Managing and Presenting Test Results

In this lab, we will cover the following topics:

- Managing and presenting test results
- Approach - generating a professional pentest report with Serpico

Approach - generate a professional pentest report with Serpico

A summary of the security testing documentation will help you to communicate with stakeholders. The report should not only list the security findings but also how they were identified, the testing scope, the methodology, and also mitigation suggestions. It's a common practice for an independent security testing firm to produce such documentation. The PCI DSS Penetration Test Guidance suggests a Penetration Test Report Outline as follows:

- Executive summary
- Statement of Scope
- Statement of methodology
- Segmentation test results
- Findings
- Tools used

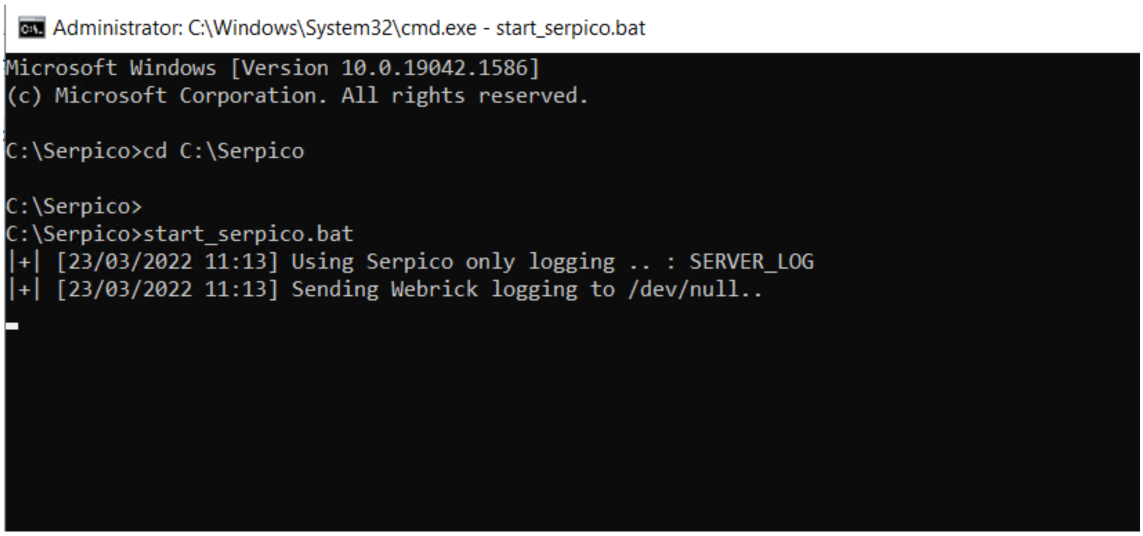
Serpico is a penetration testing report generator, which can help to produce such a document. Although Serpico doesn't import the security testing results from tools, it allows users to select security findings/mitigation's based on templates. Follow the steps in the next sectionto generate your own penetration testing document.

Step 1 -- Start Serpico

Serpico has been installed in the lab environment. Serpico can be launched with the [start_serpico.bat] script:

```
cd C:\Serpico

start_serpico.bat
```



Administrator: C:\Windows\System32\cmd.exe - start_serpico.bat

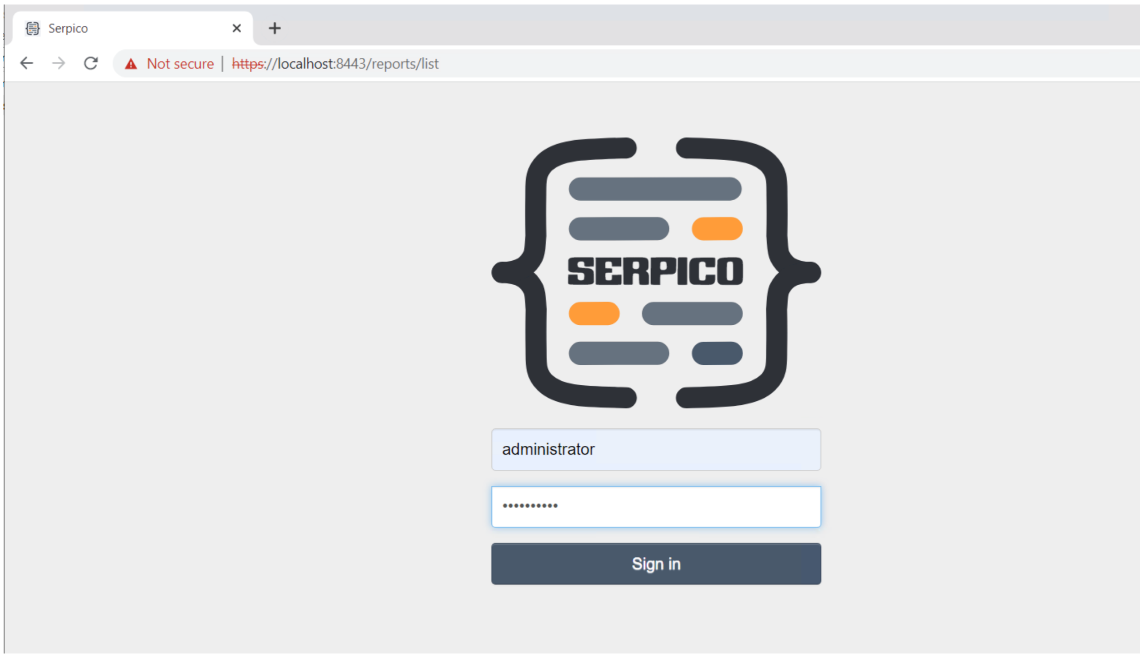
```
Microsoft Windows [Version 10.0.19042.1586]
(c) Microsoft Corporation. All rights reserved.

C:\Serpico>cd C:\Serpico

C:\Serpico>
C:\Serpico>start_serpico.bat
|+| [23/03/2022 11:13] Using Serpico only logging .. : SERVER_LOG
|+| [23/03/2022 11:13] Sending Webrick logging to /dev/null..
```

Run the above script and press `Enter` key. Then, use a browser to visit [https://localhost:8443/].

Username: administrator *Password:* oaqqtbai0a



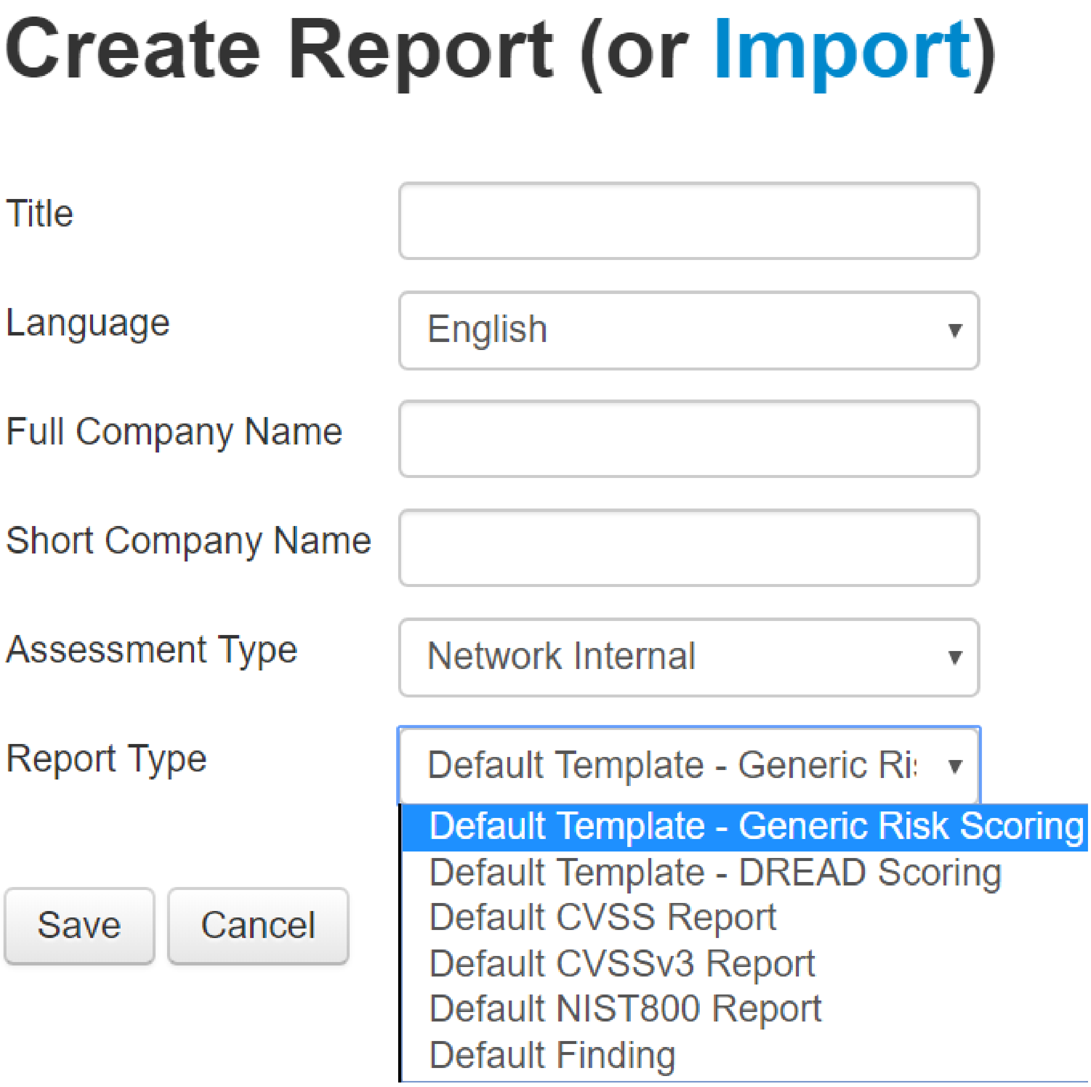
Username field: administrator

Password field: ••••••••••

Step 2 -- Create a Report based on Templates

To create a report, click `New Report` from the menu at the top. There are some report templates you may select, such as assessment type, and also report types such as DREAD, CVSS, and NIST 800.

This screenshot shows `Create Report` in Serpico:



Create Report (or Import)

Title

Language: English

Full Company Name

Short Company Name

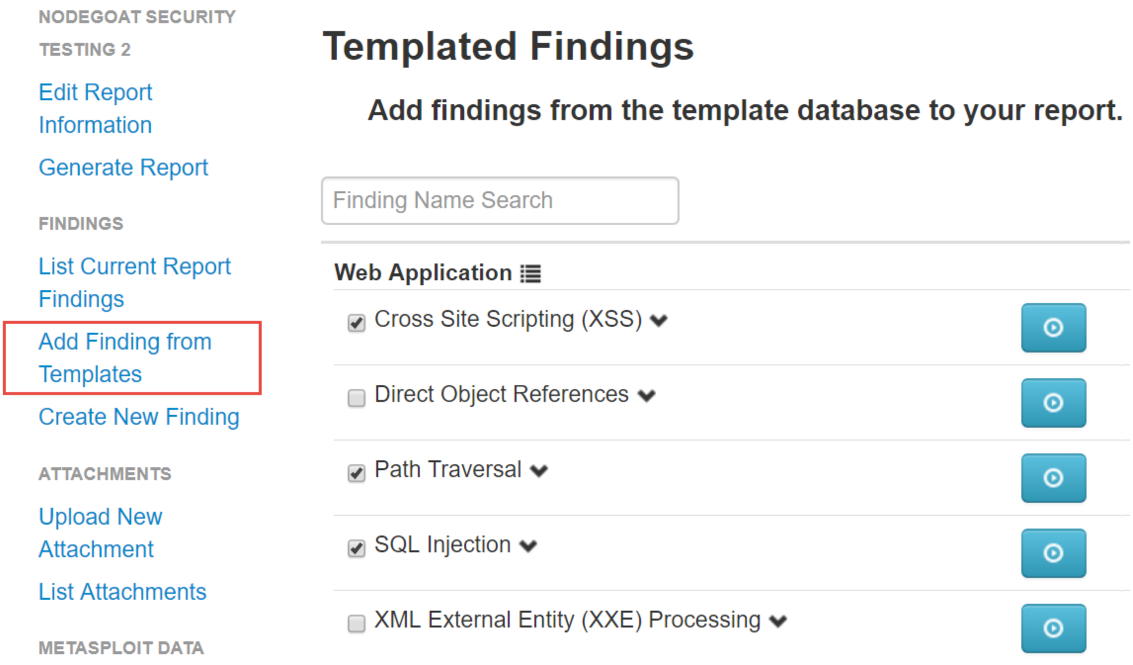
Assessment Type: Network Internal

Report Type: Default Template - Generic Ri:

Step 3 -- Add Finding from Templates

After creating a report with basic project information, it's suggested to [Add Finding From Templates] instead of add every finding from scratch. The finding templates include some common attacks and mitigation information. We may edit the security findings based on these templates and project testing results.

This screenshot shows `Add Finding from Templates`:



NODEGOAT SECURITY TESTING 2

Edit Report Information

Generate Report

FINDINGS

List Current Report Findings

Add Finding from Templates

Create New Finding

ATTACHMENTS

Upload New Attachment

List Attachments

METASPLOIT DATA

Templated Findings

Add findings from the template database to your report.

Finding Name Search

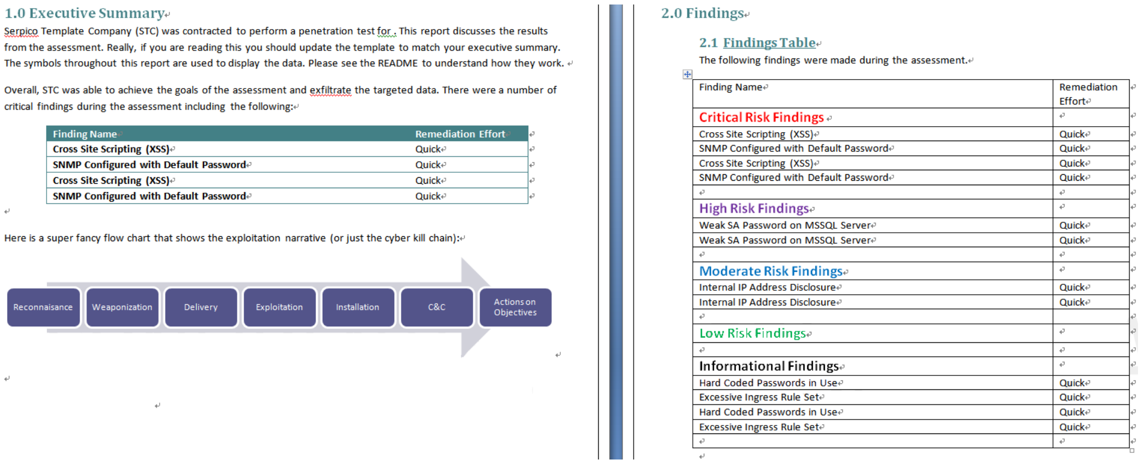
Web Application ☰

- ☑ Cross Site Scripting (XSS)
- □ Direct Object References
- ☑ Path Traversal
- ☑ SQL Injection
- □ XML External Entity (XXE) Processing

Step 4 -- generate a report

To generate a report, click [Generate Report] on the left menu. One Word document will be automatically generated based on your selected information and security findings.

This screenshot shows a sample of a generated report in Word format:



1.0 Executive Summary

Serpico Template Company (STC) was contracted to perform a penetration test for . This report discusses the results from the assessment. Really, if you are reading this you should update the template to match your executive summary. The symbols throughout this report are used to display the data. Please see the README to understand how they work.

Overall, STC was able to achieve the goals of the assessment and exfiltrate the targeted data. There were a number of critical findings during the assessment including the following:

Finding Name	Remediation Effort
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick

Here is a super fancy flow chart that shows the exploitation narrative (or just the cyber kill chain):

2.0 Findings

2.1 Findings Table

The following findings were made during the assessment.

Finding Name	Remediation Effort
Critical Risk Findings	
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick
Cross Site Scripting (XSS)	Quick
SNMP Configured with Default Password	Quick
High Risk Findings	
Weak SA Password on MSSQL Server	Quick
Weak SA Password on MSSQL Server	Quick
Moderate Risk Findings	
Internal IP Address Disclosure	Quick
Internal IP Address Disclosure	Quick
Low Risk Findings	
Informational Findings	
Hard Coded Passwords in Use	Quick
Excessive Ingress Rule Set	Quick
Hard Coded Passwords in Use	Quick
Excessive Ingress Rule Set	Quick

Summary

In this lab, we have introduced approaches to managing the testing results. First, we can use the script to integrate all the testing results. We demonstrated the uses of a Python script, RapidScan, which executes several security testing tools and presents the security findings in a console with highlighted colors. Secondly, we also introduced the document generator Serpico, which can help to generate professional penetration testing documentation, which includes the summary, security findings, risk ratings, and mitigations.