



The Risks that Pen Tests don't Find

- Gary Gaskell
- Infosec Services
- gaskell@infosecservices.com
- 0438 603 307

OWASP

13 April 2012

Copyright © The OWASP Foundation
Permission is granted to copy, distribute and/or modify this document
under the terms of the OWASP License.

The OWASP Foundation

<http://www.owasp.org>

Objectives

- ✦ Raise debate about testing completeness
- ✦ Promote clear communication of testing scope and utility
- ✦ Describe risks from IT trends not found in pen tests
- ✦ Revisit other risks not reported from pen tests
- ✦ Share info about
 - ✦ security holes that are hard to find by black box testing but very easy by inspection

Caveats

- ✦ Penetration testing is essential and a highly valued practice
- ✦ This talk's scope is limited to technical weaknesses
- ✦ This talk focuses on identification and analysis of vulnerabilities that cannot be ***efficiently*** discovered through pen testing

Finifter and Wagner, UC Berkley

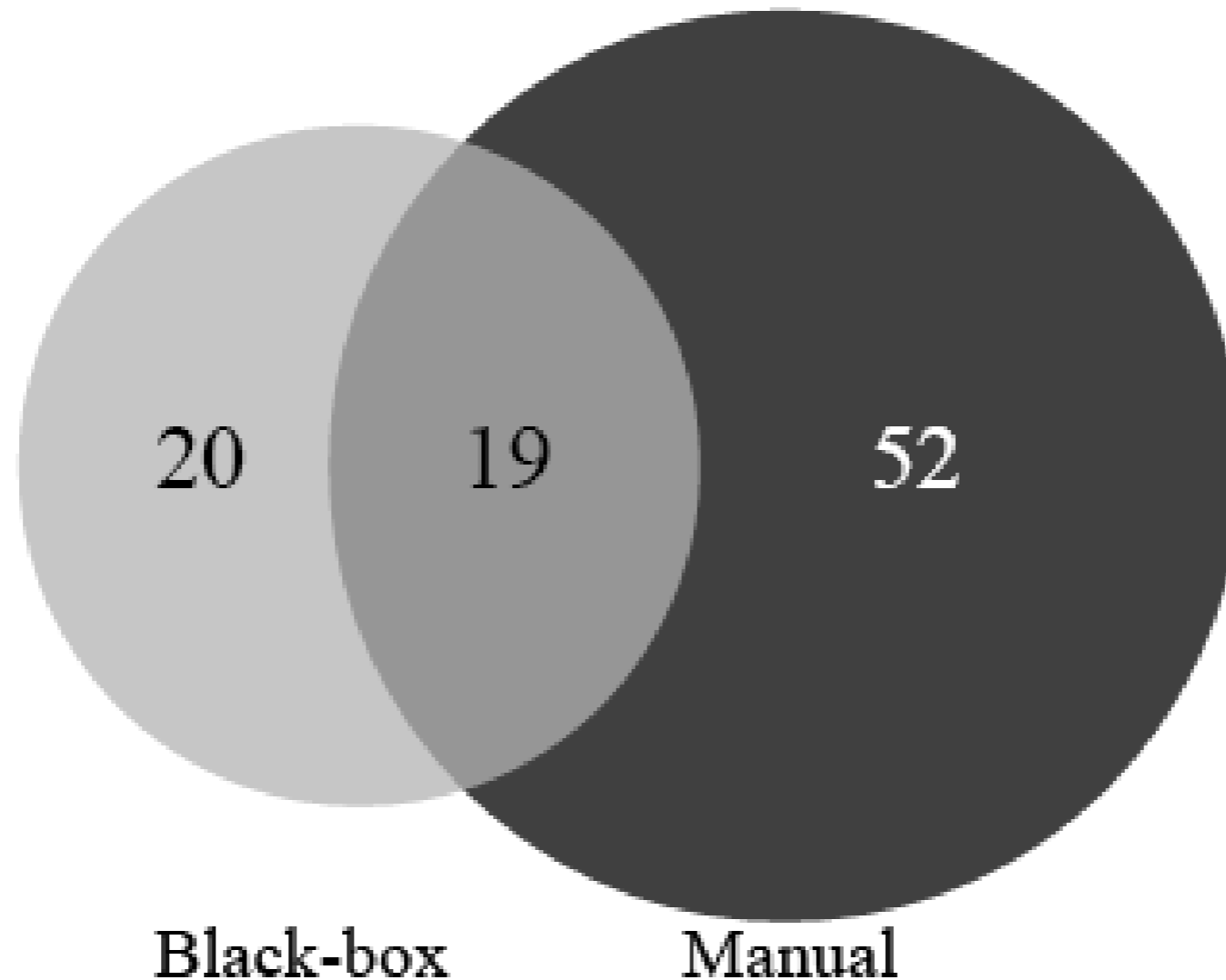


Figure 3: Vulnerabilities found by manual analysis and black-box penetration testing.

Scope: code review

<http://www.cs.berkeley.edu/~daw/papers/webapps11.pdf>

Used with permission.



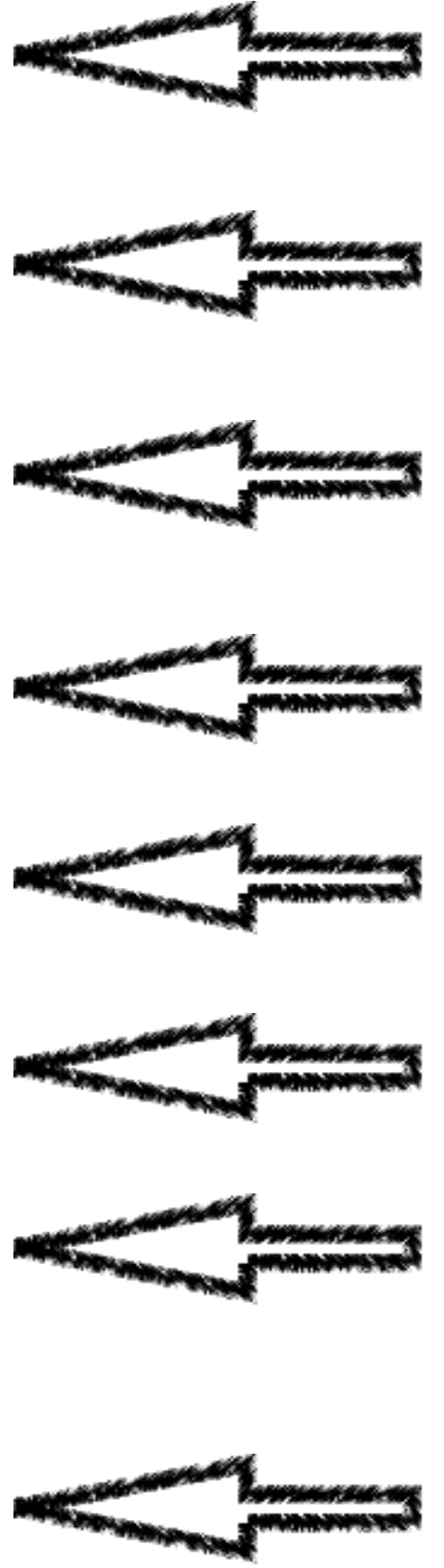
?

.....

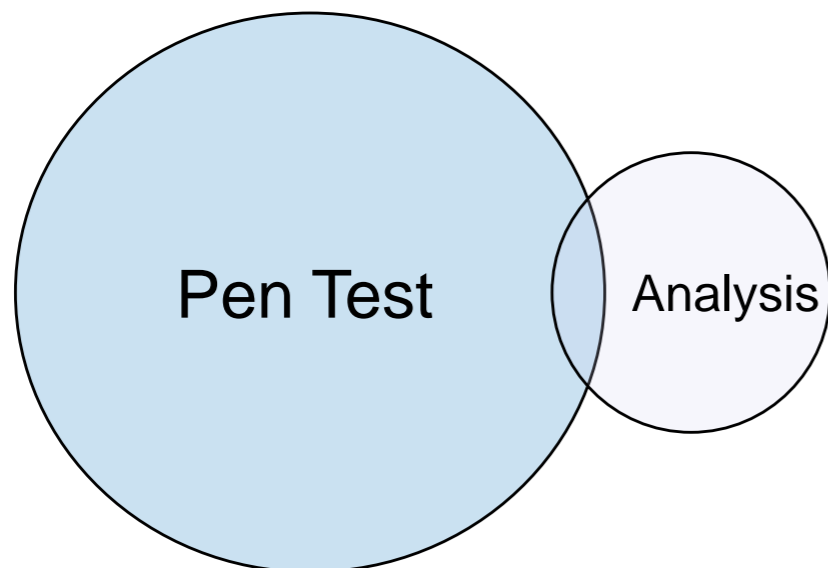
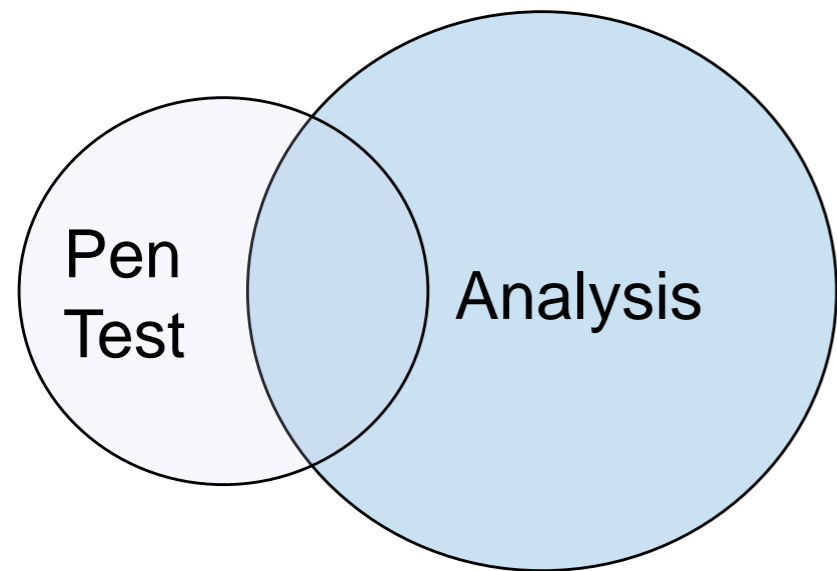
?

Testing

Analysis



Venn Diagrams – Depend on scope



Scope ?

- ✂ Infrastructure configuration
- ✂ Patching
- ✂ Design
- ✂ Coding
- ✂ Controls
- ✂ Crypto v's
- ✂ Input validation

Theory

- ✦ The Venn diagram proportions will be different for a broader scope
- ✦ Pen tests
 - ✦ check the first line of defense
 - ✦ Ideal to provide assurance after design and implementation
- Inspections and analysis
 - ✦ check defense in depth
 - ✦ Determine the level of resilience
 - ✦ Validation against policy and legal requirements

Terminology

✦ Black box

- ✦ No prior knowledge of design or target

✦ White box

- ✦ Design and implementation detail provided
- ✦ Testing by probing

✦ Analysis & inspection

- ✦ Review the design

✦ Inspection

- ✦ code
- ✦ Configuration
- ✦ Accounts and ACLs
- ✦ etc

Web Deployment Trends



- Virtualisation, virtualisation, virtualisation
 - Co-hosting with other's web services
 - Server virtualisation
 - Storage virtualisation

Trends - Storage Virtualisation

- ✦ Stretching of SANs into the DMZ
- ✦ Alternative route into the inside
- ✦ All of an organisation's data in one place
- ✦ SAN controls
 - ✦ Zoning, with Host Bus Adapters
 - ✦ LUN masks or Access Control Lists
 - ✦ Virtual servers can have very broad SAN access
 - ✦ Use a separate SAN

Trends - Storage Virtualisation (2)

References

-  SAN Vendor guides
-  IBM Red Book – SAN Security

Trends - Server Virtualisation

- ⚡ Internet servers on the internal VM farm,
 - ⚡ but mainly separate VM farms
- ⚡ Several key controls not on by default
 - ⚡ ARP spoofing
 - ⚡ MAC changes
 - ⚡ Many DOS controls
 - ⚡ Persistent log files

Trends - Server Virtualisation (2)

🔪 Sprawl

- 🔪 Duplicates running

- 🔪 AV forgotten

- 🔪 Copies of other system snapshots

- 🔪 Clones of insecure development configurations

- 🔪 Snapshots unprotected on file system

🔪 References

- 🔪 VMware Security Hardening Guide , 4.0, 4.1

- 🔪 Microsoft Security Compliance Manager (Hyper-V)

Network Filtering

- ✦ Pen tests and nmap great for obvious stuff ups
- ✦ Weaknesses harder to find
 - ✦ Rules with source network filters
 - ✦ Still seeing plaintext pop
 - ✦ Rules for decommissioned servers (firewall hole reuse)
 - ✦ No filtering from DMZ to internal networks
 - ✦ No egress filtering
 - ✦ Stuff up firewall object definitions
 - ✦ Firewall software flaws and patches
 - ✦ E.g. Cisco Pix ACL bypass

Network Filtering

- ⚔ Vulnerable after a reboot
 - ⚔ Cisco – different running and saved configs
 - ⚔ Unix – disabled daemons that restart next boot
- ⚔ Dodgy browser and proxy certificate trust roots

Network Route Authenticity

- ✦ DOS and Confidentiality attacks
- ✦ BGP authentication
- ✦ Border router outside the firewall
- ✦ Reference, NIST SP800-54
- ✦ Real world attacks and accidents
 - ✦ China Telecom advertised 37 000 unowned networks 2010
 - ✦ Pakistan Telecom blocks YouTube 2008
 - ✦ Malaysian ISP blocks Yahoo 2004
 - ✦ Turkish ISP takes over the Internet 2004,
 - ✦ TTNNet sent out a full table of Internet routes via BGP that routed most Internet traffic through Turkey for several hours
- ✦ (never seen this risk reported by a pen test)

Checking server security resilience

- ✦ Server resilience – easier to find
 - ✦ Network attack surface – services
 - ✦ Pen test – hampered by the firewall
 - ✦ Inspection = very quick
 - ✦ `'netstat -a'`
 - ✦ `'rpcinfo -p '`
 - ✦ Password practices
 - ✦ Account maintenance – former admins
 - ✦ Privilege escalation risks
 - ✦ Process account controls
 - ✦ Race conditions
 - ✦ Protection of access to logs (e.g. password copies)
 - ✦ Protection of log tampering

Server Resilience – Privilege Escalation

- ✦ Plaintext admin access from jump box
- ✦ Common admin/root passwords
- ✦ Sufficient logging of events
- ✦ Poor OS file ACLs
 - ✦ E.g. Unix crontabs
 - ✦ Unix admin trusted path
- ✦ Patch level
 - ✦ Can quickly tell patch status of all packages and not rely on fingerprinting
- ✦ Default passwords on other internal systems

Server Security

🔪 Pen tests

- 🔪 great for checking intrusion detection capabilities

🔪 Systems analysis

- 🔪 Logs not kept for long enough

- 🔪 Increasingly seeing only 2-4 weeks of logs

- 🔪 Faulty or incomplete backup schedules

- 🔪 Faulty 10% of the time (in my experience)

- 🔪 Only cover log data 1/3 of time

- 🔪 Appropriate DR plan & testing

- 🔪 Leakage of data through logs

Windows Server Security

- ✦ Systems analysis
 - ✦ Very easy to inspect GPO
 - ✦ Log settings that help forensics
 - ✦ Good for checking AV deployments
 - ✦ Coverage of systems – particularly virtualised environments
 - ✦ Currency and configuration – heuristics
 - ✦ Run MS tools on the box, MBSA, Sec template

Web Services Security

✦ Systems analysis

- ✦ Check ACLs to services in containers

✦ WS layer

- ✦ user interface protections bypassed
- ✦ inconsistent implementation of access controls compared to user interface
- ✦ simplistic authentication (e.g. single user for all access)
- ✦ lack of authorisation controls and/or acls on service actions (all or nothing).
- ✦ inappropriately detailed error messages (trying to make it easier for developers to build/debug clients)

Wireless Security

- ✦ Systems analysis
 - ✦ Easier to check quality of PSK deployments
 - ✦ Check for Rogue AP detection processes

Resilience – Privilege Escalation via Networks

- ✦ Poor egress filtering
- ✦ Easy access from an owned server
 - ✦ DMZ filtering
 - ✦ Multiple homed servers
 - ✦ Still seeing Unix servers routing
 - ✦ Very easy to check – ndd command
 - ✦ Pen testing – try source routing??
 - ✦ VLAN jumping via shared or trunked switches
- ✦ Access to admin interfaces
 - ✦ Poor authentication policy
 - ✦ Unencrypted access

Resilience – Privilege Escalation via Networks

- ✂ Hacked virtual server spoofing
 - ✂ MAC changes permitted by default

Finding Database Risks

- ✦ Costly or incomplete by pen test
- ✦ Easy to inspect for
 - ✦ DBA roles
 - ✦ Table design – e.g. Application password storage
 - ✦ DB level auditing settings
 - ✦ DB password policies, e.g. DBA password expiry
 - ✦ Limited privileges, e.g. select any tables
 - ✦ Check DB parameters – many compensating controls

Finding DOS Risks

- ✦ Costly to pen test for many DOS risks
- ✦ Easy to inspect for – particularly virtualisation

APT Controls – DSD's 35 Mitigations

- ✦ Can pen test much of DSD
 - ✦ But it is slow
 - ✦ More efficient to test via interviews, then check
- ✦ SPF records published – but filtering of incoming mail?
- ✦ List of blocked file types
- ✦ Web content filtering
- ✦ Randomised local administrator passphrases

Some Poor Pen Tests

- ✦ No tests of authentication lockout
- ✦ No comment on authentication policies
 - ✦ No email address validations
 - ✦ No password complexity checks
 - ✦ No minimum password length
- ✦ No TLS certificate
- ✦ No cookie checks – expiry or ‘secure’
- ✦ Not scanning High UDP ports

Poor Pen Test Reports

- ✦ VPN risks not reported –
 - ✦ ESP aggressive mode
 - ✦ Poor keys – 6 character passwords
- ✦ Firewall unpatched for ACL bypass vulnerability
- ✦ Reporting & communication
 - ✦ “high vulnerability” != “High risk”
 - ✦ Technical security audience v’s CFO or CIO

Take Home Thoughts

✦ Let's be clear to our organisations or clients about

✦ Scope

✦ Assurance provided

✦ Tests conducted

✦ What was not tested (scope, time)

✦ Other recommended testing or analysis

✦ Other possible sources of security risks

✦ Risk levels

✦ v's vulnerability levels

✦ Business v's technical risks