Collect Packet Captures on Windows Client and Server OS

Contents

Introduction

This document describes how to collect packet captures on the Windows platform using the Windows **pktmon** utility in a highly secured customer environment. For example, banking, defense, navy, and more.

Problem

Highly secured government environment viz banks, defense, navy, and more, restrict installing 3rd party tools. Especially, the packet capture tool **Wireshark** in order to troubleshoot voice, video, and data packets. Change management approvals undergo time consumption and unnecessary delays in resolving an issue. Utility by default available with Windows can help to avoid the delay.

Solution

By default, the tool name **PKTMON** is a by-default packet snippet utility bundled with Microsoft Windows client and server operating systems. **PKTMON** is available on Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub, and Azure. Setting up is very easy and less time-consuming. The utility is run using the Windows command prompt (cmd) utility with administrator privileges.

Executable directory: C:\Windows\System32\PktMon.exe

Here it is assumed to trace the packet capture between System-1 (PG-A) and System-2 (Logger-A).

You must first identify the interface ID or Network Interface Controller or Card (NIC) ID on the system/virtual machine.

pktmon list - This command lists the interfaces on the system/virtual machine.

Output:

```
Network Adapters:
Id MAC Address Name
-- ----------- ----
9 00-50-56-BD-C1-83 vmxnet3 Ethernet Adapter #2
10 00-50-56-BD-82-7B vmxnet3 Ethernet Adapter
```

Note: For help, use the suffix help at the end of the command. That is, pktmon list help.

Table 1. Interface tables.

Once the interface ID is identified, the packet capture starts. The command enables the packet captures and packet counters.

Method 1. pktmon start --capture

This command starts capturing the packets at the default Windows logged-in user path.

Output:

```
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Users\Administrator\PktMon.etl
Max file size: 512 MB
Memory used: 64 MB
```

```
Collected Data:
Packet counters, packet capture

Capture Type:
      All packets

Monitored Components:
      All

Packet Filters:
      None
```

Table 2. Packet capture start indication.

Method 2. pktmon start --capture --file-name C:\Cisco\Campaigninactive\pga.etl

This command starts capturing the packets at the custom-defined path.

Output:

```
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None
```

Note: By default, it captures all interfaces and all packet types.

Table 3. Packet capture with path address in order to store the capture file.

In the middle of capture, the packet capture status can also be validated.

pktmon status- This command displays the ongoing active **pktmon** executed packet capture.

Output:

```
Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
```

```
None

Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga_1.etl
Max file size: 512 MB
Memory used: 64 MB
Events lost: 0

Event Providers:

ID                                              Level   Keywords
--                                               --------  ---------------
Microsoft-Windows-PktMon     4          0x12

C:\Users\Administrator>
```

Table 4. Validate the status of packet capture.

Once the issue is reproduced, stop the packet capture with the pktmon stop command.

Output:

```
Flushing logs...
Merging metadata...

Log file: C:\Cisco\Campaigninactive\pga.etl (No events lost)
```

Table 5. Stop the packet capture.

By default, **pktmon** stores in the default .etl format and there is a way to convert it into **pcapng** in order to review using Wireshark.

Method 1. pktmon etl2pcap PktMon.etl --out C:\Cisco\Campaigninactive\pga.pcapng

This command converts the default saved in the PktMon.etl file at the default directory to the **pcapng** format.

Output:

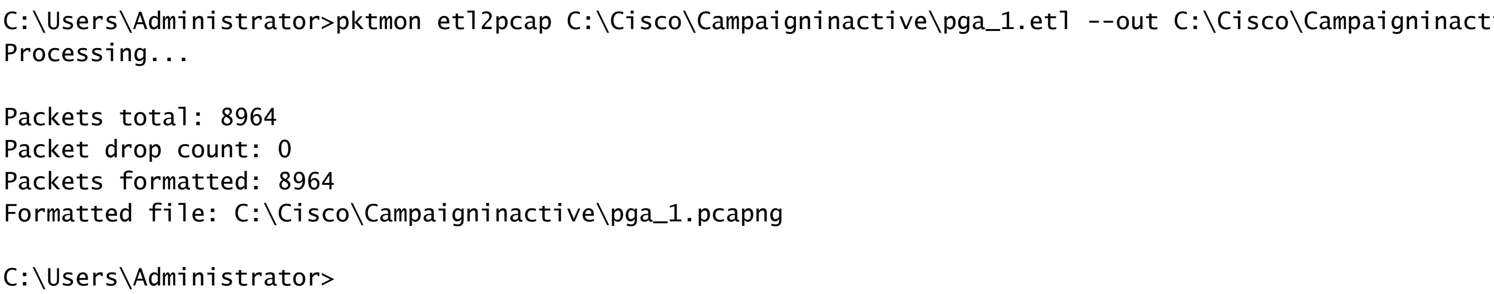
```
C:\Users\Administrator>pktmon etl2pcap PktMon.etl --out C:\Cisco\Campaigninactive\pga_2.pcapng
Processing...

Packets total: 606
Packet drop count: 0
Packets formatted: 606
Formatted file: C:\Cisco\Campaigninactive\pga_2.pcapng

C:\Users\Administrator>
```

Table 6.

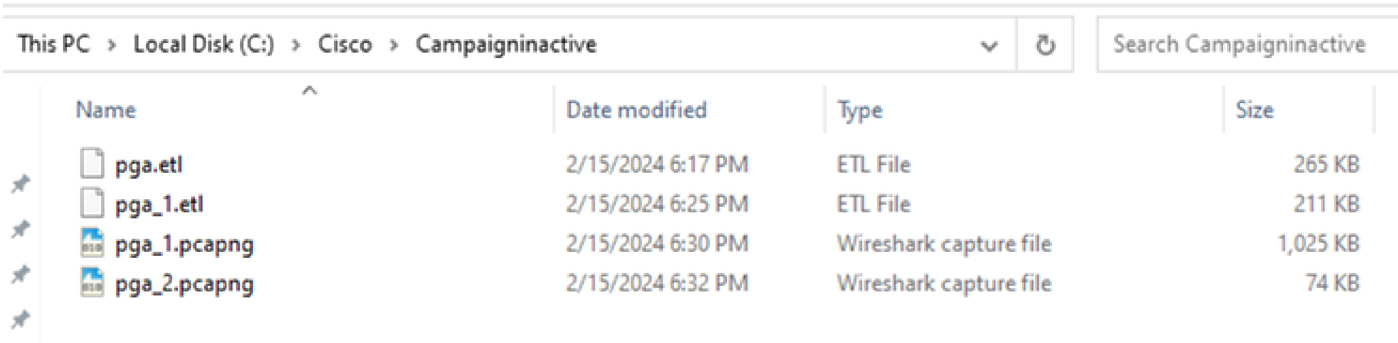
Method 1. To convert packet capture from native extension **.etl** to Wireshark readable format **.pcapng**.

Method 2. pktmonetl2pcapC:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga.pcapng

Output:



```
C:\Users\Administrator>pktmon etl2pcap C:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninact
Processing...

Packets total: 8964
Packet drop count: 0
Packets formatted: 8964
Formatted file: C:\Cisco\Campaigninactive\pga_1.pcapng

C:\Users\Administrator>
```



Name	Date modified	Type	Size
pga.etl	2/15/2024 6:17 PM	ETL File	265 KB
pga_1.etl	2/15/2024 6:25 PM	ETL File	211 KB
pga_1.pcapng	2/15/2024 6:30 PM	Wireshark capture file	1,025 KB
pga_2.pcapng	2/15/2024 6:32 PM	Wireshark capture file	74 KB

Image 1.

Method 2. to convert packet capture from native extension **.etl** to Wireshark readable format **.pcapng**.

These basic commands help collect the files and are useful in troubleshooting for TAC.

Related Information

- https://learn.microsoft.com/en-us/windows-server/networking/technologies/pktmon/pktmon
- Cisco Technical Support & Downloads