Análise Forense em Rede de Computadores

Fabiano Santos Florentino – fabianoflorentino@outlook.com
Computação Forense e Perícia Digital
Instituto de Pós-Graduação - IPOG
Goiânia, GO, 02, outubro de 2016

Resumo
Muitas noticias se espalham pela midia de que estão comentendo crimes cibernéticos, quadrilhas de crackers, assaltos a banco, venda ilicita de drogas, armas e tudo mais que se pode querer ilegalmente, roubo de informações de grandes corporações e até mesmo orquestração de atentados terroristas são feitos com o uso da internet e da tecnologia. Muitos pensam que por estar atraz de um sistema computacional se torna intocável ou inalcançavél, mas a tecnologia também anda a favor da justiça, hoje ao contrário do que pensam essas pessoas, pode-se se achar qualquer pessoa em qualquer lugar com as informações e as ferramentas corretas. Com isso, esse documento traz um pouco do conceito de rede de computadores, computação forense e ferremantas que são utilizadas para se realizar grampos digitais para auxilar o judiciario a ter embasamento técnico e teorico para melhor julgar as pessoas por traz de conteúdos ilicitos e de qualquer contravesão feita através das redes de computadores e internet.

Palavras-chave*: crimes cibernéticos, rede de computadores, computação forense.*

1. Introdução

Tendo em vista o crescimento do uso dos meios digitais, se faz necessário o entendimento de técnicas para análise de toda a informação que é gerada. A perícia dessas informações pode trazer respostas a acontecimentos ilícitos feitos através do meio digital. Com isso surge a oportunidade de estudar e se capacitar para oferecer o suporte necessário as autoridades auxiliando e respondendo questões sobre a análise realizada em meios digitais, disponibilizando assim embasamento teórico para que o julgamento seja mais preciso. Todas as pessoas que usam qualquer equipamento digital hoje estão de alguma forma conectado a uma rede de computadores seja ela com ou sem fio gerando grandes volumes de dados. Essas informações ficam armazenadas em registros de dados (*log*) e sobre demanda (*On Demand*). Com a técnica e as ferramentas (*softwares*) corretas, é possível determinar a origem, granularidade, integridade e privacidade, garantindo condições legais dos dados para trata-los como uma evidência.

2. Conceitos de Forense Computacional

A perícia forense fornece suporte especializado aos magistrados julguem da melhor forma, essa perícia é realizada preferencialmente por pessoas com formação e conhecimento especifico, nas mais diversas áreas do conhecimento, para responder a quesitos para os quais o judiciário não dispões de embasamento para julgar com precisão.

> Nesse contexto, a perícia forense em computação, ou computação forense, pode ser definida, de forma superficial, mas direta, como a área da computação responsável por dar respostas ao judiciário em questões envolvendo sistemas operacionais, sejam os objetivos da investigação equipamentos, mídias, estruturas computacionais ou que tenham sido utilizados como meio em atividades sob investigação. Envolve, pois, a obtenção e análise de informações digitais e/ou equipamentos, infraestrutura e mídias

> computacionais para o uso como evidências em casos cíveis, criminais ou administrativos. (M. GALVÃO, 2013:19)

3. Redes de Computadores

Define-se rede de computadores um conjunto de computadores independentes interligados pela mesma tecnologia, dois ou mais computadores estão interconectados quando trocam informações entre si. Existem muitas maneiras de se interligar computadores, fio de cobre, fibras óticas, micro-ondas, ondas de infravermelho e até mesmo satélite. As redes podem ser de diversos tamanhos, modelos e formatos. Um dos propósitos de se criar redes é para interliga-las e criar redes ainda maior assim como a internet é hoje.

> Rede de computadores ou network caracteriza-se por dois ou mais computadores, interligados por qualquer meio, capazes de trocar informações entre si e/ou compartilhar recursos de hardware. A interligação poderá ser realizada por cabos, fibras ópticas, linha telefônica, ondas de rádio, sinais de satélite, sinalização infravermelha etc. Abaixo será explicado como se dá à abrangência dessas redes. (MOTA FILHO, 2013:38)

3.1. Abrangência Geográfica

As redes de computadores são classificadas através de sua escalabilidade, a distância é um critério importante como métrica de classificação, determinadas tecnologias são usadas em diferentes escalas, a seguir teremos uma breve introdução ao hardware de rede por escala.

3.2. PAN

Para Tanenbaum e Wetherall esse é o conceito de PAN:

"As redes pessoais**,** ou PANs (Personal Area Networks), permitem que dispositivos se comuniquem pelo alcance de uma pessoa. Um exemplo comum é uma rede sem fio que conecta um computador com seus periféricos". (TANENBAUM, WETHERALL, 2011:11)

3.3. LAN

Tanenbaum e Wetheral explicam também o conceito de LAN:

> Uma LAN (Local Area Network) é uma rede particular que opera dentro e próximo de um único prédio, como uma residência, um escritório ou uma fábrica. As LANs são muito usadas para conectar computadores pessoais e aparelhos eletrônicos, para permitir que compartilhem recursos (como impressoras) e troquem informações. Quando LANs são usadas pelas empresas, elas são chamadas de redes empresariais. (TANENBAUM, WETHERALL, 2011:12)

Para (MOTA FILHO, 2013:45) LAN (Local Area Network), ou rede local, é uma rede de curta abrangência geográfica, geralmente limitada a uma organização, não ultrapassando 5 ou 10 quilômetros.

3.4. MAN

Tanenbaum e Wetherall explicam o conceito de MAN:

> Uma rede metropolitana, ou MAN (Metropolian Area Network), abrange uma cidade. O exemplo mais conhecido de MANs é a rede de televisão a cabo disponível em muitas cidades. Esses sistemas cresceram a partir de antigos sistemas de antenas comunitárias usadas em áreas com fraca recepção de sinal de televisão pelo ar. Nesses primeiros sistemas, uma grande antena era colocada no alto de colina próxima e o sinal era, então, conduzido até as casas dos assinantes. (TANENBAUM, WETHERALL, 2011:15)

Segundo (MOTA FILHO, 2013:38) MAN, ou rede metropolitana, é uma rede de abrangência média, chegando a 50 ou 100 quilômetros. Podemos citar como exemplo a Rede Rio que interliga estabelecimentos de ensino superior na cidade do Rio de Janeiro.

3.5. WAN

Tanenbaum e Wetherall também o conceito de WAN:

> Uma rede a longa distância, ou WAN (Wide Area Network), abrange uma grande área geográfica, com frequência um país ou continente. Vamos começar nossa discussão com as WANs conectadas por fios, usando o exemplo de uma empresa com filiais em diferentes cidades. Na maioria das WANs, a sub-rede consiste em dois componentes distintos: linhas de transmissão e elementos de comutação. As linhas de transmissão transportam bits entre máquinas. Elas podem ser formadas por fios de cobre, fibra ótica, ou mesmo enlaces de radiodifusão. Os elementos de comutação, ou apenas comutadores, são computadores especializados que conectam três ou mais linhas de transmissão. Quando os dados chegam a uma interface de entrada, o elemento de comutação deve escolher uma interface de saída para encaminhá-los. Esses computadores de comutação receberam diversos nomes no passado; o nome roteador é, agora, o mais comumente utilizado. (TANENBAUM, WETHERALL, 2011:15)

Ainda (MOTA FILHO, 2013:45) diz que WAN, ou rede global, é uma rede de grande abrangência, sem limitações máximas de distância, podendo abranger todo o planeta e, até mesmo, o espaço sideral (pense em satélites). É uma rede de baixa velocidade. A Internet é uma rede WAN.

4. IANA

“A Internet Assigned Numbers Authority (IANA) é uma organização, criada na década de 1970, responsável por importantíssimas atividades de controle da internet, a saber: " (MOTA FILHO, 2013:48)

- Coordenar os DNS raízes mundiais (que são os servidores DNS principais da internet);
- Coordenar a distribuição mundial de endereços IP (IPv4 e IPv6) para uso na internet;
- Determinar as faixas de endereços IP para usos especiais;
- Coordenar a associação de números de portas a serviços de rede;
- Manter uma base de dados de fusos horários mundiais, para que computadores possam consultar e sincronizar seus relógios;

5. IEEE

O Institute of Electrial and Eletronics Engineers (IEEE) é uma organização, criada na década de 1960, que reúne engenheiros, cientistas e especialistas nas áreas aeroespacial, de computação e de telecomunicações. Nessas duas últimas áreas, há também envolvimentos relativos à engenharia biomédica, estudos da energia elétrica e produtos eletrônicos diversos.

6. IETF

O Internet Engineering Task Force (IETF), criado em 1986, é uma grande comunidade internacional, composta de arquitetos de rede, operadores, comerciantes e pesquisadores, todos voltados a assuntos relativos à evolução da arquitetura da Internet e também ao seu bom funcionamento.

O IETF é tão importante que possui até mesmo uma RFC para documentar sua missão. Trata-se da RFC 3935.

Em resumo, a sua missão principal é produzir documentos técnicos de alta qualidade, que criem caminhos para que as pessoas planejem, gerenciem e usem a Internet de uma forma melhor.

7. Protocolo IP (Internet Protocol)

O Internet Protocol (IP) é o protocolo mais importante da família TCP/IP, sendo responsável pelo sucesso no tráfego de dados nas redes.

O a versão mais utilizada hoje ainda é a versão 4 do protocolo IP, comumente conhecido pela sigla IPv4. No entanto, existe a versão 6 (IPv6) que está sendo aderida em todo o mundo, substituindo o IPv4. A versão 6 do protocolo traz inúmeras modificações e melhorias ao protocolo IP. A seguir uma breve descrição dessas duas versões do protocolo.

7.1. IPv4

O IPv4 foi lançado em 1979 e trabalha com endereços de 4 bytes (32bits), como 10.0.0.1, por exemplo, temos a possibilidade de 2^32 endereços IP, o que equivale a 4.294.967.296 IPs (4 bilhões de endereços).

Em 2011 a população mundial alcançou a marca de 7 bilhões de pessoas, o que equivale a um endereço IP para cada duas pessoas no mundo. Hoje esse número se torna muito pequeno considerando que as pessoas não vivem mais sem estar conectadas a Internet. A quantidade de novos dispositivos conectados como geladeiras, fornos, câmeras residências, iluminação de ambientes deixa ainda pior essa estatística.

7.2. IPv6

Para solucionar a previsão esgotamento dos endereços IPv4, em 1994 foi iniciado o desenvolvimento da versão 6 do protocolo IP, já em 1995 surgiram as primeiras RFCs 1752 e 1883 trazendo regulamentação para essa versão do protocolo.

Atualmente existe um grande esforço mundial na adoção do novo protocolo em substituição a versão 4.

O IPv6 trabalha com endereços de 16 bytes o equivalente a 128bits, temos a possibilidade de 2^128 endereços IP, ou seja, 340.282.366.920.938.463.463.374.607.431.768.211.456 IPs (340

undecilhões de endereços). Com a estatística de crescimento da população de 2011, 7 bilhões de pessoas, temos cerca de 48,5 octilhões de endereços por pessoa, hoje esse número parece grande, e no futuro próximo?

8. Protocolo TCP

O TCP (Transmission Control Protocol), foi definido na RFC 793 em setembro de 1981. Ele foi projetado especificamente para oferecer um fluxo de bytes fim a fim confiável através de uma rede não confiável. Redes interligadas são diferentes de uma única rede porque suas diversas partes podem ter topologias, larguras de banda, atrasos, tamanhos de pacote e outros parâmetros completamente diferentes.

O seu projeto foi para que se adaptasse dinamicamente às propriedades da rede interligada e ser robusto diante dos muitos tipos de falhas que podem ocorrer.

9. Protocolo UDP

O UDP (User Datagram Protocol) está definido na RFC 768 de agosto de 1980, é um protocolo extremamente simples e rápido.

Os protocolos da Internet admitem o transporte não orientado a conexões como o protocolo de datagrama de usuário. Oferece um meio para as aplicações enviarem datagramas IP encapsulados sem que seja necessário estabelecer uma conexão.

10. Protocolo ICMP

ICMP, referenciado pela RFC 792 de setembro de 1981, é a sigla de Internet Control Message Protocol, ou em português, Protocolo de Mensagens de Controle do IP. Esse é um dos mais importantes protocolos IP, pois emite avisos, em forma de mensagens, sobre a situação da rede. Com exceção do TCP, que tem seus próprios métodos de controle, quase todos os outros protocolos IP, se não todos, dependem do ICMP. (MOTA FILHO, 2013:48)

11. Protocolos Ethernet

11.1. ARP

Segundo (Reis, 2015), O protocolo ARP fornece resolução dinâmica de endereços, que é um mapeamento entre as duas firmas de endereçamento distintas: endereços IP, e qualquer outro tipo de endereço usado na camada de enlace. No caso dos quadros Ethernet, a camada de enlace usa o MAC Address (Media Access Control), endereço físico da interface.

11.2. NDP (Neighbor Discovery Protocol)

O protocolo de descoberta de vizinhança foi desenvolvido sob a finalidade de resolver os problemas de interação entre nós vizinhos em uma rede. Para isso ele atua sobre dois aspectos primordiais na comunicação IPv6, a autoconfiguração de nós e a transmissão de pacotes. No caso da autoconfiguração de nós, o protocolo fornece suporte para a realização de três funcionalidades:

- Parameter Discovery: atua na descoberta por um nó de informações sobre o enlace (como MTU) e sobre a Internet (como hop limit).
- Address Autoconfiguration: trabalha com a autoconfiguração stateless de endereços nas interfaces de um nó.
- Duplicate Address Detection: utilizado para descobrir se o endereço que se deseja atribuir a uma interface já está sendo utilizado por um outro nó na rede.

Já no caso da transmissão de pacotes entre nós, o suporte é dado para a realização de seis funcionalidades:

- Router Discovery: trabalha com a descoberta de roteadores pertencentes ao enlace.
- Prefix Discovery: implementa a descoberta de prefixos de redes do enlace, cuja a finalidade é decidir para onde os pacotes serão direcionados numa comunicação (se é para um roteador especifico ou direto para um nó do enlace).
- Address Resolution: descobre o endereço fisico através de um endereço lógico IPv6.
- Neighbor Unreachability Detection: permite que os nós descubram se um vizinho é ou se continua alcançavel, uma vez que problemas podem acontecer tanto nos nós como na rede.
- Redirect: permite ao roteador informar ao nó uma rota melhor ao ser utilizada para enviar pacotes a determinado destino.
- Next-Hop Determination: algoritmo para mapear um endereço IP de destino em um endereço IP de um vizinho para onde o trafego deve ser enviado.

12. Protocolos de Aplicação

12.1. HTTP

Hypertext Transfer Protocol (HTTP) é definido na RFC 1945 para a sua versão HTTP/1.0 e na RFC 2616 para sua versão HTTP/1.1. Por padrão os serviços que implementam esse protocolo utilizam por padrão a porta de comunicação 80/TCP e tem como principal cliente o navegador (browser). A troca de conteúdo cliente/servidor, além de mensagens de controle do protocolo através de requisições do cliente (navegador) e respostas do servidor, geralmente trafega informações e arquivos importantes como imagens, documentos, nome de usuários, senhas e também informações pessoais.

12.2. FTP

O File Transfer Protocol é definido pela RFC 959 e foi concebido com o objetivo de proporcionar a transferência rápida de arquivos entre sistemas interligados em uma rede. Tem por padrão do lado do servidor, a porta 21/TCP, para estabelecimento e controle de conexão, e a porta 20/TCP, para a transferência de arquivos.

FTP (File Transfer Protocol) é um serviço confiável orientado a conexão que usa o TCP para transferir arquivos entre sistemas que suportam o FTP. Ele suporta arquivo binário bidirecional e transferências de arquivo ASCII. (RCFIB, 2017)

12.3. DNS

O DNS (Domain Name Server), é um dos protocolos mais importantes que temos hoje em dia, ele nos proporciona transcrever endereços IP em nomes (domínios) amigável de fácil entendimento, deixando simples a busca por uma página hospeda em um servidor web ou um serviço ou um aplicativo online.

A essência do DNS é a criação de um esquema hierárquico de atribuição de nomes baseado no domínio e de um sistema de banco de dados distribuído para implementar esse esquema de nomenclatura. Ele é mais usado para mapear nomes de hosts em endereços IP, mas também pode servir para outros objetivos. (TANENBAUM, WETHERALL, 2011:384)

12.4. SMTP

O protocolo de transferência de mensagem simples do inglês *Simple Mail Transfer Protocol* (SMTP) tem como objetivo entregar e receber mensagens de e-mail (correio eletrônico) entre seu destinatário e remente sendo bem simples a sua utilização, durante a conexão ele também pode enviar vários status de entrega e também de erro.

> O protocolo SMTP (Simple Mail Transfer Protocol) é definido pela RFC 821, tendo recebido, posteriormente, funcionalidades complementares na forma de extensões MIME – Multipurpose Internet Mail Extensions (suporte a anexos e possibilidade de formatação da exibição de suas mensagens, como o uso de tags HTML). Seu funcionamento básico prevê um cabeçalho com a indicação do remetente e do destinatário (s) da mensagem, assunto da mensagem e a mensagem propriamente dita em texto ASCII. (M. GALVÃO, 2013:48)

12.5. POP3/IMAP

POP (Post Office Protocol) e o IMAP (Internet Message Access Protocol) são protocolos que permitem o usuário acessar o servidor de correio e manipular suas mensagens, O Protocolo POP possibilita que as mensagens sejam baixadas para o cliente de e-mail enquanto o protocolo IMAP manipula as mensagens no próprio servidor.

12.6. P2P (Peer-to-Peer)

Uma rede P2P (Peer-to-Peer) consiste em muitos computadores interconectados compartilhando arquivos e recursos assim formando uma rede de distribuição de conteúdo.

> A ideia básica de uma rede de compartilhamento de arquivos P2P (Peer-to-Peer) é muitos computadores se juntam e compartilham seus recursos para formar um sistema de distribuição de conteúdo. Os computadores normalmente são apenas computadores domésticos. Eles não precisam ser máquinas nos centros de dados da internet. Os computadores são chamados de peers (Pares) porque cada um pode alternadamente atuar como um cliente para outro peer, buscando conteúdo, e como servidor, fornecendo conteúdo para outros peers. O que torna o sistema peer-to-peer interessante é que não existe uma infraestrutura dedicada, diferente de uma CDN. (TANENBAUM, WETHERALL, 2011:470)

13. Análise em Redes de Computadores

Em uma análise de redes seja em tempo de execução capturando e analisando o tráfego em tempo real ou em um arquivo pcap, os elementos mais importantes são as informações que

identificam o tráfego de origem e destino sendo IP de origem, IP de destino, porta de origem, porta de destino e protocolo de transporte.

Esses elementos possuem informações sobre os hosts envolvidos na comunicação entre cliente e servidor, e também qual serviço está sendo explorado. Com essas informações podemos definir qual melhor técnica será utilizada e quais ferramentas são necessárias para realizar a análise.

Existem três tipos de análise consideradas como indispensáveis na análise de pacotes de redes, a seguir será explicado um pouco delas.

13.1. Parttern Matching (Casamento de padrões)

Parttern Matching consiste na busca por padrões combinados por filtros usando um valor em específico durante ou em um arquivo de captura tendo uma análise mais detalhada.

Com essa técnica de análise definimos o escopo da investigação antes que a captura e/ou filtragem ocorra, esse escopo é definido de acordo com o que se está procurando.

Na análise baseada em uma suspeita de atividade maliciosa a partir de um determinado host, o escopo inicial é o tráfego de origem e destino para este host. Assim devemos excluir pacotes que não sejam originários ou designados àquele host em específico.

Quando a suspeita inicial não possui um alvo em específico, é necessário fazer uso de ferramentas para adquirir informações relevantes ao tráfego no corpo (payload) dos protocolos de aplicação de um ou mais hosts não identificados.

Se a rede que está sendo analisada possui um proxy (web proxy), os logs e caches podem auxiliar consideravelmente na identificação de origem do host alvo sem a necessidade de busca por padrões no tráfego analisado. Caso a rede não possua um proxy ou algum serviço/protocolo não faz uso do mesmo, será necessário o auxílio de ferramentas para buscar padrões como strings (linhas) específicas de acordo com a investigação corrente.

Existem muitas ferramentas que podem auxiliar nessa busca, como por exemplo o ngrep, se utilizado por exemplo o ngrep combinado da seguinte maneira “ngrep -I analise_forense.pcap ‘cracker|trojam|worn’ “ , será buscado no arquivo analise_forense.pcap por palavras (padrões) com os dizeres “cracker”, “trojam” e “worn” resultando em uma filtragem que trará as strings (linhas) contendo essas palavras (padrões).

13.2. Parsing Protocol Fields (Análise dos Campos dos Protocolos)

O Parsing Protocol Fields (Análise dos Campos dos Protocolos) consiste em buscar de forma detalhada nos pacotes de dados as informações dos campos dos cabeçalhos e payloads dos protocolos envolvidos, a extração pode ser feita pela ferramenta Tshark, nela é informado os hosts os, protocolos e os campos significativos para uma extração completa.

Na análise de um host que está fazendo uso do protocolo SMTP o Tshark é capaz de extrair dados como o nome, e-mails e palavras relacionadas ao assunto do host investigado. No payload do pacote é possível identificar os endereços de origem e destino, os servidores de e-mails, anexos e o corpo da mensagem.

13.3. Packet Filtering (Filtragem de Pacotes)

A filtragem de pacotes, consiste na separação dos pacotes por meio de filtros baseados em seus metadados dos protocolos no payload, esse filtro pode ser feito utilizando BPFs.

Uma ferramenta que pode ser utilizada para realizar essa filtragem é o tcpdump, no host investigado que por exemplo tem a interface eth0 como principal meio de comunicação o grampo pode ser aplicado com o seguinte filtro.

~]# tcpdump -X -vvv -n -i eth0 -s0 host 192.168.94.2 and host 200.123.214.111 and port 25 \ -w captura.pcap

14. Análise de Protocolos de Alto Nível

Nesse tipo de análise são utilizadas 2 abordagens para à análise automatizada dos protocolos das camadas de alto nível.

- O uso de ferramentas simples, especializadas que são projetadas especificamente para realizar a análise de um determinado protocolo/serviço na camada de aplicação.
- Utilização de ferramentas multiuso buscando varrer rapidamente um amplo número informações sobre o tráfego a ser analisado.

14.1 Ferramentas Especializadas

As ferramentas especificas para a análise de um determinado protocolo/serviço, são pequenas com recursos específicos para o protocolo/serviço analisado tornando preciso a verificação das informações capturadas. Essas ferramentas geralmente são utilizadas para complementar a análise de uma ferramenta multiuso tornando mais preciso a captura.

14.2 Ferramentas Multiuso

Existem várias ferramentas que propõem analisar uma grande variedade de protocolos/serviços de rede. O uso desses frameworks tem aumentado em função da quantidade de protocolos que existem, realizando o cruzamento das informações capturadas para análise. Se utilizado de forma exclusiva esse tipo de ferramenta, existe a possibilidade de se obter resultados não esperados como o uso de ofuscação na transmissão dos dados como o uso de compactação, codificação e ou tunelamento, comprometendo toda a captura e análise.

14. Ferramentas de Apoio para Análise

Existem inúmeras ferramentas para apoio e analise de rede de computadores na grande maioria essas ferramentas utilizam a biblioteca chamada libpcap. A libcap foi desenvolvida em linguagem C de código-fonte aperto (open source) que consegue monitorar o tráfego de rede em baixo nível ou seja na camada de enlace, capturando os pacotes com base na interface de rede.

> A libpcap é uma biblioteca escrita na linguagem C, com código-fonte aberto e sem restrições de cópias ou modificações (open source), que oferece uma infraestrutura flexível para monitoramento, em baixo nível, de redes de computadores a partir da captura de pacotes e da recuperação dos frames com base nas interfaces de rede. O projeto dessa biblioteca foi concebido em 1987

> pelo grupo de pesquisa NRG (Network Research Group), formado pelos pesquisadores Van Jacbson, Grig Leres e Steven MacCanne, todos do laboratório Lawrence Berkeley. (M. GALVÃO, 2013:48)

14.1. TCPDUMP

O tcpdump é o melhor analisador de tráfego em mode texto que existe. Ele é baseado na libpcap, uma poderosa API para a captura de pacotes de rede durante seu tráfego. Assim, o tcpdump mostra as conexões estabelecidas e o tráfego correspondente. (MOTA FILHO, 2013:96)

Para (M. GALVÃO, 2013:70) o tcpdump é o sniffer open source mais conhecido e utilizado na atualidade. Esta ferramenta foi desenvolvida pelo mesmo grupo que criou a biblioteca libpcap, também em 1987.

14.2. NMAP

Para um melhor entendimento da ferramenta as informações a seguir foram retiradas do próprio manual, que explica da seguinte maneira:

> O Nmap ("Network Mapper") é uma ferramenta de código aberto para exploração de rede e auditoria de segurança. Ela foi desenhada para escanear rapidamente redes amplas, embora também funcione muito bem contra hosts individuais. O Nmap utiliza pacotes IP em estado bruto (raw) de maneira inovadora para determinar quais hosts estão disponíveis na rede, quais serviços (nome da aplicação e versão) os hosts oferecem, quais sistemas operacionais (e versões de SO) eles estão executando, que tipos de filtro de pacotes/firewalls estão em uso, e dezenas de outras características. Embora o Nmap seja normalmente utilizado para auditorias de segurança, muitos administradores de sistemas e rede consideram-no útil para tarefas rotineiras tais como inventário de rede, gerenciamento de serviços de atualização agendados, e monitoramento de host ou disponibilidade de serviço. (NMAP MANUAL, 2017)

14.3. Wireshark

Para um melhor entendimento da ferramenta as informações a seguir foram retiradas do próprio manual que explica da seguinte maneira:

> O Wireshark é o analisador de protocolo de rede mais utilizado em todo o mundo. Ele permite que você analise o que está acontecendo em sua rede em um nível muito baixo, utilizado como ferramenta padrão em muitas empresas comerciais e sem fins lucrativos, agências governamentais e instituições de ensino. O desenvolvimento do Wireshark é cada vez melhor graças as contribuições de voluntários especialistas em rede de todo o mundo e é a continuação de um projeto iniciado por Gerald Combs em 1998. (WIRESHARK ABOUT, 2017)

14.4. Network Miner

Para um melhor entendimento da ferramenta as informações a seguir foram retiradas do próprio manual que explica da seguinte maneira:

> NetworkMiner é uma Ferramenta de Análise Forense de Rede (NFAT) para Windows. O NetworkMiner pode ser usado como um sniffer de rede passivo / ferramenta de captura de pacotes para detectar sistemas operacionais, sessões, nomes de host, portas abertas etc. sem colocar nenhum tráfego na rede. O NetworkMiner também pode analisar arquivos PCAP para análise off-line e para regenerar / reassemblar arquivos e certificados transmitidos de arquivos PCAP. (NETRESEC AB, 2017)

14.5. Xplico

Para um melhor entendimento da ferramenta as informações a seguir foram retiradas do próprio manual, que explica da seguinte maneira:

> O Xplico tem como objetivo extrair de um tráfego de internet a captura dos dados contidos nas aplicações monitoradas. Por exemplo, a partir de um arquivo pcap, o Xplico extrai cada email (protocolos POP, IMAP e SMTP), todo o conteúdo HTTP, cada chamada VoIP (SIP), FTP, TFTP e assim por diante. Xplico não é um analisador de protocolo de rede. O Xplico é uma Ferramenta de Análise Forense de Rede de Código Aberto (NFAT). (XPLICO, 2017).

17. Validando o Tráfego como Prova em Perícias

O uso da computação forense como parte do processo de perícia ajuda a determinar, em tese, qual é o suspeito e a vítima buscando nas evidências comprovar a materialidade de delito "virtual", demonstrando se de fato existiu uma conduta ilícita. É essencial provar a materialidade quanto demonstrar a autoria, uma vez que se faz necessário para que seja determinada uma sentença.

Nas leis preexistentes foram incorporados/alterados parágrafos no código de processo civil brasileiro sendo fundamental para a jurisprudência que servem como base na avaliação das evidências digitais, visto que técnicas cientificamente comprovadas para a coleta e preservação dos dados e posteriormente análise e apresentação de resultados à prova de contestações.

> O suporte legal às perícias em tráfego de rede, por meio de "grampos digitais" e da análise dos dados capturados, veio com as alterações na Lei de Interceptações de Comunicações Telefônicas, que estendeu a norma aplicada aos "grampos digitais" telefônicos aos meios de comunicação telemáticos e de informática. (M. GALVÃO, 2013:142)

18. Questionamentos para um Caso

Para todo caso analisado existem algumas perguntas a serem feitas buscando sempre reunir o máximo de informações oferecendo evidencias suficientes para que o juiz possa julgar da maneira mais assertiva.

Em um caso hipotético de acesso indevido a conteúdo web proibido, é feito a solicitação ao juiz para realizar o grampo, a autorização do responsável pelo ambiente onde será instalado as ferramentas de sniffer e acesso aos equipamentos onde passa o tráfego suspeito para ser capturado e analisado.

a) **Qual o site acessado pelo suspeito?**

b) Qual o endereço IP do site acessado pelo suspeito?

c) Quais os tipos e nomes dos arquivos acessados pelo suspeito?

d) Qual a data/hora do início (primeiro acesso) e do final (último acesso) da conexão?

18.1 Captura do tráfego

Com as devidas autorizações em mãos se instala o grampo no local designado, para que a captura do tráfego seja restrita ao escopo do tráfego a ser capturado, se utiliza uma ferramenta de captura com a opção de se criar um filtro especifico para não capturar informações que não sejam do alvo, a ferramenta TCPDump tem uma gama muito ampla de filtros para restringir bem a captura do tráfego suspeito.

Durante o período determinado previamente aplica-se um filtro conforme demonstrado abaixo:

~]# tcpdump -X -vvv -n -i eth0 -s0 host <IP ALVO> and port 80 -w caso1.pcap

Com isso é gerado o arquivo “caso1.pacp” para ser analisado posteriormente.

18.2. Analisando o tráfego

Desde a captura do tráfego juntamente com a análise sempre será utilizado mais de uma ferramenta para responder de forma assertiva os questionamentos do judiciário. Para realizar a análise do tráfego capturado e registrado no arquivo “caso1.pcap” será utilizado as ferramentas Wireshark e Chaosreader.

Com base na análise feita com as ferramentas citadas, foi possível identificar a troca de informação entre o alvo e os sites acessados pelo mesmo comprovando o acesso indevido a conteúdo ilícito. Ainda com o a ferramenta Wireshark utilizando sua função “Follow TCP Stream” é possível ver com detalhes o tráfego HTTP entre o cliente e o servidor web.

Com a ferramenta Chaosreader é possível gerar um relatório no formato HTML para melhor ilustrar todas as informações trocadas entre o suspeito e o servidor web.

18.3. Respostas ao questionamento judiciário

a). Qual o site acessado pelo suspeito?

Resposta: www.alvo.rk

b). Qual o endereço IP do site acessado pelo suspeito?

Resposta: 8.7.6.5

c). Quais os tipos e nomes dos arquivos acessados pelo suspeito?

Resposta: image/jpeg -> **foto.jpg** e também pdf -> **rede.pdf**

d). Qual data/hora do ínicio (primeiro acesso) e do final (último acesso) da conexão?

Resposta: Inicio: 01/07/2013 – 21h54min41s / **Final:** 01/07/2013 – 22h00min15s

Conclusão:

Hoje não se pode mais utilizar a internet de forma indevida e ficar impune, com a constante evolução da tecnologia as legislações de todo o mundo estão buscando fechar as brechas que se encontra para tentar se fazer o ilícito através de um computador. Em direção a essas adequações existe um campo ainda pouco explorado pelos especialistas em tecnologia e segurança da informação para auxiliar o judiciário a julgar da maneira mais assertiva casos onde o suspeito praticou ou pratica crimes através de um computador, tornando a internet e todo o mundo virtual que existe um lugar seguro também onde pessoas de bem possam usufruir de toda a tecnologia oferecida hoje em dia.

Referências

TANENBAUM, Andrew S., WETHERALL, David. **Rede de Computadores**. São Paulo: Pearson, 2011.

MOTA FILHO, João Eriberto. **Análise de Tráfego em Redes TCP/IP**. São Paulo: Novatec, 2013.

M. GALVÃO, Ricardo Kléber. **Introdução à Análise Forense em Rede de Computadores**. São Paulo: Novatec, 2013.

Bóson Treinamentos. Disponível em: http://www.bosontreinamentos.com.br/redes-computadores/curso-de-redes-protocolo-arp-address-resolution-protocol/ Acesso em: 17/01/2017.

IPv6.br. Disponível em: http://ipv6.br/post/funcionalidades-basicas/ Acesso em: 17/01/2017.

RCFIB. Disponível em: http://rcfib.xpg.uol.com.br/segunda-parte-redes-de-computadores.pdf Acessado em: 24/01/2017.

NMAP. Disponível em: https://nmap.org/man/pt_BR/index.html Acesso em: 29/01/2017.

WIRESHARK. Disponível em: https://www.wireshark.org/#learnWS Acesso em: 29/01/2017.

XPLICO. Disponível em: http://www.xplico.org/about Acesso em: 29/01/2017.