Atividade individual

Valor: 3,0 pontos - P1

Enviar respostas através do Google Classroom

**Bruno Camargo Manso**

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

Os alicerces da Segurança da Informação são reconhecidos por 3 pilares básicos: Confidencialidade, Integridade e Disponibilidade.

A Confidencialidade remete a ideia de que os dados devem ser classificados em níveis de permissões, trocando em miúdos podemos observar o exemplo de uma empresa, cujos usuários se dividem em usuários finais, funcionários diversos e de variados níveis hierárquicos: secretaria, atendimento, suporte, supervisão, coordenação, executivos etc. Cada um possuindo um tipo de acesso restrito, isso com o objetivo de garantir que conteúdos sensíveis, por exemplo, certas informações sobre patentes, organogramas estratégicos não acabem erroneamente sendo acessados por pessoas não autorizadas.

A Integridade diz respeito à “saúde” desses dados. O fluxo de dados de uma empresa deve ser funcional, não apresente falhas ou quaisquer alterações fora do permitido pelas políticas internas da mesma. Daí a importância desses dados serem apenas acessados por pessoas devidamente autorizadas a fazer modificações. Imagine uma situação na qual é injetado um código malicioso dentro de um arquivo comumente utilizado por usuários finais. Tal arquivo perderá assim, sua integridade afetando usuários e gerando prejuízos à empresa.

Apenas a falta desse arquivo necessário já acarretaria em diversos problemas e consequentemente gerando prejuízo. Abordando assim o terceiro caso: o de Disponibilidade. Dados devem estar sempre disponíveis, falhas podem tornar dados indisponíveis (tanto os sensíveis quanto os comuns). Isso abrange: falhas em servidores, nos envios de pacotes pela rede, na má programação, até mesmo a falta de energia elétrica em caso de falha no fornecimento e em geradores. Todas opções seriam trágicas e consequentemente trariam prejuízos a uma empresa, a uma organização, a um órgão público etc.

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

O ataque MitM (man-in-the-middle) é bastante corriqueiro. Acontece que, o atacante intermedeia o fluxo de dados que deve apenas ocorrer entre dois pontos, no caso de uma conexão entre um cliente e um servidor, tomemos o exemplo do ataque utilizando protocolo ARP (indispensável para o funcionamento de uma rede). Tal protocolo ARP é usado por um outro protocolo, o TCP/IP com objetivo de mapear um endereço IPV4 qualquer e seu respectivos dados contidos que fluem da camada 2 para camada 3, assim, tal quadro deve apresentar um endereço MAC específico e seu IP. Para que o MAC do destinatário seja devidamente reconhecido, algum dispositivo de origem deverá solicitar a tabela ARP desta rede local. O dispositivo requerido responde com uma resposta ARP que contêm o endereço IPV4 e o número MAC do destinatário, o requerente então irá armazenar tal informação em seu *cache* para assim ser visualizado pelo PC requerente, com objetivo de armazenar rotas e endereços, para agilizar uma futura nova operação.

Utilizando de breves comandos, um atacante pode assim, usurpar um dispositivo intermediário armazenando, por ele mesmo, tais endereços e rotas, redirecionando o tráfego, podendo monitorar todo conteúdo sensível ou não dessa conexão, daí o termo Man in the middle, devido a posição topográfica do mesmo na rede, permitindo tal intermediação.

O papel de monitoramento, basicamente seria de “cheirar” (*sniff*) dados que fluem entre os dispositivos-vítimas, utilizando de ferramentas do tipo *Wireshark,* sendo perfeitamente possível a interpretação desses dados, escolhendo quais os sensíveis, quais os não, quais são criptografados, os não...

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

Sendo o ataque de MitM vastamente utilizado, existe também uma contra-medida eficaz para evitar a prática, que seria simplesmente fixar o endereço IP e o respectivo número MAC do Gateway. Isso inviabilizaria que o atacante efetuasse tal “troca” de posição com o Gateway pois, o PC, pré configurado, apenas reconheceria como seu Gateway aquele que fora imposto pelo usuário, garantindo uma rota “fixa” e confiável entre o PC e tal dispositivo.

4. Explique cada um dos conceitos a seguir:

a) Vulnerabilidade

Vulnerabilidade têm um conceito amplo, a tal “Brecha de segurança” pode ocorrer em códigos fontes mal elaborados, redes abertas, sistemas com falhas hierárquicas nas permissões e até mesmo em uma falha de mídia física, por exemplo um cabo mal posicionado. Pode ocorrer nos três níveis de segurança já descritos acima: na Confidencialidade, na Integridade e na Disponibilidade.

b) Ameaça

Quando uma falha qualquer em um sistema, é detectada, pode ser considerada como uma ameaça. Ameaças também operam nos mesmos níveis acima descritos. Ameaças podem ser detectadas ou não, no último caso, seria catastrófico….

c) Exploit

Exploit, ou espoliação seria o ato de *tirar proveito, explorar* vulnerabilidades de um sistema utilizando de uma sequência de comandos, para uma consequente invasão podendo assim *injetar* outros códigos maliciosos com efeito de ampliar o ataque, aumentar a vulnerabilidade conforme o objetivo do atacante e o tipo de dados que a vítima contêm.

d) Incidente (ou ataque)

Qualquer ação que afete na Confidencialidade, na Integridade e na Disponibilidade podem ser considerados ataques, mesmo sendo um ataque de baixo nível do tipo *a vassoura da tia da limpeza* que de repente, de alguma maneira, interrompe uma rede, ou de alto nível, como no caso de um ataque Hacker.

e) Risco

Risco é tudo aquilo que pode nos conduzir a uma ameaça real, o simples fato de atravessar uma rua, com a premissa de que a mesma é movimentada, com muito tráfego, pode gerar riscos diversos, não sendo muito diferente quando se trata de computadores. A partir da hora que se expõe dados, de alguma maneira, estes estão automaticamente sob um enorme escopo de riscos.

f) Impacto

Toda a vez que existe uma ameaça, um risco eminente ou um incidente, existe a necessidade de mensurar a amplitude do dano que irá gerar em uma empresa, uma organização, um órgão público etc. Os chamados *Impactos*, também podem ser positivos de alguma maneira, por exemplo: um sistema de segurança bem projetado, ou ainda, um software bem feito, bem instalado, tanto ergonomicamente quanto visualmente bem projetado, pode ter sim impactos positivos entre os funcionários e no funcionamento de uma empresa. Tais impactos, tanto negativos, quanto positivos, devem ser de alguma forma, mensurado para a devida governança de uma empresa, instituição etc.

g) Tratamento (ou defesa/contramedida)

Um caça de guerra, quando em combate ao se deparar, em seu radar, com um míssil vindo em sua direção, seu piloto tem a opção de disparar um *flare,* que seria uma contra medida ao míssil inimigo. Mísseis normalmente funcionam por detecção de ondas de calor, assim ele seguirá a fonte até atingi-la. O papel do *flare* seria o de “distrair” o projétil para outra direção. Tendo em vista que tal contramedida funciona por emissão de outras fontes de calor além da própria fonte do caça. O *flare*, que também tem outras aplicações (por exemplo como sinalizador) é inofensivo e de baixo custo, não é uma arma, porém é bastante eficaz para a dispersão do ataque quando lançado no momento certo. Da mesma forma podemos observar em Segurança da Informação: para evitar ataques é necessário o bom compreendimento de como o ataque é efetuado, talvez uma simples técnica, às vezes até barata, pode ser extremamente eficaz para impedir danos em um sistema.

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

Através de comandos SQL, é possível inserir uma série de instruções personalizadas pelo atacante usando do sistema de consultas (SQL Query) e as entradas de dados de uma aplicação como um formulário, por exemplo. Desta forma, está aberto o caminho para espoliação de dados sensíveis existentes em um banco de dados e até mesmo conseguir controle de superusuário de um cliente ou até mesmo de um servidor. Através desse processo é possível conseguir, no caso de falta de verificação de dados (validação), que o atacante realize autenticação nesse sistema e confisque o sistema, sem mesmo ter posse de um cadastro válido, permanecendo assim anônimo na rede.

6. O que é criptografia? Como ela funciona?

Do Grego, *Kryptós* significa escondido e *gráphien* significa escrita. Embaralhar, cifrar, disfarçar, confundir, deixar inteligível ao humano é a premissa da criptografia. Criado durante o longínquo reinado de Júlio César na Roma antiga (por volta de 600 a.C e 500 a.C), tinha o objetivo de ao entregar cartas ao *front* de batalha, utilizando de batedores sobre cavalos, e se em caso de algum ataque desferido contra o batedor, não comprometeria o conteúdo da mensagem e deixando-os de alguma maneira expostos. Eram chamadas de *Cifras de César*. Também utilizadas para comunicação entre aliados do Império Romano. Contemporaneamente, tal conceito ressurgiu em um romance de Edgar Allan Poe, no livro “Escaravelho de Ouro”, no qual o autor descreve um dispositivo chamado *criptógrafo* que tinha o objetivo de “revelar” um *criptograma*, desenrolando, em torno disso, uma trama. Na atualidade, equivalente em computadores, é possível utilizar de técnicas semelhantes porém bem mais avançadas com o mesmo objetivo.

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

“Qual foi a chave utilizada para cifrar essa frase?”

Resposta: Cifra #9

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.”

Cifra #21

Resposta: Cifra # wxsfh