Segurança da Informação

Fundamentos

Conteúdo

- Normas
- Principais normas de segurança
- Conceitos e definições
- Medidas de segurança
- Gestão de vulnerabilidades técnicas
- Política de Segurança da Informação
- Classificação da Informação
- Gestão da continuidade do negócio
- Conformidade com requisitos legais
- Legislações e regulamentações
- Simulados

Normas

- **Normas**
  - Normas são documentos estabelecidos por consenso e aprovado por um organismo reconhecido, que fornece, para uso comum e repetitivo, regras, diretrizes ou características para atividades ou seus resultados, visando a obtenção de um grau ótimo de ordenação em um dado contexto.

- **Normas da família ISO IEC 27000**
  - As normas da família ISO/IEC 27000 são normas internacionais que apresentam os requisitos necessários para a implementação de um Sistema de Gestão da Segurança da Informação (SGSI) em qualquer organização por meio do estabelecimento de políticas de segurança, controles e gerenciamento de risco.

Principais normas de segurança

- ISO/IEC 27000
  - Overview and vocabulary (Termos e definições aplicáveis a todas as normas da família 27000)
- ABNT NBR ISO/IEC 27001
  - Sistemas de gestão da segurança da informação — Requisitos
- ABNT NBR ISO/IEC 27002
  - Código de prática para controles de segurança da informação
- ABNT NBR ISO/IEC 27003
  - Diretrizes para implantação de um sistema de gestão da segurança da informação
- ABNT NBR ISO/IEC 27004
  - Gestão da segurança da informação — Medição
- ABNT NBR ISO/IEC 27005
  - Gestão de riscos de segurança da informação

Outras normas importantes

- ABNT NBR ISO/IEC 24762:2009
  - Diretrizes para os serviços de recuperação após um desastre na tecnologia da informação e de Comunicação
- ABNT NBR ISO 31000:2009
  - Gestão de riscos - Princípios e diretrizes
- ABNT NBR ISO/IEC 20000-1
  - Tecnologia da informação — Gestão de serviços
    Parte 1: Requisitos do sistema de gestão de serviços
- ABNT NBR ISO/IEC 20000-2
  - Tecnologia da informação — Gerenciamento de serviços
    Parte 2: Guia de aplicação do sistema de gestão de serviços
- ABNT NBR ISO/IEC 38500
  - Governança corporativa de tecnologia da informação
- ABNT NBR ISO 22301
  - Requisitos para um sistema de gestão da continuidade de negócios

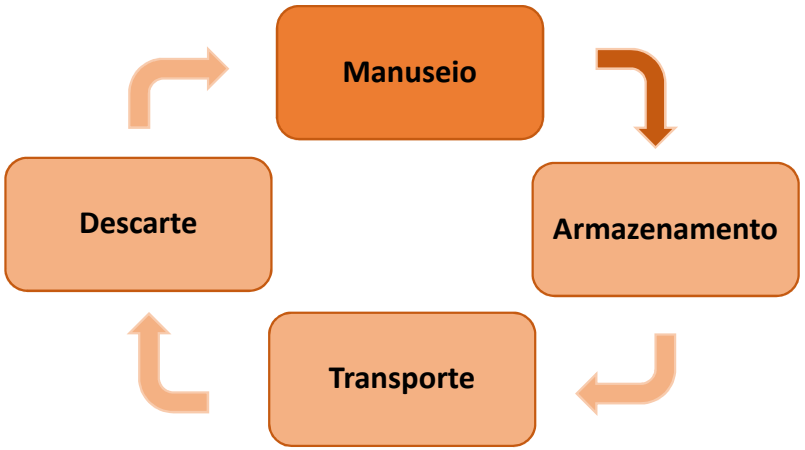
Conceitos e definições

- **Informação**
  - A informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e, consequentemente, necessita ser adequadamente protegida.

  - A informação pode existir em diversas formas:
    - Impressa ou escrita em papel;
    - Armazenada eletronicamente;
    - Transmitida pelo correio ou por meios eletrônicos ;
    - Arquivos de imagem, áudio ou vídeo.

Conceitos e definições

- **Ciclo de vida da informação**
  - Manuseio: trata-se do início do ciclo, onde a informação é gerada e manipulada;
  - Armazenamento: momento em que a informação é armazenada;
  - Transporte: momento em que a informação é enviada e/ou transportada;
  - Descarte: parte final do ciclo, onde a informação é descartada, eliminada, apagada, destruída de forma definitiva.



Conceitos e definições

- **Requisitos de segurança**
  - Identificação: permitir que uma entidade se identifique, ou seja, diga quem ela é.
  - Autenticação: verificar se a entidade é realmente quem ela diz ser.
  - Autorização: determinar as ações que a entidade pode executar.
  - Integridade: proteger a informação contra alteração não autorizada.
  - Confidencialidade: proteger uma informação contra acesso não autorizado.
  - Não repúdio: evitar que uma entidade possa negar que foi ela quem executou uma ação.
  - Disponibilidade: garantir que um recurso esteja disponível sempre que necessário.

Conceitos e definições

- **Ativo**
  - Qualquer coisa que tenha valor para a organização.

- **Classes de ativos**
  - Ativo tangível – produto, bem, equipamento, imóvel, informação em papel;
  - Ativo intangível – marca, reputação e catálogo intelectual.

- **Ativo de informação**
  - Bases de dados, arquivos, documentação de sistema, manuais de usuário, planos de continuidade do negócio, contratos, etc...

Conceitos e definições

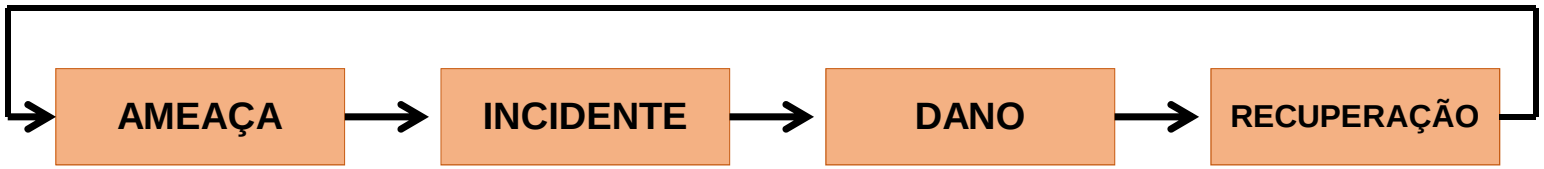
- **Vulnerabilidade**
  - Fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.
  - É uma condição que, quando explorada por um atacante, pode resultar em uma violação de segurança.
- **Patch**
  - Termo atribuído à correção desenvolvida para eliminar falhas de segurança em um programa ou sistema operacional.

Conceitos e definições

- **Ameaça**
  - Causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização.
  - **Tipos de ameaça**
    - **Humana intencional** – danos causados de forma proposital.
      - Hackers;
      - Engenharia social;
      - Vandalismo;
      - Roubo e furto;
      - Sabotagem;
      - Incêndio culposo.
    - **Humana não intencional** – danos causados de forma involuntária.
      - Pen-drive com vírus;
      - Uso inadequado de extintor de incêndio.
    - **Não humana**
      - Incêndio;
      - Relâmpagos;
      - Inundação;
      - Enchente.

Conceitos e definições

- **Incidente de segurança da informação**
  - Qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores.
  - Alguns exemplos de incidentes de segurança são: tentativa de uso ou acesso não autorizado a sistemas ou dados, tentativa de tornar serviços indisponíveis, modificação em sistemas (sem o conhecimento ou consentimento prévio dos donos) e o desrespeito à política de segurança ou à política de uso aceitável de uma organização.
- **Ciclo de vida do incidente**



Conceitos e definições

- **Gestão de incidentes de segurança da informação**
  - Convém que responsabilidades e procedimentos de gestão sejam estabelecidos para assegurar respostas rápidas, efetivas a incidentes de segurança da informação.

- **Notificação de fragilidades e incidentes de segurança da informação**
  - Assegurar que fragilidades e eventos de segurança da informação associados com sistemas de informação sejam comunicados, permitindo a tomada de ação corretiva em tempo hábil.

- **Time de respostas a incidentes de segurança da informação (CSIRT)**
  - É o nome dado à organização responsável por receber, analisar e responder a notificações e atividades relacionadas à incidentes de segurança da informação.

Conceitos e definições

- **Danos**
  - São as consequências de um incidente. Os danos podem ser diretos ou indiretos.
    - **Danos diretos** – são consequências diretas do incidente.
      - Exemplo: furto de um veículo.
    - **Danos indiretos** – são consequências indiretas do incidente.
      - Exemplo: após o furto do veículo, a pessoa perder compromissos.

- **Impacto**
  - Mudança adversa no nível obtido dos objetivos do negócio.

Medidas de segurança

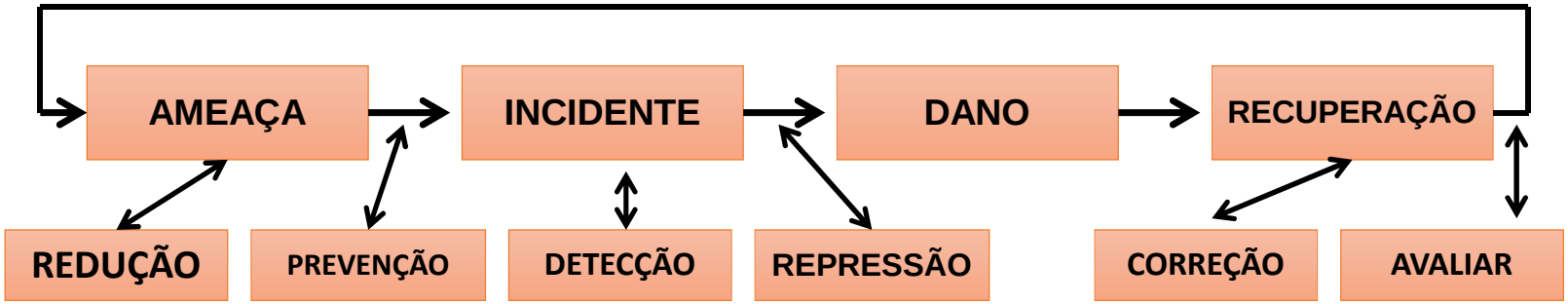
- **Funções das medidas de segurança**
- **Redutivas**
  - Medidas redutivas são aquelas destinadas a reduzir a probabilidade de que um incidente ocorra.
    - Exemplo: Instalação de um antivírus.
- **Preventivas**
  - Medidas preventivas são aquelas cujo objetivo é evitar a exploração de uma vulnerabilidade. Visam evitar o risco e reduzir a zero a probabilidade de ocorrência de um incidente, eliminando também a atividade geradora do risco.
    - Exemplo: uso de um sistema de chave de acesso (crachá) ou o armazenamento de informações sigilosas em um cofre.
- **Detectivas**
  - As medidas detectivas são aquelas que procuram identificar um incidente no momento em que ele ocorre.
    - Exemplo: sistema de detecção de instrusão.

Medidas de segurança

- **Funções das medidas de segurança (cont.)**
- **Repressivas**
  - As medidas repressivas são aquelas que combatem o dano causado pelo incidente.
    - Exemplo: combate a um incêndio.
- **Corretivas**
  - As medidas corretivas, ou de recuperação, visam a restauração do ambiente após um incidente de segurança. As medidas corretivas são importantes para que as operações da organização voltem à normalidade após um incidente.
    - Exemplo: restaurar o banco de dados usando backup.

Medidas de segurança

- **Medidas de segurança x ciclo de vida do incidente**



Medidas de segurança

- **Segurança física e do ambiente**
  - A segurança física e do ambiente tem por objetivo previnir o acesso físico não autorizado, danos e interferências com as instalações e informações da organização.

- **Perímetro de segurança física**
  - Proteção contra acesso físico não autorizado;
  - Barreiras como paredes , portões de entrada, portas, fechaduras, etc;
  - Alarmes;
  - Sistemas de detecção de intrusos.

- **Controles de entrada**
  - Assegurar que somente pessoas autorizadas tenham acesso;
  - Identificações, registro de entrada e saída, crachás, etc.

- **Segurança em escritórios, salas e instalações**

Medidas de segurança

- **Segurança física e do ambiente (cont.)**
- **Proteção contra ameaças externas e do meio ambiente**
  - Convém que sejam levadas em consideração todas ameças à segurança representadas por instalações vizinhas.

- **Segurança de equipamentos**
  - Impedir perdas, danos, furto ou roubo, ou comprotimento de ativos e interrupção das atividades da organização;
  - Monitoramento das condições ambientais, como temperatura e umidade;
  - Proteção contra raios;
  - Proteção contra falta de energia (no-breaks, UPS, geradores de emergência, etc.).

- **Segurança do cabeamento**
  - Evitar interferências;
  - Cabos de energia segregados dos cabos de comunicações;
  - Blindagem eletromagnética para proteção dos cabos;
  - Piso elevado.

Medidas de segurança

- **Segurança em recursos humanos**
  - Tem por objetivo estabelecer diretrizes e controles para a implementação de uma efetiva gestão de segurança em recursos humanos.
- **Antes da contratação**
  - Seleção
    - Verificações do histórico de todos os candidatos a emprego (Referências, informações do currículo, confirmação das qualificações acadêmicas e profissionais, verificação independente da identidade e atestado de Antecedentes Criminais).
  - Termos e condições de contratação
    - Assinatura de um termo de confidencialidade.
- **Durante a contratação**
  - Conscientização, educação e treinamento em segurança da informação;
  - Processo disciplinar.
- **Encerramento da contratação**
  - Devolução de ativos;
  - Retirada de direito de acesso.

Medidas de segurança

- **Proteção contra códigos maliciosos**
  - Visa proteger a integridade do software e da informação por meio da implantação de controles de detecção, prevenção e recuperação contra códigos maliciosos e conscientização de usuários.

- **Diretrizes para implantação**
  - Proibir o uso de softwares não autorizados;
  - Instalar e atualizar regularmente softwares de detecção e remoção de códigos maliciosos;
  - Estabelecer planos de continuidade do negócio para recuperação em casos de ataques por códigos maliciosos;
  - Conscientização dos usuários.

Medidas de segurança

- **Descarte de mídias**
  - Garantir que as mídias sejam descartadas de forma segura e protegida quando não forem mais necessárias para minimizar o risco de vazamento de informacões sensíveis para pessoas não autorizadas.

Medidas de segurança

- **Cópias de segurança**
  - Convém que as cópias de segurança sejam efetuadas e testadas regularmente conforme a política de backup.
  - Convém que as cópias de segurança sejam armazenadas em uma localidade remota.
  - Convém que os procedimentos de recuperação sejam testados e verificados regularmente.

Medidas de segurança

- **Autenticação segura**
  - A autenticação, apesar de ser também utilizada para controle de acesso lógico, é um instrumento indispensável na segurança física. A autenticação se dá através de um ou mais fatores dentre os três a seguir:
    - O que você sabe? – Nome de usuário e senha;
    - O que você tem? – Cartão, crachá, *smartcards* e *tokens*;
    - Quem você é? – Dispositivo biométrico.
  - Para termos uma autenticação considerada segura, aconselha-se a utilização de, no mínimo, dois requisitos de autenticação agregados. Exemplos:
    - ID + Senha + Crachá;
    - Crachá + Biometria.

Medidas de segurança

- **Segregação de funções**
  - Prega a divisão de tarefas e permissões na organização, não concentrando o conhecimento em apenas uma pessoa, reduzindo, consequentemente, o risco de fraudes, uma vez que seriam necessários dois ou mais colaboradores para que essa se consumasse.

- **Gerenciamento de acesso**
  - Manter um controle efetivo sobre os direitos de acesso necessários para que os colaboradores exerçam suas atribuições, sem que lhes seja concedido nenhum direito além do necessário.

Medidas de segurança

- **Gestão de mudanças**
  - Modificações em equipamentos, sistemas operacionais e aplicativos devem ser devidamente controladas. Em particular, devem ser considerados os seguintes items:
    - Identificação e registro das mudanças significativas;
    - Planejamento e testes de mudanças;
    - Avaliação de impactos;
    - Comunicação dos detalhes das mudanças para todas as pessoas envolvidas;
    - Procedimento formal de aprovação das mudanças;
    - Procedimentos de recuperação.

Medidas de segurança

- **Monitoramento**
  - Tem por objetivo detectar atividades não autorizadas de processamento da informação. Inclui itens como:
    - Registros de auditoria;
    - Monitoramento do uso dos sistemas;
    - Proteção das informações de registro (*log*);
    - Registro (*log*) de falhas;
    - Sincronização dos relógios.

Medidas de segurança

- **Gerenciamento de acesso do usuário**
  - Assegurar o acesso de usuário autorizado e previnir acesso não autorizado a sistemas de informação.
  - Convém que procedimentos formais sejam implementados para controlar a distribuição de direitos de acesso a sistemas de informação e serviços.
  - Inclui itens como:
    - Registro de usuário;
    - Gerenciamento de privilégios;
    - Gerenciamento de senha do usuário.

Medidas de segurança

- **Responsabilidades dos usuários**
  - Garantir que os usuários estejam conscientes de suas responsabilidades para manter efetivo controle de acesso, principalmente em relação ao uso de senhas e equipamentos.
    - Uso de Senhas;
    - Política de mesa limpa e tela limpa.

- **Controle de acesso a rede**
  - Prevenir acesso não autorizado aos serviços da rede.
    - Política de uso dos recursos da rede;
    - Autenticação para conexão externa do usuário;
    - Segregação de redes.

Medidas de segurança

- **Vulnerability Management Foundation**
- **Gestão de vulnerabilidades técnicas**
  - A Gestão de vulnerabilidades técnicas tem por objetivo reduzir riscos resultantes da exploração de vulnerabilidades técnicas conhecidas.
  - Convém que seja obtida informação em tempo hábil sobre vulnerabilidades técnicas dos sistemas de informação em uso, avaliada a exposição da organização a estas vulnerabilidades e tomadas as medidas apropriadas para lidar com os riscos associados.
  - A norma ISO/IEC 27002 estabelece que a gestão de vulnerabilidades técnicas seja implementada de forma efetiva, sistemática e de forma repetível com medições de confirmação de efetividade.

Medidas de segurança

- **Gestão de vulnerabilidades técnicas (cont.)**
  - Diretrizes para implementação:
    - Um inventário completo e atualizado dos ativos de informação é um pré-requisito para uma gestão efetiva de vulnerabilidade técnica.
    - Utilização de ferramentas para identificação de vulnerabilidades técnicas.
      - Exemplo: OpenVAS - http://www.openvas.org/ (Ferramenta de varreduras e gerenciamento de vulnerabilidades open-source largamente utilizada).
    - Uma vez que uma vulnerabilidade técnica potencial tenha sido identificada, convém que a organização avalie os riscos associados e as ações a serem tomadas.
    - Se um *patch* for disponibilizado, convém que sejam avaliados os riscos associados a sua instalação (*patches* devem ser testados e avaliados antes de serem instalados).
    - O processo de gestão de vulnerabilidades técnicas deve ser regularmente monitorado e avaliado.

Medidas de segurança

- **Gestão de vulnerabilidades técnicas (cont.)**
  - **Exemplos de vulnerabilidades técnicas**
    - Vulnerabilidade de software
      - Procedimentos de teste de software insuficientes ou inexistentes.
    - Vulnerabilidade de hardware
      - Sensibilidade à variação de temperatura.
    - Vulnerabilidade de rede
      - Conexão de redes públicas desprotegidas.
    - Vulnerabilidade do local ou das instalacões
      - Inexistência de mecanismos de proteção física no prédio, portas e janelas.
    - Vulnerabilidade em recursos humanos
      - Procedimentos de recrutamento e seleção inadequados.

Medidas de segurança

- **Sistema de gestão da segurança da informação (SGSI)**
  - A organização deve estabelecer, implementar, operar, analisar criticamente, manter e melhorar um SGSI;
  - O SGSI deve ser baseado no modelo “Plan-Do-Check-Act” (PDCA).

Política de Segurança da Informação

- **Information Security Policy Foundation**
- **Introdução a Política de Segurança da Informação (PSI)**
  - Uma política de segurança não é apenas um documento contendo instruções de uso de senhas, mas, sim, um documento estruturado que estabelece um conjunto de regras, normas e procedimentos que define as obrigações e as responsabilidades referentes à segurança da informação e deve ser observado e seguido pelos colaboradores da organização, sob pena de advertência e até desligamento por justa causa, no caso do não cumprimento.
  - É considerada como um importante mecanismo de segurança, tanto para as instituições como para os usuários.

Política de Segurança da Informação

- **Objetivos de uma PSI**
  - O objetivo da política de segurança da informação é prover uma orientação e apoio da direção para a segurança da informação de acordo com os requisitos do negócio e com as leis e regulamentações pertinentes.
  - "*Convém que a direção estabeleceça uma clara orientação da política, alinhada com os objetivos do negócio e demonstre apoio e comprometimento com a segurança da informação por meio da publicação e manutenção de uma política de segurança da informação para toda a organização*." (ISO/IEC 27002).
  - Os principais objetivos de uma política de segurança da informação são:
    - Proteger os negócios da organização frente ao impacto de incidentes;
    - Padronizar a segurança da informação dentro da organização;
    - Orientar colaboradores, prestadores de serviço e terceiros a respeito de suas obrigações quanto à segurança da informação.
  - Uma política de segurança atribui direitos e responsabilidades às pessoas em relação à segurança dos recursos computacionais com os quais trabalham.
  - Uma política de segurança também estipula as penalidades às quais estão sujeitos aqueles que a descumprem.

Política de Segurança da Informação

- **Benefícios da adoção de uma PSI**
  - O principal benefício da adoção de uma PSI é o estabelecimento de um padrão de conduta que seja amplamente difundido na organização e que sirva como referência para tomada de decisões da alta direção em assuntos relacionados à segurança da informação.
  - A Política de Segurança da Informação tem a importante função de fornecer as diretrizes para proteger ativos de informação contra ameaças ou incidentes, assegurando:
    - Redução da probabilidade da ocorrência de incidentes por meio da adoção de controles de segurança e diminuição dos riscos;
    - Tratamento imediato de quaisquer violações de segurança da informação detectadas e minimização dos danos provocados;
    - Efetividade dos planos de continuidade de negócios por meio de avaliações, manutenções e testes periódicos;
    - Comprometimento e responsabilidade de todos os funcionários com a PSI, observando as normas de conduta e ética da empresa;
    - Treinamentos e conscientização regulares disponíveis para todos os usuários com acesso ao sistema de informações.

Política de Segurança da Informação

- **Diretrizes para implementação de uma PSI**
  - **Conjunto de regras efetivas e atuais**
    - Uma PSI deve especificar um conjunto de regras efetivas e atuais:
      - Efetivas: as regras precisam ser tangíveis e aplicáveis dentro da realidade da organização no momento de sua efetivação e publicação;
      - Atuais: as regras devem cobrir todos os elementos relativos às novas tecnologias.
  - **Extratificação**
    - A política de segurança da informação deve especificar processos e controles de segurança da informação, em diferentes níveis de detalhamento, com a finalidade de proporcionar a devida segurança da informação.
    - As regras devem ser organizadas de forma hierárquica.
    - Extratificação da PSI em diretrizes, regras e procedimentos.
  - **Responsabilização**
    - Indica as sansões cabíveis em casos de violação ou não observância à PSI.

Política de Segurança da Informação

- **Diretrizes para implementação de uma PSI (cont.)**
  - **Viabilidade**
    - O custo de implantação de todas as exigências da PSI deve ser justificado pelo valor do ativo e do negócio a ser protegido.
    - A política deve estar alinhada com os objetivos do negócio e ser aderente à realidade da organização.
  - **Aplicabilidade**
    - As regras estabelecidas em uma PSI devem ser aplicáveis e implementáveis.
  - **Clareza e objetividade**
    - A linguagem utilizada na redação da PSI deve ser clara, objetiva e concisa, facilitando a leitura e a compreensão. Textos longos podem desestimular a leitura ou suscitar dubiedade na interpretação.
    - "*A política de segurança da informação deve ser um documento simples e de fácil entendimento, pois será lida por todos os colaboradores da organização, de todos os níveis hierárquicos.*" (Campos, 2007)

Política de Segurança da Informação

- **Diretrizes para implementação de uma PSI (cont.)**
  - **Respaldo**
    - O comprometimento da alta direção é indispensável para o sucesso da implementação da PSI.
    - "*A aprovação da direção para as iniciativas de segurança da informação é essencial.*" (Campos, 2007)
  - **Conhecimento**
    - A PSI deve ser amplamente divulgada. As pessoas precisam estar devidamente informadas e conscientizadas sobre a importância do cumprimento das regras, normas e procedimentos estabelecidos na política de segurança da informação.
    - "*Convém que um documento da política da segurança da informação seja aprovado pela direção, publicado e comunicado para todos os funcionários e partes externas relevantes.*" (ISO/IEC 27002)
  - **Obrigatoriedade**
    - O cumprimento da PSI deve ser obrigatório com consequências efetivas em caso de descumprimento.
    - Recomenda-se que os usuários estejam cientes de que existam ou possam existir meios de identificação do descumprimento da PSI.

Política de Segurança da Informação

- **Análise crítica da PSI**
  - *"Convém que a política de segurança da informação seja analisada criticamente, atualizada e aprimorada dentro de intervalos preestabelecidos ou quando ocorrem mudanças significativas que possam comprometer a sua pertinência, adequação e eficácia."* (ISO/IEC 27002)

Política de Segurança da Informação

- **Políticas específicas**
  - A política de segurança pode conter outras políticas específicas, como:
    - **Política de senhas**: define as regras sobre o uso de senhas nos recursos computacionais, como tamanho mínimo e máximo, regra de formação e periodicidade de troca.
    - **Política de backup**: define as regras sobre a realização de cópias de segurança, como tipo de mídia utilizada, período de retenção e frequência de execução.
    - **Política de privacidade**: define como são tratadas as informações pessoais, sejam elas de clientes, usuários ou funcionários.
    - **Política de confidencialidade**: define como são tratadas as informações institucionais, ou seja, se elas podem ser repassadas a terceiros.

Política de Segurança da Informação

- **Políticas específicas (cont.)**
  - **Política de mesa limpa e tela limpa**
    - Política que tem por objetivo evitar que papéis e mídias removíveis fiquem acessíveis a terceiros.
    - Informações sensíveis ou críticas, por exemplo, em papel ou em mídia de armazenamento eletrônico devem ser guardadas em lugar seguro (cofre ou armário) quando não em uso.
    - Documentos que contenham informação sensível devem ser removidos da impresssora imediatamente.
    - Computadores e terminais quando não utilizados devem ser mantidos desligados ou protegidos por mecanismos de travamento de tela e teclado.
    - Controle do uso de copiadoras.
    - Proteção de correspondências e fax.

Política de Segurança da Informação

- **Política de uso aceitável (PUA) ou Acceptable Use Policy (AUP)**: também chamada de "Termo de Uso" ou "Termo de Serviço", define as regras de uso dos recursos computacionais, os direitos e as responsabilidades de quem os utiliza e as situações que são consideradas abusivas.
- A política de uso aceitável costuma ser disponibilizada na página *Web* e/ou ser apresentada no momento em que a pessoa passa a ter acesso aos recursos. Algumas situações que geralmente são consideradas de uso abusivo (não aceitável) são:
  - compartilhamento de senhas;
  - divulgação de informações confidenciais;
  - envio de boatos e mensagens contendo *spam* e códigos maliciosos;
  - envio de mensagens com objetivo de difamar, caluniar ou ameaçar alguém;
  - cópia e distribuição não autorizada de material protegido por direitos autorais;
  - ataques a outros computadores;
  - comprometimento de computadores ou redes.

Política de Segurança da Informação

- **Código de conduta**
  - Dentro das organizações, utiliza-se o código de conduta como uma forma de direcionar as atitudes dos colaboradores para que estejam em conformidade com a conduta esperada pela alta gestão. Para que seja efetivo, o código precisa ser publicado e divulgado constantemente, desde o momento da contratação até o desligamento.
  - Para que a política de segurança seja igualmente inserida no cotidiano dos colaboradores, ela deve ser inserida no código de conduta da empresa, tornando-se parte do conjunto de diretrizes que todo colaborador deve seguir para atender aos requisitos da organização.

Política de Segurança da Informação

- **Considerações finais**
  - O desrespeito à política de segurança ou à política de uso aceitável de uma instituição pode ser considerado como um incidente de segurança e, dependendo das circunstâncias, ser motivo para encerramento de contrato (de trabalho, de prestação de serviços, etc.).
  - Se a política de segurança da informação for distribuída fora da organização, convém que sejam tomados cuidados para não revelar informações sensíveis.

Classificação da informação

- A classificação da informação tem por objetivo assegurar que a informação receba um nível adequado de proteção.
- Convém que a informação seja classificada em termos do seu valor, requisitos legais, sensibilidade e criticidade para a organização.
- A classificação dada a informação é a maneira de determinar como a informação vai ser tratada e protegida.
  - A classificação da informação não é necessariamente fixa;
  - Documentos de outras organizações devem ser reclassificados;
  - Muitos níveis de classificação podem deixar o processo complexo e economicamente inviável;
  - O proprietário da informação deve ser o responsável pela sua classificação e análise crítica;
  - Rótulos e tratamento da informação: definir e implementar um conjunto de procedimentos para rotulação e tratamento da informação segundo o esquema de classificação adotado pela empresa.
- **Níveis de classificação**
  - Pública;
  - Interna;
  - Restrita;
  - Confidencial.

Gestão da continuidade do negócio

- **Gestão da continuidade do negócio**
  - A gestão da continuidade do negócio tem por objetivo não permitir a interrupção das atividades do negócio, proteger os processos críticos contra efeitos de falhas ou desastres significativos e assegurar a sua retomada em tempo hábil.

- **Planos de continuidade do negócio**
  - Os planos de continuidade do negócio devem ser testados e atualizados regularmente, de forma a assegurar a sua permanente atualização e efetividade.
  - Os planos de continuidade do negócio devem incluir o plano de recuperação de desastres e o plano de gerenciamento de crise.

Conformidade com requisitos legais

- **Direitos de propriedade intelectual**
  - Convém que sejam adotados procedimentos apropriados para assegurar a proteção aos direitos de propriedade intelectual.

- **Proteção de registros organizacionais**
  - Registros organizacionais devem ser protegidos contra perda, destruição e falsificação.

- **Proteção de dados e privacidade de informações pessoais**
  - Convém que privacidade e a proteção de dados sejam asseguradas conforme exigido nas legislações, regulamentações e, se aplicável, nas cláusulas contratuais pertinentes.

Legislações e regulamentações

- **PCI DSS**
  - Conjunto de requisitos de segurança desenvolvido para proteger os dados de portadores de cartão de crédito.

- **Lei Sarbanes-Oxley**
  - Lei promulgada pelo governo norte-americano que tem por objetivo estabelecer maior responsalibidade e transparência na divulgação de informações financeiras por parte dos executivos.

Legislações e regulamentações

- **Lei 12.737, de 30 de novembro de 2012 (Lei "Carolina Dieckmann")**
  - Lei que torna crime no Brasil invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.

- **LEI Nº 12.965, DE 23 DE ABRIL DE 2014 (Marco Civil da Internet)**
  - Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil.

questão

1. Identifique nas alternativas abaixo a etapa na qual se inicia o ciclo de vida da informação.

a. Descarte

b. Manuseio

c. Transporte

d. Armazenamento

questão

2. Selecione nas alternativas abaixo o termo atribuído a fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças.

a. Vulnerabilidade

b. Impacto

c. Ameaça

d. Dano

questão

3. Selecione nas alternativas abaixo o conjunto de requisitos de segurança desenvolvido para proteger os dados de portadores de cartão de crédito.

a. PCI DSS

b. PGP

c. SSH

d. WPA

Ethical Hacking

Conteúdo

- Introdução a Ethical Hacking
- Penetration Testing
- Análise de vulnerabilidades
- Ataques
- Spoofing
- Malware
- Senhas
- DoS (Denial of Service)
- Mecanismos de Segurança
- Ferramentas
- Simulados

Introdução a Ethical Hacking

- **Ethical Hacker (White Hat Hacker)**
  - Tipo de hacker que tem por objetivo realizar testes de intrusão a fim de ajudar as organizações a identificar vulnerabilidades às quais seus ativos de informação estejam expostos para que sejam tomadas as medidas apropriadas para lidar com os riscos associados.
- **Black Hat Hacker**
  - Tipo de hacker que utiliza seus conhecimentos para roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial.
- **Script kiddie**
  - Termo utilizado para identificar individuos que possuem poucos conhecimentos técnicos e que geralmente não tem alvos definidos e utilizam exploits e scripts prontos ("receitas de bolo") para invadir sistemas.

Introdução a Ethical Hacking

- **Crackers**
  - São os responsáveis pela criação dos cracks, ferramentas que quebram a ativação de um software comercial, permitindo que qualquer pessoa tenha uma versão pirata do software em seu computador.
  - São responsáveis pelo prejuízo das empresas de software, e também por desenvolver vírus e outras pragas como *spywares* e *trojans*.

- **Defacer**
  - Pessoa responsável pela desfiguração de uma página.

Penetration Testing

- **Penetration Testing**
  - Teste realizado por um hacker ético, cujo objetivo é tentar invadir um sistema, rede ou ambiente no qual se deseja detectar falhas a fim de gerar um relatório indicando os problemas encontrados e as recomendações para corrigi-los.
- **Tipos de Penetration Testing**
  - **Black box**
    - Tipo de Penetration Testing no qual o auditor não possui qualquer conhecimento prévio sobre a estrutura, rede ou sistema alvo.
- **Tipos de Penetration Testing**
  - **Gray box**
    - Tipo de Penetration Testing no qual o auditor possui conhecimento parcial da estrutura e da rede da empresa.
- **Tipos de Penetration Testing**
  - **White box**
    - Tipo de Penetration Testing no qual o auditor possui todo conhecimento necessário sobre a estrutura, rede ou sistema alvo.

Penetration Testing

- **Fases da realização de um Penetration Testing**
  - Planejamento
  - Execução
  - Pós-teste

Penetration Testing

- **Planejamento**
  - Coleta de informações necessárias para realização do Penetration Testing.
  - Os funcionários e clientes da empresa serão notificados a respeito da realização do teste?
  - Quais são os resultados esperados?
  - O teste será realizado durante o expediente?
  - Quais sistemas serão testados?
  - Definição do escopo e do objetivo do teste.
  - Levantamento de informações (dispositivos de hardware, topologia da rede, sistemas operacionais, etc...).
  - Obtenção de permissão para realização do teste.

Penetration Testing

- **Execução**
  - Etapa de realização do Penetration Testing propriamente dito.
  - Identificação de vulnerabilidades e falhas de segurança.
- **Pós-teste**
  - Elaboração de relatório
  - Vulnerabilidades e falhas de segurança encontradas
  - Análise de risco
  - Matriz GUT
  - Recomendações

Penetration Testing

- **Etapas técnicas**
  - **(1) Footprinting**
    - Refere-se a busca detalhada de informações iniciais sobre um determinado alvo.
    - É o primeiro passo para uma intrusão bem-sucedida.
    - Inclui recursos de mapeamento de redes e consulta a banco de dados whois.
  - Tem por objetivo descobrir:
    - Faixa de endereços IP;
    - Informações relacionadas à rede;
    - Nomes e informações sobre funcionários;
    - Documentos com informações úteis.
  - Pode ser realizada de forma manual, automatizada ou por meio de consulta a sites de busca (Google e archive.org).
  - O site archive.org mantém um projeto chamado WayBack Machine que mantém versões antigas de mais de 478 bilhões de páginas.

Penetration Testing

- **Etapas técnicas (cont.)**
  - **(2) Varredura**
    - É etapa de um Penetration Testing que tem objetivo identificar hosts ativos e portas abertas na rede alvo.
    - Consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados.
    - Pode se realizada manualmente ou por meio de ferramentas específicas chamadas de *Scanners*.

Penetration Testing

- **Etapas técnicas (cont.)**
  - **(2) Varredura (cont.)**
    - **Scanners**
      - Programa usado para efetuar varreduras em redes de computadores, com o intuito de identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles.
      - Amplamente usado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.
      - **Nmap**
        - Ferramenta de código fonte aberto largamente utilizada para realização de varredura em redes e coleta de informações sobre hosts e serviços ativos, estado das portas e sistemas operacionais utilizados.
        - Possui interface gráfica e por linha de comando.
        - Multi plataforma(Linux, UNIX, Windows e Mac OS X).

Penetration Testing

- **Etapas técnicas (cont.)**
  - **(3) Enumeração**
    - Etapa de um Penetration Testing que tem objetivo identificar os serviços que estão rodando em determinadas portas.
    - Identificação do sistema operacional do alvo (*Fingerprinting*).
    - Compilação de dados sobre recursos disponíveis, compartilhamentos e usuários.

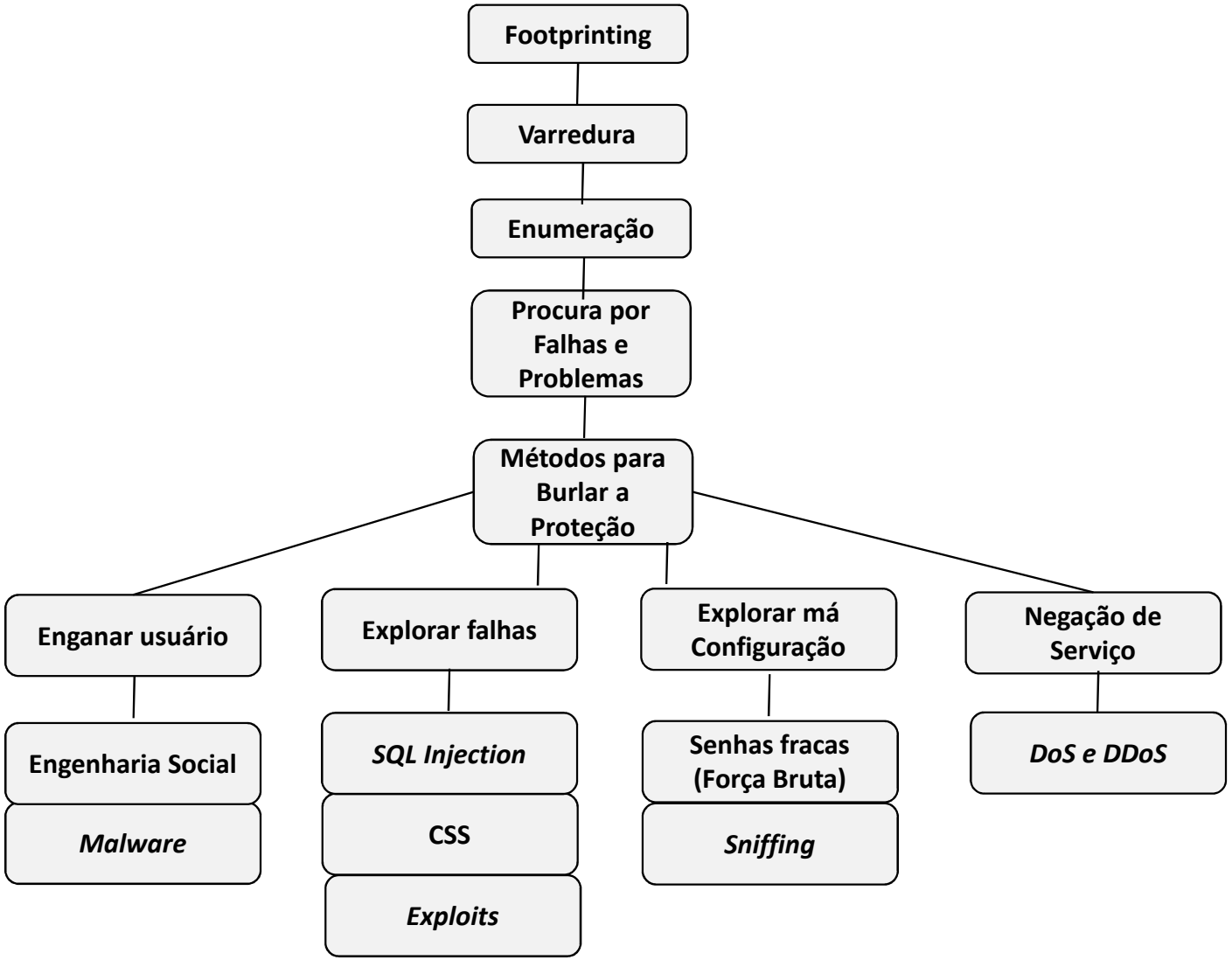
Penetration Testing

- **Etapas técnicas (cont.)**
  - **(4) Procura por falhas e problemas**
    - Identificação de vulnerabilidades e falhas de segurança.
    - Utilização de *scanners*.

Penetration Testing

- **Etapas técnicas (cont.)**
  - **(5) Utilização de métodos para burlar proteção**
  - **Enganar o usuário**
    - Engenharia social
    - *Malwares*
  - **Explorar falhas**
    - *SQL Injection*
    - *Cross Site Scripting*
    - *Exploits*
  - **Explorar má configuração**
    - Senhas fracas (Força Bruta)
    - *Sniffing*
  - **Negação de serviço**
    - *DoS e DDoS*

Penetration Testing



Análise de Vulnerabilidades

- **Análise de vulnerabilidades**
  - Análise de vulnerabilidades consiste na verificação da existência de falhas de segurança no ambiente analisado.
  - O objetivo da análise de vulnerabilidades é verificar se o ambiente atual fornece condições de segurança compatíveis com a importância estratégica dos serviços que fornece ou desempenha.

Ataques

- **Cross Site Scripting (CSS ou XSS)**
  - Tipo de ataque que tem por objetivo roubar cookies do usuário geralmente utilizando um código em JavaScript.
- **SQL Injection**
  - Tipo de ataque que consiste na injeção de comandos SQL dentro de uma consulta (query) por meio da manipulação das entradas de dados de uma aplicação.
- **Session Hijacking**
  - É o sequestro de uma sessão. Ocorre quando um usuário malicioso intercepta cookies com dados do início da sessão da vítima em algum serviço online. Assim, o cracker consegue acessar a página do serviço como se fosse a vítima e realizar roubos de informações e modificações.
- **Buffer Overflow**
  - Tipo de ataque que ocorre quando um programa recebe uma quantidade de dados superior à capacidade de armazenamento do buffer ocasionando comportamentos inesperados, ou mesmo o travamento do programa.

Ataques

- ***Phishing***
  - Tipo de fraude por meio da qual golpistas tentam induzir o usuário a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição; da instalação de códigos maliciosos, projetados para coletar informações sensíveis; e do preenchimento de formulários contidos na mensagem ou em páginas *Web*.
- **Exploits**
  - Programa criado para testar falhas de segurança, geralmente como prova de conceito, outras vezes com fins maliciosos para explorar e invadir sistemas.
  - Projetado para explorar vulnerabilidades existentes em programas de computador.
  - **Metasploit**
    - Framework open source largamente utilizado para escrever, testar e utilizar exploits.
- **Sniffing**
  - Técnica utilizada para inspecionar dados trafegados em redes de computadores, por meio do uso de softwares específicos chamados de *sniffers*.

Spoofing

- **Spoofing**
  - É a arte de criar endereços falsos e utilizá-los para diversos propósitos.
  - Tipo de ataque no qual uma entidade impostora se faz passar por uma entidade verdadeira.
  - Existem diversos tipos de ataques tipo *spoofing*:
    - **MAC *Spoofing***: personificação de um endereço MAC ou envenenamento de tabela do switch.
    - **ARP Spoofing**: envenenamento da tabela ARP.
    - **IP Spoofing**: personificação de um endereço IP.
    - **DNS Spoofing**: falsificação de traduções DNS.

Spoofing

- **MAC Spoofing**
  - Técnica de ataque baseando-se no envenenamento de tabela do switch, permitindo ao atacante receber pacotes direcionados a outra máquina.
  - Funcionamento:
    - Enviar ao *switch* um pacote ethernet falso com o endereço MAC da máquina vítima.
- **ARP Spoofing**
  - Técnica de ataque de envenenamento da tabela ARP de uma máquina, permitindo ao atacante receber pacotes direcionados a outra máquina.
- **IP Spoofing**
  - Técnica de invasão onde o atacante finge ser outra máquina falsificando o seu endereço IP.
  - Ataque simples de ser realizado principalmente se o impostor estiver na mesma rede IP da máquina verdadeira.
  - Diversos tipos de ataques usam o IP *Spoofing*, que é potencialmente perigoso em sistemas que baseiam sua segurança em endereços IP.

Spoofing

- **DNS Spoofing**
  - Tipo de ataque no qual uma entidade impostora se faz passar por uma entidade verdadeira, enviando respostas falsas à requisições DNS legítimas.
  - Programa para DNS Spoofing
    - Necessita obter/concentrar os pacotes da rede, ou simplesmente realizar o “sniffing”.
    - Quando observa uma requisição válida de DNS envia imediatamente uma resposta contendo uma tradução falsa.
  - (1) Cliente realiza requisição DNS;
  - (2) Atacante envia uma resposta DNS falsa;
  - (3) O servidor DNS envia a resposta. Porém ela será descartada pelo cliente;
  - (4) O cliente contata o servidor falso.

Malwares

- **Malwares**
  - São programas especificamente desenvolvidos para executar ações danosas e atividades maliciosas em um computador.
  - Alguns exemplos:
    - **Backdoors**
      - Softwares que tem por objetivo, uma vez instalados em um computador, assegurar o acesso futuro ao computador infectado, permitindo que ele seja acessado remotamente, sem que haja necessidade de recorrer novamente aos métodos utilizados na realização da invasão ou infecção e, na maioria dos casos, sem que seja notado.
    - **Rootkit**
      - Conjunto de programas comumente utilizado para instalar *backdoors e* esconder atividades e informações, como arquivos, diretórios e processos em um computador comprometido.

Senhas

- **Métodos para descobrir senhas**
  - *Password guessing*
    - Tentativa de adivinhação de senhas.
  - Engenharia social
    - É o termo utilizado para descrever um método de ataque em que alguém faz uso da persuasão, muitas vezes abusando da ingenuidade ou confiança do usuário, para obter informações que podem ser utilizadas para ter acesso não autorizado a computadores ou informações.
  - Sniffers
    - Dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando em uma rede de computadores.
  - Keyloggers
    - Programas capazes de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador.
  - Força Bruta
    - Tipo de ataque que consiste em adivinhar, por tentativa e erro, um nome de usuário e senha.

Senhas

- **Métodos para descobrir senhas (cont.)**
  - *Man-in-the-middle*
    - Interceptação de dados.
  - Ataque de dicionários
    - O ataque de dicionários consiste em criar uma lista de palavras (wordlist) ou senhas muito utilizadas e valer-se dessas informações.
  - Rainbow Tables
    - Uma tabela de consulta que relaciona strings com seus respectivos *hashes*.

Senhas

- Senhas mais utilizadas em 2016

1. 123456	11. qwertyuiop	21. google
2. 123456789	12. mynoob	22. 1q2w3e4r5t
3. qwerty	13. 123321	23. 123qwe
4. 12345678	14. 666666	24. zxcvbnm
5. 111111	15. 18atcskd2w	25. 1q2w3e
6. 1234567890	16. 7777777	
7. 1234567	17. 1q2w3e4r	
8. password	18. 654321	
9. 123123	19. 555555	
10. 987654321	20. 3rjs1la7qe	

Fonte: Keeper Security

Denial of Service

- **Negação de serviço, ou DoS (*Denial of Service*)**
  - É uma técnica pela qual um atacante utiliza um computador para tirar de operação um serviço, um computador ou uma rede conectada à Internet.
  - Quando utilizada de forma coordenada e distribuída, ou seja, quando um conjunto de computadores é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (*Distributed Denial of Service*).

Mecanismos de Segurança

- **Firewall**
  - Dispositivo de segurança usado para dividir e controlar o acesso entre redes de computadores.
- **IDS**
  - Sistema que monitora e analisa eventos de uma rede a procura de indícios de comportamento anômalo com o intuito de fornecer alertas em tempo real sobre acessos não autorizados aos recurso da rede.
- **Honeypots**
  - Sistema criado com objetivo de enganar um atacante e fazê-lo pensar que conseguiu invadir o sistema, quando, na realidade, ele está em um ambiente simulado, tendo todos os seus passos registrados.
- **Ferramentas antimalware**
  - Ferramentas *antimalware* são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um computador.
  - Antivírus, antispyware, antirootkit e antitrojan são exemplos de ferramentas deste tipo.

Ferramentas

- **Network Mapper**
  - Nmap
    - https://nmap.org/
- **Network protocol analyzer**
  - Wireshark
    - https://www.wireshark.org/
- **Packet generator and analyzer**
  - hping
    - http://www.hping.org/
- **Kali Linux**
  - Distribuição Linux voltado para realização de Penetration Testing.
- **Scanners**
  - GFI LanGuard
    - http://www.gfi.com/products-and-solutions/network-security-solutions/gfi-languard
  - Nessus
    - http://www.tenable.com/products/nessus-vulnerability-scanner

Ferramentas

- **Keyloggers**
  - Ardamax Keylogger
    - http://www.ardamax.com/keylogger/
  - Perfect Keylogger
    - http://www.blazingtools.com/bpk.html
- **IDS**
  - Snort
    - https://www.snort.org/

questão

1) Como é chamado o teste realizado por um hacker ético, cujo objetivo é tentar invadir um sistema, rede ou ambiente no qual se deseja detectar falhas a fim de gerar um relatório indicando os problemas encontrados e as recomendações para corrigi-los.

a) Stress testing

b) Usability testing

c) Software testing

d) Penetration testing

questão

2) Identifique o tipo de Penetration Testing no qual o auditor não possui qualquer conhecimento prévio sobre a estrutura, rede ou sistema alvo.

a) White Box

b) Black Box

c) Gray Box

d) Blue Box

questão

3) Identifique nas alternativas abaixo o termo que se refere a busca detalhada de informações iniciais sobre um determinado alvo.

a) Spoofing

b) Footprinting

c) Session Hijacking

d) Phishing

questão

4) Qual é o nome atribuído ao ataque que consiste na injeção de comandos SQL dentro de uma consulta (*query*) por meio da manipulação das entradas de dados de uma aplicação.

a) PHP Injection

b) SQL Injection

c) Buffer overflow

d) Phishing

questão

5) Indique nas alternativas abaixo a técnica que consiste em alterar campos do cabeçalho de um *e-mail*, de forma a aparentar que ele foi enviado de uma determinada origem quando, na verdade, foi enviado de outra.

a) Sniffing

b) Scam

c) Identity theft

d) E-mail spoofing

Computer Forensics

Conteúdo

- Introdução a Computação Forense
- Normas
- Conceitos gerais
- Locais de crime envolvendo equipamentos computacionais
- Fases do exame forense em dispositivos de armazenamento
- Principais desafios
- Principais ferramentas
- Simulados

Introdução a Computação Forense

- Computação Forense é uma ciência que consiste em preservar, coletar e analisar evidências digitais que possam fornecer informações sobre uso indevido ou abusivo de recursos computacionais e que possuam valor probatório.

Introdução a Computação Forense

- **Computação forense envolve os seguintes aspectos:**
  - Adquirir a evidência sem alterar ou danificar o original;
  - Analisar os dados sem modificá-los;
  - Verificação de uma quantidade grande de dados, às vezes, gigabytes de dados;
  - Procura por palavras, frases ou termos específicos;
  - Exame de arquivos de registros ou logs para identificar o tempo em que eventos ocorreram;
  - Correlacionamento de eventos;
  - Fornecer evidências de que um usuário realizou ou não um determinado ato ilícito.

Introdução a Computação Forense

- **Principais motivações**
  - Incidentes de segurança;
  - Fraudes financeiras;
  - Espionagem;
  - Uso indevido de recursos;
  - Violação de direito de propriedade intelectual;
  - Pornografia infantil;
  - Ameaças.

Introdução a Computação Forense

- **Âmbito da investigação**
  - Extrajudicial
    - Interna à uma organização privada;
    - Interna à uma organização pública (sindicância);
    - Fiscalização (realizada por órgão de fiscalização);
    - Policial.
  - Judicial (instrução probatória)

Normas

- **ABNT NBR ISO/IEC 27037:2013**
  - Estabelece diretrizes para identificação, coleta, aquisição e preservação de evidência digital.

Conceitos gerais

- **Termos e definições**
  - **Aquisição** – processo de criação de cópia de dados de uma potencial *evidência digital*.
  - **Cadeia de custódia –** é o processo de documentar a história cronológica da evidência, visando garantir o seu rastreamento em processos judiciais, registrar quem teve acesso ou realizou o manuseio desta evidência.
  - **Dados não voláteis** – dados que não se perdem quando um equipamento (exemplo computador) é desligado ou mediante interrupção de energia.
  - **Dados voláteis** – dados que são propensos a alteração e que podem ser facilmente modificados ou apagados.
  - **Evidência digital** – informações ou dados, armazenados ou transmitidos em forma binária, que podem ser utilizados como evidência de um crime.

Conceitos gerais

- **Termos e definições (cont.)**
  - **Identificação** – processo envolvendo a busca, reconhecimento e documentação da potencial *evidência digital*.
  - **Laudo pericial** – é o relatório final da perícia, que deverá conter a exposição do objeto da perícia, a análise técnica ou científica realizada pelo perito, a indicação do método utilizado e a conclusão.
  - **Mídia de destino** – mídia que receberá a cópia da *mídia de provas*, ou onde uma *imagem pericial* é restaurada.
  - **Mídia de provas** – mídia digital original, foco da perícia, onde se encontram evidências de um crime.
  - **Preservação** – processo para manter e proteger a integridade e/ou a condição original da potencial *evidência digital*.

Conceitos gerais

- **Crimes cometidos com uso de equipamentos computacionais**
- **Equipamento computacional utilizado como ferramenta de apoio aos crimes convencionais**
  - Nesta modalidade de crime, o computador é utilizado apenas como ferramenta na prática de crimes convencionais, como sonegação fiscal, falsificação de documentos, entre outros.

- **Equipamento computacional utilizado como meio para o cometimento do crime**
  - Nesta modalidade, o computador é utilizado como meio para o cometimento de crimes informáticos, como propagação de códigos maliciosos, envio de spam, golpes e ataques na Internet. (*Phishing,* Desfiguração de página, Furto de identidade, Falsificação de *e-mail, entre outros).*

Conceitos gerais

- **Origem das informações**
  - Computadores
  - Conteúdos de disco rígidos;
  - Mídias ópticas (CDs, DVDs e Blu-Rays);
  - Fitas;
  - Cartões de memória e pen-drives;
  - Informações preservadas registry (Windows);
  - Smartphones e PDAs;
  - Câmeras.
- Logs
  - Computadores;
  - Roteadores;
  - Firewalls;
  - Servidores ;
  - Provedores de Internet.
- Sniffers

Locais de crime envolvendo equipamentos computacionais

- **Local de crime de informática**
  - É o local de crime convencional acrescido de equipamentos computacionais que podem ter relação com o delito investigado.

- **Atuação do perito em buscas e apreensões em informática**
  - Ao participar de equipe para o cumprimento de mandado de busca e apreensão, o perito é o responsável em orientar a equipe quanto à seleção, preservação e coleta dos equipamentos computacionais para posterior realização dos exames forenses.
  - Devem ser tomados providências para preservação dos vestígios digitais.
  - Em alguns casos, quando computadores estiverem ligados, pode ser necessário copiar os dados da mémoria RAM antes de serem desligados utilizando ferramentas que façam *dump* dos dados voláteis.
  - Equipamentos computacionais que contenham as evidências desejadas devem ser acondicionados e transportados de maneira adequada.

Locais de crime envolvendo equipamentos computacionais

- **Atuação do perito em locais de crime de informática**
  - Assim como em buscas e apreensões, todos os procedimentos de identificação e preservação de dados contidos nos equipamentos computacionais devem ser realizados.
  - A principal diferença é que neste caso, os procedimentos forenses serão realizados no local do crime de informática utilizando ferramentas e dispositivos que permitem acessar e realizar cópias da mídia original sem alterar o conteúdo.
  - Tal procedimento tem por objetivo preserver as evidências e evitar a inviabilidade da prova.

Locais de crime envolvendo equipamentos computacionais

- **Apreensão de equipamentos computacionais**
  - Identificar os equipamentos computacionais existentes.
  - Selecionar os equipamentos computacionais a serem apreendidos de acordo com o foco da investigação.
  - Descrever todo material apreendido corretamente para garantir a cadeia de custódia.
    - Exemplo de descrição:
      - Um pen drive da marca Kingston, modelo DataTraveler Elite, número de série 6431KG000075E234C1, com capacidade nominal de 4 GB, fabricado em Taiwan.
  - Todo o material apreendido deve ser cuidadosamente acondicionado e transportado a fim de evitar danificações que possam causar perdas de evidências. Utilização de capas plásticas para acondicionar mídias ópticas, material antistático para envolver discos rígidos e plástico-bolha para amenizar vibrações.

Fases do exame forense em dispositivos de armazenamento

Fase 1 - Preservação

- Consiste em garantir que as informações armazenadas nos equipamentos computacionais não sofram alterações. Devido à fragilidade e sensibilidade das mídias de armazenamento computacional, os exames forenses devem, sempre que possível, ser realizados em cópias obtidas à partir do material original.
  - **Espelhamento**
    - O espelhamento é uma técnica que consiste na cópia exata e fiel dos dados (bit a bit) contidos em um dispositivo de armazenamento para outro. É necessário que exista um dispositivo a ser copiado (material questionado) e um para receber a cópia (destino).
  - **Imagem**
    - Semelhante ao espelhamento, mas ao invés de copiar os dados bit a bit, os dados são copiados para arquivos.
  - **Equipamentos forenses mais utilizados em duplicação de mídias**
    - **Bloqueadores de escrita de disco rígido**
      - São dispositivos mais comuns e simples de serem utilizados. Garante que nenhum dado será escrito no disco rígido questionado, de forma a disponibilizá-lo somente como leitura.
    - **Duplicadores forenses**
      - São equipamentos mais avançados e, além de realizarem bloqueio de escrita em disco rígidos, também permitem a realização de cópias (espelhamento ou imagem) para outros discos rígidos.

Fases do exame forense em dispositivos de armazenamento

Fase 2 – Extração

- A fase de extração de dados consiste basicamente na recuperação de todas as informações contidas na cópia de dados provenientes da fase de preservação. Vale lembrar que o material original (questionado) foi copiado, lacrado e guardado em lugar adequado, e todos os procedimentos serão realizados na cópia (espelho ou imagem).
- Os principais procedimentos utilizados na fase de extração são:
  - Recuperação de arquivos apagados.
  - Indexação de dados.

Fases do exame forense em dispositivos de armazenamento

Fase 3 – Análise

- A análise de dados é a fase que consiste no exame das informações extraídas na fase anterior, a fim de identificar evidências digitais presentes no material examinado, que tenham relação direta com o delito investigado.
- Em alguns casos, um disco rígido com capacidade de 200 GB, que é considerado pequeno para os padrões atuais, pode conter mais de 1 milhão de arquivos.
- As principais técnicas utilizadas na fase de análise são:

- **Utilização de *Known File Filter* (KFF)**
  - É uma lista com os resumos (*hash*) de arquivos conhecidos e pode se utilizado para filtrar o conteúdo de um dispositivo a ser examinado. Dessa forma, é possível diminuir, o número de arquivos a serem examinados em um disco rígido, descartando, por exemplo, arquivos de sistemas operacionais e diversos programas instalados.

Fases do exame forense em dispositivos de armazenamento

Fase 3 – Análise (cont.)

- **Pesquisas por palavra-chave**
  - É uma maneira eficiente de localizar arquivos, uma vez que os dados já foram indexados. Vale ressaltar que se o conteúdo dos arquivos estiver criptografado, a busca não encontrará os valores procurados.

- **Navegação pelo Sistema de pastas e arquivos**
  - Percorrer os dados dos dispositivos de armazenamento por meio da estrutura de pastas e arquivos, a fim de localizar arquivos nas pastas onde os usuários geralmente armazenam seus arquivos (Meus Documentos, Desktop, no Windows, por exemplo).

- **Visualização adequada de arquivos**
  - Depois de recuperar os arquivos encontrados no dispositivo examinado, é essencial que o perito disponha de ferramentas capazes de identificar e exibir o conteúdo dos arquivos em seu formato correto.

Fases do exame forense em dispositivos de armazenamento

Fase 4 – Formalização

• É a fase final dos exames forenses e consiste na elaboração do laudo pelo perito, apontando o resultado e apresentando as evidências digitais encontradas nos materias examinados.

- **Estrutura do laudo**
  - Preâmbulo: identificação do laudo.
  - Material: descrição detalhada do material examinado no laudo. A descrição do material deve ser minuciosa, incluindo tipo, marca, modelo, número de série, cor, estado de conservação, capacidade, país de fabricação e outras características importantes.
  - Objetivo: objetivo do laudo.
  - Considerações técnicas (opcional): conceitos e informações importantes para o entendimento do laudo.
  - Exames: é a principal seção do laudo. Deve detalhar todos os procedimentos, técnicas e métodos utilizados pelo perito para a localização das evidências. O perito pode escrever as técnicas de preservação e de recuperação de dados utilizadas e detalhar as etapas realizadas para obtenção das evidências encontradas.
  - Respostas aos quesitos: resumo objetivo dos resultados obtidos.

Principais desafios

- **Quantidade de arquivos**
  - O volume de dados dificulta o processamento. Um disco de 200 GB pode conter facilmente mais de 1 milhão de arquivos.
- **Existência de senhas**
  - Durante a realização de exames forenses é comum se deparar com arquivos e programas protegidos por senha. Neste caso, é necessário que o perito conheça as principais técnicas para quebrar senhas.
    - Ataque de força bruta
      - Consiste em tentar descobrir a senha de um arquivo por meio do processo de tentativa e erro.
    - Ataque de dicionário
      - Uso de lista de palavras. Em muitos casos, é possível utilizar combinação de palavras.
    - *RainBow Tables*
      - Uso de tabelas pré-compiladas de *hashes*.

Principais desafios

- **Uso de criptografia**
  - Buscar por programas de criptografia que estejam instalados no próprio equipamente analisado, de modo a tentar determinar o algoritimo utilizado ou, até mesmo, utilizar o próprio software para decodificar o conteúdo do arquivo.
- **Uso de esteganografia**
  - Técnica que consiste em ocultar uma mensagem dentro de outra. Caso o perito não descubra a técnica utilizada para ocultar a mensagem, uma alternativa é verificar a existência de softwares específicos instalados no dispositivo examinado.

Principais ferramentas

- **Forensic Toolkit (FTK)**
  - Reúne as principais funcionalidades para realização de exames forenses em dispositivos de armazenamento de dados.
    - Oferece recursos de indexação de dados, recuperação de arquivos, visualização de imagens, separação por tipos de arquivos, utilização de *Known File Filter* (KFF), pesquisas por palavra-chave, entre outras.
  - Dispõe de módulos para duplicação de dados e visualização de registros internos do Sistema Operacional.
  - Interface gráfica intuitiva
  - http://accessdata.com/solutions/digital-forensics/forensic-toolkit-ftk
- **EnCase® Forensic**
- Oferece recursos de duplicação de discos, recuperação de arquivos apagados, pesquisa por palavra-chave, visualização de arquivos em formatos adequados.
- https://www.guidancesoftware.com/encase-forensic

Principais ferramentas

- **WinHex: Computer Forensics & Data Recovery Software, Hex Editor & Disk Editor**
  - https://www.x-ways.net/winhex/

- **Ontrack EasyRecovery**
  - https://www.krollontrack.com/products/data-recovery-software/

- **Password Recovery Toolkit (PRTK)**
  - http://accessdata.com/product-download/digital-forensics/password-recovery-toolkit-prtk-version-7.6.0

questão

1. Selecione nas alternativas abaixo a sequencia correta das fases do exame forense em dispositivos de armazenamento computacional.

a. Preservação, Extração, Análise e Formalização

b. Preservação, Análise, Extração e Formalização

c. Formalização, Extração, Análise e Preservação

d. Preservação, Formalização, Extração e Análise

questão

2. Selecione nas alternativas abaixo o processo que tem por objetivo manter e proteger a integridade e/ou a condição original da potencial evidência digital.

a. Preservação

b. Aquisição

c. Identificação

d. Extração

Referências bibliográficas

- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27002. Rio de Janeiro, 2005.
- ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. NBR ISO/IEC 27017. Rio de Janeiro, 2016.
- ASSUNÇÃO, Marcos F. A. Segredos do Hacker Ético. 5. ed. Florianópolis: Visual Books, 2014.
- CAMPOS, André. Sistema de segurança da informação: controlando os riscos. 2. ed. São Paulo: Visual Books, 2007.
- CARTILHA DE SEGURANÇA PARA INTERNET – Cert.br. Disponível em http://cartilha.cert.br/
- ELEUTÉRIO, Pedro M. S.; MACHADO, Marcio P. Desvendando a computação forense. 1. ed. São Paulo: Novatec, 2011.
- FARMER, D; VENEMA, W. Perícia Forense Computacional. 1. ed. São Paulo: Pearson Brasil, 2006.
- SÊMOLA, Marcos. Gestão de Segurança da Informação - Uma visão executiva. 2. ed. Rio de Janeiro: Elsevier, 2013.