Forensic Investigation Report By Kevin Harianto

Text

Description automatically generated

Text

Description automatically generated

^Following instruction to install GRR after research for the two clients and server .

Text

Description automatically generated

^setting up sql server

Text

Description automatically generated with medium confidence

^setting up servers.

Text

Description automatically generated

Graphical user interface, text, application, email

Description automatically generated

^Finished setting up grr server

Graphical user interface, text, application, email

Description automatically generated

^downloading binaries from the windows client.

Graphical user interface, text, application

Description automatically generated

^both windows and Ubuntu -linux- clients are up. NOTE: user ubntu from linux OS is changed to uber due to the requirement of reinstateing the image from corruption issues as well as IEUser was just the admin userrname the username still shows to be the student number assigned previously when expanded.

Graphical user interface, text, application, email

Description automatically generated

^analyzing the list of processes for splunk integration of the two clients

Graphical user interface, text, application, email

Description automatically generated

^downloading windows 10 information logs as CSV to be sent to splunk for analyses.

Graphical user interface, application

Description automatically generated

^Downloading Linux Client information logs as CSV to be sent to splunk for analyses.

Graphical user interface, text, application, email

Description automatically generated

^insertting the two CSV files into splunk

Graphical user interface, text, application

Description automatically generated

^extracted information from both Linux and windows clients from running the splunk search to find the information reported by GRR. Not for this practice I only analyzed for a short amount making two changes for linux and one change to process for windows due to the lack of space available in my laptop.

Graphical user interface, text

Description automatically generated

^With the two clients proven to be both linux and windows this concludes the lab

Graphical user interface, application

Description automatically generated

^linux fields extracted in terms of network logs.

Graphical user interface, table

Description automatically generated

^Windows Client analyses from splunk using grr, shows how host is from vmware as well.