Title: Cybersecurity in Action: Constructing and Compromising a Secure Network Environment

Author: Asagba Jeremiah Ayomide
Date: 8-04-2024

Abstract

This report documents a step-by-step journey of setting up a virtualized network environment, implementing an Active Directory infrastructure, conducting brute force attacks, and utilizing advanced monitoring tools to detect and analyze these attack patterns. It is a reflective narrative of the skills honed, the challenges faced, and the tools leveraged to understand the cybersecurity landscape from an attacker's and defender's perspective.

Objective

The goal of this project was to construct a simulated, secure network environment and observe firsthand the dynamics of cyber threats and defenses. By establishing an Active Directory structure and integrating Splunk for event monitoring, the project aimed to offer a tangible understanding of how various cybersecurity tools interact and how potential intrusions can be detected and analyzed within a controlled setting. The overarching objective was to craft an insightful narrative that could be shared to help others learn about the nuances of network security through practical engagement.

The importance of practical experience in cybersecurity cannot be overstated. While theoretical knowledge provides the foundational principles, hands-on application reveals the complexities and unpredictabilities of real-world systems. Such experience is invaluable, as it allows for a deeper comprehension of security concepts, encourages critical thinking, and fosters a problem-solving mindset that is crucial for any cybersecurity professional.

Skills Learned

- Network configuration and management.
- Active Directory setup and user management.
- Brute force attack methods and their signatures.
- Event logging and monitoring.
- Usage of the MITRE ATT&CK Framework for understanding threat models.

Tools Used

- VirtualBox for virtualization.
- Kali Linux for penetration testing.
- Windows Server 2022 and Windows 10 for setting up a target environment.
- Splunk for data aggregation and analysis.
- Hydra and Atomic Red Team for simulating attacks.

Steps Taken

Design and Visualization:

- Developed a comprehensive logical diagram to establish a clear vision of the data flow and overall structure of the project.

Virtual Environment Setup:

- Deployed all required virtual machines to create a diverse and interactive network.
- Executed network configuration to ensure all systems operate on the same NAT-Network, facilitating communication and internet access.

IP Configuration and Monitoring Infrastructure:

- Assigned static IP addresses to each virtual machine, adhering to the initial project design.
- Installed and configured Splunk on Ubuntu, along with the Splunk Universal Forwarder and Sysmon on Windows platforms for event monitoring.

Active Directory Installation and Configuration:

- Installed Active Directory on Windows Server and promoted it to a domain controller to manage network resources securely and efficiently.
- Organizational Structure and Access Management:
- Created organizational units representing different departments and provisioned user accounts, setting the stage for role-based access control.

Network Integration and Domain Connectivity:

- Seamlessly integrated the target Windows machine into the domain, consolidating the network and enabling centralized management.

Attack Simulation, Detection, and Learning:

- Executed a brute force attack using Hydra to test network defenses.
- Employed Splunk for the detection and analysis of attack patterns, facilitating a practical understanding of event logs and security breaches.
- Utilized Atomic Red Team for further attack simulations, enhancing detection capabilities.
- Expanded knowledge of key Windows event codes and the MITRE ATT&CK Framework, applying this to the threat simulation and detection processes.

Challenges Encountered:

The primary challenge encountered during the project was the initial use of Crowbar for a brute force attack. Crowbar was expected to run through a wordlist to attempt various login combinations; however, it failed to utilize the wordlist correctly and did not yield the expected results. This obstacle necessitated a shift in approach, leading to the adoption of Hydra, a more robust and reliable tool for this type of attack. The switch was not just a mere substitution of tools but also a learning moment that emphasized the importance of flexibility and adaptability in cybersecurity efforts.

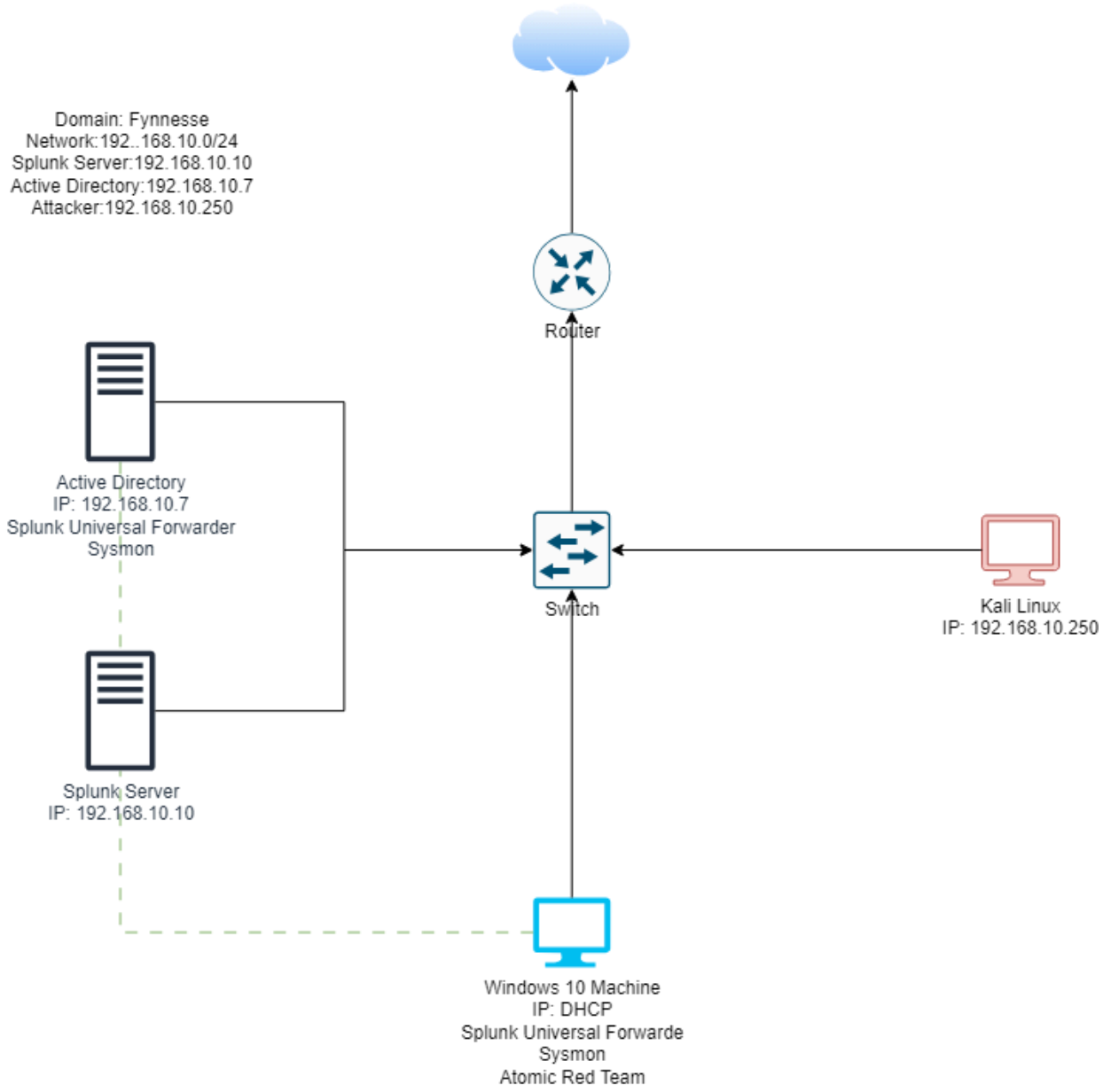
Conclusion:

The key takeaways from this project reinforce the notion that security is not a static field; it requires constant learning and adaptation. Tools and strategies must be continually evaluated and tested against emerging threats. The use of Hydra illustrated the critical need to select the right tools for specific scenarios, which could mean the difference between a breached and a secure system.

Moreover, this project showcased that practical, hands-on projects serve as excellent learning conduits, significantly enhancing one's understanding and skills in cybersecurity.

Appendices:

Logical Diagram



Scripts or Command lines that were crucial to setup.

PowerShell execution policy to Bypass for the current user, allowing them to run any PowerShell scripts without restrictions or warnings:
Set-ExecutionPolicy Bypass CurrentUser

Atomic Red Team Powershell Command:
https://raw.githubusercontent.com/redcanaryco/invoke-atomicredteam/master/install-atomicredteam.ps1. -UseBasicParsing);
Install-AtomicRedTeam -getAtomics

Sysmon Config:
https://raw.githubusercontent.com/olafhartong/sysmon-modular/master/sysmonconfig.xml

Splunk Inputs.conf:
https://github.com/Fynnesse/Active-Directory-Project/blob/main/Splunk%20Input.conf