УДК 621
Дзядик В.Я.– ст. гр. КСМм-51
Тернопільський національний економічний університет

ДОСЛІДЖЕННЯ СТІЙКОСТІ КОМПЮТЕРНИХ МЕРЕЖ ДО АКТИВНИХ АТАК

Науковий керівник: к.т.н., доц. Паздрій І.Р.

Показано, що активні атаки можуть набирати різних форм. Існують три загальні типи цих атак з точки зору їх здійснення: знищення обмеженого або невідновлюваного мережевого засобу, знищення чи зміна конфігураційної інформації, фізичне знищення чи зміна елементів КМ.

Згідно з вищенаведеним можна провести наступний поділ атак DoS: атаки, що грунтуються на імплементації протоколів TCP/IP, атаки які базуються на стандарті TCP/IP, атаки, що використовують обмежені мережеві засоби. Серед атак DoS можна виділити такі.

1. Атака Ping of Death. Специфікація TCP/IP регламентує пакети з максимальною довжиною 65536 байт, які містять мінімум 20 байт інформаційного заголовку IP, 0 чи більше байт додаткової інформації. Якщо операційна система пристрою відбере пакети, що виходять за дані межі, то може спричинитися аварія - зависання чи рестартування системи. Найчастіше атакам цього типу піддаються пристрої, що містять операційні системи класу Unix, а також пристрої такі як маршрутизатори, принтери, тощо.

2. Атака Teardrop.Атака використовує недосконаліть процесу складання фрагментів пакету IP. В атаці Teardrop навмисно створюються фрагменти, в яких зсув зумовить їх накладання. Якщо операційна система намагається поскладати всі фрагменти, то виникає аварійна ситуація чи зависання.

3. Атака SYN Flood. Атака використовує недосконаліть протоколу TCP, яка виникає в процесі нав'язування "напіввідкритого" з'єднання. Під потенційною загрозою є кожна приєднана до Інтернету система, що ґрунтується на послугах TCP. Крім цього ціллю атаки можуть бути маршрутизатори чи інші спеціалізовані пристрої.

4. Атака Smurf використовує недосконаліть розголошувальній адресації, а також пакет ICMP для її здійснення. В КМ пакет може потрапити безпосередньо до адресованого комп'ютера чи до всіх пристроїв в КМ. Зловмисник висилає розголошувальний пакет, а потім маршрутизатор його перепускає і спрямовує до сегменту КМ, де мережевий комутатор розсилає його до кожного пристрою. Пристрої відповідають зворотнім повідомленням на адресу жертви. Слід відзначити, що генерований рух впливає не лише на жертву, але також на маршрутизатор.

5. Атака Fraggle подібна do атаки Smurf, за винятком застосованого протоколу для здійснення атаки. Замість протоколу ICMP і повідомлення *Echo Request* використано протокол UDP для висилання пакету UDP *Echo*. Не дивлячись на те, що ця атака не є настільки ефективною в порівнянні з іншими атаками цього типу, однак вона зумовлює генерування інтенсивного руху в КМ до комп'ютера жертви, з метою заблокування йому доступу до КМ. Зловмисник, який знає про те, де можна вислати в КМ розголошувальні пакети, висилає пакет UDP *Echo*. Результат атаки є такий самий як і в випадку атаки Smurf – призводить до заблокування КМ і заблокування доступу до послуг атакованих пристроїв.