

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 17, 2024

Date Submitted: November 17, 2024

**Introduction**

The Blue Team started week one of three different week-long offensive and defensive cybersecurity actions. The Blue Team experienced some successes after experiencing growing pains in a new environment. The following documents outline the team's actions throughout the week.

*Brief Overview*

* Implemented System Monitoring (Sysmon) on the Windows Desktop. Sysmon is a Windows service and device driver which stays persistent on the machine after reboots. It provides detailed information about process creations, network connections, and changes to files.
  + Sysmon was monitored and reviewed daily to identify suspicious activity.
* Attempted to implement Sysmon on the Kali Linux Desktop; however, was unable to. Since Sysmon would not work, attempted to install Gnome. Was unable to install Gnome. Currently researching another Sysmon option for Kali Linux.
* Conducted a Nikto scan on the Kali Linux Desktop. Two vulnerabilities were identified.
  + The X-XXS-Protection header is not defined.
  + The X-Content-Type-Options header is not set.
* Installed Atera Patch Management on the Windows and Kali Linux Desktops. Atera offers a 30-day free trial. It offers patch management, network discovery, and other automation and management functions.
* Conducted Legion scans of the Kali Linux and Windows Desktops identifying multiple open ports and associated CVE’s in relation to those open ports.
  + Steps were taken to disable those ports and remove vulnerabilities.
* Conducted Legion scans of the Windows Server, Linux Server, and pfSense firewall which identified vulnerabilities associated with open ports and the associated CVE’s were identified and remediation strategies were put into place.
* Downloaded Snort on the Windows OS. Currently in the process of configuring the system and adding rules. Snort monitors network traffic to detect and mitigate threats ans suspicious activity. It can be configured to block malicious traffic and provides detailed logs and alerts for traffic analysis.
* Planning to deploy Snort on Linux within the next few days.
* Utilized the netstat command on Windows. Monitored network connections and listening ports.

*Defensive Actions*

The first thing that the Blue Team accomplished was to identify potential holes in the firewall, servers, and Windows environment. This was achieved by reviewing firewall settings and updating access controls, which in review were found to have several areas of defense that needed to be modified to increase our defensive posture. This included blocking high-risk ports (RDP 3389, NetBIOS 135/139/445) on the pfSense firewall. In addition, to meet the defined terms of engagement, Blue Team identified and disabled an unauthorized "block all inbound WAN traffic" rule, informing the professor and team.

In order to find additional areas of remediation within the environment, Blue Team began vulnerability testing of our respective environments. This included the utilization of passive/active reconnaissance tools such as Nmap, Legion, and netdiscover; this provided information about potential vulnerabilities inherent within the environment respective to each VM. The discovered information prompted Blue Team to take measures to remedy the potential vulnerabilities that were discovered. This included the filtering/blocking of the following ports:

* 21 (FTP)(TCP): This port was disabled to prevent data and credentials from being transmitted via the FTP protocol.
* 23 (Telnet)(TCP): Disabled to prevent the transmission of data, including passwords.
* 135 (NetBIOS)(TCP): This port was disabled due to potential vulnerabilities with the deprecated NetBIOS service.
* 137 (NB-Name-In)(UDP): Disabled to prevent NetBIOS name resolutions from inbound sources. Blocks nmap device identification.
* 137 (NetBIOS)(TCP): This port was disabled due to potential vulnerabilities with the deprecated NetBIOS service.
* 139 (NetBIOS Session Service)(TCP): This port was disabled due to potential vulnerabilities with the deprecated NetBIOS service.
* 445 (Kerberos/DS)(TCP): Disabled to prevent utilizing common Kerberos vulnerabilities to imbed malware or worms within Blue Team environments.
* 161/162 (SNMP)(TCP/UDP): Disabled due to potential vulnerabilities with SNMP and because it’s not needed.
* 1536-1547
* 3306 (MySQL)(TCP): This port was disabled due to potential security vulnerabilities associated with MySQL.
* 3389 (Windows RDP)(TCP): Disabled due to potential vulnerabilities revolving around Windows RDP.
* 5357 (WSDAPI)(TCP): Disabled due to potential exploits leveraging deprecated API services
* 5985 (Windows PowerShell Remote Management)(TCP): Disabled due to potential vulnerabilities revolving around Windows RDP.
* 10247 (DIAL Protocol Server)(TCP): Disabled to prevent HTTP remote control and XSS.

The next step was to establish a security information and event management (SIEM) monitor. The IR team with the help of other Blue Team members identified resources to establish an Elastic trial that assists with detection and centralizes the logs. The individual responsible for the SIEM pivoted amongst several strategies in order to attempt to gain seamless integration of the Elastic Siem. The individual found a resource that enabled him to use the Windows machine to establish and log information in order to quickly identify potential attacks. Current highlighted fields include agent name, event action, event id, and process command line. The Blue Team continuously monitors Windows Event Viewer, Process Monitor, and Sysmon. While the trial and error was lengthy the SIEM is established for week two to further establish rules, notifications, and alerts. Additionally, the responsible individual will attempt to incorporate the servers into the SIEM.

*System Hardening:*

Conducted a Lynis scan to identify vulnerabilities and recommendations for the Linux server.

Adjusted password policies (max days: 90, min days: 10) and included complexity requirements for all passwords amongst all user groups and attributed roles.

Additionally, User Groups were reviewed and modified to reflect the needs of Blue Team and to eliminate potential avenues of attack from Red Team offensive practitioners.

Despite repository and update issues, Blue Team increased the system's assessment index from 62 to 64.

*Fail2Ban Implementation:*

Installed and configured Fail2Ban to monitor SSH access.

Set ban time to 10 minutes and retry limit to three attempts, mitigating brute-force attacks.

Establish Linux Desktop IP address as exclusion IP to prevent lockout.

Plan to change ssh port but validation and verification needed before changes are implemented to prevent unforeseen issues and concerns regarding future implementation of tools or attack efforts.

*Service and Update Challenges:*

Encountered persistent repository and update signature issues, preventing full implementation of Lynis recommendations such as updates and upgrades effectively thus requiring the installation of unattended upgrades for better stability and automatic updates. Going forward remediations will be researched in order to efficiently achieve updates to affected services and devices within the environment. This will include a complete investigation into the existing certifications, signatures, and keyrings of the respective environments to achieve a more seamless patching process.

*Blue Team Offensive Operations*

During the course of this operation, multiple methods of active reconnaissance were utilized in order to attempt to identify the Red Team’s environment. This included the utilization of tools such as Nmap, which allows for the identification of network components and terminals by sending and receiving network packets to open ports. The most commonly discovered ports indicated a filtered status, which leads me to believe that the Red Team effectively set inbound rules into their pfSense firewall.

The following list denotes what we believe to be the Red Team environment:

* IP Address: 192.168.3.1 (Windows Server)
  + Filtered ports indicate the utilization of WindowsOS services such as NetBIOS and MSRPC which would not be found on a Linux Server.
* IP Address: 192.168.3.2 (Linux Server):
  + This is believed to be the Linux Server due to Legion scans that identify the hardware as Linux 2.6.18 at 100% accuracy.
* IP Address: 192.168.5.1 (pfSense Firewall (RedTeam)):
  + Information obtained from Legion/Nmap points to the above IP address as the potential pfSense firewall of Red Team. Information obtained from Legion matches gathered information that mimics Blue Team’s firewall identification, leading us to believe that this is one of our target environments.
* IP Address: 192.168.5.250 (Linux Terminal):
  + Information gathered from Legion/Nmap mimics known information of Blue Team’s Linux Terminal(Kali) environment, leading us to believe that this is the Red Team’s Linux Terminal.
* IP Address: 192.168.6.1 (Windows Terminal):
  + This is believed due to the filtered and closed status of specific ports that only function on the WindowsOS. This includes such notable ports as 137/139 which govern NetBIOS communication which is only utilized on WindowsOS. In addition, port 135 which governs standard connection traffic for the MSRPC (Microsoft Remote Protocol).

Notable TCP ports that have been filtered include:

* 20-25, 53, 80, 110, 119, 123, 143, 161, 194, 443

This eliminates a large portion of potential standing CVE’s to leverage against the more commonly vulnerable ports listed above. While filtering status does not make exploitation completely unavailable, it does require that we establish access from a different point of access prior to attempting any exploits within the filtered settings.

Additional reconnaissance is going to be necessary going forward to obtain definitive information in regards to the Red Team environment. Following successful identification of the Red Team environment, appropriate research will be conducted in order to attempt to achieve persistent access via leveraging exploitations based upon discovered findings.

*Blue Team Detections*

* Did not identify any Indications of Compromise during the first week in the environment. Continuous monitoring has been enabled with appropriate notification methods integrated to respond quickly to any IoC’s within the environment. Additionally, several more methods of monitoring including the upcoming utilization of additional IPS/IDS software is currently being implemented in order to provide a more robust availability of response to potential IoC’s in the future.

**References**

Abu-Dabaseh, F., & Alshammari, E. (2018). Automated Penetration Testing: An Overview. Computer Science & Information Technology. Retrieved from <https://doi.org/10.5121/csit.2018.80610>

Atera. (2024). *Next level patch management for IT professionals.* Atera. Retrieved from [All-in-one RMM and PSA platform - Atera](https://www.atera.com/lp/aw/patch-management-solution/?cq_src=google_ads&cq_cmp=11137892546&cq_term=atera%20patch%20management&cq_plac=&cq_net=g&cq_plt=gp&utm_adgroup=atera_patch_management&utm_adname=&utm_audience=&utm_source=adwords&utm_campaign=brand-usa-ateraplus-exact-m&utm_medium=cpc&utm_term=atera%20patch%20management&hsa_cam=11137892546&hsa_grp=108819483803&hsa_ad=692896501589&hsa_kw=atera%20patch%20management&hsa_tgt=kwd-604433531256&hsa_mt=e&hsa_acc=6675104902&hsa_src=g&hsa_net=adwords&hsa_ver=3&gad_source=1&gclid=Cj0KCQiAouG5BhDBARIsAOc08RR0yvZIxN1Yz95Hf1SBr6ERike8L3-fEM-J3IqCvvDEf0MEYGvB-ywaAtrAEALw_wcB)

Atumu, M. (2024). Tactical server hardening checklist for Windows and Linux security. Retrieved from https://www.liquidweb.com/blog/server-hardening-checklist/#:~:text=Operating%20System%20(OS)%20hardening%20is,Additional%20important%20steps%20include:

Canada Centre for Cyber Security. (2021). Top 10 IT security actions to protect Internet connected networks and information (ITSM.10.089). Retrieved from https://www.cyber.gc.ca/en/guidance/top-10-it-security-actions-protect-internet-connected-networks-and-information-itsm10089

Crandford, J.J. (2023). Incident Response Plan: Frameworks and Steps. Retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/incident-response/incident-response-steps/

Exabeam. (n.d.). SANS Incident Response: 6-Step Process & Critical Best Practices. retrieved from https://www.exabeam.com/explainers/incident-response/sans-incident-response-6-step-process-critical-best-practices/

Fortinet. (n.d.). What Are Honeypots (Computing)? retrieved from https://www.fortinet.com/resources/cyberglossary/what-is-honeypot

Gartner. (n.d.). Security Information And Event Management (SIEM). retrieved from https://www.gartner.com/en/information-technology/glossary/security-information-and-event-management-siem

Holik, F., Horalek, J., Marik, O., Neradova, S., & Zitta, S. (2014). Effective penetration testing with Metasploit framework and methodologies. 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics(CINTI). Retrieved from https://doi.org/10.1109/cinti.2014.7028682

Kidd, C. (n.d.). SIEM: Security Information & Event Management Explained. retrieved from https://www.splunk.com/en\_us/blog/learn/siem-security-information-event-management.html

LaBarge, R. (2012). Cloud Penetration Testing. International Journal on Cloud Computing: Services and Architecture. Retrieved from https://doi.org/10.5121/ijccsa.2012.2604

Netwrix. (n.d.). Linux Server Hardening and Security Best Practices. Retrieved from https://www.netwrix.com/linux\_hardening\_security\_best\_practices.html

Russinovich, M. & Garnier, T. (2024). Sysmon v.15.15.Retrieved from https://learn.microsoft.com/en-us/sysinternals/downloads/sysmon

SolarWinds. (2024). What is Packet Capture (PCAP)? Retrieved from https://www.solarwinds.com/resources/it-glossary/pcap

Stanham, L. (2023). Behavioral Analytics. retrieved from https://www.crowdstrike.com/en-us/cybersecurity-101/exposure-management/behavioral-analytics/?srsltid=AfmBOoqYJ6aDcgvQqmej4xTI-VljPEr3yr7DqCOfpw9WZYmW-2N9HPpU

Tatam, R. (2023). Automatic system hardening: Checklist + examples to ensure system security. Retrieved from https://www.puppet.com/blog/system-hardening

Udochukwu ThankGod Ikechukwu Igwenagu, Abidemi Ayodotun Salami, Abayomi Shamsudeen Arigbabu, Cassandra Esambe Mesode, Tunbosun Oyewale Oladoyinbo, & Oluwaseun Oladeji Olaniyi. (2024). Securing the Digital Frontier: Strategies for Cloud Computing Security, Database Protection, and Comprehensive Penetration Testing. Journal of Engineering Research and Reports, 26(6), 60–75. https://doi.org/10.9734/jerr/2024/v26i61162

Xcitium. (n.d.). What are Types of Detection? retrieved from https://www.xcitium.com/what-are-types-of-detection/