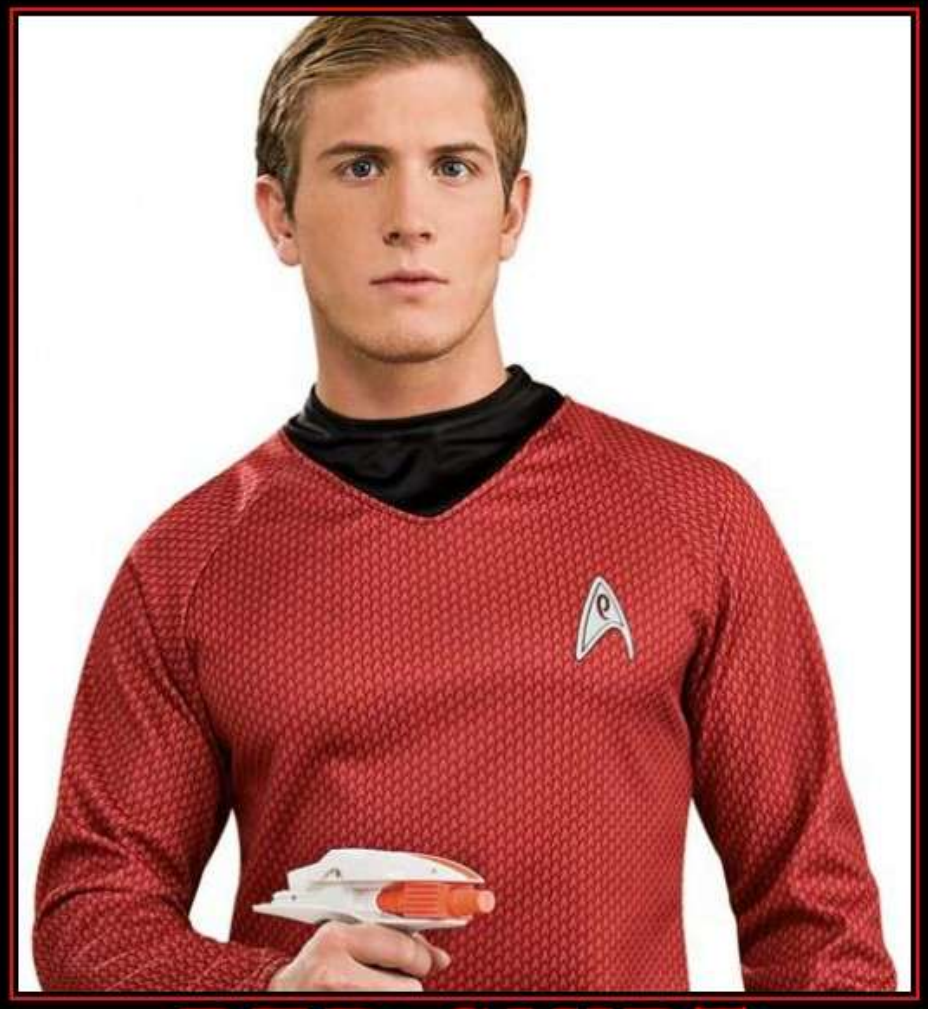
How I Learned to Stop Worrying and Love Compliance

Ron Gula, CEO Tenable Network Security

PART 1 - COMPLIANCE STANDARDS

PART 2 – SECURITY IMPACT



THEMES – BUILD A MODEL

THEMES – MONITOR FOR FAILURE

THEMES – DEMONSTRATE COMPLIANCE

WE ARE IN A GREAT CAREER FIELD

Amount of grey hair

BBN

USi

enterasys Secure Networks

NSW NETWORK SECURITY WIZARDS, INC.

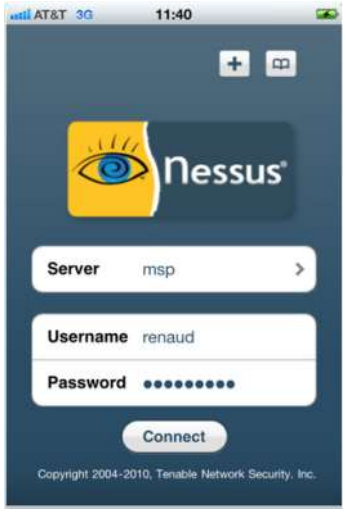
TENABLE Network Security

Nessus

90's 2000 2010

TENABLE

Network Security®



TENABLE
Network Security®

**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

Demonstrating compliance is just as difficult as understanding why

Figuring out ways to enforce desired state isn't that easy either!

Precision landing FAIL

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 $&$&$!!

Mission and Overview

NVD is the U.S. government repository of standards based vulnerability management data. This data enables automation of vulnerability management, security measurement, and compliance (e.g. FISMA).

Resource Status

NVD contains:

26244 CVE Vulnerabilities
114 Checklists
91 US-CERT Alerts
1987 US-CERT Vuln Notes
2966 OVAL Queries
11941 Vulnerable Products

Last updated: 08/24/07
CVE Publication rate:
17 vulnerabilities / day

Email List

Select the email list(s)

National Checklist Program

Formerly the (NIST Security Configuration Checklist Program)

Federal Desktop Core Configuration settings (FDCC)

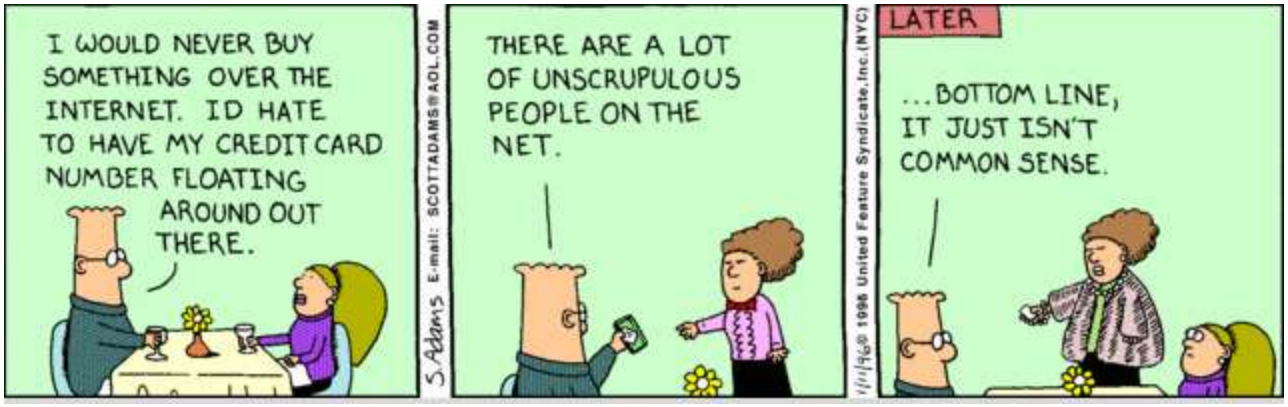
NVD contains content (and pointers to tools) for performing configuration checking of systems implementing the FDCC using the Security Content Automation Protocol (SCAP).
FDCC Checklists are available here (to be used with SCAP FDCC capable tools).
SCAP FDCC Capable Tools are available here.

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

Government	Commercial
Single standard with enforcement	Many standards and no enforcement
Trying to make agency communication work	Trying to make department communication work
Moving towards continuous monitoring	Figuring our that anti virus isn’t working

CIS Benchmarks/Scoring Tools Now Available, Free of Charge!

Operating Systems

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

ANNOUNCEMENTS

August 7, 2007 - CIS awards Security Software Certification to Tenable Network Security's Nessus v3.0 and Security Center v3.2.
Click Here for more information.

August 6, 2007 - ISSA toolsmith releases article on the CIS Benchmarks.
Click Here for information.

August 2, 2007 - CIS awards Security Software Certification to Tripwire's Tripwire Enterprise v7.
Click Here for more information.

August 2, 2007 - CIS awards Security Software Certification to nCircle's CCM v5.0.

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...

Download the What Works in Implementing the 20 Critical Security Controls & SANS Cyber Attack Threat Map.


Predictions for the future of compliance
MOTOROLA
The World in Your Mouth
Features include:
• Subvocalization system for silent chatting
• Hear via bone conduction
• Voice dialing
• Data sync via Bluetooth®
• Decay-proof
Motorola MOLR-V6 Tooth Phone
Free implantation at participating dental providers.
Two-year T-Mobile® service activation required.
Not valid in Alaska, Hawaii, or any US Samar colony.
Offer expires 12/31/2019.


Their numbers add up, but they aren't XCCDF compliant!

TENABLE Network Security®

Tenable Store

Register | Log In

Enter search keywords

Home

Categories

ProfessionalFeed
Training

Renewals

You must log into your Tenable Support Portal account to initate 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

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

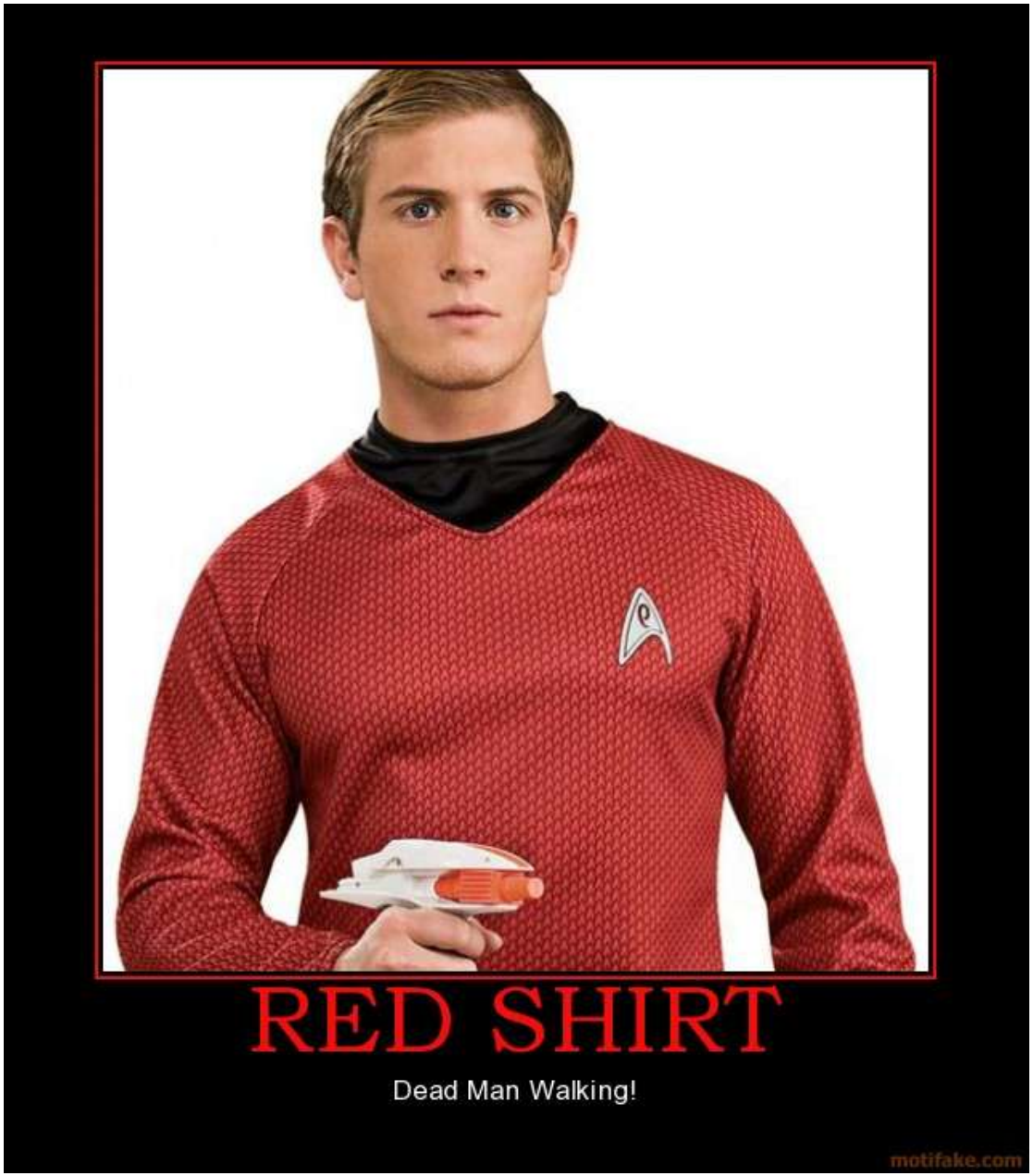
buy now


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.
BEST PRACTICES
www.dilbert.com scottadams@aol.com
IF EVERYONE IS DOING IT, BEST PRACTICES IS THE SAME THING AS MEDIOCRE.
1-3-08 ©2008 Scott Adams, Inc./Dist. by UFS, Inc.
STOP MAKING MEDIOCRITY SOUND BAD!
SORRY.


IN ADDITION TO ISO 9000, WE WILL STRIVE TO BE QS-9000 COMPLIANT.
www.dilbert.com scottadams@aol.com
THAT MEANS FALSIFYING THE FOLLOWING DOCUMENTS: QSR, APQP, FMEA, MSA, SPC, PPAP AND QSA.
11-4-99 © 1999 United Feature Syndicate, Inc.
REMEMBER, YOU CAN'T SPELL COMPLIANCE WITHOUT "LIANCE."

PART 2 – SECURITY IMPACT




A always
B be
C compliant
A allentio
intere
act


yoism.org

Information Technology Process Institute

Research - Benchmarking - Prescriptive Guidance

IT Controls Performance Stud

Buy Now $1,695

Spending on I… o see a strong business case for spending o…

The ITPI has re… hat shows that IT audit and control related … mance!

With the help o… University of Oregon -- we analysed the s… performance measures.

Key findings of…

- Best pr…
- 21 Fou…
- Organiz…

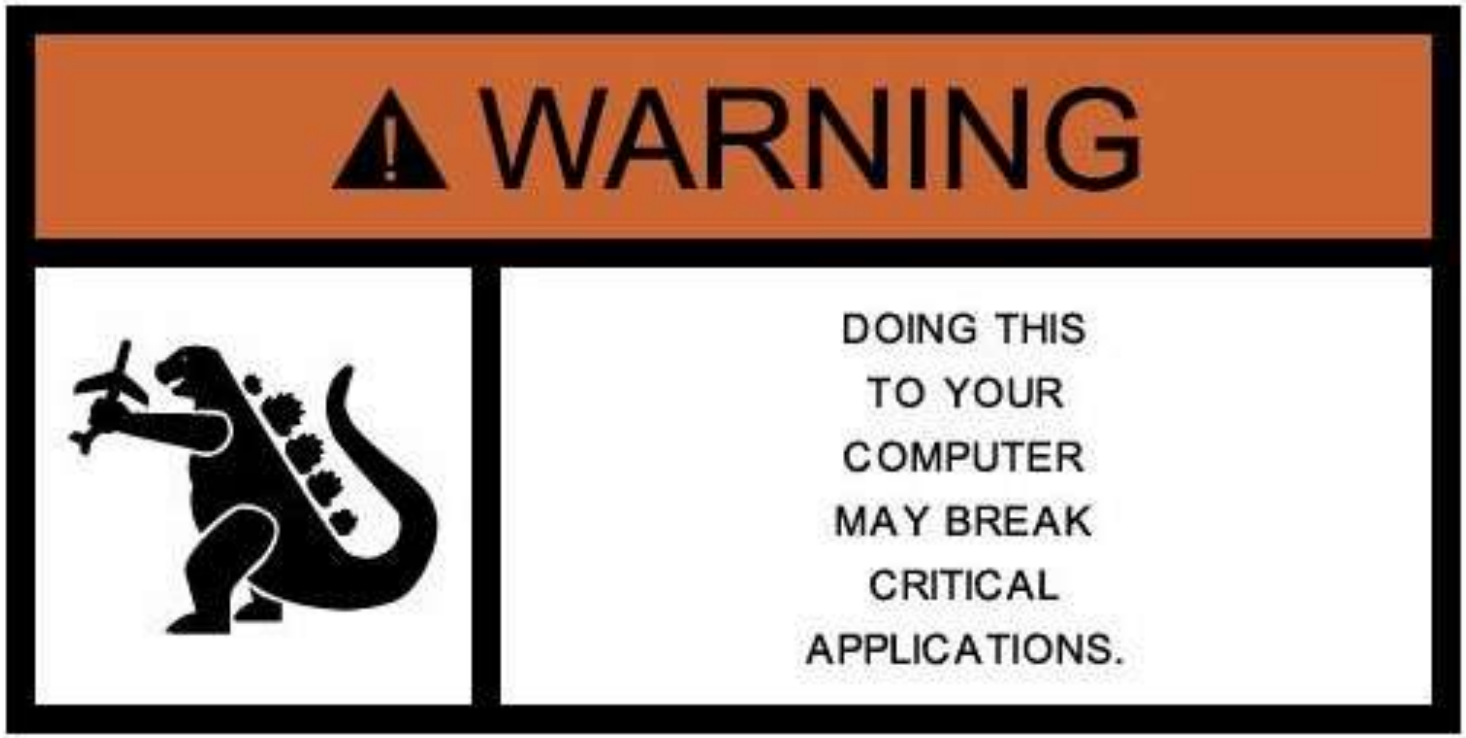
Organizations …

- 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

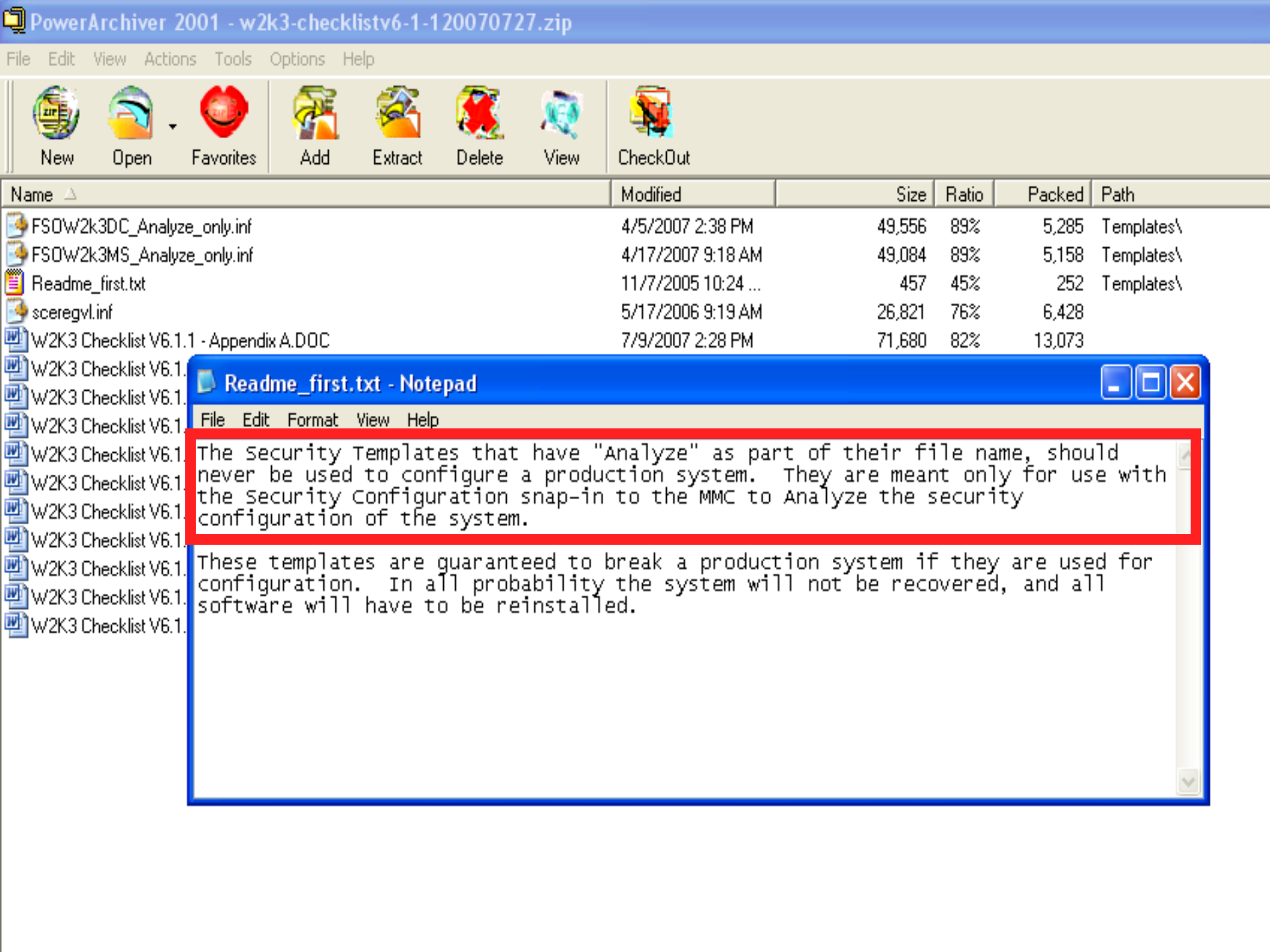
For the price of sending another IT employee to an ITIL foundations class you get:

- 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**



- **T** **n**
  C **at**
  a
  C **er**
  C: **or in the user's Outlook "temp" directory.**


PowerArchiver 2001 - w2k3-checklistv6-1-120070727.zip
File Edit View Actions Tools Options Help
New Open Favorites Add Extract Delete View CheckOut
Name Modified Size Ratio Packed Path
FSOW2k3DC_Analyze_only.inf 4/5/2007 2:38 PM 49,556 89% 5,285 Templates\
FSOW2k3MS_Analyze_only.inf 4/17/2007 9:18 AM 49,084 89% 5,158 Templates\
Readme_first.txt 11/7/2005 10:24 ... 457 45% 252 Templates\
sceregvl.inf 5/17/2006 9:19 AM 26,821 76% 6,428
W2K3 Checklist V6.1.1 - Appendix A.DOC 7/9/2007 2:28 PM 71,680 82% 13,073
Readme_first.txt - Notepad
File Edit Format View Help
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.
LIVE
ALERT
FOX NEWS channel
WHITE HOUSE CONFERENCE ON FDCC CYBER COMPLIANCE
LIVE DESK
LENCE AND INTIMIDATION CAMPAIGNS
NAS 4.50

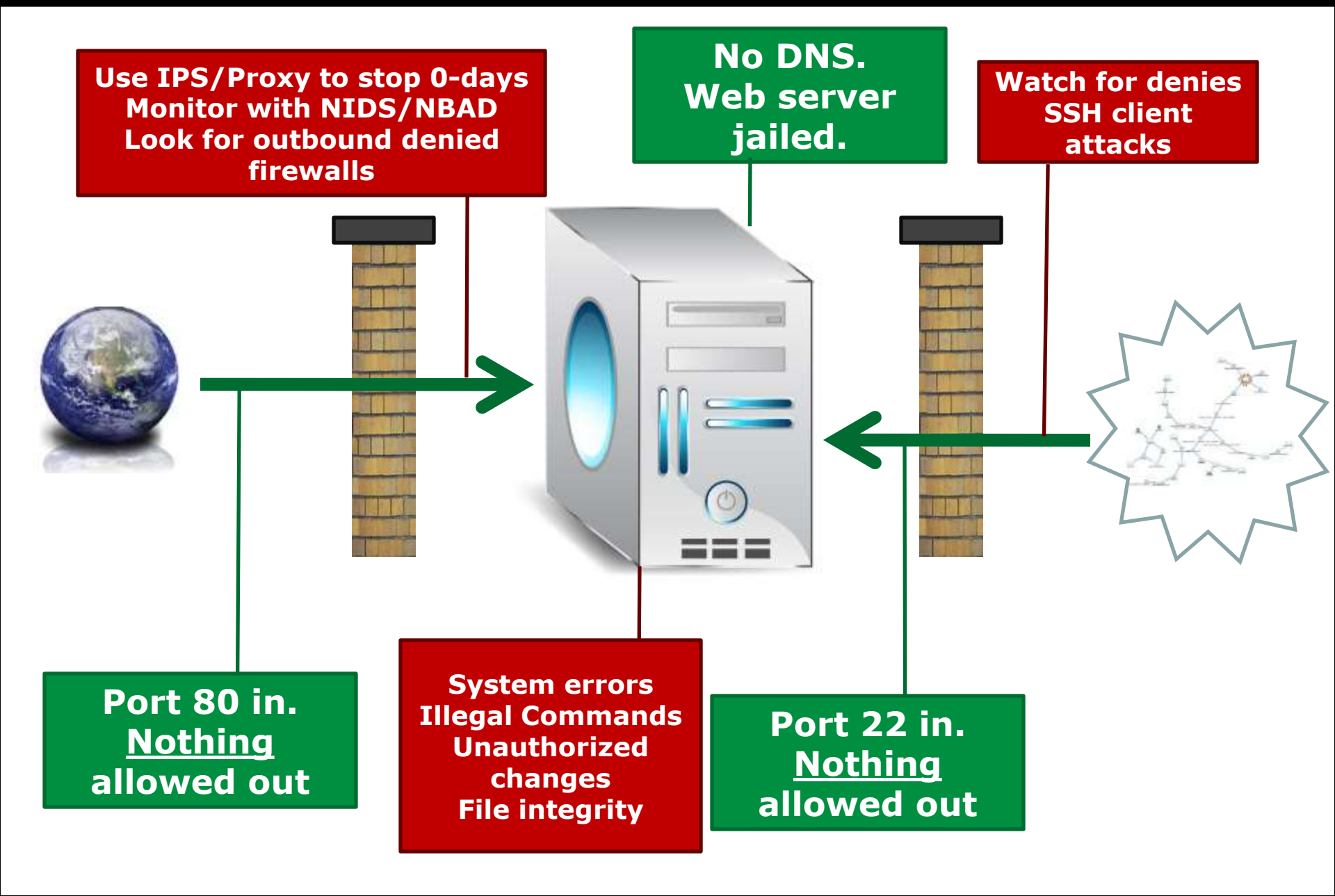

AUTOMATION

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



SIMPLE EXAMPLE – HTTP SERVER

Boundary	Desired Model	Real World Monitoring	Trigger
Internet	No vulnerabilities	Daily scanning	Any “high” vuln
DMZ	No system vulnerabilities	Weekly patch audits	Any security patches older than 15 days
DMZ	Correct configuration	Weekly config audit	Any configuration issues older than 15 days
Internet	No successful internet attacks	Use NIDS, web logs and NBAD to monitor sessions	Trend events. Alert on anomalies. Alert on “long” web sessions.
Internet	No Outbound network connections	Log all firewall logs	Alert on any denied outbound firewall event
DMZ	No unauthorized system changes	Log all admin and user actions	Alert on any new changes including file integrity
DMZ	System is error free	Log all system and application errors	Trend and alert on anomalies in error records.
Corp LAN	No Internal connections	Log all firewall logs	Alert on any denied internal firewall event
Corp LAN	All clients secure	Weekly patch audits	Any security patches older than 7 days


Your network is a Rube Goldberg machine

Tenable Network Security: How did you test for MS08-067? - Mozilla Firefox

File Edit View History Bookmarks Tools Help

http://blog.tenablesecurity.com/2008/12/how-did-you-test-for-ms08-067.html

Most Visited Google Cerberus CVS Mantis N.org Alfred SC3Away SC3Home GW UFL Eval TSC

Tenable Network Security | National Vulnerability Databas... | sager blackhat - Google Search | Tenable Network Securit...

TENABLE Network Security®

« Tenable Job Opportunities | Main | Marcus Ranum PaulDotCom Interview on Penetration Testing »

How did you test for MS08-067?

Microsoft recently released a critical security bulletin, MS08-067 that described a privately reported vulnerability in the Server service and provided a patch for this vulnerability. What was unusual was that this bulletin was released independently of Microsoft's usual patch notification process and caused quite a bit of concern for many organizations. Tenable used this opportunity to help a number of organizations monitor their networks to determine if this issue had been mitigated. I had the opportunity to speak with many different customers and was surprised at the different priorities, techniques and level of response that varied from organization to organization. In this blog, I will share some of the situations and trends I ran into while working with Tenable Nessus and Security Center customers.

Tenable's research team released two checks for MS08-0
plugin #34477, works without any credentials. It verifie
connecting to Windows systems on port 445 or port 139
for it. This plugin has the advantage of being fast and
credentials. The other check (plugin #34476) performs
audit for the same vulnerability. This plugin performs fil

TENABLE NETWORK SECURITY

Nessus

The official BLOG of Tenable Network Security and the Nessus vulnerability scanner.

You must understand technology limitations

Done

Now: Snow, 33° F | Tue: 34° F | Wed: 29° F

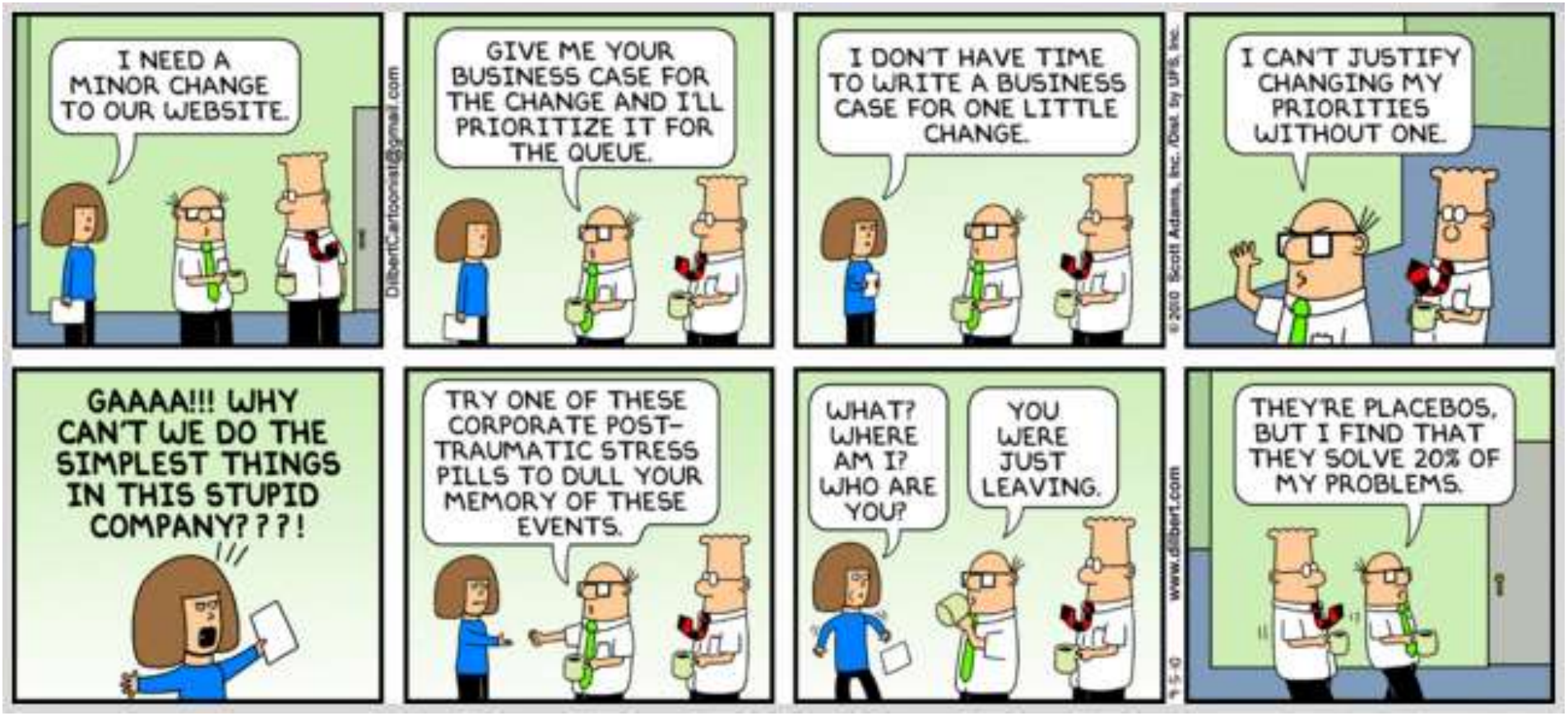
YOU CAN AUDIT IN MANY WAYS

Jockey

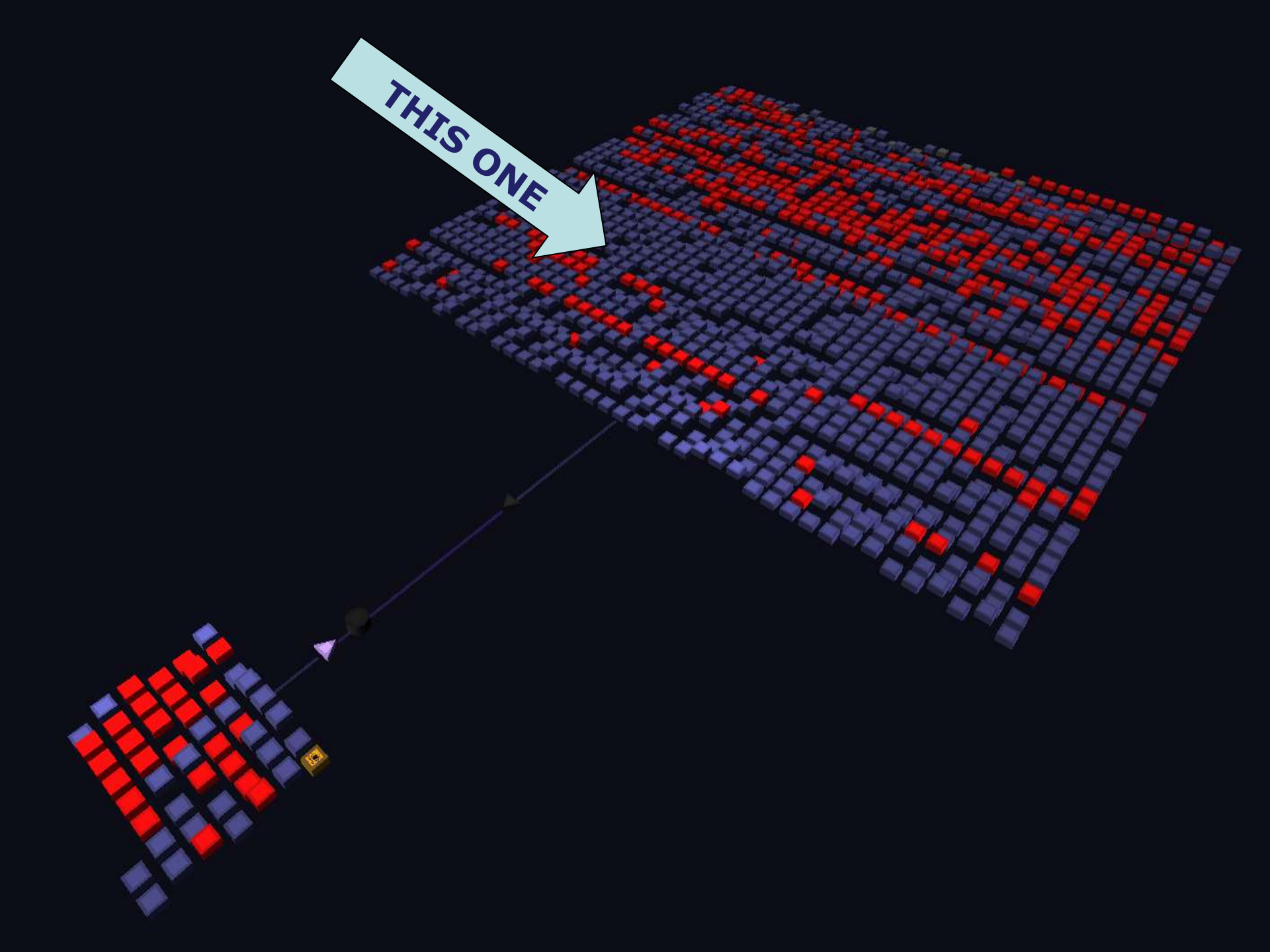
Monkey

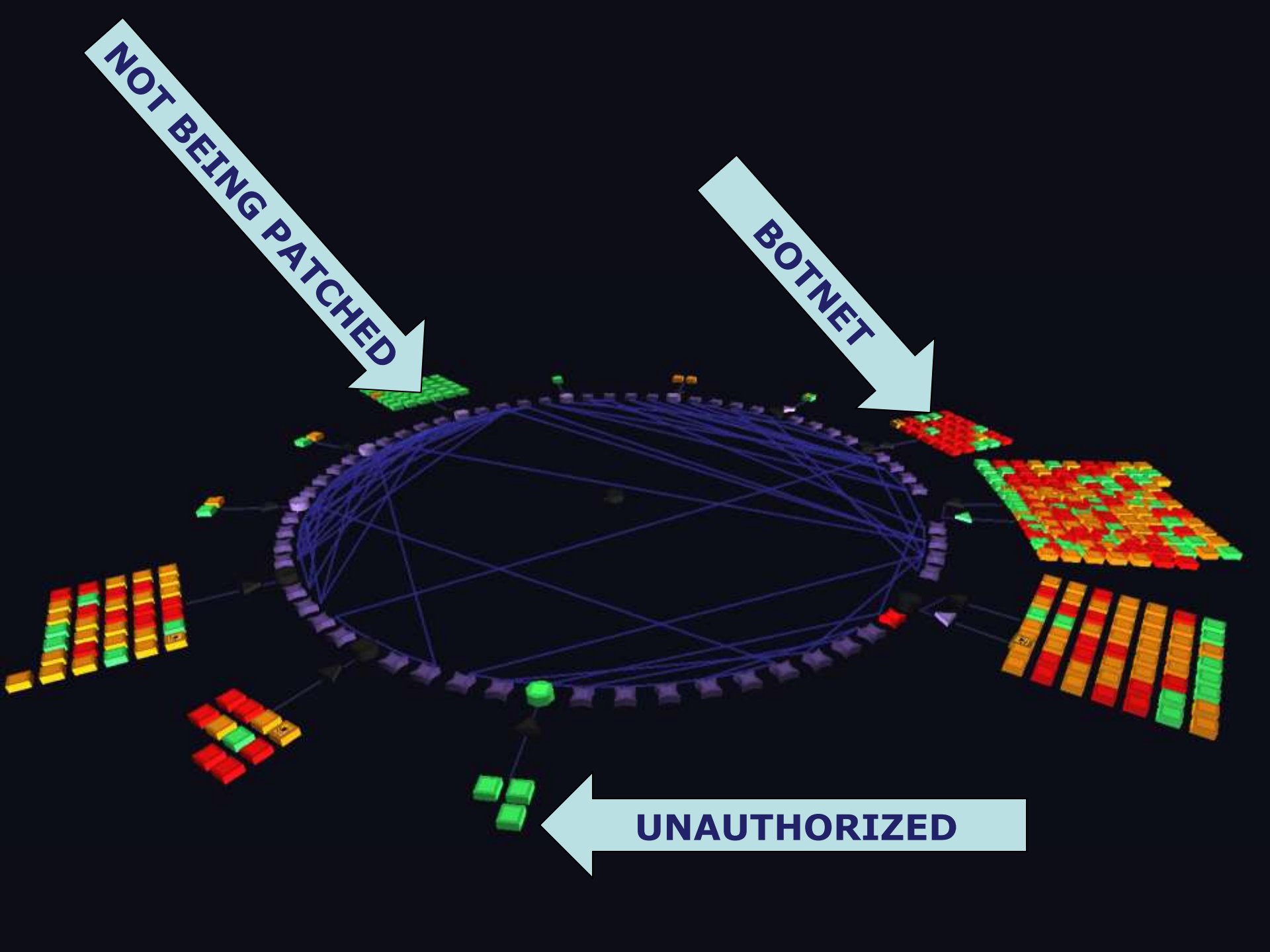
Freak

HOW WOULD YOU DETECT CHANGE?




NETFLOW ANOMALY
VIRUS OUTBREAK
INTRUSION
LOGIN FAILURES
LOGIN FAILURES
FILE CHECKSUM
NETFLOW ANOMALY
INTRUSION
FIREWALL DENY


THIS ONE


NOT BEING PATCHED
BOTNET
UNAUTHORIZED

snort[1578]: [1:2002910:4] ET SCAN Potential VNC Scan 5800-5820 [Classification: Attempted Information Leak] [Priority: 2]: {TCP} 192.168.20.24:36493 -> 192.168.20.16:5800

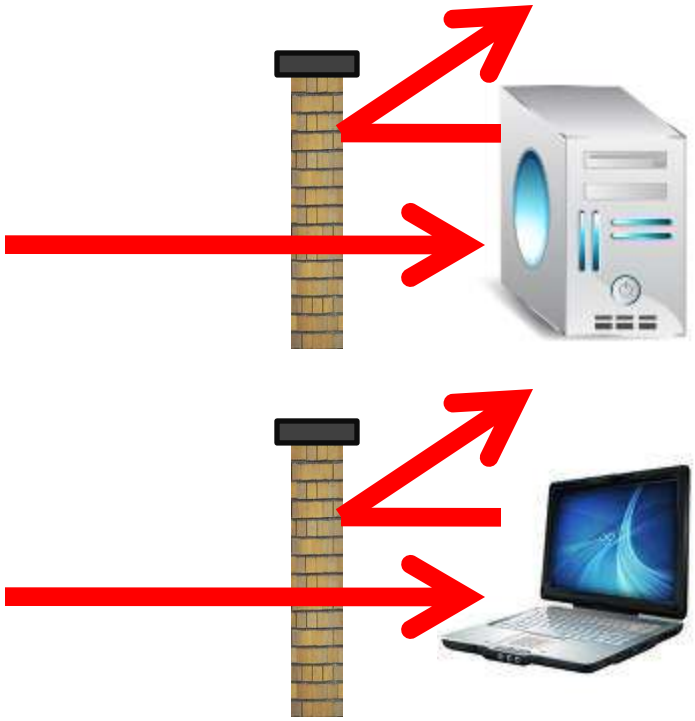
snort[1578]: [1:2001743:8] ET TROJAN HackerDefender Root Kit Remote Connection Attempt Detected [Classification: A Network Trojan was detected] [Priority: 1]: {TCP} 192.168.20.24:45379 -> 192.168.20.16:1025

snort[1578]: [1:1551:6] WEB-MISC /CVS/Entries access [Classification: access to a potentially vulnerable web application] [Priority: 2]: {TCP} 192.168.20.24:45896 -> 192.168.20.21:80

snort[1578]: [1:469:4] AUTHORIZED PENETRATION TEST [Classification: OK To Ignore, But Tell Your Boss] [Priority: 2]: {TCP} 192.168.20.24 -> 192.168.20.92

EXPECT TO BE COMPROMISED

Make them work harder to leverage any compromised target

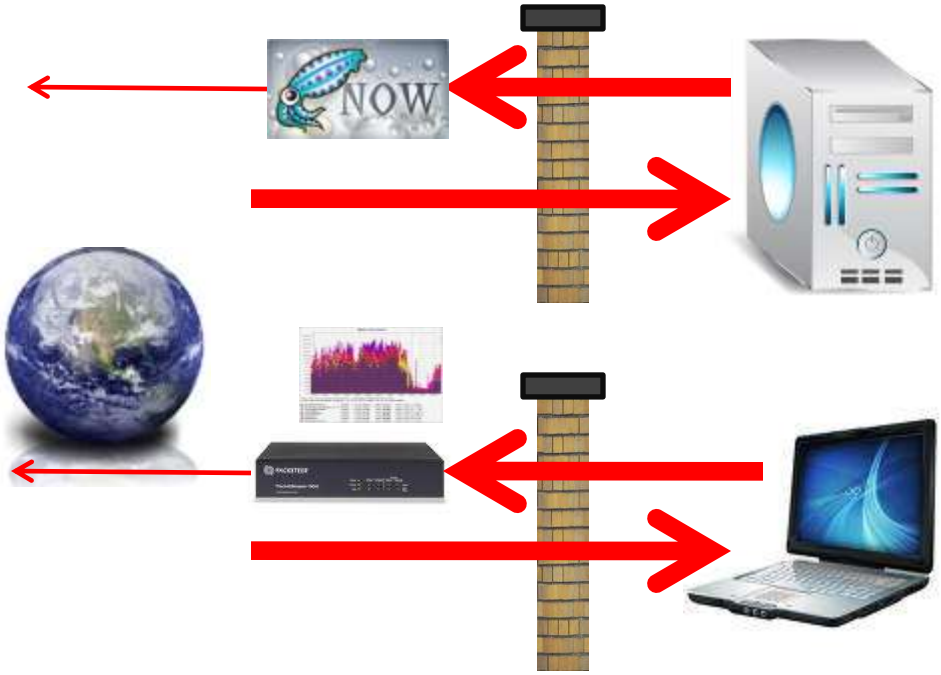


Reverse shells, phone homes,..etc prevented by ACL in network

Exploits work, but we're leveraging that the attacker does not know our defenses
Need to have a process to investigate false positives

MAKE THEM JUMP THROUGH HOOPS

Make them work harder to leverage any compromised target

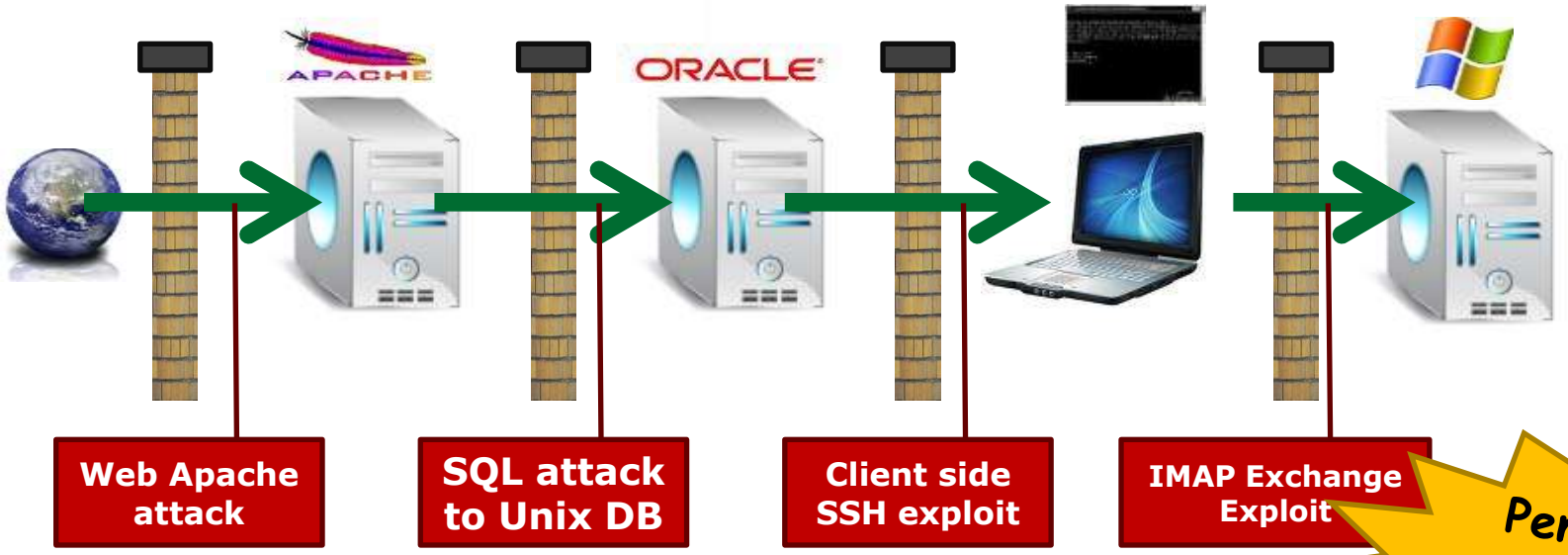


Proxies prevent some tunneling. Packet shapers can slow access.

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

MAKE ATTACKERS REQUIRE DIFFERENT EXPLOITS

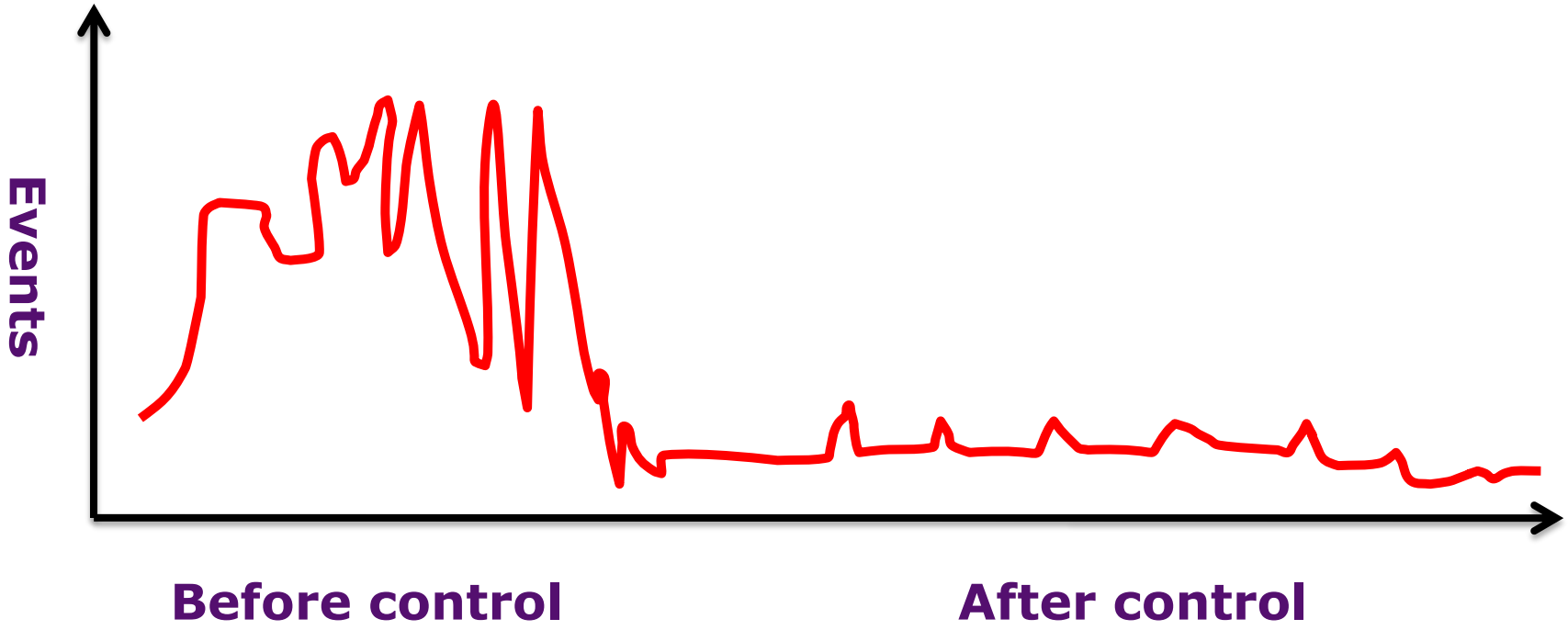
Force them to think – and less likely be a botnet



Pen testers pride themselves on doing this.

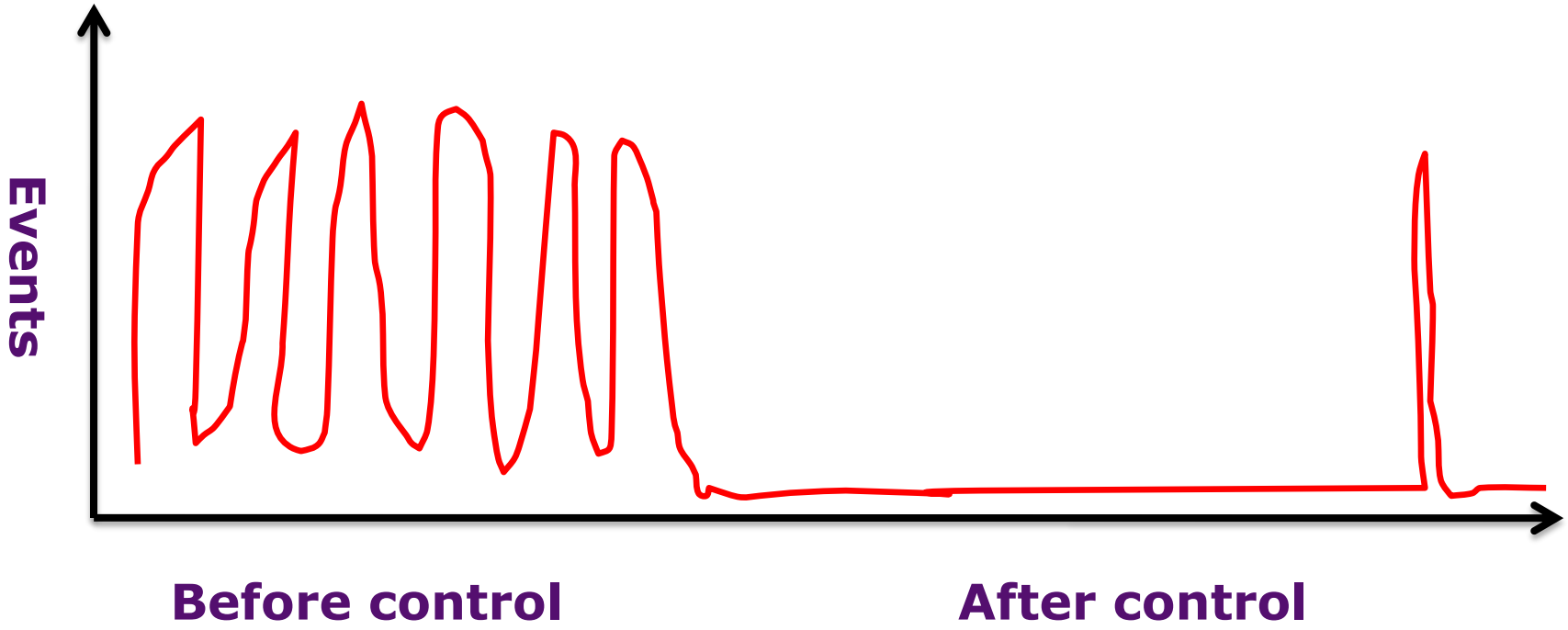
Are you looking for these exploits to begin with?
Does your SIM chain together these types of attacks?

Impact on Security Posture



- **Should <u>simplify</u> 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
SOUTHWEST


Does
RISK X ASSET VALUE
really help?


How do
you handle
inheritance?


Does risk scoring
help out in *triage*?

twitter

Have an account? Sign in

Get short, timely messages from Ron Gula.

Twitter is a rich source of instantly updated information. It's easy to stay updated on an incredibly wide variety of topics. **Join today** and **follow @RonGula**.

Sign Up ›

Get updates via SMS by texting **follow RonGula** to **40404** in the United States
Codes for other countries

RonGula

Thanks for your attention!

More Nessus plugins for WebAppScans: 49704 lists external URLs: http://bit.ly/9Ri0E3 49705 lists email addrs: http://bit.ly/cokkHY

3 minutes ago via TweetDeck

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

Name Ron Gula
Web http://www.nessus...
Bio CEO of Tenable Network Security. Knows things about compliance, security, vulns and intrusion techniques.

927 following | 1,198 followers | 106 listed

Tweets 494

Favorites

Following

rgula@tenable.com
YouTube Videos
Discussions Forum
Security Webinars