# ВИКОРИСТАННЯ ВІЛЬНОГО ТА ВІДКРИТОГО ПРОГРАМНОГО ЗАБЕЗПЕЧЕННЯ ДЛЯ ТЕСТУВАННЯ НА ПРОНИКНЕННЯ В КОМП'ЮТЕРНІ МЕРЕЖІ ТА СИСТЕМИ

Національний університет Львівська політехніка

Андріян Піскозуб, 2013

# БЕЗПЕКА, ЗАХИЩЕНІСТЬ – НЕВІД'ЄМНІ АТРИБУТИ СЬОГОДЕННЯ В БУДЬ-ЯКІЙ СФЕРІ

# Нормативні чинники



- стандарти,
- закони,
- інфраструктурні рішення,
- бібліотеки кращих практик

Мета в них одна – забезпечити виконання організаційних та технічних рекомендацій, що дозволить підняти рівень захищеності

# ISO/IEC 27001:2005



забезпечує підтримку рішень на основі ITIL (Information Technology Infrastructure Library) та COBIT (Control Objectives for Information and Related Technology.

Згідно з ISO 27001:2005 на підприємстві створюється система управління інформаційною безпекою (СУІБ), яка повинна відповідати усім вимогам міжнародних стандартів в галузі ІБ

# Задачі організації згідно стандартів



- оцінка своїх активів
- оцінка специфічних ризиків, яким піддається її діяльність щодо збереження, конфіденційності та цілісності інформації
- сформування політики безпеки, яка дозволить уникнути або мінімізувати ці ризики і, таким чином, зробити Ваш бізнес безпечним.

# Задачі організації згідно стандартів безпеки



Ефективна політика безпеки повинна бути **проактивною**, щоб забезпечити достатній захист від різних відомих і невідомих атак і випадків.

Не лише підтримка в актуальному стані програмного та апаратного забезпечень!

Людські помилки - неправильна конфігурація чи підходи, що робить всю мережу вразливою для атак!

# Тестування на проникнення



Наша мета –

висвітлення методики тестування на проникнення (етичного хакінгу) як засобу забезпечення всебічного рівня безпеки IT – інфраструктури компанії

# Тестування на проникнення



Тестування на проникнення (пентест) – невід'ємна компонента повного аудиту безпеки компанії.

Для Payment Card Industry Data Security Standard (PCI DSS) необхідно проводити пентест щорічно і після кожної зміни конфігурації систем

Пентест – перевірка стану ефективності захисту системи через застосування технік, якими користуються реальні зловмисники

# Етичний хакінг



базується на правилах застосування (rules of engagement), яких повинен дотримуватися аудитор, якого наймає організація для проведення тестування на проникнення до її інформаційних ресурсів:

- як слід проводити тестування;
- визначення масштабів тестування;
- підготовка плану тестування;
- перебіг процесу тестування;
- забезпечення конфіденційної звітності по проведеній роботі тощо

# Види пентестів



- Electronic Penetration Test
- Social Engineering Penetration Test
- Physical Penetration Test

Разом повний пентест

# Підходи для проведення пентесту



- Black-Box
- White-Box
- Grey-Box

# Методики оцінки системи безпеки



За допомогою цих методик оцінки можна легко скоротити час на проведення важливих і складних завдань оцінки системи безпеки в залежності від його розміру та складності.

# Методики оцінки системи безпеки



Методики з відкритим кодом, покликані задовольнити потреби оцінки безпеки:

- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Open Web Application Security Project (OWASP) Top Ten
- Web Application Security Consortium Threat Classification (WASC-TC)

# Методики оцінки системи безпеки



Наведені методики покликані допомогти фахівцям з безпеки вибрати кращу стратегію, яка могла б вписатися у вимоги клієнтів, і кваліфікувати підходящий прототип тестування.

Перші дві методики забезпечують загальні принципи і методи, забезпечуючи тестування безпеки для практично будь інформаційних активів,

останні дві – відповідно в основному стосуються оцінки безпеки на прикладному рівні.

# Оцінка захищеності



Оцінка політики інформаційної безпеки організації та процесів з метою їх відповідності галузевим стандартам IT, діючим законам та нормативним вимогам

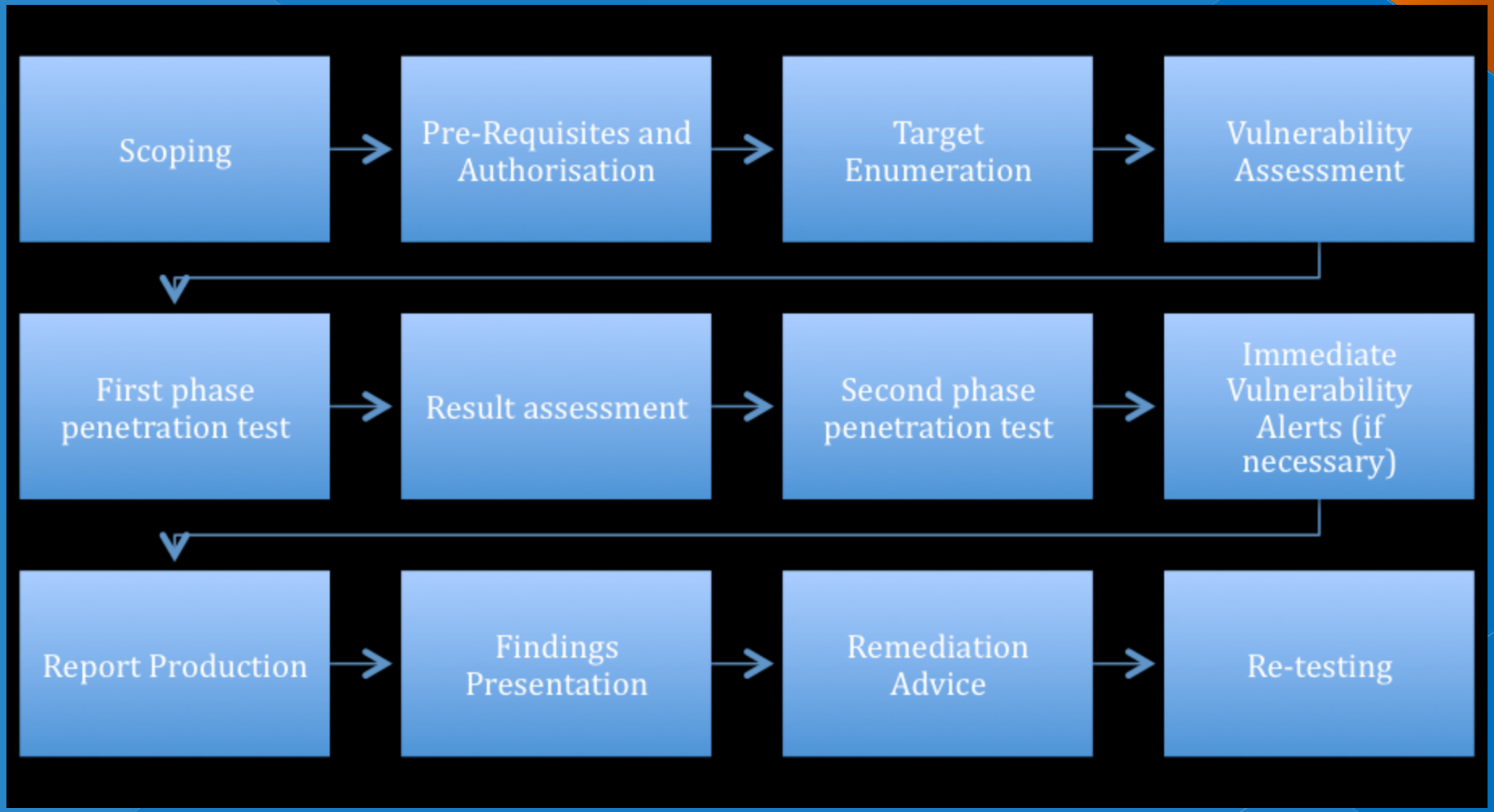
Виявлення та оцінка залежності бізнесу від IT-сервісів

Проведення оцінки вразливості і тестування на проникнення для  виявлення в системі вразливостей, які можуть призвести до потенційних ризиків для інформаційних активів. Сюди включають:

# Оцінка захищеності



- виявлення неправильних конфігурацій і їх усунення
- визначення ризиків, пов'язаних з IT-технологіями та їх вирішення
- визначення ризиків,  пов'язаних з людьми або бізнес-процесами та їх вирішення укріплення існуючих процесів і технологій
- застосування передових практик і процедур для підтримки ініціатив безперервності бізнесу


Scoping
Pre-Requisites and Authorisation
Target Enumeration
Vulnerability Assessment
First phase penetration test
Result assessment
Second phase penetration test
Immediate Vulnerability Alerts (if necessary)
Report Production
Findings Presentation
Remediation Advice
Re-testing

# OWASP



- OWASP Application Security Verification Standard
- OWASP Development Guide
- OWASP Testing Guide
- OWASP Code Review Guide
- OWASP ZAP Project
- OWASP Top Ten
- OWASP Software Assurance Maturity Model
- Webgoat

# Google hacking



Google Dorks, Google scanning, Search engine hacking

Google hacking – хакерська техніка, що використовує Google Search та інші Google аплікації для виявлення дір в безпеці в конфігурації і комп'ютерний код, які веб-сайти використовують

Google hacking передбачає використання додаткових операторів в пошуковій системі Google, щоб знайти конкретні текстові рядки в результатах пошуку.

**http://www.exploit-db.com/google-dorks/**

# Google hacking



Пошук важливої інформації MySqlServer , "uid, and password" в web.config через ftp:
**filetype:config inurl:web.config inurl:ftp**

Пошук login-сторінок:

**allintext: "Please login to continue..." "ZTE Corporation. All rights reserved."**

Пошук c99 backdoor

**filetype:php inanchor:c99 inurl:c99 intitle:c99shell -seeds -marijuana**

Пошук username та password з Microsoft FrontPage серверів:

**"#-Frontpage-" inurl:administrators.pwd**

# Автоматизація процесу тестування



Раніше цим займалися tiger team - команди

Зараз – використання автоматизованих рішень

# Спеціалізовані дистрибутиви



BackTrack 5 R3 (Linux Ubuntu 10.04) до останнього часу найпопулярніший.

Kali Linux правонаступник BackTrack (Linux Debian):

- вища стійкість,
- великі депозитарії ОС Debian,
- багатомовну підтримку
- сумісність з Filesystem Hierarchy Standard (FHS)
- підтримка APM платформ - rk3306 mk/ss808, Raspberry Pi, ODROID U2/X2 та Samsung Chromebook.

# Етапи пентесту



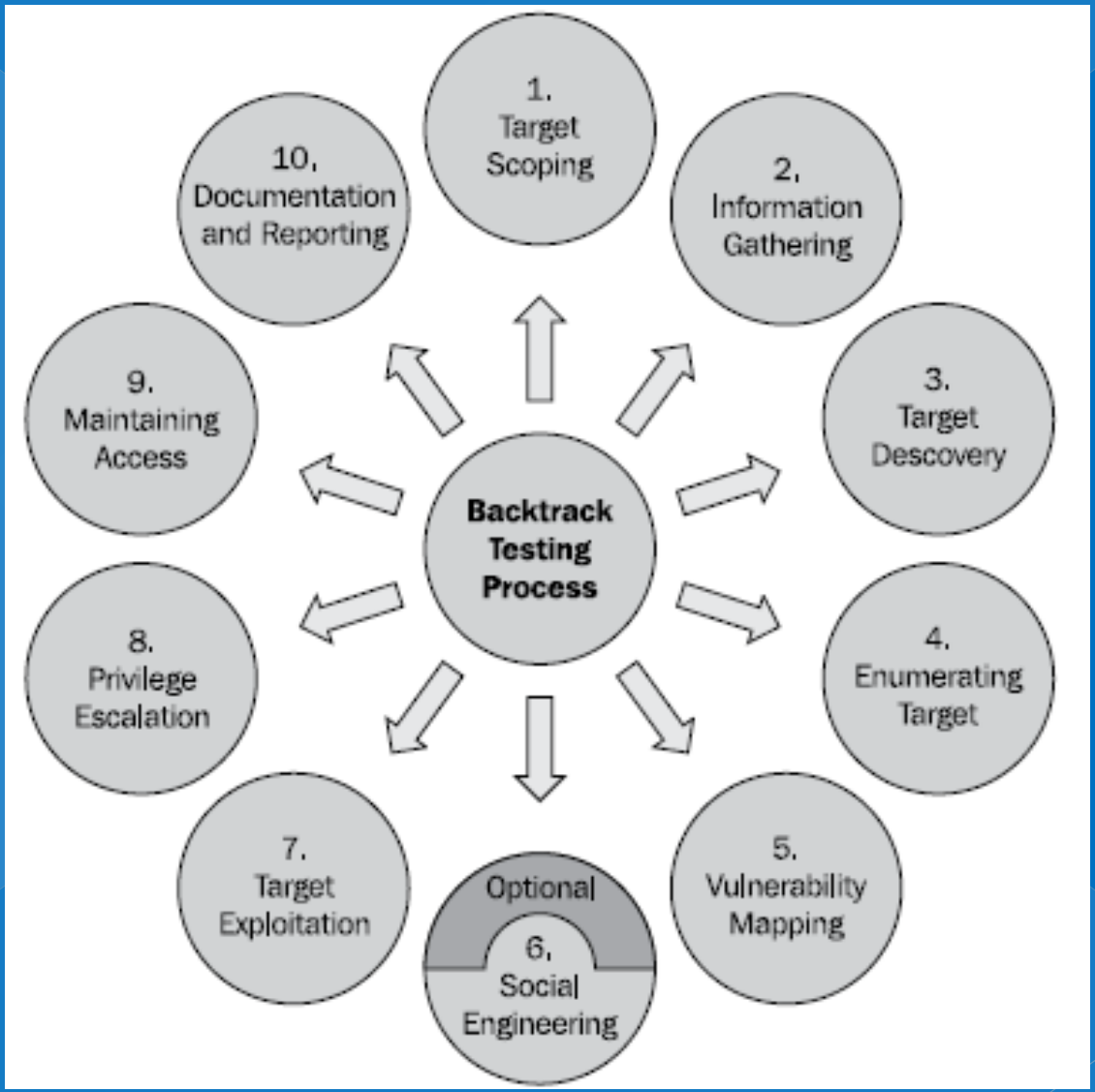
10 етапів:

- визначення меж тестування (Target Scoping),
- збір інформації про цільову систему (Information Gathering),
- виявлення працюючих цільових хостів (Target Discovery),
- виявлення працюючих сервісів на цільових хостах (Enumerating Target),
- визначення вразливостей на цільових хостах (Vulnerability Mapping),

# Етапи пентесту (продовж.)



- соціальна інженерія (Social Engineering),
- злам цільових систем (Target Exploitation),
- підвищення привілеїв на цільових системах (Privilege Escalation),
- збереження доступу після зламу цільових систем (Maintaining Access),
- документація та звітність (Documentation and Reporting)


1. Target Scoping
2. Information Gathering
3. Target Descovery
4. Enumerating Target
5. Vulnerability Mapping
Optional
6. Social Engineering
7. Target Exploitation
8. Privilege Escalation
9. Maintaining Access
10. Documentation and Reporting
Backtrack Testing Process

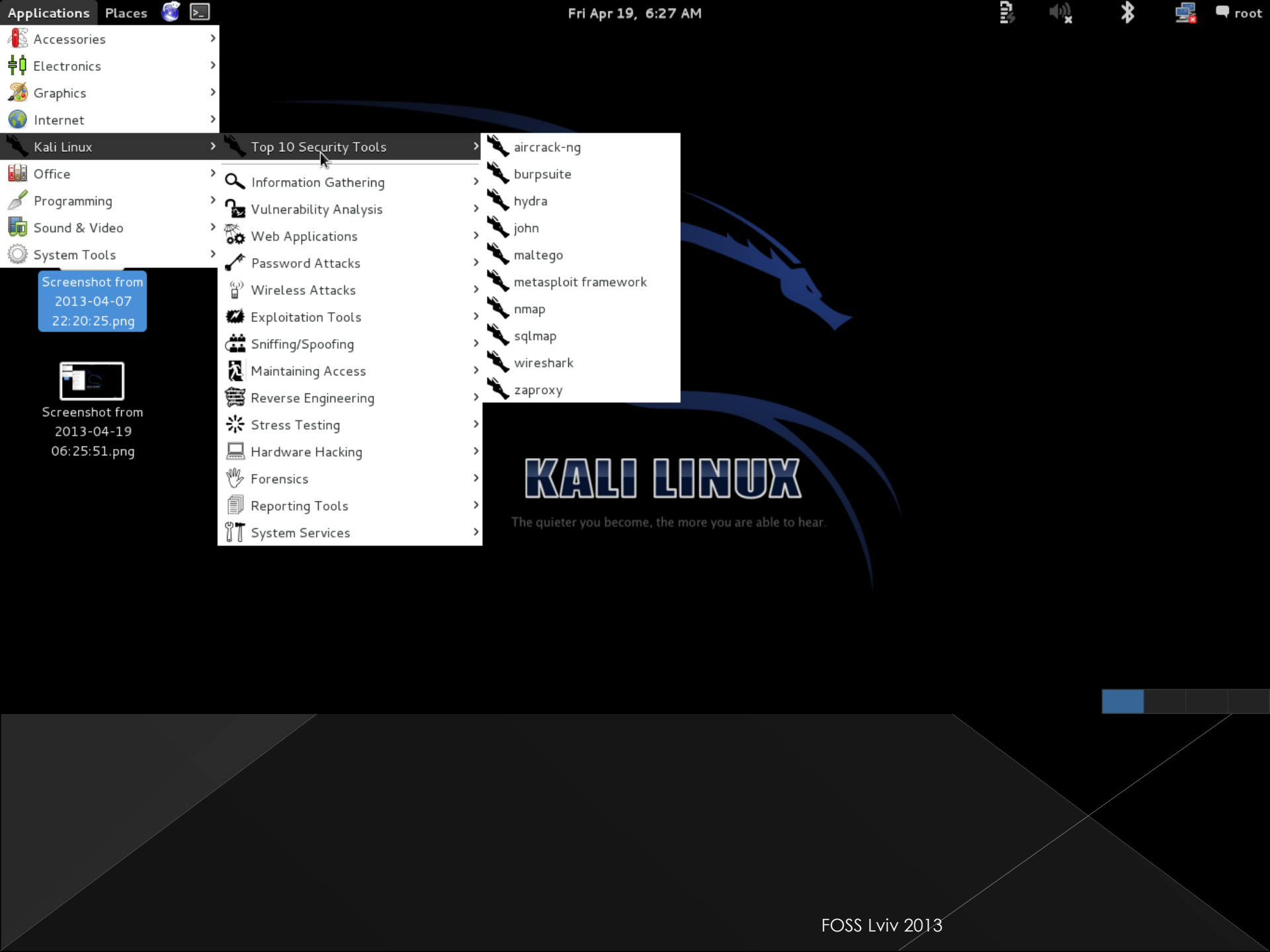
# ПЗ в складі Backtrack / Kali Linux



Біля 300 open source security інструментів, організованих в наступні групи:

- “Information Gathering”,
- “Vulnerability Assessment”,
- “Exploitation Tools”,
- “Privilege Escalation”,
- “Maintaining Access”,
- “Reverse Engineering”,
- “RFID Tools”,
- “Stress Testing”,
- “Forensics”,


Applications
Places
System
Mon Apr 15, 11:04 AM
Accessories
BackTrack
Graphics
Internet
Office
Other
Sound & Video
System Tools
Wine
xprofile
Information Gathering
Vulnerability Assessment
Exploitation Tools
Privilege Escalation
Maintaining Access
Reverse Engineering
RFID Tools
Stress Testing
Forensics
Reporting Tools
Services
Miscellaneous
<< back | track 5 r3
the quieter you become, the more you are able to hear


Applications
Places
Fri Apr 19, 6:27 AM
root
Accessories
Electronics
Graphics
Internet
Kali Linux
Office
Programming
Sound & Video
System Tools
Top 10 Security Tools
Information Gathering
Vulnerability Analysis
Web Applications
Password Attacks
Wireless Attacks
Exploitation Tools
Sniffing/Spoofing
Maintaining Access
Reverse Engineering
Stress Testing
Hardware Hacking
Forensics
Reporting Tools
System Services
aircrack-ng
burpsuite
hydra
john
maltego
metasploit framework
nmap
sqlmap
wireshark
zaproxy
Screenshot from 2013-04-07 22:20:25.png
Screenshot from 2013-04-19 06:25:51.png
KALI LINUX
The quieter you become, the more you are able to hear.

# ПИТАННЯ?



# ДЯКУЮ ЗА УВАГУ!

azpiskozub@gmail.com