Collegiate Cyber Defense Competitions

Inject Name	External Perimeter Assessment
Inject ID	EVAL04T

Description	Evaluate the perimeter of the network at the external interface of the firewall(s) in order to capture all the network services that are exposed. Use the following methodology: 1. Use Masscan for high speed initial discovery. Example command: *masscan 192.168.1.0/24 -p0-65535 —rate=500 —wait=10* *rate: limits packet rate to reduce false positives.* *wait: delay to finalize results.* 2. Use Nmap for detailed TCP followup on the hosts discovered by Masscan. Example command: *map -sS -sV -T4 -Pn -p <open ports> <target IPs>* *-sS: for SYN scan (TCP)* *-sV: for version detection* *-t4: avoid overwhelming network* *3.* Use Nmap for limited UDP scan of common ports. Example command: *map -sU -T4 —top-ports 10 <target IPs>*
Deliverables	Respond with a business memo which documents the 3 step process with screen shots showing the tools' command lines and initial outputs. Prepare a table in the memo that lists each alive host and the services found on that host. For each service found, identify whether the service is needed to be exposed to the external network, or are further refinement of the FW rules needed.