



# /Pktmon.exe Star

## Reconnaissance

Capture Network Packets on the windows 10 with October 2018 Update or later.

### Paths:

c:\windows\system32\pktmon.exe  
c:\windows\syswow64\pktmon.exe

### Resources:

- <https://binar-x79.com/windows-10-secret-sniffer/>

### Acknowledgements:

- Derek Johnson

### Detections:

- Sigma: [proc\\_creation\\_win\\_lolbin\\_pktmon.yml](#)
- IOC: .etl files found on system

## Reconnaissance

1. Will start a packet capture and store log file as PktMon.etl. Use pktmon.exe stop

```
pktmon.exe start --etw
```

**Use case:** use this a built in network sniffer on windows 10 to capture sensitive traffic  
**Privileges required:** Administrator  
**Operating systems:** Windows 10 1809 and later, Windows 11  
**ATT&CK® technique:** [T1040: Network Sniffing](#)

2. Select Desired ports for packet capture

```
pktmon.exe filter add -p 445
```

**Use case:** Look for interesting traffic such as telnet or FTP  
**Privileges required:** Administrator  
**Operating systems:** Windows 10 1809 and later, Windows 11  
**ATT&CK® technique:** [T1040: Network Sniffing](#)