**UC Sistemas Computacionais e Segurança – 2025.1**

- Júlia Helena Leite Nadal

-RA : 825141371

- Prof. Calvetti

Exercícios de Revisão

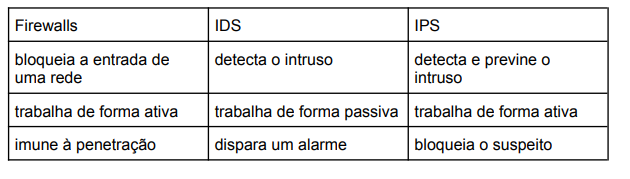
1. Um **pentest,** é uma simulação controlada de um ataque cibernético contra um sistema, rede ou aplicação com o objetivo de **identificar vulnerabilidades de segurança** que poderiam ser exploradas por invasores reais.

Etapas: Planejamento e reconhecimento, enumeração, ganho de acesso, escalada de privilégios, manutenção de Acesso, cobertura de Rastros, relatório.

1. Ataque DoS: o ataque vem de **vários dispositivos comprometidos**, dificultando a defesa, com objetivo de **sobrecarregar os recursos** (CPU, memória), fazendo com que o serviço fique **lento, indisponível ou caia completamente.**

Ransomware: Pode tornar **sistemas inteiros indisponíveis**, afetando hospitais, empresas, governos, etc. O atacante exige **resgate** ($) para liberar o acesso.

infraestrutura de rede (como DNS spoofing): Visam comprometer **serviços essenciais de rede**, como DNS (que traduz domínios para IPs) ou BGP (que controla o tráfego entre roteadores da internet). Podem redirecionar tráfego ou simplesmente **tornar sites e serviços inacessíveis.**

1. Conformidade, em inglês é conhecido como compliance.
2. 
3. Criar senhas fortes, com letras, números e símbolos.

Evitar usar a mesma senha em vários sites.

Ativar a verificação em duas etapas sempre que possível.

1. a) O uso de um sistema operacional não original (pirata), isso pode ter falhas de segurança, ausência de atualizações e deixar o computador exposto a riscos.

b) Possibilidade de ataques, como vírus, malwares ou roubo de dados, justamente por causa da falta de proteção em um sistema pirata.

c) Instalar uma versão original do Windows e manter o sistema sempre atualizado, além de usar antivírus confiável.

1. a) Uso de nome de usuário padrão (admin), que é fácil de adivinhar.

b) Invasores podem acessar o sistema usando essas credenciais conhecidas.

c) Trocar o nome de usuário e senha padrão por credenciais fortes e personalizadas.

1. A- Ana deve cifrar a mensagem usando a chave pública de Bob(criptografia assimétrica). B- Bob deve usar sua chave privada para decifrar a mensagem (criptografia assimétrica). C- Ana deve usar sua chave privada para cifrar a mensagem (criptografia assimétrica). D-Carlos deve usar a chave pública de Ana para decifrar a mensagem (criptografia assimétrica).
2. A-Na origem se usa a chave privada para decifrar/descriptografar mensagens e dados e no destino a chave pública é usada para cifrar a mensagem. São usadas chaves públicas e privadas(combinação de chave simétrica e assimétrica) B-1=Mais tranquilidade e segurança de ambos os lados. 2=Certeza de que quem está efetuando a transação é o Banco do Brasil
3. 1-Horário de atividade em cada site acessado. 2-Erros e falhas cometidas. 3-Modificação de dados.

**Estudo do caso 1, aula 7.**

1. O firewall e o servidor Web usados pela Linen Planet fornecem serviços de criptografia?Em caso afirmativo, que tipo de proteção estava em vigor?

Sim, o firewall e o servidor web utilizados pela Linen Planet oferecem **serviços de codificação de dados**. A segurança aplicada nesse cenário consiste em **transformar as informações em formatos ilegíveis** para qualquer pessoa que não possua a **chave da criptografia**, resultando em **mensagens cifradas**. Isso assegura a **proteção dos dados enquanto trafegam pela rede**, impedindo **espionagem, garantindo a integridade** assim, evitando que as informações sejam modificadas durante a transmissão e permitindo a **verificação da identidade do servidor**, garantindo que Maris está de fato se conectando ao servidor legítimo da Linen Planet e **não a um site falso**, desde que o **certificado digital seja confiável.**

1. Como o acesso ao servidor Web da Linen Planet poderia ser mais seguro?

O acesso ao servidor web da Linen Planet poderia ser **mais protegido** se fossem implementadas soluções como **autenticação baseada em múltiplos fatores**, incluindo o que o usuário **sabe** (como uma senha), **possui** (como um token ou dispositivo) e **é** (como impressões digitais ou reconhecimento facial). Além disso, o uso de **honeypots** , sistemas criados para **atrair atacantes e desviá-los de recursos críticos**, além de possibilitar a **coleta de dados sobre suas ações** também contribuiria para a segurança. Outro cuidado importante seria **evitar o compartilhamento de senhas,** seja por telefone ou presencialmente, principalmente em **ambientes públicos.**

**Estudo do caso 2, aula 7.**

1. A política da ATI sobre o uso da Web parece dura para você? Por que ou por que não?

Não, porque se o funcionário fosse vítima de um malware, como um ataque de phishing, isso poderia resultar em uma invasão aos sistemas da empresa, causando grandes prejuízos financeiros. Um ato aparentemente inofensivo, como buscar passagens de viagem para as férias, poderia acabar expondo a organização a riscos sérios de segurança e possíveis perdas econômicas significativas.

1. Você acha que Ron foi justificado em suas ações?

Não, porque ele tinha conhecimento das diretrizes da empresa e ainda assim optou por desrespeitá-las, realizando uma ação sem autorização. Mesmo que aparentemente sem causar danos, o acesso ainda foi indevido.

1. Como Andy deve reagir a essa situação se Ron é conhecido por ser um funcionário confiável e diligente?

Andy deve lidar com a situação de forma justa, compreensiva e responsável, levando em conta tanto o comportamento anterior de Ron quanto as normas internas da empresa. Ele pode chamar Ron para uma conversa reservada e calma, buscando esclarecer a situação. Além disso, pode aproveitar o caso como um exemplo educativo para reforçar com toda a equipe a importância do uso adequado da internet no ambiente corporativo, e ainda sugerir que Ron participe de treinamentos ou capacitações, como mencionado no texto.