

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: November 24, 2024

Date Submitted: November 24, 2024

**Introduction**

The Blue Team entered Phase Two 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 Two.

*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*

* Conducted a device scan with Atera. Atera was able to discover three devices on our network: 1) Windows Desktop; 2) Kali Linux Desktop; 3) pfSense Firewall.
  + Atera was linked to the Kali Linux Desktop. All patch management, device scanning, etc., can be conducted from the GUI within the Windows Desktop.
  + Atera recommends one operating system patch for the Windows Desktop: Feature update to Windows 10, version 20H2. This update requires a reboot.
  + 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.
* 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. Need to conduct additional research into identifying public keys to implement system monitoring on Kali Linux.
* Configured Snort for real-time network monitoring and intrusion detection.
  + Added a lot of custom rules to detect suspicious activities, including ICMP pings, unauthorized SSH access attempts, malware downloads, and SQL injection attacks.
* Monitored network connections and listening ports.
  + No listening ports were detected.
* The Blue Team established a SIEM using Elastic in the first phase. The Blue Team add several items to the SIEM
  + Installed over 200 alerts including: Threat Intel IP Address Indicator Match, Rapid7 Threat Command CVEs Correlation, Potential Invoke-Mimikatz PowerShell Script, Ransomware Machine Learning Detection and others.
  + While the Rules were installed cybersecurity professionals must enable notifications and the rules for a SIEM to be effective.
  + Further, The team member responsible for the SIEM started to examine integrations and working with dashboards.
  + The Blue Team member is trying to find a method to import Windows Server Logs into the SIEM.
* 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 a specialized skill within the Cybersecurity industry and take extensive experience and knowledge to execute the activities 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.

*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**