PurpleOps-Playground — Blue Team Report

Ethical Hacker / Defender Analysis

Author: Bobo Nikolov | Date: 27-10-2025 | Status: Completed

Objective

Simulate an end-to-end cyber attack in an isolated environment to test blue team detection and analysis skills. The project demonstrates reconnaissance, initial access, execution, persistence, and privilege escalation, followed by detailed defensive analysis using Wazuh and Wireshark.

Architecture & Scope

Attacker: Kali Linux — IP: 10.10.10.10 (labnet). Tools: msfvenom, msfconsole, python3 -m http.server, nmap.
Victim: Ubuntu Desktop — IP: 10.10.10.20 (labnet / intnet). Tools: wget, chmod, bash, sudo. Wazuh agent installed; Wireshark capturing.
Network: Isolated internal network (no Internet). Snapshots taken before testing and reverted after.
Evidence storage: Projects/PurpleOps-Playground/ — screenshots, PCAPs, Wazuh alerts.

MITRE ATT&CK; Mapping (Defender Play-by-Play)

Tactic	Technique(s)	Defender Notes
Reconnaissance (T1595)	Nmap active scan (-sS -sV)	Detect port scanning and high SYN rate; alert on clu
Initial Access (T1190/T1204)	HTTP fetch of ELF payload; wget + chmod +x execute	Alert on wget/curl downloads followed by immediate
Execution (T1059/T1110/T1190)	Reverse shell; SQLi; brute-force attempts	Correlate suspicious command sequences and login
Persistence (T1136/T1547)	Created user + sudoers NOPASSWD entry	Monitor /etc/sudoers.d additions and unexpected us
Privilege Escalation (T1068/T1548)	Sudo /bin/bash to root	Alert on non-standard sudo shells and privilege char
Defense Evasion (T1562)	Logging gaps; missed file-download	Enable auditd/Sysmon-like logging and cross-correla
Credential Access (T1110)	Brute-force attempts	Rate-limit and alert on failed auth spikes.
C2 (T1071)	Meterpreter reverse TCP	Detect persistent reverse TCP to internal hosts and
Exfiltration (T1041)	Meterpreter file transfer	Add detection for abnormal outbound transfers and t

Timeline Summary

Phase	Time (UTC)	Defender Event	Artifact
Recon	22:29	Scan Detected	Wazuh, Wireshark
Initial Access	22:40	ELF download	Wireshark
Execution	22:41	SQLi / Brute Force	Wazuh
Persistence	22:45	sudoers file edit	Wazuh
Privilege Escalation	22:46	Root shell	Wazuh
C2	22:47	Reverse shell active	Wireshark

Lessons Learned & Mitigations

Missing detection on ELF download: Wazuh missed the binary fetch; add auditd exec logs for /tmp and correlate network/host events.
No reverse TCP alert: Add IDS signatures for reverse C2 patterns and implement internal network anomaly detection.
sudoers persistence detected: Continue monitoring sudoers.d and user creation events.
SQLi/Brute Force detected: Maintain thresholds and tune false positives; monitor web payloads for anomalies.

Disclaimer

All testing performed in an isolated lab environment for educational and ethical purposes only.

Report generated: 2025-11-11 13:22 UTC