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

CI 491

Implementation Cycle 1

December 3, 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>

Relevant materials:  
 sysmon\_install.bat

config.xml

Dashboard boilerplate materials (MaterialUI Component Wrappers)

*Link to Demo*

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

Short Architecture Description:  
 In order to have some infrastructure for us to work off of when implementing our designs

next term we needed to set up a small scale network of servers and endpoints that could

handle and generate logs respectively. We set up 3 machines to start us off in that respect.

Two of the machines were set up as servers and one of them as an endpoint that a fake user

would interact with. One of the servers was set up as a domain controller and on it we

created the FREEEDR.lab domain. Now that our domain was created we could domain join the

other machines and create some domain users. A user account was created on the domain for

every member of our team. The user accounts of the team members who's explicit role is to

work on infrastructure, were added to the Domain Admins group in Active Directory. This

grants them the ability to control and configure any settings on the machines provisioned

across the network. The other server was set up as an IIS server to be eventually used

for the dashboard of the FreeEDR tool during our implementation cycle. This infrastructure

was stood up to give us a headstart on next term, however there is room for it to expand.

We plan on adding more endpoints as well as potential attacker machines used to generate

malicious traffic.









