REPORT (SANS Template)

Executive Summary:

On 12 September 2025 at 17:23, Zeek network sensors observed anomalous FTP activity from 192.168.1.39 targeting Metasploitable2. Analysis of Zeek ftp/conn logs revealed the vsftpd_234_backdoor exploit pattern, indicating a successful remote exploit. The instance was isolated and the attacker IP was blocked; no lateral movement to other VMs was observed.

Timeline:

• 17:23 — Zeek conn/ftp logs show suspicious control commands and a backdoor connection attempt.
• 17:23 — Kibana alert triggered for high-frequency FTP sessions + unusual payload.
• 17:23 — Compromised VM network interface disabled and VM snapshot taken.
• 17:25 — CrowdSec decision added (manual ban) and firewall rule applied to block attacker IP.
• 17:26 — Verification tests confirm attacker IP cannot reach VM; logs archived.

Impact & Findings:

The exploit targeted a known vsftpd backdoor (T1190). Only the Metasploitable2 VM showed compromise; no data exfiltration was observed in the captured session metadata. Root cause: vulnerable service exposure combined with missing virtual network segmentation for test VMs.

Recommendations:

- Remove/patch vulnerable services; replace Metasploitable2 with isolated lab network behind a dedicated VLAN.
- Harden monitoring: create persistent Kibana detection rules for FTP anomalies and signature-based checks.
- Integrate automated playbook to isolate compromised hosts and add CrowdSec decisions from Kibana alerts.