PENJANA HRDF Place and Train

MILE2 CPTE

1.	Course Title	**Certified Penetration Testing Engineer**
2.	Type of Course	Technical
3.	Training Methodology	Classroom or E-learning
4.	Skill Area	Information Security
5.	Duration (Days)	5 days/40 hours
6.	Level of Certification	Mile2 Certified Penetration Testing Engineer
7.	Certification Body (If Applicable)	Established in 2006, Mile2 is headquartered in the USA, and offers 15 internationally recognized, proprietary cybersecurity certifications. The certifications are utilized by numerous private and public bodies, including Boeing, the United States Air Force and the U.S. Federal Bureau of Investigation. Upon completing the course, the CPTE exam is taken online through Mile2's Assessment and Certification System ("MACS")
8.	Course Overview	The CPTE certification is one of the core certifications of the cybersecurity industry, and is recognized by the US National Security Agency as one of several information assurance accreditations. The course aims to equip students with not just a solid foundation in the technical skills needed to conduct a penetration test, but also emphasizes the need for proper reporting and ethics in a penetration tester.
9.	Prerequisites	Foundational knowledge in cybersecurity concepts and networking technologies,
10.	Course Objective	Establish industry acceptable auditing standards with current best practices and policies. Students will also be prepared to competently take the CPTE exam.
11.	Learning Objectives	Knowledge of commonly utilized technical skills, reporting methodologies and professional ethics in carrying out a penetration test.
12.	Course Content	Module 0: Course Introduction Module 1: Business & Technical Logistics of Pen Testing Module 2: Information Gathering Reconnaissance- Passive (External Only) Module 3: Detecting Live Systems – Reconnaissance (Active) Module 4: Banner Grabbing and Enumeration Module 5: Automated Vulnerability Assessment Module 6: Hacking Operating Systems Module 7: Advanced Assessment and Exploitation Techniques Module 8: Evasion Techniques Module 9: Hacking with PowerShell Module 10: Networks and Sniffing Module 11: Accessing and Hacking Web Techniques

		Module 12: Mobile and IoT Hacking Module 13: Report Writing Basics Appendix: Linux Fundamentals
13.	Learning Activities	Full time course, involving Online Video and Practical Exercises
14.	Target Group	Individuals interested in gaining practical cybersecurity knowledge, penetration testers, cybersecurity professionals