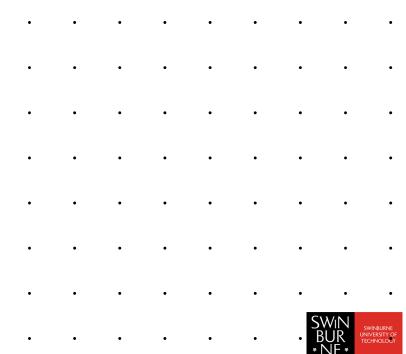


Vulnerability Assessment



Vulnerability Assessment

- Black Box
- -Inner working of system unknown
- Based on documentation,binary/working system only.
- –Simulates real attacker (zero knowledge)

- White Box
- -Source code, design docs available
- –More expensive than BB (experts needed)
- -Can uncover undocumented "features"



Vulnerability Assessment

- Static Analysis
- -Examine code and data
- -Audit source code, binaries.
- -Use analysis tools to discover (e.g.) potential -Use Fuzz testing to trigger errors, create proof buffer overflows.
- -Disassemble binaries, reverse engineer.
- -Not so good for design / architecture problems.

- Dynamic Analysis
- -Examine running system.
- -Use debugger tools, VMs, sandboxes.
- of concept exploits.



Disclosure

- Responsible disclosure
- -Reveal vuln. to software vendor, suggest fixes, mitigation.
- -Pwn2Own, Bug Bounty
- -Some vendors don't want to patch; punish hackers

- Full Disclosure
 - Publish all details of vuln.
 immediately.
 - Force vendors to patch immediately.
 - Black hats, criminals get info. immediately and can craft exploits.

Secure Admin

- Adopt the right policies:
- Principle of least privilege
- •Use a good Access control system
- Enforce strong passwords (but not too strong)
- •Use well-known, well-tested crypto.
- Patch

