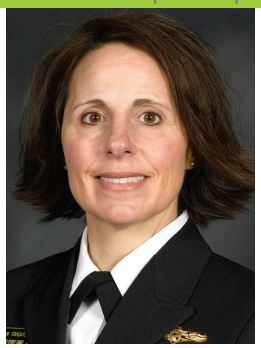




Sarah Standard Raymond Greenlaw Andrew Phillips David Stahl John Schultz

Network Reconnaissance, Attack, and Defense Laboratories for an Introductory Cyber-Security Course

CYBER-SECURITY is an area in which much curriculum development is taking place; it is important that such efforts be evaluated and shared. We describe three laboratories developed at the United States Naval Academy (USNA) for use in its fundamentals of cyber-security course. All three labs are conducted in a sandboxed virtual environment. Detailed instructor notes, student instructions, worksheets, grading guidance and supporting course software were developed for these labs. In this paper we share our experiences with these labs, assessment and evaluation material, and lessons learned so that others might benefit from our work.

1. Introduction

The USNA is charged with ensuring that all midshipmen (undergraduate students at USNA) receive an education that is sufficient to prepare them to preserve, protect, and defend the nation. Influenced by President Obama's May 2009 Cyberspace Policy Review, which included the need to "expand and train the workforce, including ... cyber-security expertise in the Federal government" [5], a committee of USNA faculty members was charged with exploring and defining the scope of understanding of cyber-security needed by midshipmen in their capacity as future naval officers. The committee worked with the Chief of Naval Operations and the Commandant of the Marine Corps staffs, analyzed the other service academies' inclusion of cyber-warfare concepts in their curricula, and examined various other academic cyber programs from across the nation. In spring 2011, USNA decided that, beginning in fall 2011, all first-year students would be required to take an introductory course in the technical foundations of cyber-security. The course that resulted from the aforementioned efforts was taught in fall 2011 to six-hundred freshman midshipmen—half of the freshman class; it was offered again in spring 2012 to the remaining half of the class. During the academic year 2012–13, the process was repeated with the subsequent freshman class, so at this point over 2,400 students in two years have taken this required course. Everyone involved wanted the course to have a significant hands-on component; this paper describes the three hands-on capstone labs in the course: network reconnaissance, attack, and defense.

Cyber-security education is important and needs to be broadened, as USNA has done, to encompass more than only those interested in pursuing a degree or a career in the field. We believe that the need for the basic understanding by all computer/internet users about the fundamental risks, including why and how to minimize or prevent problems, is more important than ever. Intentional or unintentional human errors are consistently the weakness that allows an advanced persistent threat into a network. Some experts believe that our critical infrastructures are already embedded with such threats. People are well aware of publicized cyber-attacks and threats, but most are likely to be disconnected from the reality that their errors could cause an attack. The vast majority of employees on any network generally do not understand how computers and networks function, or how their individual actions impact the network, until it is too late. Often, employees assume that the causes are the result of the information technology (IT) departments not doing their jobs, and personnel are irritated by the security controls in place on the networks.

The U.S. Navy depends on cyberspace just as much as, or arguably more than, any other organization, and has an extremely large workforce representing a cross section of the population. In four short years, the USNA midshipmen graduate and begin serving as leaders in the Navy and Marine Corps, and the majority will not be involved with IT in their careers,

yet every single graduate is operating on the Navy's networks regardless of whether they are flying an aircraft, on a ship or submarine, in the Marine Corps, and so on. USNA has recognized the reality of the weakest link in cyberspace: people. The required first-year cyber-security course is an effort to begin to address that weakness. In fact, USNA is also requiring all midshipmen to take a follow-on technical cyber-security course in their junior year. The second required cyber-security course will be taught to approximately six-hundred juniors beginning in the fall of 2013. The authors of this paper hope to encourage more education programs to require that all students increase their understanding of the human-error impact on computer networks by demonstrating the positive results of the three capstone labs in improving the majority of enrolled student's realization of how information systems are attacked and defended, as well as their own personal role in contributing to the weakness of a system.

In order to provide some context for this paper it is worth discussing our introductory cyber-security course in more detail. The course, "Introduction to Cyber Security Technical Foundations" consists of three main sections: the Cyber Battlefield, Models and Tools, and Cyber Operations. In the first section, the Cyber Battlefield, students learn about digital data, elementary concepts in computer architecture, operating systems, programs, the web, networks and protocols, wireless networks (including WEP cracking and wireless sniffing), and the internet. In the second section, Models and Tools, students learn the basics about formal models of security and risk in information systems. With this foundational knowledge of what computer security means, they are then exposed to some basic tools for providing security: firewalls, symmetric encryption, cryptographic hashing, asymmetric encryption, digital certificates, and steganography. In the final section, Cyber Operations, students learn about cyber reconnaissance, attack, defense, and forensics. In this paper, we focus on the final labs that constitute the Cyber Operations part of the course.

Once the students understand the battlefield they are trying to defend (or attack), and the defenses they can employ (or must defeat), midshipmen move into the final part of the course: "Cyber Operations."

Once the students understand the battlefield they are trying to defend (or attack), and the defenses they can employ (or must defeat), midshipmen move into the final part of the course: "Cyber Operations." Thus, the first thirteen weeks of the course are (largely) a preparation for the last three weeks, which culminate in a series of three hands-on labs in which the students in each section break up into two teams, each with its own network. Students reconnoiter their opponent's network, attack their opponent's network, and finally defend (that is, harden) their own network and re-attack their opponent's hardened network. All of this activity takes place on a network of virtual hosts running on a virtualization server that is

- **a.** completely isolated from USNA's public network,
- **b.** able to be reset in seconds to its initial configuration following each lab period, and
- **c.** indistinguishable from a real physical network.

The course format involves two 50-minute lectures per week and one 110-minute hands-on lab per week. During the labs, students practice what they have learned throughout the course, including material from the early weeks. Given the volume of technical material presented in the course, it is somewhat unrealistic to expect students to remember all of the technical details for both the UNIX and Windows systems used in the lectures and labs, so we have developed "tip sheets" for students that provide lists of commonly used commands for these two operating systems; useful network commands; and services, ports, protocols, whether TCP or UDP is used, and the tools needed to use the service. Students and instructors have found these supplements to be invaluable. In addition, the faculty members involved with the course have developed an extensive set of student notes as there is no textbook associated with the course. These notes are available publicly at [10].

In reviewing relevant work done at other universities, we found that in 2003, Syracuse University, in partnership with the Air Force Research Laboratory in Rome, New York, developed an advanced cyber-security elective aimed at junior and senior year ROTC students [4]. The course has now evolved into a paid internship with the Air Force Research Lab in Rome, New York, and focuses not only on the technical aspects of cyberspace, but also on leadership challenges faced when securing a domain, "with emphasis on assuring Air Force mission essential functions in a contested environment [1]." In addition, although not yet a common trend, some high schools are creating cyber-related curricula, as is the case at the Rome Catholic School in Rome, New York. Rome Catholic School offers K–12 cyber education integrated into the weekly curriculum for K-6 that focuses on basic computer security and prevention of cyber-bullying. In grades 7-12, the school requires three cyber-security courses with a fourth elective [9]. The courses include hands-on labs in internet research, introduction to computers, network hardware, command-line interfaces, and networking commands.

Other universities that we have explored offer networking labs in network-security courses, but typically these labs are for specialized majors such as computer science or information technology, and occur at the junior or senior level [3,9]. We also contacted the other two major military-service academies to determine what cyber-security education was provided to their students. The United States Air Force Academy (USAFA) requires an introductory computer-systems and information-technology course that includes five lessons focused on the fundamentals of computer security. In the summer of 2011, USAFA rolled out an elective two-week, full-time program to about ninety cadets that provides them with hands-on experience in cyber-security. The content of the elective's labs have approximately a 50% overlap with the content of the USNA labs [7]. The United States Military Academy's curriculum includes a required information-technology-related course, but the focus is not in computer or network security [6].

The remainder of this paper is as follows: Section 2 describes the laboratory framework; Sections 3, 4, and 5 present the reconnaissance, attack, and defense labs, respectively; Section 6 describes lessons learned and recommendations; a summary is given in Section 7. We also provide a list of references.

2. Laboratory Framework

This section discusses the lab setup. We should point out that there are a maximum of six sections of the course taught concurrently at any time of day, but our setup could have supported more than six sections, if necessary. We discuss the hardware configuration, student laptops, lab-related software, and student prior experiences.

2.1 Hardware Configuration

Our discussion of the hardware in this subsection is from Brown et al. [2]. All students at USNA are required to purchase a computer, and both the requirements and configuration of the machine are proscribed for all members of the class. Beginning with the class of 2015, the first-year midshipmen all have laptops to use in the cyber-security course. Students are required to bring their laptops to class every day, and the course is conducted via the local (and Academy-wide) intranet wirelessly using those laptops. Some of the labs in the course require students to use a set of penetration testing programs that can probe for and exploit vulnerabilities in unpatched operating systems. Due to the sensitive nature of these applications and to prevent a security incident, we established a virtual environment in which students could work. The following is a description of that system.

Each classroom has ceiling-mounted wireless access point (WAP) connecting student laptops to the system shown in Figure 1. The WAP are connected via Ethernet to a 1000 Mbps Catalyst switch. The switch has connections to both the ESX server (described below) and the USNA intranet, allowing students to access classroom items, notes, and other online resources, while also providing students access to the virtual sandbox environment via VMware Remote Console [2].

To handle the load imposed by 126 concurrent users (120 students and 6 instructors), a four-server system was installed as indicated in the center of Figure 1. Three of the servers are ESX virtualization servers, while the fourth is the vCenter™ server—providing administrative control over the virtualized environment. Each server is connected via a Catalyst switch to a 9.6 TB Dell EqualLogic PS4000X SAN. Server specifications are itemized below, and the classroom connectivity to the server is depicted in Figure 1.

- **ESX Server Specifications:**
  - DELL PowerEdge R710
  - 6-core Intel Xeon 5645 2.4GHz, 128GB RAM, 600GB disk
  - 2 × quad-port gigabit NIC
- **vCenter™ Server Specifications:**
  - DELL PowerEdge R210II
  - quad-core Intel Xeon E3-1270 3.4GHz, 8GB RAM, 600GB disk

2.2 Student Laptops

USNA acquires and configures the laptops that midshipmen are required to purchase, independent of the cyber-security course. The following is a listing of the Class of 2015's laptop specifications:

- **System:**
  Lenovo ThinkPad T430 Laptop
- **Memory:**
  8 GB
- **Hard Drive:**
  128GB SSD
- **DVD-ROM Drive:**
  SATA 8X DVD Multi-Burner
- **Ethernet:**
  Intel 82579LM Gigabit Ethernet
- **Wireless LAN:**
  802.11a/b/g/n Intel Centrino Advance-N 6205
- **Operating System:**
  MS Windows™ 7 SP1 Enterprise
- **Power:**
  9-cell battery and AC adapter

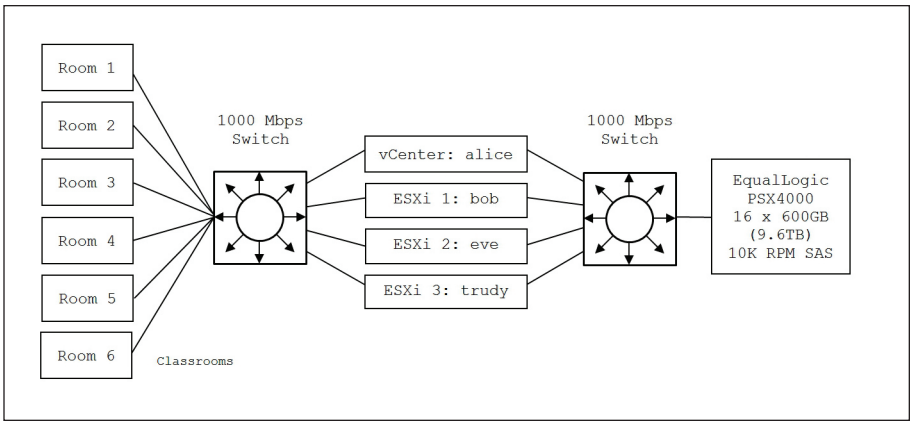


Figure 1. Topographical View of Classroom Connectivity to the ESX-Server System

2.3 Software Setup for the Virtual Environment

The VMware vCenterTM server runs on Microsoft Windows™ Server 2008. Within vCenter, one master class of virtual machine images was created for instructors, students, routers, and target VMs, which was then duplicated to create six identical classrooms. Student and instructor VMs were built on Backtrack 5, while the VMs designed for students to attack and defend during the final labs of the class include Linux 2.6.x, Windows™ XP Pro 2002, and Windows™ Server 2003 hosts. Routers were implemented within the virtual space using the open-source Vyatta Core software. Within each class, VMs were organized into four networks: BLUE and GOLD student networks, the instructor RED network, and the neutral "internet".

2.4 Students' Prior Experiences

Earlier in the course, students engage in lessons, activities, and homework using basic JavaScript, understanding simple programs, embedding JavaScript into HTML, designing web pages, performing injection attacks, running shell commands, and configuring basic firewalls. The students also have multiple lessons, activities, and homework involving the concepts of networks, which include setting up a wired, and a wireless network, client-server systems, services, ports, protocols, and the TCP/IP stack. The students use the shell commands *ipconfig*, *ping*, *nslookup*, traceroute, *netstat*, *arp*, and *netcat* on several occasions during the lessons, activities, and homework for the course.

The students learn the five pillars of information assurance (IA): confidentiality, integrity, availability, non-repudiation, and authentication. They learn about symmetric and asymmetric encryption, hashing, steganography, firewalls, operating system permissions, X.509 certificates, and sometimes use tools relating to these concepts. That is, they learn about tools that can help secure the IA pillars, and they learn that an attack must defeat the tools that violate the pillars. The importance of password complexity and length are illustrated and reinforced throughout the course. Students learn about password files, and how hashing and "salt" can minimize or prevent an attacker from determining passwords if the password file is stolen.

Students engage in lessons that present some typical attack vectors, including phishing, malware, guessing usernames and passwords, attacking a network service by exploiting vulnerabilities in a server, and escalating privileges by either stealing the password file and cracking passwords or hijacking a process running with higher privileges.

To illustrate network vulnerabilities and the process of conducting a successful attack, we use a concentric circle diagram as illustrated in Figure 2. Each circle in the diagram represents a barrier (e.g. firewall or level of privilege) that the attacker must penetrate. The outermost barrier in Figure 2 represents the firewall for the network separating an attacker from the network itself. "Holes" in the firewall represent services that the firewall allows through. In Figure 2, only port 80, the HTTP service, is allowed by the outermost firewall. Therefore, at step 0 of an attack, the attacker must determine how to gain access through port 80 to a webserver, represented as "other host." In Figure 2, each host within the network also is represented by two concentric circles. The outermost circle for a host represents that particular host's local firewall. The two hosts in Figure 2 have different firewall settings. "Other host" has two services running with access through the firewall: HTTP (port 80) and SSH (port 22). The target host has only one such service running: SSH (also on port 22). Within the firewall of each host is an area that provides unprivileged access to the host. So, on the "other host" in Figure 2 the attacker who successfully gains access to that host via port 80 at step 1 has gained unprivileged access to the host. The innermost circle on that same host represents privileged access as root, administrator, or the owner of any files an attacker wants to access; therefore the barrier between unprivileged and privileged access represents the escalation of privileges up to and possibly including root access. In Figure 2, steps 1 to 2 use SSH to gain unprivileged access to the target host. Finally, step 3 shows that the attacker has successfully escalated their privileges and gained access to that system that could represent complete control of the target. Armed with the experience presented in this section, the students have enough knowledge to undertake the three capstone labs.

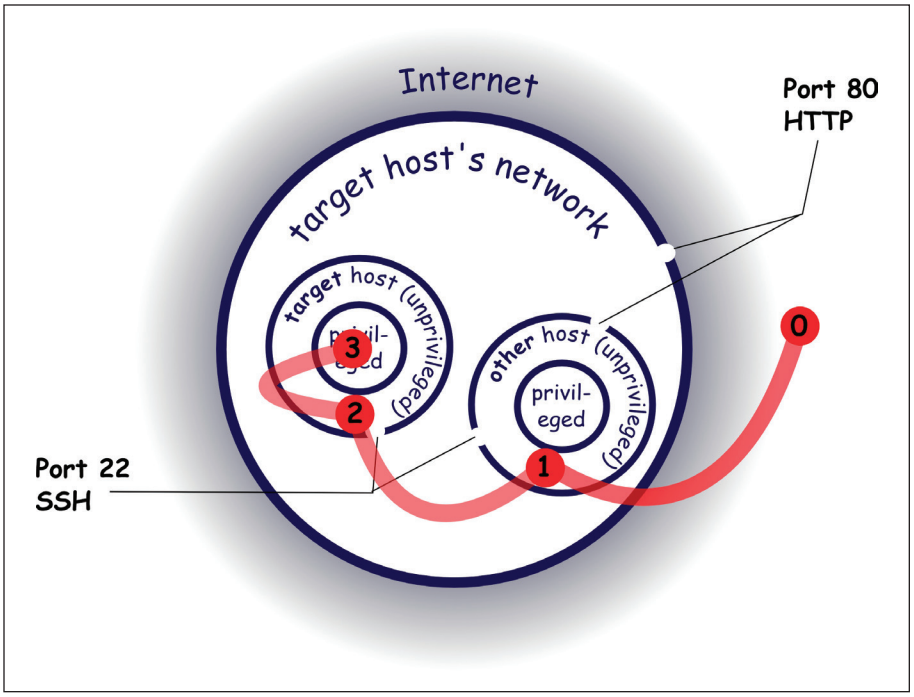


Figure 2. Diagram of a Network and Infiltration Stages

3. Network Reconnaissance Lab

3.1 Introduction

The first of the three capstone labs is the network reconnaissance lab which focuses on the practical application of techniques used to identify weak points in the other team's network. There are two virtual team networks: blue.net and gold.net. Each section is divided into a Gold team and a Blue team and each student is assigned a virtual student host from which to conduct their reconnaissance. The student hosts are running the Backtrack 5 operating system, giving them access to Metasploit, *nmap*, and the denial of service tool Low Orbit Ion Cannon (LOIC). Both networks have 14 hosts: 11 student hosts (enough to permit one host per student on each team), a webserver, nameserver, and file-sharing workstation. The Blue and Gold networks are identical with the same ports open on all of the hosts. The lab exercise lasts for 110 minutes, and upon conclusion, students turn in their individual reconnaissance on a lab worksheet.

All course notes and homework, activities and tools, lab instructions and supplementary materials are made available to students in the sandboxed environment by mirroring the publicly accessible course web site on www.red.net, the instructor VM.

3.2 Learning Outcomes

The first part of the reconnaissance lab is designed to teach the students how to conduct their reconnaissance using the tool *nmap* in a command shell. Prior to this lab, students have developed shell command experience in both Windows and Linux, however the only network scanning and mapping tools they used were *netcat*, *ping*, *traceroute*, and *nslookup*, and typically only used them on single hosts. This lab introduces them to the inefficiencies that exist when using *ping* and *netcat*, in particular, for scanning a block of IP addresses as well as for determining all of the services running on a host. Typically, the instructor works with the students to explain the different *nmap* command options, the results of the scans, and the time required to complete the scans while comparing to the results and time required to use *ping* on a single host, and to use *netcat* for a single port on a single host.

The rest of the lab is designed for each student to independently conduct a more extensive reconnaissance effort on the opponent's network and website. Students access their opponent's websites (see Figures 3 and 4) to search the open-source information in an attempt to find possible usernames, passwords, and other company secrets. On the opponent's home page, they discover the ability to conduct an injection attack in the site's message post tool as well as notice encrypted information. On the second page, students can view the page source to discover email addresses, and therefore usernames since most organizations use the email address username as the network username. Students also discover the system administrator's username, and several pieces of personal information about the users, such as a pet's name, hobbies, and favorite places. Students never gather information about their own classmates' user accounts or hosts, and are instructed to focus their efforts on the three exploitable hosts and the "employees" described on the Blue and Gold websites.

Students are expected to use *nmap* to conduct a *ping* scan of the opponent's network to determine the IP addresses of all hosts in the IP address block. This narrows the scope to 14 IP addresses of the various hosts on each network. Students scan to discover that 11 hosts have port 22 (*ssh*) open with all other ports closed; these hosts represent student machines and are not to be exploited during the lab exercise. After students separate the 11 student IP addresses, they have three hosts left with varying services, which they list in a table in their lab report. Students deepen their scans on the three "target" hosts by determining what version of software is

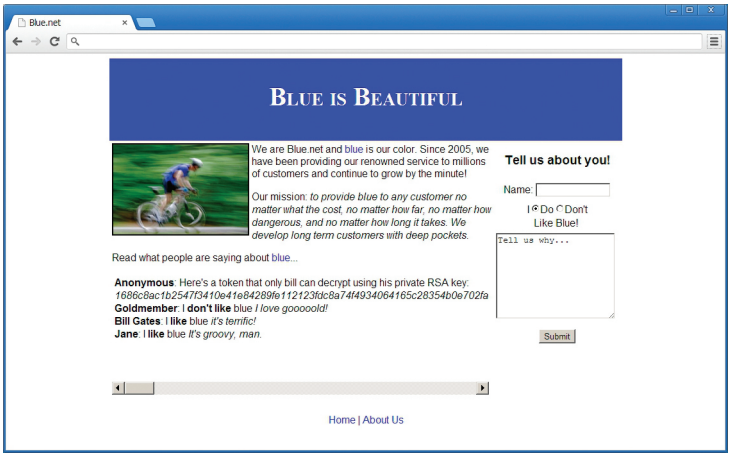


Figure 3. Blue Team's Web Page: index.html

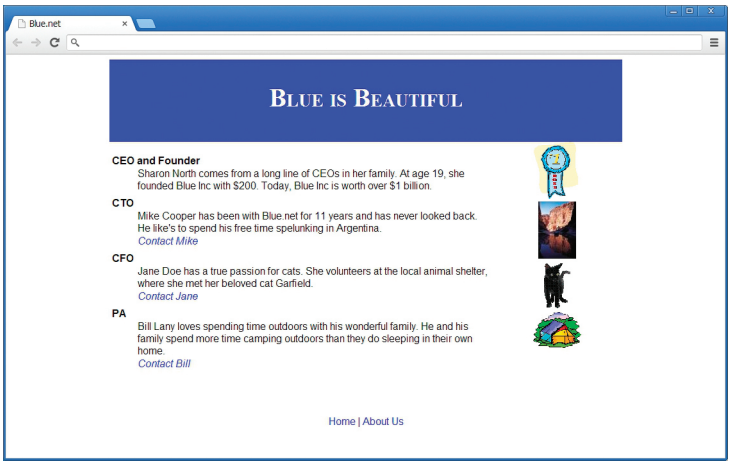


Figure 4. Blue Team's Web Page: aboutus.html

being used for the services and also what operating system family the host is using. They are also expected to use the opponent's DNS server to look up the domain names of the three hosts. Students further explore the network topology using *traceroute*. The entirety of the scans reveals that no firewall is in place on the network.

3.3 Worksheet

While gathering information, the students document the results of their scans and any pertinent information discovered on the opponent's website and they produce a concentric-circle target diagram to display the network topology (see Figure 5).

As expected, students have varying levels of success at gathering the reconnaissance data, and in order to provide all students with the same "starting point" for the network attack lab to follow, the worksheets were graded and returned to the students prior to the network-attack lab, with the corrections and feedback necessary to be able to complete the next lab successfully.

4. Network Attack

4.1 Introduction

The network-attack lab focuses on conducting a limited-in-scope network attack on the opposing team's network.

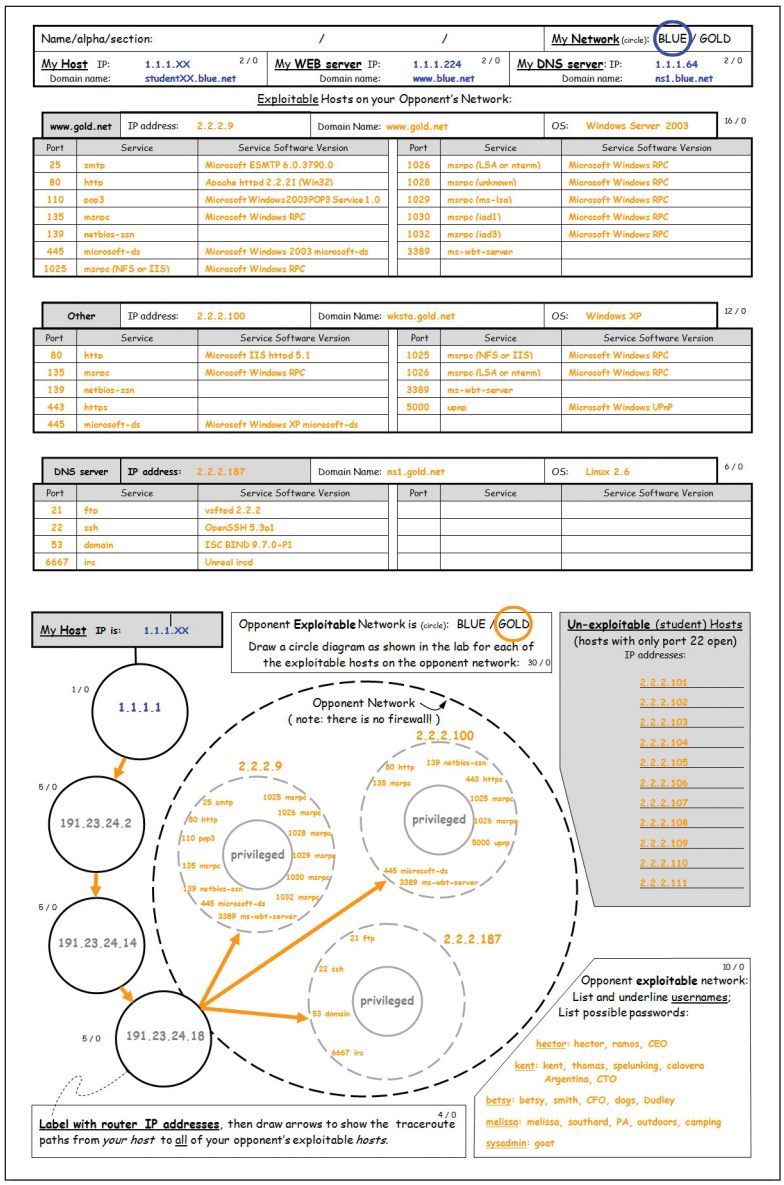


Figure 5. Cyber Reconnaissance Student Completed Lab Report—Example (Two Pages)

The major goals for each team are to conduct denial of service attacks on the opponent's DNS server and webserver, deface the two webpages, and reveal the secrets (called tokens) contained in four files. Minor goals are to create accounts (backdoors), delete files, plant spurious information, and delete access log evidence. The lab runs for 110 minutes as students use their corrected worksheets from the network reconnaissance lab to help them with choices for infiltrating a host, while recording their attack efforts on the network-attack worksheet. At the end of the lab, students turn in their network-attack worksheets.

Due to the wide variety of possible attacks, not every student has the opportunity to take part in every attack, but all students are expected to be busy attempting a subset of possible attacks. Teammates are also expected to brief each other about their individual approaches so that all students become knowledgeable about most aspects of the lab. Each team is assigned a team leader and provided with an IRC chat network to share the information discovered by team members. The team leader is responsible for organizing what team members actually do during the lab and for ensuring all passwords and tokens are documented and shared with all team members. Teams are not allowed to defend their networks during this lab. Due to the virtual nature of the networks, after successful attacks are conducted the instructors can easily reset a virtual host at any time, and as many times as necessary, during the lab so that additional attacks can continue.

In the first part of the lab, each team performs a distributed denial of service attack on their opponent's DNS server using LOIC. In the second part of the lab, individual team members attempt to infiltrate the opposing team's three hosts, as assigned by the team leader, and work towards accomplishing all of the team's major and minor goals.

4.2 Instruction and Navigation

The lab instructions are designed to allow the students to experience different methods of attacking a host and to discover multiple weaknesses that networks can

potentially have. Reinforcing a recurring theme, the students are presented with an interactive lab-navigation tool where they have to first understand what level of access to a host they presently have: none, unprivileged, or privileged, and then they use the interactive tool to display the lab instructions associated with that level of access (see Figure 6).

Figure 6 depicts four possible selections that the student can make for the www host (the web server). The diagram without any highlighting (far left) is the one that is shown on the home page of the lab before the students have started to attack a host. All students start on that page where the basic instructions for the lab are presented. The shading on the arrow, outer ring, and inner circle in the other three diagrams in Figure 6 indicates that the student has selected that level of access to the www host. Each host has its own set of instructions for each level of access. The student has to make the decision, and click the diagram in the lab instructions to explore what to do next.

When students click on the arrow for a host, it is because they have no access to the host and are beginning their attack. A new lab page loads with suggestions for what to try in order to gain remote access to that host. If a student clicks on the outer ring of one of the hosts, then that indicates the student has infiltrated the host but only has unprivileged access. The new page loads with instructions for what kind of information to look for and suggestions for how to escalate privileges to that of root or administrator. When a student successfully infiltrates a host and has root or administrator privileges, the student clicks on the center circle. A new page loads with instructions for accomplishing either the major or minor goals there. It is in this way that the students are guided step by step and at their own pace through the techniques for accessing, infiltrating, and then accomplishing their attack goals.

4.3 Learning Outcomes

As the team members find successful methods of infiltration, such as a vulnerable network service or a username and password combination, they post their findings to the team chat and other team members can then try similar approaches to infiltrate the same host, or a different host. Also, as team members reveal their opponent's secret tokens, the team members copy and paste the tokens into the team chat, allowing all team members to record the tokens on their individual worksheets.

All the students were keenly aware that they needed privileged access to accomplish the majority of their major goals, and many students and teams struggle initially with understanding how to escalate their privileges. Ultimately, the breakthrough comes when the students use Metasploit to attack a network service on the workstation host and gain a meterpreter administrator shell on the workstation. With administrator access, they are able to steal the password file and crack the passwords using the password cracking tool john-the-ripper. The students then discover that the "employees" use the same passwords on multiple hosts on the network and also for the email server. This information opens up several options for accomplishing their goals.

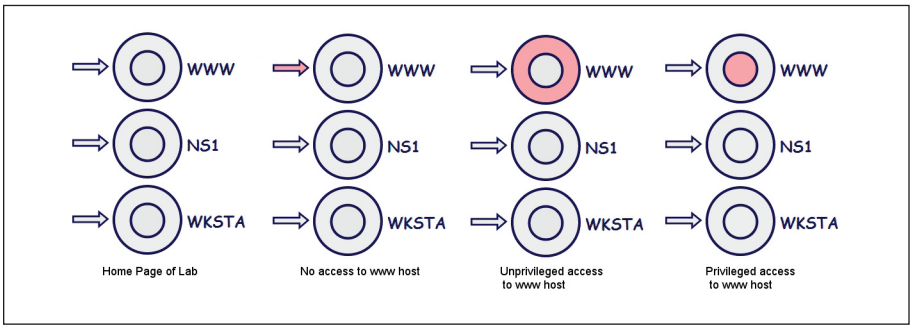


Figure 6. Network Attack Lab Navigation Levels

Two of the four tokens have to be decrypted using tools that the students learned and used earlier in the course, Asymmetric Encryption using RSA, and Symmetric Encryption using AES and an MD5 hashed passphrase. The token encrypted using RSA is publicly shared, but the private key had to be found. Students find it through accessing the user's files, where they find a file storing the public and private RSA keys for that user. The token encrypted with AES is in another user's files and the clue to finding the secret-encryption key is discovered in the user's email. A third token is hidden in an image using steganography and the image is on the website. Students used a steganography tool written by one of the faculty members, that they have previous experience with, to reveal the hidden token. The final token was not encrypted, but file-navigation skills on a UNIX host had to be used to find and display the token.

Although privileged access was not required to gain access to any of the files or emails where clues and tokens were found, usernames and passwords were required. All of the user passwords could be guessed, but most students were only successful at guessing the same one. Since each of the three user accounts afforded access to only one of the token files, having only one user password available resulted in expected frustration until the students attacking the workstation finally cracked and shared the passwords.

As mentioned earlier, having administrator access was the key to accomplishing many of the major goals. The web pages could not be defaced without administrator access to the webserver files. The DNS service could not be disrupted, through poisoning or shutting down services, without root access. Root access to the DNS server was dependent upon hijacking a program on the server that ran with administrator privileges. The students found out how to hijack the program because all of the user email accounts had an email containing the instructions. Figure 7 is a complex diagram for the instructors that depicts the puzzle each team had to work together to solve in order to accomplish the various goals of the lab.

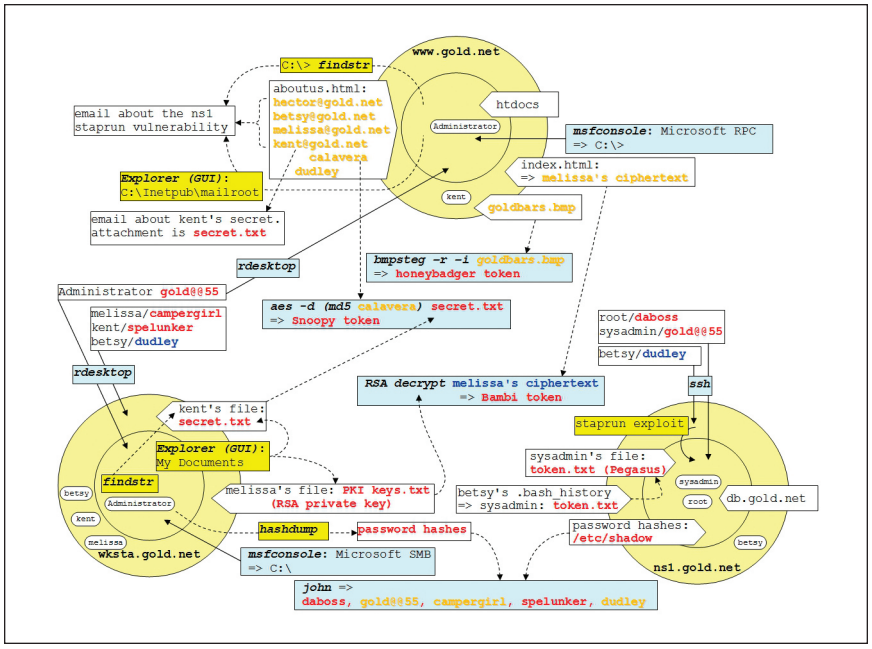


Figure 7. Instructor Diagram to Clues and Major Goals in Attack Lab—Blue Team

Since some of the more proficient students completed all of the goals assigned to them by their team leader, many instructors would either have those students help other students, encourage them to try to infiltrate other hosts in the time that they had left in order for them to gain experience by using different attack approaches, or tell them about a fourth vulnerable host—the team's gateway router, which students soon found out has an unchanged default administrator password.

In the end, all students should have identified several vulnerabilities allowing them to infiltrate the hosts on their opponent's network. These vulnerabilities are the same for both networks, and therefore they know what vulnerabilities they must fix or minimize in the third phase of the capstone lab, the network-defense lab. These vulnerabilities are weak passwords, unpatched servers and operating systems, unnecessary user accounts on hosts, unchanged default passwords, programs vulnerable to hijacking (to escalate privileges), unnecessary services, non-configured firewalls, publically available information, website injection-attack vulnerabilities, and weak protection of sensitive information.

4.4 Worksheet

Throughout the lab, team members track their efforts, both successes and failures, on their own lab worksheet (see Figure 8). They also were expected to share all of their discoveries with teammates, from username/password combinations, to tokens and vulnerabilities discovered.

5. Network Defense

5.1 Introduction

The network-defense lab focuses on the two teams, Blue and Gold, securing their own networks from the vulnerabilities revealed during the network-attack lab. The lab runs for 110 minutes, and students are provided all information for their own network and are instructed what services the network must provide. Throughout the course, the students are taught that the definition of security for an information system is the ongoing ability to provide the services for the system while maintaining the IA pillars. This lab expects the students to rely on their entire semester of knowledge, skills, and experiences to ensure their network is secure. A list of "How to" links are provided in the lab to guide students on managing accounts and passwords, encrypting and decrypting data, protecting against injection attacks on a website, configuring a firewall, shutting down services, removing unnecessary software, and patching known vulnerabilities. After the team leaders tell the instructor that their networks are secure, both teams are allowed to attack their opponent's network to test their security.

5.2 Learning Outcomes

The primary learning outcome for students is an appreciation for how difficult network defense truly is. Students become acutely aware that an attacker only needs to find a single vulnerability to exploit, while a defender must secure all possible vulnerabilities, for every host, and every user. This knowledge of asymmetry for cyber-security is intended to encourage students, as individuals, to do their part in contributing to global cyber-security when they use a computer or digital device.

The team leaders must again organize their team's efforts and typically some team leaders make mistakes in their assignments. For example, a team leader will instruct one student to manage accounts and passwords on the Windows machines and tell another student to work on patching known vulnerabilities. These activities can apply to the same host, which must be accessed via remote desktop—a tool that may not allow more than one connection at a time. Therefore, while one student is in the process of changing passwords or removing user accounts as the administrator, another student logs in to remote desktop to patch the vulnerabilities and either has the wrong password now or bumps off the first user. Usually, the team leader figures out that the best way to organize the team is by host, not by task, or by having one student wait until the other has completed a given task on a host.

The students have four hosts to defend: the webserver, the DNS server, the Windows workstation, and the gateway router. All hosts have accounts and passwords to be removed or updated. The webserver and the workstation operating systems, both Windows, must be patched and software updated as well. The DNS server has an unnecessary software program and an unnecessary service running. The website uses server-side scripts, and

(**Front** of sheet) Do not wait to fill in these tables! Team **Member** worksheet

For each successful attack: *immediately* draw it on the **BACK** side of this sheet

		Attacks I Attempted	**45 / 35 / 20 / 0**
My goal, and target host: Examples: get unprivileged access, elevate privilege, steal info, add a backdoor account, deface a webpage, ...	**What I did to try to achieve this goal:**	**My action attacks this pillar:**	**Success or Failure**
DoS – ns1	*used LOIC*	*Availability*	*S*
priv access - wksta	*beat up Sysadmin to get password*	*Authentication*	*S*
unpriv access - wksta	*guess username SI110, passwords 12345, iloveyou*	*Authentication*	*F*

Tokens Found (ASCII art)		**20 / 15 / 10 / 0**
Description	**Found on host**	**Found using (circle)**
		priv / unpriv / decrypt
		priv / unpriv / decrypt
		priv / unpriv / decrypt
		priv / unpriv / decrypt

Authentication attacks		**10 / 8 / 5 / 0**
Username	**Password**	**Works on these host(s)**

(**Back** of Sheet)

Member Name / Alpha / Section:	/ /	Chat Name:	**10 / 0**
Team: BLUE / GOLD	Draw **YOUR Successful** Attacks (you recorded them on the **FRONT** side of this worksheet)		**15 / 10 / 5 / 0**

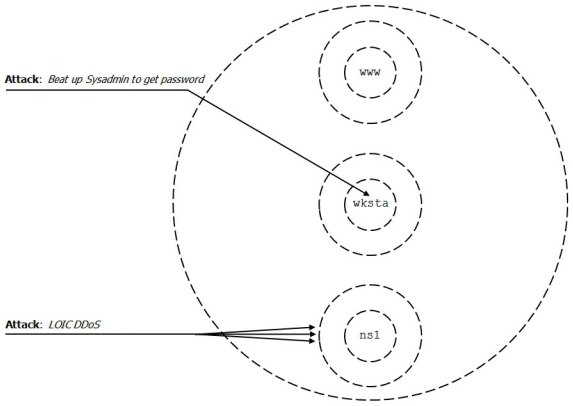


Figure 8. Network Attack Lab Student Worksheet (Two Pages)

the students have to choose between using client-side or server-side validation. Most teams do both, however the instructions do not point out to the students that there are two HTML-form fields which need protecting on the website. The instructions only guide them on protecting one of the fields— leaving a vulnerability that the majority of the defenders and attackers do not consider.

The two encrypted team tokens have to be decrypted and encrypted again with more secure methods to protect the encryption keys. The token hidden using steganography has to be encrypted first and then hidden using steganography. The final token must be encrypted. The firewall configuration is a critical part of the defense lab because this mechanism is the first line of defense on any network. Students working on the router initially begin configuring by trying to block all the ports they know are open on hosts until they realize that at any point someone can decide to open some other port. They then make smart use of the drop all ports to all hosts configuration setting after allowing the services that the network must provide. The firewall configuration must also "limit bursts" on the ports that they are allowing through. This setting will defeat a distributed denial of service attack using LOIC because if an IP address is sending packets too fast to one host on the network, the firewall will block that IP address.

The instructor works on grading the team's accomplishments as they establish their defenses using Figure 9. This worksheet allows the instructor to inform the teams who "wins" on the defense.

5.3 Attacking a "Secure" Network

After the defenses are in place, teams are allowed to attack the other team's network again to test their defenses. Students typically try LOIC and also the attacks that they used in the preceding week's attack lab. If the defense phase has been done correctly, then all of these attacks fail except that some students may be able to conduct an injection attack on the website using the HTML-form field that is not protected—if the student who worked on denying injection attacks did not think to protect the name field. To further emphasize the asymmetry of defense, the instructor provides all students with a link in the virtual hosts that explains how to use Metasploit to attempt a zero-day exploit on the other team's chat server. The exploit works extremely well and grants root access to the other team's DNS server. At that point, the students typically steal the password file and begin to shutdown services, often resorting to the popular command shutdown now.

5.4 Worksheet

The students complete a lab worksheet (see Figure 10) documenting what they secured and how, as well as what attacks they attempted. The worksheet is turned in at the end of lab.

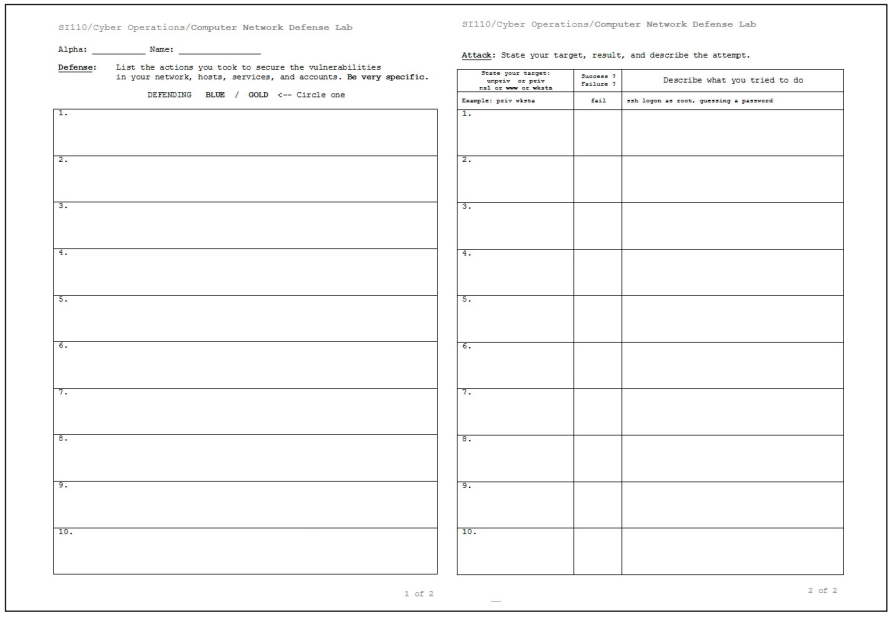
6. Lessons Learned and Recommendations

6.1 Introduction

In this section we describe some of the lessons learned, present some of our assessment data, and discuss the portability of the labs. Instructor preparation for all three lab phases is critical because the labs are technical enough that even a highly

TASK	BLUE				GOLD			
	ns1 token: Bambi	wksta token: Pegasus	www token: honeybadger token: Snoopy	gw	ns1 token: Pegasus	wksta token: Snoopy	www token: honeybadger token: Bambi	gw
Provide needed services	☐ ssh ☐ dns ☐ chat	☐ SMB	☐ web ☐ message post ☐ email		☐ ssh ☐ dns ☐ chat	☐ SMB	☐ web ☐ message post ☐ email	
Provide public info			☐ index.htm ☐ aboutus.htm				☐ index.htm ☐ aboutus.htm	
Change passwords	☐ root ☐ sysadmin	☐ Administrator ☐ bill ☐ jane ☐ mike	☐ Administrator	☐ vyatta	☐ root ☐ sysadmin	☐ Administrator ☐ betsy ☐ kent ☐ melissa	☐ Administrator	☐ vyatta
Stop unneeded services	☐ ftp	☐ IIS			☐ ftp	☐ IIS		
Delete unneeded accounts	☐ jane		☐ sharon		☐ betsy		☐ kent	
Remove unneeded software	☐ staprun				☐ staprun			
Patch the OS		☐ Win XP SP2	☐ WinSrv2K3 SP2			☐ Win XP SP2	☐ WinSrv2K3 SP2	
Protect sensitive information	☐ encrypt Bambi ☐ file perms	☐ new pass phrase ☐ encrypt bill's RSA priv key	☐ encrypt & hide honeybadger ☐ encrypt Snoopy		☐ encrypt Pegasus ☐ file perms	☐ new pass phrase ☐ encrypt melissa's RSA priv key	☐ encrypt & hide honeybadger ☐ encrypt Bambi	
Filter against script injection			☐ server side				☐ server side	
Configure firewall ACL	☐ 53 in ☐ 53 out ☐ 53 rate ☐ 6667 in ☐ 6667 out ☐ 6667 rate		☐ 80 in ☐ 80 out ☐ 80 rate		☐ 53 in ☐ 53 out ☐ 53 rate ☐ 6667 in ☐ 6667 out ☐ 6667 rate		☐ 80 in ☐ 80 out ☐ 80 rate	
	___ of 16	___ of 9	___ of 14	___ of 1	___ of 16	___ of 9	___ of 14	___ of 1
	___ of 40				___ of 40			

Figure 9. Instructor Worksheet for Tracking Team Defensive Tasks



SI110/Cyber Operations/Computer Network Defense Lab

Alpha: _____ Name: _____

Defense: List the actions you took to secure the vulnerabilities in your network, hosts, services, and accounts. Be very specific.

DEFENDING BLUE / GOLD <-- Circle one

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

1 of 2

SI110/Cyber Operations/Computer Network Defense Lab

Attack: State your target, result, and describe the attempt.

State your target: wspstv or priv nal or www or whsta	Success ? Failure ?	Describe what you tried to do
Example: priv whsta	fail	ssh logon as root, guessing a password
1.		
2.		
3.		
4.		
5.		
6.		
7.		
8.		
9.		
10.		

2 of 2

Figure 10. Network Defense Lab Student Worksheet

skilled instructor would not be able to conduct the labs properly without having tried out the labs first. Instructors must be skilled not only in Windows and UNIX environments and lab related software, but also in the setup and shutdown of the virtual environment. Labs must be ready for the next instructor and class, since many of our sections are back-to-back during the day.

Lab assistants would be useful to help with answering student questions, although we did not have the resources for providing assistants to each lab, every period. Many instructors would voluntarily attend the labs of other instructors in their same classroom in order to get more practice themselves, as well as to aid other instructors. Instructors often found themselves bouncing around the room answering questions. Students were unaware that nearly all of them were operating independently, attacking different hosts, and were at different stages than their fellow classmates in the lab. So, when an instructor approached a student, the instructor first had to ask for context: what the student was working on, what the student tried, what errors did the student receive, and so on. For each student with a question, this baseline context first had to be established making the time spent with each student take longer than if all the students were working on the same attacks. Everyone found it important to remind students to follow directions precisely and in the correct order. Sometimes, if students did steps out of order, it was impossible to recover to a midpoint. That is, they would have to start that part over from the beginning.

Each lab supplied a fixed number of activities, and students were usually paired up to accomplish tasks together. Unfortunately, this resulted in some students getting less hands-on experiences. The team leaders, in particular, performed none of the actions to attack or defend since they were directing the actions of the team. Additionally, most students were only attacking or defending one host and therefore did not get experience with other forms of attacking and defending on the other hosts. Hence, most instructors held a lab review at the beginning of the next class period (the day after the lab) in order to expose all students to all aspects of the labs.

We attempted to produce lab instructions that were not prescriptive in the sense that students had some choices as to what they could work on. However, students often found themselves with too many windows open: a Windows shell, a Linux shell, a meterpreter shell, several browsers, and so forth. Thus, they would sometimes execute a command in the wrong shell. Once they understood the context again, they could proceed. We tried to describe the use of commands as much as possible. Some commands were complicated and utilized numerous flags, for example,

aes -e $(head | md5sum | cut -d' ' -f1) -i foo.plain -o foo.cipher

and students were not really sure what the command was doing nor what each flag meant. As best we could, we tried to simplify the commands and provide intuitive ideas of the meanings of the commands, but this area is one where we can still improve.

The worksheets served several purposes. We learned that worksheets were a valuable tool to guide students during the lab, as well as a way of keeping students engaged. In addition, the worksheets provided instructors feedback, so we would know how well the students were succeeding in the labs. The worksheets also allowed us to give the students feedback on their performance, and sometimes fill in missing details—details that may have been required in the succeeding lab.

We noticed that teams worked together more smoothly, as we progressed through the labs. Thus, the labs seemed to teach teamwork. Given the complexity of the labs, it may be worthwhile to have students do more team exercises early on in the course. We also realized that some students are particularly adept at the keyboard. It was not always desirable to have such students assigned as team leaders. Team leaders were in more of a management role and less of a hands-on role. So, taking a key player off the team and putting them in the team-leader role had its tradeoffs. Occasionally, there were students who were overwhelmed by the amount of different things going on in the lab. Students who had not carefully followed the class throughout the semester were forced to rely heavily on their teammates for support. And, students who had not practiced operating systems commands on their own were not able to function efficiently on their team. Taking into account that this course is required of all students at the Naval Academy, instructors were generally pleased by the level of engagement of the students.

6.2 Assessment Data

The labs are a critical part of our course. As such, we tried to measure the success of the labs using a number of different metrics. These assessment measures are also part of our continuous improvement process for the labs. Corresponding to each lab is a lesson designed to prepare the students for the actions to be taken in the labs, as well as to familiarize them with concepts and terminology associated with the lab. There was also a related homework assignment for the lesson. We sampled the homework scores relating to the labs for the fall Academic Year 2013 semester. For the reconnaissance lab the average homework score was 91.9%, for the network-attack lab the average homework score was 91.2%, and for the network-defense lab the average homework score was 80.5%. Instructors tried to return graded homework as soon as possible, so that students could use that feedback in order to succeed more fully in the lab.

We also recorded the average grades for the labs themselves for a sampling of sections for fall 2013. For the reconnaissance lab the average lab grade was 96.4%; for the network-attack lab the average grade was 95.7%; for the network-defense lab the average grade was 98.9%. The high averages associated with homework and labs represent a course perspective that the homework and labs are not the primary tools for student assessment. Exams are intended to measure student knowledge.

On the final exam we included a number of questions that directly related to the labs and cyber operations. Instructors report the individual scores of these questions for each student. During academic year 2012, which was the first year the course was offered, the final exam was the same for both semesters to allow the assessment team a means to compare semester results because there were changes in the way some foundational topics were stressed and reinforced.

For the 2012 final-exam questions concerning the reconnaissance lab, the average problem score was 87.5% in the fall, and 83.2% in the spring; for the 2012 exam questions concerning the network-attack lab, the average problem score in the fall was 88.6%, and the spring average was 83.0%; for the 2012 exam questions concerning the network-defense lab the average problem score in the fall was 85.1%, and the average in the spring was 88.2%. These problem averages are a few points higher than the average problem score for the majority of other problems. So, although this content is perhaps the conceptually most difficult in the class, the students seem to do quite well on this subject relative to other material. And, we hope that part of the reason for their good understanding of the material is the hands-on nature of the labs.

The final exam given for academic year 2013 was different from the previous year, although there were approximately the same number of questions on the final related to the labs and cyber operations. For the 2013 exam questions concerning the reconnaissance lab, the average problem score was 77.9% in the fall, and 83.8% in the spring; for questions concerning the network-attack lab, the average problem score was 75.7% in the fall, and 81.2% in the spring; for questions concerning the network-defense lab the average problem was 72.7% in the fall, and 76.7% in the spring. The lower scores were probably related to a more challenging exam rather than anything else. We will continue to gather data through our assessment process, and also assess the exam questions themselves, so that we can make more valid comparisons from year-to-year. We need to look more carefully at the exam questions in the context of the labs, and see if these lower averages can guide us further in improving the labs.

In addition, at the end of each semester, we conducted a survey of the students to determine how they reacted to the labs and how much the students felt they understood cyber operations. Table 1 presents the questions that we asked the students and the survey results for the questions. In analyzing this data we feel that the majority of our students gained a general understanding about cyber operations and how to conduct basic network reconnaissance, attack, and defense. One of the three capstone-labs (among our total of ten labs) was consistently a favorite for 37–50% of the students, possibly because, as capstone-labs, the students are able to see a convergence of the course content applied directly to cyber operations which reinforced the entire semester. In general, most students felt that the final three labs were a valuable experience,

with 76% or more each semester choosing "very useful" or "somewhat useful" as the survey results in Table 1 indicate. The final question is the strongest indicator of the effectiveness of the labs with 88–90% of students every semester indicating they have a "much better" or "somewhat better understanding of how information systems are attacked and defended."

6.3 Lab Portability

The labs required a significant development effort, and we continue to refine the labs. However, how portable are the labs themselves? The labs required a great deal of technical support and perhaps could be ported to other installations running similar server configurations. Students would not need their own laptops, but could conduct the labs in a fixed computer lab that had workstations or other machines. The ideas presented in the labs, and the basic setup of the labs is portable. But again, one would need to do all the prior work similar to what we do to make the labs work. Otherwise, students would not have the background to conduct or understand the labs. Thus, from a practical point of view, instructors could borrow some of our techniques and ideas, but probably not adopt the labs wholesale. Certainly, using a tool similar to our worksheets could benefit many who are conducting labs.

7. Summary

We have shared information and processes about our three capstone labs from our required-of-all-students fundamentals of cyber-security course. The effort required of faculty and technical-support staff is great. In addition, there is considerable work involved in training new staff and in maintaining the labs. However, the benefits to the students of such labs are immense. When the students are actually able to carry out attacks in a hands-on fashion, in what is a realistic environment, they really seem to internalize the concepts. We hope that others will utilize some of the ideas that we have developed in our labs, and that this paper

TABLE 1. END OF COURSE SURVEY RESULTS PERTAINING TO THE NETWORK-RECONNAISSANCE, ATTACK, AND DEFENSE LABS AND OVERALL COMPREHENSION OF CYBER OPERATIONS

Survey Question	Results		
The final three labs had you doing network recon, attack and defense in a virtual network (via the VSphere client). How useful were these activities in helping you gain a concrete understanding of how information systems get attacked and defended?	Fall AY 2012	Spring AY 2012	Fall AY 2013
	570 students enrolled, 499 responded:	609 students enrolled, 544 responded:	581 students enrolled, 569 responded:
Very useful	41.7%	30.3%	43.7%
Somewhat useful	40.1%	46.7%	40.1%
Of little use	11.8%	17.3%	12.5%
Not at all useful	6.4%	5.7%	3.7%
Which was your favorite lab?	499 responded:	543 responded:	568 responded:
PC disassembly	10.2%	13.3%	15.8%
Build a webpage	25.1%	28.0%	26.6%
Attack the message board	6.8%	8.6%	8.3%
Build a wired network	1.4%	1.3%	.9%
Build a wireless network	2.8%	4.4%	3.5%
Certificates	.4%	0.9%	2.3%
Forensics	3.0%	3.7%	4.7%
Network recon	4.0%	5.0%	6.2%
Network attack	35.1%	22.8%	22.0%
Network defense	11.2%	12.0%	9.7%
The third portion of the course covered "Cyber Operations." Which of the following most accurately describes you at this point in the course:	499 responded:	544 responded:	560 responded:
I have a much better understanding of how information systems are attacked and defended than I did before the course started.	45.3%	41.3%	52.5%
I have a somewhat better understanding of how information systems are attacked and defended than I did before the course started.	43.3%	46.9%	38.9%
I understood a lot about how information systems are attacked and defended than I did before the course started, and haven't learned much new.	2.4%	1.5%	1.6%
I didn't understand much about how information systems are attacked and defended before the course started and I still don't.	9.0%	10.3%	7.0%

facilitates the development of reconnaissance, attack, and defense labs at other institutions. As we continue to gather assessment data and make further improvements to the labs, we hope to keep the community informed of our work. Mostly, we hope that the efforts at USNA to improve the understanding of cyber-security risks, threats, and vulnerabilities among the future leaders in the U.S. Navy and U.S. Marine Corps will inspire other institutions to develop a generic cyber-security curriculum and encourage or require their students to become part of the cyber-security solution, instead of the problem. **Ir**

Acknowledgements
We thank LCDR Mariangel Ibarra for her assistance with reviewing and editing this paper. We thank Christopher Brown for his allowing us to share lab materials in this paper.

References

[1] Anon, "Information Assurance Internship," http://iainternship.com/images/IA_internships_flyer_2013_v2.pdf, 2013. Accessed 2013 July 5.

[2] Brown, W. C. et al. "Anatomy, Dissection, and Mechanics of an Introductory Cyber-Security Class's Curriculum at the United States Naval Academy." ASEE Computers in Education Journal, 3, 3 (2012): 63–80.

[3] Department of Computer Science, University of Maryland. "CMSC 498L/ENEE 459L, Cybersecurity Lab," http://www.cs.umd.edu/class/fall2012/cmsc498L/, 2012. Accessed 2013 July 5.

[4] Jabbour, K. and Older, S. "A Learning Community for Developing Cyber-Security Leaders. The Advanced Course in Engineering on Cyber Security," http://www.cis.syr.edu/~sueo/papers/ace-wecs.pdf, 2010. Accessed 2013 July 5.

[5] Obama, B. "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure." http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, May 2009. Accessed 2013 July 5.

[6] Office of the Dean, United States Military Academy, West Point, New York, "Academic Program: Curriculum and Course Descriptions." http://www.usma.edu/curriculum/RedBook/AY13_RedBook.pdf Accessed 2013 July 5.

[7] Personal communication from Col. David Gibson, the Department Head for Computer Science at USAFA, to Raymond Greenlaw.

[8] Rome Catholic School, Diocese of Syracuse, "Cyber Security K–12 Curriculum." http://www.romecatholic.org/elementary/cyber-security-k-12-curriculum, 2010. Accessed 2013 July 5.

[9] School of Computing, Department of Information Technology, University of South Alabama. "ITE 476 – Network Management Security." http://www.southalabama.edu/bulletin/courite.htm Accessed 2013 July 5.

[10] USNA, "Introduction to Cyber Security Technical Foundations", faculty notes. http://www.usna.edu/cs/si110/ Accessed 2013 July 5.

SARAH STANDARD, RAYMOND GREENLAW, DAVID STAHL, AND JOHN SCHULTZ
United States Naval Academy
572M Holloway Road
Computer Science Department/Michelson Hall, Stop 9F
Annapolis, Maryland 21402 USA
{standard, Greenlaw, stahl}@usna.edu; sublimion@gmail.com

ANDREW PHILLIPS
Office of the Academic Dean and Provost
United States Naval Academy
Nimitz Hall, Mail Stop 10g, 589 McNair Road
Annapolis, Maryland 21402 USA
aphillips@usna.edu

Categories and Subject Descriptors: K.3.2 [Computers and Education]: Computer and Information Science Education – curriculum, information systems education, literacy; K.6.3 [Management of Computing and Information Systems]: Software Management – software selection
General terms: Design, Documentation, Security
Keywords: Cyberspace Policy Review, Cyber-Security Education, Hands-On Laboratory Exercises, Information Assurance, Network Attack, Network Defense, Naval Academy, Network Reconnaissance

DOI: 10.1145/2505990.2506002