ACH2014 – Fundamentos de Sistemas de Informação

AULA 11 – SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

Prof. Marcelo Medeiros Eler
marceloeler@usp.br

Introdução

- Sistemas de Informação captam, processam e distribuem dados e informações para controlar e auxiliar tomadas de decisões
- Muitas organizações manipulam e armazenam informações próprias ou de terceiros que são críticas, sigilosas, o que as obriga a se proteger de forma que seus sistemas de informação não fiquem vulneráveis a ataques internos ou externos

Introdução

- Segurança da Informação é o processo de proteção das informações mantidas e manipuladas por uma organização
- Com o advento das redes de computadores e a intensificação do uso dessas pelas empresas, a segurança da informação tem sido um assunto que vem exigindo, cada vez mais, maiores cuidados do que aqueles até então existentes antes das redes.

Introdução

- Nesta aula serão abordados os ataques mais comuns de pessoas mal intencionadas e também políticas básicas de segurança
- Algumas partes desta aula foram extraídas do material de aula de:
  - Prof João Bosco M. Sobral (INE 5630)
  - Eduardo Luzeiro Feitosa

Requisitos de segurança

- Disponibilidade
- Privacidade
- Confidencialidade
- Integridade
- Autenticidade
- Controle de Acesso
- Não-Repúdio da Informação

Disponibilidade (Availability)

- É o requisito de segurança em que a informação deve ser entregue para a pessoa certa, no momento que ela precisar.
- A informação estará disponível para acesso no momento desejado.
- Proteção contra interferência como meio para acessar os recursos.

Privacidade (Privacy)

- É o requisito de segurança em que a informação deve ser fornecida para qualquer fim, mas somente com a autorização do proprietário da informação.
- Exemplo: Informações médicas ou financeiras.

Confidencialidade

- É o requisito de segurança que visa a proteção contra a revelação de informação a indivíduos não autorizados.
- Garante que a informação em um sistema, ou a informação transmitida são acessíveis somente a partes autorizadas.

Integridade

- É o requisito de segurança que visa a proteção da informação contra modificações não autorizadas.
- Garante que somente partes autorizadas podem modificar a informação.
- Modificação inclui: escrever, mudar, mudar status, apagar, criar e atrasar ou responder mensagens.

Autenticidade

- É o requisito de segurança que visa validar a identidade de um usuário, dispositivo, ou outra entidade em um sistema, frequentemente como um pré-requisito a permitir o acesso aos recursos de informação no sistema.
- Garante que a origem da informação é corretamente identificada, assegurando que a identidade não é falsa.

Controle de Acesso (Access Control)

- Acesso é a interação entre um usuário e o sistema que permite a informação fluir de um para o outro.
- Controle de Acesso corresponde aos procedimentos operacionais de gerenciamento para detectar e prevenir acessos não autorizados e permitir acessos autorizados num sistema.

Não-Repúdio

- Requer que nem o transmissor nem o receptor da informação, possam negar o envio da informação.
- O sistema não permite a negação, por parte do usuário, do envio de determinada informação.

Infra para garantir a segurança da informação

- Segurança da Informação trata de garantir a existência dos requisitos fundamentais para proporcionar um nível aceitável de segurança nos recursos de informação.
- Ações:
  - Definir restrições aos recursos da informação.
  - Definir políticas de segurança.
  - Um conjunto de políticas de segurança define um Modelo de Segurança.

Infra para garantir a segurança da informação

O **projeto de segurança** da informação pode ser definido como segue:

- Criação de uma **política de segurança corporativa** e **análise de riscos.**
- Processo de **conscientização do pessoal** de informática e demais usuários.
- Proteção contra **softwares maliciosos.**

Infra para garantir a segurança da informação

- *Firewall.*
- Sistemas de Criptografia (Protocolos de Segurança).
- Sistemas de Detecção de Intrusão.
- Sistemas de Análise de Vulnerabilidades.
- Ferramentas de Autenticação de Usuários: assinaturas digitais, certificação digital.
- Procedimentos de Auditoria.
- Aspectos Jurídicos .

Infra para garantir a segurança da informação

- ***Firewall.***
- **Sistemas de Criptografia (Protocolos de Segurança).**
- **Sistemas de Detecção de Intrusão.**
- Sistemas de Análise de Vulnerabilidades.
- Ferramentas de Autenticação de Usuários: assinaturas digitais, certificação digital.
- Procedimentos de Auditoria.
- Aspectos Jurídicos .

Infra para garantir a segurança da informação

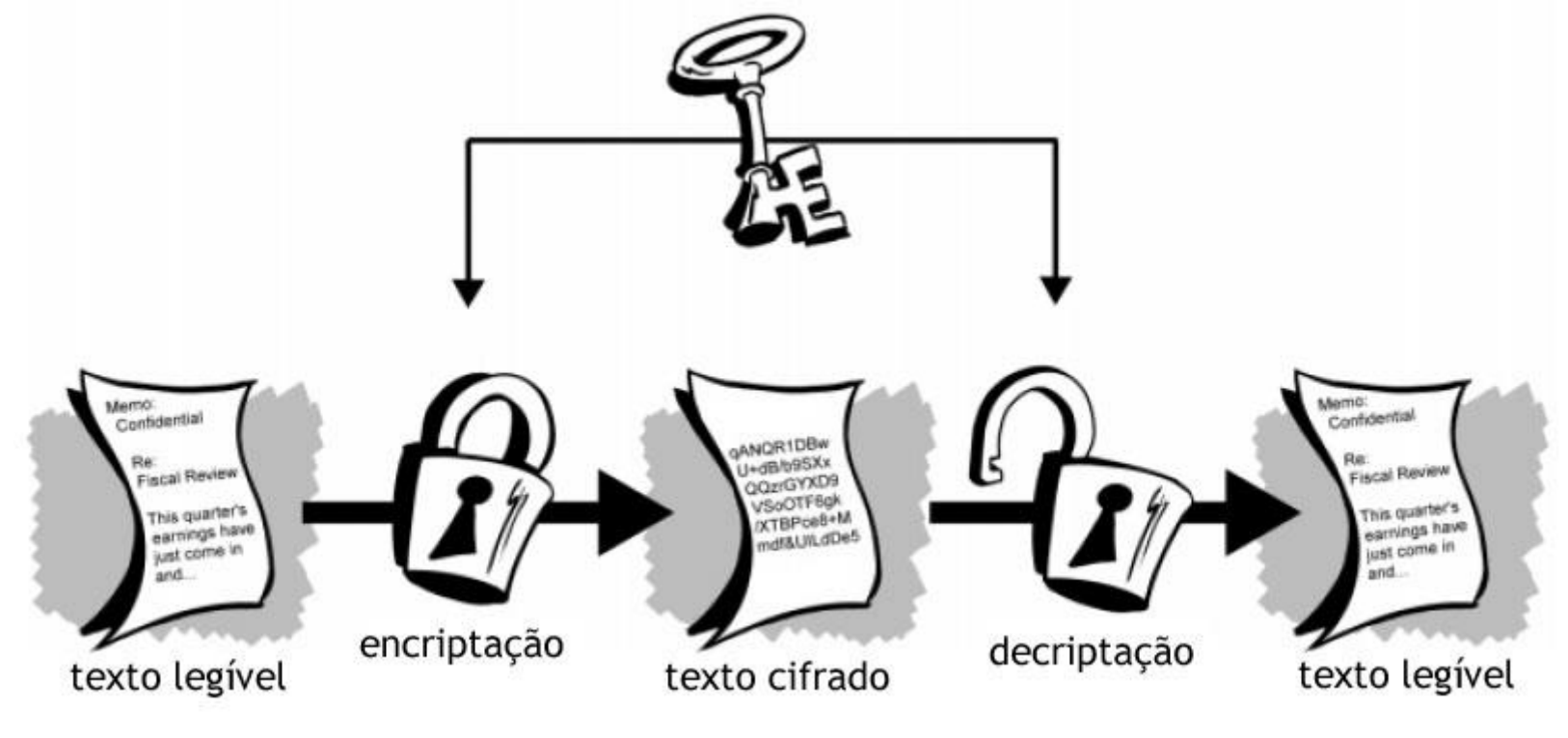
- Firewall
  - Dispositivo que tem por objetivo aplicar uma política de segurança a um determinado ponto da rede.
  - Pode ser do tipo filtros de pacotes, proxy de aplicações, etc.
  - Existe na forma de software e de hardware
  - A complexidade de instalação depende do tamanho da rede, da política de segurança, da quantidade de regras que controlam o fluxo de entrada e saída de informações e do grau de segurança desejado.

Infra para garantir a segurança da informação

- Criptografia
  - Ciência que oculta e/ou protege informações – escrita, eletrônica ou de comunicação.
  - A palavra criptografia vem das palavras gregas que significam “escrita secreta”.
  - Kriptos (em grego) = Secreto + Grafia (de escrever)
  - Criptografia = Escrita secreta.
  - Criar mensagens cifradas.

Infra para garantir a segurança da informação

- Criptografia



Infra para garantir a segurança da informação

- Sistema de detecção de intrusão
  - Refere-se aos meios técnicos de descobrir em uma rede acessos não autorizados que podem indicar a ação de um invasor ou até mesmo de funcionários mal intencionados.
  - Monitoramento

Segurança da informação

- Exemplo de política e boas práticas de segurança da informação
  - Tribunal de Contas da União
  - Boas práticas de segurança de informação (2012)
    - http://portal2.tcu.gov.br/portal/pls/portal/docs/2511466.PDF
  - Cartilha de segurança
    - http://www.tce.se.gov.br/sitev2/assets/files/cartilhasitce.pdf?cat=223

Normas para segurança da informação

- ABNT NBR ISO/IEC 27001:2013
- ABNT NBR ISO/IEC 27002:2013
- BS-7799-1:2000
- BS-7799-2:2002
- ISO/IEC 17799:2005 (internacionalização da BS-7799)

Terminologia

- Os Sistemas de Informação que armazenam e manipulam informações críticas estão sujeitos a vulnerabilidades que podem permitir intrusões (ou invasões)
- Risco:
  - Possibilidade de sofrer perda ou dano; perigo
- Vulnerabilidade
  - É uma falha que pode permitir a condução de um ataque
- Ameaça
  - Qualquer evento que pode causar dano a um sistema ou rede
  - A existência de uma vulnerabilidade implica em uma ameaça

Terminologia

- Incidente
  - A ocorrência de um ataque; exploração de vulnerabilidades
- Ataque:
  - Acesso a dados ou uso de recursos sem autorização
  - Execução de comandos como outro usuário
  - Violação de uma política de segurança, etc

Exemplos de vulnerabilidades

- Pessoas chaves para uma organização
  - Sem controle de acesso
- Servidores de arquivos
  - Aplicação incorreta de correções (patches)
- Dados dos alunos
  - Terceirizados não averiguados
- Equipamentos de produção
  - Controles fracos de acesso físicos

Exemplos de ameaças

- Pessoas chaves para uma organização
  - Ferimento, morte
- Servidores de arquivos
  - Ataques DoS
- Dados dos alunos
  - Acesso interno não autorizado
- Equipamentos de produção
  - Desastre natural

Vulnerabilidades

- RFC 2828 – Glossário de segurança da Internet
  - Uma falha ou fraqueza em um sistema
  - Que pode ocorrer
    - No projeto
    - Na implementação
    - Na operação ou gerenciamento
  - Que pode ser explorada para violar a política de segurança do sistema
- Livro do Nessus (programa de verificação de falhas e vulnerabilidades de segurança)
  - Erro de programação ou configuração errada que pode permitir que um intruso tenha acesso não autorizado a algum ativo

Tipos de Vulnerabilidades

- Não existe ainda consenso sobre classificação e/ou taxonomia para vulnerabilidades
  - Por serviço afetado
  - Por gravidade
  - Por sistema operacional alvo
- Classificação por impacto potencial (Nessus)
  - Vulnerabilidades Críticas
  - Vazamento de informações
  - Negação de serviços
  - Falha em implementar melhores práticas

Vulnerabilidades críticas

- São os problemas de mais alta prioridade
- A sua exploração podem levar a execução de programas, escalada de privilégios, comprometimento do sistema, etc
- Critérios para classificar uma falha como crítica
  - Possibilidade de exploração remota
  - Exploração sem conta de usuário local
  - Permissão de acesso privilegiado
  - Exploração automática e confiável (para o atacante)
- Vermes exploram vulnerabilidades críticas

Vulnerabilidades críticas (exemplos)

- Sasser worm
  - Buffer overflow no Local Security Authority Subsystem Service (LSASS) do Windows
- Witty worm
  - Buffer overflow no parser do ICQ de produtos para IDS da Internet Security Systems (ISS)
- Slapper worm
  - Falha na biblioteca OpenSSL do Apache que permite executar uma shell remota e explorar DoS
- Solaris sadmind
  - O serviço RPC do sadmind permite que usuários não autenticados executem comandos como root

Vulnerabilidades críticas (classificação)

- Buffer overflow (transbordamento de memória)
- Travessia de diretórios
- Ataques de formatação de strings
- Senhas default
- Configurações erradas
- Backdoors conhecidos

Vulnerabilidades críticas

- Buffer Overflow
  - O tipo mais famoso e explorado de vulnerabilidade crítica
    - O programador não limita a quantidade de informação que pode ser escrita em uma determinada área de memória (string, array, etc)
  - Ocorre quando o programa copia os dados de entrada para o buffer sem verificar o seu tamanho
  - Metade das vulnerabilidades descobertas nos últimos anos são de buffer overflow (CERT)
  - http://www.sans.org/rr/whitepapers/threats/481.php

Vulnerabilidades críticas

- Travessia de Diretórios
  - Problema comum encontrado em várias protocolos/aplicações que mapeiam pedidos dos usuários para caminhos de arquivos locais
  - Exemplo: através de uma conta de FTP que remete ao /home/userX, o atacante consegue acessar outros diretórios e arquivos
  - Vulnerabilidades descobertas
    - TFTP
    - Apache
    - rsync
    - Mcrosoft IIS

Vulnerabilidades críticas

- Formatação de strings
  - Permite que um atacante passe como parâmetro especificadores de conversão (ex: %d", "%s") e faça com que seja processados mais dados do que o programador considerou originalmente
  - Permite que endereços de memória sejam sobrescritos e código malicioso seja executado
  - Vulnerabilidades descobertas
    - Solaris rpc.rwalld
    - Tripwire

Vulnerabilidades críticas

- Senhas default
  - A maioria dos equipamentos e softwares vem configurados com usuários e senhas default (padrão), documentados e bem conhecidos
    - Elas facilitam a instalação e configuração inicial
  - É muito comum os administradores esquecerem de alterar esses usuários e contas
  - Exemplos
    - Cisco: conta: cisco, senha: cisco
    - WLAN: SSID (service set identifier) linksys
    - SNMP: comunidade public
    - Windows: administrator

Vulnerabilidades críticas

- Configurações erradas
  - A vida dos administradores de sistemas e de redes é dura
    - Eles sempre têm que fazer tudo às pressas
  - Por inexperiência, displicência ou pressa, muitas vezes configurações erradas ficam ativas por muito tempo
  - Exemplo: FTP anônimo
    - Para permitir que um web designer um administrador configura um FTP “seguro” e esquece da conta padrão “anonymous”
    - Um atacante coletou durante 3 meses o arquivo de senhas de uma instituição financeira, antes que o problema fosse detectado

Vulnerabilidades críticas

- Backdoors conhecidos
  - Geralmente são programas que escutam portas e possibilitam algum tipo de acesso
  - Redes com administradores inexperientes facilmente facilmente têm pelo menos um sistema com backdoors conhecidos
    - Trojans: capturadores de teclado, mouse, senhas, área de desktop, relay para outros sistemas
  - Geralmente são instalados por um atacante para ter novo acesso após um ataque bem sucedido
  - Ou seja, um backdoor significa que a rede já foi atacada e vários ativos podem ter sido comprometidos

Etapas de um Ataque

1. Footprinting (reconhecimento)
2. Scanning (varredura)
3. Enumeration (enumeração)
4. Ganhando acesso (invasão)
5. Escalada de privilégios
6. Acesso à informação
7. Ocultação de rastros
8. Instalação de Back doors (portas de entrada)
9. Denial of Service (negação de serviço)

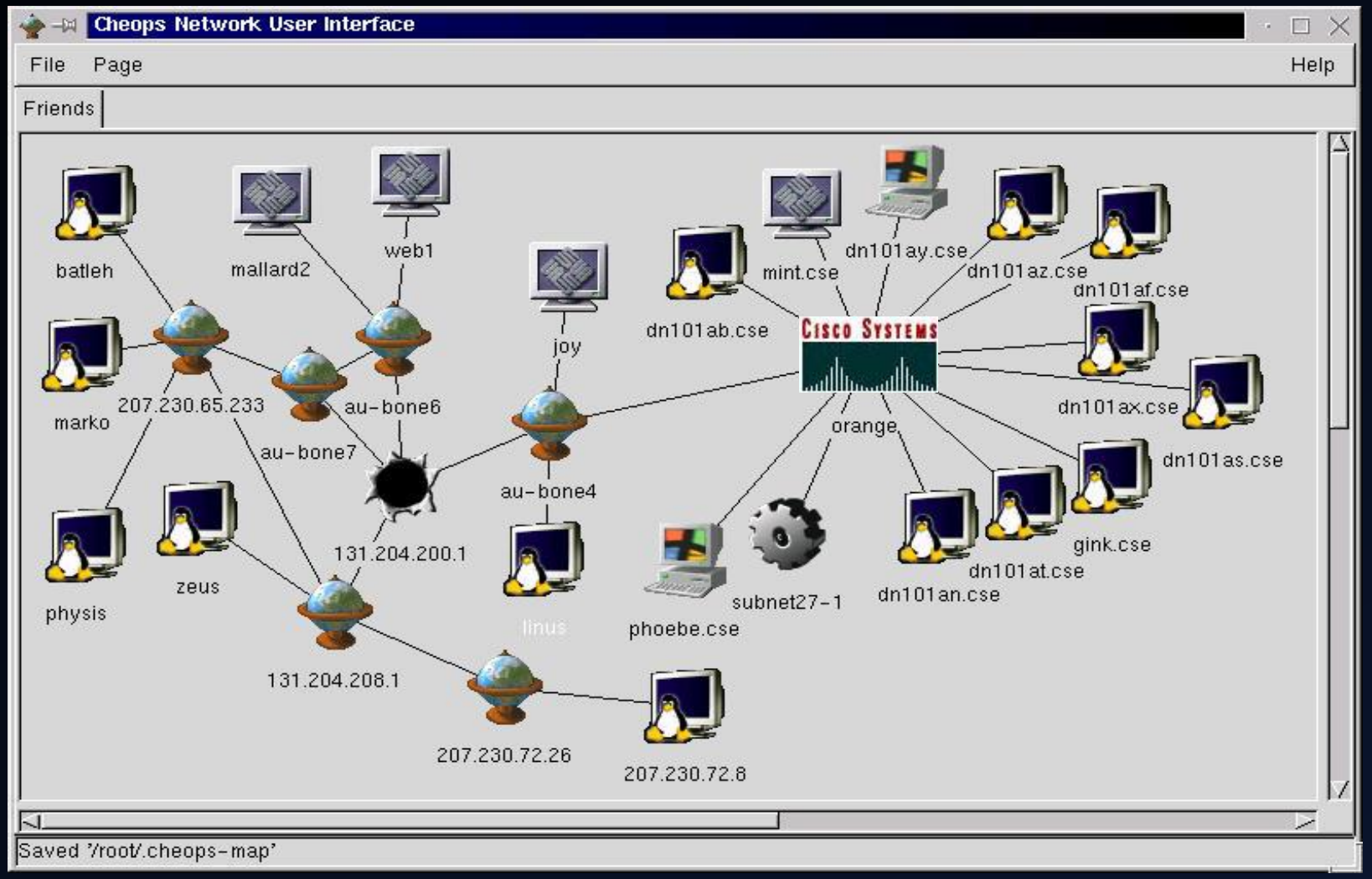
1. Footprinting (reconhecimento)

- Informações básicas podem indicar a postura e a política de segurança da empresa
- Coleta de informações essenciais para o ataque
  - Nomes de máquinas, nomes de login, faixas de IP, nomes de domínios, protocolos, sistemas de detecção de intrusão
- São usadas ferramentas comuns da rede
- Engenharia Social
  - Qual o e-mail de fulano?
  - Aqui é Cicrano. Poderia mudar minha senha?
  - Qual o número IP do servidor SSH? e o DNS?

2. Scanning (varredura ou mapeamento)

- De posse das informações coletadas, determinar
  - Quais sistemas estão ativos e alcançáveis
  - Portas de entrada ativas em cada sistema
- Ferramentas
  - Nmap, system banners, informações via SNMP
- Descoberta da Topologia
  - Automated discovery tools: cheops, ntop, …
  - Comandos usuais: ping, traceroute, nslookup
- Detecção de Sistema Operacional
  - Técnicas de fingerprint (nmap)
- Busca de senhas contidas em pacotes (sniffing)
  - Muitas das ferramentas são as mesmas usadas para gerenciamento e administração da rede

Mapeamento de rede



Tela do Cheops (http://cheops-ng.sourceforge.net)

3. Enumeration (enumeração)

- Coleta de dados intrusiva
  - Consultas diretas ao sistema
  - Está conectado ao sistema e pode ser notado
- Identificação de logins válidos
- Banners identificam versões de HTTP, FTP servers
- Identificação de recursos da rede
  - Compartilhamentos (windows) - Comandos net view, nbstat
  - Exported filesystems (unix) - Comando showmount
- Identificação de Vulnerabilidades comuns
  - Nessus, SAINT, SATAN, SARA, TARA, ...
- Identificação de permissões

4. Ganhando acesso (invasão)

- Informações coletadas norteiam a estratégia de ataque
- Invasores tem uma "base" de vulnerabilidades
  - Bugs de cada SO, kernel, serviço, aplicativo – por versão
  - Tentam encontrar sistemas com falhas conhecidas
- Busca privilégio de usuário comum (pelo menos)
- Técnicas
  - Password sniffing, password crackers, password guessing
  - Session hijacking (sequestro de sessão)
  - Ferramentas para bugs conhecidos (buffer overflow)
- Hackers constróem suas próprias ferramentas

5. Escalada de privilégios

- Uma vez com acesso comum, busca acesso completo ao sistema (administrator, root)
- Ferramentas específicas para bugs conhecidos
  - "Exploits"
- Técnicas
  - Password sniffing, password crackers, password guessing
  - Session hijacking (sequestro de sessão)
  - Replay attacks
  - Buffer overflow
  - Trojans

6. Acesso a informação

- Alguns conceitos relacionados à “informação”
  - Confidencialidade – trata do acesso autorizado
  - Integridade – trata da alteração autorizada
  - Autenticidade – trata da garantia da autoria da informação
  - Disponibilidade – disponível quando desejada, sem demora excessiva (com autorização)
  - Auditoria – trata do registro do acesso
- Invasor pode atuar contra todos os conceitos acima, de acordo com seus interesses

7. Ocultação de rastros

- Invasor usa tenta evitar detecção da presença
- Usa ferramentas do sistema para desabilitar auditoria
- Toma cuidados para não deixar “buracos” nos logs
  - excessivo tempo de inatividade vai denuciar um ataque
- Existem ferramentas para remoção seletiva do Event Log
- Esconde arquivos “plantados” (back doors)

8. Instalação de Back doors

- Objetivo é a manutenção do acesso
  - Rootkits – ferramentas ativas, mas escondidas
  - Trojan horses – programas falsificados
  - Back doors – acesso/controle remoto sem autenticação
- Trojans podem mandar informação para invasor
  - Captura teclado
  - Manda um e-mail com a senha
- Rootkits se confundem com o sistema
  - Comandos modificados para não revelar o invasor
- Back doors
  - Sistemas cliente/servidor
  - Cliente na máquina invasora controlando Servidor na máquina remota
  - Não aparecem na "Task List" do Windows NT/2k

9. Denial of Service (negação de serviço)

- Ataques com objetivo de bloquear serviços, através de:
  - Consumo de banda de rede
  - Esgotamento de recursos
  - Exploração de falhas de programação (ex: ping da morte)
  - Sabotagem de Roteamento
  - Sabotagem no DNS
- DDoS →Distributed Denial of Service
  - Ataques coordenados de múltiplas fontes

Tipos de ataque

- Extraído integralmente de:
  - http://www.tecmundo.com.br/seguranca/8284-glossario-do-mal-conheca-os-diferentes-tipos-de-ataque-ao-computador.htm
- Adware: um aplicativo que baixa ou exibe, sem exigir autorização, anúncios na tela do computador.
- Application-Layer Attack: os “ataques na camada de aplicação” podem ser feitos tanto em servidores remotos quanto em servidores de rede interna. São ataques nas comunicações dos aplicativos, o que pode gerar permissões de acesso aos crackers em computadores infectados. Aplicativos que utilizam base de dados online (como Adobe Reader) também podem ser atingidos.

Tipos de ataque

- Backdoor: traduzindo literalmente, “porta dos fundos”. São falhas de segurança no sistema operacional ou em aplicativos, que permitem que usuários acessem as informações dos computadores sem que sejam detectados por firewalls ou antivírus. Muitos crackers aproveitam-se destas falhas para instalar vírus ou aplicativos de controle sobre máquinas remotas.
- Black Hat: o mesmo que “Cracker”. São os usuários que utilizam os conhecimentos de programação para causar danos em computadores alheios.

Tipos de ataque

- Bloatware: os “softwares bolha” não são considerados aplicativos de invasão. Na verdade, são programas que causam perda de espaço livre nos computadores por serem muito maiores do que deveriam ser. Ou possuem muitas funções, mas poucas que são realmente funcionais. Alguns dos softwares considerados Bloatwares são iTunes, Windows Vista e Nero.
- Bluebugging: é o tipo de invasão que ocorre por meio de falhas de segurança em dispositivos Bluetooth. Com equipamentos de captura de sinal Bluetooth e aplicativos de modificação sem autorização, crackers podem roubar dados e senhas de aparelhos celulares ou notebooks que possuam a tecnologia habilitada.

Tipos de ataque

- Botnet: são computadores “zumbis”. Em suma, são computadores invadidos por um determinado cracker, que os transforma em um replicador de informações. Dessa forma torna-se mais difícil o rastreamento de computadores que geram spams e aumentam o alcance das mensagens propagadas ilegalmente.

Tipos de ataque

- Crapware: sabe quando você compra um computador pré-montado e ele chega à sua casa com algumas dúzias de aplicativos que você não faz ideia da funcionalidade? Eles são chamados de crapware (em português: software porcaria) e são considerados um “bônus” pelas fabricantes, mas para os usuários são poucos os aplicativos interessantes.
- Compromised-Key Attack: são ataques realizados para determinadas chaves de registro do sistema operacional. Quando o cracker consegue ter acesso às chaves escolhidas, pode gerar logs com a decodificação de senhas criptografadas e invadir contas e serviços cadastrados.

Tipos de ataque

- Data Modification: alteração de dados. O invasor pode decodificar os pacotes capturados e modificar as informações contidas neles antes de permitir que cheguem até o destinatário pré-definido.
- Denial of Service (DoS): “Ataque de negação de serviços” é uma forma de ataque que pretende impedir o acesso dos usuários a determinados serviços. Alvos mais frequentes são servidores web, pois os crackers visam deixar páginas indisponíveis. As consequências mais comuns neste caso são: consumo excessivo de recursos e falhas na comunicação entre sistema e usuário.
- Distributed Denial of Service (DDoS): o mesmo que DoS, mas realizado a partir de vários computadores. É um DoS distribuído.

Tipos de ataque

- DNS poisoning: “envenenamento do DNS” pode gerar alguns problemas graves para os usuários infectados. Quando ataques deste tipo ocorrem, os usuários atingidos conseguem navegar normalmente pela internet, mas seus dados são todos enviados para um computador invasor que fica como intermediário.
- “Drive by Java”: aplicativos maliciosos “Drive-by-download” são arquivos danosos que invadem os computadores quando os usuários clicam sobre alguns anúncios ou acessam sites que direcionam downloads sem autorização. O “Drive-by-Java” funciona da mesma maneira, mas em vez de ser por downloads, ocorre devido à contaminação de aplicativos Java.

Tipos de ataque

- Hacker: são usuários mais curiosos do que a maioria. Eles utilizam essa curiosidade para buscar brechas e falhas de segurança em sistemas já criados. Com esse processo, conseguem muito aprendizado e desenvolvem capacidades de programação bastante empíricas. Quando utilizam estes conhecimentos para causar danos passam a ser chamados de crackers.
- ICMP Attack: ataques gerados nos protocolos de controle de mensagens de erro na internet. Um computador com o IP alterado para o endereço de outro usuário pode enviar centenas ou milhares de mensagens de erro para servidores remotos, que irão enviar respostas para o endereço com a mesma intensidade. Isso pode causar travamentos e quedas de conexão no computador vitimado.

Tipos de ataque

- ICMP Tunneling: podem ser criados túneis de verificação em computadores invadidos, por meio da emissão de mensagens de erro e sobrecarga da conexão. Com isso, arquivos maliciosos podem passar sem interceptações de firewalls do computador invadido, passando por esses “túneis” de maneira invisível.
- IP Spoofing: é uma técnica utilizada por crackers para mascarar o IP do computador. Utilizando endereços falsos, os crackers podem atacar servidores ou computadores domésticos sem medo de serem rastreados, pois o endereço que é enviado para os destinatários é falso.

Tipos de ataque

- Keylogging: é uma prática muito utilizada por ladrões de contas bancárias. Aplicativos ocultos instalados no computador invadido geram relatórios completos de tudo o que é digitado na máquina. Assim, podem ser capturados senhas e nomes de acesso de contas de email, serviços online e até mesmo Internet Banking.

Tipos de ataque

- Lammer: é o termo utilizado por hackers mais experientes para depreciar crackers inexperientes que utilizam o trabalho de outros para realizar suas invasões. Não se limitam a invadir sites, quando o fazem modificam toda a estrutura e até assinam as “obras” em busca de fama na comunidade.
- Logic Bomb: este termo pode ser empregado em dois casos. O primeiro refere-se a programas que expiram após alguma data e então deixam de apresentar algumas de suas funcionalidades. O segundo, mais grave, é utilizado em casos de empresas que utilizam aplicativos de terceiros e quando os contratos são rompidos, estes softwares ativam funções danosas nos computadores em que estavam instalados.

Tipos de ataque

- Malware: qualquer aplicativo que acessa informações do sistema ou de documentos alocados no disco rígido, sem a autorização do administrador ou usuário, é considerado um malware. Isso inclui vírus, trojans, worms, rootkits e vários outros arquivos maliciosos.
- Man-in-the-Middle-Atack: este tipo de ataque ocorre quando um computador intercepta conexões de dois outros. Cliente e servidor trocam informações com o invasor, que se esconde com as máscaras de ambos. Em termos mais simples: pode ser um interceptador de uma conversa de MSN, que passa a falar com os dois usuários como se fosse o outro.

Tipos de ataque

- Password-based Attacks: é o tipo de ataque gerado por programas criados no intuito de tentar senhas repetidas vezes em curtos intervalos de tempo. Criando instabilidades na verificação do logon referido, podem ser geradas duplicatas de senhas ou logons válidos.
- Ping of Death: um invasor realiza constantes Pings na máquina invadida para causar travamentos na banda e até mesmo para travar o computador. É um tipo de ataque Denial of Service.
- Phishing: mensagens de email enviadas por spammers são criadas com interfaces e nomes que fazem referência a empresas famosas e conhecidas, como bancos. Nestas mensagens são colocados links disfarçados, que dizem ser prêmios ou informações sobre a empresa em questão, mas na verdade são arquivos maliciosos.

Tipos de ataque

- Phreaker: os hackers de telefonia. São responsáveis pelo roubo de sinal de outros aparelhos e também por desbloquear aparelhos famosos, como é o caso dos especializados em desbloqueio do iPhone.
- Pod Slurping: é o nome atribuído às práticas de roubo de informações por meio de dispositivos portáteis pré-configurados para a atividade. Podem ser utilizados pendrives, iPods e muitos outros aparelhos de armazenamento portátil. Há ataques diretos desta maneira e também ataques que apenas abrem portas dos computadores para invasões.
- Port Scanning: atividade realizada por Port scanners. É a varredura de servidores em busca de portas vulneráveis para a invasão posterior.

Tipos de ataque

- Repudiation Attacks: quando aplicativos ou sistemas não são criados com os comandos corretos de rastreamento de logs, crackers podem utilizar isso para remodelar os envios de comandos. Assim, podem ser modificados os dados de endereçamento das informações, que são enviadas diretamente para servidores maliciosos.
- Rootkit: tipo de malware que se esconde nas bases do sistema operacional, em localidades que não podem ser encontradas por antivírus comuns. São utilizados para interceptar solicitações do sistema operacional e alterar os resultados.

Tipos de ataque

- Scareware: malwares que são acessados pelos usuários mais desavisados, pois ficam escondidos sobre banners maliciosos. Podem ser percebidos em páginas da web que mostram informações do tipo: “Você está infectado, clique aqui para limpar sua máquina”.
- Session hijacking: roubo de 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 todos os roubos de informações e modificações que desejar.
- Scanners: são softwares que varrem computadores e sites em busca de vulnerabilidades.
- Script Kiddy: o mesmo que Lammer.

Tipos de ataque

- Server Spoofing: o mesmo que IP Spoofing, mas direcionado a servidores VPN.
- Sidejacking: prática relacionada ao Session hijacking, mas geralmente com o invasor e a vítima em uma mesma rede. Muito frequentes os ataques deste tipo em hotspots Wi-Fi sem segurança habilitada.
- Shovelware: é o tipo de aplicativo que se destaca mais pela quantidade de funcionalidades do que pela qualidade das mesmas. Muitos conversores multimídia fazem parte deste conceito de shovelware.

Tipos de ataque

- SMiShing: similar a phishing, mas destinado a celulares (SMS).
- Smurf: o mesmo que ICMP Attack.
- Sniffer Attack: tipo de ataque realizado por softwares que capturam pacotes de informações trocados em uma rede. Se os dados não forem criptografados, os ofensores podem ter acesso às conversas e outros logs registrados no computador atacado.
- Snooping: invasões sem fins lucrativos, apenas para “bisbilhotar” as informações alheias.

Tipos de ataque

- Social Engineering (Engenharia Social): é o ato de manipular pessoas para conseguir informações confidenciais sobre brechas de segurança ou mesmo sobre senhas de acesso a dados importantes.
- Spam: mensagens enviadas em massa para listas conseguidas de maneira ilegal. Geralmente carregam propagandas sobre pirataria de medicamentos. Também podem conter atalhos para páginas maliciosas que roubam listas de contatos e aumentam o poder de ataque dos spammers.
- Spoof: mascarar informações para evitar rastreamento.
- Spyware: são aplicativos (malwares) instalados sem o consentimento dos usuários. Eles são utilizados para capturar informações de utilização e navegação, enviando os logs para os invasores. Keyloggers fazem parte desta denominação.

Tipos de ataque

- TCP Syn / TCP ACk Attack: ataques realizados nas comunicações entre servidor e cliente. Sendo enviadas mais requisições do que as máquinas podem aguentar, a vítima é derrubada dos servidores e perde a conexão estabelecida. Podem ocorrer travamentos dos computadores atingidos.
- TCP Sequence Number Attack: tentativas de previsão da sequência numérica utilizada para identificar os pacotes de dados enviados e recebidos em uma conexão. Quando é terminada com sucesso, pode emular um servidor falso para receber todas as informações do computador invadido.

Tipos de ataque

- TCP Hijacking: roubo de sessão TCP entre duas máquinas para interferir e capturar as informações trocadas entre elas.
- Teardrop: uma forma de ataque Denial of Service. Usuários ofensores utilizam IPs inválidos para criar fragmentos e sobrecarregar os computadores vitimados. Computadores mais antigos podiam travar facilmente com estes ataques.
- Trojan: tipo de malware que é baixado pelo usuário sem que ele saiba. São geralmente aplicativos simples que escondem funcionalidades maliciosas e alteram o sistema para permitir ataques posteriores.

Tipos de ataque

- Vírus: assim como os vírus da biologia, os vírus de computador não podem agir sozinhos. Anexam-se a outros arquivos para que possam ser disseminados e infectar mais computadores. São códigos que forçam a duplicação automática para aumentar o poder de ataque e, assim, criar mais estrago.
- White Hat: hackers éticos.
- Worm: funcionam de maneira similar aos vírus, mas não precisam de outros arquivos hospedeiros para serem duplicados. São arquivos maliciosos que podem replicar-se automaticamente e criar brechas nos computadores invadidos. Disseminam-se por meio de redes sem segurança.

ACH2014 – Fundamentos de Sistemas de Informação

AULA 11 – SEGURANÇA EM SISTEMAS DE INFORMAÇÃO

Prof. Marcelo Medeiros Eler
marceloeler@usp.br