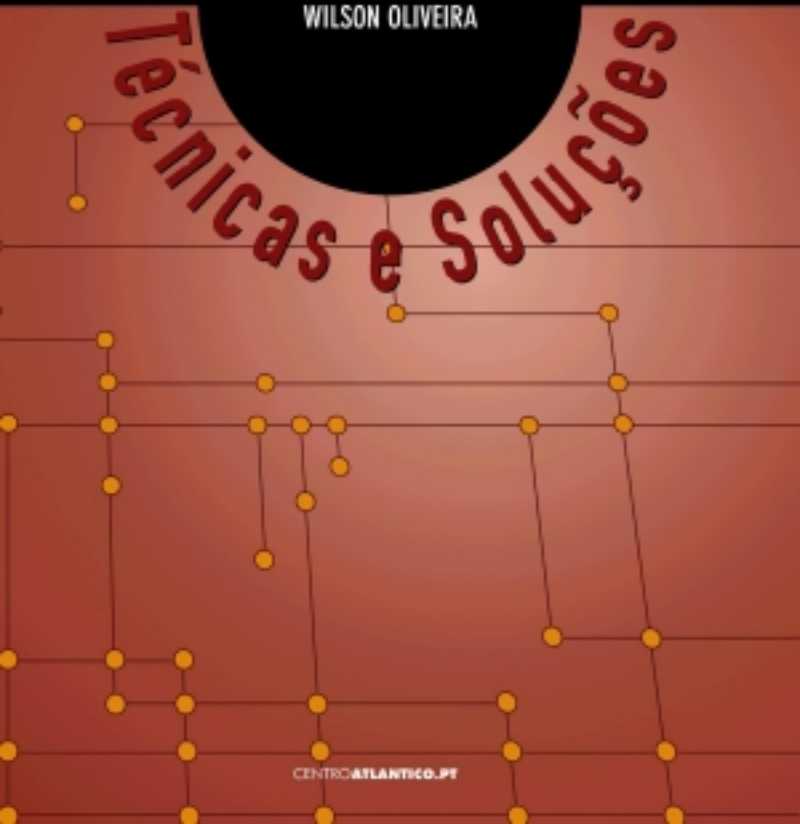
SEGURANÇA da informação

WILSON OLIVEIRA

Técnicas e Soluções



CENTROATLANTICO.PT

Wilson Oliveira

Segurança da Informação
Técnicas e Soluções

Portugal/2001

SEGURANÇA DA INFORMAÇÃO – TÉCNICAS E SOLUÇÕES

Colecção: Sociedade da Informação

Autor: **Wilson Oliveira**

Direcção gráfica: Centro Atlântico

Revisão: Nuno Garcia Lopes

Capa: Paulo Buchinho

Ap. 413 – 4764-901 V. N. Famalicão

Porto - Lisboa

Portugal

Tel. 808 20 22 21

geral@centroatlantico.pt

www.centroatlantico.pt

Fotolitos: Centro Atlântico

Impressão e acabamento: Inova

1ª edição: Outubro de 2001

ISBN: 972-8426-44-5

Depósito legal: 170.705/01

SOBRE O AUTOR

Wilson José de Oliveira é administrador de empresas e analista de sistemas, com larga experiência em desenvolvimento de sistemas cliente/servidor e sistemas para *e-commerce* utilizando principalmente as linguagens Delphi, Visual C++, C++ Builder, ASP, Java, PERL e as bases de dados Oracle, MS-SQL Server e Interbase.

Actualmente o autor é gestor de TI, sendo responsável técnico por soluções de *e-business*, *m-business* e CRM, e lecciona MBA Executivo Internacional com ênfase em *e-business* na Fundação Getúlio Vargas (FGV – Brasil) e Ohio University (EUA).

1

INTRODUÇÃO

Diariamente, no mundo inteiro, redes de computadores e *hosts* são sendo invadidos. O nível de sofisticação destes ataques varia amplamente; enquanto geralmente se acredita que a maioria das invasões tem sucesso devido a códigos secretos fracos, há ainda um número grande de intrusões que usam técnicas mais avançadas para invadir. Pouco se sabe sobre a maioria das técnicas de invasão, porque elas podem ser de diversa natureza e então tornam-se muito mais difíceis de descobrir.

Até à década de 80, quando experiências iniciadas no projecto ARPANET conseguiram estabilizar um primeiro protocolo para *routing* de dados entre redes autónomas (BGP 4, que ainda faz parte do conjunto de padrões TCP/IP), a tecnologia para interligação de computadores permitia apenas redes com hierarquia fixa, que pressupõem o controlo de algum meio ou infra-estrutura de comunicação, usado para interligar os seus componentes. O projecto ARPANET foi motivado por um sentimento de insegurança e relativa paranóia em relação ao risco de ataque nuclear a que estava exposta a infra-estrutura de telecomunicações das forças armadas norte-americanas, dando início ao desenvolvimento de tecnologia para redes abertas, onde redes de computadores já operantes poderiam ser interligadas sem necessidade de reestruturação do meio de comunicação que fossem utilizar e sem necessidade de controlo centralizado no processo de *routing* adaptativo para o tráfego de pacotes de dados.

A tecnologia de redes com hierarquia aberta para transmissão de dados permitiu que interligações entre computadores pudessem

atingir escala mundial, ao evitar o colapso decorrente da explosão exponencial das tabelas de *routing*, já que tal explosão seria inevitável em arquitecturas fechadas nesta escala, criando assim o potencial de interligação via TCP/IP através da infra-estrutura mundial de telecomunicações então disponível. O serviço de tipo "melhor esforço" para *routing* de pacotes IP pôde utilizar-se da capacidade ociosa inerente às redes de transmissão e comutação telefónica, para fornecer ligações de dados em escala mundial às redes de computadores já existentes, pela adesão aos protocolos de transporte TCP e UDP. Este potencial de interligação relativamente simples e barato induziu a sua própria procura, forçando mudanças em cascata no perfil da procura tecnológica e de serviços nas telecomunicações.

Estas explosões da procura, e a transformação social que engendram, ocorrem num contexto cognitivo inédito para a humanidade. Até aos anos 80 a forma de se conceberem redes de computadores, a nossa tradição cultural que legitima a autoridade dos discursos, a nossa organização social que transmite e consolida valores, moldando assim a nossa percepção e acção no mundo, sempre se haviam enquadrado em modelos hierárquicos fechados de redes de comunicação. A Internet não se enquadra, e tentar enquadrá-la por força do hábito constitui aquilo que designamos por verdadeiro *bug* do milénio. Referências à "Internet comercial" não implicam, como o termo pode sugerir, a sua posse ou controlo por alguma empresa, mas a etapa da sua evolução na qual empresas vendendo transporte e distribuição de tráfego electrónico de dados, serviços ou produtos, passam a criar associações estratégicas para desempenhar com melhor fiabilidade e eficácia as suas funções. A Internet não tem dono, gestor, comando central ou direcção. Guia-se por um método de cooperação *sui generis* para propostas e validações de novos padrões operacionais e políticas de gestão cooperada.

A Criptografia pode proteger o acesso ao valor sintáctico e a integridade das cadeias de bits nas comunicações de dados, o

que é apenas um dos ângulos da questão que estamos a abordar. Precisamos confiar não apenas nos controlos de acesso a essas cadeias de bits e na sua integridade, mas principalmente no significado das mensagens que estas cadeias veiculam. Precisamos confiar no significado do que se desenha no ecrã do monitor e dos programas que se executam no CPU de nossas máquinas, expressos através dessas cadeias de bits, sendo portanto sensato associar este outro lado da questão, de natureza semântica, à nossa percepção sobre origens e intenções nas comunicações dessas cadeias. É aí que o alcance e os limites das técnicas criptográficas – e as diferenças fundamentais entre redes de hierarquia fixa e aberta – começam a se manifestar. A compreensão de significados inicia-se pela identificação de referências a significantes. E as redes "fluidas" apresentam sérios problemas relacionados com a confiança que se pode ter em processos de identificação que nelas operam.

Nenhuma área da informática é tão vasta e apreciada como a segurança da informação: o ponto principal da segurança leva a um outro ponto principal, o ser humano, isso mesmo, todo o processo de segurança se inicia e tem o seu término num ser humano. Não adianta nada gastarmos fortunas em equipamentos e sistemas de segurança se não conhecermos quem utilizará os nossos sistemas, e quem pode ter acesso a eles mesmo sem autorização.

No ciberespaço, a percepção do que é ser herói ou bandido dissipa-se nos interesses pessoais, opções políticas, ideologias e vínculos ao poder, e a acção puramente sintáctica da criptografia encontra enormes obstáculos para realizar o papel principal que pode exercer no processo da segurança de redes fechadas.

Neste livro iremos mostrar alguns métodos para segurança de sistemas. Em vez de meramente falar sobre os problemas, vamos observar através dos "olhos" de um intruso em potencial (com os olhos de um intruso), e mostrar "por que" ele é um intruso. Vamos mostrar que até mesmo aparentemente inofensivos serviços de

rede podem ser valiosas ferramentas para pesquisar os pontos fracos de um sistema, e que mesmo quando os serviços operam correctamente eles são usados para ataques.

Num esforço para irradiar alguma luz sobre a forma como as mais avançadas invasões ocorrem, este livro descreve vários mecanismos que os *crackers* usam actualmente para obter acesso a sistemas e, em complemento, algumas técnicas que qualquer intruso suspeito pode usar, ou que usamos nas nossas próprias máquinas ou em máquinas de amigos ou com autorização do administrador.

A motivação para escrever este livro é que se os administradores de sistemas frequentemente não sabem ou não sentem a presença do perigo também não conhecem os ataques triviais. Também para informar que o nível de protecção depende do que deve ser protegido. Muitos *sites* parecem ter carência de documentos para avaliar que nível de segurança é adequado para computadores e redes. Para mostrar o que os intrusos podem fazer para conseguir acesso a um computador remoto, vamos tentar montar uma ajuda para os administradores de sistemas ficarem "informados" de quanto os seus *sites* são seguros – ou não. Vamos limitar a discussão a técnicas que podem permitir a um intruso remoto ter acesso (talvez não interactivo) *shell* em máquinas UNIX.

Deixamos claro que o objectivo deste livro é testar a segurança do seu próprio *site*, e não invadir sistemas de terceiros. As técnicas de invasão que vamos mostrar aqui com frequência deixam registos nos seus ficheiros de *log* – isto talvez seja construtivo para examinar após tentar algumas das técnicas de ataque, para ver o que um ataque real talvez o deixe ver. Certamente outros *sites* e administradores de sistemas vão ver as suas actividades se você decidir usar estas técnicas nas máquinas deles para testar a segurança sem a sua autorização; pode ser que não digam nada, mas se perceberem que é um ataque é provável que acções legais sejam movidas contra si.

2

TERMOS TÉCNICOS

De início vamos fornecer alguns dos principais termos técnicos que serão utilizados no decorrer desta obra, sendo muito interessante que o leitor os verifique para ter um melhor entendimento global da mesma.

Access Control Lists (ACL):
Lista de permissões de acesso configuradas em dispositivos de rede, principalmente *routers* e *firewall*.

Ameaça:
A tentativa de atacar um sistema explorando as suas vulnerabilidades. Qualquer elemento humano ou da natureza que pode causar dano à confidencialidade, integridade e disponibilidade dos sistemas. As ameaças podem ser intencionais ou não intencionais, internas ou externas.

Ataque CGI:
Ataque que explora vulnerabilidades do Common Gateway Interface.

Backdoor:
Programa implementado secretamente num computador com o objectivo de obter informações e dados armazenados, interferir com a operação ou obter controlo total do sistema.

BSI - British Standard Institute:
Órgão britânico responsável pela publicação de normas, entre as quais as normas de segurança para informática BS 7799.

CERT - Computer Emergency Response Team:
Órgão destinado a investigar os ataques e a melhorar a segurança na Internet.

Detector de Intrusos:
Sistema inteligente de análise e detecção automática de ataques ou eventos suspeitos na rede ou nos servidores.

DIG - Domain Information Gopher:
Ferramenta utilizada para procurar informações em servidores DNS.

DMZ (de-militarized zone):
Termo que designa a rede localizada entre a rede interna e a Internet. Na DMZ normalmente estão localizados os servidores de acesso público.

DNS - Domain Name Service:
Serviço de replicação que interpreta os números pelos quais os servidores ligados à Internet são identificados e os apresenta ao utilizador como um nome textual. Por exemplo, 10.10.10.10 como www.nome.com.pt .

DoS; DDoS - Denial of Service e Distributed Denial of Service:
Ataques cujo objectivo é a retirada de serviço de um *site*, servidor ou outro dispositivo ligado à Internet. O termo Distributed refere-se a um aperfeiçoamento da técnica do ataque, na qual a sua origem é distribuída por até milhares de computadores.

ÍNDICE