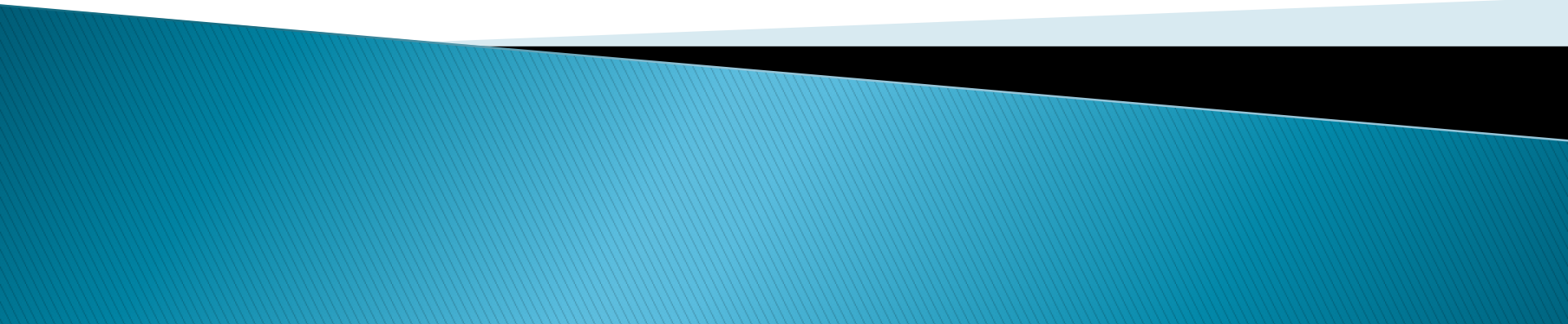


unconventional privilege escalation

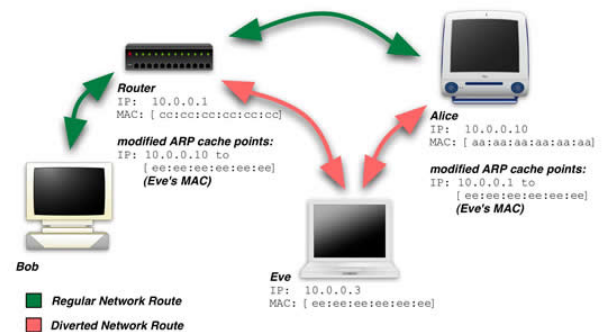


```
# nmap -A -T4 scanme.nmap.org
Starting Nmap 4.01 ( http://www.nmap.org )
Interesting ports on scanme.nmap.org:
(The 1667 ports scanned but not shown here)
PORT      STATE SERVICE VERSION
22/tcp    open  ssh      OpenSSH 4.3p1
25/tcp    open  smtp     Postfix 2.3.6
53/tcp    open  domain   ISC BIND 9.3.3
70/tcp    closed gopher
80/tcp    open  http     Apache/2.0.46
113/tcp   closed auth
Device type: general purpose
Running: Linux 2.6.X
OS details: Linux 2.6.0 - 2.6.10
Uptime: 26.177 days (since Wed Aug 1 12:00:00 2006)
Interesting ports on d0ze.intel.com:
(The 1664 ports scanned but not shown here)
```

MILWORM



read
unim



formal
ceremonious

nuclear

unconventional

conventional

square

established

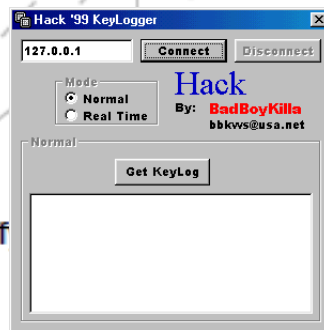
SUBVERTING THE WINDOWS KERNEL

ROOTKITS

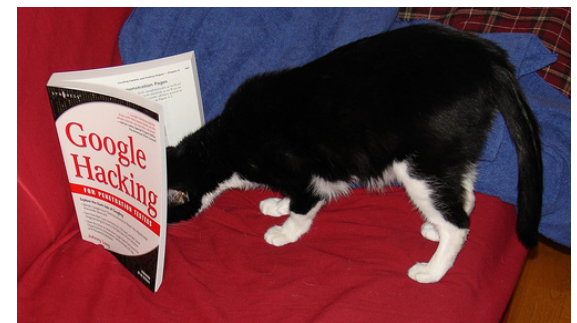
知識

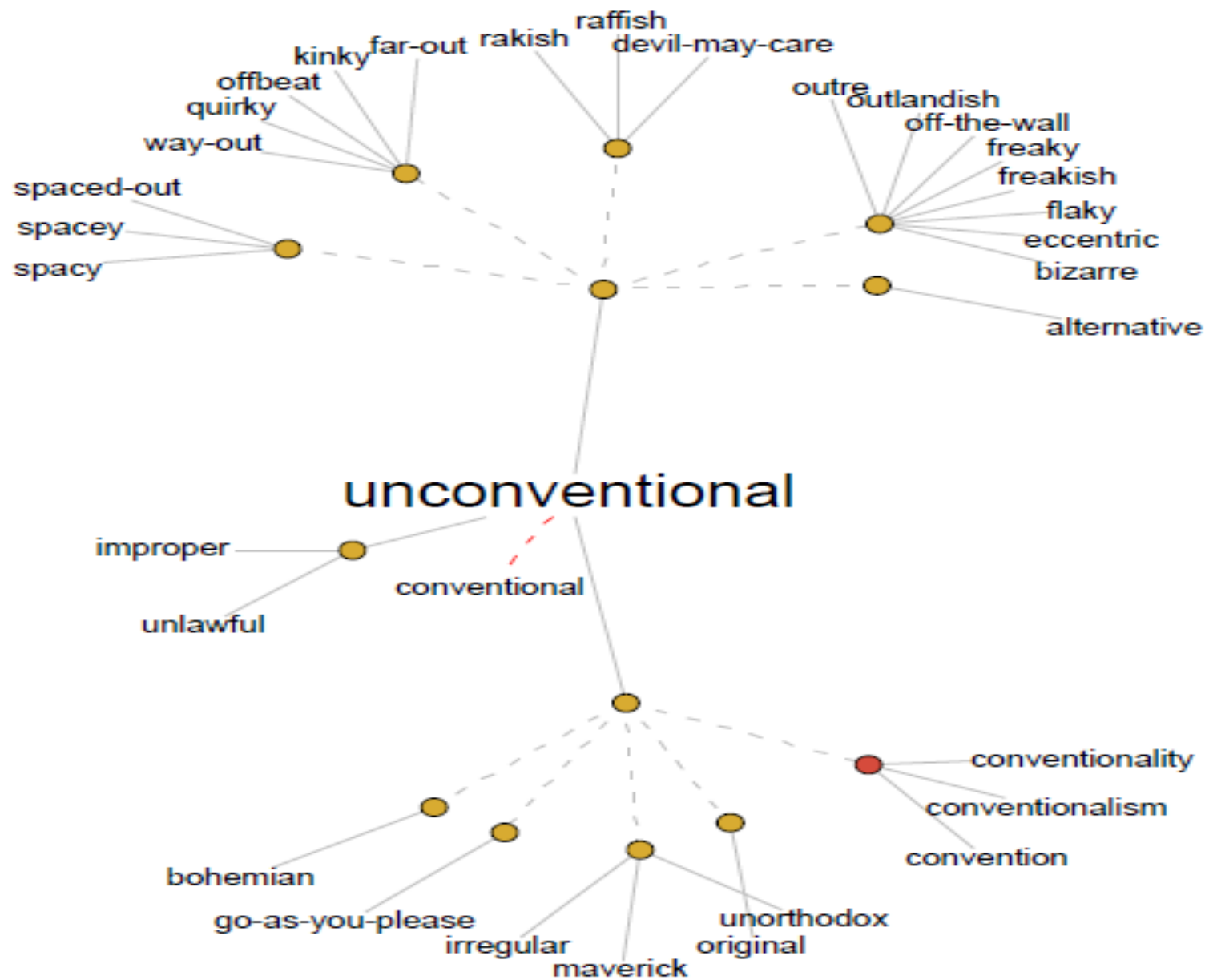


GREG HOGLUND JAMES BUTLER

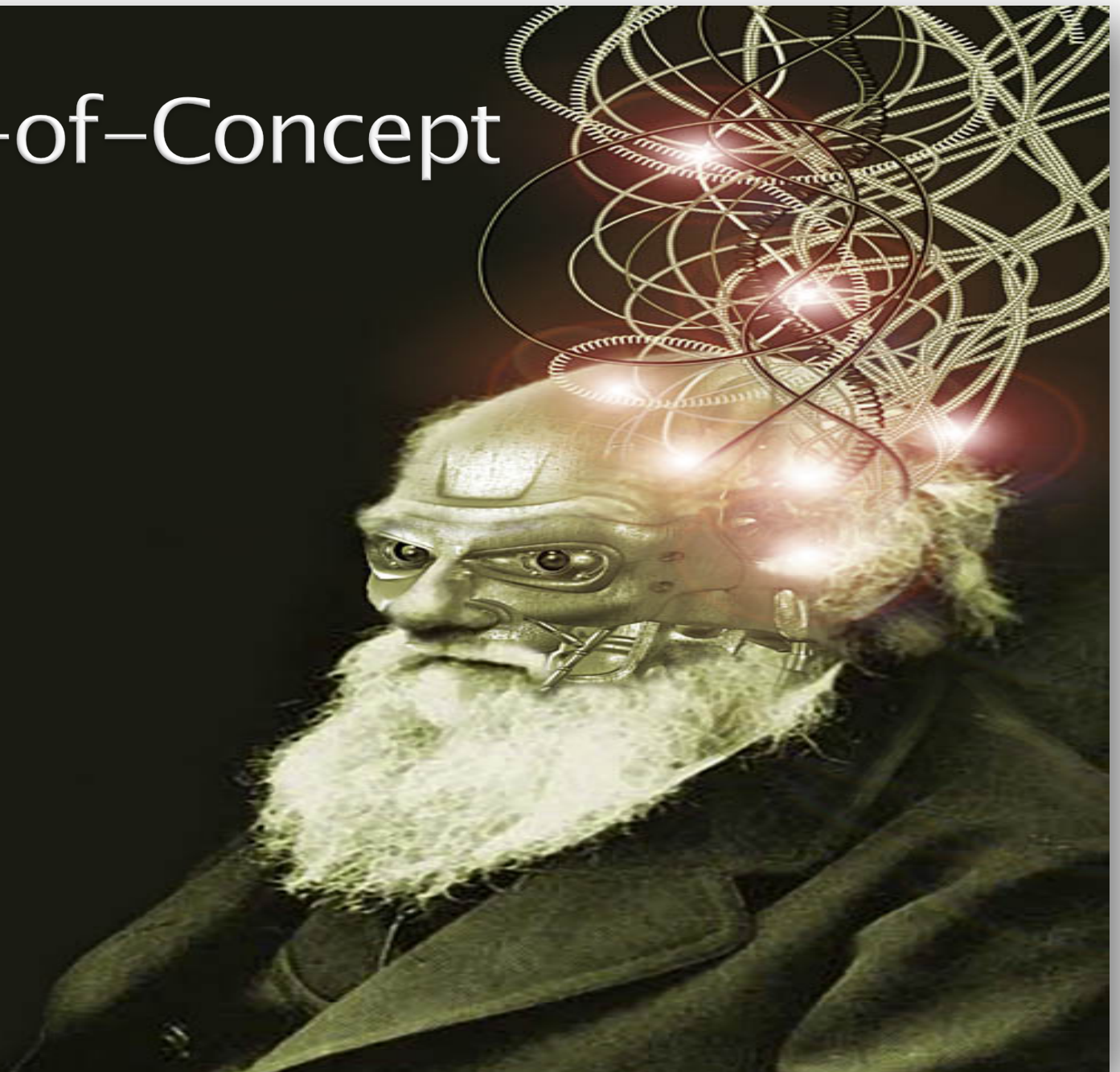


conventionalism
ation





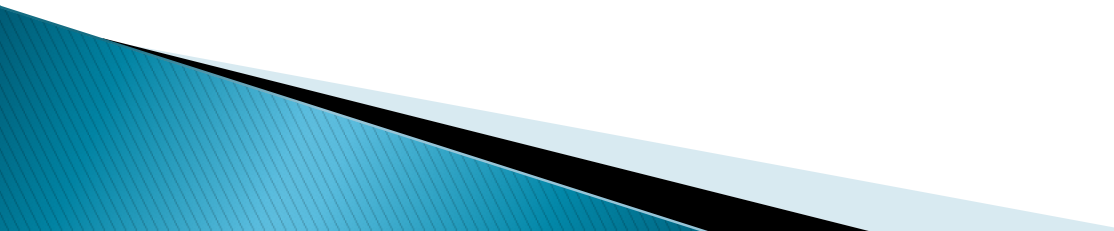
Proof-of-Concept



WARNING

**Contents of this presentation
are for educational purposes
only.**

**It is strongly suggested
that you do not use this
knowledge for illegal purposes!**



IHS

IHS

IHS

I'M JOHNNY.
I HACK STUFF.

HOME HACKERS FOR CHARITY JOHNNY? FORUMS GHOB INFORMER

HOME HACKERS FOR CHARITY JOHNNY? FORUMS GHOB INFORMER

Date 4/16/2009 Time 7:44:01 AM

Adding New User

User Name:	<input type="text"/>
Domain:	<input type="text" value="No Domain"/>
Real Name:	<input type="text"/>
Password:	<input type="password"/>
Confirm Password:	<input type="password"/>
Forward Address:	<input type="text"/>
"Sent Items" Folder:	<input type="text" value="Sent Items"/>
"Dummy" account:	<input type="checkbox"/>
Active:	<input type="checkbox"/>
Mailbox Size (Mb, 0 = Unlimited):	<input type="text"/>
Keep Copies:	<input type="checkbox"/>
Return Address:	<input type="text"/>
Finger Information:	<input type="text"/>

Your account **jdelacruz** has been created. Your password is: **O9mx******

Date 4/12/2009 Time 10:18:54 PM

Welcome to Administration

If you wish to password protect this URL, set password from *Administration - Change Administrator Password* menu from mail server controller application.

[SMTP Status](#)
[Outgoing](#)

[General](#)

[Logging](#)

[Local Domains](#)

["Mailbag" Domains](#)

[SMTP Authentication](#)

[POP Before SMTP](#)

[Ports](#)

[Advanced](#)

[Advanced 1](#)

[Advanced 2](#)

[Web Interface](#)

[Relay Service](#)

[Smart Server](#)

[DNSBL](#)

[User Administration](#)

[Distribution Lists](#)

[Mailing List Server](#)

[White Lists](#)

[Graylists](#)

SMTP Statistics

Between **11/18/2008 2:39:00 PM** - **4/12/2009 10:29:47 PM**

Number of email messages accepted:	136379	
Total messages rejected:	990304	
SMTP authentication failure:	3834	Enabled
Invalid domain names in the MAIL FROM command:	0	
Rejected by "Address verification" indicated, that the address of sender is invalid:	0	Disabled
Attempts to deliver mail to non-existing local users:	649802	
Rejected by SPF (Sender Policy Framework):	0	Disabled
Rejected by DNS Based Spam Databases (DNSBL):	313822	Enabled
Rejected by filters or server extensions:	117	
No reverse PTR records:	8110	Enabled
Rejected by "Reverse Lookup Matching":	0	Disabled
Exceeded allowed message size:	14005	Enabled
Exceeded allowed number of RCPT TO commands:	0	Enabled
Attempts to relay, when relay is not allowed:	0	Enabled
Exceeded domain quota:	0	
Exceeded the quota for a mailbox:	0	
SMTP protocol violations:	614	
Attempts to deliver to deactivated accounts:	0	

4/12/2009 12:00:09 AM - (79699) Checking with 2 DNS based spam databases
4/12/2009 12:00:09 AM - (79699) Checking 7[REDACTED]4 with sbl-xbl.spamhaus.org
4/12/2009 12:00:12 AM - (79699) In sbl-xbl.spamhaus.org
4/12/2009 12:00:12 AM - (79700) Rejected by DNS based Spam Database: Rejected by SpamHaus BL
4/12/2009 12:00:12 AM - (79700) 554 Rejected by SpamHaus BL
4/12/2009 12:00:12 AM - SMTP connection with 8[REDACTED]1 [8[REDACTED]1] ended. ID=79700
4/12/2009 12:00:12 AM - (79700) END SMTP
4/12/2009 12:00:12 AM - (79702) START POP3
4/12/2009 12:00:12 AM - Requested POP3 connection from 1[REDACTED]3 [1[REDACTED]3], ID=79702
4/12/2009 12:00:12 AM - (79702) +OK [REDACTED] Server Pro for WinNT/2000/XP, Version 1.8 (1.8.9.5)
4/12/2009 12:00:12 AM - (79702) USER [REDACTED]
4/12/2009 12:00:12 AM - (79702) +OK Password required for cme[REDACTED]
4/12/2009 12:00:12 AM - (79702) PASS XXXXXXXX
4/12/2009 12:00:12 AM - (79702) +OK Mailbox locked and ready
4/12/2009 12:00:12 AM - (79702) STAT
4/12/2009 12:00:12 AM - (79702) +OK 163 33115601
4/12/2009 12:00:12 AM - (79702) LIST
4/12/2009 12:00:12 AM - (79702) +OK
4/12/2009 12:00:12 AM - (79702) .
4/12/2009 12:00:12 AM - (79702) UIDL 1
4/12/2009 12:00:12 AM - (79702) +OK 1 xvyr4hjiyb1alg7w
4/12/2009 12:00:12 AM - (79702) UIDL
4/12/2009 12:00:12 AM - (79702) +OK
4/12/2009 12:00:12 AM - (79702) .
4/12/2009 12:00:13 AM - (79702) QUIT
4/12/2009 12:00:13 AM - (79702) +OK Aba he
4/12/2009 12:00:13 AM - POP3 connection with 1[REDACTED]3 [1[REDACTED]3] ended. ID=79702
4/12/2009 12:00:13 AM - (79702) END POP3
4/12/2009 12:00:15 AM - (79699) Rejected by DNS based Spam Database: http://www.spamhaus.org/query/bl?ip=7[REDACTED]2
4/12/2009 12:00:15 AM - (79699) 554 http://www.spamhaus.org/query/bl?ip=7[REDACTED]4
4/12/2009 12:00:15 AM - SMTP connection with 7[REDACTED]4 [7[REDACTED]4] ended. ID=79699
4/12/2009 12:00:15 AM - (79699) END SMTP
4/12/2009 12:00:16 AM - (79696) RCPT TO: <prob[REDACTED]s>
4/12/2009 12:00:16 AM - (79696) 554 V [REDACTED] 0 1000 140 11

Date 4/7/2009 Time 10:29:56 PM

User nk [redacted]

Folder **inbox**

You have **207** messages waiting.

Last Login: On 4/7/2009 1:31:34 PM via POP3 from [redacted]

Compose Delete Check Mail Settings WhiteLists Filters Addr Book Log Out

Inbox

Sent Items

Drafts

[\[Add\]](#)

Select... ▾

Select an Action ▾


Go...

Go to folder... ▾

		From	Subject	Date	Size
1	<input type="checkbox"/>	Dennis [redacted]	RE: Event Information	4/7/2009 8:06:38 PM	8450
2	<input type="checkbox"/>	Greg [redacted]sh	RE: Event Information	4/7/2009 7:21:06 PM	4339
3	<input type="checkbox"/>	PC Mall Gov	Deep Discounts While Quantities Last	4/7/2009 6:21:57 PM	17135
4	<input type="checkbox"/>	flin [redacted]om	Did you receive your March Biology Edition of FlinnFax!?	4/7/2009 4:09:44 PM	4191
5	<input type="checkbox"/>	Netflix Shipping	For Wed: Wanted	4/7/2009 4:07:59 PM	8253
6	<input type="checkbox"/>	Linda [redacted]tin	RE: when are you gone to boise with janet again	4/7/2009 3:24:07 PM	44881
7	<input type="checkbox"/>	Dennis [redacted]	NCAA Tournament Brackets	4/7/2009 2:39:26 PM	24282
8	<input type="checkbox"/>	Facebook	Jo [redacted]in wrote on your Wall...	4/7/2009 2:31:01 PM	2458
9	<input type="checkbox"/>	Linda [redacted]tin	RE: when are you gone to boise with janet again	4/7/2009 1:49:44 PM	44633
10	<input type="checkbox"/>	T [redacted]el	RE: Senior Project Presentation Day	4/7/2009 1:02:23 PM	13287
11	<input type="checkbox"/>	G [redacted]a	*****SPAM***** Calbiotech - a worldwide provider of Immunoassay products and services.	4/7/2009 12:58:11 PM	9201
12	<input type="checkbox"/>	MyLife (Reunion.com)	Still Looking For 1 Person, Nick? Try Search Scout!	4/7/2009 12:57:19 PM	34752

Message List		Server Administration	- Members	
108	Mike Groves	RE: Recently declassified photos of Twin Towers 9/11/2001.....	4/7/2009 1:36:11 PM	14483
109	Mike Groves	FW: Girl finds magic lamp]	4/7/2009 1:32:59 PM	1892348
110	Kristi Raap	meeting minutes	4/7/2009 1:31:19 PM	700
111	Kristi Raap	information request	4/7/2009 1:19:19 PM	807
112	Michelle Sheppard	Monthly Math scores	4/7/2009 12:32:38 PM	10803
113	gnorah@siboneylg.com	Orchard Software and PracticePlanet	4/7/2009 12:23:26 PM	13607
114	Tina Houchin	missing items	4/7/2009 11:42:18 AM	2586
115	Mike Groves	FW: Recently declassified photos of Twin Towers 9/11/2001.....	4/7/2009 11:24:09 AM	6397506
116	Amy Galloway	FW: Order Confirmation Order #333-1983171	4/7/2009 11:02:34 AM	2676
117	TERC Using Data	Proven Solutions for USING DATA from TERC	4/7/2009 11:01:56 AM	13681
118	Kristi Raap	student passwords	4/7/2009 10:46:01 AM	746
119	Matt Coleman	[No Subject]	4/7/2009 10:36:19 AM	24779
120	Pam Hinsz	IEP meeting for Philip Chilgren	4/7/2009 10:14:33 AM	15999
121	Pam Hinsz	IEP meeting for Chandler Holling	4/7/2009 10:13:54 AM	15959
122	Pam Hinsz	IEP meeting for Jesann Neubauer	4/7/2009 10:13:00 AM	15983
123	Pexagon Technology	Hurry! Teacher Appreciation Week is Approaching!	4/7/2009 10:05:28 AM	27030
124	Michelle Sheppard	Re: missing books	4/7/2009 10:02:44 AM	10710
125	julianna@science.edu	Acellus Deadline Coming Up	4/7/2009 9:53:39 AM	2327
126	Michelle Sheppard	missing books	4/7/2009 9:34:29 AM	11566
127	Eric Snow - WATCH DOGS	Are you already thinking about next school year?	4/7/2009	27957

Date 2/22/2009 Time 6:23:59 AM

 Compose  Reply  Reply to All  Forward  Next  Previous  Msg List  Delete  Log Out

[Inbox](#)

[Sent Items](#)

[Drafts](#)

From: Todd [redacted] <[redacted]> [Add to Addressbook](#)

To: 'Nick [redacted]' <[redacted]>

CC:

Subject: RE: dma dwa username and password

Date: Fri, 20 Feb 2009 12:27:11 -0800 [View Headers](#)

Thanks.

From: Nick H [redacted] [mailto:[redacted]]

Sent: Friday, February 20, 2009 12:10 PM

To: 'Todd [redacted]'

Subject: RE: dma dwa username and password

Actually it is supposed to be a secret but I will tell you since you are such a nice guy ... ndAD95

I sent the spreadsheet to Rhonda this am and asked her to put it on the W drive at your school so the teachers could access it also.

nick

From: Todd H [redacted] [mailto:[redacted]]

Sent: Friday, February 20, 2009 11:40 AM

To: 'Nick [redacted]'

Subject: dma dwa username and password

Can you tell me what the district/school password is to get our dma and dwa results?

PROFILE - Websense Enterprise

Seats: 330

Expiration Date: 6/27/2011

Disclaimer

Your Account ID is 2[REDACTED]7. Please refer to your Account ID when calling the Technical Support Services team

[MY PRODUCTS AND SERVICES](#)

NEWS

[Announcing version 7 of Websense Web Security](#)

[Learn about the new Web Security Gateway](#)

[Technical Support Holiday Schedule](#)

[LEARN MORE](#)



[INTRODUCING THE V10000 APPLIANCE](#)

MY WEBSENSE

[MY WEBSENSE HOME](#) | [MY PRODUCTS AND SERVICES](#) | [PATCHES](#) | [DOWNLOADS](#) | [EVALUATIONS](#)

CURRENT SUBSCRIPTION

Product:

Websense Enterprise

Expiration:

6/27/2011

SUPPORT QUICK LINKS

[Support Home](#)

[Knowledge Base](#)

[Top Customer Issues](#)

[Support by Product](#)

[Forums](#)

[ask.websense.com](#)

[Tech Alerts](#)

PATCHES

Install the latest hotfixes and Service Packs.

[View Patches](#)

DOWNLOADS AND UPGRADES

Download the latest Websense software or refresh your current version of Websense.

[View Product Downloads](#)

See how Websense discovers, investigates and reports on internet threats.

[THREATWATCHER](#) [LEARN MORE](#)

[SITEWATCHER](#) [LEARN MORE](#)

[BRANDWATCHER](#) [LEARN MORE](#)

[READ SECURITY ALERTS \(SIGN UP\)](#)

[CONTACT WEBSENSE](#)

[Sales](#)

[Support](#)

[Databases selected:](#) Multiple databases...

Publication Search

Tools: [Search Tips](#)

[Search](#)[Clear](#)

[Show all publications](#)

[0-9](#) [A](#) [B](#) [C](#) [D](#) [E](#) [F](#) [G](#) [H](#) [I](#) [J](#) [K](#) [L](#) [M](#) [N](#) [O](#) [P](#) [Q](#) [R](#) [S](#) [T](#) [U](#) [V](#) [W](#) [X](#) [Y](#) [Z](#)

1-6 of 6

[ACM Transactions on Information and System Security; New York](#)

[Information Management & Computer Security; Bradford](#)  Full Text: 1995 - current, delayed 1 year(s) [Create RSS Feed](#)

[Information Security Journal; New York](#)  Full Text: 2004 - 2007 [Create RSS Feed](#)

[International Journal of Information Security; Heidelberg](#)  Full Text: 2001 - current, delayed 1 year(s) [Create RSS Feed](#)

[International Journal of Information Security and Privacy; Hershey](#)  Full Text: 2007 - current, delayed 6 month(s) [Create RSS Feed](#)

[Journal of Information Privacy & Security; Marietta](#)  Full Text: 2005 - current [Create RSS Feed](#)

1-6 of 6

Admin Main

School:

[Admins](#)

[Instructors](#)

[Options](#)

[Import/Export](#)

[What's New?](#) NEW

[Academic Years](#)

[Students](#)

[Grading Periods](#)

[Course Catalog](#)

[Grading Scales](#)

[Classes](#)

[Email Addresses](#)

[Email/Announcements](#)

[Reports](#)

[Grade Reporting](#)

[Attendance](#)

[Scheduling](#)

[Tuition/Fees](#)

[Lunch](#)

[Discipline](#)

[Letter Templates](#)

[Standards](#)

[Standards Scales](#)

[Curriculum Map Templates](#)

[Curriculum Maps](#)

[Search Curriculum Maps](#)

[Lesson Plan Templates](#)

[Search Lesson Plans](#)

[User Guides](#)

[Data Setup](#)

[Defaults](#)

[Subscriptions](#)

[Email Signature](#)

[Update Account](#)



Date 2/22/2009 Time 6:32:39 AM

 Compose  Reply  Reply to All  Forward  Next  Previous  Msg List  Delete  Log Out

Inbox
Sent Items
Drafts

From: Amazon.com <store-news@amazon.com> [Add to Addressbook](#)
To: m [REDACTED] s <n [REDACTED] s>
CC:
Subject: Amazon.com: Free Songs and Inexpensive Albums
Date: Wed, 18 Feb 2009 03:18:48 -0800 (PST) [View Headers](#)

Please [click here](#) if the e-mail below is not displayed correctly.

amazon.com

Let them choose from millions of items [Amazon.com Gift Cards](#)

[Your Amazon.com](#)

[Today's Deals](#)

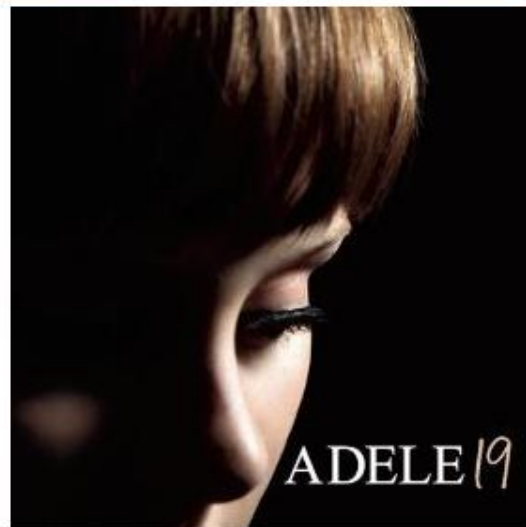
[See All Departments](#)

Dear Amazon.com Customer,

As someone who has shopped for music at Amazon.com, you might like to know about our Special MP3 Deals store.

There, you'll find loads of free songs, our Daily Deal, and albums priced from \$5 to \$7.99.

[Learn more about Special MP3 Deals](#) 



YourAccount


Orders

See & Modify Recent Orders



If you want to:

- [Track Packages](#)
- [Print an Invoice](#)
- [Combine Orders](#)
- [Cancel or Change Orders](#)

[View Recent and Open Orders](#) 

Purchase History

[View Older Orders](#)
[View Your Digital Orders](#)
[View Used Item Pre-orders](#)
[View Marketplace Transactions](#)

More Order Actions

[Return Items or Gifts](#)
[Manage Subscribe & Save Items](#)
[Leave Seller Feedback](#)
[Leave Packaging Feedback](#)

Payment

Credit Cards & Gift Cards

Payment Methods

[Manage Payment Options](#)
[Add a Credit Card](#)
[View Check Balance](#)

Gift Cards

[View Gift Certificate/Card Balance](#)
[Apply a Gift Certificate/Card to Your Account](#)
[Purchase a Gift Card](#)

Settings

Password, Prime & E-mail

Account Settings

[Change Name, E-mail Address, or Password](#)
[Forgot Your Password?](#)
[1-Click Settings](#)
[Manage Prime Membership](#)

Address Book

[Manage Address Book](#)
[Add New Address](#)

E-mail from Amazon

[E-mail Preferences & Notifications](#)
[Amazon Delivers E-mail Subscriptions](#)
[Product Availability Alerts](#)
[Special Occasion Reminders](#)



The Best Of 1980 - 1990

by [U2](#)

Price: **\$7.99**

Album Savings: ~~\$6.86~~ compared to buying all songs

★★★★☆ (5 customer reviews)

Original release date: May 13, 2008

Format: [MP3, 256 kbps](#) — plays on iPod® and all MP3 players

Also available in [CD Format](#)

[See larger image](#)

[Share your own customer images](#)

[Buy MP3 album with 1-Click®](#)

[Redeem a gift card or promotion code & view balance](#)

Requires [Amazon MP3 Downloader](#)

Amazon MP3 Downloader



Adds songs instantly to iTunes or Windows Media Player. [Get it free.](#)

MP3 Songs

[Preview all](#)

	Song Title	Time	Price	
▶	1. Pride (In The Name Of Love)	3:49	\$0.99	Buy MP3
▶	2. New Year's Day	4:19	\$0.99	Buy MP3
▶	3. With Or Without You	4:58	\$0.99	Buy MP3
▶	4. I Still Haven't Found What I'm Looking For	4:41	\$0.99	Buy MP3
▶	5. Sunday Bloody Sunday	4:42	\$0.99	Buy MP3
▶	6. Rattle and Hum	5:52	\$0.99	Buy MP3
▶	7. The Fly	4:36	\$0.99	Buy MP3
▶	8. The Unforgettable Fire	3:38	\$0.99	Buy MP3
▶	9. The Unforgettable Fire	4:55	\$0.99	Buy MP3
▶	10. Sweetest Thing	3:03	\$0.99	Buy MP3

Match case



Amazon MP3 Downloader

Now downloading the track "Khanada" by "Duran Duran."



Wind...

Amaz...

100%



4:45 PM

Amazon.com Gift Cards

Get them what they've always wanted. (Even if you don't know what it is.)

- Redeemable for millions of items
- Ships for free, never expires
- Available in any amount from \$5 to \$5,000

Need a box of gift cards?

Buy gift cards by the [box](#), or order [individual gift cards](#), in denominations of \$10, \$25, or \$50.

Add to Wish List

Add to Shopping List

Add to Wedding Registry

Add to Baby Registry

Give to Family and Friends



E-mail a gift card

E-mail a personalized gift card for immediate delivery.

Buy now



Print at home

Print a personalized gift card on your own printer. (Remember to have your credit card handy when you're ready to print).

Buy now



Send a gift card by mail

Mail a personalized gift card (shipping is free, of course). Please allow 5-7 business days for delivery.

Buy now

[Terms and conditions](#) apply to Amazon.com gift cards. See below for more details.

Have a Gift Card?

Shop now

Amazon.com gift cards are redeemable for millions of items on our site.

[Read more](#)

Apply to account

Apply your gift card to your account, and you can use it whenever you're ready.

[Read more](#)

View account balance

See how much you have left to spend on your gift card.

[Read more](#)

Need to Resend a Gift Card?

Resend

Resend a gift card to a recipient. [Read more](#)

Subject: friends sent you an Amazon.com Gift Card!

Date: Sat, 3 Jan 2009 01:14:07 -0800 (PST) [View Headers](#)

Grocery **DON'T DELETE THIS MESSAGE! You've received a \$100.00 Amazon.com Gift Card!** **DVD & VH**
Music, Textbooks, Unbox, Video, Downloads, Apparel, & Music, Textbooks, Unbox

amazon.com®
gift card

amount:
\$100.00

claim code:
E - HZKM8G -

[Learn how to redeem your gift card](#)

Start shopping 

DOGBERT THE
SECURITY CONSULTANT

BE ON THE LOOKOUT
FOR ANY SUSPICIOUS
BEHAVIOR.



www.dilbert.com
scottadams@aol.com

IF YOU SEE A GUY
DO SOMETHING THAT
YOU WOULDN'T DO,
BEAT HIM TO DEATH
WITH A TRASH CAN.



10-30-07 © 2007 Scott Adams, Inc./Dist. by UFS, Inc.

CAN WE
USE
RECYCLE
BINS?

I
WOULDN'T
HAVE ASKED
THAT
QUESTION.



Almost invariably, security awareness and training is one of the most cost effective measures that can be employed to protect corporate and organizational information assets. This is largely due to the fact that protecting information, generally more so than any other asset, is best achieved through routine business practices that permeate every element of an organization. Therefore, where each individual entrusted with sensitive information takes prudent measures and personal responsibility for protecting those assets, a robust security environment should occur naturally.