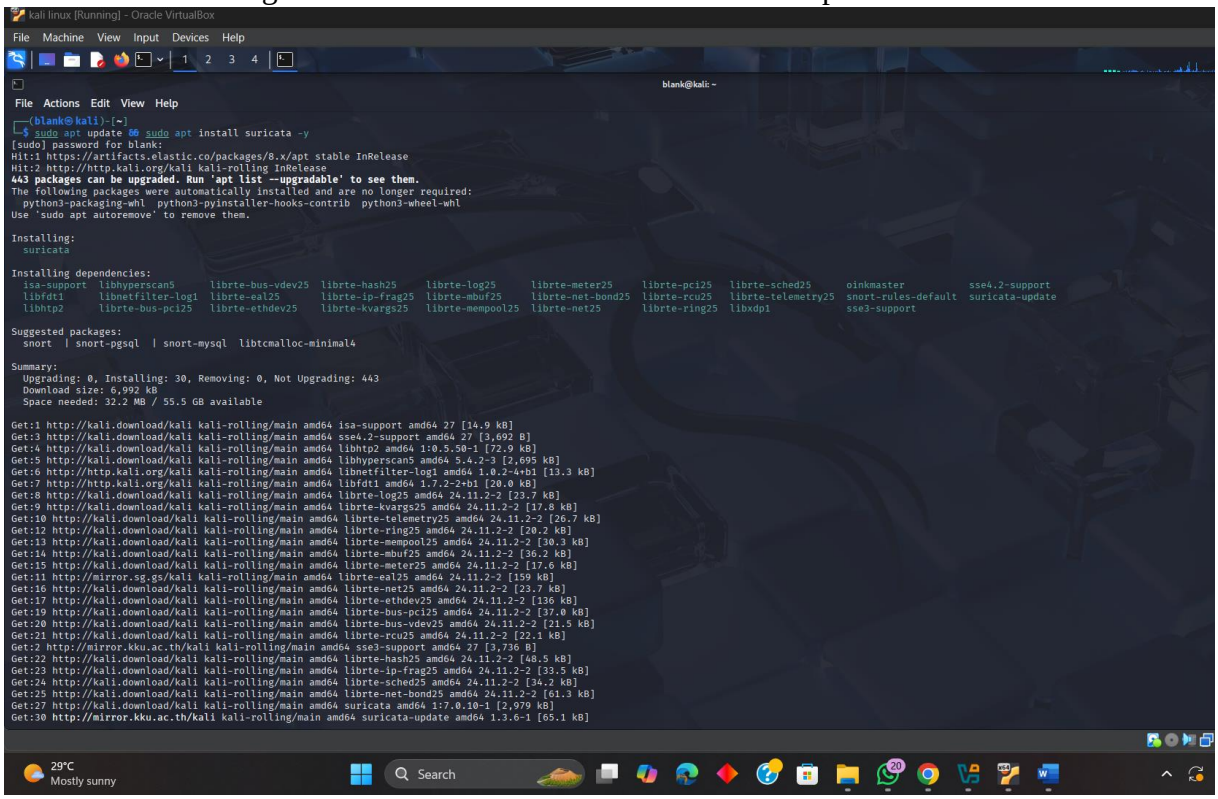
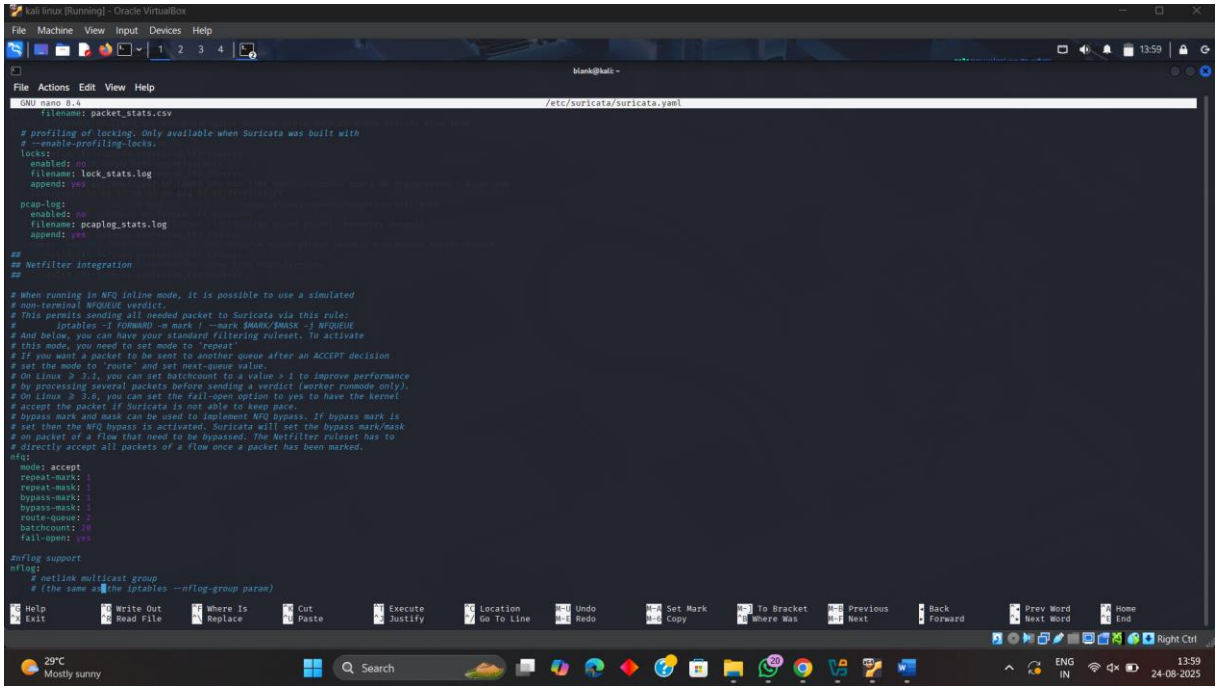
5. Network Defense with Open-Source Tools

Activities:

- **Tools:** Suricata, Elastic SIEM, CrowdSec.
- **Task:** Configure Suricata to block malicious IPs and map alerts to MITRE ATT&CK.



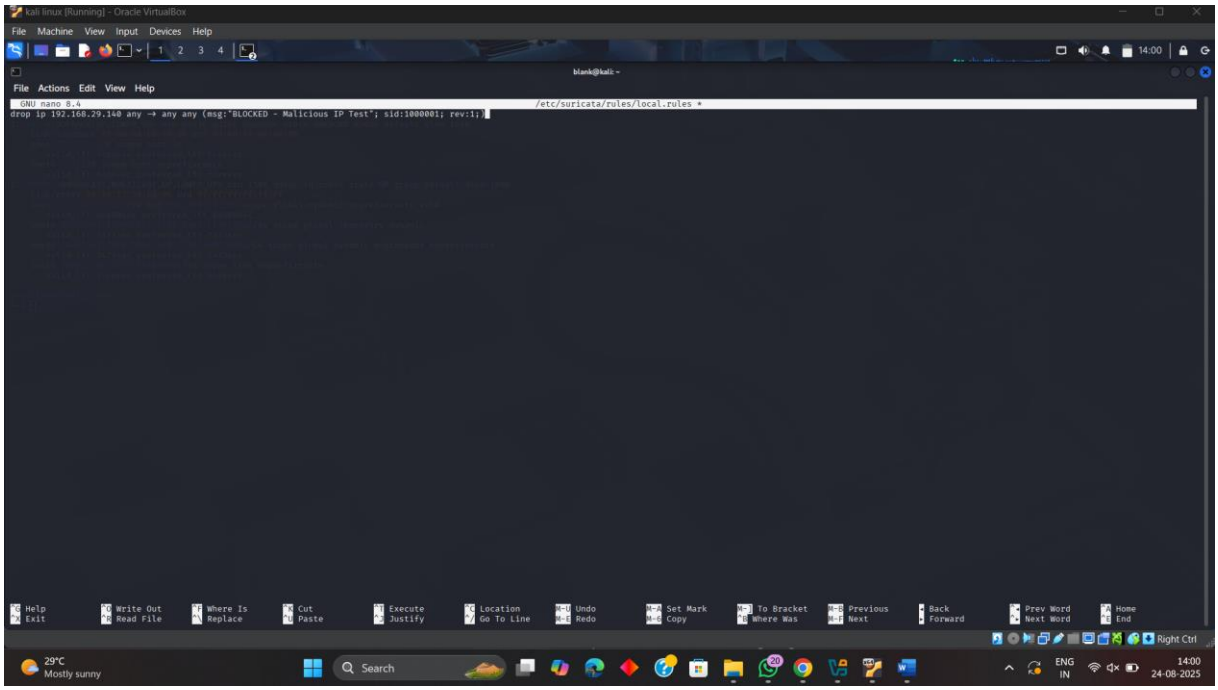


```
# Linux high speed capture support
af-packet:
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    threads: 1
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or per hash.
    # This is only supported for Linux kernel > 3.1
    # possible value are:
    #  * cluster_flow: all packets of a given flow are sent to the same socket
    #  * cluster_cpu: all packets treated in kernel by a CPU are sent to the same socket
    #  * cluster_qm: all packets linked by network card to a RSS queue are sent to the same
    #  socket. Requires at least Linux 3.14.
    #  * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hardware/ebpf-xdp.rst for
    #  more info.
    # Recommended modes are cluster_flow on most boxes and cluster_cpu or cluster_qm on system
    # with capture card using RSS (requires cpu affinity tuning and system IRQ tuning)
    # cluster_rollover has been deprecated; if used, it'll be replaced with cluster_flow.
    cluster-type: cluster_flow
    # In some fragmentation cases, the hash can not be computed. If "defrag" is set
    # to yes, the kernel will do the needed defragmentation before sending the packets.
    defrag: yes
    # To use the ring feature of AF_PACKET, set 'use-mmap' to yes
    #use-mmap: yes
    # Lock memory map to avoid it being swapped. Be careful that over
    # subscribing could lock your system
    #mmap-locked: yes
    # Use tpacket_v3 capture mode, only active if use-mmap is true
    # Don't use it in IPS or TAP mode as it causes severe latency
    #tpacket-v3: yes
    # Ring size will be computed with respect to "max-pending-packets" and number
    # of threads. You can set manually the ring size in number of packets by setting
    # the following value. If you are using flow "cluster-type" and have really network
    # intensive single-flow you may want to set the "ring-size" independently of the number
    # of threads:
    #ring-size: 2048
    # Block size is used by tpacket_v3 only. It should set to a value high enough to contain
    # a decent number of packets. Size is in bytes so please consider your MTU. It should be
    # a power of 2 and it must be multiple of page size (usually 4096).
    #block-size: 32768
```

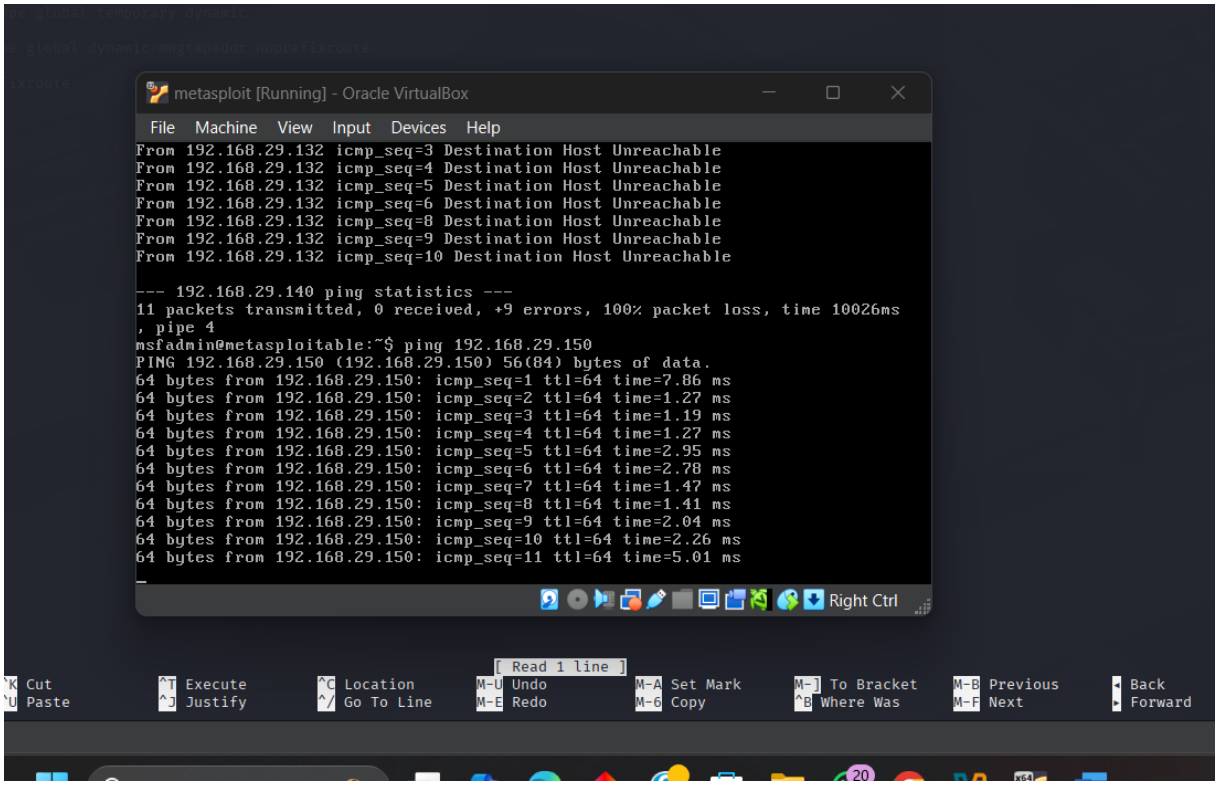
Enhanced Tasks:

- **Suricata Rule:** Create a rule to block a malicious IP:

drop ip 192.168.1.100 any -> any any (msg:"Block Malicious IP"; sid:1000001;)



- Test by pinging from another VM.



- **ATT&CK Mapping:** Map a Suricata alert to a MITRE ATT&CK technique:

Alert	Tactic	Technique	Notes
Suspicious HTTP	Command and Control	T1071	Outbound traffic to C2

MITRE ATTsCK Mapping Summary

Alert Name	Tactic	Technique ID	Technique Name	Notes
Suspicious HTTP	Command and control	T1071	Application Layer Protocol	Outbound traffic to C2