Relatório de Incidente de Segurança Cibernética

# 1. Resumo Executivo

Clientes não conseguiam acessar www.yummyrecipesforme.com. A análise do tcpdump mostrou que as consultas DNS (UDP/53) falharam, recebendo mensagens ICMP “udp port 53 unreachable”. Portanto, o serviço DNS estava inacessível, impedindo a resolução do nome e, consequentemente, o acesso ao site.

# 2. Linha do Tempo (carimbos do log)

13:24:32.192571 – Envio de consulta DNS (UDP/53) para 203.0.113.2.

13:24:36.098564 – ICMP de 203.0.113.2 → 192.51.100.15: udp port 53 unreachable.

13:26:32.192571 – Nova tentativa DNS.

13:27:15.934126 – Novo ICMP com o mesmo erro.

13:28:32.192571 – Terceira tentativa DNS.

13:28:50.022967 – Terceiro ICMP com o mesmo erro.

# 3. Impacto

Falha geral de resolução de nome para o domínio analisado.

Usuários não conseguem carregar a aplicação web (HTTPS nunca é estabelecido).

# 4. Protocolo/Serviço Afetado

DNS (UDP/53).

# 5. Protocolo Observado para Avaliação

ICMP, que retornou a mensagem de erro “udp port 53 unreachable”.

# 6. Causa Provável

Uma (ou mais) das hipóteses abaixo:  
- Serviço DNS no host 203.0.113.2 está parado.  
- Firewall/ACL bloqueando UDP/53.  
- Roteamento incorreto até o servidor DNS.  
- Rate limiting / mitigação DDoS configurada incorretamente.

# 7. Recomendações

- Verificar se o daemon DNS (ex.: named, bind, unbound) está em execução no 203.0.113.2.  
- Checar firewall/ACL/NACL/Security Groups para garantir que UDP/53 esteja liberado para as origens corretas.  
- Testar DNS por TCP (porta 53) como fallback e habilitar no servidor (alguns resolvers tentam TCP quando o UDP falha).  
- Configurar servidores DNS redundantes/ secundários e apontar os clientes para eles.  
- Monitorar com alertas (Zabbix, Prometheus, CloudWatch, etc.) para indisponibilidade de portas/serviços críticos.  
- Registrar métricas e logs (falhas ICMP, quedas do serviço) para resposta mais rápida em incidentes futuros.

# 8. Próximos Passos

Acionar a equipe de infra/segurança para corrigir a disponibilidade do DNS/UDP/53 no 203.0.113.2.  
Validar com dig/nslookup após o ajuste.  
Documentar a mudança e implementar check de saúde contínuo do serviço DNS.