**Урок № 4**

**Тема. Технічні та програмні засоби добування інформації**

**Мета:**

- ✓ ***навчальна:*** ознайомитися з технічними та програмними засобами добування інформації; різновидами злочинного ПЗ.

**Актуалізація опорних знань**

1. Що таке інформаційна загроза? Які є джерела загроз?
2. Якими шляхами поширюються загрози?
3. Які є загрози залежно від обсягів збитків?
4. Який принцип безпеки порушено, якщо було отримано доступ до керування інформаційною системою?
5. Що таке спам? Який він буває?
6. Що таке фішинг? Ddos –атака?
7. Які існують "природні" загрози?.

Комп'ютерне тестування – Урок 3(Mytest)

**Вивчення нового матеріалу**

Однією з небезпечних загроз є витік інформації технічними каналами і добування інформації програмними засобами.

Технічні і програмні засоби добування необхідної інформації - це подолання системи захисту, обмеження або заборона доступу до них посадових осіб, дезорганізації роботи технічних засобів, вивід з ладу комунікаційних і комп'ютерних мереж, усього високотехнологічного забезпечення функціонування системи управління.

Спроба одержати несанкціонований доступ до комп'ютерної мережі з метою ознайомитися з нею, залишити інформацію, виконати, знищити, змінити або викрасти програму або іншу інформацію кваліфікується як **«комп'ютерне піратство»**.

Способи несанкціонованого доступу до інформації здійснюються шляхом:

1) Застосування засобів підслуховування, фото, відеоапаратури, підкуп осіб, використання «троянських» програм;
2) Використання недоліків мови програмування і недоліків в операційної системи, крадіжка носіїв інформації, копіювання інформації;
3) Отримання захищених даних за допомогою запитів дозволу, реквізитів розмежування доступу, таємних паролів.

Технічні засоби істотно розширюють і доповнюють можливості людини з добування інформації, забезпечуючи:

а) знімання інформації з носіїв, які недоступні органам почуттів людини;
б) добування інформації без порушення кордонів контрольованої зони;
в) передачу інформації практично в реальному масштабі часу в будь-яку точку земної кулі;
г) аналіз і обробку інформації в обсязі і за час, недосяжних людині;
д) консервацію і як завгодно довгий зберігання видобутої інформації.

**Технічні засоби добування інформації та їх класифікація** *( схема в презентації)*

До технічних і програмних засобів ведення інформаційної боротьби відносять :

- комп'ютерний вірус (КВ)- спеціальна програма, що впроваджується в “чуже електронне середовище”. КВ спроможний передаватися по лініях зв'язку і мережам обміну інформацією, проникати в електронні телефонні станції і системи управління. У заданий час або по сигналу КВ стирає інформацію , що зберігається в БД, або довільно змінює її.
- логічна бомба (ЛБ)- так звана програмна закладка, що завчасно впроваджується в інформаційні системи і мережі. ЛБ по сигналу, або у встановлений час, приводиться в дію, стираючи або перекручуючи інформацію в інформаційних ресурсах і виводить їх з ладу;
- ”троянський кінь” (різновид ЛБ)- програма, що дозволяє здійснювати схований, несанкціонований доступ до інформаційних ресурсів для добування даних;
- засоби впровадження КВ і ЛБ в інформаційні ресурси ОУ і керування ними на відстані. Для цих засобів найбільш уразливими є інформаційні ресурси виявлення і управління, що постійно діють у встановлених режимах реального часу.
- ”нейтралізатори текстових програм,” це програми, що забезпечують невиявлення випадкових і навмисних хиб програмного забезпечення;
- засоби придушення інформаційного обміну в телекомунікаційних мережах, фальсифікації інформації в каналах ;

**Шкідливе ПЗ**

**Зловмисний програмний засіб** або **зловмисне програмне забезпечення** (англ. *Malware* - скорочення від **mal**icious - зловмисний і soft**ware** - програмне забезпечення) — програма, створена зі злими намірами. До зловмисних програмних засобів належать віруси, рекламне ПЗ, хробаки, троянці, руткіти, клавіатурні логери, дозвонювачі, шпигунські програмні засоби, здирницькі програми, шкідливі плаґіни та інше зловмисне програмне забезпечення.

**Класифікація:**

**За видом програмного забезпечення**

- програми, що вимагають програм-носіїв - люки; - логічні бомби; - троянські коні; - віруси.
- програми, що є незалежними. - черв’яки, - зомбі; - утиліти прихованого адміністрування; - програми-крадії паролів; - “intended”-віруси; - конструктори вірусів; - поліморфік-генератори.

**За наявністю матеріальної вигоди**

- що не приносять пряму матеріальну вигоду тому, хто розробив (встановив) шкідливу програму:
  - хуліганство, жарт;
  - самоствердження, прагнення довести свою кваліфікацію;
- що приносять пряму матеріальну вигоду зловмисникові:
  - крадіжка конфіденційної інформації, включаючи діставання доступу до систем банк-клієнт, отримання PIN кодів кредитних карток і таке інше;

- отримання контролю над віддаленими комп'ютерними системами з метою розповсюдження спаму з численних комп'ютерів-зомбі;

**За метою розробки**

- програмне забезпечення, яке з самого початку розроблялося спеціально для забезпечення несанкціонованого доступу до інформації, що зберігається на ПК з метою спричинення шкоди (збитку) власникові інформації і/або власникові ПК.
- програмне забезпечення, яке з самого початку не розроблялися спеціально для забезпечення діставання несанкціонованого доступу до інформації.

**Різновиди шкідливих програм:**

**Люк** (trapdoor) – це прихована, недокументована точка входу в програмний модуль, яка дозволяє кожному, хто про неї знає, отримати доступ до програми в обхід звичайних процедур, призначених для забезпечення безпеки КС. Люк вставляється в програму в більшості випадків на етапі налагодження для полегшення роботи – даний модуль можна буде викликати в різних місцях, що дозволяє налагоджувати окремі його частини незалежно одна від одної.

**Логічна бомба** – це код, що поміщається в деяку легальну програму. Він влаштований таким чином, що при певних умовах “вибухає”. Умовою для включення логічної бомби може бути наявність або відсутність деяких файлів, певний день тижня або певна дата, а також запуск додатку певним користувачем.

**Хробаки** – вид вірусів, які проникають на комп'ютер-жертву без участі користувача. Хробаки використовують так звані «дірки» (уразливості) у програмному забезпеченні операційних систем, щоб проникнути на комп'ютер. Вразливості – це помилки і недоробки в програмному забезпеченні, які дозволяють віддалено завантажити і машинний код, в результаті чого вірус-хробак потрапляє в операційну систему і, як правило, починає дії по зараженню інших комп'ютерів через локальну мережу або Інтернет. Зловмисники використовують заражені комп'ютери користувачів для розсилки спаму або для DDoS-атак.

Так само як для вірусів, життєвий цикл хробаків можна розділити на певні стадії: 1. Проникнення в систему 2. Активація 3. Пошук "жертв" 4. Підготовка копій 5. Поширення копій

На етапі проникнення в систему хробаки діляться переважно по типах використовуваних протоколів:

• Мережні хробаки - чирви, що використають для поширення протоколи Інтернет і локальні мережі. Звичайно цей тип хробаків поширюється з використанням неправильної обробки деякими додатками базових пакетів стека протоколів tcp/ip

• Поштові хробаки - чирви, що поширюються у форматі повідомлень електронної пошти

• IRC-хробаки - хробаки, що поширюються по каналах IRC (Internet Relay Chat)

• P2P-хробаки - чирви, що поширюються за допомогою пірінгових (peer-to-peer) файлообмінних мереж

• IM-хробаки - хробаки, що використають для поширення системи миттєвого обміну повідомленнями (IM, Instant Messenger - ICQ, MSN Messenger, AIM й ін.)

Аналогічно, хробаки можуть міняти тему й текст інфікованого повідомлення, ім'я, розширення й навіть формат вкладеного файлу - виконує модуль, що, може бути прикладений як є або в заархівованому виді.

**Віруси – трояни**

**Троян** (троянський кінь) — тип шкідливих програм, основною метою яких є шкідливий вплив стосовно комп'ютерної системи. Трояни відрізняються відсутністю механізму створення власних копій. Деякі трояни здатні до автономного подолання систем захисту КС, з метою проникнення й зараження системи. У загальному випадку, троян попадає в систему разом з вірусом або хробаком, у результаті необачних дій користувача або ж активних дій зловмисника.

У силу відсутності в троянів функцій розмноження й поширення, їхній життєвий цикл украй короткий - усього три стадії:

• Проникнення на комп'ютер

• Активація

• Виконання закладених функцій

Троян може тривалий час непомітно перебувати в пам'яті комп'ютера, ніяк не видаючи своєї присутності, доти, поки не буде виявлений антивірусними засобами.

Способи проникнення на комп'ютер користувача трояни вирішують звичайно одним із двох наступних методів. Маскування — троян видає себе за корисний додаток, що користувач самостійно завантажує з Інтернет і запускає. Іноді користувач виключається із цього процесу за рахунок розміщення на Web-сторінці спеціального скрипта, що використовуючи діри в браузері автоматично ініціює завантаження й запуск троянa.

До даної групи шкідливих програм відносять:

- програми-вандали,
- «дроппери» вірусів,
- «злі жарти»,
- деякі види програм-люків;
- деякі логічні бомби,
- програми вгадування паролів;
- програми прихованого адміністрування.

**Зомбі** - це програма, яка приховано під’єднується до інших підключених в Інтернет комп’ютерів, а потім використовує цей комп’ютер для запуску атак, що ускладнює відстеження шляхів до розробника програми-зомбі.

"**Жадібні" програми** (greedy program). - це програми, що намагаються монополізувати який-небудь ресурс, не даючи іншим програмам можливості використовувати його. Доступ таких програм до ресурсів системи призводить до порушення її доступності для інших програм.

**Захоплювачі паролів** - це спеціально призначені програми для крадіжки паролів.

**Утиліти схованого адміністрування** (backdoor) Цей вид шкідливого програмного забезпечення у деяких випадках можна віднести до групи троянських коней. Вони по своїй суті є досить могутніми утилітами віддаленого адміністрування комп'ютерів у мережі

Під час запуску троянська програма встановлює себе в системі і потім стежить за нею, при цьому користувачу не видається ніяких повідомлень про дії такого трояна в системі.

**Формування практичних умінь і навичок**

**Увага!** ***Під час роботи з комп'ютером дотримуйтеся правил безпеки та санітарно-гігієнічних норм.*** (Інструктаж з правил техніки безпеки)

**Завдання 1.** Знайдіть відомості в Інтернеті та складіть список з 10 найбільш небезпечних комп'ютерних вірусів. Визначте, з якою метою вони були створені. Подайте знайдені відомості в текстовому документі у зручному вигляді

**Завдання 2.** Виконайте інтерактивну вправу https://learningapps.org/7076420

**Домашнє завдання**

1) Опрацювати **конспект**
2) Ознайомитися з інформацією про віруси і шкідливі програми на сайті Zillya! (вірусна енциклопедія) **Дослідити** типи шкідливих програм (virus Trojan, Backdoor, Dropper, Downloader, Tool, Adware, Dialer, Worm, Exploit, Rootkit), скористайтеся даними на сайті Zillya! (вірусна енциклопедія)

**Творче завдання:** Засобами редактора презентацій створіть ілюстрований інтерактивний словник термінів, які виникають при захисті від можливих загроз користувача Інтернету. Передбачте, що користувач може обирати термін у списку та переходити на сторінку із тлумаченням терміна. На такій сторінці може бути ілюстрація, що відображає зміст терміна, корисне посилання на ресурс в Інтернеті, де можна детальніше ознайомитися з поняттям..