Low-Cost Cyber Exercises with High-Fidelity Realism

Blake Platt, Ryan von Bereghy, Adam Caudle, and Sean Hodgson

INTRODUCTION

- Realistic cyber-range exercises are expensive. Commercial platforms and hand built labs require dedicated infrastructure, licensing, and weeks of setup from a team.
- Beyond cost, two problems other problems are prevalent: manually built labs aren't easily reset and lack the realism of actual users in the environment.
- We present a pipeline that generates a complete, attackable enterprise from one declarative organization file. The file is loaded into our framework, which instantiates the entire environment automatically.
- This organization file defines the entrypoint, which is a deliberately vulnerable website which will provide access to the internal company network via a VPN profile.
- The internal company networks runs Windows hosts populated with GHOSTS agents, which simulate realistic user activity like a real organization.
- These combined techniques create a high-fidelity environment that is easily reproducible, and deployable by anyone.

GHOSTS FRAMEWORK

- GHOSTS is an open-source framework that drives autonomous users on Windows hosts that can browse, email, edit documents, and run shells commands to create realistic network traffic and logs.
- GHOSTS was developed by the Carnegie Mellon SEI.

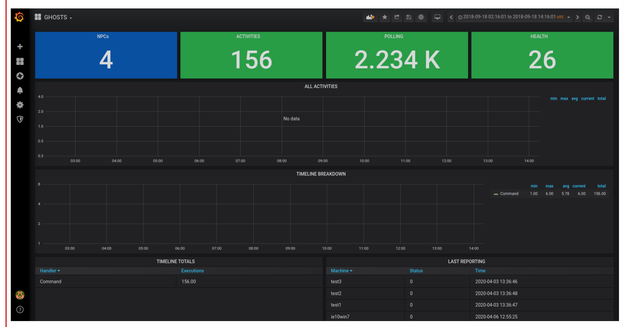

Figure 1: GHOSTS framework dashboard

- Use of GHOSTS within cyber exercises has been related to students reporting higher value in the training, especially within the realism aspect.

THE ORGANIZATION FILE

- A single declarative file that defines the entire exercise including subnets, hosts, accounts, entry point, and GHOSTS behavior
- Easily version controlled and human readable, the goal is for anyone to deploy.
- On load, the framework provisions the exposed website, VPN tunnel, and internal Windows hosts isolated within a Proxmox server.
- Every deploy aims to be the same copy, to keep it fair between teams running in the same exercises.

PROXMOX

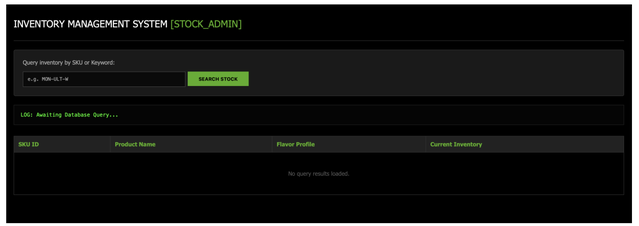

Figure 2:. Vulnerable web app

SKU ID	Product Name	Flavor Profile	Current Inventory
MON-001	Monster Original	Classic Green	4500
MON-ULT-W	Monster Ultra	Zero Ultra White	2800
MON-JS-M	Java Monster	Mean Bean	1200
MON-RE-D	Rehab	Peach Tea	900
MON-VPN	VPN-Access-Gateway	Download Config	1000000

Figure 3:. Exploiting the vulnerable web app

EXPERIMENTAL SETUP

- The exercise hosts loads a single organization file. From there, the framework utilizes completely open-source infrastructure to stand up the exercise.
- Entry Point: an internet facing vulnerable web application. This web application is designed to be flawed and eventually provide an OpenVPN profile to gain access to the rest of the exercise.
- Tunnel: An OpenVPN or WireGuard server that connects the students to the internal Windows infrastructure.
- Windows and GHOSTS: Internal Windows hosts run GHOSTS agents that generate continuous user activity, so the network produces realistic traffic and logs with no host input.
- Infrastructure: Everything was designed to run on the open-source Proxmox hypervisor, contained in a series of LXC containers that control the exercises. Proxmox allows for extensive API use which allows us to bring up and tear down whole exercises programmatically.

INTENDED PATH

- **Recon:** After getting through the vulnerable website, participants enumerate the host and the network reachable through it, including a Windows Active Directory domain. This domain connects all of the Windows hosts, mail servers, and general configuration infrastructure.
- **Initial Access/Execution:** The public facing perimeter is breached through the vulnerable web app.
- **Discovery:** From the breach, students research and map out where they can reach from within the company VPN.
- **Pivots:** Students will find a series of vulnerable machines until the end goal is reached.

REFERENCES

Updyke, Dustin; Dobson, Geoffrey B.; Podnar, Thomas G.; Osterritter, Luke J.; Earl, Benjamin L.; Cerini, Adam D. (2020). GHOSTS in the Machine: A Framework for Cyber-Warfare Exercise NPC Simulation. Carnegie Mellon University. Report. https://doi.org/10.1184/R1/12363029.v1

ACKNOWLEGEMENTS

This work is supported by funding for the VICEROY Northwest Institute for Cybersecurity Education and Research (CySER) provided by The Office of the Undersecretary of Defense for Research and Engineering, in collaboration with the Air Force Research Laboratory and Griffiss Institute.

WASHINGTON STATE UNIVERSITY