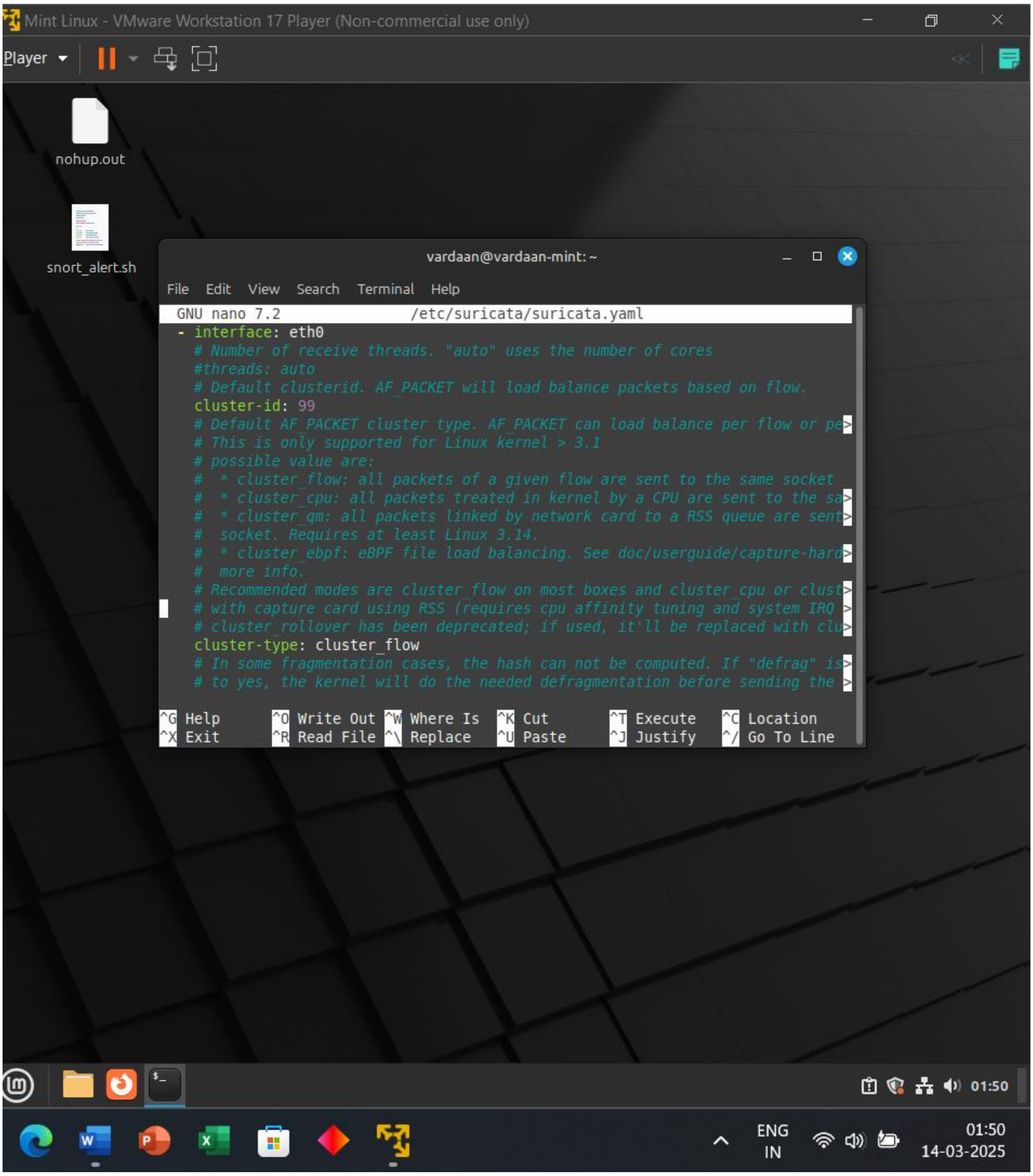
Suricata

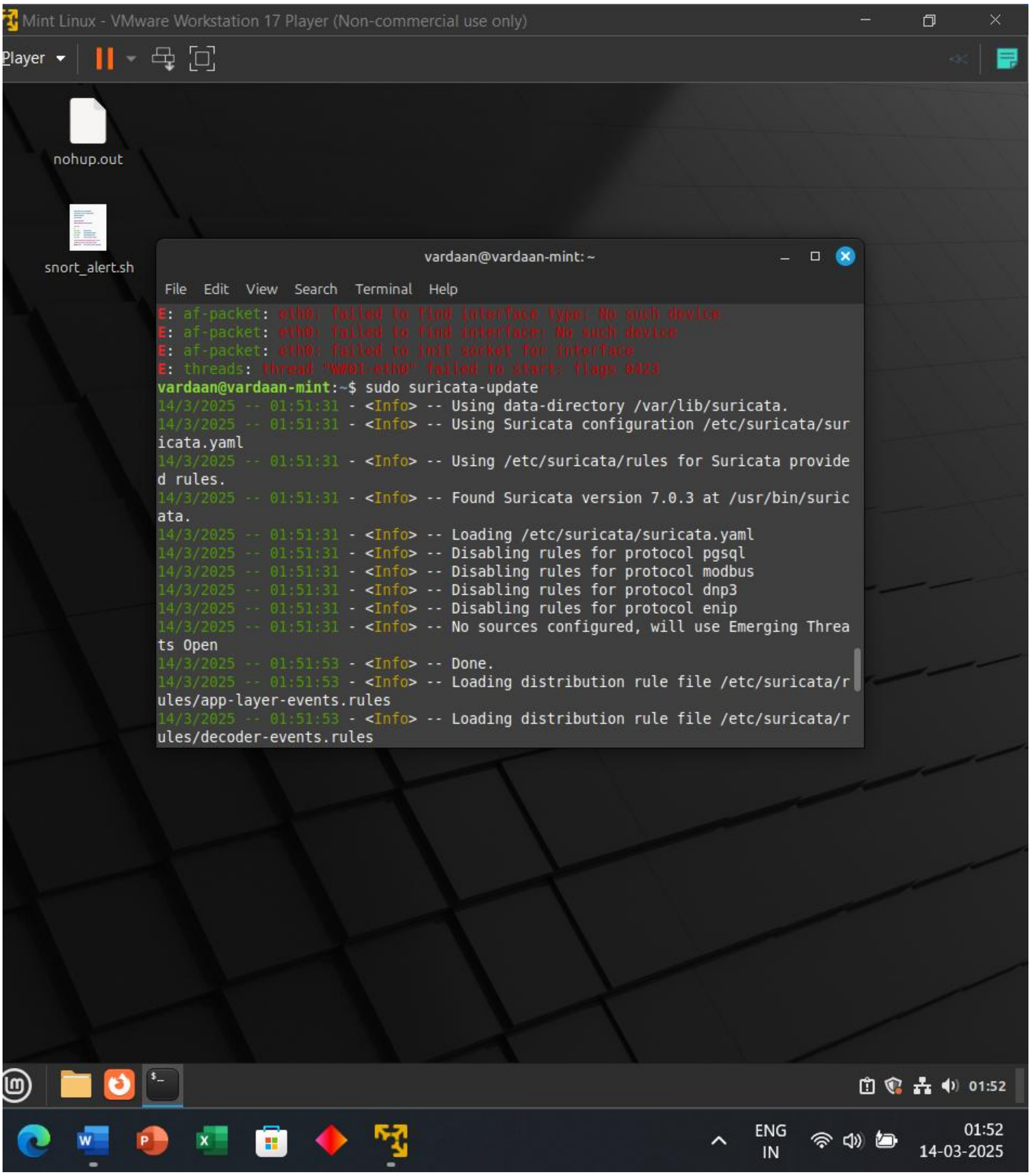


Mint Linux - VMware Workstation 17 Player (Non-commercial use only)
Player
nohup.out
snort_alert.sh
vardaan@vardaan-mint: ~
File Edit View Search Terminal Help
01:50
ENG
IN
01:50
14-03-2025

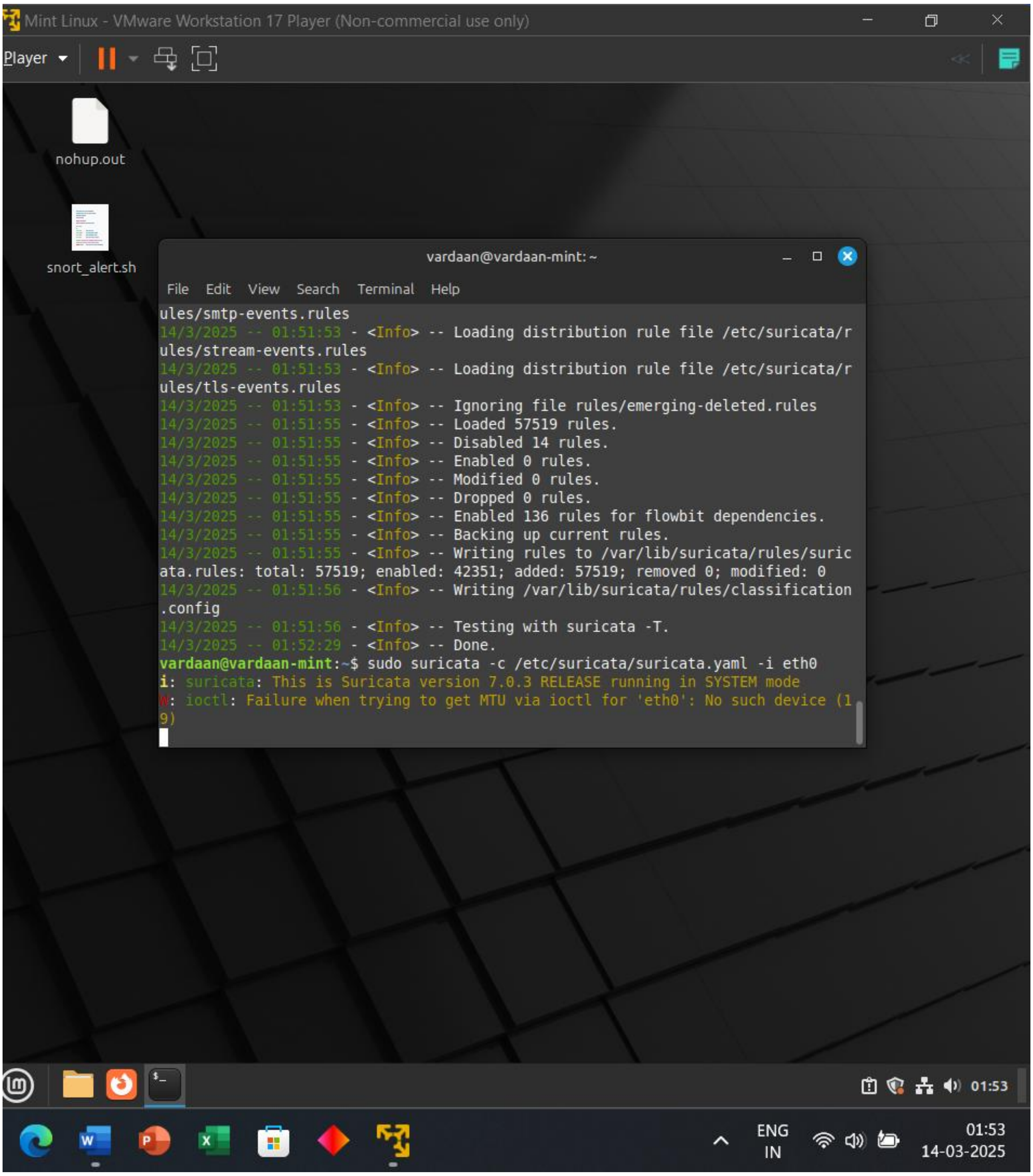
```
 GNU nano 7.2                  /etc/suricata/suricata.yaml
  - interface: eth0
    # Number of receive threads. "auto" uses the number of cores
    #threads: auto
    # Default clusterid. AF_PACKET will load balance packets based on flow.
    cluster-id: 99
    # Default AF_PACKET cluster type. AF_PACKET can load balance per flow or pe>
    # 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 sa>
    #  * cluster_qm: all packets linked by network card to a RSS queue are sent>
    #  socket. Requires at least Linux 3.14.
    #  * cluster_ebpf: eBPF file load balancing. See doc/userguide/capture-hard>
    #  more info.
    # Recommended modes are cluster_flow on most boxes and cluster_cpu or clust>
    # with capture card using RSS (requires cpu affinity tuning and system IRQ >
    # cluster_rollover has been deprecated; if used, it'll be replaced with clu>
    cluster-type: cluster_flow
    # In some fragmentation cases, the hash can not be computed. If "defrag" is>
    # to yes, the kernel will do the needed defragmentation before sending the >

^G Help      ^O Write Out ^W Where Is  ^K Cut       ^T Execute   ^C Location
^X Exit      ^R Read File ^\ Replace   ^U Paste     ^J Justify   ^/ Go To Line
```

Loading rule list and running in IDS mode with logging



```
E: af-packet: eth0: failed to find interface type: No such device
E: af-packet: eth0: failed to find interface: No such device
E: af-packet: eth0: failed to init socket for interface
E: threads: thread "W#01-eth0" failed to start: flags 0423
vardaan@vardaan-mint:~$ sudo suricata-update
14/3/2025 -- 01:51:31 - <Info> -- Using data-directory /var/lib/suricata.
14/3/2025 -- 01:51:31 - <Info> -- Using Suricata configuration /etc/suricata/sur
icata.yaml
14/3/2025 -- 01:51:31 - <Info> -- Using /etc/suricata/rules for Suricata provide
d rules.
14/3/2025 -- 01:51:31 - <Info> -- Found Suricata version 7.0.3 at /usr/bin/suric
ata.
14/3/2025 -- 01:51:31 - <Info> -- Loading /etc/suricata/suricata.yaml
14/3/2025 -- 01:51:31 - <Info> -- Disabling rules for protocol pgsql
14/3/2025 -- 01:51:31 - <Info> -- Disabling rules for protocol modbus
14/3/2025 -- 01:51:31 - <Info> -- Disabling rules for protocol dnp3
14/3/2025 -- 01:51:31 - <Info> -- Disabling rules for protocol enip
14/3/2025 -- 01:51:31 - <Info> -- No sources configured, will use Emerging Threa
ts Open
14/3/2025 -- 01:51:53 - <Info> -- Done.
14/3/2025 -- 01:51:53 - <Info> -- Loading distribution rule file /etc/suricata/r
ules/app-layer-events.rules
14/3/2025 -- 01:51:53 - <Info> -- Loading distribution rule file /etc/suricata/r
ules/decoder-events.rules
```



```
ules/smtp-events.rules
14/3/2025 -- 01:51:53 - <Info> -- Loading distribution rule file /etc/suricata/r
ules/stream-events.rules
14/3/2025 -- 01:51:53 - <Info> -- Loading distribution rule file /etc/suricata/r
ules/tls-events.rules
14/3/2025 -- 01:51:53 - <Info> -- Ignoring file rules/emerging-deleted.rules
14/3/2025 -- 01:51:55 - <Info> -- Loaded 57519 rules.
14/3/2025 -- 01:51:55 - <Info> -- Disabled 14 rules.
14/3/2025 -- 01:51:55 - <Info> -- Enabled 0 rules.
14/3/2025 -- 01:51:55 - <Info> -- Modified 0 rules.
14/3/2025 -- 01:51:55 - <Info> -- Dropped 0 rules.
14/3/2025 -- 01:51:55 - <Info> -- Enabled 136 rules for flowbit dependencies.
14/3/2025 -- 01:51:55 - <Info> -- Backing up current rules.
14/3/2025 -- 01:51:55 - <Info> -- Writing rules to /var/lib/suricata/rules/suric
ata.rules: total: 57519; enabled: 42351; added: 57519; removed 0; modified: 0
14/3/2025 -- 01:51:56 - <Info> -- Writing /var/lib/suricata/rules/classification
.config
14/3/2025 -- 01:51:56 - <Info> -- Testing with suricata -T.
14/3/2025 -- 01:52:29 - <Info> -- Done.
vardaan@vardaan-mint:~$ sudo suricata -c /etc/suricata/suricata.yaml -i eth0
i: suricata: This is Suricata version 7.0.3 RELEASE running in SYSTEM mode
W: ioctl: Failure when trying to get MTU via ioctl for 'eth0': No such device (1
9)
```

Alert files are stored in suricata Bin file.