Atividades Professor Calvetti- Davi Emanuel Silva Adriano 823149648

ATIVIDADE LAB7

ATIVIDADE 1

Lista de Exercícios

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

Um pentest é um teste feito por profissionais para verificar se um sistema está vulnerável a ataques. Eles simulam invasões reais para encontrar brechas.
As etapas são:

- Varredura: identificar serviços e falhas.
- Escalação de privilégios: tentar acessar áreas mais restritas.
- Ocultação: testar se é possível esconder a presença dentro do sistema.
- Exploração: tentar invadir usando essas falhas.

2) Explique o funcionamento de 3 ataques de segurança cibernética que podem comprometer diretamente a DISPONIBILIDADE de sistemas.

SYN Flood: envia muitos pedidos falsos para travar o servidor.
DDoS: vários computadores atacam ao mesmo tempo, derrubando o serviço.
Ransomware: bloqueia o acesso ao sistema e exige pagamento para liberar.

3) Leia o fragmento de texto a seguir.

Todas as empresas devem observar a legislação local, os seus regulamentos internos e as obrigações contratuais, além

dos acordos internacionais. Os requisitos de segurança que uma empresa deve cumprir estão fortemente relacionados a isso. (HINTZBERGEN, 2018)

O texto acima se refere a um conceito que pode ser considerado importante quando se trata de segurança da informação. De qual conceito estamos falando (em uma palavra)?

Conformidade.

4) Existem vários recursos de software e hardware para estabelecer diversos níveis de segurança em uma rede de computadores. Entre outros, podemos citar os firewalls e os sensores (IDS e IPS). Faça um quadro comparativo resumindo as características de cada um dos três recursos.

-Firewall:

Função Principal: Controla o que entra e sai da rede

Ação: Bloqueia com base em regras

Detecta Novos Ataques? Não

-IDS:

Função Principal: Detecta atividades suspeitas

Ação: Gera alertas

Detecta Novos Ataques? Sim

-IPS:

Função Principal: Detecta e bloqueia ataques em tempo real

Ação: Bloqueia automaticamente

Detecta Novos Ataques? Sim

5) Uma pessoa lhe procura e pede ajuda sobre formas de proteger as suas senhas. Cite pelo menos três conselhos que você daria a essa pessoa.

Criar senhas fortes, misturando letras, números e símbolos.
Evitar usar dados pessoais fáceis de adivinhar.
Usar autenticação em duas etapas para aumentar a segurança.

6) Observe a imagem a seguir. Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

Sistema operacional falsificado instalado.

b) A ameaça

Possibilidade de infecção por malware; instabilidade e baixo desempenho no futuro.

c) Uma ação defensiva para mitigar a ameaça

Instalando cópias legítimas e retirando as falsificadas.

7) Observe a imagem a seguir. Do ponto de vista da segurança da informação, identifique:

a) A vulnerabilidade

O uso de credenciais fracas, como o nome de usuário "Admin", que é padrão em muitos sistemas, representa uma falha de segurança.

b) A ameaça

Isso facilita para que um atacante, como um cracker, consiga descobrir a senha e invadir o sistema.

c) Uma ação defensiva para mitigar a ameaça

Uma medida de segurança seria renomear os usuários com privilégios administrativos para nomes exclusivos, tornando mais difícil o acesso não autorizado.

8) Ana tem duas mensagens para enviar de forma criptografada para dois amigos: Bob e Carlos. Bob deseja receber a mensagem de maneira que apenas ele possa decifrá-la. Carlos não está preocupado com o sigilo da mensagem, mas deseja ter certeza de que foi mesmo Ana que a enviou. Assuma que todos têm seu par de chaves pública e privada, que todas as chaves públicas são acessíveis. Visando a atender os requisitos de Bob e Carlos, descreva, em termos de uso das chaves:

a) como Ana deverá cifrar a mensagem antes de enviar para Bob;

Com a chave pública de Bob.

b) como Bob deverá decifrar a mensagem de Ana corretamente;

Com a sua chave privada.

d) como Ana deverá cifrar a mensagem antes de enviar para Carlos;

Com a sua chave privada.

e) como Carlos deverá decifrar a mensagem de Ana corretamente.

Com a chave pública de Ana.

9) Observe as imagens a seguir. Com base nelas, responda:

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.

A CA Serctigo cria um resumo dos dados de identificação do Banco utilizando uma função HASH. Esse resumo é então criptografado com a chave privada do Banco,

gerando uma assinatura digital. Para validar essa assinatura, o cliente do banco usa a chave pública do Banco, que está no certificado, para decifrá-la. Depois, o cliente recalcula o HASH da mensagem recebida. Se o HASH calculado coincidir com o valor decifrado da assinatura, a mensagem é considerada válida.

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

Autenticação da origem: O certificado digital garante que as mensagens realmente foram enviadas pelo Banco do Brasil, como indicado no certificado.
Integridade: Ele assegura que as mensagens recebidas do Banco não foram alteradas, seja de forma acidental ou intencional.
Não-repúdio: Também garante que o Banco não pode negar ou refutar o envio das mensagens, já que elas estão assinadas digitalmente.

10) Observe a imagem a seguir:

De acordo com a norma ISO 27002: 2013, "convém que registros (log) de eventos das atividades do usuário, exceções, falhas e eventos de segurança da informação sejam produzidos, mantidos e analisados criticamente, a intervalos regulares". ABNT (2013).

Cite 3 registros importantes da atividade dos usuários que podem registrados para posterior auditoria de segurança.

- Identificação dos usuários (ID): Registrar qual usuário está acessando o sistema é essencial para rastrear atividades específicas e garantir que somente pessoas autorizadas tenham acesso.
- Datas, horários e detalhes de eventos-chave: É importante registrar o horário de entrada (log-on) e saída (log-off) no sistema, além de eventos importantes que ocorrem durante a utilização do sistema. Esses registros ajudam a identificar acessos suspeitos ou comportamentos irregulares.
- Tentativas de acesso ao sistema (aceitas e rejeitadas): Monitorar e registrar as tentativas de login, tanto bem-sucedidas quanto falhas, permite detectar

atividades suspeitas, como tentativas de ataques de força bruta ou acesso não autorizado.

ATIVIDADE 2 ESTUDO DE CASO 1

Questões

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 fornecem criptografia. Isso é indicado pelo ícone de segurança no navegador, que geralmente representa o uso de SSL/TLS, um protocolo que protege os dados trocados entre o navegador e o servidor.

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

O acesso poderia ser mais seguro com autenticação multifatorial (MFA), onde além da senha, seria necessário um segundo fator de verificação, como um código enviado por SMS ou gerado por um aplicativo.

ATIVIDADE 2 ESTUDO DE CASO 2

Questões

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

Sim, a política parece dura, mas é necessária para proteger a rede da empresa e garantir que a navegação esteja alinhada com os objetivos da ATI. A rede não deve ser usada para atividades pessoais ou fora do escopo do trabalho.

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

Não, Ron não foi justificado. Ele sabia que a ATI não permite a navegação indiscriminada na Web e que o uso de um servidor proxy restringe o acesso a sites não autorizados. Ele deveria ter seguido a política.

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

Andy poderia dar uma advertência a Ron e, dependendo da situação, sugerir uma conversa sobre o uso adequado da rede. Dado que ele é confiável, um curso sobre uso adequado da Internet ou reforço na política de segurança seria mais adequado do que uma punição severa.