УДК 004.056

ВРАЗЛИВОСТІ ОПЕРАЦІЙНИХ СИСТЕМ ТИПУ UNIX

Губрій М.О.
Науковий керівник – доц. , к.т.н. Войтович О.П.

На теперішній час Unix-системи дуже поширені – вони використовуються як в класичних комп'ютерних системах, так і в різних нетрадиційних застосуваннях на зразок побутової техніки. Все частіше виникають випадки атак на ці системи, наприклад в телевізорі з камерою є можливість слідкування за приміщенням, в якому знаходиться це обладнання. Такі атаки спричинені парадигмою, що встановилась в сучасних інформаційних системах, де доступність переважає над конфіденційністю. Отже є велика необхідність впровадження систем забезпечення безпеки.

Система UNIX проектувалася як розвинена, продуктивна, багато користувацька операційна система. Забезпечення безпеки не було ключовою вимогою до системи.

Логічна послідовність виконуваних зломщиком дій полягає в проникненні за допомогою віддаленого доступу, використовуючи будь-які вади в захисті служби, що знаходиться в стані очікування запитів, з наступним отриманням локального доступу до командної оболонки. Першим кроком зловмисника є дослідження операційної системи і складання схеми вразливих місць.

Складання схеми вразливих місць - це процес знаходження відповідності між певними атрибутами безпеки системи з відповідними явними або потенційними вадами.

Можливими методами складання схеми вразливих місць можуть бути застосування загальнодоступних спеціальних інструментів або написання власного програмного коду, використання коштів, призначених для автоматичного сканування систем у пошуках уразливих місць, визначення вручну, як співвідносяться певні атрибути системи з інформацією про виявлені недоліки.

Основними причинами вразливостей є погано написані програми, наявність демонів, небезпека застосування атрибутів SUID/SGID, людський фактор.

Віддалений доступ визначається як доступ до системи, одержуваний по мережі або з інших комунікаційних каналах.

Основними методами для віддаленого проникнення є проникнення через службу, що знаходиться у стані очікування запитів, використання у якості плацдарму системи UNIX, яка забезпечує безпеку двох або більше мереж, застосування методів віддаленого злому, які мають на увазі приховане залучення користувачів.

Про локальний доступ говорять в тих випадках, коли в розпорядженні зломщика вже є інтерактивний доступ до командної оболонки або обліковий запис для реєстрації в системі.