Atividade 1,2 e 3 Professor Calvetti
Vitor Bernardes

RA:825138944

Estudo de caso 1

1: O firewall e o servidor Web usados pela Linen Planet fornecem serviços de criptografia?

R: Sim, é possivel notar isso “Ela notou que o ícone de segurança estava aparecendo na parte inferior da janela do navegador. A criptografia entre seu navegador e o servidor estava agora em vigor.”

Esse ícone de segurança geralmente representa o uso de HTTPS, que indica que uma conexão segura com criptografia.

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

R: Não compartilhar senhas por telefone ou verbalmente em público

Isso expôs as credenciais de Padma a qualquer pessoa próxima, como Maris.

Solução: Use autenticação multifator e comunique-se por canais seguros com criptografia

Uso de autenticação multifator (MFA)

Mesmo que Maris tivesse o usuário e a senha, ela não conseguiria acessar sem o segundo fator, como um código enviado por SMS ou app autenticador.

Estudo de caso 2

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

R: Motivos em que a política faz sentido:

Segurança cibernética: Restringir acesso reduz o risco de malware e ataques via sites maliciosos.

Produtividade: Limitar o uso recreativo evita que o tempo de trabalho seja usado para navegação pessoal.

Conformidade com normas: Muitas empresas precisam seguir normas de conformidade e auditoria, que exigem controle rigoroso do tráfego de internet.

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

R: Um pouco dos dois, Ele trabalhava há 6 meses em um projeto difícil e tinha acabado de concluir sua parte, mas ele sabia que a ATI tinha uma política clara de bloqueio via proxy, e mesmo assim tentou várias vezes burlar a restrição, além de ter sido alertado por uma mensagem clara ("ACESSO PROIBIDO") e continuar tentando pode ser visto como intencionalidade.

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

R: Conversar diretamente com Ron para entender o contexto e confirmar que foi realmente ele quem tentou acessar os sites.

Reconhecer o histórico positivo de Ron e destacar que confia nele, mas lembrar que mesmo boas intenções podem causar problemas em ambientes controlados.

Exercícios de Revisão

1: O que é um pentest? Quais são as etapas de um pentest?

R: Pentest (ou Penetration Test, teste de penetração) é uma simulação controlada de ataque a sistemas, redes ou aplicações com o objetivo de encontrar vulnerabilidades antes que atacantes reais as explorem.

Enumeração e Análise de Vulnerabilidades.

Mapear portas, serviços e sistemas operacionais.

Identificar vulnerabilidades conhecidas.

Tentar explorar vulnerabilidades para obter acesso não autorizado.

Escalar privilégios, manter acesso e verificar o impacto do ataque.

2: Explique o funcionamento de 3 ataques que comprometem a DISPONIBILIDADE de sistemas.

R: A. Ataque DoS (Denial of Service)

Enche um servidor com tráfego ou solicitações até ele travar ou ficar inacessível.

B. Ataque DDoS (Distributed DoS)

Similar ao DoS, mas coordenado por milhares de dispositivos zumbis (botnets), tornando o ataque mais difícil de conter.

C. Ataque de Exploração de Recursos (Fork Bomb, por exemplo)

Cria processos em cascata que consomem toda a CPU e memória do sistema, tornando-o inutilizável.

3: De qual conceito o texto fala?

R: O conceito é: Compliance

4: Quadro comparativo: Firewall vs IDS vs IPS

Recurso	Função Principal	Atua de forma ativa/passiva	Atua em que camada	Exemplo de ação
Firewall	Controla o tráfego de entrada/saída com base em regras	Ativa	Camada de rede/transport	Bloquear porta 22 (SSH)
IDS (Intrusion Detection System)	Monitora tráfego e detecta comportamentos suspeitos	Passiva	Camada de aplicação/redes	Gera alerta sobre ataque SQL Injection
IPS (Intrusion Prevention System)	Detecta e impede ataques automaticamente	Ativa	Camada de aplicação/redes	Bloqueia ataque de força bruta em tempo real

5: Três conselhos para proteger senhas

A. Use senhas fortes e únicas

Misture letras maiúsculas, minúsculas, números e símbolos.

Nunca use a mesma senha em vários serviços.

B. Ative a autenticação de dois fatores (2FA)

Mesmo que a senha seja descoberta, o acesso ainda estará protegido.

C. Use um gerenciador de senhas confiável

Eles criam e armazenam senhas seguras para você.

6:

A. A vulnerabilidade

O uso de um sistema operacional não original ou falsificado, que pode não receber atualizações de segurança, correções de bugs ou suporte oficial.

B. A ameaça

A possibilidade de o sistema estar comprometido por malwares, brechas de segurança ou softwares maliciosos, explorando a falta de atualizações e validação oficial

C. Uma ação defensiva para mitigar a ameaça

Regularizar o sistema operacional, adquirindo uma cópia original e licenciada do Windows, garantindo acesso a atualizações e suporte oficial.

7:

A. Vulnerabilidade

A senha e o nome de usuário são curtos e fáceis de serem invadidos.

B. Ameaça

O alto risco de invasão devido a vulnerabilidade

C. Uma ação defensiva para mitigar a ameaça

Alterar o nome de usuário e a senha para algo maior e menos previsível, impedindo assim, a facilidade de invasão.

8:

A. Como Ana deverá cifrar a mensagem para Bob:

Ana deve criptografar a mensagem com a chave pública de Bob.
Somente Bob poderá decifrar essa mensagem, pois só ele tem a chave privada correspondente.

B. Como Bob deverá decifrar a mensagem de Ana corretamente:

Bob deve usar sua chave privada para decifrar a mensagem que Ana criptografou com sua chave pública.

C. Como Ana deverá cifrar a mensagem para Carlos:

Ana deve criptografar a mensagem com a sua própria chave privada.
Isso é equivalente a uma assinatura digital: qualquer pessoa pode verificar a mensagem, mas só Ana poderia tê-la assinado.

D. Como Carlos deverá decifrar a mensagem de Ana corretamente:

Carlos deve usar a chave pública de Ana para verificar/decriptar a mensagem.
Se a descriptografia for bem-sucedida, ele sabe que foi Ana quem enviou, pois só a chave pública dela conseguiu abrir a mensagem.

9:

A. Como se dá a utilização do certificado na origem e no destino? Identifique como são utilizadas as chaves criptográficas do Banco do Brasil.

O certificado digital do Banco do Brasil serve para autenticar sua identidade digital perante os usuários e garantir a segurança da comunicação.

Na origem (servidor do Banco):
O servidor apresenta seu certificado digital, que contém sua chave pública e é assinado por uma Autoridade Certificadora (AC) confiável (neste caso, a Sectigo RSA Extended Validation Secure Server CA).

B. Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco.

Confidencialidade dos dados:

As informações trocadas (como senhas, dados bancários) são criptografadas e não podem ser lidas por terceiros durante a transmissão.

Autenticidade do servidor:

O certificado garante que o site realmente pertence ao Banco do Brasil, evitando ataques como phishing.

10: 3 registros importantes das atividades dos usuários

A. Registros de login e logout

Incluem data, hora, ID do usuário e local de acesso.

Importantes para rastrear quando e onde o usuário acessou o sistema.

B. Acesso a arquivos e sistemas sensíveis

Registro de quais arquivos, sistemas ou recursos o usuário acessou.

Indica se o usuário consultou ou alterou dados críticos ou confidenciais.

C. Tentativas de acesso não autorizado ou falhas de autenticação

Mostram tentativas de login com senhas incorretas ou acesso a áreas restritas.

Podem indicar tentativa de ataque interno ou comprometimento da conta.