Cybersecurity on a Budget

- FISSEA
March 2012
NIST, Gaithersburg, MD

Panelists

- Robert E. Meyers, West Virginia University
  - remeyers@mail.wvu.edu
- J. Burton Browning, Brunswick Community College
  - browningj@brunswickcc.edu
- W. Cameron Kirby, Brunswick County Public Schools
  - williamckirby@hotmail.com
- Angela Orebaugh, Booz Allen Hamilton (moderator)
  - orebaugh_angela@bah.com

Doing More with Less

- Free and low costs resources
  - People, Processes, Technology
- Cybersecurity awareness and training
- Teaching cybersecurity skills
- Identifying and mitigating vulnerabilities

Supporting Enterprise Initiatives

Security Awareness Activities on a Limited Budget

The Initiative

- In Fall of 2011, WVU instituted a new single sign-on identity manager called “MyID”
  - This replaced the ubiquitous use of PM-SSO
  - “Poor Man’s Single Sign-On” strategy (one password)

SINGLE USERNAME AND PASSWORD NOW AVAILABLE

A single username and password provides WVU faculty, staff, and students access to all core systems and services.

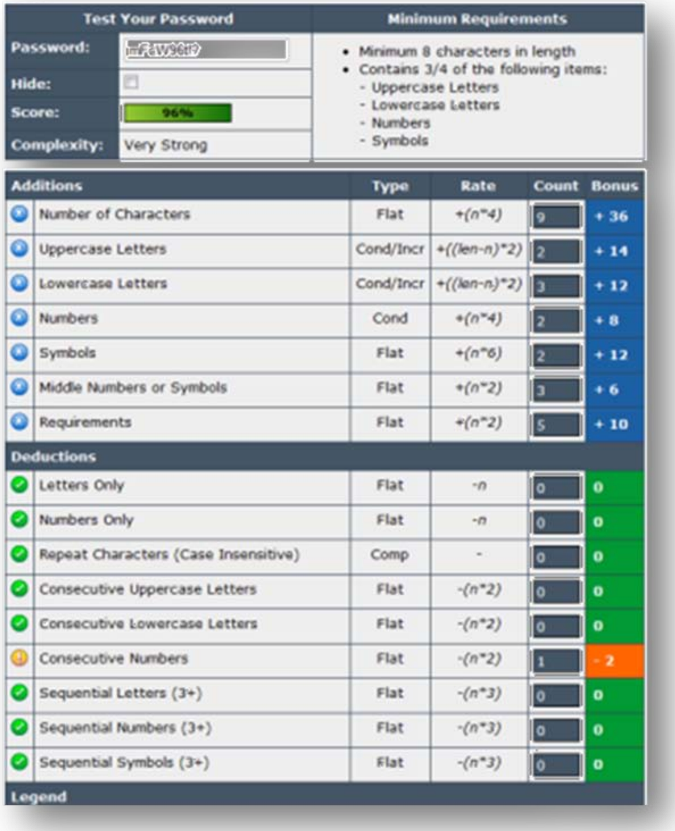
VISIT MyID

Security Awareness Challenge/Response

- Approximately 60% re-use their password on more than one account thus linking their business identity with private accounts
  - Secure password creation and use became imperative
- 2 promotional items were created for students and staff
  - T-shirts, leveraging the WVU love of their sports teams for anti-virus installation
  - 1GB flash sticks to promote strong, individual passwords

Password Challenge Game

- Having the items as mere handouts would not satisfactorily promote the two themes
  - Using www.passwordmeter.com WVU students and employee were encouraged to test their current passwords to win a flash stick

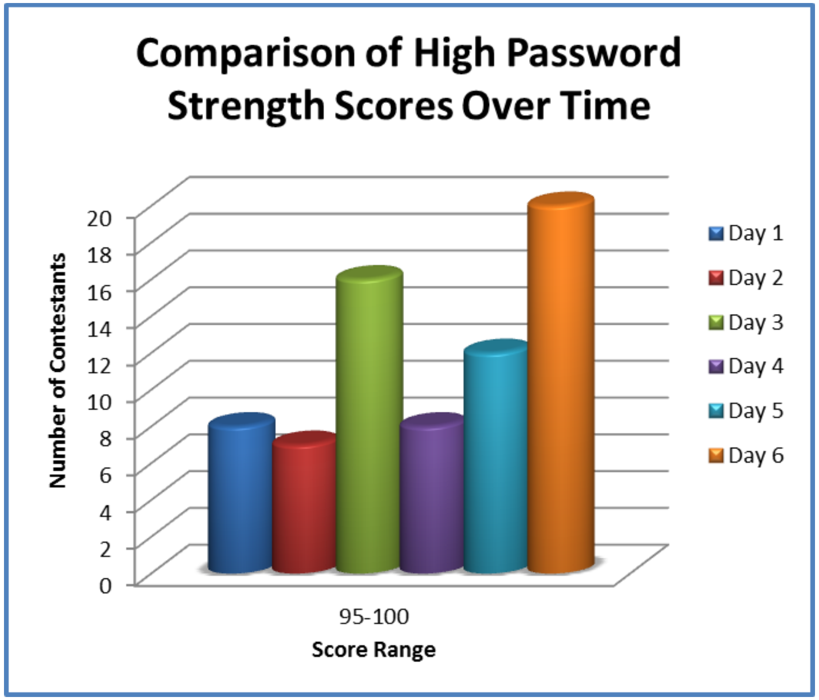


Test Your Password		Minimum Requirements
Password:	mF&W96tr?	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	□	
Score:	96%	
Complexity:	Very Strong	

	Additions	Type	Rate	Count	Bonus
●	Number of Characters	Flat	+(n*4)	9	+ 36
●	Uppercase Letters	Cond/Incr	+((len-n)*2)	2	+ 14
●	Lowercase Letters	Cond/Incr	+((len-n)*2)	3	+ 12
●	Numbers	Cond	+(n*4)	2	+ 8
●	Symbols	Flat	+(n*6)	2	+ 12
●	Middle Numbers or Symbols	Flat	+(n*2)	3	+ 6
●	Requirements	Flat	+(n*2)	5	+ 10
	Deductions				
✓	Letters Only	Flat	-n	0	0
✓	Numbers Only	Flat	-n	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	-(n*2)	0	0
✓	Consecutive Lowercase Letters	Flat	-(n*2)	0	0
!	Consecutive Numbers	Flat	-(n*2)	1	- 2
✓	Sequential Letters (3+)	Flat	-(n*3)	0	0
✓	Sequential Numbers (3+)	Flat	-(n*3)	0	0
✓	Sequential Symbols (3+)	Flat	-(n*3)	0	0
	Legend				

Results

- 150 total participants
  - The average password strength score was 79%
  - 71 1GB USB flash drives awarded
  - 110 new copies of Symantec EndPoint distributed
  - 95 OIS Defense t-shirts taken



Q & A

Information_Security@mail.wvu.edu

Open source security software use at Brunswick Community College and Brunswick County Schools Brunswick County, NC

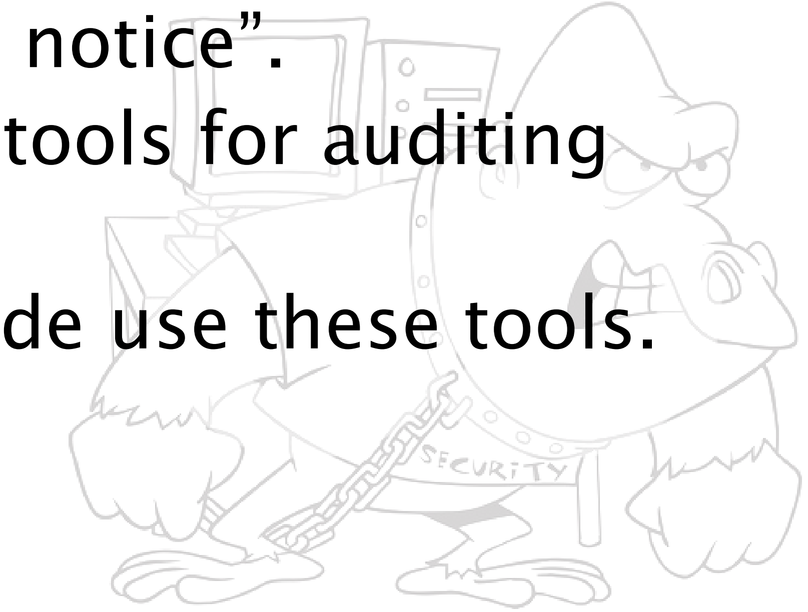
Dr. J. Burton Browning
W. Cameron Kirby

Background:

- Presenters work at BCC and BCS.
- County is rural and not a “high tech” area.
- With limited funds, open source software has helped to find and fix vulnerabilities.
- Can utilize students at the college.
- Employees main consumer with public schools.
- WIFI, labs, and admin computing are concern areas.

Opportunities, vulnerabilities, and fixes

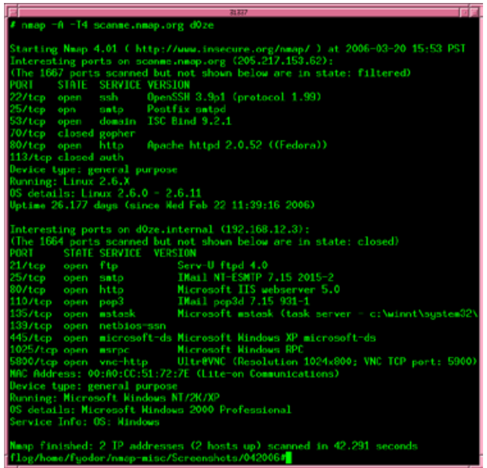
- Illegal torrent downloads: implemented a Squid proxy server to limit bit torrent on non-locked computers.
- Received performance boost from caching and reduced problem. Also implemented SNORT IDS for "advanced notice".
- We use NMAP, and other tools for auditing server hardening, etc.
- Both curriculum and IT side use these tools.



© Ron Leishman * www.ClipartOf.com/1046798

Educating students

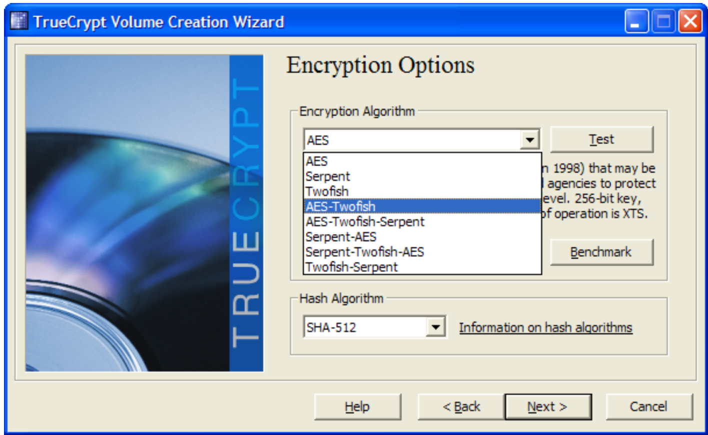
- Utilize student workers as well as students in advanced “capstone” courses. Real-world experience and resume bullet.
- Password strength, securitytube, Back Track Linux, etc.
- Public school students taught safe computing, Early College students would be exception.



```
# nmap -A -T4 scanme.nmap.org d0ze

Starting Nmap 4.01 ( http://www.insecure.org/nmap/ ) at 2006-03-20 15:53 PST
Interesting ports on scanme.nmap.org (205.217.153.62):
(The 1667 ports scanned but not shown below are in state: filtered)
PORT    STATE  SERVICE VERSION
22/tcp  open   ssh     OpenSSH 3.9p1 (protocol 1.99)
25/tcp  opn    smtp    Postfix smtpd
53/tcp  open   domain  ISC Bind 9.2.1
70/tcp  closed gopher
80/tcp  open   http    Apache httpd 2.0.52 ((Fedora))
113/tcp closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.11
Uptime 26.177 days (since Wed Feb 22 11:39:16 2006)

Interesting ports on d0ze.internal (192.168.12.3):
(The 1664 ports scanned but not shown below are in state: closed)
PORT     STATE SERVICE      VERSION
21/tcp   open  ftp          Serv-U ftpd 4.0
25/tcp   open  smtp         IMail NT-ESMTP 7.15 2015-2
80/tcp   open  http         Microsoft IIS webserver 5.0
110/tcp  open  pop3         IMail pop3d 7.15 931-1
135/tcp  open  mstask       Microsoft mstask (task server - c:\winnt\system32\
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds Microsoft Windows XP microsoft-ds
1025/tcp open  msrpc        Microsoft Windows RPC
5800/tcp open  vnc-http     Ultr@VNC (Resolution 1024x800; VNC TCP port: 5900)
MAC Address: 00:A0:CC:51:72:7E (Lite-on Communications)
Device type: general purpose
Running: Microsoft Windows NT/2K/XP
OS details: Microsoft Windows 2000 Professional
Service Info: OS: Windows

Nmap finished: 2 IP addresses (2 hosts up) scanned in 42.291 seconds
flog/home/fyodor/nmap-misc/Screenshots/042006#
```

Train employees

- Both organizations have in-service courses.
- Faculty taught via formal and informal methods.
- Tools such as antivirus and spyware solutions, Keypass, TrueCrypt, and GnuPG are game changers.
- Most faculty just want solutions, free vs. paid is not a factor, only results.



TrueCrypt Volume Creation Wizard

Encryption Options

Encryption Algorithm: AES

n 1998) that may be
l agencies to protect
evel. 256-bit key,
of operation is XTS.

Hash Algorithm: SHA-512

For more info and links:

- http://www.jbbrowning.com/sandbox/security.html
- Final questions or comments?