README.md

Executive Summary

In today's world, the use of virtual machines in daily business operations has become prolific. Virtual machines can greatly enhance the efficiency of a business and drastically reduces costs associated with purchases of physical machines, energy consumption and cooling. Consequently, as the adoption of virtual environments continues to grow, so does the concern of their security. As organizations dependence on virtual infrastructure, continues to grow, so do security attacks against these systems. A single security breach due to poor configurations can end up costing organizations much more than they saved by switching to virtual infrastructure.

As organizations move operations to virtual environments, they need tools to ensure that they are being properly utilized. The completion of "Container Configuration Verification as a Container" (CCVAS) will provide a method to evaluate systems that use a virtualization technology known as containers. In particular, CCVAS will try to solve the security problems faced when establishing and utilizing Docker. The end project deliverable will be a container that evaluates the security of other containers. This provides a simplified solution that can help reduce organizations' risk when operating in virtual environments.

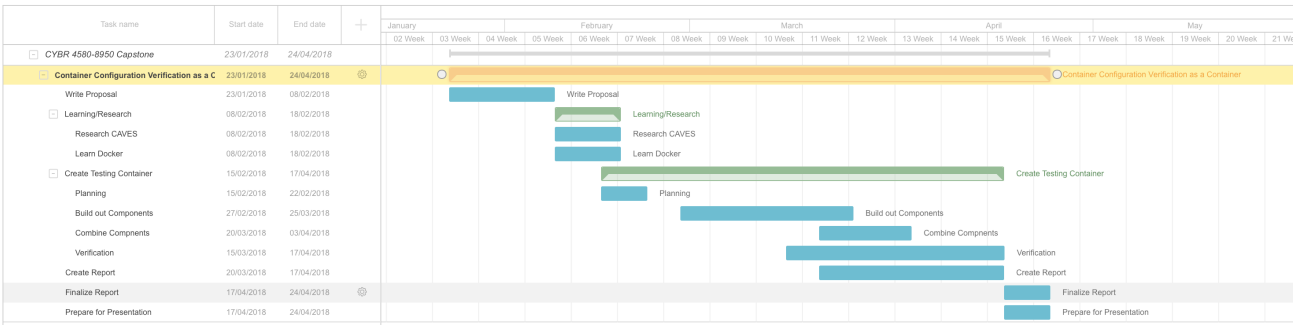
The completion of CCVAS will look to achieve the following list of goals:

- Determine a list of common Docker configurations that leave virtual environments vulnerable to attack.
- Develop a set of scripts and commands that will test for vulnerabilities.
- Test created scripts and selected commands against a container that implements CAVES.
- Generate a PDF report documenting findings of tested containers.

Proposed Project Timeline

In order to achieve all of our project goals, the team has created a timeline to help them meet important deadlines. The following list documents the basic tasks the team aims to meet throughout the weeks. A more detailed Gantt chart can be referenced below for a week-by-week breakdown of project deadlines.

Week	Team focus
0-3	Learn about CAVES and how to use Docker. Find or create CAVES virtual environment for testing.
4-7	Identify important vulnerabilities that may affect CAVES. Create scripts using relevant programs to test against identified vulnerabilities
8-9	Work on report. Combine created scripts and containers into one large Docker container.
10	Write a report which includes research, testing methods, output, and recommendations. Prepare for and deliver presentation.



Project Oriented Risks

Throughout the course of the project, the team will likely experience a variety of risks that threaten to hinder the project's completion. Likelihood displays a risk factor, and ranks the risks with a value between one and five (one being the most likely to occur and five being the least likely to occur). The impact factor shows the team's prediction of how bad the given risk will impact the completion of the project. Impact factor will be ranked with a value between one and ten (one having the least impact on project completion and ten having the most).

Risk	Description of Risk	Likelihood	Impact Factor
Lack of skill set (3)	Group has an overall lack of experience with a given skill, hindering project efficiency.	1	3
Team member availability (8)	Group is unable to meet at the same time.	2	4
Unable to obtain or replicate CAVES model. (12)	The team is unable to create/obtain a VM that follows the CAVES model for testing.	3	4
Scope creep (28)	Unable to test all desired vulnerabilities due to lack of time.	4	7
Divergence in goals (10)	Team and sponsor begin to picture different goals for project as time progresses.	5	2

Project Methodology

User Stories
In order to determine the best path for the project, some important user stories were identified. Those were:

`As a security professional, I want to confirm my organization's containers are secure, so there is no unauthorized information disclosure.`

`As a security professional, I want a automated tool to confirm the security of containers, so I can improve my efficiency and focus efforts elsewhere.`

Literature Review
Relevant research papers have been identified. These are listed in the "Relevant Literature" section below. These each somehow touch the scope of our project, and will be utilized and referenced when possible for the duration of our project.

Technical Plan

Our general plan is to create a Docker container, composed of other Docker containers and components. Each component will complete a dedicated security related task. Components will use existing scripts and tools when possible to evaluate targets. Currently, we plan to run tests such as nmap and OWASP Top 10 to discover any possible configuration vulnerabilities. Docker files will be checked for configuration issues and threats. Scripts to use these tools will be written in bash and python. Any important output will be sent up to the component caller, where it will be added to a report. This report will be a consolidation of all the important data and output in a PDF file.

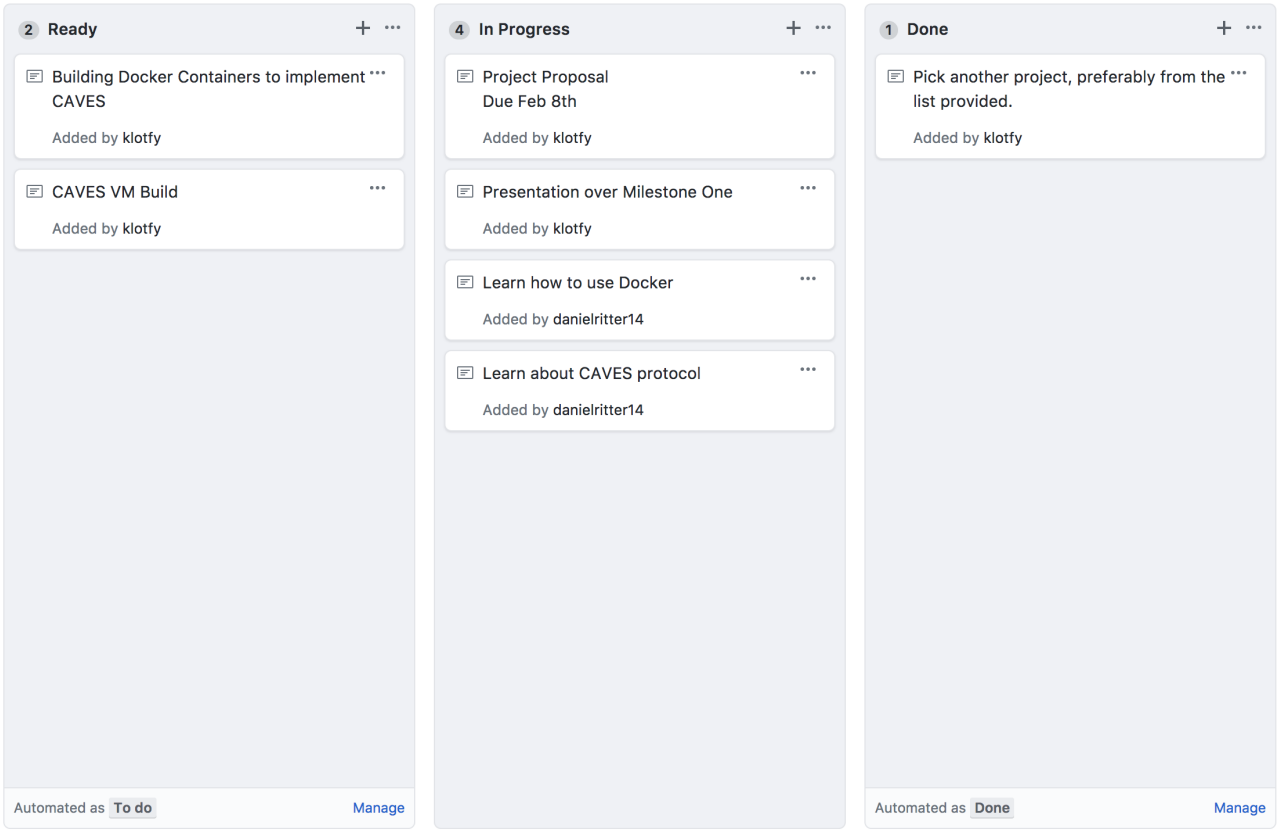
To scan a target, a configuration file will be specified and ingested by the scanning container.

Required Materials

In order to complete the CCVAC project, the team will need the following materials -

Resource	Dr. Hale Needed	Investigating Team Member	Description
Central VM to run Docker	Yes	Alex and Alisa	This VM will be hosted at UNO. The team will SSH into this machine.
Scripting Languages	No	Mike	The team will be utilizing shell and python scripts to generate our tests.
CAVES modeled VMs	No	Dan and Kero	These VMs will be used to test our container solutions on.
VMWare Workstation	No	All team members	Each student will need to download a copy of VMWare Workstation to be able to access the VMs.

First Sprint Plan



Qualifications

This team consists of two graduate students and three undergrad students from the University of Nebraska – Omaha. Each member of the team brings unique technical skills and past experiences, giving the team a diverse background. A detailed description of each team member can be found below.

- Kerolos Lotfy is an experienced in Cyber Security professional with a demonstrated history of conducting penetration tests and source code reviews. Skilled in application, network, and operating system security risks. Along with technical risk assessments, vulnerability management, and remediation. Kerolos, is also published in the 2016 IEEE International Conference on Mobile Services titled "Assessing Pairing and Data Exchange Mechanism Security in the Wearable Internet of Things." Currently finishing up Masters of Science(MS) in Cybersecurity, with an undergraduate degree in Information Assurance with a minor in Computer Science.

- Alisa Bohac is an undergraduate student at the University of Nebraska Omaha (UNO). She will graduate from UNO in May 2018 with a B.S. in Cybersecurity and a minor in Computer Science. Throughout her time as an undergrad, she has held technical positions in two industries, namely software and defense contracting. She interned at a local software company where she worked with the software engineering team on a credit card processing system. Furthermore, she spent the past summer in Lexington, Massachusetts, as a part MIT Lincoln Laboratory's cyber division. While at Lincoln, she created an encrypted communication channel for a DoD system. Finally, she was a recipient of the Walter Scott, Jr. Scholarship and was a member of the Scott Scholar community throughout college. Her interests include penetration testing and digital forensics.

- Dan Ritter is a graduate student at the University of Nebraska Omaha seeking a MS in Cybersecurity, which he is expected to graduate with in May 2018. He graduated with a BS in Cybersecurity with a Computer Science minor in May 2017, after just three years. He is currently President of NULLify, UNO's cybersecurity club. He was a computer science tutor for one year before becoming a Security Analyst Intern at Gallup. His Gallup role has since transformed into a regular part-time role, and will become a full-time role in June. He is currently working on his OSCP certification. Dan's interest include pen testing, network security, and concepts related to reverse engineering.

- Michael Keck is a undergraduate student at the University of Nebraska Omaha studying Cyber Security and Computer Science. While his professional background is not in Cyber Security or Computer Science, Michael has ten years of military experience with which has contributed to personable skills such as leadership, working in a group to accomplish a common goal, and being a overall badass. Michael is currently working on learning more about Cyber Security through classes at the university and also on his own time. His interest is in digital and mobile forensics, industrial control systems, and penetration testing. Michael is will be graduating fall 2018.

- Alexander G. Diaz is a undergraduate student at the University of Omaha at Nebraska and is currently enrolled in the Cyber Security program with an expected graduation date in the Fall of 2018. He is currently working on his Security+ Certification, which should be completed by May 2018. His interest in Cyber Security developed from an desire to harden infrastructure systems against attacks, and is therefore interested in code hardening, digital forensics, and digital industrial systems.

Contact

- Kerolos Lotfy (klotfy@unomaha.edu)
- Dan Ritter (danielritter@unomaha.edu)
- Michael Keck (michaelkeck@unomaha.edu)
- Alisa Bohac (abohac@unomaha.edu)
- Alexander Diaz (agdiaz@unomaha.edu)

Relevant Literature

- Chelladhurai, J., Chelliah, P. R., & Kumar, S. A. (2016). Securing Docker Containers from Denial of Service (DoS) Attacks. 2016 IEEE International Conference on Services Computing (SCC). doi:10.1109/scc.2016.123

    - Securing Docker Containers from Denial of Service (DOS) Attacks gives users a look at a few vulnerabilities that comes with using the Docker environment. The Paper points out that because of the way containers forwards all incoming packets without filtering them, they are open to ARP and MAC flooding attacks. This information will help by providing our team with known issues of the containers architect that we will be able look at and expand on during our testing of the containers.

- Combe, T., Martin, A., & Pietro, R. D. (2016). To Docker or Not to Docker: A Security Perspective. IEEE Cloud Computing,3(5), 54-62. doi:10.1109/mcc.2016.100

    - To Docker or Not to Docker: A Security Perspective, provides and overview of the container environment. The over view encompasses everything from Docker internals, and specifications to security issues that come with using the containers. The paper provides Common Vulnerabilities and Exposures (CVE) that are relevant to the Docker containers, and gives information on weak access controls, image distribution vulnerabilities and configuration security issues.

- Luo, Y., Luo, W., Sun, X., Shen, Q., Ruan, A., & Wu, Z. (2016). Whispers between the Containers: High-Capacity Covert Channel Attacks in Docker. 2016 IEEE Trustcom/BigDataSE/ISPA. doi:10.1109/trustcom.2016.0119

    - Due to the rapid development of the Docker environment, security was not set as a high priority leaving the system opened to security issues. This paper investigates several possible covert channels that cause information leaks between containers.

- Mp, A. R., Kumar, A., Pai, S. J., & Gopal, A. (2016). Enhancing security of Docker using Linux hardening techniques. 2016 2nd International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT). doi:10.1109/icatcct.2016.7911971

    - This paper provides Linux security features and techniques that will enhance the security of the Docker container. Using AppArmor and SELinux module settings within this systems to help harden the Docker system.