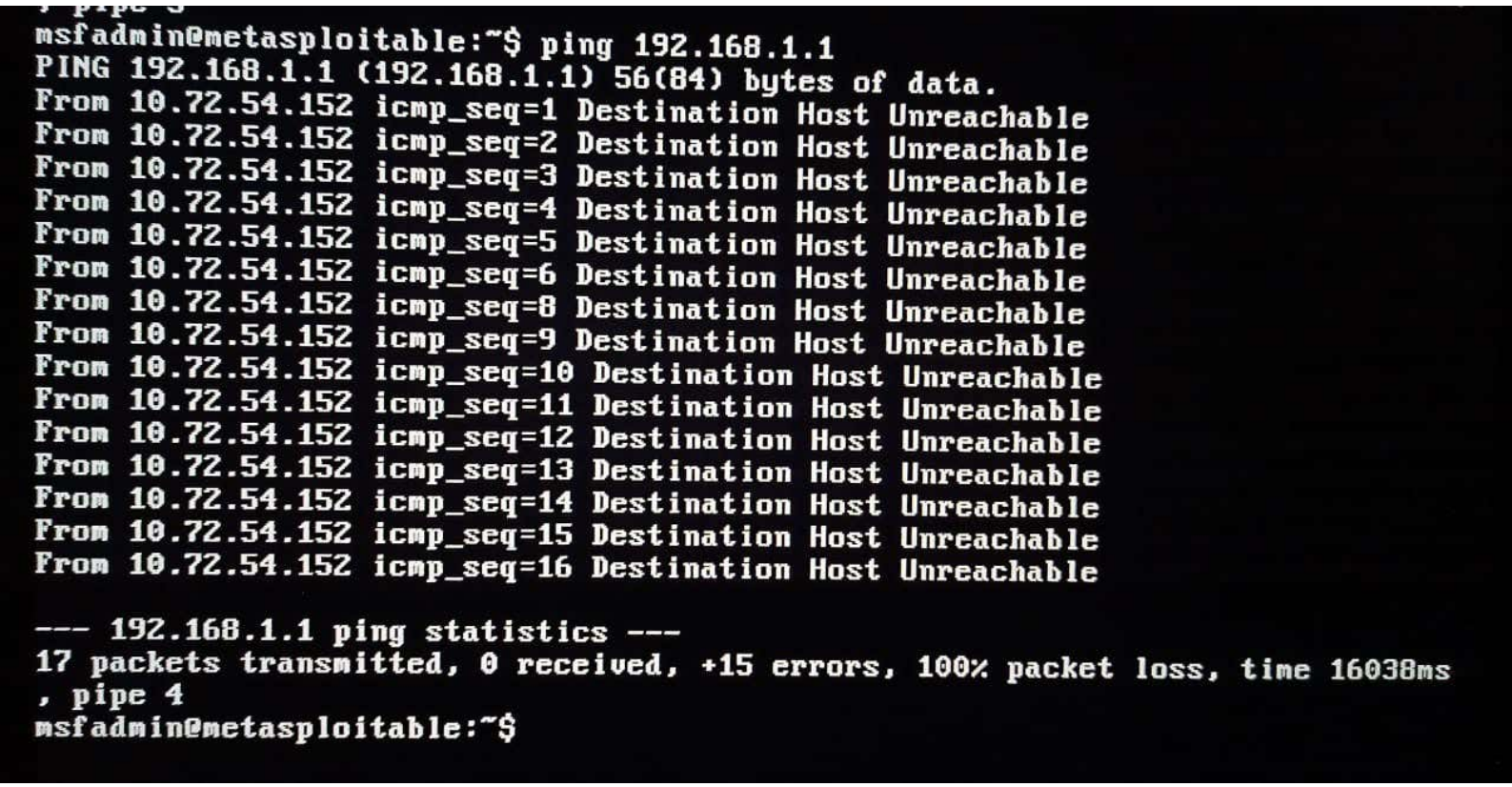
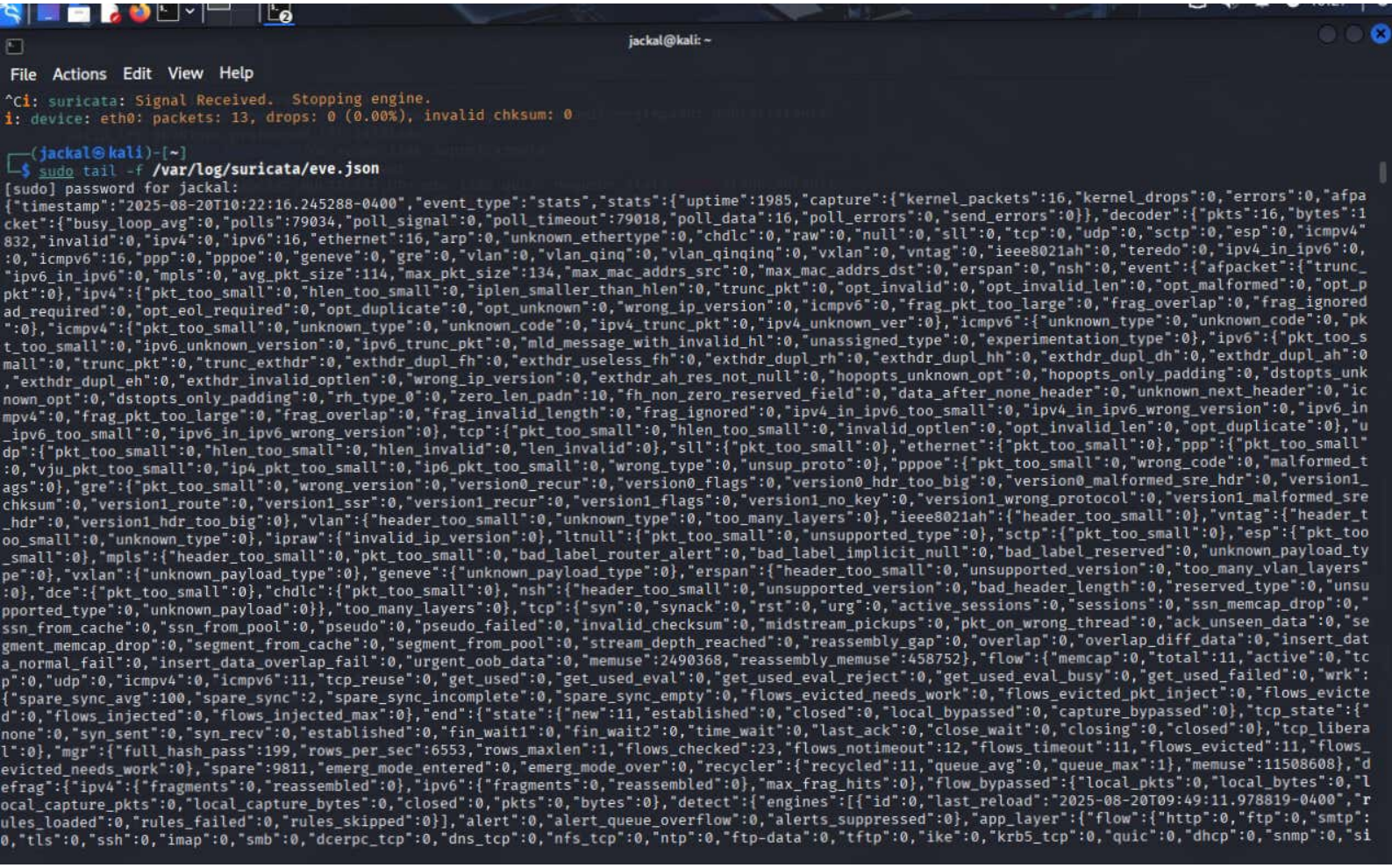
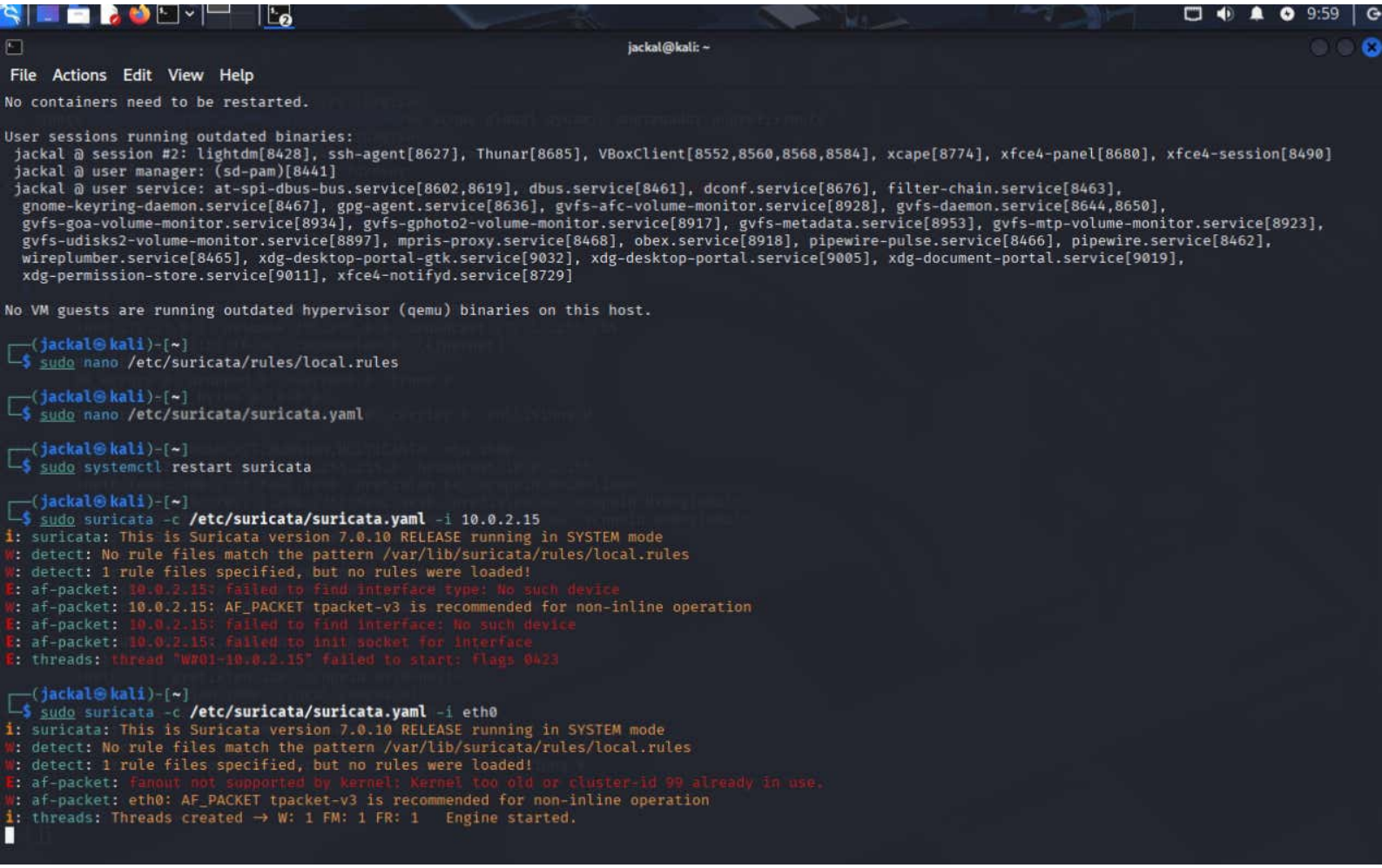
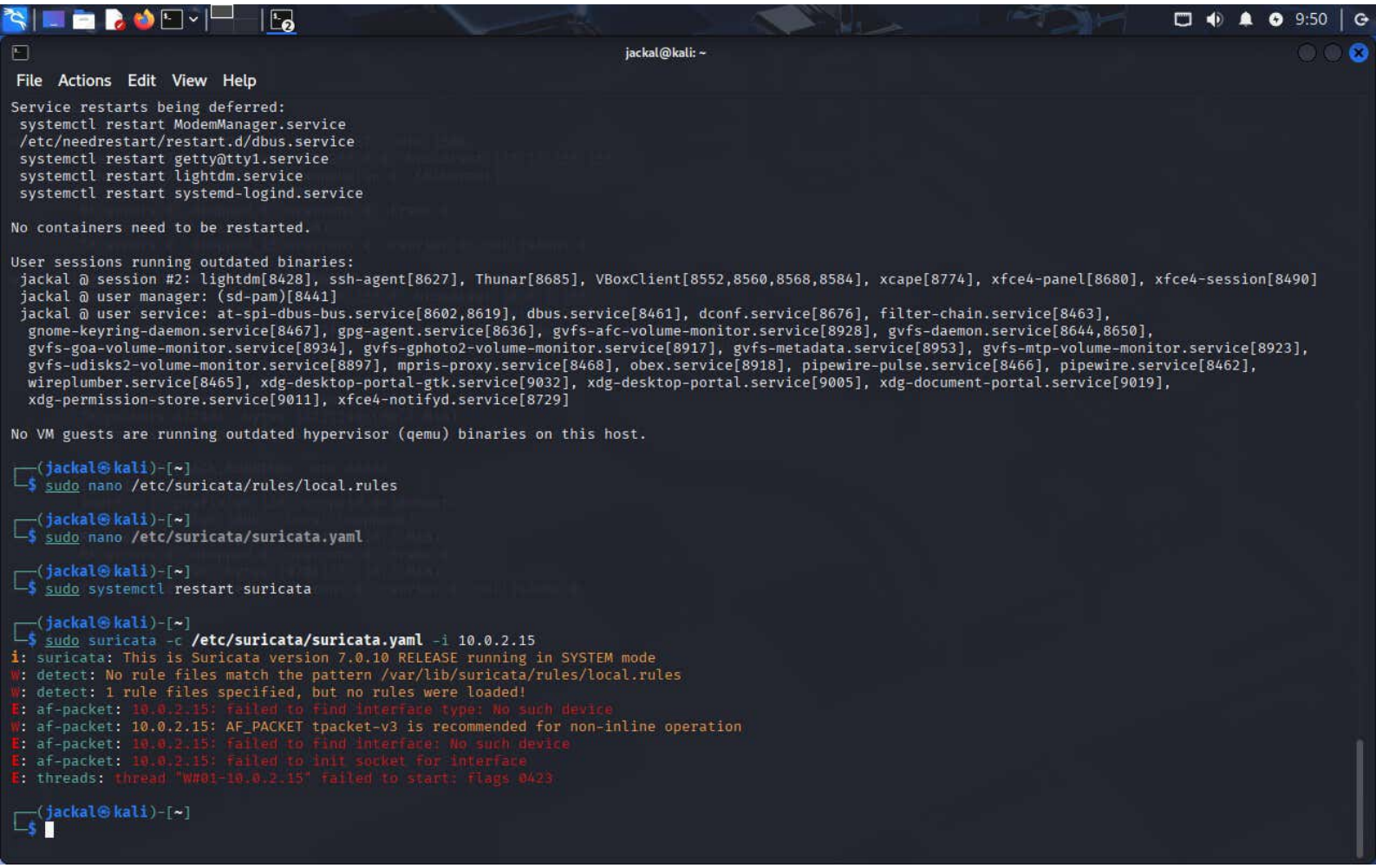

msfadmin@metasploitable:~$ ping 192.168.1.1
PING 192.168.1.1 (192.168.1.1) 56(84) bytes of data.
From 10.72.54.152 icmp_seq=1 Destination Host Unreachable
From 10.72.54.152 icmp_seq=2 Destination Host Unreachable
From 10.72.54.152 icmp_seq=3 Destination Host Unreachable
From 10.72.54.152 icmp_seq=4 Destination Host Unreachable
From 10.72.54.152 icmp_seq=5 Destination Host Unreachable
From 10.72.54.152 icmp_seq=6 Destination Host Unreachable
From 10.72.54.152 icmp_seq=8 Destination Host Unreachable
From 10.72.54.152 icmp_seq=9 Destination Host Unreachable
From 10.72.54.152 icmp_seq=10 Destination Host Unreachable
From 10.72.54.152 icmp_seq=11 Destination Host Unreachable
From 10.72.54.152 icmp_seq=12 Destination Host Unreachable
From 10.72.54.152 icmp_seq=13 Destination Host Unreachable
From 10.72.54.152 icmp_seq=14 Destination Host Unreachable
From 10.72.54.152 icmp_seq=15 Destination Host Unreachable
From 10.72.54.152 icmp_seq=16 Destination Host Unreachable
--- 192.168.1.1 ping statistics ---
17 packets transmitted, 0 received, +15 errors, 100% packet loss, time 16038ms
, pipe 4
msfadmin@metasploitable:~$


jackal@kali: ~
File Actions Edit View Help
^Ci: suricata: Signal Received. Stopping engine.
i: device: eth0: packets: 13, drops: 0 (0.00%), invalid chksum: 0
(jackal㉿kali)-[~]
$ sudo tail -f /var/log/suricata/eve.json
[sudo] password for jackal:
{"timestamp":"2025-08-20T10:22:16.245288-0400","event_type":"stats","stats":{"uptime":1985,"capture":{"kernel_packets":16,"kernel_drops":0,"errors":0,"afpacket":{"busy_loop_avg":0,"polls":79034,"poll_signal":0,"poll_timeout":79018,"poll_data":16,"poll_errors":0,"send_errors":0}},"decoder":{"pkts":16,"bytes":1832,"invalid":0,"ipv4":0,"ipv6":16,"ethernet":16,"arp":0,"unknown_ethertype":0,"chdlc":0,"raw":0,"null":0,"sll":0,"tcp":0,"udp":0,"sctp":0,"esp":0,"icmpv4":0,"icmpv6":16,"ppp":0,"pppoe":0,"geneve":0,"gre":0,"vlan":0,"vlan_qinq":0,"vlan_qinqinq":0,"vxlan":0,"vntag":0,"ieee8021ah":0,"teredo":0,"ipv4_in_ipv6":0,"ipv6_in_ipv6":0,"mpls":0,"avg_pkt_size":114,"max_pkt_size":134,"max_mac_addrs_src":0,"max_mac_addrs_dst":0,"erspan":0,"nsh":0,"event":{"afpacket":{"trunc_pkt":0},"ipv4":{"pkt_too_small":0,"hlen_too_small":0,"iplen_smaller_than_hlen":0,"trunc_pkt":0,"opt_invalid":0,"opt_invalid_len":0,"opt_malformed":0,"opt_pad_required":0,"opt_eol_required":0,"opt_duplicate":0,"opt_unknown":0,"wrong_ip_version":0,"icmpv6":0,"frag_pkt_too_large":0,"frag_overlap":0,"frag_ignored":0},"icmpv4":{"pkt_too_small":0,"unknown_type":0,"unknown_code":0,"ipv4_trunc_pkt":0,"ipv4_unknown_ver":0},"icmpv6":{"unknown_type":0,"unknown_code":0,"pkt_too_small":0,"ipv6_unknown_version":0,"ipv6_trunc_pkt":0,"mld_message_with_invalid_hl":0,"unassigned_type":0,"experimentation_type":0},"ipv6":{"pkt_too_small":0,"trunc_pkt":0,"trunc_exthdr":0,"exthdr_dupl_fh":0,"exthdr_useless_fh":0,"exthdr_dupl_rh":0,"exthdr_dupl_hh":0,"exthdr_dupl_dh":0,"exthdr_dupl_ah":0,"exthdr_dupl_eh":0,"exthdr_invalid_optlen":0,"wrong_ip_version":0,"exthdr_ah_res_not_null":0,"hopopts_unknown_opt":0,"hopopts_only_padding":0,"dstopts_unknown_opt":0,"dstopts_only_padding":0,"rh_type_0":0,"zero_len_padn":10,"fh_non_zero_reserved_field":0,"data_after_none_header":0,"unknown_next_header":0,"icmpv4":0,"frag_pkt_too_large":0,"frag_overlap":0,"frag_invalid_length":0,"frag_ignored":0,"ipv4_in_ipv6_too_small":0,"ipv4_in_ipv6_wrong_version":0,"ipv6_in_ipv6_too_small":0,"ipv6_in_ipv6_wrong_version":0},"tcp":{"pkt_too_small":0,"hlen_too_small":0,"invalid_optlen":0,"opt_invalid_len":0,"opt_duplicate":0},"udp":{"pkt_too_small":0,"hlen_too_small":0,"hlen_invalid":0,"len_invalid":0},"sll":{"pkt_too_small":0},"ethernet":{"pkt_too_small":0},"ppp":{"pkt_too_small":0,"vju_pkt_too_small":0,"ip4_pkt_too_small":0,"ip6_pkt_too_small":0,"wrong_type":0,"unsup_proto":0},"pppoe":{"pkt_too_small":0,"wrong_code":0,"malformed_tags":0},"gre":{"pkt_too_small":0,"wrong_version":0,"version0_recur":0,"version0_flags":0,"version0_hdr_too_big":0,"version0_malformed_sre_hdr":0,"version1_chksum":0,"version1_route":0,"version1_ssr":0,"version1_recur":0,"version1_flags":0,"version1_no_key":0,"version1_wrong_protocol":0,"version1_malformed_sre_hdr":0,"version1_hdr_too_big":0},"vlan":{"header_too_small":0,"unknown_type":0,"too_many_layers":0},"ieee8021ah":{"header_too_small":0},"vntag":{"header_too_small":0,"unknown_type":0},"ipraw":{"invalid_ip_version":0},"ltnull":{"pkt_too_small":0,"unsupported_type":0},"sctp":{"pkt_too_small":0},"esp":{"pkt_too_small":0},"mpls":{"header_too_small":0,"pkt_too_small":0,"bad_label_router_alert":0,"bad_label_implicit_null":0,"bad_label_reserved":0,"unknown_payload_type":0},"vxlan":{"unknown_payload_type":0},"geneve":{"unknown_payload_type":0},"erspan":{"header_too_small":0,"unsupported_version":0,"too_many_vlan_layers":0},"dce":{"pkt_too_small":0},"chdlc":{"pkt_too_small":0},"nsh":{"header_too_small":0,"unsupported_version":0,"bad_header_length":0,"reserved_type":0,"unsupported_type":0,"unknown_payload":0}},"too_many_layers":0},"tcp":{"syn":0,"synack":0,"rst":0,"urg":0,"active_sessions":0,"sessions":0,"ssn_memcap_drop":0,"ssn_from_cache":0,"ssn_from_pool":0,"pseudo":0,"pseudo_failed":0,"invalid_checksum":0,"midstream_pickups":0,"pkt_on_wrong_thread":0,"ack_unseen_data":0,"segment_memcap_drop":0,"segment_from_cache":0,"segment_from_pool":0,"stream_depth_reached":0,"reassembly_gap":0,"overlap":0,"overlap_diff_data":0,"insert_data_normal_fail":0,"insert_data_overlap_fail":0,"urgent_oob_data":0,"memuse":2490368,"reassembly_memuse":458752},"flow":{"memcap":0,"total":11,"active":0,"tcp":0,"udp":0,"icmpv4":0,"icmpv6":11,"tcp_reuse":0,"get_used":0,"get_used_eval":0,"get_used_eval_reject":0,"get_used_eval_busy":0,"get_used_failed":0,"wrk":{"spare_sync_avg":100,"spare_sync":2,"spare_sync_incomplete":0,"spare_sync_empty":0,"flows_evicted_needs_work":0,"flows_evicted_pkt_inject":0,"flows_evicted":0,"flows_injected":0,"flows_injected_max":0},"end":{"state":{"new":11,"established":0,"closed":0,"local_bypassed":0,"capture_bypassed":0},"tcp_state":{"none":0,"syn_sent":0,"syn_recv":0,"established":0,"fin_wait1":0,"fin_wait2":0,"time_wait":0,"last_ack":0,"close_wait":0,"closing":0,"closed":0},"tcp_liberal":0},"mgr":{"full_hash_pass":199,"rows_per_sec":6553,"rows_maxlen":1,"flows_checked":23,"flows_notimeout":12,"flows_timeout":11,"flows_evicted":11,"flows_evicted_needs_work":0},"spare":9811,"emerg_mode_entered":0,"emerg_mode_over":0,"recycler":{"recycled":11,"queue_avg":0,"queue_max":1},"memuse":11508608},"defrag":{"ipv4":{"fragments":0,"reassembled":0},"ipv6":{"fragments":0,"reassembled":0},"max_frag_hits":0},"flow_bypassed":{"local_pkts":0,"local_bytes":0,"local_capture_pkts":0,"local_capture_bytes":0,"closed":0,"pkts":0,"bytes":0},"detect":{"engines":[{"id":0,"last_reload":"2025-08-20T09:49:11.978819-0400","rules_loaded":0,"rules_failed":0,"rules_skipped":0}],"alert":0,"alert_queue_overflow":0,"alerts_suppressed":0},"app_layer":{"flow":{"http":0,"ftp":0,"smtp":0,"tls":0,"ssh":0,"imap":0,"smb":0,"dcerpc_tcp":0,"dns_tcp":0,"nfs_tcp":0,"ntp":0,"ftp-data":0,"tftp":0,"ike":0,"krb5_tcp":0,"quic":0,"dhcp":0,"snmp":0,"si


jackal@kali: ~
File Actions Edit View Help
No containers need to be restarted.
User sessions running outdated binaries:
jackal @ session #2: lightdm[8428], ssh-agent[8627], Thunar[8685], VBoxClient[8552,8560,8568,8584], xcape[8774], xfce4-panel[8680], xfce4-session[8490]
jackal @ user manager: (sd-pam)[8441]
jackal @ user service: at-spi-dbus-bus.service[8602,8619], dbus.service[8461], dconf.service[8676], filter-chain.service[8463], gnome-keyring-daemon.service[8467], gpg-agent.service[8636], gvfs-afc-volume-monitor.service[8928], gvfs-daemon.service[8644,8650], gvfs-goa-volume-monitor.service[8934], gvfs-gphoto2-volume-monitor.service[8917], gvfs-metadata.service[8953], gvfs-mtp-volume-monitor.service[8923], gvfs-udisks2-volume-monitor.service[8897], mpris-proxy.service[8468], obex.service[8918], pipewire-pulse.service[8466], pipewire.service[8462], wireplumber.service[8465], xdg-desktop-portal-gtk.service[9032], xdg-desktop-portal.service[9005], xdg-document-portal.service[9019], xdg-permission-store.service[9011], xfce4-notifyd.service[8729]
No VM guests are running outdated hypervisor (qemu) binaries on this host.
(jackal㉿kali)-[~]
$ sudo nano /etc/suricata/rules/local.rules
(jackal㉿kali)-[~]
$ sudo nano /etc/suricata/suricata.yaml
(jackal㉿kali)-[~]
$ sudo systemctl restart suricata
(jackal㉿kali)-[~]
$ sudo suricata -c /etc/suricata/suricata.yaml -i 10.0.2.15
i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
W: detect: No rule files match the pattern /var/lib/suricata/rules/local.rules
W: detect: 1 rule files specified, but no rules were loaded!
E: af-packet: 10.0.2.15: failed to find interface type: No such device
W: af-packet: 10.0.2.15: AF_PACKET tpacket-v3 is recommended for non-inline operation
E: af-packet: 10.0.2.15: failed to find interface: No such device
E: af-packet: 10.0.2.15: failed to init socket for interface
E: threads: thread "W#01-10.0.2.15" failed to start: flags 0423
(jackal㉿kali)-[~]
$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
W: detect: No rule files match the pattern /var/lib/suricata/rules/local.rules
W: detect: 1 rule files specified, but no rules were loaded!
E: af-packet: fanout not supported by kernel: Kernel too old or cluster-id 99 already in use.
W: af-packet: eth0: AF_PACKET tpacket-v3 is recommended for non-inline operation
i: threads: Threads created → W: 1 FM: 1 FR: 1 Engine started.


jackal@kali: ~
File Actions Edit View Help
Service restarts being deferred:
systemctl restart ModemManager.service
/etc/needrestart/restart.d/dbus.service
systemctl restart getty@tty1.service
systemctl restart lightdm.service
systemctl restart systemd-logind.service
No containers need to be restarted.
User sessions running outdated binaries:
jackal @ session #2: lightdm[8428], ssh-agent[8627], Thunar[8685], VBoxClient[8552,8560,8568,8584], xcape[8774], xfce4-panel[8680], xfce4-session[8490]
jackal @ user manager: (sd-pam)[8441]
jackal @ user service: at-spi-dbus-bus.service[8602,8619], dbus.service[8461], dconf.service[8676], filter-chain.service[8463],
gnome-keyring-daemon.service[8467], gpg-agent.service[8636], gvfs-afc-volume-monitor.service[8928], gvfs-daemon.service[8644,8650],
gvfs-goa-volume-monitor.service[8934], gvfs-gphoto2-volume-monitor.service[8917], gvfs-metadata.service[8953], gvfs-mtp-volume-monitor.service[8923],
gvfs-udisks2-volume-monitor.service[8897], mpris-proxy.service[8468], obex.service[8918], pipewire-pulse.service[8466], pipewire.service[8462],
wireplumber.service[8465], xdg-desktop-portal-gtk.service[9032], xdg-desktop-portal.service[9005], xdg-document-portal.service[9019],
xdg-permission-store.service[9011], xfce4-notifyd.service[8729]
No VM guests are running outdated hypervisor (qemu) binaries on this host.
(jackal㉿kali)-[~]
$ sudo nano /etc/suricata/rules/local.rules
(jackal㉿kali)-[~]
$ sudo nano /etc/suricata/suricata.yaml
(jackal㉿kali)-[~]
$ sudo systemctl restart suricata
(jackal㉿kali)-[~]
$ sudo suricata -c /etc/suricata/suricata.yaml -i 10.0.2.15
i: suricata: This is Suricata version 7.0.10 RELEASE running in SYSTEM mode
W: detect: No rule files match the pattern /var/lib/suricata/rules/local.rules
W: detect: 1 rule files specified, but no rules were loaded!
E: af-packet: 10.0.2.15: failed to find interface type: No such device
W: af-packet: 10.0.2.15: AF_PACKET tpacket-v3 is recommended for non-inline operation
E: af-packet: 10.0.2.15: failed to find interface: No such device
E: af-packet: 10.0.2.15: failed to init socket for interface
E: threads: thread "W#01-10.0.2.15" failed to start: flags 0423
(jackal㉿kali)-[~]
$