Instituto Federal de Educação, Ciência e Tecnologia do RN
Câmpus Currais Novos
Curso: Tecnologia em Sistemas para Internet
Disciplina: Segurança e Preservação de Dados

Atividade Prática em Laboratório (Roteiro) - Computação Forense em Redes

Esta é uma prática de fixação para exercitar um dos conteúdos apresentados no tópico 'Computação Forense'. A intenção da atividade é praticar a análise/extração/recuperação de evidências a partir de arquivos de captura de tráfego de redes usando ferramentas de **Análise Forense em Redes**.

01. Crie um arquivo (docker-compose.yml) para subir um docker simples usando uma imagem leve do Linux Debian:

```
services:
  analise_redes:
        image: debian:12-slim
        container_name: analise_redes
        hostname: analise_redes
        command: /bin/bash -c "tail -f /dev/null"
```

02. Execute/ative o contêiner:

```
$ docker compose up -d
```

03. Acesse o contêiner:

```
$ docker exec -it analise_redes bash
```

04. Atualize os pacotes:

```
# cd
# apt update
```

05. Instale os pacotes que precisaremos para a prática:

```
# apt install wget iproute2 chaosreader tcpxtract apache2
```

06. Inicialize o servidor web no docker (utilizaremos esse servidor web para visualizar os resultados a partir de um navegador em seu host físico):

```
# service apache2 start
```

07. Crie um diretório dentro da área visível a partir de um navegador externo (área de trabalho do servidor web instalado no docker):

```
# mkdir /var/www/html/resultados
```

08. Mude o diretório de trabalho para o diretório criado:

```
# cd /var/www/html/resultados
```

09. Baixe o arquivo de captura de tráfego de redes que será analisado nesta atividade:

```
# wget https://www.segurancaderedes.com.br/spd/pratica11/http01.pcap
```

10. Crie os diretórios que serão utilizados pelas ferramentas de análise de tráfego de redes para armazenar os arquivos extraídos da mídia de origem:

```
# mkdir tcpxtract
# mkdir chaosreader
```

11. Execute o '`tcpxtract`' informando como origem o arquivo que será analisado e como destino a pasta criada para os resultados:

```
# tcpxtract -f http01.pcap -o tcpxtract
```

12. Execute o '`chaosreader`' informando como origem o arquivo que será analisado e como destino a pasta criada para os resultados:

```
# chaosreader http01.pcap -D chaosreader
```

13. Mude a propriedade dos diretórios criados e utilizados para que o servidor web tenha permissão de exibi-los ao acessar via navegador:

```
# chown -R www-data:www-data /var/www/html/resultados/
```

14. Identifique o endereço ip atribuído pelo aplicativo docker de seu computador ao docker criado:

```
# ip a
```

O resultado será algo como indicado abaixo. O `endereço IP` estará indicado pelo parâmetro `inet` na interface virtual criada (no exemplo abaixo o IP é `172.18.0.2`)

```
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
       link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
       inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
       inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0@if572: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default
       link/ether aa:30:f9:f8:05:1f brd ff:ff:ff:ff:ff:ff link-netnsid 0
       inet 172.18.0.2/16 brd 172.18.255.255 scope global eth0
       valid_lft forever preferred_lft forever
```

15. Acesse a partir de seu host real, utilizando um navegador, o endereço IP indicado no docker e navegue pelos diretórios onde foram extraídos os arquivos (Atenção: use HTTP não HTTPS!!!). Exemplo: `http://172.18.0.2/resultados`