**MITM**

**1) O que é man in the middle?**

**R:** O ataque Man-in-the-Middle (MITM) é uma técnica em que um invasor intercepta e possivelmente altera as comunicações entre dois dispositivos sem o conhecimento deles. O atacante age como um intermediário nas comunicações, podendo capturar informações sensíveis, como senhas e dados confidenciais.

**2) Qual é o software usado como demonstração no artigo?**

**R:** O software utilizado para demonstração no artigo é o "Cain & Abel".

**3) Qual a diferença de um tráfego regular e um tráfego envenenado de uma rede?**

**R:** O tráfego regular em uma rede ocorre normalmente, sem interferências maliciosas. Já o tráfego envenenado ocorre quando um atacante manipula o fluxo de dados na rede, por exemplo, através de ataques como ARP Cache Poisoning, DNS Spoofing, entre outros.

**4) Quais as principais características do software usado no artigo?**

**R:** O Cain & Abel é um software projetado para monitorar o tráfego, capturar pacotes de dados, verificar sua confiabilidade e recuperar senhas em sistemas Windows. Ele possui funcionalidades como quebra de senhas, captura de tráfego de rede, recuperação de chaves de rede sem fio, entre outras.

**5) Quais protocolos se mostram vulneráveis segundo o artigo para a captura de senhas?**

**R:** O artigo menciona que o programa Cain & Abel pode hackear senhas de vários protocolos, incluindo APOP-MD5, Cisco IOS-MD5, Cisco PIX-MD5, CRAM-MD5, Hashes de banco de dados Oracle e SIP, Kerberos 5, LM e NTLM, MADURA MD-160, MD2, MD4, MD5, MSSQL, MySQL, NTLMv2, OSPF-MD5, RIPv2 MD5, SHA-1, SHA-2 e VNC Triplo DES - HMAC.

**6) O programa usado nos testes se divide em duas partes? quais são elas e quais suas funções?**

**R:** Sim, o programa Cain & Abel se divide em duas partes: Cain, responsável por quebrar senhas, e Abel, um serviço do Windows NT que protege o envio de senhas em redes locais. Cain & Abel é usado para monitorar o tráfego, capturar pacotes de dados e verificar a confiabilidade, sendo útil para profissionais de segurança, administradores de rede, entre outros.