Relatório de incidente de segurança #2

Seção 2: Identifique o protocolo de rede envolvido no incidente
Os protocolos de rede envolvidos no incidente são o Domain Name System (DNS), que é usado para mapear nomes em endereços IP e vice-versa , e o Hypertext Transfer Protocol (HTTP) um protocolo de rede utilizado para comunicações na web.

Seção 2: Documente o incidente
A tarde recebemos reclamações no helpdesk onde os clientes afirmaram que ao acessar o site da empresa, ele foi levado a baixar um arquivo e após isso seu computador começou a apresentar lentidão. Ao ser designado a investigar o incidente, utilizei o analisador de protocolo de rede, tcpdump e acessei o site da empresa. Ao investigar os registros, foi identificado o tráfego de pacotes DNS e HTTP. Além do tráfego normal de DNS para o site da empresa, foi encontrado um redirecionamento para um site malicioso. Logo, é evidente que um agente de ameaças conseguiu acesso ao sistema e injetar código malicioso.

Seção 3: Recomendo uma medida de remediação de tentativas de ataques brutos
O incidente foi causado por uma vulnerabilidade no acesso ao sistema, logo é preciso reforçar as senhas por meio de: - Senhas mais fortes - Autenticação de dois fatores (2FA)