

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 8, 2024

Date Submitted: December 8, 2024

**Introduction**

The Blue Team entered Phase Three of the Cyber Warfare simulation. The Blue Teams is functioning smoothly while attempting to maintain the learning objective while entering offensive barriers. The Blue Team was able to establish a network device scanner and enable further implementations of the team’s SIEM. Additionally, the Blue Team was able to identify unauthorized access through the Windows Server Guest Account and a false positive.

Below are the actions and findings the Blue Team performed throughout Phase Three.

*Brief Overview*

* The Blue Team focused on enhancing network defenses, establishing and maintaining real-time monitoring, and addressing vulnerabilities. The Blue Team also took offensive steps to infiltrate the Red Team’s environment.

*Defensive Actions*

* Reviewed Atera for alerts. There were no critical alerts. Atera identified the open ports in our environment and still identified our three devices.
  + Atera set up a sample ticket which caused some confusion. At first I thought “John Smith” was messing with our ticketing system. Upon further review, it was Atera demonstrating its capabilities.
  + Atera recommends one operating system patch for the Windows Desktop: Feature update to Windows 10, version 20H2. This update requires a reboot. Did not implement this patch as did not want to cause potential issues prior to the end of the exercise.
  + No critical patch updates were identified.
* System Monitoring (Sysmon) data was reviewed and analyzed on a regular basis for suspicious activities. To date, nothing was identified as suspicious or concerning.
* Againt, attempted to install a system monitoring tool on Kali Linux (Glances, Nedata, Conky, and Grafana and Prometheus); however, kept receiving error messages stating there was no public key available.
  + A public key was created; however, the install command for Glances and Conky returned a different error message.
* Connected system hardening on the Windows OS
  + Utilized the CISA Windows hardening checklist and other resources to strengthen our Windows OS.
* Attempted to install SCuBA (CISA tool) but encountered issues with PowerShell during the installation process. Despite re-installing PowerShell and resolving the initial issues, errors persisted when installing SCuBA.
* Regularly monitored Snort reviewing and analyzing logs. Observed normal traffic and no intrusions or abnormal activity was detected.
* Monitored network connections and listening ports.
  + No listening ports were detected.
* The Blue Team established Splunk Enterprise for monitoring purposes. The Blue Team was able to monitor several logs, including:
  + Security
  + Application
  + System logs
  + Key Management Service
  + Setup
  + and others
* The other tools continuing to be used are Windows Event Monitor, Procmon, and system internal tools, including Sysmon, to identify potential events in coordination with the SIEM.
  + SOC/SIEM activities are specialized skills within the Cybersecurity industry, and they require extensive experience and knowledge to execute well.

*System Hardening:*

Additional resources were further limited during the course of the second week in order to promote a more robust defensive posture. Networking protocols were examined, in depth, to exhume any potential areas of vulnerability which led to the discovery of multiple alternate accounts within the Windows 10 environment. These accounts were immediately disabled to deny potential avenues of attack, and permanently deleted from the group policy settings following deactivation.

Furthermore, all account settings, password complexity requirements, user permissions, and group policy objectives were redefined to prevent potential vulnerabilities from becoming exploited. During the course of these events, multiple low criticality vulnerabilities were discovered in relation to the above mentioned objects and were remediated expeditiously.

*Fail2Ban Implementation:*

Fail2ban is implemented and currently monitoring for failed login attempts over SSH and IP address documentation of attempted logins. Currently no detection have been observed.

*Service and Update Challenges:*

Continuous issues resolving certification resolution for updating and upgrading service via Linux desktop environment. Ongoing research will be conducted to resolve this issue in upcoming efforts.

*Blue Team Offensive Operations*

Over the course of the second week in the environment Blue Team offensive members attempted to gain access to the Red Team’s environment. This included the utilization of new tools and resources in an attempt to garner additional information from potential targets.

In conjunction with Blue Team defensive operations, we were able to definitively identify the following Red Team Environment:

* Kali Linux Terminal (RED): 192.168.6.1

Tenitive identification remains the same for the following Red Team Environments:

* Windows Server (RED): 192.168.3.1
* Linux Server (RED): 192.168.3.2
* pfSense Firewall (RED): 192.168.5.1
* Windows Terminal (RED): 192.168.5.250

During the course of operations multiple exploits were launched against identified vulnerabilities on the Red Team network. These vulnerabilities mainly revolved around Ports 22(TCP), Port 80 (http/nginx) and Port 123 (NTP). The objective of the multiple exploits launched was to gain persistence access to the Red Team Environment; as of this report persistence was not achieved nor were additional vulnerabilities detected.

Caldera was installed on the Kali Linux terminal. Caldera supports red team operations by providing tools to execute attack chains. Caldera was installed without issues; however, the Python requirement kept returning errors. The Blue Team attempted to use the Manx plug-in, which is a reverse shell. Manx has a GUI which allows for the dropping of reverse-shells on the target hosts and interacts manually with the hosts. Burp Suite free edition located on the Windows Commando VM Desktop was attempted to be used as a pentest engagement to launch payloads, unfortunately the Java resulted in an error and a JNI error occurred. Reinstallment of Burp Suite offered no resolution as suggested by research.

*Blue Team Detections*

The Blue team had two major detections. The Blue Team’s offensive team was able to identify the Red Team’s Kali Linux machine. This discovery led to the identification that the Red Team’s Kali Linux was able to access the Guest Account on the Windows Server. This is a common exploit that malicious actors tend to use to gain persistence. The Blue Team responded to the discovery and immediately disabled the account. Additionally, the Blue Team did not identify further information that the Red Team managed to gain persistence within the Windows Server. The individual responsible for the SIEM was using Sysinternal tools such as Sysmon and Procmon. After running Sysmon processes the individual discovered a buffer overflow. The Individual traced the file system and examined Windows debuggers. The identified file was a log for the Blue Team’s Elastic SIEM. The assumed conclusion is that the SIEM is running in a limited academic environment with constrained memory and power which may provide the reason why the Sysmon internal tool identified it. The debugger did not identify other findings.

**References**