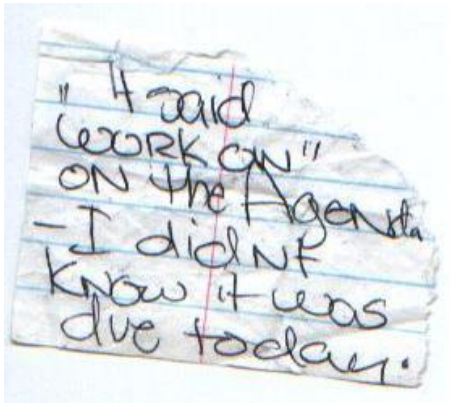
War Games, from laptop to real life: Making the Cyber World a Safer Place

COL Curtis A. Carver Jr.
Associate Dean, Information and Educational Technology

What to Take from this Presentation

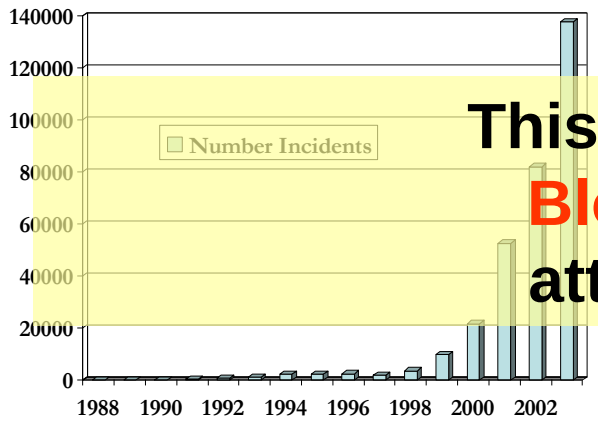
- The situation is getting worst.
- Perimeter defenses are not working.
- Centralized management is not working.
- Passive approaches to awareness and training are not working.
- Active approaches are necessary to create an army of one.

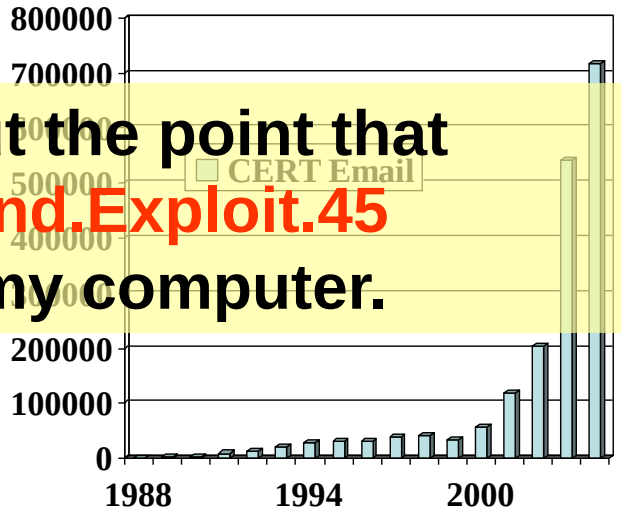


The Situation is Getting Worst

- Increasing number of attacks
- Increasing complexity of attacks
- Decreasing interval between patch release and attack exploitation

Increasing Attacks





This is about the point that Bloodhound.Exploit.45 attacked my computer.

	Date	Filename	Threat	Original Location	Status
	10/11/2005 8:37:15 PM	3B67DD5E.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected
	10/11/2005 8:37:15 PM	62655091.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected
	10/11/2005 8:37:10 PM	366DCE75.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected
	10/11/2005 8:37:04 PM	1305368F.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected
	10/11/2005 8:37:04 PM	E03CB46.emf	Bloodhound.Exploit.45	C:\Documents and Setti...	Infected

How could I be Attacked!

- Antivirus on perimeter.
- Antivirus updates 14 times a day.
- Anti-spam updated automatically.
- Windows patches update automatically.
- Firewalls on computer and on perimeter.
- Was working over an encrypted VPN channel.

Attacked occurred at 8:00PM.
Patches released 6:00 PM.

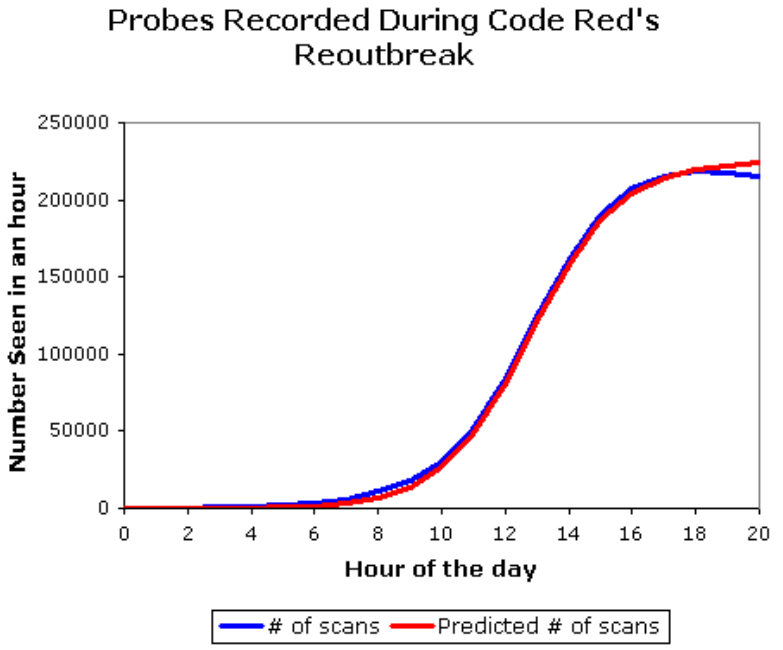
Remedial Action

- Check for updates to anti-virus and anti-spam (didn't work).
- Ran anti-virus (didn't work), ran anti-spam (didn't work), ran windows update (worked!)
- Set anti-virus to run at reboot. Reboot (worked!).

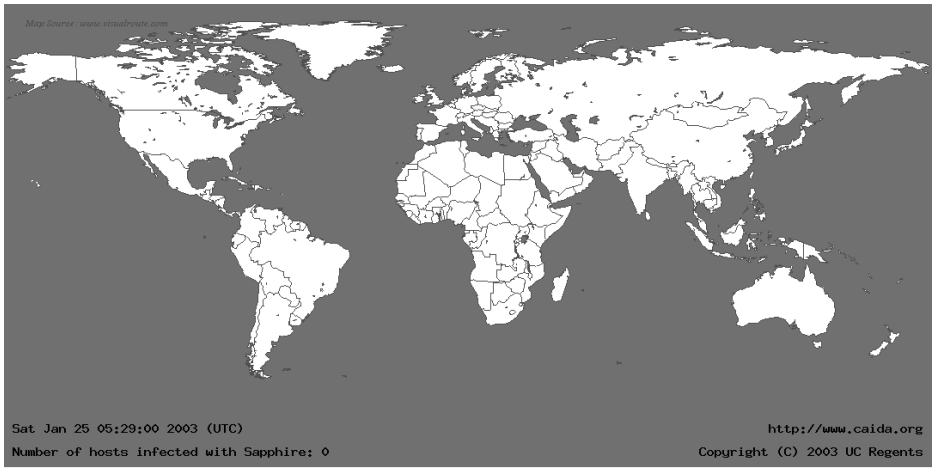
Changing Environment

(Speed of Attack)

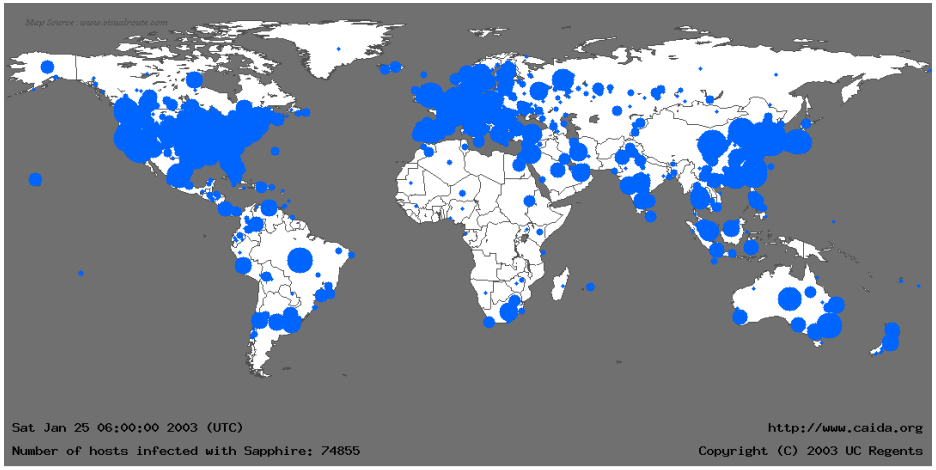
- **Morris Internet Worm** (1988 - Over 72 hours affected 6,000 computers taking 90 minutes to bring a system down).
- **Melissa Virus** (May 1999 – Over 72 hours affected 100,000 computers. One site received 32,000 Melissa email messages in 45 minutes.)
- **Code Red** (July 2001 approx. 250,000 computers in 20 hours)



Slammer



The World
January 25, 2003



Slammer penetration 30 minutes after release.

http://www.cs.berkeley.edu/~nweaver/sapphire/

Increasing Complexity

Slammer

- Sapphire contains a simple, fast scanner in a small worm with a total size of only 376 bytes.
- In the first minute, the infected population doubled every 8.5 seconds.
- Achieved full scanning rate in less than 3 minutes. Full scanning rate was 55 million scans per second.
- The scanning rate was limited because significant portions of the internet ran out of bandwidth.
- Sapphire spread nearly two orders of magnitude faster than Code Red.

http://www.cs.berkeley.edu/~nweaver/sapphire/

Perimeter Defenses are not Working

(Necessary but not Sufficient)

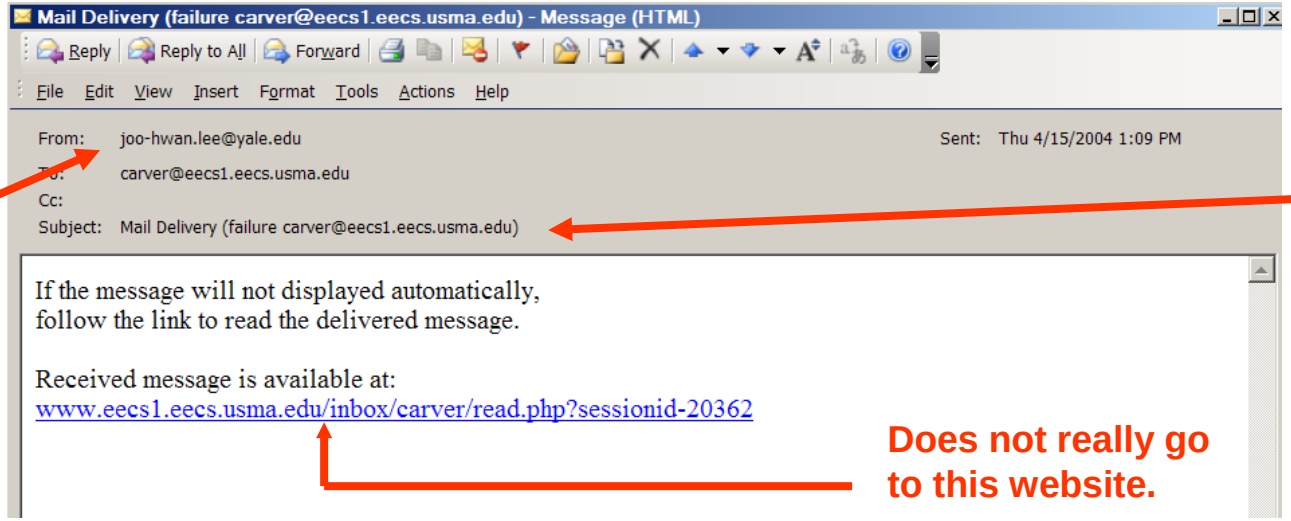
- Anti-virus, anti-spam, firewall, intrusion detection, and intrusion prevention systems are all necessary but not sufficient.
- Why?
  - Mobile worker population is out there working hard to pick up new and exotic attacks.
  - Insider threat much greater than outside threat.
  - New computing devices are coming in all shapes and sizes.

My Projector is attacking my network!

Centralized Management is not Working
(Necessary but not Sufficient)

- Anti-virus and software update servers are necessary but not sufficient. Active directory helps with authentication and authorization but is not enough.
- Why?
  - Mobile work force
  - Time between release of patch and release of an attack tool, “flash to bang”, is rapidly shrinking.
  - As you hardened the perimeter and central management, attackers attempt to bypass these defenses through social engineering attacks.

Social Engineering
(Hidden Attack)



Who is Joo-hwan Lee is and why is he sending you email?

How can someone at Yale post email messages in EECS and you cannot?

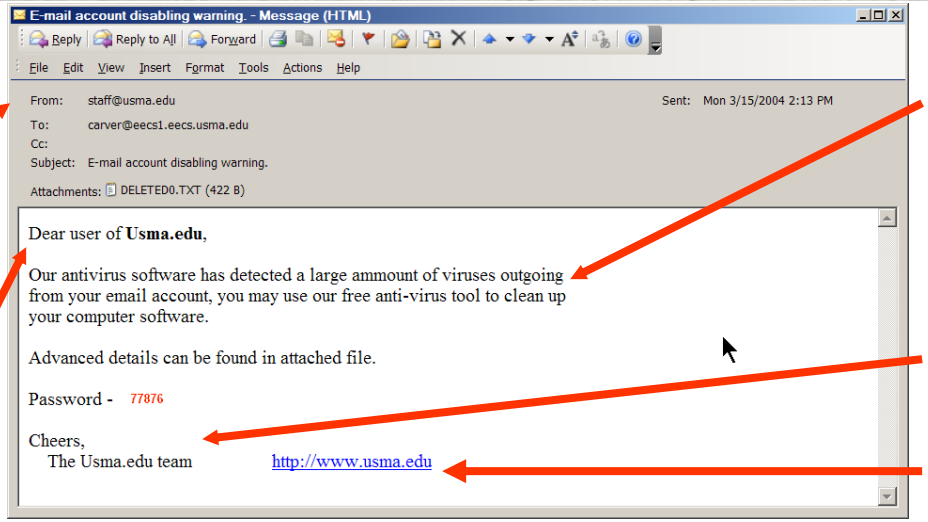
Does not really go to this website.

In this case, the attacker is trying to trick you into clicking on the embedded link. The link does not go to an webserver in the Electrical Engineering and Computer Science (EECS) department but instead opens an invisible frame and launches a program embedded in another part of the email message.

Social Engineering (Hidden Encrypted Attack)

The Military Academy does not use non-personal accounts such as staff@usma.edu to send security announcements.

The Military Academy will not refer to you as "Dear member of usma.edu" – it will refer to you by name.



Military Academy can automatically update software – no need to ask permission.

An email from the "usma.edu team" sounds suspicious

Does not really go there.

As you might imagine, the virus creators were not thrilled about their viruses being deleted by the corporate virus checkers so they tried another approach. They encrypted the virus to disguise it, gave the user the password to decrypt it and install it, and hide it behind a familiar looking web address that did not go to the website but launched the virus.

Social Engineering
(Hidden Zipped File)

From: Gaskins, F. MS DOIM
Sent: Wednesday, September 07, 2005 09:36 AM
To: allusers
Subject: Required Password Change

In order for West Point \ USMA to comply with DA policies in regards to computer passwords, **ALL** users of the West Point \ USMA network will be required to change their domain password. Passwords must be changed no later than 1700 19 Sep 2005 in order to comply with the new password guidelines.

When choosing your new password please keep the following in mind:

- Password must contain no less than **10** characters.
- Password must contain **2 characters of each of the 4 types of characters listed**: uppercase letters, lower case letters, numeric characters (0 – 9), Nonalphanumeric characters, (!, @, #, $, etc.).
- Password can **NOT** contain three or more characters from the user's account name, social security numbers, birthdays, names, and dictionary words.
- The password can **NOT** be the same as any of your previous **10** passwords.

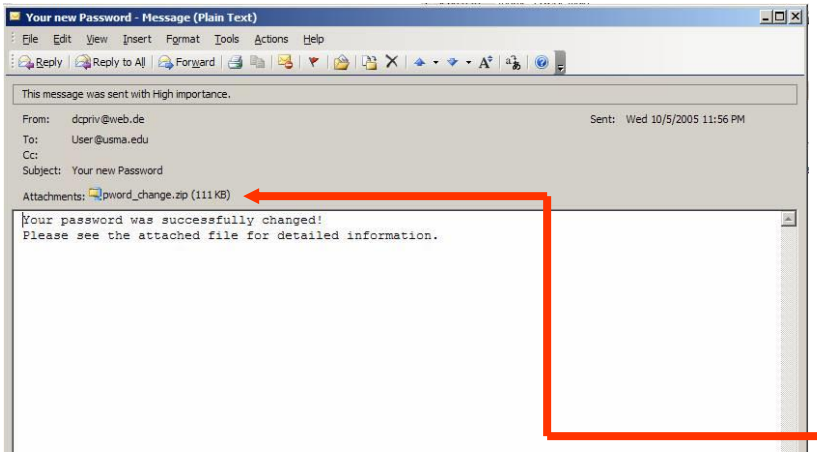
Please be sure to pass this note along to any personnel who may be currently located outside of West Point \ USMA (i.e. TDY, leave, sabbatical) and using resources remotely (i.e. Webmail, VPN).

Users inside USMA can press CTRL+ALT+DEL while logged onto their machines and choose the "Change Password" option.

From outside USMA passwords can be changed by logging on to Webmail and choosing "options" in the lower left hand corner, scroll down the options page and click the "Change Password" button.

For additional information please contact your Department Computer Officer, Information Management Officer or Information Assurance Manager.

Legitimate email to all users.



Illegitimate email to all users 28 days later.

The attack contained in the zipped file is new and host anti-virus software cannot protect the computer. The computer must be reimaged.

Passive Approaches to Awareness and Training are not working

- Attacks are bypassing perimeter defenses.
- Sophistication of attacks is increasing.
- Every user is an attack point.
- Every user is a vulnerability.
- Even one user fails, insider attack occurs and it will spread very rapidly.

Passive to Active

- Users remember:
  - 30% of what they hear
  - 40% of what they see and hear
  - 70% of what they do.

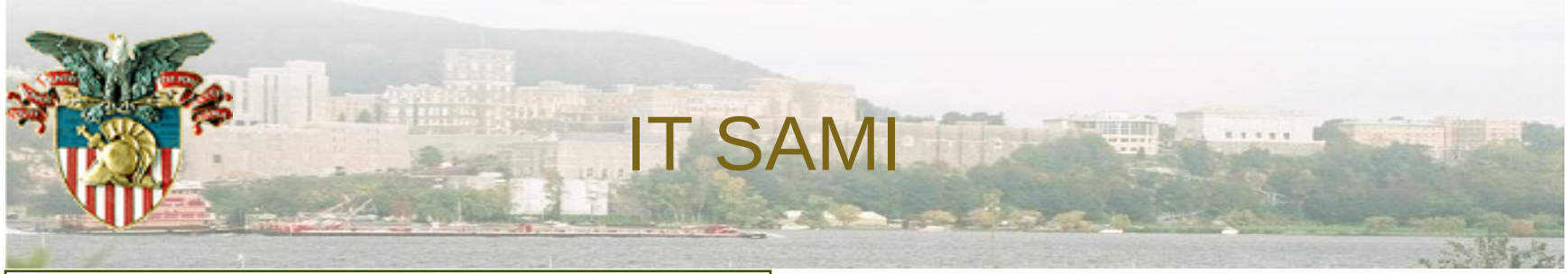
- We have to get the users actively involved in learning.

Active approaches are necessary to create an **Army of One**

- Cadet Information Security Officers (ISOs)
- Carronade
- CDX
- MAADNET

Cadet Information Security Officers

- Empower **students** to administer their companies, fix problems locally, conduct training, conduct exercises, and lead.
- Results
  - Increased notification of outages
  - ISO Empowerment through Active Roles
  - New User Training led by students
  - IT SAMI
  - Carronade Exercise



IT SAMI

IT-SAMI INSPECTION SHEET

Cadet Name	Company	Year	Inspector Name	
Category				
ITEM		POINTS		
AD-AWARE				
INSTALLED?		NO,		-30
CHECK UPDATES		>= 1 WEEK OLD,	- 05	
		>=3 WEEKS,		-10
		>= 1 MONTH,		- 20
LAST SYSTEM SCAN		>= 1 WEEK OLD,	- 05	
		>=3 WEEKS,		-10
		>= 1 MONTH,		- 20
SCAN RESULTS				
	For each process		-10	
	For every 20 additional items,			-05
DEFRAGEMENT ANALYZE				
SYSTEM SUGGESTED?			YES,	-10
ADD/REMOVE PROGRAM LIST				
WILD TANGENT			YES,	-10
WEATHER BUG			YES,	-10
WELL KNOWN FILE SHARING		YES,	-20/item	
BROWSER HEALTH				
SEARCH BAR OTHER THAN GOOGLE			YES,	-10
VIRUSES				
DEFENITION FILES		>= 1 WEEK OLD,	- 5	
		>=3 WEEKS,		-10
		>= 1 MONTH,		- 20
SYSTEM DATA				
SPACE REMAINING ON C-DRIVE			< 20%,	-10
MAJORITY OF ACDEMIC DATA				
STORED ON C-DRIVE			YES,	-20

11/30/2020 4:37 PM

Best In BDE

Best Regiment:	86.13
Best Company:	95.00
Worst Reg:	75.00
Worst Company:	53.50

Carronade

- Active learning phishing exercise.
- Student controlled, student initiated.
- Four messages
- Leadership and IT infrastructure aware of concept but not deployment date

From: sr1770@usma.edu [mailto:sr1770@usma.edu]
Sent: Tuesday, June 22, 2004 4:57 PM
To: cadet@usma.edu
Subject: Grade Report Problem

There was a problem with your last grade report. You need to:

Select this link Grade Report and follow the instructions to make sure that your information is correct; and report any problems to me.

Robert Melville
COL, USCC
sr1770@usma.edu
Washington Hall, 7th Floor, Room 7206

Carronade Results

	Email Scheme					
	Embedded		Attachment		Sensitive	
Class	**open**	**%**	**open**	**%**	**open**	**%**
Freshmen	82	8%	129	13%	117	12%
Sophomores	70	7%	126	12%	110	11%
Juniors	86	9%	117	12%	115	12%
Seniors	58	6%	114	11%	114	11%
Total	296	29%	486	48%	456	46%
Total sent	1010		1014		999	

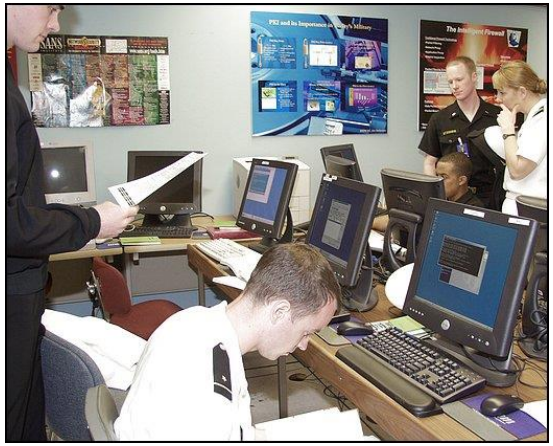
CDX

- Active learning competition between Army, Navy, Air Force, Coast Guard, Merchant Marine, and Air Force Institute of Technology.
- Cadets take onsite pass for the exercise and man the site 24 hours a day.
- NSA attacks through VPN channels. The sites defend and offer a standard suite of services.

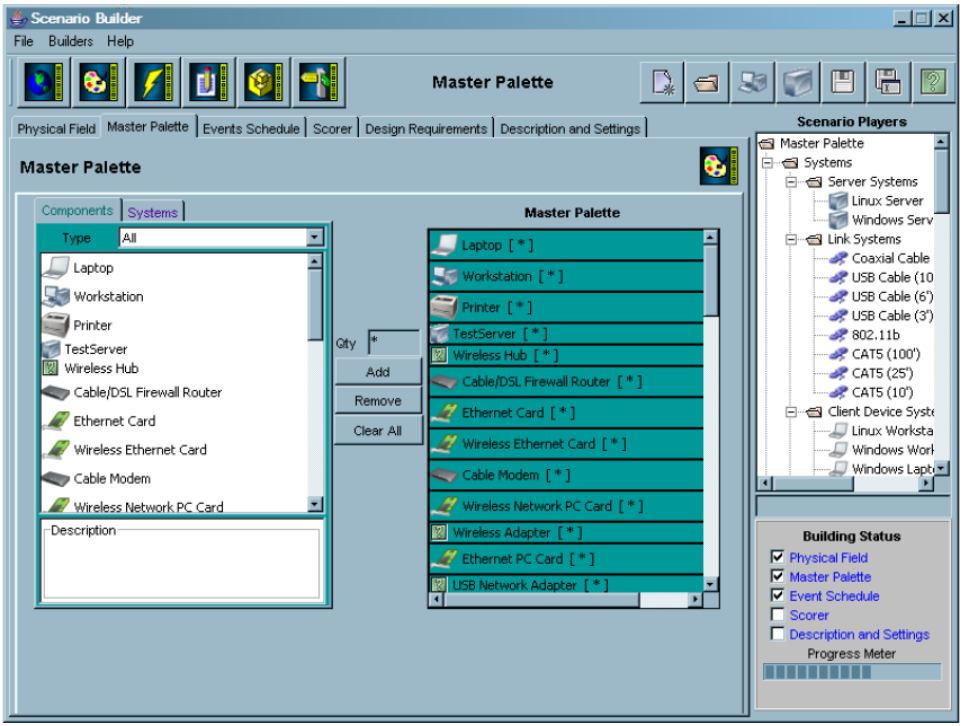
CDX

Principal benefit is leadership and education.

Capt. Allen Harper of the U.S. Marine Corps, a student at the Naval Postgraduate School and head of the blue team, begins analyzing the red team's attack.

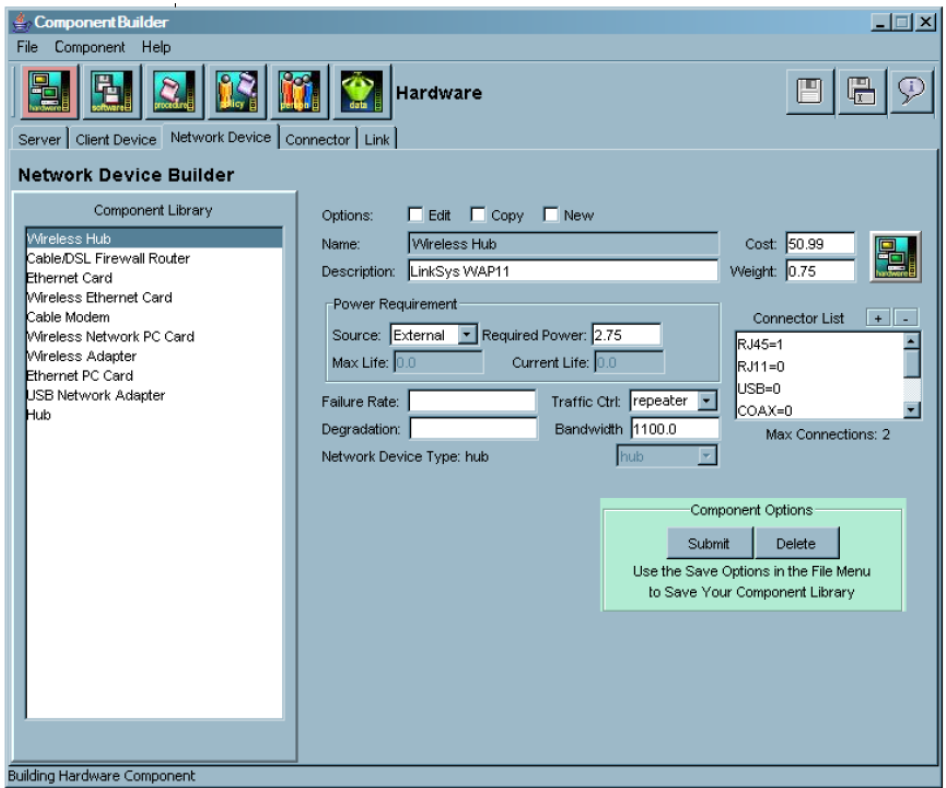


MAADNET

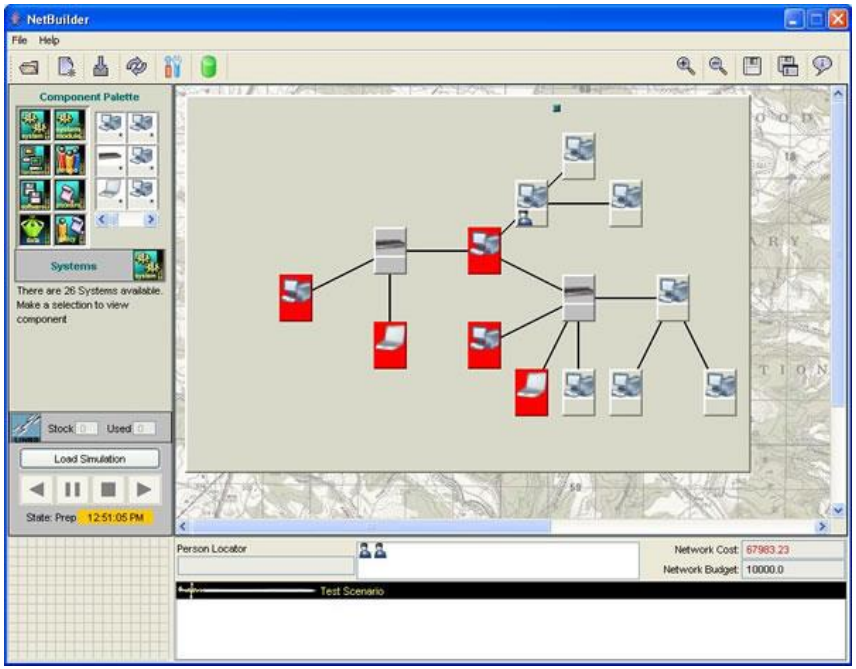


Game that incorporates people, procedures, data, hardware, and software into a realistic simulation.

Build components, systems, Networks, and then scenarios.

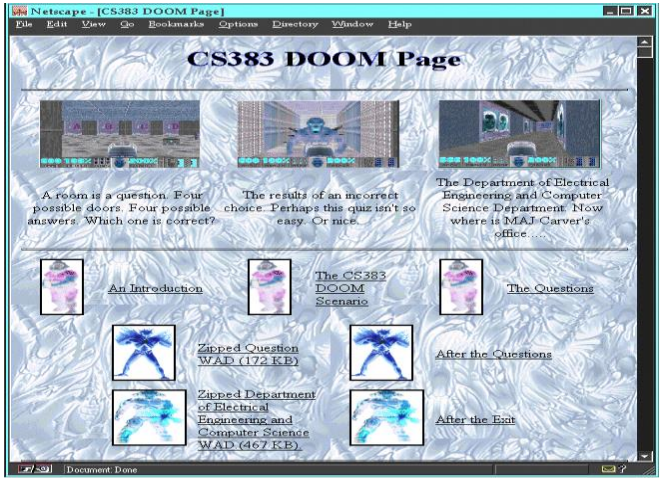


MAADNET

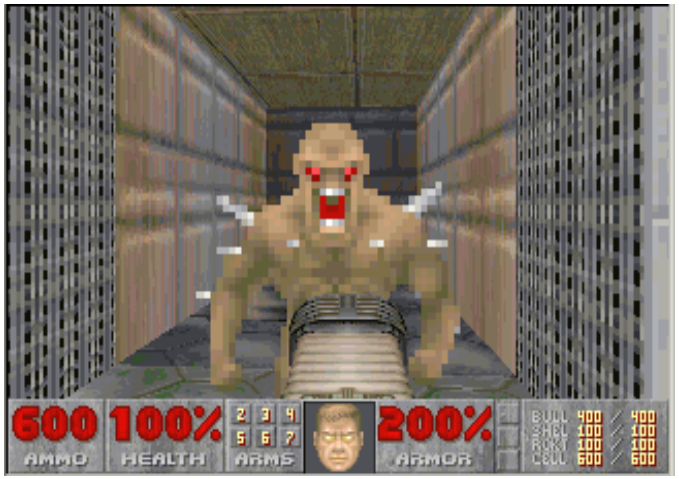


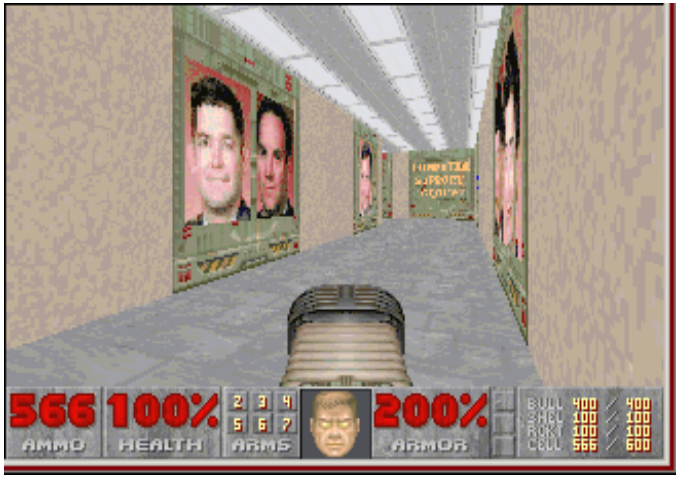
MAADNET will support nationwide competitions as teams compete to design the most productive and best defended networks.

DOOM


Netscape - [CS383 DOOM Page]
File Edit View Go Bookmarks Options Directory Window Help
CS383 DOOM Page
A room is a question. Four possible doors. Four possible answers. Which one is correct?
The results of an incorrect choice. Perhaps this quiz isn't so easy. Or nice.
The Department of Electrical Engineering and Computer Science Department. Now where is MAJ Carver's office....
An Introduction
The CS383 DOOM Scenario
The Questions
Zipped Question WAD (172 KB)
After the Questions
Zipped Department of Electrical Engineering and Computer Science WAD (467 KB)
After the Exit
Document Done


A
B
C
D
600 AMMO
100% HEALTH
2 3 4 5 6 7 ARMS
200% ARMOR
BULL 400 / 400
SHEL 100 / 100
ROKT 100 / 100
CELL 600 / 600


600 AMMO
100% HEALTH
2 3 4 5 6 7 ARMS
200% ARMOR
BULL 400 / 400
SHEL 100 / 100
ROKT 100 / 100
CELL 600 / 600


566 AMMO
100% HEALTH
2 3 4 5 6 7 ARMS
200% ARMOR
BULL 400 / 400
SHEL 100 / 100
ROKT 100 / 100
CELL 566 / 600

USMA Team

- COL Curt Carver
- **LTC Ron Dodge**
- Dr Aaron Ferguson
- LTC John Hill
- Dr John James
- MAJ Fernando Maymi
- COL Dan Ragsdale
- COL Gene Ressler

Thing to Take Away

- The situation is getting worst.
- Perimeter defenses are not working.
- Centralized management is not working.
- Passive approaches to awareness and training are not working.
- Active approaches are necessary to create an **Army of one**.

Questions, Queries, Comments, A Conversation

Class of 2009 Computing System

- Dell Precision M70 Laptop
  - 15.4” Screen/256MB Video w/PCI-E
  - 2.0 GHz PM(Dothan) CPU
  - 1 GB DDR2 Memory
  - 60 GB 7200 rpm Hard Drive
  - CD-RW/DVD Drive
  - Docking Station
  - WindowsXP, Office 2003
- Iomega External HD
  - 160 GB HD
  - USB 2.0/Firewire
  - Backup Software
- DELL A922 Printer
  - Color Printer
  - Copier/Scanner
- 1GB Thumb Drive