ngrep in examples

Filtering

Print udp packets

```
  ngrep “” udp
```

Print packets passing `eth0` device. Without `-d` ngrep listens to a default interface.

```
  ngrep -d eth0
```

Print packets for port 80 regardless of device

```
  ngrep -d any port 80
```

Only print packets that contain “interesting-domain.com”

```
  ngrep -d any “interesting-domain.com” port 80
```

You can use regex such as ‘.*’ in the search string

```
  ngrep -d any “domain-.*.com” port 80
```

Or use regex to search for ‘pass’ or ‘USER’

```
  ngrep -d any “pass|USER” port 80
```

Ignore case with `-i` to match for ‘user’ as well

```
  ngrep -d any -i “pass|USER” port 80
```

If you’re logged in via SSH you might want to ignore your own traffic

```
  ngrep -d any port not 22
```

ngrep

grep through network traffic

Common usage: `ngrep -d any -W byline “needle” port 80`

Other Options

Suppress the ‘#’, with `-q` (for ‘quiet’)
Only print packet headers and payload (if relevant)

```
  ngrep -q -d any “needle” port 80
```

Use `-W byline` for more readable output

```
  ngrep -d any -W byline “needle” port 80
```

Limit the number of results with `-n`

```
  ngrep -d any “needle” -n 3 port 80
```

Print empty packets with `-e`

```
  ngrep -e -d any
```

WALL-
SKILLS

Content adapted from aerokid240.blogspot.de/2009/11/ngrep.html
Designed by Wall-Skills.com - Spread knowlegde with 1-Pagers