

First Experiences with DETER Testbed

Dr. Xiao Su

Computer Engineering

San Jose State University

<http://www.sjsu.edu/people/xiao.su>

Agenda

2

- ❑ **Prior experience with PlanetLab**
 - Setup
 - Challenges in using PlanetLab in security research/education
- ❑ **DETER Testbed**
 - Overview
 - Setting up DETER experiments
 - Running DETER experiments
- ❑ **Demo**

Our Network Security Class

3

- ❑ **How attackers think and work?**
 - Attack phases

- ❑ **What are the tools and algorithms to counter such attacks?**
 - Crypto tools
 - Authentication
 - Access control
 - Key distribution

Experimental Setups

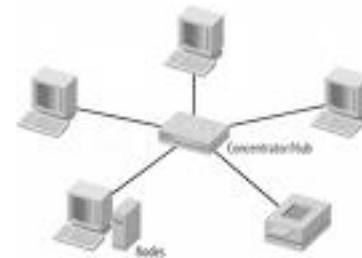
4

- ❑ **Personal computer**



- ❑ **Local testbed**

- Isolated from campus networks



- ❑ **Internet scale testbed**



Challenges in Teaching Network Attacks

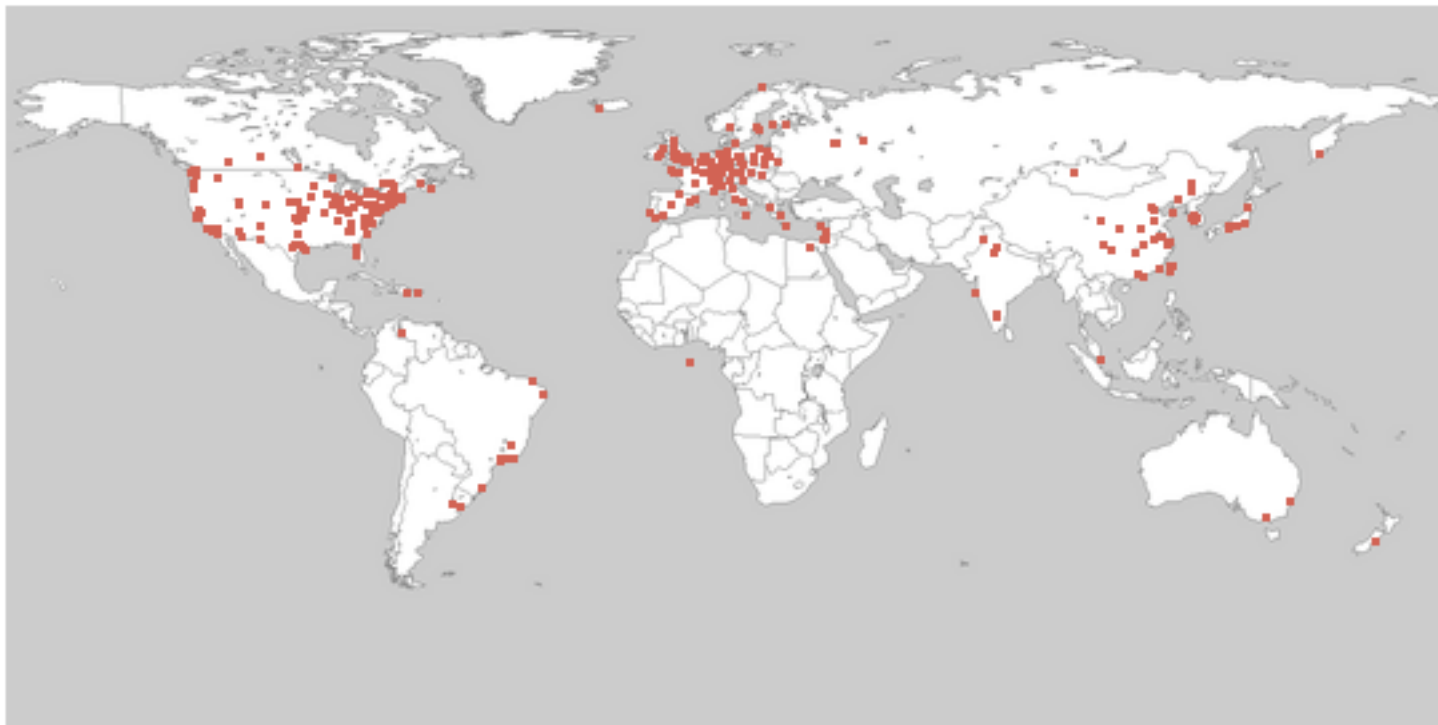


SAN JOSÉ STATE
UNIVERSITY

5

- ❑ **Many tools need admin privilege**
 - Sniffing, spoofing, MIM,...
- ❑ **Attacking experiments hard to set up**
 - Not interfering with normal network operations
 - Contained in a closed network
 - Some experiments heavily depend on compiler, OS types (e.g., buffer overflow)
- ❑ **Hard to conduct security experiments in the Internet scale?**
 - Evaluate how effective anti-DDoS schemes are?
- ❑ **Need to use Internet scale testbed!!**

Internet Scale Testbed - PlanetLab



Picture taken from <http://www.planet-lab.org>

□ **1127 nodes at 544 sites (as of June 18, 2012)**

NSF TRUST WISE 2012

Running Services in PlanetLab

- ❑ **First, create a slice (by PI only)**
 - UNIX shell access to a set of PlanetLab nodes
 - virtual machines
 - Faults or misbehaviors can be isolated and traced back to virtual machines
- ❑ **Create public/private key pair (by users)**
- ❑ **Upload public key to PlanetLab (by users)**
- ❑ **Remote access machines using ssh with slice name as the user name**
- ❑ **Install packages, deploy and run services**

Why Not PlanetLab in Security Experiments



SAN JOSÉ STATE
UNIVERSITY

- ❑ **PlanetLab nodes are part of the Internet**
 - Traffic impact the Internet: what happens when you experiment DoS on PlanetLab?
 - The testbed is closely monitored by a team of professionals, for network attacks, worm propagation, copyright infringement, and other malicious traffic.
- ❑ **PlanetLab nodes run uniform Linux-based OS**
 - Not possible if experiments require different types of OS
 - OS and network configurations on PlanetLab nodes are not customizable
- ❑ **Operational concerns**
 - Nodes in the same experiment (slices) don't share home directories: lots of ssh copies
 - A good percentage of nodes not accessible by ssh, due to different ssh policies and versions

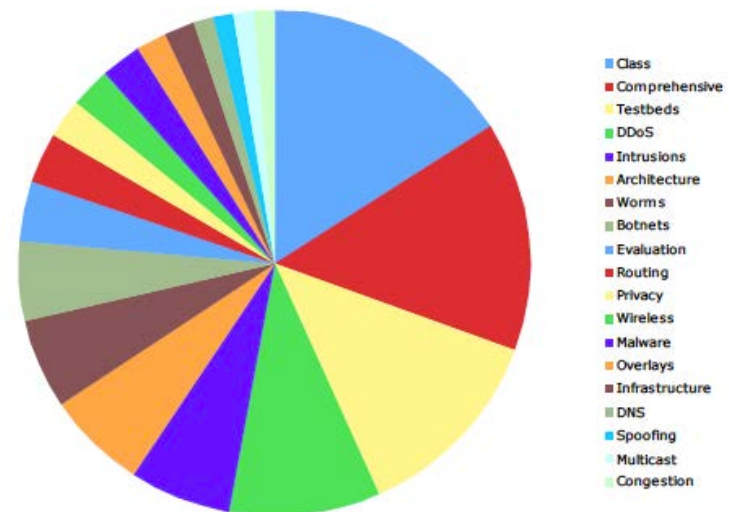
Here We Have DETER

9

Where is DETER Used?



Types of DETER Projects



- ❑ **DETER is a public testbed to run repeatable security experiments**
 - Based on Univ. of Utah's Emulab
 - Specially enhanced for security research/education
 - Jointly run by USC's ISI and UC Berkeley

PlanetLab vs. DETER

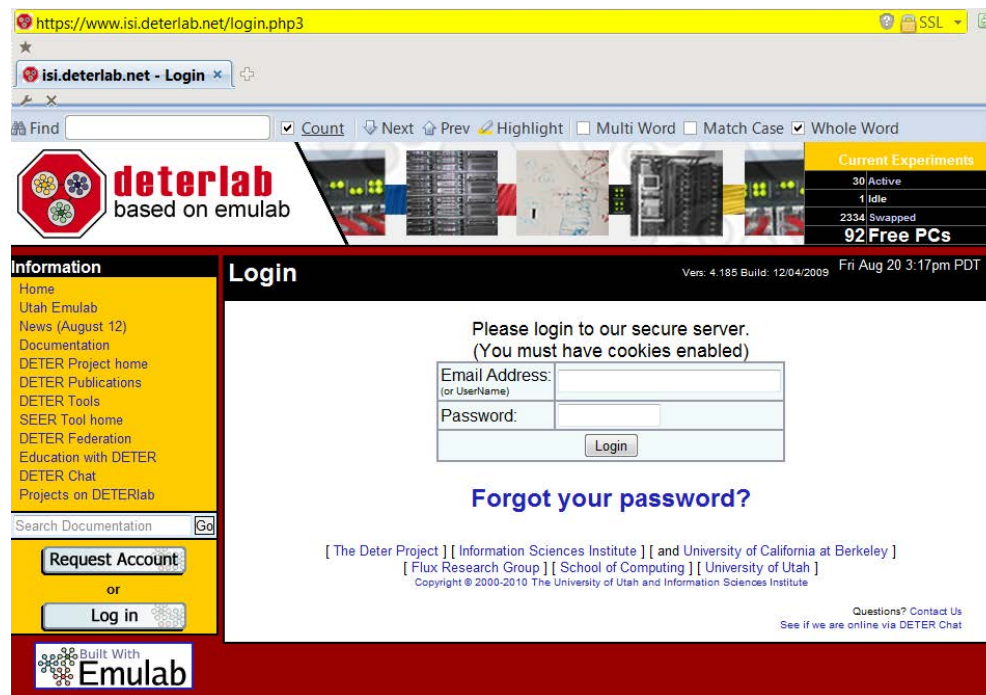
10

	PlanetLab	DETER
Isolated or Open Network	Part of the Open Internet	Isolated Testbed
OS Uniformity	Only runs Linux OS (FC based)	Supports a large list of OS types
OS Customization	Not possible	Supports customized OS images
Network Configuration	Static, part of the Internet	Supports configuration of network, defined by NS scripts
Home directory	Different nodes have different home directories	Same home directory for all nodes
User Management	Site PI's task	DETER support

Accessing DETER Testbed

11


- Login to <https://www.isi.deterlab.net/login.php3>



The screenshot shows a web browser window displaying the login page for the DETERlab testbed. The browser's address bar shows the URL <https://www.isi.deterlab.net/login.php3>. The page features a navigation menu on the left with links such as Home, Utah Emulab, News, Documentation, and DETER Project home. The main content area is titled "Login" and contains a form with fields for "Email Address (or UserName)" and "Password", along with a "Login" button. A message above the form reads: "Please login to our secure server. (You must have cookies enabled)". Below the form, there is a link for "Forgot your password?". The footer includes copyright information for The Deter Project, Information Sciences Institute, and the University of California at Berkeley, along with contact information and a link to the DETER Chat.

DETER Experiments

12

lab | Logout | News [New!](#) | Contact Us **166 Free PCs**
1 PCs reloading
40 active users
35 active expts. 

News:

DETER Chat (IRC) no longer official support medium (2011-04-14)

Web Login by email address is no longer supported. (2011-03-23)

CSET'11 Call for Papers (2011-02-07)

[Full news stories](#)

Scheduled downtime: **Wednesdays: 5PM-7PM, Saturdays: 10AM-1PM Pacific Time.**

[Experiments](#)

[Projects](#)

[Profile](#)

Current Experiments

PID	EID	State	Nodes [1]	Hours Idle [2]	Description
SJSUCMPE209	BufferOverflow1004	swapped	1		Single node buffer overflow experiments on Ubuntu 10.04
SJSUCMPE209	SampleExp	swapped	3		To experiment with buffer overflow on Ubuntu 8.04
SJSUCMPE209	switchf2009	swapped	4		Experimenting with Active Sniffing
SJSUCMPE209	synflood	swapped	5		TCP SYN flooding attack

1. Node counts in **green** show a rough estimate of the minimum number of nodes required to swap in. They account for delay nodes, but not for node types, etc.
2. A ? indicates that the data is stale, and at least one node in the experiment has not reported on its proper schedule.

Beginning a New DETER Experiment

13



My DETERlab | Logout | News | Contact Us | Search Documentation | 166 Free PCs | 2 PCs reloading | 40 active users | 34 active expts. | Built With Emulab

My DETERlab

- My DETERlab
- Begin an Experiment
- Begin a Risky Experiment
- Experiment List
- Node Status
- List ImageIDs
- List OSIDs
- Start New Project
- Join Existing Project

News:

- DETER Chat (IRC) no longer official support medium (2011-04-14)
- Web Login by email address is no longer supported. (2011-03-23)
- CSET'11 Call for Papers (2011-02-07)

Full news stories

Scheduled downtime: Wednesdays: 5PM-7PM, Saturdays: 10AM-1PM Pacific Time.

Experiments | Projects | Profile

Current Experiments

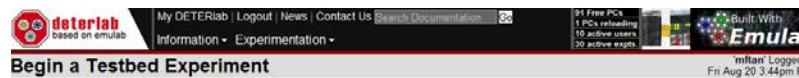
□ Parameters to fill in

- Name of your experiment
- Description of your experiment
- Your NS file to specify a network topology
 - Don't know NS? Use the GUI editor!

Beginning a New DETER Experiment

14

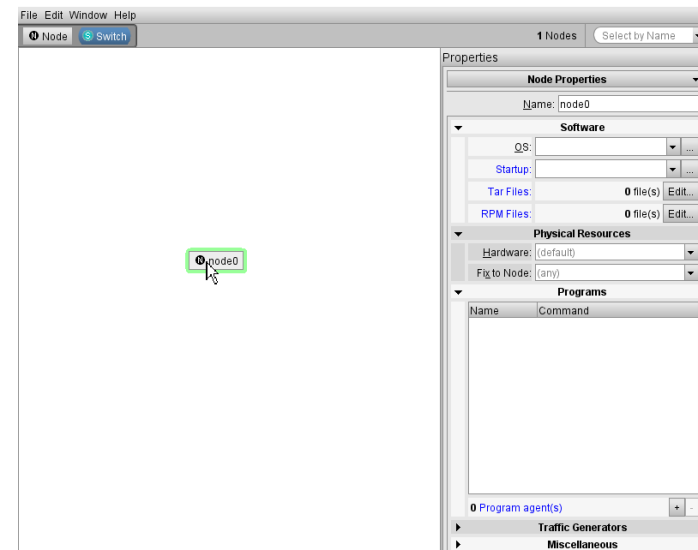
□ Beginning experiment page



- If you have an NS file:
You may want to [syntax check it first](#)
- If you **do not** have an NS file:
[New GUI editor](#) An enhanced Java applet for editing topologies.
- For manipulating your experiment, consider [SEER](#).

Select Project:	SJSUCMPE209
Group:	Default Group (Must be default or correspond to selected project)
Name: (No blanks)	<input type="text"/>
Description: (A concise sentence)	<input type="text"/>
Your NS file:	Upload (500k max) <input type="text"/> <input type="button" value="Browse..."/> or On Server <input type="text"/> (/group, /admin, /groups)
Swapping:	<input checked="" type="checkbox"/> Idle-Swap: Swap out this experiment after 4 hours idle. If not, why not? <input type="text"/> <input checked="" type="checkbox"/> Max. Duration: Swap out after 24 hours, even if not idle.
Linktest Option:	Skip Linktest (What is this?)
<input type="checkbox"/> Do Not Swap In	<input type="button" value="Submit"/>

□ This is how a GUI editor looks like

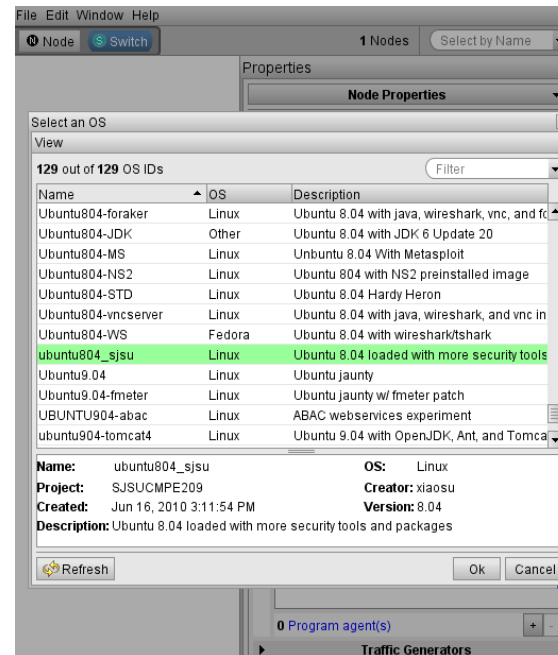
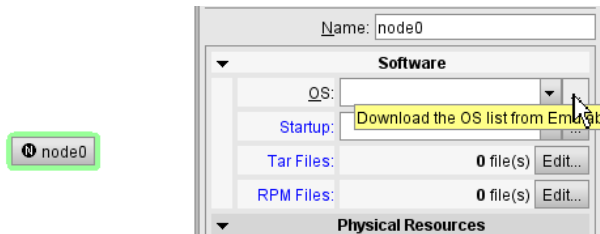


Configuring OS and Network Settings



❑ Configuring OS

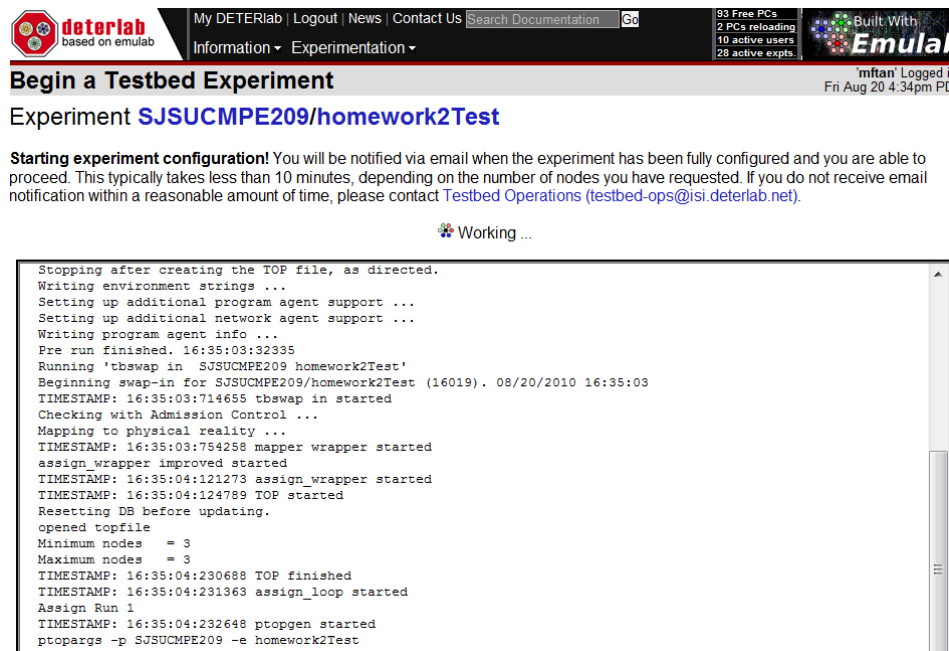
❑ List of supported OS



Next Step: Swap Your Experiment In

16

- ❑ Be patient, may take sometime



deterlab based on emulab

My DETERlab | Logout | News | Contact Us | Search Documentation | Go

93 Free PCs
2 PCs reloading
10 active users
28 active expts.

Built With
Emulab

infan Logged in
Fri Aug 20 4:34pm PC

Begin a Testbed Experiment

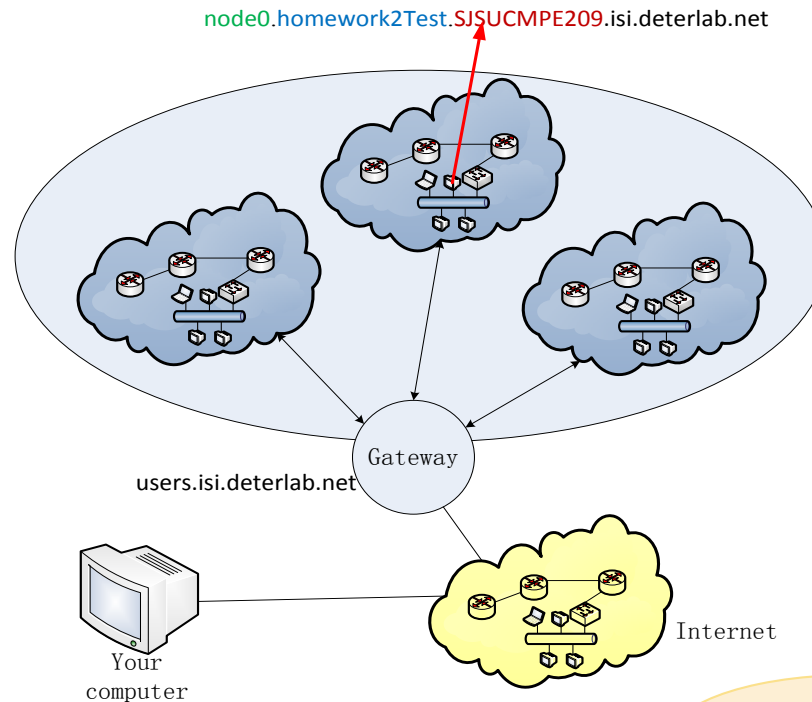
Experiment [SJSUCMPE209/homework2Test](#)

Starting experiment configuration! You will be notified via email when the experiment has been fully configured and you are able to proceed. This typically takes less than 10 minutes, depending on the number of nodes you have requested. If you do not receive email notification within a reasonable amount of time, please contact [Testbed Operations \(testbed-ops@isi.deterlab.net\)](mailto:testbed-ops@isi.deterlab.net).

Working ...

```
Stopping after creating the TOP file, as directed.
Writing environment strings ...
Setting up additional program agent support ...
Setting up additional network agent support ...
Writing program agent info ...
Pre run finished. 16:35:03:32335
Running 'tbswap in SJSUCMPE209 homework2Test'
Beginning swap-in for SJSUCMPE209/homework2Test (16019). 08/20/2010 16:35:03
TIMESTAMP: 16:35:03:714655 tbswap in started
Checking with Admission Control ...
Mapping to physical reality ...
TIMESTAMP: 16:35:03:754258 mapper wrapper started
assign_wrapper improved started
TIMESTAMP: 16:35:04:121273 assign_wrapper started
TIMESTAMP: 16:35:04:124789 TOP started
Resetting DB before updating.
opened topfile
Minimum nodes = 3
Maximum nodes = 3
TIMESTAMP: 16:35:04:230688 TOP finished
TIMESTAMP: 16:35:04:231363 assign_loop started
Assign Run 1
TIMESTAMP: 16:35:04:232648 ptopgen started
ptopargs -p SJSUCMPE209 -e homework2Test
```


Accessing Nodes in Your Experiment



❑ First log into the gateway node

- ssh users.isi.deterlab.net

❑ On gateway, accessing your nodes by

- ssh node0.homework2Test.SJSUCMPE209.isi.deterlab.net

Experiment
name

Project
name

Cleaning Up

18

- ❑ **Swapping out your experiment**
- ❑ **Terminating an experiment**

How Did We Use DETER in Our Class

19

□ We used DETER

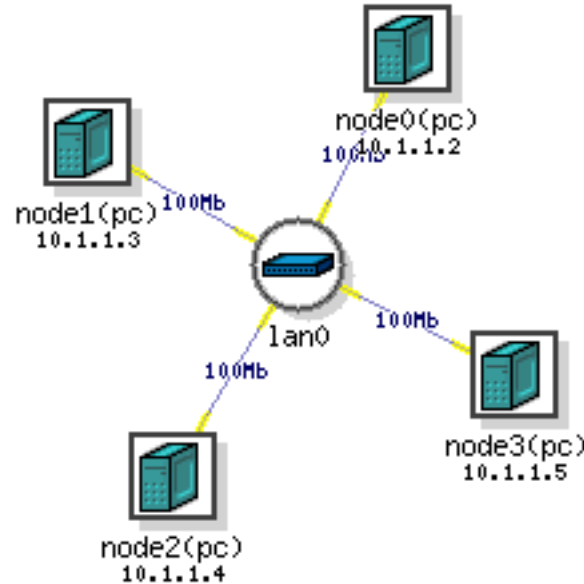
- In-class demos
- Assignments
 - Buffer overflow (Ubuntu 8.04LTS, gcc 3.x) – This combination of gcc compiler and OS version is hard to find now
 - TCP SYN flooding – Not possible on regular lab environments
 - Man-in-the-middle attack

Man-in-the-Middle Experiment on DETER



❑ Network configuration

- 4 nodes interconnected using a switch
- 3 nodes running Ubuntu 8.04LTS, and 1 node running Ubuntu 10.04



Can Node0 Sniff Other Nodes' Packets?



SAN JOSÉ STATE
UNIVERSITY

21

❑ Logging into Node0 in the experiment

```
Macintosh-6:~ xsu$ ssh -l xiaosu users.isi.deterlab.net
```

```
Password:
```

```
Last login: Fri Apr 29 14:29:50 2011 from x130-65-152-108
```

```
> ssh node0.switchf2009.sjsucmpe209
```

```
Linux node0.switchf2009.sjsucmpe209.isi.deterlab.net 2.6.24-23-deter #4 SMP
```

```
Wed Jan 21 23:15:52 MST 2009 i686
```

```
node0:~>
```

Can Node0 Sniff Other Nodes' Packets?



22

Starting ettercap

```
Macintosh-6:~ xsu$ sudo ettercap -C
```

```
File Sniff Options Help NG-0.7.3
Unified sniffing... U
Bridged sniffing... B
-
Set pcap filter... p
```

```
File Sniff Options Help NG-0.7.3

Network interface : eth13

NSF TRUST WISE 2012
```

Can Node0 Sniff Other Nodes' Packets?



SAN JOSÉ STATE
UNIVERSITY

23

□ Scan for hosts

```
Start Targets Hosts View Mitm Filters Logging Plugins Help NG-0.7.3
Hosts list...
10.1.1.3 00:15:17:57:C3:4E
10.1.1.4 00:15:17:57:C7:D6
10.1.1.5 00:15:17:57:C3:A2

User messages:
1698 tcp OS fingerprint
2183 known services
Randomizing 255 hosts for scanning...
Scanning the whole netmask for 255 hosts...
3 hosts added to the hosts list...
```



Can Node0 Sniff Other Nodes' Packets?

24

- ❑ Start sniffing
- ❑ Generate packets from node1 to node2

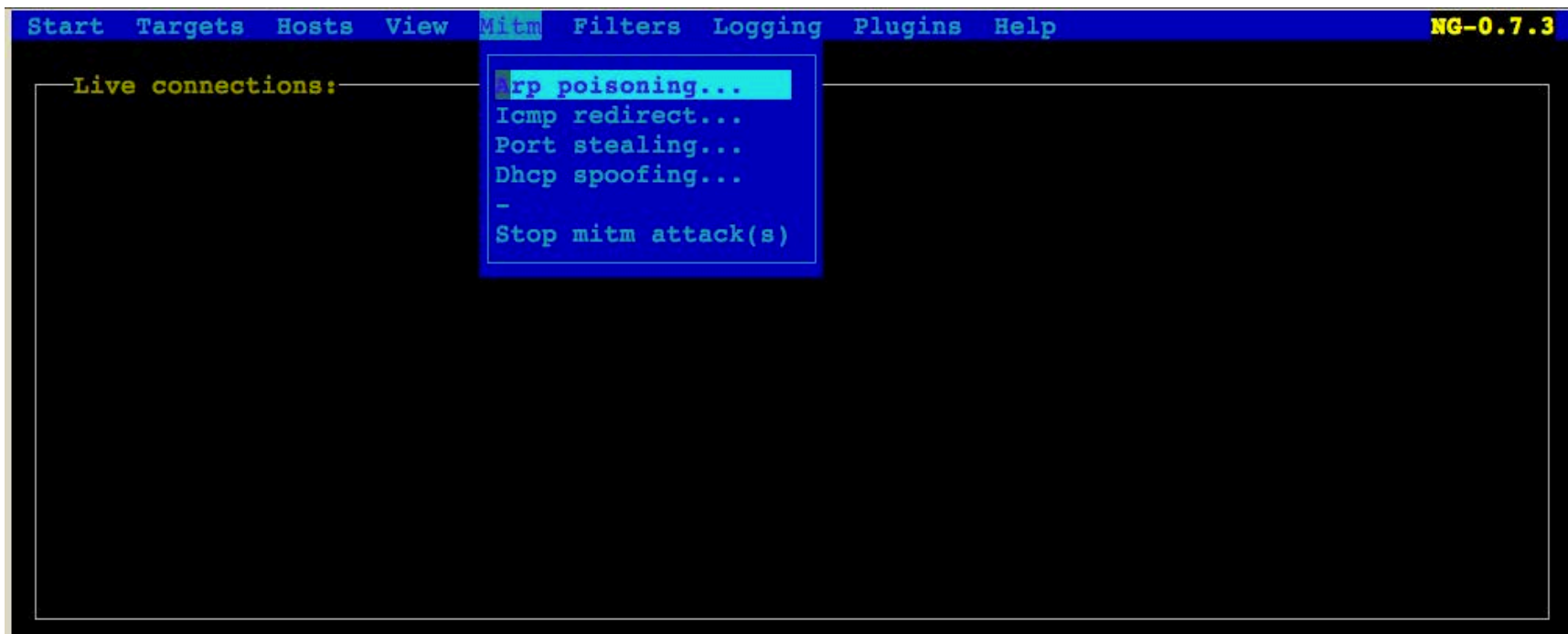
```
Start Targets Hosts View Mitm Filters Logging Plugins Help NG-0.7.3
Start sniffing C-w
Stop sniffing C-e
-
Exit C-x
15:17:57:C3:4E
15:17:57:C7:D6
15:17:57:C3:A2
```

node1:~> nc node2 54321
1st try: can you see me?

node2:~> nc -l -p 54321
1st try: can you see me?

Now Enabling ARP Poisoning

25



What Will Happen Next?

26

❑ Sending something from node1 to node2

```
node1:~> nc node2 54321  
1st try: can you see me?  
2nd try: can you see me?
```

```
node2:~> nc -l -p 54321  
1st try: can you see me?  
2nd try: can you see me?
```

```
Start Targets Hosts View Mitm Filters Logging Plugins Help NG-0.7.3  
  
Connection data  
10.1.1.3:42720  
2nd try: can you see me?  
  
10.1.1.4:54321  
  
NSF TRUST WISE 2012
```

Modifying Packet

27

❑ Step 1: defining a filter

- What does the filter do?

```
node2:~> cat ASniffing/ch.filter  
# change TCP payload  
if (tcp.dst == 54321 && search(DATA.data, "install")) {  
    replace("install", "upgrade");  
}
```

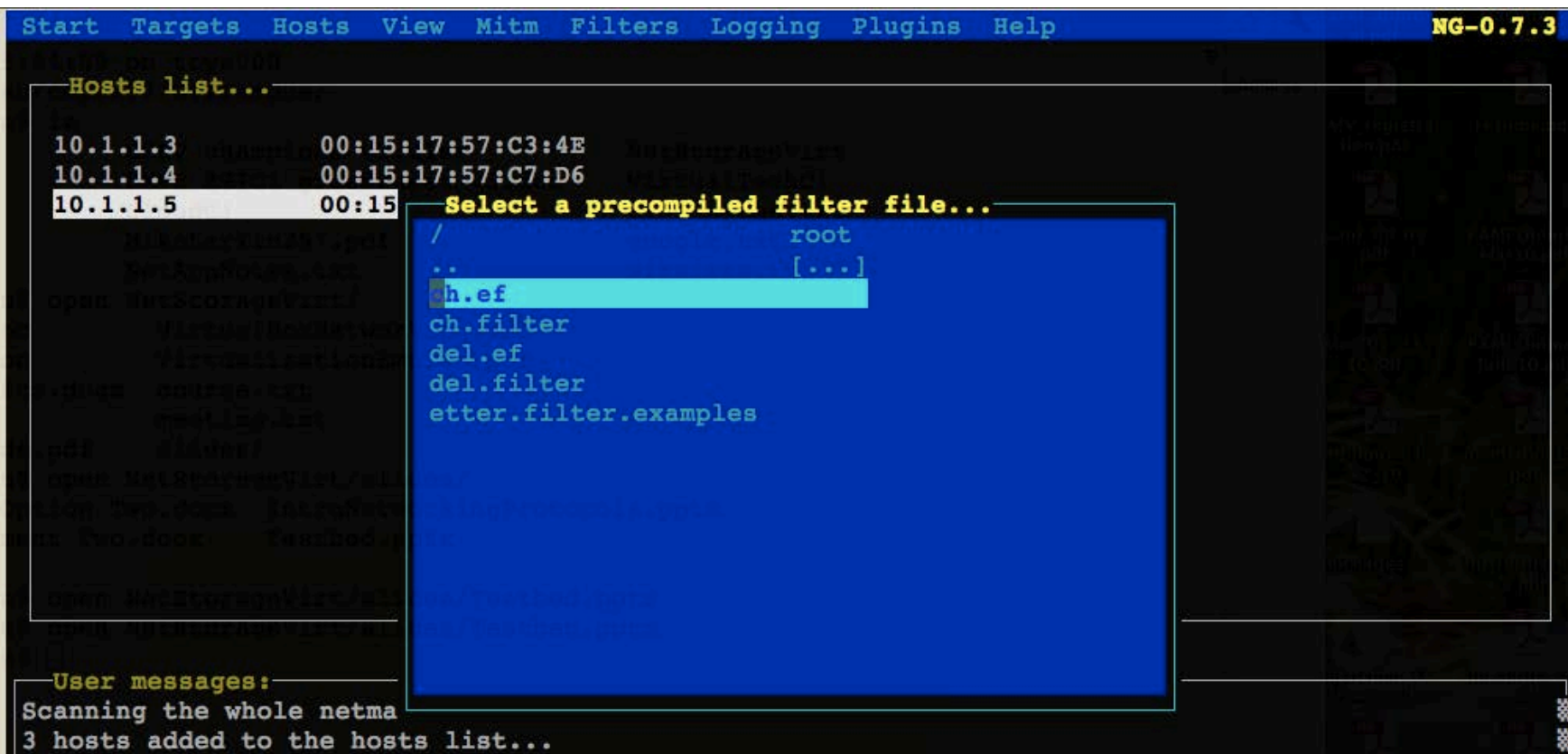
❑ Step 2: compiling the filter

```
node2:~/ASniffing> etterfilter -o ch.ef ch.filter
```

Modifying the Packet

28

Step 3: load the filter



The screenshot shows a terminal window with a blue header bar containing the menu: Start Targets Hosts View Mitm Filters Logging Plugins Help and the version number NG-0.7.3. The main area is divided into several sections. On the left, a 'Hosts list...' window shows a table with IP addresses and MAC addresses. The IP 10.1.1.5 is highlighted. In the center, a 'Select a precompiled filter file...' dialog box is open, listing several filter files: / root, .. [...], h.ef (highlighted), ch.filter, del.ef, del.filter, and etter.filter.examples. At the bottom left, a 'User messages:' section displays the text: 'Scanning the whole netma' and '3 hosts added to the hosts list...'. The background of the terminal is dark with some faint, illegible text.

```
Start Targets Hosts View Mitm Filters Logging Plugins Help NG-0.7.3

Hosts list...
10.1.1.3      00:15:17:57:C3:4E
10.1.1.4      00:15:17:57:C7:D6
10.1.1.5      00:15:17:57:C7:D6

Select a precompiled filter file...
/ root
.. [...]
h.ef
ch.filter
del.ef
del.filter
etter.filter.examples

User messages:
Scanning the whole netma
3 hosts added to the hosts list...
```

Will Packets Be Modified?

29

- ❑ Packets sent and received, after loading the filter

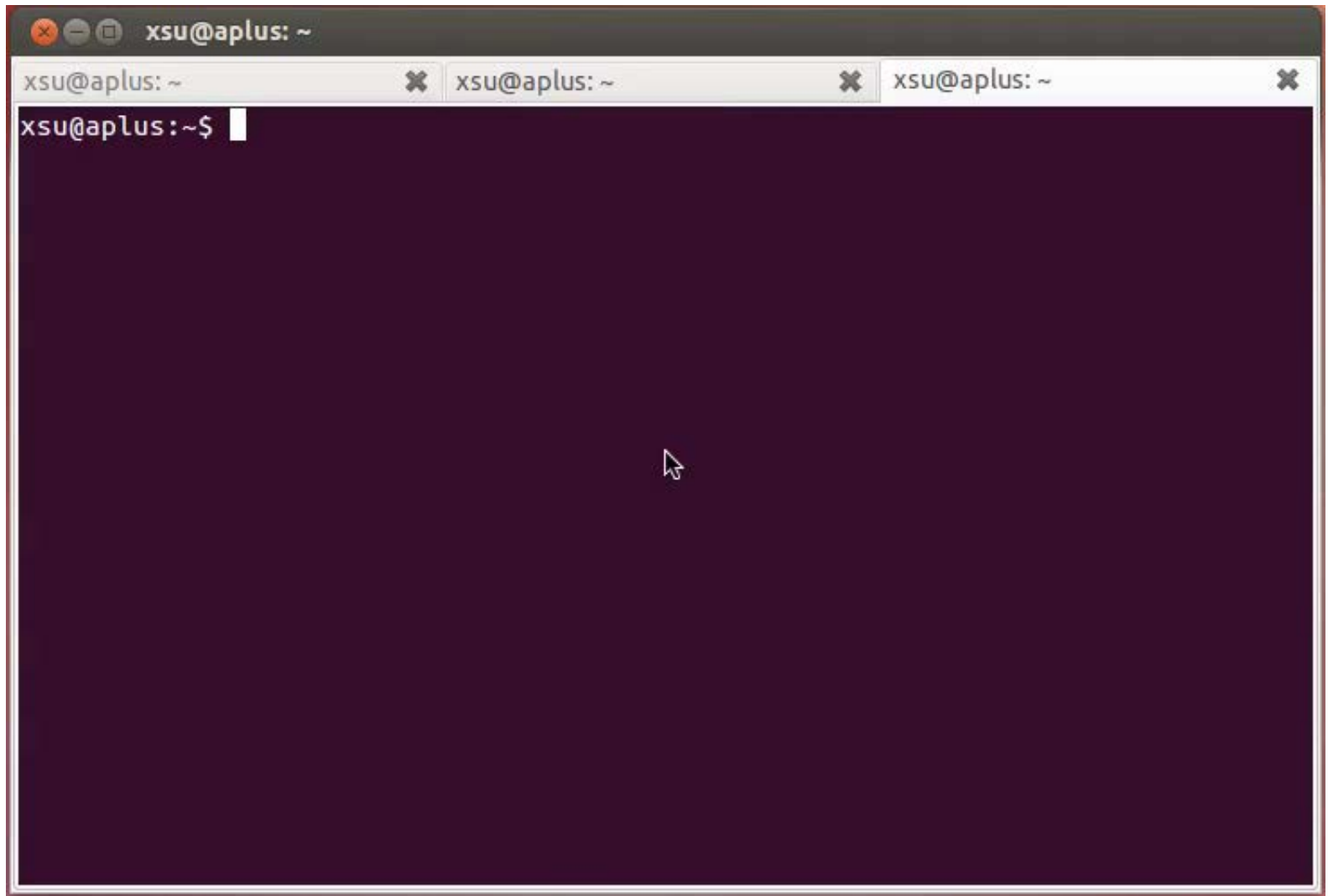
```
node1:~> nc node2 54321  
1st try: can you see me?  
2nd try: can you see me?  
apt-get install gcc4
```

```
node2:~> nc -l -p 54321  
1st try: can you see me?  
2nd try: can you see me?  
apt-get upgrade gcc4
```

DEMO Video

30

- ❑ **Video capturing the above experiments**
 - Sniffing without arp spoofing
 - Sniffing with arp spoofing enabled
 - Sniffing with arp spoofing enabled and filter loaded to modify packet



Questions?