V. 10, n. 2 p. 46-58, 2019
http://www.unibalsas.edu.br/revista

UNIBALSAS
Faculdade de Balsas

ANÁLISE FORENSE: TÉCNICAS E FERRAMENTAS APLICADAS EM RECONSTITUIÇÕES DE ATAQUES CIBERNÉTICOS EM AMBIENTES CORPORATIVOS.

RODRIGUES, Ana Paula Silva.[1]
COSTA, Edilmárcio Reis.[2]
Sousa, Jakson Ferreira de.[3]
Turibus, Sérgio Noleto.[4]

Resumo: A Análise Forense tem obtido cada vez mais notoriedade no atual cenário mundial devido aos altos índices de crescimento do cibercrime nas últimas décadas. O objetivo deste trabalho é identificar e expor as principais técnicas e ferramentas forenses que podem ser utilizadas na reconstrução de cenários comprometidos por crimes digitais. Para o cumprimento deste objetivo foi idealizado um cenário simulado e controlado, comprometido por um crime cibernético. Com base nesse cenário foram executadas todas as etapas da investigação forense, desde a fase de coleta das mídias até os resultados obtidos com a análise dos dados. Ao final foi identificado que o melhor contexto para prevenção do cenário apresentado foi à adoção de uma política de segurança juntamente com análises forenses proativas ao invés de reativas.

Palavras-chave: Análise Forense. Cibercrimes. Ferramentas forenses.

Abstract: Forensic analysis has gained increasing notoriety in the current world scenario due to the high growth rates of cybercrime in recent decades. The objective of this paper is to identify and expose the main forensic techniques and tools that can be used in the reconstruction of scenarios committed by digital crimes. To achieve this goal a simulated and controlled scenario was conceived, compromised by a cyber crime. Based on this scenario, all stages of forensic investigation were performed, from the media collection phase to the results obtained with the data analysis. In the end it was identified that the best context to prevent the scenario presented was the adoption of a security policy along with proactive rather than reactive forensic analysis.

Keywords: Forensic analysis. Cybercrime. Forensic tools.

1. INTRODUÇÃO

A migração para a era tecnológica revolucionou muitos aspectos da sociedade, principalmente a forma como as empresas gerenciam seus negócios. Sendo beneficiada pela facilidade de comunicação, integração e disponibilidade de seus dados e informações, a maioria das corporações hoje tem a informação que está armazenada em sistemas e trafegando por redes como um de seus ativos mais valiosos.

[1]Acadêmica do Curso de Sistemas da Informação na Faculdade de Balsas – Unibalsas. E-mail: anapaulasr963@gmail.com
[2]Professor na Faculdade Balsas – Unibalsas. E-mail: edilmarcio@newagroma.com.br
[3]Mestre em Ensino pela UNIVATES/RS, Coordenador do Núcleo de Educação a Distância na Faculdade de Balsas, Gestor do Núcleo de Tecnologia da Informação na Universidade Estadual do Marenhão / UEMA--CESBA, Professor na Faculdade de Balsas – Unibalsas. E-mail: jaksontecmicro@gmail.com
[4]Doutor em Engenharia Nuclear na Área de Física Nuclear Aplicada pela COPPE/UFRJ, Mestre em Ciências e Tecnologia de Materiais pela UERJ. Professor efetivo na Universidade Estadual do Maranhão – UEMA/ Campus Balsas. E-mail: s.turibus@gmail.com.

Com isso, o cibercrime voltado para o roubo dessas informações cresceu em escala exponencial nas últimas décadas e a ocorrência destes crimes acaba então por trazer enormes prejuízos, principalmente para as corporações, uma vez que, a informação é a base dos negócios de qualquer empresa na atualidade e que sua perda ou indisponibilidade, pode gerar uma perda de capital significativa.

Segundo McAfee (2018), o Brasil é a segunda maior fonte de ataques cibernéticos e o terceiro país que mais é afetado com a incidência desses crimes digitais atualmente e a ascensão dessa nova modalidade criminosa custa ao mundo todo um prejuízo de quase 600 bilhões de dólares por ano, o que resulta em 0.8% do Produto Interno Bruto (PIB) global.

Diante desse cenário a Análise Forense se torna cada vez mais necessária no processo de reconstrução dos ambientes comprometidos, por permitir a identificação dos atacantes, a extensão dos danos causados pelos mesmos, a reconstrução dos eventos que sucederam ao ataque e ainda a delimitação de possíveis soluções para os cenários que são analisados.

O objetivo central desta pesquisa foi evidenciar as principais técnicas e ferramentas da análise forense que podem ser comumente utilizadas durante todo o processo de investigação forense de forma a facilitar o processo de reconstrução de cenários comprometidos. Para isso, a metodologia utilizada foi de caráter bibliográfica que teve como base a busca por embasamento através de documentos expostos por autores de obras da área da Computação Forense, de sites, artigos e afins com conteúdos relacionados a área analisada.

A execução da pesquisa foi dividida nas seguintes etapas: formação do embasamento através das bibliografias da área, criação de um cenário controlado para fins de testes com as ferramentas e práticas forense, análise interpretativa em cima dos dados obtidos no período de testes e análise descritiva dos resultados alcançados.

2. FUNDAMENTAÇÃO TEÓRICA

A seguir serão apresentados os principais tópicos relacionados à Análise Forense, onde foi exposto o conceito de segurança da informação, os principais crimes digitais que ocorrem em ambientes corporativos, o conceito de computação Forense e as técnicas e principais ferramentas da Análise Forense.

2.1 SEGURANÇA DA INFORMAÇÃO

Com o avanço das tecnologias da informação e o advento da *internet* as corporações passaram por um processo de reestruturação de seus negócios de forma a garantir sua melhoria. Com isso, acabaram por migrar boa parte de seus serviços para a *internet*, necessitando da sua utilização para disponibilidade de serviços. Com informações de grande valor comercial trafegando por essa gigantesca rede e com o crescimento exponencial de ataques cibernéticos, o investimento em segurança da informação se tornou primordial para garantir a disponibilidade, integridade e confidencialidade dessas informações.

Segundo Galvão (2015, p. 12) “a segurança da informação tem como meta a proteção de sistemas de informação contra a invasão e modificação dos dados por pessoas não autorizadas”, logo, é possível definir a partir desse pressuposto que a segurança da informação é aplicada como uma política de controle que visa implementar medidas que diminuam os níveis de ataques a que uma rede está exposta.

Porém, mesmo com boas políticas de segurança ainda vão existir vulnerabilidades presentes em uma infraestrutura, uma vez que o conceito de ambiente totalmente seguro é apenas idealizado, mas não é viável em prática, pois deve ser levado em consi-

V. 10, n. 2 p. 46-58, 2019
http://www.unibalsas.edu.br/revista

deração que todos os dias surgem novas formas de prevenção contra ameaças conhecidas, mas também surgem novas ameaças que nunca foram estudadas. Dessa forma, empresas ficam suscetíveis a invasões que podem afetar os pilares da segurança, podendo deixar as informações inacessíveis, por exemplo, e consequentemente gerando perda de capital.

Ransomware, Phishing, Denial of Service (DDoS), *Botnets, backdoors,* são só alguns dos exemplos de tipos de *malwares* que atacam ambientes corporativos. No tópico a seguir serão apresentados alguns desses *malwares* que mais vem gerando prejuízos para as empresas nas últimas décadas.

2.2 CRIMES DIGITAIS EM AMBIENTES CORPORATIVOS

A criminalidade sempre esteve presente em diversos aspectos da sociedade e com o passar dos anos o conceito de crime foi originando novas ramificações, uma vez que novos tipos foram surgindo no meio social em que as pessoas habitam, indicando assim que a criminalidade evoluiu ao mesmo passo em que a humanidade.

Segundo Kil *apud* Capez (2007, p. 16) um crime é "qualquer ato do ser humano lesivo a outrem e a um bem jurídico tutelado, afetando, assim, a normalidade da conservação e desenvolvimento da sociedade".

Com base nesse conceito convencional de crime têm-se a origem de variações nos tipos de criminalidade como é o caso dos tipos de crimes: organizados, militares, políticos, comuns, complexos, de mão própria e crimes digitais também conhecidos como cibercrimes ou crimes cibernéticos.

Para Maras (2015) o cibercrime difere dos crimes tradicionais principalmente pelo fato de que o mesmo não tem uma barreira física como limitação de atuação uma vez que a *internet* permite que um crime digital seja direcionado a qualquer alvo independente de sua localização.

Esse é um dos principais motivos para que essa prática tenha crescido tanto na atualidade, além é claro da evolução das técnicas de invasões e dos novos tipos de *malwares* que os criminosos estão utilizando em seus ataques.

Segundo a Kaspersky (2018) em uma pesquisa realizada pela empresa a respeito dos ataques cibernéticos que mais geraram prejuízos e repercussão nas últimas décadas, têm-se o *Ransomware*, um *malware* que deixa inacessível informações presentes em computadores para depois pedir um pagamento em troca, como um dos líderes do ranking, principalmente depois da visibilidade que esse *malware* gerou por meio de uma de suas versões *crypto* conhecida como *WannaCry*, que infectou mais de 200 mil computadores gerando um prejuízo na faixa de 4 a 8 bilhões de dólares para as vítimas que foram infectadas em 2017.

A pesquisa também incorporou o *DDoS*, um ataque que visa tornar serviços indisponíveis, como um dos que geraram repercussão ao relatar o caso do *Mirai*, um *malware* que criava "máquinas zumbis" para serem incorporados a uma *Botnet*, rede de computadores "zumbis" controladas por um atacante, que mais tarde veio causar a desestabilização da *internet* ao realizar um ataque de *DDoS* à Dyn, uma empresa provedora de serviços de *DNS* (*Domain Name System*), que tinha como clientes Netflix, Spotify, Amazon, Twitter, Reddit, entre outros, e que acabou por deixar os usuários dessas aplicações sem acesso ao conteúdo por um período de tempo em 2016.

A PSafe (2018) disponibilizou ainda em seu relatório de segurança digital no Brasil referente ao segundo trimestre de 2018 que um dos ataques que mais geram problemas para os brasileiros foi o *Phishing*, uma técnica de invasão que através de e-mails, mensagens e sites fraudulentos, consegue roubar informações das vítimas, com 57,7% de incidência somente na cate-

goria de *Phishing* via *app* de mensagens.

Esses dados disponibilizados pela Kaspersky e PSafe demonstram que os crimes digitais, apesar de não gerarem danos físicos para as pessoas, acabam por ocasionar grandes prejuízos em termos materiais, prejudicando principalmente a disponibilidade dos serviços de muitas empresas, em alguns casos. A Computação Forense surge então como uma ciência que visa trabalhar especificamente com os crimes digitais que vem crescendo de forma significativa conforme apresentado no tópico a seguir.

2.3 COMPUTAÇÃO FORENSE

A constante evolução de tecnologias nos diversos setores de uma sociedade faz com que seja necessário passar por um processo constante de melhorias para se adaptar às novas tecnologias que o mercado disponibiliza. Um dos setores que se encontra em adaptação atualmente é o criminal, uma vez que os crimes digitais cresceram exponencialmente nas últimas décadas e para sua resolução se fez necessária a criação de uma nova ciência que trabalhasse especificamente com esse tipo de ocorrência. Essa ciência é conhecida atualmente como Computação Forense.

Maras (2015) define a computação forense como uma ciência que foca na resolução de crimes envolvendo dispositivos eletrônicos, visando coletar evidências que ajudem no processo de resolução de crimes digitais.

Isso significa dizer que as informações recolhidas pela computação forense não estão somente armazenadas em computadores *desktops*, mas sim em qualquer dispositivo eletrônico que possa armazenar informações, como é o caso de *tablets*, *smartphones* e *Personal Digital Assistant* (PDA), por exemplo.

Maras (2015, p. 62) define ainda que a computação forense "diz respeito ao processo de obtenção, processamento, análise e armazenamento de informações digitais para uso como evidência em casos civis e administrativos".

Desse modo, é possível definir que o principal objetivo da computação forense é realizar a análise de informações de forma a determinar que as mesmas sejam ou não usadas como evidências na resolução de cibercrimes. A Análise Forense é uma vertente da computação forense que trabalha essencialmente com a análise de informações.

2.4 ANÁLISE FORENSE

A Análise Forense opera atualmente como um mecanismo que promove etapas e ferramentas necessárias em um processo de reconstituição de crimes digitais.

Junior, Oliveira e Beskow (2013, s/n) definem a Análise Forense como o

> [...] uso de métodos cientificamente desenvolvidos e provados visando a preservação, coleta, validação, identificação, análise, interpretação, documentação e apresentação de evidência digital oriundas de fontes digitais com o propósito de facilitar ou expandir a reconstrução de eventos de origem criminosa, ou ajudar a antecipar ações não autorizadas que prejudiquem operações planejadas.

Dessa maneira, é possível compreender que a Análise Forense é muito utilizada atualmente como uma medida reativa principalmente. Ou seja, só é acionada após o acontecimento do crime, porém ela também pode ser utilizada como uma forma de antecipação de ações que ainda venham a acontecer e a gerar prejuízo.

Galvão (2013) afirma que a Análise Forense pode ser utilizada em dois tipos de investigações: investigações públicas que é quando o crime já está sendo avaliado pelo sistema judiciário e em investigações privadas ou corporativas que é executada por um interesse particular da empresa, não necessariamente envolvendo o judiciário, poden-

V. 10, n. 2 p. 46-58, 2019
http://www.unibalsas.edu.br/revista

do até mesmo ser realizada como uma forma de auditoria interna que busca identificar possíveis falhas que possam vir a acontecer, agindo assim de forma proativa ao invés de reativa.

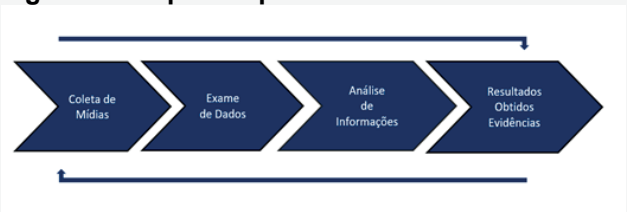
A seguir serão apresentadas as fases da Análise Forense que estão presentes em investigações de caráter público ou privado.

2.4.1 Técnicas da Análise Forense

Independentemente do tipo de investigação que vai ser aplicada, a Análise Forense possui um conjunto pré-definido de etapas que constituem as técnicas que são necessárias no processo de resolução de qualquer crime digital.

Segundo Sousa (2016, p. 100 *apud* Eleutério e Machado, 2011) essas etapas podem ser melhor delimitadas em quatro fases principais: Coleta, Exame, Análise e Resultados obtidos, conforme ilustra a figura 1.

Figura 1 - Etapas do processo da Análise Forense



Fonte: Adaptado de Sousa (2016).

De acordo com a figura 1, as etapas de coleta, exame, análise e resultados obtidos podem ser definidas como:

- **Coleta**: consiste no processo de isolamento da área que vai ser analisada posteriormente para que a mesma mantenha seu estado original sem interferências ou modificações depois que o processo de investigação iniciar. Quando a área tiver sido isolada, as evidências deverão ser coletadas nas mídias apontadas como parte do cenário, sempre visando garantir sua integridade;
- **Exame**: na etapa de exame serão identificados, extraídos, filtrados os dados que foram coletados na primeira etapa. Sendo extraídos e filtrados somente os dados que serão relevantes no processo de resolução do crime;
- **Análise**: no processo de análise em si, que é a mais primordial de todas as etapas, os dados examinados na fase anterior deverão formar informações que promovam a identificação dos possíveis envolvidos, permitindo que seja feita a reconstituição do cenário;
- **Análise dos Resultados Obtidos**: também conhecida como a etapa de relatório, essa é a última fase desse processo, e consiste na demonstração das evidências obtidas, através da redação de um laudo que deve ter como anexo todas as evidências encontradas nas mídias examinadas e os demais documentos que foram produzidos durante o processo de Análise Forense.

Existe atualmente um vasto conjunto de ferramentas forenses disponíveis para auxiliar no processo de reconstituição criminal. Algumas dessas ferramentas serão apresentadas no próximo tópico.

2.4.2 Ferramentas Forenses

Para cada etapa do processo de Análise Forense existem hoje diversas ferramentas para serem utilizadas como uma forma de facilitação no desenvolvimento de uma investigação forense, como é o caso das ferramentas FTK, Autopsy, IPED, EnCase e Celebrite, por exemplo.

Na etapa de coleta e aquisições das evidências, o FTK Imager é uma das ferramentas que podem ser utilizadas. Ela funciona como uma extensão da ferramenta FTK (Forensic ToolKit) que permite a criação de uma imagem forense de discos rígidos, *CDs*, *DVDs*, *pendrives*, pastas ou arquivos individuais para análise posterior. A ferramenta ainda permite a criação de um *dump* de memória com base nas imagens forenses adquiridas (ACCESSDATA, 2018).

O Autopsy Linux é uma ferramenta forense digital que permite a análise de um sistema de arquivo de uma determinada

imagem forense, podendo ser utilizado para fins militares e corporativos de forma a realizar a reconstrução dos eventos que aconteceram em determinado host e que geraram o comprometimento do mesmo. (AUTOPSY, 2003).

A ferramenta Autopsy é composta por diversos módulos, que possuem funcionalidades diversas, como identificado na Tabela 1.

Tabela 1 - Funcionalidades do Autopsy

Listagens de arquivos	Permite verificar e analisar arquivos e diretórios, inclusive os que foram apagados.
Visualização do Conteúdo do arquivo	Permite a visualização do conteúdo do arquivo que pode ser visto em hexadecimal, raw, ou em strings ASCII.
Hash Databases	Mantêm um banco de dado de hash de todos os arquivos e sistemas de arquivos.
Organização por tipo de arquivo	Permite organizar os arquivos conforme as assinaturas de tipos de arquivos.
Timeline das ações	Permite criar uma linha de tempo, das ações ocorridas no sistema.
Procura por palavra	Permite procurar uma String específica dentro do sistema de arquivo.

Fonte: Adaptado de Silva (2018).

Porém, além de ferramentas que executam cada fase do processo de Análise Forense separadamente, existem atualmente sistemas operacionais voltados especificamente para esse tipo de investigação, como é o caso de sistemas como o DEFT, CAINE, Paladin, SANS Sift, ADIA e KALI, por exemplo.

CAINE (Computer Aided INvestigative Environment) é uma distribuição *GNU/Linux live* que tem como principal objetivo integrar um conjunto de ferramentas forenses de forma a facilitar e dar suporte ao analista forense durante o processo de reconstituição de um crime (CAINE, 2018).

Esses sistemas operacionais têm como principal vantagem a integração de ferramentas forenses em um único ambiente de forma que os profissionais da área evitem trabalhar com diversos mecanismos separadamente.

Com isso, é possível compreender que, apesar dos números significativos de ataques cibernéticos que acontecem no Brasil e em outros países do mundo, existe hoje uma ciência que trabalha especificamente com técnicas e ferramentas eficazes para a solução dos prejuízos causados por esses ataques. É uma área que vem ganhando notoriedade recentemente, mas que ainda tem muito a evoluir e por isso estudos e pesquisas a respeito da Análise Forense e da Computação Forense em si se tornam cada vez mais essenciais.

3. CENÁRIO DE APLICAÇÃO

Durante os processos de coleta de mídias, exames de dados, análise de informações e apresentação dos resultados obtidos, existem técnicas e ferramentas dedicadas para cada uma destas etapas. A apresentação do cenário que levou ao resultado desta pesquisa busca deixar isso de forma evidente.

Em muitos casos de ataques em ambientes corporativos o acesso direto ao servidor que executa as aplicações pode ser quase inacessível diante das medidas de segurança que são adotadas para a proteção do mesmo, e por este motivo alguns ataques visam conseguir acesso de uma outra máquina da rede para depois utilizar da escalação de privilégio para chegar até o alvo original.

Partindo deste ponto de vista, o cenário que foi utilizado nesta pesquisa foi composto por um terminal Ubuntu 18.04.01, *Desktop* virtualizado pela ferramenta VirtualBox no qual foi infectado com um *rootkit*, que segundo Rosanes (2011, p. 3) é “um conjunto de programas utilizados para impedir a detecção de atividades maliciosas no sistema, como a presença de usuários não autorizados”. O *rootkit* utilizado é popularmente conhecido como Diamorphine e foi desenvolvido por Victor Ramos Mello e está disponível no repositório do Github. O Diamorphine funciona em versões 2.6.x/3.x/4.x

V. 10, n. 2 p. 46-58, 2019
http://www.unibalsas.edu.br/revista

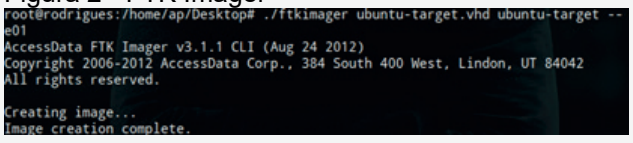
específicas de *Kernels*, sendo usado na máquina alvo a versão 4.15.0.29-generic. A seguir serão então apresentadas as técnicas e ferramentas utilizadas no processo de investigação para a reconstrução dos eventos do cenário descrito anteriormente.

3.1 COLETA DE MÍDIAS

A primeira etapa do processo de investigação forense consiste em coletar as mídias que possam conter possíveis informações que ajudarão no processo de reconstrução dos eventos. Nessa fase deve ser realizado primeiramente o isolamento da área para que as informações não sofram mais nenhum tipo de alteração a partir do momento em que a investigação começa. Após esse processo devem ser coletadas as mídias físicas ou imagens, para a sequência do processo forense. Um dos pontos primordiais deste estágio é garantir a integridade dos dados que estão sendo coletados de forma que sejam os mesmos que os originais, logo, o ideal é gerar um *hash*, um resumo de dados que muitas vezes é utilizado para a verificação de integridade de arquivos, do registro original e comparar com o hash do arquivo que vai ser utilizado no processo de análise.

Neste primeiro passo foi utilizada a ferramenta FTK Imager para a criação de uma imagem forense a partir do disco virtual da máquina alvo conforme ilustrado na figura 2.

Figura 2 - FTK Imager



Fonte: Próprio autor (2019)

A figura 2 demonstra o processo de criação de uma imagem forense para a utilização posterior na ferramenta de análise Autopsy. O FTK Imager permite que sejam criadas imagens forenses a partir do próprio disco local do sistema, ou de arquivos virtuais de máquinas virtualizadas, conforme demonstrado na figura 2. Com a finalização da coleta de mídias a investigação avança para a segunda fase: o exame de evidências.

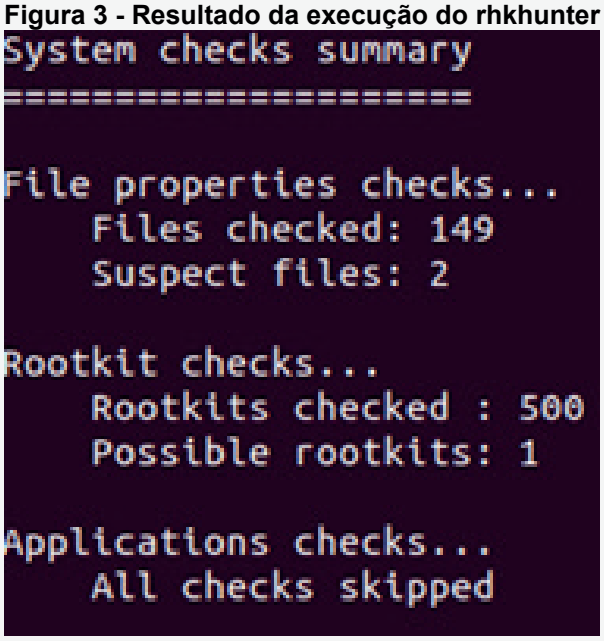
3.2 EXAME DE EVIDÊNCIAS

Depois que as mídias foram coletadas o processo de investigação avançou então para a etapa de exame de dados, onde deveriam ser identificados e filtrados os dados de maior relevância para a fase de análise de informações que foi executada posteriormente.

Nesta fase foram utilizadas duas ferramentas que funcionam especificamente para a identificação de *rootkits*: o chkrootkit e o rkhunter.

O chkrootkit e o rkhunter nada mais são que mecanismos que realizam uma verificação local por sinais de *rootkit* em um determinado sistema. Porém, ao executar o chkrootkit não foram obtidos os mesmos resultados do que quando foi utilizado o rkhunter, pois enquanto o chkrootkit foi menos preciso e não identificou nenhum arquivo suspeito no sistema, a outra ferramenta identificou dois possíveis arquivos duvidosos e ainda a possibilidade de ter um *rootkit* instalado na máquina alvo, conforme demonstrado na figura 3.

Figura 3 - Resultado da execução do rhkhunter



Fonte: Próprio Autor (2019)

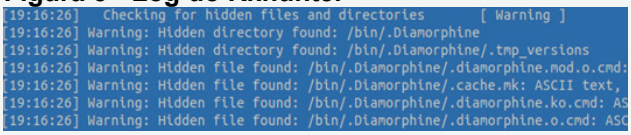
A figura 3 consolida o fato de que apesar de terem a mesma finalidade a ferramenta rkhunter acaba sendo mais precisa no processo de identificação desse *malware*, considerando o caso em estudo, pois um dos passos de sua inspeção é a busca em um banco de dados de *rootkits* pré-determinado para verificar se estão instalados na máquina. O Diamorphine é um dos 500 *rootkits* deste banco citado e que são checados no teste da ferramenta, porém não foi a partir dessa informação que se chegou à conclusão de que tinha um *rootkit* instalado, conforme demonstrado na figura 4.

Figura 4 - Resultados obtidos com rkhunter

Fonte: Próprio Autor (2019)

De acordo a figura 4, a ferramenta durante a checagem no banco de dados de *rootkits* não conseguiu identificar que havia algum instalado na máquina. Porém, ao final do processo de escaneamento durante a verificação do arquivo de *log* que fica no diretório /var/log/rkhunter foi exposto a existência de uma pasta oculta que contém os arquivos de instalação do Diamorphine. Essa informação foi obtida durante a checagem de arquivos e diretórios ocultos realizadas pela ferramenta.

Figura 5 - Log do Rkhunter



Fonte: Próprio Autor (2019)

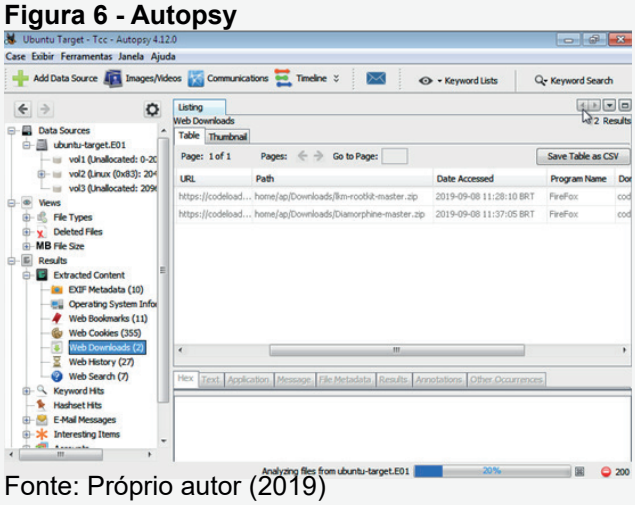
Com base nos dados da figura 5 ficou evidente que a máquina está infectada por um *rootkit*, porém para a finalização do processo de investigação forense ainda faltam questões a serem respondidas como: de onde o ataque foi originado e quem foi o invasor. Diante deste princípio, a investigação evoluiu para uma das etapas mais importantes de todo esse processo: a análise de informações.

3.3 ANÁLISE DE INFORMAÇÕES

Na etapa de análise de informações foi utilizada a ferramenta Autopsy que tem funcionalidades essenciais para esta parte do processo de investigação. Depois do processo de importação da imagem forense, gerada na primeira etapa do processo, a ferramenta disponibiliza uma série de informações para serem analisadas de forma que seja possível finalizar o caso em questão. Na figura 6 é demonstrado o painel principal do Autopsy.

V. 10, n. 2 p. 46-58, 2019
http://www.unibalsas.edu.br/revista

Figura 6 - Autopsy



Fonte: Próprio autor (2019)

Na figura 6 item 1 é possível identificar o sistema operacional da qual a imagem é composta, no caso um sistema Linux. Essa informação pode ser valiosa quando o perito em questão não participa da etapa de coleta e desse modo, é possível identificar com qual sistema se está trabalhando. Seguindo para a seção *view* da árvore de evidências é possível identificar outra funcionalidade que a ferramenta disponibiliza e que pode ser muito útil: visualização de arquivos deletados, uma funcionalidade de data *carving* e que permite explorar os arquivos que foram recentemente apagados do disco. E no item 3, é possível identificar uma informação essencial para o processo de reconstrução dos eventos: o arquivo para a instalação do *rootkit* foi adquirido através de um *download* no dia 08/09/2019 às 11:37:05 do navegador Firefox.

Prosseguindo com o processo de análise, um dos artefatos que também são bem empregados como evidências e que são passíveis de análise são os arquivos de log de um sistema operacional, uma vez que esses arquivos gravam todas as execuções que foram executadas ou que falharam em um sistema. Sistemas Linux contam com uma gama destes arquivos de *Logs*, sendo os que foram utilizados nesta pesquisa listados na tabela 2.

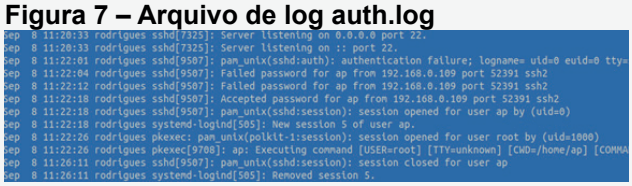
Tabela 2 - Arquivos de logs no Linux

history	Comando que é utilizado para buscar comandos armazenados que foram digitados em um terminal.
.bash_history	arquivo de log que armazena os comandos digitados pelo usuário *root* ou padrão.
auth.log	arquivo de log que armazena os registros de conexões, autenticações que foram bem-sucedidas ou que falharam.

Fonte: Próprio autor (2019)

A partir do arquivo de log de autenticação localizado no diretório **/var/log/auth.log** foi possível identificar que houve tentativas de conexões remotas no dia 8 de setembro a partir das 11:22:04, conforme a figura 7.

Figura 7 – Arquivo de log auth.log



Fonte: Próprio autor (2019)

A figura 7 demonstra que duas dessas tentativas foram falhas, supostamente por que o invasor tinha algumas possibilidades de senha a sua disposição e somente na terceira tentativa ele conseguiu efetivar o processo de *login*, ou a outra possibilidade é que o mesmo tenha digitado a senha incorreta por descuido no processo de digitação. Porém essas duas tentativas falhas já levantam suspeitas, uma vez que o administrador de um sistema não costuma errar sua senha mais de uma vez de propósito.

Ainda na figura 7 é possível identificar que o invasor teve uma escalação de privilégio ao logar com o usuário padrão **ap** e depois logar como *root*, pressupondo que essa escalação de privilégio foi possível por que a mesma senha de *root* era a senha de usuário padrão, sendo esse um erro que os administradores e analistas de sistemas cometem em determinados cenários.

Verificando então o arquivo de log **.bash_history** do usuário *root* foi possível identificar que foi realizado o *download* de um arquivo malicioso via linha de comando, como é demonstrado na figura 8.

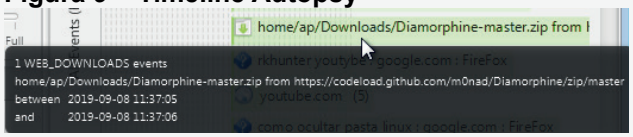
Figura 8 – Arquivo .bash_history

Fonte: Próprio Autor (2019)

A partir da figura 8 é possível visualizar que via terminal o atacante baixou de um repositório do Github uma pasta chamada de **Reptile**, sendo essa uma variação de um *rootkit LKM*, que atua em nível de *Kernel*. Nas linhas 10, 11 e 12 fica então comprovado que o invasor tentou fazer o processo instalação desse *rootkit*, mas esse processo não foi bem-sucedido uma vez que na execução dos dois scanners de *rootkits* não foi encontrado nenhum vestígio de execução do mesmo.

Através da imagem forense criada com a ferramenta FTK Imager e que foi gerada a partir da imagem do sistema corrompido foi feita uma análise de informações com a ferramenta Autopsy que permitiu chegar a uma nova conclusão a respeito desse cenário, conforme é possível analisar a partir da figura 9.

Figura 9 – Timeline Autopsy

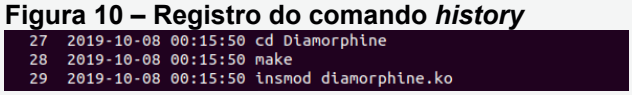


Fonte: Próprio Autor (2019)

A figura 9 demonstra o resultado da utilização de uma funcionalidade da ferramenta Autopsy conhecida como linha do tempo (*Timeline*), onde de forma automática a ferramenta gera, a partir da imagem forense que está sendo analisada, uma linha do tempo de execuções que ocorreram no sistema da imagem em análise.

Está representado na figura 9 um trecho específico da *Timeline* de eventos que foi gerado a partir do histórico do navegador da máquina alvo, no qual é possível identificar que entre 11:37:05 e 11:37:06 do dia 08 de setembro de 2019 foi realizado o *download* do segundo *rootkit* que viria a ser instalado na máquina. O *rootkit* identificado como Diamorphine LKM teve sua instalação comprovada de acordo com a figura 5, que demonstrou a presença no sistema da pasta oculta desse *rootkit* que supostamente foi ocultada pelo invasor na intenção de camuflar seus atos. Além é claro da comprovação da instalação do mesmo via linha de comando conforme mostra a figura 10.

Figura 10 – Registro do comando *history*



Fonte: Próprio autor (2019)

A figura 10, obtida a partir do comando ***history***, listou dentre os comandos digitados pelo usuário *root* no terminal os três comandos representadas pelas linhas 27, 28, 29 que evidenciam a tentativa do invasor de instalar o *rootkit* Diamorphine.

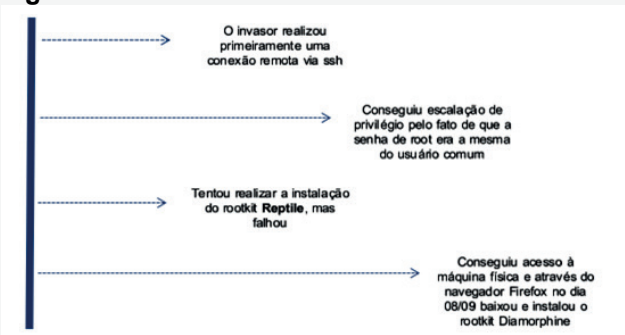
4. RESULTADOS OBTIDOS (EVIDÊNCIAS)

Durante as três etapas iniciais do processo de invasão foram coletadas evidências com base em técnicas e ferramentas que foram anteriormente apresentadas. A quarta e última etapa visa apresentar, de forma cronológica, todas as comprovações que foram obtidas para que por fim seja possível apresentar o autor da invasão e o que ocorreu de fato no cenário que foi investigado.

Diante das evidências coletadas nas etapas anteriores é possível ter a seguinte reconstrução do cenário analisado:

V. 10, n. 2 p. 46-58, 2019
http://www.unibalsas.edu.br/revista

Figura 11 – Timeline de eventos



Fonte: Próprio autor (2019)

De acordo com a figura 11 o processo de reconstrução do cenário contém os seguintes fatos:

- 1º Fato: o invasor teria realizado primeiramente uma conexão remota onde tinha posse da senha de usuário comum **ap** e a partir da escalação de privilégios conseguiu acesso ao controle de super usuário pelo fato de que a senha de *root* ser a mesma do usuário padrão.

- 2º Fato: após realizada a conexão com o usuário *root* o invasor teria baixado o arquivo malicioso do primeiro *rootkit* que o mesmo tentou instalar, o Reptile, mas de acordo com as evidências encontradas, essa instalação falhou.

- 3º Fato: Não houve uma nova tentativa de conexão remota para continuidade do processo de invasão, pois ficou comprovado que o *rootkit* que infectou a máquina alvo foi instalado na própria máquina física por alguém que tinha acesso à mesma, uma vez que as evidências que comprovam isso foram retiradas do histórico de navegação dessa máquina.

Dessa forma, o que se pode concluir é que o invasor conseguiu efetivar sua invasão por ter conseguido o acesso ao usuário *root* e por ter conseguido acesso à máquina física e que diante destes fatos é que foi possível que o mesmo infectasse a máquina com o *rootkit* Diamorphine.

Portanto, o invasor foi a pessoa que teve acesso a essa máquina no dia 08 de setembro por volta de 11:37. Os danos causados foram mínimos, pois o autor não chegou a realizar nenhuma ação que de fato impactasse nas informações contidas na infraestrutura na qual a máquina alvo fazia parte.

5. CONSIDERAÇÕES FINAIS

A Análise Forense vem ganhando, atualmente, espaço e repercussão no cenário de segurança da informação devido aos índices elevados de cibercrimes em diversas organizações. Diante deste cenário, a presente pesquisa evidenciou as principais técnicas e ferramentas da Análise Forense que podem ser comumente utilizadas durante todo o processo de investigação forense de forma a facilitar o processo de reconstrução de ambientes comprometidos.

A partir de um cenário controlado foi possível construir um ambiente comprometido e trabalhar com o mesmo aplicando as etapas que compõem um processo forense para identificar as principais técnicas e ferramentas que podem ser utilizadas nesses contextos.

De acordo com o estudo bibliográfico realizado, foi identificado que o processo de reconstrução forense é composto basicamente por quatro etapas: Coleta de evidências, exame de dados, análise de informações e apresentação dos resultados obtidos.

Ao seguir esse contexto foi detectado que na etapa de coleta de evidências o FTK Imager é uma das ferramentas que pode ser utilizada para criação de imagens forenses para análise posterior. Também foi detectado que, para garantir a exatidão desta etapa o ambiente comprometido não deve ser submetido a nenhuma alteração após o início do processo de investigação para garantir a fidelidade dos dados.

Na etapa de exame de dados foi observado que as ferramentas chkrootkit e rkhunter facilitam o processo de identifi-

cação de *rootkits* nos cenários analisados, enquanto que na fase de análise de informações o Autopsy é uma das possibilidades de ferramentas que pode ser útil no processo de análise de informações, mas que apesar de ter ferramentas para facilitarem esse ponto da investigação o que realmente conta é o *know-how* e a expertise do perito que está avaliando o caso, de forma que saiba ligar as informações de forma correta.

Por fim, a etapa de apresentação dos resultados obtidos consiste na apresentação das evidências em ordem cronológica, deixando claro quais eventos resultaram no comprometimento do ambiente.

Como solução para o cenário com características semelhantes ao que foi analisado seria necessário que políticas de segurança bem definidas fossem aplicadas na infraestrutura em questão. Pois, dessa forma uma política de senhas evitaria questões como a que foi apresentada, em que a senha de usuário comum não deve ser a mesma que a senha de um super usuário.

Porém, uma forma mais efetiva para evitar cenários como esses seria realizar um processo de análise forense proativa, para que fossem identificados possíveis problemas antes dos mesmos virem a se tornar problemas reais.

Estudos futuros podem ser voltados então para questões de análises proativas e sua aplicabilidade no cotidiano nas empresas como forma de prevenção contra crimes digitais.

6. REFERÊNCIAS

ACCESSDATA, **FTK Imager 4.2.0**. Disponível em: https://marketing.accessdata.com/ftkimager4.2.0 .Acesso em 20 de maio de 2019.

AUTOPSY - THE SLEUTH KIT, Autopsy. Disponível em: <https://www.sleuthkit.org/autopsy/ . Acesso em 08 de setembro de 2019.

BARRETO, A.; BRASIL, B. **Manual de Investigação Cibernética, à luz do Marco Civil da Internet**. 1º Edição. Rio de Janeiro: BRASPORT Livros e Multimídia Ltda., 2016.

CAINE, **Caine Computer Forenses Linux Live Distro**. Disponível em: https://www.caine-live.net/index.html . Acesso em 20 de maio de 2019.

GALVÃO, Michele da Costa. **Fundamentos em Segurança da Informação**. 1º Edição. São Paulo: Pearson Education Brasil, 2015.

GALVÃO, Ricardo Kléber M. **Introdução à Análise Forense em Redes de Computadores: conceitos, técnicas e ferramentas para "Grampos Digitais"**.1 Ed. São Paulo: Novatec Editora Ltda, 2013.

GITHUB, **Diamorphine**. Disponível em: https://github.com/m0nad/Diamorphine Acesso em 08 de setembro de 2019.

JUNIOR, M.; OLIVEIRA, F.; BESKOW, G. **Análise Forense Digital**: Conceitos e Modelos. Disponível em: https://www.gta.ufrj.br/grad/13_1/forense/sobre.html Acesso em: 06 de abril de 2019.

KASPERSKY, **Os Ciberataques Mais Famosos dos Últimos Tempos**. Disponível em:https://www.kaspersky.com.br/blog/five-most-notorious-cyberattacks/11042/ Acesso em 20 de maio de 2019.

KIL, Bertodo. **Princípio da Insignificância no Direito Penal**. Disponível em: http://www.ri.unir.br/jspui/bitstream/123456789/1250/1/PRINC%C3%8DPIO%20DA%20INSIGNIFIC%C3%82NCIA%20NO%20DIREITO%20PENAL.pdf Acesso em 20 de maio de 2019.

MARAS, Marie H. **Computer Forensics**:

V. 10, n. 2 p. 46-58, 2019
http://www.unibalsas.edu.br/revista

Cybercriminals, Laws and Evidence. 2º Edi. New York: Jones & Bartlett Learning, 2015.

McAfee, **The economic Impact of Cybercrime - No Slowing Down.** Disponível em: https://www.mcafee.com/enterprise/en-us/assets/executive-summaries/es-economic-impactcybercrime.pdf Acesso em: 31 de março 2019.

PSAFE. **Relatório da Segurança Digital no Brasil**. Disponível em: https://www.psafe.com/dfndr-lab/wp-content/uploads/2018/08/Relat%C3%B3rio-daSeguran%C3%A7a-Digital-no-Brasil-2-trimestre-2018.pdf Acesso em 20 de maio de 2019.

ROSANES, Pedro. **Rootkits**. Disponível em: http://jeiks.net/wpcontent/uploads/2013/10/rootkits.pdf Acesso em 08 de setembro de 2019.

SILVA, Tiago Gonçalves. **Análise Forense**: Técnicas e Reconstituição de Ataques. Revista Especialize On-Line IPOG. Goiânia, v. 16, 2018.

SOUSA, Adriano Gomes. **Etapas do Processo de Computação Forense**: Uma Revisão. Revista Acta de Ciência e Saúde. Distrito Federal, v. 02, n. 05, 2016.