Bryan Bolesta, Ryan Fiers, Matthew Horger, Declan Kelly, Layla Phills, Marisa Tranchitella, Zach Santoro

CI 491

Implementation Cycle 1

December 2, 2019

*Summary*

This term, the team worked on standing up the virtual test environment that will be used to implement the EDR tool we are developing. The team was able to host the environment on Cyberdragons’ servers. A Windows 2012 server was stood up as the domain controller and the FREEEDER.lab domain was subsequently created. Another windows 2016 server was stood up as a repository and web server, as such it was configured as an IIS Server (Internet Information Services). A single windows 10 machine was also stood up as an example endpoint for the environment. Both the IIS server and the endpoint were then joined to the domain and domain users were created for each member of our team. The infrastructure team members were then added to the domain admin group in Active Directory to grant them the appropriate privileges. Modifications were also made to the domain group policy (GPO) to generate log events.

*Link to Repository*

<https://github.com/mhorger3/FreeEDR>

*Link to Demo*

<https://docs.google.com/presentation/d/1sj6AP5HcI03NskAO3a0rWbLIZivbLqhXlpR5cKBV5us/edit?usp=sharing>