Технічні й програмні засоби добування інформації

Сучасний світ переповнений технологіями, які з одного боку полегшують наше життя, а з іншого – створюють нові виклики для безпеки. Одним з таких викликів є використання засобів для добування інформації, що може становити серйозну загрозу для користувачів.

Технічні й програмні засоби добування інформації забезпечують отримання, обробку та аналіз даних з різних джерел. У контексті безпеки та захисту інформації такі засоби відіграють важливу роль у попередженні кіберзагроз, моніторингу мережевої активності та підтримці інформаційної безпеки.

Технічні засоби добування інформації

Це фізичні пристрої, які використовуються для збору даних. Вони можуть бути як простими, так і досить складними. Приклади:

- Шпигунське обладнання: *Підслуховуючі пристрої, приховані камери, сканери.*
- Мережеве обладнання: *Спеціалізовані пристрої для перехоплення мережевого трафіку.*
- Фізичний доступ: *Несанкціонований доступ до комп'ютерів, серверів, носіїв даних.*

Програмні засоби добування інформації

Це програмне забезпечення, яке використовується для аналізу та обробки даних. Приклади:

- Шкідливе програмне забезпечення: *Віруси, трояни, черв'яки, ransomware.*
- Інструменти для віддаленого доступу: *Backdoors, RAT (Remote Access Tools).*
- Веб-скрейпери: *Автоматизовані програми для збору даних з веб-сайтів.*
- Фішингові програми: *Створення підроблених сайтів для виманювання паролів.*

> **Ransomware**
>
> Програма-вимагач, програма-здирник, програма-шантажист (англ. ransomware, ransom — викуп і software — програмне забезпечення) — це тип шкідливої програми, який злочинці встановлюють на комп'ютерах користувачів. Програми, які вимагають викуп, надають злочинцям можливість віддалено заблокувати комп'ютер.

Backdoor

Бекдор (від англ. back door, чорний хід) — це прихована функціональність в програмному забезпеченні, яка дозволяє отримати несанкціонований доступ до системи, обходячи стандартні процедури автентифікації. Це як таємні двері, які відкривають шлях до ваших даних та систем без вашого відома.

Бекдори можуть з'являтися різними способами:

1. Навмисно вбудовані розробниками. Іноді бекдори закладаються ще на етапі розробки програмного забезпечення з метою подальшого доступу до системи.
2. Впроваджені зловмисниками. Хакери можуть інфікувати систему шкідливим програмним забезпеченням, яке створює бекдор.
3. Використання вразливостей. Зловмисники можуть скористатися відомими вразливостями в програмному забезпеченні для створення бекдору.

RAT (Remote Access Tools)

RAT (Remote Access Tools, укр. Інструменти віддаленого доступу, Віддалене адміністрування) - програми або функції операційних систем, що дозволяють отримати віддалений доступ до комп'ютера через Інтернет або локальну комп'ютерну мережу і здійснювати управління та адміністрування віддаленого комп'ютера в реальному часі. Програми віддаленого адміністрування надають майже повний контроль над віддаленим комп'ютером: вони дають можливість дистанційно керувати робочим столом комп'ютера, можливість копіювання або видалення файлів, запуску додатків і т.д.

Існує безліч реалізацій програм віддаленого адміністрування. Всі реалізації відрізняються інтерфейсами і використовуваними протоколами. Інтерфейс може бути візуальний або консольний. Одними з найпопулярніших і нійпоширеніших програм є, наприклад, компонент Windows Remote Desktop Services з клієнтом Remote Desktop Connection, Radmin, DameWare, PuTTY, VNC, UltraVNC, TightVNC, Apple Remote Desktop, Hamachi, TeamViewer, Remote Office Manager, Ammyy Admin та ін.

Web scraping

Вебскрейпінг (англ. scraping — «вишкрібання», вебзбирання або витягнення вебданих) — це процес збору даних з вебсайтів. За допомогою спеціальних програм, скриптів, а інколи і ручного копіювання зловмисник отримує структуровані дані, які можуть бути використані для аналізу, досліджень чи інтеграції в інші системи.

Етапи Вебскрейпінгу:

1. **Завантаження сторінки**
   Скрейпер відправляє HTTP-запит до вебсайту і отримує HTML-код сторінки.
2. **Аналіз HTML**
   Отримані дані обробляються для вилучення потрібної інформації, наприклад, тексту, зображень, посилань.
3. **Збереження даних**
   Витягнуті дані зберігаються у зручному форматі (CSV, Excel; База даних; Інший формат, залежно від завдання).

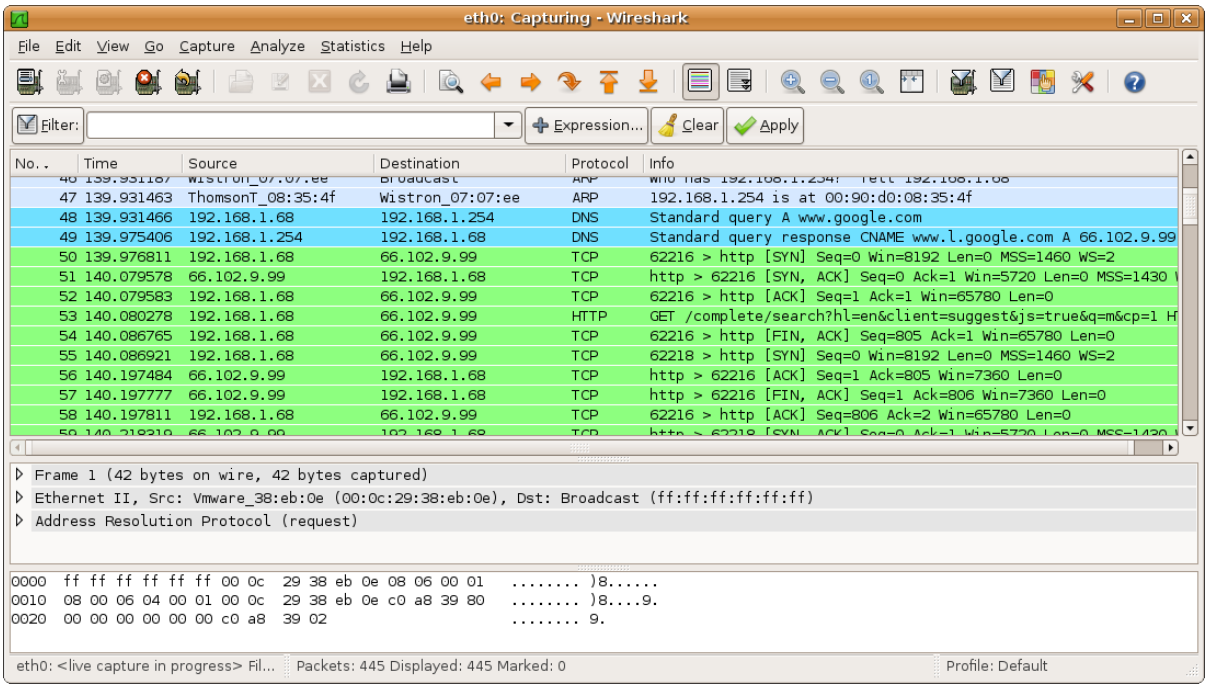
Sniffing (Аналіз трафіку)

Sniffing – це перехоплення та перевірка мережевого трафіку для захоплення даних під час їх переміщення через комп’ютерну мережу. Це робиться за допомогою програмних інструментів,

які називаються аналізаторами пакетів або мережевими аналізаторами, які призначені для захоплення та аналізу мережевого трафіку в режимі реального часу. Сніфінг можна використовувати як для **законних цілей**, наприклад для усунення несправностей мережі, так і для **зловмисних цілей**, наприклад для викрадення конфіденційної інформації, наприклад паролів, номерів кредитних карток або інших конфіденційних даних. Важливо мати належні заходи безпеки мережі, щоб запобігти несанкціонованому перехопленню та захистити від потенційних порушень даних. У комп'ютерних мережах сніффінг — це техніка, яка використовується для моніторингу та захоплення мережевого трафіку. Це включає в себе перехоплення та аналіз мережевих пакетів, що передаються між різними пристроями в мережі, часто без відома або згоди користувачів.

Мережеві сканери та перехоплювачі трафіку є популярними технічними засобами для збору інформації з мережі. Вони дозволяють зловмисникам перехоплювати пакети даних, що передаються через інтернет або локальну мережу.

Wireshark (раніше звався Ethereal) — програма для аналізу мережевих пакетів Ethernet і інших мереж (сніфер) з вільним вихідним кодом. Має графічний інтерфейс користувача. У червні 2006 року проєкт був перейменований на Wireshark через проблеми з торговою маркою



Tcpdump: Аналогічний інструмент для моніторингу мережі. tcpdump (від TCP і англ. dump — звалище, скидати) — сніфер, що дозволяє захоплювати і аналізувати мережний трафік, що проходить через комп'ютер, на якому запущена ця програма.

```
13:08:05.737768 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 1449 win 31856 <nop
,nop,timestamp 1247771 114849487> (DF)
13:08:07.467571 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 1449:2897(1448) ack 342 win 31856
<nop,nop,timestamp 114849637 1247771> (DF)
13:08:07.707634 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 2897:4345(1448) ack 342 win 31856
<nop,nop,timestamp 114849637 1247771> (DF)
13:08:07.707922 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 4345 win 31856 <nop
,nop,timestamp 1247968 114849637> (DF)
13:08:08.057841 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1045 > ns.de.ibm.net.domain: 8928+ PTR? 110.107.102.209.in-addr.arpa. (46)
13:08:08.747598 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: P 4345:5793(1448) ack 342 win 31856
<nop,nop,timestamp 114849813 1247968> (DF)
13:08:08.847870 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: FP 5793:6297(504) ack 342 win 31856
<nop,nop,timestamp 114849813 1247968> (DF)
13:08:08.848063 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: . 342:342(0) ack 6298 win 31856 <nop
,nop,timestamp 1248082 114849813> (DF)
13:08:08.907566 ppp0 < ns.de.ibm.net.domain > slip139-92-26-177.ist.tr.ibm.net.1045: 8928* 3/1/1 PTR dsl-usw-cust-110.inetarena.com., P
TR fingerless.or (199)
13:08:09.151742 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1221 > dsl-usw-cust-110.inetarena.com.www: F 342:342(0) ack 6298 win 31856 <nop
,nop,timestamp 1248112 114849813> (DF)
13:08:10.137603 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1221: . 6298:6298(0) ack 343 win 31856 <no
p,nop,timestamp 114849967 1248112> (DF)
13:09:01.984210 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: S 920197285:920197285(0) win 32120 <
mss 1460,sackOK,timestamp 1253395 0,nop,wscale 0> (DF)
13:09:03.097569 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: S 1222277738:1222277738(0) ack 92019
7286 win 32120 <mss 1460,sackOK,timestamp 114855252 1253395,nop,wscale 0> (DF)
13:09:03.098197 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 1:1(0) ack 1 win 32120 <nop,nop,ti
mestamp 1253507 114855252> (DF)
13:09:03.102171 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: P 1:322(321) ack 1 win 32120 <nop,no
p,timestamp 1253507 114855252> (DF)
13:09:04.147613 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1:1(0) ack 322 win 31856 <nop,nop,
timestamp 114855369 1253507> (DF)
13:09:04.507608 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1:1449(1448) ack 322 win 31856 <no
p,nop,timestamp 114855369 1253507> (DF)
13:09:04.507934 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 1449 win 31856 <nop
,nop,timestamp 1253648 114855369> (DF)
13:09:05.627604 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 1449:2897(1448) ack 322 win 31856
<nop,nop,timestamp 114855491 1253648> (DF)
13:09:05.857649 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 2897:4345(1448) ack 322 win 31856
<nop,nop,timestamp 114855491 1253648> (DF)
13:09:05.857918 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 4345 win 31856 <nop
,nop,timestamp 1253783 114855491> (DF)
13:09:06.907557 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: FP 4345:5792(1447) ack 322 win 31856
 <nop,nop,timestamp 114855627 1253783> (DF)
13:09:06.907887 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: . 322:322(0) ack 5793 win 31856 <nop
,nop,timestamp 1253888 114855627> (DF)
13:09:07.401205 ppp0 > slip139-92-26-177.ist.tr.ibm.net.1222 > dsl-usw-cust-110.inetarena.com.www: F 322:322(0) ack 5793 win 31856 <nop
,nop,timestamp 1253937 114855627> (DF)
13:09:08.317623 ppp0 < dsl-usw-cust-110.inetarena.com.www > slip139-92-26-177.ist.tr.ibm.net.1222: . 5793:5793(0) ack 323 win 31856 <no
p,nop,timestamp 114855780 1253937> (DF)
```

Системи перехоплення та аналізу сигналів (SIGINT)

SIGINT — сигнал на POSIX-сумісних платформах, який посилається для переривання роботи процесу

POSIX (Portable Operating System Interface for uniX) — набір стандартів, які описують інтерфейси між операційною системою та застосунками. Стандарт створений для забезпечення сумісності різних UNIX-подібних операційних систем та переносимості прикладних програм на рівні початкового коду програм.

Ці технічні засоби використовуються для перехоплення електронних сигналів, таких як радіочастотні хвилі, телефонні дзвінки або інші види зв'язку. Вони дозволяють отримувати дані, що передаються бездротовими технологіями.

Радіочастотні сканери: Використовуються для виявлення бездротових пристроїв, що передають дані, включаючи Wi-Fi мережі та Bluetooth пристрої.

Камери спостереження та шпіонські пристрої

Зловмисники можуть використовувати мікрофони, камери або інші сенсори для фізичного стеження за користувачами і збору інформації в реальному часі.

Шпигунські камери: Малі камери, що можуть бути заховані в різних предметах (наприклад, в годинниках або ручках), використовуються для запису приватних розмов або дій без відома жертви.

Аудіо-шпигунські пристрої (bugging devices): Маленькі мікрофони, які можуть бути встановлені в офісах або будинках для прослуховування розмов.

Інструменти для сканування вразливостей мереж (Vulnerability Scanners)

Ці пристрої або програмні інструменти сканують мережі на наявність вразливих точок доступу. Вони дозволяють зловмисникам знайти слабкі місця в системах безпеки та використовувати їх для подальшого несанкціонованого доступу.

Nmap: Інструмент, який дозволяє сканувати мережі, визначати відкриті порти та доступні сервіси, що допомагає виявити потенційні вразливості.

Інтерсептори бездротових мереж

інтерцептор — інтерце́птор (лат. interceptor – перехоплювач, переривач, від intercipio – перехоплюю, відбиваю) пристрій (рухома пластинка), що «зриває» повітряний потік з крила літальних апаратів, поліпшуючи за певних обставин їхню керованість.

Зростаюча доступність бездротових технологій для комп’ютерів призвела до нових проблем безпеки.

Перехоплення бездротової передачі даних, при якому нешифрований бездротовий трафік мережі перехоплюється, а конфіденційна інформація компрометується.

WiPhishing (або Wi-Fi phishing) — це метод кібератаки, при якому зловмисники створюють фальшиві бездротові мережі Wi-Fi для обману користувачів і крадіжки їхніх особистих даних. Зазвичай такі мережі маскуються під легітимні громадські Wi-Fi точки доступу, наприклад, у кафе, готелях або аеропортах, з метою змусити людей підключитися до них.

Як це працює:

1. Створення фальшивої точки доступу: Хакер створює бездротову точку доступу з ім'ям, дуже схожим на ім'я справжньої мережі (наприклад, “UniversityWiFi” замість “University_WiFi”).
2. Приманювання користувачів: Коли ви підключаєтесь до цієї фальшивої мережі, ви насправді підключаєтесь до пристрою хакера.
3. Збір інформації: Як тільки ви підключені, хакер може перехоплювати ваш інтернет-трафік, включаючи паролі, номери кредитних карток та іншу конфіденційну інформацію.
4. Встановлення шкідливого програмного забезпечення: Крім того, хакер може спробувати встановити на ваш пристрій шкідливе програмне забезпечення, таке як віруси або трояни.

Ретранслятори Wi-Fi (Wi-Fi Pineapple): Пристрої, що можуть виступати в ролі зловмисного маршрутизатора, перехоплюючи трафік Wi-Fi або вставляючи шкідливі інтерсептори в комунікацію.

GPS та інші системи відстеження

Для добування інформації про фізичне місцезнаходження користувачів зловмисники можуть використовувати пристрої для відстеження, такі як GPS-датчики.

Трекери GPS: Маленькі пристрої, які можна приховати в транспортних засобах або особистих предметах для отримання інформації про переміщення людини чи об'єкта.

Як захистити себе?

Будьте обережні з дозволами

Ретельно вивчайте дозволи, які ви надаєте програмам при встановленні.

Використовуйте складні паролі

Створіть унікальні і складні паролі для кожного акаунту.

Увімкніть двофакторну аутентифікацію

Це додатковий рівень захисту, який вимагає введення коду підтвердження крім пароля.

Регулярно оновлюйте програмне забезпечення
Оновлення часто містять виправлення вразливостей, які можуть бути використані зловмисниками.

Будьте обережні з публікацією особистої інформації в Інтернеті
Не діліться зайвою інформацією про себе і своїх близьких.

Використовуйте антивірусне програмне забезпечення
Воно допоможе захистити ваш пристрій від шкідливого програмного забезпечення.

Будьте обережні з підозрілими посиланнями і файлами
Не відкривайте підозрілі посилання і не завантажуйте файли з невідомих джерел.

Звертайте увагу на налаштування конфіденційності в соціальних мережах
Обмежте доступ до вашої інформації для сторонніх осіб.

> **Пам'ятайте**
>
> Ваша безпека в Інтернеті залежить від вас. Будьте обережні і дотримуйтесь простих правил, щоб захистити себе від загроз, пов'язаних з технічними засобами добування інформації.

Джерела

- Бекдор
- Віддалене адміністрування
- Understanding Wireless Intercept and "WiPhishing"
- інтерцептор — Великий тлумачний словник сучасної мови
- POSIX
- SIGINT_(POSIX)
- Wireshark
- №5. Ethical Hacking Labs. Сніфінг - HackYourMom
- Web scraping