Coletar Capturas de Pacotes no Sistema Operacional do Cliente e do Servidor Windows

Contents

Introdução

Este documento descreve como coletar capturas de pacotes na plataforma Windows usando o utilitário pktmon do Windows em um ambiente de cliente altamente seguro. Por exemplo, bancos, defesa, marinha e muito mais.

Problema

O ambiente governamental altamente protegido, como bancos, defesa, marinha e muito mais, restringe a instalação de ferramentas de terceiros. Especialmente a ferramenta de captura de pacotes Wireshark para solucionar problemas de voz, vídeo e pacotes de dados. As aprovações de gerenciamento de alterações sofrem consumo de tempo e atrasos desnecessários na resolução de um problema. Utilitário por padrão disponível com o Windows pode ajudar a evitar o atraso.

Solução

Por padrão, o nome da ferramenta PKTMON é um utilitário de snippet de pacote fornecido com os sistemas operacionais cliente e servidor Microsoft Windows. O PKTMON está disponível no Windows Server 2022, Windows Server 2019, Windows 10, HCI do Azure Stack, Hub do Azure Stack e Azure. A configuração é muito fácil e menos demorada. O utilitário é executado usando o utilitário de prompt de comando do Windows (cmd) com privilégios de administrador.

Diretório executável: C:\Windows\System32\PktMon.exe

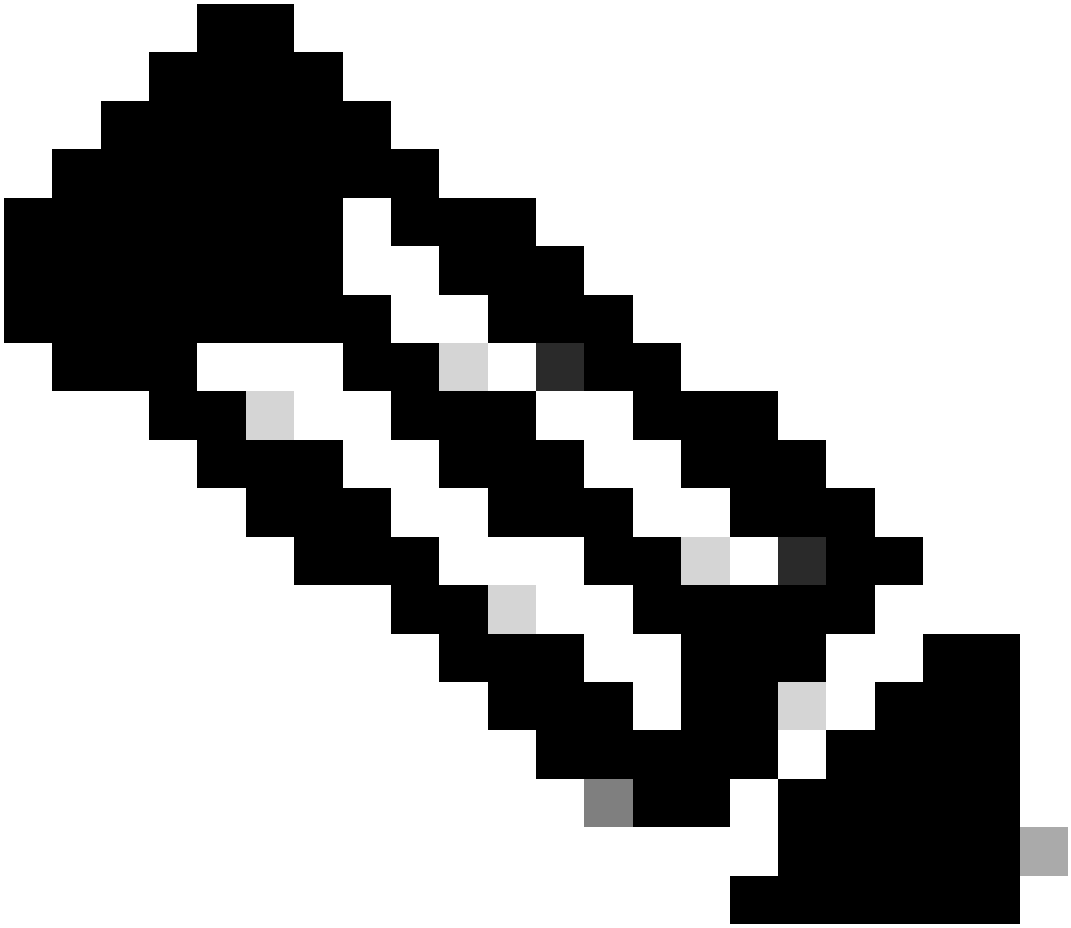
Aqui, presume-se que rastreie a captura de pacotes entre System-1 (PG-A) e System-2 (Logger-A).

Você deve primeiro identificar o ID da interface ou o ID da placa ou do controlador de interface de rede (NIC) no sistema/máquina virtual.

pktmon list - Esse comando lista as interfaces no sistema/máquina virtual.

Saída:

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



Observação: para obter ajuda, use o sufixo help no final do comando. Isto é, pktmon list ajuda.

Tabela 1. Tabelas de interface.

Uma vez identificado o ID da interface, a captura do pacote é iniciada. O comando ativa as capturas de pacotes e os contadores de pacotes.

Método 1. pktmon start --capture

Esse comando inicia a captura dos pacotes no caminho de usuário conectado do Windows padrão.

Saída:

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

Tabela 2. Indicação de início de captura de pacote.

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

Esse comando começa a capturar os pacotes no caminho definido pelo cliente.

Saída:

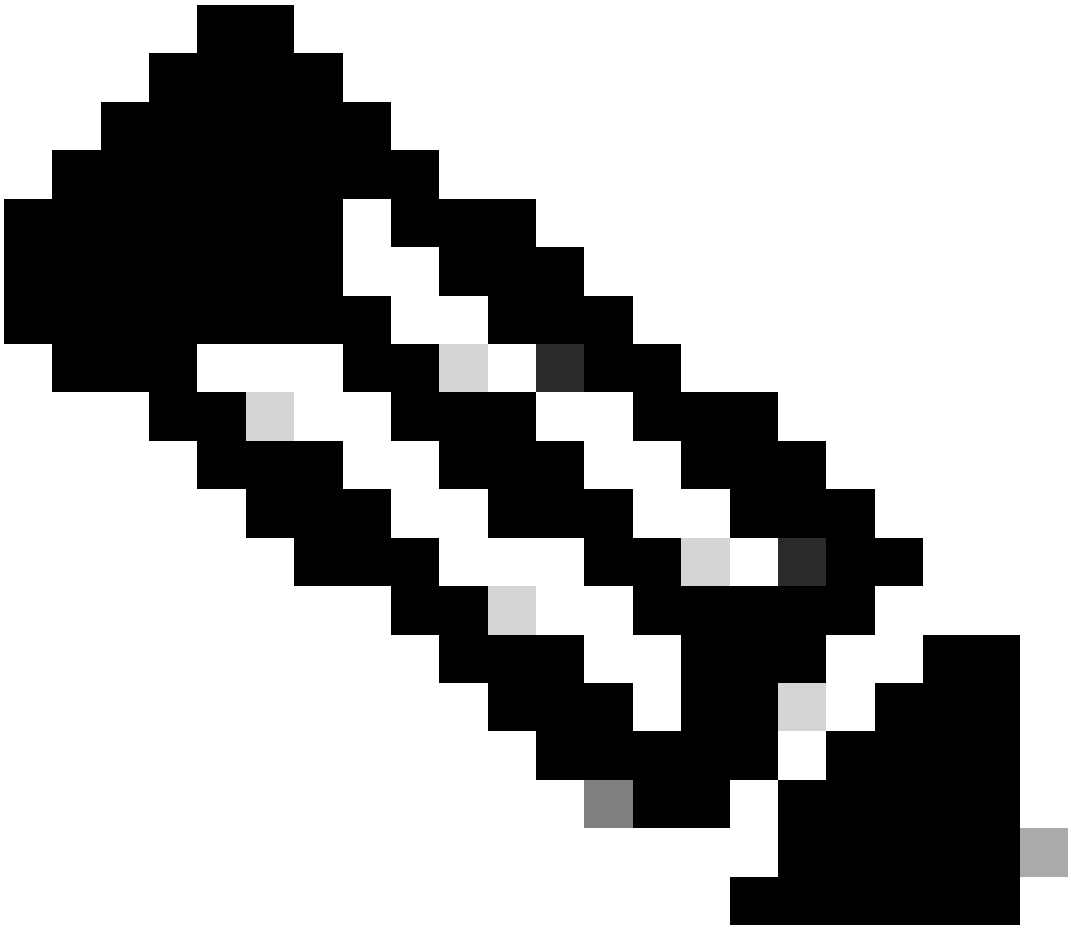
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None



Observação: por padrão, ele captura todas as interfaces e todos os tipos de pacotes.

Tabela 3. Captura de pacote com endereço de caminho para armazenar o arquivo de captura.

No meio da captura, o status da captura do pacote também pode ser validado.

pktmon statusEste comando exibe a captura de pacotes em andamento e **pktmon** executado.

Saída:

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>

Tabela 4. Validar o status da captura de pacotes.

Depois que o problema for reproduzido, interrompa a captura de pacotes com o pktmon stop comando.

Saída:

Flushing logs...
Merging metadata...

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

Tabela 5. Pare a captura de pacotes.

Por padrão, o **pktmon** armazena no formato padrão.etl e há uma maneira de convertê-lo em **pcapng** para revisar usando o Wireshark.

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

Esse comando converte o padrão salvo no arquivoPktMon.etl no diretório padrão para o **formato pcapng**.

Saída:

```
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>
```

Tabela 6.

Método 1. Para converter a captura de pacotes da extensão nativa **.etl** para o formato legível do Wireshark **.pcapng**.

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

Saída:

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

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

C:\Users\Administrator>
```

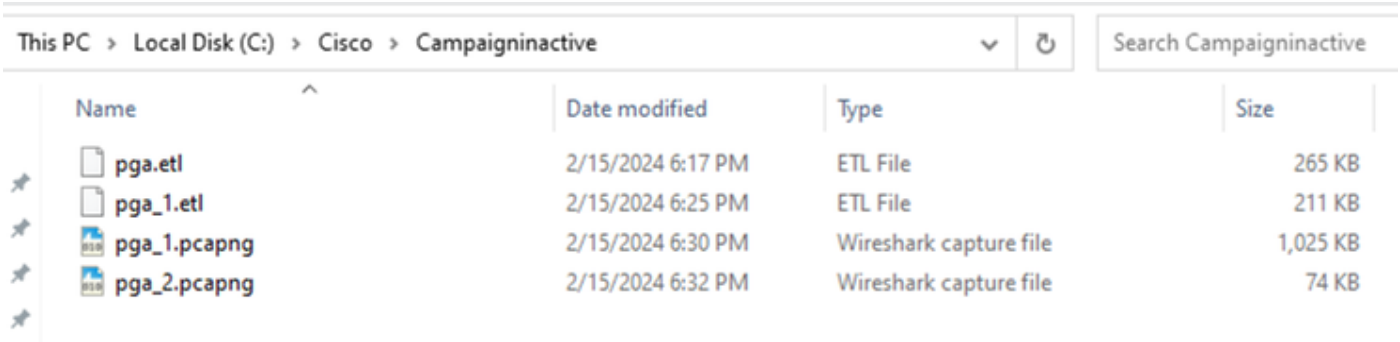


Imagem 1.

Método 2. para converter a captura de pacotes da extensão nativa **.etl** para o formato legível do Wireshark **.pcapng**.

Esses comandos básicos ajudam a coletar os arquivos e são úteis na solução de problemas do TAC.

Informações Relacionadas

- https://learn.microsoft.com/en-us/windows-server/networking/technologies/pktmon/pktmon

- Suporte técnico e downloads da Cisco

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.