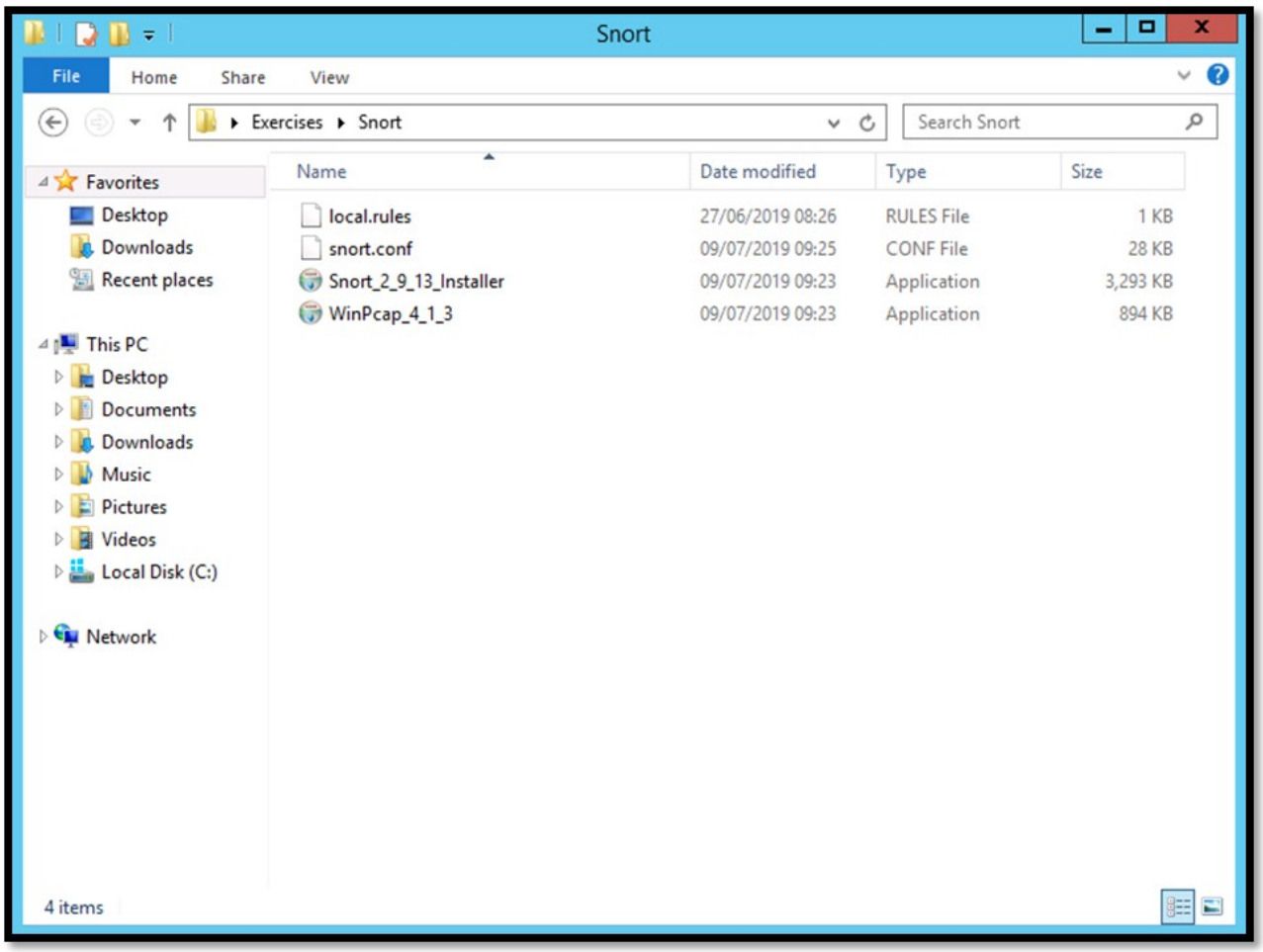
4.4 Guided Exercise: Implementing an IDS

Resources	
Files	None
Machines	Windows Server, Ubuntu Server

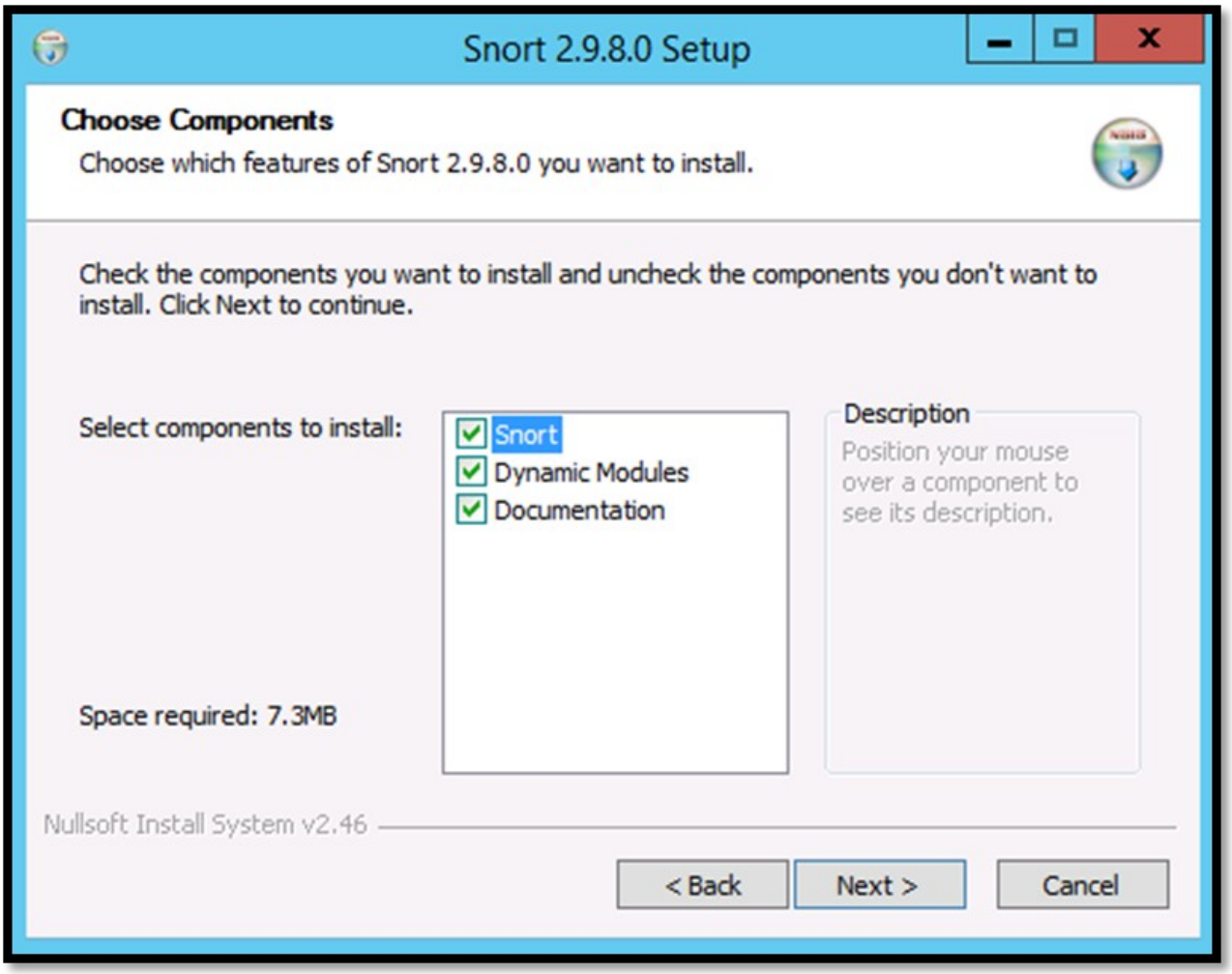
In this exercise you are required to install Snort on Windows Server and capture data for analysis.

Login to Windows Server and open the desktop folder Exercises -> Snort. Double click the Snort Installer file to install it.



Accept the License Agreement by clicking I Agree.

Click Next on the Choose Components window.

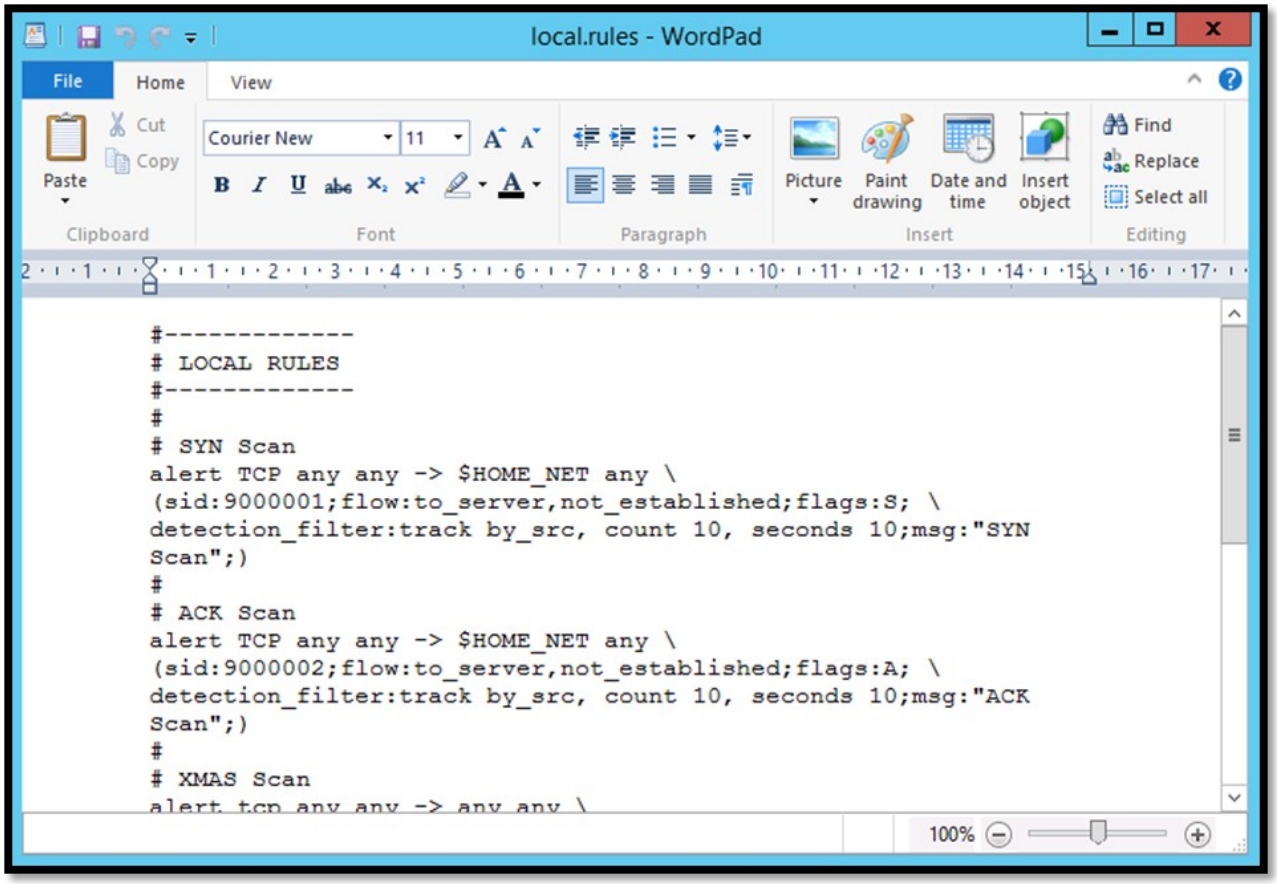


Click Next on the Choose Install Location.

Click Close once the installation finishes and then OK on the Snort Setup.

Copy the file snort.conf from the Desktop folder Exercises -> Snort to C:\Snort\etc and overwrite the file that is already there. Copy the file local.rules from the Desktop folder Exercises -> Snort to C:\Snort\rules.

Open the file local.rules using WordPad. Under the LOCAL RULES section there are different rules having a header and a body. The first rule detects a SYN scan and the second rule detects an ACK scan.

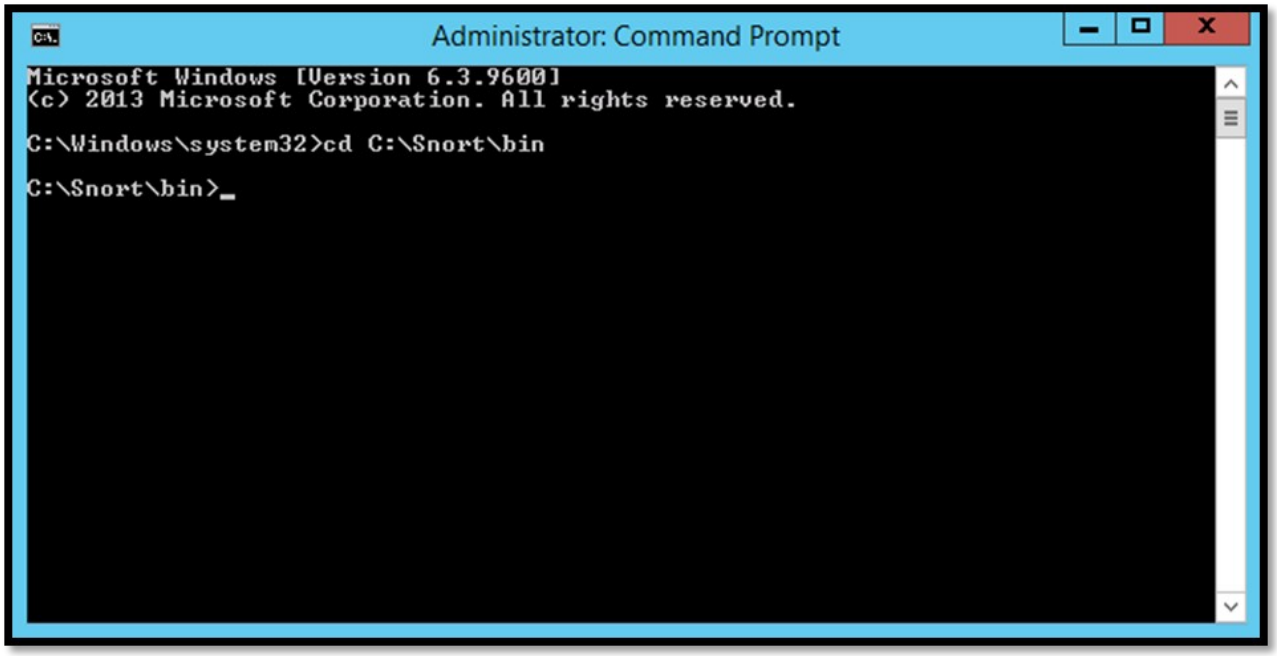


On the folder Exercises -> Snort double click the file WinPcap to install it. Click Next on the WinPcap Setup window and then click I Agree. Click Install on the next window and leave the check mark on Automatically start the WinPcap driver at boot time.

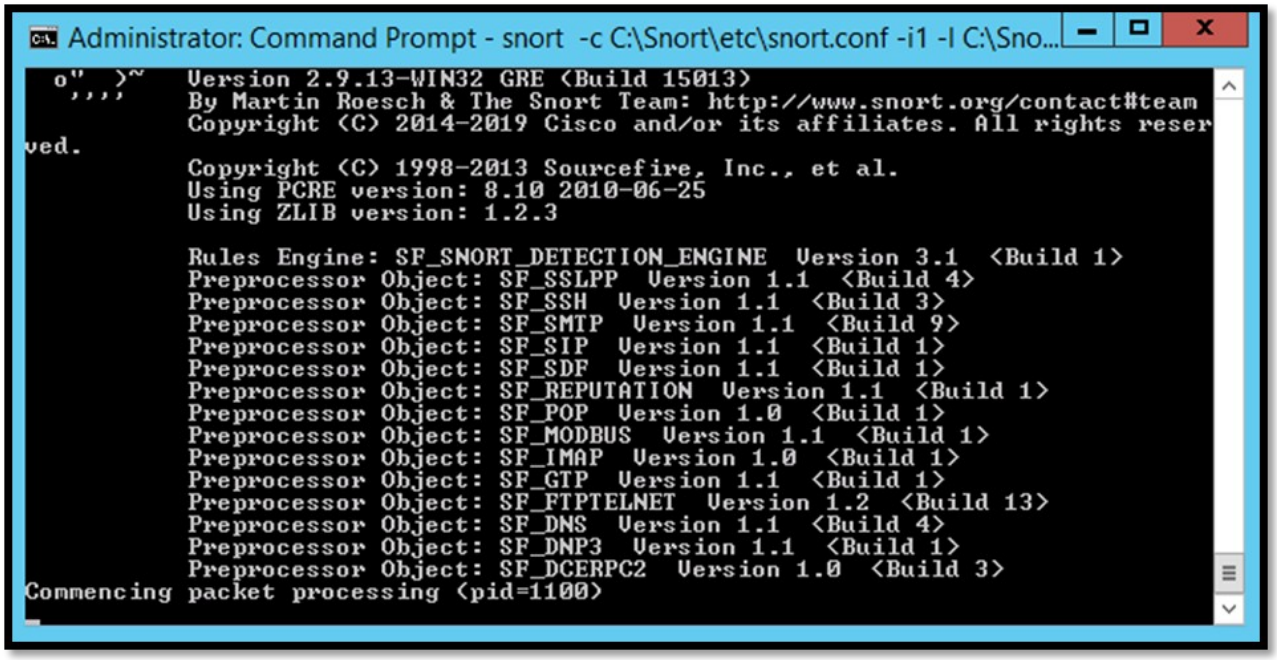
Once the installation finishes click on Finish.

Open a command prompt by right clicking the Start button and select Command Prompt (Admin).

Type cd C:\Snort\bin where bin is the default directory where the snort executable resides.



Type the following command “snort –c C:\Snort\etc\snort.conf –i1 –l C:\Snort\log –A console” and press enter. The option –c tells Snort to find the configuration file. The option –i1 tells Snort to capture on interface 1. The –l option tells Snort to log alerts and where to save them. The –A console option tells Snort to send alerts also to the console. This option is normally not used because it slows down detection and Snort may drop packets.



Login to Ubuntu Server and run the comannd nmap –A 192.168.1.20. Allow the scan to complete and then check the Snort command prompt on Windows Server.

```
user@ubuntu:~$ nmap -A 192.168.1.20

Starting Nmap 7.60 ( https://nmap.org ) at 2019-07-12 09:50 BST
```

Switch to the Windows Server and on the Snort command prompt you should see 5 SYN scan alerts and 5 ACK scan allerts. Press Control + C to stop Snort.

```
Administrator: Command Prompt - snort  -c C:\Snort\etc\snort.conf -i1 -l C:\Sno...
            Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
            Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
            Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
Commencing packet processing (pid=1100)
07/09-11:20:07.885081  [**] [1:9000001:0] SYN Scan [**] [Priority: 0] {TCP} 192.
168.1.30:58432 -> 192.168.1.20:80
07/09-11:20:07.885081  [**] [1:9000001:0] SYN Scan [**] [Priority: 0] {TCP} 192.
168.1.30:59492 -> 192.168.1.20:5900
07/09-11:20:07.885082  [**] [1:9000001:0] SYN Scan [**] [Priority: 0] {TCP} 192.
168.1.30:35746 -> 192.168.1.20:445
07/09-11:20:07.885082  [**] [1:9000001:0] SYN Scan [**] [Priority: 0] {TCP} 192.
168.1.30:45484 -> 192.168.1.20:587
07/09-11:20:07.885147  [**] [1:9000001:0] SYN Scan [**] [Priority: 0] {TCP} 192.
168.1.30:48140 -> 192.168.1.20:23
07/09-11:20:10.430549  [**] [1:9000002:0] ACK Scan [**] [Priority: 0] {TCP} 192.
168.1.30:48182 -> 192.168.1.20:49161
07/09-11:20:11.235890  [**] [1:9000002:0] ACK Scan [**] [Priority: 0] {TCP} 192.
168.1.30:50186 -> 192.168.1.20:49155
07/09-11:20:11.558003  [**] [1:9000002:0] ACK Scan [**] [Priority: 0] {TCP} 192.
168.1.30:48686 -> 192.168.1.20:49160
07/09-11:20:11.870010  [**] [1:9000002:0] ACK Scan [**] [Priority: 0] {TCP} 192.
168.1.30:56298 -> 192.168.1.20:49157
07/09-11:20:11.900065  [**] [1:9000002:0] ACK Scan [**] [Priority: 0] {TCP} 192.
168.1.30:56090 -> 192.168.1.20:49159
```

Once you stop Snort a list with different statistics will be revealed.

Administrator: Command Prompt

```
168.1.30:56090 -> 192.168.1.20:49159
*** Caught Int-Signal
===============================================================================
Run time for packet processing was 454.779000 seconds
Snort processed 4225 packets.
Snort ran for 0 days 0 hours 7 minutes 34 seconds
   Pkts/min:          603
   Pkts/sec:            9
===============================================================================
Packet I/O Totals:
   Received:         4225
   Analyzed:         4225 (100.000%)
    Dropped:            0 (  0.000%)
   Filtered:            0 (  0.000%)
Outstanding:            0 (  0.000%)
   Injected:            0
===============================================================================
Breakdown by protocol (includes rebuilt packets):
        Eth:         4234 (100.000%)
       VLAN:            0 (  0.000%)
        IP4:         3793 ( 89.584%)
       Frag:            0 (  0.000%)
       ICMP:           11 (  0.260%)
        UDP:           24 (  0.567%)
        TCP:         3758 ( 88.758%)
        IP6:           23 (  0.543%)
    IP6 Ext:           23 (  0.543%)
   IP6 Opts:            0 (  0.000%)
      Frag6:            0 (  0.000%)
      ICMP6:            1 (  0.024%)
       UDP6:           22 (  0.520%)
       TCP6:            0 (  0.000%)
     Teredo:            0 (  0.000%)
    ICMP-IP:            0 (  0.000%)
      EAPOL:            0 (  0.000%)
    IP4/IP4:            0 (  0.000%)
    IP4/IP6:            0 (  0.000%)
    IP6/IP4:            0 (  0.000%)
    IP6/IP6:            0 (  0.000%)
```