pktmon - tcpdump for Windows

Here's a great series of articles by Rickard Nobel on using PKTMON.

Filter basics

```
# Layer-3
pktmon filter add "Some IP Address" -i 192.168.88.1
pktmon filter add "Some IP Subnet"  -i 192.168.88.0/24

pktmon filter add "All ICMP" -t ICMP
pktmon filter add "All TCP"  -t TCP
pktmon filter add "All UDP"  -t UDP

pktmon filter add "All DNS"  -p 53
pktmon filter add "DNS-UDP"  -t UDP -p 53
pktmon filter add "DNS-TCP"  -t TCP -p 53
pktmon filter add "LDAP"     -t TCP -p 389

pktmon filter add "Google DNS1" -i 8.8.8.8 -t UDP -p 53
pktmon filter add "Google DNS2" -i 8.8.4.4 -t UDP -p 53

pktmon filter add "All HTTP connections"  -p 80  -t TCP SYN RST FIN
pktmon filter add "All HTTPS connections" -p 443 -t TCP SYN RST FIN

pktmon filter add "IGMP"      -t 2
pktmon filter add "IPIP"      -t 4
pktmon filter add "GRE"       -t 47
pktmon filter add "IPSEC ESP" -t 50
pktmon filter add "OSPF"      -t 89
pktmon filter add "VRRP"      -t 112
```

```
# Layer-2
pktmon filter add "MAC Address" -m 00-11-22-33-44-55
pktmon filter add "MAC Address" -m 00:11:22:33:44:55

pktmon filter add "Cisco Discovery Protocol - CDP" -m 01:00:0C:CC:CC:CC

pktmon filter add "ARP"         -d ARP
pktmon filter add "Wake-on-Lan" -d 0x0842
pktmon filter add "LACP"        -d 0x8809
pktmon filter add "QinQ"        -d 0x88A8
pktmon filter add "LLDP"        -d 0x88cc

pktmon filter add "VLAN 101"    -v 101
```

Example: tcpdump like cli for Mikrotik MNDP packets

```
# clear filters
pktmon filter remove

# add MNDP filter
pktmon filter add Mikrotik_MNDP -t UDP -p 5678

# list interfaces available to capture on
pktmon list

# assign the capture interface number to a variable for use below
$captureInterface = x

# replace <interface> below with the interface number you wish to run the capture on
pktmon start -c -m rt -s 16 --comp $captureInterface

# same as above but removing the lines containing PktGroup if desired
pktmon start -c -m rt -s 16 --comp $captureInterface | Select-String -Pattern "PktGroup" -
NotMatch
```

Example: tcpdump like cli for LLDP packets

```
# clear filters
pktmon filter remove

# add MNDP filter
pktmon filter add "LLDP" -d 0x88cc

# list interfaces available to capture on
pktmon comp list

# assign the capture interface number to a variable for use below
$captureInterface = x

# replace <interface> below with the interface number you wish to run the capture on
pktmon start -c -m rt -s 16 --comp $captureInterface

# same as above but removing the lines containing PktGroup if desired
pktmon start -c -m rt -s 16 --comp $captureInterface | Select-String -Pattern "PktGroup" -
NotMatch
```

-end

Revision #7
Created 2024-09-17 17:39:55 UTC by bluecrow76
Updated 2024-09-17 18:48:00 UTC by bluecrow76