How I Learned to Stop Worrying and Love Compliance

Ron Gula, CEO Tenable Network Security
PART 2 – SECURITY IMPACT

RED SHIRT
Dead Man Walking!
THEMES – BUILD A MODEL
THEMES – MONITOR FOR FAILURE

FAIL
THEMES – DEMONSTRATE COMPLIANCE
WE ARE IN A GREAT CAREER FIELD

THE GEEKS SHALL INHERIT THE EARTH
Enterprise Vulnerability, Patch and Config Auditing

Continuous PCI and FDCC System and event monitoring

Agent and Agentless Log Aggregation and Search

Network monitoring of Servers, Clients and Databases

Continuous Web Application Security Assessments and Monitoring

- Database Activity Monitoring
- USB Device usage
- Botnet and Virus detection
- Software Enumeration
- Insider Threat detection
- Antivirus auditing
- 3D network and event graphs
- File integrity monitoring
- 24x7 discovery of systems
... and much more!
PART 1 - COMPLIANCE STANDARDS

Monty Python's Flying Circus
Ministry of Silly Walks
Demonstrating compliance is just as difficult as understanding why.

Figuring out ways to enforce desired state isn’t that easy either!
When we do get it right, we don’t want to stray from the desired behavior.
The USA Federal government has outpaced commercial and international standards.
If I change that setting, it won’t be compliant Sir.

SCAP #&!0 XCCDF 
%#! FISMA $^$& 
CNA my $&$&$!!
National Checklist Program
Formerly the (NIST Security Configuration Checklist Program)

Federal Desktop Core Configuration settings (FDCC)
NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP). FDCC Checklists are available here (to be used with SCAP FDCC capable tools). SCAP FDCC Capable Tools are available here.

Checklist resources:
- Checklist Program Website
- Checklist Repository
- NIST Special Publication 800-70: Security Configuration Checklists Program for IT Products

The Cyber Security Research and Development Act of 2002 tasks the National Institute of Standards and Technology (NIST) to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government." Such checklists, when combined with well-developed guidance, leveraged with high-quality security expertise, vendor product knowledge, operational experience, and accompanied with tools, can markedly reduce the vulnerability exposure of an organization.
PCI is still criticized for not being tough enough or too difficult.
What is PCI?

Pass Quarterly Vuln Scans

Demonstrate that your patching, AV, firewall, IDS, web apps, wireless, WAF, user access, configs and databases are secure.
PCI IS **GOOD** – BUT IT POINTS FINGERS
<table>
<thead>
<tr>
<th><strong>Government</strong></th>
<th><strong>Commercial</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Single standard with enforcement</td>
<td>Many standards and no enforcement</td>
</tr>
<tr>
<td>Trying to make agency communication work</td>
<td>Trying to make department communication work</td>
</tr>
<tr>
<td>Moving towards continuous monitoring</td>
<td>Figuring our that anti virus isn’t working</td>
</tr>
</tbody>
</table>
CIS Benchmarks/Scoring Tools
Now Available, Free of Charge!

### Operating Systems

<table>
<thead>
<tr>
<th>Benchmark</th>
<th>Version</th>
<th>Updated</th>
</tr>
</thead>
<tbody>
<tr>
<td>Windows XP Professional SP1/SP2</td>
<td>2.01</td>
<td>09/09/2005</td>
</tr>
<tr>
<td>Windows Server 2003</td>
<td>1.2</td>
<td>10/25/2005</td>
</tr>
<tr>
<td>Windows 2000 Professional</td>
<td>2.2.1</td>
<td>12/17/2004</td>
</tr>
<tr>
<td>Windows 2000 Server</td>
<td>2.2.1</td>
<td>12/17/2004</td>
</tr>
<tr>
<td>Windows 2000</td>
<td>1.2.2</td>
<td>02/04/2005</td>
</tr>
<tr>
<td>Windows NT</td>
<td>1.05</td>
<td>03/04/2005</td>
</tr>
<tr>
<td>Mac OS X</td>
<td>2.0</td>
<td>10/16/2006</td>
</tr>
<tr>
<td>FreeBSD</td>
<td>1.0.5</td>
<td>10/21/2005</td>
</tr>
<tr>
<td>Solaris 10</td>
<td>2.1.3</td>
<td>06/26/2007</td>
</tr>
<tr>
<td>Solaris 2.5.1 - 9.0</td>
<td>1.3</td>
<td>08/11/2004</td>
</tr>
<tr>
<td>Red Hat Linux</td>
<td>1.0.5</td>
<td>11/02/2006</td>
</tr>
<tr>
<td>SUSE Linux</td>
<td>1.0</td>
<td>03/17/2006</td>
</tr>
<tr>
<td>Slackware Linux</td>
<td>1.1</td>
<td>06/16/2006</td>
</tr>
<tr>
<td>HP-UX</td>
<td>1.3.1</td>
<td>10/21/2005</td>
</tr>
<tr>
<td>AIX</td>
<td>1.01</td>
<td>10/21/2005</td>
</tr>
<tr>
<td>Novell OES:NetWare</td>
<td>1.0</td>
<td>08/14/2006</td>
</tr>
<tr>
<td>Debian Linux</td>
<td>1.0</td>
<td>08/17/2007</td>
</tr>
</tbody>
</table>
20 Critical Security Controls

Twenty Critical Security Controls for Effective Cyber Defense: Consensus Audit Guidelines

Click here to view our 20 Critical Controls interactive feature!

The Twenty Critical Security Controls have already begun to transform security in government agencies and other large enterprises by focusing their spending on the key controls that block known attacks and find the ones that get through. These controls allow those responsible for compliance and those responsible for security to agree, for the first time, on what needs to be done to make systems safer. No development in security is having a more profound and far reaching impact.

These Top 20 Controls were agreed upon by a powerful consortium brought together by John Gilligan (previously CIO of the US Department of Energy and the US Air Force) under the auspices of the Center for Strategic and International Studies. Members of the Consortium include NSA, US Cert, DoD JTF-GNO, the Department of Energy Nuclear Laboratories, Department of State, DoD Cyber Crime Center plus the top commercial forensics experts and pen testers that serve the banking and critical infrastructure communities.

The automation of these Top 20 Controls will radically lower the cost of security while improving its effectiveness. The US State Department, under CISO John Streufert, has already demonstrated more than 80% reduction in “measured” security risk through the rigorous automation and measurement of the Top 20 Controls.

Click here to view the user vetted tools...

Predictions for the future of compliance
Their numbers add up, but they aren’t XCCDF compliant!
Welcome to the new Tenable Store. You will need to create a new account. Previous account data is available by request to purchases@tenable.com

Featured Products

1 Year Nessus ProfessionalFeed Subscription
$1,200.00
buy now

2 Year Nessus ProfessionalFeed Subscription
$2,400.00
buy now

3 Year Nessus ProfessionalFeed Subscription
$3,600.00
buy now

Renewals
You must log into your Tenable Support Portal account to initiate the renewal process.

Purchase Orders
Please contact one of Tenable's Authorized Partners if you need to submit a Purchase Order. Our W9 form is also available online.

Information
Privacy Policy
Terms of Use

Contact Info
7063 Columbia Gateway Drive
Suite 100
Columbia, MD 21046
410-872-0555
sales@tenable.com

DigiCert Seal

Copyright © 2010 Tenable Network Security.
Did you do the penetration test this week?

I sorted it out with a ruby script.
WE WILL BE ADOPTING THE BEST PRACTICES IN OUR INDUSTRY, JUST LIKE EVERYONE ELSE.

IF EVERYONE IS DOING IT, BEST PRACTICES IS THE SAME THING AS MEDIocre.

STOP MAKING MEDIocrITY SOUND BAD!

SORRY.

IN ADDITION TO ISO 9000, WE WILL STRIVE TO BE QS-9000 COMPLIANT.

THAT MEANS FALSIFYING THE FOLLOWING DOCUMENTS: QSR, APQP, FMEA, MSA, SPC, PPAP AND QSA.

REMEMBER, YOU CAN'T SPELL COMPLIANCE WITHOUT "LIANCE."
PART 2 – SECURITY IMPACT

RED SHIRT
Dead Man Walking!
A always
B be
C compliant

A attention
ADA act
IT Controls Performance Study

Spending on IT controls has increased by 16% in the last year. The ITPI has released a new report that shows that IT audit and control related spending increased by 22% in the last year.

With the help of ITPI research analyst Jeff Wachter, the report has been used to analyse the state of IT controls in the United States.

Key findings of the study include:

- Best practices for IT controls
- 21 Foundational Controls for IT controls
- Organizational maturity of IT controls

Organizations have invested in IT controls for the following benefits:

- 12% to 37% less unplanned work
- 12% to 26% higher change success rate
- 2.5 to 5.4 times higher server to system administrator ratio

For the price of sending another IT employee to an ITIL foundations class you get:

- Empirical evidence that can guide ongoing IT audit and control investment decisions
- A list of Foundational Controls that have the highest impact on performance
- Details needed to create a business case for ITIL and COBIT projects
- Administrative tools -> Local Security Policy
  - Go to Software Restriction Policies

- New Rule:
  - Allow execution from:
    - %systemroot%
    - %programfilesdir%
  - Deny execution from:
    - %systemroot%
    - %systemroot%

- Go to Security Level
  - Enable Default

This rule basically prevents programs other than those in C:\Windows and C:\Program Files from being executed at all. This is a bit intrusive but prevents viruses, since Outlook attachments and other viruses get installed under C:\ or in the user's Outlook "temp" directory.
The Security Templates that have "Analyze" as part of their file name, should never be used to configure a production system. They are meant only for use with the security Configuration snap-in to the MMC to Analyze the security configuration of the system.

These templates are guaranteed to break a production system if they are used for configuration. In all probability the system will not be recovered, and all software will have to be reinstalled.
The White House audits 100 more items beyond NIST.
Which target would you rather hit?

Of course if you have a lot of the same targets ...
You have a monoculture!
SIMPLE EXAMPLE – HTTP SERVER

Use IPS/Proxy to stop 0-days
Monitor with NIDS/NBAD
Look for outbound denied
firewalls

No DNS. Web server
jailed.

Watch for denies
SSH client
attacks

Port 80 in.
Nothing
allowed out

System errors
Illegal Commands
Unauthorized
changes
File integrity

Port 22 in.
Nothing
allowed out
<table>
<thead>
<tr>
<th>Boundary</th>
<th>Desired Model</th>
<th>Real World Monitoring</th>
<th>Trigger</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>No vulnerabilities</td>
<td>Daily scanning</td>
<td>Any “high” vuln</td>
</tr>
<tr>
<td>DMZ</td>
<td>No system vulnerabilities</td>
<td>Weekly patch audits</td>
<td>Any security patches older than 15 days</td>
</tr>
<tr>
<td>DMZ</td>
<td>Correct configuration</td>
<td>Weekly config audit</td>
<td>Any configuration issues older than 15 days</td>
</tr>
<tr>
<td>Internet</td>
<td>No successful internet attacks</td>
<td>Use NIDS, web logs and NBAD to monitor sessions</td>
<td>Trend events. Alert on anomalies. Alert on “long” web sessions.</td>
</tr>
<tr>
<td>Internet</td>
<td>No Outbound network connections</td>
<td>Log all firewall logs</td>
<td>Alert on any denied outbound firewall event</td>
</tr>
<tr>
<td>DMZ</td>
<td>No unauthorized system changes</td>
<td>Log all admin and user actions</td>
<td>Alert on any new changes including file integrity</td>
</tr>
<tr>
<td>DMZ</td>
<td>System is error free</td>
<td>Log all system and application errors</td>
<td>Trend and alert on anomalies in error records.</td>
</tr>
<tr>
<td>Corp LAN</td>
<td>No Internal connections</td>
<td>Log all firewall logs</td>
<td>Alert on any denied internal firewall event</td>
</tr>
<tr>
<td>Corp LAN</td>
<td>All clients secure</td>
<td>Weekly patch audits</td>
<td>Any security patches older than 7 days</td>
</tr>
</tbody>
</table>
Your network is a Rube Goldberg machine
You must understand technology limitations.
YOU CAN AUDIT IN MANY WAYS

Scanner
Jockey
I scan my DMZ to list open ports
Packet Monkey
To slow, I sniff in real time.
Change Control Freak
Screw you guys. I track config changes.
HOW WOULD YOU DETECT CHANGE?

I NEED A MINOR CHANGE TO OUR WEBSITE.

GIVE ME YOUR BUSINESS CASE FOR THE CHANGE AND I'LL PRIORITIZE IT FOR THE QUEUE.

I DON'T HAVE TIME TO WRITE A BUSINESS CASE FOR ONE LITTLE CHANGE.

I CAN'T JUSTIFY CHANGING MY PRIORITIES WITHOUT ONE.

GAAAA!!! WHY CAN'T WE DO THE SIMPLEST THINGS IN THIS STUPID COMPANY??!!

TRY ONE OF THESE CORPORATE POST-TRAUMATIC STRESS PILLS TO DULL YOUR MEMORY OF THESE EVENTS.

WHAT? WHERE AM I? WHO ARE YOU? YOU WERE JUST LEAVING.

THEY'RE PLACEBOS, BUT I FIND THAT THEY SOLVE 20% OF MY PROBLEMS.
NOT BEING PATCHED

BOTNET

UNAUTHORIZED


EXPECT TO BE COMPROMISED

Make them work harder to leverage any compromised target

Exploits work, but we’re leveraging that the attacker does not know our defenses

Need to have a process to investigate false positives

Reverse shells, phone homes, etc prevented by ACL in network
MAKE THEM JUMP THROUGH HOOPS

Make them work harder to leverage any compromised target

Most IT organizations are OK with proxies and packet shapers
Are they hooked up to your SIM or NBAD and part of your monitoring?

Proxies prevent some tunneling. Packet shapers can slow access.
MAKE ATTACKERS REQUIRE DIFFERENT EXPLOITS

*Force them to think – and less likely be a botnet*

Are you looking for these exploits to begin with? Does your SIM chain together these types of attacks?
Impact on Security Posture

• Should simplify NIDS, firewall, SIM and other types of monitoring.
Impact on Security Posture

- Should make detecting anomalies much easier
Let’s talk about RISK METRICS in closing.
Does \textit{RISK X ASSET VALUE} really help?
How do you handle inheritance?
Does risk scoring help out in triage?
Thanks for your attention!


I'm looking forward to seeing everyone in NY City on Wednesday for the Tenable Security Showcase - http://bit.ly/9MdVOx
about 6 hours ago via TweetDeck

I'm speaking and attending the first annual ISSA Baltimore Info Security Summit tomorrow - http://bit.ly/dnEE8D
about 6 hours ago via TweetDeck

Tenable's new ecommerce site is online and makes the Nessus renewal process much easier : http://bit.ly/aNZQTS
about 7 hours ago via TweetDeck