Zeek

Wednesday, September 14, 2022 2:27 PM

Task5 :

Investigate the **notice.log.** What is the number of unique events?	cat notice.log | zeek-cut uid| sort -r| uniq|nl
What is the number of ftp-brute signature matches?	cat notice.log | zeek-cut uid| sort -r| uniq|nl

Task6:

Investigate the bigFlows.pcap file. Investigate the dhcp.log file. What is the number of identified unique hostnames?	cat dhcp.log | zeek-cut host_name| sort -r| uniq|nl
Investigate the dns.log file. What is the number of unique queries?	cat dns.log | zeek-cut query| sort -r| uniq|nl|grep -v -e '*' -e '-'| wc

Task 7:

Go to folder TASK-7/101.
Investigate the sample.pcap file with 103.zeek script. Investigate the terminal output. What is the number of the detected new connections?

ans	zeek -C -r sample.pcap 103.zeek | grep -e "New Connection Found!" | wc

Go to folder TASK-7/201.
Investigate the ftp.pcap file with ftp-admin.sig signature and 201.zeek script. Investigate the signatures.log file. What is the number of signature hits?

ans	zeek -C -r ftp.pcap -s ftp-admin.sig 201.zeek | wc

Investigate the signatures.log file. What is the total number of "administrator" username detections?

ans	cat signatures.log | grep -e "administrator" |wc

Investigate the ftp.pcap file with all local scripts, and investigate the loaded_scripts.log file. What is the total number of loaded scripts?

ans	zeek -C -r ftp.pcap local	cat loaded_scripts.log | grep -v "#" | wc

Go to folder TASK-7/202.
Investigate the ftp-brute.pcap file with "/opt/zeek/share/zeek/policy/protocols/ftp/detect-bruteforcing.zeek" script. Investigate the notice.log file. What is the total number of brute-force detections?

ans	2

Task 8:

Investigate the case1.pcap file with intelligence-demo.zeek script. Investigate the intel.log file. Look at the second finding, where was the intel info found?

ans	zeek -C -r case1.pcap intelligence-demo.zeek

zeek -C -r case1.pcap hash-demo.zeek

ans	zeek -C -r case1.pcap file-extract-demo.zeek	cat extract-1561667874.743959-HTTP-Fpgan59p6uvNzLFja

Task 9:

Investigate the http.pcap file with the zeek-sniffpass module. Investigate the notice.log file. Which username has more module hits?

ans	zeek -Cr http.pcap zeek-sniffpass

Investigate the case2.pcap file with geoip-conn module. Investigate the conn.log file. What is the name of the identified City?

ans	zeek -Cr case2.pcap geoip-conn