Assinatura do Ataque Teardrop no Wireshark

Descrição do Ataque

- Atacam SOs mais antigos como Windows 95, Windows NT e versões anteriores do Linux. Foram detectados no Windows 7 e Vista, mas já foram corrigidos na versão 8;
- Ataque de negação de serviço (DoS);
- Caso o tamanho de um pacote seja maior que UMT (Unidade Máxima de Transmissão), ele deve ser fragmentado para depois os fragmentos serem reorganizados no destino para reproduzir a mensagem ou dados originais. O Teardrop explora as vulnerabilidades na recuperação de fragmentos de pacotes IP;
- Nesse caso, o campo de deslocamento do cabeçalho IP (que mantém as informações de uso necessárias para que a máquina destino organize os fragmentos), chamado campo offset, torna-se defeituoso e a máquina destino não consegue encontrar as peças relevantes;
- Nesse ataque, os pacotes ficam com defeitos e o aparelho destino não consegue remontar os pacotes devido a um erro na fragmentação TCP/IP. Assim, os pacotes continuam se acumulando na máquina e esta trava com um estouro do buffer;
- O ataque cria uma série de fragmentos IP com campos de deslocamento sobrepostos e quando reunidos na máquina destino, pode travar ou reiniciar a máquina.

Assinatura (Wireshark)

- Foram elaboradas duas assinaturas:

ip.flags.mf == 1 or ip.frag_offset gt 0

ip.flags.mf == 1 or ip.frag_offset gt 0 and udp.length.bad