Sources:

pcap files:

Most pcap files were found from this list:
https://www.netresec.com/?page=PcapFile

Normal Traffic:

Source:
http://tcpreplay.appneta.com/wiki/captures.html

Filename:
smallFlows.pcap

Number of Packets: 14261

Attack 1, JBoss Exploits:

Source:
http://www.deependresearch.org/2016/04/jboss-exploits-view-from-victim.html

Filename:
jexboss_attack_v6_victim_vantage.pcap

Number of Packets: 131

Attack 2, Neutrino Exploit:

Source:
https://broadanalysis.com/2016/08/16/neutrino-exploit-kit-via-pseudodarkleech-hopto-org-gate-delivers-crypmic-ransomware-2/

Filename:
2016-08-16-Neutrino-EK.pcap

Number of Packets: 692

Attack 3, W32/Sdbot infected machine:

Source:
Russ McRee, W32/Sdbot infected machine
http://holisticinfosec.org/toolsmith/files/nov2k6/toolsmith.pcap

Filename:
toolsmith.pcap

Number of Packets: 392

Attack 4, Packet Injection:

Source:
Packet injection against www.02995.com, doing a redirect to www.hao123.com (read more)
https://www.netresec.com/files/hao123-com_packet-injection.pcap

Filename:
hao123-com_packet-injection.pcap

Number of Packets: 202

Attack 5, Malspam Pushing Emotet:

Source
http://malware-traffic-analysis.net/2017/11/29/index.html

Filename
2017-11-29-Emotet-malspam-2nd-run.pcap

Number of Packets: 552

Wireshark:

https://www.wireshark.org/

Weka:

https://www.cs.waikato.ac.nz/ml/weka/
https://www.youtube.com/watch?v=QtNYArb0Tkc
https://www.youtube.com/watch?v=m7kpIBGEdkI

Snort:

https://www.snort.org/
https://snort-org-site.s3.amazonaws.com/production/document_files/files/000/000/214/original/snort_manual.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAIXACIED2SPMSC7GA%2F20191017%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20191017T03

1315Z&X-Amz-Expires=172800&X-Amz-SignedHeaders=host&X-Amz-Signature=99ce3d98e188050e2be3799c525aaf4d8d704f3e887eb11828530e466dfeaab6

Python:

https://www.python.org/

Online IP tools:

https://www.ipaddressguide.com/cidr
http://www.aboutmyip.com/AboutMyXApp/IP2Integer.jsp