Безпека операційних систем і комп'ютерних мереж

Лекція 15

Анотація

Лекція присвячена можливим атакам на на протоколи ICMP, SNMP і DNS. Один з варіантів атаки — це передача пакета зловмисником від імені одного з учасників з'єднання або встановлення з'єднання від імені іншої хоста. Також проілюстрована атака Митника, наведено приклади використання можливостей протоколу ICMP для розвідки і атаки, а саме: атака Smurf, атака Tribe Flood Network, атака WinFreeze, а також програма Loki - найнебезпечніший спосіб експлуатації можливостей ICMP. Для протидії атакам і просочування інформації наведено детальні рекомендації, що відносяться до блокування ICMP-трафіку. Також в лекції розглянуто протокол SNMP, його переваги і недоліки, і як можна убезпечити його використання. Описується протокол DNS і можливі сценарії атак на нього.