Sistemas Computacionais e Segurança

Exercícios de Revisão e análise de estudo de caso

Professor: Robson Calvetti

Annely Desireé Jünemann – R.A: 824217739

Larissa da Silva Maschio – R.A: 824221401

ANO 2024.1

Fontes de estudo principais

- Material curado da UC Sistemas Computacionais e Segurança no U-Life

- Curso Cisco Fundamentos de Segurança Cibernética

- Material das aulas

Questões

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

Pentest é a tradução de *Penetration Test*, traduzindo teste de intrusão. Nada mais que avalia a segurança do sistema/redes, no qual simula ataques cibernéticos, tentando em diferentes ativos, como: *Web, Mobile, cloud, smart contract,* redes internas e externas, fusões, aquisições, dispositivos IoT e APIs;

Etapas:

- Coletar Informações: Entender as necessidades e particularidades do negócio e dos ativos que serão testados;
- Planejamento: Momento em que é definido o escopo, com base nas informações levantadas;
- Identificação exploração de vulnerabilidade: Onde se iniciados os testes propriamente dito, em busca de brechas na aplicação;
- Relatório: é a entrega com detalhes sobre a vulnerabilidade e as recomendações (proposta) para a correção;
- Mitigação: Responsabilidade da empresa (responsável pela equipe, corrigir as vulnerabilidades encontradas no teste;
- Reset: Realização der novos teste, com o objetivo de analisar se foram feitas as correções, assim eliminando a vulnerabilidade.

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

DoS: É um tipo de ataque, no qual inunda um computador ou rede;

Phishing: Visa obter informações confidenciais de uma pessoa ou empresa, O *cracker* fingi ser uma pessoa ou empresa idônea, enviando mensagens ou *e-mail*, que há um *link* para acessar no qual é um ambiente falso.

Ataques baseando em IoT: Seu foco é atingir um dispositivo ou rede de internet das coisas (IoT). Com a propagação desses dispositivos nas empresas, é uma preocupação cada vez maior. Quando o *cracker* assume o controle do dispositivo, rouba dados ou usa o dispositivos afetados para deixar o ataque de DDoS mais robusto.

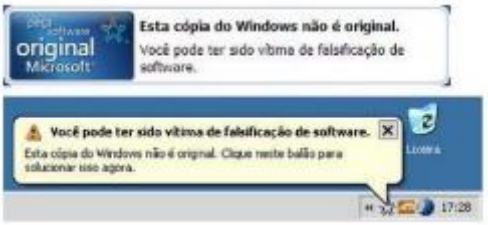
3) **Leia o fragmento de texto a seguir.**
Todas as empresas devem observar a legislação local, os seus regulamentos internos e as obrigações contratuais, além dos acordos internacionais. Os requisitos de segurança que uma empresa deve cumprir estão fortemente relacionados a isso. (HINTZBERGEN, 2018)
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)?
O base da análise do texto, o conceito sendo dito é sobre conformidade, onde há a necessidade de seguir leis, regulamentos, normas internas e obrigações, para garantir que a segurança da informação e que seja atendido conforme o padrão exigido por cada empresa.

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.**

	IDS	IPS	Firewall
Finalidade	Monitora o tráfego em busca de atividades maliciosas ou violações de políticas e envia alertas ao detectar.	Detecta, classifica e inspeciona o tráfego. Impede tráfego malicioso.	Dispositivo de segurança de rede que filtra o tráfego de entrada e saída com base em regras predeterminadas.
Funcionamento	Detecta o tráfego em tempo real e procura por anomalias ou assinaturas de ataque e gera alertas sobre as ameaças.	Inspeciona o tráfego em tempo real e procura por anomalias ou assinaturas de ataque e bloqueia as ameaças.	Filtra o tráfego baseado em endereçamento IP, portas e protocolos.
Configuração	Elemento de rede (como uma estação de trabalho) para monitoramento e detecção. Recebe uma cópia do tráfego para análise.	Modo *inline*, geralmente *Layer* 2.	*Layer* 3 ou modo transparente.
Posicionamento	Monitoramento e detecção através de uma "porta *span* ". Geralmente após o Firewall.	*Inline*, geralmente após o Firewall.	*Inline* no perímetro da rede. Primeira linha de defesa.
Análise de Tráfego	Sim.	Sim.	Não.
Ação	Alertas/alarmes na detecção de anomalias.	Bloqueia o tráfego ao detectar anomalias ou assinaturas de ataque.	Bloqueia o tráfego.
Terminologias	Detecção baseada em anomalias. Detecção baseada em assinaturas. Ataques de dia zero. Monitoramento. Alarmes.	Detecção baseada em anomalias. Detecção baseada em assinaturas. Ataques de dia zero. Bloqueio de ataques.	Filtragem de pacotes *stateful*. Permite e bloqueia o tráfego por regras de IP/porta/protocolo.

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.**
Recomendaria que não usasse informações pessoais, como datas de aniversário ou número de algum documento. Não usar números sequenciais e nem palavras reais e procurar sempre criar as senhas mais longas possíveis.

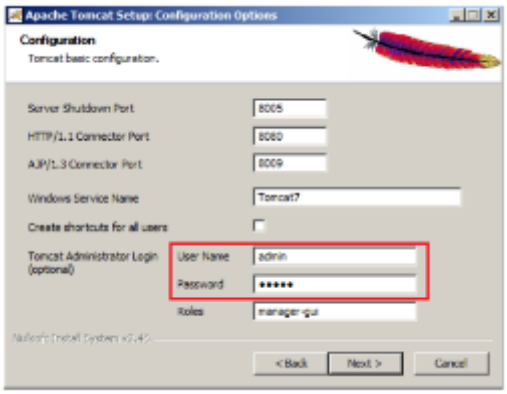
6) **Observe a imagem a seguir:**



Do ponto de vista da segurança da informação, identifique:

a) **A vulnerabilidade:** Sistemas operacionais desatualizados.
b) **A ameaça:** Infecção por um malware (software mal intencionado-vírus)
c) **Uma ação defensiva para mitigar a ameaça:** Atualização do sistema operacional, retirar cópias não licenciadas e instalando cópias legítimas.

7) **Observe a imagem a seguir.**



Do ponto de vista da segurança da informação, identifique:

a) **A vulnerabilidade:** Nesse caso foi usado um nome de usuário muito fraco.
b) **A ameaça:** O hacker poderá descobrir o nome de usuário muito rápido, pois é padrão e consequentemente invadir o sistema.
c) **Uma ação defensiva para mitigar a ameaça:** Nomear todos os nomes de usuários.

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. Assume 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:** Bob deseja que a mensagem seja confidencial, ou seja, que

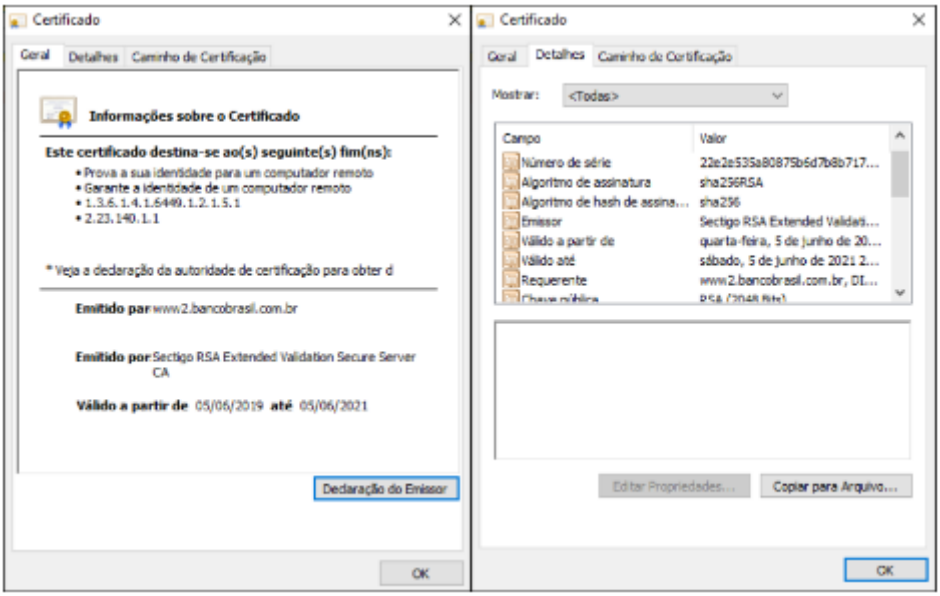
apenas ele possa decifrá-la, com isso, a melhor forma seria o uso de chave pública.

b) **como Bob deverá decifrar a mensagem de Ana corretamente:** Utilizando apenas a chave privada, pois corresponde a necessidade de Bob para poder decifrá-la.

c) **como Ana deverá cifrar a mensagem antes de enviar para Carlos:**
Como Carlos deseja autenticidade, Ana pode assinar digitalmente a mensagem, assim, criptografando um resumo (*hash*) da mensagem com sua própria chave privada, tendo uma assinatura digital.

d) **como Carlos deverá decifrar a mensagem de Ana corretamente:**
Em forma de assinatura digital, usando a chave pública de Ana para decifrar o *hash* da mensagem que foi cifrado por Ana. Se o *hash* decifrado correspondente ao que Carlos recebeu, ele pode ter certeza de que a mensagem veio de Ana e veio alterada.

9) Observe as imagens a seguir:



As imagens apresentam informações do certificado digital do site www.bb.com.br. 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. Os certificados digitais são validados através da função de HASH. O banco envia uma mensagem criptografada com uma chave privada, o receptor poderá decifrar com a chave pública, mas para isso os valores de HASH precisam bater, se os valores coincidirem, então a mensagem é validada.

9.b) Cite dois benefícios de segurança que uma transação eletrônica recebe com a utilização do certificado digital do Banco. Garante a proteção dos documentos, uma vez que as transações são criptografadas e a autenticidade das informações contidas no documento eletrônico.

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 <u>atividade dos usuários</u> que podem registrados para posterior auditoria de segurança.

1.Tentativas de login (sucesso e falha): Registros de todas as tentativas de autenticação dos usuários, tanto as bem-sucedidas quanto as falhas. Isso ajuda a identificar tentativas de acesso não autorizadas.

2.Acessos e modificações de arquivos ou dados sensíveis: Registro de quais arquivos ou dados foram acessados, alterados, deletados ou copiados, e por quem. É fundamental para auditoria de integridade de dados e para rastrear o uso indevido de informações confidenciais.

3.Uso de privilégios administrativos: Registros de ações realizadas por usuários com privilégios elevados (administração), como a instalação de software, mudanças nas configurações do sistema, ou criação e exclusão de contas. Isso ajuda a controlar o uso correto de permissões especiais e identificar abusos de autoridade.

Referências

- ABNT (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS). NBR ISO/IEC 27002:2013: Tecnologia da informação -

Técnicas de segurança - Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2013.

- HINTZGBERGEN, Jule. Fundamentos de Segurança da Informação: com base na ISO 27001 e na ISO 27002. 3. ed.

Brasport, Rio de Janeiro, 2018.

Estudo de caso 1:

Criptografia e Firewalls*

Padma Santhanam, a CTO da Linen Planet, estava se deslocando para o trabalho de sua maneira habitual – pegando o

trem da estação suburbana perto de sua casa para seu escritório em uma área comercial do outro lado da cidade. Ao

virar a página do jornal da manhã, seu celular tocou. Ela olhou para o identificador de chamadas e viu que era seu

assistente, David Kalb.

"Olá, David. E aí?"

“Oi, Padma. Crise aqui como sempre. Nosso representante de atendimento ao cliente na ATI está na outra linha. Ele

diz que você precisa fazer login no sistema de ordem de serviço e aprovar a solicitação de alteração o mais rápido

possível ou eles perderão a próxima janela de alteração para a nova versão do nosso aplicativo de crédito online.”

Padma disse: “Tudo bem. Estarei no escritório em 25 minutos ou mais. O trem acabou de sair da estação Broadmore.”

“Ele diz que eles não podem esperar tanto tempo. Você deveria fazer isso anteontem, e de alguma forma foi

esquecido. Eles dizem que precisam agora ou perderemos uma semana esperando pela próxima janela de mudança.”

Padma suspirou. Então ela disse: “Tudo bem. Eu quero que você navegue no site da ordem de serviço, você sabe o

que usamos em linhoplanet.biz/wo, e faça login para mim. Você pode aprovar o pedido de alteração e não perderemos

a janela. Vou mudar minha senha quando chegar lá. Meu nome de usuário é papa, serra, alfa, novembro, tango, alfa.

Percebido?"

David disse “Entendi. Senha?" Olhando para os dois lados primeiro, Padma abaixou um pouco a voz e disse: “Romeu,

lima, oito, quatro, bang, zulu, índia, vencedor, cifrão.”

David repetiu de volta. Ele disse: “OK, estou logado agora e acabei de aprovar a ordem de serviço. Vou dizer ao nosso

representante que estamos prontos para ir.”

“Obrigado, Davi.”

Na fila atrás de Padma, Maris Heath fechou o bloco de notas e fechou a caneta esferográfica. Sorrindo, ela ergueu a

bolsa do laptop e se levantou para sair do trem na próxima estação, que ela sabia que ficava bem ao lado de um

cibercafé. Maris abriu seu laptop e conectou seu navegador ao servidor Linen Planet Web. O firewall pediu seu nome

de usuário e senha. Ela abriu o bloco de notas e digitou os dados que havia anotado enquanto escutava a ligação do

celular de Padma. Seu navegador conectou em um instante. 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. Pelo

menos nenhum outro hacker poderia observá-la enquanto ela colocava um backdoor nos servidores da Web do Linen

Planet.

Ela passaria várias horas nos próximos dias explorando a rede e planejando seu ataque...

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 servidor Web da Linen Planet e o firewall estão utilizando criptografia. O

ícone de segurança no navegador que Maris viu indica que a comunicação entre o navegador e o servidor está criptografada, provavelmente usando HTTPS(Hypertext Transfer Protocol Secure), que utiliza SSL/TLS para criptografia. Isso protege os dados em trânsito, garantindo que eles não possam ser interceptados por outros hackers. No entanto, a criptografia só protege os dados durante a transmissão; isso não impede um ataque baseado na captura das credenciais de login, como foi o caso;

2. Como o acesso ao servidor Web da Linen Planet poderia ser mais seguro? Utilizando uma autenticação de múltiplos fatores, já que ela conseguiu acessar porque houve um vazamento de senha.

***WHITMAN, Michael E. MATTORD, Herbert J. Readings and Cases in Information Security: Law and Ethics. Course**

Technology, Cengage Learning: Boston (MA), 2011.

Estudo de caso 2:

Trabalhando com servidores proxy e firewalls em nível de aplicativo*

Ron Hall estava sonhando com suas próximas férias. Ele trabalhava para Andy Ying, gerente do

grupo de consultoria de segurança, em um projeto muito exigente, há quase seis meses.

Hoje ele finalmente terminou o trabalho e teve alguns minutos para navegar na Web e planejar

sua próxima viagem à Nova Zelândia.

Ron sabia que a ATI não permitia a navegação indiscriminada na Web e que eles usavam um

servidor proxy para garantir a conformidade com essa política, mas ele sentiu que merecia esse

tratamento e acreditava que Andy não teria problemas com um pouco de navegação recreativa

na Web. Além disso, eram quase 17h e estava quase na hora de ir para casa.

O Google foi autorizado pelo servidor proxy, então Ron foi até lá para iniciar sua busca. Ele

digitou “pontos de férias na Nova Zelândia”. Mais rápido do que ele conseguia piscar, o gigante

mecanismo de busca Google voltou com uma lista de links relevantes. A primeira entrada

parecia promissora: “New Zealand Tourism Online: New Zealand Travel Guide”. Mas o segundo

ficou ainda melhor: “Fotos da Nova Zelândia”. Ele clicou nesse URL.

Nenhuma imagem foi aberta. Nada de vales verdes. Sem recifes de coral. Nada de belas

montanhas. Apenas uma tela branca com letras pretas que diziam:

ACESSO PROIBIDO — ENTRE EM CONTATO COM O ADMINISTRADOR DO PROXY SERVER PARA

INSTRUÇÕES DE COMO ACESSAR O CONTEÚDO SOLICITADO.

Ron não ficou surpreso, mas esperava. Ele clicou no botão “Voltar” e tentou o próximo link. Ele

recebeu a mesma mensagem. Ele tentou mais três ou quatro vezes e então percebeu que não

estava conseguindo nenhuma foto hoje.

Ron chegou à sua mesa um pouco cedo na manhã seguinte. Ele ligou seu PC e foi tomar uma

xícara de café enquanto ele inicializava. Quando voltou, abriu seu programa de e-mail. Na lista

de novos e-mails havia uma nota do grupo de segurança de rede. Ele abriu a mensagem e viu

que tinha sido endereçada a ele e a Andy Ying, seu chefe. Também tinha um CC para o

departamento de RH. A mensagem dizia:

Recentemente, sua conta foi usada para acessar conteúdo da Web que não foi aprovado para

uso dentro da ATI. Estamos pedindo que você explique suas ações ao seu supervisor. Você é

encorajado a se matricular em um curso sobre uso apropriado da Internet na ATI o quanto antes.

Até que você complete a aula ou seu supervisor entre em contato com este escritório, seus

privilégios de rede foram suspensos. Se esta tentativa de acesso foi para fins comerciais

legítimos, peça ao seu supervisor que nos notifique imediatamente para que este local da Web

possa ser adicionado à lista de locais da Web aprovados pela ATI.

Que aborrecimento. Ron não estava ansioso por sua conversa com Andy.

Questões

1. A política da ATI sobre o uso da Web parece dura para você? Por que ou por que não? Para mim, a política da ATI não é dura, porque isso é uma política de segurança instalada pela empresa para dificultar a entrada de hackers em seu sistema. Hoje em dia a informação é a coisa mais valiosa e consequentemente cara, que uma empresa possui. Se um hacker conseguir acesso, isso pode gerar prejuízos imensuráveis**.**

2. Você acha que Ron foi justificado em suas ações? Não, pois Ron sabia da política de segurança da empresa e deveria ter seguido as regras para evitar qualquer tipo de problema.

3. Como Andy deve reagir a essa situação se Ron é conhecido por ser um funcionário confiável e diligente? Geralmente poderíamos indicar que Ron fizesse um curso de segurança, mas ele já faz parte da equipe de segurança da empresa e sabe que esse tipo de acesso deixa as informações à mercê de hackers. Então, nesse caso Andy deveria aplicar uma advertência.

***WHITMAN, Michael E. MATTORD, Herbert J. Readings and Cases in Information**