UNIVERSIDADE SÃO JUDAS TADEU

Emilly dos santos ferreira
RA: 825153657

Sistemas computacionais e segurança

Atividade aula 07

Professor Robson Calvetti

Sao Paulo - 2025

Questões estudo de caso 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?

Resposta: Sim fornecem, o tipo de proteção que estava em vigor entre o servidor e o firewaal como o próprio texto menciona é a criptografia

---

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

Resposta: Acredito que autenticação em dois fatores seria o ideal.

Questões estudo de caso 2

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

Resposta: Não me parece dura, é para a segurança, pode ser que ela seja bem rígida, mas pra segurança vale tudo.

---

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

Resposta: Mesmo ele tendo finalizado o trabalho e feito a pesquisa após, não é justificado, pois ele tem noção que a segurança da empresa e dele estão em jogo.

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

Resposta: Conversando e fazendo treinamento para que não ocorra mais esse tipo de situação.

EXERCICIOS /RESPOSTAS

1 - Basicamente são os crackers, eles fazem simulações de ataques para que as empresas possam se proteger contra os hackers que fazem o ato na maldade. As etapas são planejamento, varredura para ver as vulnerabilidades, exploram as falhas e manutenção do acesso.

---

2 - Ataque DdoS, aquele ataque que junta vários computadores pra derrubarem um site por exemplo, o ransomware que é um vírus maligno que rouba os dados e o próprio usuário que talvez seja o pior de todos, aquela pessoa que tem acesso a tudo na empresa e pode acabar com a empresa.

---

3 - Conformidade mais conhecido como compliance

Questao 4

Recurso	Função principal	Ponto forte	Limitação
Firewall	Filtrar pacotes e conexões entre redes	Bloqueio/permitir tráfego conforme regras	Não detecta ataques "por dentro" (aplicação)
IDS (Intrusion Detection System)	Monitorar tráfego e gerar alertas em caso de anomalias	Identifica invasões e padrões maliciosos	Passivo: só avisa, não bloqueia
IPS (Intrusion Prevention System)	Detectar e **bloquear** ativamente tráfego malicioso	Alerta + resposta automática (drop de pacote)	Pode gerar falsos positivos e interromper serviço

5 - Autenticação em dois fatores, usar senhas diferentes nos sites e usar um gerenciador de senhas..

---

6 - a) **vulnerabilidade:** o Windows é falso
b) **Ameaça:** é um vírus e pode roubar os dados se caso for utiliizado
c) **Ação defensiva:** usar o Windows original

---

7 - a) **vulnerabilidade:** a senha parece fraca
b) **Ameaça:** facil acesso a algum invasor
c) **Ação defensiva:** colocar uma senha mais forte

---

8 - a) cifra a mensagem com a chave pública de Bob
b) decifra com a sua chave privada
c) gera assinatura digital usando sua chave privada sobre a mensagem.
d) verifica/decifra a assinatura com a chave pública de Ana, confirmando que foi ela mesma.

---

9 - a)Origem (servidor BB): o servidor envia ao cliente o certificado, que contém sua chave pública e assinatura da autoridade certificadora.
Destino (navegador): o browser valida a assinatura, extrai a chave pública e a usa para trocar a chave simétrica da sessão TLS (criptografia de canal)

b) **1.** Autenticação do servidor: você tem certeza de que está falando com o site legítimo do bb.
2. Confidencialidade e integridade: todo o tráfego fica protegido contra espionagem e alterações por terceiros

10. 1 - Logs de autenticação e falhas de login (quem tentou entrar, quando e de onde).
2 - Alterações de privilégios/configurações (elevações de permissão, mudanças em contas).
3 - Acesso a recursos críticos (arquivos sensíveis, bancos de dados, consoles de administração).

OBRIGADA

*Em algumas questões recorri a ajuda do chat gpt