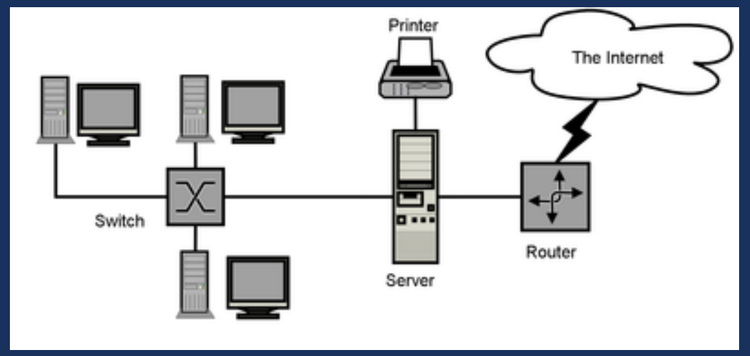
CHERNIHIV POLYTECHNIC
NATIONAL UNIVERSITY

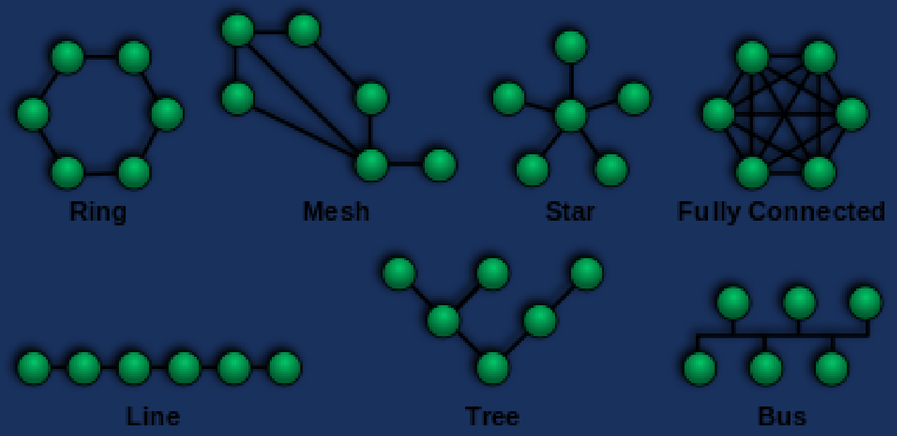
Науковий гурток “CybersecurityLab”

Науковий керівник гуртка
Семендяй С.М.
Завідувач лабораторії кібебезпеки,
ст. викладач кафедри КБММ

Підсекція «Безпека мереж»

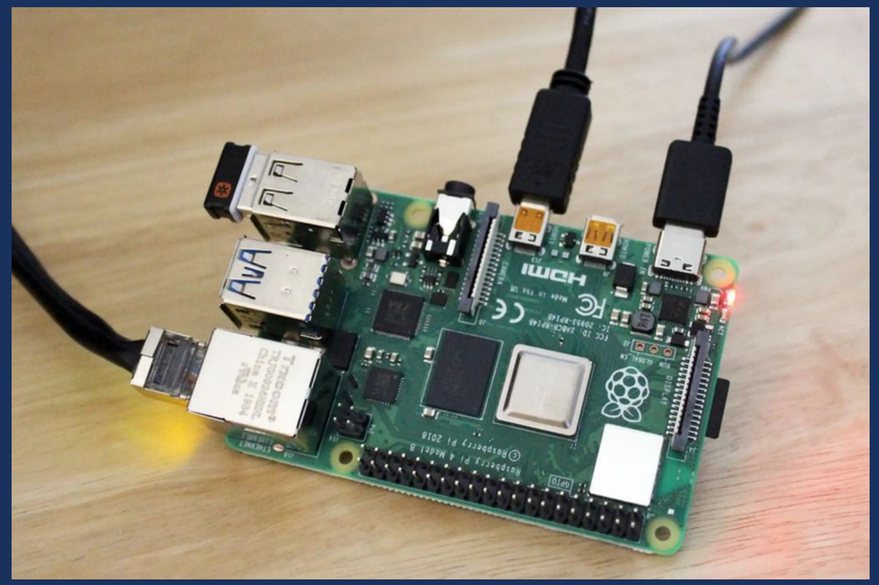
- Будова комп’ютерних мереж
- Стандартні фізичні компоненти мереж
- Характеристики мереж
- Топології мереж
- Необхідність забезпечення безпеки мереж
- Зловмисники, їх мотиви та класифікація атак

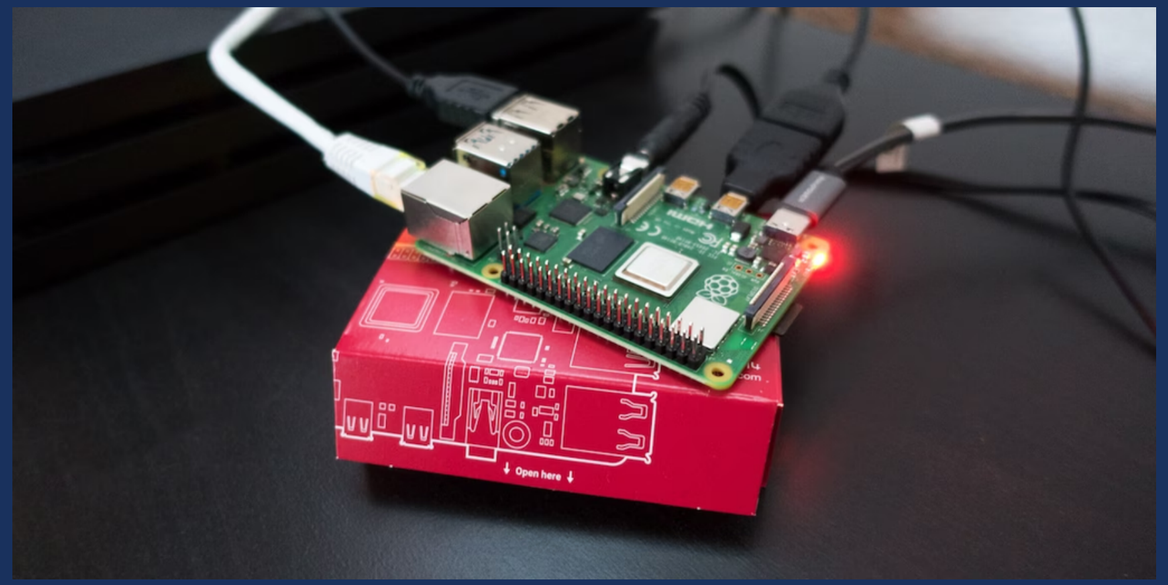




Підсекція «Безпека мереж»

- Практика застосування міні-комп’ютерів Raspberry Pi 4 для вардрайвінгу



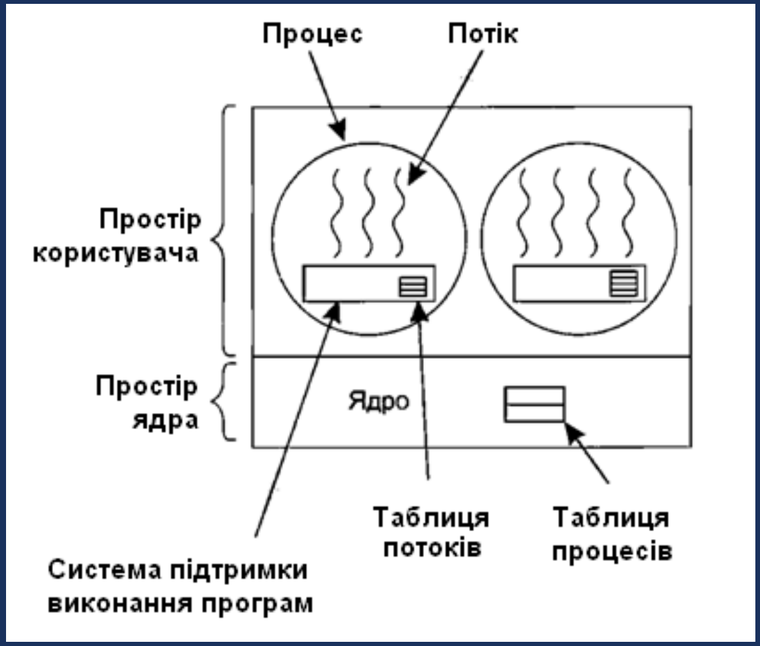


Підсекція «Безпека мереж»

- Хакінг та його концепція
- Знайомство зі стадіями хакінгу
- Різновиди хакерських атак
- Алгоритм сканування мережі
- Способи сканування
- Знайомство з техніками виявлення живих хостів
- Знайомство з прийомами сканування відкритих портів
- Знайомство з прийомами прихованого сканування
- Яким чином можна ухилитися від систем виявлення вторгнень
- Сканування вразливостей
- Збирання банерів

Підсекція «Безпека мереж»

- Введення в схематизацію операційної системи
- Де вразлива операційна система
- Огляд способів хакінгу
- Алгоритм системи хакінгу
- Суть злому паролів
- Прийоми підвищення рівня привілеїв
- Суть приховування файлів



Підсекція «Безпека мереж»

- Практика застосування утиліти John The Ripper для злому паролів.

```
┌──(root㉿kali)-[~]
└─# unshadow /etc/passwd /etc/shadow > passwords.out
Created directory: /root/.john

┌──(root㉿kali)-[~]
└─# john --format=crypt ./passwords.out
Using default input encoding: UTF-8
Loaded 5 password hashes with 5 different salts (crypt, generic crypt(3) [?/64])
Cost 1 (algorithm [1:descrypt 2:md5crypt 3:sunmd5 4:berypt 5:sha256crypt 6:sha512crypt]) is 0 for all loaded hashes
Cost 2 (algorithm specific iterations) is 1 for all loaded hashes
Will run 2 OpenMP threads
Proceeding with single, rules:Single
Press 'q' or Ctrl-C to abort, almost any other key for status
vagrant          (vagrant)
Almost done: Processing the remaining buffered candidate passwords, if any.
Warning: Only 10 candidates buffered for the current salt, minimum 96
Proceeding with wordlist:/usr/share/john/password.lst
password         (root)
secret           (user)
lakers           (testuser)
```

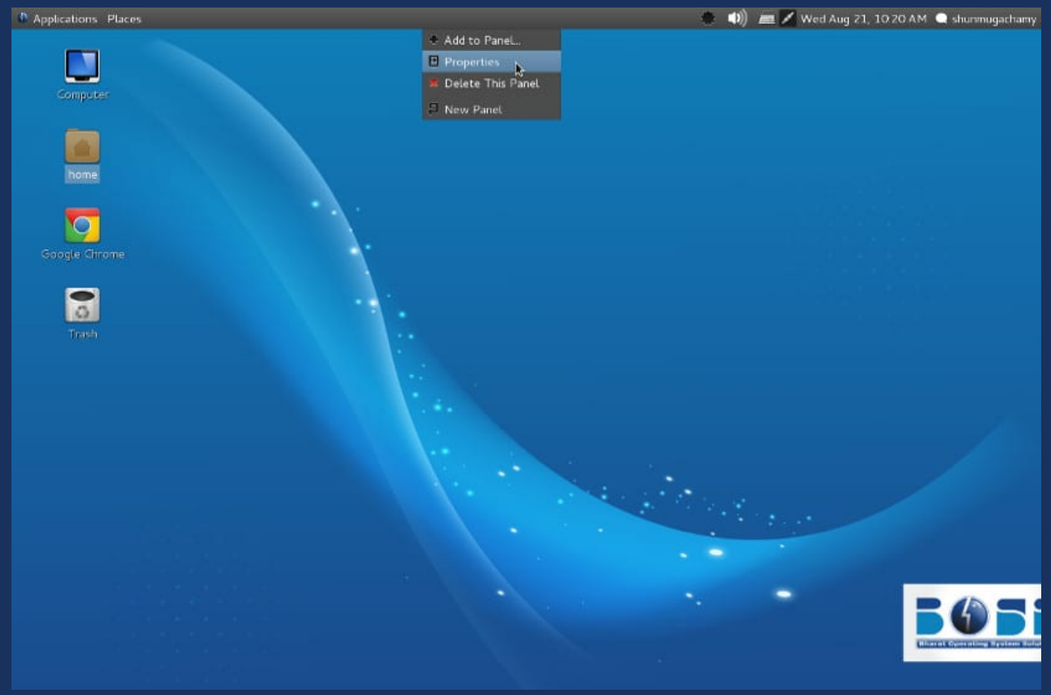
```
┌──(root💀kali)-[~]
└─# john
John the Ripper 1.9.0-jumbo-1 OMP [linux-gnu 64-bit x86_64 AVX AC]
Copyright (c) 1996-2019 by Solar Designer and others
Homepage: http://www.openwall.com/john/

Usage: john [OPTIONS] [PASSWORD-FILES]
--single[=SECTION[,..]]    "single crack" mode, using default or named rules
--single=:rule[,..]        same, using "immediate" rule(s)
--wordlist[=FILE] --stdin  wordlist mode, read words from FILE or stdin
                  --pipe   like --stdin, but bulk reads, and allows rules
```

Підсекція «Безпека мереж»

- Суть шпигунського ПЗ;
- Захищені операційні системи та їх адміністрування

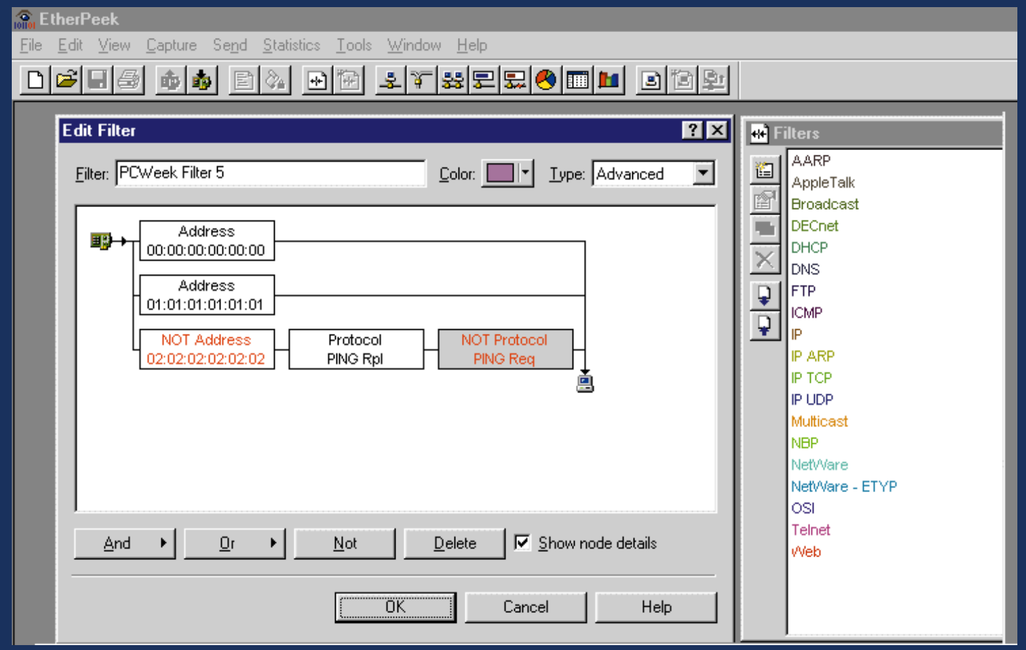
Підсекція «Безпека мереж»

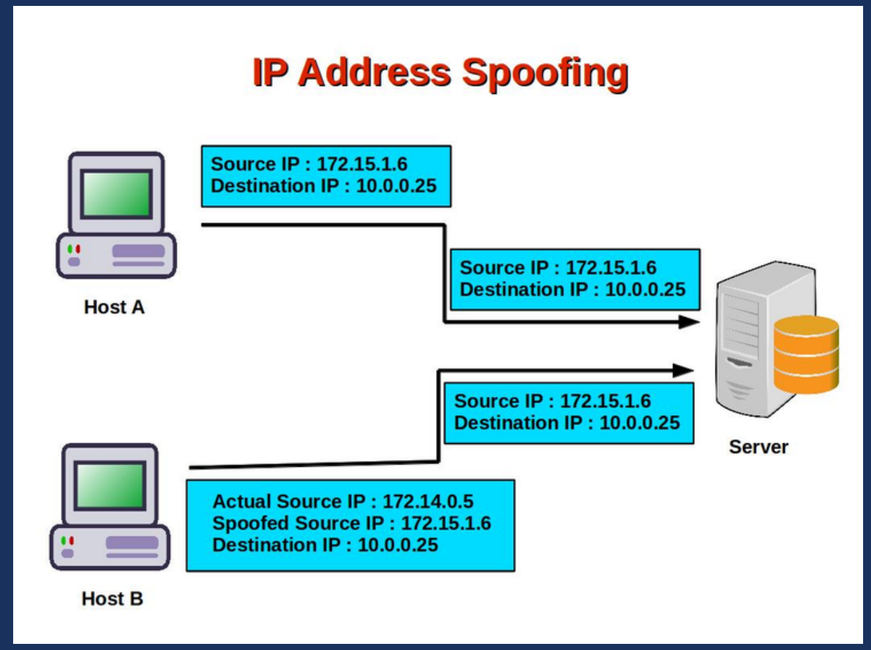
- Практичні навички роботи із захищеною операційною системою BBOS



Підсекція «Безпека мереж»

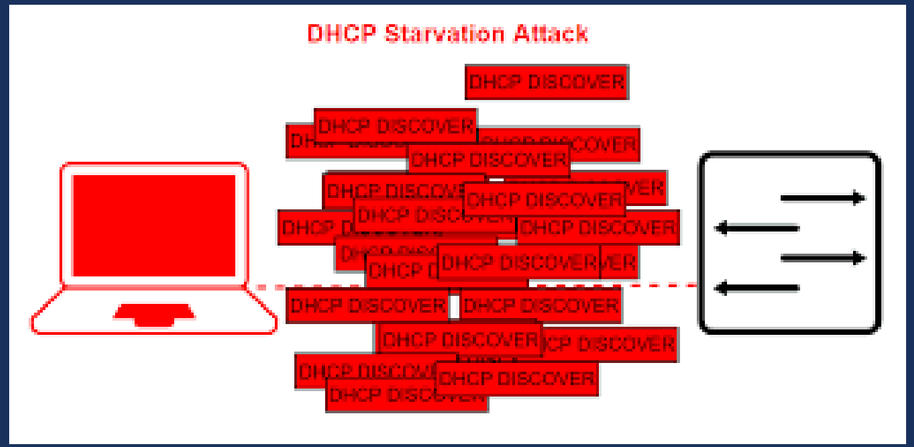
- Сніфінг, принципи роботи, види сніфінгу;
- Знайомство з апаратними аналізаторами протоколів;
- Спуфінг

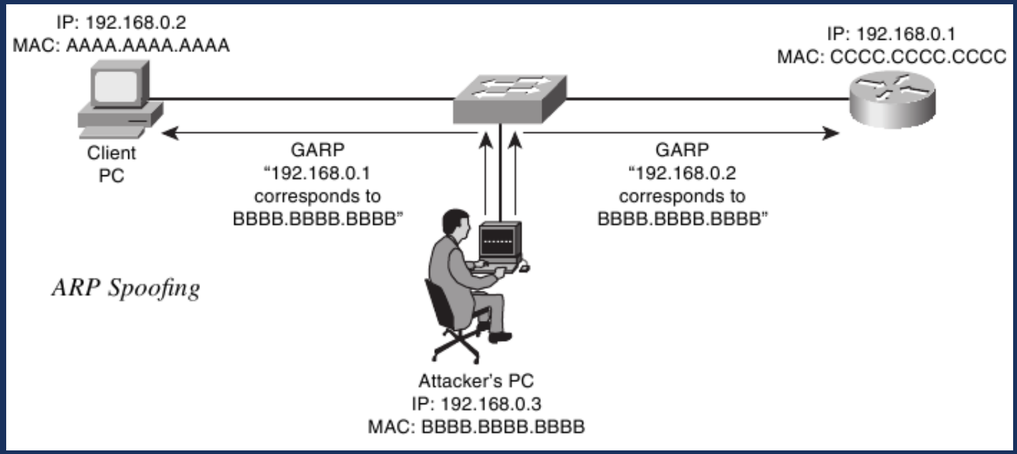




Підсекція «Безпека мереж»

- Знайомство з ARP-атаками
- Знайомство з MAC-атаками
- Знайомство з DHCP-атаками
- Введення в порт SPAN
- Як проходить отруєння DNS-кешу
- Знайомство з методами протидії сніфінгу.



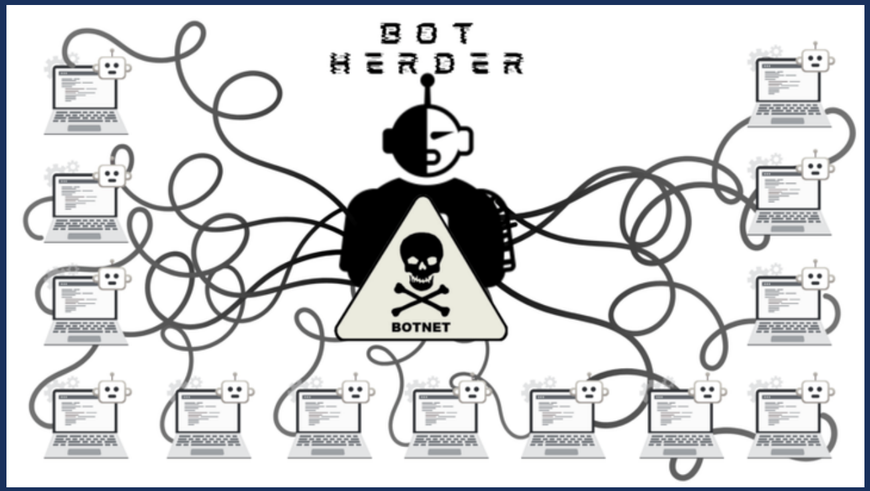


Підсекція «Безпека мереж»

- Набуття практичних навичок роботи з універсальним пошуковим приладом ANDRE.

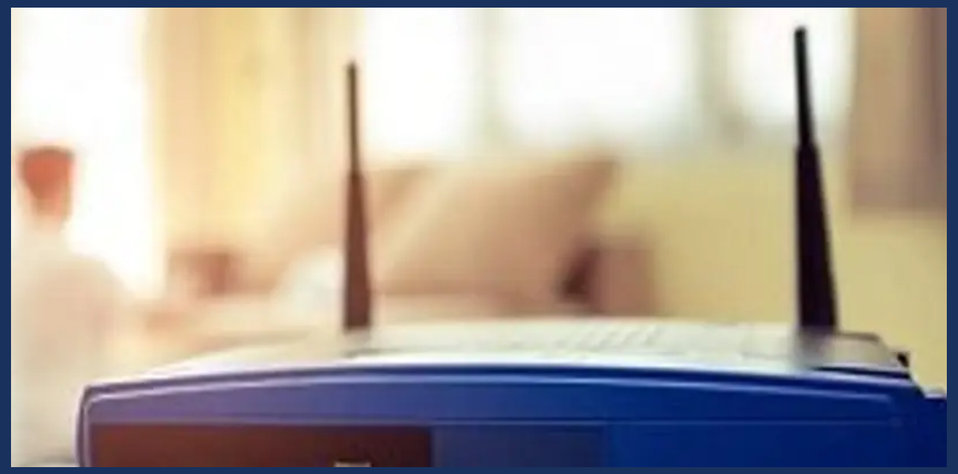
Підсекція «Безпека мереж»

- Знайомство з концепцією Denial-of-Service, DDoS-атака
- Знайомство з техніками атак DoS/DDoS
- Бот-мережі
- Знайомство з інструментарієм, за допомогою якого проводяться DoS-атаки
- Як реалізується атака DDoS
- Яким чином можливо протидіяти DoS-атакам
- Знайомство з інструментарієм захисту від DoS



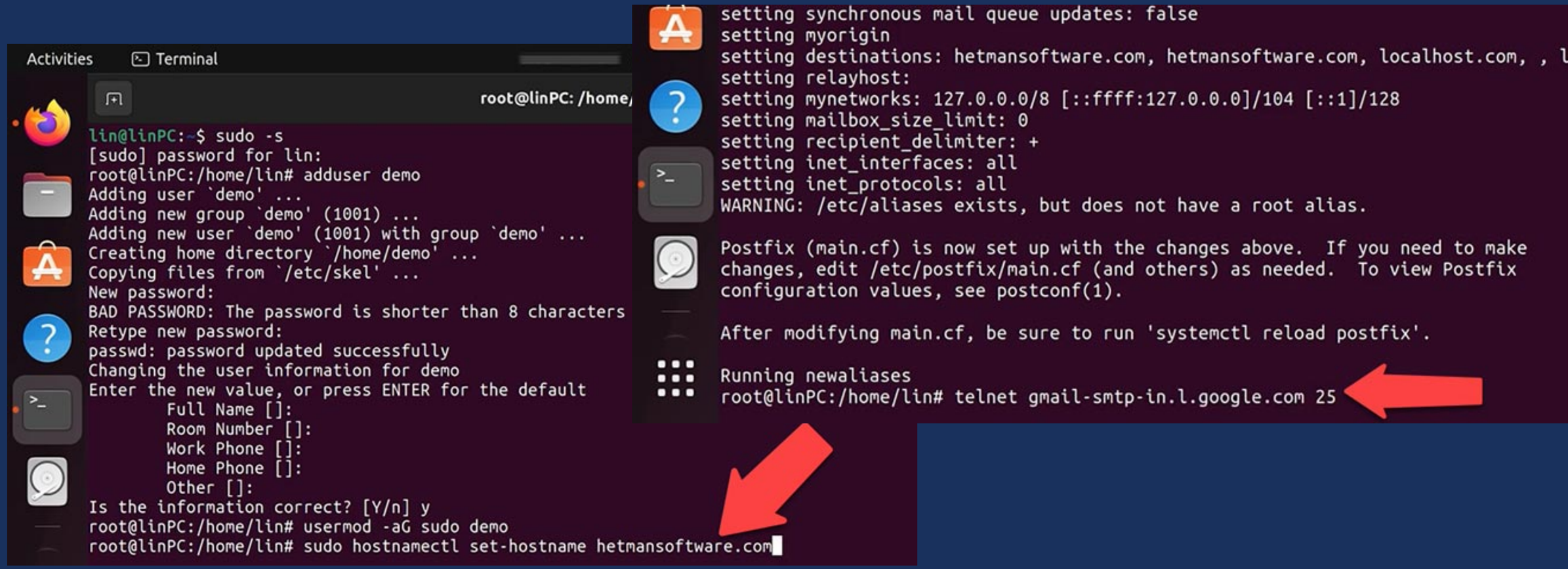
Підсекція «Безпека мереж»

- Безпека бездротових і мобільних мереж
- Правила роботи з детекторами бездротових протоколів



Підсекція «Безпека мереж»

- Адміністрування Ubuntu-сервера лабораторії кібербезпеки

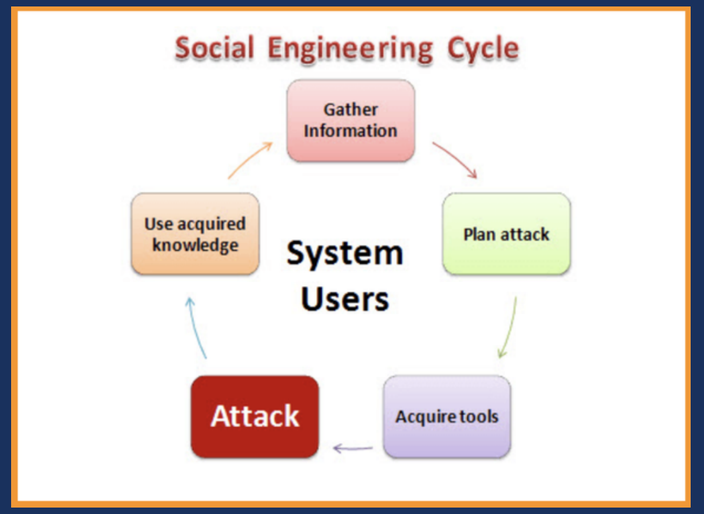


Підсекція «Безпека мереж

- Отримання практичних навичок роботи з детектором бездротових протоколів

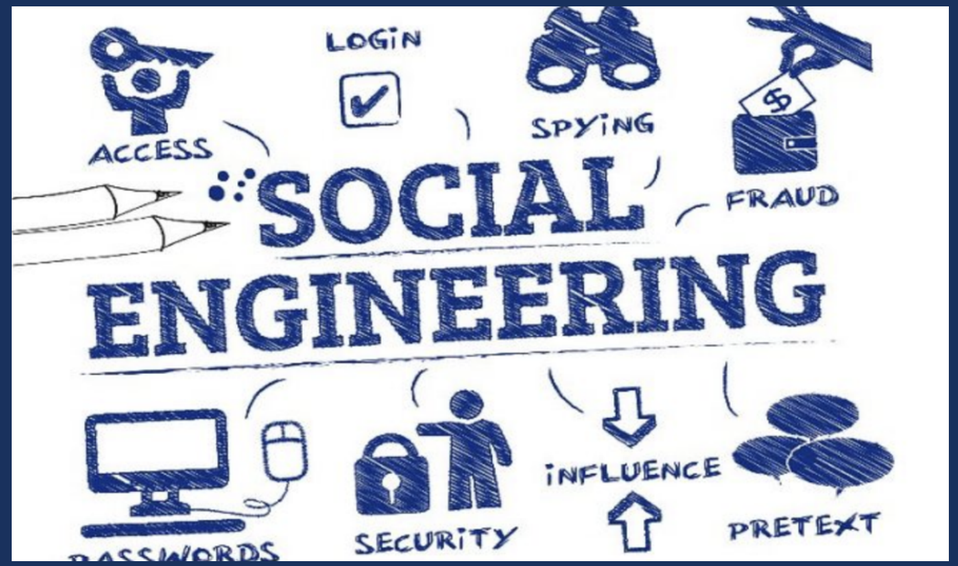
Підсекція «OSINT»

- Сутність, структура та функції соціальної інженерії
- Методологічні основи соціальної соціальної інженерії
- Соціальна технологія як засіб забезпечення соціальної інженерії



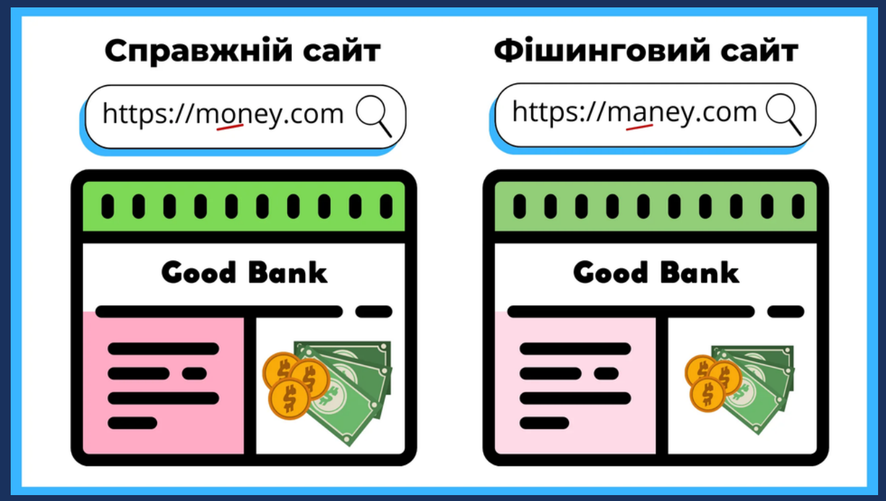
Підсекція «OSINT»

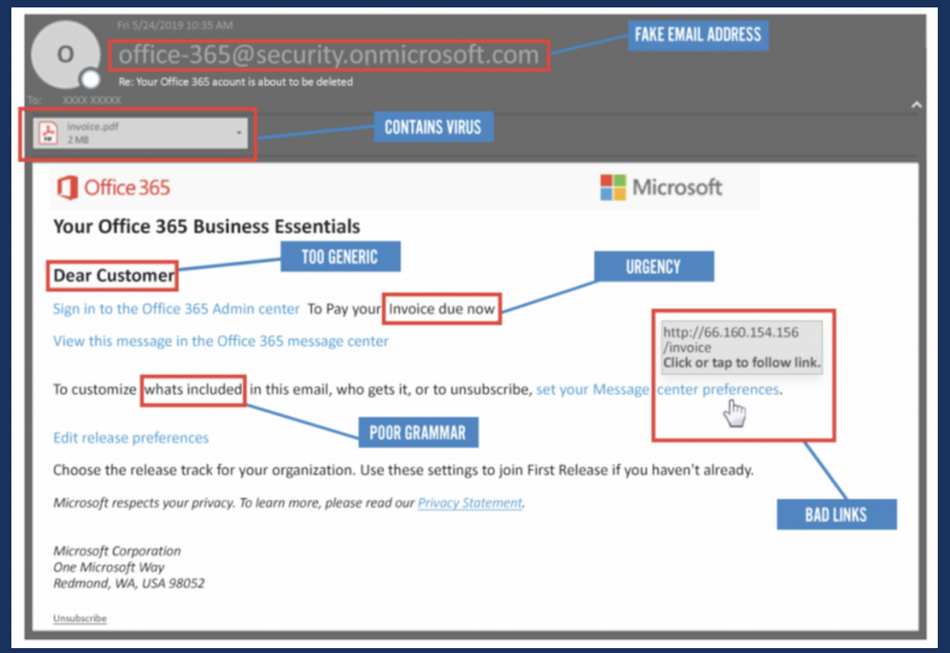
- Предмет і завдання курсу “Основи соціальної інженерії”
- Ідеї соціальної інженерії в соціології



Підсекція «OSINT»

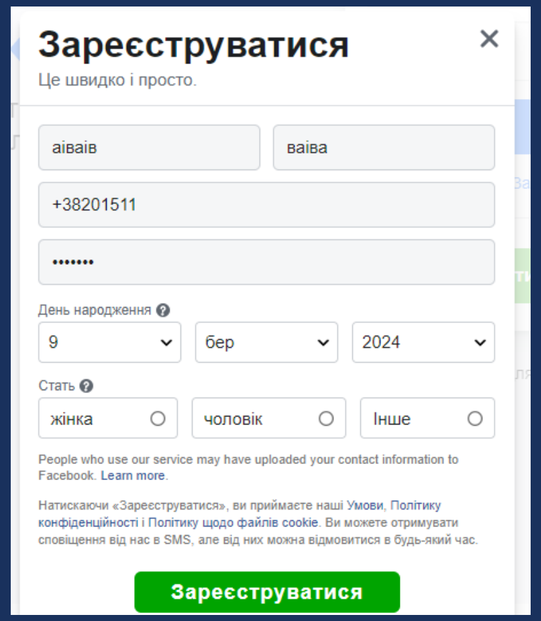
- Практика застосування фішингового сайту.
- Проективні методи
- Ігрові методи
- Інноваційні методи

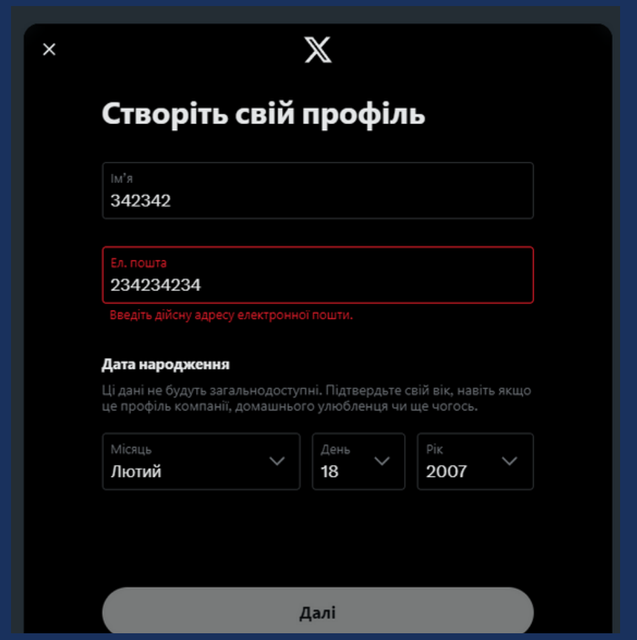




Підсекція «OSINT»

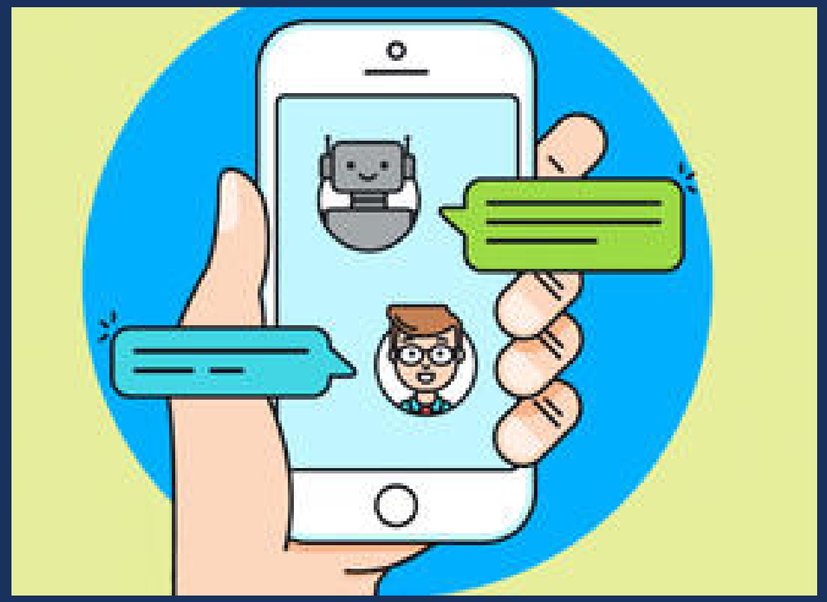
- Практика застосування системи “OSINT”, створення фейкового аккаунту
- Аналітичні методи
- Евристичні методи введення в схематизацію операційної системи

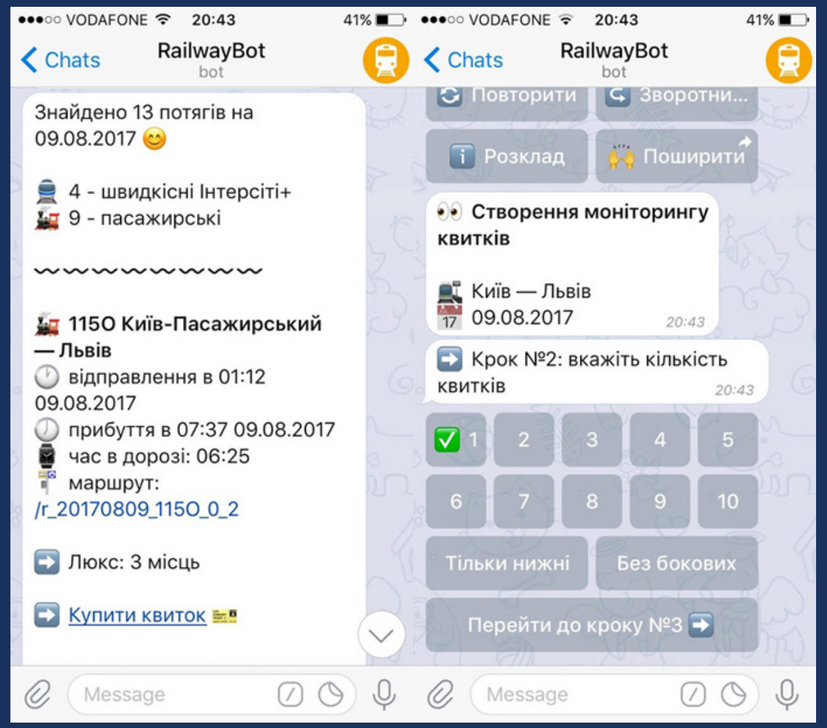




Підсекція «OSINT»

- Практичні навички роботи із Телеграм ботами





Підсекція «OSINT»

- Соціальна діагностика
- Соціальне проектування.

Підсекція «OSINT»

- Соціальне програмування
- Організація впровадження й використання соціальних технології

Підсекція «OSINT»

- Набуття практичних навичок роботи з пошуковими сервісами за зображеннями

Підсекція «OSINT»

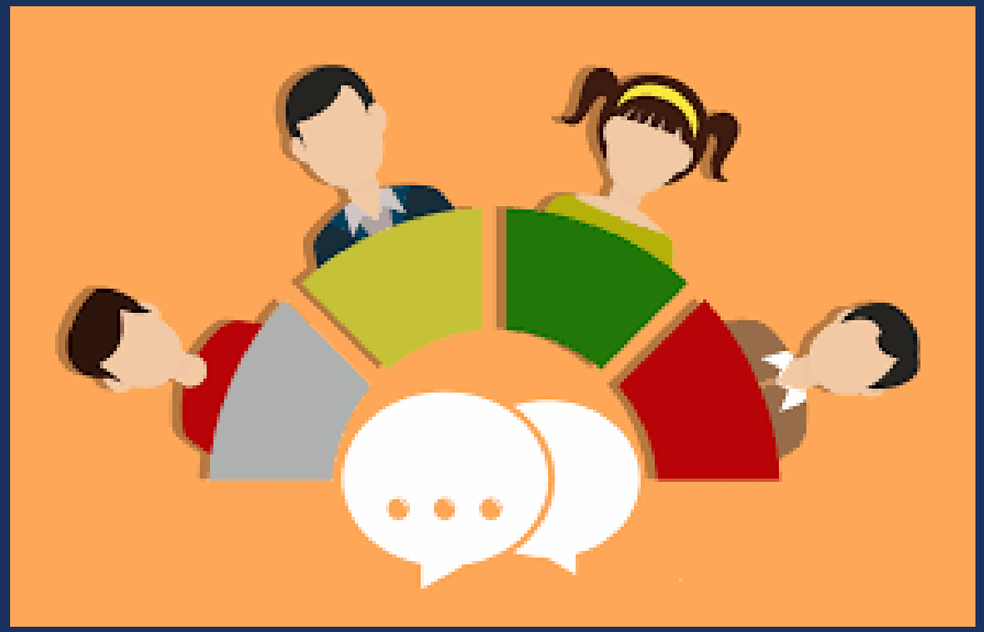
- Соціо-інженерне забезпечення соціальної політики держави;
- Формування інститутів громадянського суспільства (соціо-інженерний підхід);
- Соціо-інженерна діяльність у регіоні та місті.

Підсекція «OSINT»

- Робота з публічними реєстрами

Підсекція «OSINT»

- Соціо-інженерна діяльність на підприємстві
- Соціо-інженерні методи оптимізації внутрішньо-колективних відносин
- Соціо-інженерне обґрунтування особистісних змін



CHERNIHIV POLYTECHNIC
NATIONAL UNIVERSITY

Як нас знайти:

Вулиця Шевченка, 95,
Чернігів, Чернігівська область,
14035
Перший корпус 108 кабінет

Наша пошта:

cybersec_dep@stu.cn.ua