Sistemas Computacionais e Segurança

Aula 07

Estudo de casos 1

• 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 é o servidor web da Linen Planet oferecem criptografia. Essa proteção transforma as informações em códigos que só podem ser entendidos por quem tem a chave certa. Isso evita espionagem, garante que os dados não sejam modificados durante o envio e confirma que a Maris está se conectando ao site verdadeiro da Linen Planet, e não um falso – desde que o certificado esteja válido

• 2: Como o acesso ao servidor Web da Linen Planet poderia ser mais seguro?

- A segurança do servidor web da Linen Planet poderia ser reforçada com métodos de autenticação que envolvem algo que a pessoa sabe (como senhas), algo que ela possui (como um token ou celular) e algo que ela é (como impressão digital). Também seria útil usar honeypots — sistemas criados para distrair e estudar invasores, mantendo os dados reais protegidos. Além disso, é importante evitar passar senhas por telefone ou pessoalmente, principalmente em locais públicos.

Estudos de casos 2

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

- Não , pois se o funcionário acessasse um site malicioso, como um de phishing, a empresa poderia sofrer sérias consequências. Um simples acesso para buscar passagens de férias poderia abrir brechas de segurança, resultando em invasões e até prejuízos financeiros consideráveis.

• 2: Você acha que Ron foi justificado em suas ações ?

- Não. Ele violou as políticas de segurança ao acessar sites não autorizados, colocando a empresa em risco.

• 3: Como Andy deve reagir a essa situação se Ron é conhecido por ser um funcionário confiável e diligente?

- Andy deve abordar a situação de forma construtiva, explicando a importância das políticas de segurança e reforçando as regras. Dado que Ron é confiável, uma conversa explicativa e o incentivo para participar do curso de uso adequado da internet seriam abordagens adequadas.

Sistemas Computacionais e Segurança

Lista de exercícios –

• 1: O pentest é uma análise de segurança que simula uma invasão virtual para identificar falhas. Suas fases incluem: preparação e coleta de informações, identificação e avaliação de vulnerabilidades, obtenção de acesso, permanência no sistema, eliminação de vestígios e elaboração do relatório final.

• 2:

1. DDoS (Ataque Distribuído de Negação de Serviço): Envia uma grande quantidade de tráfego para sobrecarregar o sistema, tornando-o inacessível.
2. Ransomware: Bloqueia o acesso aos dados ou sistemas até que um resgate seja pago, interrompendo totalmente o serviço.
3. Ataque de Exploração de Falhas (Exploit): Usa vulnerabilidades para travar ou desligar sistemas, impedindo seu funcionamento normal.

• 3: Compliance

• 4:

|  |  |  |
| --- | --- | --- |
| Firewall | IDS | IPS |
| Bloqueia a entrada de uma rede | Detecta o intruso | Detecta e previne o intruso |
| Trabalha de forma ativa | Trabalha de forma passiva | Trabalha de forma ativa |
| Imune a penetração | Dispara um alarme | Bloqueia o suspeito |

• 5: 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.

• 6: A-O windows utilizado na máquina é falso.

B-Malwares escondidos dentro desse windows.

C-O uso de anti vírus

• 7: A-Utilização de um nome de usuário padrão conhecido.

B-O invasor pode usar a força bruta ou a utilização de credenciais padrões para

acessar a interface.

C-Alteração do nome de usuário e a autenticação de 2 fatores.

• 8: A - Ana deve criptografar a mensagem com a chave pública de Bob, garantindo que só ele possa decifrar.

B- Bob usará sua chave privada para descriptografar a mensagem, já que foi cifrada com sua chave pública.

C- Ana deve assinar digitalmente a mensagem usando sua chave privada, provando que foi ela quem enviou.

D- Carlos usará a chave pública de Ana para verificar a assinatura digital e confirmar a autoria da mensagem.

Sistemas Computacionais e Segurança

• 9: A – No envio, utiliza-se a chave pública para criptografar os dados, enquanto no recebimento, a chave privada é usada para decodificar a informação. Essa técnica combina criptografia simétrica e assimétrica para reforçar a proteção.

B1- Garante maior confiança e proteção para ambas as partes envolvidas.

B2- Permite confirmar que a operação está realmente sendo realizada pelo Banco do Brasil.

• 10: 1-Horário de atividade em cada site acessado.

2-Erros e falhas cometidas.

3-Modificação de dados.

Giovana Ayumi Nakano

Ra: 825110732