МІНІСТЕРСТВО ОСВІТИ І НАУКИ, МОЛОДІ ТА СПОРТУ УКРАЇНИ
НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ІМЕНІ ІГОРЯ СІКОРСЬКОГО»
ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ
Кафедра Інформаційної Безпеки

Аналіз та моніторинг кібербезпеки

Практичне завдання №9

Аналіз політики безпеки в ІТС

Перевірив:
Козленко О. В.

Виконав:
студент IV курсу
групи ФБ-01
Сахній Н. Р.

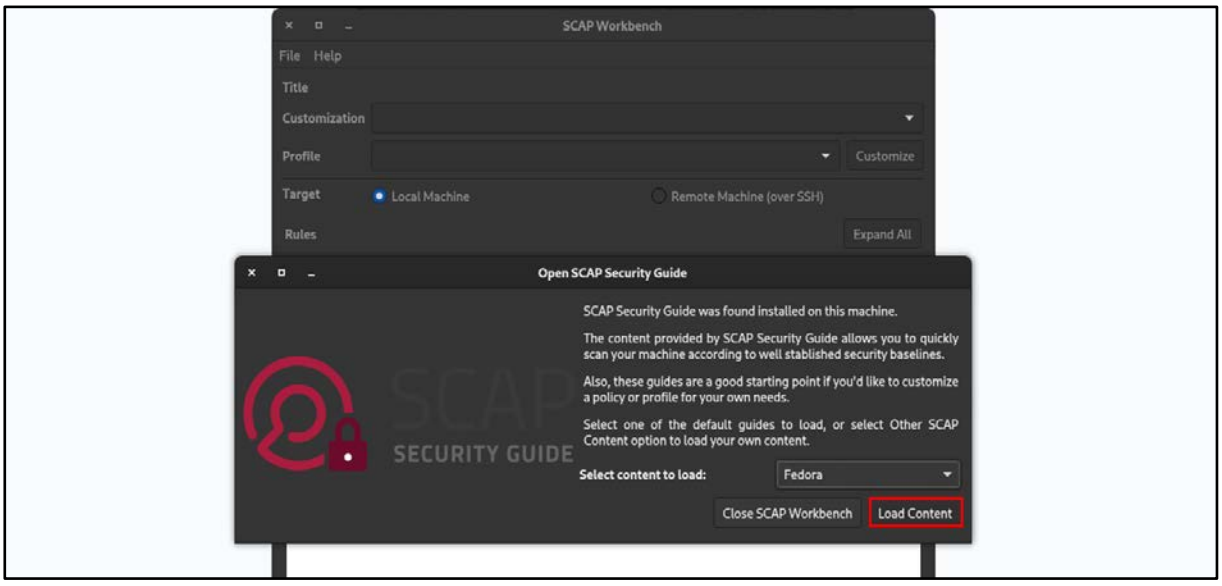
Київ 2024

Мета: Здобуття досвіду з використання хакерських інструментів для пошуку вразливостей у власній ІТС та пошук шляхів усунення цих вразливостей.

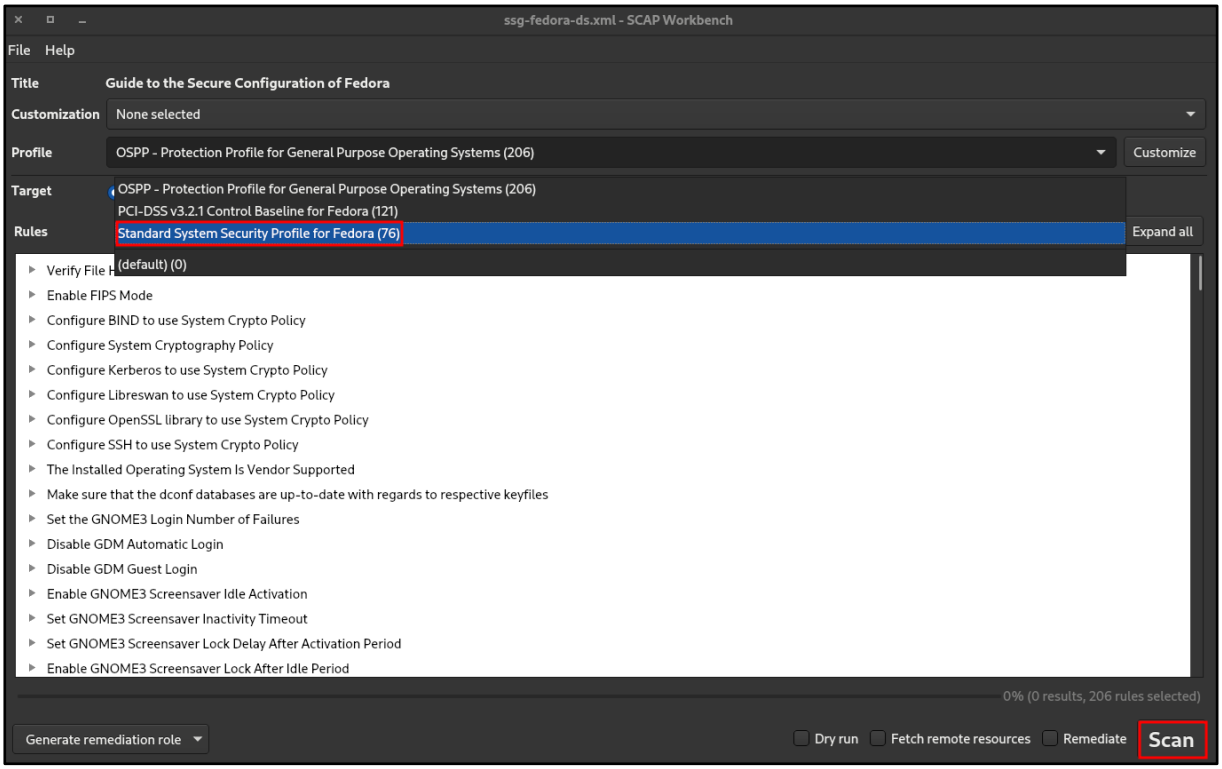
Завдання: Зробити аналіз системи на недотримання вимог політики безпеки за допомогою OpenSCAP.

1. Оцінка політики безпеки за допомогою інструмента SCAP Workbench
   - Встановимо всі необхідні залежності та запустимо наш інструмент:

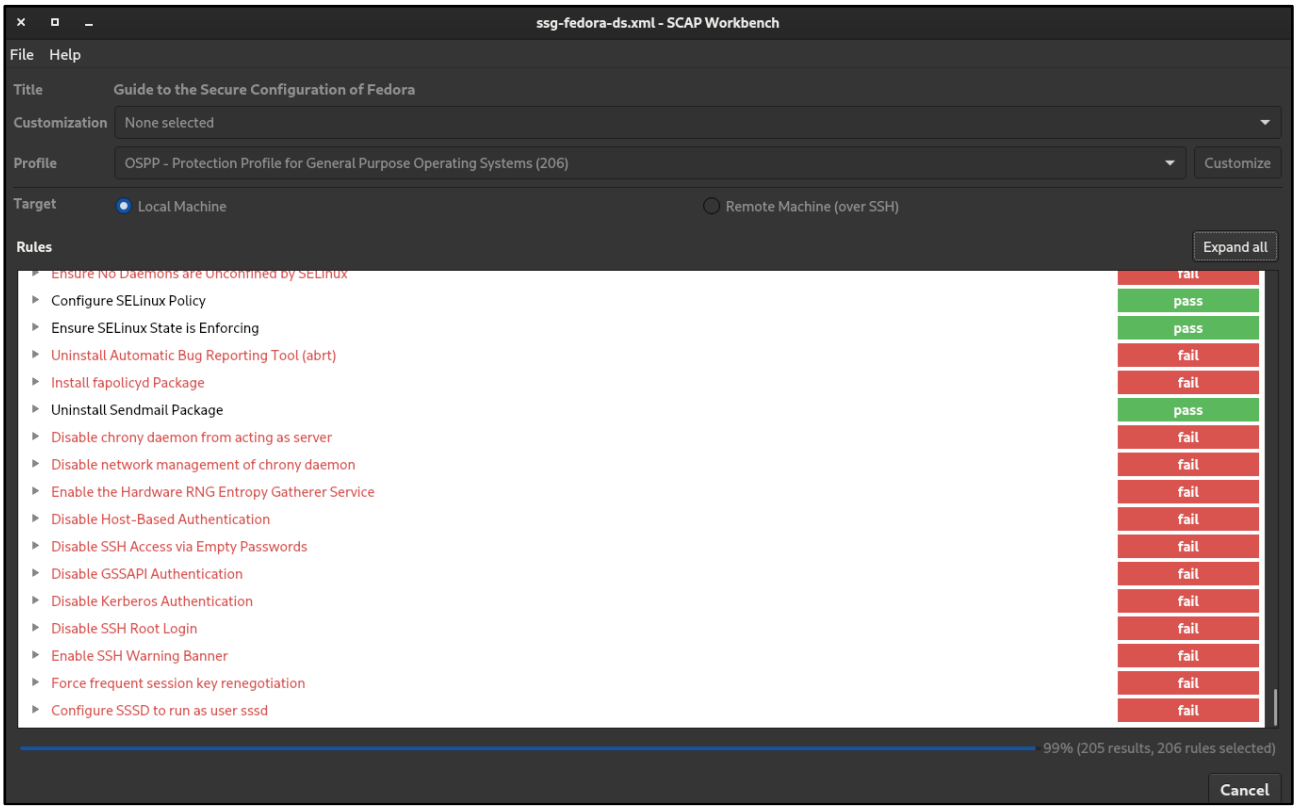
```
> sudo dnf install scap-workbench-1.2.1-12.fc37.x86_64
[sudo] password for yog-sothoth:
Sorry, try again.
[sudo] password for yog-sothoth:
Last metadata expiration check: 0:14:52 ago on чт, 16-бер-2023 19:42:32 +0200.
Dependencies resolved.
================================================================================
 Package                 Architecture    Version                 Repository      Size
================================================================================
Installing:
 scap-workbench          x86_64          1.2.1-12.fc37           fedora         1.8 M
Installing dependencies:
 annobin-docs            noarch          11.11-1.fc37            updates         92 k
 annobin-plugin-gcc      x86_64          11.11-1.fc37            updates        890 k
 ansible-srpm-macros     noarch          1-8.1.fc37              updates        8.6 k
 debugedit               x86_64          5.0-7.fc37              updates         77 k
 dwz                     x86_64          0.14-7.fc37             fedora         129 k
 ed                      x86_64          1.18-2.fc37             fedora          78 k
 efi-srpm-macros         noarch          5-6.fc37                fedora          22 k
 fakeroot                x86_64          1.30.1-1.fc37           updates         92 k
```



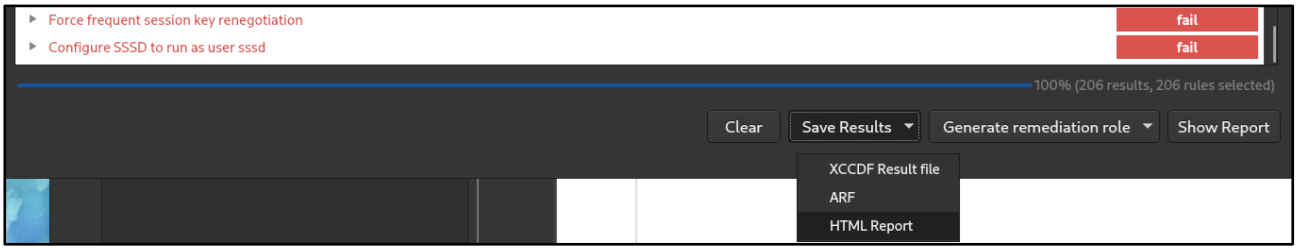
- Обираємо профіль відповідної політики безпеки для нашої Fedora:

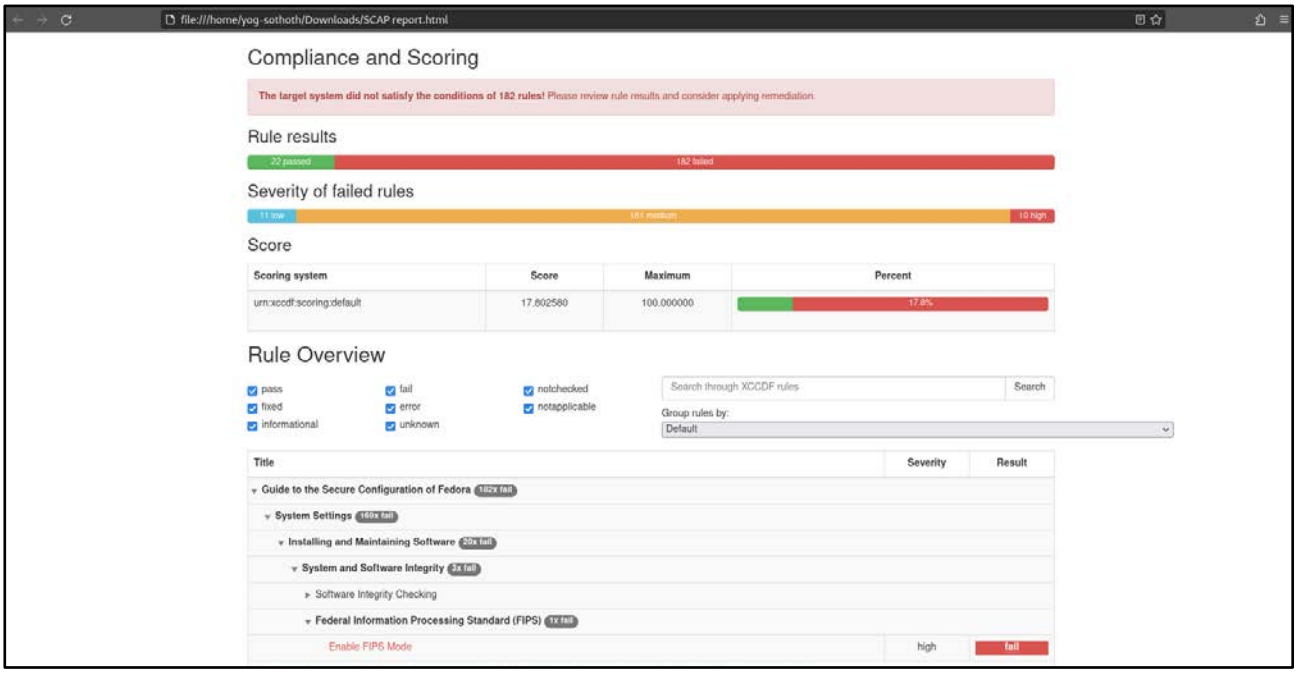


- Розпочинаємо сканування та отримаємо наступне оцінювання:



- Збережемо цей результат у форматі HTML-звіту:





2. Оцінка безпеки за допомогою сертифікованого NIST сканера OpenSCAP

- Переглянемо правила із обраного профілю деякої політики безпеки:

```
> oscap info /usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
Document type: Source Data Stream
Imported: 2023-02-06T14:41:04

Stream: scap_org.open-scap_datastream_from_xccdf_ssg-fedora-xccdf.xml
Generated: (null)
Version: 1.3
Checklists:
        Ref-Id: scap_org.open-scap_cref_ssg-fedora-xccdf.xml
                Status: draft
                Generated: 2023-02-06
                Resolved: true
                Profiles:
                        Title: OSPP - Protection Profile for General Purpose Operating Systems
                                Id: xccdf_org.ssgproject.content_profile_ospp
                        Title: PCI-DSS v3.2.1 Control Baseline for Fedora
                                Id: xccdf_org.ssgproject.content_profile_pci-dss
                        Title: Standard System Security Profile for Fedora
                                Id: xccdf_org.ssgproject.content_profile_standard
                Referenced check files:
                        ssg-fedora-oval.xml
                                system: http://oval.mitre.org/XMLSchema/oval-definitions-5
                        ssg-fedora-ocil.xml
                                system: http://scap.nist.gov/schema/ocil/2
Checks:
        Ref-Id: scap_org.open-scap_cref_ssg-fedora-oval.xml
        Ref-Id: scap_org.open-scap_cref_ssg-fedora-ocil.xml
        Ref-Id: scap_org.open-scap_cref_ssg-fedora-cpe-oval.xml
Dictionaries:
        Ref-Id: scap_org.open-scap_cref_ssg-fedora-cpe-dictionary.xml
```

- Запускаємо сканування та переглянемо результат:

```
> sudo oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_standard --results-arf arf.xml --report ~/Downloads/scanner_report.html /usr/share/xml/scap/ssg/content/ssg-fedora-ds.xml
[sudo] password for yog-sothoth:
--- Starting Evaluation ---

Title   Verify File Hashes with RPM
Rule    xccdf_org.ssgproject.content_rule_rpm_verify_hashes
Result  pass

Title   Verify and Correct File Permissions with RPM
Rule    xccdf_org.ssgproject.content_rule_rpm_verify_permissions
Result  fail

Title   Build and Test AIDE Database
Rule    xccdf_org.ssgproject.content_rule_aide_build_database
Result  fail

Title   Configure BIND to use System Crypto Policy
Rule    xccdf_org.ssgproject.content_rule_configure_bind_crypto_policy
Result  pass

Title   Configure System Cryptography Policy
Rule    xccdf_org.ssgproject.content_rule_configure_crypto_policy
Result  pass

Title   Configure Kerberos to use System Crypto Policy
Rule    xccdf_org.ssgproject.content_rule_configure_kerberos_crypto_policy
Result  pass

Title   Configure Libreswan to use System Crypto Policy
Rule    xccdf_org.ssgproject.content_rule_configure_libreswan_crypto_policy
Result  pass

Title   Configure OpenSSL library to use System Crypto Policy
Rule    xccdf_org.ssgproject.content_rule_configure_openssl_crypto_policy
Result  pass

Title   Configure SSH to use System Crypto Policy
Rule    xccdf_org.ssgproject.content_rule_configure_ssh_crypto_policy
Result  pass

Title   Ensure gpgcheck Enabled In Main dnf Configuration
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_globally_activated
Result  fail

Title   Ensure gpgcheck Enabled for All dnf Package Repositories
Rule    xccdf_org.ssgproject.content_rule_ensure_gpgcheck_never_disabled
Result  pass
```

- Переглянемо збережений звіт по проведеному оцінюванню: