Intern Details; -

Name: Manahil Naeem

Intern I'd: CA/AG1/27171

Domain: Cyber Security

Internship Duration: 1st Aug to 30th Aug

Task 04

For developing a network intrusion detection system Suricata tool is used in Kali Linux. Step by step description along with screenshots is provided here.

First step is to install Suricata in Kali Linux using the following commands.

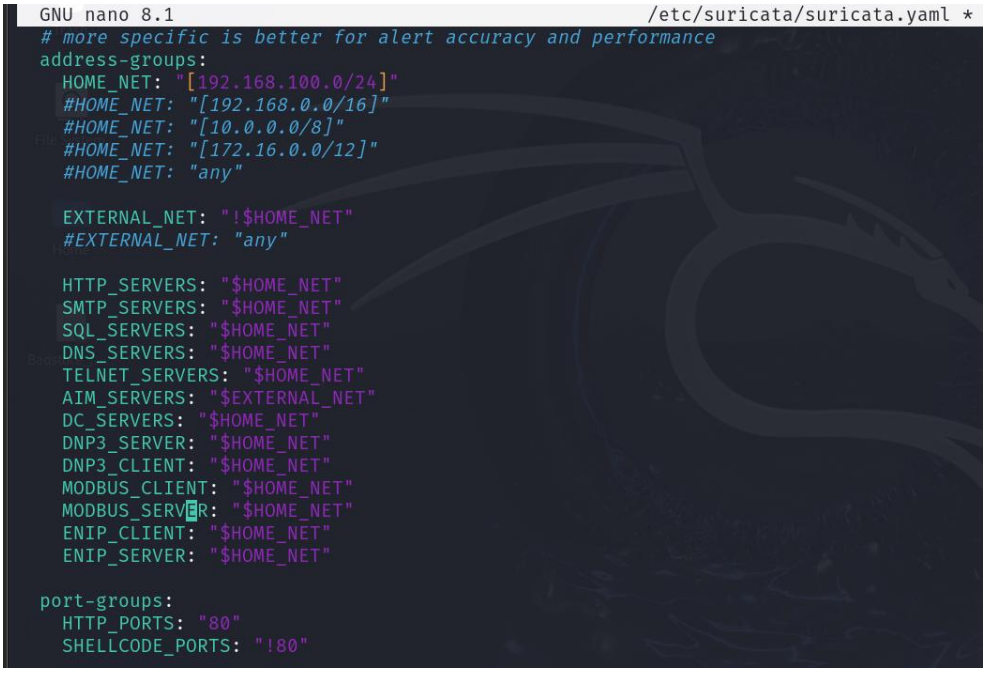
```
┌──(kali㉿kali)-[~]
└─$ sudo apt-get install suricata

Reading package lists ... Done
Building dependency tree ... Done
Reading state information ... Done
The following packages were automatically installed and are no longer required:
  libdaxctl1 libgeos3.12.1t64 libjxl0.7 libndctl6 libpmem1 librav1e0 libre2-10 libroc0.3 libsvtav1enc1d1 libu2f-udev libx265-199
  openjdk-21-jre openjdk-21-jre-headless python3-diskcache python3-mistune0 python3-pendulum python3-pytzdata samba-ad-provision
  samba-dsdb-modules
Use 'sudo apt autoremove' to remove them.
The following additional packages will be installed:
  isa-support libfdt1 libhtp2 libhyperscan5 libnetfilter-log1 librte-bus-pci24 librte-bus-vdev24 librte-eal24 librte-ethdev24
  librte-hash24 librte-ip-frag24 librte-kvargs24 librte-log24 librte-mbuf24 librte-mempool24 librte-meter24 librte-net-bond24
  librte-net24 librte-pci24 librte-rcu24 librte-ring24 librte-sched24 librte-telemetry24 libxdp1 sse3-support sse4.2-support
  suricata-update
Suggested packages:
  libtcmalloc-minimal4
The following NEW packages will be installed:
  isa-support libfdt1 libhtp2 libhyperscan5 libnetfilter-log1 librte-bus-pci24 librte-bus-vdev24 librte-eal24 librte-ethdev24
  librte-hash24 librte-ip-frag24 librte-kvargs24 librte-log24 librte-mbuf24 librte-mempool24 librte-meter24 librte-net-bond24
  librte-net24 librte-pci24 librte-rcu24 librte-ring24 librte-sched24 librte-telemetry24 libxdp1 sse3-support sse4.2-support
  suricata suricata-update
0 upgraded, 28 newly installed, 0 to remove and 272 not upgraded.
Need to get 6,475 kB of archives.
After this operation, 29.7 MB of additional disk space will be used.
Do you want to continue? [Y/n] y
Get:1 http://kali.download/kali kali-rolling/main amd64 isa-support amd64 24 [14.4 kB]
Get:2 http://kali.download/kali kali-rolling/main amd64 sse3-support amd64 24 [3,536 B]
Get:3 http://kali.download/kali kali-rolling/main amd64 sse4.2-support amd64 24 [3,496 B]
Get:4 http://kali.download/kali kali-rolling/main amd64 libhtp2 amd64 1:0.5.48-2 [71.9 kB]
```

Next we update the rule set with Suricata's update command as shown in the following screenshot.

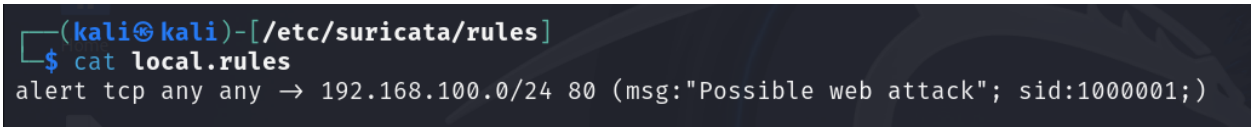
```
└─$ sudo suricata-update

27/8/2024 -- 13:58:16 - <Info> -- Using data-directory /var/lib/suricata.
27/8/2024 -- 13:58:16 - <Info> -- Using Suricata configuration /etc/suricata/suricata.yaml
27/8/2024 -- 13:58:16 - <Info> -- Using /etc/suricata/rules for Suricata provided rules.
27/8/2024 -- 13:58:16 - <Info> -- Found Suricata version 7.0.6 at /usr/bin/suricata.
27/8/2024 -- 13:58:16 - <Info> -- Loading /etc/suricata/suricata.yaml
27/8/2024 -- 13:58:16 - <Info> -- Disabling rules for protocol pgsql
27/8/2024 -- 13:58:16 - <Info> -- Disabling rules for protocol modbus
27/8/2024 -- 13:58:16 - <Info> -- Disabling rules for protocol dnp3
27/8/2024 -- 13:58:16 - <Info> -- Disabling rules for protocol enip
27/8/2024 -- 13:58:16 - <Info> -- No sources configured, will use Emerging Threats Open
27/8/2024 -- 13:58:16 - <Info> -- Fetching https://rules.emergingthreats.net/open/suricata-7.0.6/emerging.rules.tar.gz.
 100% - 4422997/4422997
27/8/2024 -- 13:58:22 - <Info> -- Done.
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/app-layer-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/decoder-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/dhcp-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/dnp3-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/dns-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/files.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/http2-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/http-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/ipsec-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/kerberos-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/modbus-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/mqtt-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/nfs-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/ntp-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/quic-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/rfb-events.rules
27/8/2024 -- 13:58:23 - <Info> -- Loading distribution rule file /etc/suricata/rules/smb-events.rules
```

Now Open the Suricata configuration file and set the HOME_NET variable in the YAML file to your network's IP range.

```
  GNU nano 8.1                                    /etc/suricata/suricata.yaml *
%YAML 1.1
---

# Suricata configuration file. In addition to the comments describing all
# options in this file, full documentation can be found at:
# https://docs.suricata.io/en/latest/configuration/suricata-yaml.html

# This configuration file generated by Suricata 7.0.6.
suricata-version: "7.0"

##
## Step 1: Inform Suricata about your network
##

vars:
  # more specific is better for alert accuracy and performance
  address-groups:
    HOME_NET: "[192.168.100.0/24]"
    #HOME_NET: "[192.168.0.0/16]"
    #HOME_NET: "[10.0.0.0/8]"
    #HOME_NET: "[172.16.0.0/12]"
    #HOME_NET: "any"

    EXTERNAL_NET: "!$HOME_NET"
    #EXTERNAL_NET: "any"

    HTTP_SERVERS: "$HOME_NET"
    SMTP_SERVERS: "$HOME_NET"
```



Open the local rules file and add a rule to detect a web attack.



Start Suricata with the specified configuration file and interface.

Checking the logs which are saved eve.json and fast.log files in the /var/log/suricata directory

```
┌──(kali㉿kali)-[~]
└─$ cd /var/log/suricata/

┌──(kali㉿kali)-[/var/log/suricata]
└─$ ls
eve.json  fast.log  stats.log  suricata.log
```

```
┌──(kali㉿kali)-[/var/log/suricata]
└─$ cat fast.log
08/27/2024-14:11:33.415753  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP} 192.168.44.132:68 → 192.168.44.254:67
08/27/2024-14:11:33.415802  [**] [1:2022973:1] ET INFO Possible Kali Linux hostname in DHCP Request Packet [**] [Classification: Potential Corporate Privacy Violation] [Priority: 1] {UDP} 192.168.44.132:68 → 192.168.44.254:67
```

```
┌──(kali㉿kali)-[/var/log/suricata]
└─$ cat eve.json
{"timestamp":"2024-08-27T14:06:33.209223-0400","event_type":"stats","stats":{"uptime":67,"capture":{"kernel_packets":0,"kernel_drops":0,"errors":0,"afpacket":{"busy_loop_avg":0,"polls":231,"poll_signal":0,"poll_timeout":231,"poll_data":0,"poll_errors":0,"send_errors":0}},"decoder":{"pkts":0,"bytes":0,"invalid":0,"ipv4":0,"ipv6":0,"ethernet":0,"arp":0,"unknown_ethertype":0,"chdlc":0,"raw":0,"null":0,"sll":0,"tcp":0,"udp":0,"sctp":0,"esp":0,"icmpv4":0,"icmpv6":0,"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":0,"max_pkt_size":0,"max_mac_addrs_src":0,"max_mac_addrs_dst":0,"erspan":0,"nsh":0,"event":{"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":0,"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,"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,
```

```
,"insert_data_overlap_fail":0,"memuse":2424832,"reassembly_memuse":458752},"flow":{"memcap":0,"total":15,"active":1,"tcp":0,"udp":13,"icmpv4":0,"icmpv6":2,"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":4,"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":14,"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":39,"rows_per_sec":6553,"rows_maxlen":1,"flows_checked":38,"flows_notimeout":24,"flows_timeout":14,"flows_evicted":14,"flows_evicted_needs_work":0},"spare":9614,"emerg_mode_entered":0,"emerg_mode_over":0,"recycler":{"recycled":14,"queue_avg":0,"queue_max":2},"memuse":7234304},"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":"2024-08-27T14:06:25.008406-0400","rules_loaded":39785,"rules_failed":0,"rules_skipped":0}],"alert":1,"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":1,"snmp":0,"sip":0,"rfb":0,"mqtt":0,"telnet":0,"rdp":0,"http2":0,"bittorrent-dht":0,"failed_tcp":0,"dcerpc_udp":0,"dns_udp":0,"nfs_udp":0,"krb5_udp":0,"failed_udp":12},"tx":{"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":2,"snmp":0,"sip":0,"rfb":0,"mqtt":0,"telnet":0,"rdp":0,"http2":0,"bittorrent-dht":0,"dcerpc_udp":0,"dns_udp":0,"nfs_udp":0,"krb5_udp":0},"error":{"http":{"gap":0,"alloc":0,"parser":0,"internal":0},"ftp":{"gap":0,"alloc":0,"parser":0,"internal":0},"smtp":{"gap":0,"alloc":0,"parser":0,"internal":0},"tls":{"gap":0,"alloc":0,"parser":0,"internal":0},"ssh":{"gap":0,"alloc":0,"parser":0,"internal":0},"imap":{"gap":0,"alloc":0,"parser":0,"internal":0},"smb":{"gap":0,"alloc":0,"parser":0,"internal":0},"dcerpc_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"dns_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"nfs_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"ntp":{"gap":0,"alloc":0,"parser":0,"internal":0},"ftp-data":{"gap":0,"alloc":0,"parser":0,"internal":0},"tftp":{"gap":0,"alloc":0,"parser":0,"internal":0},"ike":{"gap":0,"alloc":0,"parser":0,"internal":0},"krb5_tcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"quic":{"gap":0,"alloc":0,"parser":0,"internal":0},"dhcp":{"gap":0,"alloc":0,"parser":0,"internal":0},"snmp":{"gap":0,"alloc":0,"parser":0,"internal":0},"sip":{"gap":0,"alloc":0,"parser":0,"internal":0},"rfb":{"gap":0,"alloc":0,"parser":0,"internal":0},"mqtt":{"gap":0,"alloc":0,"parser":0,"internal":0},"telnet":{"gap":0,"alloc":0,"parser":0,"internal":0},"rdp":{"gap":0,"alloc":0,"parser":0,"internal":0},"http2":{"gap":0,"alloc":0,"parser":0,"internal":0},"bittorrent-dht":{"gap":0,"alloc":0,"parser":0,"internal":0},"failed_tcp":{"gap":0},"dcerpc_udp":{"alloc":0,"parser":0,"internal":0},"dns_udp":{"alloc":0,"parser":0,"internal":0},"nfs_udp":{"alloc":0,"parser":0,"internal":0},"krb5_udp":{"alloc":0,"parser":0,"internal":0}},"expectations":0},"memcap_pressure":5,"memcap_pressure_max":5,"http":{"memuse":0,"memcap":0},"ftp":{"memuse":0,"memcap":0},"file_store":{"open_files":0}}}
```