Teaching Information Warfare with Lab Experiments via the Internet

Doug Jacobson
Associate Professor Electrical and Computer Engineering, Iowa State University,
2419 Coover Hall, Ames, IA 50011 dougj@iastate.edu

Abstract - Iowa State University has offered a course in information warfare for the past 8 years to both on campus and off campus students via streaming media. The class looks at computer security from an attack/defend view point. We study attacks and look at methods to stop the attacks. The course has several lab experiments where student will try out attack tools and defense mechanisms. Both on-campus and off-campus students access the lab via the internet which creates a unique set of challenges of trying to keep the attacks off the internet. The largest lab experiment is where the students are given the web site address to a company that was designed for the experiment. They are to break into the company and gather as much information as they can about the company and its employees. The students must submit a report where they document every step they took to break-in and then develop a plan to fix the problems.

Index Terms - Computer Security, Distance Education, Information Warfare, Laboratory.

INTRODUCTION

At present, Iowa State University is already a leader in computer security education and offers over twelve courses in information assurance. Iowa State University (ISU) promotes education, research, and outreach in information assurance through its Information Assurance Center [1]. Over two dozen faculty members from six academic departments work together in the Information Assurance Center to explore the problems of securing information in application areas ranging from software to networks to electronic democracy. ISU offers an M.S. in Information Assurance, concentrations in Information Assurance through one of the home departments supporting BS, MS, and PhD studies, and a graduate certificate in Information Assurance. Iowa State University was one of the first seven universities designated a Center of Excellence in Information Assurance Education [2] by the National Security Agency as authorized by Presidential Directive PDD63.

As part its land grant mission, Iowa State University has been teaching courses to off campus students for several decades and has been teaching security courses since 1995. This article outlines one of the more unique courses offered by the information assurance program (Information Warfare), and as far as we know is the only information warfare course taught via distance education. What makes this course even more unique is the hands-on laboratory experiments which are performed over the internet using a specially designed lab environment. The primary focus of this article is the teaching of a break-in lab experiment over the internet, which has students trying to break-in to a network modeled after a typical corporate environment. This article will first provide a brief discussion of the course and the early labs followed by a detailed discussion of the break-in lab.

COURSE INFORMATION

Computer Engineering 532 (Information warfare) was first introduced in the spring of 1996 as a follow on to the introduction to computer security course. The information warfare course looks at computer security from an attack/defend standpoint. We spend the first couple of weeks in class looking at the processes attackers use to identify, study, and then attack a system or network. We develop our own process for attacking computer systems. We also look at risks and potential effects of information warfare on computer systems and critical infrastructure. We then spend the next 6 weeks looking at various sub systems and protocols used in a typical information system. A topic will be introduced like authentication and the attack methodologies will be studied followed by looking at various defense mechanisms. During this time there are numerous lab experiments which help drive home the concepts introduced. Some of the lab experiments have the students actively probing networks and gaining information that could be used in an attack. About two thirds of the way through the course I assign the break-in lab. After the break-in lab we spend time looking at the results and studying the defenses used by the company. Several universities run cyber defense exercises which are run on isolated networks and are intense short duration activities [3], [4], [5].

Information Warfare Course Description

The course uses the text “Hacking Exposed” [3] plus course notes and handouts. Since security is a rapidly evolving field with new vulnerabilities and attacks every day we make use of the internet and other resources to keep the material current. The catalog description of the course is “Computer Systems and network security: implementation, configuration, testing of security software and hardware, network monitoring, Computer attacks and countermeasures. Emphasis on laboratory experiments.”
The course has a large set of course objectives many of which are reinforced using lab experiments. The course learning objectives are listed below.

Upon completing this course a student will:

- Understand the ethics of using hacking tools
- Be able to describe the TCP/IP network protocols and the effect of an open network protocol on security
- Be able to snoop and decode traffic from a network
- Be able to describe methods to counter traffic attacks like snooping, spoofing, redirection, and flooding.
- Understand the importance of passwords and methods to select good passwords
- Be able to crack passwords and understand the importance of authentication
- Understand the issues of social engineering when used to discover passwords
- Be able to describe a centralized key distribution center and its uses in authentication
- Be able to use one-time passwords, Kerberos, and other authentication systems.
- Understand the issues of anonymous email and email forgery, email privacy.
- Understand and be able to use an encrypted email system
- Understand the relationship of public and private keys to email and the uses of a Public Key Infrastructure
- Be able to identify the security problems with standard terminal based protocols like telnet, ftp, NFS, and web.
- Be able to identify solutions to the security problems with telnet, ftp, NFS, and web traffic.
- Understand how secure protocols like SSH, SSL, and VPN's operate and how they enhance security.
- Be able to develop a plan to attack a network of computer systems and then be able to develop a plan of countermeasures.
- Understand the use of firewalls and the strengths and weaknesses of a firewall
- Be able to read and identify information in log files for possible security violations
- Be able to use probe software to determine the weaknesses of a computer system.
- Understand how intrusion detection system operate and how they can be used to detect attacks

The labs

There are several labs assigned throughout the course, all of the labs are designed to be completed remotely. Most of the labs require the use of the computer lab at ISU, which students access via SSH or telnet (which is not secure) through the internet. The lab environment will be described later. While these lab experiments are not the focus of this article they are important to help set the stage for the break-in lab assignment.

Lab assignment #1

Using the tools discussed in chapter 1 of *Hacking Exposed* footprint Iowa State University. You should not do any scanning or anything else other than gather public information about the ISU computing system.

Turn in a list of the information gathered and how it was obtained. Identify any items that you found that you think should not be public.

Lab assignment #2

Using the tools discussed in chapter 2 of *Hacking Exposed* [3] scan the subnet 129.186.215.0/24 at Iowa State University. In case you need access to a tool, I have provided nmap for you on two machines called bones.ee.iastate.edu and spock.ee.iastate.edu. You can telnet or SSH to bones or spock and use the username/password provided in the lecture. Turn in a list of the information gathered in a table; try to identify the OS type of each machine you find.

Lab assignment #3

Find crack or some other software package to break UNIX password on an ftp site somewhere.

Build crack and use it to try and get the passwords from the passwd file stored in /home/issl/cpre532/passwd1. Turn in a list of which passwords you found and what they were. Run crack on the class passwd file stored in /home/issl/cpre532/passwd2. Turn in a list of which passwords you found and what they were.

Lab assignment #4

Login to scotty.ee.iastate.edu using your username.

- Use kdb edit to create a kerberos principal for yourself. Make it the same as your login name.
- Use kinit to test the entry
- Use kpasswd to change your passwd
- Use klist to list your tickets
- Use kdb util dump “filename” to dump a copy of the kerberos data base.

Lab assignment #5

- Use telnet to connect to spock.ee.iastate.edu SMTP server and send a message as GWBush@whitehouse.gov to the user cpre532 on spock. Include your name in the message.
- Use telnet to connect to the POP3 server on spock.ee.iastate.edu and read and then delete your mail message you sent in step 2.
- Login to spock or bones use pgp to create a key pair for yourself
- Using anonymous ftp obtain my public key from ftp.ee.iastate.edu.
- Create a signed and encrypted message that can be read by me.
- Store both the encrypted message and the public key in the directory: /usr/cpre532/hw5 on spock.

Lab assignment #6

Login to spock.ee.iastate.edu and create a directory called public_html. Put an html document in this directory which
links to three subdirectories. Make one directory that contains an html document that can only be accessed by someone with the user name of lorien and a password of firstone. Make one directory that contains an html document that can only be accessed by someone who comes from the machine bones.ee.iastate.edu. Turn in a listing of the .htaccess files.

The Break-In Lab Exercise

As you can see the first six labs have been focused on both tools and processes used to attack and secure a network of computers. The next lab is the break-in lab. I will first introduce the problem statement then talk about the process to redesign the lab each year and the physical lab itself. I will walk through the process the students go through and talk about how I handle the postmortem.

The problem statement

Listed below is the problem statement which I hand out a few days prior to the lab being ready just so they can start thinking about the lab.

Using (bones.ee.iastate.edu or spock.ee.iastate.edu) and any of the tools we have discussed during the class (both installed on bones/spock and those that have not been installed) perform the following:

Break into the computers belonging to the company 532 Corp (domain 532corp.issl.iastate.edu)

The goals are:

- Obtain as many user names and passwords as you can
- Obtain any files ending with .secret that are found in the users home directories. Some maybe encrypted and should be decrypted if possible.
- Obtain any diagrams of the corporation network
- Turn in the following:
  - The user names and passwords for all users on each of the machines you broke into.
  - The step by step method used to gain access to and decode the files. List both successes and failures and the time required to obtain and decode the files.
  - Provide a detailed description of how you would plug the holes you found along the way.

Notes:

- There are many methods to gain access to the computers in the 532 corporation. I have intentionally left several security holes in place.
- There are several machines on the network 129.186.215.0 which are possible targets. Please limit your attacks only to machines in the 532corp.issl.iastate.edu domain.
- You will not be able to get all passwords for all users.
- Also do not change any files on the machines or leave behind files. The goal is to break in undetected.
- You may not be able to solve the problem completely. Turn in what you have finished.

The lab setup

Each year I must redesign the break-in lab experiment to take into account both for new technology and for the fact the solution for the previous year is in circulation. The basic idea of the lab experiment is to break into a company network. The company called 532Corp has a number of employees and maintains a public website. The students must try to break into the company and gather as much information as they can (i.e., usernames, passwords, and data files) and then write a report that documents how they broke in and then how they would fix the holes they found.

The first time I taught this class it became obvious that this lab experiment was going to be popular, but was going to have to be carefully designed. The first design requirement was to create an environment that could be accessed remotely, yet not have the attacks carried out across the internet. This meant I needed to have a set of attack machines that students would have access to and could install attack software. I also wanted to make sure that what I was doing was approved by ISU and that the departments in charge of security on campus knew about the class and the lab experiments. Fortunately I have a very good relationship with the campus computing center and telecommunication department. They even gave me my own subnet which they further divided into 6 subnets. This enabled me to design a lab with routers and firewalls. The also gave me control of my DNS name space.

Another aspect of the lab became obvious after I taught the course for the first time. While all students were excited about the class and the break-in lab their level of excitement varied. Not all students have the skills necessary to be a skilled hacker. It became clear I needed to design the target network with multiple levels of complexity so that every student can manage to gather some data and break into a few accounts. While it would be possible to design a target network that would be difficult to hack into by using all of the most recent defense systems, I decided it would be better to design in weaknesses into the system. Since part of what the students need to do is to document how they would fix all of the holes they found, I designed the target network for three different types of students. The first type of student (about 20% of the class) find the idea of hacking interesting, but are not very excited about it. For these students I leave one or two obvious holes in the security system. The second group of students (about 70%) is excited about the experiment and will work hard to complete as much as they can. While motivated they do not have what it takes to be a skilled hacker. For these students I have designed more difficult to find holes in the security system. The third group of students (about 10%) start asking about the lab the first day of class and once it is assigned they stop sleeping trying to get all of the data. I designed the target system so that every piece of information can be obtained thus completing the experiment. However the last 5% of the solution is difficult and is designed for these students, to date I have yet to have a student get every piece of information.
One of the more interesting aspects of this experiment is the social engineering aspect of the attacks. We spend a great deal of time throughout the course talking about the social aspects of hacking even reading from Sun Tzu. This lab really drives that aspect home. In order for a student to be successful they must learn all they can about the employees of 532corp. So every year I start by designing the social fabric of the company and after that I work on the computing infrastructure of the company.

For purposes of this article I will focus on the lab solution for 2003. One interesting aspect of this article will be how it might impact the 2005 version of this course since until now the process I go through to develop the lab experiment has not been known to the students. The best students not only do social engineering on the 532corp employees but do social engineering on me. The first couple of years I created profiles of the 532corp employees that were patterned after my interests. For example they all liked the TV shows I liked. Students use that information to aid them in the attacks. These students are part of that 10% group.

The first step is to design the employee list and the social relationships between the employees. I start by creating a table shown below. A couple of key columns in this table are the theme, the roll, and the passwords. The theme is used for the social engineering aspect of the lab. In some cases the employee may like a TV show and use names from the show as their passwords. In some cases they may use family relationships for password and some do not have a theme. The passwords are part of the central password system within the company. Users also have passwords on many machines within the company. I worry about what users have what passwords on what machines after I get social aspects finished and after I design the network. The roll is sometimes used to determine which machines they have access to and in some cases it is used to determine who might have certain types of information. For example the CIO might have network diagrams or network passwords in their directory.

Once I have completed the relationship table I then start to design the actual network. The first couple of years I taught this course the actual lab moved between semesters so that every year I would spend countless hours rebuilding systems and rewiring the lab. The last couple years the equipment has remained intact which has reduced the amount of time needed to build the experiment. I just spend time changing network addresses, and functions. I also always try to add new holes and new defenses each year to both keep the lab current and to help stop the students that type to reuse last years solution. Figure 1 is the network diagram of the entire lab including the attacking network.

<table>
<thead>
<tr>
<th>Name</th>
<th>user</th>
<th>Theme</th>
<th>Roll</th>
<th>passwd</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mary Jones</td>
<td>maryj</td>
<td>None</td>
<td>Engineer</td>
<td>ace135</td>
</tr>
<tr>
<td>Jack Randall</td>
<td>jackr</td>
<td>farscape</td>
<td>Engineer</td>
<td>moyra7</td>
</tr>
<tr>
<td>Cliff Wilson</td>
<td>cliffw</td>
<td>Andromeda</td>
<td>Engineer</td>
<td>dhunt8</td>
</tr>
<tr>
<td>Ted Smith</td>
<td>teds</td>
<td>Wife Mary</td>
<td>Engineer</td>
<td>j3ssica</td>
</tr>
<tr>
<td>Sam Spade</td>
<td>sams</td>
<td>SG1</td>
<td>CTO</td>
<td>c@rt3r</td>
</tr>
<tr>
<td>Connie Wilson</td>
<td>conniew</td>
<td>Simpsons</td>
<td>Marketing</td>
<td>h0m3rs</td>
</tr>
<tr>
<td>Carrie Olson</td>
<td>carrieo</td>
<td>None</td>
<td>Net admin</td>
<td>975zyx</td>
</tr>
<tr>
<td>Carol Wong</td>
<td>carolw</td>
<td>Bob</td>
<td>CPU admin</td>
<td>p@tr1ck</td>
</tr>
<tr>
<td>Mary Smith</td>
<td>marys</td>
<td>Kids John, Jessica</td>
<td>CIO</td>
<td>jsmith</td>
</tr>
<tr>
<td>Ray Green</td>
<td>rayg</td>
<td>First wave</td>
<td>HR</td>
<td>3dd13</td>
</tr>
<tr>
<td>Harry Wallace</td>
<td>harryw</td>
<td>None</td>
<td>CEO</td>
<td>rfv567</td>
</tr>
<tr>
<td>Bob Brown</td>
<td>bobb</td>
<td>Dog, Cory</td>
<td>Admin Assist.</td>
<td>12guage</td>
</tr>
</tbody>
</table>

The Physical Lab

First most of the equipment is used equipment that the department was taken out of service. Since most of the machines are targets of attacks and they don’t need to be state of the art. I like to put in one or two very old systems that
often do not have exploit code available for them. The students often don’t know what to do with the “legacy” systems. I majority of the software I use is public domain and most of the systems are PC based. The only commercial equipment I have used to date are two security devices. A internal virtual firewall (FireBlock) that is used to control which computers can talk to which computer inside the company and a honey pot (SmokeDector) that can emulate up to 19 different computers where each computer can look like it is running one of about 20 operating systems. I use two honeypots, one inside the company and one outside the company. While I have not kept details on the costs of the lab, I would estimate the total cost for equipment is less than $10,000.

Referring to the diagram there are four subnets. The first subnet contains the attack machines that are accessed by the students and are used to attack the 532Corp. 532Corp has two subnets, one subnet is outside the firewall and contains the company web server plus a honeypot and an intrusion detection system. The third subnet is used to manage some of the security devices. This manage network is viewed as an isolated network and would require physical access in order for students to compromise it. I use this network to monitor and control the network. I talk about this concept of an isolated management network after the break-in lab is finished.

The fourth subnet is behind the firewall and contains the heart of the 532Corp. The 532Corp internal network has a honeypot and a virtual firewall (FireBlock) to segment the communications between computers. There a total of about ten machines inside 532Corp and several honeypot machines. A wireless access point is also part of the internal network.

Description of the lab

Once the physical lab has been designed I need to put together what I call the puzzle. Table II shows one machine of the puzzle. The puzzle shows which user has an account on which machine and their password. In addition the table shows the method used to break in the account. SE means the student needs to use social engineering, CR means the password can be broken (cracked), web file means the password in found in clear text somewhere. The password column lists the passwords for each user and the secret file column indicates if the user as a secret file in their home directory. If the word Crypt is in the secret file column then the file has been encrypted and the password follows.

The biggest problem with the break-in lab is the time involved in putting the lab together, while I do not keep close track of my time (which is probably a good thing) I have estimated it takes at least 40 hours to get all of the machines reconfigured and the equipment running and the lab planned. I have often been asked if a TA could do this, a benefit of me doing the entire lab is then I can answer the questions that come up and I can deal with the problems. I would like to get to the point where I can off load some the busy work to a graduate student.

<table>
<thead>
<tr>
<th>User</th>
<th>Method</th>
<th>Password</th>
<th>Secret file</th>
</tr>
</thead>
<tbody>
<tr>
<td>Marys</td>
<td>SE/CR</td>
<td>jessica</td>
<td>Yes</td>
</tr>
<tr>
<td>Carolw</td>
<td>SE</td>
<td>sandy</td>
<td>No</td>
</tr>
<tr>
<td>Cliffw</td>
<td>SE/CR</td>
<td>tr@nce</td>
<td>Crypt- becka</td>
</tr>
<tr>
<td>Teds</td>
<td>SE</td>
<td>mary</td>
<td>Yes</td>
</tr>
<tr>
<td>Jackr</td>
<td>Web file</td>
<td>J0hnc</td>
<td>No</td>
</tr>
<tr>
<td>Webtest</td>
<td>SE</td>
<td>tester</td>
<td>Crypt - aeryn</td>
</tr>
<tr>
<td>Machine: Bester Website</td>
<td>Teds</td>
<td>mary</td>
<td>FW/PW - eng</td>
</tr>
<tr>
<td></td>
<td>Sams</td>
<td>j@ck</td>
<td>Phone dir</td>
</tr>
<tr>
<td></td>
<td>Carolw</td>
<td>sandy</td>
<td>FW/PW -angled</td>
</tr>
<tr>
<td></td>
<td>Marys</td>
<td>joh</td>
<td>Net layout</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>TABLE II PUZZLE TABLE</th>
</tr>
</thead>
</table>

**RUNNING THE EXERCISE**

During the exercise I have to check on the lab every few hours. I tell the students that if something that use to work stops working to send me an email. The most common problems are with the most used components like the firewall, the router, the outside web server, and the attack computers. I dedicate the first minutes of each class period to answer questions about the lab. During the lab I monitor several of the honeypots and the intrusion detection system to see if the students are doing things that makes it difficult for others to finish the lab. If a student is doing something detrimental to the lab I will try to stop the activity. I have installed a device that can kill any connection without being detected. That is the only time the company will react to an attack. The most common attack that at least one student will try each semester is writing a program that will keep trying passwords over the network. This type of attack consumes a large amount of network bandwidth and is something that would be easily detected and killed by any system administrator. I talk about these types of attacks after the lab is completed. Another interesting thing I see are students trying to use previous years answers against the lab. It is fun to see what the students try and how successful they are. I will talk about some of these events during the postmortem.

Over the years I have had some interesting events occur. Two years ago I had two students walk into the lab facility when the door was left open. A couple of machines had someone logged into them. The students used that opportunity to gain information and gather data. They wrote this up in their report and I thought is was a great lesson that I told the other students. Security professionals often forget the physical break-ins. Last year I setup a wireless access point that was left open (no security), hoping that students would walk by and try to access the lab. Granted this would have been something only on-campus students could have done. No student tried it. This year I will add a wireless hacking lab early in the course and I hope they can use the wireless sniffing tools during the break-in lab. I will leave the tools on the attack machines.
Postmortem

As far as off-campus verses on-campus, since the students all have the same level of access to the lab, except for the physical break in. The biggest problem is that the off-campus students are up to two weeks behind the on-campus students. This means that the lab needs to be kept running it also means that I need to be careful handing out the solution. I do post the solution with a note that indicates if they haven’t finished the lab they should not open the file. I have not had any problems, primarily because the lab is not graded on how far they get, but on how they document what they did and how they would fix it. I hand out the two tables and a complete network diagram to the students when the lab is completed and we spend a class period talking about the company network.

One problem I have each semester is at least one student will accidentally use one of the attack tools against machines outside the 532Corp. This will often be detected by the campus security group and access to the machine will be disabled. I then have to talk to the campus computing center and get the access enabled.

As far as grading of the lab I do not spend much time looking at the details of how many passwords or file they found. I look at the process they use to obtain the information and how they would fix them problems they found. I divide the solutions into different categories and assign scores based on the category. Typically I have an A and a B pile, on rare occasions I have a student that does poorly on the lab and will receive a C or D.

Once the lab has finished I then introduce the concepts of intrusion detection systems and honey pots. I provide the students access to the intrusion detections I installed in 532corp so they can look at attacks they carried out. The honey pots upset the most students. They get very mad when they find out they “wasted” their time on the honey pots.

CONCLUSIONS

This class is the most challenging course I have ever taught and one of the most enjoyable. It takes a large amount of time, but I can see students put everything together during this course. The students start to see the difficulty in protecting systems and hopefully see that the challenge is in the protection and defense of computer networks. I often talk about how it is easier to hack than to protect. The attacker only needs to find one hole and the defenders need to defend all holes.

While I have not done any formal assessment of the course other than the course evaluation performed by the department. I have receive many positive comments on the course and the enrollment has increased over they years. On the final exam I also ask what I can do to make the break-in lab better. I typically only get a few minor suggestions. The most common suggestion made by the students is that the students would like to play “king of hill” where groups of students set up systems and then defend it against other students. We have discussed this and may create another course to do this. This would be very difficult with off-campus students and with 60 on-campus students.

In 2004 I’m planning on several changes to the lab environment. I will be adding a couple of lectures on wireless security. We do teach a course on wireless security, but I want to include a lab experiment where students can capture wireless packets. I have received several pieces of equipment from Cisco that I will be adding to the lab. I will add the Cisco IDS and Cisco Pix firewall to the inside of the company. I hope to also have the students use a commercial network vulnerability scanner. I will also add a few more employees in the company and I’m working on a way to generate internal traffic between employees. I will reduce the number of internal honeypots, an I will probably add username and password information to one of honeypot machines so students will try that machine, because they have a username and password. I would like to get to the point where I can have them try some interactive social engineering by having an internal email address for tech support that I answer, or monitor and answer email for all of the employees. If I pick an employee that is either not very computer savvy or maybe one that can be coerced into giving up information that would provide a new avenue for students to explore. I’m not sure what I will try, but this would add a new dimension to the lab, which a couple of students have commented would make it even more realistic.

REFERENCES