Makara Ramoabi

20240045

Security

1. DDoS Attack Scenario

A mid-sized e-commerce company, ShopSecure, faces a massive DDoS attack during its peak holiday sales. Hackers, motivated by extortion, commandeer a botnet of 100,000 compromised IoT devices worldwide to flood ShopSecure's servers with volumetric UDP floods exceeding 500 Gbps. Within minutes, legitimate customer traffic is choked, causing website crashes, abandoned carts, and $2 million in lost revenue over 12 hours. Internal teams scramble as application-layer attacks mimic real user requests, evading basic firewalls. Customers rage on social media, stock plummets 15%, and competitors capitalize. Recovery demands cloud scrubbing services, revealing unpatched edge servers as the entry point. This underscores the need for always-on mitigation and redundancy.

2. Ransomware Threat Summary

Ransomware encrypts critical files, demanding payment for decryption keys, crippling operations across sectors like healthcare and finance. In 2025, attacks like LockBit 4.0 caused global outages, with average costs hitting $4.88 million per incident, including downtime, recovery, and fines. Impacts include data theft for double extortion, supply chain disruptions, and eroded trust. Mitigation involves regular offline backups, patch management, endpoint detection tools, network segmentation, and employee phishing training. Zero-trust architecture limits lateral movement, while AI-driven behavioral analytics flags anomalies early. Never pay ransoms, as it funds further crimes.

3. Tool Practice Reflection

In Wireshark, I analyzed a sample PCAP of suspicious HTTP traffic simulating a malware C2 beacon. Filters like "http.request.method == POST" revealed anomalous User-Agents and base64-encoded payloads in requests to a shady domain. Timestamps showed rhythmic intervals (every 60s), indicative of beaconing. Cross-referencing with tcp.stream revealed sustained sessions bypassing firewalls. This exercise highlighted Wireshark's power for deep packet inspection—extracting payloads via "Follow TCP Stream" exposed commands like "exfiltrate data." Challenges included noise from legit traffic; practicing Lua dissectors improved custom parsing. Kali's Nmap scan simulation (nmap -sV -A target) complemented by identifying open

RDP ports vulnerable to brute-force. Key takeaway: Integrate tools in incident response workflows for faster triage.

4. Threat Diagram Explanation

Imagine a Canva diagram for DoS protection: Central "Web Server" orbited by threat vectors (volumetric floods, SYN floods) blocked by layered defenses—a WAF perimeter filtering malicious IPs, CDN absorbing traffic, and IDS/IPS core engine with rate limiting. Arrows show scrubbed traffic rerouted to legit users via cloud mitigation service. Bottom flow: Incident detection → Auto-scale → Blackholing → post-attack forensics.

This visual map the kill chain: Attackers → Botnet → Target, intercepted by proactive controls. It emphasizes redundancy—e.g., BGP anycast for geo-distribution—reducing downtime by 90%. Stakeholders use it for audits, proving compliance with NIST frameworks. Simple icons (shields, locks) aid non-tech reviews.