Building and Hardening Windows Server with the Institute for Defense Analyses (IDA)

A Professional Readiness Experiential Program (PREP) Project Effort

----- ***Authors / Student Project Team Members*** -----

Jonathan Luu

Ruth Fikru Balcha

Angelo Michael Santos

----- ***Industry Participant / Mentor*** -----

Chris Murphy
Manager, Enterprise IT Operations
Institute for Defense Analyses

----- ***Faculty Member*** -----

Brian K. Ngac, PhD
Instructional Faculty & Dean's Teaching Fellow
George Mason University's Costello College of Business
bngac@gmu.edu

Interested in being an Industry Participant and or PREP Sponsor? Please reach out to bngac@gmu.edu, Thanks!

Introduction

The internship at the Institute for Defense Analyses (IDA) provided students with an opportunity to work on critical cybersecurity and IT infrastructure projects. Over the 12-week program, interns were assigned the task of building, securing, and accrediting a Windows Server 2022 baseline to replace outdated systems. This hands-on experience allowed them to develop technical skills, collaborate with mentors, and navigate real-world IT challenges.

Business Challenge

The primary challenge was upgrading IDA's server environment from Windows Server 2012, which was nearing the end of its extended support, to Windows Server 2022. This required ensuring the new server met Defense Information Systems Agency (DISA) Security Technical Implementation Guide (STIG) compliance and was properly configured to meet NIST 800-53 cybersecurity standards.

The second challenge involved scanning for vulnerabilities and ensuring compliance with security benchmarks. The team had to conduct STIG scans, Tenable security assessments, and group policy enforcement to strengthen system security. They also worked on addressing discrepancies between different security scanning tools.

Activities Done to Address the Business Challenge

For the first project of Server Deployment and Security Configuration, the interns first used VMware vSphere to create and configure Windows Server 2022 virtual machines. They then installed essential security tools including SCAP Scan, SCCM, and Trellix (antivirus). They continued to harden the server by configuring security policies, disabling unnecessary services (e.g., IPv6 to prevent spoofing attacks), and enforcing DISA STIG requirements. Finally, they tested and refined the security settings through multiple configuration cycles.

For the second project of Vulnerability Scanning and Compliance Testing, the interns conducted STIG scans to assess server security posture before and after configurations. They used Tenable security scans to detect additional vulnerabilities not flagged by STIG. The interns then had to resolved vulnerabilities through system hardening and documentation of risk acceptances where immediate fixes weren't feasible. They also implemented Group Policy (GPO) configurations to enforce security controls across multiple systems.

Results & The Positive Impact

The work resulted in four major positive impacts for IDA:

- Successfully built and hardened a Windows Server 2022 baseline with a compliance score of 95.11%.
- Significantly reduced security vulnerabilities by addressing open findings and enforcing group policies.
- Created comprehensive security documentation, including risk assessments and remediation plans.
- Provided IDA with a secure, operational server environment that meets federal cybersecurity standards.

Conclusion

The internship provided invaluable experience in server deployment, security hardening, and compliance testing. Interns gained technical expertise, problem-solving skills, and an understanding of real-world IT operations. Despite challenges such as software deployment issues, documentation discrepancies, and access restrictions, the team successfully delivered a secure Windows Server 2022 environment, preparing them for future careers in cybersecurity and IT.

PREP Student Reflection

In their final presentation to IDA, the interns reflected on their experience as follows:

- Learning from Mistakes: Mistakes such as accidentally shutting down a company server reinforced the importance of careful execution and documentation.
- Improving Documentation Practices: Initially, poor documentation led to confusion when mentors requested details. The team adapted by recording every configuration change systematically.
- Building Stronger Team Collaboration: Differences in documentation styles and security settings required the team to communicate and standardize their approach.
- Gaining Hands-on Cybersecurity Experience: Working with STIG, Tenable, and Group Policy enforcement provided practical skills that will be valuable in their careers.