Criptografia e Segurança da Informação

Criptografia

António Santos

ISTEC

Tópicos

Definição

A **Vulnerabilidade** é definida como uma falha no projeto, implementação ou configuração de um software ou sistema operativo que, quando explorada por um atacante, resulta na violação da segurança de um computador.

Principais Causas

- Ignorância e falta de conscientização por parte dos utilizadores e os responsáveis pelas tecnologias de informação das organizações;
- Disponibilidade de ferramentas que facilitam ataques
- Limitação governamental ao tamanho das chaves criptográficas e ao uso de tais tecnologias
- Existência de "backdoors"nos sistemas
- Negligência dos fabricantes.

Tipos de Vulnerabilidades

- A vulnerabilidade **Física** é a possibilidade de alguém não autorizado aceder diretamente ao equipamento do sistema de informação, para lhe extrair informações, alterá-lo ou destruí-lo, quer sejam a nivel de configurações, de hardware e/ou software.
- A vulnerabilidade das **comunicações** é a possibilidade de que vários utilizadores possam aceder a um sistema de informação ligado a uma rede de informação ou a uma rede global (internet).

Tipos de Vulnerabilidades

- Vulnerabilidades por **Má Configuração**, resulta da configuração incorreta das ferramentas de segurança, como o firewall, ou podem possuir brechas para ataques maliciosos. Infraestrutura de acesso também precária e muitas vezes doméstica, implementada num ambiente corporativo.

Tipos de Vulnerabilidades

- As vulnerabilidades a nível **Software**, também conhecidas como bugs, é a possibilidade do sistema estar acessível a terceiros devido a falhas do design e criação do software, erros de código, distrações dos programadores, etc. Grande parte das vulnerabilidades surgem do erro de tamanho do buffer, uma região da memória reservada para escrita e leitura dos dados. Outro erro também comum, é a possibilidade de inserção de códigos de consulta SQL, brecha considerada dentre as mais graves a nível mundial.

Tipos de Vulnerabilidades

- As vulnerabilidades **Naturais** são a possibilidade do sistema sofrer danos devido a causas ambientais ou desastres naturais, tais como: incêndios, tempestades, inundações, terremotos, humidade excessiva, picos de temperatura.
- A **Emanação** é a possibilidade de interceptar a radiação eletromagnética para decifrar ou alterar as informações enviadas e recebidas.

Tipos de Vulnerabilidades

- As vulnerabilidades **Humanas** são aquelas em que existe a possibilidade de erro humano, como a execução de arquivos maliciosos manualmente e outros habitos menos ortodoxos, neste ambito temos os administradores e os utilizadores do sistema, pois eles têm acesso à rede e ao computador.

Análise de Vulnerabilidades

- Identificar e tratar falhas de softwares que possam comprometer seu desempenho, funcionalidade e/ou segurança;
- Providenciar uma nova solução de segurança como, por exemplo, o uso de um bom antivírus, com possibilidade de update constante e implementação de sistemas de detecção e prevenção de intrusão;
- Alterar as configurações de softwares a fim de torná-los mais eficientes e menos suscetíveis a ataques;

Análise de Vulnerabilidades

- Utilizar mecanismos para bloquear ataques automatizados (worms, bots, entre outros);
- Implementar a melhoria constante do controle de segurança;
- Documentar os níveis de segurança atingidos para fins de auditoria e compliance com leis, regulamentações e políticas.

Importância da Análise de Vulnerabilidades

- Identificar e mitigar as falhas que podem vir a comprometer o desempenho, funcionalidade e segurança da sua aplicação;
- Listar as ações necessárias para correção das fragilidades;
- Possibilitar o alinhamento às normas de conformidade;
- Visualizar relatórios mais completos, com visão privilegiada da infraestrutura;
- Realizar o acompanhamento da evolução de segurança do ambiente.

Relatório da Análise de Vulnerabilidades

- A deteção de vulnerabilidades que está presente nos sistemas da organização é o mínimo a ser feito;
- O histórico das ações tomadas e tratados, assim como informações sobre o funcionamento da Vulnerabilidade;
- Qual o envolvimento com outras áreas da empresa que lidaram com a ameaça além do pessoal de tecnologia ou da informação.

Ferramentas de Análise de Vulnerabilidade

- Um **Port Scanner** varre as portas de serviço TCP/IP de cada host analisado na rede, identificando quais destas portas estão abertas ou expostas;
- Analisadores de Protocolo (Protocol Analyzer), ou Sniffers são ferramentas capazes de visualizar o tráfego de rede, capturando pacotes transitados e permitindo a análise de seu conteúdo.

Ferramentas de Análise de Vulnerabilidade

- Os **Vulnerability Scanners** são ferramentas inteligentes capazes de scanear o sistema, analisando serviços, versões de software, sistemas operativos, base de dados e outros elementos no ambiente, identificando versões desatualizadas, patches de correção não aplicados, má configuração e outros detalhes que possam expor a Organização às ameaças.

Ferramentas de Análise de Vulnerabilidade

- Os **Honeypots/Honeynets**, têm esse nome porque são utilizados para atrair ameaças que normalmente seriam direcionadas para o ambiente real de produção. Tratam-se de implementações de software complexas, que tentam se parecer com sistemas vulneráveis, com o intuito de atrair atacantes, afim de conhecer e identificar as técnicas utilizadas por estes, para melhorar os processos de mitigação de ataques.

Definição

Uma **Ameaça** é entendida como uma condição do ambiente do sistema de informação (pessoa, máquina, evento ou idéia) que, dada uma oportunidade, pode levar a uma violação da segurança (confidencialidade, integridade, disponibilidade ou uso legítimo).

Tipos de Hacker

- Hacker de Chapéu Branco (White Hat): Ético, especialistas em segurança informática, especializados em realizar testes de intrusão e avaliações de segurança.
- Hacker de Chapéu Cinzento (Gray Hat): às vezes violam a lei e geralmente não atacam maliciosamente ou com interesses pessoais, mas suas motivações estão relacionadas a protestos ou desafios pessoais.
- Hacker de Chapéu Negro (Black Hat): também conhecido como crackers, eles violam os sistemas de informação com fins maliciosos.

Ameaças Mais Comuns

- Scan: trata-se de um ataque que quebra a confidencialidade com o objetivo de analisar detalhes dos computadores presentes na rede (como sistema operativo, atividade e serviços) e identificar possíveis alvos para outros ataques. A principal forma de prevenção é a manutenção de um firewall na empresa e uma configuração adequada da rede.

Ameaças Mais Comuns

- Worm: Worms são alguns dos malwares mais comuns e antigos. Malwares são softwares com o intuito de prejudicar o computador "hospedeiro". Essa categoria engloba tanto os vírus quanto os worms, entre diversos outros tipos de programas maliciosos. Os worms são perigosos devido à sua capacidade se espalhar rapidamente pela rede e afetar arquivos sigilosos da empresa.

Ameaças Mais Comuns

- Rootkit: Esta é uma ameaça que teve origem na exploração de kits do Linux. Tem como objetivo fraudar o acesso, logando no sistema como root, ou seja, utilizador com poder para fazer qualquer coisa. Os ataques de rootkit são feitos a partir de um malware. Quando a máquina é infetada, os arquivos maliciosos se escondem no sistema e, com essa discrição, libertam o caminho para os invasores agirem.

Ameaças Mais Comuns

- Malware: Apesar de seu surgimento no Linux, o malware é capaz de causar danos nos sistemas operativos Windows e Mac. Sem dúvidas, trata-se de um grande perigo para ambientes corporativos.

Ameaças Mais Comuns

- DDoS (negação de serviço): Os ataques de negação de serviço, mais conhecidos como DDoS (Distributed Denial of Service), estão entre os mais frequentes. Eles têm como objetivo tornar um sistema, infraestrutura ou servidores indisponíveis, causando interrupção dos serviços.
  Como isso acontece? Ao receber o ataque, o alvo é sobrecarregado de diferentes formas (uso de banda larga, falhas de software ou excessivo uso de recursos), o que pode gerar muito prejuízo à vítima.

Ameaças Mais Comuns

- Ransomware: A família ransomware é um conjunto de vírus do tipo malware e tem sido massivamente utilizada para a prática de crimes de extorsão de dados - prática também conhecida como sequestro de dados.
  O modo como o ransomware age varia conforme a sua versão, pois cada malware lançado explora uma diferente brecha do sistema operativo. Esse detalhe, inclusive, é o que torna os ataques tão repentinos e, ao mesmo tempo, fatais.

Ameaças Mais Comuns

- vírus: Embora a maneira como o vírus se manifesta varie, a finalidade é a mesma: bloquear todos os arquivos do computador, impedindo que o sistema possa ser utilizado adequadamente, e encaminhando mensagens solicitando o pagamento pelo resgate. Algumas empresas chegaram a negociar valores milionários com os criminosos para que os dados fossem devolvidos. Contudo, fazer o pagamento não é uma atitude recomendável, porque não há garantias de que a situação se normalize - além de acabar estimulando o crime.

Ameaças Mais Comuns

- Antivírus falsos: Selecionar os produtos de antivírus não é uma tarefa tão simples como parece, visto que existem soluções que, na verdade, são raízes para problemas ainda maiores que sua rede possa estar enfrentando. Da mesma maneira que existe o vírus de resgate, uma nova onda de antivírus falsos, os quais oferecem um produto para rastrear ameaças e limpar o computador. Esses vírus são conhecidos como do tipo locker (bloqueador), assim como o ransomware e o malware, solicita pagamentos por bitcoins ou cartão de crédito.

Ameaças Mais Comuns

- Phishing: A prática de phishing consiste no envio de mensagens de email, onde o invasor se passa por uma instituição legítima e confiável (bancos e serviços de transação online), induzindo a vítima a passar informações pessoais. Ultimamente o phishing vem sendo utilizado em ataques de BEC (Business Email Compromise), que tem como propósito fazer com que representantes da empresa alvo pensem estar se comunicando com executivos. Dessa maneira, as instituições acabam por fazer depósitos na conta de terceiros sem saber que se trata de uma fraude. O pior disso tudo é que o criminoso não deixa rastro, pois a mensagem não contém nenhum anexo ou links.

Vulnerabilidade vs Ameaça

Uma vulnerabilidade (em termos computacionais) é uma fraqueza ou falha num sistema de informações que coloca em risco a segurança das informações, permitindo que um invasor comprometa a integridade, disponibilidade ou confidencialidade das informações, portanto é necessário encontrá-las e remove-las o mais rápido possível. Esses "buracos"podem ser de origens diferentes, por exemplo: falhas de projeto, erros de configuração ou carência de procedimentos.

Vulnerabilidade vs Ameaça

Uma ameaça é qualquer ação que explora uma vulnerabilidade para ameaçar a segurança de um sistema de informações. As ameaças podem advir de ataques (fraude, roubo, vírus), eventos físicos (incêndios, inundações) ou negligência e decisões institucionais (manuseio incorreto de passwords, sem uso de criptografia). Do ponto de vista de uma organização, elas podem ser internas e externas.

Definição

O **Risco** é a probabilidade de ocorrência de um incidente de segurança, uma ameaça que se materializa e causa perda ou dano. É medido assumindo que existe uma certa vulnerabilidade a uma certa ameaça, como um hacker, um ataque de negação de serviços, um vírus, etc.

Quem põe em Risco o SI

- Hackers: invasores que entram nos sistemas para demonstrar e testar sua inteligência, conhecimento, etc. O perfil do hacker é o de um jovem, com amplo conhecimento de ciência da computação e da Internet (especialista em programação, arquiteturas de servidores, protocolos, sistemas operativos).

Quem põe em Risco o SI

- Crackers: são pessoas interessadas em atacar um sistema de computador para obter benefícios ilegalmente ou simplesmente causar danos à organização que possui o sistema, motivados por interesses económicos, políticos, religiosos, etc.

Quem põe em Risco o SI

- Sniffers: são indivíduos dedicados a rastrear e tentar recompor e decifrar as mensagens que circulam pelas redes de computadores.
- Phreakers: Eles são intrusos especializados em sabotar redes de telefone para fazer chamadas gratuitas. Os phreakers desenvolveram as famosas caixas azuis que podiam emitir diferentes tons nas frequências usadas pelos operadores para a sinalização interna das suas redes, quando ainda eram analógicas.

Quem põe em Risco o SI

- Spammers: Eles são responsáveis pelo envio em massa de milhares de mensagens de email não solicitadas, causando colapso do servidor e sobrecarga nas caixas de correio dos utilizadores. Algumas dessas mensagens também contêm códigos maliciosos que tentam fazer os golpes caso como "phishing"ou "vishing"(phishing de voz).

Quem põe em Risco o SI

- Lamers ("wannabes"): Script-kiddies ou Click-kiddies - São todos aqueles utilizadores iniciantes que baixam scripts ou programas da Internet e os executam sem realmente ter um conhecimento técnico do que estão a fazer ou como funcionam.
- Piratas: são os indivíduos especializados em programas de hackers e conteúdo digital, violando a legislação sobre propriedade intelectual.

Quem põe em Risco o SI

- Criadores de vírus e/ou programas nocivos: são especialistas em programação e sistemas de informação que pretendem demonstrar o seu conhecimento criando vírus e outros programas, que procuram uma disseminação exponencial e, assim, alcançam maior visibilidade.
- Ameaças da equipe interna: bisbilhoteiros, inocentes ou ignorantes, utilizadores infelizes ou injustos que pretendem causar danos à instituição.

Quem põe em Risco o SI

- Ex-funcionários: pessoas que, por despeito ou vingança, agem contra sua antiga empresa, aproveitando contas não canceladas para deixar "bombas lógicas"
- Intrusos pagos: são especialistas em informática, contratados por terceiros para subtrair informações confidenciais, realizar sabotagem de sistemas de informação contra uma organização específica, etc.

Fontes de Risco

- Malware ou código malicioso: permite ações diferentes de um invasor. Desde ataques genéricos até o uso de cavalos de Troia, até ataques de precisão direcionados, com objetivos específicos e projetados para atacar um dispositivo, configuração ou componente de rede específico.

Fontes de Risco

- Engenharia social: Utilizam técnicas de persuasão por forma a tirar proveito da boa vontade da vítima e falta de cautela para obter informações sensíveis ou confidenciais. Os dados assim obtidos são posteriormente utilizados para realizar outros tipos de ataques ou para venda.

Fontes de Risco

- APT ou ameaças persistentes avançadas (Advanced Persistent Threats): são ataques coordenados direcionados contra uma empresa ou organização, que tentam roubar ou filtrar informações sem serem identificados. Eles geralmente são ajudados por técnicas de engenharia social e são difíceis de detectar.

Fontes de Risco

- Botnets: conjunto de computadores infectados que executam programas de forma automática e autónoma, o que permite ao criador da botnet controlar os computadores infectados e usá-los para ataques mais sofisticados, como ataques DDoS.
- Redes sociais: o uso descontrolado desse tipo de rede pode colocar em risco a reputação da empresa.

Fontes de Risco

- Serviços na nuvem: uma empresa que contrata esse tipo de serviço deve ter em mente que deve exigir os mesmos critérios de segurança que seu provedor de serviços possui nos seus sistemas. Certifique-se de contratá-los com empresas cuja segurança é demonstrada e assine ANS ou SLA (Service Level Agreements) nos quais a segurança de que a empresa precisa é definida.
- Alguns incidentes podem envolver problemas legais que podem resultar em multas financeiras e danos à reputação e imagem da empresa.

Precauções

- Evitar riscos, eliminando suas causas, por exemplo: quando for possível evitar atividades ou processo que possa envolver riscos.
- Adotar medidas que mitiguem o impacto ou a probabilidade de risco por meio da implementação e monitorização de controles.
- Compartilhe ou transfira o risco com/para terceiros através de seguros, contratos etc.
- Aceite a existência do risco e monitorize-o.

Definição

Um **Ataque** é quando um conjunto de passos são executados no âmbito da exploração de vulnerabilidades a que permite concretizar uma ação ilicita.

Categorias Gerais de Ataques

- Interrupção: trata-se de um ataque à disponibilidade, pois um recurso do sistema é destruído ou fica indisponível.
- Interceptação: É um ataque contra a confidencialidade, pois uma entidade não autorizada (uma pessoa, um programa ou um computador) obtém acesso a um recurso.

Categorias Gerais de Ataques

- Modificação: Consiste num ataque contra a integridade, no qual uma entidade não autorizada não apenas obtém acesso a um recurso, mas também é capaz de manipulá-lo.
- Fabricação: um ataque contra a autenticidade; nesse caso, uma entidade não autorizada insere objetos falsificados no sistema.

Tipos de Ataques

- Ataques Ativos: São ataques que intervêm no fluxo normal da informação. Alterando o seu conteúdo e produz informação não válida, com o intuito de atentar contra a segurança de um sistema.
- Ataques Passivos: São ataques que não alteram a informação, nem seu fluxo normal, apenas ficam sob canal de escuta.

Sniffing de Rede

- Captura automática de passwords enviadas em nomes de utilizadores claros e de rede. Essa habilidade é frequentemente usada para atacar sistemas posteriormente.
- Conversão de tráfego de rede num formato compreensível pelos seres humanos.
- Análise de falhas para descobrir problemas de rede, como: porque o computador A não pode estabelecer comunicação com o computador B?

Sniffing de Rede

- Medição de tráfego, através da qual é possível descobrir gargalos em algum lugar da rede.
- Detecção de intrusos. Embora existam programas específicos chamados IDS (Intrusion Detection System), que são praticamente sniffers com funcionalidades específicas.
- Criação de registros de rede, para que os invasores não possam detectar que estão sendo investigados.

Principais Tipos de Ataques

- Malware: o termo refere-se genericamente a qualquer software malicioso que tem como objetivo infiltrar-se num sistema para o danificar. Geralmente são associados como tipos de malware alguns vírus, worms e cavalos de Troia.

Principais Tipos de Ataques

- Vírus: é um código que infecta os arquivos do sistema mediante programa malicioso, mas para isso é preciso que o utilizador o execute diretamente. Uma vez este ativo, é disseminado por todo o sistema ao qual o equipamento ou conta de utilizador tenham acesso, desde dispositivos de hardware até unidades virtuais ou locais remotos enuma rede.

Principais Tipos de Ataques

- Worms: é um programa que, uma vez infectado o equipamento, faz cópias de si mesmo e as espalha pela rede. Ao contrário do vírus, este não precisa de intervenção do utilizador, pois pode ser transmitido usando redes ou email. Eles são difíceis de se detectar, pois o seu principal objetivo é espalhar-se pelo sistema e infectar outros equipamentos e, inicialmente, não afetam o funcionamento normal do sistema. Seu principal uso é a criação de redes zumbis (botnets), usadas para executar ações remotamente como um ataque de negação de serviço (DoS) a outro sistema.

Principais Tipos de Ataques

- Cavalos de Troia (Trojans): semelhante aos vírus, no entanto, enquanto o virús é destrutivo por si só, o cavalo de troia procura abrir um porta (backdoor) para favorecer a entrada de outros programas maliciosos. A sua principal missão é precisamente passar despercebido e entrar nos sistemas sem ser detectado como uma ameaça em potencial. Eles não se propagam e geralmente são integrados a arquivos executáveis aparentemente inofensivos.

Principais Tipos de Ataques

- Spyware: é um programa espião, cujo objetivo é recolher informações de um equipamento/utilizador e transmiti-las a uma entidade externa sem o consentimento do proprietário. Seu trabalho é geralmente silencioso, sem mostrar sinais de seu funcionamento, chegando inclusive até a instalar outras aplicações sem ser notado. As consequências da sua infecção (atuação), incluem, também, uma perda considerável de desempenho do sistema bem como uma dificuldade de conexão com a Internet/rede.

Principais Tipos de Ataques

- AdWare: A sua principal função é mostrar publicidade. Embora a sua intenção não seja danificar o equipamento, ela é considerada por alguns como uma classe de spyware, pois pode recolher e transmitir dados para estudar o comportamento do utilizador e direcionar melhor o tipo de publicidade.

Principais Tipos de Ataques

- Ransomware: Este é um dos ataques mais sofisticados e modernos, pois o que faz é sequestrar dados (encriptando-os) e solicitar um resgate por eles. Normalmente, é solicitada uma transferência em dinheiro eletrónico (bitcoins), para evitar rastreamento e localização. Esse tipo de ataque cibernético está a aumentar e é um dos mais temidos atualmente.

Principais Tipos de Ataques

- Verificação de porta: É uma técnica usada para auditar dispositivos e redes para saber quais portas estão abertas ou fechadas, os serviços oferecidos, além de verificar a existência de alguns firewalls, a arquitetura da rede ou o sistema operativo, entre outros aspectos. Seu uso permite ao invasor realizar uma análise preliminar do sistema e de suas vulnerabilidades, com vista a algum outro tipo de ataque, uma vez que cada porta aberta num dispositivo é uma possível porta de entrada (gateway) para ele.

Principais Tipos de Ataques

- Phishing: Não é software, é uma variedade de técnicas de roubo de identidade para obter dados privados das vítimas, como senhas ou dados bancários. Os meios mais comumente usados são email, mensagens ou telefonemas e personificam qualquer entidade ou organização conhecida, solicitando dados confidenciais, para serem posteriormente utilizados por terceiros para seu próprio benefício.

Principais Tipos de Ataques

- Redes de robôs (Botnets): são computadores ou dispositivos conectados à rede (smartphones, tablets, etc.) infetados e controlados remotamente, que se comportam como robôts (bots) ou "zumbis", sendo incorporados a redes distribuídas, que enviam e-mails massivamente de "spam"ou código malicioso, com o objetivo de atacar outros sistemas ou deixá-los fora de serviço.

Principais Tipos de Ataques

- Negação de serviços: Visa desativar o uso de um sistema de informação ou computador, a fim de bloquear o serviço para o qual está destinado. Os servidores da Web têm a capacidade de resolver um certo número de solicitações ou conexões de utilizadores em simultâneo. Se excederem esse número, começam a ficar mais lentos ou até bloquear e desconetar-se da rede.

Principais Tipos de Ataques

- Ataque MITM (Man In The Middle): ocorre quando uma comunicação entre dois sistemas é interceptada por uma entidade externa que simula uma identidade falsa. Nesse sentido, o invasor tem controle total das informações trocadas, podendo manipulá-las à vontade, sem que o remetente e o destinatário o perceba rapidamente. É comum que se realize usando redes WIFI públicas e abertas, e é muito perigoso, já que se pode obter informações sensíveis das vítimas, e é difícil identificá-las se não houver conhecimento mínimo sobre o assunto.

Técnicas para esse ataque MITM

A negação de serviço ou DoS (Denial of Service)
A negação de serviço distribuído ou DDoS (Distributed Denial of Service);