Comandos Linux – Comando tcpdump, guia de referência e introdução

Sobre este documento

Introdução e instalação

Em muitas situações necessitamos de efetuar monitoramento em nossas redes e servidores por diversos motivos, seja um usuário que não consegue acessar determinado recurso, ou um software que não se tem documentação disponível disponível o suficiente para determinar que portas e endereços são utilizados. Estas e muitas outras situações podem causar transtornos e perda de tempo caso não seja efetuado um monitoramento rápido e preciso na rede. Neste artigo será apresentada uma das mais utilizadas ferramentas de monitoramento de redes, o **tcpdump**. Ao contrário do que mutios pensam, o tcpdump é uma ferramenta de simples utilização bastando apenas o entendimento do básico de redes locais e protocolos.

Neste tutorial explicaremos o funcionamento do tcpdump no sistema Debian Lenny, porém o mesmo pode ser seguido em outras distribuições modificando a forma de instalaçao, esta está disponível na documentação do tcpdump em http://www.tcpdump.org. Para instalar o tcpdump, basta que o sistema esteja com a ferramenta apt-get configurada corretamente, esta configuração encontra-se disponível em diversos tutoriais na internet e no site oficial da distribuição Debian http://www.debian.org. Com o apt-get configurado corretamente basta executar o a linha de comandos: **apt-get install tcpdump** estando logado com o usuário root que possui todos os direitos de alteração e administração no sistema operacional. Uma outra observação importante, é que por motivos de segurança somente o usuário root poderá executar o tcpdump devido ao acesso a bibliotecas restritas a usuários comuns. Se executado sem argumentos, o tcpdump mostrará o tráfego que estiver passando através da interface de rede primária, na figura temos um exemplo da execução da linhas de comandos onde utilizamos o comando |head, para que o comando tcpdump fosse interrompido após a apresentação de 10 linhas. Para interropmper o tcpdump, basta pressionar as teclas ctrl + c simultameamente.

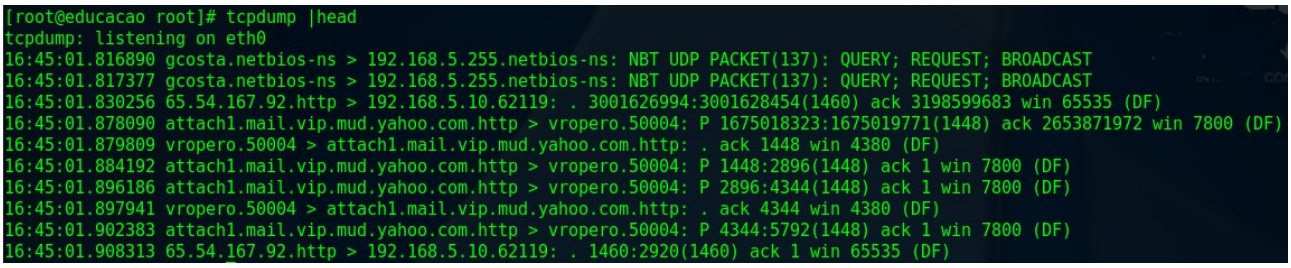

Figura 1: Executando o tcpdump sem argumentos

O tcpdump é muito flexível as necessidades do administrador, permitindo a especificação desde a interface desejada para a aexecução do monitoramento até a especificação de portas de origem ou destino que serão monitoradas. Na figura 2. é exibido um exemplo onde monitoramos todas as conexões de dentro da rede para a porta de destino 80, desta forma temos como saber quais hosts de nossa rede estão navegando na internet.

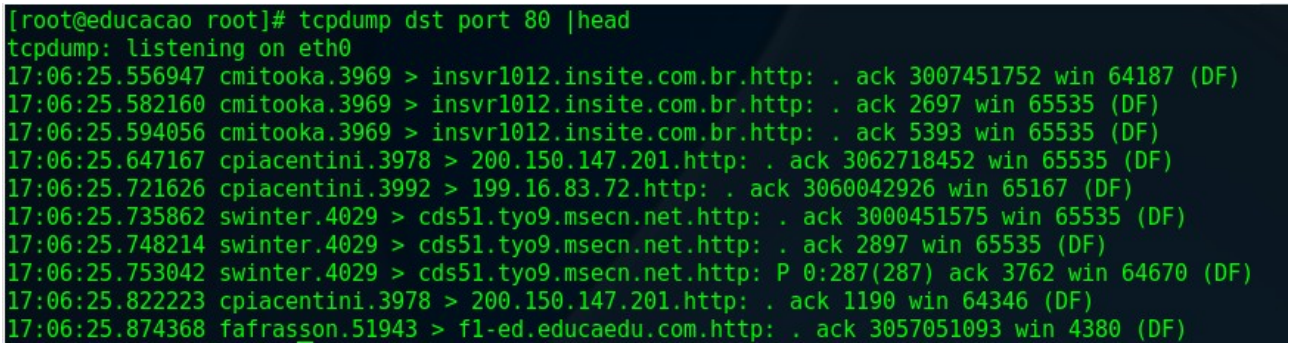

Figura 2: tcpdump monitorando a porta 80

Monitoramento

No capítulo anterior foi exibido um exemplo básico de monitoramento, onde monitoramentos a porta 80, neste capítulo serão exibidas informações mais detalhadas de monitoramento utilizando recursos avançados, como filtros de origem, destino, interfaces e protocolos. Abaixo abordamos um exemplo um pouco mais complexo de monitoramento, onde podemos monitorar o host de origem com endereço ip 192.168.0.20 e porta de destino 80, ou seja, estaremos monitorando o acesso a internet deste host.

tcpdump -i any src host 192.168.0.20 and dst port 80

O exemplo acima traz algumas novas opções como a opção -i, que recebeu o parâmetro any, especificando todas as interfaces, no caso de monitorar a terceira interface de rede, parâmetro src host que indica source host ou host de origem o endereços ip que desejamos monitorar e o parâmetro dst port que indica a porta de destino. Por padrão o tcpdump mostra os resultados do monitoramento por nome de hosts, se for desejada a exibição dos endereços ip, devemos utilizar a opção **-n**, esta opção não resolve nomes e serão exibidos os endereços dos hosts de origem e destino. Da mesma forma que foi especificado o destino através do parametro dts, é possível especificar a origem como párâmetro src, bastando apenas substituir pelo mais adequado, de forma equivalente é possível também especificar portas de origem ou destino, abaixo podemos visualizar um exemplo de comunicação do Windows Live Messenger utilizando a porta 1863 vindas do host 192.168.0.20:

tcpdump -i any src host 192.168.0.20 and dst port 186

Também é possível monitorar por protocolo, muito útil para verificar problemas na rede, no exemplo abaixo é exibido o filtro que monitora o host 192.168.0.20 e o protocolo icmp, da mesma forma podem ser especificdos os protocolos tcp, udp, etc.

tcpdump -i any src host 192.168.0.20 and proto ICMP

Em casos de lentidão na rede ou no firewall, uma das ações a serem tomadas seria a verificação de pacotes de broad-cast na rede, é de grande utilidade verificar quais hosts enviam pacotes a toda a rede sem necessidade, muitos worms e vírus também podem ser identificados por esta forma de análise, par aisso podemos utiklizar a seguinte expressão com o tcpdump:

tcpdump -i any ip broadcast

Com este filtro é possível identificar todos os hosts que estão efetuando broad-cast na rede e ter idéia do que pode estar causando problemas na mesma.

Trabalhando com arquivos

Um dos recursos mais interessantes presentes no tcpdump, é a possibilidade de trabalhar com arquivos, por exemplo, você podemos monitorar o tráfego de nossa rede durante determinando período e após isso analisar os logs utilizando filtros. Para que o tcpdump gere arquivos, poderá ser utilizada a opção -w

tcpdump -i any -w teste.pcap

Desta forma, estaremos redirecionando a saída do tcpdump para o arquivo teste.pcap, o arquivo utiliza a extensão .pcap, isso porque em determinados casos pode ser de desejo do administrador analisar os pacotes em uma interface gráfica, como por exemplo o Wire Shark. Que é um analisador de protocolo de redes em modo gráfico. O arquivo teste.pcap que foi gerado necessita ser lido pelo próprio tcpdump, não podendo ser lido por editores de texto e sim utilizando a opção -r do tcpdump. Abaixo um exmplo de leitura:

tcpdump -r teste.pcap

Abaixo um exemplo de utilizaçãode filtros naleitura de arquivos:

tcpdump -r teste.pcap src host 192.168.0.10 -nn

Conclusão

Neste guia introdutŕorio foram apresentadas opções algumas das diversas opções e exemplos de utilização do tcpdump. É recomendada a visita ao seu site oficial em www.tcpdump.org. Também é recomendada a leitura de sua página de manual sendo utilizada através do comando man:

man tcpdump