

Assignment Title:

Offensive and Defensive Actions

By

Blue Team

Joshwa Edsall, Michael Moore,

Kristen Netter, Courtney Roberts, Steven Trudell

OPSC-590

Fall 2 2024

By submitting this assignment, I acknowledge that I have read and agree to abide by the Champlain College Academic Honesty Policy. I declare that all work within this assignment is my own or appropriately attributed. I accept that failure to follow the academic honesty policy may result in a failure grade, or expulsion from Champlain College.

Date Due: December 15, 2024

Date Submitted: December 15, 2024

**Introduction**

From 17 Nov 2024 to 8 Dec 2024, the Blue Team conducted a War Game Capstone scenario against the Red Team. During this time, each team defended their environments while attacking the opposing teams’ environments. This After-Action Report (AAR) discusses the Blue Teams efforts.

*What did you set out to achieve?*

* During the Capstone, the Blue Team’s goals included hardening their environments to prevent an intrusion, respond to an intrusion if one occurred, and to compromise the Red Team’s environment.

*What was your plan to achieve this?*

* The Blue Team drafted a plan to achieve their attended goals. Specific roles were developed with responsibilities and assigned to team members, with a secondary for each role. Roles and responsibilities were as follows:
  + Team Lead/Coordinator – oversees all operations, ensures communication flow between offensive and defensive teams, coordinates the team’s overall strategy
  + Network Defense Specialist (Firewall/IDS/IPS Monitoring) – focus on setting up, maintaining, and monitoring intrusion detection and prevention systems, to include firewalls; ensure essential services are available.
  + System Administrator (Patch Management and System Hardening) – manage operating systems, apply patches, harden the environment, and ensure all servers are running securely.
  + Offensive Security Specialist (Penetration Tester) – focus on identifying weaknesses within the internal network; evaluate vulnerabilities, explore entry points which could be exploited.
  + Incident Response Specialist (Forensics and Threat Mitigation) – Leads the incident response for any intrusions by analyzing logs, conduct forensic analysis, or coordinate remediation.

*How did this change as you progressed?*

* As more information and knowledge was gained on the Blue Team and Red Team environments, processes and tools were changed. For example, some system monitoring tools which were selected for the Kali Linux environment were not compatible. Those tools needed to be changed to tools which were compatible. Additionally, as members of the Blue Team had emergencies and work travel, the secondary for the job roles took on a more active role to assist the primary.

*What went well and why?*

* The overall experience went well. Everyone on the Blue Team contributed to the Capstone. Typically, in group projects there are individuals who do all the work and those who do the bare minimum. Everyone contributed equally. On top of that, each member also gained knowledge and experience.

*What could have gone better?*

* Unfortunately, the Blue Team was spread across different time zones. This made it difficult to set up team discussions with all members and sometimes caused a lack of communication. Communication could have been better, but each team member did the best they could with their work schedule and their life balance.

*What advice would you give yourself if you were to go back to where you were at the start of the project?*

* Conduct more research a head of implementation. A lot of time was spent research tools and troubleshooting tools while the Capstone was live. If more research was conducted a head of time, less time would have been spent research and more time could have been spent on implementation and attacking.

*What were the two or three key lessons you would share with others?*

1. Open communication is key to any exercise, which includes active listening.
2. Adaptability and flexibility are needed when working in a team. Knowing each other’s roles and responsibilities and being able to step in to assist when life happens is important.
3. Back-ups, back-ups, and back-ups. Ensure to make images as the environment changes in case something happens, and the environment needs to revert back.

*What next for you in terms of this project?*

* Even though this is the end of the class, and of the program, the lessons learned from this project will assist in our professional careers. The tools will be incorporated into future Blue Team and Red Team exercises, in a hope the implementation will go quicker as there is more experience with the tools.

*Can you think of a story that summarizes your experience of work on this project?*

* Yes

*What should we have learned from this project a year from now?*

* Looking back a year from now, the lessons learned will still be applicable. No group project will be successful without open communication, and adaptability and flexibility. Back-ups are the most important first step to take, and to continue to take as modifications are made to any environment.

*Are there any lessons for you personally?*

* Trust in myself and my skill set. Even though I was not comfortable as I was unfamiliar with the more “hands-on-keyboard” work, I knew what I was doing and I needed to trust myself. I need to step outside my comfort zone more and try even if I might fail.

**References:**

NetApp. (2024). *What is Data Backup and Recovery?* NetApp. Retrieved from https://www.netapp.com/cyber-resilience/data-protection/data-backup-recovery/what-is-backup-recovery/

Stevenson University. (2024). *The Importance of Effective Communication.* Stevenson University. Retrieved from <https://www.stevenson.edu/online/about-us/news/importance-effective-communication/>