2008

Wanted: Trained Security Specialists'

Brent Wilson
George Fox University, bwilson@georgefox.edu

Jim Aman
Saint Xavier University

Josée Bourget

Recommended Citation

Wilson, Brent; Aman, Jim; and Bourget, Josée, "Wanted: Trained Security Specialists'" (2008). *Faculty Publications - Department of Electrical Engineering and Computer Science*. 26.
https://digitalcommons.georgefox.edu/eecs_fac/26

WANTED: TRAINED SECURITY SPECIALISTS[*]

Brent Wilson, M.S.
George Fox University
Newberg, OR. U.S.A.
bwilson@georgefox.edu

Jim Aman, Ph.D.
Saint Xavier University
Chicago, IL. U.S.A.
aman@sxu.edu

Josée Bourget, M.S., C.I.S.S.P.
The Logistics Company, Inc.
Fayetteville, NC. U.S.A.
jbourget@nc.rr.com

ABSTRACT

This paper looks at security concerns within the IT industry and how to increase student interest in this field of study. One specific activity is presented as a way to expose students to security concerns they are likely to encounter as a system administrator.

INTRODUCTION

Only a few areas of computing are growing quickly in student interest. One of these is computer security. Just a few years ago, this was a “fun” area of computing – an interesting sidelight. Penetration testing, information security, and digital forensics were neither well understood by faculty nor widely taught in the discipline. Since 1991, however, threats to all parts of the social environment have come under scrutiny. The world economy is now so tied to electronic commerce that crippling communication capabilities can have serious repercussions. CERT-US, law enforcement agencies at all levels, and numerous governmental agencies now closely monitor electronic threats to their operations and to the national and international infrastructures. Now, all these agencies are seriously seeking people trained in computer security, digital forensics, penetration testing, and other facets of the broad field of computer security.

With this increased emphasis, many colleges have introduced computer security courses or entire programs to their curricula in the past few years. For students, this has meant immediate employment in a very high-demand field with consequently high starting salaries, estimated at $62,500-88,250 in the Robert Half Technology 2007 Salary Guide for an Information Technology Manager or Technical Services Manager with responsibilities in security [1]. Driven by a strong assumption that security is unlikely to lessen in demand in the near future, the attraction to a field which is intellectually demanding, rapidly growing in importance, and pays very well is understandable. Ever pragmatic, graduates who recognize that "the money is in the mystery" [2] where computing is concerned are also making the transition into security.

Of particular appeal to the inquiring person is the variety of jobs, skills, and media involved. Certainly UNIX/Linux experience is necessary (many of the "tools of the trade" are *nix-based), but a sound working knowledge of the various Microsoft Windows operating systems is also required. Penetration testing, in particular, depends upon tools in both these operating system families. Digital forensics can extract information from any hard drive – laptop computer, cell phone, iPod, PDA, even an automobile computer – and demands a broad base of knowledge about the different techniques and underlying virtual structures in each category. Computer security work is ideally suited for the truly inquisitive and the truly patient, but the rewards are great.

ENTERPRISE SECURITY

"The behavior of people plays a principal role in cyber security, and this behavior often supersedes that of any technical safeguards that may be in place" [5]. Computer systems are only as reliable and safe as those who maintain and use them. Safe usage and maintenance are difficult tasks if not properly planned, consistently implemented, and appropriately funded. The question becomes "What makes a good security program in a live environment?" In short, "… a good program cannot guarantee anything. Good programs are not only based on the latest and greatest technology, good programs do not ignore the people component. The goal is to manage an organization's risk." [3]

Typically, the first security problem every system administrator faces is how soon an appropriate program can be in place, rather than how much of a security risk exists. In light of current events throughout the world, it has become painfully obvious that we need to readjust our thinking [6]. New system administrators entering today's professional arena must focus on a type of cultural change… fast is good, but secure is better.

Computer security professionals all agree that no server is ever 100% secure. Anyone who has installed an operating system will agree that default configurations are ambiguous and provide mediocre protection at best. To truly create a level of effective protection requires configuring multiple services and security features to harden the installation. Any given operating system offers numerous possibilities for customization of its services to suit the environment it serves. Because of the multiple possible permutations, numerous potential opportunities exist for attacker exploitation in attempts to corrupt or steal sensitive information. Thus, a dilemma: how far must an organization go in order to reduce risk to an acceptable level, guarantee a level of security which protects corporate IT resources adequately, and still allows the desired level of accessibility to employees?

For a system administrator this means knowing how to harden the operating system to provide a service level which will sustain the users and the organization in a relatively secure environment. Being an effective system administrator involves knowing the vulnerabilities of each supported platform and knowing how to initiate appropriate hardening measures. It also involves ensuring that all measures are taken to enforce company policies and procedures in terms of a minimum security baseline as well as ensuring an uninterrupted IT experience for end-users.

HANDS ON SECURITY FOR STUDENTS

Many schools do not have the faculty or resources to offer a standalone security course. One could argue that security should not stand in isolation but, rather, be incorporated into various appropriate courses across the curriculum. All courses should be examined for ways to integrate some security aspects. A common project evaluation question and cultural mindset needs to be “How much of a security risk is this?”

To begin integrating security, we began with the Network Administration course at George Fox University and defined an activity which allowed students to demonstrate their knowledge of the course material while engaging in various security scenarios. The activity consisted of each student being a system administrator for a Linux machine. Our computer labs are dual-boot so any issues students encounter do not affect the normal operations of the lab. During the second half of the course, students are given “system emergencies” through an executable binary on a weekly basis. For each system emergency, the class is given a scenario such as: “It is Thursday afternoon and we have been hacked. Payroll must be run by tomorrow 2:00pm and our servers are down. You now have 24 hours to find and fix the problems without losing any data.”

During the first system emergency it is not uncommon for students to cause even more damage to the server while trying to fix it. Several students will end up with a re-installation within the 24 hours. Obviously they lose the “leave the data untouched” points. As the course progresses, the students become much better problem solvers. They begin asking themselves questions like “What facts do I know?” and, more importantly, “What facts do I not know?”

SYSTEM EMERGENCY SOURCE CODE

The system emergencies presented below are a representative subset of the type and style given to the students throughout the course.

```
#include <iostream.h>

int main(int argc, char *argv[])
{
    int choice;

    cout << "DO NOT BEGIN SYSTEM EMERGENCIES UNLESS YOU\n";
    cout << "- understand how to use alternative boot methods,\n";
    cout << "- have access to another machine to do research on,\n";
    cout << "- have a lot of free time (relatively speaking),\n";
    cout << "- are not tired, angry, depressed or frustrated.\n\n";
    cout << "Please enter the number to run (99 to exit)";
    cin >> choice;

    switch(choice)
    {
        case 1: /* System hang on boot */
            system("chmod 664 /etc/rc.d/rc.sysinit");
            break;

        case 2:  /* No one is allowed to login to server */
            system("sed -i.backup -e 's/bash/nologin/'
/etc/passwd");
            system("rm -f /etc/passwd.backup");
            break;

        case 3: /* No network connectivity */
            system("sed -i.backup -e 's/10.10.10/10.10.11/'
                /etc/sysconfig/network-scripts/ifcfg-eth0");
            system("rm -f /etc/sysconfig/network-scripts/ifcfg-
eth0.backup");
            break;

        case 4: /* No home directories */
            system("mv -f /home /tmp/house");
            break;

        case 5: /* Constant reboot - run level 6 */
            system("sed -i.backup -e
's/id:5:initdefault:/id:6:initdefault:/'
                /etc/inittab");
            system("rm -f /etc/inittab.backup");
            break;

        case 6: /* pseudo-random rebooting */
            system("mkdir /etc/cron.minutely");
            system("touch /etc/cron.minutely/logger");
            system("echo '#!/bin/sh' >> /etc/cron.minutely/logger");
            system("echo 'reboot' >> /etc/cron.minutely/logger");
            system("chmod 755 /etc/cron.minutely/logger");
            system("echo '0,7,15,28,32,48 * * * * root run-parts
                /etc/cron.minutely' >> /etc/crontab");
    }

    if (choice != 99)
    {
        /* delete this program & reboot */
        system("rm -f system_emergency");
        system("reboot");
    }

    return 0;
}
```

Case 1 –

The first system emergency removes the executable permissions to the `rc.sysinit` file which controls the boot process. The machine will hang on boot up, a somewhat helpful error message will scroll by during boot before the machine hangs if the students are paying attention.

Case 2 –

This emergency takes anyone who has their default shell set to `bash` in the `passwd` file and changes it to `nologin`. The effect is that no user has the ability to log into the server.

Case 3 –

This emergency changes the network configuration for the default Ethernet card in `ifcfg-eth0`. The code above changes the network address from 10.10.10.x to 10.10.11.x. All network packets can no longer be sent from or received by the server. The server had addressing for 10.10.11.x and yet it is sitting on the 10.10.10.x network. If effectively has a bad address on the network.

Case 4 –

This emergency moves the entire home directory structure to `/tmp/house`. No users other than root will have a home directory when they log in. Students who log into the server as root will not see this one initially because it does affect the root user.

Case 5 –

This emergency changes the run level to 6. A run level of 6 will create a continual reboot loop. An additional modification to this emergency is to change the run level to 0. A run level of 0 will immediately shut down the server upon boot up.

Case 6 –

This emergency is one of my favorites. It creates a `cron` job called `logger`. Students will overlook this job because it "makes sense" to have a `cron` job logging something. This `cron` job reboots the server every hour on the hour along with every 7, 15, 28, 32, and 48 minutes past each hour. Students will see this emergency as intermittent because they will not connect it to time.

CONCLUSION

Security continues to be a major concern among IT professionals. Advances in wireless technology and mobile devices have created even more concerns within the profession. There is increasing need for security professionals in virtually every domain in today's society. It is apparent that we do not have enough individuals to supply the demand. To increase students' interest in security, they need to be exposed to security concepts and concerns continually throughout their education.

REFERENCES

[1] *Occupational Outlook Handbook.* http://www.bis.gov/oco/ocos258.htm.

[2] Jeff Duncan (VeriSign, Inc.) in comments as a guest lecturer to a computer science class at Saint Xavier University, Fall, 2007.

[3] D. Ochs, *Network Security: The First Line of Defense for BCP and DRP*. Fortrex

Technologies, Inc. 2002.

[4] R. Panko, *Corporate Computer and Network Security*, Upper Saddle River, NJ: Prentice Hall Pub. 2004.

[5] L., Volonin, S.R. Robinson. *Principles and Practice of Information Security*, Upper Saddle River, NJ: Prentice Hall Pub. 2004.

[6] B. Wiedman. *Database Security (Common-sense Principles).* http://www.governmentsecurity.org/articles/DatabaseSecurityCommon-sensePrinciples.php