

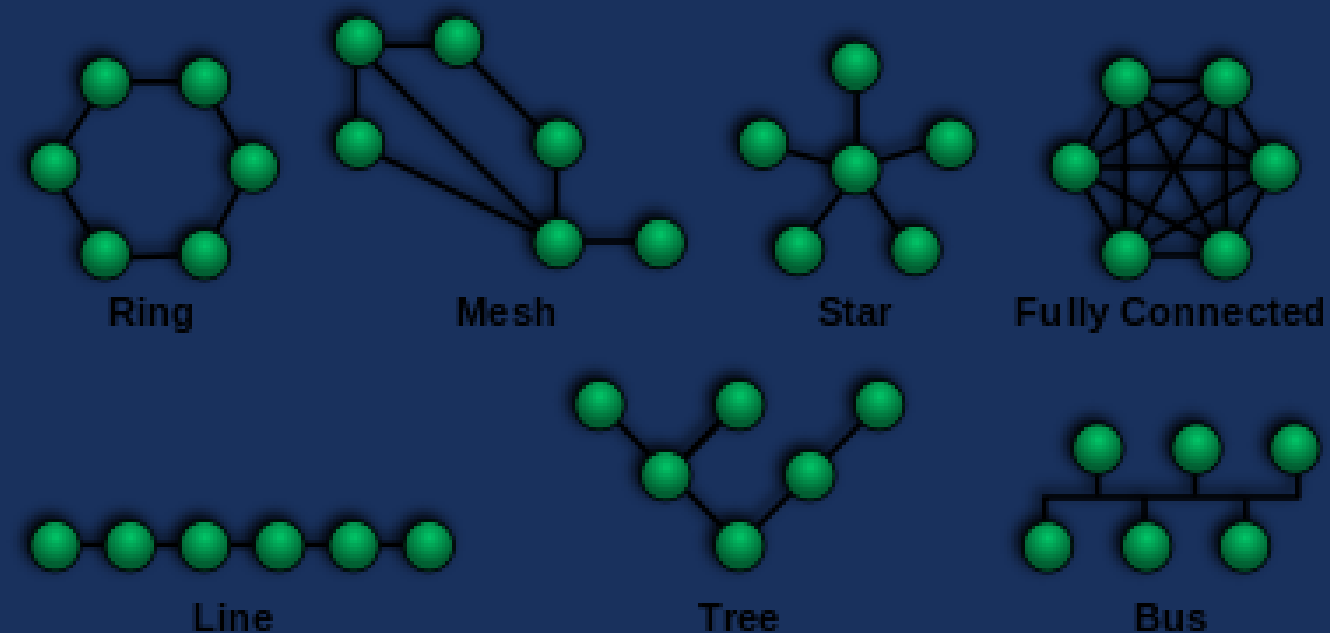
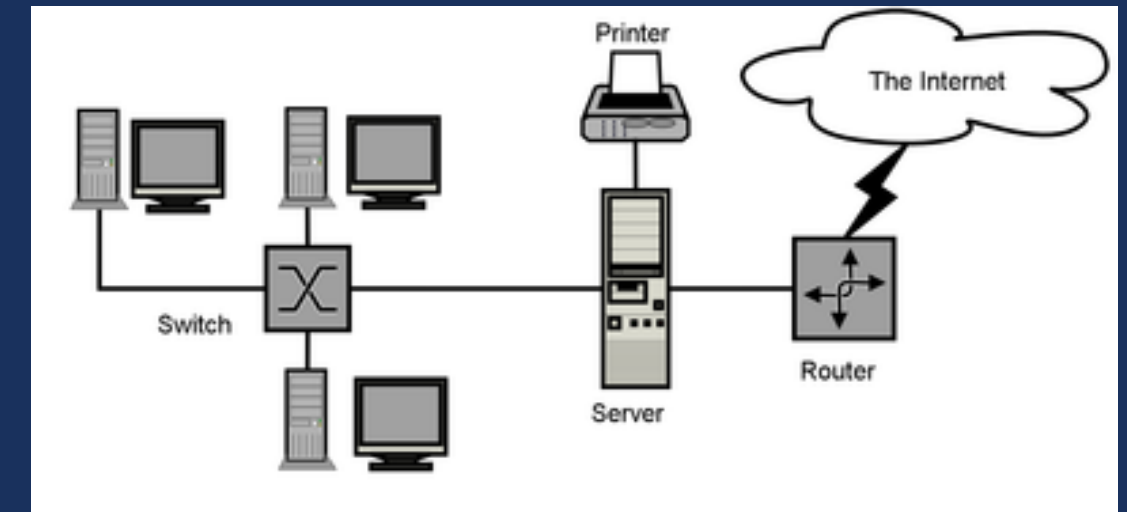


Науковий гурток “CybersecurityLab”

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

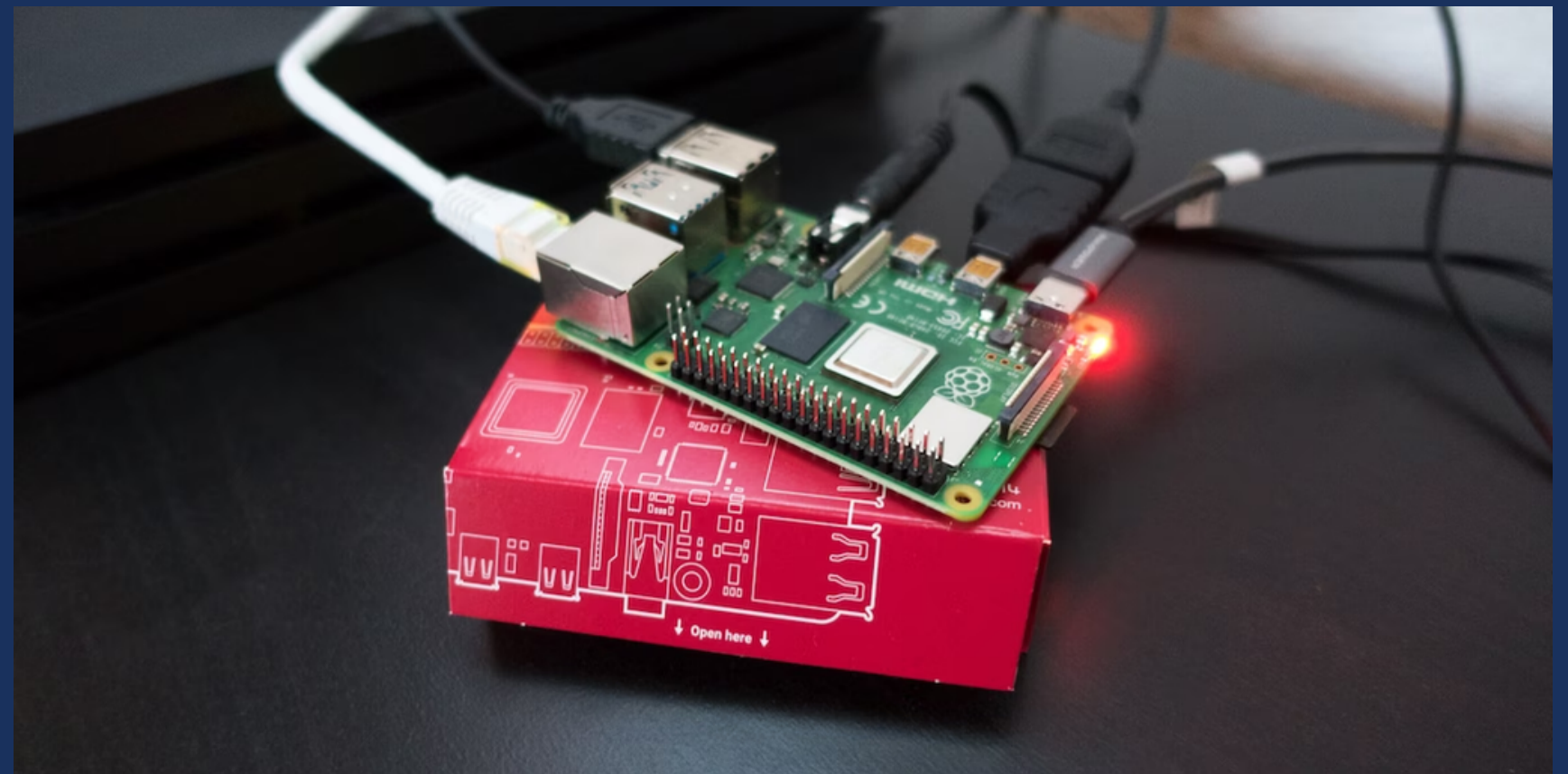
Підсекція «Безпека мереж»

- 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

```
Tests performed: 209   Plugins enabled: 0

Warnings:
-----
- Found BIND version in banner [NAME-4210]
- Found one or more vulnerable packages. [PKGS-7392]
- iptables module(s) loaded, but no rules active [FIRE-4512]
- Found one or more stratum 16 peers [TIME-3116]
- Found local source as selected time source [TIME-3124]

Suggestions:
-----
- Default umask in /etc/init.d/rc could be more strict like 027 [AUTH-9328]
- To decrease the impact of a full /home file system, place /home on a separated partition
- To decrease the impact of a full /tmp file system, place /tmp on a separated partition
- Disable drivers like USB storage when not used, to prevent unauthorized storage or data
- The version in BIND can be masked by defining 'version none' in the configuration file
- Purge old/removed packages (66 found) with aptitude purge or dpkg --purge command. This
- Update your system with apt-get update, apt-get upgrade, apt-get dist-upgrade and/or
- Access to CUPS configuration could be more strict. [PRNT-2307]
- Disable iptables kernel module if not used or make sure rules are being used [FIRE-4512]
- Harden PHP by disabling risky functions [PHP-2320]
- Check what deleted files are still in use and why. [LOGG-2190]
- Add a legal banner to /etc/issue, to warn unauthorized users [BANN-7126]
- Add legal banner to /etc/issue.net, to warn unauthorized users [BANN-7130]
- Enable sysstat to collect accounting (disabled) [ACCT-9626]
- Check ntpq peers output [TIME-3116]
- Check ntpq peers output [TIME-3124]
- Check ntpq peers output for time source candidates [TIME-3128]
- One or more sysctl values differ from the scan profile and could be tweaked [KRNL-6000]
- Harden the system by removing unneeded compilers. This can decrease the chance of
- Harden compilers and restrict access to world [HRDN-7222]

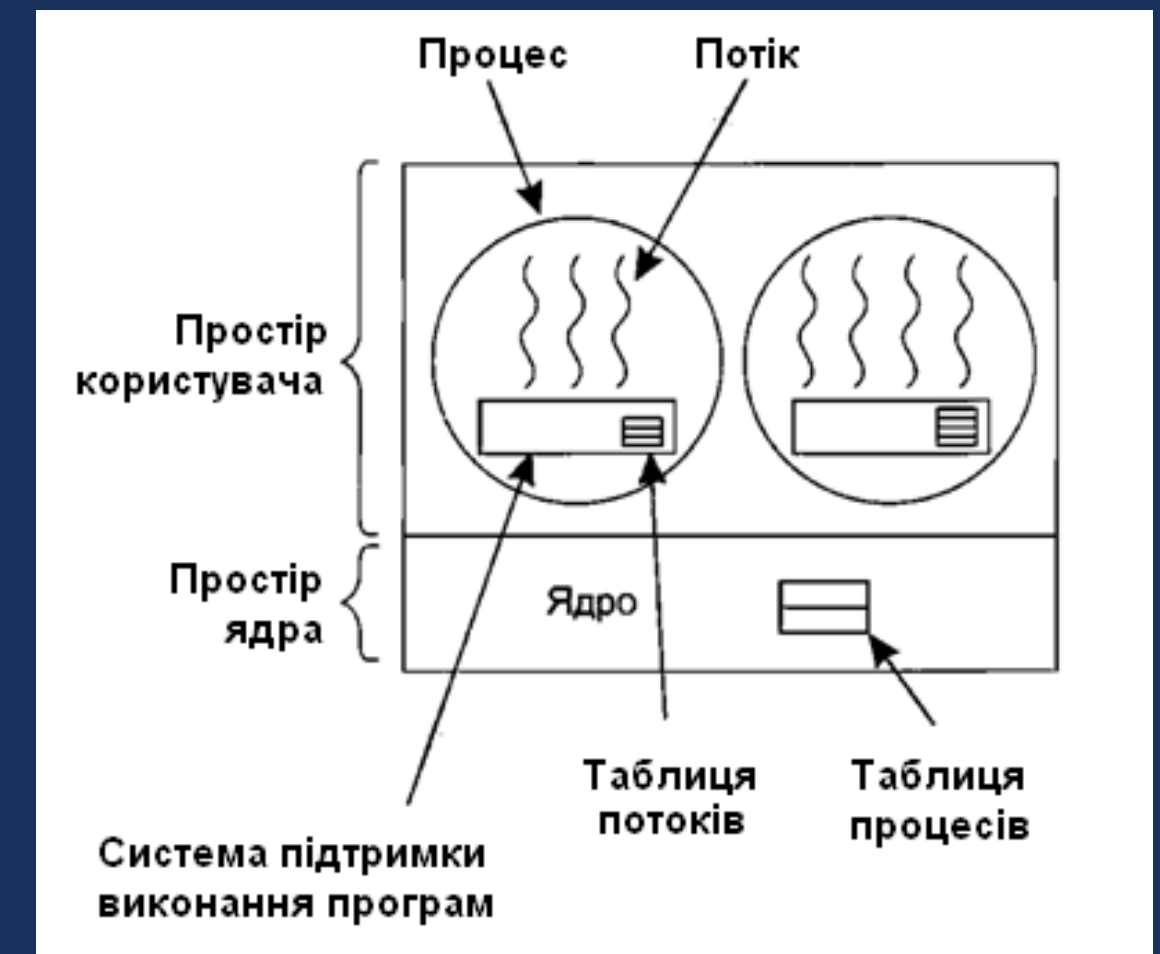
Follow-up:
-----
- Fix findings, see security controls overview and documentation
- Upload data to Lynis Enterprise for further analysis
- Create a report and implementation plan

Enterprise support and plugins available via CISofy - http://cisofy.com
-----
Hardening index : [75]  [#####]

Files:
- Test and debug information      : /var/log/lynis.log
- Report data                    : /var/log/lynis-report.dat
-----
```

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) [7/64])  
Cost 1 (algorithm [1:descript 2:md5crypt 3:sunmd5 4:bcrypt 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
```

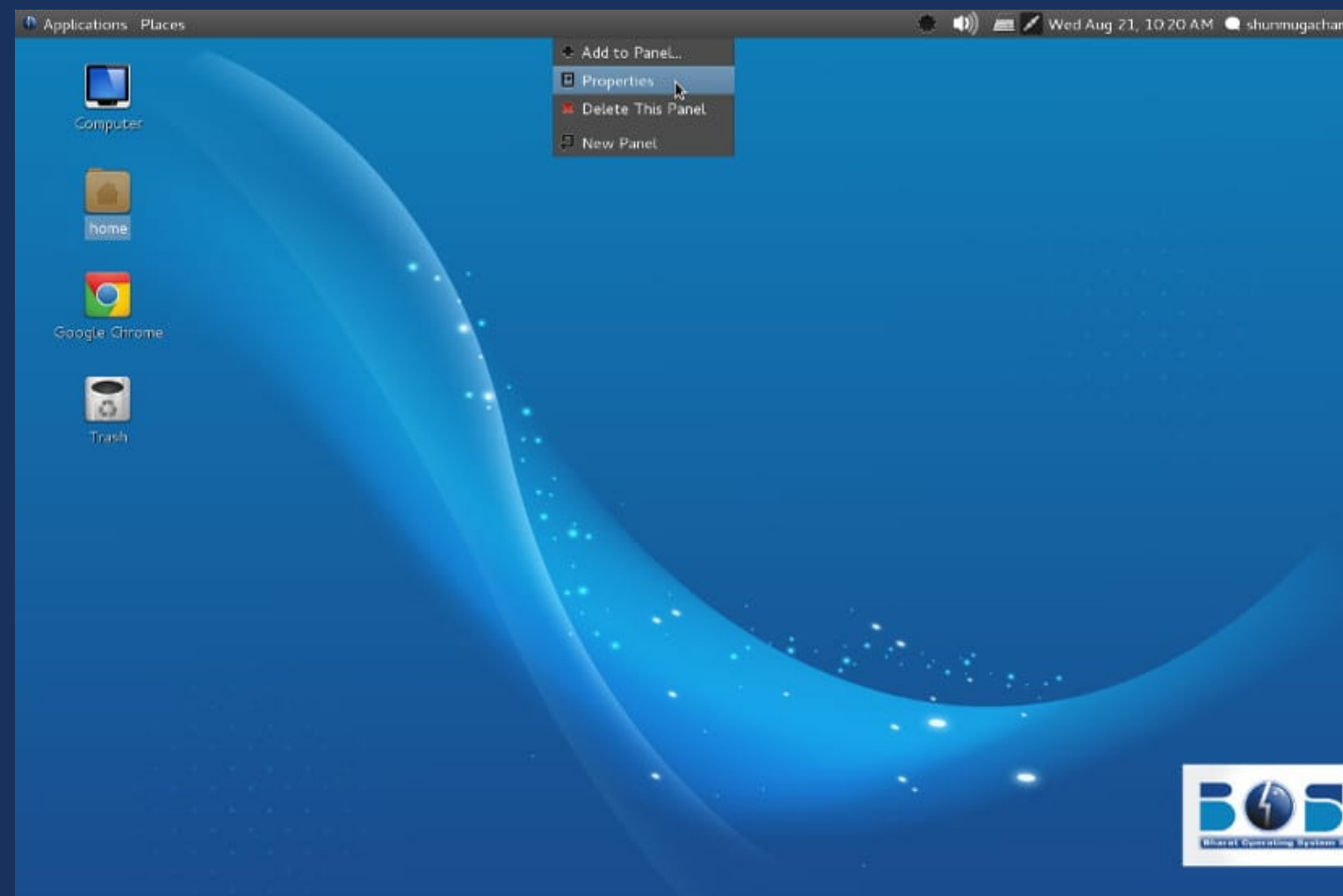
Підсекція «Безпека мереж»

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



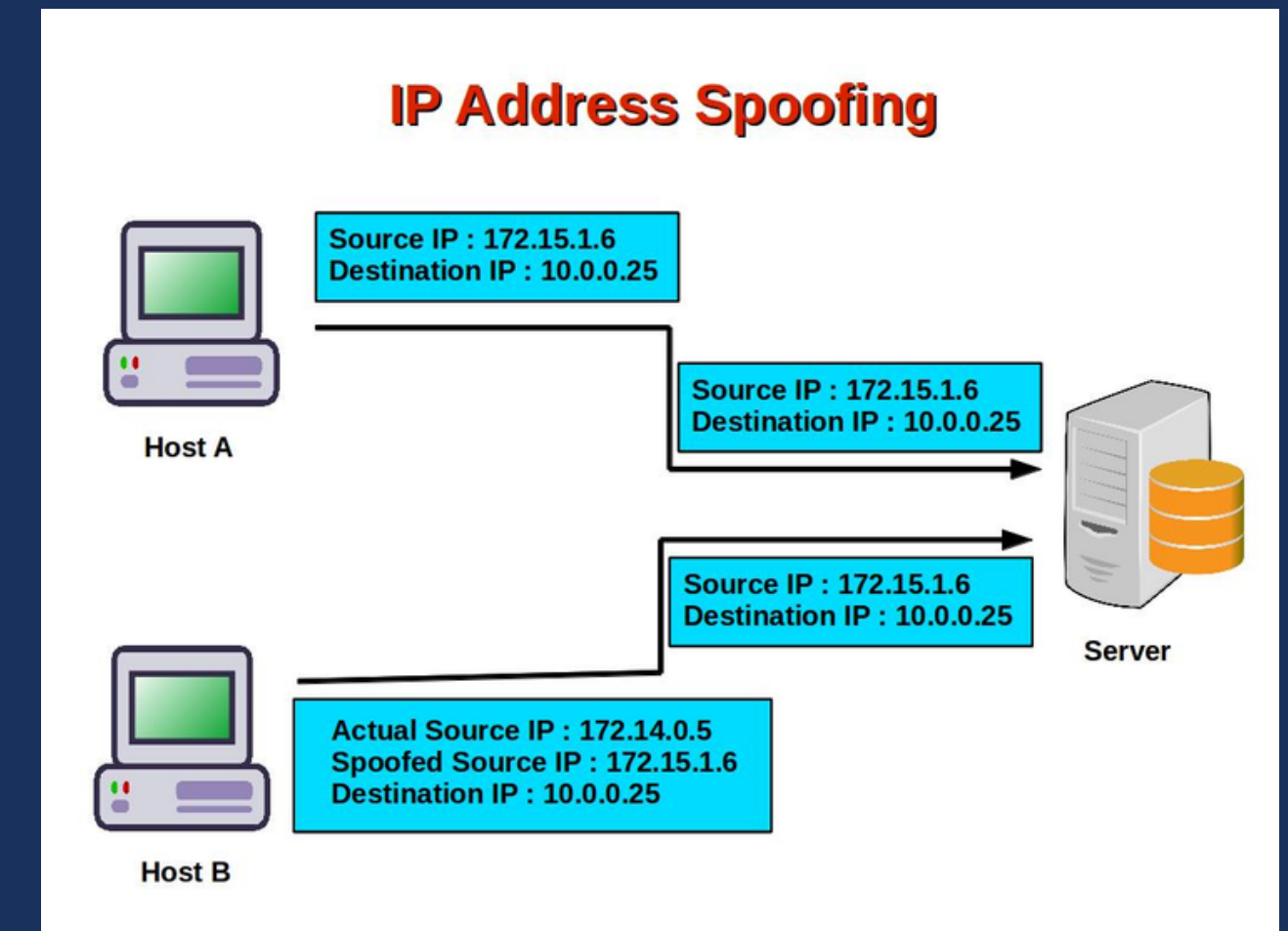
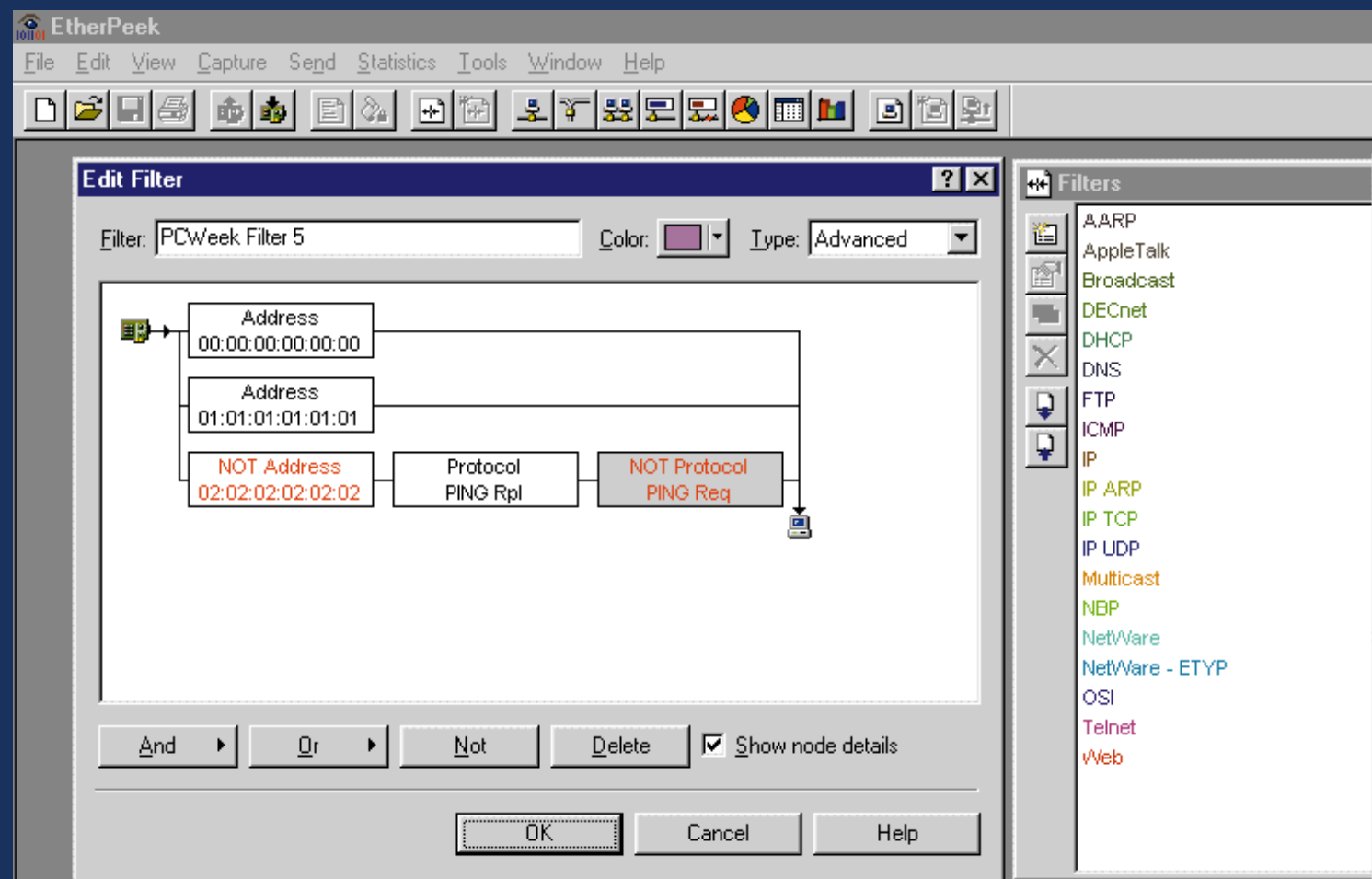
Підсекція «Безпека мереж»

- Практичні навички роботи із захищеною операційною системою BBOS



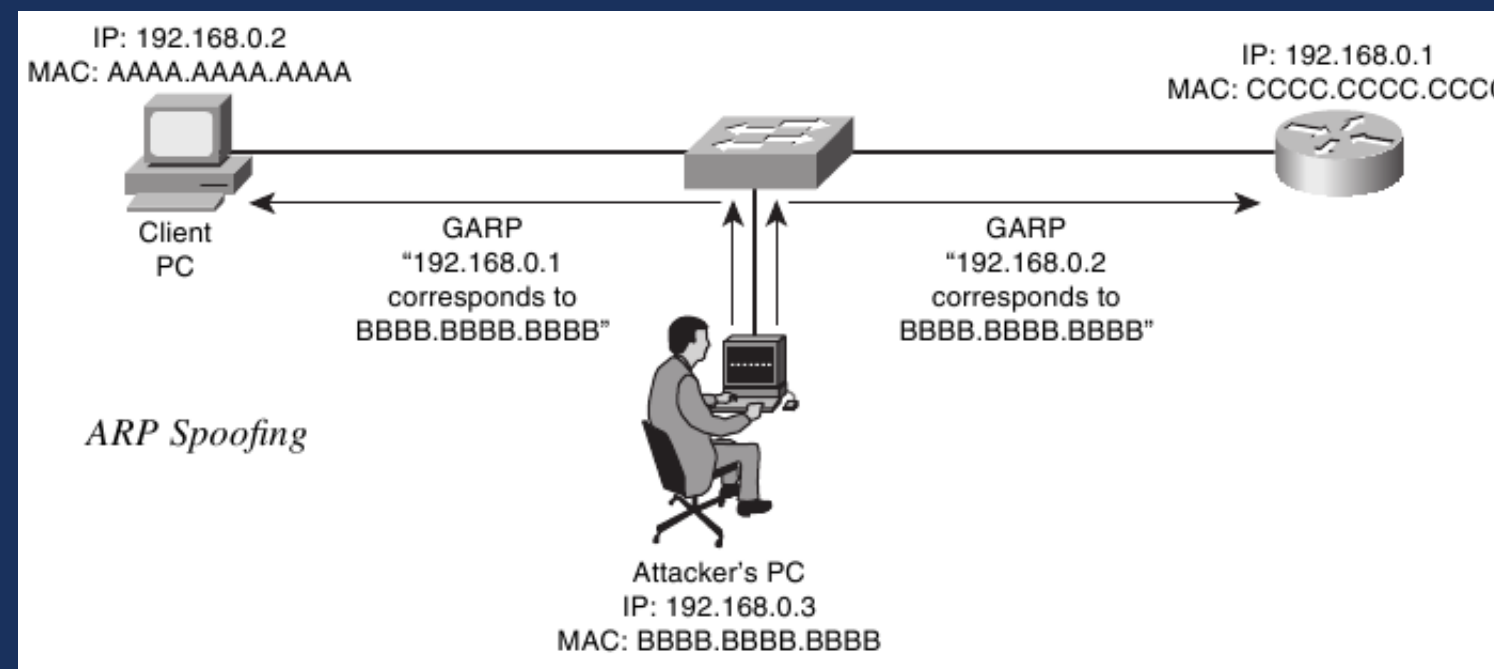
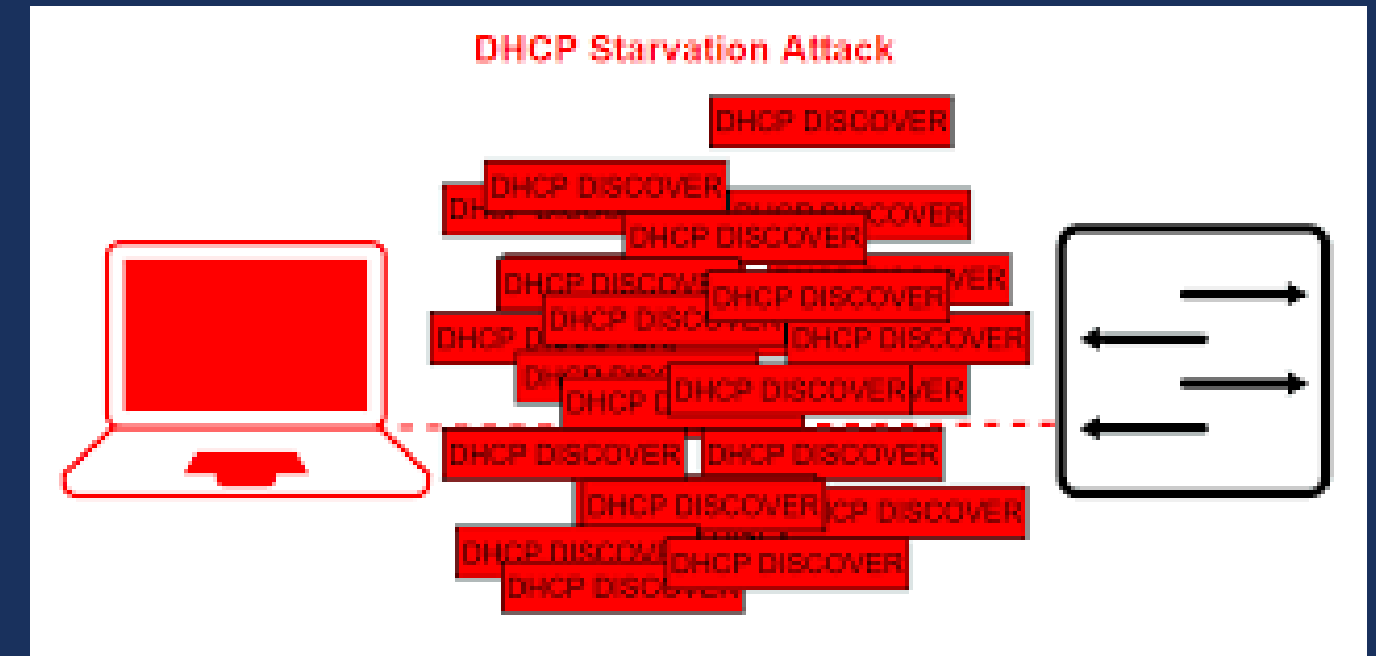
Підсекція «Безпека мереж»

- 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.



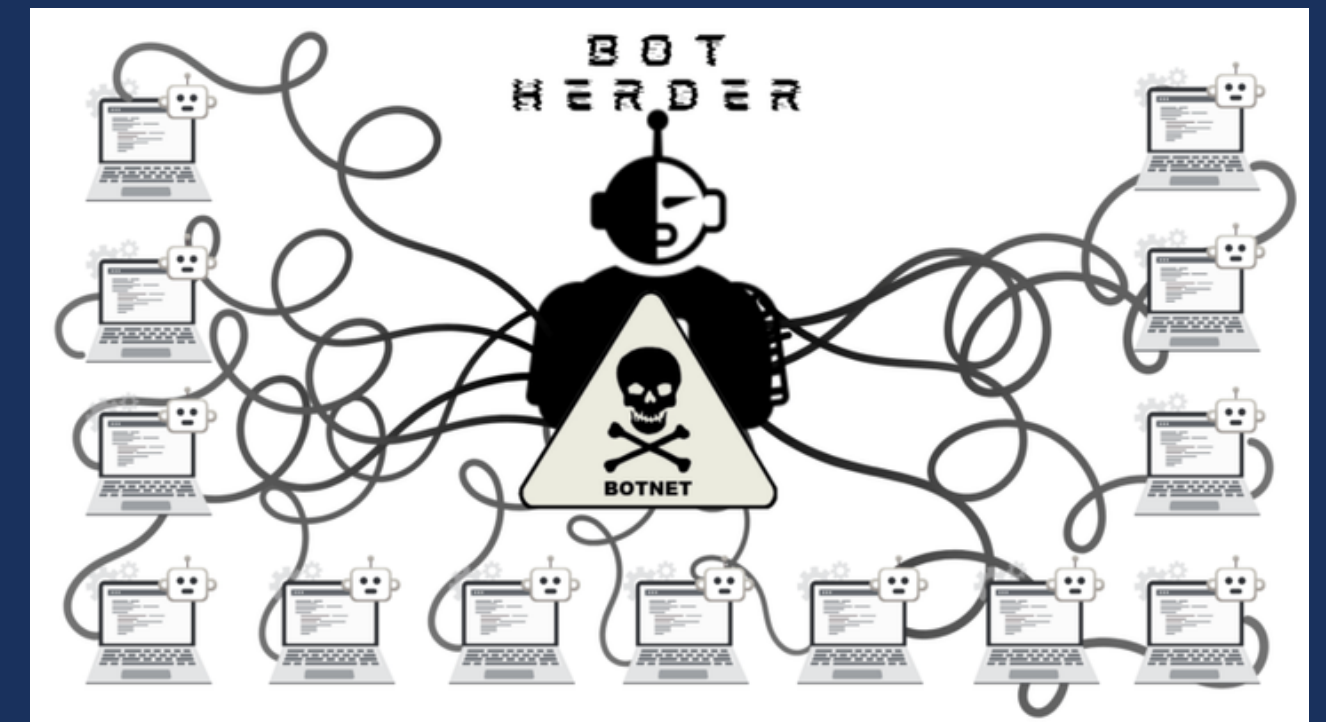
Підсекція «Безпека мереж»

- 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



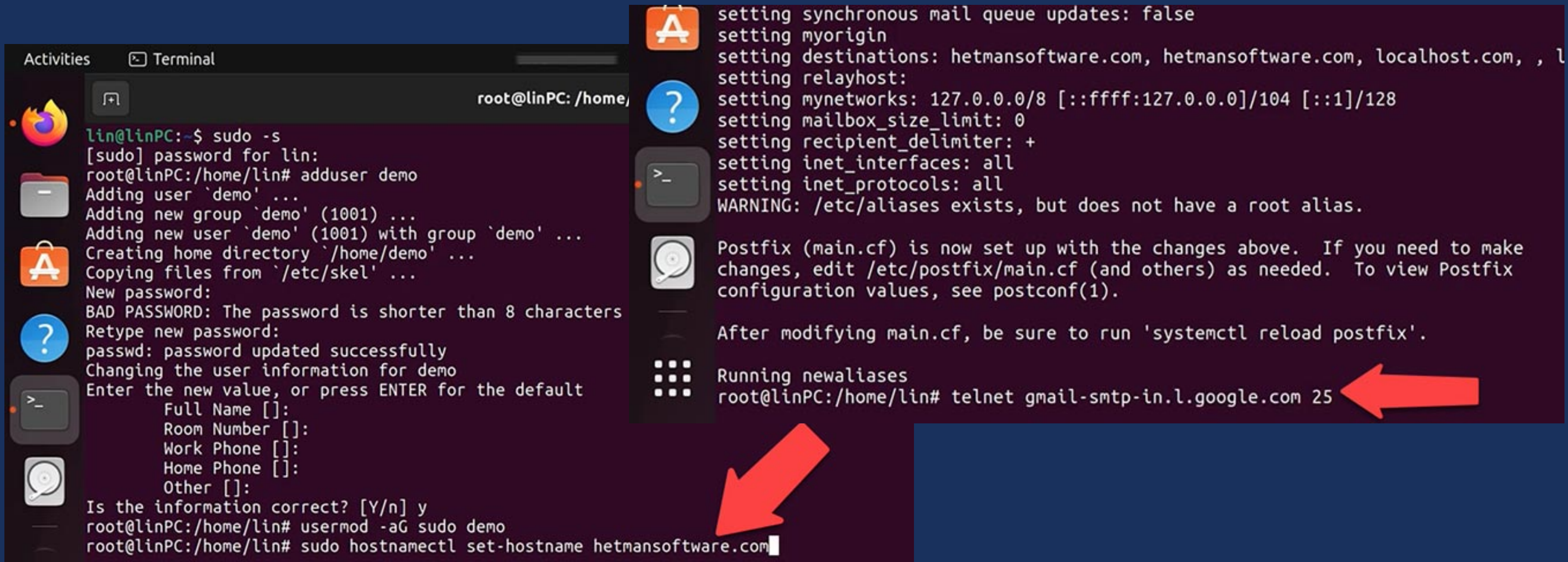
Підсекція «Безпека мереж»

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



Підсекція «Безпека мереж»

- Адміністрування Ubuntu-сервера лабораторії кібербезпеки



```
lin@linPC:~$ sudo -s
[sudo] password for lin:
root@linPC:/home/lin# adduser demo
Adding user `demo' ...
Adding new group `demo' (1001) ...
Adding new user `demo' (1001) with group `demo' ...
Creating home directory `/home/demo' ...
Copying files from `/etc/skel' ...
New password:
BAD PASSWORD: The password is shorter than 8 characters
Retype new password:
passwd: password updated successfully
Changing the user information for demo
Enter the new value, or press ENTER for the default
  Full Name []:
  Room Number []:
  Work Phone []:
  Home Phone []:
  Other []:
Is the information correct? [Y/n] y
root@linPC:/home/lin# usermod -aG sudo demo
root@linPC:/home/lin# sudo hostnamectl set-hostname hetmansoftware.com
```

```
setting synchronous mail queue updates: false
setting myorigin
setting destinations: hetmansoftware.com, hetmansoftware.com, localhost.com, , l
setting relayhost:
setting mynetworks: 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
setting mailbox_size_limit: 0
setting recipient_delimiter: +
setting inet_interfaces: all
setting inet_protocols: all
WARNING: /etc/aliases exists, but does not have a root alias.

Postfix (main.cf) is now set up with the changes above.  If you need to make
changes, edit /etc/postfix/main.cf (and others) as needed.  To view Postfix
configuration values, see postconf(1).

After modifying main.cf, be sure to run 'systemctl reload postfix'.

Running newaliases
root@linPC:/home/lin# telnet gmail-smtp-in.l.google.com 25
```

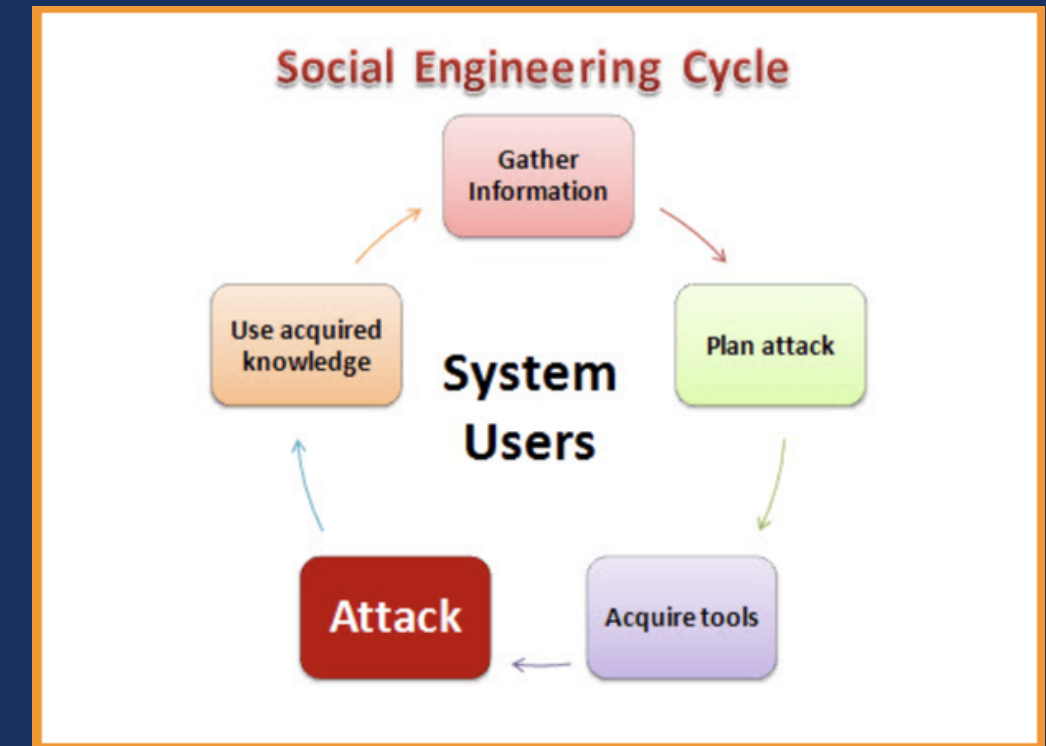
Підсекція «Безпека мереж»

- Отримання практичних навичок роботи з детектором бездротових протоколів



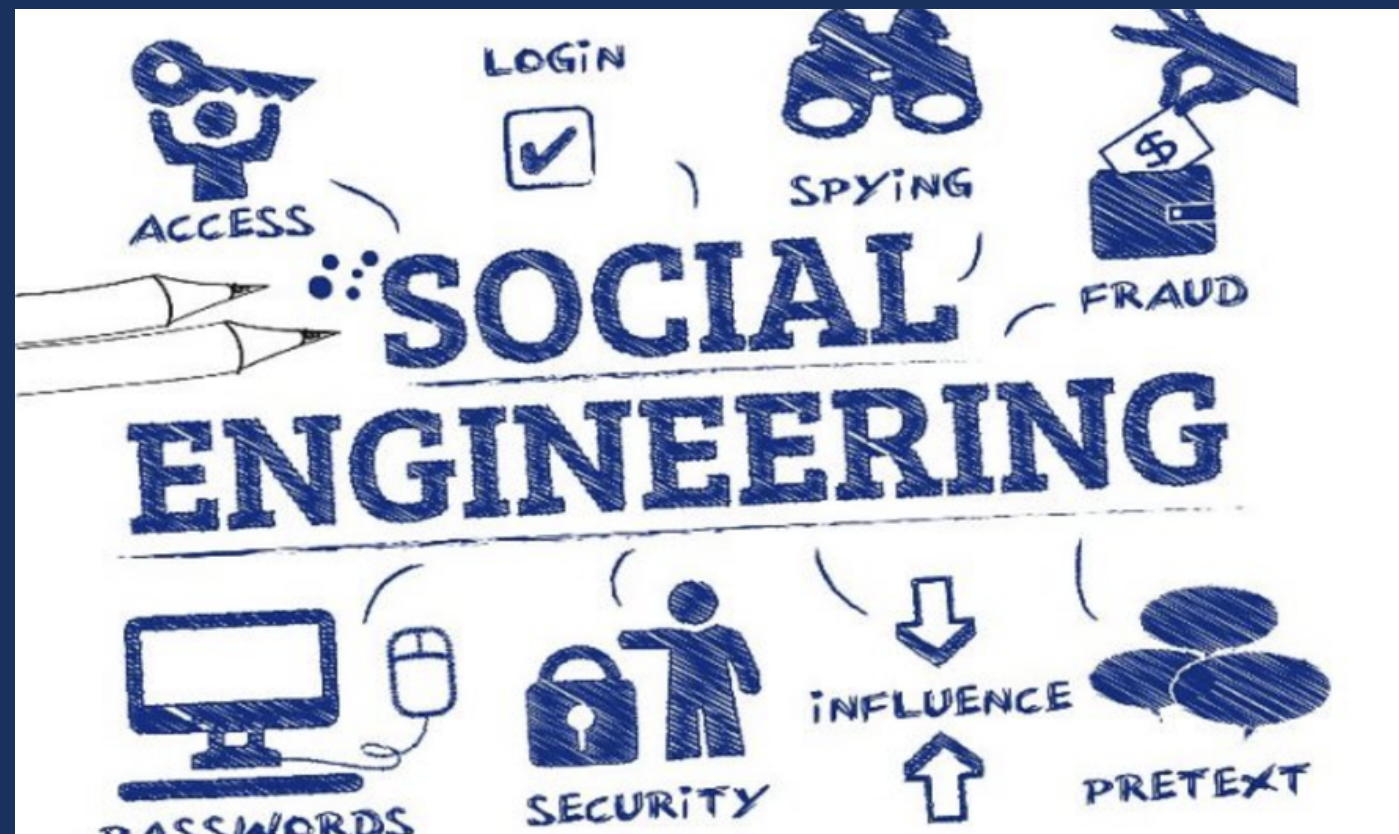
Підсекція «OSINT»

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



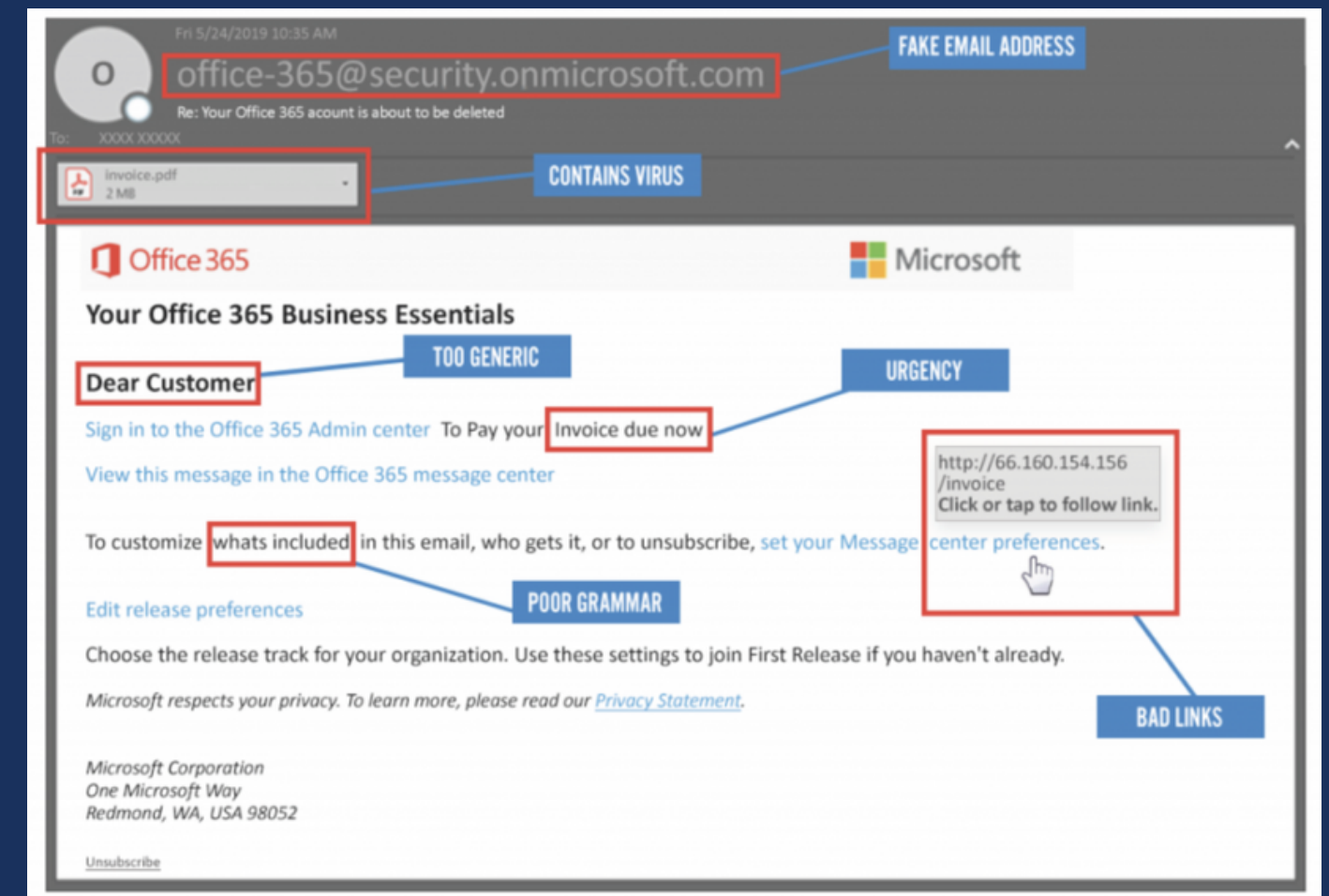
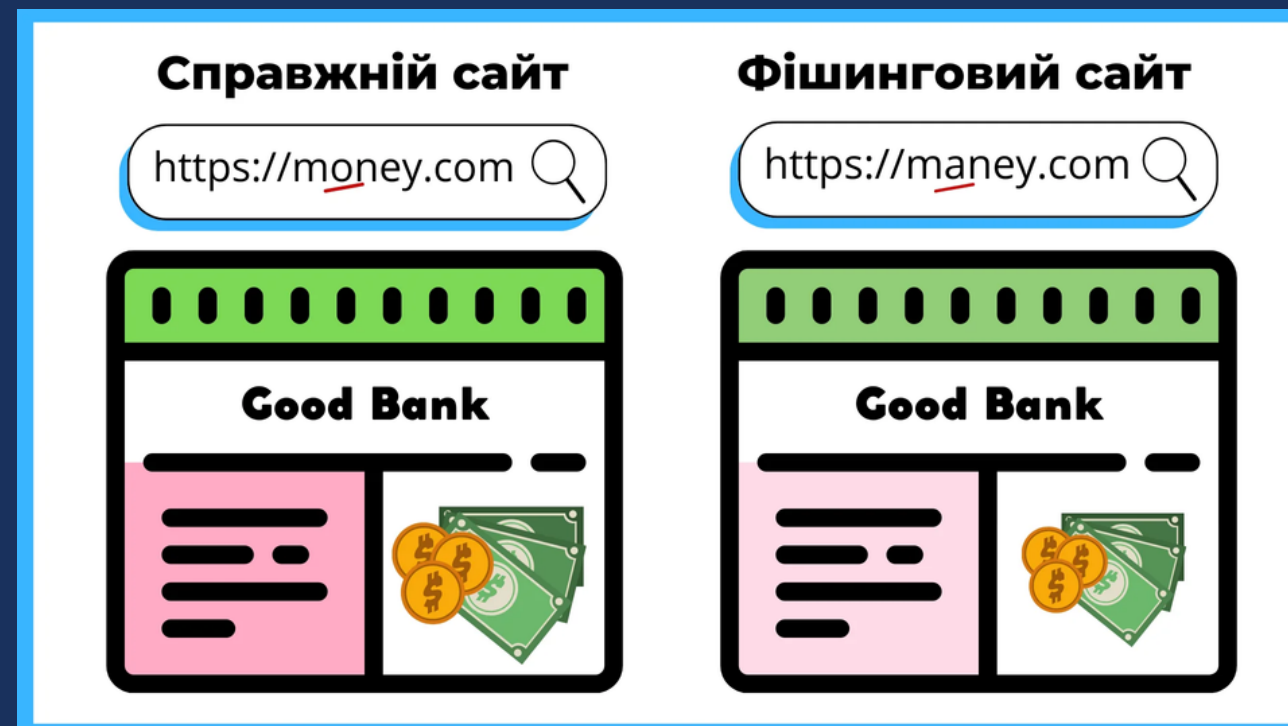
Підсекція «OSINT»

- 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

Зареєструватися ×
Це швидко і просто.

аіваів ваіва

+38201511

.....

День народження [?]
9 бер 2024

Стать [?]
 жінка чоловік Інше

People who use our service may have uploaded your contact information to Facebook. [Learn more.](#)

Натискаючи «Зареєструватися», ви приймаєте наші [Умови](#), [Політику конфіденційності](#) і [Політику щодо файлів cookie](#). Ви можете отримувати сповіщення від нас в SMS, але від них можна відмовитися в будь-який час.

Зареєструватися

Створіть свій профіль ×

Ім'я
342342

Ел. пошта
234234234
Введіть дійсну адресу електронної пошти.

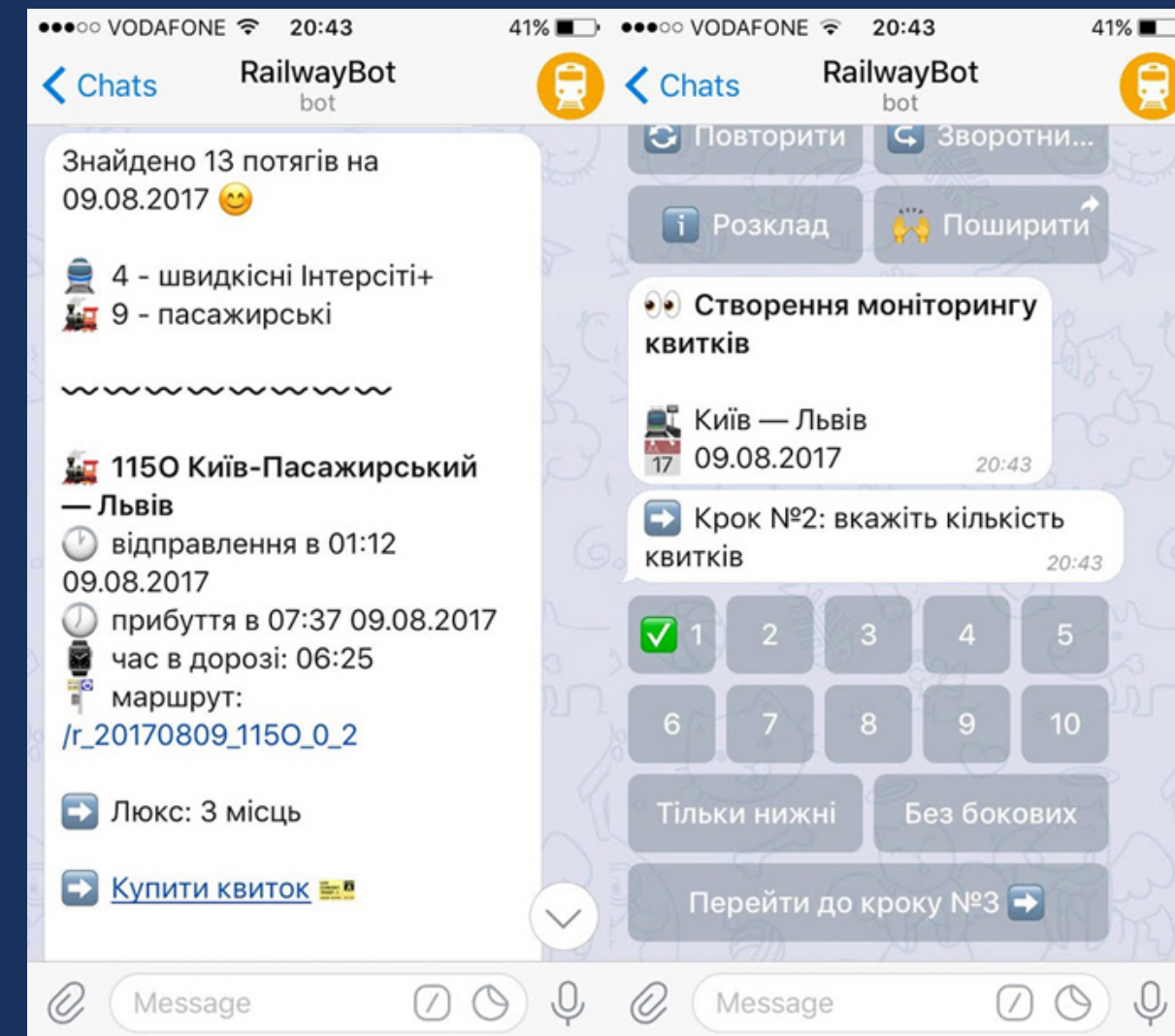
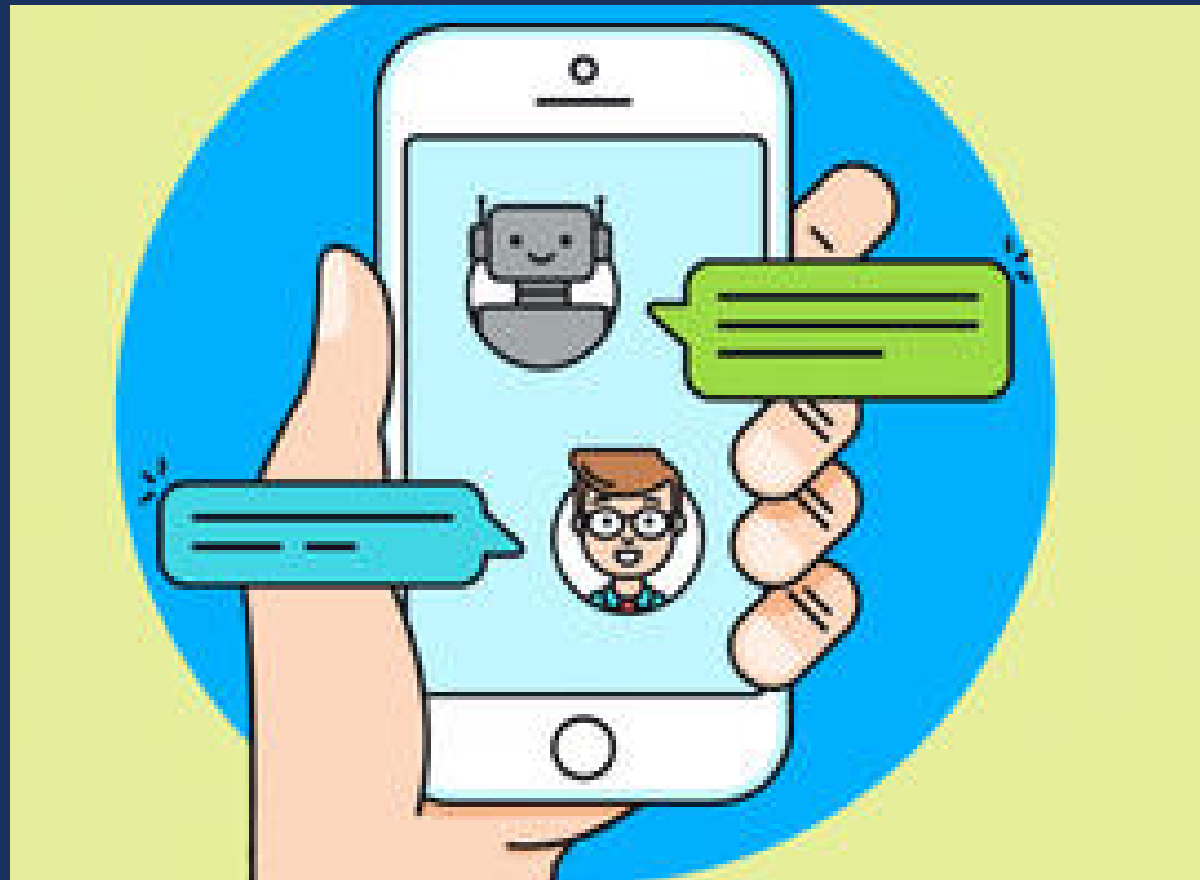
Дата народження
Ці дані не будуть загальнодоступні. Підтвердьте свій вік, навіть якщо це профіль компанії, домашнього улюбленця чи ще чогось.

Місяць День Рік
Лютий 18 2007

Далі

Підсекція «OSINT»

- Практичні навички роботи із Телеграм ботами



Підсекція «OSINT»

- Соціальна діагностика
- Соціальне проектування.



Підсекція «OSINT»

- Соціальне програмування
- Організація впровадження й використання соціальних технологій



Підсекція «OSINT»

- Набуття практичних навичок роботи з пошуковими сервісами за зображеннями



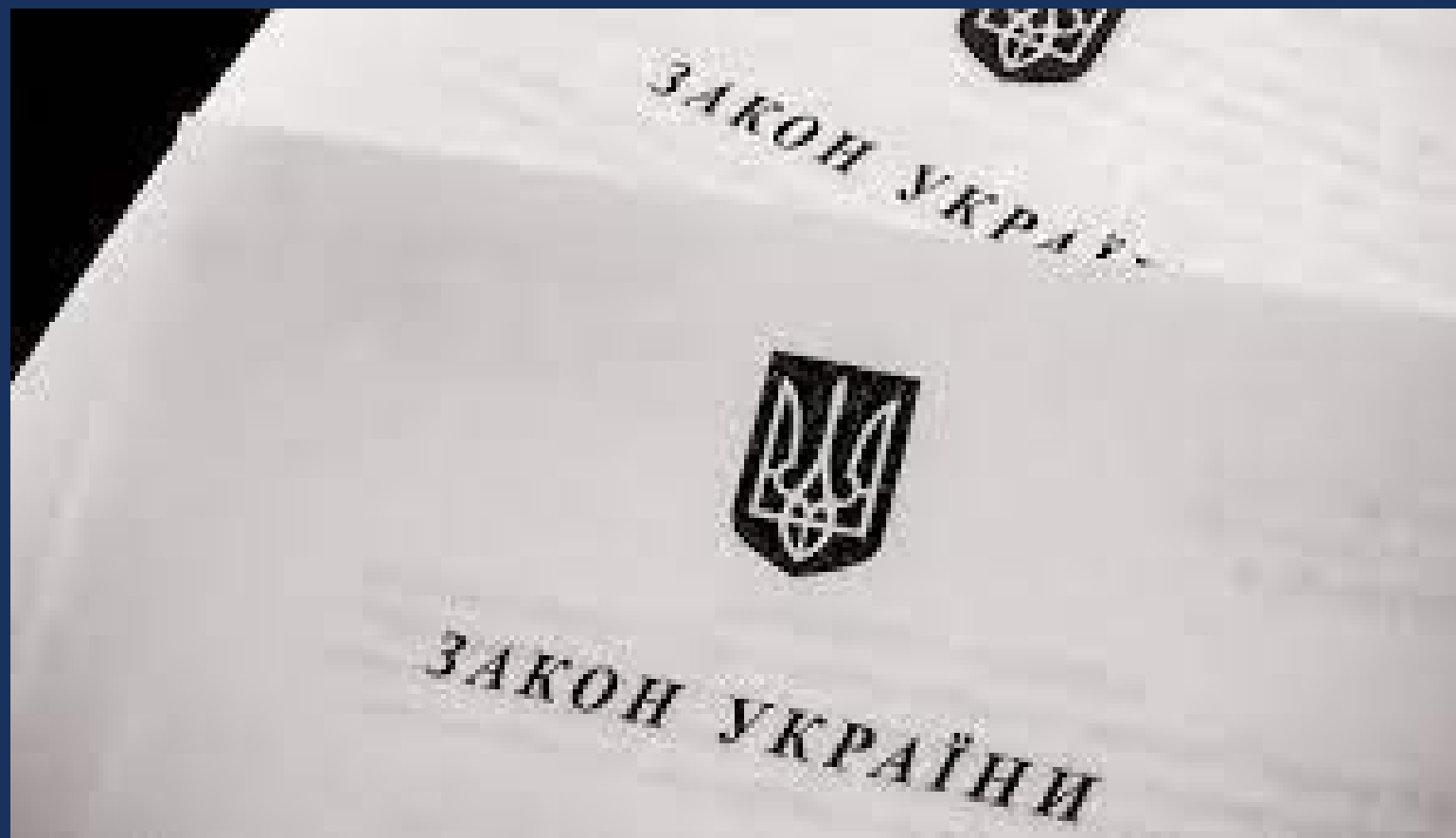
Підсекція «OSINT»

- 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





Як нас знайти:

Вулиця Шевченка, 95,
Чернігів, Чернігівська область,
14035

Перший корпус 108 кабінет

Наша пошта:

cybersec_dep@stu.cn.ua