

# T1040 - Network Sniffing

## Description from ATT&CK

Adversaries may sniff network traffic to capture information about an environment, including authentication material passed over the network. Network sniffing refers to using the network interface on a system to monitor or capture information sent over a wired or wireless connection. An adversary may place a network interface into promiscuous mode to passively access data in transit over the network, or use span ports to capture a larger amount of data. Data captured via this technique may include user credentials, especially those sent over an insecure, unencrypted protocol. Techniques for name service resolution poisoning, such as [LLMNR/NBT-NS Poisoning and SMB Relay](#), can also be used to capture credentials to websites, proxies, and internal systems by redirecting traffic to an adversary.

Network sniffing may also reveal configuration details, such as running services, version numbers, and other network characteristics (e.g. IP addresses, hostnames, VLAN IDs) necessary for subsequent Lateral Movement and/or Defense Evasion activities.



interface	Specify interface to perform PCAP on.	String	ens33
-----------	---------------------------------------	--------	-------

Attack Commands: Run with `bash` ! Elevation Required (e.g. root or admin)

```
tcpdump -c 5 -nnni #{interface}
tshark -c 5 -i #{interface}
```

Dependencies: Run with `bash` !

Description: Check if at least one of tcpdump or tshark is installed.

Check Prereq Commands:

```
if [ ! -x "$(command -v tcpdump)" ] && [ ! -x "$(command -v tshark)" ]; then exit :
```

Get Prereq Commands:

```
(which yum && yum -y install epel-release tcpdump tshark) || (which apt-get && DEBIAN
```

## Atomic Test #2 - Packet Capture macOS

Perform a PCAP on macOS. This will require Wireshark/tshark to be installed. TCPdump may already be installed.

Upon successful execution, tshark or tcpdump will execute and capture 5 packets on interface en0A.

Supported Platforms: macOS

auto\_generated\_guid: 9d04efee-eff5-4240-b8d2-07792b873608

Inputs:

Name	Description	Type	Default Value
------	-------------	------	---------------

interface	Specify interface to perform PCAP on.	String	en0A
-----------	---------------------------------------	--------	------

Attack Commands: Run with `bash` ! Elevation Required (e.g. root or admin)

```
sudo tcpdump -c 5 -nnni #{interface}
if [ -x "$(command -v tshark)" ]; then sudo tshark -c 5 -i #{interface}; fi;
```

Dependencies: Run with `bash` !

Description: Check if at least one of tcpdump or tshark is installed.

Check Prereq Commands:

```
if [ ! -x "$(command -v tcpdump)" ] && [ ! -x "$(command -v tshark)" ]; then exit ;
```

Get Prereq Commands:

```
(which yum && yum -y install epel-release tcpdump tshark) || (which apt-get && DEBIAN
```

## Atomic Test #3 - Packet Capture Windows Command Prompt

Perform a packet capture using the windows command prompt. This will require a host that has Wireshark/Tshark installed.

Upon successful execution, tshark will execute and capture 5 packets on interface "Ethernet".

Supported Platforms: Windows

auto\_generated\_guid: a5b2f6a0-24b4-493e-9590-c699f75723ca

Inputs:

Name	Description	Type	Default Value
------	-------------	------	---------------

interface	Specify interface to perform PCAP on.	String	Ethernet
wireshark_url	wireshark installer download URL	Url	<a href="https://1.eu.dl.wireshark.org/win64/Wireshark-win64-latest.exe">https://1.eu.dl.wireshark.org/win64/Wireshark-win64-latest.exe</a>
tshark_path	path to tshark.exe	Path	c:\program files\wireshark\tshark.exe
npcap_url	npcap installed download URL	Url	<a href="https://nmap.org/npcap/dist/npcap-1.31.exe">https://nmap.org/npcap/dist/npcap-1.31.exe</a>
npcap_path	path to npcap.sys	Path	C:\Program Files\Npcap\npcap.sys

Attack Commands: Run with `command_prompt` ! Elevation Required (e.g. root or admin)

```
"c:\Program Files\Wireshark\tshark.exe" -i #{interface} -c 5
```

Dependencies: Run with `powershell` !

Description: tshark must be installed and in the default path of "c:\Program Files\Wireshark\Tshark.exe".

Check Prereq Commands:

```
if (test-path "#{tshark_path}") {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Invoke-WebRequest -OutFile $env:temp\wireshark_installer.exe #{wireshark_url}
Start-Process $env:temp\wireshark_installer.exe /S
```

Description: npcap must be installed.

Check Prereq Commands:

```
if (test-path "#{npcap_path}") {exit 0} else {exit 1}
```

#### Get Prereq Commands:

```
Invoke-WebRequest -OutFile $env:temp\npcap_installer.exe #{npcap_url}  
Start-Process $env:temp\npcap_installer.exe
```



## Atomic Test #4 - Windows Internal Packet Capture

Uses the built-in Windows packet capture After execution you should find a file named trace.etl and trace.cab in the temp directory

**Supported Platforms:** Windows

**auto\_generated\_guid:** b5656f67-d67f-4de8-8e62-b5581630f528

**Attack Commands:** Run with **command\_prompt** ! Elevation Required (e.g. root or admin)

```
netsh trace start capture=yes tracefile=%temp%\trace.etl maxsize=10
```



#### Cleanup Commands:

```
netsh trace stop >nul 2>&1  
TIMEOUT /T 5 >nul 2>&1  
del %temp%\trace.etl >nul 2>&1  
del %temp%\trace.cab >nul 2>&1
```



## Atomic Test #5 - Windows Internal pktmon capture

Will start a packet capture and store log file as t1040.etl. <https://lolbas-project.github.io/lolbas/Binaries/Pktmon/>

**Supported Platforms:** Windows

auto\_generated\_guid: c67ba807-f48b-446e-b955-e4928cd1bf91

Attack Commands: Run with **command\_prompt** ! Elevation Required (e.g. root or admin)

```
pktmon.exe start --etw -f %TEMP%\t1040.etl  
TIMEOUT /T 5 >nul 2>&1  
pktmon.exe stop
```



Cleanup Commands:

```
del %TEMP%\t1040.etl
```



## Atomic Test #6 - Windows Internal pktmon set filter

Select Desired ports for packet capture <https://lolbas-project.github.io/lolbas/Binaries/Pktmon/>

Supported Platforms: Windows

auto\_generated\_guid: 855fb8b4-b8ab-4785-ae77-09f5df7bff55

Attack Commands: Run with **command\_prompt** ! Elevation Required (e.g. root or admin)

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



Cleanup Commands:

```
pktmon filter remove
```

