

War Games

An Exercise in Ethical Cracking

Greg Travis

greg@indiana.edu

Associate Director,
Advanced Network Management Laboratory
Indiana University

Management Service Description

David A. J. Ripley

daripley@indiana.edu

Lead Network Security Developer,
Advanced Network Management Laboratory
Indiana University

Network security infrastructure development

Who are we

Networking laboratory on a “five year mis

Soft-money funded

- To explore strange new anomalies
- To seek out new protocols
- To boldly present at every venue we can

What do we c

“Networky” stuff

- Fast file transfer protocols (e.g. Tsunami)
- Last-mile issues (e.g. L2QP)
- Porcupine/Warscope

Security stuff

- Forensics (SEBEK, Walleye, Honeynets)

What's going to happen this afternoon

We're going to have a workshop

- Relatively free-format
- Break into teams (due to resource limits)
- We'll act as proctors/supervisors/advisors/agents provocateurs

What will we be able to accomplish?

Demonstrate some methods of initiating system compromise

- Buffer overflow
- Synchronization
- Etc.

Demonstrate the relative ease with which these exploits can be obtained and used

- Little skill needed! (For certain values of “little”)

How hard can i

We're here to discuss network security (and other things)

- But how hard *is* it to break into someone else's system?
- How hard is it to stop someone from getting in to your system?
- How hard is it to get them out once they're in?
- Can you ever trust that machine again?

Playtime

We're going to give you the chance to connect to someone else's machine

- The only catch - they're trying to compromise yours.

No-one is going to get into any trouble. Here's why:

- Controlled, isolated environment.

Your Situation

You have a normal, unprivileged account on

You know there are other machines on the network
you're hungry for computing resources.

You think perhaps the administrator of the machine
you use is some kind of super-user

- You suspect he's got code that will enable you to gain access to other machines on the network

Your Mission

Your Mission:

- Gain root access on your own machine.
- Find the remote exploit code (*where could it be?*)
- Gain access to as many other machines on the LAN as you can

For bonus points:

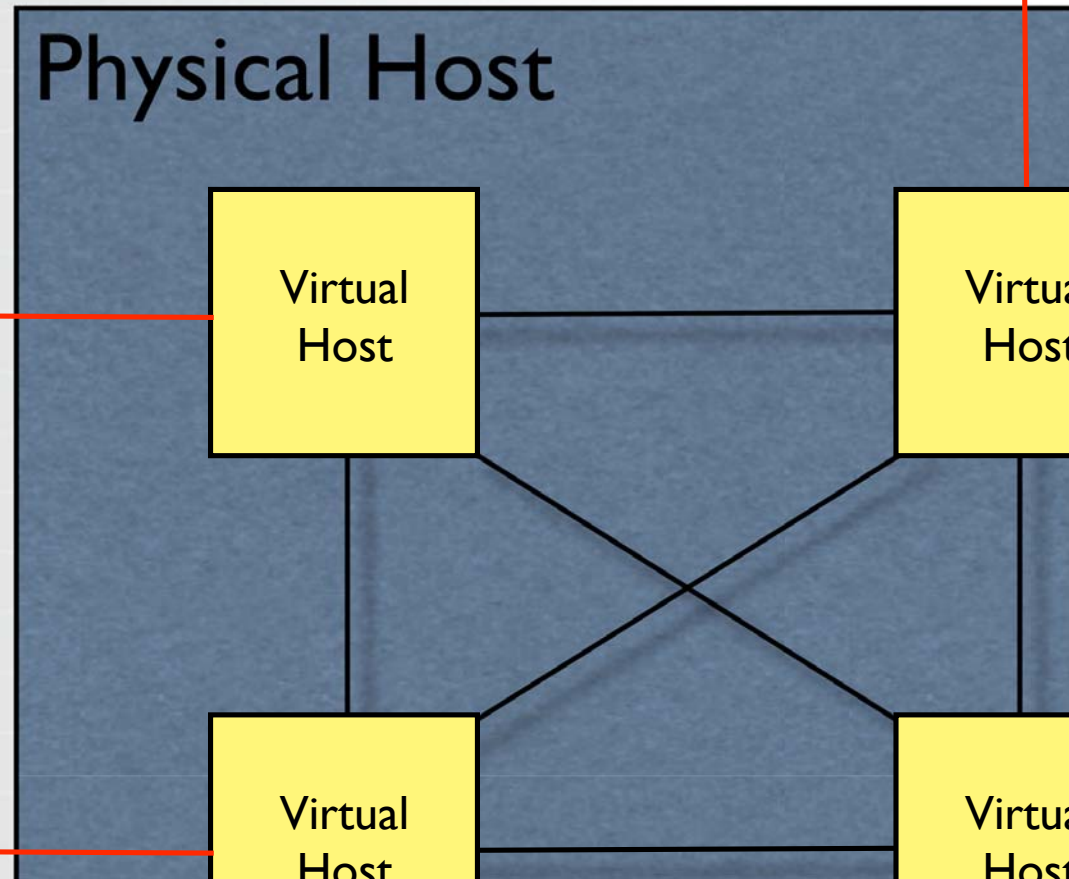
- Keep people from compromising your machine
 - While keeping it functional! Those network services are IMPORTANT!

Your Mission

You have to wear two hats at once

- Which hat goes on top?
- You're the good guy *and* the bad guy.
- Is defending your resources worth the effort?
- Is a good offence the best defence?

War Game Archi



War Games Archi

Virtual hosts attached to a virtual network

One way bridge from the “outside world”
hosts.

Still retain an air gap between the wargame
and the “real” internet.

Ground Rule

No throwing up a firewall or turning services off on your machine.

- Your boss will get angry if the web server goes down or he can't get his mail.

No DOS attacks (at least, not from your own machine!)

Other things you should

How will the winner be determined?

- The person who controls the most computers. Or maybe the one who cracks another host in the most stylish manner. TBD.

What are the prizes?

- The respect of your peers!
- The privilege of explaining how you did it.

You *are* being watched (maybe)

- So we'll know if you cheat!