Prática - Conhecendo algumas funcionalidades do nfdump

Orientamos que nas demonstrações visualize em tela cheia e em alta definição.

nfdump

nfdump é um programa de visualização e análise de flows de rede. Ele lê os arquivos armazenados via nfcapd ou sfcapd e processa de acordo com as opções solicitadas. Os flows de rede, lembrando, nada mais são do que os pacotes de tráfego que passam pelo nosso dispositivo de rede e outras informações adicionais capturadas.

nfdump - opções de leitura

-r - Faz a leitura de um arquivo padrão nfdump.

Ex: $ nfdump -r /data/nfsen/profiles-data/live/roteador/2023/03/20/nfcapd.202303200830

-R - Faz a leitura de vários arquivos

Ex:$ nfdump -R /data/nfsen/profiles-data/live/roteador/2023/03/19

-M - Faz a leitura de múltiplos sources

Ex: $ nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R 2023/03/19/nfcapd.202303191800:2023/03/20/nfcapd.202303200000

nfdump - opção de agregação de valores

-A - Faz a agregação dos flows de acordo com a opção especificada.

proto	Protocolo de transporte utilizado
srcip,dstip	IP origem ou destino
srcnet , dstnet	Rede CIDR
srcport, dstport	Porta origem e destino

nfdump - formatação de saída - parte 1

-o - Define o formato de saída do relatório. Para que possamos melhor visualizar a saída do nfdump e não quebrar a linha vamos personalizar os campos de saída ocupando assim menos colunas da tela.

fmt:format define um formato personalizado

Vamos utilizar:
- **ts -** Data e horário que foi capturado o primeiro flow da conexão
- **sa/sap -** Endereço:Porta Origem
- **da/dap -** Endereço:Porta destino
- **pr -** Protocolo
- **fl -** Número de Flows coletados
- **pkt -** Número de pacotes coletados
- **byt -** Número agregado de bytes

nfdump - exemplo de leitura e agregação

```
 $ nfdump -M /data/nfsen/profiles-data/live/roteador:servicos
-R 2023/03/19/nfcapd.202303191800:2023/03/20/nfcapd.202303200000
-o 'fmt:%ts %pr %fl %pkt %byt' -A proto
```

nfdump - ordenação de valores

-O : Faz a apresentação em ordem de acordo com o especificado

flows	Quantidade de flows
packets	Número de pacotes packets(in)
bytes	Número de bytes bytes(in)
pps,bps	Pacotes/bits por segundo
tstart	Em ordem de tempo

nfdump - exemplo de ordenação de valores

```
$ nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/19/nfcapd.202303191800:2023/03/20/nfcapd.202303200000  -O
packets -o 'fmt:%ts %pr %fl %pkt %byt' -A proto
```

nfdump - geração de estatísticas

-s - Gera estatísticas “Top N” dos flows

-n - Define o número de flows ”N” a serem visualizados na estatística. O default é 10.

Obs: A opção “-s” desativa a formatação de saída personalizada

srcip, dstip, ip	Estatística sobre endereço IP
port, srcport, dstport	Estatísticas de portas
as, srcas, srcas	Estatísticas de número AS
if, outif, inif	Estatísticas de interfaces
proto	Protocolo de Transporte Utilizado

nfdump - exemplo de geração de estatísticas

```
$ nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/19/nfcapd.202303191800:2023/03/20/nfcapd.202303200000 -O
bytes -s dstip
```

nfdump - Quem consultou no dia 20 entre 00:00 e 10:30 o serviço de DNS do endereço 8.8.8.8

```
$   nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/20/nfcapd.202303200000:2023/03/20/nfcapd.202303201030  -o
'fmt:%ts %sap %dap %fl %byt' 'ip 8.8.8.8 and port 53'
```

nfdump - Quem acesso o serviços HTTP do host serviços no dia 20 entre 00:00 e 10:45

```
$ nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/20/nfcapd.202303200000:2023/03/20/nfcapd.202303201045 -A
srcip,dstip 'port 80 and not ip 177.8.96.2'
```

nfdump - formatação de saída - parte 2

-o - Define o formato de saída do relatório

Opções mais utilizadas:

raw	Imprime cada registro em multiplas linhas
line	Imprime cada flow e 1 linha. Formato default.
long	Imprime cada flows em 1 linha só que com mais detalhes.
extended	Igual ao long só que com mais detalhes.
csv	Imprime com os campos separados por vírgulas
fmt:format	define um formato personalizado

nfdump/nfsen - exemplo de formatação de saída 1/3

Formatação default é o **line**

```
$  nfdump -M
/data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/16/nfcapd.202303160000:2023/03/20/nfcapd.20230320000
0 -O bytes -n 3  'net 2801:8a::/32'
```

Valores de Endereços ficam truncados utilizar **line6**

```
$  nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/16/nfcapd.202303160000:2023/03/20/nfcapd.202303200000 -O
bytes -n 3 -o line6  'net 2801:8a::/32'
```

nfdump/nfsen - exemplo de formatação de saída 2/3

Para mais detalhes de informações utilizar o extended/extended6

```
$  nfdump -M
/data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/16/nfcapd.202303160000:2023/03/20/nfcapd.2023032
00000 -O bytes -n 3  -o extended6 'net 2801:8a::/32'
```

nfdump - exemplo de formatação de saída 3/3

Permite a visualização dos flows em múltiplas linhas

```
$  nfdump -M /data/nfsen/profiles-data/live/roteador -R
2023/03/20/nfcapd.202303201420:2023/03/20/nfcapd.2023032
01422 -n 10 -o raw -O tstart '(ip 177.8.96.11 and ip
177.8.96.4) and port 22'
```

nfdump - consulta em base de abuse

Podemos criar um script para executar pelo **cron** se algum de nossos endereços de rede trocou dados com algum endereço ativo de **Botnet**.

Download na abuse.ch de uma blocklist de Botnets ativas :
wget https://feodotracker.abuse.ch/downloads/ipblocklist_recommended.txt
.
nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R 2023/03/20/nfcapd.202303200000:2023/03/21/nfcapd.202303211120 -O bytes -o 'fmt:%ts %sa %da %pkt %byt %fl' -A srcip,dstip 'ip in [@include ipabuse.txt]'

nfdump - correlação de eventos - parte 1/5

Recebemos uma notificação do nosso provedor que o endereço 177.8.96.4 de nossa responsabilidade fez scan no endereço do roteador do provedor 177.8.96.9 por volta das 17:00 horas do dia 21/03/2023.

Verificar nos flows evidências desta ação:

```
$ nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/21/nfcapd.202303211700:2023/03/21/nfcapd.202303211730
-O flows -o 'fmt:%ts %sap %dap %pr %flg %fl' 'src ip 177.8.96.4
and ip 177.8.96.9'
```

nfdump - correlação de eventos - parte 2/5

O sysadmin do servidor serviços encontrou os seguintes logs nos arquivos last e /var/log/auth.log

```
$ last | grep "Mar 21" | grep test
test     pts/0        177.8.96.11      Tue Mar 21 16:29 - 17:56  (01:27)

$ more /var/log/auth.log | grep "Mar 21 16:00" | grep -v "pam_unix"
Mar 21 16:00:12 cliente sshd[6783]: Invalid user user from 177.8.96.11 port 42730
Mar 21 16:00:12 cliente sshd[6785]: Invalid user admin from 177.8.96.11 port 42744
Mar 21 16:00:12 cliente sshd[6788]: Connection closed by 177.8.96.11 port 42796 …
Mar 21 16:00:12 cliente sshd[6787]: Connection closed by 177.8.96.11 port 42784 …
Mar 21 16:00:12 cliente sshd[6786]: Accepted password for test from 177.8.96.11 …
Mar 21 16:00:12 cliente systemd-logind[556]: New session 195 of user test.
Mar 21 16:00:12 cliente systemd-logind[556]: Session 195 logged out. …
```

nfdump - correlação de eventos - parte 3/5

Buscar nos flows evidências que comprovem estes logs:

```
$ nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/21/nfcapd.202303211600:2023/03/21/nfcapd.202303211650
-O tstart -o 'fmt:%ts %sap %dap %pr %flg %fl' 'ip 177.8.96.4
and ip 177.8.96.11 and port 22'
```

nfdump - correlação de eventos - parte 4/5

O sysadmin do servidor serviços nos reportou também que por volta de 15:35 foi detectado nos logs do firewall diversas tentativas de conexões em portas aleatórias com origem o endereço 177.8.96.11.

```
$ nfdump -M /data/nfsen/profiles-data/live/roteador:servicos -R
2023/03/21/nfcapd.2023032114:35:2023/03/21/nfcapd.202303211550
-O flows -o 'fmt:%ts %sap %dap %pr %flg %fl' 'src ip
177.8.96.11 and ip 177.8.96.4'
```

nfdump - correlação de eventos - parte 5/5

Conclusão: Foi verificado que o atacante 177.8.96.11 às 15:35 horas do dia 21/03/2023 executou um scan procurando por portas abertas no host 177.8.96.4 e foi encontrado o serviço SSH aberto. Sua próxima ação foi realizar um ataque de força bruta às 16:00 horas buscando credenciais fracas. Foi descoberta a credencial "**test**" que foi configurada com senha fraca. De posse da credencial o atacante realizou um acesso SSH às 16:29 horas e executou um scan via nmap às 17:00 horas,com destino e roteador do provedor endereço 177.8.96.9. A conta foi bloqueada.