Using Nagios as a Security Tool

JARED BIRD
JAREDBIRD@GMAIL.COM
TWITTER: @JAREDBIRD

Nagios World Conference North America

Introduction

- Who is Jared Bird?

Nagios World Conference North America

Reasons to care

- Prevent data theft
- Deter identity theft
- Avoid legal issues
- Protect brand

Nagios World Conference North America

Similarities

Nagios World Conference North America

Headlines

MySQL.com Sold for $3k, Serves Malware

189 tweets TOP ★1K retweet

A security firm revealed today that **mysql.com**, the
used Web database software, was hacked and booby-t
malicious software. The disclosure caught my eye beca
evidence that administrative access to mysql.com w
underground for just $3,000.

Web security firm Armorize stated in its blog that mysql.com w

Epsilon Hacked, Major Bank, Retailer Customers' Email Addresses Stolen

Millions of Names and Email Addresses Gained From Major Email Marketing Firm

WordPress Servers Hacked At Root Level

Source code exposed, putting passwords for WordPress.com-hosted blogs at risk of being cracked.

By **Mathew J. Schwartz** InformationWeek
April 14, 2011 11:13 AM

On Wednesday, Automattic, which produces the WordPress blogging

RSA SecurID authentication tokens hacked

Published: June 7, 2011 at 1:57 PM

BEDFORD, Mass., June 7 (UPI) -- Computer hackers recently broke into RSA's SecurID two-factor

r Rivest, Shamir and Adleman, has acknowledged that the intrusion in
e system's security, CNET Web site reported Tuesday.

t hacking attacks against the networks of major U.S. military contractors
Communications and Northrop Grumman.

Sony Hacked Again, 1 Million Passwords Exposed

**Hacker group LulzSec releases 150,000 Sony Pictures r
passwords, in latest setback for consumer electronics g**

NASA Computer Hacked, Satellite Data Accessed

May 17, 2011 | 6:40 PM ET | By Matt Liebowitz, SecurityNewsDaily Staff Writer

Nagios World Conference North America

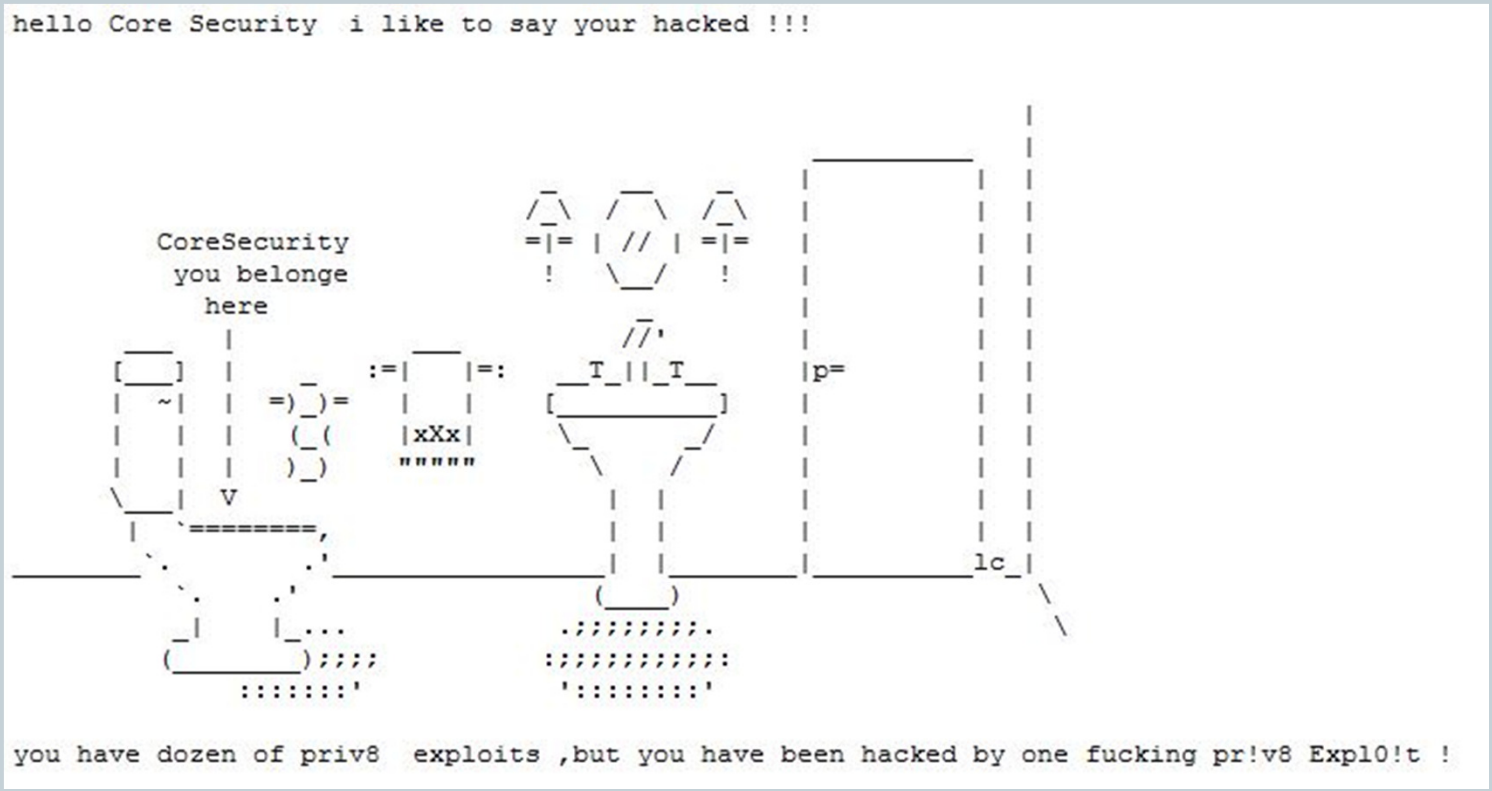
"It wont happen to us"

- It can happen to anyone (even security vendors)

Nagios World Conference North America

Uh Oh

- http://www.coresecurity.com – September 22, 2011



Nagios World Conference North America

What to protect

- Data
- Hardware
- Intellectual Property
- Brand

Nagios World Conference North America

Threats

- Default configurations
- Website defacement
- Missing patches
- DNS redirection
- Unused services
- Unauthorized use
- Many, many more

Nagios World Conference North America

Monitoring

- Automation
- Early detection
- Quick resolution
- Integrity

Nagios World Conference North America

Default Configurations

- Default passwords
- blank sa account
  - Once password is set, monitor with new credentials
- XI Auto-discovery check for insecure protocols
- Scheduled scans and output to Nagios

Nagios World Conference North America

Web

- Monitor for defacement
  - check_http –H www.yoursite.com –s “sekret”
    - Checks for “sekret” string
- Check certificate
  - check_http –H www.mysite.com –C 21
    - Checks certificate for 21 days of validity
- DDOS alerts

Nagios World Conference North America

Software Installed

- Check url for content (version)
- Ex: http://www.adobe.com/software/flash/about/
  - Check for string “10.3.183.10”
- Manually update string
- Better way?

Nagios World Conference North America

DNS

- Have DNS entries changed?
- DNS hijacked
- High Impact

Nagios World Conference North America

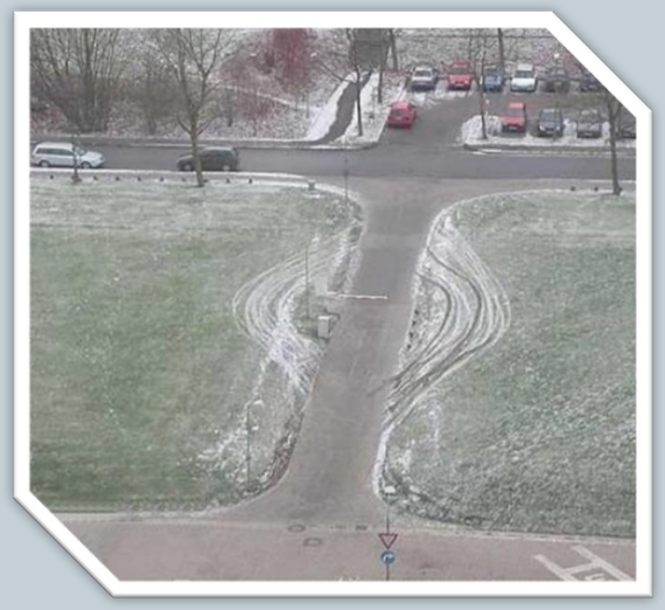
Unused Services

- Auto-discovery
- Check for insecure services
- Check for previously disabled services

Nagios World Conference North America

Unauthorized Use

- LDAP check for account creation
- Syslog output from infrastructure
- Snort alert (snmp)



Nagios World Conference North America

Other Uses?

- Monitor video cameras
  - http://bit.ly/bY2tjd
- Ideas?

Nagios World Conference North America

Questions?

Jared Bird
jaredbird@gmail.com
Twitter: @jaredbird

Thank You