapas: Planejamento e Reconhecimento, Varredura e Enumeração, Ganho de Acesso, Escalada de Privilégio, Pós-Exploração, Relatório.

2 - Ataque de Negação de Serviço (DoS / DDoS)

O que é?

Um ataque que sobrecarrega um sistema, servidor ou rede, tornando-o indisponível para usuários legítimos.

Ataque de Exploração de Recurso (Fork Bomb / Lógica Maliciosa)

O que é?

Ataques que exploram recursos computacionais, como CPU e memória, criando processos em cascata ou loops infinitos**.**

Ataque de Ransomware com Encriptação de Sistemas Críticos

O que é?

Embora normalmente afete a confidencialidade e integridade, quando criptografa arquivos essenciais ao funcionamento do sistema, também afeta diretamente a disponibilidade.

3 - Compliance (ou compliance, em inglês) refere-se ao cumprimento de leis, regulamentos, políticas internas, obrigações contratuais e padrões aplicáveis. No contexto da segurança da informação, significa garantir que todas as práticas e controles estejam alinhados com os requisitos legais e normativos.

4 - Firewall: Foca no controle de tráfego entre redes, permitindo ou bloqueando pacotes com base em políticas predefinidas.

IDS: Detecta possíveis intrusões ou comportamentos anômalos e gera alertas, mas não interfere diretamente no tráfego.

IPS: Vai além do IDS, prevenindo ataques ao interromper ou bloquear pacotes de dados que são considerados maliciosos.

5 - Use senhas fortes, com letras maiúsculas, minúsculas, números e símbolos. Ative a autenticação em dois fatores (2FA). Evite reutilizar senhas e use um gerenciador de senhas.

6 - a) A vulnerabilidade**:**
Uso de uma cópia não original do sistema operacional Windows.

b) A ameaça:
Instalação de malwares, falhas de segurança não corrigidas e exposição a ataques devido à falta de atualizações e suporte oficial da Microsoft.

c) Uma ação defensiva para mitigar a ameaça:
Utilizar uma versão legítima e licenciada do sistema operacional, garantindo atualizações automáticas de segurança e suporte técnico confiável.

7 -a) A vulnerabilidade:
Uso de credenciais fracas, como nome de usuário e senha fáceis ou padrão (ex.: “admin/admin”).

b) A ameaça:
Acesso não autorizado ao sistema por meio de força bruta ou simples tentativa com credenciais comuns.

c) Uma ação defensiva para mitigar a ameaça:
Implementar políticas de senha forte, desabilitar usuários padrão (como “admin”), e usar autenticação multifator (MFA/2FA).

8 a) Para Bob: Ana cifra com a chave pública de Bob.

b) Bob decifra com sua chave privada.

c) Para Carlos: Ana cifra com sua própria chave privada (para assinar digitalmente).

d) Carlos verifica a assinatura com a chave pública de Ana.

9.a - O navegador (cliente) usa a chave pública do Banco (contida no certificado digital) para cifrar dados. O Banco decifra os dados com sua chave privada. Garante sigilo e autenticação do site.

9.b Autenticidade do site, prevenindo ataques como phishing.
Criptografia da comunicação, garantindo confidencialidade dos dados.

10. Tentativas de login (sucesso e falha). Acesso a arquivos ou sistemas sensíveis. Alterações em configurações de segurança.