Abstrakt Cílem této práce je prozkoumat problematiku detekce útoků na počítačové systémy a vytvořit jednoduchá pravidla, která jsou schopna detekovat jednotlivé útoky. Útoky jsou prozkoumány na realistickém datasetu CSE-CIC-IDS2018. Nejprve se práce zabývá analýzou datasetu. V analýze jsou spočítány různé statistiky datasetu a na závěr jsou otestované různé metody redukce dimenzí pro zobrazení dat v dvou demenzionálním prostoru. Po analýze následuje příprava a normalizace dat. Proces trénování se pak zaměřuje na výběr vhodných příznaků a hledání nejlepšího modelu. Stejné příznaky jsou pak použity i pro vytváření pravidel. Pravidla jsou extrahována ze souboru rozhodovacích stromů. V závěru práce jsou pravidla porovnána s nejlepším modelem. Experimenty ukazují, že jednoduchá pravidla jsou schopna dosáhnout podobných výsledků jako nejlepší model. Mohou být použita v pravidlových systémech pro detekci útoků nebo nasazena jako jednoduchý model.