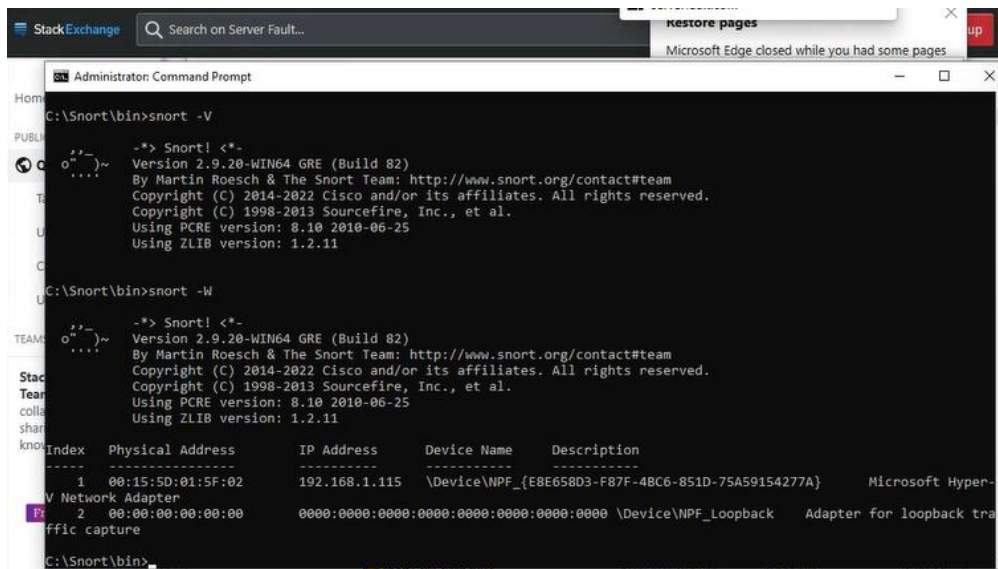


Commandos:

Snort -V

Snort -W



The screenshot shows a Windows Command Prompt window titled "Administrator: Command Prompt". The user is in the directory C:\Snort\bin. They run the command "snort -V", which displays the Snort version (2.9.20-WIN64 GRE (Build 82)) and copyright information. Then, they run "snort -W", which displays a table of network interfaces.

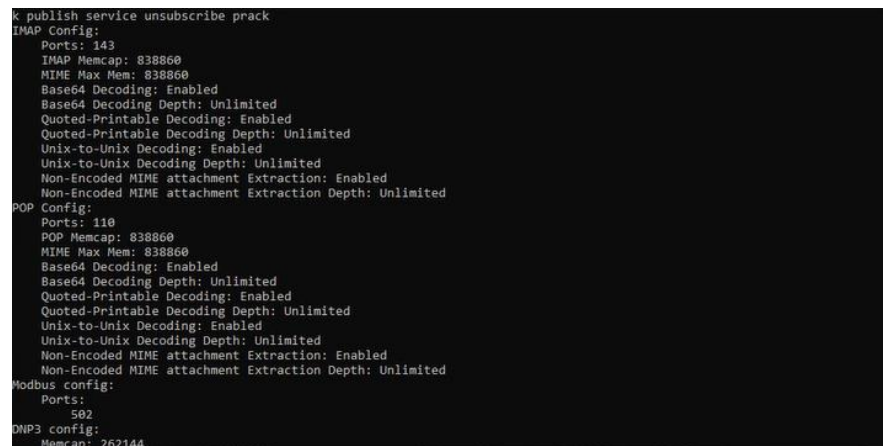
```
C:\Snort\bin>snort -V
-*> Snort! <*-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

C:\Snort\bin>snort -W
-*> Snort! <*-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Index  Physical Address      IP Address      Device Name      Description
-----
1      00:15:50:01:5F:02      192.168.1.115   \Device\NPF_{E8E658D3-F87F-4BC6-851D-75A59154277A}  Microsoft Hyper-
V Network Adapter
2      00:00:00:00:00:00      0000:0000:0000:0000:0000:0000:0000:0000 \Device\NPF_Loopback  Adapter for loopback tra
ffic capture

C:\Snort\bin>
```

snort -i 1 -c c:\Snort\etc\snort.conf -T



The screenshot shows the output of the command "snort -T". It displays the configuration for IMAP, POP, Modbus, and DNP3 services, including ports, memory limits, and decoding options.

```
K publish service unsubscribe prack
IMAP Config:
  Ports: 143
  IMAP Memcap: 838860
  MIME Max Mem: 838860
  Base64 Decoding: Enabled
  Base64 Decoding Depth: Unlimited
  Quoted-Printable Decoding: Enabled
  Quoted-Printable Decoding Depth: Unlimited
  Unix-to-Unix Decoding: Enabled
  Unix-to-Unix Decoding Depth: Unlimited
  Non-Encoded MIME attachment Extraction: Enabled
  Non-Encoded MIME attachment Extraction Depth: Unlimited
POP Config:
  Ports: 110
  POP Memcap: 838860
  MIME Max Mem: 838860
  Base64 Decoding: Enabled
  Base64 Decoding Depth: Unlimited
  Quoted-Printable Decoding: Enabled
  Quoted-Printable Decoding Depth: Unlimited
  Unix-to-Unix Decoding: Enabled
  Unix-to-Unix Decoding Depth: Unlimited
  Non-Encoded MIME attachment Extraction: Enabled
  Non-Encoded MIME attachment Extraction Depth: Unlimited
Modbus config:
  Ports:
    502
DNP3 config:
  Memcap: 262144
```

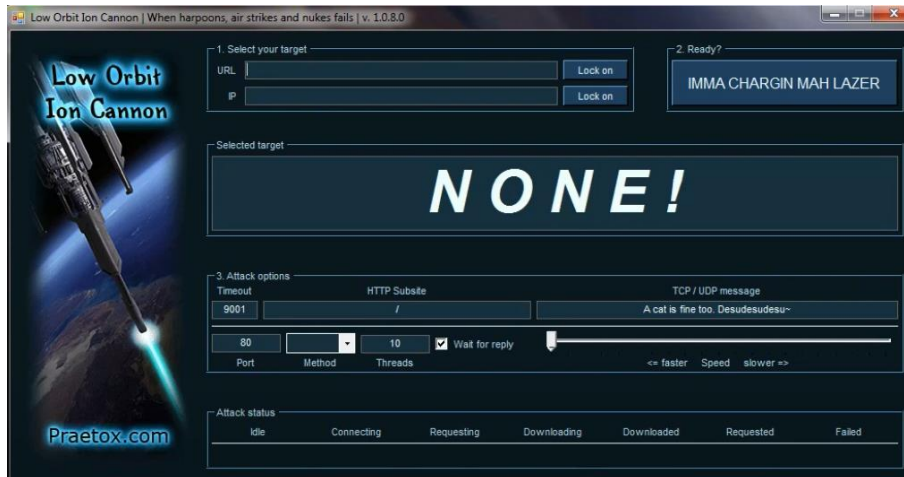
```
Select Administrator Command Prompt

-*) Snort! <*-
Version 2.9.20-WIN64 GRE (Build 82)
By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
Copyright (C) 2014-2022 Cisco and/or its affiliates. All rights reserved.
Copyright (C) 1998-2013 Sourcefire, Inc., et al.
Using PCRE version: 8.10 2010-06-25
Using ZLIB version: 1.2.11

Rules Engine: SF_SNORT_DETECTION_ENGINE Version 3.2 <Build 1>
Preprocessor Object: SF_SSLPP Version 1.1 <Build 4>
Preprocessor Object: SF_SSH Version 1.1 <Build 3>
Preprocessor Object: SF_SMTP Version 1.1 <Build 9>
Preprocessor Object: SF_SIP Version 1.1 <Build 1>
Preprocessor Object: SF_SDP Version 1.1 <Build 1>
Preprocessor Object: SF_REPUTATION Version 1.1 <Build 1>
Preprocessor Object: SF_POP Version 1.0 <Build 1>
Preprocessor Object: SF_MODBUS Version 1.1 <Build 1>
Preprocessor Object: SF_IMAP Version 1.0 <Build 1>
Preprocessor Object: SF_GTP Version 1.1 <Build 1>
Preprocessor Object: SF_FTPTELNET Version 1.2 <Build 13>
Preprocessor Object: SF_DNS Version 1.1 <Build 4>
Preprocessor Object: SF_DNP3 Version 1.1 <Build 1>
Preprocessor Object: SF_DCERPCZ Version 1.0 <Build 3>

Total snort Fixed Memory Cost - MaxRss:1910855072
Snort successfully validated the configuration!
Snort exiting
C:\Snort\bin>
```

## LOIC APP



Selected target

145.14.145.16

3. Attack options

Timeout

9001

HTTP Subsite

/

TCP / UDP message

A cat is fine too. Desudesudesu~

80

Port

Method

10

Threads

☒ Wait for reply

<= faster

Speed

slower =>

Attack status

Idle

Connecting

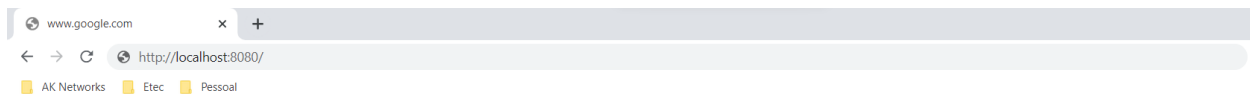
Requesting

Downloading

Downloaded

Requested

Failed



## No internet

No internet

Try:

- Checking the network cables, modem, and router
- Reconnecting to Wi-Fi
- [Running Windows Network Diagnostics](#)

DNS\_PROBE\_FINISHED\_NO\_INTERNET

snort -i 1 -c c:\Snort\etc\snort.conf -T

```

Select Administrator: Command Prompt
DCE/RPC 2 Preprocessor Configuration
Global Configuration
DCE/RPC Defragmentation: Enabled
Memcap: 102400 KB
Events: co
SMB Fingerprint policy: Disabled
Server Default Configuration
Policy: WinXP
Detect ports (PAF)
SMB: 139 445
TCP: 135
UDP: 135
RPC over HTTP server: 593
RPC over HTTP proxy: None
Autodetect ports (PAF)
SMB: None
TCP: 1025-65535
UDP: 1025-65535
RPC over HTTP server: 1025-65535
RPC over HTTP proxy: None
Invalid SMB shares: C$ D$ ADMIN$
Maximum SMB command chaining: 3 commands
SMB file inspection: Disabled
DNS config:
DNS Client rdata txt Overflow Alert: ACTIVE
Obsolete DNS RR Types Alert: INACTIVE
Experimental DNS RR Types Alert: INACTIVE
Ports: 53
SSLPP config:
Encrypted packets: not inspected
  
```

```
Server side data is trusted
Maximum SSL Heartbeat length: 0
Sensitive Data preprocessor config:
Global Alert Threshold: 25
Masked Output: DISABLED
SIP config:
Max number of sessions: 40000
Max number of dialogs in a session: 4 (Default)
Status: ENABLED
Ignore media channel: DISABLED
Max URI length: 512
Max Call ID length: 80
Max Request name length: 20 (Default)
Max From length: 256 (Default)
Max To length: 256 (Default)
Max Via length: 1024 (Default)
Max Contact length: 512
Max Content length: 2048
Ports:
5060 5061 5000
Methods:
invite cancel ack bye register options refer subscribe update join info message notify benotify do qauth sprack
publish service unsubscribe prack
```