



Where serious technology buyers decide

What you Need to Know About Security Vulnerability Assessments *...that no one is willing to share*



Principle Logic

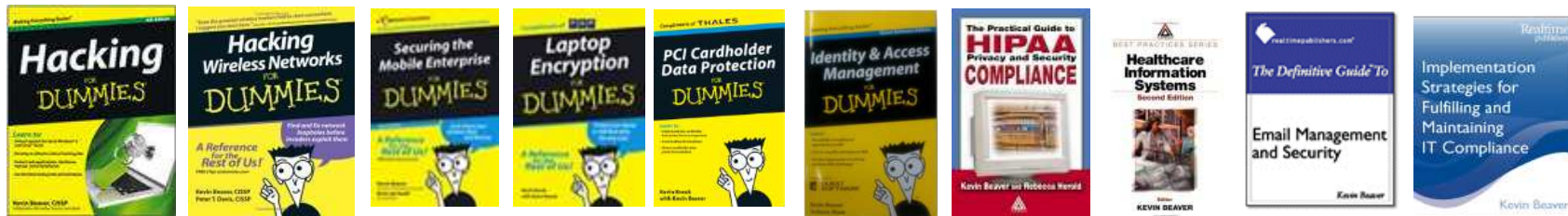
Your Answer to Information Security™



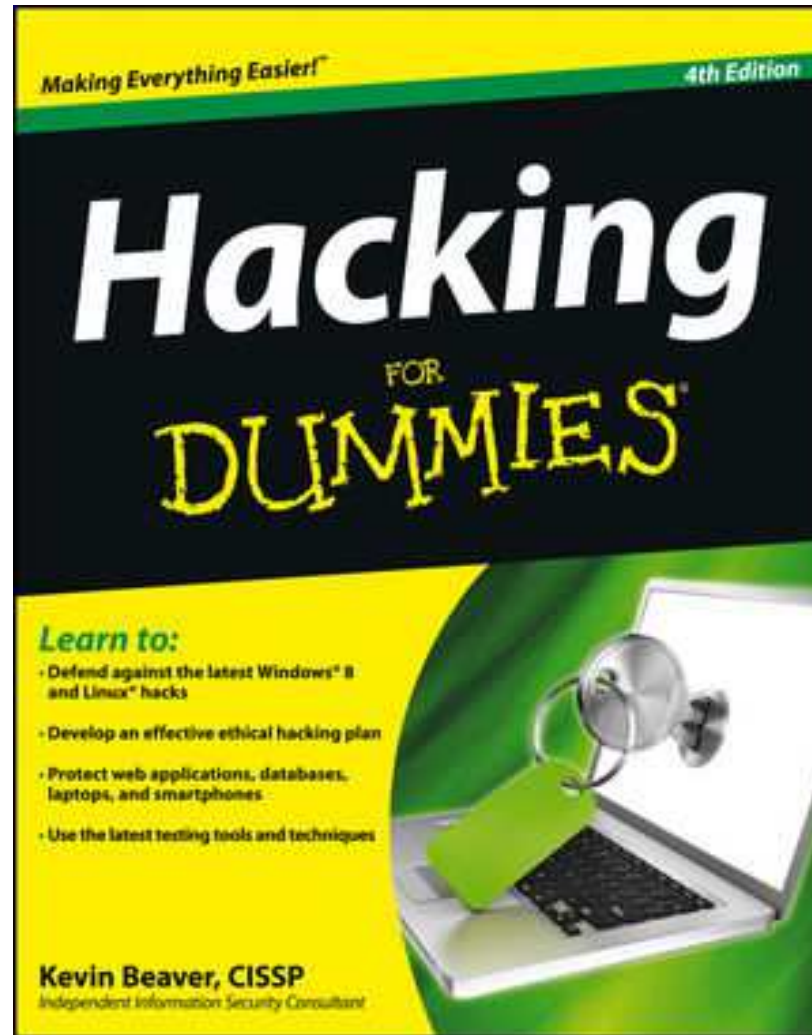
Kevin Beaver, CISSP
*Independent Information Security
Consultant + Writer + Speaker*

A bit about Kevin Beaver

- Independent consultant
 - 24 years experience in IT – 18 years in information security
 - Focus on performing security assessments
- Professional Speaker
- Creator/author of **Security On Wheels** audiobooks & blog (securityonwheels.com)
- Writer



Kevin's latest book: *Hacking for Dummies*





All's well
in IT...
Right?


Not so fast

Well, if marketing
says so...

AM I HACKER PROOF?

FIND OUT
WITH JUST
ONE CLICK!



A diverse group of approximately 15 people of various ages and ethnicities are standing behind a large white banner. They are all smiling and looking towards the camera. The banner is held up by their hands and contains the text "Don't worry. We'll find the flaws if you don't." in a bold, black, sans-serif font. The background is a plain, light-colored wall.

**Don't worry. We'll find the
flaws if you don't.**

To think you'll
find everything is
delusional.

Pen tests

v.

Audits

v.

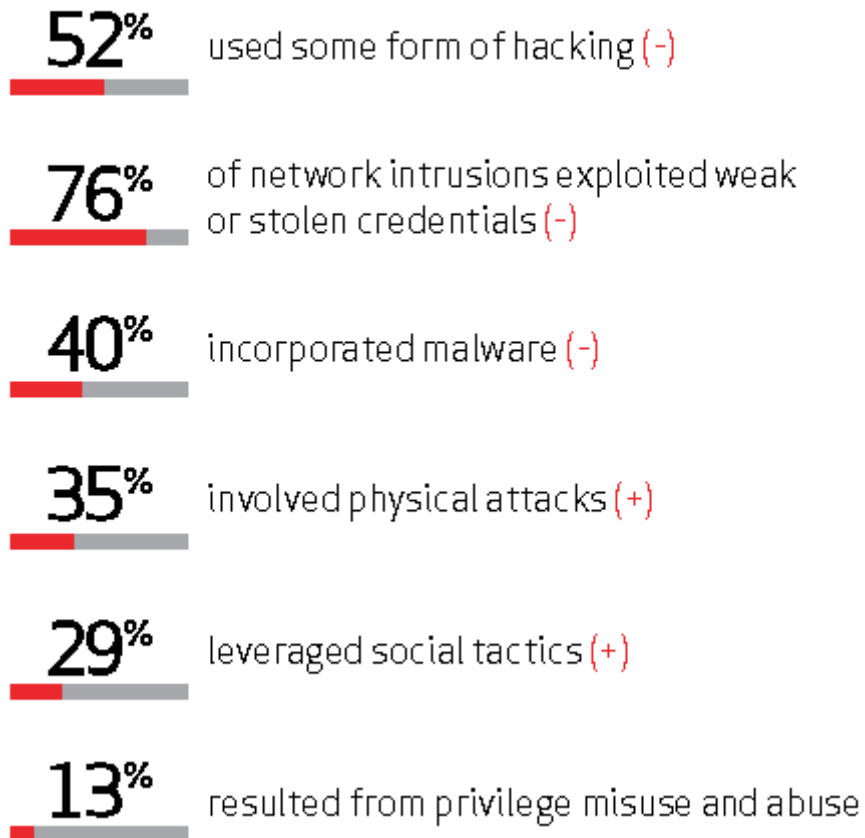
Vulnerability
Assessments

Who am I?



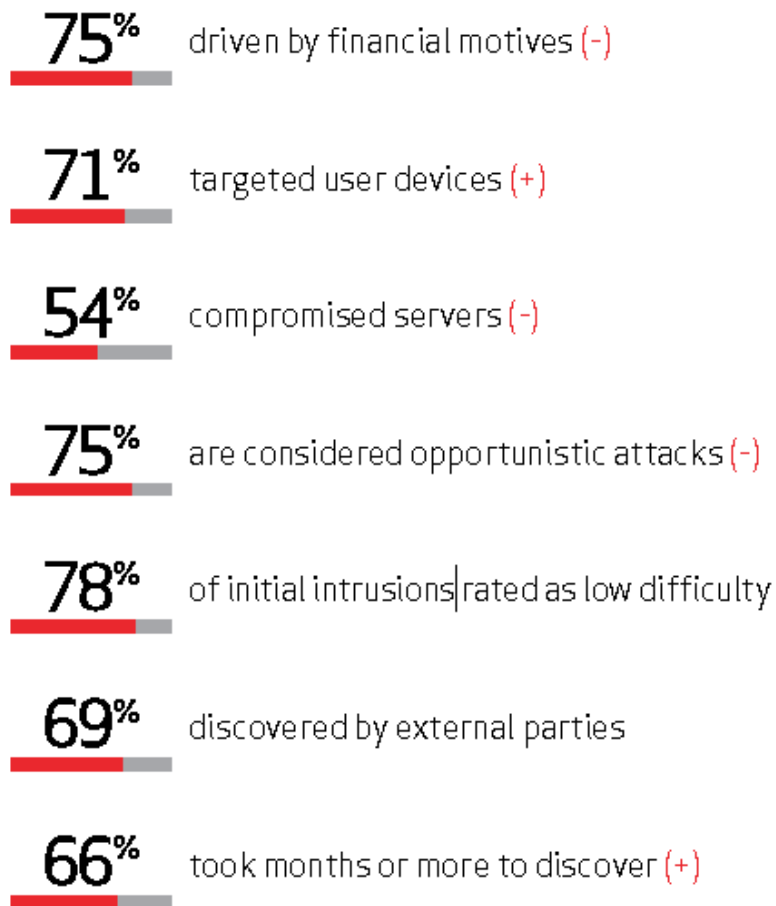
2013 Verizon Data Breach Investigations Report

How do breaches occur?



2013 Verizon Data Breach Investigations Report

What commonalities exist?







Minimal testing.
De facto **standard**.

A definition

equivocal \ih-KWIV-uh-kul\ adjective

- 1 a: subject to two or more interpretations and usually used to mislead or confuse
b: uncertain as an indication or sign

- 2 a: of uncertain nature or classification
b: of uncertain disposition toward a person or thing : undecided
c: of doubtful advantage, genuineness, or moral rectitude

-Merriam-Webster

Critical to your vendor.
Meaningless to your
business.



It's all in your
perspective.



Look for the
vulnerabilities that
count.

Most **urgent** flaws.

on your

Most **important**

systems.

Scanners won't easily find...

- ▶ Open shares exposing PII to groups who don't need access
- ▶ Missing whole disk encryption
- ▶ Improperly secured phones and tablets
- ▶ Default passwords on physical security systems
- ▶ Network protocol anomalies

But they may uncover...

- ▶ BIG “flaws” that aren’t a problem
- ▶ Data in transit weaknesses that will likely never be exploited
- ▶ Zero-day vulnerabilities with no known fixes

Focus on
the givens.

Only *you* will know.



Think
reasonable.

A pair of hands is holding a white rectangular sign against a white background. The sign contains the text "Common sense is a virtue." in a bold, sans-serif font. The word "virtue" is highlighted in red, while the rest of the text is black.

**Common
sense is
a virtue.**

A definition

UNequivocal \ən-ih-KWIV-uh-ku\ adjective


- 1 a: leaving no doubt
- b: clear, unambiguous
- 2 : unquestionable

-Merriam-Webster

Apathy is the enemy



Underimplemented

Two hands are positioned to form a rectangular frame around the central text. The top hand is on the left, with the index finger pointing right and the thumb pointing down. The bottom hand is on the right, with the index finger pointing left and the thumb pointing up. The text is centered within this frame.

Lack of
perceived risk
does not
mean **no** risk

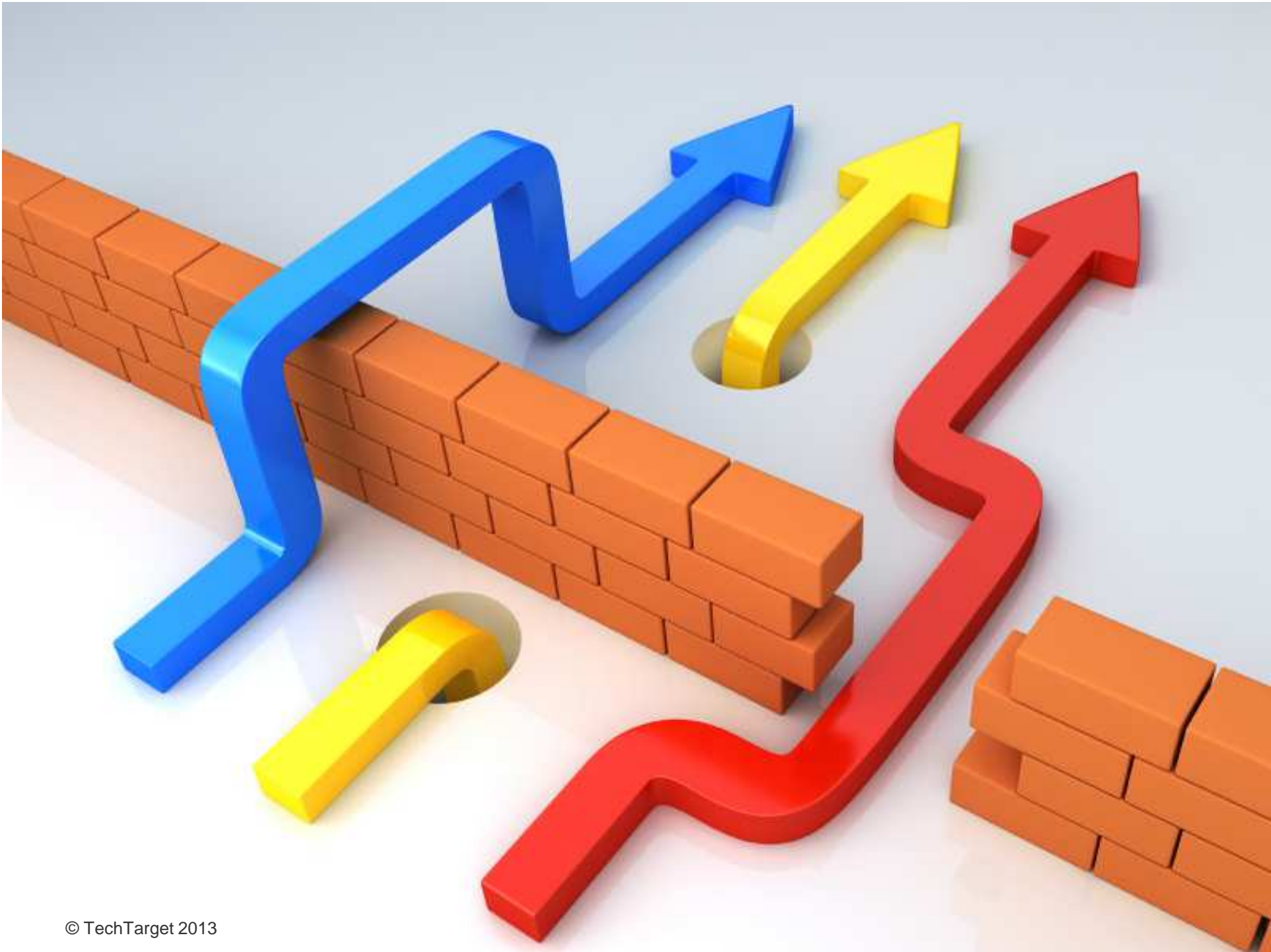
Never **assume** the
right people know all
the right things.



Never assume the
right people are
talking to one
another.

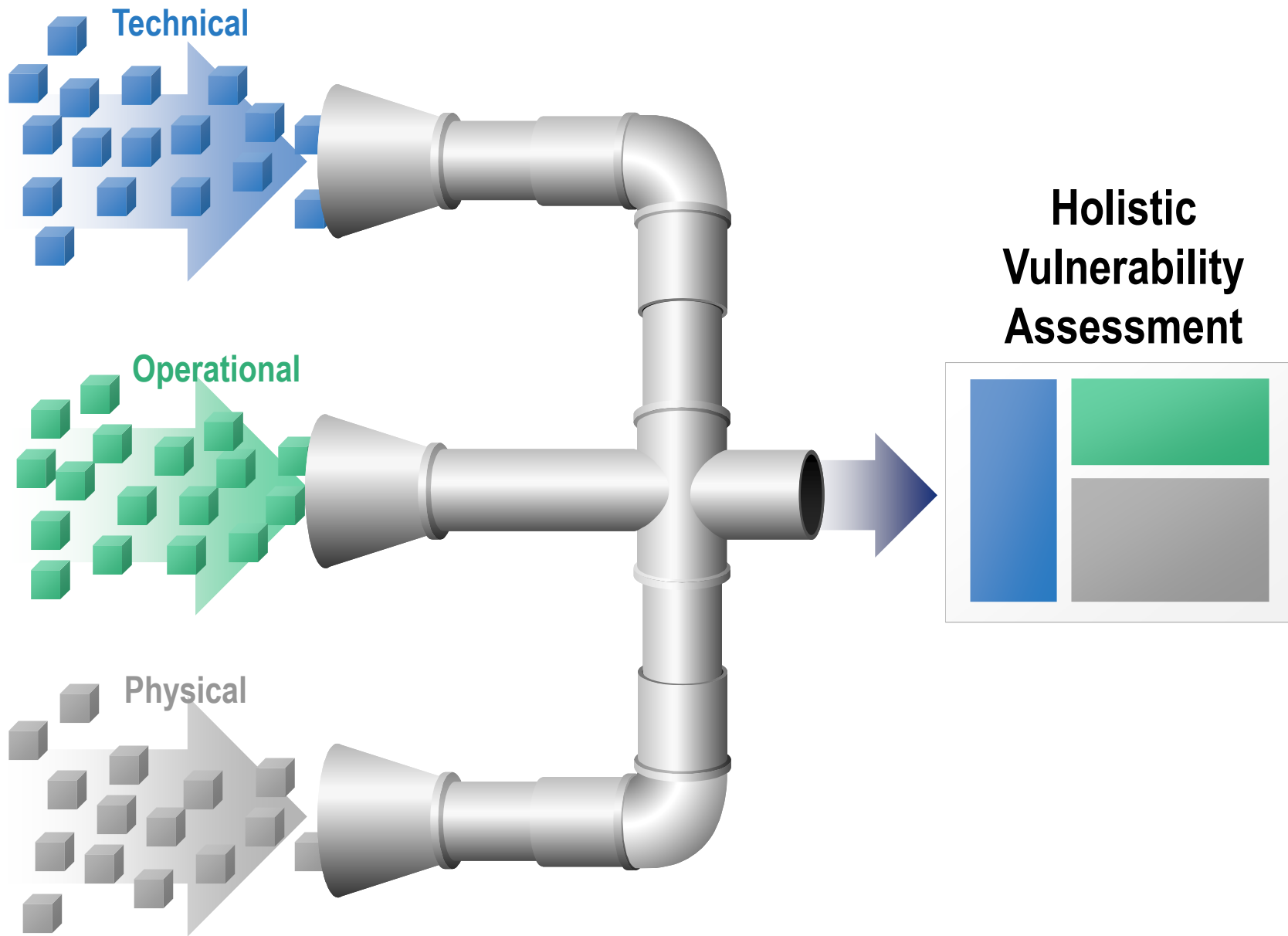


When was the last
time...?



What are you trying to do?

- ✓ What are you trying to protect?
- ✓ What are you trying to protect against?
- ✓ What audit requirements do you have?
- ✓ What regulations are you up against?
- ✓ Are you assessing what matters?
- ✓ What do your policies say? Contracts & SLAs?



The five phases

PHASE 1: Planning

PHASE 2: Testing

PHASE 3: Analyzing

PHASE 4: Reporting

PHASE 5: Implementing
Changes

Planning things out

- What will be tested?
- Dates/times?
- How often?
- Blind or knowledge assessments?
- Denial of service testing?
- Who's the sponsor?
- It's all about expectations.

What's your scope?

- Network hosts
- Servers
- Workstations
- Websites
- Web applications (cloud included!)
- Databases
- Storage
- Mobile devices
- Mobile apps
- Physical security controls

If it has an **IP address**
or a **URL**, it's fair
game...eventually.

Carrying out your tests

STEP 1: Reconnaissance

STEP 2: Enumeration

STEP 3: Vulnerability
Identification

STEP 4: Proof

Demonstrate rather
than exploit.

Things I've learned the hard way

Under-scoping projects

Relying only on manual analysis

Relying only on scans

Assuming that a completed scan = completion

Believing that a failed scan = good enough

Only scanning systems running on default/assumed ports

Web Security Testing....

Things to Consider

- ✓ Browser-specific flaws
- ✓ User-specific flaws
- ✓ Authentication mechanism
- ✓ DoS susceptibility
- ✓ “Possible” SQL injections
- ✓ WAFs & SSL = false sense of security
- ✓ Everything below layer 7
- ✓ Multiple scanners are required

Multiple Web
vulnerability scanners
are *required*.

Tools I Often Use (Network, OS)

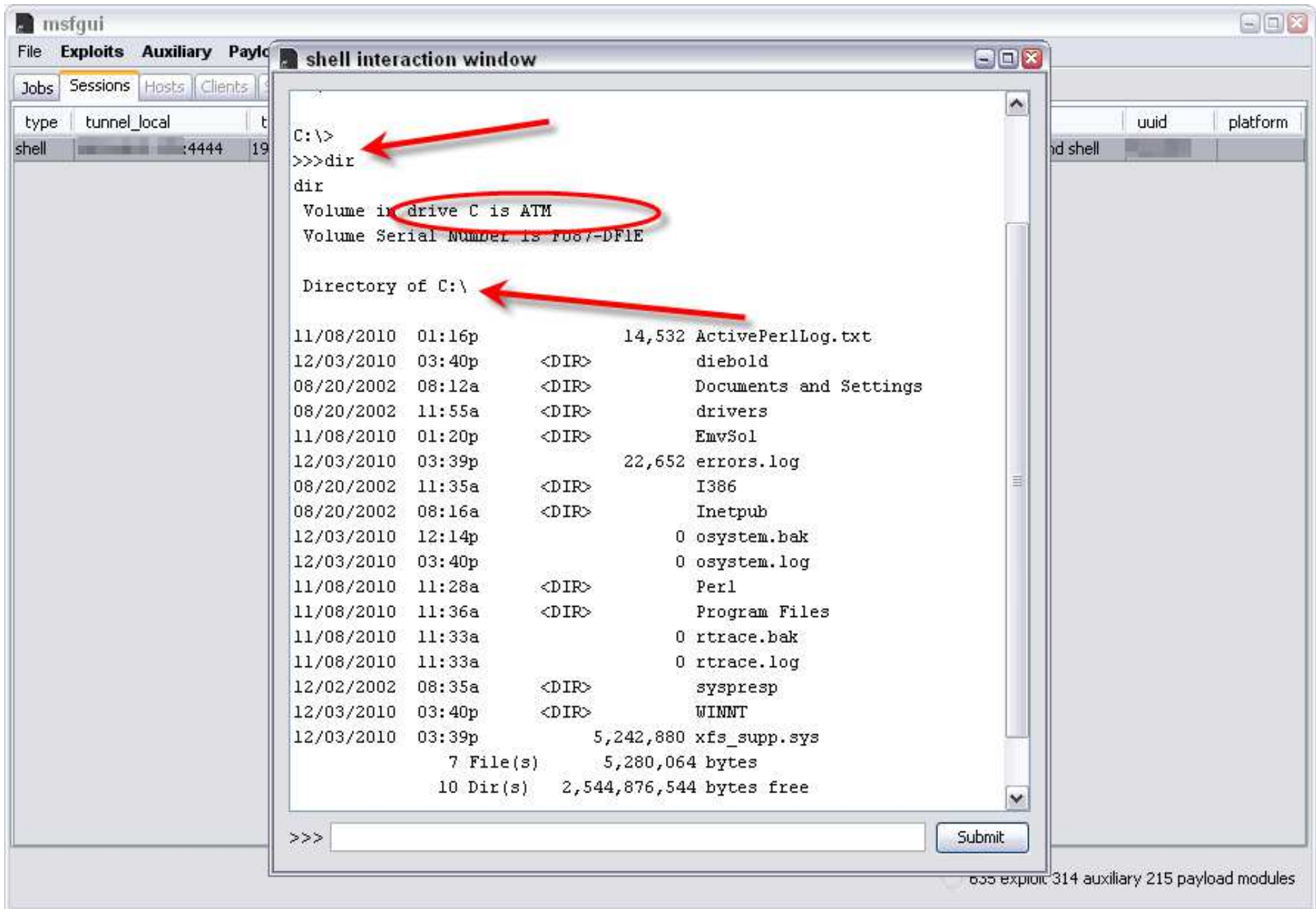
- NetScanTools Pro
- QualysGuard
- Nexpose
- GFI LanGuard
- Metasploit
- OmniPeek
- Cain & Abel
- AlgoSec Firewall Analyzer



Tools I Often Use (Web)

- QualysGuard
- Nexpose
- WebInspect
- Acunetix Web Vulnerability Scanner
- Netsparker
- NTOspider
- Firefox Web Developer
- Checkmarx CxDeveloper

Authenticated
testing is critical.





Tools I Often Use (Mobile)

- IdentityFinder
- CommView for WiFi
- Reaver Pro
- Ophcrack
- Elcomsoft System Recovery
- Elcomsoft Forensic Disk Decryptor
- Elcomsoft iOS Forensic Toolkit
- Oxygen Forensic Suite
- Passware Kit Forensic

Your tools will
be an *enabler*
or a **hindrance**.

Owning the tool ≠
knowing how to
properly use the tool.

Only You!

(never forget this)

Look for the
vulnerabilities that
count.

Identity Finder Status



identityfinder

Searching: Search Completed in 3 days, 20 hours, 4 minutes, and 51 seconds

Progress: 00.00% Overall: 00/00

Locations Containing Identity Matches/Total Locations Searched: 24290/116263 Total Identities Found: 3256101

Files: 116054	Messages: 0	Browser Data: 0
Compressed: 209	Attachments: 0	Registry: 0

Social Security: 3255824	Date of Birth: 0	SIN(Canada): 0	Keyword: 0
Credit Card: 240	Phone: 0	NINO(UK): 0	RegEx: 0
Password: 37	E-Mail Addr: 0	NHS No.(UK): 0	Dictionary: 0
Bank Account: 0	Address: 0	TFN(Australia): 0	
Driver License: 0	Passport: 0	Maiden Name: 0	



Operational and Technical


Respect the law of
diminishing returns.



Report your findings.

Follow-up on your
findings.

Checklist

- 
- Get to know your network
 - Understand the risk requirements
 - Learn your existing tools
 - Try out new tools
 - Stay sharp

Test now.
Test often.

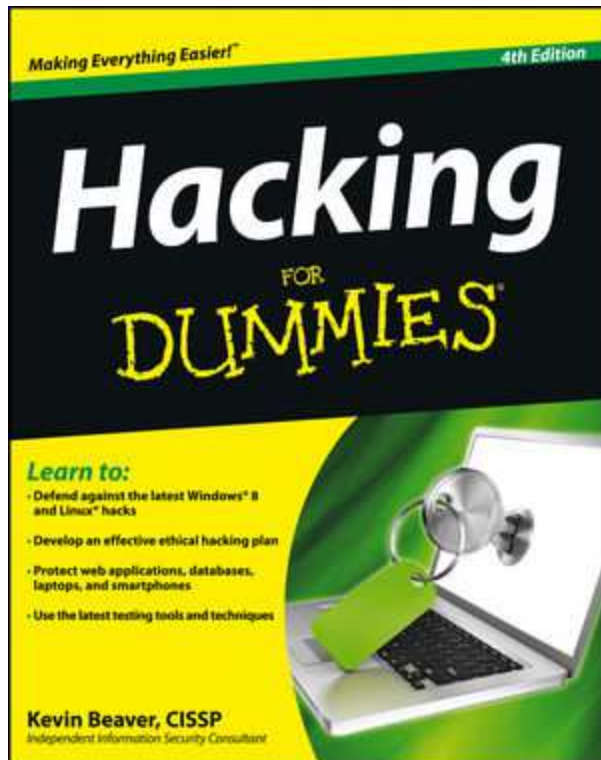
Prevention is easier
than repair.



Unless
and
until...

**You *cannot* secure
what you don't
acknowledge.**

Hacking for Dummies: Downloadable sample chapters



Hacking For Dummies (4th ed.) Chapter 7 Passwords
<http://searchenterprisedesktop.techtarget.com/feature/Chapter-excerpt-Defending-the-enterprise-from-password-hacking>

IT Knowledge Exchange Book excerpts: Hacking for Dummies

<http://itknowledgeexchange.techtarget.com/bookworm/book-excerpt-hacking-for-dummies>

<http://itknowledgeexchange.techtarget.com/bookworm/book-excerpt-hacking-for-dummies-part-2>

Hacking For Dummies (1st ed.) Chapter 10 Wireless LANs

<http://searchsecurity.techtarget.com/tip/Hacking-for-Dummies-Chapter-10-Wireless-LANs>

About Kevin Beaver

- My website: principlelogic.com/resources
- My blog: securityonwheels.com/blog
- My audio programs: securityonwheels.com



@kevinbeaver
PrincipleLogic



www.linkedin.com/in/kevinbeaver

Live Q&A with Kevin Beaver

- Submit questions for Kevin via the text chat area
- Kevin will answer questions during and/or after his presentation
- At the end of today's webcast, participants who ask the best questions (as determined by Kevin) will receive a free copy of *Hacking for Dummies*
- Those selected should contact us at:
editor@searchsecurity.com

