

## **PCAP Analysis Notes**

### **1. Tcpdump Basics**

- Read pcap: tcpdump -nn -r file.pcap
- Filter by host: tcpdump -nn -r file.pcap host 10.251.96.4
- Filter by port: tcpdump -nn -r file.pcap port 80

### **2. User-Agent Extraction**

- tcpdump -A -r file.pcap | grep "User-Agent"
- Identify scanners: gobuster, sqlmap, etc.

### **3. Text Processing**

- Extract IP/port fields:
- awk '{print \$5}' | cut -d ":" -f5 | sort -n | uniq -c
- Combine cut, grep, sort to summarize traffic.

### **4. TCP SYN Scan Detection**

- SYN packets only (half-open scan): Flags [S]
- Tcpdump filter:  
○ tcpdump 'tcp[tcpflags] & tcp-syn != 0 and tcp[tcpflags] & (tcp-ack|tcp-fin|tcp-rst) == 0'
- Check destination ports to see scanned targets.

### **5. Web Shell Awareness**

- Look for suspicious commands in HTTP requests (python -c, cmd=, etc.)
- Indicates reverse shell attempts or remote code execution.