13 Ferramentas de monitoramento e análise de hosts e redes

13.1 PING ICMP echo-request (ping-pong)

O comando comando verifica se o host está ativo e caso esteja envia pacotes e aguarda respostas, por isso echo-request ou pingo-pong.

No entanto, ao não haver resposta não signidica que o host-alvo esteja off, mas que pode estar ocupado ou sob ação de alguma ferramenta de segurança, por exemplo, um firewall com regras para bloquear ping.

```
$ ping -c3 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
64 bytes from 192.168.1.1: icmp_seq=1 ttl=64 time=932 ms
64 bytes from 192.168.1.1: icmp_seq=2 ttl=64 time=203 ms
64 bytes from 192.168.1.1: icmp_seq=3 ttl=64 time=303 ms
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 3 received, 0% packet loss, time 2001ms
rtt min/avg/max/mdev = 203.468/479.811/932.893/322.947 ms
```

Exemplo de ping que não obtém resposta por ter política de entrada de pacote icmp bloqueda:

```
$ ping -c3 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2034ms
```

Exemplo de ping que não sai do host ou da rede por ter política de saída de pacote icmp bloqueda:

```
$ ping -c3 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
ping: sendmsg: Operation not permitted
--- 192.168.1.1 ping statistics ---
3 packets transmitted, 0 received, 100% packet loss, time 2041ms
```

13.2 FPING – varredura ICMP

Para verificar a comunicação de vários dispositivos utiliza-se o fping para passar um range de IP para serem analisados.

Caso o fping não esteja instalado, basta executar o comando a seguir para instalar (Família Debian):

$ apt-get install fping

Para executar basta usar o comando da seguinte forma, que demonstra somente os hosts conectados:

$ fping -c1 192.168.1.1 192.168.1.10

192.168.1.1 : xmt/rcv/%loss = 1/0/100%

192.168.1.10 : xmt/rcv/%loss = 1/0/100%

Ou o comando a seguir para exibir todos os hosts solicitados pelo range:

$ fping -c1 -g 192.168.1.1 192.168.1.10

192.168.1.1 : [0], 84 bytes, 505 ms (505 avg, 0% loss)

192.168.1.1 : xmt/rcv/%loss = 1/1/0%, min/avg/max = 505/505/505

192.168.1.2 : xmt/rcv/%loss = 1/0/100%

192.168.1.3 : xmt/rcv/%loss = 1/0/100%

192.168.1.4 : xmt/rcv/%loss = 1/0/100%

192.168.1.5 : xmt/rcv/%loss = 1/0/100%

192.168.1.6 : xmt/rcv/%loss = 1/0/100%

192.168.1.7 : xmt/rcv/%loss = 1/0/100%

192.168.1.8 : xmt/rcv/%loss = 1/0/100%

192.168.1.9 : xmt/rcv/%loss = 1/0/100%

192.168.1.10 : xmt/rcv/%loss = 1/0/100%

Onde:

-c: quantidade de pacote a ser enviado; neste caso, apenas 1.

-g: indica o range de IP.

É possível também realizar a filtragem via redirecionamento de saídas:

$ fping -c1 -g 192.168.1.1 192.168.0.150 2> /dev/null > online.txt

$ cat online.txt

192.168.1.1 : [0], 84 bytes, 53.7 ms (53.7 avg, 0% loss)

192.168.1.103 : [0], 84 bytes, 0.07 ms (0.07 avg, 0% loss)

Onde:

2>: envia as saídas de erros para /dev/null.

>: envia as saídas sem erros para /root/arquivos.txt.

13.3 hping3

O hping3 é uma ferramenta utilizado para verificar conexões e suas portas. Permite o uso de opções de flags do pacote TCP para descobrir qual o estado real da porta, como por exemplo, verificar se a porta foi rejeitada ou bloqueada por um firewall.

Caso não esteja instalado basta executar o comando a seguir (Família Debian):

$ sudo apt-get install hping3

As opções de uso das flags do hping são:

- syn : flag de solicitação de sincronização
- syn-ack : resposta ao pacote com a flag syn habilitada
- ack : flag para sinalizar a comunicação
- fin : finaliza a conexão (processo normal de finalização)
- rst : reseta a conexão (processo forçado de finalização)
- SA - SYN/ACK
- RA - RST/ACK

Exemplos:

$ sudo hping3 --syn -c 1 -p 80 192.168.1.1

HPING localhost (wlo1 192.168.1.1): S set, 40 headers + 0 data bytes

len=44 ip=1192.168.1.1 ttl=64 DF id=0 sport=80 flags=SA seq=0 win=65495 rtt=3.9 ms

--- localhost hping statistic ---

3 packets transmitted, 3 packets received, 0% packet loss

round-trip min/avg/max = 3.7/5.1/7.7 ms

Onde:

--syn : envia um pacote SYN (syncronize).

-c 1 : quantidade de pacotes, no exemplo 1.

-p 80 : define a porta a ser analisada, no exemploa porta 80.

O hping3 retorna como informação que o campo flag tem como resposta SA, que significa que houve resposta do servidor e que a porta está aberta, ou seja, não existe nenhum filtro atuando na porta.

No entanto, na análise com o hping3 na porta 80 com uma regra/filtro de firewall, por exemplo o iptables, configurada para rejeitar pacotes (REJECT) a saída será diferente.

Regra iptables:

iptables -A INPUT -p tcp --dport 80 -j REJECT

Para visualizar se a regra foi criada digitar:

iptables -L

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  --  anywhere             anywhere            tcp dpt:http reject-with icmp-port-unreachable
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Após veificação da regra de rejeição de pacotes TCP na porta 80, utilizar o comando hping3 para verificar a sua saída:

hping3 --syn -c 1 -p 80 192.168.1.1

```
HPING localhost (wlo1 192.168.1.1): S set, 40 headers + 0 data bytes
ICMP Port Unreachable from ip=192.168.1.1 name=server
--- localhost hping statistic ---
1 packet transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

A resposta que ohping3 emite é que recebeu uma resposta dizendo que a porta não está alcançável, pois a regra com a ação REJECT (bloqueia enviando resposta) bloqueia o pacote e envia um erro ao remetente, informando que o pacote foi bloqueado.

A seguir, testar a análise com o hping3 na porta 80 em um alvo com regras de firewall iptables bloqueando pacotes com a ação DROP (bloqueia NÃO enviando resposta).

Regra iptables:

iptables -A INPUT -p tcp --dport 80 -j DROP

iptables -L

```
Chain INPUT (policy ACCEPT)
target     prot  opt  source               destination
DROP       tcp   --   anywhere            anywhere            tcp dpt:http
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Seguindo do comando do hping3:

hping3 --syn -c 1 -p 80 192.168.1.1

```
HPING localhost (wlo1 192.168.1.1): S set, 40 headers + 0 data bytes
--- 192.168.1.1 hping statistic ---
1 packets transmitted, 0 packets received, 100% packet loss
round-trip min/avg/max = 0.0/0.0/0.0 ms
```

No caso da regra do iptables bloquendo a porta 80com DROP, o hping 3 não obteve nenhuma resposta, pois a regra com a ação DROP bloqueia o pacote silenciosamente, ou seja, não retornando nenhuma mensagem.

Outra análise que pode ser realizada com o hping3, novamente na porta 80 por exemplo, em que o firewall iptabes aplica um filtro/regra com ação REJECT e com opção de parâmetro o reset de pacotes (Exemplo: REJECT --reject-with tcp-reset).

Regra iptables:

iptables -A INPUT -p tcp --dport 80 -j REJECT --reject-with tcp-reset

iptables -A INPUT -p tcp --dport 80 -j REJECT --reject-with tcp-reset

iptables -L

```
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
REJECT     tcp  --  anywhere             anywhere             tcp dpt:http reject-with tcp-reset
Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
```

Novamente executar o comando hping3:

#hping3 --syn -c 1 -p 80 192.168.1.1

```
HPING localhost (wlo1 192.168.1.1): S set, 40 headers + 0 data bytes
len=40 ip=127.0.0.1 ttl=64 DF id=0 sport=80 flags=RA seq=0 win=0 rtt=3.7 ms
--- 192.168.1.1 hping statistic ---
1 packets transmitted, 1 packets received, 0% packet loss
round-trip min/avg/max = 3.7/3.7/3.7 ms
```

Nesta situação o hping3 retorna uma resposta rejeitando pacotes. Importante notar que a informação recebida no campo flag= é uma resposta RA, isso indica que houve uma resposta do servidor de que a porta está fechada.