*Лекція № **14**.*
ТЕЗИ

Питтання мережевої безпеки

Питання безпеки, безумовно, починають набирати багато більшої ваги для комп'ютера, підключеного до мережі. Згадаймо першу лекцію — від роботи мережевого адміна залежить багато біьше ніж тільки робота його комп'ютера.

“Справді безпечною можна вважати хіба що систему, яка виключена, замурована в бетонний корпус, закрита в приміщенні з свинцевими стінами, охороняєься озброєним караулом, - але і в цьому випадку сумніви не полишають мене...”
Юджин Х. Спаффорд

Аналогія з автострадою (закриваємо двері на ключ, а не забарикадовуємо вулиці) — іншими словами ціна нашої присутності в мережі: ми плтимо тим, що повинні думати про безпеку.
Аналогі з житлом у малому селі, де двері можна і не закривати взагалі, і з житлом в мегаполісі: Інет колись був “містечком” а зараз - “мегаполіс”.

Мережа зараз — назагал агресивне середовище. Тому ніколи не можна ігнорувати питання безпеки. Безпека, однак, коштує як грошей так і потребує інтелектуальної роботи, тому нею досить часто жертвують в догоду іншим видам діяльності.
Однак ліки не повинні бути гіршими від хвороби і параноїдальне ставлення до питань безпеки — це інша крайність.
Тут найкраща порада - користуватися здоровим глуздом.

За останні роки характер атак на системи змінився з деструктивного на такий, який своєю метою ставить використання систем в несанкціонованих цілях та отримання конфіденційної інформації.
BotNets — бот-мережі — мережі зомбованих комп'ютерів.
Розвиток і використання таких мереж — серйозний бізнес в криміналізованому середовищі. З метою розширення таких мереж невідомі “дірки” в програмному забезпеченні зараз навіть продаються і купуються.
Більше того, величезні бази даних офіційно опублікованих експлойтів, дають сьогодні змогу здійснити атаку фактично навіть слабо підготовленій в цій області людині.

Кожна, навіть найменша, організація на сьогоднішній день повинна мати (розробити) ***свій план дотримання безпеки*** в роботі з елетронними видами інформації, в роботі з мережею.
Найчастіше розробка такого плану — робота мережевого адміністратора.
Такий план допоможе в першу чергу вирішити ЩО потрібно захищати, ЯК (похідне від що) і ХТО має відповідати за безпеку.

Перший крок в розробці такого плану — ***оцінка загрози.***
RFC 2196 (Site Security Handbook) описує три види загроз, пов'язаних з підключенням до мережі:

- ***несанкціонований доступ***
- ***розкриття інформації***

- ***відмова в обслуговуванні (DoS — Denial of Service)***

Всі ці загрози слід оцінювати відносно кількості користувачів, яких можуть заторкнути потенційні проблеми, а також ступенем секретності інформації, яка потенційно може бути розкрита.

Ще одна, інша класифікація загроз:
- ***загрози секретності***
- ***загрози доступності***
- ***загрози цілісності даних***

Зрозуміло, що самими мережевими загрозами справа не обмежується (хоча дійсно, мережа є серйозним джерелом загроз для комп'ютерних систем).
Не менш серйозними причинми втрати інформації є також
- **причини фізичного характеру** (пожежі, збої апаратної частини і т.д.)
- **людський фактор** — цей найбільше (кражі, роздачі паролів, безпечність, нехлюйство, некомпетентність і т.д.)

Тут ми говоритимемо виключно про **мережеву безпеку**.

Існує два принципово різні (часами навіть несумісні) підходи до організації мережевої безпеки:
- централізація управіління мережею
- розприділене управління мережею

Переваги і недоліки є у обох:
зокрема мережі із своїм поділом на підмережі в принципі дуже добре надаються до розприділеного управління і розприділення відповідальності (кожна підмережа — свій адмін). З іншого боку, якщо компетентності “на місцях” недостатньо, то краще (і набагато легше) управляти мережею централізовано. Має значення також розмір мережі.

Перевірка автентичності користувачів.

Користувачі і їх паролі — перше, на що сисадмін повинен звернути увагу.
Часто для проникнення в систему навіть не треба паролі красти, бо:
- буває пароль співпадає з ім'ям користувача (joe passwords -”тупі” паролі)
- існують гостьові або демонстраційні аккаунти без паролів або з широко відомими (опублікованими) паролями
- існують системні аккаунти з паролями по замовчуванню (особливо стосується наприклад СУБД)
- користувачі просто повідомляють свій пароль стороннім людям

Кожна відкрита в мережі система РЕГУЛЯРНО сканується зловмисниками на предмет таких (і інших — див нижче) доступів. На нашому студентському сервері можна це дуже добре бачити в логах (/var/log/messages)

Паролі також підбираються на основі або словника або конкретної інформації про користувача.
Тому зокрема в UNIX паролі як правило виненсені з файлу /etc/passwd в т.зв. “тіньовий” файл (etc/shadow, /etc/master-passwd etc.) - на даний момент є програми з допомогою який можна таким способом “зламати” більшість паролів в системі взагалі (питання тільки в обч. ресурсах і часі).

В UNIX існує також ***механізм застарівання паролів*** і примусової їх зміни — тут теж важливо не переборщити.

Існує також механізм ***одноразових паролів*** (як апаратні так і програмні рішення).

Багато аплікацій (сервісів) можуть використовувати і власні паролі.

Згідно деяких протоколів паролі можуть передаватися відкритим текстом — тоді вони можуть бути перехоплені аналізаторами трафіку (напр утилітою tcpdump — див. Лабораторні)

Безпека на рівні аплікацій

полягає в

- видаленні непотрібних програм
- регулярному оновленні програм, бібліотек та й самої ОС

Більшість успішних атак використовують дірки в програмному забезпеченні.

Сис адмін повинен регулярно отримувати інформацію про оновлення для його програмного забезпечення а також інформацію про дірки в програмному забезпеченні.
BugTrack
securityfocus
Як правило експлойти публікуються після того, як виробник випускає патч на проблему, тому важливо бути в курсі і оновлюватися в залежності від критичності проблем.

Спостереження і регулярний аудит системи

Журнальні файли (lastlog, messages, maillog, httpd-logs і т.д.) слід переглядати регулярно.

Сисадмін повинен також знати які прощеси мають працювати на сервері і для чого.

Повинна відслідковуватись також активність користувачів.

Завантаженість системи теж має відслідковуватись.

Зловмисники можуть залишати на сервері т.зв. BackDors - “лазейки”, через які повторний доступ до системи їм буде гарантовано.
Тому повинні відслідковуватись також зміни в файловій системі на пердмет su exec файлів (таких, як /bin/passwd).

Більшість UNIX-систем мають скріпти для щоденного та щомісячного аудиту. Результат їх виконання (щоденно, через cron) відправляється на e-mail адміну.

Обмеження доступу

як

- ***на основі засобів, які є вбудовані в окремі сервіси,***
- ***на рівні мережевої системи: файрвол (брандмауер), wrapper, файли hosts.alow, hosts.deny***

Файрволи в linux — iptables, ipchains, в FreeBSD — ipfw. Є також інші.
Файрвол являє собою не що інше, як просто пакетний фільтр. На основі правил, створених адміністраторм, певні ***tcp/ip/icmp/udp*** і т.п. пакети пропускаються далі по стеку, а певні — ні (торхи грубо). Ці правила пишуться адміністратором, зазвичай. Зрозуміло, що ці правила використовують інфо з заголовків пакету.
В сучасних лінуксах для полегшення роботи адміна з файрволом створені скріпти, які генерують правила на основі файлу конфігурації файрволу, але суті роботи з фільтром це не міняє. Фільтри також часто використовують для збору статистичних даких (зокрема з метою білінгу — обліку трафіку)

Шифрування

Шифрування трафіку використовується зараз дуже широко.
Однак воно теж не вирішує всіх проблем, пов'язаних з безпекою.

Історично першим в мережі приміненим було т.зв. шифрування на основі закритого ключа — коли обидві сторони (і відправляюча-шифруюча і приймаюча-дешифруюча) користувалися одним ключам.
Шифрування, яке вимагає попереднього узгодження і використання секретного ключа, називається ***симетричним***.

Зараз найширше використовується ***шифрування на основі відкритого ключа,*** коли дані шифруються-розшифровуються ***на основі пари публічний-приватний (ще називають відкритий-закритий) ключ***.
Публічний ключ є у відкритому доступі (часто в загальнодоступних базах даних в Інет) а приватний зберігається виключно власником секретно.
Будь-хто може зашифрувати інформацію, але розшифрувати може тільки той, чиїм публічним ключем зашифрували: робить це з допомогою свого приватного ключа.

Таке шифрування, що використовує для кодування-розкодовування різні ключі, називається ***асиметричним***.
Воно більш вимогливе до системи в плані ресурсів.

Використовується як для шифрування самих даних, ***так і для перевірки аутентичності в процесі встановлення з'єднання*** (сервери обмінюються між собою загальним приватним(закритим) ключем, шифруючи його своїми публічними ключами).

ssh, SSL працюють на основі асиметричного шифрування.

VPN

Віртуальні приватні мережі.

Правила:
-- знай свою систему
-- не довіряй користувачам
-- система повинна бути відкитою рівно на стільки, наскільки потрібно для робот її служб
-- вся не необхідна стороннім інформація доступною бути НЕ повинна