HomeLab

Date: [YYYY-MM-DD] **Objective:** [e.g., Design, build, and secure a virtual environment for malware analysis.] **Components:** [List major systems, e.g., pfSense Firewall, Kali VM, Windows Server 2022 AD, Splunk SIEM]

?? Architectural Design

Provide a high-level overview (a diagram is best here, mentioned as an image).

Network Topology

- **VLAN 10 (Management):** [Description of access and purpose]
- **VLAN 20 (Target/DMZ):** [Where vulnerable targets or public services reside]
- **VLAN 30 (Analysis/SIEM):** [Where monitoring tools are isolated]

[Image of the network diagram/topology]

?? Security Control Implementation

Detail the specific defensive tools and configurations you implemented.

?? Perimeter Defense (pfSense/Firewall)

Control	Mechanism	Configuration Detail
IDS/IPS	**Snort/Suricata**	Configured ruleset for C2 and known exploit detection.
Egress Filtering	**Firewall Rules**	Blocking outbound traffic on non-standard ports (e.g., 25, 139, 445).
VPN Access	**OpenVPN**	Enforced 2FA and strong cryptography ($AES-256-GCM$).

? Monitoring & Logging (SIEM)

- **SIEM Used:** [Splunk / ELK Stack / Security Onion]
- **Data Sources:** Ingested logs from:
  - Active Directory (Security Event Logs)
  - pfSense (Firewall logs)
  - Endpoint Protection ([e.g., Sysmon on Windows])
- **Detection Rules Created:** [e.g., "Alert on 10+ failed login attempts within 60 seconds."]

? Testing and Validation

How did you ensure the defenses were working?

- **Testing Method:** [e.g., Ran a controlled **Metasploit** attack from the Kali VM to the Target VM.]
- **Validation:** [e.g., "Confirmed that the Snort IDS successfully blocked the initial exploit attempt and logged the traffic."]
- **Post-Mortem:** [e.g., "Found a bypass path, requiring a rule change in the firewall."]

? Technical Learnings

- [Specific command or configuration learned, e.g., "Mastered the use of `rsyslog` for centralized logging."]
- [Insight into enterprise-level challenges, e.g., "The difficulty of correctly tuning SIEM rules to avoid false positives."]

Revision #1
Created 2025-12-02 17:05:49 UTC by David Rizzo
Updated 2025-12-02 17:06:03 UTC by David Rizzo