Sockets are software that act as an endpoint so that programs can communicate over a network. To work with sockets, Python offers the socket library. This library allows the programmer to create socket objects by binding the IP address and port number of a listening network. This creates a communication channel through which the program can send/receive data from the server over a TCP or UDP connection. Python also offers the telnetlib library to remotely log into devices using the Telnet protocol. This allows the user to remotely log in and manage devices like routers and create powerful scripts to automatic device configuration. The only downside is that Telnet isn’t encrypted.

To provide more secure SSH connections, python has the Paramiko library. Paramiko is great at creating more secure remote connections using SSHv2 protocol. What’s also nice about this library is that it provides both client and server functionality as well as SSH file transfer protocol to allow for secure file transfers. This allows the python application to perform a myriad of functions including running commands, upload and downloading files, and automated device configuration.

Next, we have Pyshark which is a library the gives python applications the ability to capture and analyze network packets similar to how Wireshark functions. Pyshark can be used to capture live network traffic and use that data for filtering, analysis, and summarizing the data into relevant information. You can also build intrusion detection and analytics into a pyshark program as well as read existing network recording files like .pcap files.

The final topic of discussion is security scripting, the practice of writing python scripts to perform and automate system security tasks. Password auditing checks to see if user passwords meet complexity and reuse requirements. Password auditing can be achieved through a library like “re”. Log scanning inspects log files and analyzes them to detect areas of interest or threats. Anomaly detection seeks to flag suspicious activity such at network activity, user behavior, or unauthorized changes to the system.