Lista Princípios de Segurança da Informação

Aluno:João Netto Natal Pinheiro

1.Quais são as principais características da informação segura? Dê um exemplo da violação de cada um desses "pilares" da segurança.

Uma informação segura é aquela que chega sem problema, a pessoa que deveria chegar sem que ninguém intercepte, e também a que siga os pilares da segurança da informação, ou seja confidencialidade, integridade e disponibilidade. Um exemplo, seria um caso de vazamento de mensagens e e-mails como o da sony de 2014, onde os e-mails da companhia foram vazados ao público geral, causando perda de dinheiro e status pela companhia.

2.  Explique como funciona um ataque "Man-in-the-Middle". Descreva como ele poderia ser executado utilizando o protocolo ARP.

Man-in-the-middle é o ataque em que uma pessoa funciona como a pessoa do meio, ou seja, tendo acesso a tudo que se passa na máquina de outra pessoa, tudo o que entra e sai e visualizado. Usando o arp você pode fazer isso com um ARP spoofing. Primeiro você realiza o ataque de ARP spoofing na maquina e depois na maquina virtual. Que assim que efetivado pode dar acesso a você consiga ativar o man-in-the-middle.

3. Explique como o ataque mencionado no exercício 02 poderia ser impedido.

Existe nesse caso a prevenção e a solução. Para prevenir deve-se evitar redes publicas abertas, ou em lugares que você não confia. Para solucionar esse problema deve-se atualizar seu antivírus constantemente ou simplesmente ter um firewall disponível. Para o firewall estes ataques são simples de se defender.

4. Explique cada um dos conceitos a seguir:  
a) Vulnerabilidade

Uma fraqueza ou fragilidade em um sistema que pode dar oportunidade para que alguém possa efetuar ataques ao sistema, ou que possa explorar o sistema.  
b) Ameaça

Qualquer evento que explore as vulnerabilidades, ou simplesmente as formas que ataque que podem ser executadas contra o sistema, causando algum tipo de dano a empresa ou pessoa.  
c) Exploit

Um exploit é uma sequência de comandos, dados ou uma parte de um software elaborada por hackers que conseguem tirar proveito de uma vulnerabilidade.  
d) Incidente (ou ataque)

Corresponde a qualquer evento adverso relacionado a segurança da informação, como exemplos seria os ataques de DoS ou roubo de informação.  
e) Risco

É uma forma de medir o quão propenso um sistema pode estar de ser atacado por um ataque especifico. O risco pode ser muito alto, alto, médio, e baixo.  
f) Impacto

É uma forma de medir o quanto de dano pode ser causado pelo ataque especifico. Podendo variar entre baixo, médio, alto e desastre (o que seria normalmente perda total de serviço).  
g) Tratamento (ou defesa/contramedida)

Seria ou como evitar o ataque ou uma forma de acabar com um ataque. Algumas vezes a prevenção é a forma mais simples, entretanto alguns ataques necessitam defesas especificas para evitar problemas.

5. Pesquise sobre o ataque "SQL Injection" e determine cada um dos quesitos definidos na questão 03.

O SQL Injection é um ataque onde o invasor pode inserir ou manipular consultas criadas pela aplicação, que são relacionadas ao banco de dados. A vulnerabilidade é uma fraqueza no banco de dados, e a ameaça é o sql injection, o exploit pode ser tão simples quanto digitar ‘-- ou ‘ or 1=1 no login para ter acesso. O risco é alto, pois dá acesso ao banco de dados. Impacto provavelmente é alto, entretanto a defesa é relativamente simples, apenas prevenindo no código para que não seja confiante demais nas informações de login.

6. O que é criptografia? Como ela funciona?

Criptografia significa escrever de forma oculta (termo originado no grego), e se trata de regras que visa codificar a informação de uma maneira que apenas as pessoas certas consigam receber e entender as mensagens, sem que esta seja interceptada. Normalmente a criptografia transforma uma mensagem em outra usando um chave criptográfica que apenas as pessoas especificas sabem para que assim se possa quebrar o código e entender o que se está na mensagem. Essas chaves podem ser simétricas (usa a mesma chave para abrir e fechar) ou assimétricas (usa mais de uma chave e bem mais código).

7. Xbhs mvp h johcl bapspghkh whyh jpmyhy lzah myhzl?

qual foi a chave utilizada para cifrar esta frase?

Cifra de Cesar, +19.

8. Jxhwjaf f ufqfawf xjsfh zynqnefsit f hnkwf ij hjxfw htr zr afqtw ij hmfaj nlzfq f hnsht.

escreva a palavra senac utilizando a cifra de cesar com um valor de chave igual a cinco.

XJSFH.