Security Operations Management (SOM) – Lab Session 2

1 INTRODUCTION

This lab aims to enhance the understanding of vulnerability management processes and activities. Background to this was covered in lecture 5 of the Security Operations Management module.

A vulnerability management standard will be created jointly before you will perform a vulnerability scan, analyse the results, compile a summary report and prepare a governance meeting.

The following sections provide the instructions for this Lab including submission requirements.

2 SCOPE OF THIS LAB

This lab comprises 3 parts:

1) Creation of a vulnerability management standard (20% of mark).
2) Perform a vulnerability scan, analyse the results and compile a summary report (50 % of mark).
3) Prepare a governance meeting by compiling a meeting presentation (30% of mark).

3 INSTRUCTIONS

Vulnerability Management Standard:
The class will jointly draft a vulnerability management standard in a group activity guided by the instructor who will capture the draft in a word document. Each student will download the draft and finalise (formulate out the content bullet points captured) for submission to the lab 2 assignment page.

The finalised draft should be submitted following the following naming convention: “vulnerability_management_standard_som_2024_<your name>” where <your name> contains your first and surname separated by an underscore (example “vulnerability_management_standard_som_2024_matthias_neuroth”).

Submit the finalised document (MS Word format) to the moodle lab 2 submission page.

***Vulnerabiliy Scanning and Reporting*:**

Download the blank template report (VM-Summary-Lab2.pptx) which is on moodle page prior to starting this scanning activity.

DUE TO CHANGES IN THE COMPTIA LABS, THE TIME FOR SCANNING APPEARS MUCH LONGER AND NOT FINISHING. THEREFORE, THERE IS NO NEED TO RUN THE SCANNING EXERCISE IN THE COMPTIA LAB. INSTEAD, SCREENSHOTS FOR THE SCANS ARE PROVIDED IN THE FILE "SCANRESULTS-LAB2-MAR25.DOCX". THESE SHOULD BE USED FOR COMPLETING THE "VM-SUMMARY-LAB2.PPTX TEMPLATE.

~~Perform a vulnerability scan using the Comptia Security+ assisted lab "Analyzing the Results of a Credentialed Vulnerability Scan".~~

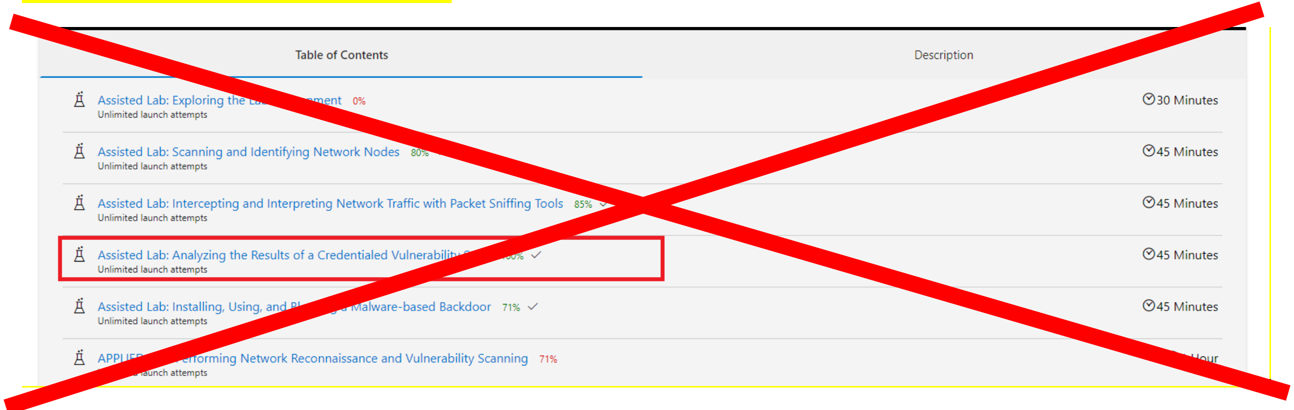


Table of Contents | Description

Assisted Lab: Exploring the La[illegible]ment 0% — 30 Minutes
Unlimited launch attempts

Assisted Lab: Scanning and Identifying Network Nodes 80% — 45 Minutes
Unlimited launch attempts

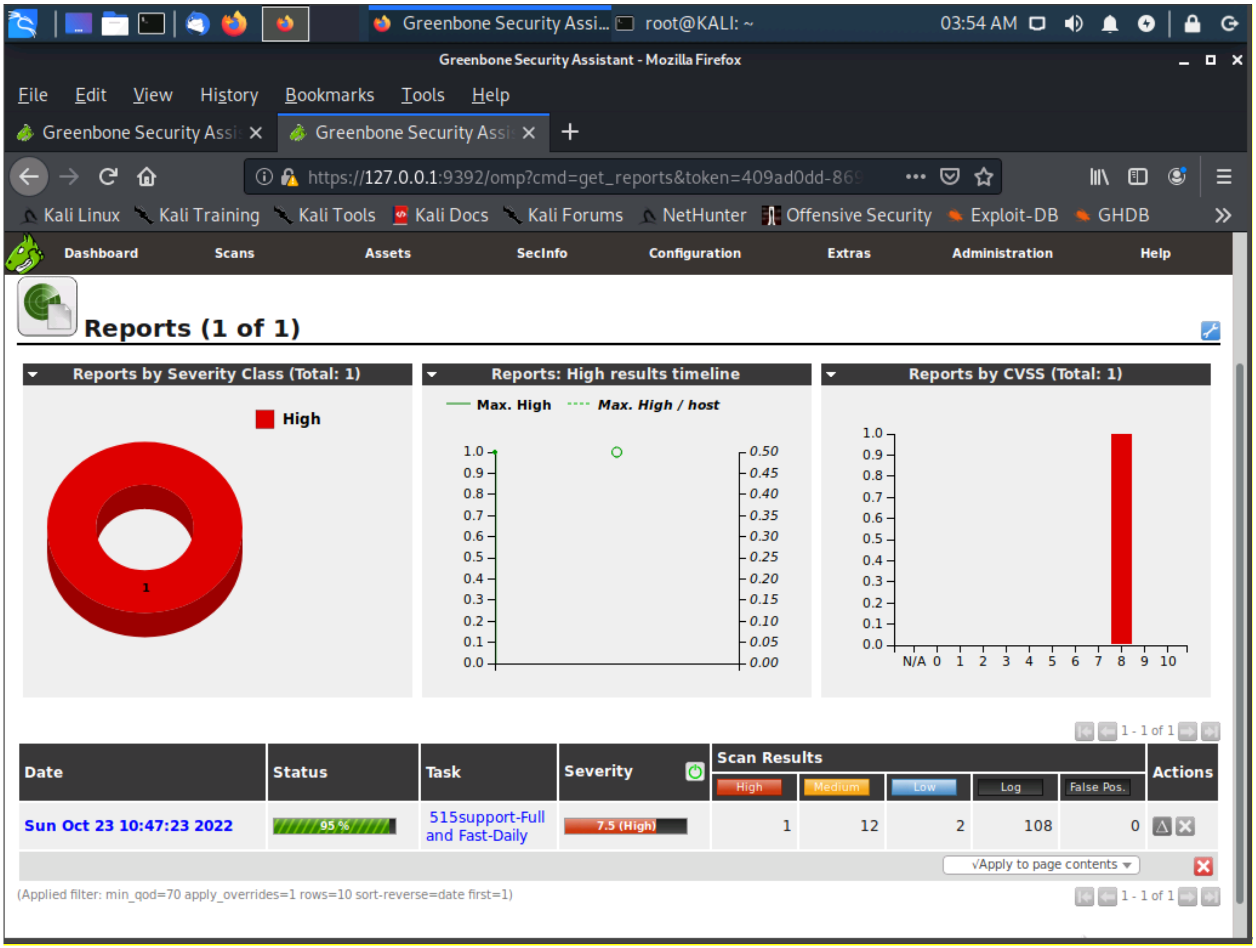
Assisted Lab: Intercepting and Interpreting Network Traffic with Packet Sniffing Tools 85% ✓ — 45 Minutes
Unlimited launch attempts

Assisted Lab: Analyzing the Results of a Credentialed Vulnerability [illegible] ✓ — 45 Minutes
Unlimited launch attempts

Assisted Lab: Installing, Using, and Bl[illegible] Malware-based Backdoor 71% ✓ — 45 Minutes
Unlimited launch attempts

APPLIE[illegible]erforming Network Reconnaissance and Vulnerability Scanning 71% — [illegible]Hour
[illegible] launch attempts

~~Launch the lab and step through the instructions which will lead to starting a vulnerability scan (this will take a few minutes, you will be able to monitor progress):~~

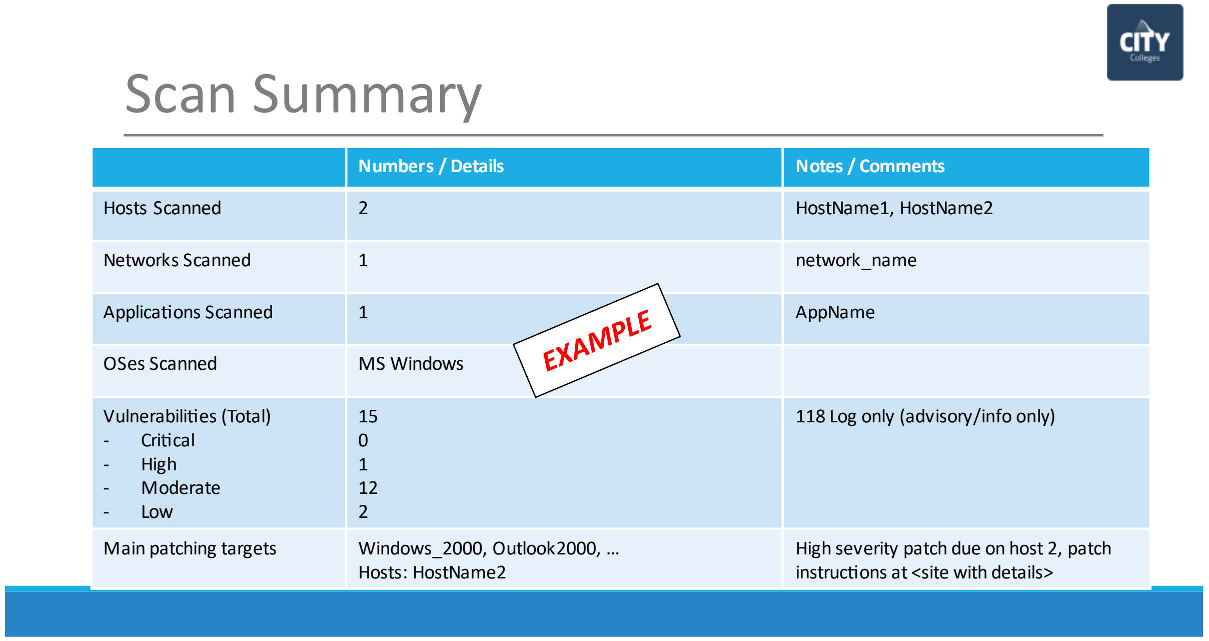

Greenbone Security Assi...
root@KALI: ~
03:54 AM
Greenbone Security Assistant - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Greenbone Security Assi
Greenbone Security Assi
https://127.0.0.1:9392/omp?cmd=get_reports&token=409ad0dd-86
Kali Linux Kali Training Kali Tools Kali Docs Kali Forums NetHunter Offensive Security Exploit-DB GHDB
Dashboard Scans Assets SecInfo Configuration Extras Administration Help
Reports by Severity Class (Total: 1)
High
1
Reports: High results timeline
Max. High
Max. High / host
1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0
0.50 0.45 0.40 0.35 0.30 0.25 0.20 0.15 0.10 0.05 0.00
Reports by CVSS (Total: 1)
1.0 0.9 0.8 0.7 0.6 0.5 0.4 0.3 0.2 0.1 0.0
N/A 0 1 2 3 4 5 6 7 8 9 10
1 - 1 of 1
√Apply to page contents
1 - 1 of 1

Reports (1 of 1)

Date	Status	Task	Severity	Scan Results					Actions
				High	Medium	Low	Log	False Pos.	
Sun Oct 23 10:47:23 2022	95 %	515support-Full and Fast-Daily	7.5 (High)	1	12	2	108	0	

(Applied filter: min_qod=70 apply_overrides=1 rows=10 sort-reverse=date first=1)

~~Once the scan has completed, use the vulnerability scanner interface to populate the details for the summery report.~~

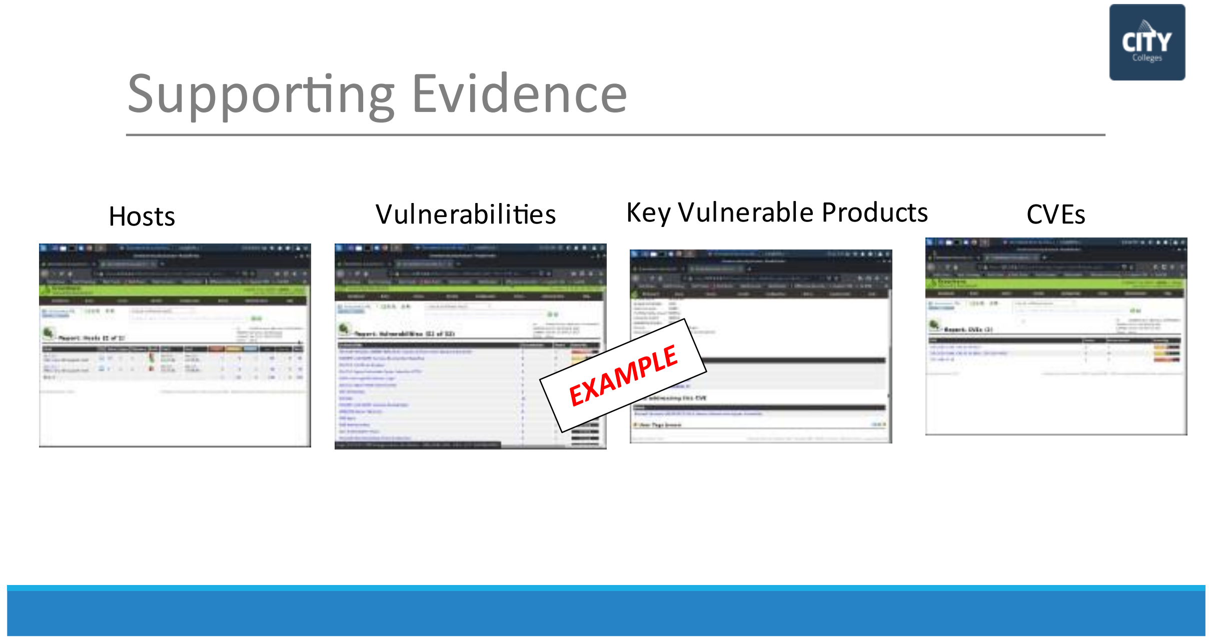


Scan Summary

	Numbers / Details	Notes / Comments
Hosts Scanned	2	HostName1, HostName2
Networks Scanned	1	network_name
Applications Scanned	1	AppName
OSes Scanned	MS Windows	
Vulnerabilities (Total) - Critical - High - Moderate - Low	15 0 1 12 2	118 Log only (advisory/info only)
Main patching targets	Windows_2000, Outlook2000, … Hosts: HostName2	High severity patch due on host 2, patch instructions at <site with details>

EXAMPLE

Please also take screenshots as evidence for the summary report details and show them in the Evidence slide(s).



Supporting Evidence

Hosts

Vulnerabilities

Key Vulnerable Products

CVEs

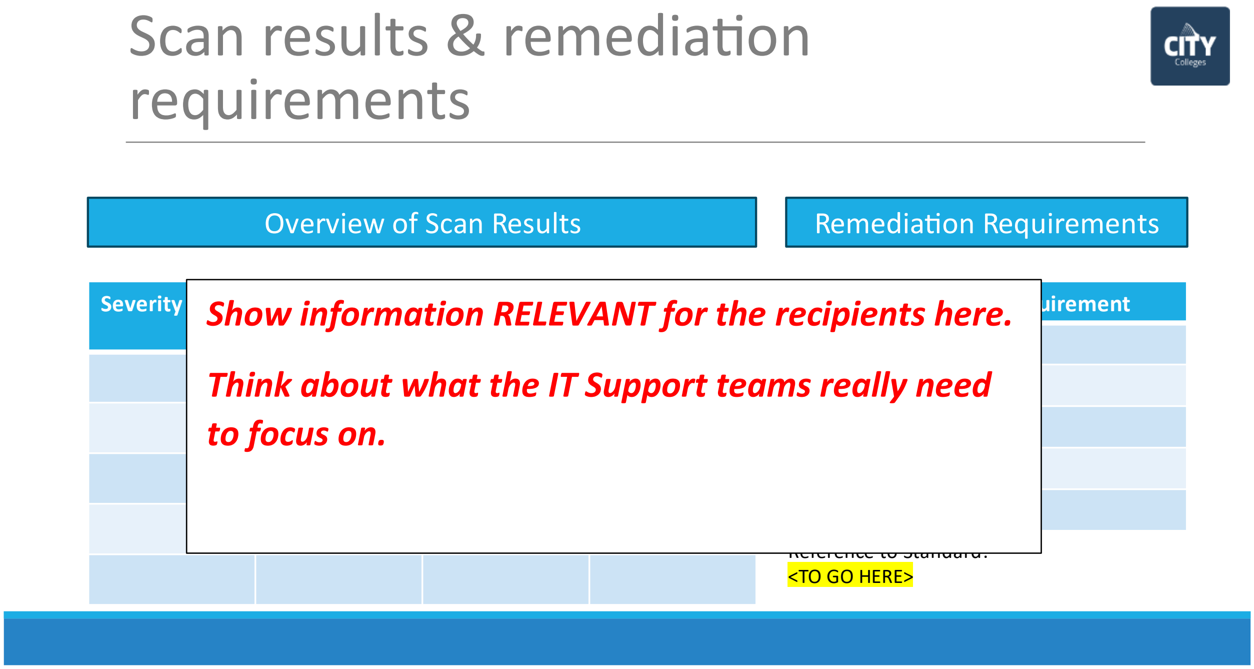
EXAMPLE

The completed summary report (powerpoint file) should be submitted to the moodle lab 2 submission page.

Governance Meeting Preparation:

Prepare a governance meeting by compiling a governance meeting powerpoint presentation that guides the discussion with the stakeholders (Vulnerability Management team and IT support team responsible for patching). A blank template is on the lab2 moodle assignment page (VM-Governance-Lab2-v2.pptx).

Download the template and populate the details for the following slides:



Scan results & remediation requirements

Overview of Scan Results

Remediation Requirements

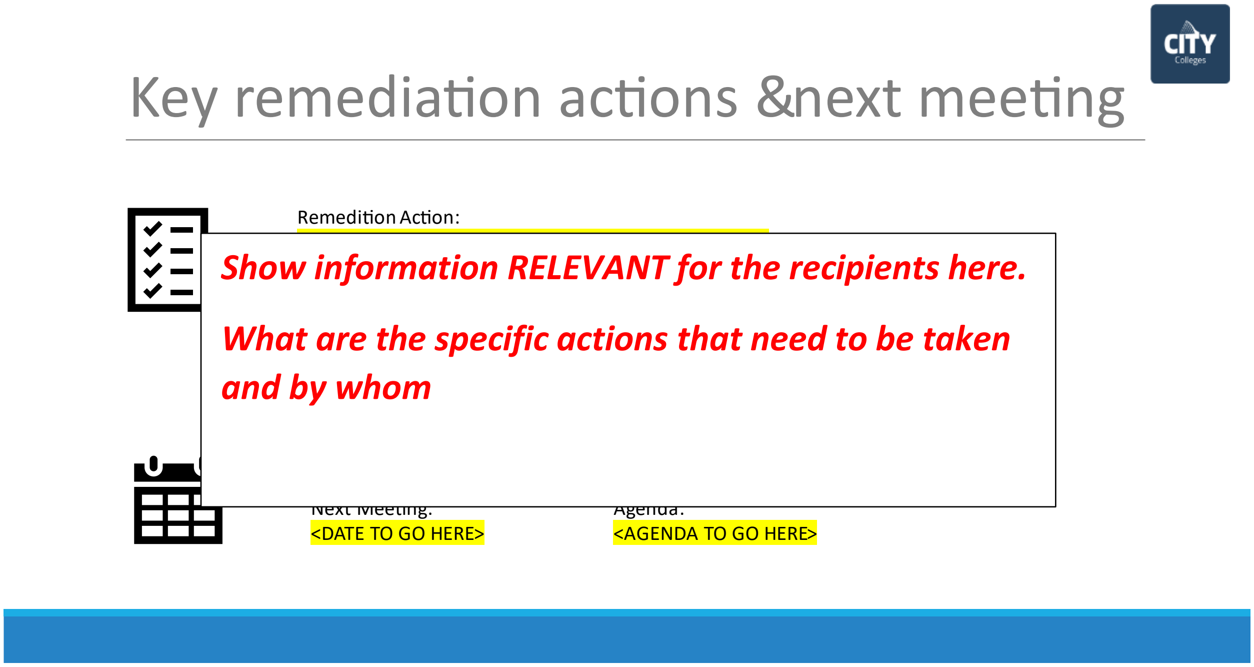
Severity

uirement

Show information RELEVANT for the recipients here.

Think about what the IT Support teams really need to focus on.

Reference to Standard:
<TO GO HERE>



Key remediation actions &next meeting

Remedition Action:

Show information RELEVANT for the recipients here.

What are the specific actions that need to be taken and by whom

Next Meeting:
<DATE TO GO HERE>

Agenda:
<AGENDA TO GO HERE>

The completed governance meeting presentation (powerpoint file) should be submitted to the moodle lab 2 submission page.

4 SUBMISSION

Submit **1 Word document and 2 Powerpoint documents** as specified in section 3 above to the moodle lab 2 submission page.

Deadline: **Wednesday, 23rd March 2025, 10.00pm GMT**.

Late submission treatment:

- Up to one day late (24th March 25 @ 10.00pm): maximum mark achievable = 70%
- Up to following lecture (27th March 25 @ 6.30pm): maximum mark achievable = 40%
- Beyond that: 0%