Session 1432

Teaching Information Warfare with a Break-in Laboratory

Dr. Doug Jacobson
Department of Electrical and Computer Engineering, Iowa State University

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 is 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 new graduate certificate in Information Assurance. Faculty research interests cover the breadth of Information Assurance, including intrusion detection, security of wireless networks, mobile ad-hoc tactical networks, secure e-commerce, public policy for electronic democracy, and the development of a curriculum framework for 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 paper outlines one of the more unique courses offered by the information assurance program (CprE 532 Information Warfare), and as far as we know is the only information warfare course taught nation wide 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 paper 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.

About the course

Computer Engineering (CprE) 532 (Information warfare) is the second course in a sequence. I introduced the course in spring of 1996 as a follow on course to CprE 531 which is the introduction to computer security. 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 subsystems and protocols used in a typical information system. A topic will be introduced like authentication and the attack methodologies will be studied. That will be 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.

This paper will first provide a brief discussion of the course objectives and the early labs. The majority of this paper will discuss the break-in lab.

CprE 532 Information Warfare Course Description

Goal:
This is the second course in a sequence. This course is intended to provide students with hand-on experience in installing, configuring, and testing state-of-the-art security software and hardware. Methods of attack will be examined to better understand how to detect and prevent attacks.

Prerequisite: CprE 531

Course Length: 45 hours in 15 weeks, 2 eighty minutes meetings per week

Textbook:

Hacking Exposed, 4th ed, McClure, Scambray & Kurtz, McGraw-Hill Osborne Media, ISBN: 0072227427

Course Description:

Computer Systems and network security: implementation, configuration, testing of security software and hardware, network monitoring. Computer attacks and countermeasures. Emphasis on laboratory experiments.

Course Learning Objectives:

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 traffic from a network and decode the data
- 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 can be used to 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 screening routers and software filters to defend a computer system from attack.
- 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

Major Topics:

- Introduction & Ethics
- Network Protocols
- Traffic attacks and defenses
- Authentication attacks and defenses
- eMail Attacks and defenses
- Terminal Services, NFS, and X
- WEB
- Intrusion detection
- Firewalls
- Screening Routers
- Link encryption
- Encryption tools
- Trapping a hacker
- Probe software
- Security management

Method of Instruction:

The course is taught using lectures which are also provided to the off campus students via streaming media. The course also has a strong laboratory component where the students connect to the lab remotely to carry out experiments. The labs range from using tools (both attack tools and defend tools) to looking at network protocols. The largest lab is the attack and defend lab where the students try to break into a small company designed by the faculty. The students must detail the attack plan and then provide a detailed description of how to defend against the 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 via the internet. The lab environment will be described later. While these lab experiments are not the focus of this paper 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* scan the subnet 129.186.215.0/24 at Iowa State University. **NOTE: Scan only this network and no others.**

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

Login to spock, bones, scotty, issl1, issl4, issl5 (ee.iastate.edu) Note: spock & bones run the same OS and the isslX machines run a different OS, so which ever OS you build the cracking software on, you will need to use for the rest of the lab.

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

4. You can do this lab on any machine, just copy the password file over to the machine and port crack to that machine.

Lab assignment #4

Login to scotty.ee.iastate.edu using your user name. The password for the Kerberos database is **dogs**

1. Use kdb_edit to create a kerberos principal for yourself. Make it the same as your login name.
2. Use kinit to test the entry
3. Use kpasswd to change your passwd
4. Use klist to list your tickets
5. Use kdb_util dump "filename" to dump a copy of the kerberos data base.

Nothing to turn in.

Lab assignment #5

PART 1

1. Login to bones
2. 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.
3. 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.

POP 3 commands:

```
user  name     use cpre532
pass  passwd   use cpre532
retr #  will retrieve message #
dele #  will delete message #
quit
```

Nothing to turn in.

PART 2

1. Login to spock or bones
2. use pgp to create a key pair for yourself
3. Using anonymous ftp obtain my public key from ftp.ee.iastate.edu. The key is stored in /pub/courseware/cpre/532/dougj.asc
4. Create a signed and encrypted message that can be read by me.
5. Create an ASCII version of your public key.

6. Store both the encrypted message and the public key in the directory: /usr/cpre532/hw5 on spock. For the file name of the message use login_name.mess.asc ; for the key use login_name.asc

Nothing to turn in.

Homework assignment #6

1. Login to spock.ee.iastate.edu
2. You should create a directory called public_html.
3. Put an html document in this directory which links to three subdirectories.
4. 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**.
5. Make one directory that contains an html document that can only be accessed by someone who comes from the machine bones.ee.iastate.edu
6. Make one directory that contains an html document that can only be accessed by someone who does not come from the machine bones.ee.iastate.edu

Turn in a listing of the .htaccess files

Note: On bones use the command lynx as your web browser to test it.

The break-in lab

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 I assign is the break-in lab. Before I introduce the problem statement I first want to 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 the how I handle the postmortem.

The 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 in to a company network. The company called 532Corp has a number of employees and maintains a public website (http://www.532corp.issl.iastate.edu). The students must try to break in to 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 would 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 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 skill sets 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 in to 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[3, 4]. 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 paper I will focus on the lab solution for 2003. One interesting aspect of this paper 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. I have had students use that information to aid them in them 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.

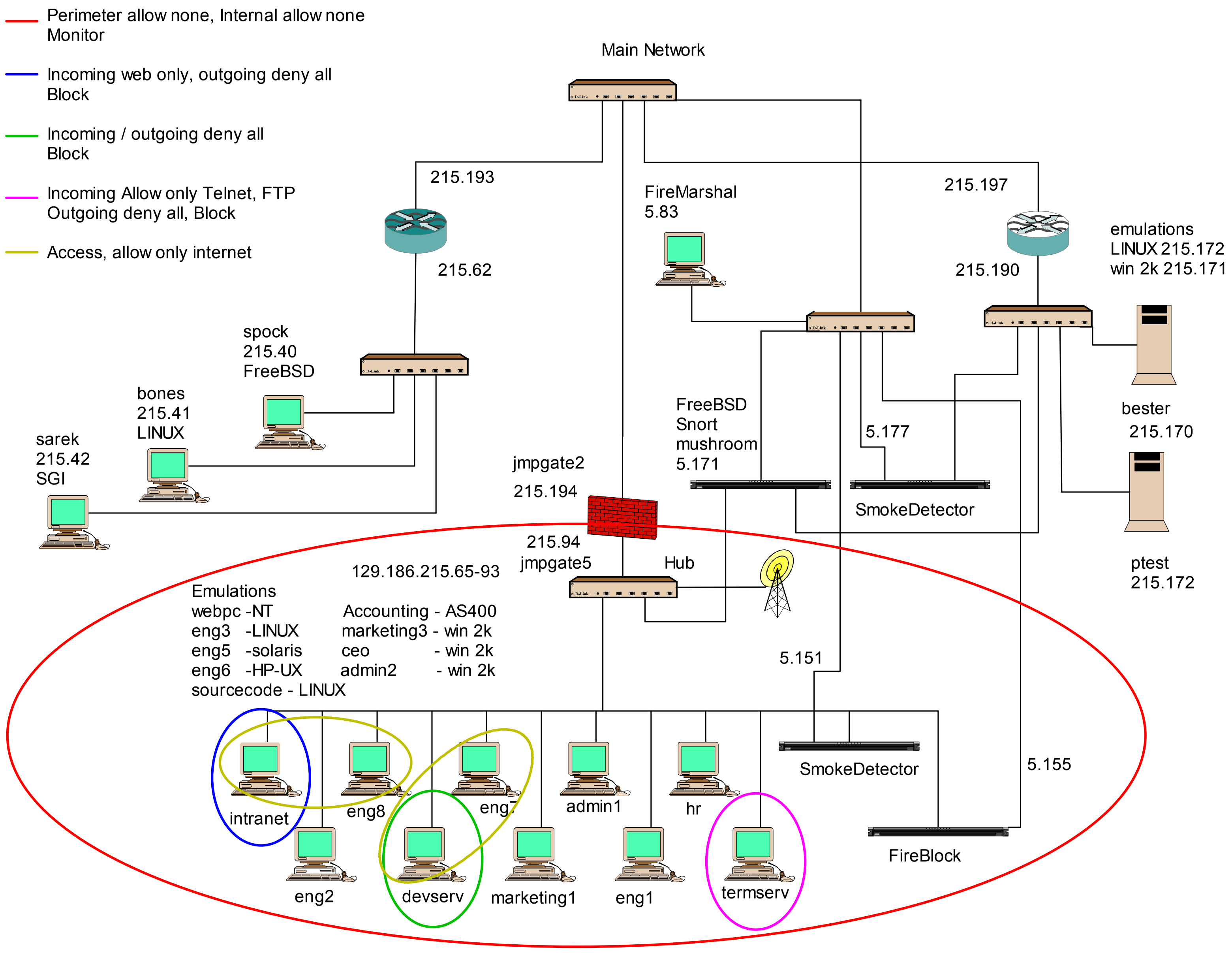
Relationships:

Name	user	Theme	Roll	Phone	Yp passwd
Mary Jones	maryj	None	Engineer	5387	ace135
Jack Randall	jackr	farscape	Engineer	5388	moyra7
Cliff Wilson	cliffw	Andromeda	Engineer	5389	dhunt8
Ted Smith	teds	Wife Mary	Engineer	6790	j3ssica
Sam Spade	sams	SG1	CTO	9234	c@rt3r
Connie Wilson	conniew	Simpsons	Marketing	8234	h0m3rs
Carrie Olson	carrieo	None	Net admin	8880	975zyx
Carol Wong	carolw	Sponge Bob	CPU admin	7634	p@tr1ck
Mary Smith	marys	2 kids John, Jessica	CIO	5885	jjsmith
Ray Green	rayg	First wave	HR	4466	3dd13
Harry Wallace	harryw	None	CEO	1145	rfv567
Bob Brown	bobb	Dog, Cory	Admin Assist.	1146	12guage

The Lab

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. The figure below is the network diagram of the entire lab including the attacking network. I need to make a few comments about the diagram and the equipment used.

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 were two security devices (FireBlock and SmokeDector)[5] Fireblock is a internal virtual firewall that is used to control which computers can talk to which computer inside the company. The SmokeDector is a honey pot 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 SmokeDectors, 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 new equipment is less than $10,000.


Perimeter allow none, Internal allow none
Monitor
Incoming web only, outgoing deny all
Block
Incoming / outgoing deny all
Block
Incoming Allow only Telnet, FTP
Outgoing deny all, Block
Access, allow only internet
Main Network
215.193
215.62
FireMarshal
5.83
215.197
215.190
emulations
LINUX 215.172
win 2k 215.171
spock
215.40
FreeBSD
bones
215.41
LINUX
sarek
215.42
SGI
FreeBSD
Snort
mushroom
5.171
5.177
SmokeDetector
bester
215.170
ptest
215.172
jmpgate2
215.194
215.94
jmpgate5
Hub
129.186.215.65-93
Emulations
webpc -NT
eng3 -LINUX
eng5 -solaris
eng6 -HP-UX
sourcecode - LINUX
Accounting - AS400
marketing3 - win 2k
ceo - win 2k
admin2 - win 2k
5.151
intranet
eng8
eng7
admin1
hr
SmokeDetector
5.155
eng2
devserv
marketing1
eng1
termserv
FireBlock

Referring to the diagram there are four subnets. The first subnet contains the attack machines (sarek, bones, and spock). These 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 (SmokeDector) and an intrusion detection system (a public domain system called snort[6]). 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. In the diagram the heading marked emulations indicate what types of computers are being emulated by the honeypots. The colored circles show how the FireBlock is controlling access between computers. For example the machine called internet can only receive incoming web connections, unless you connect from eng8 which is allowed complete access to intranet. The most interesting one I have put there to have some fun with the students. The machine termserv has several easy to obtain passwords (See the puzzle table) and therefore most students can gain access to the machine. The FireBlock allows incoming access but does not let the machine make any out going connections. So students often tell me that they think termserv is broken because they cannot make any of the network applications work. 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. The puzzle shows which user has an account on which machine and what their password is. 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, P to P means that the machine running a Peer to Peer protocol has the password in a text file. The Peer to Peer machine was new in 2003, only a small number of students actually exploited that vulnerability. 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 services column indicates what network services are of interest on that machine. The services column also indicates which machines are controlled by the FireBlock product.
The last group of machines in the table is the honey pots. I added a set of honey pots to help confuse the attackers. As I will discuss in the postmortem section of this paper I use the break-in lab as a lead in to intrusion detection and honey pots.

Puzzle Table

Machine	User	Method	Password	Secret file	Services
Bester 215.170	Marys	SE/CR	jessica	Yes	
	Carolw	SE	sandy	No	
	Cliffw	SE/CR	tr@nce	Crypt- becka	

	Teds	SE	mary	Yes	
	Jackr	Web file	J0hnc	No	
	Webtest	SE	tester	Crypt - aeryn	
Bester web	Maryj		None		
	Jackr		None		
	Cliffw		None		
	Teds		mary	FW/PW - eng	
	Sams		j@ck	Phone dir	
	Conniew		None		
	Carrieo		None		
	Carolw		sandy	FW/PW -angied	
	Marys		john	Net layout	
	Rayg		None		
	Harryw		None		
	Bobb		None		
Jmpgate2 215.194	Marys	SE	j0hn		
	Carolw	web	s@ndy		
	Maryj	P to P	wxum013		
	Sams	SE	qu1nn		
	Eng	web	d1lb3rt		
Intranet 215.65	Maryj	P to P	987wqa		FB
	Jackr	SE/CR	cr1chton		In 80
	Cliffw	SE	tr@nce		Out none
	Teds	web	m@ry	Yes	
	Sams	SE	c@rt3r		Access
	Carrieo		tre678		From
	Carolw	SE	sp0ng3		Eng8
	Marys		j0hns	Yes	
	Bobb		hunt3r		
Intranet Web	Sams	SE/CR	quinn	Yes	
	Bobb	SE/CR	blacklab		

eng2	Cliffw	SE/CR	tr@nce	Yes	
	Sams	SE/CR	oneil	Crypt – sg-1	
	Root	SE/CR	c@rter		
Eng1 215.69	Root	SE	jessica		yp client
	Yp users				

Marketing1 215.67	Harryw		xsw468	Yes	
	Conniew	SE/CR	b@rt		
	Bobb	SE/CR	duckc@ll	Yes	
	Rayg		F0st3r	Crypt eddie	
	Root	SE	532corp		
Devserv	Sams	SE	c@rt3r	No	FB
	Maryj		zlm476	Yes	In none
	Marys	SE/web	j0hn	No	Out none
Eng7 215.87	Lmaryj	P to P	zaq470	Yes	yp serv
	Ljackj		cr1chton	No	Access to
	Lcliffw		tr@nce	Yes	devserv
Admin1		Win 2K	215.80		
HR		Win 2K	215.66		
AP	Wireless		2125.89		
PTest		Win XP	215.173		
termserv 215.71	Cliffw	SE	tr@nce	No	FB
	Teds	SE	m@ry	No	In 23, 21
	Marys	SE/web	j0hn	Yes	Out none
Eng8 215.88	Cliffw	rlogin	ftc147	No	From eng2
	Teds	CR/SE	j3ss1c@	Yes	
	Root	P to P	mju468		Access to
	Maryj	P to P	mzl543		intranet
	Sams	rlogin	cde579	Crypt – SG-1	From eng1
webpc	Honey	NT	215.70		
Eng3	Honey	LINUX	215.75		
Eng5	Honey	Solaris 8	215.77		
Eng6	Honey	HP-UX	215.78		
Sourcecode	Honey	LINUX	215.79		
Admin2	Honey	Win 2K	215.81		
Accounting	Honey	AS 400	215.82		
Marketing3	Honey	Win 2K	215.84		
ftpserv	Honey	Win 2k	215.171		
Mailhub	Honey	LINUX	215.172		

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.

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.

Lab assignment #8

NOTE: The lab will be ready to start on Saturday morning the 5th of April.

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.
- This lab should be worked on individually. You should NOT discuss methods or solutions with other students.
- You may not be able to solve the problem completely. Turn in what you have finished.

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 honey pots 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 type to stop the activity. I have installed a device that can kill any connection with out 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 the network diagram I have included in this paper 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. This goes back to my earlier comment about getting approval first for teaching this type of class.

As far as grading I do not spend much time looking at the details, but more looking at the overall process. 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 also will add one encrypted channel wireless access point to the 532Corp. 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. I'm still working on that, but maybe a having an internal email address for tech support that I answer, or even 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 in to 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.

Bibliography

1. http://www.iac.iastate.edu
2. http://www.nsa.gov:8080/isso/programs/coeiae/index.htm
3. http://www.kimsoft.com/polwar.htm
4. http://www.chinapage.com/sunzi-e.html
5. http://www.paliasadesys.com
6. http://www.snort.org

Biography

DOUG JACOBSON
Doug Jacobson is an Associate Professor of Electrical and Computer Engineering at Iowa State University and director the ISU Information Assurance Center. He has received two R&D 100 awards for security technology and has two patents in the area of computer security. He has given over 40 presentations in the area of computer security and has been teaching security and networks courses for over 15 years.