



Tips & Tools for Teaching Security

MPICT Educator Conference

Dr. Mark Ciampa

Author, Course Technology/Cengage Learning

Mark.ciampa@wku.edu



Tips & Tools for Teaching Security

Changing Face of Attacks



Question 1

- Which country hosts the most Websites that have malware?
 - A. US
 - B. China
 - C. Russia
 - D. Germany



Question 2

- What is the average number of e-mails that have infected attachments?
 - A. 1 in 44
 - B. 1 in 337
 - C. 1 in 909
 - D. 1 in 714



Question 3

- When the ISP McColo was disconnected from Internet Nov 11 it disrupted their zombies to the extent that spam decreased by
 - A. 14%
 - B. 36%
 - C. 75%
 - D. 90%



Question 4

- A site showing some of the largest increases in attacks is
 - A. Microsoft
 - B. Facebook
 - C. CNN
 - D. eBay



Question 5

- Which is a reason why Apple Mac computers are under increasing attacks?
 - A. High level of complacency among Mac users about security
 - B. Use of Intel chipset
 - C. Increased sales of Macs due to popularity of iPods
 - D. All of the above



Question 6

- Which is a reason why iPhone users may be more vulnerable to phishing attacks?
 - A. Instead of entering URL via screen user may click on embedded link
 - B. iPhone version Safari not display embedded URL before clicked
 - C. iPhone browser only display partial URL in address bar
 - D. All of the above



Changing Face of Attacks

- Increasing trend compromise legitimate Web sites (iFrame, XSRF,SQL Injection, XSS)
- Significant change in attack targets (cell phones, Apple Mac, Facebook)
- Volume of malware successfully propagated via e-mail attachments is declining



Need For Changes Teaching Security

- Incorporate these changes when teaching security courses to CIS majors
- Utilize more hands-on tools to teach security vs. lecture approach
- Incorporate security into all areas of CIS
- Make all students aware of security risks and defenses



Outline

- Tools for teaching security to CIS majors
- Approaches for broadening teaching of security to all students



Tips & Tools for Teaching Security

Hands-On Tools



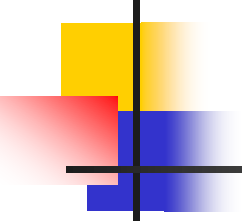
Tools

- Attack-defend labs using local virtual environment
- Virtual online labs
- Modeling tools
- Simulation tools



White Hats

- *White Hats* were typically attackers who considered themselves “good”
- *“Some hackers believe it is ethically acceptable as long as they do not commit theft, vandalism, or breach any confidentiality. These hackers (sometimes called ‘White Hats’) claim that their motive is to improve security by seeking out security holes so that they can be fixed.”*



Ethical Hacking

- *Ethical Hacker* not same as White Hat
- Ethical Hacker employed by an organization
- Trusted to attempt to penetrate networks/systems using the same methods as an attacker
- Difference is Ethical Hacker has authorization to probe the target
- Title changing to *Penetration Tester*



Teaching Pen Testing

- Many courses, books and even certificates on “Ethical Hacking”
- Division among security instructors about teaching attack mechanisms
- Pro – *“To catch a thief you must think like a thief”*
- Con – *“Students could use this knowledge to become an attacker”*



Virtual Attack-Defend Labs

- Uses multiple virtual machines on single computer to demonstrate attacks and defenses
- Eliminates need for dedicated and isolated security lab
- Students can proceed at own pace and retry activities easier
- Supports online instructional model



Virtual Attack-Defend Labs

- Configure and manage firewall
- Explore vulnerabilities of different network servers including email, DHCP, DNS, and ftp
- Explore the vulnerabilities of different application servers including SQL and web servers
- Install, configure and use an intrusion detection system like snort



Virtual Attack-Defend Labs

- Cheops-ng
- Umit
- GFI LANguazrd Network Security Scanner
- Tenable Nessus
- L0phtCrack
- John the Ripper



VMware Workstation

- VMware Workstation preferred VM (over Microsoft Virtual PC)
- VMware available in different avenues
 - 30-day download
 - Student Discount (*VMWare for U.*)
 - Free Academic Licenses (*VMWare Academic Program*)



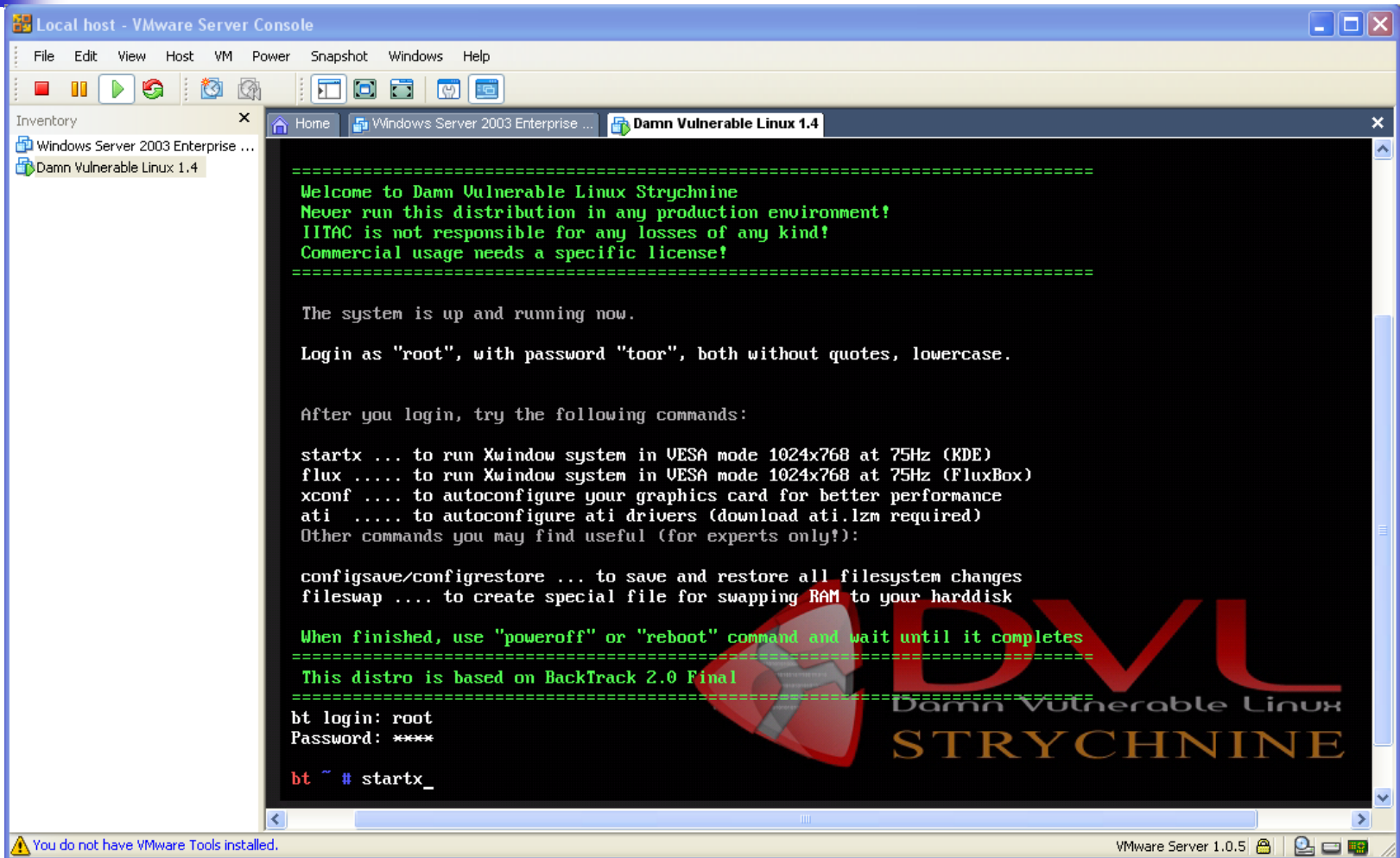
Virtual Attack-Defend Tools

- DVL is Live CD available as a 150MB ISO
- It contains older, easily breakable versions of Apache, MySQL, PHP, and FTP and SSH daemons
- Tools available to help compile, debug, and break applications running on these services, including GCC, GDB, NASM, strace, ELF Shell, DDD, LDasm, LIDa
- <http://www.damnvulnerablelinux.org>

DVL



DVL in VMware



Local host - VMware Server Console

File Edit View Host VM Power Snapshot Windows Help

Inventory

- Windows Server 2003 Enterprise ...
- Damn Vulnerable Linux 1.4

```
=====
Welcome to Damn Vulnerable Linux Strychnine
Never run this distribution in any production environment!
IITAC is not responsible for any losses of any kind!
Commercial usage needs a specific license!
=====

The system is up and running now.

Login as "root", with password "toor", both without quotes, lowercase.

After you login, try the following commands:

startx ... to run Xwindow system in VESA mode 1024x768 at 75Hz (KDE)
flux .... to run Xwindow system in VESA mode 1024x768 at 75Hz (FluxBox)
xconf ... to autoconfigure your graphics card for better performance
ati .... to autoconfigure ati drivers (download ati.lzm required)
Other commands you may find useful (for experts only):

configsave/configrestore ... to save and restore all filesystem changes
fileswap .... to create special file for swapping RAM to your harddisk

When finished, use "poweroff" or "reboot" command and wait until it completes
=====
This distro is based on BackTrack 2.0 Final
=====

bt login: root
Password: ****

bt ~ # startx_
```

DVL
Damn Vulnerable Linux
STRYCHNINE

You do not have VMware Tools installed. VMware Server 1.0.5

Virtual Attack-Defend Lab Manual



- *Virtualization Lab Manual* by Course Technology/Cengage Learning
- 14 chapters
- May 2009
- Under \$20



Virtual Online Labs

- Microsoft TechNet Virtual Labs
- Signup for free 30 or 90 minute lab time
- Examples:
 - How Firewall combines typical firewall settings with Internet Protocol security (IPSec) in a single MMC management console
 - How BitLocker used
 - Use of User Account Control (UAC)
- Obvious Microsoft focus
- <http://technet.microsoft.com/en-us/bb467605.aspx>



Virtual Labs

- CyberWATCH
- Virtual labs give students at other institutions opportunity to practice and study IT security techniques by accessing lab remotely
- Lab accommodates 12 remote students simultaneously
- Equipment to teach router, switch, and firewall security as well as workstation and server security courses
- <http://www.cyberwatchcenter.org/lab.htm>

Challenges of Lab-Based Teaching



- Laboratory-based approach to teaching data communications networking has many advantages for student learning
- Also presents challenges
 - High cost of purchasing and monitoring equipment
 - Maintaining the appropriate levels of hardware and software
 - Having an appropriate mix of equipment available
 - Ability to scale lab facilities as student demand increases
 - Need to deliver course material in a distance format



Definitions

- *Modeling* - process of producing a model
- *Model* - representation of construction and working of a system of interest
- Model is similar to actual system but is simpler
- *Simulation* is operation of a model of system
- "*Simulation* is a tool to evaluate the performance of a *model* under different configurations of interest and over periods of real time"



How Modeling Used

- Model typically used before existing system altered or new system built
 - Reduce the chances of failure to meet specifications
 - Eliminate unforeseen bottlenecks
 - Prevent under or over-utilization of resources
 - Optimize system performance.
- What is the optimum design for a new network?
- What are the associated resources that may be required?
- How will a network perform when the traffic load increases?
- What will be the impact of a link failure?
- Are the security defenses adequate?



Why Use Modeling in Instruction

- Data communication networking modeling software creates virtual model of computer network by documenting parts and enabling simulated traffic
- Astronauts use ground simulators to work through different in-flight scenarios
- Network modeling tools allow students to
 - Analyze ways to improve network performance
 - Trace causes of network problems
 - Assess the network



Why Use Modeling in Instruction

- Modifying actual data communications network production system too expensive or disruptive
- Most large networks exhibit very complex behavior as result 3 basic factors
 - Subtle protocol interactions
 - Complicated network topologies
 - Complex traffic patterns
- Difficult to recreate network problem to determine cause
- Model be created and studied to determine behavior of actual system



Advantages of Using Modeling In Instruction

- Modeling tools address these issues and expands scope of courses
- Modeling of networks can illustrate theoretical aspects of networking through practical models of computer networks (combining theory and practice)
- Modeling tools let students to explore broader range of network alternatives than can often be supported in a university lab environment



Advantages of Using Modeling In Instruction

- Modeling network allows students to visualize the impact of design decisions
- Understanding networks and how they operate requires understanding of complex and obscure concepts and processes
- Made more difficult because these cannot be easily seen or presented in a tangible manner.
- The use of tools to model, simulate and visualize lends itself very readily to teaching in this area



Advantages of Using Modeling In Instruction

- Recent research indicating that M/S tools also having significant impact on student learning
- Some teaching tools may unwittingly promote such an approach by making tasks too mechanical or easy to complete: completing the steps in exercise to simulate configuring a device will not encourage a deep understanding of the underlying process unless this is accompanied by appropriate cognitive elements
- Becomes even more important when the learning environment is remote through distant education in that the student needs to work independently and is removed from immediate teacher support.
- Modeling tools can enhance student learning by reinforcing students' understanding at the conceptual level of basic as well as advanced concepts and will also give them experience in solving the types of networking issues they will confront in a production environment



Types Mathematical Models

- A model for simulation study is mathematical model developed with help of simulation software
- Three broad types of mathematical models
 - *Deterministic* - Input and output variables are fixed values (stochastic) with minimum 1 input or output variables probabilistic
 - *Static* - Time is not taken into account
 - *Dynamic* - Time-varying interactions among variables taken into account



3 Types Software for Modeling

- General-Purpose Simulation Language
- Communications-Oriented Simulation Language
- Communications-Oriented Simulator

Communications-Oriented Simulator

- Simulation package allows simulate network in specific class of communications networks without programming
- Network developed by choosing items from menus using point-and-click, dialogue boxes (forms), and graphics
- Typical modeling constructs for LAN simulator include types of LANs (Ethernet, wireless, etc.), nodes on a LAN (personal computers, workstations, printers, etc.), LAN interconnection devices (switches, routers, etc.), and traffic (message) generators
- Advantages - simulator development in very short time; simulators have modeling constructs closely related to network components



OPNET

- Industry leader in network modeling
- 4 categories products
 - Application performance management
 - Network operations
 - Capacity planning and design
 - Network R & D
- OPNET IT Guru – Free academic software
(http://www.opnet.com/university_program/it_guru_academic_edition/)



OPNET

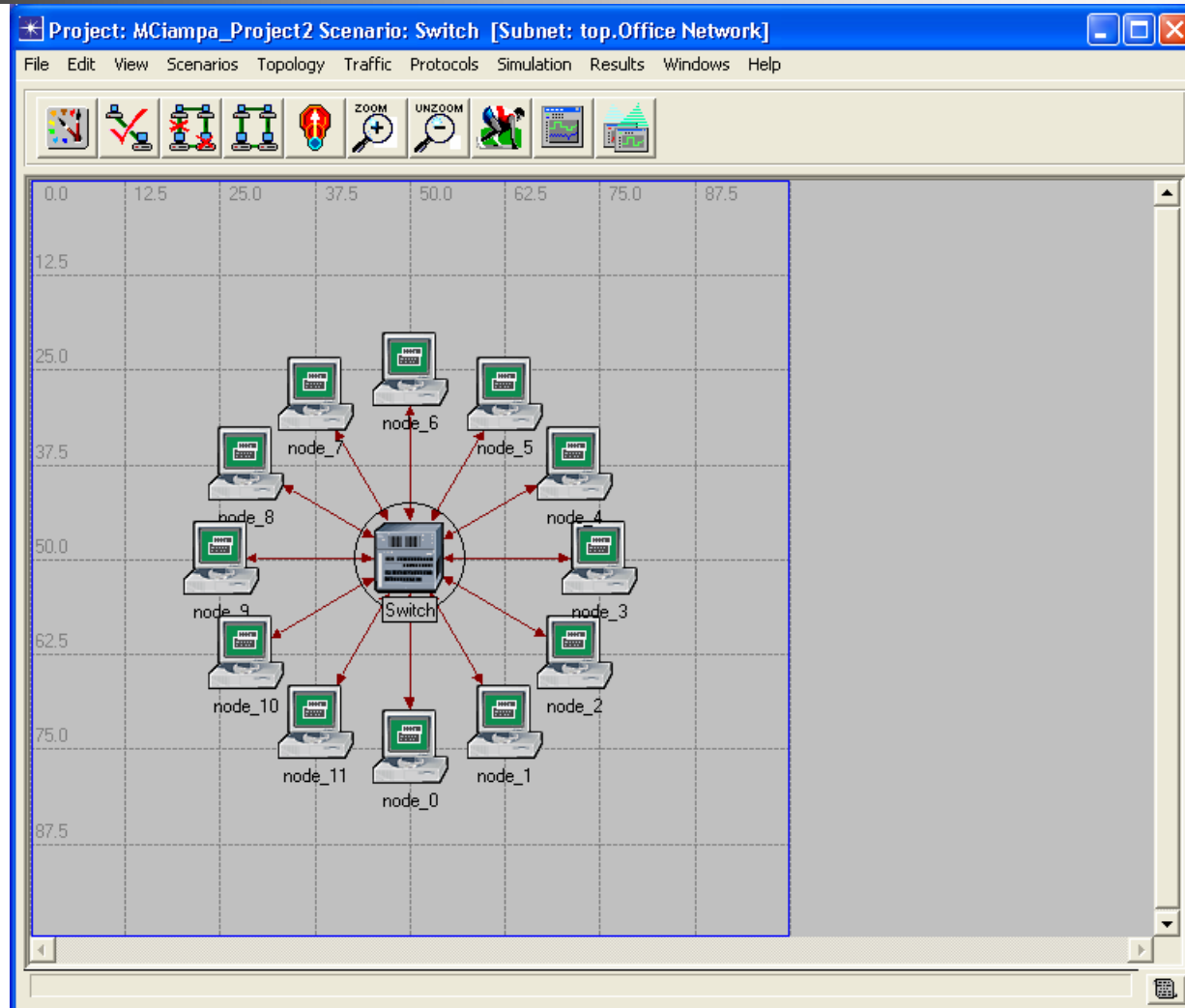
- Ability to including actual network data into model itself
- Network performance be monitored over time to create baseline functionality
- Data then imported into OPNET to create a virtual representation of network infrastructure



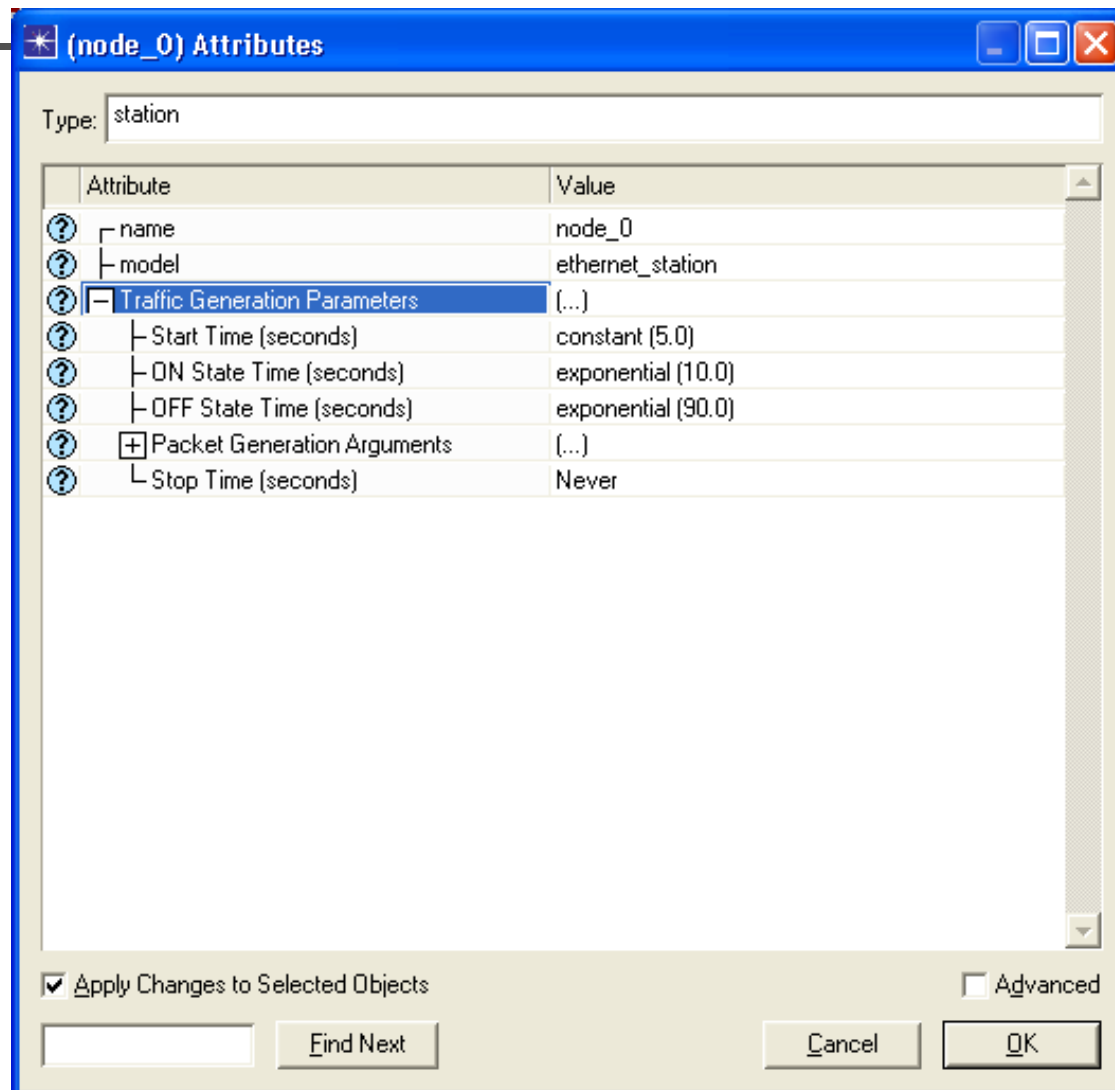
OPNET

- OPNET can be used to create models of security attacks and defenses
- Includes both wired and wireless models
- Several resources for preconfigured OPNET labs and OPNET data

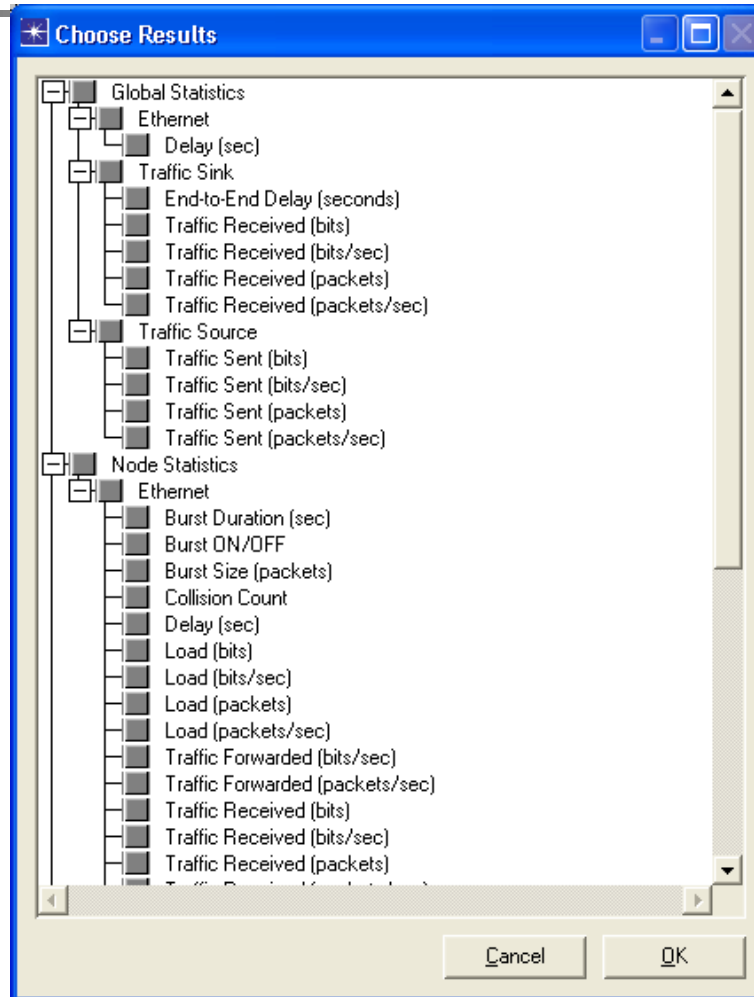
OPNET



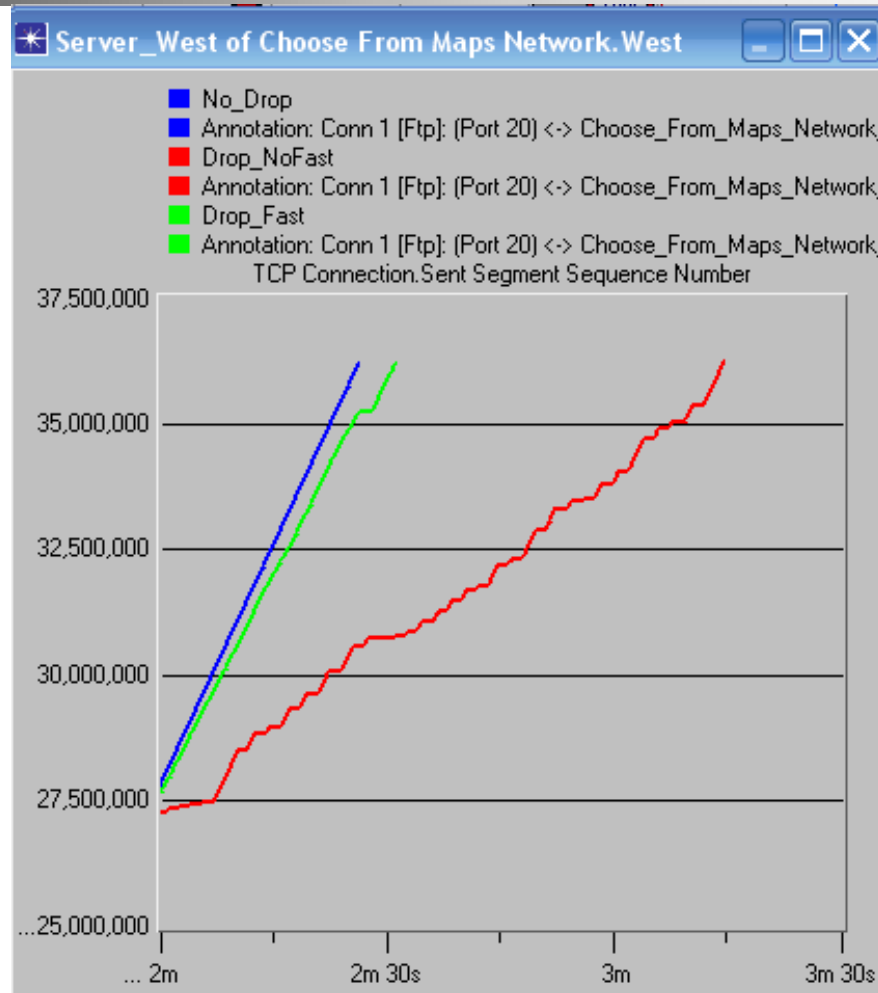
OPNET



OPNET



OPNET





Wireshark

- Network protocol analyzer
- Deep inspection of hundreds of protocols
- Live capture and offline analysis
- Multi-platform
- Captured network data can be browsed by GUI or separate utility
- Very good display filters
- View live data or can read/write many different capture file formats
- Can use precaptured files to analyze attacks

Wireshark

The screenshot displays the Wireshark interface with a packet capture of an HTTP transaction. The main pane shows a list of captured packets, and the lower pane shows the detailed view of a selected packet (Frame 36).

No.	Time	Source	Destination	Protocol	Info
29	1.238988	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [PSH, ACK] Seq=1 Ack=190
30	1.259654	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] http > 3197
31	1.266628	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [PSH, ACK] Seq=1 Ack=
32	1.266819	192.168.0.2	192.168.0.1	TCP	5000 > 1025 [PSH, ACK] Seq=1 Ack=
33	1.267850	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [ACK] Seq=510 Ack=20
34	1.274361	192.168.0.1	192.168.0.2	TCP	http > 3197 [PSH, ACK] Seq=1 Ack=
35	1.274447	192.168.0.2	192.168.0.1	TCP	3197 > http [FIN, ACK] Seq=190 Ac
36	1.274987	192.168.0.1	192.168.0.2	TCP	http > 3197 [FIN, ACK] Seq=20 Ack
37	1.275018	192.168.0.2	192.168.0.1	TCP	3197 > http [ACK] Seq=191 Ack=21
38	1.276019	192.168.0.1	192.168.0.2	TCP	http > 3197 [FIN, ACK] Seq=26645
39	1.281649	192.168.0.1	192.168.0.2	TCP	[TCP Window Update] 1025 > 5000
40	1.282181	192.168.0.1	192.168.0.2	TCP	1025 > 5000 [FIN, ACK] Seq=510 Ac

Frame 36 (60 bytes on wire, 60 bytes captured)

- Ethernet II, Src: Netgear_2d:75:9a (00:09:5b:2d:75:9a), Dst: 192.168.0.2 (00:0b:5d:20:cd:02)
- Internet Protocol, Src: 192.168.0.1 (192.168.0.1), Dst: 192.168.0.2 (192.168.0.2)
- Transmission Control Protocol, Src Port: http (80), Dst Port: 3197 (3197), Seq: 20, Ack: 190, Len: 0
 - Source port: http (80)
 - Destination port: 3197 (3197)
 - Sequence number: 20 (relative sequence number)
 - Acknowledgement number: 190 (relative ack number)
 - Header length: 20 bytes

0000 00 0b 5d 20 cd 02 00 09 5b 2d 75 9a 08 00 45 00 ..] [-u...E.
0010 00 28 00 84 00 00 40 06 f8 f8 c0 a8 00 01 c0 a8 .(. ...@.
0020 00 02 00 50 0c 7d 00 00 68 14 bc 38 dd 9b 50 11 ...P.}... h.<8..P.
0030 0c 00 93 ca 00 00 00 00 00 00 00 00

Acknowledgement number (tcp.ack), 4 bytes | P: 120 D: 120 M: 0



LabSim

- LabSim security simulator
- Video Training
- Hands-on Lab Simulations
- Written Lessons
- Certification Practice Exams



LabSim

- Configure/manage a PIX firewall
- Configure/manage security of router
- Explore vulnerabilities of network servers (email, DHCP, DNS, and ftp)
- Explore the vulnerabilities of application servers (SQL and web servers)
- Install, configure and use an intrusion detection system like snort



Other Sources

- SEED (Instructional Labs for Computer Security Education) -
<http://www.cis.syr.edu/~wedu/seed/index.html>
- Teaching Usable Privacy and Security: A guide for instructors -
<http://cups.cs.cmu.edu/course-guide/>



Tips & Tools for Teaching Security

**Practical Security
For All Students**



Why Increase In Attacks

- Speed of attacks
- More sophisticated attacks
- Faster detection weaknesses
- Distributed attacks
- User confusion



User Confusion

- Confusion over different attacks: worm or virus? adware or spyware?
- Confusion over different defenses: antivirus, firewall, patches
- Asked perform technical procedures and make technical decisions



User Confusion

- *Permission to open port?*
- *Safe quarantine attachment?*
- *Approval your bank install add-in?*
- Education and awareness are key defenses



Teaching Security Today

- Very brief coverage of security in “Introduction to Computers” courses where teach definitions
- Teach network security to computer majors
- Treat security as separate entity in CIS
- Leave out *practical security* for non-computer majors



Higher Ed Challenge

- Integrate security across CIS
- Need educate *all* students about *practical* computer security
- “*Security Literacy*” – Why and how to make personal systems secure
- ***“Users should be as fluent with security literacy as with Office or e-mail”***



Where Teach?

- *CIS Curriculum* – Integrate into all courses: programming, Web development, applications, networking
- *Intro to Computers*
 - Often minimal coverage from enterprise perspective
 - Trend to integrate practical security into all content with supplemental text



Where Teach?

- *Introduction to Business Ethics & Practical Security* – 1-hour course required all business majors
- *Continuing Education* – Course for community patrons
- *Freshman Orientation* – Practical computer security



Tips & Tools for Teaching Security

MPICT Educator Conference

Dr. Mark Ciampa

Author, Course Technology/Cengage Learning

Mark.ciampa@wku.edu