Hugh Baldwin
up2157117

Ethical Hacking
M30239
TB2

Contents

Lecture - Introduction to Penetration Testing

09:00   22/01/24   Tobi Fajana

Weekly Teaching Materials

- 1 hour lecture

- 2 hour practical

- Instructional video (Guide for Labs)

- Compulsory Moodle quiz

Assessments

- Practical Exam, 2 hours (50%, 20/03/2024)

  - 2 Devices to exploit
  - 5 Vulnerabilities expected, give the name, software, risk rating, a brief description, and corrective actions for each exploit

- Muliple Choice Exam, 1 hour (50%, May/June)

CIA

- The three main properties which are protected by cyber security

- Confidentiality - Protecting information from being disclosed to unintended parties

- Integrity - Protecting information from being modified, intentionally or otherwise

- Availability - Ensuring the information is available to access when it is needed

Penetration Testing

- Black Box - No information about the target

- Grey Box - Some information about the target, but not all

- White Box - All information given, including source code, etc

- Timeframe - There is usually a fixed timeframe for the test

- Penetration Testing is similar to vulnerability assessment, but actual exploits the vulnerabilities

Port Scanning

- Scan every port on a server to check which ports are open

- Attempt to ping the server on each port

- If a response is given from a port, it must be open