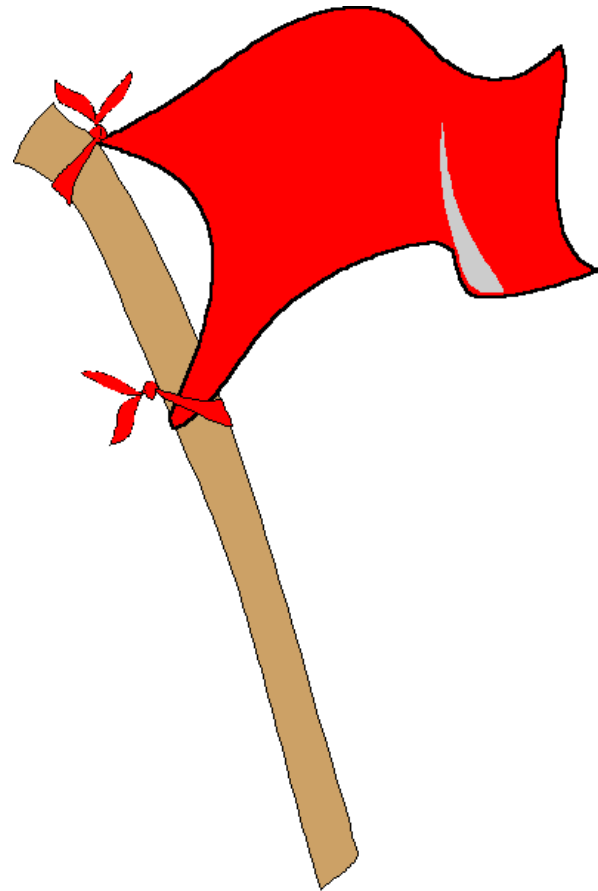


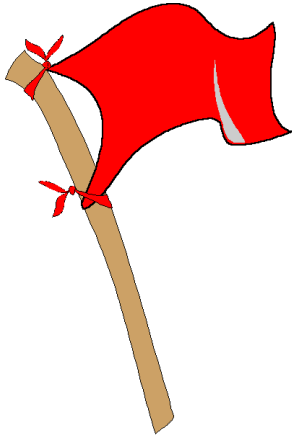
A Real-Time Information Warfare Exercise on a Virtual Network



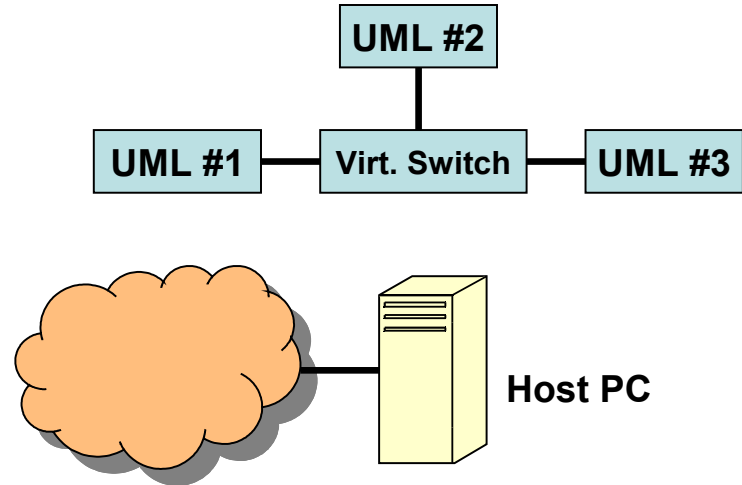
James Walden
Department of EECS
The University of Toledo

Topics

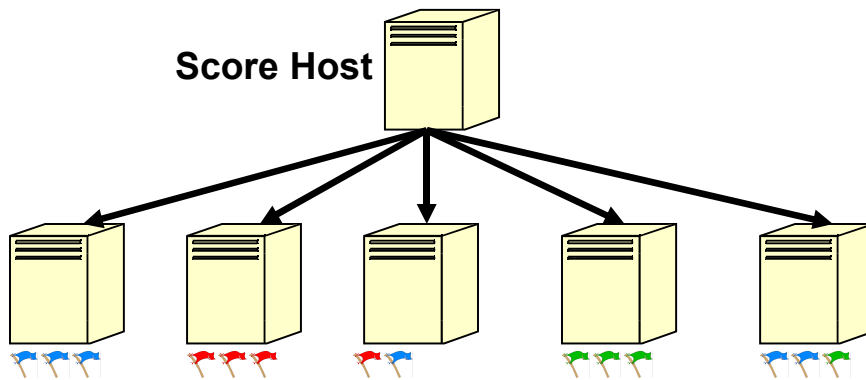
1. Capture the Flag



2. The Virtual Network

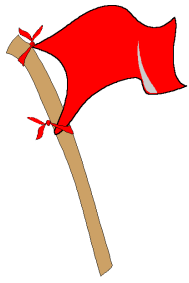


3. Implementation



4. Student Learning





Teaching information security can be a difficult task.

Need to balance theory and practice.

Security permeates many areas of technology:

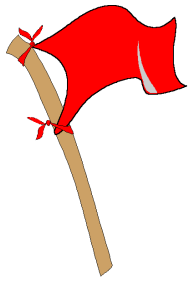
- Computer Architecture

- Operating Systems

- Networks

- Software development

Ethical issues.



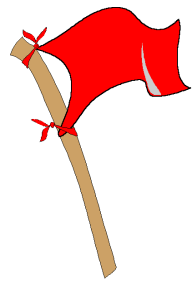
A capstone information warfare exercise offers students the opportunity to

Integrate theory and practice.

Assimilate learnings from different areas.

Experience security in a “real” environment.

Have fun.



In order to appreciate a capstone exercise, students need prior experience with

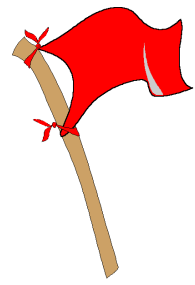
Security principles.

Ethical principles.

Application security techniques and tools.

Network security techniques and tools.

Vulnerability assessment.



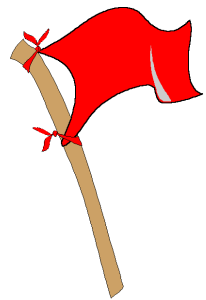
Why don't most courses offer such exercises?

Effort to setup.

Risk and liability.

Expense.

Effort to cleanup.



“Capture the Flag” is a team-based information warfare exercise.

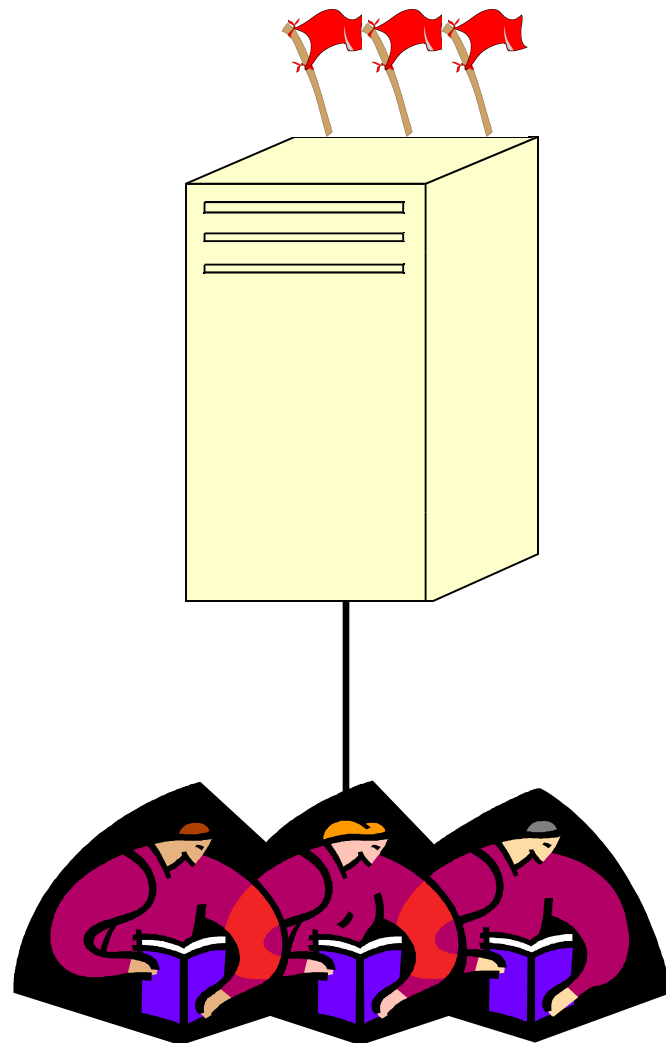
Capture means replacing opponent flag with your team’s flag.

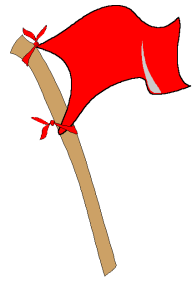
Multiple teams

Symmetric: offense/defense

One host per team

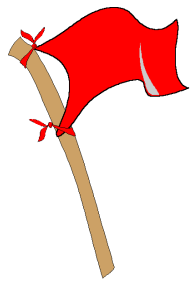
Multiple flags





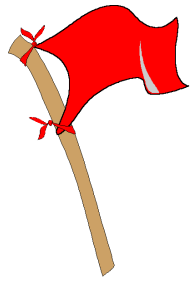
The Capture the Flag exercise was designed to give students experience in:

2. Securing a host as a team.
4. Management of a system under attack.
6. Attacker strategies and tactics.



While other types of information warfare exercises exist, only CTF satisfies all goals.

2. Red Team/Blue Team
4. Cyber Defense eXercise (CDX)
6. Treasure Hunt



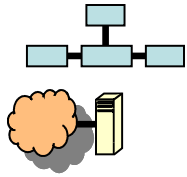
Why is it important to teach students attack strategies, techniques, and tools?

It's impossible to construct effective defenses if you don't understand what you're defending against.

It's difficult to understand the purpose of defenses without understanding the attacks they thwart.

Locksmiths know how to break lock security.

Key: ethics/legal education.



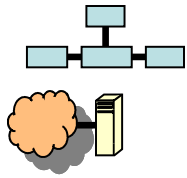
Security exercises require privileged access and may produce dangerous side effects.

Students need have root/admin access.

Privileged access may compromise network security.

Student mistakes can result in damage, ranging from denial of service to system compromises.

***Solution:* Isolate security exercises.**



Virtual machines provide an affordable, easy to administer environment for CTF.

Students can have root.

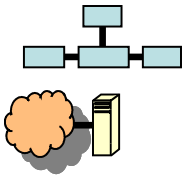
Affordable.

Easy to administer.

Performance.

No physical interface.

OS1	OS2	OS3
VM1	VM2	VM3
Host OS		
Hardware		



A wide variety of free and commercial virtual machine software is available.

Bochs

Plex86

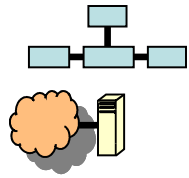
UML

VMware

VirtualPC

Xen

FreeBSD	Linux	Windows
VM1	VM2	VM3
Host OS		
x86 Hardware		

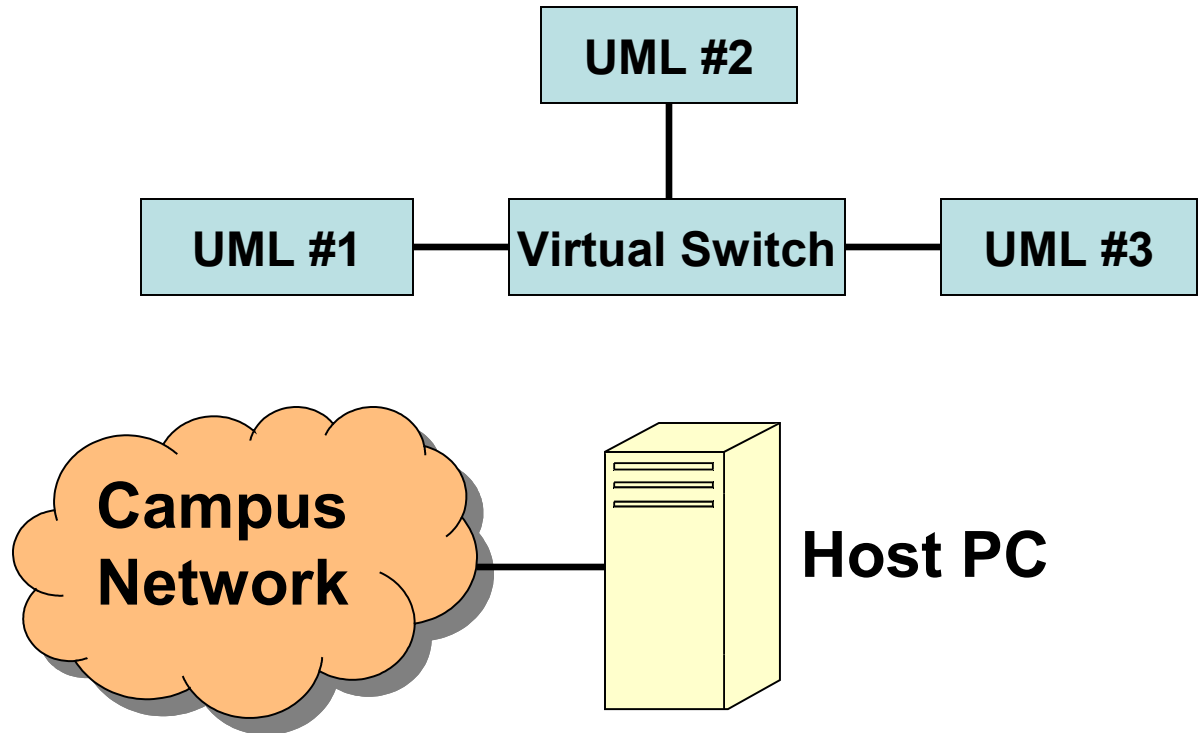


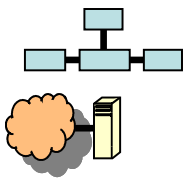
Virtual networking allows you to create a “just in time” isolated network for CTF.

UML Network Device

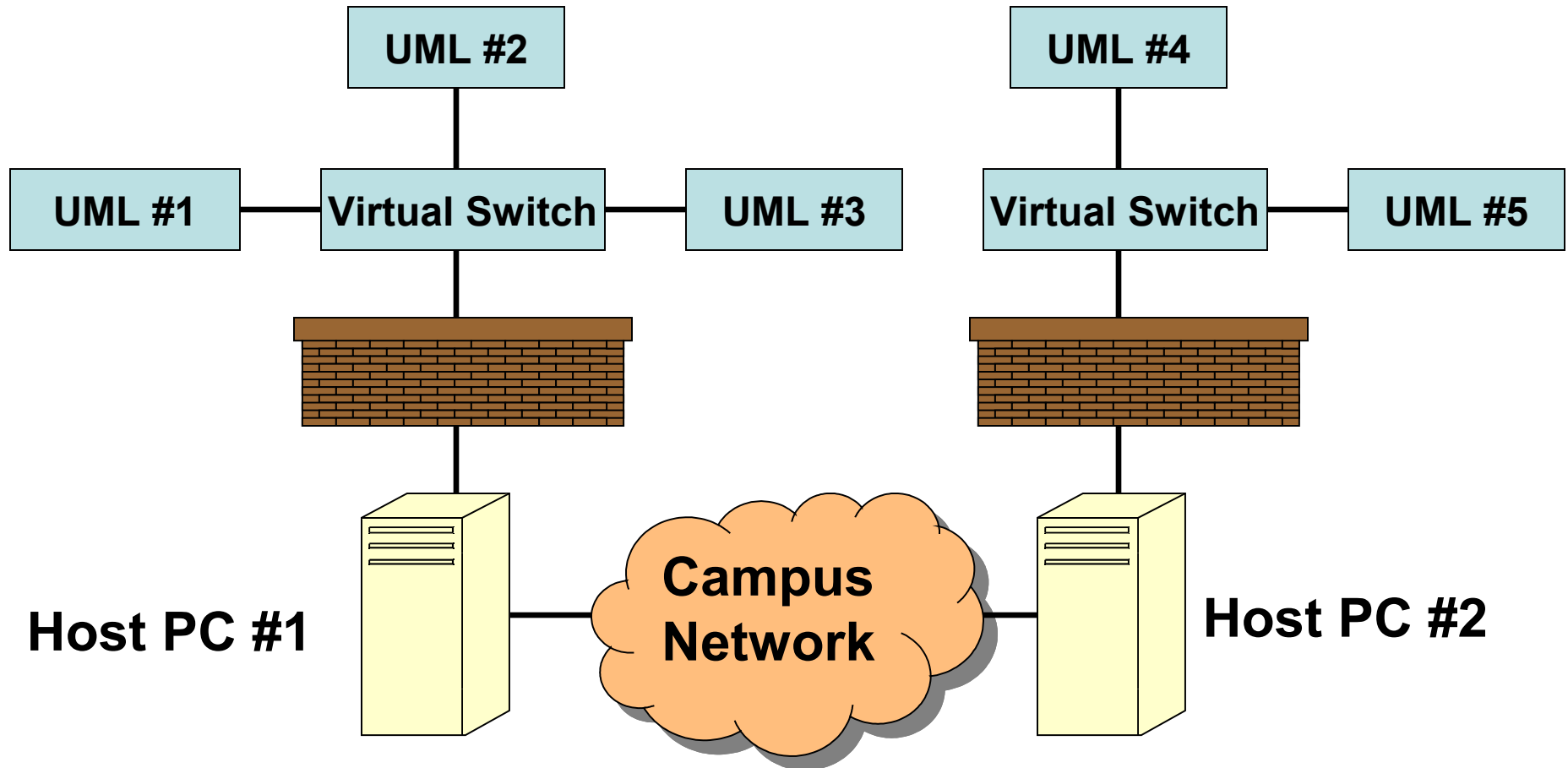
TUN/TAP Virtual Ethernet

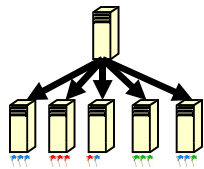
Bridge-utils





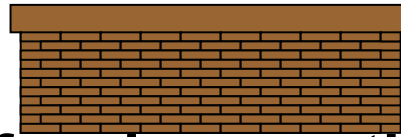
Virtual networks can span multiple physical hosts.





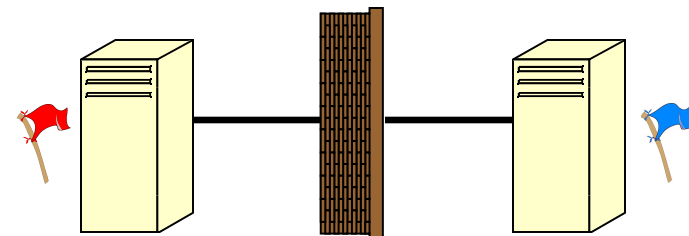
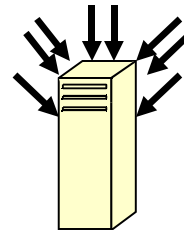
CTF was an 8 hour real-time exercise divided into two phases:

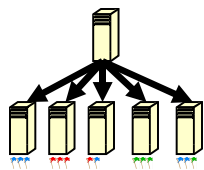
- 4. Defensive preparation.**
- 5. Offensive action and defensive reaction.**



The following actions were disallowed:

- Denial of service attacks.**
- Denying access to flags based on IPs.**





User-mode Linux is an open source VM, allowing you to run Linux VMs on x86 hosts.

Host OS: Fedora Core 2

VM OS: Redhat Linux 9.0

No security patches.

All services running.

Insecure accounts.

VM image is just a file.

Team1	Team2	Team3
UML1	UML2	UML3
Host Linux OS		
x86 Hardware		

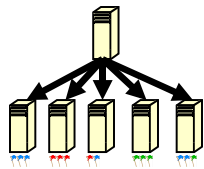


The scoring system was developed to fulfill the following requirements.

Automated: no human intervention required.

Generates reproducible results.

Encourages teams to maintain a set of services, simulating a production environment.

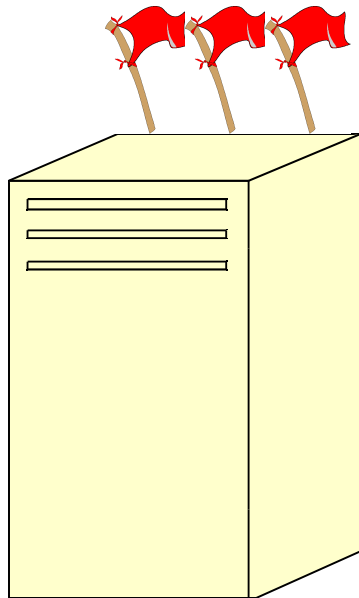


Teams were scored based on the number of services showing their flag.

4. HTTP (Apache web server)
5. SMTP (sendmail)
6. telnet

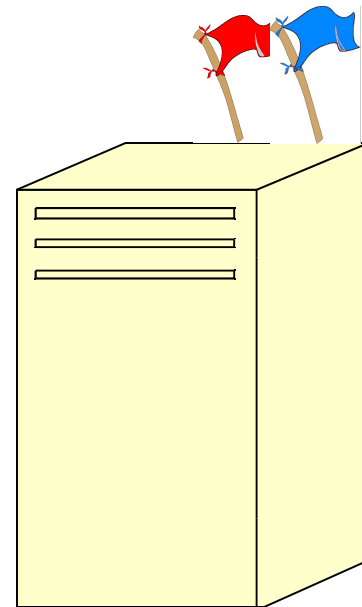
Initial State

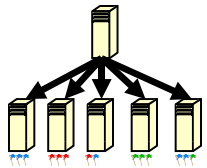
Red=3



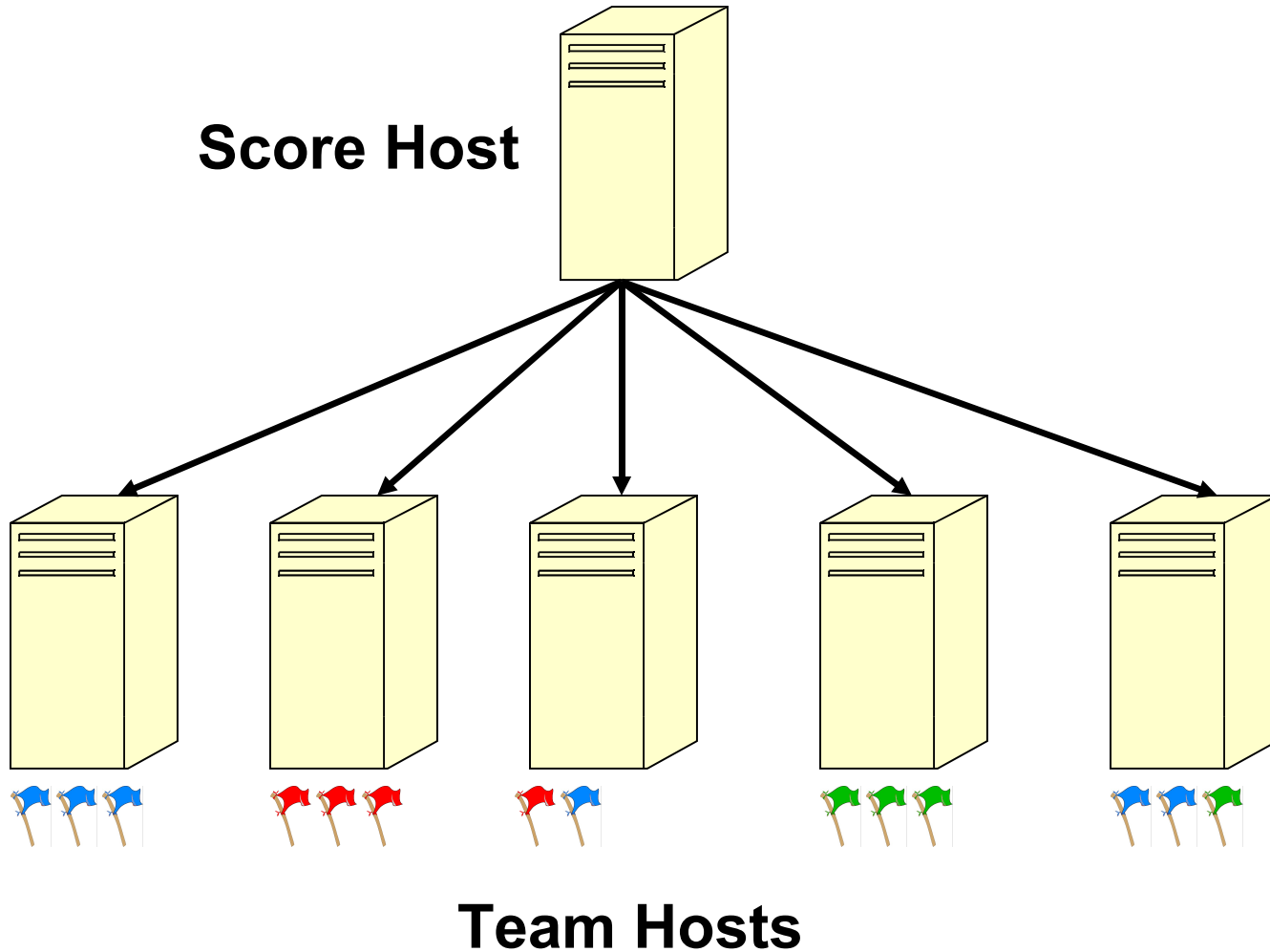
Example In-play State

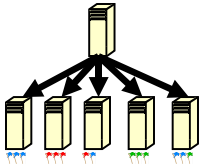
**Red=1
Blue=1**





The scoring system scans each team host for flags once every 10 minutes.





Flags were implemented by different modifications of each scored service.



HTTP: A CGI script was invoked with a filename argument. File contained flag.



SMTP: A FLAG command was added to sendmail daemon.



telnet: The login banner file, /etc/issue, contained the flag.

Flags require students to maintain specific services.



CTF serves as a capstone exercise in computer & network security. Students

Apply security principles.

Fail-safe Defaults

Least Privilege

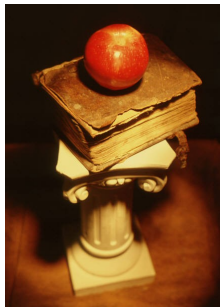
Separation of Privilege

Integrate practical experiences.

Firewalls and Intrusion Detection

Application security

Secure programming

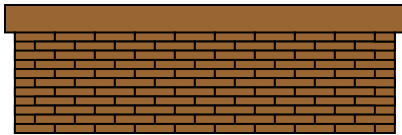


Students were required to write reports on their experience, explaining

- Defensive preparation: config, patches, tools;
- Defenses deployed as a reaction to attacks;
- Attack process, including reconnaissance activities;
- Attacks attempted against other teams;
- A retrospective analysis of their efforts, examining what they could have done better.



Students used a wide variety of tools and techniques during the exercise.

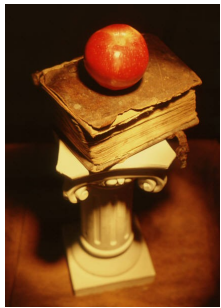


Defensive Techniques

- Applying patches
- Backups
- Configuration changes
- Firewall
- Intrusion detection
- Custom software

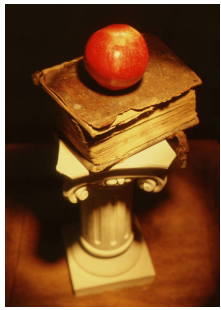
Offensive Techniques

- Automatic exploits
- Default passwords
- Network sniffing (ethereal)
- Rootkits (adore)
- Social engineering
- Custom software



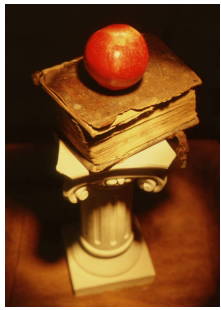
Students reports included a variety of different techniques and recognition of mistakes made during the exercise.

- Good analyses of their application of security principles.
- Several teams wrote custom software, including
 - Shell wrapper
 - Flag status (self-scoring)
 - Flag setter (offensive)
- In their retrospective analyses, students demonstrated a great deal of insight into their mistakes and how they could have improved their performance.



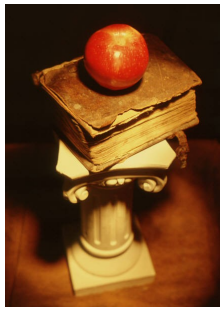
Students reports demonstrated both enthusiasm and learning.

“Capture the Flag was fun, in a mentally exhausting way that I really wasn’t expecting. While our defense made progress the entire time, offense was frustrating for the first 5 or 6 hours, but when things started to make sense and we began to get into other machines, it was a rush. It takes weeks of lectures and applies them all at once, which is a great experience.”

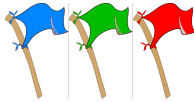


Lessons Learned

- Use a smaller number of VMs per PC for CTF teams than you would for network servers.
- Defense is easier than offense:
 - Gaining root access is difficult, even on an older Linux distribution.
 - Students need to be prepared to use multiple part exploits with privilege escalation components.
- Students need more system administration experience before the exercise.



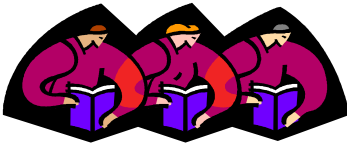
Future Directions: Fixing Problems



New flags, requiring more invasive access to each team's system, to balance the exercise.

Flags that require authenticated access.

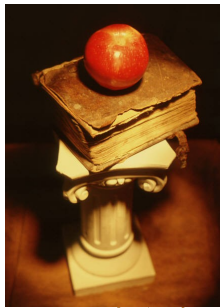
Flags that transfer files to/from score server.



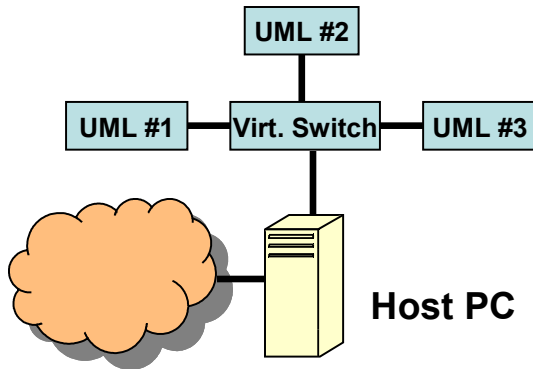
More preparation exercises to improve student security knowledge.

Applying security patches and configuration.

Password cracking.



Future Directions: Improving Simulation



Better network simulation

Virtual network for each team.

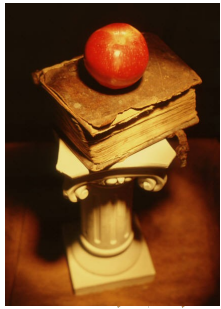
Add non-team servers to network.

Inject network traffic.

Team1	Team2	Team3
VM1	VM2	VM3
Host OS		
x86 Hardware		

Multiple operating systems.

Use multi-OS VM like Xen or VMware.

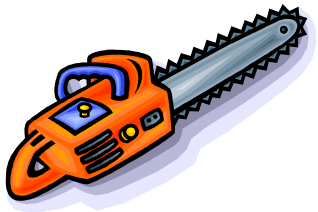


Future Directions: Improving Student Work

Encourage development of original tools.

Offer bonus to exercise grade.

Encourage tool creation in earlier assignments.



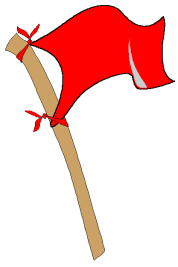
Standardize report formats.

Planned incident response procedures.

Create attack template.

Require captured packets/transcripts.





Conclusions

“Capture the Flag” is a symmetric multi-team exercise, offering students opportunity for offense and defense.

A capstone information warfare exercise offers students the opportunity to integrate their understanding of security theory and practice.

Conducting the exercise on a virtual network obviates the requirement for a dedicated, isolated network lab.

The scoring system can enforce requirements automatically, making the exercise easier to conduct and evaluate.