Practical - 3

1. Objective

The purpose of this practical was to install, configure, and test the Suricata open-source Intrusion Detection and Prevention System (IDPS). The task involved running Suricata on a pre-recorded network traffic file (PCAP) to detect possible threats based on predefined rules.

---

2. Software and Tools Used

- **IDS Engine:** Suricata 7.0.11 RELEASE
- **Operating System:** Windows
- **Interface:** Windows Command Prompt (cmd.exe)
- **Test File:** Network capture file *maccdc2012_00000.pcap*

---

3. Procedure and Execution

Suricata was tested in **PCAP replay mode**, which processes packets from a file rather than a live network. Two attempts were made:

- **Attempt 1: Using Default Configuration**
  Suricata was executed with the PCAP file and a log directory, relying on default rules.

```
C:\> "Program Files\Suricata\suricata.exe" -r
"C:\NU\SEM7\IDPS\maccdc2012_00000.pcap" -l "C:\NU\SEM7\IDPS\logs"
```

- **Attempt 2: Defining Rule Path Explicitly**
  The rule file path was specified directly to overcome suspected configuration issues.

```
C:\> "Program Files\Suricata\suricata.exe" -r
"C:\NU\SEM7\IDPS\maccdc2012_00000.pcap" -s "C:\Program
Files\Suricata\.rules" -l "C:\NU\SEM7\IDPS\logs"
```

---

4. Observations and Errors

Multiple errors prevented the PCAP analysis from completing successfully:

4.1. Rule File Loading Failure

- **Error:** Suricata could not locate rule files (e.g., emerging-dns.rules, botcc.rules).
- **Cause:** Default configuration referred to rule sets that had not been downloaded. A fresh install requires running `suricata-update` to fetch them.

4.2. Invalid PCAP File Format

- **Error:** `unknown file format` and `Failed to init pcap file`.
- **Cause:** Either the PCAP file is corrupted or the file path was misread, as shown by the duplicated filename in the error message.

4.3. Missing Configuration Files

- **Error:** `threshold.config` file missing.
- **Cause:** Required configuration file for managing alert frequency was not present in its expected location.

---

5. Corrective Actions and Recommendations

To resolve the issues and ensure Suricata runs properly:

1. **Update Rules:** Use `suricata-update` to download and organize the latest rule sets into the `/rules` directory.
2. **Check PCAP File:** Open *maccdc2012_00000.pcap* in Wireshark to confirm it is valid and not corrupted.
3. **Run with Proper Configuration:** Use the `-c` flag to load the main configuration file, ensuring all rule paths and variables are recognized.

Corrected Command:

```
suricata.exe -c "C:\Program Files\Suricata\suricata.yaml" -r
"C:\NU\SEM7\IDPS\maccdc2012_00000.pcap" -l "C:\NU\SEM7\IDPS\logs"
```

```
C:\NU\SEM7\IDPS>"C:\Program Files\Suricata\suricata.exe" -r "C:\NU\SEM7\IDPS\maccdc2012_00000.pcap" -S "C:\Program Files\Suricat
.rules" -l "C:\NU\SEM7\IDPS\logs"
Info: win32-service: Running as service: no
i: suricata: This is Suricata version 7.0.11 RELEASE running in USER mode
i: runmodes: thread stack size of 0 to too small: setting to 512k
E: detect: opening rule file C:\Program Files\Suricata\rules\suricata.rules: No such file or directory.
W: detect: 1 rule files specified, but no rules were loaded!
W: threshold-config: Error opening file: "C:\Program Files\Suricata\\\threshold.config": No such file or directory
W: suricata: setrlimit unavailable.
E: pcap: unknown file format
W: pcap: Failed to init pcap file C:\NU\SEM7\IDPS\maccdc2012_00000.pcap/maccdc2012_00000.pcap, skipping
i: threads: Threads created -> RX: 1 W: 16 FM: 1 FR: 1   Engine started.
i: suricata: Signal Received.  Stopping engine.
i: pcap: read 0 files, 0 packets, 0 bytes
```

```
C:\NU\SEM7\IDPS>"C:\Program Files\Suricata\suricata.exe" -r "C:\NU\SEM7\IDPS\maccdc2012_00000.pcap" -l "C:\NU\SEM7\IDPS\logs"
Info: win32-service: Running as service: no
i: suricata: This is Suricata version 7.0.11 RELEASE running in USER mode
i: runmodes: thread stack size of 0 to too small: setting to 512k
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\botcc.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\botcc.portgrouped.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\ciarmy.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\compromised.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\drop.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\dshield.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-activex.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-adware_pup.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-attack_response.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-chat.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-coinminer.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-current_events.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-dns.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-dos.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-exploit.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-ftp.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-games.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-icmp_info.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-icmp.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-imap.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-inappropriate.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-info.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-ja3.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-malware.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-misc.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-mobile_malware.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-netbios.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-phishing.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-p2p.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-policy.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-pop3.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-rpc.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-scada.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-scan.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-shellcode.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-smtp.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-snmp.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-sql.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-telnet.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-tftp.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-user_agents.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-voip.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-web_client.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-web_server.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-web_specific_apps.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\emerging-worm.rules: No such file or directory.
E: detect: opening rule file C:\\Program Files\\Suricata\\rules\\tor.rules: No such file or directory.
W: detect: 47 rule files specified, but no rules were loaded!
W: threshold-config: Error opening file: "C:\Program Files\Suricata\\\threshold.config": No such file or directory
W: suricata: setrlimit unavailable.
E: pcap: unknown file format
```

```
        -v                                  : be more verbose (use multiple times to increase verbosity)
        --list-app-layer-protos             : list supported app layer protocols
        --list-keywords[=all|csv|<kword>]   : list keywords implemented by the engine
        --list-runmodes                     : list supported runmodes
        --runmode <runmode_id>              : specific runmode modification the engine should run.  The argument
                                              supplied should be the id for the runmode obtained by running
                                              --list-runmodes
        --engine-analysis                   : print reports on analysis of different sections in the engine and exit.
                                              Please have a look at the conf parameter engine-analysis on what reports
                                              can be printed
        --pidfile <file>                    : write pid to this file
        --init-errors-fatal                 : enable fatal failure on signature init error
        --disable-detection                 : disable detection engine
        --dump-config                       : show the running configuration
        --dump-features                     : display provided features
        --build-info                        : display build information
        --pcap[=<dev>]                      : run in pcap mode, no value select interfaces from suricata.yaml
        --pcap-file-continuous              : when running in pcap mode with a directory, continue checking directory for pcaps unt
l interrupted
        --pcap-file-delete                  : when running in replay mode (-r with directory or file), will delete pcap files that
ave been processed when done
        --pcap-file-recursive               : will descend into subdirectories when running in replay mode (-r)
        --pcap-buffer-size                  : size of the pcap buffer value from 0 - 2147483647
        --simulate-ips                      : force engine into IPS mode. Useful for QA
        --erf-in <path>                     : process an ERF file
        --include <path>                    : additional configuration file
        --set name=value                    : set a configuration value


To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:

suricata.exe -c suricata.yaml -s signatures.rules -i eth0


C:\Program Files\Suricata>
```


```
        -v                                  : be more verbose (use multiple times to increase verbosity)
        --list-app-layer-protos             : list supported app layer protocols
        --list-keywords[=all|csv|<kword>]   : list keywords implemented by the engine
        --list-runmodes                     : list supported runmodes
        --runmode <runmode_id>              : specific runmode modification the engine should run.  The argument
                                              supplied should be the id for the runmode obtained by running
                                              --list-runmodes
        --engine-analysis                   : print reports on analysis of different sections in the engine and exit.
                                              Please have a look at the conf parameter engine-analysis on what reports
                                              can be printed
        --pidfile <file>                    : write pid to this file
        --init-errors-fatal                 : enable fatal failure on signature init error
        --disable-detection                 : disable detection engine
        --dump-config                       : show the running configuration
        --dump-features                     : display provided features
        --build-info                        : display build information
        --pcap[=<dev>]                      : run in pcap mode, no value select interfaces from suricata.yaml
        --pcap-file-continuous              : when running in pcap mode with a directory, continue checking directory for pcaps unt
l interrupted
        --pcap-file-delete                  : when running in replay mode (-r with directory or file), will delete pcap files that
ave been processed when done
        --pcap-file-recursive               : will descend into subdirectories when running in replay mode (-r)
        --pcap-buffer-size                  : size of the pcap buffer value from 0 - 2147483647
        --simulate-ips                      : force engine into IPS mode. Useful for QA
        --erf-in <path>                     : process an ERF file
        --include <path>                    : additional configuration file
        --set name=value                    : set a configuration value


To run the engine with default configuration on interface eth0 with signature file "signatures.rules", run the command as:

suricata.exe -c suricata.yaml -s signatures.rules -i eth0


C:\Program Files\Suricata>
```