Como Identificar um Ataque DDoS

Guia de Detecção de Ataque DDoS

Sinais comuns de um ataque DDoS:

1. Alta carga repentina da CPU

   - Exemplo: CPU / 95% com system: 70% ou iowait alto.

2. Aumento do load average

   - LOAD 1 min: 8.5 em máquina de 4 núcleos = carga excessiva.

3. Uso de memória anormal

   - MEM - 90%, mesmo com poucos processos ativos.

4. Alto número de conexões de rede (SYN ou UDP)

   - Use: netstat -an | grep :80 | wc -l ou ss -s

5. Picos no tráfego de rede

   - Ferramentas: iftop, vnstat, nload

6. Muitos context switches (ctx_sw) ou interrupções (inter)

   - ctx_sw: 50K ou inter: 20000+ indicam sobrecarga.

7. Serviços lentos ou indisponíveis

   - Lentidão ou falha em acessar web, API, SSH, etc.

Ferramentas para detectar DDoS em tempo real:

- iftop: sudo iftop
- nethogs: sudo nethogs
- ss: ss -ant

Como Identificar um Ataque DDoS

- netstat: netstat -an | grep :80

- htop: htop

- tcpdump: sudo tcpdump -n port 80

Como agir se estiver sofrendo DDoS:

1. Bloquear IPs suspeitos:

   sudo iptables -A INPUT -s 123.45.67.89 -j DROP

2. Limitar número de conexões:

   sudo iptables -A INPUT -p tcp --syn --dport 80 -m connlimit --connlimit-above 30 -j DROP

3. Usar firewall e rate limiting:

   - fail2ban, ufw, nginx/apache

4. Mitigação em camada superior:

   - Cloudflare, Imperva, AWS Shield