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) :: Sniffers (tráfego não encriptado)

A atividade consiste em proporcionar ao aluno o contato com a técnica de captura de pacotes (sniffing) com a ferramenta Tcpdump e análise de arquivos de captura com a ferramenta Wireshark e descoberta de informações "críticas" trafegando em redes sem criptografia.

1) Baixe o contêiner com ambiente gráfico que será usado como "cliente" para fazer o acesso a um servidor web via navegador e a servidor telnet e ftp em linha de comando (docker Linux com ambiente gráfico e ferramentas instaladas).

```
docker pull ricardokleber/rk_debian12_vnc:latest
```

2) Baixe o contêiner que será usado como servidor (docker Linux com serviços instalados)

```
docker pull ricardokleber/debian12:latest
```

3) Crie um diretório para utilizar nesta prática

```
$ mkdir pratica03
```

4) Entre no diretório onde colocará o arquivo de configurações dos contêineres

```
$ cd pratica03
```

5) Baixe o arquivo de configuração dos contêineres

```
$ wget https://www.segurancaderedes.com.br/spd/pratica03/docker-compose.yml
```

6) Execute o docker compose para iniciar os contêineres

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

7) Entre no contêiner host02 (servidor) e inicie os serviços web, ftp e telnet:

```
$ docker exec -it host02 bash
# service apache2 start
# service proftpd start
```

8) Entre no contêiner host01 via navegador (a partir de sua máquina real)

```
http://localhost:10001/acesso.html
```

Para se conectar via noVNC informe a senha: **password**

Captura HTTP: Instalando o Sniffer para capturar tráfego envolvendo o host servidor:

9) Nos host 01 execute o Tcpdump para capturar todo tráfego envolvendo o host servidor (172.31.0.3)

```
$ sudo -i (senha: password)
# tcpdump -i eth0 -X -vvv -n -s0 host 172.31.0.3 -w /home/user/trafego_web.pcap
```

Acessando o host servidor usando o navegador do host01:

10) Abra o navegador do contêiner host01 e informe o endereço do servidor (host02)

```
http://172.31.0.3
```

11) Clique e baixe (download) as 3 imagens de animais disponíveis

12) Feche o navegador !!!

13) No terminal do host01 pare o sniffer (Tcpdump)

```
CTRL+C
```

14) Inicie o servidor ssh no host01 para acesso remoto a partir de sua máquina real

```
# service ssh start
```

15) A partir de sua máquina real, abra um terminal e conecte em modo gráfico via SSH no host 01

```
$ ssh -X user@172.31.0.2 (senha: password)
```

16) Execute o Wireshark para analisar o arquivo capturado pelo sniffer

```
$ wireshark trafego_web.pcap
```

17) Use a funcionalidade do Wireshark (File ➡ Export Objects ➡ HTTP) para reconstruir as sessões e baixar as imagens capturadas no grampo.

18) Entre no host01 (via navegador + noVNC) e abra as imagens exportadas na pasta do usuário 'user'.

Captura FTP: Instalando o Sniffer para capturar tráfego envolvendo o host servidor:

19) Nos host 01 execute o Tcpdump para capturar todo tráfego envolvendo o host servidor (172.31.0.3)

```
$ sudo -i (senha: password)
# tcpdump -i eth0 -X -vvv -n -s0 host 172.31.0.3 -w /home/user/trafego_ftp.pcap
```

Acessando o host servidor usando o cliente ftp do host01:

20) Abra outro terminal no contêiner host01 e faça uma conexão ftp ao host02:

```
$ ftp 172.31.0.3
```

21) Informe propositalmente um login/senha inexistente (`login:teste | senha:qualquer`)

22) Informe agora um login/senha existente (`login:aluno | senha:aluno`)

23) Agora conectado via FTP no servidor execute um comando qualquer (ls por exemplo para listar os arquivos):

```
ftp> ls
```

24) Desconecte do servidor FTP:

```
ftp> quit
```

25) No outro terminal aberto do host01 pare o sniffer (Tcpdump)

```
CTRL+C
```

26) A partir de sua máquina real, abra um terminal e conecte em modo gráfico via SSH no host 01

```
$ ssh -X user@172.31.0.2 (senha: password)
```

27) Execute o Wireshark para analisar o arquivo capturado pelo sniffer

```
$ wireshark trafego_ftp.pcap
```

28) Use a funcionalidade de reconstrução de sessão do Wireshark (Clicando com o botão direito em uma das linhas relacionadas a seção FTP no Wireshark e Marcando 'Follow TCP Stream') e confira todos os dados capturados pelo grampo referente às conexões FTP.