Partnership and Proactive Cybersecurity Training (PACT)

PI: Salim Hariri, PhD, Professor, Electrical and Computer Engineering (ECE)
Co-PI: Tamal Bose, Head and Professor, ECE, **Co-Is:** Gregory Ditzler, PhD, Assistant Professor, ECE, for CAT Vehicle and PACT, **Coordinator:** Nancy Emptage
Sponsors: The University of Arizona, Department of Energy, National Nuclear Security Administration's Minority Serving Institution Partnership Program

Derek Major

Howard University; Computer Science

Mentor: Dr. Pratik Satam – Electrical and Computer Engineering

Partners: Kendall Hall and Richelle Javier

OpenVAS Project

ABSTRACT: The research, implementation and development of the project worked on throughout the program deals with OpenVAS technology in relation to computer security. The overall purpose of our research is to see how this open source tool is used to be able to scan networks and devices for vulnerabilities. Through the use of Virtual machines given to us from EC2 instances on amazon, we've been able to install OpenVAS for scanning machines as well as using another virtual machine to be able to install vulnerabilities for testing. The major findings uncovered through this project has been how OpenVAS can be used to generate a report on IP scans of a machine. The report given after successfully configuring a scan is able to give key data points to see how severe vulnerabilities on that IP are. The report can then give information on how to fix these vulnerabilities on a computer and can lessen the risk of one of these vulnerabilities being exploited by a hacker. On a larger scale, this tool can be used to ensure the safety of assets in a network and can ensure that the cyberspace is secure.

Kendal Hall

Howard University; Computer Science

Mentor: Dr. Pratik Satam – Electrical and Computer Engineering

Partners: Richelle Javier and Derek Major

OpenVAS Project

ABSTRACT: The research, implementation and development of the project worked on throughout the program deals with OpenVAS technology in relation to computer security. The overall purpose of our research is to see how this open source tool is used to be able to scan networks and devices for vulnerabilities. Through the use of Virtual machines given to us from EC2 instances on amazon, we've been able to install OpenVAS for scanning machines as well as using another virtual machine to be able to install vulnerabilities for testing. The major findings uncovered through this project has been how OpenVAS can be used to generate a report on IP scans of a machine. The report given after successfully configuring a scan is able to give key data points to see how severe vulnerabilities on that IP are. The report can then give information on how to fix these vulnerabilities on a computer and can lessen the risk of one of these vulnerabilities being exploited by a hacker. On a larger scale, this tool can be used to ensure the safety of assets in a network and can ensure that the cyberspace is secure.

Richelle Javier

University of Arizona; Electrical and Computer Engineering, Mathematics

Mentor: Dr. Pratik Satam – Electrical and Computer Engineering

Partners: Kendall Hall and Derek Major

OpenVAS Project

ABSTRACT: The research, implementation and development of the project worked on throughout the program deals with OpenVAS technology in relation to computer security. The overall purpose of our research is to see how this open source tool is used to be able to scan networks and devices for vulnerabilities. Through the use of Virtual machines given to us from EC2 instances on amazon, we've been able to install OpenVAS for scanning machines as well as using another virtual machine to be able to install vulnerabilities for testing. The major findings uncovered through this project has been how OpenVAS can be used to generate a report on IP scans of a machine. The report given after successfully configuring a scan is able to give key data points to see how severe vulnerabilities on that IP are. The report can then give information on how to fix these vulnerabilities on a computer and can lessen the risk of one of these vulnerabilities being exploited by a hacker. On a larger scale, this tool can be used to ensure the safety of assets in a network and can ensure that the cyberspace is secure.