Lab: Final Project: Full OpenVAS Scan, Incident Containment, and Reporting

Estimated duration: 60 minutes

Introduction

In this final lab, you will apply the skills developed throughout the course to analyze real scan results, document a critical vulnerability, and demonstrate your understanding of effective remediation practices. You will focus on the `vsftpd Compromised Source Packages Backdoor`, a well-known critical vulnerability, and generate a professional-style vulnerability report using OpenVAS findings.

In this project, you'll step into the role of a security analyst, identifying vulnerabilities, assessing their impact, and clearly communicating how to fix them.

Objectives

After completing this lab, you will be able to:

- Identify high-severity vulnerabilities using OpenVAS
- Document vulnerability details in a structured report
- Propose effective and appropriate remediations
- Analyze security impacts and recommend long-term practices

Prerequisites

To successfully complete this final project, you should have the following prerequisites:

- Kali Linux Virtual Machine with OpenVAS (Greenbone Vulnerability Manager) installed and configured
- Basic understanding of vulnerability scanning tools, particularly OpenVAS
- Familiarity with key cybersecurity concepts, including CVEs, CVSS scores, and Indicators of Compromise (IoCs)
- Working knowledge of incident response procedures and frameworks such as NIST SP 800-61 and MITRE ATT&CK
- Ability to interpret scan results and correlate them with technical documentation
- Experience using word processing tools (for example, Microsoft Word or Google Docs) for completing structured reports
- Access to the Vulnerability Report Template provided in the LMS
- Basic troubleshooting skills in Linux environments for navigating logs and identifying suspicious activity

---

Project tasks

Task 1: Review the scan result in OpenVAS and complete the vulnerability report

Purpose:

In this task, you'll apply your vulnerability scanning skills to identify and investigate a known critical security issue—`vsftpd Compromised Source Packages Backdoor`. The goal is to accurately interpret scan results generated by OpenVAS and extract key technical details needed for your final report. This exercise reinforces your ability to use scanning tools for detection, triage, and remediation planning—core competencies for any cybersecurity analyst.

I. Review the scan result in OpenVAS

To locate and confirm the details of the `vsftpd backdoor` vulnerability using OpenVAS scan data, follow these instructions:

1. Launch your **Kali Linux virtual machine** and open **OpenVAS** (Greenbone Vulnerability Manager).
2. Log in to OpenVAS at:

   ```
   https://127.0.0.1:9392
   ```

3. Navigate to:

   ```
   Scans > Reports
   ```

4. If you have already completed the previous lab titled **Run and Analyze a Basic Vulnerability Scan**, you can directly use the scan report from that lab. If not, please return to that lab and follow the instructions to run a new scan on Metasploitable2 using the "Full and Fast" configuration.
5. Locate the following vulnerability in the scan report:
   - **Vulnerability name**: `vsftpd Compromised Source Packages Backdoor`
   - **CVSS score**: 9.8 (Critical)
   - **Port(s)**: 21/tcp, 6200/tcp
6. Make detailed notes on the following elements:

- Summary and technical description
- Affected services and host
- Exploit references or public PoCs (if provided)

Why this matters: Accurate interpretation of vulnerability scan results is foundational to reporting, triage, and remediation planning.

II. Complete the vulnerability report

In this step, you will organize and present your findings from the OpenVAS scan in a structured, professional incident response report.

1. Right-click and open in a new tab to download the **Final Project Incident Response Report.docx** or **Final Project Incident Response Report.txt** template to guide your documentation. The template is divided into specific sections, each focused on a key aspect of incident analysis and response. Be sure to complete each section carefully, using clear, fact-based language and supporting your findings with evidence from your OpenVAS report.

2. Complete the following sections in the template:

- **Executive summary (3 points)**
  Provide a concise, non-technical summary of the incident. Explain what happened, how it was discovered, the impact scope, and the current remediation status.

- **Incident timeline (3 points)**
  Create a chronological account of the incident using real or simulated timestamps. Include detection, investigation, containment, remediation, and lessons learned.

- **Systems affected (3 points)**
  List all impacted assets, including hostnames, IP addresses, exposed services, user accounts, and their roles (e.g., public web server, internal database).

- **Root cause analysis (3 points)**
  Explain the technical or procedural weakness that led to the incident. Reference relevant CVEs, scan data, and log evidence.

- **Indicators of compromise (IoCs) (3 points)**
  Provide technical artifacts tied to the attack, such as malicious IPs, file hashes, registry entries, rogue processes, or suspicious command executions.

- **Threat intelligence integration (3 points)**
  Correlate observed behavior with known tactics, techniques, and procedures (TTPs) using frameworks such as MITRE ATT&CK. Cite relevant threat actor campaigns or advisories.

- **Containment actions (3 points)**
  Describe the actions taken to stop the threat, such as isolating hosts, killing processes, disabling services, revoking credentials, or blocking IP addresses. List actions in order of execution.

- **Remediation steps (3 points)**
  Detail the steps taken to clean and restore systems, including patching, re-imaging, configuration changes, and system validations. Add before-and-after scan evidence if available.

- **Lessons learned (2 points)**
  Reflect on what the incident revealed about existing weaknesses, technical, procedural, or human. Identify areas for improvement.

- **Recommendations (2 points)**
  Propose clear, actionable, and measurable steps to prevent similar incidents in the future. Include both tactical and strategic measures.

- **Appendices (2 points)**
  Include supporting materials such as OpenVAS scan outputs, CVE references, screenshots, logs, or any evidence that reinforces your analysis.

3. **File naming:** When complete, save your file using the following naming convention: Final_Report_<YourName>.docx

4. **Submission format:** Convert the completed report to a **PDF format** and upload the file in the provided submission window. This file will be AI-graded to assess the clarity, accuracy, and completeness of your analysis and recommendations.

   Why this matters: Security reporting must be clear, structured, and actionable. In cybersecurity roles, the ability to communicate findings and recommend improvements is just as critical as identifying technical vulnerabilities. Writing professional reports is a key skill that supports decision-making, compliance, and long-term risk reduction.

Task 2: Answer remediation questions

Purpose:

This task is designed to assess your understanding of secure remediation and mitigation strategies based on your analysis in Task 1. You'll apply critical thinking to evaluate how vulnerabilities should be addressed both immediately and in the long term.

What you'll be assessed on

As part of this task, you will answer **five questions**, each worth **2 points**, contributing a total of **10 points** to your final project score. These questions reflect real-world decision-making that security analysts must perform when responding to threats. Read each question carefully and select the BEST possible answer based on your findings and cybersecurity best practices.

- **Question 1:** Tests your understanding of **immediate and effective remediation actions** following the discovery of a critical vulnerability **(2 points)**

- **Question 2:** Assesses your ability to **analyze the potential impact** of an exploited vulnerability **(2 points)**

- **Question 3:** Evaluates your knowledge of **post-remediation procedures**, including investigation and validation steps **(2 points)**

- **Question 4:** Checks your understanding of **long-term security best practices** for managing FTP services **(2 points)**

- **Question 5:** Tests your ability to identify how to **verify and validate the success of remediation efforts** in a real-world scenario **(2 points)**

Wrap-up and submission

Before finalizing your submission, it's important to ensure that your report reflects the standards expected in professional cybersecurity environments. A strong incident response report doesn't just document what happened; it communicates clearly, supports findings with evidence, and provides actionable recommendations for future prevention.

To help you meet these expectations, refer to the **Reading:** **What to Include in an Incident Response Report**, which outlines essential components, reporting best practices, and formatting tips aligned with industry-recognized frameworks such as NIST SP 800-61r2, MITRE ATT&CK, and CISA guidance. The reading will help you polish your report before submission.

Author(s)

Christo Oehley