|  |
| --- |
| How do I install VirtualBox and the Extension Pack? |
| How do I install Vagrant? |
| How do I get the Splunk Enterprise RPM installer? |
| How do I get the vagrant-splunk Vagrantfile? |
| How do I start the Splunk Vagrant box? |
| How do I download and unzip the baseball data from https://www86.zippyshare.com/d/KtyWyCpR/32548/BaseballStats.zip? |
| How do I use Splunk to import the baseball data? |
| What is the passive voice? |
| How do I use Splunk to determine the total number of games played? |
| How do I use Splunk to determine the total number of unique teams? |
| How do I use Splunk to determine the total number of runs scored by all teams? |
| How do I use Splunk to create a sorted list of team names and the total number of runs they scored, descending from most runs to least runs? |
| How do I use Splunk to determine which team won the most games? |
| How do I use Splunk to determine which team lost the most games? |
| How do I use Splunk to determine the name of the pitcher that won the most games? |
| How do I use Splunk to determine the name of the team of the pitcher that won the most games? |
| How do I use Splunk to determine the arithmetic mean number of runs scored per game? |
| Submit report summarizing the baseball data. |
| What is the history that led to the creation of the Kill Chain? (KC Sections 1 & 2) |
| How do I use Vagrant to create a CentOS machine? |
| How do I create a new user named "student" on my CentOS VM? |
| How do I add the new user to the wheel group? |
| How do I update my CentOS VM? |
| How do I configure the CentOS machine to always boot into the XFCE GUI environment? |
| How do I take a snapshot of my CentOS VM? |
| How do I install Wireshark on the CentOS machine? |
| How do I install Bro (Zeek) on the CentOS machine? |
| What are indicators & what is the indicator life cycle? (KC Section 3 and 3.1) |
| What is the intrusion Kill Chain? (KC Section 3.2) |
| What is a course of action matrix? (KC - Section 3.3) |
| What is late phase detection & early phase detection? (KC Section 3.4) |
| How do I use the Kill Chain to conduct Campaign Analysis & what are TTPs? (KC Section 3.5) |
| How do I install Snort on the CentOS machine? |
| How do I configure Snort to use the Community and Emerging Threats rules? |
| Case Study 1 (KC Section 4 & 4.1) |
| Case Study 2 (KC Section 4.2) |
| Case Study 3 (KC Section 4.3) |
| How do I connect to Splunk from the CentOS machine? |
| How do I create a Slackware VM with Vagrant? |
| How do I create a user "student" and add the user to the "wheel" group on my Slackware VM? |
| How do I update my Slackware VM? |
| How do I change the hostname of the CentOS VM to "red" and the hostname of the Slackware VM to "blue"? |
| How do I edit the bash prompt to display the username, hostname, and working directory, as well as changing the text color to match the hostname for both Red and Blue VMs? |
| How do I connect both Red and Blue to an internal network named "netdef"? |
| How do I use Nmap on Red to scan Blue? |
| How do I use Netcat to listen for connections on port 80 on Blue? |
| What does an Nmap scan on Blue look like after opening port 80 on Blue? |
| How do I use Netcat on Red to connect to port 80 on Blue? |
| How can I use Tcpdump on Red to capture network traffic while I connect to Netcat listening on port 80 on Blue? |
| How do I write an Iptables firewall rule to block incoming traffic on TCP port 80 on Blue? |
| How do I open the PCAP file in Wireshark? |
| How do I view the Capture File Properties in Wireshark? |
| How do I view the Protocol Hierarchy for the PCAP file in Wireshark? |
| How do I view the Endpoints in Wireshark? |
| How do I view the Conversations in Wireshark? |
| How do I apply a Wireshark display filter to only show me HTTP traffic? |
| How do I apply a Wireshark display filter to only show me traffic involving a given IP address? |
| How do I follow a TCP Stream in Wireshark? |
| How do I use Bro to read a PCAP file? |
| How do I use Snort to read a PCAP file? |
| How do I use Bro to generate JSON metadata? |
| How do I load the Bro metadata into Splunk and show statistics? |
| How do I use tcpdump to configure a ring buffer? |
| How do I compile and install Bro on the Gateway machine? |
| How do I compile and install Snort on the Gateway machine? |