Dublin Business School
CA Assessment Brief

Assessment Details

Unit Title:	Penetration Testing and Business Continuity Management
Unit Code:	B9CY105
Unit Lecturer:	Pete Cassidy
Level:	9
Assessment Title:	CA1
Assessment Number:	1 of 2
Assessment Type:	Penetration Testing
Restrictions on Time/Length :	2000 words
Individual/Group:	Individual
Assessment Weighting:	40%
Issue Date:	2 Feb 2023
Hand In Date:	See Moodle
Mode of Submission:	On-line via Moodle

Assignment 1: Penetration Test Report

For the first assignment you will be submitting a penetration testing report containing the results of the first 3 practical labs that were completed. This includes:

- Lab 1: Password Cracking – 25%
- Lab 2: Metasploitable – 30%
- Lab 3: DVWA – 30%
- Report – 15%

As part of the submission for this assignment, you will be writing a structured pentest report consisting of the following sections:

- **Management Overview** - A key aspect of any penetration test is the ability to convey complex technical topics in short, understandable descriptions that can quickly be consumed. As part of this section, you will be describing the results of the test in high level language, and providing an overview of the most severe vulnerabilities you have identified.
- **Section 1** - This section will consist of the answers of Lab 1, including the practical questions and the results of cracking the Linux passwords.
- **Section 2** - This section will consist of the answers from Lab 2, including the practical questions and the findings to be documented.
- **Section 3** - This section will consist of the answers from Lab 3, including the practical questions and the findings to be documented.

The following template is provided to you as a guide for what is to be included in the submission and the format that can be supplied. Where you see extra detail to be added you are free to do so.

When documenting findings, try to include as much detail as possible with screenshots accompanying the description. One of the main aims of penetration test reports is to provide the client with detail enough to understand and even reproduce the vulnerabilities.

Report Template Structure:

Name of Individual Conducting Test:	
IP of Kali VM:	
Security Issues Identified:	
Date:	

Management Overview
>> Provide an overview of the results of the three lab assignments. Keep the language high level and business oriented such that senior level executives can understand the issues and their potential costs..<<

Scope

Lab 2 Target IP Address and Port Targeted	Example: 21 - proFTPd 1.1 22 - SSH
Lab 2 Target IP Address and Port Targeted	

Top 5 Most Serious Security Issues (In priority order - most important first):

>> What are the 5 most critical issues with the scanned system? Talk about each one, and what could happen if an attacker exploits the vulnerability <<

1. Most serious issue
2. Security flaw
3. Security flaw
4. Security flaw
5. Security flaw

Top 5 - Remediations (In priority order - most important first):
>> What are the suggested remediation actions to address the top 5 most critical security flaws? Re-word them, don't just copy and paste Nessus' suggestions <<

1. Most serious issue remediation
2. Security flaw remediation
3. Security flaw remediation
4. Security flaw remediation
5. Security flaw remediation

Section 1 - Lab 1

Practical Questions

1. What is the Metasploit Framework?

Answer:

2. What are Metasploit auxiliary modules?

Answer:

3. What are the types of Windows password hashing?

Answer:

4. Where and how are Windows credentials stored locally?

Answer:

5. Explain in your own words how the EternalBlue attack works.

Answer:

6. If you were working for a client who was using a Windows Server 2008 affected by EternalBlue, what would be your recommendation/remediation for them.

Answer:

7. Explain in your own words how a pass the hash attack works.

Answer:

8. Explain a method through which the SAM file can be dumped.

Answer:

9. Where are passwords stored on Linux systems?

Answer:

10. What are the common hashing methods for Linux passwords?

Answer:

Linux Password Cracking Exercise

Time Started Cracking
Time Finished

Hash Type
Username affected
Plaintext Password
Password Position in rockyou

Section 2 - Lab 2

Practical Questions:

1. Read the documentation for Nmap (nmap -h) and perform an nmap scan with the following characteristics:
    - Do not ping the machine when starting scanning
    - Run simple default scripts against the machine
    - Scan for software versions
    - Scan the entire 0-65535 port range
    - Ouput results to all nmap formats to a file called result

   What is the command that you ran to achieve these characteristics?

Answer:

2. Using the supplied report template, write up the previous exploits making sure to detail the steps taken, and to provide an overview of the exploit along with a CVSS score that matches the exploit type.
3. Using the nmap results that you have gathered, identify and write up a further 3 exploits in the format of the template provided. You will have 6 findings described in total.

Findings Overview

Finding 1- Finding Risk

Finding CVSS Score:

Attack Vector(AV)		Scope (S)	
Attack Complexity (AC)		Confidentiality (C)	
Privileges Required (PR)		Integrity (I)	
User Interaction (UI)		Availability (A)	

Description:

Remediation:

Steps to reproduce:

Finding 2- Finding Risk

Finding CVSS Score:

Attack Vector(AV)		Scope (S)	
Attack Complexity (AC)		Confidentiality (C)	
Privileges Required (PR)		Integrity (I)	
User Interaction (UI)		Availability (A)	

Description:

Remediation:

Steps to reproduce:

Section 3 - Lab 3

Practical Questions

1. When we pull the /etc/passwd file through Local File Inclusion from the server we are successful. Attempt to pull the /etc/shadow file and describe the results, and the cause behind the results.

Answer:

2. Describe in your own words how Cross-Site Scripting and Javascript can be used to steal browser cookies from a user.

Answer:

3. Describe the difference between DOM based XSS, Reflected XSS and Stored XSS.

Answer:

4. Using the supplied report template, write up the previous exploits making sure to detail the steps taken, and to provide an overview of the exploit along with a CVSS score that matches the exploit type.
5. Identify and write up a further 3 exploits in the format of the template provided. You will have 6 findings described in total.

Findings Overview

Finding 1- Finding Risk

Finding CVSS Score:

Attack Vector(AV)		Scope (S)	
Attack Complexity (AC)		Confidentiality (C)	
Privileges Required (PR)		Integrity (I)	
User Interaction (UI)		Availability (A)	

Description:

Remediation:

Steps to reproduce:

Finding 2- Finding Risk

Finding CVSS Score:

Attack Vector(AV)		Scope (S)	
Attack Complexity (AC)		Confidentiality (C)	
Privileges Required (PR)		Integrity (I)	
User Interaction (UI)		Availability (A)	

Description:

Remediation:

Steps to reproduce: