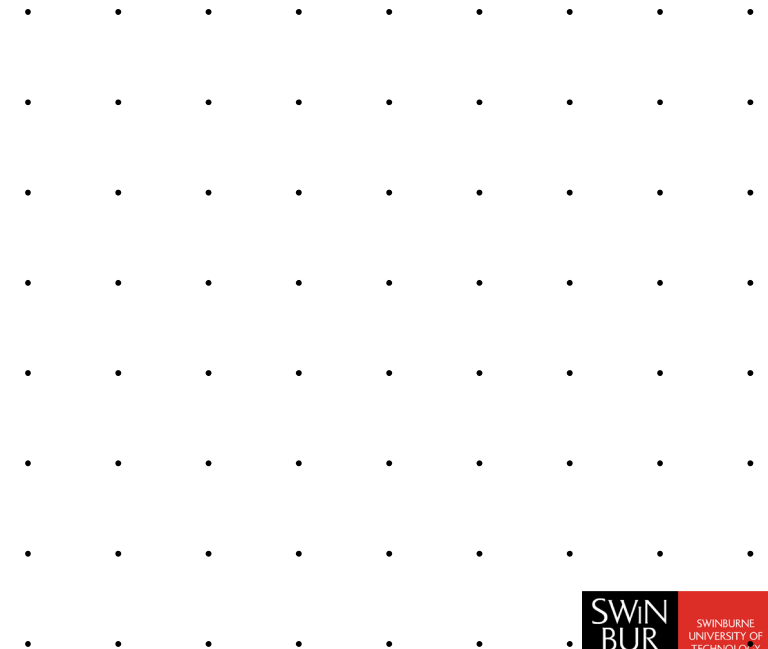


Auditing, Penetration Testing



Network Auditing

- Look at all of the business:
- e.g. Password policy
 - Strong passwords
 - Single sign-on or multiple passwords?
 - Account lock-out?
 - Password recovery process



Penetration Testing

- Simulated attack.
- Black box or white box.
- Get written agreement from customer.
- Take notes throughout the pen-test.
- Report details of findings and vulnerabilities to customer.
- Suggest mitigation, fixes.

Penetration Testing

1. Enumeration, network reconnaissance, IP scan, port scan, DNS records.
2. Network Vulnerability analysis, port scans, footprinting, find vulnerable services.
3. Web application testing, SQL mapping, injection, XSS testing, javascript injection, php passthrough, injection, fuzz testing.
4. Exploit vulnerabilities, establish foothold, additional reconnaissance, obtain privileged information/access.