Assignment 2

Subject: ITNET302A_118

Title: Penetration Test and B2R Challenge

Due Date: Check Moodle

Introduction

This assignment consists of two tasks:

- Perform a Penetration Test and write a report (70%)
- Complete a Boot-2-Root challenge. (30%)

The in-scope boxes for this task are only accessible via the VPN. You will need to download the OpenVPN configuration from Moodle and connect to the environment. The config has been set up to accommodate all operating systems (Windows/Mac/Kali) out of the box. Simply download OpenVPN (pre-installed in Kali) and run the config **as Administrator**. The UDP config is preferred.

Network Summary (where x is [1, 2, 3, 4, 5, 6, 7, 8, 9])

The environment consists of 3 boxes in total, two for your assignment and a Kali box (with Nessus) for you to perform your hacktivities from. You can launch exploits from anywhere you want (TAFE-Kali, VPN-Kali or your Windows/Mac host). **For Nessus use the VPN-Kali box otherwise some vulnerabilities will be missed. Do not use Nessus through the VPN.** Network summary:

Hostname	IP Address	Credentials	Nessus/Notes
vpn-kali	10.220.0.250	**SSH** student:student	https://10.220.0.250:8834 Username & Password: Your Moodle Email address
sploit	10.222.0.**x1** (VPN Status Page)	Username: sploit Password: *unknown*	Box for penetration test and report (The password is **not** literally *unknown*)
B2r	10.222.0.**x2** (VPN Status Page)		Box for boot-to-root challenge

Penetration Test (70%)

A penetration test is a simulated attack designed to test the security of target systems and networks for both weaknesses and strengths. A penetration test involves identifying and exploiting vulnerabilities against the targets. The penetration test is concluded by providing a report summarising all identified vulnerabilities, including methods of exploitation where applicable.

Your first task is to complete a penetration test against the target box including identifying vulnerabilities, exploitation of vulnerabilities (where applicable) and creating a report summarising your penetration test. The term "vulnerability" should be considered to include anything that poses a security risk, such as:

- Out of date software
- Misconfigurations
- Weak credentials
- ???

Vulnerabilities that you can exploit, that lead to a shell, are *critical*. As there are more than 8 critical vulnerabilities present on the box, findings submitted that are not critical will receive less marks.

A skeleton report has been provided for you, available on Moodle. Check it out.

There are 9 copies of each box in total. They are identical but shared amongst students. Do not disable any configurations/services running when you acquire administrator access. The box will be frequently reverted back to its original running configuration. If you think something's broken or would like your own personalised copy of the boxes, email me.

Boot-2-Root Challenge (30%)

A “boot-2-root” (B2R) challenge is a security gaming exercise. A B2R involves downloading a purpose-built vulnerable virtual machine, launching it and breaking in. The first two steps have been completed for you, your task is to break in to the B2R box

Additionally, there are 4 flags scattered around the box that are also worth marks. Flags are short phrases placed within curly brackets, for example:

flag{an_example}

Marks are awarded on finding flags, achieving low level access, acquiring root access.

Do not write a penetration test report on this box, a “story” of how you break in (including screenshots) will suffice. For example:

1. First I noticed _____ (include screenshot as supporting evidence)
2. So I performed _____ (include screenshot as supporting evidence)
3. This allowed me to acquire a low privileged shell _____ (include screenshot)

These boxes are shared amongst all students. Do not disable any configurations/services running when you acquire administrator access. The box will be frequently reverted back to its original running configuration. If you think something’s broken, email me and I will revert it for you.

Trick or Treat

Some tricks, tips, & extra knowledge:

- **Do not actually perform the Denial of Service (DoS) attacks**
- DoS attacks are not critical findings
- The boxes will revert every 24 hours at 4am *automagically*
- Do not waste your time on Windows ephemeral ports (40,000 or higher). They are false rabbit holes, no matter how juicy they look, they are unreliable and not the attack avenue
- Pretty much any port over 10,000 is not the way in
- A critical finding is one that allows you to get a root shell
- Some exploits may need to be run more than once
- **Pentest box only**: The username for any service is *sploit*. You should search*sploit* this (haha)
- Nessus and other scanners lie, do not take their scan results as law.
- You have a penetration test skeleton document, use it
- Nessus will not help you with the B2R challenge, you have to go looking
- Googling common privilege escalation methods will easily get you root
- Do **not** use dirtyCOW on the B2R box. It will break and not give you root

Marking Rubric

The associated marks for each component is as follows:

Type	Component	Total Marks
Penetration Test	Title page	1
Penetration Test	Table of Contents	1
Penetration Test	Executive Summary	5
Penetration Test	Scope	2
Penetration Test	Testing Methodology	4
Penetration Test	Findings Summary	4
Penetration Test	Finding #1	6
Penetration Test	Finding #2	6
Penetration Test	Finding #3	6
Penetration Test	Finding #4	6
Penetration Test	Finding #5	6
Penetration Test	Finding #6	6
Penetration Test	Finding #7	6
Penetration Test	Finding #8	6
Penetration Test	Conclusion	5
Total	**Total Marks for Penetration Test**	**70**
Boot-to-Root (B2R)	Flag Found (2 marks per flag)	8
Boot-to-Root (B2R)	Low privileged access	12
Boot-to-Root (B2R)	Root Access	10
Total	**Total Marks for Boot-to-Root**	**30**
Total	**Total Marks Overall**	**100**