Security incident report

Section 1: Identify the network protocol involved in the incident
O Protocolo de rede envolvido no acidente foi o Protocolo de Controle de Transmissão(TCP), pois há comunicação entre dois dispositivos continuamente, e de maneira maliciosa.

Section 2: Document the incident
O Usuário com o IP 14:18:36.786501, your.machine.52444, Faz um ataque de força bruta, tentando várias senhas comuns que ele sabia que utilizamos, após dois minutos de tentativas ele conecta, e monta o código de pedido de download, fazendo o browser pedir dados para o nosso site, provavelmente o pedido do arquivo malicioso, Agora os logs mostram outro pedido para o server DNS, um pedido de encaminhamento de tráfego para outro endereço IP: 192.0.2.172 e a url associada com o endereço: greatrecipesforme.com.http, o pedido é aceito e o tráfego muda a rota entre o computador de origem e o site falsificado (tráfego de saída: IP your.machine.56378 > greatrecipesforme.com.http e tráfego de entrada: greatrecipesforme.com.http > IP your.machine.56378), redirecionando o site original para o site com malwares.

Section 3: Recommend one remediation for brute force attacks
• Monitoração de logins de entrada • Mudança na política de senhas da empresa. • Limitando o número de tentativas de login erradas.