Безпека операційних систем і комп'ютерних мереж

Лекція 15

Безпека протоколів стеку TCP/IP (продовження теми)

Питання

- Безпека протоколів керування
  - ICMP
  - SNMP
- Безпека DNS

Протокол ICMP

- Протокол ICMP (Internet Control Message Protocol — протокол повідомлень керування Інтернету) був задуманий і розроблений як простий та безпечний засіб для повідомлень про помилки і для обміну повідомленнями типу запит-відповідь
  - Протокол описаний у RFC 792, деякі доповнення зроблені у RFC-4884
- У своєму природному вигляді ICMP є простим протоколом з чітко визначеними правилами використання
  - Цей протокол (зокрема, правила його застосування) може бути дещо модифікованим і в такому вигляді використаним порушниками
  - Тому важливо розрізняти нормальне та нестандартне використання цього протоколу

Використання ICMP з метою розвідки (1/3)

- Це потребує лише стандартних повідомлень протоколу
- Для визначення активності конкретного хосту, достатньо одержати від нього одне з таких ICMP-повідомлень:
  - “protocol unreachable”;
  - “port unreachable”;
  - “IP reassembly time exceeded”;
  - “parameter problem”;
  - “echo replay”;
  - “timestamp replay”;
  - “address mask replay”.

Використання ICMP з метою розвідки (2/3)

- Деякі ICMP-повідомлення відправляють лише маршрутизатори. Тому одержання одного з таких повідомлень дозволяє визначити маршрутизатор мережі:
  - “fragmentation needed but don't-fragment bit set”;
  - “admin prohibited”;
  - “time exceeded in transit”;
  - “network unreachable”;
  - “host unreachable”.
- Якщо маршрутизатор мережі буде повідомляти відправника про помилки недосяжності деяких хостів (**host unreachable**), то, припустивши активність усіх інших хостів, можна скласти схему мережі

Використання ICMP з метою розвідки (3/3)

- Додаткову інформацію можна отримати з таких ICMP-повідомлень:
  - “admin prohibited” — дозволяє дізнатись про тип блокованого трафіка;
  - “address mask replay” — надає значення маски підмережі, в якій встановлений запитаний хост;
  - “time exceeded in transit” — використовується утилітою traceroute для визначення IP-адрес маршрутизаторів і топології мережі;
  - “protocol unreachable” може використовуватись для повного сканування хосту щодо задіяних служб;
  - “port unreachable” може застосовуватись для виявлення активних хостів з відкритими UDP-портами;
  - “fragmentation needed but don't-fragment bit set” дозволяє визначити значення MTU мереж з метою проведення атаки при використанні фрагментованого трафіка.

Атака Smurf (1/2)

- Атака Smurf базується на використанні можливості протоколу ICMP розсилати дейтаграми за кількома адресами
  - Відповісти на один широкомовний ехо-запит ICMP (ping) може велика кількість хостів.
  - Ця можливість використовується для проведення атаки відмови в обслуговуванні на обраний хост або мережу.
- Порушник має сформувати широкомовний ехо-запит ICMP до хостів мережі, яку він намагається атакувати
  - При цьому як адреса відправника повинна бути підставлена IP-адреса комп'ютера – цілі атаки
  - Успішним завершенням атаки є відправлення усіма хостами, що працюють в атакованій мережі, ехо-відповідей на адресу хосту, який атакують
  - При цьому і атакований хост, і мережа, в якій він знаходиться, можуть постраждати від такої активності.

Атака Smurf (2/2)

- Необхідною умовою успішної атаки з боку зовнішнього порушника є те, що зовнішній маршрутизатор повинен пропустити цей запит з зовнішньої мережі у внутрішню. Такий запит має дві характерні ознаки, кожна з яких окремо дає достатньо підстав для заборони його передавання ззовні:
  - це є широкомовний ехо-запит ICMP
  - він надходить із зовнішньої мережі, але за адресу відправника має адресу з діапазону внутрішніх адрес (*IP spoofing*)
- Небезпека атаки Smurf — це одна з причин, через яку слід забороняти вхід іззовні пакетів з широкомовною адресою

Атака Tribe Flood Network (1/2)

- Атака Tribe Flood Network (TFN) є ще одною атакою відмови в обслуговуванні, в якій використовуються ICMP-повідомлення
- На відміну від атаки Smurf, атака TFN використовує велику кількість розподілених хостів, які називають *хостами-демонами*
  - Атака TFN є типовою *розподіленою атакою відмови в обслуговуванні* (DDoS)
- Для проведення цієї атаки потрібна інсталяція програми на головному комп'ютері — "хазяїні" (master) TFN і на кількох агентах — хостах-демонах TFN
  - Як хости-демони використовуються скомпрометовані комп'ютери ("ботнет")
  - Хазяїн TFN дає хостам-демонам команду на атаку обраної цілі

Атака Tribe Flood Network (2/2)

- Демони TFN можуть організувати
  - шторм UDP пакетів (*UDP-flooding*),
  - шторм TCP SYN-запитів (*SYN-flooding*),
  - шторм exo-запитів ICMP
  - атаку Smurf.
- Хазяїн інформує хости-демони про початок атаки за допомогою exo-відповідей ICMP
  - При цьому тип атаки визначається за значенням поля ідентифікації в ICMP-заголовку exo-відповіді
  - В області даних такої exo-відповіді передаються необхідні аргументи
- Для організації атаки замість exo-запитів застосовуються exo-відповіді
  - Справа у тім, що на багатьох маршрутизаторах (шлюзах, мережних екранах) з метою забезпечення безпеки блокуються зовнішні exo-запити ICMP
  - Водночас проходження exo-відповідей здебільшого дозволяється — це надає можливість локальним користувачам дізнатись про доступність зовнішніх хостів

Програма Loki

- Програма Loki працює за принципом клієнт–сервер, використовуючи ICMP як тунельний (транспортний) протокол для утворення прихованого каналу зв'язку
  - Програму Loki можна вважати найнебезпечнішим засобом, що застосовує можливості протоколу ICMP
- Якщо на скомпрометованому хості встановлений сервер Loki, то він буде відповідати на запити Loki-клієнта
  - Зокрема, він здатний за запитами надсилати файли.
- Слід зазначити, що ICMP ніколи не призначався для підтримки подібних функцій, але, як виявилось, може використовуватись таким чином дуже ефективно
  - Тому до ICMP-трафіка в мережі слід ставитись з максимальною увагою!!!

Рекомендації стосовно блокування ICMP-трафіка (1/4)

- Exo-запити без відповіді
  - Очевидно, що при блокуванні вхідних exo-запитів і exo-відповідей ICMP неможливо провести діагностику віддаленого хосту за допомогою утиліти ping
  - З іншого боку, ці ICMP-повідомлення не будуть використані для проведення несанкціонованих операцій
  - Іноді блокують лише вхідні exo-запити, що дозволяє діагностувати віддалені комп'ютери і отримувати результати з дозволених для проходження exo-відповідей
    - Але хакери теж знають про це, і деякі створені ними шкідливі програмні засоби, як, наприклад, програми TFN і Loki, використовують для доставки інформації в основному exo-відповіді ICMP

Рекомендації стосовно блокування ICMP-трафіка (2/4)

- Відмова від можливостей Traceroute
  - Для визначення маршрутизаторів, через які проходить дейтаграма на шляху до одержувача, в UNIX використовується команда traceroute, а в Windows — tracert
  - Блокування вхідного ICMP-трафіка не дозволить використовувати обидві ці команди з вашої мережі, оскільки для них необхідно отримувати вхідні ICMP-повідомлення про закінчення часу життя пакета (“time exceeded in transit”).
  - Команда tracert, що використовується в системах під керуванням Windows, надсилає ехо-запити ICMP, тому віддалений користувач у разі блокування вхідного ICMP-трафіка не зможе застосувати цю команду для комп’ютерів вашої мережі
  - Але UNIX-команда traceroute як тестові пакети використовує дейтаграми UDP, тому блокування вхідного ICMP-трафіка не вплине на можливості віддалених користувачів застосовувати її для комп’ютерів вашої локальної мережі

Рекомендації стосовно блокування ICMP-трафіка (3/4)

- Тиша в локальній мережі
  - При блокуванні всіх вхідних ICMP-повідомлень хости та маршрутизатори локальної мережі не зможуть отримувати повідомлення про виникнення проблем під час доставки дейтаграм певному хосту у зовнішній мережі
  - Це, зазвичай, не призводить до катастрофічних наслідків, але спричиняє деякі труднощі
    - Нехай, наприклад, хост локальної мережі намагається встановити TCP-з'єднання із зовнішнім хостом, який в цей час не працює
    - Віддалений маршрутизатор відправляє ICMP-повідомлення про недосяжність хосту, але воно блокується на вході в локальну мережу
    - Хост-відправник протягом певного часу буде повторювати спроби встановити з'єднання, засмічуючи мережу марним трафіком

Рекомендації стосовно блокування ICMP-трафіка (4/4)

- Невідоме значення MTU
  - Хост-відправник намагається уникнути фрагментації дейтаграм на шляху до адресата
    - Для цього визначається MTU всього шляху — відправляється пробний пакет з встановленим прапором DF
    - Цей пакет або буде доставлений одержувачу, або відправнику повинно повернутись ICMP-повідомлення “need to frag” із зазначенням найменшого MTU
  - Блокування усіх вхідних ICMP-повідомлень не дає працювати цьому механізму, і це може призвести до вельми серйозних проблем
    - Хост-відправник буде очікувати повідомлення про необхідність фрагментації
    - Оскільки в результаті блокування він його не отримає, буде продовжуватись відправлення занадто великих дейтаграм із встановленим прапором DF
    - Усі вони будуть відкинуті, але відправник нічого про це не дізнається.
  - Тому, якщо прийнято рішення про блокування ICMP-трафіка, слід зробити виняток для вхідних ICMP-повідомлень “host unreachable - need to frag”

Протокол SNMP

- Протокол SNMP (*Simple Network Management Protocol*) і пов'язана з ним концепція SNMP MIB (*Management Information Base*) були розроблені як тимчасове рішення для керування маршрутизаторами Інтернету
  - Як виявилось, це тимчасове рішення вирізнялось простотою, ефективністю, гнучкістю і великим потенціалом для розширення
  - Через це протокол SNMP набув значного поширення, і в наш час використовується для керування практично усіма видами мережного обладнання локальних і глобальних мереж
- Під час розробки цей протокол був однозначно орієнтований на мережі TCP/IP, але в наш час він іноді використовується і для телекомунікаційного обладнання (аналогові модеми, модеми ADSL, комутатори ATM тощо)
  - Також існують реалізації SNMP для мереж IPX/SPX, хоча в наш час такі мережі вже не є актуальними
- Протокол SNMP (версія 3) описаний в RFC 3411–3418
- SNMP — це протокол прикладного рівня. Він використовує традиційну для систем керування схему "менеджер–агент"
- Як спільна модель, якою користуються менеджери та агенти SNMP, застосовуються так звані *бази даних інформації керування* (*Management Information Base*, *MIB*)

Вади протоколу SNMP

- Протокол використовує ненадійний транспортний протокол UDP
  - Це унеможливлює застосування засобів транспортного рівня для ідентифікації й автентифікації джерела команди
  - Фактично, це означає, що насправді отриманий пакет міг надійти від будь-кого
  - Крім того, протокол UDP створює загрозу втрати пакета, що може негативно вплинути на керування мережею
  - Ніяк не буде помічена втрата команд керування Set і аварійних повідомлень Trap
- Протокол (крім версії v.3) не має засобів автентифікації, а засоби ідентифікації є ненадійними (рядок передається у відкритому вигляді)
  - Фактично, вбудовані засоби ідентифікації забезпечують структурованість керування, але не захист від несанкціонованого втручання в керування мережею

Убезпечення протоколу SNMP

- Виходячи з міркувань критичності протоколу SNMP як засобу керування з широкими можливостями, використовувати його слід обережно, дотримуючись таких рекомендацій:
  - обов’язково переходити на SNMP v.3, задіявши можливості автентифікації;
  - обов’язково здійснювати настроювання “рядків співтовариств”, не покладаючись на їхню надійність, але все ж запобігаючи елементарним атакам, в яких порушники користуються рядками за умовчанням public та private;
  - при віддаленому керуванні через глобальну мережу або через мережу, яка виходить за межі контрольованої вами території, застосовувати засоби шифрування трафіка, а краще — повноцінну VPN;
  - у локальній мережі за можливості організовувати фізично відокремлену мережу для керування, щоби не допустити прослуховування трафіка і втручання в керування неавторизованих користувачів.

DNS

- DNS (система доменних імен) призначена для перетворення доменних імен у IP-адреси (і, за потреби, навпаки)
- DNS є протоколом прикладного рівня
- DNS працює поверх протоколів UDP або TCP
  - UDP застосовується значно частіше, оскільки TCP не забезпечує належної продуктивності і має більшу латентність
- Запити DNS можуть бути ітеративними і рекурсивними
  - Якщо сервер не знає відповіді на запит
    - при ітеративному запиті він повертає помилку і адресу того сервера, який може дати відповідь
    - при рекурсивному запиті він сам робить запит більш компетентному серверу
  - DNS-сервери, які обслуговують лише "закріплені" за ними домени (наприклад, домени локальної корпоративної мережі), не приймають рекурсивних запитів
  - DNS-сервери Інтернет-провайдерів, як правило, приймають рекурсивні запити
- Наверху ієрархії знаходяться "кореневі" (root) DNS-сервери, до яких може звертатись кожний, хто бажає
  - Кореневі сервери добре захищені, але вони зберігають адреси не кінцевих вузлів, а DNS-серверів, що обслуговують відповідні домени
- Клієнтська частина реалізована у вигляді так званого "резольвера" (resolver), або "стаба" (stub), що надсилає DNS-серверу рекурсивні запити

Сценарії атак на DNS (1/3)

- Класичний сценарій атаки на DNS-сервер:
  - Спочатку на DNS сервер, що атакують, надходить шторм різних рекурсивних DNS-запитів з метою очистити DNS-кеш, витіснивши з нього популярні доменні імена типа www.microsoft.com
  - Далі порушник надсилає серверу рекурсивний DNS-запит щодо доменного імені, яке порушник бажає компроментувати, і якого вже немає у кеші
  - Сервер змушений робити запит до компетентних серверів
  - Безпосередньо після запиту порушник надсилає фальшиву відповідь від імені компетентного DNS-сервера
  - Сервер зберігає у кеші фальшиву відповідь і в подальшому розсилає її усім, хто цікавиться

Сценарії атак на DNS (2/3)

- Альтернативний сценарій (давно відомий, відроджений у 2008 р.)
  - Зловмисник спрямовує серверу рекурсивний DNS-запит щодо доменного имені *I_just_love_you_william_I_wish_you_live_forever.microsoft.com*
    - Такого імені у DNS кеші немає, оскільки його взагалі не існує
  - Сервер надсилає рекурсивний запит іншим серверам і миттєво отримує фальшиву відповідь від зловмисника. У відповіді вказані:
    - IP-адреса вузла *I_just_love_you_william_I_wish_you_live_forever.microsoft.com* (зрозуміло, що вона фіктивна)
    - Фальшива IP-адреса DNS-сервера, що ніби то краще за інших володіє інформацією про піддомени *microsoft.com*
  - Атакований DNS запам’ятовує ці дані і в подальшому будь-які запити щодо імен у зоні **.microsoft.com* спрямовує безпосередньо на хакерський сервер

Сценарії атак на DNS (3/3)

- Для стабів (клієнтських комп’ютерів) можна застосувати лише перший сценарій атаки
- На практиці його більш ніж достатньо
  - Наприклад, таким чином можна нав’язати "сторонній" сервер оновлень, з якого система автоматично скачає патчі з троянами