Trustwave® SpiderLabs®

Pentesting for fun... and profit!

David M. N. Bryan and Rob Havelt

Agenda

- Who are David & Rob?
- Why are we experts?
- Why do penetration tests?
- What is a penetration test?
- What is the goal?
- Some says it’s a fad…
- What should be included?
- Critical data?
- Who is the audience?
- Methodology of pentest…
- Scripts, Tool, and Exploits oh my!
- Stories & Examples

David M. N. Bryan

- Computer Security Professional, Aka “Hacker” – SpiderLabs
- DEFCON network goon
- OWASP Local and National
- DC612 Group
- President of TC Makers Hackerspace
- HAM radio license
- CISSP
- 10+ years security experience
- Play with electronics
- Video, Bikes, Brews beer

Rob Havelt

- Tinkering and hacking stuff since he was 7
- Hates people but loves gatherings, isn't it ironic?
- Knows an awful lot about Zombie movies
- Built the Pen Test Team at SpiderLabs in 2005
- Built 2 other successful Pen Test Teams before that
- Has been: A Webmaster, Sysadmin, Firewall Dude, Systems Guy, 3D Artist, Absurdist Performer, Pen Tester, TSCM Guy, and lots of other stuff.

Why are we experts.

- **We have a lots of experience, no really…**
  - **Over 1,900 pen tests in 2009**
    - **Finance/PCI**
    - **Retail**
    - **Manufacturing**
    - **Hospitality**
    - **Government**
    - **Education**
    - **Healthcare**
    - **Other**

Why do penetration tests?

Assessments cost $$, for what value?

- Assessments often have a large scope
- Only identify flaws of in scope items
- Take a long time
- Requires internal resources & babysitting...

So How do I get the most value out of a security engagement?

- Assessment - review policies, procedures, standards, run tools, etc... (~125-150K+)
  - Get potential threats, huge report, lots of data to sift though
- Pentest, minimal coordination & babysitting (~10-50K)
  - Get actualized threats, with real world issues
  - Receive recommendations applicable to the environment

What is a penetration test?

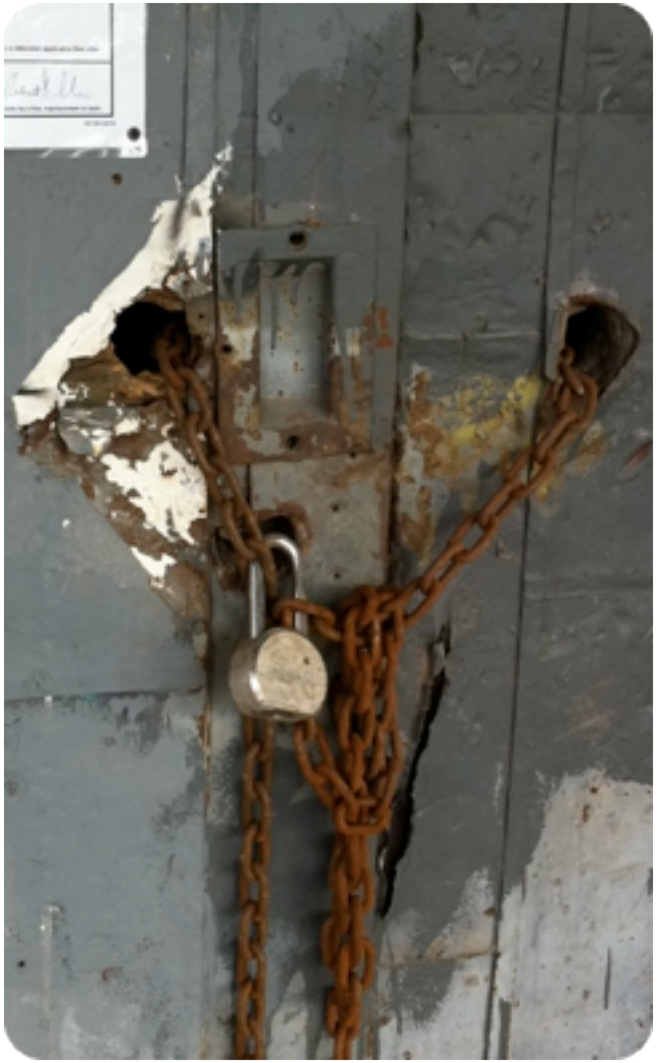
What isn’t a pentest…

- Any scan, or any automated process that results in an automated report being created
  - Many do this, but are just running Nessus, Qualys, nCircle, Rapid7, etc.
  - Just using: Metasploit, Canvas, Core Impact, etc.

What it should be…

- Finding and gaining unauthorized access to systems or computers that contain sensitive or confidential information
- Identifying systems or computers that have been left behind- not a comprehensive “scan”
  - Justify budget for tools, services, personal

Goals



Identify critical systems/applications

- Gather intel
- Identify critical assets
- Identify locations of data
- Subvert access controls of systems
- Gain access to sensitive or critical data

Recommend controls

- Patching
- Hardening
- Logging/Auditing
- NAC
- Other weak or poor controls

Marcus says it's a fad…

…just like crash testing

Intangible

A lot of people have a hard time with the intangibility of security.

- We can look to tangible processes to illustrate what is appropriate, when.
- It can also cause big problems
  - For Instance, if you hire an engineer to design something tangible and that thing immediately falls apart, you know you have an awful engineer.
  - With a Security Professional, you might not know they are awful until you are successfully attacked, or you are exposed to someone better.

Principals of Testing

In order for Testing to be a meaningful Quality Assurance Function:

- It should simulate attack conditions as accurately as possible
- It shouldn't just be focused on Gaining access to the environment or escalation of privileges – that's only 2/5ths of an attack. I.e.
- I DON'T CARE where you got shells.
- More focus should be given on ways to identify, acquire, and even exfiltrate data in the environment. If your tester isn't doing this, you are paying for a half finished job.

Oh and Also:

ENOUGH with the TOOLS already!!

- I trust a Pen Tester that immediately brings the conversation to their tool set about as much as I trust a doctor that sits me down and discusses what brand of scalpels they will be using.

Testing

Types and Uses

- Application, Web Application
- Infrastructure
- Physical
- Social

Most of what we will be talking about refers to infrastructure, physical, and social.

Scope?

What should be in scope?

- Think networks, not systems
- Even Better – think business processes
- Think data compromises, not number of systems
- Think remote access
- Define network ranges, and data targets, not specific systems
- A good pentester is quick... and doesn’t necessarily need preparation

Critical Data

This is rather the point isn't it?

- Any testing you do should be focused on this.
- We secure systems because we don't want an attacker to get critical data.
- Any test should be aimed at putting this into context.

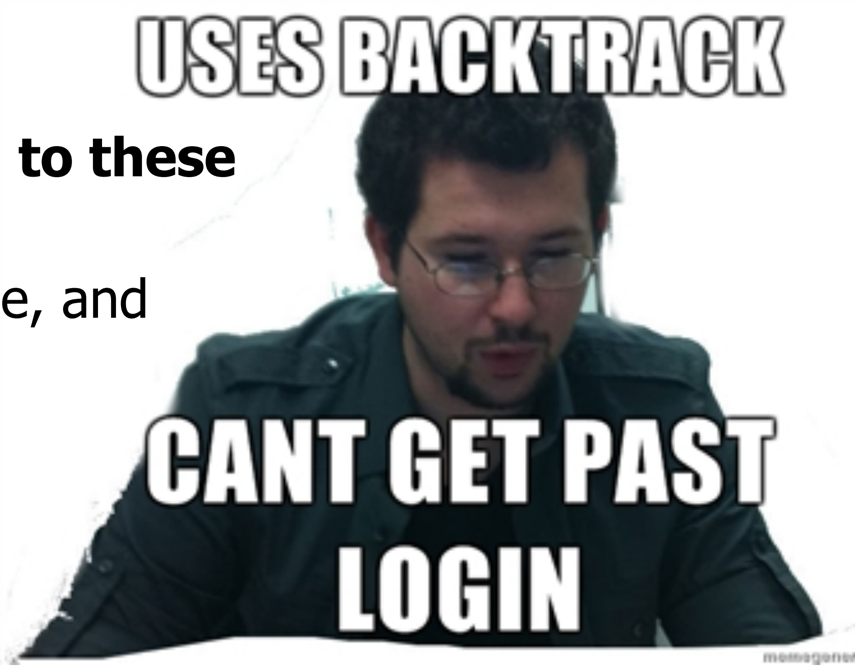
Who's your Audience

Who is going to read and make decisions based on this data?

- Decisions makers & influencers
- Middle management
- C-Level upper management

Make sure the data being presented to these different levels is consumable

- Executive reports must make sense, and provide value.



Methodology

Available Standards

- Open Source Security Testing Methodology Manual
- NIST SP800-115
- CREST
- IACRB
- GPEN
- OSCP
- Etc, etc, etc...

These "Certs" may only certify that your pentester can run tools...

Scripts, Tool, and Exploits oh my!

Remember When Photoshop became popular in the 90’s?

- It was an extremely powerful tool to digitally produce certain effects that photography professionals had to do manually via double exposure camera tricks, and lighting effects.
- Simply owning a copy of Photoshop did not make you a photography professional.
- There was and still are a lot of people that think it does.

Scripts, Tool, and Exploits oh my! Cont.

In the hands of a professional who understands the science and technique, Photoshop can be a very powerful tool.

Scripts, Tool, and Exploits oh my! Cont.

In the hands of an amateur running random filters – not so much.

Plus, Photoshop is not the only thing you need to be a professional photographer and/or digital artist.

Certs…

- **Adobe has a cert too called "Adobe Certified Expert"**

Scripts, Tool, and Exploits oh my! Cont.

Why am I taking up your time at an Infosec conference talking about Photoshop?

- Because there is a direct correlation here about what Photoshop did for professional photography and what automated pen test tools do for offensive security.
- Tools like Core, the new Metasploit Pro, and others can be useful/powerful in the hands of a professional.
- A professional doesn't really *need* these tools. They can often do amazing work without them.

Scripts, Tool, and Exploits oh my! Cont.

So what tools does a Pen Tester use?

- **Anything they need to get the job done!**
  - General Networking and sysadmin tools
  - Custom stuff to do specific tasks
  - Network proxies and servers
  - Attack and exploit frameworks
  - Monitoring and log tools
  - There might be thousands of potential tools depending on the situation.

Let's Compare Methods and Results

Let's Test an Ecom Network as an insider using host testing

- Client picks 10 IP's that are part of the Ecom system, tester only looks at those IP's and nothing else.
- What is there to test?
  - Software vulnerabilities, and grievous configuration errors on those hosts.
- What are the results?
  - There are a few minor findings and vulnerabilities noted, however, no compromise.
  -

CONGRATULATIONS! Your Ecom system is safe.

Let’s Compare Methods and Results

Let’s Test an Ecom Network as an insider using holistic testing

- Client provides direction as to where the Ecom systems are, but the tester can get info from anywhere.
- What is there to test?
  - All security controls around this system, interconnections and trust relationships that might be exploited, infrastructure configuration errors, architecture mistakes, as well as software vulnerabilities and configuration errors on the hosts.
- What are the results?
  - Tester finds a forgotten system with blank local admin, dumps cached domain logins, gets him domain admin, which leads to a whole series of events which gives access to the ecom database.
  -

OH NO! Your Ecom system is faulty! Plus you know tons more about your general security control shortcomings.

Trustwave®
SpiderLabs®

Stories and Techniques

AD Domain enumeration

Ad Tools

- enum4linux.pl - Null session?
  - UID guessing to enumerate
- smbclient
- smbtree
- winexe
- tcpdump?

Password guessing...

- VNC, try default passwords, might get lucky...
- HTTP - again default passwords
- Medusa
  - Password = username
  - Password = password
  - password = realldumbpassword
  - Follow password account lockouts from enum4linux.pl

Man-In-The-Middle

Wired Spoofing

- ettercap-ng
- cain
- dsniff

Inject

- Get client to fallback to LanMan - Bingo
- Process ntlm challenges for others
  - Bring hashes to rainbow tables
  - Simply Pass The Hash...

Wireless

- FakeAP
- Karma
- Karmetasploit

Web

Why do my pentesters have to know about the Web?

- **Directory enumeration**
- **SQL Injections**
- **Cross-Site Scripting**
- **Program execution**
- **PUT Methods**
- **Weak web systems**
- **Etc…**

Payment Environment

PCI DMZ - All was thought to be safe...

- Found a test VM system that was using unencrypted LDAP to login - Grabbed creds
- Use those creds to login to the local workstation
- Dumped system hashes and cashed creds using gsecdump (repacked)
- Grabbed local workstation admin account hash, reused it on about 50% of the machines on the domain.
- Found an AD account that could login via psexec to other domain systems (yeah!)
- Identified domain admins, found their workstation, dumped their workstation hashes (cracked off-line via rainbow tables)

Payment environment cont..

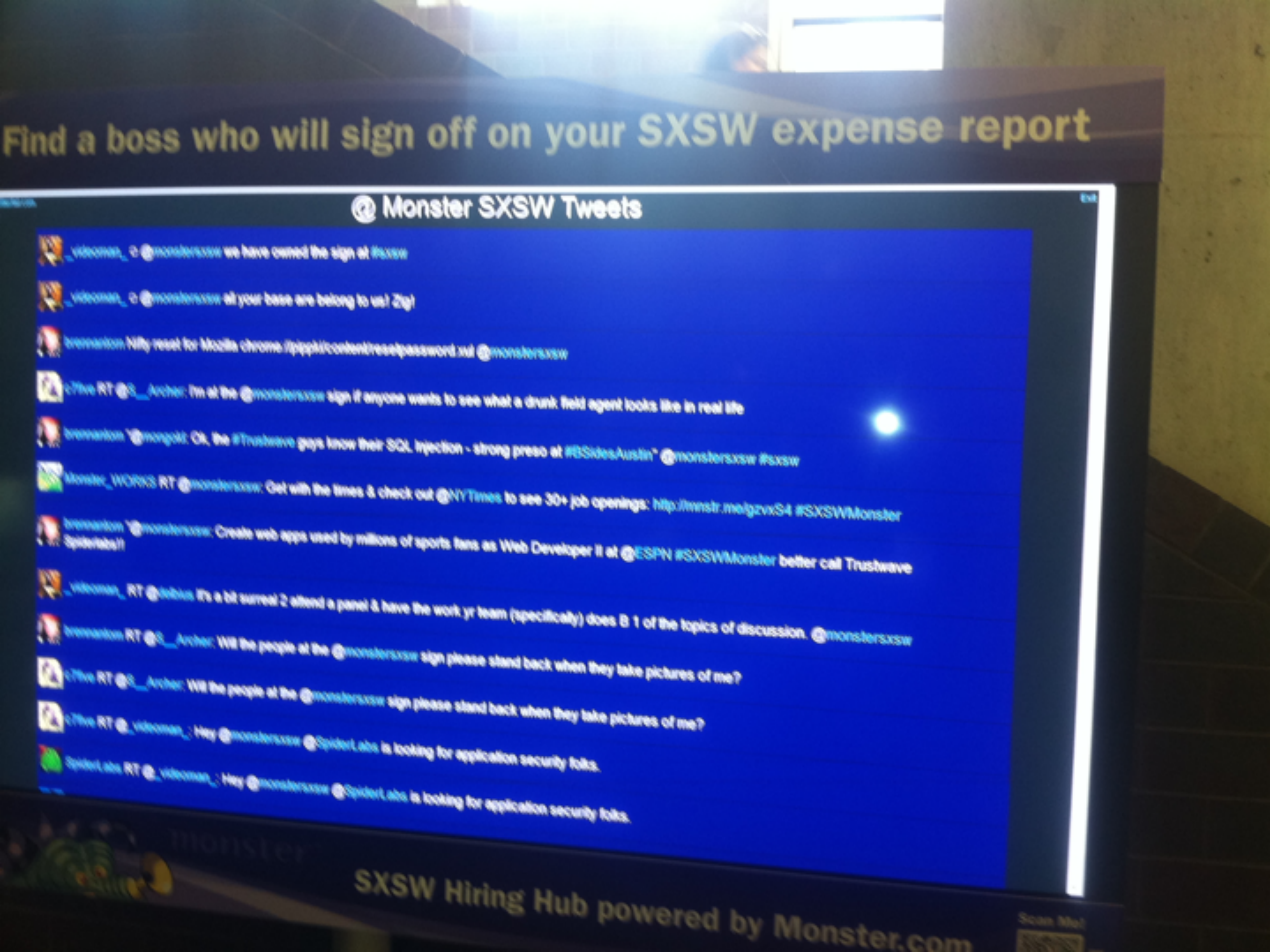
- Once I got domain admin Hashes, used psexec to loging to DC
- Added a user to the domain and that user to the domain admins group (domain pwned).
- But that’s not what the goal was... not we have to keep going...

- Next dumped 1,500+ user hashes from the DC, cracked them all.
- Found the 2 systems that were the jump servers into the PCI environment.
  - 1 windows
  - 1 Solaris
    - 4 of the 1500 credentials were the same on the Windows system
    - 104 of the 1500 worked on solaris
- Moral of the story, don’t allow the same passwords to be used between these systems.

Wrap-up

Pentesting...

- Can add a lot of value, if done right.
- The previous version of pentesting (running scanners) is dead.
- Long live the art of manual testing, with skilled and seasoned professionals!


Find a boss who will sign off on your SXSW expense report
monster
SXSW Hiring Hub powered by Monster.com
Scan Me!
Exit

@ Monster SXSW Tweets

videoman @ @monstersxsw we have owned the sign at #sxsw

videoman @ @monstersxsw all your base are belong to us! Zig!

brennantom Nifty reset for Mozilla chrome://pippki/content/resetpassword.xul @monstersxsw

c7five RT @S__Archer: I'm at the @monstersxsw sign if anyone wants to see what a drunk field agent looks like in real life

brennantom "@mongoid: Ok, the #Trustwave guys know their SQL injection - strong preso at #BSidesAustin" @monstersxsw #sxsw

Monster_WORKS RT @monstersxsw: Get with the times & check out @NYTimes to see 30+ job openings: http://mnstr.me/gzvxS4 #SXSWMonster

brennantom "@monstersxsw: Create web apps used by millions of sports fans as Web Developer II at @ESPN #SXSWMonster better call Trustwave Spiderlabs!!

videoman RT @dobius It's a bit surreal 2 attend a panel & have the work yr team (specifically) does B 1 of the topics of discussion. @monstersxsw

brennantom RT @S__Archer: Will the people at the @monstersxsw sign please stand back when they take pictures of me?

c7five RT @S__Archer: Will the people at the @monstersxsw sign please stand back when they take pictures of me?

c7five RT @_videoman_: Hey @monstersxsw @SpiderLabs is looking for application security folks.

SpiderLabs RT @_videoman_: Hey @monstersxsw @SpiderLabs is looking for application security folks.

Trustwave®

SpiderLabs®

Questions?

Thank you!

Rob Havelt

Director

Penetration Testing, SpiderLabs

rhavelt@trustwave.com

David M. N. Bryan

Senior Security Consultant

Penetration Testing, SpiderLabs

dbryan@trustwave.com

References

- http://en.wikipedia.org/wiki/Web_2
- http://blog.tenablesecurity.com/2008/12/marcus-ranum-pauldotcom-interview-on-penetration-testing-.html