ZSCV012 Security Pen-Testing (Physical Premises Penetration Testing) - (Non-Award)

DESCRIPTION

This comprehensive course provides hands-on training in physical penetration testing techniques used by security professionals to assess and improve organisational security. Participants learn to identify vulnerabilities in physical security systems through authorised testing methods.

Topics include HID-based attacks using Rubber Ducky and OMG cable, RF security and credential cloning, technical surveillance countermeasures (bug sweeping), lock picking and bypass techniques, and professional security assessment and reporting.

The course also covers social engineering techniques including pretexting, tailgating, and impersonation, enabling participants to assess human factors in physical security.

All activities are framed within lawful, ethical engagement rules with strong emphasis on authorised testing only.

Learning Focus:

Knowledge:

- Physical penetration testing lifecycle, scoping, and rules of engagement
- Legal, ethical, and safety considerations for physical testing activities
- HID-based attacks, keystroke injection, and Ducky Script syntax
- RF technologies in access control (LF/HF RFID, NFC, key fobs /faraday protection)
- Technical surveillance countermeasures and bug detection principles
- Lock mechanisms, bypass techniques, and non-destructive entry principles
- Physical security assessment frameworks and professional pen-test reporting
- Social engineering tactics and psychological principles used in physical penetration testing
- Pretexting, tailgating, and impersonation techniques within ethical and legal boundaries

Skills:

- Write and deploy Ducky Script payloads for authorised testing
- Perform RF credential assessment using appropriate tools
- Conduct structured bug sweeps and document findings
- Apply basic lock picking and bypass techniques on training equipment
- Conduct physical security walkthroughs using assessment checklists
- Draft professional security assessment reports with actionable recommendations
- Propose appropriate mitigations and security improvements
- Develop and execute social engineering pretexts for authorised security assessments
- Identify social engineering vulnerabilities and recommend security awareness measures

DELIVERY DETAILS

Location(s)	Casuarina
Duration*	10 weeks, one 3-hour session per week. Every Tuesdays from 5.00 pm to 8.00 pm
Study mode ^^	Face-to-face. Combination of theory, demonstrations, and hands-on practical exercises in a controlled lab environment.
Start Date	3rd February 2026

ELIGIBILITY/ENTRY REQUIREMENTS

Entry requirements for this short course include:

- Basic understanding of IT security concepts
- Commitment to ethical conduct and lawful use of techniques
- Signed acknowledgement of course ethics agreement

Open to security professionals and those entering the field aged 18+

FEES

Fee Type	2026 Course Fees
Flat Fee	$1,650.00

Fees shown are indicative and subject to change annually.

RESOURCES

Students can bring their own laptop device to class. However, it is not essential for training.

CONTACT DETAILS

ICT, Cyber Security and Digital

E. tafe.ict@cdu.edu.au
T. 08 8946 7517
W. https://www.cdu.edu.au/tafe

For further information regarding student life at CDU, please refer to https://www.cdu.edu.au/study/student-life.