1 Cenário de Infraestrutura e NetFlow

Contexto: O administrador de rede da UFRJ monitora o tráfego usando o *NfSen*. Durante o período de inscrições em disciplinas, ele observa anomalias no backbone da universidade e precisa agir para manter a tríade da segurança.

Tarefa: Preencha a tabela abaixo classificando qual pilar da segurança da informação (**Confidencialidade**, **Integridade** ou **Disponibilidade**) foi comprometido em cada situação, apresentando a justificativa baseada nos conceitos da disciplina (Considere as definições de Integridade de Origem e de Sistema).

Ação do Usuário/Atacante	**Pilar Comprometido**	**Justificativa**
Um ataque DDoS inunda o link de internet, impedindo o acesso ao portal.		
Um "Sniffer" na rede consegue ler os pacotes de login em texto claro.		
Um invasor envia comandos ao roteador fingindo ser o administrador da rede.		
Um vírus modifica o firmware do roteador para desviar o tráfego sem ninguém saber.		
Um usuário solicita a exclusão de seus logs de navegação baseando-se no controle sobre seus próprios dados.		
Um analista utiliza o *nfdump* para identificar um pico anômalo de tráfego que desviou do modelo estatístico usual.		
Um rompimento de fibra óptica externa deixa o campus sem conexão com o *backbone* central.		
Um aluno altera o *hash* SHA-256 no site oficial para que aponte para um instalador malicioso baixado por outros.		

Gabarito: Cenário de Infraestrutura e NetFlow

Ação do Usuário/Atacante	**Pilar**	**Justificativa**
Um ataque DDoS inunda o link de internet, impedindo o acesso ao portal.	**Disponibilidade**	O serviço foi negado aos usuários autorizados devido à sobrecarga intencional dos recursos (Negação de Serviço).
Um "Sniffer" na rede consegue ler os pacotes de login em texto claro.	**Confidencialidade**	Informações privadas (credenciais) foram divulgadas a indivíduos não autorizados por falta de criptografia.
Um invasor envia comandos ao roteador fingindo ser o administrador da rede.	**Integridade (Autenticidade)**	Violação da integridade da origem. O sistema aceita uma fonte ilegítima como se fosse a fonte legítima (Admin).
Um vírus modifica o firmware do roteador para desviar o tráfego sem ninguém saber.	**Integridade (Sistema)**	O hardware deixa de desempenhar sua função prevista de forma íntegra devido a uma manipulação não autorizada.
Um usuário solicita a exclusão de seus logs de navegação (controle sobre dados).	**Confidencialidade (Privacidade)**	Refere-se ao direito e controle do indivíduo sobre quais informações relacionadas a ele são armazenadas ou divulgadas.
Um analista utiliza o *nfdump* para identificar um pico anômalo de tráfego.	**Integridade (Detecção)**	Uso de mecanismos de detecção para verificar se o sistema ou os dados foram comprometidos por ações anômalas.
Um rompimento de fibra óptica externa deixa o campus sem conexão.	**Disponibilidade**	Incapacidade de acessar o recurso desejado no momento necessário, independentemente de a causa ser acidental ou proposital.
Um aluno altera o *hash* SHA-256 no site oficial para apontar para um vírus.	**Integridade (Dados)**	O conteúdo da informação original (o valor de verificação) foi alterado indevidamente, enganando a confiança do usuário.

2 Cenário: Sistemas Críticos e Controle de Acesso

Contexto: Uma universidade gerencia tanto o sistema acadêmico quanto o sistema de prontuários dode seu hospital universitário. Ambos lidam com dados sensíveis que exigem diferentes níveis de proteção e permissões de acesso baseadas em funções (RBAC).

Tarefa: Preencha a tabela abaixo classificando qual pilar da segurança da

informação (**Confidencialidade**, **Integridade** ou **Disponibilidade**) tem mais sentido com o cenário exposto.

Ação do Usuário/Atacante	**Pilar**	**Justificativa**
Um aluno consegue acessar o banco de dados e alterar sua nota de 5.0 para 9.0 sem rastro.		
A Professora Maria visualiza a lista de notas de todos os alunos da sua turma de Cálculo II.		
Um médico apaga acidentalmente o histórico de alergias de um paciente devido a um erro de interface.		
O sistema de prontuários fica lento e impede que enfermeiros consultem dosagens de remédios.		
Um técnico de TI, sem autorização médica, acessa o laudo de uma biópsia de um paciente famoso.		
O sistema registra automaticamente que a nota foi lançada pela "Professora Ana" às 14:30.		
Um hacker sequestra os dados do hospital (Ransomware), impedindo qualquer acesso aos exames.		
Um aluno tenta acessar o boletim de outro colega, mas o sistema bloqueia a visualização.		

Gabarito: Cenário de Sistemas Críticos

Situação	Pilar	Justificativa
Um aluno consegue acessar o banco de dados e alterar sua nota de 5.0 para 9.0 sem rastro.	**Integridade**	Violação da integridade dos dados, pois o conteúdo foi modificado de maneira não autorizada.
A Professora Maria visualiza a lista de notas de todos os alunos da sua turma de Cálculo II.	**Confidencialidade**	Pilar exercido corretamente via RBAC; o professor tem o "necessário saber" sobre sua turma.
Um médico apaga acidentalmente o histórico de alergias de um paciente devido a um erro de interface.	**Integridade**	Perda da confiabilidade dos dados e falha do sistema em preservar a informação íntegra.
O sistema de prontuários fica lento e impede que enfermeiros consultem dosagens de remédios.	**Disponibilidade**	A informação não está acessível no momento necessário, gerando riscos operacionais e clínicos.
Um técnico de TI, sem autorização médica, acessa o laudo de uma biópsia de um paciente famoso.	**Confidencialidade**	Violação de privacidade. O técnico não possui o perfil de acesso médico para visualizar o dado.
O sistema registra automaticamente que a nota foi lançada pela "Professora Ana" às 14:30.	**Integridade**	Garante a autenticidade e a integridade da origem através de trilhas de auditoria.
Um hacker sequestra os dados do hospital (Ransomware), impedindo qualquer acesso aos exames.	**Disponibilidade**	Impacto total na disponibilidade, pois o serviço é negado aos usuários autorizados.
Um aluno tenta acessar o boletim de outro colega, mas o sistema bloqueia a visualização.	**Confidencialidade**	Pilar preservado. O controle de acesso impede a divulgação de dados a terceiros não autorizados.

3 Avaliação de Sequências Pseudoaleatórias (PRNG)

Contexto: A robustez de um sistema criptográfico depende frequentemente da qualidade de seus geradores de números pseudoaleatórios (PRNG). Para garantir que uma sequência de bits não seja previsível, o NIST define o padrão *SP 800-22* com uma bateria de testes estatísticos.

Questão: Com base nos testes de aleatoriedade do NIST discutidos em aula, responda aos itens abaixo:

- **A) Motivação**: Por que não podemos simplesmente confiar que uma função matemática gera números aleatórios? Qual o objetivo de aplicar

testes de aleatoriedade?

- **B) Metodologia de Teste**: Descreva, de forma simplificada, como um administrador de segurança testaria uma sequência de 1 milhão de bits? Quais testes ele deve usar?
- **C) Interpretação**: Se uma sequência passa no Teste de Frequência, mas falha em um outro teste, ela pode ser considerada aleatória? Justifique.