Netkit e tcpdump

Roberto Sadao Yokoyama

UTFPR-CP

Agosto, 2016

Prática de hoje[1]:

[1] Material baseado em [1] e [2]

Netkit – Instalação

O Netkit é distribuído em 3 pacotes, o software base, o kernel e o sistema de arquivos. A página oficial é: http://wiki.netkit.org

Download

http://wiki.netkit.org/index.php/Download_Official

Coloque os arquivos que efetuou download em seu "home"e use os comandos a seguir:

- *[seu_nome@suamaquina]$ tar -xjSf netkit-2.7.tar.bz2*
- *[seu_nome@suamaquina]$ tar -xjSf netkit-filesystem-i386-F5.2.tar.bz2*
- *[seu_nome@suamaquina]$ tar -xjSf netkit-kernel-i386-K2.8.tar.bz2*

Após a execução dos comandos terá uma pasta netkit no seu home.

Netkit – Instalação

Execute os comandos:

- *[seu_nome@suamaquina]$ export NETKIT_HOME=/home/seu_nome/netkit*
- *[seu_nome@suamaquina]$ export MANPATH=:$NETKIT_HOME/man*
- *[seu_nome@suamaquina]$ export PATH=$NETKIT_HOME/bin:$PATH*

- Estes comandos poderão ser acrescidos ao seu arquivo *.bash_rc* para que sejam executados automaticamente quando você iniciar seu ambiente bash.
- Use o comando *cd netkit* para acessar a pasta do Netkit, e depois execute o script check_configuration.sh (comando: *./check_configuration.sh*)
- Se saída retornou uma falha nos pacotes. É necessário instalar este pacote. Numa distribuição baseada no Debian, use *apt-get install pacote*, onde "pacote" é o nome do pacote.

Netkit – Laboratório

Objetivos

- executar um laboratório no Netkit
- aprender como transportar arquivos da máq. virtual para a máq. real
- utilizar os comandos básicos para realizar as operações e configurações

Cenário reproduzido[2]

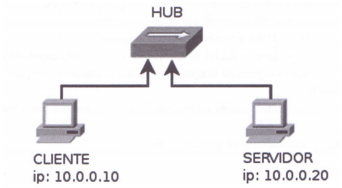

Figura: Duas máquinas ligadas em rede através de um simples hub

[2]Os laboratórios do Netkit são baseados em Gurgel [1]

Netkit – Laboratório

Execução laboratório

1. (real) Acesse a pasta *nklabs* a partir do terminal (console)
   [seu_nome@suamaquina]$ cd /home/utfpr/nklabs
2. (real) Use o comando:
   [seu_nome@suamaquina]$ tar -xf netkit_lab00.tar.gz
3. (real) Use o comando a seguir:
   [seu_nome@suamaquina]$ lstart -d /home/utfpr/nklabs/lab00
4. No computador virtual SERVIDOR ative o sniffer "tcpdump"com o comando:
   tcpdump -i eth0 -v -n -s 1600 -w /hosthome/lab00.pcap
5. No computador virtual CLIENTE, execute o comando:
   ping 10.0.0.20
6. Para interromper um comando no linux, use as teclas Ctrl+C

Netkit – Laboratório

A pasta /hosthome é uma pasta especial. O arquivo de saída lab00.pcap pode ser encontrada na pasta home do usuário logado na máquina real (/root) e seu conteúdo deverá ser estudado com o software wireshark

7. Vá ao computador SERVIDOR e interrompa o tcpdump com Ctrl+C
8. Utilize o wireshark para visualizar os pacotes. O arquivo está em sua pasta home com o nome lab00.pcap
   Pratique alguns comandos básicos de linux.
9. Use o comando *pwd* no SERVIDOR para verificar qual pasta você está. A saída deverá ser /root
10. Use o comando *cd /hosthome/* para ir para a pasta hosthome
11. Use o comando *ls* para listar o conteúdo de sua pasta de usuário
12. Use o comando *cd* ∼ para voltar para a pasta de usuário (/root)
13. Crie um diretório chamado teste com o comando *mkdir* teste.

Netkit – Laboratório

14. Use o comando *cp /root/contas.ods* ./teste para copiar o arquivo contas.ods para a pasta teste.
15. Use o comando *ps aux* para ver os processos em execução na máquina.
16. Use o comando *route* para consultar a tabela de roteamento.
17. Use o comando *arp* para ver a tabela arp.
18. (real) Use o comando a seguir para encerrar a execução do laboratório:
    [seu_nome@suamaquina]$ lhalt -d /home/utfpr/nklabs/lab00
19. (real) Use o comando a seguir para apagar os enormes arquivos.disk:
    [seu_nome@suamaquina]$ lclean -d /home/utfpr/nklabs/lab00
20. (real) Use o comando a seguir para apagar os enormes arquivos.disk que possam ter sobrado em sua máquina
    [seu_nome@suamaquina]$ rm /tmp/.disk*

tcpdump

Parâmetros importantes [2]:

-o Lista as interfaces de rede disponíveis.

-i iface Analisa somente os dados que passarem pela interface de rede especificada. A interface-padrão será a primeira listada pelo comando #,ifconfig ou pelo comando # tcpdump -n. O valor any poderá ser utilizado,para capturar dados em todas as interfaces ao mesmo tempo. É possível,usar tanto o nome da interface quanto seu número, de acordo com o que,for mostrado pela opção -o.

-n Não faz resolução de nomes de hosts nem de portas, acelerando a exibição dos resultados na tela (tempo real). É aconselhável sempre utilizar -n nas análises de tráfego.

-N Se fizer resolução de nomes, não mostrará o domínio do host.

tcpdump

-A Mostra também o conteúdo dos pacotes (payload), utilizando caracteres ASCII.

-x Mostra também o conteúdo dos pacotes (payload), usando sequências em hexadecimal e caracteres ASCII.

-x Mostra também o conteúdo dos pacotes (payload), utilizando apenas sequências em hexadecirnal.

-v Aumenta a quantidade de informações extraídas do cabeçalho do pacote.

-vv Idem ao anterior, com mais informações ainda.

-VVV Idem ao anterior, com mais informações.

-t Não mostra a data nem a hora na tela.

-tttt Mostra a data e a hora utilizando o padrão yyyy-mm-dd hh:mm:ss.ss

tcpdump

-w arq Grava o resultado da captura em um arquivo. É importante ressaltar que se nenhuma outra chave ou expressão de filtragem for utilizada, todo,o tráfego passante será gravado. É aconselhável usar as chaves -nv para,acelerar a gravação, por não resolver nomes, e para mostrar detalhes da,captura em andamento.

-r arq Lê um arquivo previamente gravado com -w. Diversas chaves e ex-pressões de filtragem poderão ser utilizadas para depurar o resultado.

-S Exibe os resultados TCP usando sua sequência absoluta, em vez da sua sequência relativa. Recomendado na análise de sequências TCP.

-e Mostra também os dados referentes à camada 2

tcpdump

Além das chaves, o tcpdump admite as expressões de filtragem fornecidas pela libcap. As expressões mais comuns são as seguintes:

host nome-ip	Especifica que somente o tráfego envolvendo a máquina em questão, referenciada por seu nome ou IP, será mostrado.
net rede/CIDR	Idem ao anterior. Contudo, a filtragem será em relação a uma faixa de rede, em vez de uma máquina única. A expressão de filtragem poderá ser com CIDR, como em 192.l68.1.0/24, ou com máscara de rede, como em 192.l68.0.16 mask 255.255.255.0.
port porta	Idem, referindo-se a uma porta.
ether host MAC	Idem, referindo-se a um endereço MAC

tcpdump

src	Delimita à origem. Pode ser associado a host, net, port e ether host. Exemplos: src host, src net, src port, ether src host.
dst	Delimita ao destino. Pode ser associado a host, net, port e ether host Exemplo: dst host.
not ou !	Operador lógico NOT. Utilizado para excluir algo do resultado da pesquisa. Exemplo: ! port 80
and ou &&	Operador lógico AND. Usado para associar duas ou mais expressões. tornando-as obrigatórias no resultado da pesquisa. Exemplo host 10.0.0.1 and port 80
or ou ||	Operador lógico OR. Utilizado para declarar duas ou mais expressões, fazendo com que pelo menos uma apareça no resultado da pesquisa. Exemplo: host 10.0.0.1 or net 192.168.0.0/24.

tcpdump

Exemplos

- *# tcpdump -nAi eth1 udp*
  Mostra todo o tráfego UDP no adaptador eth1, incluindo o payload (área de dados) em ASCII, sem resolver nomes.
- *# tcpdump -n host 10.1.1.25 and udp*
  Mostra o cabeçalho de todo o tráfego que envolva o host 10.1.1.25 e que seja UDP, sem resolver nomes.
- *# tcpdump -n host 10.1.1.25 and udp and port 53*
  Mostra o cabeçalho de todo o tráfego envolvendo o host 10.1.1.25, que seja UDP, e que tenha como origem ou destino a porta 53, sem resolver nomes.

Referências

[1] P. Gurgel, K. R. L. C. Branco, L. H. C. Branco, F. E. Barbosa, and M. M. Teixeira. *Redes de Computadores Da teoria à prática com Netkit*. Elsevier, 1ed, 2015.

[2] J. E. Mota Filho. *Análise de tráfego em redes TCP/IP*. Novatec, 2013.