“Grampos Digitais” Utilizando Software Livre

Ricardo Kléber Martins Galvão, Naris, Superintendência de Informática, UFRN

***Resumo*—Na apuração de crimes digitais e, mais especificamente, de crimes praticados utilizando microcomputadores, geralmente utilizam-se técnicas post-mortem, nas quais o sistema é periciado após o desligamento da máquina, cabendo ao perito a duplicação das mídias e avaliação de evidências armazenadas e/ou recentemente apagadas. Em muitos casos porém, (especialmente quando a máquina está conectada à Internet), para a realização da coleta de evidências é necessária a interceptação (“grampo”) dos dados em “tempo-real”, ou seja, a captura dos dados deve ser realizada com a máquina ligada e em utilização pelo(s) indivíduo(s) investigado(s). Este artigo tem por objetivo apresentar técnicas eficazes de captura e análise de tráfego (não encriptado) para utilização em casos de perícia envolvendo a utilização de microcomputadores ligados em rede. As ferramentas apresentadas são baseadas em software livre, isto é, sem custo adicional de software, perfeitamente aplicáveis nesta situação, além de adequadas a todos os orçamentos previstos para a atividade pericial.**

***Index Terms*—Computer Forensics, Network Security**

I. Definições na Área de Perícia Forense Aplicada à Informática

As investigações periciais em sistemas computacionais utilizam alguns termos, conforme definidos a seguir:

A. Perícia Forense Aplicada á Informática

Também conhecida como processo de análise de provas digitais ou análise de mídias informáticas, pode ser definido como o processo de extrair de sistemas computacionais dados que valham como prova.

1) Mídia de provas

O objeto (físico) real da investigação, isto é, o equipamento (e seus periféricos) que podem conter as provas procuradas, como arquivos armazenados em disco ou memória ou responsável pelo recebimento/geração de dados trafegados em rede quando estes forem os objetos da investigação.

2) Mídia de destino

O destino dos dados capturados e/ou copiados da mídia de provas. É a imagem pericial sobre a qual serão realizados os procedimentos de análise e busca por provas.

3) Análise ao Vivo

Análise realizada durante os procedimentos de coleta de dados (em tempo real), isto é, diretamente sobre a mídia de provas ou sobre o tráfego capturado de/para ela.

4) Análise Off-Line

Análise feita sobre a mídia de destino após a coleta de dados a partir da máquina e/ou rede investigada..

II. Preservação de “Local de Crime”

Na perícia forense tradicional, a preservação de “Local de Crime” consiste em isolar fisicamente todo o perímetro que contorna o ambiente em que foi praticado o delito de modo a preservar evidências, isto é, evitar que alguém possa manipular os componentes que serão periciados sem os cuidados recomendados.

Na perícia forense computacional, o “Local de Crime” é praticamente todo virtual, isto é, apesar dos componentes físicos utilizados para a prática do delito (microcomputador e periféricos a ele conectados), todos os indícios necessários estão em nos dados armazenados no interior da CPU em seu disco rígido e, em alguns casos, na memória principal.

III. Coleta de Evidências

Embora a definição de coleta de evidências seja bastante abrangente, já que engloba aspectos relacionados ao ambiente periciado, ferramentas e técnicas utilizadas para esta coleta, para este artigo, o procedimento de coleta de evidências restringir-se-á às modalidades relacionadas à captura de dados via rede, isto é, gerados a partir de uma máquina e/ou rede investigada e coletados utilizando "grampos" na rede utilizada para a comunicação.

Para a utilização dos conceitos apresentados neste artigo, supõe-se a autorização total para a interceptação de conteúdo das comunicações entre as máquinas das redes envolvidas (em todos os níveis da pilha de protocolos TCP/IP). A autorização total é necessária já que, em determinados casos, somente a interceptação de informações de transações (cabeçalhos dos pacotes) são autorizadas, impedindo o acesso aos dados dos usuários (necessários a este tipo de "grampo"), restringindo os resultados da coleta a determinação da origem e destino das comunicações.

A. Ferramentas Utilizadas

1) Tcpdump

Ferramenta para operação em modo texto que funciona como sniffer, capturando todos os pacotes que se apresentem os elementos da filtragem especificada em seus parâmetros de configuração de consulta.

Esta ferramenta será apresentada exclusivamente como mecanismo de captura de pacotes e geradora de arquivo binário para utilização pelo Wireshark.

2) Wireshark

Ferramenta em modo gráfico que tanto funciona como sniffer capturador de pacotes, como analisador de pacotes off-line (aceitando o padrão gerado pelo tcpdump por exemplo) e remontador de Streams TCP.

B. "Grampos" Digitais Utilizando Sniffers

Um sniffer é um hardware ou software que intercepta passivamente os pacotes que passam por uma rede. Os sniffers mais comuns são programas que permitem a uma placa de interface de rede (NIC) processar pacotes destinados a várias máquinas diferentes. Os sniffers baseados em software funcionam pondo o adaptador de rede em "modo promíscuo", que tem esse nome por aceitar todo o tráfego com o qual tem contato.

A instalação de sniffers tem por objetivo capturar todo o tráfego em uma rede, mesmo que o endereço de destino não seja o da máquina onde o sniffer está instalado.

Para realizar esta captura têm-se, basicamente, dois cenários:

1) O Sniffer Instalado em uma Rede Baseada em Hubs

2) O Sniffer Instalado no Roteador

O Roteador é o equipamento responsável pelo repasse de pacotes de/para a rede, ou seja, realiza a "ponte" entre uma rede e outra (uma Intranet e a Internet, ou entre duas redes internas por exemplo).

A instalação de um sniffer no roteador principal de uma rede investigada possibilita tanto a captura de todos os pacotes com origem na máquina/rede investigada destinados à rede externa como dos pacotes vindos da rede externa e destinados à rede/máquina investigada.

Em se tratando de uma atividade pericial, devidamente autorizada, e a conseqüente liberação de acesso a este equipamento para a instalação do sniffer esta operação independe da estrutura de conectividade da rede investigada, já que neste caso não importa se a rede utiliza hubs ou switches, a informação é coletada diretamente no roteador.

Dois são os problemas que podem surgir com esta modalidade de "grampo"

a) Embora um grande número de redes utilize microcomputadores com duas ou mais interfaces de rede para realizar a função de roteamento (ambiente ideal para a instalação do sniffer), algumas redes optam pela utilização de roteadores convencionais, isto é, equipamentos específicos para a função de roteamento, não permitindo a instalação de softwares como um

sniffer. Neste caso, é aconselhável que uma outra máquina (roteador) seja instalada entre o roteador e a intranet para forçar o tráfego a passar por este equipamento onde, finalmente, deve ser instalado o sniffer.

b) A atividade de roteamento demanda processamento e memória do equipamento, além do atraso gerado pela análise dos pacotes antes do encaminhamento ao destino, transformando os roteadores em "gargalos" naturais. A instalação de outros softwares (como um sniffer) nestes equipamentos, dependendo do volume de tráfego, pode significar um retardo adicional no encaminhamento de pacotes tal que inviabilize a operação ou, pelo menos, altere o comportamento normal da rede com relação ao acesso externo, podendo, assim, levantar suspeitas por parte dos investigados.

C. "Grampos" Digitais Utilizando Cópias de Pacotes a partir do Roteador

Este tipo de grampo consiste em retirar uma cópia de cada pacote que passa pelo roteador e enviá-la a uma rede/máquina para análise posterior.

O Netfilter/Iptables, solução de firewall utilizado por padrão nas novas versões do sistema operacional Linux suporta módulos em forma de extensão ao modelo original, permitindo a manipulação das mensagens que passam pelo roteador/firewall de acordo com necessidades específicas.

Para a realização da cópia de cada pacote que atravessa o roteador/firewall Linux baseado em Netfilter/Iptables, pode-se utilizar a extensão --ROUTE desenvolvida por Cédric de Launois, ainda em fase experimental mas bastante estável utilizada inicialmente para realizar reroteamento, ou seja, alterar a tabela de rotas de cada pacote reroteando-o para outra rede ou máquina.

O parâmetro --tee, desenvolvido por Patrick Schaaf, adicionado a esta extensão permite que o firewall/roteador realize o roteamento dos pacotes sem interferência direta, mas, retire uma cópia de cada um deles enviando-as para uma rede ou máquina específica.

Uma linha de exemplo para este tipo de "grampo" seria um cenário em que todos os pacotes destinados à servidores Web (porta 80/TCP) ao passar pelo roteador seriam copiados para a máquina 10.10.10.10 antes de serem submetidos a outras regras de filtragem/roteamento:

```
iptables -A PREROUTING -t mangle -p tcp --dport 80 -j
            ROUTE --gw 10.10.10.10 --tee
```

Assim, todo o tráfego Web seguiria até o seu destino, sem retardo adicional, porém todos os pacotes seriam copiados para uma máquina específica onde seria realizada a perícia posteriormente.

Para a utilização desta extensão, porém, é necessária a aplicação de um patch específico no kernel do Linux e no próprio Iptables, além da recompilação de ambos para a ativação da nova funcionalidade.

IV. Análise de Evidências

Desviando via Netfilter/Iptables/ROUTE/tee todos os pacotes vindos da rede/máquina investigada para uma estação pericial, ferramentas específicas são então utilizadas para realizar a separação de tráfego em arquivos específicos para a análise posterior.

A. Ferramentas Utilizadas

Para a coleta de dados a ferramenta utilizada é a tcpdump, gravando em formato binário (parâmetro -w). Para a leitura (remontagem de sessão) utiliza-se a ferramenta Wireshark, funcionalidade Follow TCP Stream.

B. Separando e Analisando Tráfego Telnet

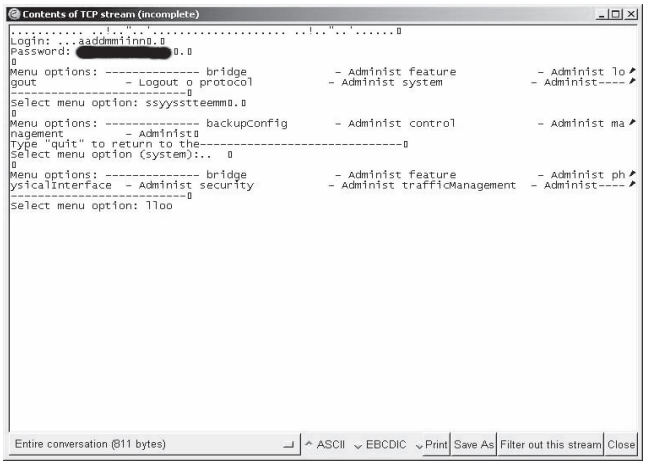
O Telnet é um protocolo de comunicação remota em modo texto que, por padrão, não utiliza encriptação dos dados, sendo, portanto, vulnerável a "grampos". Mesmo as senhas dos usuários de comunicações remotas via telnet podem ser facilmente capturadas por um "grampo".

Para realizar a separação do tráfego Telnet dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 23/TCP.

```
tcpdump –X –v –i <interface> port 23 -w
          <arquivo_específico>
```

A análise deste tipo de tráfego em “grampos” nem sempre apresenta resultados consistentes, já que não é um protocolo utilizado por usuários com pouco conhecimento técnico e, mesmo os usuários com um maior conhecimento técnico que desejam realizar comunicação remota em modo texto têm optado por utilizar o SSH, protocolo semelhante, porém, com tráfego de dados e autenticação encriptados, isto é, imune a “grampos”.

A análise apresentada a seguir é feita utilizando o Wireshark e remontando as sessões Telnet encontradas no arquivo gerado pelo tcpdump.



Neste caso a seção capturada apresenta o Login e senha (Password) para acesso a algum ativo de rede baseado em menus. Os caracteres aparecem duplicados pelo “echo” do Telnet.

C. Separando e Analisando Tráfego Web (HTTP)

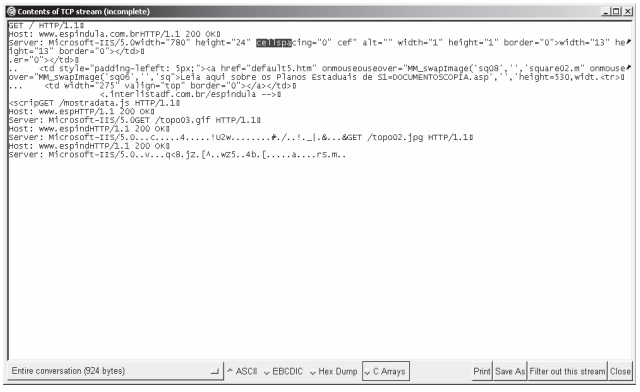
O HTTP é um dos protocolos de comunicação mais utilizados por usuários de todos os níveis e, apesar disso, não utiliza encriptação dos dados, sendo, portanto, vulnerável a “grampos”. Mesmo as senhas dos usuários de comunicações remotas via HTTP podem ser facilmente capturadas por um “grampo”.

Para realizar a separação do tráfego HTTP dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 80/TCP.

```
tcpdump –X –v –i <interface> port 80 -w
          <arquivo_específico>
```

A análise deste tipo de tráfego em “grampos” pode ser inviabilizada se o usuário utiliza, para a navegação Web, ao invés do protocolo HTTP o HTTPS, protocolo semelhante, porém, com tráfego de dados e autenticação encriptados, isto é, imune a “grampos”.

A análise apresentada a seguir é feita utilizando o Wireshark e remontando as sessões HTTP encontradas no arquivo gerado pelo tcpdump.



Neste exemplo específico, a remontagem de pacotes envolvidos na comunicação apresentam detalhes sobre um site acessado pela máquina investigada (endereço, sistema operacional do servidor e detalhes sobre a página visitada)

D. Separando e Analisando Tráfego FTP

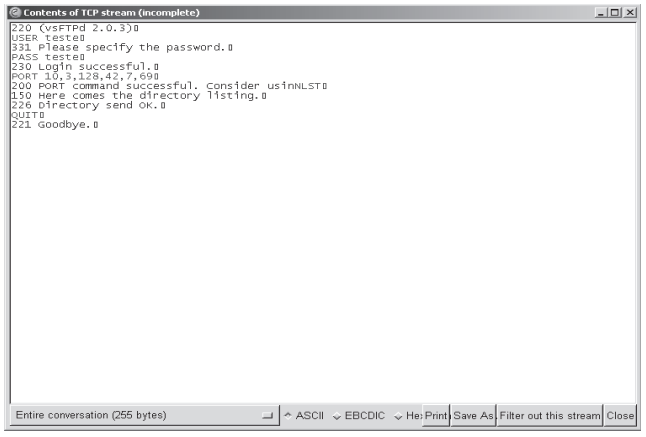
O FTP é um protocolo de comunicação bastante utilizado para transferência de arquivos entre máquinas via rede e, apesar disso, não utiliza encriptação dos dados, sendo, portanto, vulnerável a “grampos”. Mesmo as senhas dos usuários de comunicações remotas via FTP podem ser facilmente capturadas por um “grampo”.

Para realizar a separação do tráfego FTP dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino às porta 21/TCP e 20/TCP.

```
tcpdump –X –v –i <interface> port 20 or
    port 21 -w <arquivo_específico>
```

A análise deste tipo de tráfego em “grampos” pode ser inviabilizada se o usuário utiliza, para a transferência de arquivos via rede, ao invés do protocolo FTP o SCP, protocolo semelhante, porém, com tráfego de dados e autenticação encriptados, isto é, imune a “grampos”.

A análise apresentada a seguir é feita utilizando o Wireshark e remontando as sessões FTP encontradas no arquivo gerado pelo tcpdump.



Neste exemplo específico, a remontagem de pacotes envolvidos na comunicação apresentam Login do usuário (USER), senha (PASS) e comando digitado, neste caso, o usuário apenas solicitou a listagem de diretórios na máquina remota.

E. Separando e Analisando Tráfego de E-mails (SMTP, POP3 e IMAP)

Os protocolos relacionados ao serviço de Correio Eletrônico são, sem dúvida, os mais utilizados por usuários de todos os níveis e, apesar disso, não utilizam encriptação dos dados, sendo, portanto, vulnerável a “grampos”. Mesmo as senhas dos usuários de comunicações remotas via POP3 ou IMAP podem ser facilmente capturadas por um “grampo”.

Para realizar a separação do tráfego SMTP dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 25/TCP.

Para realizar a separação do tráfego POP3 dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 110/TCP.

Para realizar a separação do tráfego IMAP dos demais, na estação pericial, basta aplicar um filtro utilizando o tcpdump selecionando apenas os dados com origem ou destino à porta 143/TCP.

```
tcpdump –X –v –i <interface> port 25 or
        port 110 or port 143 -w
          <arquivo_específico>
```

A análise deste tipo de tráfego em “grampos” pode ser inviabilizada se o usuário utiliza envio autenticado de e-mails, além dos protocolos de recebimento POP3s e IMAPs, protocolos semelhantes, porém, com tráfego de dados e autenticação encriptados, isto é, imune a “grampos”.

Neste caso o Wireshark pode ser utilizado para remontar seções SMTP capturadas via tcpdump e verificar todos os e-mails enviados, com o Endereço IP de origem e endereço de e-mail de destino.

A remontagem de seções POP3 ou IMAP apresentam (ambas) informações de Login/Senha dos usuários que executarem estes serviços.

V. Considerações Finais

A falta de recursos financeiros para a compra de *softwares* comerciais para a realização de perícias em crimes digitais não representa de fato um problema atualmente pela diversidade e robustez das soluções disponíveis baseadas em *software* livre.

Esta apresentação demonstra com detalhes que todos os recursos necessários para a coleta de evidências digitais em “tempo real” estão disponíveis sem custo algum de *software*, muito embora existam soluções comerciais equivalentes, além de custos com treinamentos para utilização destas ferramentas.

References

[1] MANDIA, Kevin, PROSISE Chris, Incidence Response: Investigating Computer Crime, Osborne/McGraw-Hill, 2002.

[2] CASEY, Eoghat, Digital Evidence and Computer Crime, Academic Press, 2004.

[3] SHINDER, Debra L., Scene of the Cybercrime: Computer Forensics Handbook, Ed. Titel, 2002.

[4] Homepage do Projeto Netfilter/Iptables : http://www.netfilter.org

[5] Homepage do Tcpdump/Libpcap : http://www.tcpdump.org

[6] Homepage do Analisador de Protocolos de Rede Wireshark: http://wireshark.org