2/14/2024

Amechi Nwaeze

Course Name

Semester

Penetration Testing using Cloud

Penetration Testing using Cloud

EXECUTIVE SUMMARY

Objective

The primary objective of this cloud-based project is to design and construct a penetration testing network architecture, a multi-environment software/tool kit that is intended for ethical hacker groups. The architecture will utilize the multitude of cloud products and services provided by Google Cloud such as virtual machines (VMs), virtual private networks (VPCs), and other hardware/software solutions to provide fast and secure testing environments, while considering physical security constraints.

Background

The physical and technical necessities that penetration testers desire for their work can become a stress on company time and resources due to the complexity of setting up safe environments with all the tools and configurations needed to begin tests. This creates an opportunity for businesses to cut down on costs and down-time between tests.

Methodology

* Penetration Testing Toolkit: Start by defining the tools and software desired in the environment. This will help guide a framework of the system and network requirements from within the cloud.
* Cloud Architecture: Define/design the type of resources from Google Cloud that will provide a stable network that will host the tools and software for penetration testing.
* Product Enumeration: Selecting the configurations and specific products that are going to be used for the architecture.
* Cloud Implementation: Build networks, systems, and software as designed in planning stages to set up the penetration testing environment.
* Penetration Testing Test: Use the cloud environment in Google by testing the tools/software to test project and debug any misconfigurations.

\*Key Findings\*

* SecureAI outperforms traditional systems, detecting and mitigating 93% of cyber threats in real-time.
* The solution reduces the average response time by 65%, remaining affordable and accessible for SMEs.
* SecureAI's adaptive learning capabilities enable quick responses to new threats and customization to unique SME cyber risk profiles.

\*Recommendations\*

* SMEs should adopt AI-driven cybersecurity solutions like SecureAI.
* Policymakers should encourage the development and adoption of tailored cybersecurity solutions for SMEs.
* Cybersecurity providers should collaborate with SMEs to better understand their specific needs and challenges.

Conclusion

Cloud technology provides a platform to create ready-for-use packaged services that can cut budget costs and time for tasks such as environment building and configuration, bolstering security and project management for the average business.

Project Milestones: E.g. Major steps required to complete your project.

1. Research: Discover solutions and products in Google Cloud for setting up entirety of project (VMs, VPCs, applications, tools…etc.)
2. Creation: Configure and build the Google Cloud network including all of the needed services and virtualized hardware/systems.
3. Implementation: Use the cloud environment to run scans and execute pen testing tools to test for functionality and security.

Materials List:

1. Google Cloud Account
2. Computer with internet access
3. Cloud Resources (Unknown specifics as of 2/14/2024)

Deliverables: E.g. Report, Deployed architecture, other project outcomes etc.

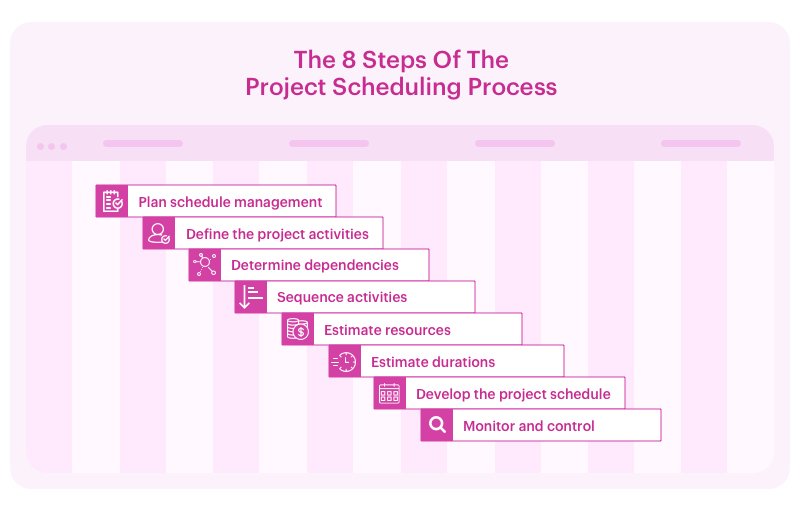
1. Project Report
2. Scan Results
3. Cloud Topology Map
4. Cloud Pen Testing environment

\*Professional Accomplishments\*: E.g. New skills that you developed

1. Accomplishment 1
2. Accomplishment 2
3. Accomplishment 3

PROJECT SCHEDULE MANAGEMENT

Create a Gantt chart with the application of your choice and replace it with the picture presented below.



Project Management Board Link (QR Code Only). Send invite to user: @gdparra

Qr code

Description automatically generated

Create a Github Project Repository and add the user “cyberknowledge” as a contributor.

<https://github.com/your_username/your_project_repo_name>

[EXECUTIVE SUMMARY 1](#_Toc132755617)

[PROJECT SCHEDULE MANAGEMENT 3](#_Toc132755618)

[Milestone 1: Title 5](#_Toc132755619)

[HEADER 1 5](#_Toc132755620)

[Header 2 5](#_Toc132755621)

[Header 3 5](#_Toc132755622)

[Milestone 2: Title 6](#_Toc132755623)

[HEADER 1 6](#_Toc132755624)

[Header 2 6](#_Toc132755625)

[Header 3 6](#_Toc132755626)

[Milestone 3: Title 7](#_Toc132755627)

[HEADER 1 7](#_Toc132755628)

[Header 2 7](#_Toc132755629)

[Header 3 7](#_Toc132755630)

[Milestone 4: Title 8](#_Toc132755631)

[HEADER 1 8](#_Toc132755632)

[Header 2 8](#_Toc132755633)

[Header 3 8](#_Toc132755634)

[Milestone 5: Title 9](#_Toc132755635)

[HEADER 1 9](#_Toc132755636)

[Header 2 9](#_Toc132755637)

[Header 3 9](#_Toc132755638)

[References 10](#_Toc132755639)

Milestone 1: Title

# HEADER 1

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec odio. Quisque volutpat mattis eros. Nullam malesuada erat ut turpis. Suspendisse urna nibh, viverra non, semper suscipit, posuere a, pede.

As shown in Fig. 1, our end-to-end system architecture is composed of …

Diagram

Description automatically generated

Vitae congue mauris rhoncus aenean vel elit scelerisque. Fringilla phasellus faucibus scelerisque eleifend. At tellus at urna condimentum mattis pellentesque id nibh tortor.

## Header 2

Body Text

### Header 3

Body Text

Milestone 2: Title

# HEADER 1

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec odio. Quisque volutpat mattis eros. Nullam malesuada erat ut turpis. Suspendisse urna nibh, viverra non, semper suscipit, posuere a, pede.

Our model’s approach to find the Root Cause Analysis of the detected vulneravility is presented in Algorithm 1.

Text

Description automatically generated

Vitae congue mauris rhoncus aenean vel elit scelerisque. Fringilla phasellus faucibus scelerisque eleifend. At tellus at urna condimentum mattis pellentesque id nibh tortor.

## Header 2

Body Text

### Header 3

Body Text

Milestone 3: Title

# HEADER 1

Lorem ipsum dolor sit amet, consectetuer adipiscing elit. Donec odio. Quisque volutpat mattis eros. Nullam malesuada erat ut turpis. Suspendisse urna nibh, viverra non, semper suscipit, posuere a, pede.

The experimental results, presented in Table 3, show that our model outperforms state-of-the-art works in terms of generazability.

Table

Description automatically generated

Vitae congue mauris rhoncus aenean vel elit scelerisque. Fringilla phasellus faucibus scelerisque eleifend. At tellus at urna condimentum mattis pellentesque id nibh tortor.

## Header 2

Body Text

### Header 3

Body Text

Milestone 4: Title

# HEADER 1

Body Text

## Header 2

Body Text

### Header 3

Body Text

Milestone 5: Title

# HEADER 1

Body Text

## Header 2

Body Text

### Header 3

Body Text

References

Parra, G. D. L. T., Selvera, L., Khoury, J., Irizarry, H., Bou-Harb, E., & Rad, P. (2022). Interpretable federated transformer log learning for cloud threat forensics. In *Proceedings of the Network and Distributed Systems Security (NDSS) Symposium*.

Parra, G. D. L. T. (2021). Distributed AI-Defense for Cyber Threats on Edge Computing Systems (Doctoral dissertation, The University of Texas at San Antonio).

Parra, G. D. L. T., Rad, P., Choo, K. K. R., & Beebe, N. (2020). Detecting Internet of Things attacks using distributed deep learning. *Journal of Network and Computer Applications*, *163*, 102662.

Egan, M. (2021, December 16). Exclusive: 'cyber is the most dangerous weapon in the world,' JPMorgan Council warns. CNN. Retrieved April 27, 2022, from <https://www.cnn.com/2021/12/16/business/cyber-security-hacking-jpmorgan/index.html>

De La Torre Parra, G. (2021, December 1). Introduction to Python. GitHub. Retrieved April 27, 2022, from <https://github.com/cyberknowledge/Python3_Turorial>

**Important Note**: Create your citations using APA format. Use the following link to help automate the process of creating these citations:

<https://www.citationmachine.net/apa>