***TTC6030 Cyber Threat Information and Data-analytics***

**Dataset Breakdown**

The dataset was generated between 01.07.2023 and 02.07.2023. Non-malicious web traffic was generated over the following sites: 10.40.20.110 (win11-1.rt.vle.fi), 10.40.20.100 (win10-1.rt.vle.fi), 10.40.20.101 (win10-2.rt.vle.fi) and 10.40.20.10 (dc.rt.vle.fi). Malicious traffic originates from *10.40.20.200*, *10.40.20.201*, *198.18.103.71*, *198.18.103.68, 198.18.103.67* and *198.18.103.65.* The exfiltration destination has been manually altered to appear as Chinese in origin. The altered IP is *113.194.88.145*.

Attacks do not correspond precisely to the scheduled times outlined in the Excel sheet. This is in some cases a by-product of concatenation. There appears to be a printing delay of approximately 1 minute in the logs. Precise attack timestamps are provided below. Timestamp deviation was calculated to be 0.74 seconds. The minimum was 0.1 seconds. The maximum was 5 seconds. A Jupyter Lab file has been included in a convenient ready-to-use format for analysis.

**Attacks**

***Tool* *Timestamp log UID***

Nmap 1688167089.280261 HTTP, conn CtpO8h3IMw4fhUhgAd

Gobuster 1688186939.096791 HTTP, conn CcuNZs4c3wZNhOA0Ac

SQLmap 1688217243.107191 HTTP, conn CABizB1F4VhvgH2hz8

PHP web commands 1688241721.80517 HTTP, conn C9DCU4J1KRnSxcfp5

DNScat 1688283171.628639 DNS CrSgJVnN2eC7PYyj8

Ddosify 1688314387.81371 HTTP CqvNwq3ONc5ADWOQf9

Exfil 1688315464.086768 Conn CBLMUN2W2XjMcM6YUi

**Indications of Attack**

Most IoAs can be found simply by searching for a specific string (eg: “nmap”). This information typically originates from the *user\_agent* field in the http log. In the case of the PHP backdoor attack the most relevant field is the *uri*. For DNScat, the most relevant fields are *query* and *answers.* The majority of DNS-related entries are malicious. They are identifiable from the string “dnscat*”.* Students should be able to identify these reasonably easily.

The first five attacks do not overlap. The DoS attack will be very easy to identify. The *user\_agent* field will provide the necessary information. Exfiltration occurs in the middle of the DoS attack, however. Students will in this case have to search for a suspicious IP address in a sea of DDosify GET requests. The relevant field is *id.resp\_h*.