Defense Wins Championships

April 16, 2014
For Educational Purposes Only

SecMN

MINNESOTA SECURITY PROFESSIONALS

For Educational Purposes Only

*


EXIT

Defense Wins Championships

The threat landscape is constantly changing and being able to detect malicious and/or unusual activity across the organization can help stop attacks before they come headline generating breaches

Selling to Leadership

- How do we get the green light to move on this topic from leadership?
- Questions to anticipate:
  - What value does this bring?
  - Will this cause resentment?
  - Will this disrupt business?

Building a Program

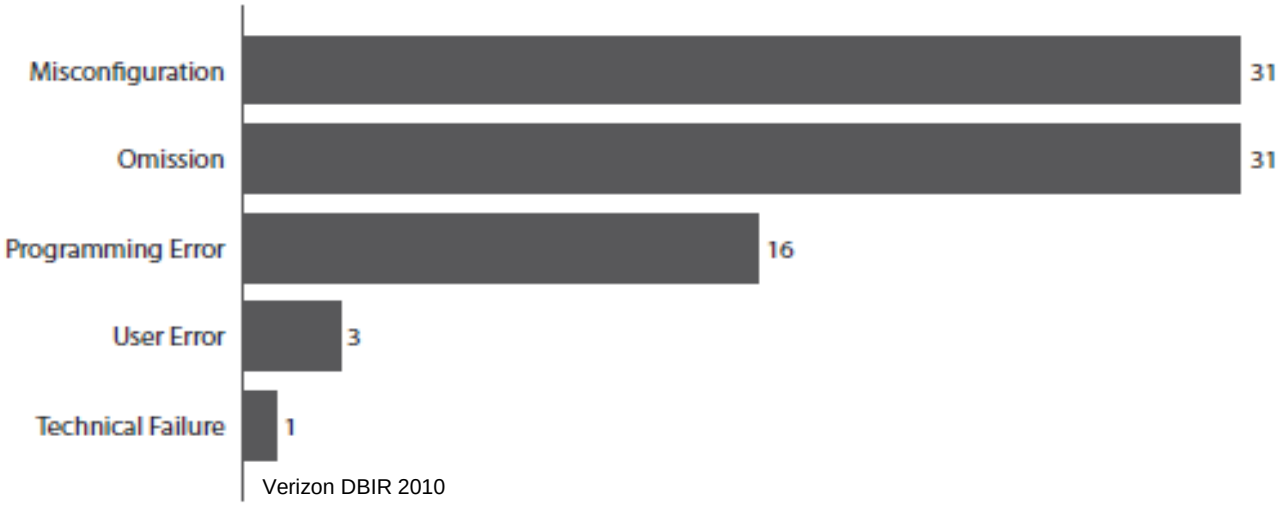
- Topics covered that should be included in an information security program
  - Vulnerability Management
  - Logging/Monitoring
  - Configuration Management

System Hardening

System Hardening

- System Hardening: Configuring systems to eliminate security vulnerabilities
- Most systems don't come secure by default
- Hardening systems is easy but often overlooked
- Checks the box for SANS Top 20 item 3
  - Secure configurations for hardware and software

Figure 21. Types of error by number of breaches



Verizon DBIR 2010

*

Common Hardening Practices

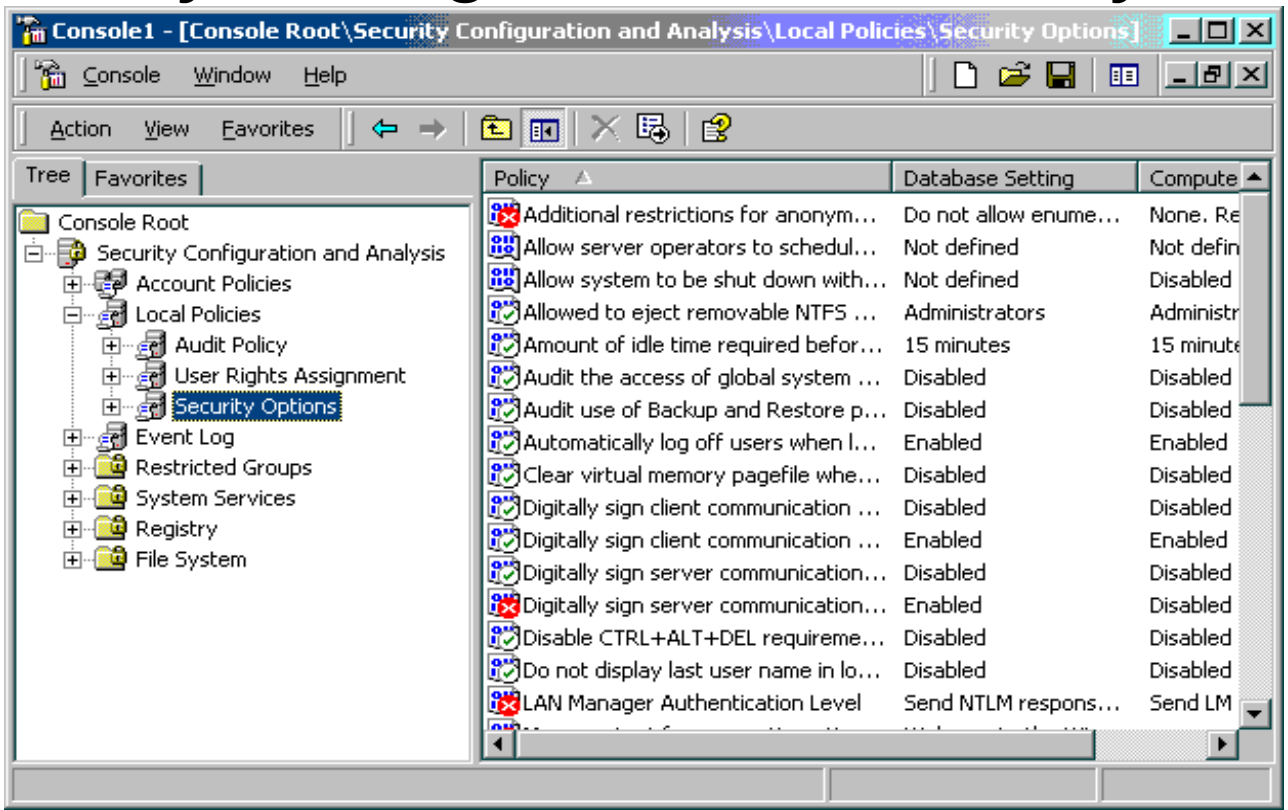
- Change default passwords
- Disable unused accounts
- Disable unused services
- Apply available patches/updates
- Remove unnecessary applications
- Enable logging

Hardening Standards

- Center for Internet Security
  http://benchmarks.cisecurity.org/downloads/browse/?category=benchmarks
  - Operating Systems (Windows, Linux, Solaris, Mac OSX)
  - Databases (MS SQL, MySQL, Oracle)
  - Networking Equipment (Cisco, Juniper, CheckPoint)
  - Web Servers (IIS and Apache)
- NSA
  - Applications
  - Operating Systems
  - Mobile

Hardening Tools - Windows

- Active Directory Group Policy
  - Once and Done (right?)
- Security Configuration and Analysis Tool

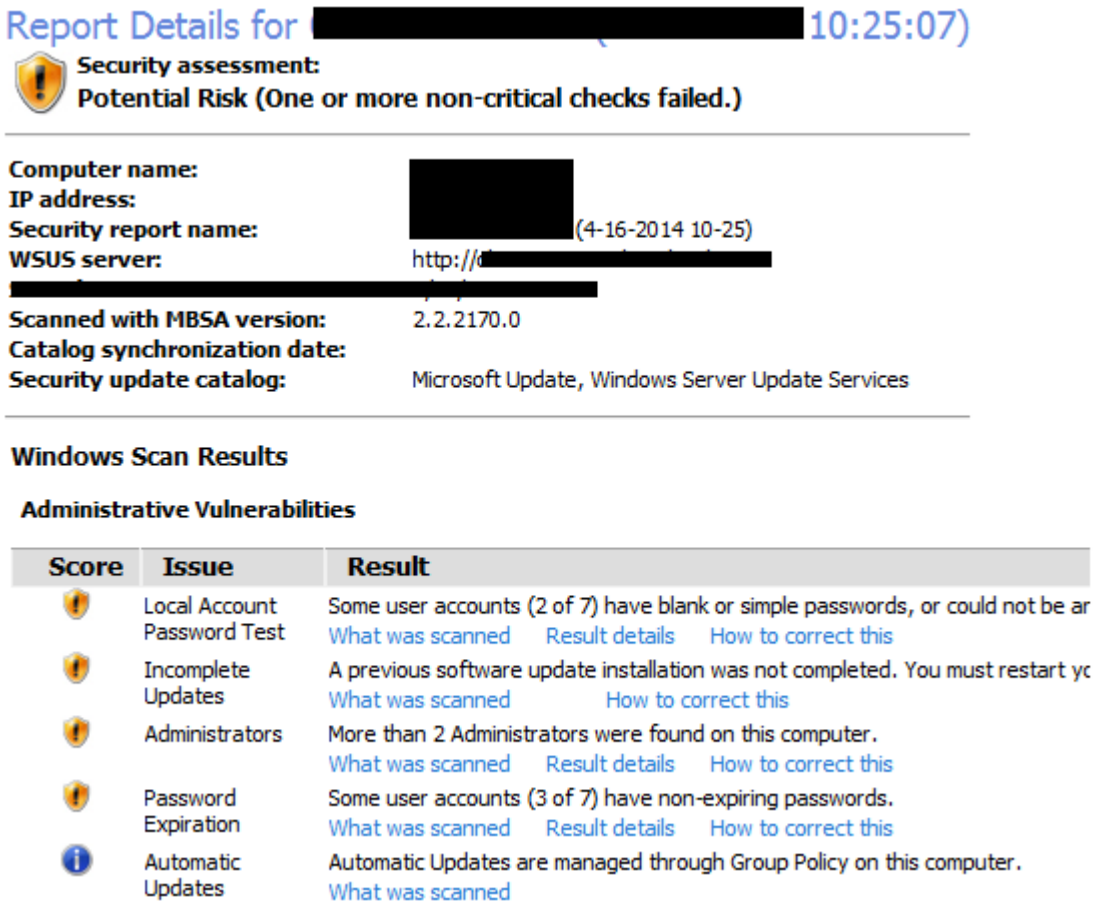


Hardening Tools – Linux/Windows

- Chef (opscode.com)
  - Cookbooks and Recipes to deliver repeatable system configurations
- Puppet (puppetlabs.com)
  - Manifests to deliver repeatable system configurations
- Your favorite scripting language (BASH, PowerShell, etc…)

Hardening/Configuration Analysis

- Microsoft Baseline Security Analyzer
  - http://technet.microsoft.com/en-us/security/cc184924



Report Details for [redacted] 10:25:07)

Security assessment:
Potential Risk (One or more non-critical checks failed.)

Computer name:	[redacted]
IP address:	
Security report name:	(4-16-2014 10-25)
WSUS server:	http://[redacted]
	[redacted]
Scanned with MBSA version:	2.2.2170.0
Catalog synchronization date:	
Security update catalog:	Microsoft Update, Windows Server Update Services

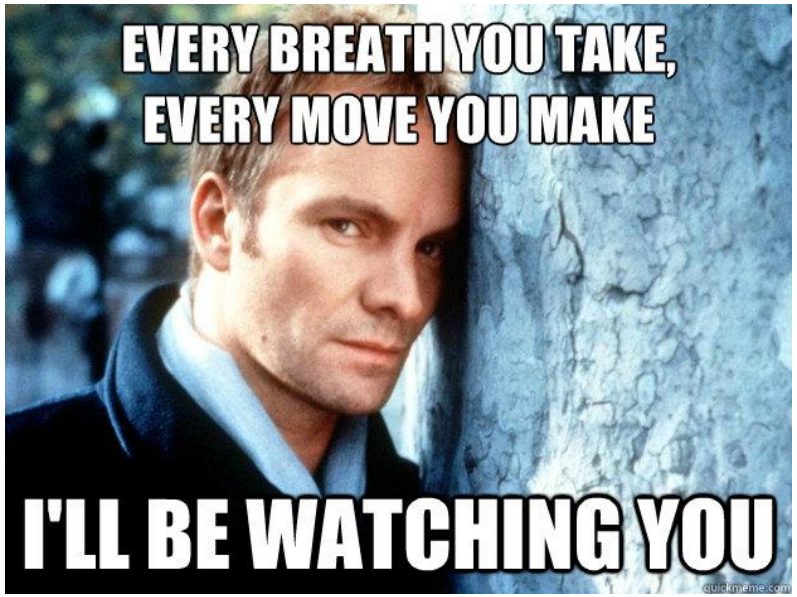
Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Local Account Password Test	Some user accounts (2 of 7) have blank or simple passwords, or could not be ar What was scanned Result details How to correct this
	Incomplete Updates	A previous software update installation was not completed. You must restart yc What was scanned How to correct this
	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
	Password Expiration	Some user accounts (3 of 7) have non-expiring passwords. What was scanned Result details How to correct this
	Automatic Updates	Automatic Updates are managed through Group Policy on this computer. What was scanned

*

Network Monitoring



Network Monitoring

- Security Onion Linux Distro 

  - For
    - Intrusion Detection
    - Network Security Monitoring
    - Log Management
  - Using

Snorby

Snort	Suricata	Bro
OSSEC	Sguil	Squert
Snorby	ELSA	Xplico
NetworkMiner	MORE!	

Security Onion

- Collects alert/log data from all the tools used to monitor your network
  - NIDS (Snort, Suricata)
  - HIDS (OSSEC)
  - Asset data (Bro)
  - Session data (Argus, Bro)
  - Transaction data (Bro)
  - Full packet captures (netsniff-ng)

Security Onion - Snorby

- Provides a graphical display of the events from the IDS platforms
- Can initiate packet capture from within the Snorby based on an event

Security Onion - Bro

- Not a typical IDS
- Can accept feeds from different sources to enhance alerting
  - Threat Intelligence
  - Malware Sites/IPs
  - Emerging Threats Signatures

Current State of Antivirus

Current State of AV – Still Relevant?

- Metasploit makes repackaging payloads to avoid AV easy
  - msfencode
- Antivirus is another layer in the Defense-in-Depth strategy
  - Stops known bad stuff (mostly)
  - If AV relies solely on signatures it might be time to look for a new product

Current State of AV – Still Relevant?

- Application Whitelisting
  - Flipping traditional AV on it's head
  - Instead of looking for bad things, only allow known good things
  - Requires more administration and people overhead than traditional AV
  - Doesn't meet the AV requirement in many regulations

IT Operations for Security

Configuration Management

- Configuration Management Database
  - Enables easy identification of hardware/software in the environment
  - Helps with patch management
  - Checks the box for SANS Top 20 top 2 items
    - Inventory of Authorized/Unauthorized devices
    - Inventory of Authorized/Unauthorized software

Change Management

- Document changes to the environment
- Document approvals for changes
- Easily identify problems related to changes
- Provides a chance to identify risks associated with change
  - Other changes happening at the same time
  - Compatibility
  - Security impacts

IT Operations Tools

- Many open source tools available
  - iTop (http://sourceforge.net/projects/itop/)
    - CMDB
    - Ticketing
    - ITIL Workflows
    - Change Management
    - Performance Monitoring
  - i-doit (http://www.i-doit.org/)
    - CMDB
    - Workflows
    - Change Management

Communicating Risks to Leadership

- How do we define the risks associated of not having an adequate defense infrastructure?
  - Data loss
    - Intellectual Property
    - Payment Card Information
    - Personally Identifiable Information
  - Reputational impact

What We've Learned

- There are many tools available for hardening IT systems
  - Most are configuration management tools
- Antivirus isn't dead
  - It's evolving
  - Shouldn't be the only endpoint control
- We can't protect what we don't know about
  - Devices
  - Software
  - Cloud

Questions?