E-fólio Global | Folha de resolução do E-fólio

UNIDADE CURRICULAR: Segurança em Redes e Computadores

CÓDIGO: 21181

DOCENTE: Henrique S. Mamede

A preencher pelo estudante

NOME: Joel José Ginga

N.º DE ESTUDANTE: 2100116

CURSO: Licenciatura em Engenharia Informática

DATA DE ENTREGA: 03/02/2022

TRABALHO / RESOLUÇÃO:

Pergunta 1 –

O que apelidamos por CIA triad é um conjunto de objetivos chave que estão no cerne da segurança de computadores e foi introduzida através da definição da mesma no NST *Computer Security Handbook*, esses objectivos são: **confidencialidade, integridade e disponibilidade**.

Apesar do uso desta tríade estar bem estabelecido, alguns no campo da segurança defendem que alguns conceitos adicionais são necessários para completar os requisitos, eles são:
- **Autenticidade**: a propriedade de ser genuíno, verificável e confiável; confiança na validade de uma transmissão, uma mensagem ou o emissor de uma mensagem. Isto implica que verificamos que os utilizadores são quem afirmam ser, e que cada entrada no nosso sistema origina de uma fonte confiável.

- **Responsabilidade**: o objetivo de segurança que gera o requesito que as ações de uma entidade sejam rastreados univocamente a essa entidade. Terá então de se suportar o não repúdio, a dissuasão, isolamento de falhas, deteção de intrusões, recuperação após ocorrências. Como um sistema perfeitamente seguro não é um objetivo alcançável, temos de conseguir fazer o rastreamento de uma falha de segurança à entidade responsável. O sistema deve manter registo das suas atividades de forma a permitir análise posterior para rastrear falhas de segurança e ajudar em disputas de transações.

Pergunta 2 –

Os modelos de cifra assimétrico e simétrico distinguem-se principalmente pela **forma como usam as chaves**. Num modelo **assimétrico são usadas duas chaves distintas**: uma designada de chave pública para encriptar os dados e outra designada de chave privada para decifrar mensagens encriptadas. Já nos modelos de cifra **simétricos é usada a mesma chave** para ambas as operações.

Como exemplo de **cifra assimétrica temos a RSA**, onde o remetente encripta a mensagem com a chave pública do destinatário, para decifrar estas mensagem, é preciso a chave privada, que é mantida em sigilo pelo destinatário. Esta Cifra assenta no princípio que é difícil fatorizar inteiros muito grandes, de facto precisamos de efetuar algumas operações matemáticas:

- escolher aleatoriamente dois primos da ordem 10^{100},

- calcular o seu produto;

- calcular a função totiente de Euler,

- arranjar um inteiro que seja primo entre si com esse totiente de Euler, que será a chave pública,

- calcular um inteiro que seja congruente com o inverso da chave pública modulo com o totiente de Euler que calculamos acima, e que será a chave privada.

Uma **cifra simétrica é a de Vigenère**, uma cifra de substituição polialfabética, ou seja com alfabetos de substituição múltiplos. O texto é mapeado para o alfabeto em cifra usado um conjunto de substituições monoalfabéticas. Para a fazer atribuímos um valor a cada uma das letras por ordem crescente, de acordo com a sua posição no alfabeto (isto é, "a" terá o valor 0 e "z" o valor 25), deslocamos a letra a encriptar um número de posições ao longo do alfabeto igual à posição original da letra da chave. A letra na posição i

do texto a encriptar é encriptada de acordo com a letra na posição i da chave. Por exemplo, se quisermos encriptar a letra "f" que tem a posição 5 com a letra "i" que tem a posição 8, então deslocamos a letra "f" oito casas, ou seja 5+8, obtemos a letra "n" que está na posição 13.

Pergunta 3 –

Um *honeypot* (ou pote de mel) é um **engodo** ou armadilha para **atrair possíveis atacantes**. Parecem um verdadeiro sistema, mas são construídos com informações sem valor, mas de forma que os atacantes pensem que nele estão informações uteis e valiosas, e são construídos também com vulnerabilidades de segurança intencionais. O utilizador legítimo do sistema não tem motivos para aceder ao *honeypot*, então, **qualquer contacto com este é sinal de ataque**.

Resumidamente, os *honeypots* são então concebidos e implementados para:

- **desviar o acesso** de um atacante a sistemas críticos,

- **recolher informações** sobre atividade do atacante,

- encorajar que o **atacante permaneça ligado** ao sistema de forma a que os administradores possam recolher dados para prevenir ataques futuros e/ou respondam com alguma ação.

Exemplos de *honeypot* são:

- as armadilhas de e-mail – podem-se por exemplo colocar endereços de e-mail falsos num local apenas acessível por colhedores automatizados de endereços de e-mail,

- bases de dados falsas,

- *honeypot* de *malware* – imita aplicativos de *software* e APIs,

- *honeypot* de *spider* – para atrair *spiders*, criando páginas web e *links* acessíveis apenas por *spiders*.

Pergunta 4 –

A designação spam vem de um *sketch* de um dos episódios dos Monthy Python, em que a palavra spam é usada de forma repetitiva e abusiva. O sketch desenrola-se num café em que uma empregada dá a escolher a um casal de uma ementa em que todos os pratos têm spam, várias vezes. Ao longo do desenrolar da conversa vai-se ouvindo no background os demais clientes (viquingues) a cantar uma música cuja letra é só "spam".

Este termo começou a ser usado pelos utilizadores dos *newsgroups* da Usenet para designar a inundação dos fóruns com mensagens, usualmente publicitárias, não solicitadas enviadas em grande quantidade. E hoje é associado ao **envio** em massa de **conteúdos não solicitados por e-mail**.

Malware é um programa construído para **aceder a um computador ou sistema, sem o consentimento do utilizador**, e para o benefício de terceiros. São exemplos de *malware*:

- vírus - executável malicioso ligado a outro executável,

- *worms* – programas que se replicam no sistema, ligando-se a ficheiros diferentes e procurando caminhos entre computadores (como redes),

- cavalos de Troia – programas que fazem operações maliciosas sob a aparência de outra operação como jogar,

- *ransomware* – um programa que rapta o sistema ou dados até que o utilizador faça um pagamento,

- *spyware* – programas para recolher informações privadas do utilizador.

O Spam pode ser utilizado para propagar o *malware*, podem ser incluídos nos emails de spam *links* ou *attatchments* que ao serem clicados ou descarregados instalam *malware* no sistema do usuário.

Pergunta 5 –

A engenharia social é uma **forma de usar explorar as vulnerabilidades humanas e a psicologia de forma a manipular as pessoas para obter acesso a dados, sistemas e informações pessoais**. O ataque é feito sem o uso de técnicas de *hacking*, é mais fácil convencer alguém a dar a sua *password* do que hackear a sua *password*.

Partilhar demasiada informação nas redes sociais – mesmo que de forma encapotada, como com posts e desafios em massa – dando acesso a demasiada informações pessoais (como data de nascimento, apelido de solteira da mãe, nome do primeiro animal de estimação, etc), podem ser utilizados por agentes maliciosos para obter as passwords ou acessos e tornar vulneráveis as informações de uma organização para a qual a pessoa trabalhe.

O agente malicioso também pode **fingir ser uma instituição ou pessoa de confiança** para obter os dados pessoais ou para roubo (como por exemplo fingindo ser uma instituição bancária para obter os dados de acesso de um cliente).

Há muitos outros tipos de ataques que envolvem engenharia social e que podem comprometer as medidas de segurança informática, como a exploração da curiosidade (deixar uma drive num sítio público), a

troca de informações pessoais por um prémio, etc. Como contramedidas podemos:

- **formar os agentes**, tornando-os menos vulneráveis a este tipo de ataques (por exemplo, numa organização ajudar as pessoas a reconhecer os emails legítimos), educar em relação aos riscos das redes sociais, especialmente da informação que é divulgada de forma pública, a divulgação aos utilizadores dos ataques quando ocorrem, etc,

- **autenticação multi-factor** adicionando um nível à verificação de identidade (impressão digital, **token RSA**, cartão, sms, etc),

- monitorizar acessos, e a localização geográfica nos quais estes ocorrem,

- dotar os equipamentos da organização com mecanismos de filtros de spam, anti-virus, firewall.