Microsoft Network Monitor

I had never heard of this tool until today... I've always used Wireshark. Today I needed to view traffic broken out by application (PID/ProcessName). I went hunting and found the Microsoft Network Monitor. Surprisingly it's very feature rich, easy to use, and did exactly what I needed it to do... and sooo much more. Check it out!

Microsoft Links

- Information about Network Monitor 3
- Download Microsoft Network Monitor 3.4 (archive)

Example Filters

Capturing everything except RDP:

```
!(tcp.port==3389)
```

Capture only DNS:

```
DNS
```

Filter Source or Destination IPv4 Address:

```
IPv4.Address == 1.1.1.1
```

Filter Source IPv4 Address:

```
IPv4.SourceAddress == 1.1.1.1
```

Filter IPV4 Source and Destination:

```
IPv4.Address==1.1.1.1 and IPv4.Address==2.2.2.2
```

Filter IPv4 Source or Destination to subnet:

```
((ipv4.Address & 255.0.0.0) == 10.0.0.0)
```

Filter IPv4 traffic to private only traffic (source and destination in RFC-1918 private subnets):

```
(((IPv4.SourceAddress & 255.0.0.0) == 10.0.0.0) || ((IPv4.SourceAddress & 255.240.0.0) == 172.16.0.0) ||
((IPv4.SourceAddress & 255.255.0.0) == 192.168.0.0))
&&
(((IPv4.DestinationAddress & 255.0.0.0) == 10.0.0.0) || ((IPv4.DestinationAddress & 255.240.0.0) ==
172.16.0.0) || ((IPv4.DestinationAddress & 255.255.0.0) == 192.168.0.0))
```

Filter CDP traffic

```
Ethernet.Address == 01-00-0c-cc-cc-cc
```

Filter LLDP traffic

```
LLDP
```

Filter Mikrotik MNDP traffic

Microsoft netmon has no protocol disassembler for the MNDP protocol. All you will see is a UDPPayloadData Binary Large Object, however, you can see data in the Hex Details view and can extract the data you need from there fairly easily.

```
(udp.DstPort==5678 AND udp.SrcPort==5678)
```

Filter CDP + LLDP + MNDP

```
Ethernet.Address == 01-00-0c-cc-cc-cc
OR
LLDP
OR
(udp.DstPort==5678 AND udp.SrcPort==5678)
```

Filter traffic by ProcessName

The filter below allows you to see if a process is communicating with any other IP address besides the one you listed:

```
ProcessName.Contains("WindTerm.exe") && IPv4.Address!= 9.9.9.9
```

Filtering NPS + Azure MFA

The Azure MFA NPS Extension uses HTTPS to communicate with login.microsoftonline.com and credentials.azure.com. The filters below enable capturing related traffic.

Suggested capture filter:

```
// Suggested capture filter
tcp.port == 443         // HTTPS
OR udp.port == 1812     // RADIUS
OR DNS.Qrecord.QuestionName.contains("login.microsoftonline.com")
OR DNS.Qrecord.QuestionName.contains("credentials.azure.com")
```

Suggested display filter:

```
// Suggested display filter
udp.port==1812 // RADIUS packets
OR DNS.Qrecord.QuestionName.contains("login.microsoftonline.com")
OR DNS.Qrecord.QuestionName.contains("credentials.azure.com")
OR ContainsBin(FrameData, ASCII, "login.microsoftonline.com") // Will show HTTPS certificate negotiation packets
OR ContainsBin(FrameData, ASCII, "credentials.azure.com")     // Will show HTTPS certificate negotiation packets
OR ((ipv4.SourceAddress & 255.255.0.0) == 20.190.0.0) || ((ipv4.DestinationAddress & 255.255.0.0) == 20.190.0.0)
OR ((ipv4.SourceAddress & 255.255.0.0) == 40.126.0.0) || ((ipv4.DestinationAddress & 255.255.0.0) == 40.126.0.0)
```

Example on other sites:

- Network Monitor Filter Examples

Running nmcap from the cmd prompt

Run the following command from anywhere to view the command line usage.

```
"C:\Program Files\Microsoft Network Monitor 3\nmcap.exe" /usage
```

Run the following command from anywhere to view the network adapters.

```
"C:\Program Files\Microsoft Network Monitor 3\nmcap.exe" /displaynetworks
```

After determining the network adapter you would like to perform the capture on, grab the command below, update the capture network interface, the capture filter, and the stop / start conditions.

```
"C:\Program Files\Microsoft Network Monitor 3\nmcap.exe" /network 4 /capture "dns || icmp || ((ipv4.Address & 255.255.248.0) == 104.244.40.0)" /CaptureProcesses /file C:\tmp\nmcap-capture-testing.cap  /TerminateWhen /KeyPress x /StopWhen /TimeAfter 30 min
```

Running nmcap from PowerShell

Run the following command from anywhere to view the command line usage.

```
& 'C:\Program Files\Microsoft Network Monitor 3\nmcap.exe' /usage
```

Run the following command from anywhere to view the network adapters.

```
& 'C:\Program Files\Microsoft Network Monitor 3\nmcap.exe' /displaynetworks
```

After determining the network adapter you would like to perform the capture on, grab the command below, update the capture network interface, the capture filter, and the stop / start conditions.

```
& 'C:\Program Files\Microsoft Network Monitor 3\nmcap.exe' /network 4 /capture "dns || icmp || ((ipv4.Address & 255.255.248.0) == 104.244.40.0)" /CaptureProcesses /file C:\tmp\nmcap-capture-testing.cap  /TerminateWhen /KeyPress x /StopWhen /TimeAfter 30 min
```

nmcap full command line usage

```
PS C:\> & 'C:\Program Files\Microsoft Network Monitor 3\nmcap.exe' /usage
Network Monitor Command Line Capture (nmcap) 3.4.2350.0

Options:
 /Help /? /Usage
      Displays this message.
      Example Usage: nmcap /Usage
```

/Example(s)

Displays a list of examples.

Example Usage: nmcap /Example

nmcap /examples

/TimeFormat

Displays the list of date and time formats available for the /Time switch.

Example Usage: nmcap /TimeFormat

/DisplayNetwork(s)

Displays the network adapters that Network Monitor can capture from.

Example Usage: nmcap /DisplayNetwork

nmcap /displaynetworks

/SetNplPath <path>[;<path>;...]

Builds a profile titled "NMCap Last Path" and attempts to compile.

If compilation is successful, the new profile is set as active.

If the provided NPL cannot compile, the Active Profile is unchanged.

On success, any existing "NMCap Last Path" profile is updated.

/DisplayNplPath

Displays the NPL path.

Example Usage: nmcap /DisplayNplPath

Note:

Nmcap gets the NPL files in the following order:

1) Files in the current directory

2) Files in the path set by /SetNplPath

3) Default NMCap installation directory

/DisplayProfiles

Display the installed profiles.

/DisplayProfileInfo <Profile Key>

Display detailed information for the indicated profile.

A Profile Key can be either the GUID or the Index displayed when using the /DisplayProfiles argument.

/UseProfile <Profile Key>

Use an alternate profile for the capture session. This setting must be before any /Capture arguments. Otherwise, the active profile is used.

A Profile Key can be either the GUID or the Index displayed when using
the /DisplayProfiles argument.

/SetActiveProfile <Profile Key>
Set the active profile for to the indicated profile. This setting changes
the default profile for other Network Monitor applications, as well.
A Profile Key can be either the GUID or the index displayed when using
the /DisplayProfiles argument.

/DeleteProfile <Profile Key>
Delete the indicated profile.
Only user-defined profiles can be deleted.
A Profile Key can be either the GUID or the index displayed when using
the /DisplayProfiles argument.

/SetDefaultParser [NplFileName.npl]
Specifies the default NPL parser
Example Usage: nmcap /SetDefaultParser sparser.npl

/DisplayDefaultParser
Displays the default NPL parser.
Example Usage: nmcap /DisplayDefaultParser
Note: If you do not explicitly set the default parser using
/SetDefaultParser, /DisplayDefaultParser does not display anything.

/MaxFrameLength <Number of Bytes>
Specifying the Max Frame Length limits the number of bytes captured per
frame to the specified value. If you enter a value of 68, every
frame is truncated to the first 68 bytes. This has an impact
on filtering because the filter may require elements defined in the frame
which are no longer present as a result of the truncation.
Example Usage: The following captures all traffic on all adapters
and limits the captured data to the first 68 bytes.
nmcap /network * /MaxFrameLength 68
Note: This does not apply to frames retrieved from /inputcapture files.

The following options are used together and have no meaning independently.
Refer to the examples to better understand how they can be used together.

Specifying Input Sources:

/Network <Network Adapter> [<network Adapter> ...]
Selects one or more space-delimited network adapters to capture from.
Adapters may be specified using their index, partial name with wildcard (*), or
quoted friendly name. (find using /DisplayNetwork above).
Example Usage: /Network inte* 2 'Local Area Connection 1'

/InputCapture <CaptureFile> [<CaptureFile> ...]
Selects one or more space-delimited capture files to capture from.
The frames in the capture files are replayed through NMCap.
Example Usage: /InputCapture dns.cap tcp.cap c:\temp\test.cap

/DisableConversations
Disables conversations. This enhances the performance of
NMCap. Some protocols such as MSRPC require conversation to be enabled.
Example Usage: /DisableConversations

/CaptureProcesses
Enables process tracking. This is incompatible with the
/DisableConversations switch as process tracking requires conversations.
Example Usage: /CaptureProcesses

/DisableLocalOnly
Disables local-only capture. This enables the capture in p-mode. All
frames seen by this computer are captured.
Example Usage: /DisableLocalOnly

/RecordFilters
Records the capture filters in the capture file.
Example Usage: /RecordFilters

/RecordConfig
Records the network configuration in the capture file.
Example Usage: /RecordConfig

/MinDiskQuotaPercentage <Minimal Disk Size Percentage>
Specifies the minimal disk size percentage allowed.
Note: Default minimal disk size percentage is 2 percent.
Example Usage: /MinDiskQuotaPercentage 20
(Sets the minimal disk size percentage to 20 percent.)

/MinDiskQuota:<Minimal disk Size>

Specifies the minimal disk size allowed.

Example Usage: /MinDiskQuota 20M

(Sets the minimal disk size to 20 MB.)

/Frame <Filter>

Frame filter. The frame filter is constructed from the NPL files.

You can use all the filter expressions that you can in the Netmon UI.

For more sample filters, type nmcap /Examples or see Standards Filter

in the Filter Toolbar of the UI.

This switch must be part of /StartWhen, /StopWhen, and /TerminateWhen.

Example Usage: /Frame Dns.Flags.Stats == 3

Capture File output:

/Capture [FrameFilter] /File <CaptureFile> [/File <CaptureFile>...]

Saves frames that pass the frame filter to the specified capture files.

Example Usage: /Capture dns.flags.status == 3 /File t.cap /File t2.cap

/ReassembleCapture [FrameFilter] /File <CaptureFile> [/File <CaptureFile>...]

An alternate to Capture (above) Saves frames that pass the frame filter

to the specified capture files, along with reassembled payloads.

Example Usage: /ReassembleCapture tcp /File tcp.cap /File tcp2.cap

/File <Capture File>[:<File Size Limit>]

Name of capture file to save frames to. Extensions are used to determine

the behavior of NMCap.

.cap -- Netmon 2 capture file

.chn -- Series of Netmon 2 capture files: t.cap, t(1).cap, t(2).cap...

<File Size Limit> is optional. It limits the file size of each capture

file generated. Default single capture file size limit is 20 MB. The

upper bound of the file size limit is 500 MB. The lower bound of the file

size limit depends on the frame size captured. (Note that the maximal size

of Ethernet frames is 1500 bytes)

The files are circular, so once the size limit is reached, new data

overwrites older data.

Example Usage: /File t.cap:50M

Starting, stopping, and events:

/StartWhen <Command Line Switch>
List of conditions that specify when to start capturing network frames.
If it is ignored, NMCap starts capturing immediately. When input
from capture files by /InputCapture, this switch is generally ignored.
Example Usage: /StartWhen /Time 7:02:00 AM 9/10/2005

/StopWhen <Command Line Switch>
List of conditions that specify when to stop capturing network frames.
Example Usage: /StopWhen /TimeAfter 20 min
This switch becomes active only after a preceding /StartWhen evaluates
to TRUE.
Example: /StartWhen /TimeAfter 10 min ... /StopWhen /TimeAfter 20 min
Nmcap starts after 10 minutes and stops after 10+20=30 minutes.
/StopWhen never terminates the program while the /StartWhen option
is set to FALSE. /TerminateWhen should be used to safely terminate immediately.

/TimeAfter <number>[units]
Indicates a time period. This switch can be part of /StartWhen, /StopWhen,
and /TerminateWhen. The user specifies the time units. By default it
is in seconds.
Example Usage: /TimeAfter 20 seconds

/Time <Time/Date>
Indicates a time of day. This switch can be part of /StartWhen, /StopWhen,
and /TerminateWhen. The time and date format depends on the settings in
the 'Region and Language' Control Panel.
Example Usage: /Time 10:30:00 AM 9/10/2005

/TerminateWhen <Command Line Switch>
This switch terminates NMCap immediately once it evaluates to TRUE.
Example Usage: /TerminateWhen /KeyPress x
Note:
The default relationship among the conditions following /Startwhen,
/Stopwhen, and /TerminateWhen is AND and the order is sensitive.
For example: /TerminateWhen /Timeafter 10 min /Keypress x
Nmcap terminates after 10 minutes have passed and the user presses the 'x' key.
And: /TerminateWhen /Keypress x /Timeafter 10 min
Nmcap terminates 10 minutes after the user press 'x' key.

/KeyPress <character>

Specifies which key to press. This switch can be part of /StartWhen,

/StopWhen, and /TerminateWhen.

Example Usage: /KeyPress z

-end

Revision #7
Created 22 January 2021 05:45:50 by bluecrow76
Updated 21 December 2023 19:58:34 by bluecrow76