SEPINF:LED CAINE

De wiki

Índice

Descrição

O DVD bootável KALI-LED-IPED-NUDETECTIVE (era LED-CAINE) é uma customização da distribuição forense Linux Kali (https://www.kali.org/) para conter os aplicativos LED (https://wiki.ditec.pf.gov.br/SEPINF:LED), IPED (https://wiki.ditec.pf.gov.br/SEPINF:IPED) e NuDetective (https://wiki.ditec.pf.gov.br/SEPINF:NuDetective), a fim de executá-los em locais de buscas.

A vantagem desta abordagem é a praticidade, onde no local de buscas o perito pode simplesmente configurar a máquina a ser examinada para ser inicializada pelo DVD ou pendrive, inicializando o sistema operacional Linux. Na inicialização deve ser selecionada a opção de boot no modo forense, para evitar a montagem do swap e partições automaticamente.

Na área de trabalho há links para a execução automática do LED, IPED e NuDetective, nos sistemas de arquivos ou dispositivos de bloco (discos rígidos - IPED) detectados.

Observação: Na última versão a distribuição Linux foi alterada para o KALI (https://www.kali.org/).

Forma de Uso

O principal cuidado ao utilizar esta ferramenta é ao configurar a máquina a ser examinada para inicializar pela unidade de DVD, ou então pela USB, se for utilizado o LED_CAINE desta forma. Cada fabricante costuma utilizar uma tecla diferente para habilitar a seleção da unidade de inicialização. Algumas teclas comuns são ESC, F1, F2, F10, F12, DEL. As imagens a seguir apresentam as teclas mais frequentemente usadas pelos principais fabricantes.

Computer Model	BIOS Key/s	Boot menu (UEFI)
Acer	F1, F2, Ctrl+Alt+Esc	Esc F2,F9 ,F12
Asus	-	Esc, or F8
AST	Ctrl+Alt+Del, Ctrl+Alt+Esc	-
Dell (All models)	-	F12
HP	-	ESC or F9
Lenovo (all models)	-	F12
Panasonic CF-25	F1	-
Samsung (all models)	-	F12
Sony Vaio (All Models)	-	F11
Toshiba (All Models)	-	F12

Computer Model	BIOS Keys
Acer®	F1, F2, CTRL+ALT+ESC
AST®	CTRL+ALT+ESC, CTRL+ALT+DEL
Compaq® 8700	F10
CompUSA®	DEL
Cybermax®	ESC
Dell® 400	F3, F1
Dell Dimension®	F2 or DEL
Dell Inspiron®	F2
Dell Latitude	Fn+F1 (while booted)
Dell Latitude	F2 (on boot)
Dell Optiplex	DEL
Dell Optiplex	F2
Dell Precision™	F2
eMachine™	DEL
Gateway® 2000 1440	F1
Gateway 2000 Solo™	F2
HP®(Hewlett-Packard)	F1, F2
IBM®	F1
IBM E-pro Laptop	F2
IBM PS/2®	CTRL+ALT+INS after CTRL+ALT+DEL
IBM Thinkpad® (newer)	Start | Programs | Thinkpad CFG
Intel® Tangent	DEL
Micron™	F1, F2, or DEL
Packard Bell®	F1, F2, DEL
Sony® VIAO	F2, F2
Tiger	DEL
Toshiba® 335 CDS	ESC
Toshiba Protege	ESC
Toshiba Satellite 205 CDS	F1
Toshiba Tecra	F1 or ESC

Nas máquinas mais novas, com Windows 10 e UEFI, deve-se desabilitar a opção de Inicialização Segura (SecureBoot). Para tanto, em alguns casos é necessário inicializar o Windows, e selecionar reiniciar com o botão Shift selecionado. Ao reiniciar desta forma, será aberta uma interface de recuperação, onde deve-se ir para "Solução de Problemas"->"Opções Avançadas"->"Configurações de Firmware UEFI". O computador será reiniciado na interface de configuração UEFI, onde será possível desabilitar a Inicialização Segura (SecureBoot). Essa opção pode ser reativada depois da análise.

Recomenda-se sempre selecionar a opção "Forensic" na inicialização, para evitar a montagem automática dos discos e também a montagem de partições swap.

Em alguns computadores o disco interno pode não estar visível no Linux, neste caso deve-se certificar que a opção SATA na BIOS esteja como AHCI, e não como RAID.

Funcionamento da Ferramenta

Na área de trabalho, há um ícone denominado **"LED - MONTAR E VASCULHAR"** que montará os sistemas de arquivos reconhecidos pelo Linux como somente leitura sob o diretório /media/ e executará automaticamente o LED neste diretório. Cada unidade encontrada será montada em um subdiretório deste diretório, como por exemplo /media/sda1, /media/sda2, /media/sdb1, utilizando a nomenclatura padrão do Linux. Este script também detecta automaticamente os RAID's em software do Windows (discos dinâmicos), montando-os sob o diretório /media/mapper/<nome_do_volume>.

ATENÇÃO: No Kali, caso se clique nos ícones dos discos reconhecidos pelo sistema na área de trabalho, estes serão montados com permissão de escrita. Para garantir que os discos a serem examinados sejam montados como somente leitura, deve-se executar o script "Monta Unidades", ou então os scripts dos aplicativos, que montarão estes discos como somente leitura.

Para executar o aplicativo IPED, pode ser utilizada a linha de comando de forma habitual conforme instruções da ferramenta ou então executando o script contido na área de trabalho denominado **"IPED - FASTMODE"**, que executará o IPED no modo "fastmode" nos discos rígidos detectados e salvará o caso num diretório

denominado "IPED-CASO" na área de trabalho, abrindo-o automaticamente ao término do processamento.

Para os casos em que o processamento do IPED ficar muito lento, a partir da versão 2017-08-18 criou-se um outro script, denominado "IPED - Somente Ativos", que processa os diretórios montados pelo Linux (como o LED), sendo normalmente mais rápido, pois não depende do Sleuthkit para decodificar os sistemas de arquivos, porém não recuperando arquivos apagados.

IPED Triage (Experimental)

O script IPED Triage realizará uma indexação básica do sistema, inclusive das caixas de e-mails suportadas, no modo triage.

Este script pode ser executado na memória, porém com a indexação isto tende a não ser efetivo, pois é necessária muita memória RAM para o armazenamento do caso, gerando erros. Como alternativa, após se gravar o ISO do Kali em um pendrive ou disco externo, pode-se criar uma partição no espaço livre, preferencialmente no formato NTFS. Para este procedimento pode ser usado o próprio gerenciador de discos do Windows. Esta partição deverá ter o nome "IPED-TRIAGE". Na raiz desta partição poderá ser salvo um arquivo denominado "palavras-chave.txt", que será utilizado no processamento como fonte de palavras-chave.

Resumindo:
Nome da partição extra: IPED-TRIAGE
Arquivo de palavras-chave: palavras-chave.txt

Para a execução deste modo, recomenda-se gravar o ISO em um disco SSD externo via um case USB 3.0, o que reduzirá de forma muito significativa o tempo de processamento.

Virtual Shadow Copies do Windows (VSS)

As unidades de Virtual Shadow Copies do Windows podem ser montadas utilizando o script "Monta VSS Windows", na área de trabalho.

O Windows gera automaticamente estas cópias de segurança em determinados momentos, como por exemplo ao instalar atualizações de segurança. O interessante é que são salvas cópias de todos os arquivos do volume, e não somente dos arquivos de sistema, o que pode ser útil na recuperação de arquivos que foram apagados do disco, mas continuam presentes nas cópias de segurança antigas.

Este script não é executado automaticamente, e seu uso é opcional. Devido à forma como o Windows utiliza o serviço de VSS, cada VSC (Virtual Shadow Copy) possui um snapshot completo do disco rígido na época em que foi realizado, contendo desta forma, além das diferenças daquele snapshot específico, todo o conteúdo do disco rígido. Desta forma, o tempo de processamento pelos aplicativos será multiplicado pelo número de VSC's que foram encontradas, devendo ser usado com cautela.

Para esta montagem é utilizada a biblioteca libvshadow.

Uso com BitLocker

O Kali já reconhece nativamente partições criptografadas com BitLocker, sendo que elas aparecerão na área de trabalho com um ícone contendo um círculo vermelho em sua parte inferior e na descrição do volume o texto "Encrypted".

Para que seja possível montar essa partição no Kali, a criptografia deve estar suspensa, ou então deve-se ter a chave de recuperação. Caso se tenha a senha de administrador do sistema operacional Windows, este sistema pode ser iniciado, e no Windows Explorer deve-se clicar com o botão direito no disco criptografado, selecionar "Gerenciar BitLocker", e em seguida suspender a proteção. Esta ação não descriptografa o volume, simplesmente deixa a chave em claro no próprio volume para que se possam realizar tarefas de manutenção. Na

tela "Gerenciar BitLocker" também é possível imprimir a chave de recuperação. Em seguida, o sistema deve ser reinicializado no Linux através do pendrive bootável. Cuidado: ao reinicializar o windows o modo de suspensão é automaticamente encerrado.

Caso a criptografia tenha sido suspensa executando o procedimento do parágrafo anterior, os scripts de execução do LED, IPED e Nudetective detectarão e montarão automaticamente a partição Bitlocker como somente leitura, e a processarão normalmente.

Caso a criptografia não esteja suspensa, será pedida a chave de recuperação de 48 dígitos do volume BitLocker no momento de execução dos aplicativos, tendo-se que digitar a chave, inclusive com os hifens.

Gravação em um Pendrive

O ISO com esta distribuição pode ser gravado em um DVD, porém o modo mais recomendado de uso é gravá-lo em um pendrive, de no mínimo 4GB, pois a velocidade de execução é muito maior. Para gravar o ISO em um pendrive, pode ser utilizada uma ferramenta específica, como por exemplo o Balena Etcher https://www.balena.io/etcher/.

Contato

Quaisquer dúvidas ou sugestões de melhorias podem ser comunicadas ao e-mail dalpian.gmd@pf.gov.br (mailto:dalpian.gmd@pf.gov.br).
