Red Team / Blue Team Simulation Report

Project Overview

This simulation modeled an internal attack scenario using Red Team and Blue Team methodology. The Red Team, operating from a Kali Linux instance, attempted to infiltrate and exploit vulnerabilities in a target Ubuntu server. The Blue Team used Splunk and system logging to monitor, detect, and respond.

Environment Setup

- Red Team Machine: Kali Linux
- Target Machine: Ubuntu Server 20.04 with outdated services
- Defensive Tools: Splunk Universal Forwarder, syslog, custom alert rules
- Network: Isolated virtual network

Red Team Tactics

1. Reconnaissance: Used Nmap to discover open ports and services.
2. Vulnerability Analysis: Identified Apache 2.4.29 with known exploits.
3. Exploitation: Launched remote code execution using Metasploit.
4. Privilege Escalation: Exploited local kernel vuln to gain root access.
5. Persistence: Created new admin user and installed backdoor service.

Blue Team Monitoring & Response

1. Alerting: Detected suspicious Nmap scan activity in Splunk.
2. Log Analysis: Identified Metasploit connection and privilege escalation.
3. Response: Terminated unauthorized session, isolated host, and patched system.
4. Prevention: Deployed firewall rule to block future exploit attempts and updated alerting.

Mapped MITRE ATT&CK Techniques

- T1046: Network Service Scanning
- T1190: Exploit Public-Facing Application
- T1055: Process Injection
- T1078: Valid Accounts
- T1003: Credential Dumping

Indicators of Compromise (IOCs)

Red Team / Blue Team Simulation Report

- Nmap scan spikes from unknown host
- Unexpected Apache crash and respawn
- New local user with sudo privileges
- Outbound connection to port 4444
- Metasploit shell process fingerprint

Lessons Learned

This simulation highlighted the value of early detection, centralized log monitoring, and fast response playbooks. The Red Team was able to exploit outdated services, but the Blue Team successfully detected, contained, and remediated the attack.