Windows 클라이언트 및 서버 OS에서 패킷 캡처 수집

목차

소개

이 문서에서는 매우 안전한 고객 환경에서 Windows pktmon 유틸리티를 사용하여 Windows 플랫폼에서 패킷 캡처를 수집하는 방법에 대해 설명합니다. 예를 들면 은행, 국방, 해군 등이 있습니다.

문제

은행, 국방, 해군 등을 통해 보안이 강화된 정부 환경에서 타사 도구 설치를 제한합니다. 특히 패킷 캡처 툴인 Wireshark는 음성, 비디오 및 데이터 패킷의 문제를 해결하기 위해 사용됩니다. 변경 관리 승인은 시간 소모와 문제 해결의 불필요한 지연을 겪습니다. Windows에서 기본적으로 제공되는 유틸리티를 사용하면 지연을 방지할 수 있습니다.

솔루션

기본적으로 PKTMON 도구 이름은 Microsoft Windows 클라이언트 및 서버 운영 체제와 함께 번들로 제공되는 기본 패킷 스니펫 유틸리티입니다. PKTMON은 Windows Server 2022, Windows Server 2019, Windows 10, Azure Stack HCI, Azure Stack Hub 및 Azure에서 사용할 수 있습니다. 설정은 매우 쉽고 시간 소모가 적습니다. 이 유틸리티는 관리자 권한으로 cmd(Windows 명령 프롬프트) 유틸리티를 사용하여 실행됩니다.

실행 파일 디렉터리: C:\Windows\System32\PktMon.exe

여기서는 System-1(PG-A)과 System-2(Logger-A) 간의 패킷 캡처를 추적한다고 가정합니다.

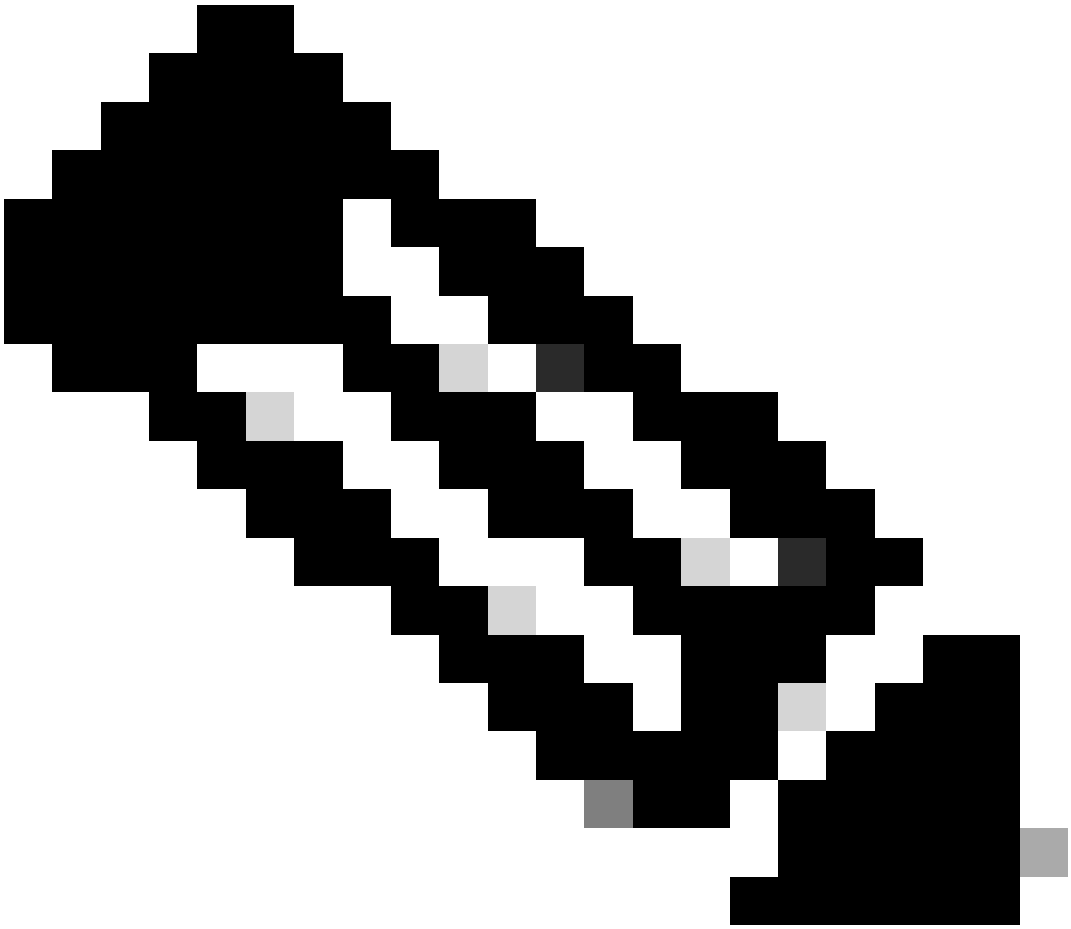
먼저 시스템/가상 머신에서 인터페이스 ID 또는 네트워크 인터페이스 컨트롤러 또는 카드(NIC) ID를 식별해야 합니다.

pktmon list - 이 명령은 시스템/가상 머신의 인터페이스를 나열합니다.

성과:

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



참고: 도움말을 보려면 명령 끝에 접미사 help를 사용하십시오. 바로, pktmon list 도와주세요.

표 1. 인터페이스 테이블.

인터페이스 ID가 식별되면 패킷 캡처가 시작됩니다. 이 명령은 패킷 캡처 및 패킷 카운터를 활성화합니다.

방법 1. pktmon start --capture

이 명령은 기본 Windows 로그인 사용자 경로에서 패킷 캡처를 시작합니다.

성과:

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

표 2. 패킷 캡처 시작 표시

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

이 명령은 사용자 정의 경로에서 패킷 캡처를 시작합니다.

성과:

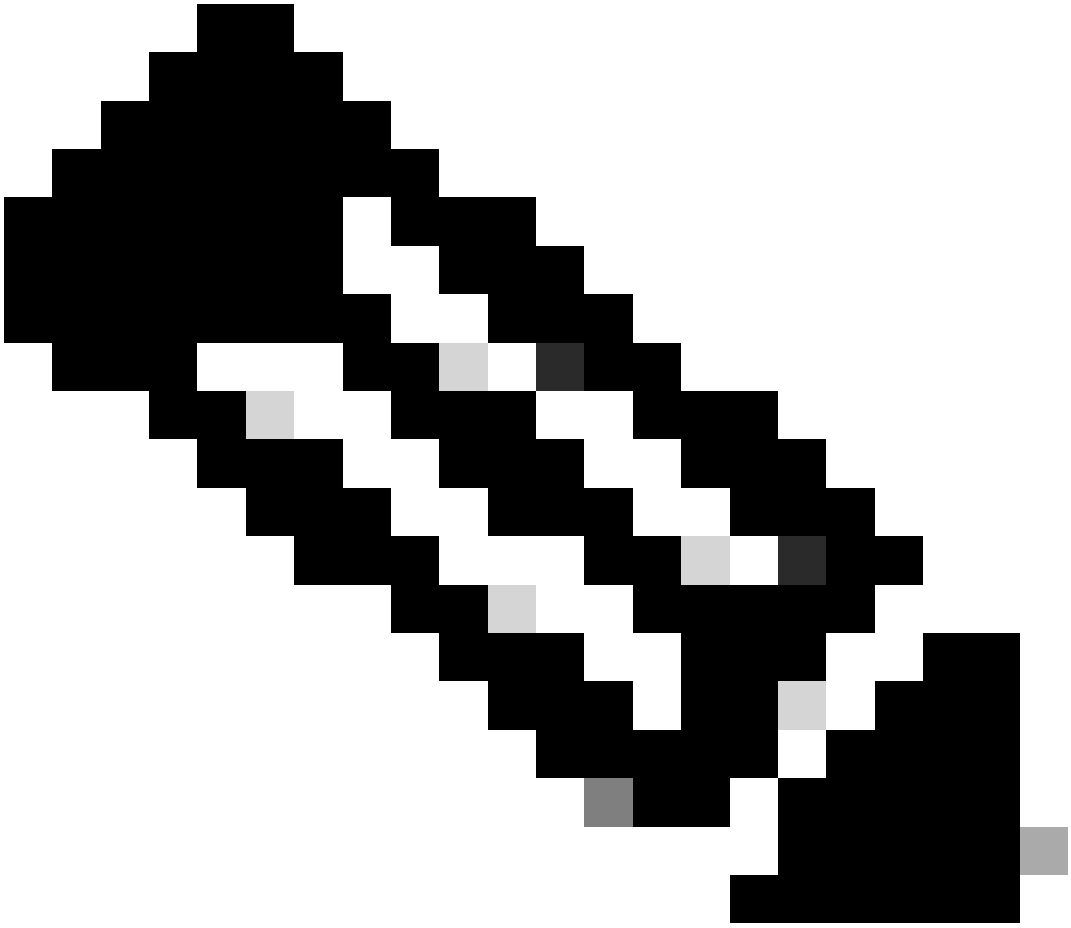
Logger Parameters:
Logger name: PktMon
Logging mode: Circular
Log file: C:\Cisco\Campaigninactive\pga.etl
Max file size: 512 MB
Memory used: 64 MB

Collected Data:
Packet counters, packet capture

Capture Type:
All packets

Monitored Components:
All

Packet Filters:
None



참고: 기본적으로 모든 인터페이스 및 모든 패킷 유형을 캡처합니다.

표 3. 캡처 파일을 저장하기 위해 경로 주소를 사용하여 패킷을 캡처합니다.

캡처 중에 패킷 캡처 상태도 검증할 수 있습니다.

pktmon status- 이 명령은 진행 중인 활성 pktmon **실행** 패킷 캡처를 표시합니다.

성과:

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>

표 4. 패킷 캡처의 상태를 확인합니다.

문제가 재현되면 명령을 사용하여 패킷 캡처를 pktmon stop 중지합니다.

성과:

Flushing logs...
Merging metadata...

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

표 5. 패킷 캡처를 중지합니다.

기본적으로 **pktmon**은 기본.etl 형식으로 저장되며 Wireshark를 사용하여 검토하기 위해 **pcapping**으로 변환하는 방법이 있습니다.

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

이 명령은 기본 디렉토리에 있는 파일에PktMon.etl 저장된 기본값을 **패핑** 형식으로 변환합니다.

성과:

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>

표 6.

방법 1. 패킷 캡처를 기본 extension**.etl**에서 Wireshark에서 읽을 수 있는 형식 .pcapping으로 **변환합니다**.

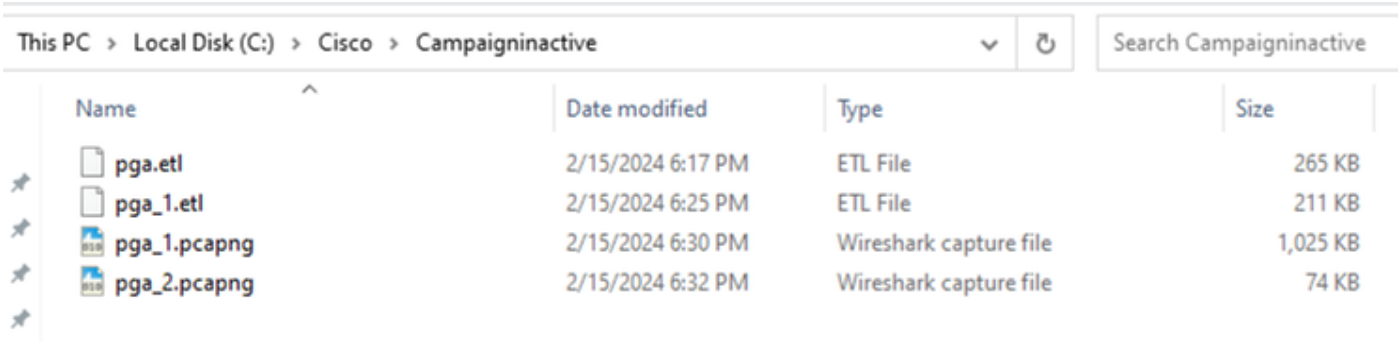
방법 2. pktmonetl2pcapC:\Cisco\Campaigninactive\pga_1.etl --out C:\Cisco\Campaigninactive\pga.pcapng

성과:

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>



이미지 1.

방법 2. 패킷 캡처를 기본 extension**.etl**에서 Wireshark에서 읽을 수 있는 형식 .pcapng으로 **변환합니다**.

이러한 기본 명령은 파일을 수집하는 데 도움이 되며 TAC의 문제 해결에 유용합니다.

관련 정보

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

- Cisco 기술 지원 및 다운로드

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.