Lab - Explore PenTest Reports

Objectives

Review examples of penetration testing reports and build your own report format on examples and pentesting notes.

- Part 1: Review Publicly Available Penetration Testing Reports
- Part 2: Develop Your Own Report Format
- Part 3: Create your Pentesting Report

Background / Scenario

At the conclusion of a security test, a penetration testing report is produced that presents a detailed analysis of the organization’s security risks. The report will cover many aspects of the organization’s security posture, vulnerabilities, high and low priority concerns, and suggested remediations. In addition, penetration testing reports are an important part of maintaining regulatory compliance. The reports provide evidence that the organization takes measures to assess its infrastructure and sensitive data security.

When it comes to creating the penetration testing report, most penetration testing professionals will start with a company template and then customize it based on the type of testing conducted and the desired deliverable.

In this lab, you will complete a report from information gathered during a penetration testing engagement performed by Protego Security Solutions. The client who will receive the report is Pixel Paradise Inc. an electronic games creator.

Required Resources

- PC or mobile device with internet access

Instructions

Part 1: Review Publicly Available Penetration Testing Reports

There are many sources on the internet for free penetration testing reports.

a. Navigate to https://github.com/santosomar/public-pentesting-reports.

   This displays a sampling of public pentesting reports.

   Search on the web for “example penetration testing reports.” You should find additional examples.

b. Select and review at least three different reports. Make notes detailing the sections included in the reports and the type of information included in each.

Note: Try to find reports that contain comprehensive penetration testing results for a client company. Reports regarding the security of software, technologies, or systems are not relevant to our needs in this lab.

What sections do the review reports have in common?

Answer Area

<!----><!---->

What is the purpose of the executive summary? Who do you think that section is intended for?

Answer Area

<!----><!---->

Part 2: Develop Your Own Report Format

There are many ways to write a penetration test report. As you know, most penetration test reports share the same key sections. In this part of the lab, you will create your own pentesting report format by creating an outline of the major sections of the report. You can also use subheadings.

Section 1: Create your report structure.

a. Review your notes from Part 1 and build an outline of the sections you will include in your report. Your outline should consist of major headings and sub-headings as required.

What major sections will you include in your report?

Answer Area

<!----><!---->

b. Create your outline in the table below using your major sections or headings. If you need more space, recreate the table on another piece of paper. You can also use outline numbering if you wish.

For each heading or subheading, describe the contents that will be found under that heading. One approach is shown in the sample answer. You are free to use other formats if you want.

Heading / Subheading	Contents
Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Answer Area <!----><!---->

Heading / Subheading	Contents
Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Answer Area <!----><!---->
Answer Area <!----><!---->	Answer Area <!----><!---->

Section 2: Assign content to report sections.

Now that you have your report structure, label the rows in the information column with your headings. The table contains notes from the penetration test conducted by Protego for their client Pixel Paradise.

Note that the information is not in the order that it will appear in in the report. You will organize it in the next section. In addition, some information could be combined under the same heading. For example, two rows of information could both appear under a Recommendations heading. The first row is done for you.

Report Section	Information
Recommendations	**General:** • Hire cybersecurity manager. • Strengthen admin security controls – policies and user agreements, penalize unauthorized devices and pages. **Specific:** • Annual user security awareness training • Periodical testing with phishing emails and other SE attacks • Remove rogue server and hidden page. • Investigate who modified firewall rules. • Discipline personnel involved. • Establish and enforce Windows policies regarding ad hoc shares. • Create an enforce password policy within Windows domains. • Further audit AD and SMB for other vulnerabilities • Implement secure coding training. • Improve input form validation to mitigate injection. • Use parameterized queries to segregate backend databases from web input. • Use randomized GUIDs for user ids, do not expose user ID info in user profiles.

Report Section	Information
	• Change default credentials and remove banner info from video controller. • Replace cameras with secure models that enable software updates, implement update program.
Answer Area <!----><!---->	• Company has growing pains that have led to some severe vulnerabilities, this must change with new success. • Security posture must be modernized to ensure continued success and business continuity. • New staff will implement comprehensive security program.
Answer Area <!----><!---->	**Goals:** • Assess web platform security. • Test employee security awareness. • Assess web applications: community forum and digital store. • Internal network vulnerability for sensitive file access, damage, and theft • Possible vulnerabilities from IoT or other devices
Answer Area <!----><!---->	• Seven staff clicked on links in phishing emails • Several staff visited fake website with logging software • Undocumented server discovered with address block scanning; weak password enabled admin access. • Internal network accessed through rogue webserver, ownership discovered, firewall configured to allow access from outside • Hidden webpage found with poor input validation on input form, vulnerable to command, code, and SQL injection. SQL injection revealed user data. • Community forum used static GUID for user ID, found user IDs included in user profiles, IDOR to access user accounts • Internal network has unprotected or weakly protect ad hoc shares (SMB); lateral movement possible • Shodan scan indicated presence of interconnected surveillance video controller/recorder. Banner showed model and sw version info. default credentials provided access, the camera model sw not updatable
Answer Area <!----><!---->	**Processes:** • Staff tested with phishing emails and duplicate websites; our honeypot ran a logging JavaScript to record visits • DNS foot printing of web domains, address block scanning to identify other servers, GVM/OpenVas, Nikto, and ZAP scans • From unauthorized access to internal network scanned with Nmap, Bloodhound (AD), and enum4Linux and Nmap SMB scripts. smbclient used to transfer files. • Web apps scanned with automated vuln. scanners, manual testing of inputs for injection vulns. • Shodan to identify internet facing devices, internal network scanned with Nmap to id. other connected devices.

Report Section	Information
Answer Area <!----><!---->	**General:** • Hire cybersecurity manager. • Strengthen admin security controls – policies and user agreements, penalize unauthorized devices and pages. **Specific:** • Annual user security awareness training • Periodical testing with phishing emails and other SE attacks • Remove rogue server and hidden page. • Investigate who modified firewall rules. • Discipline personnel involved. • Establish and enforce Windows policies regarding ad hoc shares. • Create an enforce password policy within Windows domains. • Further audit AD and SMB for other vulnerabilities • Implement secure coding training. • Improve input form validation to mitigate injection. • Use parameterized queries to segregate backend databases from web input. • Use randomized GUIDs for user ids, do not expose user ID info in user profiles. • Change default credentials and remove banner info from video controller. • Replace cameras with secure models that enable software updates, implement update program.
Answer Area <!----><!---->	• Company has growing pains that have led to some severe vulnerabilities, this must change with new success. • Security posture must be modernized to ensure continued success and business continuity. • New staff will implement comprehensive security program.
Answer Area <!----><!---->	• Contracted to comprehensive black box training. • Black box testing • Security personnel aware of some tests • All internet devices and networks in scope, intrusive testing and exploitation on dev servers, notify staff of intensive scans of external servers

Section 3: Organize your Pentesting Report

You have now assigned your information to sections of your report. Now it is time to write the report.

Put the information in the table in the order in which it should appear in your report. Follow your notes and examples to do so.

Part 3: Create Your Pentesting Report

Using the information in the table, write your report based on your notes. The notes are only fragments. You should add language so that your report uses the same style as the reports that you reviewed in Part 1. A sample report that uses the same information is available below for your review.

Some considerations:

- Always be aware of your audience and their needs. If you are not sure who the audience will be, consult the penetration testing agreement or the project manager who is responsible for the penetration test. Remember that not all stakeholders have the same needs.
- Consider the tone of the report. Should you sound informal and friendly, or should you sound formal and academic? Some organizations have preferences for this. If you are in doubt, read archived past reports or ask.
- Your writing should be succinct. It is not necessary to use fancy language or to try to sound sophisticated. Clarity is more important than style. In addition, be considerate of the stakeholder’s time when reading the report. Consult examples or ask your manager about the desirable length of your report.

Reflection Question

Why are good reporting and documentation skills important to a penetration tester?

Answer Area

```
<!----><!---->
```

Note: The Sample Report is provided to show you one way of transforming notes into a final report. There are many ways that you can do this using your own style and structure. Most penetration testing companies have their own standards for the style and structure of their reports and will likely require your work to conform to those standards.

Sample Report