DETECÇÃO DE TÚNEIS SOBRE O MÉTODO CONNECT DE PROXIES WEB

Nivio Paula de Souza, Academia Militar das Agulhas Negras
Antonio Cesar Carneiro Brandão, Academia Militar das Agulhas Negras

Resumo: As redes de dados estão sujeitas a várias ameaças quanto à segurança. Pesquisadores e profissionais da área se debruçam sobre o problema na tentativa de garantir confidencialidade, integridade, irretratabilidade e autenticidade nas transações eletrônicas. Este pôster trata do estabelecimento de conexões através de servidores proxy, criando túneis que utilizam o método CONNECT do protocolo HTTP, permitindo que outros protocolos trafeguem indevidamente entre a rede externa e a rede interna. O próprio usuário da rede interna ou um atacante poderiam usar essa técnica; para este acessar reversamente a rede interna, objetivando o roubo de informações, o controle de computadores, servidores da rede e outros; e para aquele acessar conteúdo proibido pela política de segurança estabelecida para uma rede. Foi realizado um experimento que analisa o código fonte de algumas aplicações, para verificar o funcionamento de túneis sobre o método CONNECT de proxies web, sua detecção e bloqueio, de forma a contribuir com o aumento das restrições a conexões não autorizadas que burlem as políticas de segurança.